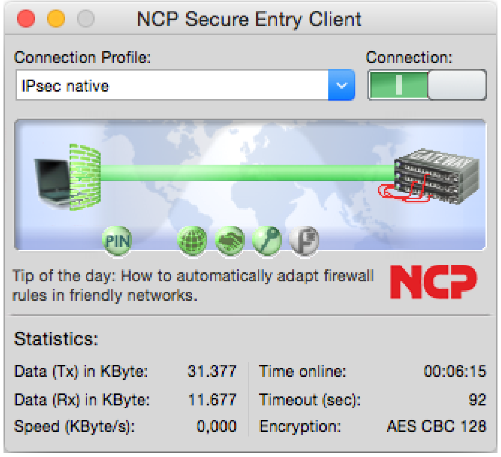
Data Sheet

NCP Secure Entry Mac Client

Universal VPN Client Suite for OS X

- 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



NCP Secure Entry Client

Connection Profile: IPsec native

Connection:

Tip of the day: How to automatically adapt firewall rules in friendly networks.

Statistics:

Data (Tx) in KByte:	31.377	Time online:	00:06:15
Data (Rx) in KByte:	11.677	Timeout (sec):	92
Speed (KByte/s):	0,000	Encryption:	AES CBC 128

Universality and Communications

The NCP Secure Enterprise Mac Client is a component of NCP's „Next Generation Network Access Technology", the comprehensive NCP Secure Enterprise Solution. Using IPsec standards as a foundation, highly secure data connections can be established, via any type of network (including iPhone Tethering via USB or Bluetooth), to VPN gateways from all well-known suppliers. Mobile workers can use their Mac devices to access their company's central data network from anywhere in the world.

Even when the Mac is located behind a firewall whose settings typically prevent IPsec data connections, NCP's "VPN Path Finder Technology" ensures that a connection to the remote gateway can always be established. "Path Finder" automatically switches to a modified IPsec protocol mode that then uses the resulting HTTPS port for the VPN tunnel. This feature mandates using an NCP Secure Enterprise VPN Server for the central VPN gateway.

Security

The NCP Secure Enterprise Mac Client provides additional security mechanisms such as the integrated, dynamic Personal Firewall. This is a managed firewall and rules for ports, IP addresses, IP subnets and applications can be defined centrally by the administrator. Based on predefined values for these security rules, "Friendly Net Detection" detects whether the Mac is located in a friendly or an unknown network. Which Firewall rule is then activated is dependent on the network detected.

Other security features include support for OTP (One-Time Password) solutions and certificates in a PKI (Public Key Infrastructure).

An Endpoint Policy Check prevents access to the corporate network by computers with inadequate security levels or that have not had the latest service-pack installed.

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).

Usability and Cost Effectiveness

"Easy-to-use" for both user and administrator – the NCP Secure Enterprise Mac Client's central management features are unique in the market. The intuitive, graphical user interface (GUI) provides information on all connection and security states and in order to save space on the desktop, the GUI can be minimized to the menu bar. A configuration wizard simplifies the set up of connection profiles and detailed log information ensures effective assistance from the help desk.

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).

Operating Systems

OS X 10.10 Yosemite, OS X 10.9 Mavericks, OS X 10.8 Mountain Lion

Security Features

The NCP Secure Entry Mac Client supports the Internet Society's Security Architecture for the Internet Protocol (IPsec) and all the associated RFCs

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (Firewall rules adapted automatically if connected network recognized based on its IP subnet address or an NCP FND server)
- Differentiated filter rules relative to: protocols, ports and addresses, LAN adapter protection
- In contrast to the application based configuration of the built-in Mac OS X firewall, the configuration of this firewall is port based

Virtual Private Networking

- IPsec (Layer 3 Tunneling)
- IPsec proposals negotiated via IPsec gateway (IKE Phase 1, IPsec Phase 2)
- Communication only in tunnel
- Message Transfer Unit (MTU) size fragmentation and reassembly
- Dead Peer Detection (DPD)
- Event log
- Network Address Translation-Traversal (NAT-T)
- IPsec Tunnel Mode

Authentication

Internet Key Exchange (IKE):

