NCP Secure Entry Client
Release Notes

Service release: 11.16 r43395
Date: April 2019

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 10, 32/64 bit (up to and including version 1809)
- Windows 8.x, 32/64 bit
- Windows 7, 32/64 bit

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Credential Provider without Hotspot Logon

The HotSpot Logon feature introduced with the new credential provider which takes place before Windows logon must be removed for security reasons. The HotSpot Logon is available as before after the user has logged on to Windows.

Update from Client Version 11.11 to 11.14 or Later Fails

Updating client version 11.11 to a newer version failed under certain circumstances. This problem has been resolved in the current version.

Troubleshooting 802.1X Authentication via LAN

Troubleshooting VPN connection in Friendly Networks

Adding a Profile Name to a Wi-Fi Profile

The Wi-Fi profile name is now displayed in the Wi-Fi configuration. This means that different Wi-Fi profiles can be used for networks with identical SSIDs.

Next Generation Network Access Technology

Broken VPN tunnel when using mobile connection

After a short time, the VPN connection was broken due to Dead Peer Detection when using a mobile connection. This issue has been resolved.

PKI error when using a Smart Card

When using a Smart Card, the client displayed a PKI error. This issue has been resolved.

3. Known Issues

None.

Next Generation Network Access Technology

NCP Secure Entry Client
Release Notes

Service release: **11.14 r42039**
Date: **December 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 1809)
- Windows 8.x, 32/64 bit
- Windows 7, 32/64 bit

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Checking Internet Availability for a Connection Medium

Checking Internet availability for a connection medium by pinging 8.8.8.8 has been limited to a maximum of four pings.

The HotSpot login functionality has been optimized

The HotSpot login received several optimizations specifically in conjunction with Seamless Roaming configurations.

Credential Provider Vulnerability

When using the NCP Credential Provider, a user could gain access to the Windows Explorer via the log window and the "Open File" button contained in it. This made it possible to get administration rights in PowerShell. This issue has been resolved.

Uninstalling the Client

Under certain circumstances, the filter driver of the VPN client was not correctly uninstalled. This issue has been resolved.

Software Update for other NCP OEM clients is not blocked

When performing a client update, the OEM variant of the client must match. The update function must be blocked. This issue has been resolved.

Next Generation Network Access Technology

Address Assignment to NCP Network Adapter

When using a Juniper gateway, it was not possible to assign a network address to the NCP network adapter under certain circumstances. This issue has been resolved.

Improvement to Connection Medium Behavior after Waking from Sleep Mode

IKEv1 / Aggressive Mode

When using IKEv1 with Aggressive Mode, problems could occur in conjunction with an automatic IKE policy. This issue has been resolved.

3. Known Issues

None.

Next Generation Network Access Technology

Service release: **11.13 r41436**
Date: **October 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 1809)
- Windows 8.x, 32/64 bit
- Windows 7, 32/64 bit

4. New Features and Enhancements

Update for Windows 10 Version 1809 – Driver Installation

Due to Microsoft updates, it was not possible to install previous clients on Windows 10 version 1809. This problem has been resolved.

5. Improvements / Problems Resolved

Friendly Net Detection Server

In networks with network access control when the IP segment changes after successful authentication, the detection of the Friendly Net Detection Server has been improved.

Performance Optimization of Data Transfer Outside the VPN

Optimization of the Client Update Process for Major Updates

Detection of major updates within the MSI installation process has now been improved. An issue with the `NcpClntInstallPath` environment variable, which may have been deleted after the client update, was also fixed.

Display of the VPN Client in the Task Bar

If the client GUI is closed, the icon is no longer displayed in the task bar. This corresponds to the behavior of client versions before 11.0.

Next Generation Network Access Technology

Diagnostic Data in the Installation Directory

If the full trace function was enabled or a HotSpot detection configured, diagnostic files were incorrectly written to the installation directory of the client. This issue has been resolved.

Improvement to Silent Installation

Under certain circumstances, the REBOOT property could be overwritten during the installation of the client. This issue has now been resolved.

Improved Compatibility to DHCP Servers

For a DHCP request, specifying the host name is optional, but not all DHCP servers support omitting the host name. For this reason, the host name is always sent as of this release.

Improved Compatibility to Third-party Gateways

IKE negotiation has been updated to improve compatibility to external gateways.

Firewall Setting: Exception for VPN Path Finder

If the "Allow IPsec protocol (ESP, UDP 500) and VPN Path Finder (TCP 443)" option was configured in the firewall settings, destinations were accessible through the VPN connection via HTTPS port 443 although this was not allowed by any other firewall rule. This issue has been resolved.

Length of the PKCS#11 File Name

The length of the input field in the PKI configuration of the client for the PKCS#11 module has been increased to 255 characters.

Reloading DLLs

The DLL loading process has been enhanced for increased security against manipulated DLLs.

Enhanced Security During Update Check

Security has been improved to avoid manipulation when the client checks for new versions.

Next Generation Network Access Technology

6. Known Issues

NCP Demo User Certificates

The NCP demo user certificates installed with previous client versions will expire on October 9, 2018. This means that existing test profiles such as for the NCP demo server "vpntest.ncp-e.com" will no longer work. From this client version on, new installations will no longer automatically configure these test profiles using this certificate. Only test profiles with the VPN configuration "Pre-shared key" can be created.

