NCP Secure Entry Client (Win32/64)

Release Notes

Service Release: **10.13 r39050**
Date: **March 2018**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit (up to and including version 1709)
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

After restarting the system, the NCP FND server will not be detected automatically

In some cases, especially when assigning the local IP address via DHCP, after restarting the system, the NCP FND Server [i]) was not detected automatically. This error is fixed.

3. Known Issues

None

Service Release: **10.13 r38935**
Date: **March 2018**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit (up to and including version 1709)
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Client-Firewall Status Feedback to the Windows operating system

An active client firewall is displayed in the Windows operating system at the appropriate place (e. g."Security and Maintenance").

Mobile Display Option in the Client GUI

If the NCP Secure Client communicates by the mobile network, this connection medium was not correctly displayed to the client GUI.

Hyper-V Compatibility

Activating Hyper-V on Windows may activate a Hyper-V network adapter which may cause this adapter may behave differently from regular network adapters in terms of DHCP, so the NCP Secure Client now treats this adapter separately.

VPN Path Finder and Client Firewall

If the VPN Path Finder option was configured in the VPN profile, it was possible to communicate externally via port 443 despite blocking firewall rules.

NCP Credential Provider

In rare cases, when logging on or unlocking the computer, a window for entering a certificate PIN could appear only for a short time, provided that the NCP credential provider had previously searched unsuccessfully for mobile phone connections to set up a tunnel and the lock screen was displayed again, this behavior has been corrected.

3. Known Issues

None

NCP Secure Entry Client (Win32/64)

Release Notes

Service Release: **10.13 r38541**

Date: **January 2018**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit (up to and including version 1709)
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

NDIS Driver Optimization

The NDIS driver has been optimized to correct problems during connection setup after leaving sleep mode.

Correction of the network mask

If the network configuration of the client was specified by the VPN Gateway during connection establishment and the VPN network gateway did not set the correct network mask, the connection could not be established. This bug is resolved by automatically replacing the wrong one with a Class C network mask (255.255.255.0).

3. Known Issues

None

Service Release: **10.13 r38189**
Date: **December 2017**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit (up to and including version 1709)
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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.

1. New Features and Enhancements

Metered Connections

If the media type of connection of the VPN tunnel is changed from LAN to a mobile connection resulting in connection costs, this can be communicated to the Secure Enterprise Server (prerequisite SES 11.x). For this purpose, the "metered connection" setting must be activated in the Wi-Fi profile under "Wi-Fi Profiles / General".
For better management of metered connections, the client receives an IP address from the server from a pool for clients using a mobile connection during tunnel setup. This is also the case if the client does not directly establish the mobile connection, but is connected via Wi-Fi to an LTE router.

2. Improvements / Problems Resolved

Change to the NCP Network Driver Type

Changing the NCP network driver type from an “Ethernet Adapter” to “Virtual Adapter” has resolved the issue that Wi-Fi adapters were deactivated by the operating system if the VPN was connected by Wi-Fi and Wi-Fi was not configured using the NCP Wi-Fi Manager.

Error in processing long domain names has been fixed

The firewall has been optimized for application-specific rules to prevent crashes of the VPN service

Incorrect display with the Budget Manager

The incorrect calculation with high maximum settings in the Budget Manager has been corrected.

Display Problems with Hotspot Login

The incorrect display of the login page during the hotspot login has been fixed.

Issues Resolved with Credential Provider

After establishing a connection via the NCP Credential Provider, the VPN user name was not stored correctly under certain conditions (manual entry of the VPN user name and a name with more than 20 characters) and was therefore incorrectly suggested for future connection attempts. This issue has now been resolved.

The NCP Credential Provider was not selected when unlocking the desktop when the Logon option “Open connection dialog automatically” was selected. With this release, the NCP Credential Provider is also selected after unlocking the desktop.

The incorrect display of the credential provider during Windows 10 logon has been corrected. The status display for Home Zone now correctly distinguishes between friendly and unfriendly networks.

Extended Information in Client Info Center

Under Windows 10, the version and build in the Client Info Center is now displayed.

IKEv2 connection after interrupted connection

If an IKEv2 connection was interrupted, the client tried to reach the gateway without success. From this release, the client will initiate a new connection attempt.

