Release Notes

NCP Secure Entry Client (Win32/64)

Major Release: 10.10 r29061
Date: April 2016

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 (32 and 64 bit)
- Windows 8.x (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)

New License Key from Version 10.10

Software Updates and License Keys

From the current software version, every new major release will require a specific license key for the same version.

If the software is updated without performing a license update, the client will receive a license for the remainder of the 30-day trial period.

New Installation and License Keys

For a new installation, the client software is installed under the Program Files directory (previously Program Files (x86)) and licensed as a trial version (for a maximum of 30 days) until a valid license is entered.

Windows 10 Update 1511 (Threshold 2/Build 10586) causes problems with installed NCP Secure Client

Microsoft's november update for Windows 10 is far more than merely a collection of patches and/or enhancements. In general it is essentially a new version of Windows. Some areas of the registry database are rewritten during the update and while doing so a few important entries of the NCP Secure Client are discarded.

To resolve this issue the lost registry keys and related values have to be written again. Therefore one has to perform an uninstall of the NCP Secure Client followed by a mandatory reboot prompted for within the uninstall procedure. After which one just has to reinstall the version of the client used before. (Please do **not** confirm the “Delete all files“ option of the uninstall process).

The full configuration will be preserved; only the license information has to be re-entered after the installation. After having completed this procedure the NCP Secure Client can be used again without any limitations.

1. New Features and Enhancements

New Hotspot Logon

Additional configuration is no longer required with the new Hotspot Logon feature. The client detects available hotspots and provides the user with an option to logon. When Hotspot Logon is started by the user, the NCP Wi-Fi Manager is displayed and the user can select the Wi-Fi network and log on to it. As soon as the Wi-Fi connection is established, the client checks access to the internet periodically. If internet access is not available, the client starts a restricted browser without the address bar. If the user has logged onto the hotspot operator's entry portal successfully, the VPN tunnel will be established automatically as soon as internet access is available.

Improved Compatibility with Gateways Provided by Other Manufacturers

Secure Client supports IKEv2 redirect (RFC 5685). This means that load balancing functions provided by other manufacturers can be used.

Monitoring the Filter Driver via the Secure Client

If the client detects a problem with the filter driver, it will attempt to resolve the error and prompt the user to restart the device.

Using Half Routes and Default Gateways in Windows 10

The default client setting for the virtual network adapter is "half routes". This can be changed to "default gateways" by editing the registry. To do this, modify the following registry key:
Path:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt]
```

Key:

```
EnableDefGw = 1
```

Type:

