

NCP Secure Entry Mac Client

Maintenance Release 1.01 Build 10
July 2010

1. New Features and Enhancements

This is a maintenance release, there are no new features or enhancements.

2. Problems Resolved

The following describe the problems resolved in this maintenance release of the NCP Secure Entry Mac Client:

Problem description: Firewall not working after system caches have been deleted

After the Mac OS X system caches have been deleted (e.g. by maintenance tools), those system caches are automatically regenerated during the next new start. Generating the system caches takes some time, lengthening the start phase of the processor considerably. Expiry of a particular timer during this lengthened start phase could make the VPN Client, including the firewall, inoperable.

Problem resolution: The timer has been set to a default value that ensures this problem no longer occurs.

Problem description: VPN Tunnel not working when connection from Mac OS X was over PPPoE or GPRS / UMTS

When an Internet connection from Mac OS X was established over PPPoE or GPRS /UMTS, the firewall could not filter the data transferred over this connection and so a working VPN Tunnel was not created.

Problem resolution: A driver for the PPP adapter has been implemented, which integrates some GPRS / UMTS adapters. This driver implementation has resolved this problem.

Problem description: Multiple starts of the Client overwrite the stored profile settings

Problem resolution: The Secure Entry Mac Client can now only be started once per processor. This ensures that, on a started Client, if a second user performs a "fast user switching" and a restart of the Client, the profile settings of the Client are not overwritten.

Any pre-existing VPN connection of the Client is not affected by a change of user; the connection remains in existence.

Problem description: Incorrect handling of IP addresses during configuration import

During configuration import, the IP addresses from the profile settings configuration area "IPsec Address Assignment" and "Split Tunneling" were handled incorrectly.

Problem resolution: IP addresses are allocated correctly in this maintenance release.

Problem description: Timeouts ineffective with pre-connected NAT devices

If the Secure Entry Mac Client is located behind a NAT device (router that performs Network Address Translation), it independently sends IKE-Keep-Alive-Packets at a pre-defined polling interval. In the previous version, this data stream inhibited the action of a timeout, configured in the "Connection Controls" profile settings.

Problem resolution: This problem has been resolved.

Problem description: Client Error Messages

Problem resolution: Client error messages in the monitor and log window have been re-worked.

Problem description: Incomplete messages in firewall-log

After removing a network adapter or terminating a PPP based connection, the firewall-log was no longer up-dated. However, the firewall functionality was not affected by this fault.

Problem resolution: This problem has been resolved; the firewall-log is now correctly up-dated under the conditions described.

Problem description: PAP/CHAP error when using XAUTH

If a VPN connection has been initialized directly after the start of the VPN client, without changing a preset profile, the connection could not be established because of a PAP/CHAP error during the XAUTH negotiation.

Problem resolution: This error has been resolved. A proper VPN connection, after the PIN request, can be established.

3. Known Issues

- None

4. Getting Help for the NCP Secure Entry Mac Client

To ensure that you always have the latest information about NCP's products, always check the NCP website at: <http://www.ncp-e.com/en/downloads.html>

For further assistance with the NCP Secure Entry Mac Client, visit: <http://www.ncp-e.com/en/about-us/contact.html>

Mail: helpdesk@ncp-e.com

5. Revision History

Features of the previous release 1.00 build 78:

Operating Systems

Mac OS X 10.5 Leopard (Intel) and Mac OS X 10.6 Snow Leopard

Security Features

The NCP Secure Entry 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 or an NCP FND server¹)
- 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.

Virtual Private Networking

- IPsec (Layer 3 Tunneling)
- 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
- Dead Peer Detection (DPD)
- Event log
- Network Address Translation-Traversal (NAT-T)
- IPsec Tunnel Mode

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 (and associated Public Key Infrastructure)
- User authentication:
 - XAUTH for extended user authentication
 - one-time passwords and challenge response systems
- Support for certificates in a PKI:
 - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying (PFS)
- RSA SecurID ready

Encryption and Encryption Algorithms

Symmetrical: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits
Asymmetrical: RSA to 2048 bits, dynamic processes for key exchange
Perfect Forward Secrecy

FIPS Inside

The IPsec 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 length of 1024 bits)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192 or 256 Bit, or Triple DES

Hash / Message Authentication Algorithms

- SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman groups 1, 2, 5, 14 used for asymmetric key exchange and PFS

Public Key Infrastructure (PKI) - Strong Authentication

- X.509 v.3 Standard
- PKCS#11 interface for encryption tokens (USB and smartcards)
- PKCS#12 interface for private keys in soft certificates
- Administrative specification for 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

Networking Features

Any type of network, iPhone tethering via USB or Bluetooth

Network Protocol

- IP

VPN Path Finder

- NCP Path Finder Technology
 - Fallback to HTTPS (port 443) from IPsec if neither port 500 nor UDP encapsulation are available (prerequisite: NCP Secure Enterprise Server V 8.0 and later)

IP Address Allocation

- Dynamic Host Control Protocol (DHCP)
- Domain Name Service (DNS) : gateway selection using a public IP address allocated by querying a DNS server

Line Management

- Dead Peer Detection with configurable time interval

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

- Security Architecture for the Internet Protocol and assoc. RFCs (RFC2401 - 2409),
 - Internet Key Exchange Protocol (IKE) (includes IKMP/Oakley) (RFC 2406),
 - Negotiation of NAT-Traversal in the IKE (RFC 3947),
 - UDP encapsulation of IPsec Packets (RFC 3948),
 - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)

Client Monitor

Intuitive Graphical User Interface

- Bilingual (English, German)
- Traffic light 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

¹ If you wish to download NCP's FND server as an add-on, please click here:

<http://www.ncp-e.com/en/downloads/software.html>

More information on NCP Secure Entry Client is available on the Internet at:

<http://www.ncp-e.com/en/products/ipsec-client.html>

You can test a free, 30-day full version of Secure Entry Mac Client here:

<http://www.ncp-e.com/en/downloads/software.html>