



SECURE COMMUNICATIONS ■

What's New

high security remote access

NCP Secure Enterprise Client (Windows 32/64 Bit)

Neue Features der Major Releases 9.23 bis 8.0

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Inhalt

Neue Features der Version 9.23 gegenüber Version 9.21	2
Neue Features der Version 9.21 gegenüber Version 9.10	6
Neue Features der Version 9.1 gegenüber Version 9.00	10
Neue Features 9.1 zu 9.03	10
Neue Features 9.03 zu 9.02	11
Neue Features 9.02 zu 9.00	12
Neue Features 9.0 gegenüber 8.3	13
Neue Features 9.0 zu 8.31	13
Neue Features 8.31 zu 8.30	16
Neue Features 8.3 gegenüber 8.1	18
Neue Features 8.30 zu 8.11	18
Neue Features 8.11 zu 8.10(SP1)	20
Neue Features 8.10(SP1) zu 8.10	20
Neue Features 8.10 gegenüber 8.0	21
Neue Features 8.1 zu 8.05	21
Neue Features 8.05 zu 8.00	22

Wichtige Hinweise:

- Die mit einem "k" gekennzeichneten Features sind kostenpflichtig, d.h. zu dessen Nutzung muss ein neuer Lizenzkey erworben werden.
- Features die in älteren Versionen bestimmten Betriebssystemen zugeordnet sind, wurden natürlich auf die neuesten 32-/64-Bit-Plattformen übernommen
- Kunden mit älteren Versionen wenden sich bitte an marketing@ncp-e.com.

Neue Features der Version 9.23 gegenüber Version 9.21

FIPS inside

Der Secure Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat 1051).

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

Erweiterung der Konfiguration für die Hotspot-Anmeldung (ab V. 9.21 B. 62)

In der Konfiguration für die Hotspot-Anmeldung kann jetzt zusätzlich zur Anwendung für die Hotspot-Anmeldung eine weitere Anwendung eingetragen werden. Über diese weitere Anwendung erfolgt die eigentliche Kommunikation, da sie Verbindungen nach außen herstellen kann. Diese Anwendung wird durch eine interne, anwendungsbezogene Firewall-Regel überwacht.

Sind beide Anwendungen identisch (Hotspot-Anmeldung und Kommunikation), so kann der Parameter "Anwendung für automatische Firewall-Regel" leer gelassen werden.

Die Hotspot-Konfiguration erfolgt über das Monitor-Menü "Konfiguration / Hotspot" die Firewall-Regel wird erstellt über "Konfiguration / Firewall".

Icon für NCP VPN Path Finder Technology

Wurde die Verbindung mit der VPN Path Finder Technology 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 ebenso wie in der Oberfläche der Windows-Anmeldung über NCP GINA oder NCP Credential Provider.

Sprachauswahl

Im Ansichts-Menü unter "Sprache" kann die Sprache für die Monitor-Oberfläche ausgewählt werden. Zur Verfügung stehen: Englisch, Deutsch und Französisch. Polnisch und Niederländisch wurden entfernt. Als Setup-Sprache stehen Englisch, Deutsch und Französisch zur Verfügung.

Statusanzeigen des SMS-Centers

Im Verbindungsmenü des Clients kann der Kurznachrichtendienst des SMS-Centers aktiviert werden, sofern die Treiber einer Mobilfunkkarte für GPRS / UMTS, die SMS unterstützt, auf dem Rechner installiert sind. (Der Menüpunkt "Mobilfunkkarte" muss im Verbindungsmenü des Monitor erscheinen).

Nach der Aktivierung erscheint im Client-Monitor ein Briefsymbol. Mit einem Klick auf dieses Briefsymbol kann das SMS-Center künftig geöffnet werden.

Zur Bedeutung der Farbsymbole:

Ein Brief-Symbol in der Farbe Rot symbolisiert, dass das SMS-Center über das Verbindungsmenü des Monitors aktiviert wurde, aber kein geeignetes Modem zur Verfügung steht. Die Farbe Gelb symbolisiert die GPRS / UMTS-Netzsuche, eine fehlerhafte Karte, eine fehlende SIM PIN etc., begleitet von entsprechenden Meldungen im Tool Tipp. Grau zeigt die Bereitschaft zum SMS-Empfang an. In Grün werden empfangene SMS symbolisiert. Die Anzahl nicht gelesener SMS kann im Tool Tipp abgelesen werden.

Verwendung der VPN-Zugangsdaten für die Windows Logon-Optionen

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

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

Alternativ können für die Windows-Anmeldung auch eigene Zugangsdaten eingesetzt werden.

Suffix für VPN-Benutzernamen

Als ein neuer "Tunnel-Parameter" kann in den Profil-Einstellungen ein "VPN-Suffix" eingegeben werden.

Der "VPN-Suffix" erleichtert die Mandanten-spezifische Einrichtung von Benutzergruppen mit dem Secure Enterprise Management (SEM).

Der Administrator kann zentralseitig für den "VPN-Suffix" oder den "VPN-Benutzernamen" auch eine Umgebungsvariable, z.B. %userdomain% oder %username%, vorkonfigurieren. Diese Variable wird dann aus den Settings des Client-PCs ausgelesen und automatisch als "VPN-Suffix" verwendet.

Der Benutzername für die VPN-Einwahl setzt sich dann zusammen aus "VPN-Benutzername" plus "VPN-Suffix", wobei beim Aufbau einer VPN-Verbindung vom Benutzer nur der "VPN-Benutzername" eingegeben werden muss. Anhand des Suffix erkennt das Gateway die Benutzergruppe.

Umgebungsvariable USERNAME:

Der String der Umgebungsvariable USERNAME wird dann als VPN-Suffix verwendet wenn im Feld für "VPN-Suffix" %username% eingetragen ist. Ist die Umgebungsvariable in den Settings des Client-PCs nicht vorhanden, wird der Eintrag %username% aufgelöst verwendet.

Initialisierung des NCP Secure Enterprise Clients bzw. der NCP Dynamic Personal Firewall

Der Initialisierungsprozess wurde durch die alternative Verwendung von Windows-Umgebungsvariablen am Client erweitert. So kann der Administrator für den Benutzer und den Authentisierungscode nun auch Umgebungsvariablen vorkonfigurieren, um den Client am zentralen Management zu authentisieren. Eine weitere Interaktion durch den Anwender ist hierfür nicht notwendig. Der Rollout der am Client-Rechner im Hintergrund arbeitenden NCP Dynamic Personal Firewall wird dadurch weiter vereinfacht.

Erkennen funktionsfähiger Mobilfunkkarten

Sofern das SMS-Center aktiviert wurde oder ein GPRS / UMTS-Profil selektiert wurde, meldet der Client wenn die Mobilfunkkarte entfernt wird und schließt das GPRS / UMTS-Panel. Wird eine funktionsfähige Mobilfunkkarte gesteckt, wird das GPRS / UMTS-Panel wieder geöffnet und das Netz erneut gescannt.

Die Reihenfolge der Suche nach verfügbarer GPRS / UMTS-Hardware wurde so angepasst, dass zunächst entfernbare und dann integrierte Hardware gesucht wird.

Zusätzliche Unterstützung weiterer GPRS / UMTS-Hardware.

Erweiterung der Attributtypen zur Zertifikats-Überprüfung

Benutzer bzw. Aussteller können in ihren Zertifikaten verschiedene Einträge anlegen. Diese Einträge können im entsprechenden Feld des angezeigten Zertifikats nachgelesen werden. Diese Einträge können vom Secure Client auch zur Überprüfung eingehender Zertifikate verwendet werden.

