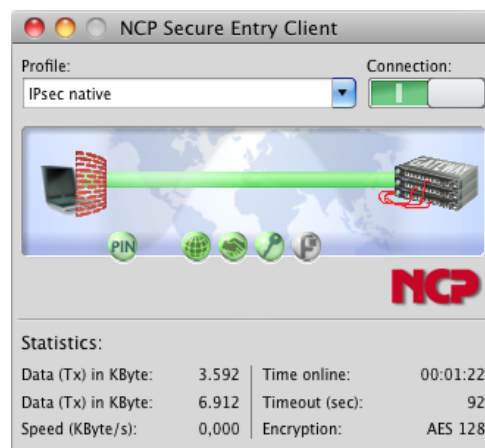


Next Generation Network Access Technology

Versatile VPN Client for Mac OS X – Simple and highly secure Remote Access via Internet.

- ▶ **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**
- ▶ **Integration of all security and communication technologies for universal remote access**
- ▶ **FIPS inside**
- ▶ **Free of charge 30 day full version**



Universality and Communication

The NCP Secure Entry Client for Mac OS X 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 within his corporate environment. Highly secure data connections to VPN gateways from all well-known suppliers can be established using IPsec standards. The connection can be set up via any type of network (also iPhone Tethering via USB or Bluetooth). Even behind firewalls, whose settings always prevent IPsec data connections, the NCP VPN Path Finder technology allows for remote access.

Security

The NCP Secure Entry Client offers extensive security mechanisms that prevent attacks in any remote access environment. Hence, it offers comprehensive security of both, the end device and the corporate 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. Apart from the graphically configurable firewall, firewall rules may also be defined for outbound connections in Mac OS X. This allows the administrator to restrict the user's internet access.

An additional safety criterion is "Friendly Net Detection" (location awareness), 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.

All Client configurations can be locked by the administrator which means, the user cannot change the locked configurations.

The IPsec Client has a cryptographic algorithm according to the FIPS standard. The embedded cryptographic module is validated according to FIPS 140-2 (certificate #1051).

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 road for effective assistant from the help desk. A configuration wizard enables easy set up of connection profiles.

Usability also means cost reduction through less time spent trainings, less documentation and fewer support cases.

VPN tunnels can be configured to be established automatically.



FIPS 140-2 Inside

Technical data

Operating Systems	Mac OS X 10.5 Leopard (Intel) and Mac OS X 10.6 Snow Leopard
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 (Firewall rules are automatically adapted, if the connected network is recognized because of its IP address area or the Mac address of a NCP FND server*), differentiated filter rules relative to: protocols, ports and addresses, LAN adapter protection; despite the built-in Mac OS X firewall the configuration of this firewall is port based.
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	Cryptographic algorithm according to the FIPS standard (Federal Information Processing Standard). The embedded cryptographic module is validated according 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: <ul style="list-style-type: none"> - 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 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; 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; PKCS#11 interface for encryption tokens (USB and smartcards); 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>).
Networking Features	Any type of network, iPhone tethering via USB or Bluetooth
Network Protocol	IP
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
Line management	DPD with configurable time interval;
Data Compression	Stac (lzs), deflate
Additional Features	UDP encapsulation, import of the file formats:*.ini, *.pcf, *.wgx, *.wge and *.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),UDP encapsulation, IPCOMP
Client Monitor Intuitive, Graphical User Interface	Multilingual (English, German); configuration, connection management and monitoring, connection statistics, log-files (color displayed,); trace tool for error diagnosis; traffic light icon for display of connection status; 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: <http://www.ncp-e.com/en/downloads/software.html>

Option: central management and endpoint security (upgrade NCP Secure Enterprise Client)

More information on NCP Secure Entry Client is available on the Internet at:
<http://www.ncp-e.com/en/solutions/vpn-products/universal-ipsec-client.html>

You can test a free, 30-day full version of Secure Entry Mac Client here: <http://www.ncp-e.com/en/downloads/software.html>