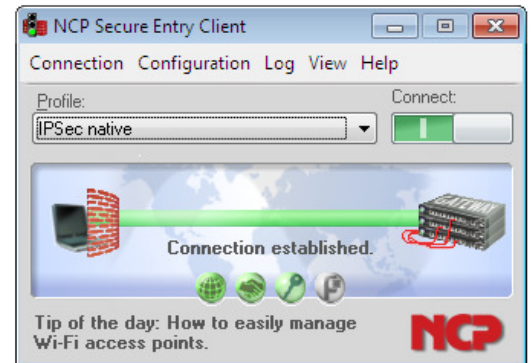


Next Generation Network Access Technology

Universal IPsec Client software for Windows 32/64-bit operating systems
incl. Windows 7

- ▶ **Compatible with VPN gateways (IPsec standard)**
- ▶ **Import of third party configuration files**
- ▶ **Integrated, dynamic personal firewall**
- ▶ **Fallback IPsec → HTTPS (VPN Path Finder Technology)**
- ▶ **Strong authentication**
- ▶ **Budget Manager for cost control**
- ▶ **Integrated support of Mobile Connect Cards**
- ▶ **Free of charge 30 day full version**



Universality and Communication

The NCP Secure Entry Client for Windows 32/64 bit operating systems is a communication software product for universal implementation in any remote access VPN environment. The teleworker works transparently and securely at any location (mobile or stationary) in the same manner as he works at his office on the corporate campus. Highly secure data connections to VPN gateways from all well-known suppliers can be established on the basis of IPsec standards. Independent of Microsoft remote data transmission dialer, the connection can be set up via any type of network (wire networks, wireless networks, LAN, Wi-Fi and internet). Teleworkers can use any end device with Windows 32 or 64 Bit operating systems to access central data networks and applications from any location. Even if the access point or the IP address changes, Wi-Fi roaming or IPsec roaming maintains the VPN connection. The NCP Secure Entry Client, a VPN Client Suite, unites all communication and security mechanisms, which are necessary for remote access, under one graphical user interface.

Security

The NCP Secure Entry Client offers extensive security mechanisms that repel attacks in any remote access environment. Hence, it offers comprehensive security of both, the end device and the corporate network. This is true, even at hotspots during the logon and logoff process to the Wi-Fi network. In addition to data encryption the most important integrated components are: a dynamic personal firewall, support of OTP (One-Time Password tokens) and certificates in a PKI (Public Key Infrastructure). Use the personal firewall to define policies for: Ports, IP addresses and segments, as well as

applications. An additional safety criterion is "Friendly Net Detection", i.e. automatic detection of secure and non-secure networks. The appropriate firewall rules are activated or deactivated depending on whether a friendly net is detected. In contrast to common firewalls, the NCP firewall is already activated at system startup. All Client configurations can be locked by the administrator which means, the user cannot change the locked configurations.

Usability and Profitability

"Easy-to-use" for both, user and administrator - the NCP Secure Entry Client offers simple installation and simple operation. A graphical, intuitive user interface provides information on all connection and security states. Detailed log information paves the ground for fast help from the help desk. The feature "automatic media detection" automatically selects the fastest communication medium available. A configuration wizard enables easy set up of profiles. Integrated support of Mobile Connect Cards for 3G, GPRS, and Wi-Fi means that additional installation of the user interface supplied by the card manufacturers is not necessary. Domain logon, too, is of course highly secure and as convenient and familiar as it is in the local network. Usability also means cost reduction through less trainings time, less documentation and fewer support cases for the help desk. An integrated budget manager guarantees cost transparency because a volume or time budget or the use of a certain provider can be set and monitored.

Technical data

Operating systems	Windows (32-bit): Windows 7, Windows Vista, Windows XP, Windows 2000 (is canceled from V.9.2) Windows (64-bit): Windows 7, Windows Vista, Windows XP
Security features	The Entry Client supports all IPsec standards in accordance with RFC
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Friendly Net Detection (analysis of: current network address, IP address and MAC address of the DHCP server); secure hotspot logon; differentiated filter rules relative to: Protocols, ports and addresses, LAN adapter protection
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 processes	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; 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, smartcards, and USB tokens: 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 and 2.0; smart card reader interfaces: PC/SC, CT-API; PKCS#12 interface for private keys in soft certificates; PIN policy; administrative specification for PIN entry in any level of complexity; revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly <i>CRL</i>), CARL (Certification Authority Revocation List, formerly <i>ARL</i>), OCSP.
Networking features	LAN emulation: Ethernet adapter with NDIS interface
Dialer	NCP Secure Dialer, Microsoft RAS Dialer (for ISP dial-in via dial-in script) connection manager for international dial-in via GoRemote (formerly <i>GRIQ</i>), UuNet, Infonet, MCI (on request)
VPN Path Finder	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is no possible (prerequisite: NCP Secure Enterprise Server V 8.0 is required)
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
Transmission media	Stationary networks: analog telephone network, ISDN, xDSL, LAN wireless networks: Wi-Fi, GSM (incl. HSCSD), GPRS, 3G, HSDPA, Internet
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 (administration of connection time and/or -volume for GPRS/ 3G and Wi-Fi, in case of GPRS/ 3G separated administration of roaming abroad).
Data compression	Stac (lzs), deflate
Additional features	Prioritization of VoIP (QoS), UDP encapsulation, WISPr-Support, IPsec-Roaming, Wi-Fi roaming, import of the file formats: *.ini, *.pcf, *.wgx und *.spd.
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over PSTN, 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, HMAC-MD5-96, HMAC-SHA-1-96, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP
Client Monitor graphic user interface	Multilingual (German, English, French, Dutch); intuitive operation; configuration, connection management and monitoring, connection statistics, log-files, trace tool for error diagnosis; traffic light icon for display of connection status; integrated support of Mobile Connect Cards (PCMCIA); password protected configuration management and profile management, configuration parameter lock

More information on NCP Secure Entry Client is available on the Internet at:
<http://www.ncp-e.com/en/solutions/vpn-products/secure-entry-client.html>
 You can test a free, 30-day full version of Secure Entry Client (Win32/64) here:
<http://www.ncp-e.com/en/downloads/software.html>