

Next Generation Network Access Technology

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

- ▶ **Compatible with Juniper VPN Gateways (IPsec-Standard)**
- ▶ **One Click Solution**
- ▶ **Simple Profile Creation (Profile Import functionality)**
- ▶ **Strong Authentication**
- ▶ **Integration of all security and communication technologies for universal remote access**
- ▶ **Easy to install**
- ▶ **Fast connection**
- ▶ **Free 30 day full version**



Universality and Communication

The NCP Secure Client – Juniper Edition for 32-/64-bit Windows 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 7, Windows Vista and Windows XP to access company data networks and applications from any location.

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).

Download 30 day full version

<http://www.ncp-e.com/en/about-us/oem-partners/ncp-juniper-cooperation.html>

NCP sales contacts for Juniper partners:

Americas: juniper_americas@ncp-e.com
Rest of World: juniper_rw@ncp-e.com

More information on NCP Secure Client – Juniper Edition is available on the Internet at:

<http://www.ncp-e.com/en/about-us/oem-partners/ncp-juniper-cooperation.html>

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.

Messaging Center

The integrated Messaging Center allows for simple yet effective authentication to take place at Wi-Fi/Hotspots using One-Time Password communicated via text messages/SMS (if required).

Technical Data

Operating Systems	Windows (32 Bit): Windows7, Windows Vista, Windows XP, Windows (64 Bit): Windows7, Windows Vista, Windows XP
Requirement	Juniper IPsec Gateway
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
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; PAP, CHAP, MS CHAP V.2; Transport Layer Security: Extended authentication relative to switches and access points using certificates (Layer 2); 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	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 in 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
Network Protocol	IP
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 Messaging center for sending and receiving SMS
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T)
Client Monitor Intuitive, Graphical User Interface	Multilingual (English, German); Client Info Center; Configuration, Connection statistics, log-files (color displayed, easy copy&paste-function); 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; password protected configuration management and profile management