

NCP Secure Entry Client (Win32/64)

Service Release: 9.31 Build 104

Datum: Januar 2013

1. Neue Leistungsmerkmale und Erweiterungen

Unterstützung von Windows 8

Mit diesem Release der NCP Secure Client Software wird Microsoft Windows 8 unterstützt, sowohl in der Professional- als auch in der Enterprise-Version. Bei der Installation dieser Version des NCP Secure Clients auf einem neu installierten System mit Windows 8 gibt es keinerlei Einschränkungen.

Upgrade eines Systems mit MS Windows 7 und NCP Secure Client Software auf MS Windows 8

Bei einem Upgrade eines Windows 7-Systems mit installiertem NCP Secure Client auf Windows 8 können unter bestimmten Umständen Fehler in der Registry auftreten, die den NCP Secure Client betreffen. Für diesen Fall empfehlen wir folgende Vorgehensweise für die jeweiligen Komponenten einzuhalten:

- Profil-Einstellungen: Erstellen Sie für die Profil-Einstellungen des Secure Clients eine Profil-Sicherung über das Konfigurationsmenü des Monitors ("Konfiguration / Profil-Sicherung / Erstellen"). Als "NCPPHONE.SAV" werden die Profil-Einstellungen im Installationsverzeichnis gesichert.
- Zertifikate: Vergewissern Sie sich, dass Kopien der Soft-Zertifikate (PKCS#12-Dateien) vorliegen. Sofern Zertifikate im Microsoft CSP User Certificate Store hinterlegt sind, folgen Sie den Anweisungen von Microsoft für ein Backup des CSP Stores oder Sie stellen sicher, dass die Original-Zertifikate verfügbar sind, die für den CSP Store verwendet wurden.
- Sichern Sie alle Backup-Dateien auf einem externen Datenträger.
- Führen Sie nun das Upgrade auf Windows 8 durch.
- Führen Sie anschließend mit der aktuellsten Client-Version eine Installation über den bereits bestehenden Client durch. Das Setup-Programm erkennt automatisch, dass bereits eine Version installiert ist, aktualisiert die entsprechenden Programmdateien und sichert die bestehenden Konfigurations-Einstellungen.
- Die gesicherten Backup-Dateien werden nur für den Fall benötigt, dass Einstellungen oder Zertifikate beschädigt wurden.

Änderung im Monitor-Hauptmenü

Das Log-Buch-Untermenü wurde in das Hilfe-Menü verschoben.

Monitor für Anzeigemodus "Hoher Kontrast" kompatibel

Optimierung des NCP Secure Clients bezüglich einer barrierefreien Benutzung.

Die Microsoft Betriebssystemoption „Hoher Kontrast“ (Tastenkombination UMSCHALTTASTE + ALT (links) + DRUCK) wird ab sofort unterstützt.

Manuelles Festlegen auf eine Edge/GPRS-Datenverbindung um ständiges Umschalten zu UMTS zu verhindern

Je nach aktueller Empfangssituation schaltet die 3G-Hardware selbständig zwischen den alternativen Funknetzen GPRS (2G) und UMTS (3G) hin und her. Ist dieser automatische Wechsel unerwünscht, so kann für Windows XP und Vista manuell das Funknetz GPRS festgelegt (aktiviert) werden.

Optimierte Hotspot-Anmeldung bei fehlender WLAN-Verbindung

Sofern das Logon an einem Hotspot erfolgen soll, ohne dass vorher eine WLAN-Verbindung aufgebaut wurde, wird der Benutzer beim Start der Logon-Prozedur darüber informiert. Der entsprechende Warnhinweis hängt davon ab, ob der WLAN-Adapter von der NCP Client Software verwaltet wird oder nicht.

Wird der WLAN-Adapter nicht von der Client Software verwaltet:

Die Hotspot-Anmeldung kann nicht durchgeführt werden!

Bitte verbinden Sie sich zunächst mit dem Hotspot-WLAN.

Danach wiederholen Sie die Hotspot-Anmeldung.

Nachdem mit "OK" fortgefahren wird, muss zuerst eine brauchbare Verbindung zum Hotspot Access Point hergestellt werden, bevor aus dem Verbindungs-Menü erneut "Hotspot-Anmeldung" selektiert wird.

Wird der WLAN-Adapter von der Client Software verwaltet:

Die Hotspot-Anmeldung kann nicht durchgeführt werden!

Bitte verbinden Sie sich zunächst mit dem Hotspot-WLAN.

Danach wiederholen Sie die Hotspot-Anmeldung.

Möchten Sie die WLAN-Konfiguration öffnen, so wählen Sie „Ja“.

Möchten Sie die Anmeldung über ein anderes Medium fortführen, so stellen Sie zuerst eine Netzwerkverbindung her und wählen Sie „Nein“.

Nach Drücken von "Ja" werden die WLAN-Einstellungen geöffnet. Dort kann ein geeignetes WLAN-Profil erstellt werden.

Nach Drücken von "Nein" muss der Benutzer in den Profil-Einstellungen ein geeignetes Profil mit einem anderen Verbindungsmedium erstellen.

Nach der Konfiguration muss die Verbindung zum Hotspot hergestellt und anschließend die Hotspot-Anmeldung wiederholt werden.

UDP-Prefiltering - neuer Standardwert

Der neue Standardwert für „UDP-Prefiltering“ ist auf „aus“ gesetzt.

Die Funktionalität UDP-Prefiltering kann nur bei aktivierter Firewall genutzt werden. Ist die Firewall nicht aktiv, wird unabhängig von der Einstellung die Funktionalität von UDP-Prefiltering auf „aus“ gesetzt. Dies bedeutet, dass bei nicht aktiver Firewall alle UDP-Pakete auf den Client PC gelangen. UDP-Prefiltering kann im Konfigurations-Menü des Monitors unter „Firewall / Optionen / Allgemein“ eingestellt werden.