Dazu öffnen Sie das Konfigurationsfeld "Zertifikats-Überprüfung" in der jeweiligen Profil-Einstellung und geben das Attribut ein, das Ihnen von der Server-Seite her bekannt gegeben wurde. Damit ist sichergestellt, dass vom Client nur eine Verbindung zu genau dem Server aufgebaut werden kann, dessen Zertifikat im Benutzer- oder Ausstellerfeld das entsprechende Attribut enthält.

Die Liste der bisher verfügbaren Attribute wurde um die Seriennummer des Benutzers bzw. Ausstellers (sn) im eingehenden Zertifikat erweitert. (Dabei handelt es sich nicht um die Seriennummer des Zertifikats.)

VMware-Gastsysteme schützen

Ein VMware-Gastsystem kann bei aktivierter Firewall eines im Hauptsystem installierten Clients geschützt werden. D. h. die Firewall des Clients am Hauptsystem muss entweder in der "gesperrten Grundeinstellung" aktiv sein, oder in der "offenen Grundeinstellung" muss mindestens eine Firewall-Regel aktiv sein.

Eingehende Verbindungen auf das Gastsystem sind dann nicht möglich.

VMware bietet verschiedenen Modi für das Gastsystem an: Bridged, NAT und Host only. (Im Host only-Modus ist unabhängig von der Firewall grundsätzlich ausschließlich eine bidirektionale Kommunikation mit dem Hauptsystem möglich.)

Bridged-Modus:

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

NAT-Modus:

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

Eine Kommunikation zwischen Gastsystem und Hauptsystem ist weiterhin bidirektional möglich.

"VMware-Gastsysteme schützen" kann in den Firewall-Einstellungen des Clients über das Konfigurationsmenü des Monitors in den "Optionen" aktiviert werden.

NCP Firewall Status im Windows Center einsehbar

Ist die Firewall des NCP Secure Enterprise Clients aktiv so wird deren Status an das Windows Vista Security-Center bzw. Windows 7 Wartungs-Center gemeldet und kann dort eingesehen werden. (Für Windows Vista muss mindestens Service Pack 1 installiert sein.)

Dynamische Umschaltung der Filterregeln bei negativem Endpoint Security Check

Gemäß der Richtlinien der Endpoint Security wird nur den Endgeräten Zugriff auf das Firmennetz gestattet, die diese Richtlinien erfüllen. Die Prüfung gemäß der Richtlinien findet zum ersten Mal während des Verbindungsaufbaus zum Gateway statt. Werden die Richtlinien nicht erfüllt, kann der Client in einer Quarantänezone gehalten werden, die der Secure Enterprise Server (entsprechend seiner Konfiguration) dafür bereitstellt. Dort hat der Anwender (entsprechend der Richtlinien-Konfiguration) die Möglichkeit, Updates auf seinen Rechner zu laden. Werden die Richtlinien der Endpoint Security nach dem Einspielen der Updates erfüllt, so erhält der Client Zugriff auf das Firmennetz indem der Secure Server die Quarantänezone durch dynamisches Umschalten der Filterregeln öffnet.

Während der Dauer der VPN-Verbindung finden nach konfigurierterm Intervall weitere Endpoint Security-Prüfungen statt. Schlägt eine folgende Prüfung fehl, weil z. B. in der Zwischenzeit am Client PC ein Virens Scanner deaktiviert wurde, werden die Filterregeln vom Secure Server wieder so zurückgesetzt, dass die VPN-Verbindung wieder nur auf die Quarantänezone beschränkt ist.

Voraussetzung für diese dynamische Rückschaltung während einer VPN-Verbindung auf die Quarantänezone ist ein NCP Secure Enterprise Server ab der Version 8.05 sowie ein NCP Secure Client ab der Version 9.23.

Fehlerbehebungen

Datenaustausch über VPN-Tunnel bei UMTS-Verbindung über Windows 7-Schnittstelle

Betrifft nur UMTS-Verbindungen, sofern der UMTS-Hardware-Treiber auf die neue unter Windows 7 eingeführte Mobile Broadband-Schnittstelle zugreift. In diesem Fall konnten unter dem Betriebssystem Windows 7 keine Daten über den VPN-Tunnel ausgetauscht werden, wenn die Internet-Verbindung über UMTS / Mobile Broadband bestand aber nicht vom Client aufgebaut worden war. Dieser Fehler ist nun behoben.

Kein VPN-Tunnel in einem bekannten Netz

In der Firewall-Konfiguration der bekannten Netze kann die Option gewählt werden, dass ein VPN-Verbindungsaufbau im bekannten Netz nicht zugelassen wird. Ist diese Option selektiert, kann weder über das Verbindungsmenü noch über den Verbinden-Button im Client-Monitor eine VPN-Verbindung hergestellt werden. Allerdings war der Verbindungsaufbau über die Kommandozeile der RWSCMD.EXE weiterhin möglich.

Dieser Fehler ist behoben, sodass bei der entsprechenden Einstellung in der Firewall-Konfiguration auch über RWSCMD keine Verbindung aufgebaut werden kann, wenn sich der Client in einem bekannten Netz befindet.

Fehlerhafte Auswertung von Zertifikaten ohne Angabe der Zeitzone

Zertifikate mit fehlerhafter Zeitangabe (ohne Angabe der Zeitzone) wurden vom Client auch nach Ablauf der Gültigkeit als gültig angesehen.

Schwachstelle in NCP Secure Client

Der NCP Secure Client hat sich als anfällig gegenüber eines als DLL-Hijacking bezeichneten Angriffs erwiesen. Dieser Angriff nutzt eine Schwäche in der Abarbeitung des Ladevorganges von DLLs unter Windows aus.

Diese Schwachstelle wurde mit Patches behoben. Weitere Informationen und Download unter: http://www.ncp-e.com/fileadmin/pdf/service_support/NCP_Client_Vulnerability_Statement.pdf

Neue Features der Version 9.21 gegenüber Version 9.10

Windows 7 Support (k)

Das neue Microsoft Betriebssystem Windows 7 wird ab der Version 9.2 ohne Einschränkungen unterstützt. Damit kann der NCP Secure Entry Client unter allen 32-/64-Bit Windows Betriebssystemen genutzt werden: Windows XP, Windows Vista, Windows 7.

(Hinweise: Ab der Version 9.2 entfällt der Support für Windows 2000. Die Installation auf Windows 7 erfordert einen Produktschlüssel der Version 9.2. Im Falle eines Updates von Windows Vista auf Windows 7 lässt sich bei einem Client der Version 9.2, der mit einem 9.1-er Schlüssel lizenziert wurde, nur der Monitor starten um die Eingabe eines 9.2-er Schlüssels zu ermöglichen.)

Nutzen

Unterstützung aller aktuellen Windows Arbeitsplatz-Betriebssystem unter einer einheitlichen Benutzeroberfläche.

VPN Path Finder inkl. Proxy-Support (k)

Die NCP VPN Path Finder Technology bewirkt ein automatisches Umschalten auf ein alternatives Verbindungsprotokoll (TCP Encapsulation mit SSL Header über Port 443), wenn Standard IPsec über Port 500 bzw. UDP Encapsulation über einen frei konfigurierbaren Port nicht möglich ist. (In Verbindung mit NCP Secure Server 8.0.)

Nutzen

Der Anwender hat auch bei beschränktem Zugang ins Internet (auf den HTTPS-Zielport 443) die Möglichkeit sich via IPsec-Tunneling mit dem Firmennetz zu verbinden.

