NCP Secure Enterprise Client
Release Notes

Major Release: 11.10 r39552
Date: May 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, 32/64 bit

Prerequisites for the central management via Secure Enterprise Management (SEM)

To manage the client software centrally via SEM the following plugins are required:

- NCP Secure Enterprise Management: Version 4.05 or newer
- NCP Management Console: Version 5.0
- Client Configuration Plugin: Version 11.10
- License Plugin: Version 11.10
- Firewall Plug-in: Version 10.11 from r33042
- Update Client: Version 6.0

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.

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.

Endpoint Policy: New variable DNS_HOSTNAME

The DNS_HOSTNAME variable returns the DNS host names as shown in ipconfig /all. The existing HOSTNAME variable returns the NetBIOS names (uppercase only, maximum 15 characters).

IKEv2 Authentication According to RFC 7427

If required the client can use the padding method according to RFC 7427 for the IKEv2 connection. The server must support and accept IKEv2 connections and the padding method.
Configuration:
In addition to the new expert parameter "Activate negotiation according to RFC 7427" (enabled as default) in the expert configuration, the "RFC 7427 Padding method" can also be selected in the same menu under "Advanced IPsec options": PKCS#1 v.1.5 Padding or RSASSA-PSS.

IKEv2 RSA Authentication with Alternative Hash Algorithm

The new expert parameter "IKEv2 RSA Authentication with PRF Hash" under "Advanced IPsec Options", allows IKEv2 RSA authentication to use a different hash algorithm to the RFC recommended standard (SHA-1).
This is done by configuring an alternative algorithm (for example "HMAC SHA2 256-bit") for the "pseudorandom function" in the configuration of the "IKEv2 policy".
Configuration:
First select the algorithm for the "pseudorandom function [IKEv2 policy]", then activate the "IKEv2 RSA authentication with PRF hash" function under "Advanced IPsec options" in the expert configuration.

2. Improvements / Problems Resolved

Update Client Included in Installer

During a software update via NCP Secure Enterprise Management (SEM), the update client associated with the client version is now installed.

MSI Updates via NCP Secure Enterprise Management

This requires using the update client version 6.0.

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.

3. 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.

4. Getting Help for the NCP Secure Enterprise Client

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 information about the Enterprise Client, visit:
http://www.ncp-e.com/en/products/centrally-managed-vpn-solution/managed-vpn-client-suite.html
For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:
http://www.ncp-e.com/en/company/contact.html

5. Features

Central Management

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

- licensing (alternatively via VLS)
- configuration updates
- certificate updates
- software updates of the client

Network Access Control / Endpoint Security
The policies for Endpoint Security (Endpoint Policy Enforcement)) are created centrally at the Secure Enterprise Management (SEM) and each NCP Secure Enterprise Client is only permitted access to the company network in accordance with the corresponding rules.

High Availability Services

The NCP Secure Enterprise Client supports the NCP HA Services. These services are client / server based and can be used in two different operating modes: load balancing or failsafe mode. Regardless of the load on the server or whether a server has failed, the VPN connection to the corporate network is established and maintained reliably, in the background and without any delay for the user of the NCP Secure Enterprise Client.

Operating Systems

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, 27-30 for asymmetric key exchange and PFS.
- Diffie Hellman groups 19 - 21, 25, 26, 27-30 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

Endpoint Security

- Endpoint Policy Enforcement [ii]

Networking Features

Secure Network Interface

- LAN Emulation
  - Virtual 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
  - Messaging Center (send & receive SMSs)
- 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)

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

- 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]

Data compression

- IPsec Compression

Link Firewall

Stateful Packet Inspection

Additional Features

- VoIP Prioritization
- UDP Encapsulation
- IPsec Roaming [iii]

- WLAN Roaming [iii]
- WISPr support (T-Mobile hotspots)
- VPN bypass

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),

Zusätzliche 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, Windows version etc.
  - Network driver information
  - 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 If you wish to download NCP's FND Server as an add-on, please click here: https://www.ncp-e.com/en/resources/download-vpn-client/

ii Prerequisite: NCP Secure Enterprise Management

iii Prerequisite: 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