

NCP Secure Enterprise 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

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 5.20 or newer
- NCP Management Console: Version 5.20 or newer
- Client Configuration Plugin: Version 12.00 or newer
- License Plugin: Version 12.00 or newer
- Firewall Plug-in: Version 12.00 or newer

Before updating to version 12, we recommend checking the client version already installed on the user computer in the case of a rollout via SEM. If the version number is version 11.14 or above, the update to version 12 can be carried out without further measures. If the client version is older, it is strongly recommended to first distribute the update client version 6.01 via SEM. This will place it first in the software update list. Furthermore, the notes under [New Directory Structure](#) must be observed.

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

Next Generation Network Access Technology



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.

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"

Entrust PKI Support has been removed

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`.

Please note when using the NCP Secure Enterprise Management:

The NCP Secure Enterprise Clients can be upgraded to version 12.x as before. The local configuration is automatically converted during the update process. When using NCP Secure Enterprise Management to assign new configurations, the paths in the configurations or templates to be assigned must be modified before distribution. Likewise, for different client versions, a distinction must be made between configurations from version 12.x and older versions. The use of absolute paths is not recommended by NCP. For more information regarding the new directory structure please read the `Read_Me.pdf` file.

Changes to Firewall Function after the End of the Trial Period

After installation and the start of the trial period, NCP Secure Client has full functionality for 30 days. At the end of the trial period, VPN connections and the firewall feature were disabled.

This behavior has now been changed. At the end of the trial period, the firewall now continues to function and the computer is still protected by the firewall.

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:

Internet connection	ISDN
Line management	Maintain IP during manual connection setup
Line management	Dynamic link
Line management	Threshold value for link activation
Callback	
Incoming calls	
Link settings	Logon to network
Link settings	MAC address
DNS management	1st and 2nd WINS server



Advanced IPsec options

Destination address for IPsec gateway

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.

INIT Rollout Process

The INIT user authentication using the environment variables %USERNAME% for the user name and %HOMEPATH% for the authentication code was not possible from Windows 10 Version 1803. This issue has been resolved.

Parameter Lock in the Wi-Fi Manager

The option "Connect automatically" can now be blocked by the parameter lock, i.e. it cannot be deactivated by manually disconnecting a Wi-Fi connection if the parameter lock is set.

Revised Message after Trial Expiration

The message *"Trial version has expired. Please license or uninstall the software."* has been replaced by the following message: *"The installation of the Secure Client has not yet been completed. Please establish a VPN connection to your company's network to complete the process."*

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.

NCP Secure Enterprise Client

Release Notes



SMS Center: Cannot Receive SMS

The NCP Secure Client offers the option of sending and receiving SMS messages if mobile phone hardware is available. Receiving SMS does not work in this client version.

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

Operating Systems

Microsoft Windows (32 and 64 bit): Windows 10 Version 1903, Windows 8.x, Windows 7

Security Features

The Enterprise Client supports all major IPsec standards in accordance with RFC

Personal Firewall

Firewall Configuration*

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*);

Start FND dependent action;

Secure hotspot logon;

Home Zone;

Differentiated filter rules relative to: protocols, ports, applications and addresses, LAN adapter protection, IPv4 and IPv6 support, Central administration*

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), RFC-conformant; IPsec proposals can be determined through the IPsec gateway (IKEv1/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,SHA384, SHA-512, MD5, DH group 1,2,5,14-21, 25, 26

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 conformance will always be maintained when any of the following algorithms are used for establishment 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

NCP Secure Enterprise Client

Release Notes



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, smart cards, and USB tokens:
Pre-shared secrets, one-time passwords, and challenge response systems;

RSA SecurID ready

Strong Authentication

X.509 v.3 Standard; biometric Authentication (Windows 8.x or higher)

Standards

PKI Enrollment*

PKCS#11 interface for encryption tokens (USB and smart cards);
smart card 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 the use of user certificates in the windows certificate store
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. CMP* (Certificate Management Protocol)

Network Access Control

Endpoint Policy Enforcement**

Networking Features

LAN emulation: Ethernet adapter with NDIS interface, full WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network, Windows 7 Mobile Broadband) support

Network Protocol

IPv4 / IPv6 Dual Stack

Dialers

NCP Internet Connector, Microsoft RAS Dialer (for ISP dial-in via dial-in script)

Next Generation Network Access Technology

NCP Secure Enterprise Client

Release Notes



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)
VPN Path Finder***	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible (prerequisite: NCP VPN Path Finder Technology on VPN gateway)
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
Communication Media	Internet, LAN, Wi-Fi, GSM (incl. HSCSD), GPRS, 3G, LTE, HSDPA, PSTN.
Line Management	DPD with configurable time interval; Short Hold Mode; Wi-Fi roaming (handover); Timeout (controlled by time and charges); Budget Manager; Connection Modes: automatic, manual, variable (reconnection dependent on how previous disconnect invoked)
APN from SIM Card	APN (Access Point Name) defines access point of a mobile data connection at a provider. If user changes provider, system automatically uses APN data from SIM card to configure Secure Client
Data Compression	IPCOMP (lzs), deflate
Quality of Service	Prioritization of configured outgoing bandwidth in VPN tunnel.
Additional Features	UDP encapsulation, WISPr-support, IPsec-Roaming, Wi-Fi roaming, Split Tunneling
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)

Next Generation Network Access Technology

NCP Secure Enterprise Client

Release Notes



Client Monitor

Intuitive, Graphical User Interface

Multilingual (English, Spanish, French, German);
Intuitive operation;
Configuration, Connection Management and Monitoring, Connection Statistics, Log-files, Internet availability test, Trace Tool for error diagnosis;
Display of connection status;
Integrated support of Mobile Connect Cards, embedded);
Client Monitor can be tailored to include company name or support information;
Password protected configuration management and profile management, configuration parameter lock

Update with SEM

To update the client software the SEM version 5.20 and the following plugins are required:

- License Plugin: Version 12.00
- Client Configuration Plugin: Version 12.00
- Firewall Plug-in: Version 12.00
- Update Client: Version 7.0

*) 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 Secure Enterprise Management

***) Prerequisite: NCP Secure Enterprise VPN Server

More information on NCP Secure Enterprise Client is available on the Internet at:

<http://www.ncp-e.com/en/products/centrally-managed-vpn-solution/managed-vpn-client-suite.html>



NCP PATH FINDER

FIPS 140-2 Inside

Next Generation Network Access Technology