# NCP Exclusive Entry Client
Release Notes

**Service Release:** **11.21 r43671**
**Datum:** **April 2019**

## Voraussetzungen

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

- Windows 10, 32/64 Bit (bis einschließlich Version 1809)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

**VPN Gateway**
Juniper SRX Series

# 1. Neue Leistungsmerkmale und Erweiterungen

Keine.

# 2. Verbesserungen / Fehlerbehebungen

## Credential Provider ohne HotSpot-Anmeldung

Die mit dem neuen Credential Provider eingeführte HotSpot-Anmeldung vor einer erfolgten Benutzeranmeldung muss aus Sicherheitsgründen entfernt werden. Die HotSpot-Anmeldung steht ohne Funktionseinschränkung wie bisher nach der Anmeldung des Benutzers an Windows zur Verfügung.

## Problembehebung bei 802.1X -Authentisierung im LAN

## Unterbrechung des VPN-Tunnels bei genutzter Mobilfunkverbindung

Nach kurzer Zeit wurde der VPN-Tunnel über eine genutzte Mobilfunkverbindung wegen Dead Peer Detection unterbrochen. Dieses Problem wurde behoben.

# 3. Bekannte Einschränkungen

Keine.

# 4. Hinweise zum NCP Exclusive Remote Access Client

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der NCP-Website. Mehr Information zum NCP Exclusive Entry Client finden Sie hier:
https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/

# 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, 27-30 für asymmetrischen Schlüsselaustausch und PFS.
- Diffie Hellman Gruppen 19 - 21, 25, 26, 27-30 mit Algorithmus elliptischer Kurven (nur unter IKEv2).

**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 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
  - Virtueller 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
  - SMS-Center (senden und empfangen von SMS)
- 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

**Datenkompression**

- IPsec Kompression

**Link Firewall**

Stateful Packet Inspection

**Weitere Features**

- VoIP Priorisierung
- UDP Encapsulation
- WISPr-Unterstützung (T-Mobile Hotspots)
- VPN-Bypass

**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),

Zusätzliche 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)
  - Monitor & Setup: en, de,
  - Online Hilfe und Lizenz en, de
- Icon, das den Verbindungsstatus anzeigt
- Client Info Center – Übersicht über :
  - Allgemeine Informationen - Version, MAC-Adresse, Windows Version und ggf. Build etc.
  - Netzwerk-Treiber Informationen

  - 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



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