Firewall Dialog sperrt die weiteren Client Dialoge nicht

Der Firewall-Dialog wurde so modifiziert, dass andere Monitor-Dialoge gleichzeitig parallel genutzt werden können.

Automatisierte Konfiguration einer Funknetz-Verbindung (Auswertung der ProviderID für die Auswahl in der Providerliste)

Beim Anlegen eines 3G-Profiles für GPRS / UMTS (im Konfigurationsmenü unter „Profil-Einstellungen“) ist keine manuelle Konfiguration mehr nötig. In der Standardeinstellung „APN aus SIM-Karte“ werden die entsprechenden Konfigurationsdaten (APN, Rufnummer, Benutzername und Passwort) mit Hilfe der ProviderID automatisch aus der APN.INI übernommen. Voraussetzung ist die korrekte Installation der 3G-Hardware.

Profilgruppen innerhalb Kontextmenü und Profilauswahl im Tray-Icon

Das aktuelle Verbindungs-Profil kann über drei Wege gewechselt werden: über das Konfigurations-Menü des Monitors unter „Profile“, über das Kontext-Menü oberhalb der Weltkarte des Client-Monitors

oder im Menü des Tray-Icons. Konnten bei Verwendung von Profil-Gruppen in den beiden letzten Fällen bislang nur die Profile der vorselektierten Gruppen ausgewählt werden, so lassen sich nun auch die Profil-Gruppen und deren einzelne Profile auswählen.

Entry Client deaktivieren

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

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

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

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

Import von Profil-Dateien im ANSI- und im UTF8-Format

INI-Dateien, welche Client-Profile auch mit Umlauten oder Sonderzeichen enthalten, werden sowohl im ANSI- als auch im UTF8-Format von der Client-Software korrekt verarbeitet.

2. Verbesserungen / Fehlerbehebungen in Service Release 9.31 Build 104

Optimierung bei Seamless Roaming

Der Einsatz von Seamless Roaming ist durch eine intelligente Auswahl des Verbindungsmediums optimiert. Beispielsweise wird bei einer aktiven LAN-Verbindung ein zur Verfügung stehendes „schlechteres“ Medium wie WLAN weitgehend ignoriert, so dass die physikalische LAN-Verbindung nicht unterbrochen wird.

3. Bekannte Einschränkungen in Service Release 9.31 Build 104

Keine

Service Release: 9.30 Build 186
Datum: Juli 2012

1. Neue Leistungsmerkmale und Erweiterungen in Service Release 9.30 Build 186

Alle Ports für die Hotspot-Anmeldung zulassen

Unter der Zielsetzung, von jedem Hotspot weltweit auf das Firmennetz zuzugreifen, kann es erforderlich sein, über die TCP Ports 80 (http) und 443 (https) hinaus, alle Ports flexibel nutzen zu können, da manche Hotspots dynamische Port-Wechsel vornehmen.

In der Konfiguration zur Hotspot-Anmeldung (Monitormenü / Konfiguration / Hotspot) kann unter „Zusätzliche Ports für Hotspot-Anmeldung“ entweder:

- a) ein bestimmter Bereich bzw. einzelne Ports eingegeben, oder
- b) die Option „Alle Ports für die Hotspot-Anmeldung zulassen“ konfiguriert werden. Das hat zur Folge, dass alle Ports 1-65535 automatisch eingetragen werden und das Feld nicht mehr editierbar ist.

Abfrage der Zugangsdaten nach Hibernation/Standby im automatischen Verbindungsmodus

Ist aus Sicherheitsgründen gefordert dass im automatischen Verbindungsmodus die zwischengespeicherten VPN-Zugangsdaten (Benutzername und Passwort) nach Standby oder Hibernation aus dem Speicher gelöscht werden, kann die Option „Eingabeaufforderung für Benutzername und Passwort nach Hibernation/Standby“ aktiviert werden. Diese findet sich unter „Konfiguration / Logon-Optionen / Abmelden“ und bewirkt, dass der Anwender nach Rückkehr des System aus dem Ruhezustand nach Benutzername und Passwort gefragt wird.

APN von SIM-Karte

Der APN (Access Point Name) definiert den Zugangspunkt um über 2G/3G/4G einen mobilen Internet-Zugang herzustellen. Jeder Mobilfunkbetreiber hat sein eigenes APN-Profil. Die APN-Daten müssen in der Client-Software passend zum Mobilfunknetz eingetragen werden.

Im Client waren bisher die APN-Einstellungen manuell konfigurierbar und wurden, um den User zu entlasten, zentral voreingestellt. Bei Nutzung der SIM-Karte eines neuen Mobilfunknetzes musste der User die entsprechenden APN-Einstellungen eigenhändig vor Ort konfigurieren.

Diese Konfigurationsmaßnahme entfällt mit der neuen Version die Zuordnung des korrekten APN erfolgt im neuen Softwarerelease automatisch.

Die APN-INI wurde um die NetID des Providers erweitert. Wird in der Profil-Konfiguration unter 3G der Typ „APN von SIM“ ausgewählt, werden alle Felder der Providerkonfiguration gelöscht. Nach diesem Kriterium wird der Secure Entry Client veranlasst, sich den APN über die NetID der SIM-Karte aus der APN.INI zu suchen. Somit muss kein APN mehr konfiguriert werden. Die Einstellung „APN von SIM“ ist ab dieser Version als Standardwert hinterlegt.