WLAN-Roaming

Bewegt sich der Teleworker mit seinem Laptop innerhalb des Empfangsbereichs mehrerer Accesspoints mit derselben SSID, so wird im Falle einer schlechten WLAN-Empfangsleistung automatisch auf einen stärkeren Accesspoint gewechselt. Anwendungen die über den VPN-Tunnel kommunizieren „merken“ davon nichts.

Nutzen

Der NCP Secure Entry Client kann innerhalb von Firmennetzen zwischen verschiedenen Accesspoints wechseln (z.B. bei Standortwechsel mit Laptop), ohne eine neue Datenverbindung aufbauen und sich neu am VPN Gateway anmelden zu müssen. D.h. kontinuierlichen Remote Access trotz wechselnder IP-Adresse.

Verbesserter Datendurchsatz auf 64 Bit Windows Plattformen.

Der Datendurchsatz konnte durch die Optimierung (RWSNT-Dienst) um ca. 20% erhöht werden.

Unterstützung der neuesten Intel WLAN Treiber Version 12.4.0.21 und höher.

Die neuen Treiber stellen sich nicht mehr als Ethernet- sondern als WLAN-Treiber dar. Das erfordert ggf. eine Deinstallation des bisherigen NCP Secure Entry Clients. Die Neuinstallation kann nach dem Reboot durchgeführt werden, wobei alle bisherigen Einstellungen erhalten bleiben.

Unterstützung der neuen Windows 7 Mobile Broadband Treiber (3G/UMTS).

Überarbeitete 3G/UMTS-Konfiguration, Providerliste ist über INI-Datei (APN.ini) konfigurierbar

Das Konfigurationsmenü wurde umbenannt in GPRS / UMTS (Darin wird auch die UMTS-Konfiguration überarbeitet).

Es existieren nun drei Varianten:

- a) Providerliste (Standardeinstellung)
bei der Auswahl des Providers werden der Access Point Name (APN) und die Einwahlnummer vorgeschlagen.
- b) APN von SIM Karte
es wird kein APN an die SIM-Karte weitergegeben und setzt voraus, dass ein APN in der SIM-Karte konfiguriert ist.
- c) Benutzerdefiniert;
der Anwender kann alle Einwahlparameter manuell konfigurieren.

Nutzen

Die GPRS/UMTS-Konfiguration wurde für den Anwender weiter vereinfacht.

Modularisierung des NCP Secure Enterprise Clients

Der NCP Secure Enterprise Client lässt sich durch Auswahl bei der Installation für einen Testzeitraum wahlweise als NCP Dynamic Personal Firewall oder NCP Secure Enterprise Client installieren. In beiden Fällen wird immer die komplette Software auf dem Zielsystem installiert. Die NCP Dynamic Personal Firewall besitzt bis auf VPN-Funktionalität alle Funktionalitäten der Software und stellt dem Anwender eine zentral administrierbare Firewall zur Verfügung. Über den Produktschlüssel ist festgelegt welche der beiden Varianten, NCP Dynamic Personal Firewall oder NCP Secure Enterprise Client, Verwendung findet.

Anwender die die Vorteile einer zentral administrierbaren Firewall inkl. Friendly Net Detection nutzen möchten, jedoch keine VPN Funktionalität benötigen, können diese Lösung nun erwerben und lizenzieren.

Ein späteres Upgrade auf den vollständigen Enterprise Client ist mit dem entsprechenden Lizenzschlüssel möglich.

Einsetzen des CSP Benutzer-Zertifikatsspeichers

In der Zertifikatskonfiguration (im Monitormenü unter Konfiguration/Zertifikate/Benutzer-Zertifikat) kann als Benutzerzertifikat auch ein Zertifikat aus dem Windows Zertifikatsspeicher eingesetzt werden. Wählen Sie den "CSP Benutzer-Zertifikatsspeicher" in der Listbox, so wird zur erweiterten Authentisierung das Zertifikat aus dem CSP Benutzer-Zertifikatsspeicher verwendet, dessen "Subject CN" und "Issuer CN" Sie in die entsprechenden Felder eintragen.

Da diese Funktionalität erst nach einer Anmeldung des Benutzers am Windows-System zur Verfügung steht, kann sie nicht zur Domänenanmeldung über VPN eingesetzt werden!

SMS-Center

Mit dem SMS-Center (Monitormenü unter Verbindung / SMS-Center) können Kurznachrichten auf komfortable Weise verschickt und empfangen werden. Dadurch lässt sich z.B. eine komfortable Authentisierung an Hotspots mittels Einmalpasswörtern realisieren.

Das SMS-Center kann unabhängig von einer Internet- oder VPN-Verbindung genutzt werden. D. h. parallel zu einer Internet- oder VPN-Verbindung kann das SMS-Center geöffnet bleiben und Nachrichten gesendet oder empfangen werden.

Überarbeitung WLAN GUI und Feldstärkemessung, Tray Icon

Ist „WLAN“ im Client aktiviert, erscheint in der Taskbar das zugehörige Tray Icon. Dieses Icon zeigt für den aktuellen Verbindungsstatus die Feldstärke und Verschlüsselungsart an. Nach einem Mausklick auf das Tray Icon werden alle verfügbaren WLANs angezeigt. Durch die Auswahl eines bestimmten WLANs wird der Verbindungsaufbau gestartet oder, sofern noch kein WLAN-Profil für dieses Netz besteht, der WLAN-Verbindungsassistent gestartet. Der WLAN-Assistent erleichtert die Profil-Erstellung und automatisiert den Verbindungsaufbau zu einem neuen WLAN. Die Verschlüsselungsart (WEP, WPA, WPA2) wird dabei automatisch erkannt.

Nutzen

Das WLAN-Handling wurde für den Anwender weiter vereinfacht.

Statusanzeige beim Scannen von WLANs und beim Verbindungsaufbau (animierte Grafik)

Ist WLAN aktiviert so wird periodisch nach allen verfügbaren WLANs gescannt. Während des Scanvorganges ist das entsprechende Icon animiert. Ein Verbindungsaufbau zu einem Accesspoint wird durch einen blinkenden, gelben Punkt, links neben der gewählten SSID des WLANs, angezeigt.

Ein grüner Punkt zeigt die bestehende WLAN-Verbindung an. Verwenden mehrere WLAN-Accesspoints dieselbe SSID, so erscheint neben der SSID zusätzlich ein kleines rotes Dreieck.

Nutzen

Das WLAN-Handling wurde für den Anwender weiter vereinfacht.

Profil-Export

Das aktuell ausgewählte Profil kann mittels dieser Funktionalität exportiert und bei einem anderen NCP Secure Entry Client importiert werden. Zertifikate müssen allerdings separat kopiert werden.

Nutzen

Der Anwender kann sein VPN Profil auf einfachste Weise von einem Rechner auf einen weiteren übernehmen.

Budgetmanager mit Historie für die letzten zwölf Monate

Dem Anwender stehen bei Bedarf alle relevanten Informationen seiner Datenkommunikation innerhalb der letzten zwölf Monate zur Verfügung.

Vodafone Websessions Unterstützung

Easy-to-Use auch für Vodafone-User. Der Anwender kann sich mit nur einem Klick auf „Verbinden“ an Vodafone Websessions anmelden und den VPN-Tunnel aufbauen.

Erweiterte Option des Konfigurationsassistenten für „Neue Profile“

D.h. direkter Import von Konfigurationsfiles. Hierzu besteht unter „Neue Profile“ die Option, ein neues Profil direkt einer Gruppe zuzuordnen.

