NCP Secure Entry Client (Win32/64)
Release Notes

Service Release: **10.10.03 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

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299