Beim Start des Monitors können die Wartezeiten für die Dienste konfiguriert werden

In seltenen Fällen kann es vorkommen, dass die voreingestellten Zeiten nach dem Start des Monitors nicht ausreichen um die NCP-Dienste zu starten und es kommt zu einer Fehlermeldung. Die Ursache für die Startverzögerung liegt in den Systemeinstellungen des Rechners. Ab sofort kann die Wartezeit wahlweise konfiguriert werden.

Beschreibung: Wird der Monitor gestartet, wartet dieser zunächst maximal 60 Sekunden bis der NCPCLCFG-Dienst gestartet und anschließend noch einmal maximal 120 Sekunden bis der NCPRWSNT-Dienst gestartet ist. Reichen diese Zeiten nicht aus, kann die Wartezeit in der NCPMON.INI durch Änderungen im Abschnitt „General“ bedarfsgerecht konfiguriert werden:

[GENERAL]

WaitForConfigService = 60 (NcpCICfg-Dienst, Standard 60 Sekunden)

WaitForDriverService = 120 (NcpRwsnt-Dienst, Standard 120 Sekunden)

Die Ursachen der Verzögerung sind von der Konfiguration des Betriebs-Systems abhängig. Folgende Fehlermeldungen werden gezeigt:

- *Service "NCPCLCFG" ist nicht gestartet*
In diesem Fall erhöhen Sie den Wert für den Parameter WaitForConfigService.
- *Die Client Software hat ein Problem mit der Treiber-Schnittstelle festgestellt (Mif32Init).*
Bitte starten Sie das System neu. Sollte das Problem weiter bestehen kontaktieren Sie den Support.
In diesem Fall erhöhen Sie den Wert für den Parameter WaitForDriverService.

Die ursächlichen Systemeinstellungen des Rechners können ggf. mit Hilfe des Supports korrigiert werden. Die Verlängerung der Wartezeiten sollte allerdings nur eine Interimslösung sein.

Support Assistent und erweiterte Log-Einstellungen

Zwei neue Hilfe-Menüpunkte erhöhen die Benutzerfreundlichkeit:

- „Support-Assistent“: Assistent mit Auswahlliste welche Informationen via E-Mail an den Herstellersupport mitgeteilt werden.
- „Erweiterte Log-Einstellungen“: Aktivieren erweiterter Logs und Trace-Funktionalität für den Supportfall.

Wichtiger Hinweis: Achtung beim Update von Windows 7 auf Windows 8

Beim Update des Betriebssystems Windows 7 auf Windows 8 ist darauf zu achten, dass der NCP Secure Client unbedingt vor dem Windows-Update deinstalliert wird. Dabei wird empfohlen die Konfigurationsdatei sowie verwendete Zertifikate separat zu sichern. Ist das Update auf Windows 8 abgeschlossen, sollte die neueste Version der NCP Secure Clients von der NCP-Website heruntergeladen und installiert werden. Erfolgt das Windows-Update ohne vorherige Deinstallation des NCP Secure Clients kann eine Neuinstallation von Windows 8 notwendig werden.

2. Verbesserungen / Fehlerbehebungen in Service Release 9.30 Build 186

Optimierung des Verbindungsaufbaus via UMTS

Soll in einer Umgebung mit schlechtem Funkempfang eine Verbindung über UMTS aufgebaut werden, so unternimmt der Client selbständig bis zu drei Versuche, um die Verbindung erfolgreich herzustellen. Dieses interne Verfahren wird in der Log-Datei protokolliert, wo es auch eingesehen werden kann.

Optimierungen im Bereich Seamless Roaming

Für Seamless Roaming wurden weitere Optimierungen vorgenommen, u.a. bei der Erkennung und Behandlung von Mobilfunkverbindungen und WLAN.

Optimierungen bei der Log-Ausgabe

Im Logbuch wird der Wechsel des Verbindungsmediums durch eine Meldung dargestellt. Z.B. "MONITOR: Communication Medium change LAN => WLAN".

Im Logbuch kam es manchmal vor, dass das Scrollen trotz Markierung einer Zeile nicht mehr angehalten werden konnte. Dies war immer dann der Fall, wenn mehr als 400 Log-Einträge im ListView enthalten waren. Der Fehler ist behoben. Zusätzlich wurden der Übersichtlichkeit halber farbliche Hervorhebungen eingebaut.

Booten, Vollversion, Firewall nicht angezeigt

Nach dem Booten wurde unter bestimmten Umständen und nur bei einer Vollversion die Firewall nicht mehr angezeigt. Dieser Fehler ist beseitigt.

Kompatibilitätsprobleme mit dem Symantec Security Center

Diese sind beseitigt.

Batch-Dateien ohne Pfad-Angabe wurden nicht gestartet

Anwendungen (Batch-Dateien und Programme), die sich im NCP-Programmverzeichnis befinden und für den automatischen verbindungsabhängigen Start in den „Logon-Optionen“ ohne Pfadangabe konfiguriert wurden, wurden nicht gestartet. Dies gilt ebenso für die Firewall-Konfiguration unter „Bekannte Netze / Aktionen“ und für die Konfiguration der Verbindungsoptionen unter „Externe Anwendungen“. Dieser Fehler ist behoben.

Änderungen der Proposals für Pre-shared key/XAUTH

Folgende Proposals wurden beim aggressive Mode in Verbindung mit Pre-shared key/XAUTH entfernt:

```
{ AES_CBC , HASH_SHA , XAUTH_INIT_PSK , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192},  
{ AES_CBC , HASH_MD5 , XAUTH_INIT_PSK , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192},  
{ AES_CBC , HASH_SHA , PRE_SHARED_KEY , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192},  
{ AES_CBC , HASH_MD5 , PRE_SHARED_KEY , ALT_MODP_1536 , SECONDS , (28800 * 3) , 0 , 192}
```

Friendly Net bei statisch konfigurierter IP-Adresse und Systemstart

Wenn bei statisch konfigurierter IP-Adresse eine Netzwerkkarte während des Systemstarts nicht an das Netzwerk angeschlossen war, wurde auch nach dem Verbinden der Netzwerkkarte mit dem Netzwerk der Friendly Net Status nicht erkannt. Dieses Problem ist behoben.

