

NCP Secure Entry Client (Win32/64)

Service Release: 9.30 Build 102
Date: February 2012

1. New Features and Enhancements

The following describe the new features introduced in this release:

Visual Feedback about Status of Tunnel

When the physical communication medium connection, used to establish a VPN tunnel, breaks, the existing VPN tunnel remains established, i.e. the tunnel remains logically active, for an unspecified length of time. Use of the logical tunnel by pre-existing connections can resume when the physical connection has been re-established.

During the period the physical connection is broken, the normally solid green line displayed in the client monitor changes to a dashed green line and the icon in the system tray flashes yellow and green. These indicators remain until the physical connection is re-established, when they return to solid green.

If the client loses the Internet connection and the tunnel remains logically connected, this status is displayed in a balloon over the tray icon. In this way the user has feedback about the status, even when the monitor is minimized.

Enhancements to Online Help and Tips

The help text has been adapted to the current version of the client. The dialog for profile groups has been enhanced with a help button. All help text is available, as usual, via a help button or, context sensitive, with the F1 key. The tips have been adapted to the current version of the client.

Enhancement of the 3G panel

The GPRS / 3G panel, displayed in the client monitor when a profile is used that makes use of these connection media or LTE, has been enhanced to include LTE, in line with the new LTE standard. The name of the network type displayed, together with its field strength, will be dependent on the provider's wireless network currently being used. This also applies for the NCP GINA 3G panel.

External applications

The facility to start external applications (Logon options / Ext. applications) has been enhanced to enable scripts with the extension *.vbs to also be started.

Importing configuration locks

Extensions have been made to the files import-de.txt and import-en.txt for importing configuration locks. The following options are now available:

- profiles can be exported
- profiles can be imported.

Wi-Fi Configuration assistant

The Wi-Fi Configuration assistant now only lists an open, unprotected Wi-Fi access point as a hotspot logon if this access point is a known SSID of a hotspot provider.

2. Problems Resolved

The following problems have been resolved in this release:

Blocked monitor

When displaying a PKI error message via the callback function, if the monitor was minimized during startup before the monitor image was fully displayed, the error message could not be displayed and the monitor was blocked.

Routing tables updated incorrectly

The client monitors DHCP requests on every network adapter, in order to keep IP related information for each adapter. Some situations require that the client triggers a DHCP exchange with a RENEW command. If a RENEW command was issued for an adapter without an IP address or with link status "down", the subsequent route table alterations could not be performed for some minutes.

Error when setting routes in split-tunneling

In some cases routes were incorrectly set when using split-tunneling.

Error in export file on network drive

Until now, a client's profile settings were not directly exported to a file on a network drive as password and pre-shared key were not transferred in such a case.

3. Known Issues

None

4. Getting Help for the NCP Secure Entry Client (Win32/64)

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 Client (Win32/64), visit:

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

Mail: <mailto:helpdesk@ncp-e.com?subject=A:%20NCP%20Secure%20Entry%20Client%20-%20Helpdesk%20message%20>

5. Features

Operating Systems

Microsoft Windows (32 & 64 bit): Windows 7, Windows Vista, Windows XP

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
 - Network Address Translation-Traversal (NAT-T)
 - Dead Peer Detection (DPD)

Authentication

- Internet Key Exchange (IKE):
 - Aggressive Mode and Main Mode, Quick Mode
 - IKEv2
 - 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:
 - User Authentication via GINA/Credential Management
 - Windows Logon over VPN connection
 - XAUTH for extended user authentication
 - One-time passwords and challenge response systems
 - Authentication details from certificate (prerequisite PKI)
- Support for certificates in a PKI:
 - Soft certificates, Smart cards, and USB tokens: Multi Certificate Configurations
- Seamless rekeying
- PAP, CHAP, MS-CHAPv2
- Pre-Authentication (Authentication before VPN establishment)
- 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): Extended authentication relative to switches and access points on the basis of certificates (layer 2)
 - Extensible Authentication Protocol – Transport Layer Security (MS-CHAP v2): Extended authentication relative to switches and access points on the basis of certificates using IKEv2 (layer 2)
- Secure hotspot logon using HTTP or EAP
- 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

Hash / Message Authentication Algorithms

- SHA1, SHA-256, SHA-384, SHA-512, MD5
- Diffie Hellman groups 1, 2, 5, 14, 15-18 used for asymmetric key exchange and PFS

