

NCP Secure Enterprise Client (Win32/64)

Maintenance Release 9.23 Build 72

Date: December 2010

1. New Features and Enhancements

The following new features and enhancements are introduced with this maintenance release:

1.1 Security Enhancement

If "SSL with Certificate" is configured in a Client's L2Sec configuration (in the Profile settings, under "Security") then that Client will only establish a connection if the Server is also configured with "SSL with Certificate", and the Server then submits the certificate to the Client during the SSL negotiations.

1.2 IPsec Compatibility Enhancement

Adjustments have been made to the Client's IPsec subsystem that enhance the compatibility with Third Party Gateways.

1.3 Minimization or Maximization of the Logon Icon

The Client's preselected icon can be displayed either minimized or maximized. The option to "Show the preselected Icon of the NCP Secure Enterprise Client maximized" can be selected in the "Logon Option" - "Options" tab. If this option is not selected then the all of the system's logon icons (Credentials) on the Windows logon screen will be displayed in the same minimized size.

2. Problems Resolved

The following problems have been resolved:

2.1 Resolution of Pre-configured Variables

If a Client configuration made use of placeholders (e.g. %INSTALLDIR%), only the NCP placeholders were resolved, the Windows placeholders were not correctly resolved. This problem has been resolved.

2.2 Displaying the Windows Logon Dialog

The logon dialog was not automatically closed when the NCP credential provider was closed, for example after switching users. In addition, the dialog for requesting the username and password was not correctly placed in the top LH corner of the screen, it was centred instead.

The dialog for requesting the username and password was not displayed at all when, after incorrect input, the message "Incorrect UserID/Password" was sent via ACE from a Cisco server and this message contained no text in the ACE buffer.

This problem has been resolved.

2.3. Other Corrections

- adjustments concerning expiration of the test period.
- a fault has been resolved which was associated with the use of a DHCP server for recognising a known network (Friendly Net Detection).
- the cause of a sporadic crash of the Client monitor after switching users has been identified and resolved.
- firewall support is now available for passive FTP connections.

3. Known Issues

None

4. Getting Help for the NCP Secure Enterprise 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 Enterprise Client (Win32/64), visit:

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

Mail: helpdesk@ncp-e.com

5. Revision History

Features of the previous release 9.23 build 62:

Operating System Requirements

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

Version Details

Operating System	Supported by NCP software version (and later)
Microsoft Windows Vista (32 and 64 bit)	9.0****
Microsoft Windows 7	9.2****
**** Support withdrawn for version 8.x and older	

Security Features

TheNCP Secure Enterprise Client (Win32/64) 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)
- RFC conformant L2TP and L2sec
 - Support for IPsec over L2TP

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:
 - 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 (PFS)
- PAP, CHAP, MS CHAP v.2
- 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)
- 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
Seamless Rekeying (Perfect Forward Secrecy)

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
- Entrust ready
- 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)*

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
- Start application before or after VPN establishment
- Differentiated filter rules relative to: protocols, ports or IP addresses,
- LAN adapter protection,
- Central administration (optional)**

Endpoint Security

- Endpoint Policy Enforcement **

Networking Features

Secure Network Interface Support

- 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
- WiFi
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
 - Messaging Center (send & receive SMSs)
- xDSL (PPPoE)
- xDSL (PPP over CAPI, AVM)
- PSDN
- ISDN
- Automatic Media Detection (AMD)
- External Dialer

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
 - Separate management of GPRS/3G at home or when roaming
 - Separate management of multiple Wi-Fi access points

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 ***

Data Compression

- IPsec Compression: lz, deflate

Link Firewall

- Stateful Packet Inspection

Additional Features

- VoIP prioritization
- UDP encapsulation
- IPsec roaming ***
- WiFi roaming ***
- 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)

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
 - Monitor & Setup: de, en, fr
 - Online Help and License de, en
- 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)
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Monitor can be tailored to include company name or support information;

Release Notes



- * 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 Management
 - *** Prerequisite: NCP Secure Enterprise Server V 8.0 and later
- More information on NCP Secure Enterprise Client (Win32/64) is available on the Internet at:
<http://www.ncp-e.com/en/products/universal-ipsec-client.html>

Test it for free. You can download a free, 30-day full version of the NCP Secure Client from NCP's website:
<http://www.ncp-e.com/en/products/ipsec-client.html>