- Aggressive mode and Main mode,
- Quick mode

Perfect Forward Secrecy (PFS)

- IKE Config. mode for dynamic allocation of private IP (virtual) address from address pool
- Pre-shared secrets or RSA Signatures (and associated Public Key Infrastructure)

User authentication:

- XAUTH for extended user authentication
- One-time passwords and challenge response systems
- Authentication details from certificate (prerequisite PKI)

Support for certificates in a PKI:

- Multi Certificate Configurations for PKCS#11 and PKCS#12 interfaces
- Seamless rekeying (PFS)

IEEE 802.1x:

- Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Extended authentication relative to switches and access points (layer 2)
- Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Ex-tended authentication relative to switches and access points on the basis of certificates (layer 2)

RSA SecurID ready

Encryption and Encryption Algorithms

Symmetrical: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits
Asymmetrical: RSA to 2048 bits, dynamic processes for key exchange
Perfect Forward Secrecy

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

Hash / Message Authentication Algorithms

SHA-256, SHA-384, SHA-512, MD5
Diffie Hellman groups 1, 2, 5, 14 used for asymmetric key exchange and PFS

Public Key Infrastructure (PKI) - Strong Authentication

- 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:
  - End-entity Public-key Certificate Revocation List (EPRL formerly CRL)
  - Certification Authority Revocation List, (CARL formerly ARL)
  - Online Certificate Status Protocol OCSP

Networking Features

Any type of network

Secure Network Interface

Interface Filter

- NCP Interface Filter interfaces to all standard Network Interfaces from the PPP and Ethernet families.
- Wireless Local Area Network (WLAN) support
- Wireless Wide Area Network (WWAN) support

Network Protocol

IP

Communications Media

LAN

Communications media supported using Apple or 3rd party media interfaces and management tools:

- LAN / Ethernet
- Wi-Fi
- GPRS / 3G and GSM
- ISDN
- Modem

iPhone tethering via USB or Bluetooth

VPN Path Finder

Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available (prerequisite: NCP Secure Enterprise Server V 8.0 and later)

IP Address Allocation

Dynamic Host Control Protocol (DHCP)

Domain Name Service (DNS) : gateway selection using a public IP address allocated by querying a DNS server

Line management

DPD with configurable time interval;

Data Compression

IPCOMP (lzs), deflate

Additional Features

UDP encapsulation, import of the file formats:*.ini, *.pcf, *.wgx, *.wge and *.spd.

Internet Society RFCs and Drafts

Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),
Internet Key Exchange Protocol (IKE) (includes IKMP/Oakley) (RFC 2406),
Negotiation of NAT-Traversal in the IKE (RFC 3947),
UDP encapsulation of IPsec Packets (RFC 3948),
IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)

Client Monitor

Multilingual (English, German)
Monitor & Setup: de, en
Online Help and License de, en

Intuitive, Graphical User Interface

Traffic light icon indicates connection status
Configuration, connection statistics, Log-book (color coded, easy copy&paste function)
Password protected configuration and profile management
Trace tool for error diagnosis
Monitor can be tailored to include company name or support information
Options for starting the Monitor automatically after system reboot: either maximized, or as an icon in the menu bar

Tip of the Day

The field is integrated into Client Monitor where configuration tips and application examples can be displayed. A mouse click in this field opens an HTML page, that provides information on how to use the Client and other feature. The tips are changed on a day-by-day basis

Project Logo

Clicking on the banner in an additional field in the Client Monitor will open a local HTML page in the Mac OS X’s default browser. The banner can be replaced by a company logo and the local HTML page by a page of your choice. Both files are located in the Client’s installation directory under /ProjectLogo as logo_en.png and secure_entry_banner_en.html. In addition a “Quick-Info“ tip can be displayed when the mouse moves over the banner

*) If you wish to download NCP's FND server as an add-on, please click here:
https://www.ncp-e.com/en/resources/download-vpn-client.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:
https://www.ncp-e.com/en/products/ipsec-vpn-client-suite.html

You can test a free, 30-day full version of Secure Entry Mac Client here:
https://www.ncp-e.com/en/resources/download-vpn-client.html

FIPS 140-2 Inside