Friendly Net Detection bei statisch konfigurierter IP-Adresse ohne Standard-Gateway

Es wurde ein Problem der Friendly Net Detection behoben. Waren auf dem Netzwerkadapter statische IP-Adressen konfiguriert und war kein Standard-Gateway vorhanden, so wurde Friendly Net Detection fehlerhaft ausgeführt. Dieser Fehler ist behoben.

Friendly Net und RWSCMD

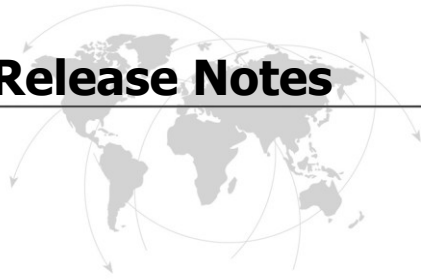
Wurde die Firewall via RWSCMD ausgeschaltet (rwscmd /firewalloff), so wurde der Friendly Net Status nicht korrekt angezeigt. Auch wurde nicht die gesamte Firewall-Funktionalität deaktiviert. Dieser Fehler ist behoben. Standardmäßig werden in der Firewall-Off-Phase keine Konfigurationsänderungen der Firewall übernommen.

Verwendung von Sonderzeichen im WLAN/WPA-Schlüssel oder Mobile Broadband Benutzer/Passwort

Sowohl innerhalb der WLAN/WPA-Schlüssel als auch in den Strings für die Zugangsdaten Benutzername und Passwort können alle Sonderzeichen verwendet werden.

Weitere behobene Fehler

- Bei einem automatischen Verbindungsaufbau wurde unter Umständen die Benutzeranmeldung fälschlicherweise abgefragt.
- Es wurde ein Fehler im NAT-Modul in Verbindung mit eingehenden Sessions behoben.
- Es wurde ein Fehler in Verbindung mit IKEv2 und UDP Encapsulation über Port 4500 behoben.
- Beim Herunterfahren des Systems wurde unter Umständen eine Fehlermeldung der Firewall angezeigt. Der Fehler wurde behoben.
- Ein Problem beim ändern der SIM PIN in Verbindung mit Mobile Broadband wurde behoben.
- Wurde in den Profil-Einstellungen in einem 3G-Profil als 3G-Passwort "<pwreq>" und als Benutzername nichts eingetragen, wurde der Benutzername/Passwort-Dialog mit Benutzername <dummy>" angezeigt. Jetzt wird in diesem Fall als Benutzername ein Leerstring angezeigt.



3. Bekannte Einschränkungen in Service Release 9.30 Build 186

Wiederholter Falsche GPRS/ UMTS / 3G PIN Eingabe

Nach wiederholter Falscheingabe der PIN (GPRS / UMTS / 3G) wird die PUK abgefragt. Diese kann nur dann korrekt eingegeben werden, wenn:

- der Monitor mit Administratorenrechten gestartet wurde
- Sicherheits-Level des Benutzerkontos (UAC) niedrig eingestellt ist

(Vista und Windows 7)

Service Release: 9.30 Build 146
Datum: April 2012

1. Neue Leistungsmerkmale und Erweiterung in Service Release 9.30 Build 146

Seamless Roaming mit IKEv2

Seamless Roaming kann auch für IPsec-Verbindungen genutzt werden, die nach IKE-Richtlinien aufgebaut werden, welche auf IKEv2 basieren. (Monitormenü / Profile / IPsec-Einstellungen / Austausch-Modus / IKEv2)

Voraussetzung: NCP Secure Enterprise Server ab Version 8.10.

Unterstützung der spanischen Sprache

Die sprachliche Darstellung der Monitor-Oberfläche, einschließlich der Online-Hilfe, kann auf Spanisch eingestellt werden (Monitormenü / Ansicht / Sprache).

Diffie Hellman Groups 15-18 – für IPsec Policies (PFS)

Die DH Gruppen 15-18 wurden in Version 9.30 Build 70 nur für den Einsatz in IKE-Richtlinien eingeführt. Ab dieser Version 9.30 Build 146 können sie auch in den IPsec-Richtlinien für PFS (Perfect Forward Secrecy) konfiguriert werden.

Neue Option: Anti-replay Protection

Zeitversetzt eintreffende IP-Pakete könnten korrupt sein. Mit dieser Funktion (nach RFC 2064) werden diese Pakete verworfen. (Monitormenü / Profile / Erweiterte IPsec-Optionen / Anti-replay Protection).

Folgende Meldung zeigt das Erkennen und Verwerfen der Pakete an:

"Esp: Warning - AntiReplay error on sequence number=xxxx"

Erweiterung der Zertifikats-Konfiguration

Wird ein Hardware-Zertifikat im lokalen Computer-Zertifikatsspeicher (CSP) von Windows abgelegt, d. h. unter Windows in diesen Zertifikatsspeicher importiert, so kann dieses Zertifikat vom Client zur Authentisierung genutzt werden. Wurden mehrere Zertifikate in den Computer-Zertifikatsspeicher importiert, so kann in der Konfigurationsoberfläche das gewünschte Zertifikat durch Eingabe von Common Name des Antragstellers und Ausstellers (Subject CN und Issuer CN) selektiert werden. Im Unterschied zu den benutzerspezifischen Zertifikaten im Zertifikatsspeicher für Windows-Benutzer-Zertifikate, die erst dann eingesetzt werden können, nachdem sich der Windows-Benutzer angemeldet hat, können Hardware-Zertifikate aus dem "Computer-Zertifikatsspeicher" bereits nach dem Booten eingesetzt werden (z. B. für die Domänen-Anmeldung).

