

NCP Secure Entry Mac Client

Major Release 2.01 Build 47
May 2011

1. New Features and Enhancements

Tip of the Day

A "Tip of the Day" field for configuration tips and application examples is incorporated in the Client Monitor. Clicking the mouse in this field opens one of a number of local HTML pages which contain support tips on how to configure and operate the NCP Secure Entry Mac Client. Tips are cycled through automatically, day by day but can also be paged through, one by one – see the Client's Help system.

Custom Branding Option in the Client's GUI.

By default the Entry Client is delivered with an additional information field - the Banner. A local HTML page can be displayed by clicking on this Banner. This Banner can be replaced by your company logo, the local HTML page by another of your choice. Both files are located in the Entry Client's installation directory under /ProjectLogo as logo_en.png and secure_entry_banner_en.html. In addition a Quick-Info can be displayed when the mouse is moved over the Banner field or the Logo.

Displaying the VPN Client Monitor in the Menubar

After being installed, the NCP Secure Entry Client is normally started such that the Entry Monitor is opened with its window maximized. However, this default setting can be changed.

Using the "NCP Secure Entry Client" menu the maximized window can be closed and set, instead, to display the Client as an icon in the menu bar. If the menu item "Display VPN Client Monitor in the menu bar" is used to minimize the Client Monitor to an icon, the Client will also be displayed as an icon in the menu bar after a reboot.

The display of the traffic light icon in the menu bar is not affected by this, and the profile selected when the window is minimized is retained in the icon. The traffic light symbol will be red (no connection), yellow (connection being established) or green (connection established), dependent on the connection state. The icon also shows the current state of the personal firewall: green (when the network adapter is in a Friendly Network) or red (when the network adapter is not in a Friendly Network).

Similar to the "NCP Secure Entry Client" menu item in the menu bar, a connection can be established or disconnected using a pull-down menu in the icon; another profile can also be selected or the NCP Secure Entry Client closed via the icon.

Using the function "Start NCP Client Monitor as Program" returns the display of the latest state of the Client Monitor from icon to maximized window.

Using Extensible Authentication Protocol

How the Extensible Authentication Protocol Message Digest5 (EAP MP5) will be used can be defined by settings in the Monitor. This protocol can be used when access to the LAN is via a switch or when access to the wireless LAN is via an access point and the switch or the access point supports this authentication. The use of Extensible Authentication Protocol (EAP MP5) prevents unauthorized users gaining access to the LAN via the hardware interface.

The following access data can be used for EAP authentication:

- the VPN User-ID and VPN password
- own EAP username EAP password
- when using EAP-TLS (with certificate), the certificate field for Common Name and E-mail can be read automatically.

DNS Domains to be resolved in the Tunnel

If Split Tunneling is being used, the data entered here defines which DNS queries are forwarded via the VPN tunnel and which are forwarded outside the tunnel.

If the default entry, "*", is retained, all DNS queries are forwarded through the VPN tunnel.

If the default "*" is deleted and the field left blank, all DNS queries are forwarded outside the tunnel to that DNS server allocated (by the provider) from the Internet.

If an address is entered, the Client checks each outgoing (from the computer) DNS packet for the DNS name being queried. If the most significant (i.e. right-most) characters in the DNS name in the packet are identical with the sequence of characters entered here, the DNS query is forwarded via the VPN tunnel. If the check fails the DNS query is sent to the Internet. DNS queries with names that do not include a "." are always routed via the VPN tunnel.

The Domain Suffix appended when using IKE Config Mode is automatically appended to all names in the list of domain names to be resolved via the VPN tunnel.

When Split Tunneling is configured, the user can surf the Internet using a web browser, as usual.

Improvements to Online Activation of the NCP Secure Entry Client

If a web proxy server without password authentication is to be used in Mac OS X, this will be automatically recognized during the online activation.

2. Problems Resolved

Error in Profile Import

Importing profile files did not always work successfully.

This problem has been resolved.

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 release 1.01 build 10:

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 server)
- 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

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

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
- Monitor can be tailored to include company name or support information;

ⁱ 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>