```
REG_DWORD
```

If the registry key EnableDefGw does not exist or is set to EnableDefGw=0, the client will use half routes.

2. Improvements / Problems Resolved

Stability Improvements

The stability of the NCPRWSNT service and update clients has been improved.

Enhancement of Log Messages

The log details for the PKI environment and ncpsec service have been enhanced.

Functionality of Wi-Fi Module

In the event of a large number of Wi-Fi profiles (greater than 56), the Wi-Fi adapter did not function correctly and the adapter was no longer displayed under Wi-Fi Management. This issue has now been resolved.

Windows Pre-Logon

Windows Pre-Logon (Credential Provider) has been adapted for Windows 10.

3. Known Issues

None

Service Release: 10.04 Revision 26745

Date: November 2015

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 (32 and 64 bit)
- Windows 8.x (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)

Windows 10 Update 1511 (Threshold 2/Build 10586) causes problems with installed NCP Secure Client

Microsoft's november update for Windows 10 is far more than merely a collection of patches and/or enhancements. In general it is essentially a new version of Windows. Some areas of the registry database are rewritten during the update and while doing so a few important entries of the NCP Secure Client are discarded.

To resolve this issue the lost registry keys and related values have to be written again. Therefore one has to perform an uninstall of the NCP Secure Client followed by a mandatory reboot prompted for within the uninstall procedure. After which one just has to reinstall the version of the client used before. (Please do **not** confirm the "Delete all files" option of the uninstall process).

The full configuration will be preserved; only the license information has to be re-entered after the installation. After having completed this procedure the NCP Secure Client can be used again without any limitations.

Information on the operation of the Secure Client under Windows 10

It is necessary to have a product key for version 10.x to operate the Client.

Note when updating the operating system to Windows 10

When updating from Microsoft Windows 7, Windows 8 or Windows 8.1 to Microsoft Windows 10, it is vital that the NCP Secure Client be uninstalled before starting the update.

At the same time it is recommended that the configuration file, as well as the certificates used, is saved separately.

When the update to Windows 10 is complete, the latest version of the NCP Secure Client (10.02 or later) should then be installed.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Installation

Users experienced a rollback of the client installation during the filter driver setup. This version contains adjustments of the setup information correcting this behavior.

Windows Pre-Logon

The processing of the user name and password entered manually for Windows logon via credential provider was corrected.

Firewall

An error in the NCP firewall application detection was fixed.

Automatic Media Detection

An error in the automatic media detection related to PPPoE connections was fixed.

Deactivate WLAN Adapter with Plugged in LAN Cable

Compatibility improvements were made for various Windows operating systems.

Split Tunneling

Error fixed in split tunneling when the remote network shared the same IP address range as the user's local network. This previously caused the local network route to be deleted if the VPN profile was changed.

Profile Import

The variable connection mode ConnMode=2 (automatic mode is started manually) was not imported during profile import. This error has been fixed.

3. Known Issues

Credentials Provider under Windows 10

If the NCP Secure Client credential provider is used under Windows 10, the user login may not function correctly.

Service Release: 10.02 Build 25056
Date: August 2015

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 (32 and 64 bit)
- Windows 8.x (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)

Information on the operation of the Secure Client under Windows 10

It is necessary to have a product key for version 10.x to operate the Client.

Note when updating the operating system to Windows 10

When updating from Microsoft Windows 7, Windows 8 or Windows 8.1 to Microsoft Windows 10, it is vital that the NCP Secure Client be uninstalled before starting the update.

At the same time it is recommended that the configuration file, as well as the certificates used, is saved separately.

