NCP Secure Managed Android Client
Release Notes

Service Release: **4.11 r42317**
Datum: **Januar 2019**

Voraussetzungen
Android 9 bis Android 4.4

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)
Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 4.05 oder neuer
- NCP Management Console: Version 5.0
- Client Configuration Plugin: Version 11.13
- License Plugin: Version 11.13

1. Neue Leistungsmerkmale und Erweiterungen
Keine.

2. Verbesserungen / Fehlerbehebungen

Fehlerhafte DNS-Anfragen bei konfiguriertem DNS-Suffix
Für den Fall konfigurierter DNS-Server inkl. DNS-Suffix im IKECFG-Mode wurde bei einer DNS-Anfrage fälschlicherweise der DNS-Suffix angefügt. Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Konfiguration von IPsec/IKE-Richtlinien via zentrales Management
Bei der Konfiguration via zentrales Management können mehreren Profilen die gleichen Richtlinien (Proposals) zugewiesen werden. Diese Art der Konfiguration wird im Client nicht unterstützt. Für jedes Profil müssen eigene Richtlinien vorhanden sein.

Konfigurationssperren
Die Konfigurationsdialoge des Management Plug-ins sind unterschiedlich zu denjenigen in der Client GUI. Dies hat zur Folge, dass nicht alle einzeln gesetzten Parametersperren im Plug-in sich auf die Konfigurationsparameter im Client auswirken.

Major Release: 4.10 r41665
Datum: November 2018

Voraussetzungen

Android 9 bis Android 4.4

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 4.05 oder neuer
- NCP Management Console: Version 5.0
- Client Configuration Plugin: Version 11.13
- License Plugin: Version 11.13

1. Neue Leistungsmerkmale und Erweiterungen

Biometrische Authentisierung (z.B. Fingerabdruck- oder Gesichtserkennung) vor VPN-Verbindungsaufbau

Zur Absicherung vor einem VPN-Verbindungsaufbau durch nicht autorisierte Dritte wurde im NCP Secure Client eine optionale biometrische Authentisierung vor der VPN-Einwahl integriert. Bei gesetzter Option erfolgt direkt nach dem Klick auf den Verbinden-Button in der Client-GUI die Aufforderung zur Benutzerauthentisierung. Der VPN-Verbindungsaufbau wird daraufhin erst nach positiver Authentisierung gestartet. Voraussetzung für die biometrische Authentisierung ist Android 6 oder neuer. Für ältere Betriebssysteme oder nicht vorhandene biometrische Hardware wird bei gesetzter Konfigurationsoption eine alternative Benutzerauthentisierung, z.B. das Passwort, abgefragt. Diese Option steht nur für den Verbindungsmodus „Auto-reconnect“ zur Verfügung.

FIPS-Modus

2. Verbesserungen / Fehlerbehebungen

Neue Test-VPN-Profile

Das bisher mit installierte Verbindungsprofil "Test IPsec Certgate PKCS#11" wurde entfernt. Weiterhin verwenden die Testprofile nun eine Konfiguration mit Pre-shared Key.

Erfolgreicher Verbindungsaufbau ohne Eingabe von Benutzername und Passwort

Im Falle eines konfigurierten VPN-Profils mit Benutzerauthentisierung via Benutzername und Passwort wurde dies nur beim ersten Verbindungsaufbau abgefragt. Erst ein Profilwechsel machte die wiederholte Eingabe von Benutzername und Passwort notwendig. Dieser Fehler ist behoben.

3. Bekannte Einschränkungen

Konfiguration von IPsec/IKE-Richtlinien via zentrales Management

Bei der Konfiguration via zentrales Management können mehreren Profilen die gleichen Richtlinien (Proposals) zugewiesen werden. Diese Art der Konfiguration wird im Client nicht unterstützt. Für jedes Profil müssen eigene Richtlinien vorhanden sein.

Konfigurationssperren

Die Konfigurationsdialoge des Management Plug-ins sind unterschiedlich zu denjenigen in der Client GUI. Dies hat zur Folge, dass nicht alle einzeln gesetzten Parametersperren im Plug-in sich auf die Konfigurationsparameter im Client auswirken.

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

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-vpn-client/versionsinformationen.html

Weitere Informationen zum NCP Secure Managed Android Client finden Sie hier:

https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/managed-clients/

Weitere Unterstützung bei Fragen zum NCP Secure Managed Android Client, erhalten Sie über die Mail-Adressen auf folgender Seite:

http://www.ncp-e.com/de/unternehmen/kontakt.html

5. Leistungsmerkmale

Zentrales Management

Das Software-Paket 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 Challenge

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.

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