Wird es zusätzlich zu einem Benutzer-Zertifikat eingesetzt, so kann sichergestellt werden, dass sich der Benutzer immer vom gleichen Rechner aus zum Gateway verbindet.

Künftige Unterstützung der Plattform Windows 8

Der NCP Secure Entry Client kann auf Windows 8 Beta-Versionen installiert werden. Das zugrunde liegende Betriebssystem wird zur Zeit nur experimentell unterstützt. NCP kann daher keine Gewähr für die korrekte Funktion des NCP Secure Entry Clients unter dem aktuell vorliegenden Windows 8 geben. Bei Installation des Clients wird darauf hingewiesen, dass es zu Fehlfunktionen kommen kann.

Optimierungen im Bereich Seamless Roaming

2. Verbesserungen / Fehlerbehebungen in Service Release 9.30 Build 146

Symantec Network Threat Protection

Es wurde ein Kompatibilitätsproblem in Verbindung mit einer Symantec Network Threat Protection behoben.

GPRS / UMTS Konfigurationsmodus: Provider-Liste: Deutschland / T-Mobile D (Germany)

Die APN für den Provider D-Mobile (Germany) wurde korrigiert nach „internet.telekom“.

3. Bekannte Einschränkungen in Service Release 9.30 Build 146

Zusätzlicher Port im Hotspot-Konfiguration

Die Funktionalität zur Definition zusätzlicher Ports innerhalb der Hotspot-Konfiguration schlägt unter bestimmten Umständen fehl:

Diese Fehlersituation tritt ausschließlich dann auf, wenn die Hotspot-Anmeldung initial über einen speziellen Port – wie beispielsweise 8080 – aufgebaut werden muss.

Im Falle der gebräuchlichen, öffentlichen Hotspots tritt dieses Fehlverhalten nicht auf, da hier eine initiale Standard-Webbrowser Abfrage via Port 80 oder 443 serverseitig auf die eigentliche Hotspot-Anmeldeseite umgeleitet wird. In diesem Fall sind die zusätzlich konfigurierten Ports wirksam.

Service Release: 9.30 Build 102
Datum: Februar 2012

1. Neue Leistungsmerkmale und Erweiterungen in Service Release 9.30 Build 102

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 System-tray gleichzeitig grün und gelb bis die physikalische Verbindung wieder hergestellt ist (grünes Licht).

Verliert der Client die Internet-Verbindung und der Tunnel wird logisch gehalten, wird dieser Status mit einem Ballon über dem Tray-Icon angezeigt. Somit wird der Benutzer auch darüber informiert, wenn der Monitor minimiert ist.

Mit der Standardeinstellung wird die logische Verbindung des Tunnels gehalten, auch wenn die physikalische Verbindung abbricht. Dieses Standardverhalten kann geändert werden, indem in den Profil-Einstellungen unter „Verbindungssteuerung“ vorgegeben wird „Logischen VPN-Tunnel bei Verbindungsunterbrechung trennen“.

Erweiterungen von Online-Hilfe und Tipps

Die Hilfetexte wurden der aktuellsten Version des Clients angepasst. Der Dialog für die Profil-Gruppen wurde um einen Hilfe-Button erweitert. Alle Hilfetexte können wie üblich über einen Hilfe-Button oder kontextsensitiv mit der F1-Taste aufgerufen werden. Die Tipps wurden der aktuellen Version des Clients angepasst.

Erweiterung des UMTS-Panels

Das Panel für GPRS / UMTS, das bei Einsatz eines Profils mit einer dieser Verbindungsarten oder LTE im Client-Monitor erscheint, wurde entsprechend des neuen LTE-Standards um die LTE-Anzeige erweitert. Je nachdem welches drahtlose Netz der Provider zur Verfügung stellt, wird dessen Name und Feldstärke angezeigt. Dies gilt auch für das UMTS-Panel der NCP GINA.

Externe Anwendungen

Die Funktion zum Starten externer Anwendungen (Logon Optionen / Ext. Anwendungen) wurde dahin gehend erweitert, dass auch Skripte gestartet werden können, die mit der Extension *.vbs verknüpft sind.

Import von Konfigurationssperren

Für den Import der Konfigurationssperren wurden Ergänzungen in den Dateien Import-de.txt und Import-en.txt eingefügt. Folgende Optionen sind dadurch möglich:

- Profile dürfen exportiert werden
- Profile dürfen importiert werden.

WLAN-Konfigurations-Assistent

Der WLAN-Konfigurations-Assistent bietet bei der Konfiguration eines offenen, ungeschützten WLANs die Hotspot-Anmeldung jetzt nur noch an, sofern es sich um die bekannte SSID eines Hotspot-Anbieters handelt.

2. Verbesserungen / Fehlerbehebungen in Service Release 9.30 Build 102

Blockierter Monitor

Wurde eine PKI-Fehlermeldung über die Callback-Funktion angezeigt, bevor der Monitor aufgebaut war und der Monitor minimierte sich beim Start, konnte die Fehlermeldung nicht angezeigt werden und der Monitor war blockiert.

Fehler beim Aufbau der Routing-Tabelle

Der Client überwacht DHCP Requests an alle Netzwerk-Adapter, um IP-Informationen über jeden Adapter zu erhalten. In bestimmten Situationen ist es erforderlich, dass der Client einen DHCP-Austausch mit einem RENEW-Kommando anstößt. Wird dieses RENEW-Kommando für einen Adapter ohne IP-Adresse oder ohne Verbindungsstatus ausgeführt, so konnte die Routing-Tabelle für einige Minuten nicht aufgebaut werden.