Improvement of Hotspot Feature

Compatibility with Hotspot login pages has been improved. The browser window that appears during the login on the HotSpot is automatically closed after the timeout value which can be configured in NCPMON.INI ([HOTSPOTBROWSER] Timeout=300; default value). Consequently, the proxy configuration in the operating system is reactivated, the dynamic firewall rules for the HotSpot login are deleted, and the Wi-Fi connection is disconnected if necessary.

Daily Log File

The logs for the client monitor, RWSCMD and NcpClientCmd are no longer written continuously. Instead, a new log file is created for each day with the date in the file name. The maximum age of the log files and their deletion can be configured within the extended log settings.

Client Firewall Status in Windows

The firewall status is now shown in Windows (under “Security and Maintenance”).

Certificate Handling

An issue has been resolved that caused the server certificate to be rejected with "unhandled critical extension".

Handling of Reading Errors

The handling of errors which can occur when reading the configuration file ncpphone.cfg, has been improved.

Windows 10 Creators Update

When using the Windows 10 Creators Update, the Enterprise Client of Version 10.11 32792 and 10.04 31799 did not reinstall after de-installation. This issue is resolved.

Stability with VPN bypass

The stability of the client may have been affected if VPN bypass was enabled. This issue has now been resolved. A further issue with name resolution while using VPN bypass has also been resolved.

Incorrectly Media Change with Seamless Roaming

When seamless roaming was used, the media change was not performed correctly. This bug has been fixed.

Loss of connection after pulling or plugging the LAN cable

In the case of a media change forced by pulling or plugging the LAN cable (when the setting "Deactivate Wi-Fi adapter when the LAN cable is disconnected" is selected), it could happen that no more connection could be established via the Wi-Fi adapter. This bug is now fixed.

Hotspot Login allows Pop-up Windows

Hotspot login now allows additional pop-up windows. The issue caused by pressing <CTRL-N> which opened a new browser window has been resolved.

3. Known Issues

None

Service Release: **10.11 r32792**
Date: **November 2016**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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.

1. New Features and Enhancements

VPN Bypass

The VPN Bypass function allows the administrator to define applications which can communicate over the Internet directly despite disabling split tunneling on the VPN connection. It is also possible to define which domains or target addresses can bypass the VPN tunnel.
This function can be used to separate regular and non-sensitive data traffic from central infrastructure, so as not to affect performance. For example, operating systems and virus scanner updates (with a known domain), can bypass the VPN connection easily, or certain cloud services can be permitted to access applications via the Internet directly. VPN Bypass is configured via “Configuration/VPN Bypass” in the client monitor and in the profile settings under "Split Tunneling / VPN bypass list".

Home Zone

The Home Zone feature has been implemented as an option in the firewall to make the resources of a home network available without the administrator knowing the configuration of the employee’s home office network.
The Home Zone can be activated under "Options" in the firewall settings and in the firewall default settings. The Home Zone can be set and deleted in the client monitor Connect menu by the user.

Selecting a User or Computer Certificate in Windows CSP

In the client configuration menu under “Certificates” (Extended Key Usage), you can select the default certificate for a user or computer.

Show Media Type Using ncpclientcmd.exe

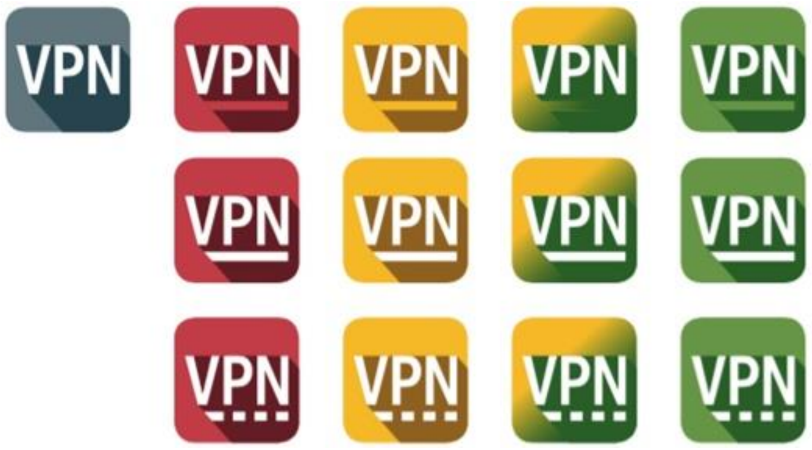
Entering the command “NcpClientCmd /getConnecionMedium” in the command prompt shows the connection media type.