Modernisierung der Benutzer-Oberfläche

Die grafische Benutzeroberfläche wurde weiter optimiert und den Markterfordernissen angepasst. Wesentliche Anpassungen sind:

- Einheitlicher Verbinden/Trennen-Schalter
- Optische Abgrenzung des NCP Secure **Enterprise** Client vom NCP Secure **Entry** Client
- Weltkarte in Abhängigkeit der Zeitzone
In Abhängigkeit der am Rechner konfigurierten Zeitzone wird ein entsprechender Ausschnitt der Weltkarte angezeigt: Europa, Amerika, Asien/Australien.

Verbessertes Log-Handling.

Bei Markierung einer Zeile im Monitor „Log“ stoppt das Log. Das erleichtert die Durchsicht und Überprüfung von Log-Ausgaben direkt im Monitor erheblich.

Beschleunigung des Verbindungsaufbaus

Das wird durch ein optimiertes Verhalten des Clients im getrennten Zustand im DHCP-Modus und manuellem Verbindungsaufbau erreicht.

Erweiterung der Encryption- und Hash Optionen.

Diffie-Hellmann-Gruppe 14, SHA-256, SHA-384 und SHA-512.

Weitere Änderungen:

- Die Konfigurationsgruppe "VPN IP Networks" heißt nun "Split Tunneling".
- Optimierte Darstellung der verfügbaren WLAN Netze.
- Setup Routine ist auch in Französisch und Polnisch verfügbar.
- Die maximale Anzahl der remote VPN Netze wurde auf 250 erweitert.
- IPsec Optimierungen: Weitere Verbesserung der Kompatibilität.
- Entlastung des Systems durch Optimierung der Personal Firewall bei Verwendung anwendungsbezogener Regeln.
- Verbessertes Menü-Handling bei der Sprachauswahl.
- Fehlerbehebung innerhalb der Diffie Hellman-Berechnung bzgl. Padding und Montgomery Reduktion.

Neue Features der Version 9.1 gegenüber Version 9.00

Neue Features 9.1 zu 9.03

Budget Manager (k)

Der Budget Manager dient zur Überwachung der Verbindungskosten über verfügbaren Verbindungsarten. Im Fokus stehen UMTS-, GPRS- und WLAN-Verbindungen. Hierzu werden per Konfiguration Volumen- bzw. Zeitlimits vorgegeben. Der Anwender kann bereits vor einer Überschreitung der vorgegebenen Limits durch Hinweise gewarnt werden. Abhängig von den Einstellungen können weitere Verbindungsaufbauten bei überschrittenen Schwellwerten verboten werden.

Ein weiterer Vorteil des Budget Managers, neben der Kostenkontrolle, ist das Einschränken bzw. Unterbinden von Roaming.

Erweiterte Zertifikatskonfiguration (k)

In der Konfiguration des Clients kann nun eine Vielzahl individueller Zertifikateinstellungen hinterlegt werden. Diese können dann innerhalb der Zielsysteme unabhängig von einander ausgewählt werden, sodass die Möglichkeit besteht gegen verschiedene VPN-Gegenstellen mit unterschiedlichen Zertifikaten zu authentifizieren, z.B. zu VPN Gateway 1 mit Softzertifikat und zu Gateway 2 mit einem auf Smartcard gespeicherten Zertifikat.

Profil-Filter (k)

Die konfigurierten Zielsysteme können zu Gruppen zusammengefasst werden, die dann über ein Kontextmenü des Client Monitors bequem ausgewählt werden können. Dadurch kann die Übersichtlichkeit der vorhandenen Verbindungsprofile für den Anwender erhöht werden, da er nur die aktuell gewünschten Einträge einblenden lassen kann.

WISPr-Unterstützung

Mittels WISPr (Wireless Internet Service Provider Roaming) unterstützt der Client zukünftig die browserlose Anmeldung an T-Mobile Hotspots in Deutschland (inkl. ICE-Zügen der Deutschen Bahn), Österreich, Tschechien, Niederlande und Großbritannien, sowie in Lufthansa Lounges größerer internationaler Flughäfen. Die Benutzer-Informationen werden in der Client-Konfiguration hinterlegt und An- und Anmeldung am Hotspot können mit der VPN-Verbindung gekoppelt werden.

Client Status Info Center

Mit dem Client Status Info Center lässt sich der User Helpdesk optimieren. Die Log- und Fehlermeldungen sind in ihrer Aussagekräftigkeit verbessert.

Neben einer Testoption zur Bestimmung einer ggf. vorhandenen Internetverbindung (im LAN- und WLAN-Umfeld), steht zusätzlich eine Übersicht mit folgenden Informationen zur Verfügung:

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

Software Update über LAN (k)

Das Software Update ermöglicht grundsätzlich die Verteilung aktueller (NCP) Software sowie Konfigurationen und zugehöriger Dateien (z.B. Softzertifikate) über das NCP Secure Enterprise Management. Mit Version 9.1 ist dies auch ohne eine bestehende VPN-Verbindung z. B. im LAN möglich. Weiter werden umfangreiche Konfigurationsoptionen zur Verfügung gestellt, um z.B. Updates bei langsamen Verbindungen zu vermeiden.

Roaming mit IPSec-Verbindungen

Wird dem Client während einer Session mit wireless LAN- oder LAN-Verbindung über DHCP eine neue IP-Adresse zugewiesen, so übernimmt der Client diese und sendet eine IKE Notify-Meldung (NCP-spezifisch) an das VPN Gateway um den Adresswechsel mitzuteilen. Die IPSec-Verbindung wird währenddessen nicht unterbrochen d.h. muss nicht neu aufgebaut werden. Voraussetzung: NCP Secure Server >= 7.02 Build 25.

iPass – CLI-Unterstützung für Credential-Übergabe

Benutzername und Kennwort für iPass-Verbindungen können nun auch über ein im iPass Client integriertes CLI-Tool übergeben werden. Voraussetzung hierfür ist eine entsprechende Version des iPass Clients.

Verbessertes UMTS-Karten-Handling

Das Verhalten des Secure Clients in Verbindung mit UMTS-Karten wurde weiter verbessert, insbesondere nach Rückkehr des Systems aus dem Standby, bei Fehlverhalten oder Nichtverfügbarkeit einer Karte. Darüber hinaus erkennt der Client bei mehreren aktiven UMTS-Geräten automatisch das Device mit gesteckter SIM-Karte.

Erweiterung der GUI um die Sprache "Französisch".

[Neue Features 9.03 zu 9.02](#)

Windows 64 Bit Betriebssysteme (k)

Für den Einsatz der Client Software unter den Windows Betriebssystemen XP und Vista 64 Bit sowie Vista 32 Bit wird ein Lizenzschlüssel ab der Version 9.0 benötigt.

Treibersignierung für Windows 2000, XP und Vista

Der NCP Intermedia-Treiber wurde für die aktuellen Windows-Betriebssysteme signiert.

CSP Unterstützung für Smart Cards und Tokens (k)

In der Zertifikatskonfiguration des Clients kann als Benutzer-Zertifikat auch CSP (Cryptographic Service Provider) verwendet werden.

Zertifikate im Benutzer-Zertifikatsspeicher können NICHT verwendet werden.

Zertifikatskonfiguration mit Entrust-Profil

Das Entrust-Profil kann mit Hilfe eines Platzhalters in der Zertifikats-Konfiguration aus dem aktuellen Benutzerverzeichnis gelesen werden.

