NCP Secure Enterprise Client
Release Notes

Major release: **13.04 r29374**
Date: **March 2022**

Prerequisites

Operating System Support

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (up to and including version 21H2)
- Windows 10, 64 bit (up to and including version 21H2)

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 5.30 or newer
- NCP Management Console: Version 5.30 or newer
- Client Configuration Plugin: Version 13.00 or newer
- License Plugin: Version 13.00 or newer
- Firewall Plug-in: Version 13.00 or newer

The following features are no longer available as of this client version:

- SMS Center
- Connection medium: modem, xDSL, ext. dialer

Before updating to version 13, 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 13 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 up to max. 7.01 via SEM. This will place it first in the software update list.
When updating from a version lower than 12.0, the notes in "New Directory Structure" must be observed.

New Directory Structure

For security reasons and compatibility with Windows, the directory structure of the NCP Secure Client has been changed as of version 12.0. 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 13.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.

1. New Features and Enhancements

Revised hotspot login

Starting with this version 13.0 of the NCP Secure Client, the Chrome-based Microsoft Edge web browser is invoked via WebView2 runtime and used exclusively for the purpose of logging into a hotspot. The prerequisite for this is the installed WebView2 runtime (from version 94.0.992.31 or newer) within the operating system. The WebView2 runtime can be downloaded here:
https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section

Support for max. 250 split tunneling remote networks

For both IPv4 and IPv6, up to 250 split tunneling configurations can be communicated from the NCP Secure Enterprise VPN Server to the client via IKEConfigMode. The prerequisite for this is an NCP Secure Enterprise VPN Server version 13.0 or higher.

Support for WPA3 encryption

The Wi-Fi Manager integrated in the NCP Secure Client can now also manage Wi-Fis encrypted with WPA3.

Support of RFC 7296

RFC 7296 defines the forwarding of split tunneling remote networks by the VPN gateway to the VPN client. This RFC is supported as of this client version.

Enhanced of the VPN status in the Windows registry

Previously, the connection status of the NCP client could be found in the registry under "`Computer \ HKEY_LOCAL_MACHINE \ SOFTWARE \ WOW6432Node \ NCP engineering GmbH \ NCP RWS / GA \ 6.0`" for the `SecClCsi` parameter with the values

0 = not connected

and

1 = connected

read out. As of this version, the client saves additional states in the Windows registry in the following location:

`HKEY_LOCAL_MACHINE \ SOFTWARE \ NCP engineering GmbH \ NCP Secure Client`

or

`HKEY_LOCAL_MACHINE \ SOFTWARE \ WOW6432Node \ NCP engineering GmbH \ NCP Secure Client`

The associated parameter `ConnectState` can have the following values:

0 = connection is disconnected

1 = connection is being established

2 = connection has been successfully established

3 = Internet connection is interrupted, VPN connection is on hold

4 = connection established but only communication with the NCP management server possible (licensing)

Reading out Windows environment variables in the certificate configuration

In the "CSP user certificate store" certificate configuration, the client supports the entry of Windows environment variables, e.g. `%userdnsdomain%`, `%userdomain%` or `%computername%`. These are queried when reading the cnf configuration in the underlying operating system and their return values are statically adopted in the configuration. A combination with additional characters is possible, for example: "`%computername%.%userdnsdomain%`".

Americas: NCP engineering, Inc. • 601 Cleveland Street, Suite 501-25 • Clearwater, FL 33755 • Phone: +1 (650) 316-6273
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

2. Improvements / Problems Resolved

Revised file handling of ncp.db

In rare cases, the `ncp.db` file became unusable during operation, causing the client to lose its license. This problem has been fixed.

„Network Location Awareness“ not available with NCP firewall active

If the client firewall is activated, the "Network Location Awareness" of the Windows operating system is not available. In the case of the exclusively desired Friendly Network Detection functionality, the "Network Location Awareness" of the Windows operating system can be used by configuring a client firewall rule "Allow all network traffic bidirectionally" and setting a registry key. For this purpose the parameter `RegDw "WscIntegration"=0` has to be configured in the registry within `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt`. The default value of this parameter is `1`.

Option "Disable Wi-Fi when LAN cable is connected": Problem with Hyper-V

When using Hyper-V functionality, the Wi-Fi adapter was incorrectly deactivated when the "Disable Wi-Fi when LAN cable is connected" option was set. This problem has been fixed.

Automatic login via credential provider

When using the logon option with configured user credentials, a locked Windows workstation could be unlocked by selecting the NCP credential provider. This problem has been fixed.

Troubleshooting for multiple certificates with the same issuer and subject in the Windows certificate store

If the Windows certificate store contained certificates with identical issuer and subject, the wrong expired certificate was sometimes used by the client and acknowledged with the message "unable to get issuer certificate". This problem has been fixed.

Support for NCP Secure VPN GovNet Box removed

Removed the internal firewall rules required to run the NCP Secure VPN GovNet Box.

Changed default value in FND options

The default value for the "Check for friendly networks periodically" option has been changed from 0 sec to 3600 sec.

Incomplete log files

Under certain circumstances, incorrect write accesses to the client log files occurred, so that log entries

were missing in the worst case. This problem has been fixed.

Revised installation routine

In rare cases, after the end of the installation process, before the computer restart, the network connection was completely disconnected. This problem has been fixed. Furthermore, the "Repair program" functionality within the MSI installation process has been removed.