New Product and Status Icons

The product and status icons have been updated in this version.
The color of the status icons change from red to green during connection.
The line under the VPN icon shows whether the firewall is active and whether the device is connected to an unknown or friendly network.

Product Icon *Status-Icons*

VPN disconnected | VPN connecting | preserve logical tunnel |VPN connected



Firewall disabled

Firewall active:
Client is connected to an unknown/unfriendly network

Firewall active:
Client is connected to a firendly network

IKEv2 Signature Authentication (RFC 7427)

The client now supports certificate authentication according to RFC 7427 for IKEv2 RSASSA-PSS which also allows for modern padding (RSASSA-PSS).

2. Improvements / Problems Resolved

Support for More than two FND Servers

The number of optional FND servers is restricted to 255 characters. Three addresses can be entered separated by a comma for example: fe80 :: E568: 8a83: 203c: 55c0,192.16.15.57, fnd2.ncp.de, 192.16.15.56

Changes to Roaming Connection Options in Budget Manager

To prevent costs from being incurred by establishing a connection when roaming users can activate “No roaming” under “Connection Options” in the Budget Manager. In previous versions of the client, “Do not establish connection” was used. This connected to the network and disconnected if roaming was detected.

Hotspot Logon

The client provides the installed version number of Internet Explorer during Hotspot Logon to avoid logon problems.

Firewall Blocked IPv6 IKE Packets

Previously only a IPv4 VPN connection could be established if the option “Allow IPsec protocol (500, 4500, ESP, 443)” was enabled in the firewall. Both IPv4 and IPv6 connections are now supported.

Alternative IPSec Port Fixed

VPN connection now works if the “Allow IPsec procol (ESP, UDP) and VPN Path Finder” firewall option is activated and an alternative IPsec port is configured.

Enabling and Disabling the Credential Provider

Starting with this release, Windows PreLogon with the Credential Provider can no longer be selected during the software installation. The credential provider can now only be enabled and disabled under “Logon Options” in the client monitor “Configuration” menu.

3. Known Issues

None

Service Release: **10.10 r31802**
Date: **September 2016**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

License Deactivation

In some cases, the client license may have been deactivated after restarting the device. This issue has been resolved.

Unavailability of Network Connection

After an installation or update of the NCP Secure Client, the network connection was unavailable until restarting the device. From this maintenance release, the network connection is available immediately after the installation or update of the NCP Secure Client.

Stability Improvements when Using the Wi-Fi Manager

In some cases a blue-screen error occurred when leaving hibernation mode with the Wi-Fi Manager active. This issue has been resolved.

3. Known Issues

None

Service Release: **10.10 r31262**
Date: **August 2016**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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

None

2. Improvements / Problems Resolved

Update Driver Signature (Anniversary Update Version 1607, Build 14393.10)

If the Anniversary Update for an older NCP Secure Client version is installed under Windows 10, the installation fails if “Secure Boot" is enabled in the BIOS /UEFI of the computer. The reason for this is that Windows 10 requires a driver signed by Microsoft after the Anniversary Update.

With this release of the NCP Secure Client (10.10 r31262), a signed driver is installed for all supported Windows versions.

Installing the Anniversary Update for a previously installed NCP Secure Client under Windows 10 does not affect the function of the client.

Wi-Fi Activation

After a restart or after leaving sleep mode, Wi-Fi could not be activated in certain cases.

Hotspot Logon

An error in the stateful inspection (SPI) mechnism caused the Hotspot Logon to fail.

3. Known Issues

None

Service Release: **10.10 r30578**
Datum: **June 2016**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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

None

2. Improvements / Problems Resolved

Problems Resolved with License File

In some cases, the license file may become corrupted or be deleted. The handling of the license file has been optimized to resolve this.

Update to Installation File Signature

The signature of the installation file is checked during online installation from Internet Explorer. This check failed because the certificate has expired. The certificate and the signature have been updated.

Flight Mode Activation

When the flight mode is activated under Windows 10, this is now recognized correctly by the client. 3G/4G hardware is no longer used when flight mode is activated.