Neue Features 9.02 zu 9.00

Silent-Installation

Für die automatisierte Einrichtung von PCs mittels Stapelverarbeitung ohne Benutzereingaben kann eine fensterlose (silent) Installation mittels einer NCP-eigenen Funktion angestoßen werden. Anstatt für jede neue Version der Client Software eine neue "Setup.iss" (Mechanismus von Installshield) zu erstellen, kann die automatisierte Installation mit Hilfe der Datei "SetupExt.ini" vordefiniert werden.

Endpoint Policy

Die Verbindungsart des Clients kann über die Endpoint Policy Enforcement abgefragt werden. Dazu wird in der Richtlinie eine Konstante verwendet, welche die entsprechende Verbindungsart angibt.

Werte:

- 0 = ISDN
- 4 = Modem
- 8 = LAN
- 10 = PPPoE (PPP over Ethernet)
- 14 = PPPoC (PPP over CAPI)
- 15 = Externer Dialer (iPass)
- 16 = PPTP
- 18 = GPRS/UMTS
- 20 = WLAN

Parametersperren über ein OneTime Password öffnen

Die Parametersperren können am Client über ein Einmalpasswort geöffnet werden. Nach einer Konfigurationsänderung durch den Benutzer, verliert das Passwort seine Gültigkeit, damit ein erneuter Zugriff auf die Konfiguration nach einem Monitor-Neustart nicht mehr möglich ist.

Parameter-Sperren für WLAN-Profile

Für WLAN-Profile kann über die Management-Console für jeden einzelnen Parameter eine Parametersperre gesetzt werden. Dadurch ist es möglich, die Update-Funktion "Nur gesperrte Parameter ändern" einzusetzen (wie bei den Zielsystemen). So kann beispielsweise die Verschlüsselung für das WLAN vorgegeben und die SSID durch den Benutzer selbständig angepasst werden.

Voraussetzung: Management Console 1.04 Build 54

Unterstützung von Zertifikaten mit 4096 Bit Schlüssellänge

Für die Benutzer-Authentisierung können Server- und Client-seitig Zertifikate mit einer Schlüssellänge von 4096 Bits eingesetzt werden.

Hardware-Zertifikat in "Microsoft CSP" (k)

In der Zertifikats-Konfiguration unter Hardware-Zertifikat wurde der Typ "Microsoft CSP" hinzugefügt. Um das Zertifikat nutzen zu können, muss es vorher in den Microsoft Cryptographic Service Provider importiert worden sein.

Dieser Parameter kann mit folgender Management-Console konfiguriert werden: Version 1.04 Build 045, Client PlugIn Version 9.00 Build 4 (für Management Console 2.0)

Benutzer-Authentisierung mittels Zertifikat ohne PIN-Eingabe

Zur Benutzer-Authentisierung ohne PIN-Eingabe kann ein Hardware-Zertifikat verwendet werden, sofern es ausschließlich und ohne Benutzerzertifikat eingesetzt wird. Bei dem Hardware-Zertifikat entfällt die Eingabe einer PIN.

Benutzersperren für EAP

Die Parameter des EAP-Konfigurations-Dialogs können über das Secure Enterprise Management einzeln gesperrt werden.

Voraussetzung: Management Console 1.04 Build 038

Neue Features 9.0 gegenüber 8.3

[Neue Features 9.0 zu 8.31](#)

Unterstützung von Windows Vista (k)

Mit der Version 9.0 des NCP Secure Enterprise Clients wird neben den Betriebssystemen Windows 2000 und Windows XP auch Windows Vista in den Varianten 32 Bit und 64 Bit unterstützt.

Für die Windows-Betriebssysteme Windows NT, Windows 98 und Windows ME erfolgt kein Support mehr, d.h. NCP übernimmt keine Gewährleistung über die volle Funktionsfähigkeit der Client Software unter diesen Betriebssystemen.

Hinweis:

Die Client Software 9.0 erfordert bei der Installation unter Windows Vista einen Lizenzschlüssel 9.0. Eine Nutzung mit einem älteren Lizenzschlüssel (<9.0) ist nicht möglich.

Neue Benutzeroberfläche (Monitor)

Die Oberfläche des Clients wurde dem Betriebssystem Windows Vista optisch angepasst. Der mit Symbolen unterlegte funktionale Ablauf von Verbindungsaufbau, Verbindungsabbau und Authentisierung wurde in seiner Darstellung noch übersichtlicher. Hinweistexte (Tooltips) erklären die einzelnen Symbole und erleichtern die Fehlersuche im Störfall. Der Status der integrierten Personal Firewall wird im Icon innerhalb der Taskleiste dargestellt.



Firewall-Einstellungen

Die Einstellungsmöglichkeiten der Firewall, im Monitormenü unter "Firewall-Einstellungen", wurden weiter verfeinert und hinsichtlich der „bekannten Netze“ erweitert. Für "bekannte Netze" wurden die Rubriken "Manuell", "Automatisch" und "Optionen" eingeführt.

Die manuelle Definition eines bekannten Netzes durch den Administrator und die automatische Erkennung eines bekannten Netzes mittels Friendly Net Detection können gleichzeitig genutzt und über die Registerkarten "Manuell" und "Automatisch" konfiguriert werden.

Unter der Optionen-Rubrik kann festgelegt werden, dass kein zusätzlicher VPN-Tunnelaufbau mehr möglich ist, wenn sich der Client bereits im bekannten Netz befindet.



Ist die Option "VPN-Verbindungsaufbau im bekannten Netz nicht zugelassen" eingeschaltet, wird der Button für den Verbindungsaufbau (bzw. der Menüpunkt) im Client-Monitor deaktiviert. Eine bereits bestehende VPN-Verbindung, die möglicherweise durch eine andere Anwendung hergestellt wurde, kann jedoch getrennt werden. Für den Fall, dass sich der Client bereits im bekannten Netz befindet, können die Logon-Optionen zur Domänen-Anmeldung ausgeblendet werden. Dazu muss die Funktion "Logon-Optionen im bekannten Netz ausblenden" aktiviert werden.

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

(Diese Einstellungen können über die Management-Console des Secure Enterprise Managements ab V 1.04 Build 24 vorkonfiguriert werden.)

Die Grundmodi der Firewall werden bei einem Tooltip auf das System Tray Icon als Quick-Info angezeigt, sodass schnell erkennbar ist, ob die Personal Firewall (FW) oder die Link-Firewall (LFW) aktiv oder inaktiv ist und ob sich der Client in einem bekannten oder unbekanntem Netz befindet. Sowohl am Tray Icon als auch am Applikations-Icon ist außerdem eine aktive Firewall in rot erkennbar, mit Friendly Net in grüner Farbe.

WLAN-Panel

Die Anzeige des WLAN-Panels kann so konfiguriert werden, dass sie permanent den aktuellen WLAN-Status anzeigt, unabhängig vom genutzten Übertragungsmedium. Der Teleworker hat damit die Möglichkeit, laufend die Feldstärke zu überprüfen und damit den Zustand seiner WLAN-Verbindung zu überprüfen um das Verbindungsmedium ggf. zu wechseln.

Automatische Erkennung des angeschlossenen PC/SC-Smartcard-Lesers

Ist für die starke Authentisierung die Verwendung eines Zertifikats am Client konfiguriert, so erkennt der NCP Client automatisch den angeschlossenen PC/SC-Kartenleser. Das vereinfacht das zentrale Management. So ist in der zentralen Zertifikats-Konfiguration kein benutzerspezifischer Chipkartenleser mehr vorzukonfigurieren. Die Benutzer können bei Bedarf verschiedene PC/SC-Kartenleser an ihrem Telearbeitsplatz einsetzen.

