NCP Secure Entry Client (Win32/64)
Release Notes

Service Release: **10.10.03 r30578**
Datum: **Juni 2016**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10 32/64 Bit
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Neue Lizenzschlüssel ab Version 10.10

Software Update und Lizenzschlüssel
Ab der aktuellen Software-Version benötigt jedes zukünftige Major Release der Software einen neuen Lizenzschlüssel gleicher Version.
Erfolgt das Software Update ohne nachfolgendes Lizenz Update so kann der Client nur für die Restlaufzeit der 30-Tage-Testversion bis zum Erhalt der neuen Lizenz für die neue Version betrieben werden.
Neue Installation und Lizenzschlüssel
Bei Neu-Installationen wird die Client Software standardmäßig im Verzeichnis „Programme“ (vorher „Programme (x86)“) installiert und als Testversion (max. 30 Tage) bis zur Eingabe der passenden Lizenz für die neue Version betrieben.

Windows 10 Update 1511 (Threshold 2/Build 10586) führt zu Problemen mit installiertem NCP Secure Client

Das November-Update von Microsoft für Windows 10 ist weit mehr als nur die Sammlung einiger Patches oder Erweiterungen sondern prinzipiell eine runderneuerte Version von Windows 10. Im Zuge des Updates werden Bereiche der Registrierungsdatenbank umgeschrieben und einige für den NCP Secure Client wichtige Einträge gehen während dieses Vorgangs verloren.
Um dieses Problem zu beheben und die nicht übernommenen Schlüssel und zugehörigen Werte neu zu schreiben, ist eine Deinstallation und nach einem anschließenden obligatorischen Neustart des Systems erneute Installation des NCP Secure Clients notwendig. (Bestätigen Sie bei der Deinstallation **nicht** die Option „Alle Dateien löschen“).
Dabei bleibt die Konfiguration komplett erhalten, jedoch müssen die Lizenzinformationen erneut eingegeben werden. Nach diesem Vorgang ist der NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Fehlerhafte Lizenzdatei

In manchen Fällen konnte die Lizenzdatei *ncp.de* beschädigt oder gelöscht werden. Das Handling der Lizenzdatei des Clients wurde optimiert, so dass dieser Fehler nicht mehr auftritt.

Aktualisierung Installationsdateisignatur

Die Signatur der Installationsdatei wird während der Installation online vom Internet Explorer geprüft. Diese Prüfung fiel negativ aus, da das Zertifikat mittlerweile abgelaufen ist. Das Zertifikat sowie die Signatur wurden aktualisiert.

Korrektur bei Einschalten des Flug-Modus

Wird der Flug-Modus innerhalb eines Windows-10-Systems aktiviert, so wird dies vom Client erkannt. Eine Nutzung der 3G/4G-Hardware findet dann nicht mehr statt.

Korrektur bei manuellem Trennen und Verbinden des VPN-Tunnels

Wurde der Verbinden/Trennen-Button schnell hintereinander gedrückt, so konnte der Client in einen Zustand fallen, der keinen Verbindungsaufbau mehr zuließ. Dieser Zustand konnte nur durch einen Profilwechsel behoben werden.

Korrektur des Update-Verhaltens bei lokalem Update

3. Bekannte Einschränkungen

Keine

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Major Release: **10.10 r29061**
Datum: **April 2016**

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme sind mit diesem Release unterstützt:

- Windows 10 32/64 Bit
- Windows 8.x 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

Neue Lizenzschlüssel ab Version 10.10

Software Update und Lizenzschlüssel

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

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

Neue Installation und Lizenzschlüssel

Bei Neu-Installationen wird die Client Software standardmäßig im Verzeichnis „Programme“ (vorher „Programme (x86)“) installiert und als Testversion (max. 30 Tage) bis zur Eingabe der passenden Lizenz für die neue Version betrieben.

Windows 10 Update 1511 (Threshold 2/Build 10586) führt zu Problemen mit installiertem NCP Secure Client

Das November-Update von Microsoft für Windows 10 ist weit mehr als nur die Sammlung einiger Patches oder Erweiterungen sondern prinzipiell eine runderneuerte Version von Windows 10. Im Zuge des Updates werden Bereiche der Registrierungsdatenbank umgeschrieben und einige für den NCP Secure Client wichtige Einträge gehen während dieses Vorgangs verloren.
Um dieses Problem zu beheben und die nicht übernommenen Schlüssel und zugehörigen Werte neu zu schreiben, ist eine Deinstallation und nach einem anschließenden obligatorischen Neustart des Systems erneute Installation des NCP Secure Clients notwendig. (Bestätigen Sie bei der Deinstallation **nicht** die Option „Alle Dateien löschen“).
Dabei bleibt die Konfiguration komplett erhalten, jedoch müssen die Lizenzinformationen erneut eingegeben werden. Nach diesem Vorgang ist der NCP Secure Client wieder ohne Einschränkungen einsatzbereit.

