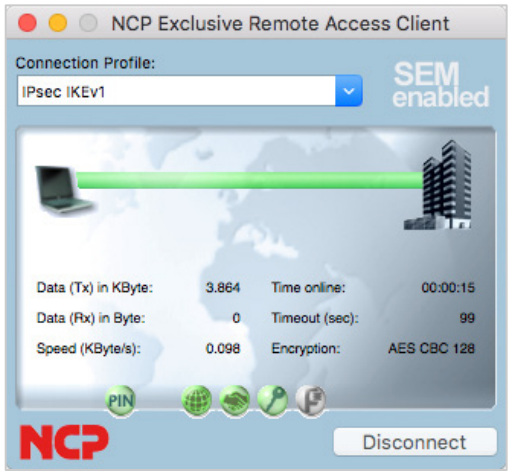
Data Sheet

NCP Exclusive Remote Access Mac Client

Centrally managed VPN Client Suite for macOS

- For Juniper SRX Series
- Central Management
- macOS 14 Sonoma, 13 Ventura, 12 Monterey, 11 Big Sur
- IPv4/6 Dual Stack Support
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- FIPS Inside
- Strong Authentication (e.g., Certificate), Biometrics
- Multi Certificate Support



Communications

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, via any type of network (including iPhone Tethering), to Juniper SRX gateways. Mobile workers can use their Mac devices to access their company's central data network from anywhere in the world.

Even when the Mac is located behind a firewall or proxy whose settings typically prevent IPsec data connections, NCP's "VPN Path Finder Technology" ensures that a connection to the remote gateway can always be established. "Path Finder" automatically switches to a modified IPsec protocol mode that then uses the resulting HTTPS port for the VPN tunnel.

Security

The NCP Exclusive Remote Access macOS Client provides additional security mechanisms such as support for OTP (One-Time Password) solutions and certificates in a PKI (Public Key Infrastructure). By storing certificates in the Apple keychain (certificate store), users are sure that their certificates are stored securely and, in conjunction with the NCP software, can be used to authenticate the secure remote-access connections. The IPsec Client incorporates cryptographic algorithms conformant with the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747).

Usability and Profitability

"Easy-to-use" for both user and administrator – the NCP Exclusive Remote Access Mac Client's central management features are unique in the market. The intuitive, graphical user interface (GUI) provides information on all connection and security states and in order to save space on the desktop, the GUI can be minimized to the menu bar. A configuration wizard simplifies the setup of connection profiles and detailed log information ensures effective assistance from the help desk.

Central Management

Rollout, commissioning and administration of NCP Exclusive Remote Access Mac Clients are all handled via the NCP Exclusive Remote Access Management as the "single point of administration". (precondition for the use of the NCP Exclusive Remote Access Clients).

Operating Systems	macOS 14 (Sonoma Apple Chip and Intel-CPU), 13 Ventura (Apple Chip and Intel-CPU), macOS 12 Monterey, 11 Big Sur (Apple Chip and Intel-CPU)
Juniper SRX/vSRX OS	Junos OS 15.1X49-D80 or higher is required
Central Management	As the "Single Point of Management", NCP's Exclusive Remote Access Management provides functionality and automation for the rollout, commissioning and efficient use of NCP Exclusive Clients. Using the VPN connection or the LAN (when on the company network), the NCP Exclusive Remote Access Management provides Exclusive Clients automatically with: ▪ configuration updates ▪ certificate updates ▪ updates to the Update Client
Security Features	The NCP Exclusive Remote Access macOS Client supports the Internet Society's Security Architecture for the Internet Protocol (IPsec) and all the associated RFCs
Virtual Private Networking	RFC conformant IPsec (Layer 3 Tunneling) ▪ IPsec Tunnel Mode ▪ IPv4/6 Dual Stack Support ▪ IPsec proposals are negotiated via the IPsec gateway (IKE Phase 1, IPsec Phase 2) ▪ Communication only in the tunnel ▪ Message Transfer Unit (MTU) size fragmentation and reassembly ▪ Network Address Translation-Traversal (NAT-T) ▪ Dead Peer Detection (DPD)
Encryption	Symmetrical: AES-CBC 128, 192, 256 Bit; AES-CTR 128, 192, 256 Bit; AES-GCM 128, 256 Bit (only IKEv2); Blowfish 128, 448 Bit; Triple-DES 112 /168 Bit *Dynamic processes for key exchange:* RSA until 4096 Bit ECDSA until 512 Bit, Seamless Rekeying (PFS); Hash Algorithms: SHA, SHA-256, SHA-384, SHA-512, MD5; Diffie Hellman groups 1, 2, 5, 14-21, 25-30 (starting from group 25: Brainpool curves)
FIPS Inside	The Secure Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747) 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 Bit or Triple DES
Authentication	Internet Key Exchange (IKE): ▪ Aggressive Mode and Main Mode ▪ Quick Mode ▪ Perfect Forward Secrecy (PFS) ▪ IKE Config. Mode for dynamic allocation of private IP (virtual) address from address pool ▪ Pre-shared secrets or RSA Signatures (with associated Public Key Infrastructure)

