

# Data Sheet

## NCP Exclusive Entry Client



### VPN Client Suite for Windows

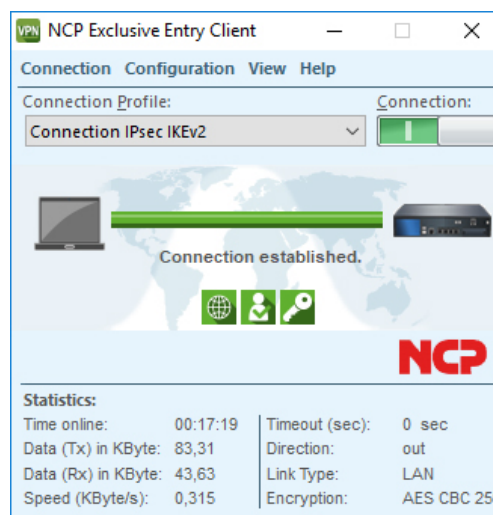
- For Juniper SRX Series
- Microsoft Windows 10, 8.x, 7
- Dynamic Personal Firewall
- Import of third party configuration files
- VPN Bypass
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- FIPS Inside
- Strong Authentication (eg. Certificate), Biometrics
- Multi Certificate Support
- Support for 3G / 4G Hardware

### Communications

The NCP Exclusive Entry Client for Windows 32/64 bit operating systems is a powerful VPN Client for the Juniper SRX Series Gateways. Recommended for organizations with up to 100 remote access users and without a requirement for the NCP Exclusive Remote Access Solution including the central management. Use the NCP Exclusive Client to establish secure, IPsec-based data links from any location in the world to Juniper SRX gateways; connection establishment over all networks is totally independent of any Microsoft dialer software.

NCP's "VPN Path Finder Technology" enables remote access even when the computer is located behind a firewall or proxy that would otherwise hinder the establishment of an IPsec tunnel; "Path Finder" automates the changeover to a modified IPsec protocol mode that uses the available HTTPS port for the VPN tunnel.

To enable a secure authentication to Microsoft Active Directory before logging into the local Windows system, the client supports domain logon via Credential Service Provider. To provide that functionality the client establishes a VPN connection to the company network before the user logon. The login procedure to the local Windows system therefore is handled through the VPN



tunnel. Secure logon to a Wi-Fi HotSpot is also supported in the pre-logon phase which means the client is optimally protected by the integrated dynamic firewall while logging on to the HotSpot. It makes no difference to the user whether they are in the office or a connected via a HotSpot.

### Security

The NCP Exclusive Entry Client also provides additional security mechanisms such as the integrated, dynamic Personal Firewall. The related configuration including rules for ports, IP addresses, IP subnets and applications can be protected by a password to disable users from unintentionally deactivating the firewall. The "Friendly Net Detection" detects whether the user's computer is located in a friendly or an unknown network. The corresponding Firewall rule is activated, dependent on the network detected, and similarly, when connecting to a hotspot, especially when logging on to and off from the Wi-Fi network. In contrast to normal firewalls, the NCP Firewall starts to work as soon as the computer is booted. Other security features include support for One-Time Password (OTP) solutions and Certificates in a Public Key Infrastructure (PKI).

### Next Generation Network Access Technology

# Data Sheet

## NCP Exclusive Entry Client



Furthermore, the VPN client features biometric user authentication before the VPN connection is established, for example via fingerprint or face recognition. Authentication takes place directly after clicking the Connect button in the client GUI, and the connection is not established until authentication is completed. If hardware for biometric authentication is not present or enabled, the user can also authenticate via their password.

The Home Zone feature was developed for the special needs of home office users. They just need to click the Home Zone button and the correct network configuration is made automatically. This includes special firewall rules set up by administrators which only apply when the user is in their home office. This means that users can access their printer or scanner in the home office network. If the user leaves the Home Zone, other firewall rules will be re-enabled.

The new bypass function in the NCP VPN Client allows the IT administrator to configure the client so that certain applications are exempted from the VPN and the data is sent over the Internet even when split tunneling is disabled. This has the advantage that applications such as video streaming no longer overwhelm the server with terabytes of data.

"Multi Certificate Support" enables VPN connections between the one computer and different companies, even when each company demands an individual user certificate. "Multi Certificate" enables a number of certificate settings to be defined and then individually allocated to specific connection profiles.

FIPS: the embedded cryptographic module is validated according to FIPS 140-2 (certificate #1747).

In the extreme case, all Secure Client parameter settings can be blocked by the administrator, preventing the user from making any changes; alternatively, certain situation specific parameters can be individually unblocked ensuring that all situations can be suitably catered for.

### **Ease of Use and Cost Effectiveness**

Ease of use serves to make the NCP Exclusive Entry Client unique on the market. The integrated dialer automatically establishes the connection to the Internet, and media type detection always selects the fastest available communication network while starting to establish the VPN tunnel. The intuitive graphical user interface (GUI) keeps the user updated on the state of the network and its security level, before and during a VPN connection. Detailed logs help to ensure rapid support from the help-desk in the event of unforeseen problems, and a configuration wizard simplifies creation of profiles. The Secure Client supports Wi-Fi/WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network, 2G, 3G, 4G). The mobile wireless network configuration, including Access Point Name (APN), is derived automatically from the SIM card being used, together with the details of the corresponding mobile wireless provider.

This is particularly beneficial when working abroad; the user is free to purchase and use a SIM card from the most cost-effective local provider.

The Budget Manager enables the most economic operation; volume or time budgets or providers can be defined and monitored.

The Secure Client's GUI includes a freely configurable area for displaying the customer logo or support notice, and the GUI itself is designed for barrier free operation, with support for the operation of a screen reader.

