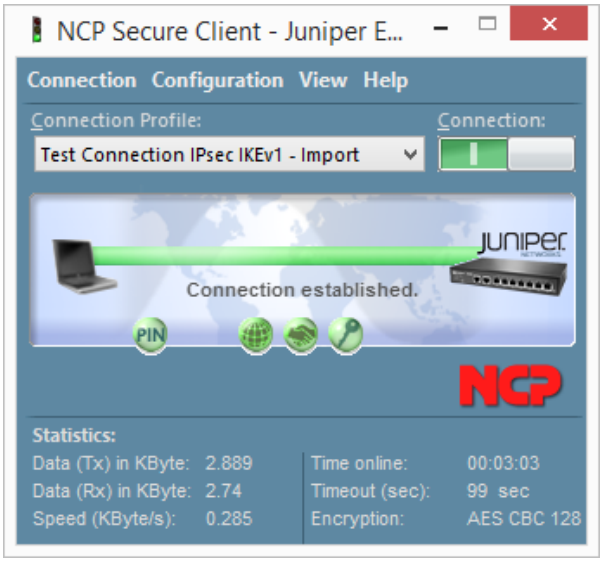
Data Sheet

NCP Secure Client – Juniper Edition

Versatile VPN Client for 32-/64-bit Windows (Windows 10, 8.x, 7, Windows Vista) – Simple and highly secure Remote Access via Internet

- Compatible with Juniper VPN Gateways (IPsec-Standard)
- Easy-to-use and easy-to-install
- Simple Profile Creation (Profile Import functionality)
- FIPS Inside
- Fast connection
- Stable connectivity in overlapping networks
- Integration of all security and communication technologies for universal remote access
- Universal support of Mobile Broadband Cards
- Perpetual license
- Free 30 day full version



Universality and Communications

The NCP Secure Client – Juniper Edition for 32-/64-bit Win-dows is a communication software package for universal implementation in any remote access VPN environment. Allowing the teleworker transparent and complete secure access to the corporate networks from any location (e.g. coffee-shop, hotel or on the road) as if one were present at the workplace at the office. Highly secure (IPsec) data connections to Juniper VPN gateways can be established. Clients can be used on 32-/64-bit versions of Windows 8.x/7, Windows Vista and Windows XP to access company data networks and applications from any location. Smooth remote access is possible even within overlapping networks, i.e. between two networks which have the same IP-address range. For example, the Wi-Fi network at a hotel and the corporate headquarters may cause such a scenario. Support for Mobile Broadband sticks for WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network) enables universal mobile computing over wireless networks.

Security

The NCP Secure Client – Juniper Edition offers extensive security mechanisms that prevent attacks in any remote access environment. In addition to data encryption the most important integrated components are: support of OTP (One-Time Password tokens) and certificates in a PKI (Public Key Infrastructure). The cryptographic module complies with the requirements of FIPS 140-2 (certificate #1051).

Usability and Profitability

"Easy-to-use" for both, user and administrator - the NCP Secure Client – Juniper Edition offers simple installation and simple operation. A graphical, intuitive user interface provides information on all connection and security states. Detailed log information paves the road for effective assistance from the help desk. A configuration wizard enables easy set up of connection profiles. The Client Monitor can be tailored to include your company name or support information. Usability also means cost reduction through less time spent for training, less documentation and fewer support cases.

VPN tunnels can be configured to be established automatically.

Product Licenses and Software Activation

The NCP Secure Client – Juniper Edition can be purchased with either a single license or volume licenses. In the case of a single license, the software must be manually activated on each separate machine.

This is not necessary with volume licensing as the Volume License Server (VLS) takes care of both license distribution and management. The VLS not only simplifies activation considerably, it makes the whole licensing process more secure as it uses the VPN infrastructure.

Data Sheet

NCP Secure Client – Juniper Edition

Operating Systems	Windows (32 Bit): Windows 10, Windows 8.x, Windows 7, Windows Vista Windows (64 Bit): Windows 10, Windows 8.x, Windows 7, Windows Vista
Requirement	Juniper IPsec Gateway (ScreenOS, Junos)
Security Features	The NCP Secure Client – Juniper Edition supports all IPsec standards in accordance with RFC
Virtual Private Networking	IPsec (Layer 3 Tunneling),conform to RFC; IPsec proposals can be determined through the IPsec gateway (IKE, 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 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 group 1,2,5,14
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 #1051). FIPS compatibility is always given if the following algorithms are used for set up 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
Authentication Standards	IKE (Aggressive mode and Main Mode), Quick Mode; XAUTH for extended user authentication; IKE config mode for dynamic assignment of a virtual address from the internal address pool (private IP); PFS; Support of certificates in a PKI: Soft certificates, smartcards, and USB tokens: Multi Certificate Configurations; Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready
Strong Authentication - Standards	X.509 v.3 Standard; Entrust Ready PKCS#11 interface for encryption tokens (USB and smartcards); smartcard 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 use of user certificates in Windows certificate store PIN policy; Administrative specification for PIN entry to any level of complexity; Revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL), OCSP
Networking Features	LAN emulation: Virtual Ethernet adapter with NDIS-Interface; full WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network) support
Network Protocol	IP

Data Sheet

NCP Secure Client – Juniper Edition

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
Line Management	DPD with configurable time interval; Short Hold Mode
Additional Features	Import of the file formats:*.ini, *.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)
Client Monitor **Intuitive, Graphical User Interface**	Multilingual (German, English, Spanish, French); Client Info Center; Configuration, Connection statistics, log-files (color displayed, easy copy&paste-function); Internet availability test; Trace tool for error diagnosis; Traffic light icon for display of connection status; Client Monitor can be tailored to include your company name or support information; Automatic check for newer software version
Volume License Server (VLS)	Simplifies license distribution - automates the management and distribution of any number of licenses to the corresponding individual machines. Windows OS (32/64bit): Windows 7, Vista. Windows Server: 2003R2 (32bit) 2008SP2 (32/64bit) 2008R2SP1 (32/64bit) VLS web-based management interface accessible from a remote machine (with password and encrypted): Web Browser (recommended): Windows Internet Explorer from v8.0, Mozilla Firefox from v5.0

Download 30 day full version:
https://www.ncp-e.com/en/resources/download-vpn-client.html

NCP sales contacts for Juniper partners:
Americas: Juniper_americas@ncp-e.com
Rest of World: Juniper_rw@ncp-e.com

FIPS 140-2 Inside

NCP PATH FINDER

Next Generation Network Access Technology