Data Sheet

NCP Secure Entry macOS Client

Universal VPN Client Suite for macOS

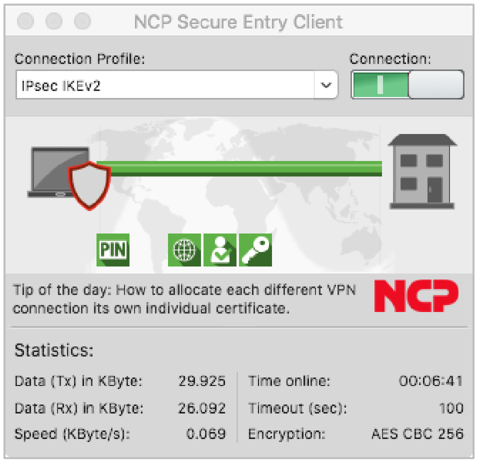
- Compatible with VPN Gateways (IPsec Standard)
- macOS 10.15, 10.14, 10.13
- VPN profile import of third-party configuration files
- IPv4/6 Dual Stack support
- Integrated, dynamic Personal Firewall
- Fallback IPsec → HTTPS (VPN Path Finder Technology)
- Strong authentication (e.g. Certificate), Biometrics
- Integration of all security and communication technologies for universal remote access
- FIPS Inside
- Support Apple Keychain
- Free of charge 30-day full version

Universality and Communication

The NCP Secure Entry macOS Client establish highly secure data connections can via any type of network (including iPhone Tethering), 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 Entry macOS 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.



Connection Profile: IPsec IKEv2

Connection:

Tip of the day: How to allocate each different VPN connection its own individual certificate.

Statistics:

Data (Tx) in KByte:	29.925	Time online:	00:06:41
Data (Rx) in KByte:	26.092	Timeout (sec):	100
Speed (KByte/s):	0.069	Encryption:	AES CBC 256

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

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 #1747).

Usability and Cost Effectiveness

"Easy-to-use" for both user and administrator – the NCP Secure Entry macOS Client's 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.

Operating Systems

macOS 10.15 Catalina, macOS 10.14 Mojave, macOS 10.13. High Sierra

Security Features

The NCP Secure Entry macOS 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
- The option “Do not allow VPN connection in friendly networks" has been added under “Friendly networks" in the firewall configuration. If this option is activated, the client cannot establish a VPN tunnel when connected to a friendly network.

Virtual Private Networking

- IPsec Tunnel mode
- IPv4/6 Dual Stack support
- IPsec proposals negotiated via IPsec gateway (IKE, Phase 2)
- Communication only in tunnel
- Message Transfer Unit (MTU) size fragmentation and reassembly

Encryption and Encryption Algorithms

Symmetric processes:
AES-CBC 128, 192, 256 Bit;
AES-CTR 128, 192, 256 Bit;
AES-GCM 128, 256 Bit (only IKEv2);
Blowfish 128, 448 Bit;
Triple-DES 112, 168 Bit
Dynamic processes for key exchange:
RSA until 4096 Bit;
ECDSA until 521 Bit, Seamless Rekeying (PFS);
Hash Algorithm: SHA, SHA-256, SHA-384, SHA-512, MD5;
Diffie-Hellman-Groups: 1, 2, 5, 14-21, 25-30 (from Group 25: Brainpool curves)

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 #1747).
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

Key Exchange

IKEv1 (Aggressive Mode und Main Mode): Pre-shared key, RSA, XAUTH;
IKEv2: Pre-shared key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP, Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383)

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 (with associated Public Key Infrastructure)

User authentication:

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

Support for certificates in a PKI:

- Multi Certificate Configurations for PKCS#11 and certificate-based authentication from file system as PKCS#12 container

Machine Authentication
Certificate based authentication with certificates from the Apple keychain

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): - relative to switches and access points on the basis of certificates (layer 2)

RSA SecurID ready

Public Key Infrastructure (PKI) - Strong Authentication

- Biometric 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, iPhone tethering via USB or Bluetooth
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 ▪ Mobile connections ▪ iPhone tethering
VPN Path Finder	Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available (prerequisite: NCP Secure Enterprise VPN Server V 8.0 and later)

IP Address Allocation	DHCP (Dynamic Host Configuration Protocol);
	IKE Config Mode (IKEv1);
	Config Payload (IKEv2);
	DNS (Domain Name Service): gateway selection using public IP address allocated by querying DNS server. When using Split-Tunneling, those domains whose DNS packets are to be routed via the VPN Tunnel can be specified exactly

Line management	DPD (Dead Peer Detection) with configurable time interval; Timeout; VPN on demand for the automatic construction of the VPN tunnel and the exclusive communication about it
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	RFC 4301 (IPsec), RFC 4303 ESP, RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IKEv1, RFC 3526, ISAKMP, RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (Redirect), RFC 7383 (Fragmentation), RFC 7427, 3279 Section 2.2.3, 3447 Section 8 (Signature Authentication), RFC

	5903, 6954, 6989, 4754 (ECC), RFC 2451, 3686 (AES with ESP), 5930 (AES-CTR), 4106 (AES-GCM), 5282, 6379 (Suite B), RFC 3447 Section 8 (Padding)
Client Monitor	Multilingual (English, German) Monitor & Setup: de, en Online Help and License de, en
Intuitive, Graphical User Interface	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 as application, 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 /Project logo 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/vpn-clients-for-windows-10-8-7-macos/

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