# NCP Secure Entry macOS Client
Release Notes

**Major Release:** **4.00 r46079**
**Datum:** **Oktober 2019**

## Voraussetzungen

**Apple macOS Betriebssysteme:**
Folgende Apple macOS Betriebssysteme werden mit dieser Version unterstützt:

- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13

# 1. Neue Leistungsmerkmale und Erweiterungen

## Anpassung an macOS Catalina 10.15

Der Client ist ab dieser Version notarisiert und damit vollständig kompatibel zu macOS Catalina 10.15. Bei der Installation muss die zu installierende Kernelextension explizit in den Einstellungen unter Sicherheit erlaubt werden.

## Virtueller Netzwerkadapter

Der Client stellt sich in macOS mit einem eigenen Netzwerkadapter dar. Dies ermöglicht u.a. VoIP-Anwendungen die Kommunikation durch den VPN-Tunnel. Des Weiteren kann der Client dank dieses Netzwerkadapters auch ein IP-Protokoll innerhalb des VPN-Tunnels nutzen obwohl es im tatsächlich verwendeten physischen Netzwerk nicht verwendet wird. Beispiel: Nutzung von IPv6 innerhalb des VPN-Tunnels obwohl im angeschlossenen Netzwerk nur IPv4 vorhanden ist.

## Verbinden/trennen-Menü im Dock-Icon

Verfügt der VPN-Client über ein konfiguriertes VPN-Profil, so kann die ausgewählte Verbindung durch Rechtsklick über dem Dock-Menü-Icon aufgebaut bzw. getrennt werden.

# 2. Verbesserungen / Fehlerbehebungen

## Optimiertes Handling von DNS-Requests

Einhergehend mit dem neu implementierten Netzwerkadapter kann das Handling von DNS-Requests verbessert werden. Dabei sind folgende zwei Fälle zu unterscheiden:

1. Kein Split Tunneling-Betrieb
   In diesem Betriebsmodus geschieht jegliche Kommunikation zu anderen IP-Adressen, die nicht innerhalb des aktuell verwendeten IP-Adressbereiches liegen, durch den VPN-Tunnel. Dies gilt demzufolge ebenso für DNS-Requests.
2. Split-Tunneling Betrieb
   In diesem Betriebsmodus wird innerhalb der Split Tunneling-Konfiguration das oder die IP-

Remotenetzwerk(e) definiert. Werden nun Ziele innerhalb des Remotenetzwerkes adressiert, so fließen die Daten durch den VPN-Tunnel. Alle anderen Daten, insbesondere auch DNS-Requests fließen am VPN-Tunnel vorbei. Dadurch lassen sich Ziele im Remotenetzwerk zunächst nicht über ihren Domainnamen erreichen, denn typischerweise lösen allgemein erreichbare DNS-Server keine firmeninternen DNS-Namen auf.
Dieses Problem lässt sich durch die explizite Konfiguration der internen Domainnamen, die innerhalb des Remotenetzwerkes liegen, lösen. So bewirkt der Eintrag `firma.local`, dass entsprechende DNS-Requests, z.B. `intranet.firma.local`, durch den VPN-Tunnel an firmeninterne DNS-Server fließen.
Durch diese Konfigurationsoption lässt sich der Datenverkehr durch den VPN-Tunnel und am VPN-Tunnel vorbei komplett trennen.

### Neuer Verbindungsmodus

Der Verbindungsmodus „automatisch“ wurde entfernt und dafür der Modus „immer“ hinzugefügt. Ist „immer“ konfiguriert, so versucht der Client zu jeder Zeit einen VPN-Tunnel aufzubauen. Dies geschieht im Unterschied zum Modus „automatisch“ ohne anliegende, zu versendende, Daten.

## 3. Bekannte Einschränkungen

### Ablageort für Zertifikatsdateien

Einhergehend mit Anpassungen für macOS Catalina können p12-Zertifikatsdateien im Client nicht von beliebigen Ablageorten genutzt werden. Im Falle der automatisch erzeugten Verzeichnisse im Home-Verzeichnis des Benutzers wie z.B. `Dokumente`, `Schreibtisch`, `Downloads`, etc., erscheint der Fehler „Zugriff verweigert“. Werden die Zertifikatsdateien direkt in einem Verzeichnis unterhalb des Benutzer-Home-Verzeichnisses abgelegt, so funktioniert der Zugriff.



Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

# 4. Hinweise zum NCP Secure Entry macOS Client

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/

E-Mail: support@ncp-e.com

# 5. Leistungsmerkmale

## Betriebssysteme

Siehe Voraussetzungen auf Seite 1.

## Security Features

Der Secure Entry Client unterstützt die Internet Society's Security Architecture für das Internet Protokoll (IPsec) und alle zugehörigen RFCs.

