NCP Secure Entry macOS Client
Release Notes

Major Release: **4.00 r46079**
Date: **October 2019**

Prerequisites

Apple macOS operating systems:
The following Apple macOS operating systems are supported with this release:

- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13

1. New Features and Enhancements

Update for macOS Catalina 10.15

The macOS client is certified by Apple from this version and is therefore fully compatible with macOS Catalina 10.15. Permission to install the kernel extension must be granted explicitly during installation in the “Security and Privacy” settings.

Virtual Network Adapter

The macOS client has its own virtual network adapter. This allows VoIP applications to route data through the VPN tunnel. It also means that the client can use the IP protocol within the VPN tunnel even when this protocol is not used in the physical network. Example: IPv6 can be used within the VPN Tunnel although the physical network only supports IPv4.

Connect/Disconnect Dock Menu

If a VPN profile is configured for the VPN client, the selected connection can be connected or disconnected via a right click on the Dock menu icon.

2. Improvements / Problems Resolved

Optimized DNS Request Handling

With the implementation of the new network adapter, the handling of DNS requests has been improved. This supports two different modes:

1. Split tunneling disabled
   If split tunneling is disabled, all communication to other IP addresses that are not within the current IP address range is routed via the VPN tunnel. This also to DNS requests.
2. Split tunneling enabled
   In this mode the IP remote networks are defined in the split tunneling configuration. If the destinations are addressed within the remote network, the data is routed via the VPN tunnel. All other data – in particular DNS requests – bypass the VPN tunnel. This means that

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

destinations on the remote network cannot initially be reached via their domain names, as public DNS servers do not usually resolve internal company DNS names.
This problem can be avoided by explicitly adding internal domain names that are used within the remote network to the configuration. For example, adding the entry `company.local` will ensure that relevant DNS requests such as `intranet.company.local` are correctly routed through the VPN tunnel to the internal company DNS server.
This configuration option enables the separation of data which is routed through the VPN tunnel and data that bypasses the VPN tunnel.

New Connection Mode

The “Automatic” connection mode has been removed and the “Always” connection mode has been added. If the connection mode is set to “Always” the client will continuously attempt to establish a connection. In comparison to the “Automatic” mode, the connection attempt will be made even without pending data transfer.

3. Known Issues

Certificate File Location

Following the updates for macOS Catalina, p12 certificate files may no longer be stored in any location. If the user attempts to store the certificate file in a system folder created automatically in the home directory such as `Documents`, `Desktop` or `Downloads`, the message "Permission denied" will be displayed. Users can only save certificate files in a folder directly beneath the home directory.

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

4. Getting Help for the NCP Secure Entry macOS Client

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/version-information/

E-Mail: support@ncp-e.com

5. Features

Operating Systems

See Prerequisites on page 1.

Security Features

Support of the Internet Society's Security Architecture for IPsec and all the associated RFCs.

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

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, applications and IP addresses

Encryption

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 to 4096 Bit;
ECDSA to 521 Bit, Seamless Rekeying (PFS);
Hash Algorithms: SHA, SHA-256, SHA-384, SHA-512, MD5;
Diffie Hellman groups: 1, 2, 5, 14-21, 25-30 (starting from group 25: brainpool curves);

Key exchange

IKEv1 (Aggressive Mode and 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);

VPN Path Finder

NCP Path Finder Technology: Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available. **

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 #1051).
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 lenght of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192, 256 Bit or Triple DES

Split Tunneling

When using Split-Tunneling, those domains whose DNS packets are to be routed via the VPN Tunnel can be specified exactly.

Authentication

Internet Key Exchange (IKE):
Aggressive Mode, Main Mode,
Quick Mode, IKEv2
Perfect Forward Secrecy (PFS),
IKE config mode for dynamic assignment of a virtual address from the internal address pool (private IP),
Pre-shared secrets or RSA signatures (with corresponding Public Key Infrastructure);

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

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

Support for certificates in a PKI:
Multi Certificate Configurations for PKCS#11 and PKCS#12;

Machine Authentication:
Authentication with certificates from filesystem or the macOS key ring;

Seamless Rekeying (PFS);

IEEE 802.1x:
EAP-MD5: Extensible Authentication Protocol (Message Digest 5), extended authentication relative to switches and access points (Layer 2);
EAP-TLS: Extensible Authentication Protocol (Transport Layer Security), extended authentication relative to switches and access points on the basis of certificates (Layer 2);

RSA SecurID Ready;

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;

Strong Authentication (Standards)

X.509 v.3 Standard;

Support for certificates in a PKI:
PKCS#11 interface for 3rd party authentication solutions (Tokens / Smartcards)
PKCS#12 interface for private keys (soft certificates);

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;

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
Intuitive GUI

English, German;
Configuration update;

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

Connection control and management;
Connection statistics, log files;
Trace tool for error diagnostics;
Network information;

* NCP FND-Server download for free: https://www.ncp-e.com/en/resources/download-vpn-client/
** Prerequisites: NCP Secure Enterprise VPN Server

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299