## Next Generation Network Access Technology

# Data Sheet

## NCP Exclusive Entry Client



### Operating Systems

Windows 10, 8.x, 7 (on x86 or x86-64 Processorarchitecture)

### Juniper SRX/vSRX OS

Junos OS 15.1X49-D80 or higher is required

### Security Features

The Exclusive Entry Client supports all major IPsec standards in accordance with RFC

### Personal Firewall

### Firewall Configuration\*

Stateful Packet Inspection;  
IP-NAT (Network Address Translation);  
Friendly Net Detection (Firewall rules adapted automatically if connected network recognized based on its IP subnet address, the DHCP server's MAC address or an NCP FND Server\*);  
Start FND dependent action;  
Secure hotspot logon;  
Homezone;  
Differentiated filter rules relative to: protocols, ports, applications and addresses, LAN adapter protection, IPv4 and IPv6 support, Central administration

### VPN Bypass

The VPN Bypass function allows the administrator to define applications which can communicate over the Internet directly despite disabling split tunneling on the VPN connection. It is also possible to define which domains or target addresses can bypass the VPN tunnel.

### Virtual Private Networking

IPsec (Layer 3 Tunneling), RFC-conformant; IPsec proposals can be determined through the IPsec gateway (IKEv1/IKEv2, IPsec Phase 2);  
Event log;  
communication only in the tunnel;  
MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T);  
IPsec tunnel mode

### Encryption

Symmetric processes: AES (CBC, CTR, GCM) 128,192,256 bits; Blowfish DES, Triple DES;  
Dynamic processes for key exchange: RSA to 2048 bits; seamless rekeying (PFS);  
Hash algorithms: SHA-1, SHA-256, SHA384, SHA-512, MD5, DH group 1,2,5,14-21, 25-30

### FIPS Inside

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

- DH 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 and 256 Bit or Triple DES

## Next Generation Network Access Technology

# Data Sheet

## NCP Exclusive Entry Client



### Authentication Processes

IKE (Aggressive Mode and Main Mode, Quick Mode);  
XAUTH for extended user authentication; IKEv2  
IKE config. mode for dynamic assignment of a virtual address from the internal address pool (private IP);  
PFS;  
PAP, CHAP, MS CHAP V.2;  
IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2);  
EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): Extended authentication relative to switches and access points on the basis of certificates (Layer 2); support of certificates in a PKI: Soft certificates, smart cards, and USB tokens and certificates with ECC  
Multi-certificate configuration, Pre-shared secrets, one-time passwords, and challenge response systems (e.g. RSA SecurID ready)

---

### Strong Authentication

X.509 v.3 Standard; biometric Authentication (Windows 8.x or higher)

---

### Standards

#### PKI Enrollment\*

PKCS#11 interface for encryption tokens (USB and smart cards); smart card operating systems: TCOS 1.2, 2.0 and 3.0; smart card reader interfaces: PC/SC, CT-API;  
PKCS#12 interface for private keys in soft certificates; CSP for the use of user certificates in the windows certificate store  
PIN policy;  
administrative specification for PIN entry in any level of complexity;  
revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL), OCSP. CMP\* (Certificate Management Protocol)

---

### Networking Features

LAN emulation: Ethernet adapter with NDIS interface, full WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network, Windows 7 Mobile Broadband) support

---

### Network Protocol

IP

---

### Dialers

NCP Internet Connector, Microsoft RAS Dialer (for ISP dial-in via dial-in script)

---

### VPN Path Finder

NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible

---

### IP Address Allocation

DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via DNS server

---

### Communication Media

Internet, LAN, Wi-Fi, GSM (incl. HSCSD), GPRS, 3G, LTE, HSDPA, PSTN, ISDN.

## Next Generation Network Access Technology

# Data Sheet

## NCP Exclusive Entry Client



---

### Line Management

DPD with configurable time interval;  
Short Hold Mode;  
Wi-Fi roaming (handover);  
Channel Bundling (dynamic in ISDN) with freely configurable threshold value;  
Timeout (controlled by time and charges);  
Budget Manager;  
Connection Modes: automatic, manual, variable (reconnection dependent on how previous disconnect invoked)

---

### APN from SIM Card

APN (Access Point Name) defines access point of a mobile data connection at a provider. If user changes provider, system automatically uses APN data from SIM card to configure Secure Client

---

### Data Compression

IPCOMP (lzs), deflate

---

### Additional Features

UDP encapsulation, WISPr-support, IPsec-Roaming, Wi-Fi roaming, Split Tunneling

---

### Point-to-Point Protocols

PPP over ISDN, PPP over GSM, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

---

### 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; RFC 7427: IKEv2-Authentication (Padding-method)

---

### Client Monitor

#### Intuitive, Graphical User Interface

Multilingual (English, German);  
Intuitive operation;  
Configuration, Connection Management and Monitoring, Connection Statistics, Log-files, Internet availability test, Trace Tool for error diagnosis;  
Traffic light icon for display of connection status;  
Integrated support of Mobile Connect Cards, embedded);  
Client Monitor can be tailored to include company name or support information;  
Password protected configuration management and profile management, configuration parameter lock

\*) If you wish to download NCP's FND server as an add-on, please click here:

<https://www.ncp-e.com/en/resources/download-vpn-client.html>

More information: <https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/>

You can test a free, 30-day full version of the Exclusive Entry Client here:

<https://www.ncp-e.com/en/resources/download-vpn-client.html>



**NCP** PATH FINDER

Option: Central management and endpoint security (upgrade to NCP Exclusive Remote Access Client)

## Next Generation Network Access Technology