Error after standby state in connection with IPv6 fixed

After the standby state of the PC there were connection problems with IPv6. This error has been fixed.

Newly imported certificates in Computer CSP were not taken over

In rare cases, connection errors occurred when using NCP Secure Client 12.20 when a new certificate was distributed by Entrust. This error has been fixed.

Problem during installation with `certmgr.exe`

During the installation of the NCP Secure Client, the `certmgr.exe` file created by Microsoft was used to install the NCP manufacturer certificate. This file was recognized as not signed. Starting from this version, the newer `certutil.exe` is used instead of `certmgr.exe`. This has fixed the problem.

Dynamic certificate selection

The certificate selection has been significantly improved. In addition, only valid certificates will be imported in the future.

Import of a `ncpphone.cnf` via `ncpclientcmd.exe` before user login

Starting with version 12.x of the NCP Secure Client, the CLI tools `rwscmd.exe` and `ncpclientcmd.exe` could not read in a cnf configuration before user login. This problem has been fixed.

Bugfix in ESP header for IPv6

Revised parameter locks in the client GUI

In the client GUI, measures have been taken to ensure that blocked buttons cannot be activated by certain tools and that blocked functions are made available as a result.

Fixed a problem when establishing a connection with VPN Path Finder via IPv6

Improvement of the FND compatibility with network switches

Optimization of the establishment of an IKEv2 connection with EAP

In certain situations, the establishment of the VPN tunnel with IKEv2 and EAP could take an unusually long time. This problem has been resolved.

Improvement of the VPN bypass compatibility with MS Teams

3. Known Issues

Compatibility of the Update Client

The Update Client 8.0 included in the NCP Secure Client is not compatible with older versions of the NCP Secure Client and accordingly cannot be distributed for these versions via SEM Update.

Option: "Automatically Open Connection Setup Dialog“

Under certain circumstances, the Logon option "Automatically Open Connection Dialog" does not work.

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:

https://www.ncp-e.com/en/service-resources/download-vpn-client/version-information/

For further information about the Enterprise Client, visit:

https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/

For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:

https://www.ncp-e.com/en/company/contact/

5. Features

Operating Systems	Microsoft Windows (64 bit): Windows 11, Windows 10 x86-64 platform
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 the connected network is 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, 25-30
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 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

Authentication Processes	IKE (Aggressive Mode and Main Mode, Quick Mode); XAUTH for extended user authentication; IKEv2; 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; Multi Certificate Configurations; Pre-shared secrets, one-time passwords, and challenge response systems; RSA SecurID ready
Strong Authentication	X.509 v.3 Standard; biometric Authentication (Windows 8.1 or higher) PKCS#11 interface for encryption tokens (USB and smart cards); smart card operating systems: TCOS 1.2, 2.0 and 3.0 Signature Card Version 2.0 Release 1, Atos CardOS V5.3 QES, V1.0; Smart card reader interfaces: PC/SC, CT-API, Microsoft CSP; PKCS#12 interface for private keys in soft certificates; CSP for the use of user certificates in the windows certificate store CSP for the use of smart cards via vendor API 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
PKI Enrollment*	CMP* (Certificate Management Protocol)
Network Access Control	Endpoint Policy Enforcement**
Networking Features	LAN emulation: Ethernet adapter with NDIS interface, full Wi Fi (Wireless Local Area Network) and WWAN (Wireless Wide Area Network, Mobile Broadband) support
Network Protocol	IPv4 / IPv6 Dual Stack
Dialers	NCP Internet Connector or Microsoft RAS Dialer (for ISP dial-in via dial-in script)
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 (Virtual) Secure Enterprise VPN Server)

Americas: NCP engineering, Inc. • 601 Cleveland Street, Suite 501-25 • Clearwater, FL 33755 • Phone: +1 (650) 316-6273
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

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 (administration of connection time and/or –volume for GPRS/ 3G and Wi-Fi, in case of GPRS/ 3G separated administration of roaming abroad) 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 (only for IKEv1)
Quality of Service	Prioritization of configured outgoing bandwidth in VPN tunnel.
Additional Features	Automatic media detection; UDP encapsulation, WISPr-support, IPsec-Roaming, Wi-Fi roaming, Split Tunneling
Point-to-Point Protocols	PPP over GSM, PPP over Ethernet; MLP, CCP, CHAP
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 (English, Spanish, French, German); Client Info Center; 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; Client Monitor can be tailored to include company name or support information; Password protected configuration management and profile management, configuration parameter lock

Americas: NCP engineering, Inc. • 601 Cleveland Street, Suite 501-25 • Clearwater, FL 33755 • Phone: +1 (650) 316-6273
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

Update with SEM	To update the client software the SEM version 5.30 and the following plugins are required: • License Plugin: Version 13.00 • Client Configuration Plugin: Version 13.00 • Firewall Plug-in: Version 13.00 • Update Client: Version 8.00

*) If you wish to download NCP's FND server as an add-on, please click here:
https://www.ncp-e.com/en/service-resources/download-vpn-client/
**) Prerequisite: NCP (Virtual) Secure Enterprise VPN Server

More information on NCP Secure Enterprise Client is available on the Internet at:
https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/

FIPS 140-2 Inside

Americas: NCP engineering, Inc. • 601 Cleveland Street, Suite 501-25 • Clearwater, FL 33755 • Phone: +1 (650) 316-6273
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299