Connecting and Disconnecting the VPN Tunnel Manually

After clicking the Connect or Disconnect button in quick succession, the client may enter a state which does not allow a connection to be established. Previously this could only be remedied by changing the profile.

Update Behavior for Local Update or SEM Update

3. Known Issues

None

Major Release: **10.10 r29061**
Datum: **April 2016**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10 32/64 bit
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Windows Vista, 32/64 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

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 Enterprise Client (Win32/64), visit:
http://www.ncp-e.com/en/company/contact.html

E-Mail: support@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)
  - Communikation only in the tunnel or Split Tunneling
  - Message Transfer Unit (MTU) size fragmentation and reassembly
  - Network Address Translation-Traversal (NAT-T)
  - Dead Peer Detection (DPD)
  - Anti-replay Protection

Authentication

- Internet Key Exchange (IKE):
  - Aggressive Mode, Main Mode, Quick Mode
  - Perfect Forward Secrecy (PFS)
  - IKE-Config-Mode for dynamic allocation of private (virtual) IP address from IP-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 Enterprise Client with VPN gateway, PKI certificate used to authenticate VPN gateway with Client
  - EAP unterstützt 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 Credential Management
    - Windows Logon over VPN connection
  - XAUTH (IKEv1) 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
- HTTP 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-CHAPv2): Extended authentication relative to switches and access points on the basis of certificates with 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 (only IKEv2 and IPsec); 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 Authentisierungs-Algorithmen

- SHA-1, SHA-256, SHA-384, SHA-512, MD5.
- Diffie Hellman groups 1, 2, 5, 14, 15-18, 19-21, 25, 26 for asymmetric key exchange and PFS.
- Diffie Hellman groups 19 - 21, 25, 26 employ Elliptical Curve Cryptography (only under IKEv2).

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 und 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 Service Provider (CSP) for the use of user certificates in 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 Server[i])
  - Starting programs depending on FND
- Supports secure hotspot logon feature
- Start application before or after VPN establishment
- Differentiated filter rules relative to:
  - Protocols, ports, applications and IP addresses
  - LAN adapter protection
- Protect VMware guest systems
- IPv4 and IPv6 support
- Option: "Reject Outgoing Traffic" or drop without response

Networking Features

Secure Network Interface

- LAN Emulation
  - Ethernet adapter with NDIS interface
  - Full support of Wireless Local Area Network (WLAN)

  - Full support of Wireless Wide Area Network (WWAN)

Network Protocol

- IPv4 protocol
  - IPv4 traffic inside and outside VPN tunnel can use IPv4 protocol;
- IPv6 protocol
  - IPv6 traffic used to establish and maintain the VPN tunnel can use IPv6 protocol (Client to VPN gateway and Client to NCP Secure Enterprise HA Server);
  - IP traffic inside any VPN tunnel MUST use IPv4 protocol;

Communications Media

- LAN
- Wi-Fi
- Mobile Network, GSM - LTE
  - From Windows 7 on – Mobile Broadband support
- xDSL (PPPoE)
- PSTN
- ISDN
- Automatic Media Detection (AMD)
- External Dialer
- Seamless Roaming (LAN / Wi-Fi / Mobile Network)

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
  - always
  - automatic (connection initiated by data transfer)
  - 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, Mobile Network, xDSL, PPTP, ISDN and modem connections
  - Duration or volume based budgets
  - Management of Mobile Network 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]

Datenkompression

- IPsec Compression

Link Firewall

Stateful Packet Inspection

Weitere Features

- VoIP Prioritization
- UDP Encapsulation
- IPsec Roaming [iii]
- WLAN 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 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),

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 lenght of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit
- Encryption Algorithms: AES with 128, 192, 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. If the user changes provider, the system automatically takes APN data from the corresponding SIM card and uses it in client configuration. This makes it easy to use inexpensive, local providers abroad.

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
- 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
- Password protected configuration and profile management
- Trace tool for error diagnosis
- Monitor can be tailored to include company name or support information
- Hotkey Support for connect/disconnect
- Custom Branding Option
- Internet Availability Tests
- VPN Tunnel Traffic Monitoring (Tunnel Availability Tests)

Hinweise

i NCP FND- Server kann kostenlos als Add-On hier heruntergeladen werden: http://www.ncp-e.com/de/downloads/download-software.html

iii Voraussetzung: NCP Secure Enterprise Server V 8.0 und später