NCP Secure Entry Client

Release Notes

Service release: **12.00 r45109**

Date: **August 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 1909)
- Windows 8.x, 32/64 bit
- Windows 7, 32/64 bit

1. New Features and Enhancements

Quality of Service

Outgoing data from the client can be prioritized within the VPN tunnel. The total outgoing bandwidth must be entered in the QoS configuration for this purpose. The configured total bandwidth is static. The QoS feature is therefore only conditionally suitable for use in the mobile environment.
Data can be prioritized according to their origin by .exe file name (case sensitive) or directory (without subdirectories). These data sources can be grouped and each group can be assigned a minimum bandwidth. Outgoing data that is not assigned to a group are limited according to the remaining bandwidth. If a group is inactive, the remaining bandwidth is increased by the bandwidth that would have been allocated to the inactive group. The outgoing bandwidth allocated for the configured groups can be viewed under the menu item Connection/Connection Info/Quality of Service.

Temporary Home Zone

The option "Only set Home Zone temporarily" was added. Previously, the NCP Secure Client recognized the Home Zone after it had been set once. If the new option is set, the Home Zone is forgotten after restart, standby or change of connection medium and must be enabled again if necessary.

IPv4 / IPv6 Dual Stack Support

Both the IPv4 and IPv6 protocols are supported within the VPN tunnel. Split tunneling can be configured separately for IPv4 and IPv6.

Expert Mode

An expert mode has been added to the client configuration. In addition to the previous configuration options, the expert mode also includes other rarely used or experimental options.

Enhanced Connection Management

The connection management of the NCP Secure Client has been extended by two connection options:
"Disable mobile network when LAN cable is connected" and
"Disable mobile network when &Wi-Fi connection is established"

Enhancements to the Support Assistant

From the current version, the Support Assistant always collects all available log files for forwarding to Support. The files `setup.msilog, ncpdrvinst.log, ncpdrvupd.log` and `rwsrsu.log` have been added to the support wizard.

2. Improvements / Problems Resolved

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed. The following directories that were previously in the installation directory under `Programs\NCP\SecureClient\` have been migrated to `ProgramData\NCP\SecureClient\`:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
These are configuration files, certificates or log files. Binaries or resources remain in `Programs\....`
During the update process, the new directory structure is created automatically and the configuration is transferred accordingly. Configuration paths within the certificate configuration that contain the variable `%InstallDir%` are converted to paths with `%CertDir%`. `%CertDir%` refers to the path `C:\ProgramData\NCP\SecureClient\certs`.
Note: The configuration entry `%CertDir%\client1.p12` is equivalent to `client1.p12`.
For more information regarding the new directory structure please read the `Read_Me.pdf` file.

Enhanced Connection Status Information

The Connection Information status window displays the algorithms negotiated for the current VPN connection within the IKE negotiation and IPsec protocol.

Removal of Obsolete Configuration Parameters

The following configuration parameters have been removed from the configuration because they are now obsolete:

Communication Medium	ISDN

ISDN	PPP Multilink
ISDN	Multilink Threshold
IPsec Address Assignment	1st and 2nd WINS server
Link firewall	Can only be configured in expert mode

Support for Gemalto IDPrime 830 SmartCard

The PIN handling for Gemalto IDPrime 830 SmartCards configured via Microsoft Smart Card Key Storage Provider (CSP) has been optimized.

Optimization of the NCP Filter Driver

The data throughput of the NCP filter driver has been optimized.

Optimization of Logon via time-based OTP

GUI Scaling

Some configuration dialogs were not displayed correctly if GUI scaling was enabled. This issue has been resolved.

3. Known Issues

Temporary Home Zone

If two network adapters are available, the Home Zone will only be forgotten on one adapter if the "Only set Home Zone temporarily" option is set.

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	Microsoft Windows (32 and 64 bit): Windows 10, Windows 8.x, Windows 7
Security Features	The Entry Client supports all IPsec standards in accordance with RFC

Personal Firewall	Stateful Packet Inspection;
	IP-NAT (Network Address Translation);
	Friendly Net Detection (FND) (Firewall rules are automatically adapted, if the connected network is recognized because of its IP address area, or the NCP FND server's*);
	start FND dependent action;
	home zone;
	secure hotspot logon;
	differentiated filter rules relative to: protocols, ports, applications and addresses, LAN adapter protection;
	IPv4 and IPv6 support