Hinweis:

Dieses Feature ist nur nutzbar in Verbindung mit Smartcards, die ohne Schnittstellen-Software direkt angesprochen werden können (z. B. TCOS, Netkey von Telesec und TC Trust).

Erweiterte Konfigurationsmöglichkeiten des Clients mit der Management Console des Secure Enterprise Managements ab V 1.04

Sperre, so dass der Benutzer den Monitor nicht beenden kann.

- Erweiterungen der Parametersperren: Lizenzinformationen können wenn gewünscht vom Benutzer nicht mehr ausgelesen werden.

Endpoint Policy – Message Box für den Benutzer

Automatische Anzeige von zentral vorgegebenen Meldetexten in einer Message Box.

Beispielsweise. „Der Virenschanner hat veraltete Signaturen und wird automatisch aktualisiert. Bitte starten Sie nach Beenden Ihren PC neu“

Sperren des Ad-hoc-Modus bei WLAN-Profilen

Ad-hoc Abfragen sind eine flexible Möglichkeit, um schnell auf Daten eines fremden Rechners zuzugreifen. D.h. dieser Modus wird vom Microsoft Betriebssystem auch in WLAN-Umgebungen standardmäßig unterstützt. Bei mobilen Telearbeitsplätzen sind solche PC-PC-Verbindungen grundsätzlich aus sicherheitstechnischen Gründen zu unterbinden. Der NCP Client kann innerhalb der WLAN-Profile entsprechend eingestellt werden, so dass eine PC-PC-Verbindung über WLAN nicht möglich ist.

Vereinfachte Eingabe von Benutzernamen- und Kennwort-Dialogen

Um die Benutzerfreundlichkeit weiter zu erhöhen, wurden Benutzernamen- und Kennworteingabe in einem Dialog zusammengefasst, falls diese nicht bereits in der Konfiguration hinterlegt sind.

Integrierte Unterstützung weiterer Multifunktionskarten (Mobile Connect Cards)

Ist eine Multifunktionskarte gesteckt, die vom Client erkannt wurde, wird im Monitormenü "Verbindung" der Menüpunkt "Multifunktionskarte" sichtbar.

Zu den bereits unterstützten Multifunktionskarten* sind neu hinzugekommen:

- integrierte Karte des Lenovo Notebooks (Sierra Chipset)
- Vodafone EasyBox USB-Adapter für UMTS/GPRS.

Über den Menüpunkt "Multifunktionskarte" stehen folgende Funktionen zur Verfügung:

- Netzsuche
- UMTS bzw. GPRS aktivieren
- SIM PIN eingeben bzw. ändern

Die Funktionen "Netzsuche" und "UMTS bzw. GPRS aktivieren" können auch über das Feld zur grafischen Anzeige der Signalstärke ausgelöst werden. Dieses Feld wird immer dann geöffnet, wenn ein Profil mit der Verbindungsart "UMTS/GPRS" aus den Profil-Einstellungen selektiert wurde.

Der PIN-Dialog zur Eingabe der SIM PIN erscheint immer dann, wenn in einem Profil der Mediatyp "UMTS/GPRS" konfiguriert und eine Multifunktionskarte gesteckt wurde, die der Client erkennt.

*) siehe Kompatibilitätsliste unter: <https://www.ncp-e.com/de/support/kompatibilitaeten/umts-3g-hardware.html>

Erweiterter Schutz des Telearbeitsplatzes durch UDP-Filter

In den Firewall-Einstellungen des Monitormenüs kann ein UDP-Filter eingestellt werden, der verhindert, dass bei gestartetem Client - unabhängig von der Firewall - UDP-Pakete ausgefiltert werden. So wird eine UDP-Verbindung von außen auf den Telearbeitsplatz verhindert.

Neue Features 8.31 zu 8.30

Betriebssysteme

Mit der Support-Abkündigung von Microsoft wird auch NCP den Support für Windows NT 4.0, Win 95, Win98 und WinMe einstellen. Davon betroffen sind die aktuelle Version des NCP Enterprise Client, zukünftige Versionen des NCP Entry Clients, die Server Management-Console (für den Secure Enterprise Server) und der Server Manager (für das Secure Enterprise Management System) sowie der Secure Enterprise Server und der Secure Enterprise Management Server unter WinNT.

Weitere UMTS/GPRS Karten

Unterstützung der integrierten Karte des Lenovo Notebooks (Sierra Chipset) und der HUAWEI E620

Löschen des Telefonbuchs

Das Löschen des Telefonbuchs durch den Benutzer ist auch nach einem Update auf diese Version und dem ersten Speichern des Telefonbuchs nicht mehr möglich.

EAP-Zugangsdaten aus Zertifikat

Bei EAP-TLS (mit Zertifikat) kann der EAP-Benutzername direkt aus der Zertifikats-Konfiguration bezogen werden.

EAP-Authentisierung

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

- Deaktiviert
- Für alle Netzwerkkarten
- Nur für WLAN-Karten
- Nur für LAN-Karten

Hinweis:

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

EAP-Authentisierung vor der Zielauswahl bei Einsatz der Gina

Unter den "Logon-Optionen" des Monitor-Menüs wurde der Parameter "EAP-Authentisierung vor Zielauswahl durchführen" hinzugefügt. Ist dieser Parameter aktiviert, wird vor dem Zielauswahl-Dialog in der Gina die EAP-Authentisierung durchgeführt und nach der erforderlichen PIN gefragt, unabhängig davon, ob zur späteren Einwahl EAP benötigt wird oder nicht. Dieser Parameter kann z.B. dann verwendet werden, wenn die NCP Gina nur für die EAP-Authentisierung verwendet werden soll, ohne dass eine Verbindung zu einem Zielsystem aufgebaut wird (Verwendung als reiner EAP-Client).

EAP für WPA-Verschlüsselung (k)

Im Monitormenü kann unter "Konfiguration / WLAN-Profil" für die WPA-Verschlüsselung unter "Schlüsselverwaltung" die Option "EAP" hinzugefügt werden. Vorausgesetzt, es wurde ein Zertifikat konfiguriert. Unabhängig von der EAP-Konfiguration wird hier immer EAP mit Zertifikat genutzt.

Zertifikatsüberprüfung bei HTTP-Authentisierung mit Script (k)

Ab sofort können auch die eingehenden Zertifikate bei der HTTP-Authentisierung überprüft werden. Hierzu muss im Script die Variable CACERTDIR gesetzt worden sein. Desweiteren sind auch Inhalte des WEB Server-Zertifikats überprüfbar.

Stimmt der Inhalt der Variable mit dem eingegebenen Zertifikat nicht überein, wird keine SSL-Verbindung aufgebaut und eine Log-Meldung im Monitor ausgegeben.

Erweiterung der IPSec Hash-Algorithmen

Sowohl für die IKE-Richtlinien als auch für die IPSec-Richtlinien können zur Authentisierung die Algorithmen SHA 256, SHA 384 und SHA 512 Bit eingesetzt werden.

Anwendungsausführung für spezifischen Telefonbucheintrag

Im Konfigurations-Menü des Monitors können unter "Verbindungssteuerung / Ext. Anwendungen" Programme eingetragen werden, die nach dem Verbindungsaufbau automatisch gestartet werden. Zusätzlich lassen sich diese auszuführenden Anwendungen auch an einen bestimmten Telefonbucheintrag binden. Der Dialog, aus dem die verfügbaren Ziele auswählbar sind, ist mit einer Combo-Box versehen.

