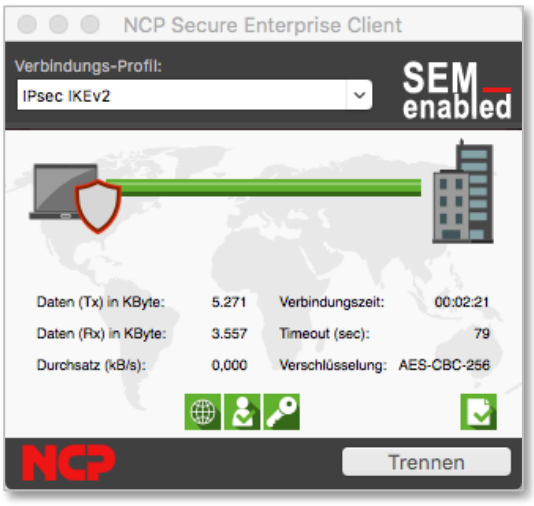
NCP
SECURE COMMUNICATIONS

Datenblatt

NCP Secure Enterprise macOS Client

Universelle, zentral managebare VPN Client Suite für macOS

- Zentrales Management und Network Access Control
- macOS 13 Ventura, 12 Monterey, 11 Big Sur
- Kompatibilität zu VPN Gateways (IPsec-Standard)
- IPv4/6 Dual Stack Unterstützung
- VPN Path Finder Technology (Fallback IPsec / HTTPS)
- Starke Authentisierung (Zertifikate), Biometrie
- Unterstützung Apple Zertifikatsspeicher
- FIPS Inside
- Kostenlose 30-Tage-Vollversion



Universalität und Kommunikation

Der NCP Secure Enterprise macOS Client ist ein Baustein von NCP „Next Generation Network Access Technology“ - der ganzheitlichen Remote Access VPN-Lösung. Auf Basis des IPsec-Standards können hochsichere Datenverbindungen zu VPN Gateways aller namhaften Anbieter hergestellt werden. Der Verbindungsaufbau erfolgt über beliebige Netze (auch iPhone Tethering). Mobile Mitarbeiter können mit macOS-Endgeräten von jedem Standort, weltweit auf das zentrale Datennetz zugreifen.

Die von NCP entwickelte „VPN Path Finder Technology“ ermöglicht Remote Access auch hinter Firewalls bzw. Proxies, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert. Hierbei wird automatisch in einen modifizierten IPsec-Protokoll-Modus gewechselt, der den zur Verfügung stehenden HTTPS-Port für den VPN-Tunnel nutzt.

Sicherheit

Der NCP Secure Enterprise Client verfügt über zusätzliche Sicherheitsmechanismen wie die Unterstützung von OTP-Lösungen (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure). Zur Identifizierung firmenzugehöriger Hardware kann auf dem Endgerät ein Maschinen-zertifikat abgelegt werden.

Dieses Zertifikat kann wahlweise im Dateisystem oder im Zertifikatsspeicher von macOS, dem Schlüsselbund, abgelegt sein. Ein Endpoint Policy-Check verhindert den Zugriff ungenügend geschützter bzw. nicht dem aktuellen Service Pack-Stand entsprechender Endgeräte auf das zentrale Datennetz.

Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747).

Usability und Wirtschaftlichkeit

Die einfache Bedienung und die zentrale Administrierbarkeit des NCP Secure Enterprise macOS Clients sind einzigartig am Markt. Die grafische, intuitive Benutzeroberfläche informiert über alle Verbindungs- und Sicherheitsstaus vor und während einer Datenverbindung. Wahlweise lässt sich die Benutzeroberfläche des Clients auch platzsparend in der Menüleiste von macOS minimiert darstellen. Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Ein Konfigurations-Assistent ermöglicht das ein-fache Anlegen von Profilen.

Zentrales Management

Rollout, Inbetriebnahme und Administration des NCP Secure Enterprise macOS Client erfolgen über das NCP Secure Enterprise Management als „Single Point of Administration“