	User authentication: ▪ XAUTH for extended user authentication ▪ One-time passwords and challenge response systems ▪ Access details from certificate (prerequisite PKI) Support for certificates in a PKI: ▪ Multi Certificate Configurations for PKCS#11 and certificate-based authentication from file system as PKCS#12 container Machine Authentication Certificate based authentication with certificates from the Apple keychain Seamless rekeying (PFS) IEEE 802.1x: ▪ Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Extended authentication relative to switches and access points (layer 2) ▪ Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): - relative to switches and access points on the basis of certificates (layer 2) RSA SecurID ready
Public Key Infrastructure (PKI) - Strong Authentication	Biometric Authentication X.509 v.3 Standard Support for certificates in a PKI via the following interfaces: ▪ PKCS#11 interface for 3rd party authentication solutions (Tokens / Smartcards) ▪ PKCS#12 interface for private keys (soft certificates) PIN policy: administrative specification of PIN entry to any level of complexity Revocation: End-entity Public-key Certificate Revocation List (EPRL formerly CRL) Certification Authority Revocation List, (CARL formerly ARL) Online Certificate Status Protocol (OCSP) Certificate Management Protocol (CMP)
Networking Features	
Secure Network Interface	Interface Filter ▪ NCP Interface Filter interfaces to all standard Network Interfaces from the PPP and Ethernet families ▪ Wireless Local Area Network (WLAN) support ▪ Wireless Wide Area Network (WWAN) support
Network Protocol	IP
Line Management	Dead Peer Detection with configurable time interval Short Hold Mode Inactivity Timeout (send, receive or bi-directional)
VPN Path Finder	NCP Path Finder Technology Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available

IP Address Allocation	Dynamic Host Control Protocol (DHCP) Domain Name Service (DNS): gateway selection using public IP address allocated by querying DNS server. When using Split-Tunneling, those domains whose DNS packets are to be routed via the VPN Tunnel can be specified exactly
Data Compression	IPsec Compression: LZS, deflate
Additional Features	VoIP prioritization UDP encapsulation PPP over Ethernet
Standards Conformance Internet Society RFCs and Drafts	Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409), Internet Key Exchange Protocol (includes IKMP/Oakley) (RFC 2406), Negotiation of NAT-Traversal in the IKE (RFC 3947), UDP encapsulation of IPsec Packets (RFC 3948), Encapsulating Security Payloads (ESP) IKE Ext. Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
Client Monitor Intuitive Graphical User Interface	Multiple language support (English, German) ▪ Monitor & Setup ▪ Online Help and License Icon indicates connection status Configuration, connection statistics, log-book (color coded, easy copy&paste function) Password protected configuration and profile management Trace tool for error diagnosis Options for starting the Monitor automatically after system reboot: either maximized; or as an icon in the menu bar

More information on NCP Exclusive Remote Access Mac Client is available on the Internet at:
https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/

For further assistance with the NCP Exclusive Remote Access Mac Client, visit:
https://www.ncp-e.com/en/service-resources/faqs/

NCP PATH FINDER

FIPS 140-2 Inside

NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com