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.
Virtual Private Networking	IPsec (Layer 3 Tunneling), conform to RFC; IPsec proposals can be determined through the IPsec gateway (IKE/IKEv2, IPsec Phase 2); Event log; communication only in the tunnel; MTU size fragmentation and reassembly, DPD, NAT-Traversal (NAT-T); IPsec tunnel mode
Encryption	Symmetric processes: AES 128,192,256 bits; Blowfish 128,448 bits; Triple-DES 112,168 bits; Dynamic processes for key exchange: RSA to 2048 bits; seamless rekeying (PFS); Hash algorithms: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH group 1,2,5,14-21, 25-30
FIPS Inside	The IPsec Client incorporates cryptographic algorithms conformant with the FIPS standard. The embedded cryptographic module incorporating these algorithms has been validated as conformant to FIPS 140-2 (certificate #1747). FIPS compatibility is always given if the following algorithms are used for set up and encryption of the IPsec connection: ▪ DH Group: Group 2 or higher (DH starting from a length of 1024 Bit) ▪ Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit ▪ Encryption Algorithms: AES with 128, 192 and 256 Bit or Triple DES

Authentication Processes	IKE (Aggressive mode and Main Mode), Quick Mode; XAUTH for extended user authentication; IKE config mode for dynamic assignment of a virtual address from the internal address pool (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): Extended authentication relative to switches and access points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): Extended authentication relative to switches and access points on the basis of certificates (Layer 2); Support of certificates in a PKI: Soft certificates, smartcards, and USB tokens: Multi Certificate Configurations; Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready
Strong Authentication	Biometric Authentication (Windows 8.x or higher) X.509 v.3 Standard; PKCS#11 interface for encryption tokens (USB and smartcards); smartcard operating systems: TCOS 1.2, 2.0 and 3.0; smart card reader interfaces: PC/SC, CT-API; PKCS#12 interface for private keys in soft certificates; CSP for use of user certificates in Windows certificate store PIN policy; PIN policy; administrative specification for PIN entry in any level of complexity; Revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL), OCSP.
Networking Features	LAN emulation: Ethernet adapter with NDIS interface, full WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network, Mobile Broadband from Windows 7) support
Network Protocol	IPv4 / IPv6 Dual Stack
Dialers	NCP Internet Connector, Microsoft RAS Dialer (for ISP dial-in via dial-in script)
VPN Path Finder**	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible
Seamless Roaming**	If a communications medium error occurs, automatic switchover of VPN tunnel to another Internet communication medium (LAN/WWAN/3G/4G) without altering IP address ensures that applications communicating over VPN tunnel are not disturbed and application session is not disconnected. (prerequisite: NCP Secure Enterprise VPN Server)
Additional Features	UDP encapsulation, WISPr-support, IPsec-Roaming, Wi-Fi roaming, import of the file formats:*.ini, *.pcf, *.wgx and *.spd, Multi Certificate Support

Transmission Media	Internet, LAN, WI-FI, GSM (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA, PSTN
IP Address Allocation	DHCP (Dynamic Host Control Protocol), DNS: Dial-in to the central gateway with changing public IP addresses through IP address query via DNS server
Line Management	DPD with configurable time interval; Short Hold Mode; Wi-Fi roaming (handover); channel bundling (dynamic in ISDN) with freely configurable threshold value; timeout (controlled by time and charges); budget manager (administration of connection time and/or –volume for GPRS/ 3G and Wi-Fi, in case of GPRS/ 3G separated administration of roaming abroad)
APN of 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
Data Compression	IPCOMP (lzs), deflate
Quality of Service	Prioritization of configured outgoing bandwidth in VPN tunnel.
Point-to-Point Protocols	PPP over ISDN, PPP over GSM, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP security architecture, ESP, ISAKMP/Oakley, IKE, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, RFC 7427: IKEv2-Authentication (Padding-method)
Client Monitor Intuitive, Graphical User Interface	Multilingual (German, English, Spanish, French); Client Info Center; Configuration, connection management and monitoring, connection statistics, log-files (color displayed, easy copy&paste-function); Internet availability test; Trace tool for error diagnosis; Traffic light icon for display of connection status; Integrated support of Mobile Connect Cards (PCMCIA, embedded); The Client Monitor can be tailored to include your company name or support information; Password protected configuration management and profile management, configuration parameter lock; Automatic check for newer software version

*) 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.html

**) Prerequisite: NCP VPN Path Finder Technology on the Gateway is required or NCP Secure Enterprise Server

More information on NCP Secure Entry Client is available on the Internet at:
https://www.ncp-e.com/en/products/ipsec-vpn-client-suite.html

You can test a free, 30-day full version of Secure Entry Client (Win32/64) here:
https://www.ncp-e.com/en/resources/download-vpn-client.html

FIPS 140-2 Inside