Betriebssysteme	macOS 13 Ventura (Apple M1/M2 Chip und Intel-CPU), macOS 12 Monterey, 11 Big Sur (Apple M1 Chip und Intel-CPU)
Zentrale Verwaltung	Das NCP Secure Enterprise Management (SEM) bietet als „Single Point of Administration“ alle Funktionalitäten und Automatismen für Rollout, Inbetriebnahme und den wirtschaftlichen Einsatz eines Secure Enterprise Clients. Das Secure Enterprise Management (SEM) versorgt den Enterprise Client über die VPN-Verbindung oder LAN (im Firmennetz) automatisch mit ▪ Konfigurations-Updates ▪ Zertifikats-Updates ▪ Aktualisierungen des Update Clients
Network Access Control	Die Richtlinien für eine Endpoint Security (Endpoint Policy Enforcement) werden am Secure Enterprise Management (SEM) zentral erstellt. Entsprechend der erstellten Regeln erhält der Enterprise Client Zugang zum Firmennetz
High Availability Services	Der NCP Secure Enterprise Client unterstützt die NCP HA Services, die nach dem Client Server-Prinzip arbeiten und in unterschiedlichen Betriebsmodi (Load Balancing- und Failsafe-Modus) eingesetzt werden können. Die VPN-Verbindung wird für den Anwender des Enterprise Clients im Hintergrund auch bei hohem Lastaufkommen oder einem Serverausfall ohne zeitliche Verzögerung sicher ins Firmennetz aufgebaut
Security Features	Unterstützung aller IPsec-Standards nach RFC
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 ▪ Network Address Translation-Traversal (NAT-T) ▪ Dead Peer Detection (DPD)
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
FIPS Inside	Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 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 einer 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

Authentisierungsverfahren	Internet Key Exchange (IKE): ▪ Aggressive Mode und Main Mode ▪ Quick Mode ▪ Perfect Forward Secrecy (PFS) ▪ IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP) ▪ 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 (PKI) Unterstützung von Zertifikaten in einer PKI: ▪ Multi-Zertifikats-Konfiguration für die Schnittstellen PKCS#11 und zertifikatsbasierte Authentisierung mittels Zertifikaten aus dem Dateisystem als PKCS#12Container Geräte-Authentisierung: ▪ Zertifikatsbasierte Authentisierung mittels Zertifikat aus dem macOS-Schlüsselbund Seamless Rekeying (PFS) 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): - gegenüber Switches und Zugriffspunkten auf der Basis von Zertifikaten (Layer 2) RSA SecurID Ready
Starke Authentisierung - Standards	Biometrische Authentisierung X.509 v.3 Standard Zertifikats-Unterstützung in einer PKI über folgende Schnittstellen: ▪ PKCS#11-Schnittstelle für Authentisierungs-Lösungen von Drittanbietern (Token / Smartcards) ▪ PKCS#12-Schnittstelle für private Schlüssel (Soft-Zertifikate) PIN Richtlinien: Administrative Vorgabe für die Eingabe beliebig komplexer PINs Widerrufs- und Sperrverfahren (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)
Networking Features	
Sichere Netzwerk Schnittstelle	Interface Filter ▪ NCP Interface-Filter stellen die Schnittstelle zu allen Netzwerk-Interfaces der PPP- und Ethernet-Familie her. ▪ Volle Unterstützung von Wireless Local Area Network (WLAN) ▪ Volle Unterstützung von Wireless Wide Area Network (WWAN)
Netzwerkprotokoll	IPv4/IPv6
Verbindungssteuerung	Dead Peer Detection mit konfigurierbarem Zeitintervall Short Hold Mode Timeout (für ausgehende, eingehende und bi-direktionale Verbindungen)

Verbindungs-Medien	LAN Unterstützte Verbindungsmedien für Apple oder Medienschnittstellen und Management Tools von Drittherstellern: ▪ LAN / Ethernet ▪ WLAN ▪ Mobilfunk ▪ iPhone Tethering
VPN Path Finder	NCP Path Finder Technology Fallback bis HTTPS (port 443) von IPsec wenn Port 500 bzw. UDP Encapsulation nicht möglich ist *
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 Bei Split-Tunneling ist die genaue Spezifizierung jener Domains möglich, deren DNS-Pakete über den VPN-Tunnel geleitet werden sollen
Datenkompression	IPsec Compression: LZS, deflate
Weitere Features	VoIP Priorisierung UDP Encapsulation PPP über Ethernet
Unterstützte Standards Internet Society RFCs und Drafts	Security Architecture for the Internet Protocol und 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), Encapsulating Security Payloads (ESP)
Client Monitor Intuitive, grafische Benutzeroberfläche	Mehrsprachigkeit (Englisch, Deutsch) ▪ Monitor & Setup ▪ Online-Hilfe und Lizenz Icon, das den Verbindungsstatus anzeigt Passwort-geschützte Konfiguration und Profil-Management Trace Tool für Fehlerdiagnose Start des Monitors optional automatisch nach Systemstart als Vollbild oder als Icon in der Menüleiste

*) Voraussetzung: Installation NCP Secure Enterprise Management

Weitere Informationen zum NCP Secure Enterprise macOS Client finden Sie hier:
https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/managed-clients/

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

FIPS 140-2 Inside

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com