

NCP Secure Enterprise Client (Win32/64)

Service Release **9.30 Build 092**
Date: **November 2011**

1. New Features and Enhancements

The following new features were introduced in this release:

Dynamic Net Guard

The NCP Secure Enterprise Client Suite includes the Dynamic Net Guard (re-named from Enterprise Dynamic Firewall), a firewall product that when installed, does not include the VPN Client functionality. Dynamic Net Guard functionality is as described in the appropriate firewall sections of the NCP Secure Enterprise Client release 9.30 build 086 Release Notes – also listed below in this document.

Seamless Roaming

Seamless Roaming supports the automatic switchover of the existing VPN tunnel to another Internet communication medium. If a laptop, for example, is set into a docking station, the switchover is from the previously used Wi-Fi or GPRS/3G connection to the LAN connection. In doing so, the VPN tunnel IP address is preserved, ensuring that any application(s) communicating over the VPN tunnel are not disrupted during operation.

If, due to poor signal reception for example, the Internet connection is temporarily interrupted, the VPN tunnel is logically preserved. Again, in such a case, an application communicating via the VPN tunnel is unaffected by the disruption.

Prerequisite is an NCP Secure Enterprise VPN Server.

International Expansion of the 3G Provider List

Support of Profile settings for 3G and GPRS connections has been expanded with an International Provider List. When in configuration mode, selection of a country will display the most important providers and selection of a provider will automatically configure the parameters associated with that provider. The Provider List is editable and stored as APN.ini in the installation directory. (Configuration settings are stored in the Profile Settings under GPRS / 3G.)

Windows 7 - Mobile Broadband Support

The higher transfer rates supported by LTE would have meant that the earlier implementation based on MS Windows virtual COM ports would have been a bottleneck. Communication via the MS Windows Mobile Broadband interface removes this bottleneck.

IKEv2 Support

The implementation of Internet Key Exchange Protocol Version 2 (IKEv2), including the Mobility Extensions (MOBIKE), in the Client's base, makes the Secure Client compatible with the latest versions of IPsec gateways such as Microsoft Windows Server 2008 R2.

Selection of the alternatives, IKEv1 or IKEv2, is configured in the Entry Client's profile settings under the "IPsec Settings / Exchange Mode" rubric.

Wi-Fi Configuration Wizard enhancement

If a new Wi-Fi profile is created using the Wi-Fi configuration wizard, on completion a new connection is immediately established using the new profile.

Disable Proxy System Settings

Any proxy server settings defined for the system can be disabled with a switch in the hotspot configuration settings. The proxy server will be automatically re-activated immediately after expiry of the timeout (see below) or successful establishment of a VPN connection.

Note that these settings only work with browsers that make use of the system settings, such as Safari, Google Chrome, Internet Explorer, Firefox.

Simplified Profile Configuration with optimized Profile Overview

The importance of parameters and the frequency with which they must be configured is reflected in three new configuration modes now available in the profile settings: Standard, Extended and Expert. Automatic Media Detection and definition of the Default Profile are duplicated and can be altered in the list of "Profiles Available", meaning that the profile settings no longer have to be opened.

Project Logo has been renamed Custom Branding Option

"Project Logo" option has been renamed in this and further versions to "Custom Branding Option" in all languages.

Testing for Internet Availability

Network Tests are an option the Client Monitor's Help Menu and these can be used to test Internet availability. They support both PING to an IP Address in the Internet as well as resolution of an Internet Domain Name to an IP address. Domain names should be of the form "ncp-e.com".

Enter the address and press the corresponding Test button. The test results are displayed via a symbol (success: green tick, failure: red cross). More details are displayed in a clear text log. The tests are particularly useful for testing firewall rules for DNS requests and outgoing connections to the Internet.

Diffie Hellman Groups 15-18

The Diffie Hellman Group enhancements are exclusively for IKE Policies.

Animation of Connection Establishment

The user gets an optical feedback immediately after the Connect button has been pressed, in the form of a rotating symbol. This symbol, signaling the process of connection establishment, is displayed for the duration of this process. If the connection cannot be established, the rotating symbol disappears and an error message is displayed in the Client Monitor's graphics field instead of the normal green connection bar.

Disconnect Wi-Fi when VPN Tunnel disconnects

Security in a hotspot environment is increased by setting the option "Disconnect Wi-Fi when VPN tunnel disconnects". This parameter has been introduced into the Wi-Fi Profile configuration under "General".

