NCP Secure Entry macOS Client

Release Notes

Service Release: **3.20 r43098**
Date: **March 2019**

Prerequisites

Apple macOS operating systems:

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

- macOS Mojave 10.14
- macOS High Sierra 10.13
- macOS Sierra 10.12

1. New Features and Enhancements

IPv6 Support

The client supports dual stack operation. For this purpose IPv4 only, IPv6 only or IPv4 and IPv6 can be selected in the configuration. Split tunneling configuration can be configured individually for both protocols.

Dark Mode Support

The client GUI supports the dark mode introduced with macOS Mojave.

macOS Keychain Support

A user certificate can be configured under computer certificate configuration for use in the macOS keychain. This requires the certificate to be imported into the system keychain beforehand. To use the private key contained in the certificate, access must be granted for the NCP service `ncprwsmac` to the directory `/Library/Application Support/NCP/Secure Client/`.

2. Improvements / Problems Resolved

Uninstall for macOS Mojave

During deinstallation, the user may have been asked for permission to access the address book, calendar, and photos. Although the uninstall routine did not access any data in this location this issue has now been fixed. The application icon is now also correctly removed from the Dock after uninstallation.

FND Detection

After booting the computer, friendly networks that were already connected were not detected. Friendly networks could only be detected by removing and reconnecting the network cable. This issue has been resolved.

Incorrect Access Rights for Log Files

Following an operating system update, the VPN client did not function correctly. An error message "Open log files failed" was displayed. This error scenario is detected in this client version and the access rights are automatically set correctly when the client is started.

Computer Certificates

If a computer certificate was used in the macOS keychain and RSA-PSS padding was enabled at the same time, a connection could not be established. This issue has been resolved.

Extension of Split Tunneling Configuration for Multiple DNS Suffixes

Client GUI Improvements

3. Known Issues

None.

Service Release: **3.10 r40218**
Date: **July 2018**

Prerequisites

Apple OS X operating systems:

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

- macOS High Sierra 10.13
- macOS Sierra 10.12
- OS X El Capitan 10.11
- OS X Yosemite 10.10

1. New Features and Enhancements

Biometric Authentication (Fingerprint recognition) Before VPN Connection

To prevent unauthorized third parties from establishing a VPN connection, optional biometric authentication has been integrated in the NCP Secure Client prior to VPN connection. The configuration of this option can be found under "Profile … ⇨ 'Choose profile' ⇨ Pre-Authentication ⇨ Fingerprint / Biometric authentication". If this option is enabled, the prompt for user authentication is displayed directly after clicking the Connect button in the client GUI. The VPN will only connect if authentication is successful.

Biometric authentication requires macOS Sierra 10.12.1 or newer. When using Apple hardware without fingerprint sensor, the user's password will be prompted. With older OS X platforms and enabled fingerprint option, the NCP Secure Client will not start establishing a VPN tunnel.

In conjunction with set connection mode to automatic, the user authentication is not necessary for automatic establishment of the VPN tunnel.

2. Improvements / Problems Resolved

OTP Functionality

The dialog box for entering the OTP passcode was not displayed. This issue has been fixed.

Certificate Fingerprint

The fingerprint of a certificate was not displayed in the certificate view. A comparison of the fingerprint could therefore not take place. This issue has been fixed.

3. Known Issues

FIPS mode cannot be enabled under Mac OSX 10.10.

After a system restart, the NCP FND Server is not automatically detected.
Workaround: Pull and plugin the LAN cable once

NCP Demo User Certificates

The NCP demo user certificates installed with previous client versions will expire on October 9, 2018. This means that existing test profiles such as for the NCP demo server "vpntest.ncp-e.com" will no longer work. From this client version on, new installations will no longer automatically configure these test profiles using this certificate. Only test profiles with the VPN configuration "Pre-shared key" can be created.
New certificates with extended validity are located in the certs subdirectory after installation. Previously, these certificates were located directly in the installation directory.

Service Release: **3.00 r38902**
Date: **March 2018**

Prerequisites

Apple OS X operating systems:

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

- macOS High Sierra 10.13
- macOS Sierra 10.12
- OS X El Capitan 10.11
- OS X Yosemite 10.10

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

VPN services not started due to high number of network adapters

A high number of active network adapters on your system could impede the start of the VPN client. In that case you got noticed that the VPN services could not be started. The handling of a high number of network adapters has been optimized with the result that they won't interfere with the VPN services anymore.

3. Known Issues

FIPS mode cannot be enabled under Mac OSX 10.10.

Major Release: **3.00 r37856**
Date: **November 2017**

Prerequisites

Apple OS X operating systems:

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

- macOS High Sierra 10.13
- macOS Sierra 10.12
- OS X El Capitan 10.11
- OS X Yosemite 10.10

1. New Features and Enhancements

Support for macOS High Sierra 10.13

macOS High Sierra 10.13 is fully supported. Permission to install the kernel extension must be granted manually in the system settings so that the VPN service can be started and a connection established.

New Client UI Design

Support of FIPS mode

The client can be configured with FIPS support during installation.

Full Support for IKEv2 and IKEv2 Redirect

The client supports IKEv2 from this version onwards, and IKEv2 redirect in accordance with RFC 5685 is also supported within IKEv2.

New Firewall Option

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.

2. Improvements / Problems Resolved

Improvement of DPD functionality

3. Known Issues

FIPS mode cannot be enabled under Mac OSX 10.10.

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
- 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[i])
- 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,
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);

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

Machine Authentication:
Authentication with certificates from filesystem or the OS X 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 authentification 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;
Connection control and management;
Connection statistics, log files;
Trace tool for error diagnostics;
Network informations;

* NCP FND-Server download for free: https://www.ncp-e.com/en/resources/download-vpn-client/
** Prerequisitives: NCP Secure Enterprise Server V 10.x or later