Public Key Infrastructure (PKI) - Strong Authentication

- X.509 v.3 Standard
- Support for certificates in a PKI
 - Smart cards and USB tokens
 - PKCS#11 interface for encryption tokens (smart cards and USB)
 - Smart card operating systems
 - TCOS 1.2, 2.0 and 3.0
 - Smart card reader systems
 - PC/SC, CT-API
 - Soft certificates
 - PKCS#12 interface for private keys in soft certificates
- PIN policy: administrative specification of PIN entry to any level of complexity
- Certificate Status Protocol (CSP) for the use of user certificates in the Windows certificate store
- 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)ⁱ

Personal Firewall

- Stateful Packet Inspection
- IP-NAT (Network Address Translation)
- Friendly Net Detection (FND)
 - Firewall rules adapted automatically if connected network recognized based on its IP subnet address or an NCP FND serverⁱ
 - FND dependent actions
- Supports secure hotspot logon feature
- Start application before or after VPN establishment
- Differentiated filter rules relative to:
 - Protocols, ports or IP addresses
 - LAN adapter protection,
- Protect VMware Guest systems
- IPv4 and IPv6 support



Networking Features

Secure Network Interface

- LAN Emulation
 - NCP Virtual Ethernet adapter with NDIS interface
 - Wireless Local Area Network (WLAN) support
 - Wireless Wide Area Network (WWAN) support

Network Protocol

- IP

Communications Media

- LAN
- Wi-Fi
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
 - Windows 7 – Mobile Broadband Support
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSTN
- ISDN
- Automatic Media Detection (AMD)
- External Dialer
- Seamless Roaming (LAN / Wi-Fi / GPRS / 3G)

Dialers

- NCP Secure Dialer
- Microsoft RAS Dialer (for ISP dial-up using dial-up script)

Line Management

- Dead Peer Detection with configurable time interval
- Short Hold Mode
- Inactivity Timeout (send, receive or bi-directional)
- Channel Bundling (dynamic in ISDN) with freely configurable threshold value
- Wi-Fi Roaming (handover)
- Budget Manager
 - Separate management of Wi-Fi, GPRS/3G, xDSL, PPTP, ISDN and modem connections
 - Duration or volume based budgets
 - Management of GPRS/3G roaming costs
 - Separate management of multiple Wi-Fi access points
- Seamless Roaming

IP Address Allocation

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

VPN Path Finder

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

Data Compression

- IPsec Compression: lzs, deflate

Link Firewall

- Stateful Packet Inspection

Additional Features

- VoIP prioritization
- UDP encapsulation
- IPsec roaming ⁱⁱ
- Wi-Fi roaming ⁱⁱ
- WISPr support (T-Mobile hotspots)

Point-to-Point Protocols

- PPP over Ethernet
- PPP over GSM,
- PPP over ISDN,
- PPP over PSTN,
 - LCP, IPCP, MLP, CCP, PAP, CHAP, ECP

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),
- IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
- Additional Extended Key Usages:
 - id-kp-ipsecIKE (1.3.6.1.5.5.7.3.17) in accordance with RFC 4945
 - anyExtendedKeyUsage (2.5.29.37.0) in accordance with RFC 4945
 - IKEIntermediate (1.3.6.1.5.5.8.2.2) in accordance with draft-ietf-ipsec-pki-req-03

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

- Language support (English, German, French)
 - Monitor & Setup: en, de, fr
 - Online Help and License en, de
- Icon indicates connection status
- Client Info Center – overview of:
 - General information - version#, MAC address etc
 - Connection – current status
 - Services/applications – process(es) – status
 - Certificate Configuration – PKI certificates in use etc.
- Configuration, connection statistics, Log-book (color coded, easy copy&paste function)
- Integrated support of Mobile Connect Cards (PCMCIA, embedded)
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Monitor can be tailored to include company name or support information
- Tip of the Day
- Hotkey connection establishment and disconnection
- Custom Branding Option
- Internet Availability Tests

Notes

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>

ⁱⁱ Prerequisite: NCP Secure Enterprise Server V 8.0 and later

More information on the NCP Secure Entry Client (Win32/64) is available on the Internet at:

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

Test it for free: download a free, 30-day full version of the NCP Secure Entry Client (Win32/64) from NCP's website:

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

Release Notes

