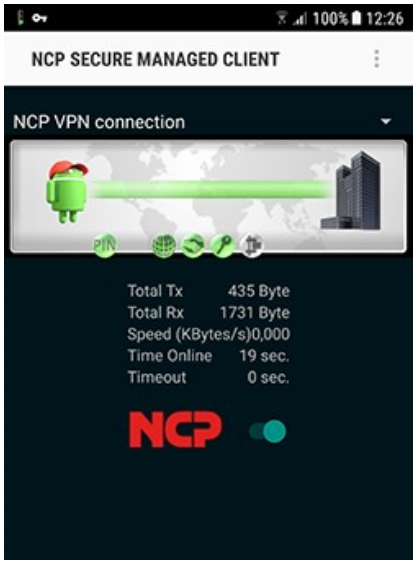
Datenblatt

NCP Secure Enterprise Android Client

Universeller, zentral administrierbarer VPN Client für Android ab V. 4.4

- Zentrales Management
- Kompatibilität zu VPN Gateways (IPsec-Standard)
- Konfigurationsimport von Drittherstellern
- Fallback IPsec / HTTPS (VPN Path Finder Technology)
- FIPS Inside
- Starke Authentisierung, (z.B. Zertifikate), Biometrie (Fingerprint)
- Multi Zertifikatsunterstützung
- Reconnect Mode (Always On)
- Ab Android Version 4.4
- Kein Rooten des Betriebssystems
- Bezug über den Fachhandel



Universalität und Kommunikation

Der NCP Secure Enterprise Android Client ermöglicht eine hochsichere VPN-Verbindung zu zentralen Datennetzen von Firmen und Organisationen. Der Zugriff ist auf mehrere unterschiedliche Datennetze mit jeweils eigenem VPN-Profil möglich. Auf Basis des IPsec-Standards können Tablets und Smartphones verschlüsselte Datenverbindungen zu VPN Gateways aller namhaften Anbieter herstellen.

Auto Reconnect (Always On) bietet den permanenten Fernzugriff auf zentrale Resourcen und Datenbestände.

Die NCP Path Finder Technology ermöglicht Remote Access auch hinter Firewalls bzw. Proxies, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert.

Sicherheit

Die starke Authentisierung des NCP VPN Client bietet einen umfassenden Schutz vor dem Fernzugriff unberechtigter Dritter. Unterstützt werden hierfür OTP-Token (One Time Passwort) und Zertifikate in einer PKI (Public Key Infrastructure). Das Feature "Multi Zertifikats-unterstützung" ermöglicht VPN-Verbindungen mit unterschiedlichen Firmen, die jeweils ein eigenes Benutzerzertifikat erfordern.

Das Kryptografiemodul ist nach FIPS 140-2 gemäß Implementation Guidance section G.5 guidelines zertifiziert (Zertifikat #1747).

Usability und Wirtschaftlichkeit

Mit "Easy-to-use" bieten die NCP Secure Android Clients eine einfache Bedienung über eine grafische, intuitive Benutzeroberfläche. Sie informiert über alle Verbindungs- und Sicherheitsstati vor und während einer Datenverbindung.

Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Usability bedeutet auch Kosteneinsparungen durch Verringerung des Schulungsaufwands, weniger Dokumentation und Entlastung des Helpdesk.

Zentrales Management

Der NCP Secure Enterprise Android Client ist optimiert für die zentrale Administration mit dem NCP Secure Enterprise Management (SEM) und beinhaltet ein umfassendes Endpoint Security-Konzept. Dadurch lassen sich beispielsweise User-Konfigurationen und Zertifikats-Updates zentral managen.

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

Datenblatt

NCP Secure Enterprise Android Client

Betriebssysteme	Android 4.4 und höher
Lizenzverwaltung	Verteilung der VPN Konfiguration und Zertifikate über das NCP Secure Enterprise Management
Standards	Unterstützung aller IPsec Standards nach RFC
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec -Gateway (IKE, IPsec Phase 2); Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Verschlüsselung (Encryption)	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-18
FIPS Inside	Der NCP Secure Android 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: ▪ DH-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	IKEv1 (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS IKEv2 Pre-Shared Secrets
Starke Authentisierung	PKCS#12 Interface zur Nutzung von Benutzer-(Soft)-Zertifikaten, biometrische Authentisierung mit Fingerprint, Multi-Zertifikatskonfiguration One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready
Netzwerkprotokoll	IP
Auto Reconnect	Automatischer Verbindungsaufbau falls die Internet-Verbindung unterbrochen war bzw. ein Wechsel zwischen WLAN und mobiler Datenverbindung stattgefunden hat. Konfigurierbarer Verbindungsmodus: (Always, Manuell)
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: NCP VPN Path Finder Technology am VPN Gateway erforderlich)

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

Datenblatt

NCP Secure Enterprise Android Client

IP Adress-Zuweisung	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; WLAN-Roaming (Handover); Timeout
Datenkompression	IPCOMP (LZS), Deflate
Weitere Features	UDP-Encapsulation; Importfunktion der Dateiformate:*.ini, *.pcf, *.wgx und *.spd
Internet Society RFCs und Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP
Client Monitor **Intuitive, grafische Benutzeroberfläche**	Englisch; Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files; Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus

Weitere Informationen zu den NCP Secure Android Clients finden Sie hier:
https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/managed-clients/

FIPS 140-2 Inside

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