NCP Android Secure Managed Client

mit Kommissionierung für
NCP Secure Enterprise Management als NCP Secure Enterprise Android VPN Client
oder
NCP Volume License Server als NCP Secure Android Client Volume Edition

Major Release: 3.0 r29870
Datum: Mai 2016

Neue Lizenzschlüssel ab Version 3.0

Software Update und Lizenzschlüssel

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

Nach dem Update der Software muss ein Lizenz-Update durchgeführt werden. Dieses kann automatisiert mittels SEM (Secure Enterprise Management) erfolgen (Voraussetzung: Client Plugin 10.10 oder höher).

Erfolgt das Software Update ohne nachfolgendes Lizenz-Update so kann der Client nur für die Restlaufzeit der 10-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 als Testversion (max. 10 Tage) installiert, bis die Eingabe der zugehörigen Lizenz erfolgt.

1. Neue Leistungsmerkmale und Erweiterungen

Unterstützung für One-Time-Passwort mit Challenge

Durch die separate Abfrage eines Passcodes wird die Zwei-Faktor-Authentisierung umfänglich unterstützt.

DNS-Konfiguration

In der neuen Konfigurationsgruppe „DNS-Einstellungen" können die IP-Adressen für primären und sekundären DNS-Server vom Anwender manuell eingegeben werden.

Erweiterte Konfigurationsmöglichkeiten für IPsec

Für jedes VPN-Profil kann eine eigene IKE- und eine eigene IPsec-Richtlinie konfiguriert werden.

Zur Aushandlung der Richtlinien für den IPsec-Verbindungsaufbau können in neuen Konfigurationsgruppen (IKE Policy, IPsec Policy) am Client die vorgegebenen IKE- und IPsec-Richtlinien "automatisch" gesetzt werden oder „benutzerspezifisch" in einer weiteren Konfiguration erstellt werden.

Sofern Richtlinien manuell konfiguriert werden, muss jedes VPN-Profil seine eigene dezidierte Richtlinie erhalten. Im Management-Betrieb erhält der Client die IPsec-Konfiguration vom SEM. Über die Parametersperre am SEM muss dem Anwender lesender Zugriff auf das VPN-Profil verwehrt werden, da ansonsten die Zuordnung von Richtlinie und VPN-Profil verfälscht wird.

Zertifikatsbasierte Authentisierung konfigurieren

Soll zur Authentisierung ein bestimmter Zertifikatsinhalt verwendet werden, so kann dieser über den Konfigurationsschalter „VPN ID Source" selektiert werden.

2. Verbesserungen / Fehlerbehebungen

Anpassung an Android 6

Unterstützung der neuen Open/SSL Version 1.0.2p

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Managed Client

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
http://www.ncp-e.com/de/downloads/download-software/versionsinformationen.html

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

E-Mail: support@ncp-e.com

5. Leistungsmerkmale

Betriebssysteme

Android 4.0 und höher

Zentrales Management

Das Software-Packet des Android Secure Managed Clients ist für zwei unterschiedliche Infrastrukturen der NCP Secure VPN-Lösung konzipiert:

a) Bei Einsatz des Secure Enterprise Managements werden sowohl die Lizenzierung als auch die Bereitstellung und Verteilung der VPN-Verbindungsprofile zentral vom Secure Enterprise Management-System gesteuert.

b) Bei Einsatz des Volume License Servers wird nur die Lizenzierung für jeden einzelnen Secure Managed Client zentralisiert vom NCP Volume License Server besorgt.

Standards

Unterstützung aller IPsec Standards nach RFC:

Virtual Private Networking

- RFC-konform IPsec (Layer 3 Tunneling):
  - IPsec Tunnel Mode
  - IPsec-Proposals können determiniert werden durch das IPsec-Gateway (IKEv1, IKEv2, IPsec Phase 2)
  - Event log
  - Kommunikation nur im Tunnel
  - Message Transfer Unit (MTU) Size Fragmentation und Reassembly
  - Network Address Translation -Traversal (NAT-T)
  - Dead Peer Detection (DPD)

Verschlüsselung (Encryption)

Symmetrische Verfahren: AES-CBC, AES-CTR (RFC 3686, 5930) je mit 128, 192, 256 Bits; Blowfish 128, 448 Bits; Triple-DES 112, 168 Bits;
Dynamische Verfahren für den Schlüsselaustausch: RSA bis 4096 Bits; Seamless Rekeying (PFS);
Hash Algorithmen: SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-18, 19-21, 25, 26;

FIPS Inside

Der NCP Secure Android Client Volume Edition 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 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);
  - Perfect Forward Secrecy (PFS)
- IKEv2
- Pre-shared Secrets
- One-Time-Passwort mit Challange

Starke Authentisierung

- PKCS#12-Schnittstelle für Private Schlüssel in Soft Zertifikaten,
- PKCS#11 Bibliothek (Certgate und TCOS (auf Anfrage)) für Verschlüsselungs-Token (nur für ARM Architektur).
- 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: (Immer, 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);

IP Adress-Zuweisung

- Dynamic Host Control Protocol (DHCP);
- Domain Name Server (DNS):
  - Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server;

Line Management

- Dead Peer Detection (DPD) mit konfigurierbarem Zeitintervall
- WLAN-Roaming (Handover)
- Timeout

Datenkompression

- IPCOMP (lzs), Deflate

Weitere Features

- UDP-Encapsulation;
- Importfunktion der Dateiformate:*.ini, *.pcf, *.wgx und *.spd

Internet Society RFCs and Drafts

RFC 4301 (IPsec), RFC 4303 (ESP), RFC 3947 (NAT-T), RFC 3948 (UDP encapsulation), RFC 7296 (IKEv2), RFC 4555 (MOBIKE)

Client Monitor Intuitive, grafische Benutzeroberfläche

- Widgets,
- Konfiguration, Import und Export,
- Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files,
- Trace-Werkzeug für Fehlerdiagnose,
- Ampelsymbol für Anzeige des Verbindungsstatus.