Fehler beim Setzen der Routen im Split-Tunneling

In bestimmten Fällen wurden die Routen bei Verwendung von Split-Tunneling nicht korrekt gesetzt.

Fehlerhafte Export-Datei auf Netzlaufwerk

Bisher konnten die Profil-Einstellungen eines Clients nicht direkt in eine Datei auf einem Netzlaufwerk exportiert werden, da Passwörter und Pre-shared Key in diesem Fall nicht übertragen wurden.

3. Bekannte Einschränkungen in Service Release 9.30 Build 102

Keine

Major Release: 9.30 Build 70
Datum: Oktober 2011

1. Neue Leistungsmerkmale und Erweiterungen in Major Release 9.30 Build 70

Seamless Roaming

Seamless Roaming bietet die automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium. Wird ein Laptop beispielsweise in eine Dockingstation abgelegt, so wird automatisch von einer zuvor genutzten WLAN bzw. 3G/UMTS-Verbindung auf LAN umgeschaltet. Dabei bleibt die IP-Adresse erhalten, so dass eine – über den VPN-Tunnel kommunizierende – Anwendung nicht im Betrieb gestört ist.

Wird die Internetverbindung z. B. wegen schlechten Empfangs kurzzeitig unterbrochen, so wird der VPN-Tunnel logisch gehalten. Auch in diesem Fall kann eine den VPN-Tunnel nutzende Anwendung kurzzeitige Unterbrechungen ohne Session-Verlust überstehen.

Voraussetzung ist der Einsatz eines NCP Secure Servers ab Version 8.05. Seamless Roaming wird nur für IKEv1-Verbindungen unterstützt.

Internationale Erweiterung der UMTS-Providerliste

Die Möglichkeiten einer Profil-Einstellung für GPRS- und UMTS-Verbindungen wurden um eine internationale Provider-Liste erweitert. Im Konfigurationsmodus mit Provider-Liste werden mit der Auswahl eines Landes die dortigen wichtigsten Anbieter angezeigt und mit Auswahl eines Providers die weiteren Parameter automatisch eingetragen. Die Provider-Liste ist editierbar im Installationsverzeichnis als APN.ini abgelegt. (Die Konfiguration wird in den Profil-Einstellungen unter GPRS / UMTS vorgenommen.)

Windows 7 - Mobile Broadband Unterstützung

Aufgrund der bei LTE möglichen, hohen Übertragungsraten wurde die frühere Implementierung via MS Windows virtuellen COM-Ports zum Flaschenhals. Die Kommunikation via MS Windows Mobile Broadband Schnittstelle hebt diese Beschränkung auf.

IKEv2 Unterstützung

Mit der Implementierung des Internet Key Exchange Protocol Version 2 (IKEv2), eingeschlossen der Mobility Extensions (MOBIKE), in den Client-Unterbau, verhält sich der Secure Client kompatibel zu anderen IPsec Gateways wie Microsoft Windows Server 2008 R2.

Die alternative Verwendung von IKEv2 bzw. IKEv1 wird am Entry Client in den Profil-Einstellungen unter der Rubrik „IPsec-Einstellungen / Austausch-Modus“ konfiguriert.

Erweiterung des WLAN-Konfigurations-Assistenten

Wird über den WLAN-Konfigurations-Assistenten ein WLAN-Profil angelegt, so wird unmittelbar nach Abschluss der Konfiguration mit diesem WLAN die Verbindung hergestellt.

Deaktivieren der Proxy-Systemeinstellungen

Der für das System definierte Proxy-Server kann im Konfigurationsmenü unter Hotspot deaktiviert werden. Nach Ablauf eines Timeouts, sowie unmittelbar nach erfolgreichem VPN-Verbindungsaufbau, wird der Proxy-Server automatisch wieder aktiviert.

Beachten Sie, dass diese Einstellung nur mit Browsern funktioniert, die den System-Einstellungen folgen, zum Beispiel: Safari, Google Chrome, Internet Explorer, Firefox.

Umbenennung von Projekt-Logo in Custom Branding Option

Die Funktionalität „Projekt-Logo“ ist in dieser und künftigen Versionen für alle Sprachen in „Custom Branding Option“ umbenannt.

Tests zur Internet-Verfügbarkeit

Das Hilfemenü des Client-Monitors bietet Tests an, womit die Internet-Verfügbarkeit getestet werden kann. Sie gestatten sowohl einen PING auf eine IP-Adresse im Internet auszuführen als auch die Auflösung eines Internet-Domain-Name (DNS-Request) in die entsprechende IP-Adresse zu prüfen, wobei der Domain-Name in Form von „ncp-e.com“ angegeben wird.

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

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

Die Tests sind insbesondere von Bedeutung wenn Firewall-Regeln für DNS-Request und ausgehende Internetverbindungen angelegt wurden.

Diffie Hellman Gruppen 15-18

Die Erweiterung der Diffie Hellman Gruppen wurden ausschließlich für die IKE-Richtlinien hinzugefügt.

Animation zum Verbindungsaufbau

Unmittelbar nach Druck auf den Verbinden-Button erhält der Anwender eine optische Rückmeldung neben dem Button durch ein Drehsymbol. Dieses Symbol zum Vorgang des Verbindungsaufbaus wird angezeigt, solange dieser dauert. Kann keine Verbindung hergestellt werden, verschwindet die Animation und im grafischen Feld des Client-Monitors erscheint statt eines grünen Verbindungsbalkens eine Fehlermeldung.

Automatisierte Prüfung auf eine neue Version

Wird der Menüpunkt „Auf Updates prüfen“ aufgerufen, wird ein neuer Dialog angezeigt, über den der Abfragezyklus (nie, täglich, wöchentlich, monatlich) konfiguriert werden kann. Zusätzlich ist ein Button enthalten „Jetzt prüfen“.

