NCP Secure Managed Android Client
Release Notes

Major release: 4.10 r41665
Date: November 2018

Prerequisites

Android 9 to Android 4.4

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 4.05 or newer
- NCP Management Console: Version 5.0
- Client Configuration Plugin: Version 11.13
- License Plugin: Version 11.13

1. New Features and Enhancements

Biometric Authentication (e.g. Fingerprint or Face Recognition) Before VPN Connection

To prevent unauthorized third parties from establishing a VPN connection, optional biometric authentication has been integrated in the NCP Secure Client prior to VPN connection. If this option is enabled, the prompt for user authentication is displayed directly after clicking the Connect button in the client GUI. The VPN will only connect if authentication is successful. Biometric authentication requires the Android 6 or above. For older operating systems or if a biometric device is not available, an alternative authentication method such as a password can be enabled. This option is only available for manual and variable connection modes.

FIPS-Mode

2. Improvements / Problems Resolved

New Test VPN Profiles

The previously installed connection profile "Test IPsec Certgate PKCS#11" has been removed. Furthermore, the test profiles now use a configuration with a pre-shared key.

Successful Connection Without Entering Username and Password

If a VPN profile was configured with user authentication via username and password, credentials were only queried during the first connection. The user was only prompted to enter the username and password again if the profile was changed. This issue has been resolved.

3. Known Issues

Configuration of IPsec/IKE Proposals via Central Management

Several profiles can be assigned the same proposals with configuration via central management. This type of configuration is not supported in the client. Each profile must have its own proposals.

Configuration Locks

The configuration dialogs in the Management Plug-in differ from the client GUI. This means that not all individually set parameter locks in the plug-in affect the configuration parameters in the client.

4. Getting Help for the NCP Secure Managed Client

To ensure that you always have the latest information about NCP's products, always check the NCP website at:

http://www.ncp-e.com/en/downloads/software/version-information.html

For further information about the NCP Secure Managed Android Client, visit:

http://www.ncp-e.com/en/products/centrally-managed-vpn-solution/managed-vpn-client-suite.html

For further assistance with the NCP Secure Managed Android Client, visit:

http://www.ncp-e.com/en/company/contact.html

5. Features

Management and Licensing

The Android Secure Managed Client software package is designed to be used in one of two different secure VPN infrastructure scenarios:

a) In this scenario, license and VPN Connection Profile parameters are centrally managed by and distributed from an NCP Secure Enterprise Management server.

b) In this scenario, only the license for each individual Secure Managed Client is managed and distributed by the NCP Volume License Server.

Standards

Support of all Internet Society IPsec Standards

Virtual Private Networking

- RFC conformant IPsec (Layer 3 Tunneling),
  - IPsec Tunnel Mode
  - IPsec proposals can be determined by the IPsec gateway (IKE, IPsec Phase 2);
  - Event log;
  - Communication only in tunnel;
  - Message Transfer Unit (MTU) Size Fragmentation und Reassembly;
  - Network Address Translation -Traversal (NAT-T);
  - Dead Peer Detection (DPD);
  - NAT-Traversal (NAT-T);

Encryption

Symmetric processes: AES-CBC, AES-CTR (RFC 3686, 5930) je mit 128, 192, 256 Bits; Blowfish 128, 448 Bits; Triple-DES 112, 168 Bits;
Dynamic processes for key exchange: RSA bis 4096 Bits; Seamless Rekeying (PFS);
Hash Algorithms: SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-18, 19-21, 25, 26;

FIPS Inside

The NCP Secure Enterprise Android Client uses an embedded FIPS 140-2-validated cryptographic module (Certificate #1747) running on an Android platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.

FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection:

- Diffie Hellman Group: Group 2 or higher (DH starting from a length of 1024 bits)
- Hash Algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits
- Encryption Algorithms: AES with 128, 192 or 256 bits or Triple DES

Authentication Process

- IKEv1 (Aggressive und Main Mode), Quick Mode;
  - XAUTH for extended user authentication;
  - IKE Config Mode for the dynamic assignment of a virtual address from an IP pool (private IP);
  - PFS
- IKEv2
- Pre-shared Secrets
- One-Time-Password with challenge response

Strong Authentication

- PKCS#12 Interface for using User (Soft) Certificates
- PKCS#11 library (Certgate and TCOS (on request)) for encryption tokens (only for ARM architecture)
- One-Time Passwords and Challenge Response System; RSA SecurID Ready

Network Protocol

- IP

Auto Reconnect

- A connection is automatically established if the Internet connection has been interrupted or the communication medium has changed from WiFi to mobile data transmission.
- Configurable connection mode (always, manual)

VPN Path Finder

- NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) when port 500 or UDP encapsulation can not be used (prerequisite: NCP VPN Path Finder Technology required at the VPN Gateway)

IP Address Assignment

- Dynamic Host Control Protocol (DHCP);
- Domain Name Server (DNS):
  - central VPN gateway selection using public IP address allocated by querying a DNS server

Line Management

- Dead Peer Detection (DPD) with configurable polling interval;
- WLAN Roaming (Handover);
- Timeout

Data Compression

- IPCOMP (lzs), Deflate

Other Features

- UDP encapsulation
- Import function supporting file formats: *.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 GUI

- Widgets,
- Configuration, import and export,
- Connection control and management, connection statistics, log files,
- Trace tool for error diagnosis,
- Traffic light icon indicates connection status.