When the update to Windows 10 is complete, the latest version of the NCP Secure Client (10.02 or later) should then be installed.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Installation Adjustment

Users experienced a rollback of the client installation during the filter driver setup.

This version contains adjustments of the setup information correcting this behavior.

3. Known Issues

None

Service Release: **10.02 Build 24934**
Date: **July 2015**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 (32 and 64 bit)
- Windows 8.x (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)

Information on the operation of the Secure Client under Windows 10

It is necessary to have a product key for version 10.x to operate the Client.

Note when updating the operating system to Windows 10

When updating from Microsoft Windows 7, Windows 8 or Windows 8.1 to Microsoft Windows 10, it is vital that the NCP Secure Client be uninstalled before starting the update.

At the same time it is recommended that the configuration file, as well as the certificates used, is saved separately.

When the update to Windows 10 is complete, the latest version of the NCP Secure Client (10.02 or later) should then be installed.

1. New Features and Enhancements

Extensions inside the Log Protocolling

For the evaluaton of the log text two search functions were implemented, that facilitate the searches in the log protocol. These functions are opened by clicking in the log display window with two input fields on "Show Search".

Scaling the Monitor for Better Touch Operation

So that the touch operation of the client monitor can be comfortably done on tablets, the monitor's surface is now scaleable.

A scaling degree of 150% is pre-set and can be activated or deactivated by pressing on the NCP logo.

Via the main monitor menu under "View / GUI Scaling" the display size in levels of 100, 125, 150, 175 and 200% van be variably set. A dynamic change to the scaling is possible with the key combination [CTRL] [+] or [CTRL] [+].

Check for friendly networks periodically

The periodical testing should then be enabled when a change to the condition of the network adapter has not occurred – e.g. on taking out the LAN cable. This can be the consequence of using the client in a virtual environment.

The function that is checked in pre-set intervals, checks whether the client is still in a friendly network. As soon as the friendly network is no longer available this status change will be shown as a red firewall symbol on the monitor.

This configuration option is located in the monitor menu under: Firewall / Friendly Networks / Automatic.

VPN Profile with IKEv2 receives Diffie Hellman 14 for the PFS Group

On setting up a new VPN profile with IPsec protcoll the Diffie Hellman Group 14 is pre-set as the standard value for the key exchange process in the IPsec policy. This setting can be done under "PFS Group" and also be altered there.

Changing the Password Entry Dialog to Non-Modal

Modal dialogs (eg: pin entry, password check) stop the status display of the client (eg: FND display in the system tray). The modal dialogs are therefore switched to non-modal.

Automatic Tunnel Build-up without User Entries before Windows Logon

The NCP Secure Entry Client builds up a VPN tunnel immediately after the system start without the user having to enter a password or a PIN before Windows Logon.

Pre-requisites:
The client exclusively uses a hardware certificate to extend the authentication, and the VPN profile to be used automatically (in the basic settings set as standard profile after every new start) has the following configuration settings:
- Line Management / Connection Mode "always": causes a continuous connection build-up regardless of waiting data flow or user entries.

Customer-specific Adaptation for OTP Field Identifier

The file NCPMON.INI can be edited in order to be able to see the fields in mixed architectures for the same inputted values, also with the same field titles.

Example: in the dialog for the OTP registration there is the field title "PIN" and "One Time Password". Should the value of the windows code word be entered into the PIN field and the value of a token be entered into the one time password field, then at the same time the relevant field title can be changed. That can be done via the client plug-in of the SEM under the new title "Extended Options".

Alternatively the NCPMON.INI can also be modified:

After opening the file, look for the configuration section [OTP]. Then change the field title on the right next to the equals sign:

```
[OTP]
Caption_User = User name:
Caption_Pin = Windows code word:
Caption_Pw = Token:
```

Should the titles be changed in several languages, the abbreviation name of the language must be added as an annex note. If there is no entry for the language in the GUI then the entry will be used without the annex note.

```
[OTP]
Caption_Pin_de = Windows code word:
Caption_Pin_en = Windows Password:
Caption_Pin_fr = Windows Mot de passe:
Caption_Pin_es = Windows Contraseña:
Caption_Pw_de = Token:
Caption_Pw_en = Token:
Caption_Pw_fr = Token:
Caption_Pw_es = Token:
```

Deactivate WLAN Adapter with Plugged in LAN Cable

With help of the function "Deactivate WLAN Adapter with plugged in LAN cable" mobile teleworkers are saved some manual switching. As soon as a teleworker, who is connected via WLAN with the company network, plugs the LAN cable into his Notebook inhouse, the WLAN adapter is deactivated and the LAN connection into the company network is used. That happens independent of whether the NCP WLAN manager or that of an unknown producer is used. When the LAN cable is unplugged, the WLAN adapter is again activated.

The function is situated in the monitor configuration for the WLAN settings under "Options". It is only visible with a license key >= 10.00.

2. Improvements / Problems Resolved

Improving Friendly Net Detection

With this optimization the Entry Client carries out the checking of the incoming FND server certificates correctly.

3. Known Issues

None

Major Release: **10.00 Build 21521**
Date: **January 2015**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 8.x (32 and 64 bit)
- Windows 7 (32 and 64 bit)
- Windows Vista (32 and 64 bit)

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Improvements to the Update Process

The process for taking an existing license into the updated software has been improved. It is now no longer necessary to re-input the license key or serial number after the update; these are copied from the previous version. However, activation must still be carried out, using either online or offline activation.

Improvements in connection with Strong Authentication using OTP

An error occurred when, using "always" mode and OTP for strong authentication, the OTP was entered incorrectly. This problem has been resolved.

3. Known Issues

None

Major Release: **10.00 build 21336**
Datum: **January 2015**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit

1. New Features and Enhancements

MSI Installer - Updating to NCP Secure Entry Client Version 10.0

NCP Secure Entry Client version 10.00 software is distributed in the Microsoft .msi format. The impact of this move is as follows:

- All NCP Secure Entry Client software versions earlier than 10.00, must first be de-installed using the Microsoft "Programs and Features" functions. Then the new software can be installed from the .msi package; existing profiles can be preserved across the update. Subsequent updates can be applied, when available, using the MSI Update feature.

Enhanced Connection Modes

Connection Mode has been enhanced with two additional modes and the selections have been given more explanatory names as follows:

manual / (default Connection Mode)

When this mode is set, the user must manually establish the VPN connection by pressing "Connect". The connection will be disconnected dependent on timeout settings. If timeout is set to null (0) the connection must be disconnected manually.

automatic (connection initiated by data transfer)

When this mode is set, the Client software automatically establishes the connection as soon as data must be transferred across the connection. How the connection is disconnected is dependent on how the Client is configured, i. e. according to application requirements and profile settings.

always

When Connection Mode is set to "always", a VPN connection is always established automatically when the Client starts. Connection establishment is independent of the "Connect" button, of the onset of data transfer, or of how the monitor is set to be displayed

variable (Connect starts "automatic" mode)

When this mode is set, the first VPN connection is established manually (by pressing "Connect") The mode used to establish the next connection is dependent on how the previous connection was disconnected:

– if the connection was disconnected due to a timeout, then the next connection will be established whenever data transfer to a remote host is initiated by a Client application.

– If the connection was disconnected manually (by pressing "Disconnect")then the next connection must be established manually.

If timeout is set to zero (0), i.e. no timeout, then the connection must be disconnected manually.

Important: if connection mode is set to "manual" then activate a timeout (i.e. set timeout to non zero) in order to automate disconnection.

variable (Connect starts "always" mode)

When this mode is set, the first time "Connect" is pressed to establish a VPN connection, the connection mode is set to "always". This "always" mode stays set until the monitor is closed, when the mode is changed back to "variable (Connect starts "always" mode)".

Extended Log Settings

Under the monitor menu "Help/Extended Log Settings" the maximum log-entries retention period (in days) can be defined.

Execution of the RWSCMD and NcpClientCmd comman-line tools, including the calling parameters, can be written to a log file. To do this the application must be activated in the "Extended Log Settings". Alternatively this can be done by adding the line "[RWSCMD]Logs=1" to the NCPMON.INI. The output is logged to "RwscmdLog.txt" in the log directory.

Enhancements to the Support Assistant