WLAN trennen wenn VPN-Tunnel beendet

Durch setzen der Option "WLAN trennen wenn VPN-Tunnel beendet" wird die Sicherheit im Hotspot-Umfeld erhöht. Dieser Parameter wurde in der Konfiguration der WLAN-Profiles unter "Allgemein" hinzugefügt.

Neue Firewall-Konfiguration GUI

Die GUI der Firewall ist dahingehend überarbeitet, dass Firewall-Regeln direkt - mit einem Mausklick - aktiviert und deaktiviert werden können, sowie vordefinierte Regeln erstellt werden können. Insbesondere wird eine bessere Übersicht über das Regelwerk angeboten. Eine DENY-Regel steht immer zu Beginn des Regelsatzes. Die „offene Grundeinstellung“ fällt weg.

Firewall – Neuer Parameter „FND-abhängige Aktionen starten“

Sobald der Client den Wechsel von einem bekannten zu einem unbekannten Netzwerk (oder umgekehrt) erkennt, kann in Abhängigkeit davon eine beliebige Aktion gestartet werden. So könnte beispielsweise ein externes Programm aufgerufen werden welches die Proxy-Einstellung des Windows-Systems umschaltet.

IPv6-Fähigkeit der Firewall

In der Client Firewall können nun Regeln für IPv6 definiert werden.

Kommandozeilen-Tool "NcpClientCmd"

Alternatives Kommandozeilenprogramm zu rWSCMD welches über keinerlei graphische Ausgabe verfügt.

Ausblenden gesperrter Menüpunkte

Menüpunkte in den Pulldown-Menüs des Client-Monitors, die vom Administrator für die Benutzung gesperrt werden, werden vollständig ausgeblendet, nicht mehr ausgegraut wie in früheren Versionen. Auf diese Weise werden die Pulldown-Menüs entsprechend verkürzt. Die Sperrung erfolgt über die Konfigurationssperren im Konfigurations-Menü.

2. Verbesserungen / Fehlerbehebungen in Major Release 9.30 Build 70

Änderung des WLAN-Assistenten

Wird ein offenes WLAN eingefügt, wird ein Dialog zur Hotspot-Anmeldung gezeigt. Dieser führte häufig zu Verwirrungen, da hier nur Telekom-Hotspots für Deutschland ausgewählt werden konnten.

Der WLAN-Konfigurations-Assistent bietet bei der Konfiguration eines offenen, ungeschützten WLANs die Hotspot-Anmeldung jetzt nur noch an, sofern es sich um die bekannte SSID eines Hotspot-Anbieters handelt.

3. Bekannte Einschränkungen in Major Release 9.30 Build 70

Keine

4. Hinweise zum NCP Secure Entry Client (Win32/64)

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

<http://www.ncp-e.com/de/downloads/download-software/versionsinformationen.html>

Weitere Unterstützung bei Fragen zum Enterprise, erhalten Sie über die Mail-Adressen auf folgender Seite:

<http://www.ncp-e.com/de/unternehmen/kontakt.html>

E-Mail: support@ncp-e.com

5. Leistungsmerkmale

Betriebssysteme

Microsoft Windows (32 & 64 bit): Windows 8, Windows 7, Windows Vista, Windows XP

Security Features

Unterstützung aller IPsec-Standards nach RFC.

Virtual Private Networking

- RFC-konformes IPsec (Layer 3 Tunneling)
 - IPsec Tunnel Mode
 - IPsec-Proposals können determiniert werden durch das IPsec-Gateway (IKE, IPsec Phase 2)
 - Kommunikation nur im Tunnel
 - Message Transfer Unit (MTU) Size Fragmentation and Re-assembly
 - Network Address Translation-Traversal (NAT-T)
 - Dead Peer Detection (DPD)

Authentisierung

- Internet Key Exchange (IKE):
 - Aggressive Mode, Main Mode, Quick Mode
 - IKEv2
 - Perfect Forward Secrecy (PFS)
 - IKE-Config-Mode für dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
 - Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure)
- Benutzer-Authentisierung:
 - User Authentisierung über GINA/Credential Management
 - Windows Logon über VPN-Verbindung
 - XAUTH für erweiterte Benutzer-Authentisierung
 - One-Time-Passwörter und Challenge Response Systeme
 - Zugangsdaten aus Zertifikaten (PKI)
- Unterstützung von Zertifikaten in einer PKI:
 - Soft-Zertifikate, Smart Cards, USB Token: Multi-Zertifikats-Konfiguration
- Seamless Rekeying
- PAP, CHAP, MS-CHAP v2
- HTTP Authentisierung vor VPN
- IEEE 802.1x:
 - Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (Layer 2)
 - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Erweiterte Authentisierung an Switches und Zugriffspunkten auf der Basis von Zertifikaten (Layer 2)
 - Extensible Authentication Protocol – Transport Layer Security (MS-CHAPv2): Erweiterte Authentisierung an Switches und Zugriffspunkten auf der Basis von Zertifikaten mit IKEv2 (Layer 2)
- Hotspot Anmeldung mit HTTP oder EAP
- RSA SecurID Ready

Verschlüsselung (Encryption)

Symmetrisch: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits

Asymmetrisch: RSA bis 2048 bits, für dynamischen Schlüsselaustausch

Hash / Message Authentisierungs-Algorithmen

- SHA-1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman Gruppen 1, 2, 5, 14, 15-18 für asymmetrischen Schlüsselaustausch und PFS

