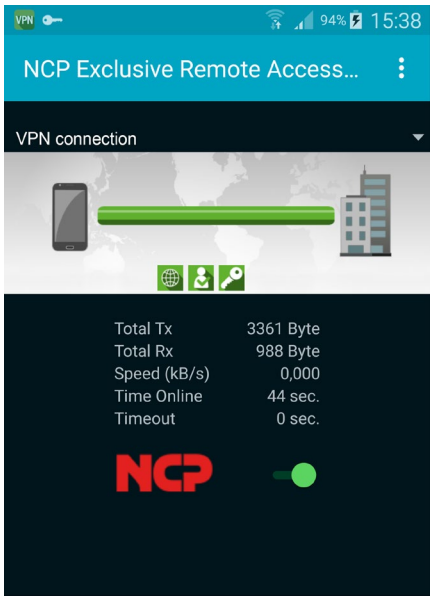
Data Sheet

NCP Exclusive Remote Access Android Client

Centrally Managed
VPN Client for Android version 4.4 or later

- Central management
- Compatible with Juniper SRX Gateways
- Fallback IPsec / HTTPS
  (VPN Path Finder Technology)
- FIPS Inside
- Strong authentication
- Multi certificate support
- Reconnect mode (Always On)



Communication

The NCP Exclusive Remote Access Client is part of the NCP Exclusive Remote Access Solution for Juniper SRX Gateways. The VPN client is only available with NCP Exclusive Remote Access Management. Using IPsec standards as a foundation, highly secure data connections can be established to Juniper SRX gateways, via any type of network (including iPhone tethering via USB or Bluetooth). Remote workers can use their Android devices to access the company network from anywhere in the world.

Always On ensures a permanent connection to the company network and that all data is transferred via the VPN tunnel. NCP VPN Path Finder Technology enables remote access even when the device is located behind firewalls or proxies that would otherwise block IPsec traffic.

Security

The strong authentication of the NCP Exclusive Remote Access Android VPN Client 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 updated on the state and security level of the connection.

Detailed logs provide useful troubleshooting information for the helpdesk easing support workload. and usability features reduce training and documentation costs.

Central Management

NCP Exclusive Remote Access Android Client is managed centrally through NCP Exclusive Remote Access Management which means user configuration and certificate updates can be deployed centrally. The NCP Exclusive Remote Access Management is required for the NCP Exclusive Remote Access Android Client

Data Sheet

NCP Exclusive Remote Access Android Client

Operating Systems	Android 4.4 and above
Juniper SRX/vSRX OS	Junos OS 15.1X49-D80 or higher is required
Central Management	Distribution of VPN configurations and certificates from the NCP Exclusive Remote Access Management
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 bit; Blowfish 128, 448 bit; Triple DES 112,168 bit; Dynamic processes for key exchange: RSA up to 2048 bit; Seamless Rekeying (PFS); Hash Algorithms: SHA-256, SHA-384, SHA-512, MD5, DH Groups 1, 2, 5, 14-18
FIPS Inside	The NCP Exclusive Remote Access 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 bit) ▪ Hash Algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bit ▪ 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
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) when port 500 or UDP encapsulation cannot be used
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; WLAN-Roaming (Handover);

	Timeout
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)
Data Compression	IPCOMP (lzs), Deflate
Other Features	UDP encapsulation Import function supporting file formats: *.ini, *.pcf, *.wgx and*.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 troubleshooting; traffic light icon indicates connection status

Further information on the managed NCP Secure Android Client is available from:
https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/

FIPS 140-2 Inside

NCP PATH FINDER