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

1. Neue Leistungsmerkmale und Erweiterungen

Neue Hotspot-Anmeldung

Innerhalb der neuen Hotspot-Anmeldung entfällt die zugehörige Konfiguration. Der Client erkennt potenziell verfügbare Hotspots und bietet dem Anwender in der Client GUI die Anmeldung daran an. Startet der Anwender die Hotspot-Anmeldung, so erscheint der NCP WLAN-Manager, womit der Anwender das gewünschte WLAN-Netz auswählen und die Anmeldung daran starten kann. Sobald die WLAN-Verbindung aufgebaut ist prüft der Client periodisch diese Verbindung auf Zugriff ins Internet. Ist kein Internetzugang verfügbar, startet der Client einen funktionsreduzierten Webbrowser ohne Adressleiste. Hat sich der Anwender erfolgreich am Eingangsportal des Hotspot-Betreibers angemeldet, wird der Aufbau des VPN-Tunnels automatisch gestartet, sobald der Zugang ins Internet möglich ist.

Erhöhung der Kompatibilität zu Gateways anderer Hersteller

Der Secure Client unterstützt IKEv2 Redirect (RFC 5685). Damit können Load Balancing-Funktionen anderer Hersteller genutzt werden.

Überwachung des Filtertreibers durch den Secure Client

Erkennt der Client eine Fehlfunktion des Filtertreibers, so wird diese selbsttätig behoben und der Anwender aufgefordert einen Neustart durchzuführen.

Verwendung von Half-Routes und Default Gateways unter Windows 10

Die Client Software verwendet in der Standardeinstellung für den virtuellen Netzwerkadapter „Half-Routes“. Durch einen Registry-Eintrag kann auf die Verwendung von „Default Gateways“ umgestellt werden. Der Registry Key hierfür lautet:
Pfad:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt]
Schlüssel:
EnableDefGw = 1
Type:
REG_DWORD
Ist der Registry-Eintrag EnableDefGw nicht vorhanden oder EnableDefGw=0 gesetzt, werden Half-Routes verwendet.

2. Verbesserungen / Fehlerbehebungen

Stabilitätsverbesserungen

Die Stabilität des NCPRWSNT-Dienstes und des Update-Clients wurde verbessert.

Erweiterungen der Log-Meldungen

Die Log-Ausgaben für das PKI-Umfeld und den ncpsec-Dienst wurden erweitert.

Funktionsfähigkeit des WLAN-Moduls

Bei einer großen Anzahl von WLAN-Profilen (über 56) war die Funktion des WLAN-Adapters beeinträchtigt und der Adapter wurde im WLAN-Management nicht mehr angezeigt. Dieser Fehler ist behoben.

Windows Pre-Logon

Die Windows Pre-Logon-Funktionalität (Credential Provider) wurde für Windows 10 angepasst.

3. Bekannte Einschränkungen

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:
https://www.ncp-e.com/de/service/download-vpn-client/versionsinformationen.html

Weitere Unterstützung bei Fragen zum Enterprise, erhalten Sie über die Mail-Adressen auf folgender Seite:
https://www.ncp-e.com/de/unternehmen/kontakt.html

E-Mail: support@ncp-e.com

5. Leistungsmerkmale

Betriebssysteme

Beachten Sie dazu die “Voraussetzungen” auf Seite 1.

Security Features

Unterstützung aller IPsec-Standards nach RFC.

Virtual Private Networking

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

Authentisierung

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - 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)
- Internet Key Exchange v2 (IKEv2):
  - Pre-shared secrets
  - RSA Signatures (und entsprechende Public Key Infrastructure)
  - Extended Authentication Protocol (EAP) – (Benutzername und Passwort für Client-Authentisierung gegenüber Gateway; Zertifikat zur Server-Authentisierung gegenüber Client)
  - EAP unterstützt: PAP, MD5, MS-CHAP v2, TLS (ausgewählt durch Responder/Gateway)
  - IKEv2 Mobility und Multihoming Protokoll (MOBIKE)
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode für dynamische Zuteilung einer privaten (virtuellen) Adresse aus IP-Pool
- Benutzer-Authentisierung:
  - Benutzer-Authentisierung über GINA/Credential Management
    - Windows Logon über VPN-Verbindung
  - XAUTH (IKEv1) 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-GCM 128, 256 bits (nur IKEv2 & IPsec); AES-CTR 128, 192, 256 bits (nur IKEv2 und IPsec); AES (CBC) 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, 19-21, 25, 26 für asymmetrischen Schlüsselaustausch und PFS.
- Diffie Hellman Gruppen 19 - 21, 25, 26 mit Algorithmus elliptischer Kurven (nur unter IKEv2).