Hinweis:

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

Lokale Anmeldung mit GINA

Die Anmelde-Option "Lokal anmelden" kann als Standard-Wert über den Client Version 8.31 bzw. die Management-Console 1.04 Build 8 vorkonfiguriert werden. In der NCP GINA ist als Standard-Wert normalerweise die Anmelde-Option "Domänen-Anmeldung über eine VPN-Verbindung" gesetzt.

Dies ermöglicht eine Anmeldung an einer Windows-Domäne über ein VPN. Die Benutzerschnittstelle wurde bezüglich Handhabung und Optik überarbeitet.

Firewall-Friendly Networks

Es wird unterschieden, ob Firewall-Konfigurationen vom Enterprise Management vorgegeben werden oder manuell angelegt wurden. Nur Einträge, die bereits über das Enterprise Management angelegt wurden, werden bei einem Konfigurations-Update vom Management-System überschrieben. Zusätzlich kann über die Management-Console ab Version 1.04 Build 5 angegeben werden, ob alle oder nur die vom Management-System vorkonfigurierten Friendly Networks überschrieben bzw. gelöscht werden sollen.

WLAN-Automatik (k)

Mit der Version 8.31 steht eine intelligente WLAN-Automatik zur Verfügung, über die im Hintergrund das passende Profil für das aktuell vorliegende WLAN eingesetzt wird.

Hotspot-Anmeldung

Die HotSpot-Anmeldung der 2. Generation erfolgt über das Monitor-Menü "Verbindung / HotSpot-Anmeldung" und erlaubt in der erweiterte Konfiguration die Einstellung eines alternativen Browsers und einer Default Startseite welche bei bestehender Internet Verbindung aufgerufen wird. Der alternative Browser lässt sich speziell für die Anforderungen an HotSpots konfigurieren, d.h. es wird kein Proxy Server konfiguriert und alle aktiven Elemente (Java, Javascript, ActiveX) werden deaktiviert. (Der alternative Browser ist nicht Bestandteil der Client Software!) Darüber hinaus kann der MD5-Hash-Wert der Browser-Exe-Datei ermittelt und in das Feld "MD5-Hash" eingetragen werden. Auf diese Weise wird sichergestellt, dass nur mit diesem Browser eine HotSpot-Verbindung zustande kommt.

Im Client kann ein Projekt-Logo hinzugefügt werden

Das Logo erscheint in einem Panel des Clients ganz unten und über die gesamte Breite des Monitors. Für das Logo muss eine Ini-Datei (ProjectLogo.ini) angelegt werden. Eine Beispiel Ini-Datei befindet sich im Installationsverzeichnis.

Erweiterung der GUI um die Sprache "Holländisch".

Verfügbare Verbindungsarten

Im Monitor-Menü unter "Verbindung" kann ein Informationsfenster zu den verfügbaren Verbindungsarten geöffnet werden. Dieses Fenster dient ausschließlich der Benutzerinformation über die zur Verfügung stehenden Verbindungsarten und die aktuell genutzte. Werden wechselweise unterschiedliche Verbindungsarten genutzt, so erkennt der Client automatisch, welche Verbindungsarten aktuell zur Verfügung stehen und wählt davon die schnellste aus. Die zur Verfügung stehenden Verbindungsarten werden mit gelber Signallampe dargestellt, die ausgewählte Verbindungsart mit einer grünen.

Externe Anwendungen vor Windows-Anmeldung

Über den Menüpunkt "Logon-Optionen" im Monitormenü "Konfiguration" können externe Anwendungen (Consolen-Anwendungen oder Batch-Dateien, keine Windows-Programme!) auch mit der NCP Gina gestartet werden:

- vor Verbindungsaufbau starten (precon)
- nach Verbindungsaufbau starten (postcon)
- nach NCP Logon starten (immer)

Letztere Startoption gestattet das Starten von Anwendungen nach der EAP-Verhandlung über die NCP Gina und anschließender "lokaler Anmeldung" ohne VPN-Verbindung.

Neue Features 8.3 gegenüber 8.1

Neue Features 8.30 zu 8.11

Integrierte WLAN-Konfiguration (für Windows 2000/XP) (k)

Die WLAN-Karte ist direkt ansteuer- und konfigurierbar. Die Installation der Managementsoftware kann entfallen. Für den User erfolgt unter dem grafischen Feld des Monitors ein weiteres Feld mit zusätzlichen Anzeigen für Feldstärke, Provider etc.

Automatische Medienerkennung (k)

Der Client erkennt automatisch die aktuell zur Verfügung stehenden Verbindungsarten und wählt die jeweils schnellste aus. Die manuelle Auswahl eines Mediums aus den Telefonbucheinträgen erübrigt sich. D.h. Easy-to-use bei oft wechselnden Übertragungsmedien.

Friendly Net Detection (FND)

Friendly Net Detection ist eine integrierte Funktion der Personal Firewall im NCP Client und dient der automatischen Erkennung eines "Friendly Net". Was ein „Friendly Net“ ist, bestimmt der Administrator in den Firewall-Einstellungen. Easy-to-use für den Anwender, denn er muss sich nicht um die Einstellung der Personal Firewall kümmern. In Abhängigkeit von der jeweiligen Kommunikationsumgebung greift der NCP Client auf das passende Firewall-Regelwerk zu. Versehentliche oder absichtliche Fehlbedienungen sind ausgeschlossen. Attacken auf das Firmennetz sind ausgeschlossen. Das Ende-zu-Ende-Sicherheitsprinzip zur Durchsetzung der Security Policies bleibt uneingeschränkt wirksam. Alle Parameter können optional durch das zentrale Management administriert werden.

Statusanzeige der FND und Endpoint Policy im Client Monitor

Bei Aktivierung des Features FND wird im Client Monitor, für den User ersichtlich das ansonsten rote Firewall-Icon grün eingefärbt.

Wenn zwischen Client und VPN Gateway Sicherheitsrichtlinien festgelegt sind, die es vor dem Zugriff auf das Firmennetz zu erfüllen gilt, erfolgt im Client Monitor eine zusätzliche Anzeige in Form eines Endpoint Policy-Icons. Während der Überprüfung der Sicherheitsrichtlinien erscheint das Icon mit gelben Haken, der bei Erfolg grün erscheint. Ist nur eine Richtlinie nicht erfüllt, wechselt der Haken in rot. Für diesen Fall stehen dem Administratoren verschiedene Konfigurationsoptionen zur Verfügung.

Unterstützung weiterer Chipkarten

Folgende Chipkarten werden zusätzlich über die PC/SC- oder CT_API-Schnittstelle unterstützt:

- Signtrust
- NetKey 2000
- TC Trust
- Telesec PKS SigG

Externe Anwendungen

Im Rahmen der Verbindungssteuerung können Anwendungen (Consolen Anwendung oder Batch-Dateien) auch mit der NCP GINA vor der Windows-Anmeldung gestartet werden. Weiter kann definiert werden, wann diese gestartet werden sollen:

- vor Verbindungsaufbau
- nach Verbindungsaufbau
- nach Verbindungsabbau

Sind mehrere Batch-Dateien nacheinander auszuführen, sorgt die „Wait-Funktion“ (Warten bis Anwendung ausgeführt und beendet ist) für einwandfreien Betrieb.

Hotspot-Anmeldung mit externem Dialer

Unabhängig vom integrierten NCP Dialer kann der Client so konfiguriert werden, dass die Anmeldung an einem Hotspot über einen externen Dialer erfolgt.

