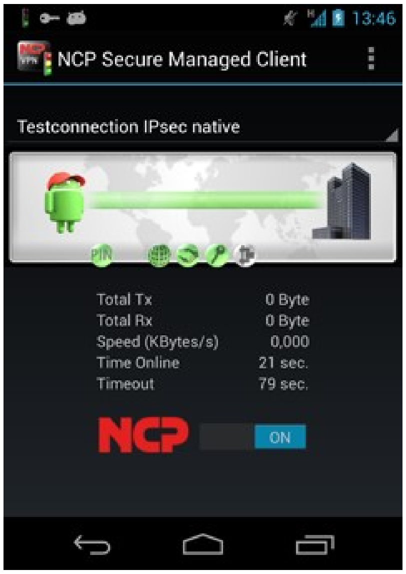
Data Sheet

NCP Secure Android Client Volume Edition

Universal VPN Client Suite for Android version 4.4 or later with License Management

- Central License Distribution
- Compatible with all VPN Gateways (IPsec Standard)
- Import configurations from 3rd party products
- Fallback IPsec / HTTPS (VPN Path Finder Technology)
- FIPS Inside
- Strong authentication (eg. Certificate), Biometrics
- Multi certificate support
- Reconnect mode (Always On)
- Android version 4.4 and later
- No need to "root" the operating system
- Available from NCP Distributors and Partners



13:46

NCP Secure Managed Client

Testconnection IPsec native

Total Tx 0 Byte
Total Rx 0 Byte
Speed (KBytes/s) 0,000
Time Online 21 sec.
Timeout 79 sec.

Universally Applicable

The NCP Secure Android Client Volume Edition enables a highly secure Virtual Private Network (VPN) connection to the corporate networks of companies or organizations. Access to multiple networks is supported, each connection being defined by its own VPN profile.

Using standard IPsec protocols, connections can be established from tablets and smartphones to the VPN gateways of all well-known manufacturers.

Auto reconnect provides permanent remote access to central resources and information.

NCP Path Finder Technology enables remote access even when the device is located behind firewalls or proxies that would otherwise hinder the establishment of an IPsec tunnel.

Security

The strong authentication of the NCP Secure Android Client Volume Edition provides comprehensive protection against access by unauthorized third parties.

Data encryption: support for OTP (One Time Password) tokens and certificates in a PKI (Public Key Infrastructure). "Multi certificate support" enables VPN connections between the one device and different companies, even when each company demands an individual user certificate.

The embedded cryptographic module is validated according to FIPS 140-2 (Certificate #1747), Implementation Guidance section G.5.

Usability and Cost Effectiveness

The intuitive, graphical user interface not only makes NCP Secure Android Clients "easy to use", but also keeps the user continuously updated on the state and security level of the connection, both while the VPN is established and while it is disconnected.

Detailed logs help to ensure rapid support from the help-desk in the event of unforeseen problems. Usability, in turn, means cost savings as less training and documentation are required, and the load on the help-desk is reduced.

Central License Management

The NCP Secure Android Client Volume Edition works in conjunction with an NCP Volume License Server (VLS) that is responsible for managing the central distribution of any number of licenses to an equivalent number of Clients within a corporate network. In doing so, the transfer of license details between VLS and Client is secured against manipulation, eavesdropping and theft.

Operating Systems	Android 4.4 and above
License Management	Distribution of licenses by the Volume License Server
Standards	Support of all Internet Society IPsec Standards
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC conformant; IPsec proposals can be determined by the IPsec Gateway (IKE, IPsec Phase 2); Event log; Communication only in tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Encryption	Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple DES 112,168 bits; Dynamic processes for key exchange: RSA to 2048 bits; Seamless Rekeying (PFS); Hash Algorithms: SHA-256, SHA-384, SHA-512, MD5, DH Groups 1, 2, 5, 14-18
FIPS Inside	The NCP Secure 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 internal pool (private IP) ; PFS IKEv2 Pre-Shared Secrets
Strong authentication	PKCS#12 Interface for using User (Soft) Certificates, biometric Authentication with fingerprint, Multi Certificate configuration 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	DHCP (Dynamic Host Control Protocol); DNS: central VPN gateway selection using public IP address allocated by querying a DNS server

Line Management	DPD (Dead Peer Detection) with configurable polling interval; Short Hold Mode; 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 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 GUI	English; Connection control and management, connection statistics, log files; trace tool for error diagnosis; traffic light icon indicates connection status

Further information about the managed NCP Secure Android Client is available from:
https://www.ncp-e.com/en/products/ipsec-vpn-client-suite/ipsec-vpn-client-for-android.html

FIPS 140-2 Inside