Public Key Infrastructure (PKI) - Starke Authentisierung

- X.509 v.3 Standard
- Entrust Ready
- 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 Service Provider (CSP) zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
- Revocation:
  - End-entity Public-key Certificate Revocation List (EPRL vormals 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[i])
  - FND-abhängige Aktionen starten
- Sicheres Hotspot Anmeldung
- Anwendung starten vor oder nach VPN-Verbindungsaufbau
- Differenzierte Filterregeln bezüglich:
  - Protokolle, Ports, Applikationen und Adressen
  - Schutz des LAN Adapter
- Schutz des VMware Gastsystems
- IPv4- und IPv6-Fähigkeit
- Option: ausgehenden Verkehr mit Reject quittieren oder ohne Rückmeldung verwerfen

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

- IPv4-Protokoll
  - IPv4 für Tunnelaufbau und Datenverkehr innerhalb des VPN-Tunnels;
- IPv6-Protokoll
  - IPv6 für Tunnelaufbau von Client zu NCP Server-Komponenten (Secure Enterprise VPN Server);
  - zur Datenübertragung innerhalb des VPN-Tunnels wird IPv4 genutzt

Verbindungs-Medien

- LAN
- WLAN
- Mobiles Netzwerk, GSM - LTE
  - Ab Windows 7 – Mobile-Broadband-Fähigkeit
- xDSL (PPPoE)
- PSTN (analoges Modem)
- ISDN
- Automatic Media Detection (AMD)
- Externer Dialer
- Seamless Roaming (LAN / Wi-Fi / Mobiles Netzwerk)

Dialers

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

Verbindungssteuerung

- Dead Peer Detection mit konfigurierbarem Zeitintervall
- WLAN Roaming (handover)
- Modi des Verbindungsaufbaus
  - manuell
  - immer
  - automatisch (Datenverkehr initiiert VPN-Verbindung)
  - wechselnd (automatischen Modus manuell starten)
  - wechselnd (Immer-Modus manuell starten)
- Timeout (für ausgehende, eingehende und bi-direktionale Verbindungen)
- Short Hold Mode
- Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert
- Budget Manager
  - Eigenes Management für WLAN, Mobilfunk, xDSL, ISDN und Modem-Verbindungen
  - Budgets nach Verbindungsdauer oder Volumen
  - Management der Roaming-Kosten (Mobilfunk)
  - Eigenes Management verschiedener WLAN-Zugriffspunkte

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 Technologie
  - Fallback auf HTTPS (port 443) wenn IPsec-Port 500 bzw. UDP Encapsulation nicht möglich ist [iii]

Datenkompression

- IPsec Kompression

Link Firewall

Stateful Packet Inspection

Weitere Features

- VoIP Priorisierung
- UDP Encapsulation
- IPsec Roaming [iii]
- WLAN Roaming [iii]
- WISPr-Unterstützung (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 v1 (IKE) (includes IKMP/Oakley) (RFC 2406),
  - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
  - Negotiation of NAT-Traversal in the IKE (RFC 3947)
- Internet Key Exchange Protocol v2 (IKEv2) (RFC 4306, 5996)
  - IKEv2 Mobility and Multihoming Protocol (MOBIKE) (RFC 4555)
- UDP encapsulation of IPsec Packets (RFC 3948),

Extended Key Usages:

- id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) nach RFC 4945

- anyExtendedKeyUsage (2.5.29.37.0) nach RFC 4945
- IKEIntermediate (1.3.6.1.5.5.8.2.2) nach 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 wird:

- 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, 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.

Secure Client Monitor

Intuitive graphische Benutzeroberfläche

- Mehrsprachigkeit (Englisch, Deutsch, Französisch, Spanisch)
  - Monitor & Setup: en, de, fr, es
  - Online Hilfe und Lizenz en, de
- 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 Mobilfunk-Hardware
- Passwort-geschützte Konfiguration und Profil-Management
- Trace Tool für Fehlerdiagnose
- Monitor kann firmenspezifisch mit Firmenlogo und Support-Informationen ausgestattet werden

- Hotkey Support für Verbindungsauf- und -abbau.
- Custom Branding Option
- Tests zur Internet-Verfügbarkeit
- Tests zur VPN-Tunnel-Verfügbarkeit (Tunnel Traffic Monitoring)

Hinweise

i NCP FND- Server kann kostenlos als Add-On hier heruntergeladen werden:
http://www.ncp-e.com/de/downloads/download-software.html

iii Voraussetzung: NCP Secure Enterprise Server V 8.0 und später