

## Next Generation Network Access Technology

**VPN Client für 32/64 Bit Betriebssysteme - Windows 7, Windows Vista, Windows XP**  
**Einfacher, hochsicherer Remote Access via Internet.**

- ▶ **Kompatibilität zu allen Juniper VPN Gateways (IPsec-Standard)**
- ▶ **One Klick - Solution**
- ▶ **Einfache Profilerstellung (Importfunktion)**
- ▶ **Starke Authentisierung**
- ▶ **Integration aller für Remote Access erforderlichen Sicherheits- und Kommunikationstechnologien**
- ▶ **Kostenlose 30-Tage Vollversion**



einfach per Copy & Paste übernommen werden. Fehlbedienungen sind damit ausgeschlossen.

### Universelle Kommunikation

Der NCP Secure Client – Juniper Edition ist eine Kommunikationssoftware für den Einsatz in beliebigen Remote Access-Umgebungen. Ob von zuhause oder unterwegs im Hotel oder bei Geschäftspartnern, Teleworker arbeiten in der gewohnten Weise wie am Büroarbeitsplatz. Auf Basis des IPsec-Standards können hochsichere Datenverbindungen zu allen Juniper VPN Gateways hergestellt werden. Der Zugriff auf zentrale Datenbestände und Ressourcen kann von beliebigen Standorten, weltweit mit jedem Endgeräte unter einem Windows 32 oder 64 Bit-Betriebssystem erfolgen.

### Sicherheit

Die integrierten Sicherheitsmechanismen des NCP VPN Clients bieten einen umfassenden Schutz des Endgerätes und Firmennetzes vor jedweden Attacken unberechtigter Dritter. Wichtigste Security-Bausteine sind neben der performanten Datenverschlüsselung, eine starke Authentisierung auf Basis von OTP-Tokens (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure).

Ein Novum ist das NCP SMS-Center. Es dient der einfachen Authentifizierung am WiFi/Hotspot via SMS. Die Anfrage per SMS an den Provider erfolgt direkt über die Client Software. Das übermittelte Einmalpasswort kann ebenfalls

### Usability und Wirtschaftlichkeit

„Easy-to-use“ für Anwender und Administrator – d.h. die Einfachheit von Bedienung und Installation der NCP VPN Client Software ist einzigartig am Remote Access-Markt. Die grafische, intuitive Benutzeroberfläche informiert über alle Verbindungs- und Sicherheitsstati vor und während einer Datenverbindung. Detaillierte Log-Informationen sorgen im Servicefall für rasche Hilfe durch den Helpdesk. Ein Konfigurations-Assistent ermöglicht das einfache Anlegen von Profilen. Ein Textfeld im Monitor kann beliebig gestaltet werden, z.B. Firmenlogo, Supporthinweise. Usability bedeutet auch Kosteneinsparungen durch Verringerung des Schulungsaufwands, weniger Dokumentation und Entlastung des Helpdesk.

### Download 30 Testversion

<http://www.ncp-e.com/de/ueber-uns/oem-partner/ncp-juniper-kooperation.html>

### NCP Vertriebskontakt für Juniper Partner:

Nordamerika: [juniper\\_americas@ncp-e.com](mailto:juniper_americas@ncp-e.com)  
 Rest of World: [juniper\\_rw@ncp-e.com](mailto:juniper_rw@ncp-e.com)

## Technische Daten

<b>Betriebssysteme</b>	Windows (32 Bit): Windows7, Windows Vista, Windows XP, Windows (64 Bit): Windows7, Windows Vista, Windows XP
<b>Security Features</b>	Unterstützung aller IPsec Standards nach RFC
<b>Virtual Private Networking</b>	IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec - Gateway (IKE, IPsec Phase 2); Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T);IPsec Tunnel Mode
<b>Verschlüsselung (Encryption)</b>	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 2048 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-256, SHA-384, SHA-512,MD5, DH Gruppe 1,2,5,14
<b>Authentisierungsverfahren</b>	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; PAP, CHAP, MS CHAP V.2; Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens; Multi-Zertifikatskonfiguration;Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme; ORSA SecurID Ready.
<b>Starke Authentisierung - Standards</b>	X.509 v.3 Standard; Entrust Ready PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2, 2.0 und 3.0 Smart Card ReaderInterfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; CSP zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher. PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-Key Certificate Revocation List, <i>vorm. CRL</i> ), CARL (Certification Authority Revocation List, <i>vorm. ARL</i> ), OCSP.
<b>Networking Features</b>	LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface
<b>Netzwerkprotokoll</b>	IP
<b>IP Address Allocation</b>	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
<b>Line Management</b>	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode;
<b>Weitere Features</b>	Importfunktion der Dateiformate*.ini und *.spd. SMS-Center zum Empfangen und Versenden von SMS-Nachrichten
<b>Internet Society RFCs und Drafts</b>	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)
<b>Client Monitor Intuitive, grafische Benutzeroberfläche</b>	Mehrsprachig (Deutsch, Englisch); Client Info Center; Konfiguration, Verbindungsstatistik, Log-Files (farbige Darstellung, einfache Copy&Paste-Funktion); Trace-Werkzeug für Fehlerdiagnose; Ampelsymbol für Anzeige des Verbindungsstatus; individuell gestaltbares Textfeld; Konfigurations- und Profil-Management mit Passwortschutz