Public Key Infrastructure (PKI) - Starke Authentisierung

- X.509 v.3 Standard
- Zertifikats-Unterstützung in einer PKI
 - Smart Cards und USB Tokens
 - PKCS#11-Schnittstelle für Verschlüsselungs-Tokens (USB und Smart Cards)
 - Smart Card Betriebssysteme
 - TCOS 1.2, 2.0 und 3.0
 - Smart Card Reader-Schnittstellen
 - PC/SC, CT-API
 - Soft-Zertifikate
 - PKCS#12-Schnittstelle für private Schlüssel in Soft-Zertifikaten
- PIN Richtlinien: Administrative Vorgabe für die Eingabe beliebig komplexer PINs
- Certificate Status Protocol (CSP) zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
- Revocation:
 - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
 - Certification Authority Revocation List, (CARL vormals ARL)
 - Online Certificate Status Protocol (OCSP)
 - Certificate Management Protocol (CMP)ⁱ

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des IP-Adressbereiches oder eines NCP FND-Servers)
 - FND-abhängige Aktionen starten
- Sicheres Hotspot Anmeldung
- Anwendung starten vor oder nach VPN-Verbindungsausbau
- Differenzierte Filterregeln bezüglich:
 - Protokolle, Ports, Applikationen und Adressen
 - Schutz des LAN adapter
- Schutz des VMware Gastssysteme
- IPv4 und IPv6 fähigkeit

Networking Features

Sichere Netzwerk Schnittstelle

- LAN Emulation
 - Ethernet-Adapter mit NDIS-Schnittstelle
 - Volle Unterstützung von Wireless Local Area Network (WLAN)
 - Volle Unterstützung von Wireless Wide Area Network (WWAN)

Netzwerk Protokoll

- IP

Verbindungs-Medien

- LAN
- WLAN
- GPRS / 3G (UMTS, HSDPA), GSM (einschl. HSCSD)
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)

- PSTN (analoges Modem)
- ISDN
- Automatic Media Detection (AMD)
- External Dialer
- Seamless Roaming (LAN / Wi-Fi / GPRS / 3G)

Dialers

- NCP Secure Dialer
- Microsoft RAS Dialer (für ISP Einwahl mit Einwahl-Script)

Verbindungssteuerung

- Dead Peer Detection mit konfigurierbarem Zeitintervall
- Short Hold Mode
- Timeout (für ausgehende, eingehende und bi-direktionale Verbindungen)
- Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert
- WLAN Roaming (handover)
- Budget Manager
 - Eigenes Management für WLAN, GPRS/UMTS, xDSL, PPTP, ISDN und Modem-Verbindungen
 - Budgets nach Verbindungsdauer oder Volumen
 - Management der Roaming-Kosten (GPRS/UMTS)
 - Eigenes Management verschiedener WLAN-Zugriffspunkte
- Seamless Roaming

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS) : Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server

VPN Path Finder

- NCP Path Finder Technology
 - Fallback auf HTTPS (port 443) von IPsec wenn Port 500 bzw. UDP Encapsulation nicht möglich ist

Datenkompression

- IPsec Compression: LZS, deflate

Link Firewall

Stateful Packet Inspection

Weitere Features

- VoIP Prioritization
- UDP Encapsulation
- IPsec Roaming ⁱⁱ
- WLAN Roaming ⁱⁱ
- WISPr support (T-Mobile Hotspots)

Point-to-Point Protokolle

- PPP über Ethernet
- PPP über GSM,
- PPP über ISDN,
- PPP über PSTN,
 - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

Unterstützte Standards

Internet Society RFCs und Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),

- Internet Key Exchange Protocol (includes IKMP/Oakley) (RFC 2406),
- Negotiation of NAT-Traversal in the IKE (RFC 3947),
- UDP encapsulation of IPsec Packets (RFC 3948),
- IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
- zusätzliche Extended Key Usages, id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) und anyExtendedKeyUsage (2.5.29.37.0) nach RFC 4945, IKEIntermediate (1.3.6.1.5.5.8.2.2) entsprechend zu draft-ietf-ipsec-pki-req-03

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 eine 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

Benutzerfreundliche Features

APN von SIM-Karte

Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen. Das erleichtert die Nutzung von günstigen lokalen Providern im Ausland.

Client Monitor

Intuitive graphische Benutzeroberfläche

- Mehrsprachigkeit (Englisch, Deutsch, Französisch, Spanisch)
 - Monitor & Setup: en, de, fr, es
 - Online Hilfe und Lizenz en, de, es
- Icon, das den Verbindungsstatus anzeigt
- Client Info Center – Übersicht über :
 - Allgemeine Informationen - Version#, MAC-Adresse etc.
 - Verbindung – aktueller Status
 - Services/Applications – Prozess-Status
 - Zertifikats-Konfiguration – eingesetzte Zertifikate etc.
- Konfiguration, Verbindungsstatus, Logbuch (mit Farbmarkierungen und Copy&Paste-Funktion)
- Unterstützung von 3G-Karten (PCMCIA, embedded) integriert
- Passwort-geschützte Konfiguration und Profil-Management
- Trace Tool für Fehlerdiagnose
- Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden
- Tipp des Tages
- Hotkey Support für Verbindungsauf- und -abbau.
- Custom Branding Option
- Tests zur Internet-Verfügbarkeit



Hinweise

i NCP FND- Server kann kostenlos als Add-On hier heruntergeladen werden:

<http://www.ncp-e.com/de/downloads/download-software.html>

ii Voraussetzung: NCP Secure Enterprise Server V 8.0 und später

Weitere Informationen zum NCP Secure Entry Client (Win32/64) finden Sie hier:

<http://www.ncp-e.com/de/produkte/universelle-vpn-client-suite.html>

Testen Sie 30 Tage kostenlos die uneingeschränkt nutzbare Vollversion des NCP Secure Entry Clients (Win32/64):

<http://www.ncp-e.com/de/downloads/download-software.html>