The support assistant has been enhanced to enable the Microsoft log file from the driver installation to be included.

The following files are included, if present:

WINDOWSDIR\inf\setupapi.dev.log

WINDOWSDIR\inf\setupapi.app.log

WINDOWSDIR\inf\setupapi.setup.log

IKEv2 Profile Configuration - GUI Improvements

IKEv2 based polices can be defined in the Client monitors' IPsec settings. IKEv2 key exchange is then handled according to these settings.

Further IKEv2 configuration settings are made in a profile's standard configuration, where the corresponding authentication can be selected - Certificate, Pre-shared Key or EAP.

The input fields for username and password or the IKE ID are blanked out, dependent on which authentication method is chosen,

In the profile settings under "IPsec" the required IKEv2 policy can be selected, unless automatic mode has been chosen. In addition the Diffie-Helman and PFS Groups can be selected which will be used for the elliptical curve IKEv2 key exchange (ECP with DH Groups: 19, 20, 21, 25, 26)

The "Policy Editor" button can be used to switch directly from the IPsec profile settings to the IPsec policies configuration.

Support for Elliptic Curves in Certificates and Key Exchange Processes (ECC, Elliptic Curve Cryptography)

Various storage media and locations can be accessed when using certificates that employ Elliptical Curve Cryptography. Such certificates can be read from PKCS#12 files or from PKCS#11 or PC/SC interfaces via a smart card reader, or they can be accessed via the Windows CSP or CNG.

Verification of signatures using ECC is only supported under IKEv2. Therefore newer smart cards such as TCOS 3.0 V2, which only employ Elliptical Curve Cryptography, can only be used in connection with IKEv2 connections.

Checking that Data is Passing Through the Tunnel

In locations with poor mobile wireless reception, there is a chance that, despite a VPN tunnel being established and marked green, data is not actually transferred across the tunnel. In order to give the correct feedback to the user in such a situation, "Tunnel Traffic Monitoring" can be enabled in the Client connection profile under the "Line Management" folder; this causes a configurable, target address in the remote network to be automatically pinged periodically. The VPN tunnel status is modified in line with the response from the ping.

AES-GCM - Galois/Counter Mode

Galois/Counter Mode (GCM), an authenticated encryption algorithm, is a mode of operation for symmetric key cryptographic block ciphers that combines encryption with integrity protection. It has been widely adopted because of its efficiency and performance.

AES_GCM 128 or 256 can be selected as the encryption algorithm in IPsec or IKEv2 profiles; doing so removes the need for additional integrity algorithms

Firewall: New Option:

"Reject Outgoing Traffic"

When set, outgoing packets are rejected and a corresponding acknowledgement message returned to the sending application.

Support for xDSL (PPP over Capi) Communication Medium and PPTP Withdrawn

Support for IPsec over L2TP Withdrawn

MSI Installer – NCP-specific Functions

Adding a .cnf file when installing

When installing a .msi package, a .cnf file can be included in the installation. In previous setup procedures the .cnf file had to be copied to the installation directory. Now the installer copies the .cnf autonomously to the installation directory, providing the .cnf file is stored in the directory from which the .msi package, (or the installer as a .exe file) is to be executed. The return value from the copy is ignored. If errors occur, the installation is not aborted.

Adding files during the installation

Additional files, for example certificates or customer specific project logo files (CBO) which should be included in the setup can be installed.

Previously a directory ncple, was created under "Disk1" from where all files and directories were recursively copied to the installation directory.

This is now performed in a different way. If a directory IMPORTDIR is located in the directory from which the .msi package, (or the installer as a .exe file) is to be executed, this directory is copied recursively to the installation directory. The return value from the copy is ignored. If an error occurs, the installation is not aborted. As such files are not recognized by the installer, these are neither updated nor de-installed.

Another mechanism for adding files, icons, registry entries, etc. to an installation is the transform file. Using the admin tools from various software manufacturers (such as InstallShield, SuperOrca), the .msi package can be opened, any features, components, files etc., added, and a transform file created which can be passed as a parameter to the installation.

msiexec /i myproduct.msi TRANSFORM=mytransfom.mst

This is the officially supported method for extending an existing .msi package. The advantage is that the extensions are known to the installer and can be updated and de-installed by the installer.

Executing a batch file during the installation

If a batch file NcpInstall.bat is located in the directory from which the .msi package, (or the installer as a .exe file) is to be executed, this file is executed as the last process in the installation. The return value from the execution is ignored. If an error occurs during execution of the batch file, the installation is not aborted. The installer is unaware of the execution and therefor cannot manage it.

Starting a test version immediately

In many projects there is the wish to "Start the test version now" when starting the monitor but without the need to prompt the user. This can be achieved using the command line parameter "STARTTESTVERSION".

