

NCP Secure Enterprise MAC Client

Service Release 2.02 Build 11

Date: August 2011

1. New Feature

Compatibility to Mac OS X 10.7 Lion

This version of the des Secure Enterprise MAC Client can be used on Mac OS X 10.7 Lion platform.

2. Problems Resolved

None

3. Known Issues

None

4. Getting Help for the NCP Secure Enterprise 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 Enterprise MAC Client, visit:

<http://www.ncp-e.com/en/about-us/contact.html>

Mail: helpdesk@ncp-e.com

5. Features

Operating System Requirements

Mac OS X 10.5 Leopard (Intel) & Mac OS X 10.6 Snow Leopard, Mac OS X 10.7 Lion

Central Management

As the "Single Point of Management", NCP's Secure Enterprise Management (SEM version 2.05 or higher) 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 version 2.05 or higher) provides Enterprise Clients automatically with:

- configuration updates,
- certificate updates, and
- 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.

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
 - Network Address Translation-Traversal (NAT-T)
 - Dead Peer Detection (DPD)
 - Dynamic Host Control Protocol (DHCP)

Authentication

- Internet Key Exchange (IKE):
 - Aggressive Mode and Main Mode,
 - Quick Mode
 - Perfect Forward Secrecy (PFS)
 - IKE Config. Mode for dynamic allocation of virtual IP 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 PKCS#12 interfaces
- 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

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
Seamless Rekeying (Perfect Forward Secrecy)

Hash / Message Authentication Algorithms

- SHA-1, 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
- 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)*

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

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

Communications Media

- LAN
- Communications media supported using Apple or 3rd party media interfaces and management tools:
 - LAN / Ethernet
 - Wi-Fi
 - GPRS / 3G and GSM
 - ISDN
 - Modem
- iPhone tethering via USB or Bluetooth

Line Management

- Dead Peer Detection with configurable time interval
- Short Hold Mode
- Inactivity Timeout (send, receive or bi-directional)

Split Tunneling

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

VPN Path Finder

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

Data Compression

- IPsec Compression: LZS, deflate

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)

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 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

Client Monitor

Intuitive Graphical User Interface

- Bilingual (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 menubar

* 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>

** Prerequisite: NCP Secure Enterprise Server V 8.0 and later