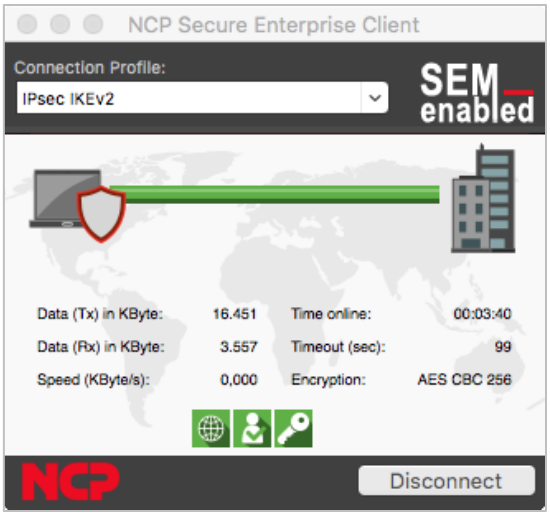
Data Sheet

NCP Secure Enterprise macOS Client

Universal, centrally managed VPN Client Suite for macOS

- Central Management and Network Access Control
- macOS 10.15, 10.14, 10.13
- Compatible with VPN Gateways (IPsec Standard)
- IPv4/6 Dual Stack Support
- Integrated, dynamic Personal Firewall
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Strong Authentication (eg. Certificate), Biometrics
- FIPS Inside



Universality and Communications

The NCP Secure Enterprise macOS 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), 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 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.

Other security features include support for OTP (One-Time Password) solutions and certificates in a PKI (Public Key Infrastructure). By storing certificates in the Apple keychain (certificate store), users are sure that their certificates are stored securely and, in conjunction with the NCP software, can be used to authenticate the secure remote-access connections. 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 #1747).

Usability and Profitability

"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.

Central Management

Rollout, commissioning and administration of NCP Secure Enterprise Mac Clients are all handled via the NCP Secure Enterprise Management as the “single point of administration”.

Data Sheet

NCP Secure Enterprise macOS Client

Operating Systems	macOS 10.15 Catalina, macOS 10.14 Mojave, macOS 10.13 High Sierra
Central Management	As the "Single Point of Management", NCP's Secure Enterprise Management (SEM) provides functionality and automation for the rollout, commissioning and efficient use of Secure Enterprise Clients. Using the VPN connection or the LAN (when on the company network), the Secure Enterprise Management (SEM) provides Enterprise Clients automatically with: ▪ configuration updates ▪ certificate updates ▪ updates to the Update Client
Network Access Control	The policies for Endpoint Security (Endpoint Policy Enforcement)) are created centrally at the Secure Enterprise Management (SEM) and each Enterprise Client is permitted access to the company network according to the corresponding rules
High Availability Services	The NCP Secure Enterprise Client supports the NCP HA Services. These services are client server based and can be used in two different operating modes: load balancing or failsafe mode. Regardless of the load on the server or whether a server has failed, the VPN connection to the company network is established reliably, in the background and without any delay for the user of the Enterprise Client
Security Features	The NCP Secure Enterprise 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, the DHCP server's MAC address or an NCP FND server*)
	▪ Supports secure hotspot logon feature
	▪ Differentiated filter rules relative to:
	  ▪ Protocols, ports or IP addresses
	  ▪ LAN adapter protection

Virtual Private Networking	RFC conformant IPsec (Layer 3 Tunneling) ▪ IPsec Tunnel Mode ▪ IPv4/6 Dual Stack Support ▪ IPsec proposals are negotiated via the IPsec gateway (IKE Phase 1, IPsec Phase 2) ▪ Communication only in the tunnel ▪ Message Transfer Unit (MTU) size fragmentation and reassembly ▪ Network Address Translation-Traversal (NAT-T) ▪ Dead Peer Detection (DPD)

Encryption and Encryption Algorithms	Symmetrical: 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 512 Bit, Seamless Rekeying (PFS); Hash Algorithms: 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 Secure Client incorporates cryptographic algorithms conformant to the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747) FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection: ▪ Diffie Hellman 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 or 256 Bit or Triple DES
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 (macOS Sierra or higher) Biometric authentication X.509 v.3 Standard Support for certificates in a PKI via the following interfaces: ▪ PKCS#11 interface for 3rd party authentication solutions (Tokens / Smartcards) ▪ PKCS#12 interface for private keys (soft certificates) PIN policy: administrative specification of PIN entry to 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) Certificate Management Protocol (CMP)*
Networking Features	
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
Line Management	Dead Peer Detection with configurable time interval Short Hold Mode Inactivity Timeout (send, receive or bi-directional)
Communications Media	LAN Communications media supported using Apple or 3rd party media interfaces and management tools: ▪ LAN / Ethernet ▪ Wi-Fi ▪ Mobile communication ▪ iPhone Tethering
VPN Path Finder	NCP Path Finder Technology: Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available**

Data Sheet

NCP Secure Enterprise macOS Client

IP Address Allocation	Dynamic Host Control Protocol (DHCP) Domain Name Service (DNS): 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
Data Compression	IPsec Compression: LZS, deflate
Additional Features	VoIP prioritization UDP encapsulation PPP over Ethernet
Standards Conformance **Internet Society RFCs and Drafts**	Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409), Internet Key Exchange Protocol (includes IKMP/Oakley) (RFC 2406), Negotiation of NAT-Traversal in the IKE (RFC 3947), UDP encapsulation of IPsec Packets (RFC 3948), Encapsulating Security Payloads (ESP) IKE Ext. Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
Client Monitor **Intuitive Graphical User Interface**	Multiple language support (English, German) ▪ Monitor & Setup: ▪ Online Help and License 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 Options for starting the Monitor automatically after system reboot: either maximized; or as an icon in the menu bar

*) 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

**) Prerequisite: NCP Secure Enterprise Management

More information on NCP Secure Enterprise MAC Client is available on the Internet at:
https://www.ncp-e.com/en/products/centrally-managed-vpn-solution.html

To ensure that you always have the latest information about NCP's products, always check the NCP website at:
https://www.ncp-e.com/en/resources/download-vpn-client.html

For further assistance with the NCP Secure Enterprise MAC Client, visit:
https://www.ncp-e.com/en/company/contact.html, Email: helpdesk@ncp-e.com

FIPS 140-2 inside