New Firewall Configuration GUI

The Firewall GUI has been reworked to enable firewall rules to be activated and deactivated directly with a mouse click. New rules can be created more easily and there is a better overview of the rules. A DENY rule is always placed at the head of the rules. The "Open Basic Setting" has been removed.

Firewall – New parameter "Start FND Dependent Action"

As soon as the Client detects a change from unknown to friendly networks (or the reverse), a dependent action can be started. This enables, for example, an external program to alter proxy system settings of a Windows system.

Firewall IPv6 Capability

The firewall is now capable of handling IPv6 traffic.

Command Line Tool "NcpClientCmd"

Alternative command line program to "rws cmd", which does not make use of graphical output.

Hiding blocked Menu Items

Those menu items in the Client Monitor's pull down menus that have been locked from use by the administrator are completely suppressed, and the pull down menus contracted accordingly, and not just grayed out as in the previous versions. Locking is configured using the Configuration Locks in the Secure Entry Client "Configuration" pull down menu.

New Client Plug-in for Secure Enterprise Management

The new features described above can be reproduced and configured on the Secure Enterprise Management by using the new Client Plug-in, version 9.30 build 005 onwards.

In addition the menu item "Load Last Configuration" (on the Client Monitor under "Configuration") can be blocked.

Automatically Setting of VPN User ID

The administrator can centrally pre-configure the VPN User ID (in "Expert mode" under "VPN Tunneling") via an environment variable, either %USERNAME% or %NCPUSERNAME%. This variable is then read from the Client PC's Windows environment settings and used automatically to instantiate the VPN User ID.

If the string %USERNAME% is entered, the USERNAME Windows environment variable is read once (and used to instantiate the VPN User ID) when the Client is first started, and remains unchanged over all subsequent restarts.

If %NCPUSERNAME is entered, the USERNAME Windows environment variable is read anew each time the Client is started. In this way different users can logon to Windows and each user's specific USERNAME will then be passed to the Client software to instantiate the VPN User ID.

This variable and the associated functionality cannot be used if Windows logon is performed via the NCP GINA.

2. Changes Made and Problems Resolved

The following problem has been resolved in release 9.30 build 086:

Changes in the WLAN Assistant

Previously, if, using the Wi-Fi configuration wizard, an unprotected Wi-Fi connection was configured, the dialog for Hotspot logon was displayed. This often led to confusion as only a limited list of hotspots was displayed.

Now, if an unprotected Wi-Fi connection is configured, the Hotspot dialog is only displayed when the SSID is from a known hotspot provider. In such a case the Hotspot List will contain the associated SSID.

The following configuration option has been removed

FND Configuration via MAC address

The capability to configure or define a friendly network by use of the MAC address has been removed.

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 information about the Enterprise Client, visit:

<http://www.ncp-e.com/en/products/central-managed-vpn-solution/remote-access-vpn-management.html>

For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:

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

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

5. Features List

Central Management

As the **Single Point of Management**, NCP's Secure Enterprise Management (SEM) provides functionality and automation for the rollout, commissioning and efficient use of Secure Enterprise Clients. The Secure Enterprise Management (SEM) makes use of a VPN connection or the LAN (when on the company network), to automatically provide NCP Secure Enterprise Clients with:

- configuration updates,
- certificate updates, and
- updates to the Update Client.

Network Access Control / Endpoint Security

The policies for Endpoint Security (Endpoint Policy Enforcement)) are created centrally at the Secure Enterprise Management (SEM) and each NCP Secure Enterprise Client is only permitted access to the company network in accordance with 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 corporate network is established and maintained reliably, in the background and without any delay for the user of the NCP Secure Enterprise Client.

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 incl. MOBIKE
 - 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 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

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
- 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)ⁱ

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 serverⁱ⁾)
- 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)ⁱⁱ⁾
 - Protect VMware Guest systems
 - IPv4 and IPv6 support

Endpoint Security

- Endpoint Policy Enforcement ⁱⁱ⁾

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
 - Messaging Center (send & receive SMSs)
- 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

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 ⁱⁱⁱ

Data Compression

- IPsec Compression: lzs, deflate

Link Firewall

- Stateful Packet Inspection

Additional Features

- VoIP prioritization
- UDP encapsulation
- IPsec roaming ⁱⁱⁱ
- Wi-Fi roaming ⁱⁱⁱ
- 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
- 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 Management
- iii Prerequisite: NCP Secure Enterprise Server V 8.0 and later

More information on the NCP Secure Enterprise Client (Win32/64) is available on the Internet at:
<http://www.ncp-e.com/en/products/central-managed-vpn-solution.html>