NCP Android Secure Managed Client

can be commissioned for use in one of two environments:

NCP Secure Enterprise Management as an NCP Secure Enterprise Android VPN Client
or
NCP Volume License Server as an NCP Secure Android Client Volume Edition

Major Release: **3.0 r29870**
Date: **May 2016**

New License Key from Version 10.10

Software Updates and License Keys

From the current software version, every new major release will require a specific license key for the same version.

After the software has been installed, the license must be updated. This can be done automatically via SEM (Secure Enterprise Management) which requires the client plugin version 10.10 or higher.

If the software is updated without updating the license, the client can only be used for the remainder of the 10-day trial period until the license is updated.

Re-installation and License Key

In the event of re-installation, the client software will be installed as a test version (max 10 days) until the required license key is entered.

1. New Features and Enhancements

Support for one-time password with challenge response

Two-factor authentication is now supported via an additional passcode prompt.

DNS Configuration

In the new "DNS Settings" configuration group, users can now enter IP addresses for primary and secondary DNS servers manually.

Advanced Configuration Options for IPsec

An individual IKE and IPsec policy can be created for each VPN profile.

The negotiation of the IPsec connection policies can be set automatically using the predefined IKE and IPsec policies in the new configuration groups (IKE Policy, IPsec Policy) in the client or user-specific in another configuration.

If policies are configured manually, each VPN profile must have a dedicated policy. In managed mode, the client receives the IPsec configuration from SEM. The user must be denied read permissions for the VPN profile via the Parameter Lock in SEM, otherwise the assignment of the policy and VPN profile will be incorrect.

Configure Certificate-based Authentication

To use a specific value from the certificate for authentication, select it from the VPN ID source configuration options.

2. Improvements / Problems Resolved

Support for Android 6

Support for Open/SSL Version 1.0.2p

3. Known Issues

None

4. Getting Help for the NCP Android 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 assistance with NCP's Android products, please send mail to the address listed on:

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

or to

E-Mail: support@ncp-e.com

5. Features

Operating System

Android 4.0 and later

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 challange 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.