**Virtual Private Networking / RFC-konformes IPsec (Layer 3 Tunneling)**

- IPsec Tunnel Mode
- IPv4/6 Dual Stack-Unterstützung
- IPsec-Proposals werden über das IPsec-Gateway ausgehandelt (IKE, Phase 2)
- Kommunikation nur im Tunnel
- Message Transfer Unit (MTU) Size Fragmentation und Re-assembly

**Personal Firewall**

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (autom. Umschaltung der Firewall-Regeln bei Erkennung des Netzwerkes anhand des IP-Adressbereiches, der Mac-Adresse des DHCP-Servers oder des NCP FND-Servers*)
- Differenzierte Filterregeln bezüglich:
  - Protokolle, Ports und Adressen

**Verschlüsselung (Encryption)**

*Symmetrische Verfahren:*
AES-CBC 128, 192, 256 Bit;
AES-CTR 128, 192, 256 Bit;
AES-GCM 128, 256 Bit (nur IKEv2);
Blowfish 128, 448 Bit;
Triple-DES 112, 168 Bit;

*Dynamische Verfahren für den Schlüsselaustausch:*
RSA bis 4096 Bit;

ECDSA bis 521 Bit, Seamless Rekeying (PFS);
Hash Algorithmen: SHA, SHA-256, SHA-384, SHA-512, MD5;
Diffie-Hellman-Gruppen: 1, 2, 5, 14-21, 25-30 (ab Gruppe 25: Brainpool-Kurven);

**Schlüsselaustauschverfahren**

IKEv1 (Aggressive Mode und Main Mode): Pre-shared key, RSA, XAUTH;
IKEv2: Pre-shared key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP,
Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383);

**VPN Path Finder**

NCP VPN Path Finder Technology: Fallback IPsec / HTTPS (Port 443) von IPsec wenn Port 500 bzw. UDP Encapsulation nicht möglich ist. **

**FIPS Inside**

Der Secure Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 gemäß Implementation Guidance section G.5 guidelines zertifiziert (Zertifikat #1747).
Die FIPS-Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

- Diffie Hellman Gruppe: Gruppe 2 oder höher (DH ab 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

**Split Tunneling**

Bei Split-Tunneling ist die genaue Spezifizierung jener Domains möglich, deren DNS-Pakete über den VPN-Tunnel geleitet werden sollen.

**Authentisierungsverfahren**

*Internet Key Exchange (IKE):*
Aggressive Mode, Main Mode,
Quick Mode, IKEv2
Perfect Forward Secrecy (PFS),
IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP-Adresse),
Pre-shared Secrets oder RSA-Signaturen (mit entsprechender Public Key Infrastructure);

*Benutzer-Authentisierung:*
XAUTH für erweiterte Benutzer-Authentisierung,
One-Time-Passwörter und Challenge Response Systeme,
Zugangsdaten aus Zertifikaten;

*Unterstützung von Zertifikaten in einer PKI:*
Multi-Zertifikats-Konfiguration für die Schnittstellen PKCS#11 und PKCS#12;

*Maschinen-Authentisierung:*
Zertifikatsbasierte Authentisierung mittels Zertifikaten aus dem Dateisystem oder dem macOS-Schlüsselbund;

*Seamless Rekeying (PFS);*

*IEEE 802.1x:*
EAP-MD5: Extensible Authentication Protocol (Message Digest 5), erweiterte Authentisierung gegenüber Switches und Zugriffspunkten (Layer 2);
EAP-TLS: Extensible Authentication Protocol (Transport Layer Security), erweiterte Authentisierung gegenüber Switches und Zugriffspunkten auf Basis von Zertifikaten (Layer 2);

*RSA SecurID Ready;*

**IP Adress-Zuweisung**

DHCP (Dynamic Host Configuration Protocol);
IKE Config Mode (IKEv1);
Config Payload (IKEv2);
DNS (Domain Name Service): Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server. Bei Split-Tunneling ist die genaue Spezifizierung jener Domains möglich, deren DNS-Pakete über den VPN-Tunnel geleitet werden sollen.

**Starke Authentisierung (Standards)**

*X.509 v.3 Standard;*

*Schnittstellen zur Zertifikatsunterstützung in einer PKI:*
PKCS#11-Schnittstelle für Authentisierungslösungen von Drittanbietern (Token / Smartcards);
PKCS#12-Schnittstelle für private Schlüssel (Soft-Zertifikate);

**Line Management**

DPD (Dead Peer Detection) mit konfigurierbarem Zeitintervall;
Timeout;
VPN on Demand für den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber;

**Internet Society, RFCs und Drafts**

RFC 4301 (IPsec), RFC 4303 ESP, RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IKEv1, RFC 3526, ISAKMP, RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (Redirect), RFC 7383 (Fragmentation), RFC 7427, 3279 Section 2.2.3, 3447 Section 8 (Signature Authentication), RFC 5903, 6954, 6989, 4754 (ECC), RFC 2451, 3686 (AES with ESP), 5930 (AES-CTR), 4106 (AES-GCM), 5282, 6379 (Suite B), RFC 3447 Section 8 (Padding)

**Client GUI**
**Intuitive graphische Benutzeroberfläche**

Deutsch, Englisch;

Konfigurations-Update;
Profilauswahl;
Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files;
Fehlerdiagnose-Export;
Netzwerkinformationen;

* NCP FND-Server als kostenloses Add-On: https://www.ncp-e.com/de/service/download-vpn-client/
** Voraussetzung: NCP Secure Enterprise VPN Server