New certificates with extended validity are located in the certs subdirectory after installation. Previously, these certificates were located directly in the installation directory.

Next Generation Network Access Technology

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com   **7 / 18**

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

Major Release: **11.10 r39753**

Date: **June 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 1803)
- Windows 8.x 32/64 bit
- Windows 7, 32/64 bit
- Not supported: Windows Vista

1. New Features and Enhancements

Biometric Authentication (e.g. Fingerprint or Face Recognition) Before VPN Connection

To prevent unauthorized third parties from establishing a VPN connection, optional biometric authentication has been integrated in the NCP Secure Client prior to VPN connection. The configuration of this option can be found under "Profile Settings ⇨ Advanced Authentication ⇨ Pre-Authentication ⇨ Fingerprint reader / Biometric authentication". If this option is enabled, the prompt for user authentication is displayed directly after clicking the Connect button in the client GUI. The VPN will only connect if authentication is successful. Biometric authentication requires the Windows Hello feature in Windows 8.1 or above. For older operating systems or if a biometric device is not available, an alternative authentication method such as a password can be enabled. This option is only available for manual and variable connection modes.

Improved Client GUI

The client GUI and the tray popup window launched from the taskbar have been adapted to the current Windows 10 design.

Full 64-bit Support in NCP Secure Client

Starting from this version, all components of the NCP Secure Client have a 64-bit version.

Next Generation Network Access Technology

New Credential Provider GUI including Hotspot Logon

If the NCP Secure Client is configured to connect to the VPN before the user logs on to the Windows system, a reduced-feature version of the client monitor is displayed. Users can now also log on to a hotspot before logging on to Windows which works in the same way as the existing Hotspot Logon feature. The NCP Credential Provider icon shows the VPN connection status through a red or green background.

7. Improvements / Problems Resolved

Configuration of VPN Tunnel Endpoints

Starting from this version, multiple VPN tunnel endpoints can be configured with your domain names.

Optimization of DPD Feature

FIPS-Inside

FIPS mode can be switched on or off during a new installation or when changing the installation. Using a command line parameter, the FIPS mode can be configured as follows:
Add: ADDLOCAL=FIPSMode; Remove: REMOVE=FIPSMode

Extended Display of Connection Information

IPv6 addresses of the tunnel endpoint are now also displayed in the connection information.

Extended Information in Client Info Center

A new section with driver information in the Client Info Center shows the following values in the registry:
Name, Version, IfType, InfPath, MtU, NetCfgInstanceId
Under Windows 10, the version and build in the Client Info Center is now displayed.

Improvement of Hotspot Logon Feature

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

Next Generation Network Access Technology

Extended Client Update Function

From this version onwards, the client update function supports comparison with the central definition file via the HTTPS protocol. This definition file must now be signed to ensure that information about any existing updates reaches the client securely without unauthorized manipulation. Installation files deployed in this way are also compared by the client with the signature specified in the definition file.

8. Known Issues

NCP Demo User Certificates

The NCP demo user certificates installed with previous client versions will expire on October 9, 2018. This means that existing test profiles such as for the NCP demo server "vpntest.ncp-e.com" will no longer work. From this client version on, new installations will no longer automatically configure these test profiles using this certificate. Only test profiles with the VPN configuration "Pre-shared key" can be created.
New certificates with extended validity are located in the certs subdirectory after installation. Previously, these certificates were located directly in the installation directory.

Next Generation Network Access Technology

2. 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

3. 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

Next Generation Network Access Technology

- o Pre-shared Secrets or RSA signatures (and associated Public Key Infrastructure)
- Internet Key Exchange v2 (IKEv2):
  - o Pre-shared secrets
  - o RSA signatures (and associated Public Key Infrastructure)
  - o 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
  - o EAP unterstützt supported: PAP, MD5, MS-CHAP v2, TLS (selected by responder)
  - o IKEv2 Mobility and Multihoming protocol (MOBIKE)
  - o Perfect Forward Secrecy (PFS)
  - o IKE Config. Mode for dynamic allocation of private IP (virtual) address from address pool
- User authentication:
  - o User Authentication via Credential Management
    - – Windows Logon over VPN connection
  - o 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:
  - o 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:
  - o Extensible Authentication Protocol – Message Digest 5 (EAP-MD5): Extended authentication relative to switches and access points (layer 2)
  - o Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Extended authentication relative to switches and access points on the basis of certificates (layer 2)
  - o 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

Next Generation Network Access Technology

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

Next Generation Network Access Technology

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com   **13 / 18**

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

- 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)

Next Generation Network Access Technology

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com   **14 / 18**
Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

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

Next Generation Network Access Technology

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

Next Generation Network Access Technology

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)
  - o Monitor & Setup: en, de, fr, es
  - o Online Help and License en, de
- Icon indicates connection status
- Client Info Center – overview of:
  - o General information - version#, MAC address etc.
  - o Connection – current status
  - o Services/Applications – process(es) – status
  - o 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

Next Generation Network Access Technology

- Internet Availability Tests
- VPN Tunnel Traffic Monitoring (Tunnel Availability Tests)

Hinweise

i   NCP FND- Server is available for free as an Add-On and can be downloaded from here:
        http://www.ncp-e.com/de/downloads/download-software.html
iii   Prerequisites: NCP Secure Enterprise Server V 10.0 or newer

Next Generation Network Access Technology