HTTP-Authentisierung (k)

Die "HTTP-Authentisierung" gestattet eine verbesserte automatisierte, scriptgesteuerte Anmeldung mobiler User an Hotspots (und DSL), wenn der Access Point einen HTTP-Redirect ausführt. In diesem Fall entfällt die Eingabe von Benutzername und Passwort im Browserfenster. Die Authentisierungsdaten für dieses Zielsystem werden automatisch aus den WLAN-Einstellungen übernommen. Die Authentisierung erfolgt über ein entsprechendes Script. Eine Message-Box weist den Benutzer darauf hin, dass diese Verbindung gebührenpflichtig ist und er die Vertragsbedingungen des Hotspot-Betreibers akzeptiert.

Neue Features 8.11 zu 8.10(SP1)

Erzwingung der Endpoint Sicherheitsrichtlinien (k)

In Verbindung mit dem zentralen Management kann ein VPN so eingerichtet werden, dass überprüfbar ist, ob die Endpoint Sicherheitsrichtlinien auch wirklich eingehalten werden. Abweichungen werden nicht zugelassen.

Die Sicherheits-Richtlinien beinhalten alle sicherheitstechnischen Vorgaben vom Secure Enterprise Management. Bei jedem Verbindungsaufbau eines Clients zum Firmennetz wird die Endpoint Policy heruntergeladen. Bei Abweichungen können unterschiedliche Meldungen und Aktionen an zentraler Stelle erfolgen. (Siehe hierzu die Beschreibung „NCP Secure Enterprise Management“).

Sicherung der PIN-Benutzung ("PIN-Abfrage bei jedem Verbindungsaufbau")

Um auszuschließen, dass ein unbefugter Benutzer bei einer bereits eingegebener PIN eine unerwünschte Verbindung aufbaut, kann der Client so konfiguriert werden, dass bei jedem Verbindungsaufbau erneut eine PIN eingegeben werden muss.

Unterstützung weiterer Chipkarten

NetKey Chipkarte mit Siemens Chip SLE66CX322P

Erweiterung der Anzahl konfigurierbarer VPN IP-Netze

Die Anzahl der konfigurierbaren Netze wurde auf 20 erhöht.

VPN-Etablierung nach erfolgreicher EAP-Verhandlung

Dieses Feature ist immer dann von Bedeutung, wenn ein Access Point das Extensible Authentication Protocol (EAP) erfordert. Bei erfolgloser EAP-Authentisierung wird kein VPN-Tunnel aufgebaut.

EAP kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder für das WLAN ein Access Point verwendet werden, die 802.1x-fähig sind und eine entsprechende Authentisierung unterstützen. EAP verhindert, dass unberechtigte User über die Hardware-Schnittstelle in das Firmennetz eindringen.

Neue Features 8.10(SP1) zu 8.10

Integrierte Unterstützung von Multifunktionskarten für UMTS/GPRS

Bei Vorhandensein einer UMTS/GPRS-Karte im Endgerät, erscheint im Monitor ein zusätzliches Feld mit Feldstärke (grafischer Balkenpegel und Prozentwert)- und Provideranzeige.

PIN-Handling für SIM

Für die Nutzung von Multifunktionskarten wurde das PIN-Handling für die SIM erweitert. Es erfolgt automatisch die Aufforderung zur Eingabe der PIN bzw. PUK. Über das Menü kann die aktuelle PIN der SIM geändert werden.

Neue Features 8.10 gegenüber 8.0

Neue Features 8.1 zu 8.05

Domain Name

Im Client kann neben einem DNS/WINS-Server auch ein "Domain Name" angegeben werden. Dieser wird ansonsten per DHCP dem System in den Netzwerkeinstellungen übergeben.

Deflate-Kompression

Bei IPSec-Verbindungen kann neben LZS auch Deflate für die Datenkompression genutzt werden.

Verteilung der Zertifikate über CMP-Protokoll

Die Verteilung der VPN- und Hardware-Zertifikate kann auf Basis des CMP-Protokolls (Certificate Management Protocol) erfolgen.

Dynamische Personal Firewall (k)

Fester Bestandteil des Clients ist eine Personal Firewall. Die Firewall-Mechanismen sind optimiert für alle Remote Access-Umgebungen und werden bereits zum frühestmöglichen Zeitpunkt, also beim Start des Rechners aktiviert und bleibt dies auch nach dem Abbau einer VPN-Verbindung. Der Telearbeitsplatz ist zu jeder Zeit vor Angriffen geschützt. Alle Firewall-Regeln können zentral vom Administrator vorgegeben und deren Einhaltung erzwungen werden. Voraussetzung hierfür ist das NCP Secure Enterprise Management

Automatische Hotspot-Anmeldung – One Click(k)

Voraussetzung ist die integrierte Personal Firewall im NCP Client. Ihre intelligenten Sicherheitsmechanismen garantieren, dass der User auch in besonders gefährdeten Remote Access Umgebungen wie am Hotspot, sicher arbeiten kann und Attacken vom Unternehmensnetz ferngehalten werden. Kurze Beschreibung: Befindet sich ein User mit seinem Endgerät im Empfangsbereich eines öffentlichen WLAN, muss er für eine VPN-Verbindung nur den Menüpunkt „Hotspotanmeldung“ anklicken und seine Zugangsdaten eingeben. Die dynamische Firewall gibt für den Zeitraum der Anmeldung am Hotspot die Ports für http/https frei. Nicht angeforderte Datenpakete, die also nicht vom Hotspot-Server kommen, werden abgewiesen. Die direkte Kommunikation zum Internet unter Umgehung des VPN-Tunnels ist nicht möglich. Attacken aus dem WLAN und dem Internet werden also verhindert.

[Neue Features 8.05 zu 8.00](#)

Überwachung der PKCS#12-Datei

Es wird überwacht, ob die PKCS#12-Datei vorhanden ist. Ist diese beispielsweise auf einem USB-Stick oder einer SD-Karte gespeichert, wird nach deren entfernen die PIN zurückgesetzt und eine bestehende Verbindung abgebaut. Um eine erneute Verbindung aufzubauen, muss z.B. die SD-Karte wieder gesteckt und die PIN erneut eingegeben werden.

Unterstützung von Hardware-Zertifikaten

Die starke Authentisierung ist auch für Hardware-Komponenten möglich. Hierfür werden Hardware-Zertifikate unterstützt. Als Zertifikatstyp kann zwischen "PKCS#12-Datei" und "Entrust-Profil" gewählt werden. Die PIN-Eingabe erfolgt automatisch im Hintergrund. Als PIN für das Hardware-Zertifikat wird Seriennummer des Rechners oder der Festplatte verwendet.

Anzeige der Meldungen des ACE-Servers für RSA-Token

Alle Nachrichten vom ACE-Server werden am Monitor angezeigt, wie beispielsweise "Ablauf der Gültigen PIN".

Externer Dialer

In bestimmten internationalen Remote Access Umgebungen wird anstatt dem integrierten NCP-Dialer ein externer Dialer z.B. der iPass-Dialer für den Verbindungsaufbau in's Internet eingesetzt.

Bei Verwendung der RAS-Dialer kann der Client so konfiguriert werden, dass nur Kommunikation im VPN-Tunnel erlaubt ist. Eine parallele Verbindung in das Internet ist somit nicht möglich.

Aussagekräftige Fehlermeldungen

Fehlermeldungen werden nicht nur als Code sondern auch als Klartext im Monitor angezeigt.