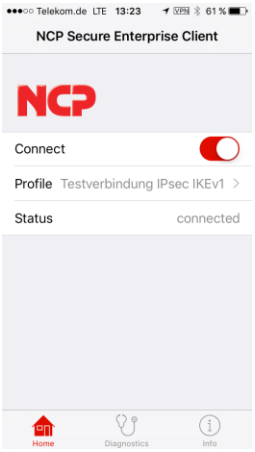
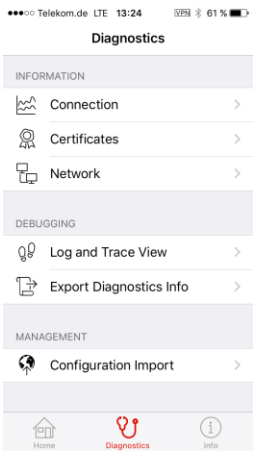
Data Sheet

NCP Secure Enterprise iOS Client

Centrally Administered
VPN Client for Apple iOS 9 & 10

- Central Management
- Configuration via NCP Secure Enterprise management
- Fallback IPsec / HTTPS (VPN Path Finder Technology)
- Central certificate rollout
- Reconnect mode (Always On)
- iOS Keychain support
- Strong Authentication





The NCP Secure Enterprise client for iOS meets the highest demands on reliability, stability and security. With an unparalleled intuitive interface, professional end users benefit from seamless integration of the client with their Apple iPhone and iPad devices.

Universally Applicable

The NCP Secure Enterprise iOS VPN Client enables a highly secure Virtual Private Network (VPN) connection to the corporate networks of companies or organizations. Access to multiple networks is supported, each connection being defined by its own VPN profile.
Using standard IPsec protocols, connections can be established from tablets and smartphones to NCP VPN gateways.

NCP VPN Path Finder Technology enables remote access even when the device is located behind firewalls or proxies that would otherwise hinder the establishment of an IPsec tunnel.

Security

The strong authentication of the NCP Secure Enterprise iOS VPN Client provides comprehensive protection against access by unauthorized third parties. Data encryption: support for OTP (One Time Password) tokens and certificates in a PKI (Public Key Infrastructure).

Usability and Cost Effectiveness

The intuitive, graphical user interface not only makes NCP Secure iOS Clients "easy to use", but also keeps the user continuously updated on the state and security level of the connection, both while the VPN is established and while it is disconnected.
Detailed logs help to ensure rapid support from the helpdesk in the event of unforeseen problems. Usability, in turn, means cost savings as less training and documentation are required, and the load on the helpdesk is reduced.

Central Management

The NCP Secure Enterprise iOS VPN Client is optimized for management by NCP's Secure Enterprise Management (SEM). SEM incorporates extensive Endpoint Security capabilities which can be integrated, for example, in the central manage and distribution of user configurations and certificate updates.
So user configurations and certificate updates can be managed centrally. For the initial set-up the client is pre-configured with a minimum configuration. Then its individual configuration and any certificates are provided by the SEM. After that, the user will not be able to gain access to the assigned configuration.

Data Sheet

NCP Secure Enterprise iOS Client

Operating Systems	iOS 9.0 and above
Central Management	Distribution of VPN configurations and certificates from the NCP Secure Enterprise Management
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC conformant; Communication only in tunnel; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Encryption	Symmetric processes: AES-CBC, AES-CTR (RFC 3686, 5930) and AES-GCM (RFC 4106, 5282) both with 128,192,256 bits; Blowfish 128,448 bits; Triple DES 112,168 bits; Dynamic processes for key exchange: RSA to 4096 bits; ECDSA to 521 bit; Seamless Rekeying (PFS); Hash Algorithms: SHA-256, SHA-384, SHA-512, MD5, DH Groups 1, 2, 5, 14-18, 19-21, 25, 26
Authentication Process	IKEv1 Pre-shared key, RSA, XAUTH IKEv2 Pre-shared key, RSA, EAP, Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383)
Strong authentication	iOS Keychain for using User (Soft) Certificates One-Time Passwords and Challenge Response System; RSA SecurID Ready
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) when port 500 or UDP encapsulation cannot be used (prerequisite: NCP VPN Path Finder Technology required at the VPN Gateway
IP Address Assignment	IKE Config Mode (IKEv1); Config Payload (IKEv2); manuel configuration
Line Management	DPD (Dead Peer Detection) with configurable polling interval; Timeout
Data Compression	IPCOMP (lzs), Deflate
Other Features	UDP encapsulation, Split Tunneling
Internet Society RFCs and Drafts	RFC 4301 (IPsec), RFC 4303 (ESP), RFC 3947 (NAT-T), RFC 3948 (UDP encapsulation), RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (IKEv2 Redirect), RFC 7383 (IKEv2 Fragmentation), RFC 7427 (IKEv2 Signature Authentication)
Client Monitor **Intuitive GUI**	English, German; Connection control and management, connection statistics, log files; trace tool for error diagnosis

Technical changes reserved

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299