msiexec /i myproduct.msi STARTTESTVERSION=1

Silent Installation und De-installation

The previous "silent installation" has been replaced by a new form, handled by the installer. Its own "silent installation" is used, initiated by the display options.

e.g.: msiexec /i myproduct.msi /qn myproduct.exe /v"/qn"

The previous form of "silent installation" is replaced with one which is initiated via the display options.

e.g.: msiexec /x myproduct.msi /qn

Logging

Previously parts of the setup could be logged using the NCP specific SetupExt.ini. Now the Windows installer performs extensive logging. This can be configured using the logging options.

e.g.: msiexec /i myproduct.msi /log "c:\temp\myinstall.log" myproduct.exe /v"/log "c:\temp\myinstall.log""

Deleting all files during de-installation

Previously, during the last part of the de-installation, the user was asked whether personal files should deleted. Using "silent installation" the parameter -delall could be used for this purpose.

This has now changed and is dependent on the type of de-installation. If the Client is de-installed using the assistant, the user is prompted as previously. If it is de-installed directly (no dialog), the user is not prompted as no personal files are deleted. In this case the command line parameter DELETEALL=1 can be used, causing all files to be deleted.

e.g.: msiexec /x myproduct.msi DELETEALL=1

2. Improvements / Problems Resolved

OpenSSL Version 1.0.1j

OpenSSL 1.0.1j is used within the Client software. Security deficiencies associated with previous versions of the OpenSSL libraries are thereby resolved.

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/software/version-information.html

For further assistance with the NCP Secure Entry Client (Win32/64), visit:
http://www.ncp-e.com/en/about-us/contact.html

Mail: helpdesk@ncp-e.com

5. Features

Operating Systems

See Prerequisites on page 1.

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. Mobility and Multihoming Protocol (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)
- Internet Key Exchange v2 (IKEv2):
  - Pre-shared secrets
  - RSA Signatures (and associated Public Key Infrastructure)
  - Extended Authentication Protocol (EAP) - username and password used to authenticates NCP Secure Entry Client with VPN gateway, PKI certificate used to authenticate VPN gateway with Client
    EAP Types supported: PAP, MD5, MS-CHAP v2, TLS (selected by responder)
  - IKEv2 Mobility and Multihoming Protocol (MOBIKE)
  - Perfect Forward Secrecy (PFS)
  - IKE Config. Mode for dynamic allocation of private IP (virtual) address from address pool
- 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 v2
- 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-GCM 128, 256 bits (only IKEv2 & IPsec); AES-CTR 128, 192, 256 bits; AES (CBC) 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
- Diffie Hellman groups 19, 20, 21, 25,26 employ Elliptical Curve Cryptography algorithm.

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
- Certificate Service Provider (CSP) for the use of user certificates in Windows certificate store
- 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)[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 Server[i]
  - 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
- Option: "Reject Outgoing Traffic"

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

- IPv4 protocol
  - IP traffic inside and outside VPN tunnel can use IPv4 protocol
- IPv6 protocol
  - IP traffic used to establish and maintain the VPN tunnel can use IPv6 protocol (Client to VPN gateway),
  - IP traffic inside any VPN tunnel MUST use IPv4 protocol.

Communications Media

- LAN
- Wi-Fi
- GPRS / 3G (UMTS, HSDPA), GSM (incl. HSCSD)
  - Windows 7 and 8 – Mobile Broadband Support
- xDSL (PPPoE)
- 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
- Wi-Fi Roaming (handover)
- Connection Modes
  - manual / (default Connection Mode)
  - automatic (connection initiated by data transfer)
  - always

  - variable (Connect starts "automatic" mode)
  - variable (Connect starts "always" mode)
- Inactivity Timeout (send, receive or bi-directional)
- Short Hold Mode
- Channel Bundling (dynamic in ISDN) with freely configurable threshold value
- 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 [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 v1 (IKE) (includes IKMP/Oakley) (RFC 2406),
  - IKE Extended Authentication (XAUTH), IKE configure (IKECFG) and Dead Peer Detection (DPD)
  - Negotiation of NAT-Traversal in the IKE (RFC 3947)
- Internet Key Exchange Protocol v2 (IKEv2) (RFC 4306, 5996)
  - IKEv2 Mobility and Multihoming Protocol (MOBIKE) (RFC 4555)
- UDP encapsulation of IPsec Packets (RFC 3948),
- 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

Usability Features

APN from SIM Card

The APN (Access Point Name) defines the access point of a mobile data connection at a provider. This option makes it easy to change to a less expensive provider when roaming, especially when abroad. The system automatically takes APN data from the new SIM card and uses it to configure the corresponding profile.

Secure Client Monitor

Intuitive Graphical User Interface

- Language support (English, German, French, Spanish)
  - Monitor & Setup: en, de, fr, es
  - Online Help and License en, de, es
- 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
- VPN Tunnel Traffic Monitoring (Tunnel 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 VPN 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/universal-vpn-client-suite.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