NCP Secure Entry Client
Release Notes

Major release: **13.11 r29631**
Date: **September 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)

HotSpot login

For the correct function of the HotSpot login, at least version 101.0.1210.39 of the Microsoft WebView2 Runtime must be installed.

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 `Program Files\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 `Program Files\...`.
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`.

1. New Features and Enhancements

New option: "DNS domains to be resolved in the tunnel".

The split DNS functionality can be configured using the new option "DNS domains to be resolved in the tunnel". In the case of configured split tunneling, the DNS requests of the configured domains are sent into the VPN tunnel. All other DNS requests bypass the VPN tunnel.

RFC 7296 support

The VPN client now supports RFC 7296 for distributing split tunneling configurations from the VPN gateway.

2. Improvements / Problems Resolved

New rights structure within `C:\ProgramData\NCP\`

A user had write permissions within the directory `C:\ProgramData\NCP\`. These were limited to a minimum. For example, a user can now no longer store CA certificates in the designated directory. Likewise, the directory and permissions structure has been rebuilt so that no application in the user and system context writes to the same directory. This problem has been fixed.

Improvements in server-side configured Split DNS

Automatic Windows logon

If the option "Automatic Windows logon with configured credentials" was selected within the logon options, the Windows logon did not work. Likewise, there was a problem in connection with 2-factor authentication via TOTP. This problem has been fixed.

Fix for Seamleass Roaming and IPv6 destination addresses

VPN username from cache

After updating a previous version, the cached VPN username was sometimes not displayed correctly in the login dialog. This problem has been fixed.

Wrong status display after profile change

After a profile change from a certificate-based profile with successful PIN entry to a profile with pre-shared key, the entered PIN was not deleted and the PIN icon was not removed from the client GUI. This issue has been fixed.

PKI error when switching profiles

When switching profiles from a certificate-based profile with *.p12 file to a profile with SmartCard reader, a PKI error was displayed. This problem has been fixed.

Update to zlib version 1.2.12

The zlib version used in the VPN client was raised to 1.2.12. This closed the zlib security vulnerability [CVE-2018-25032].

OpenSSL security patch

The vulnerabilities [CVE-2022-0778] and [CVE-2020-1971] have been fixed in OpenSSL.

Migration to TLS 1.2

TLS versions 1.0 and 1.1 are no longer supported with this client release.

Update to cURL library 7.84.0

The cURL version used in the VPN client has been upgraded to 7.84.0. This closed the cURL vulnerabilities [CVE-2022-27776], [CVE-2022-27775], [CVE-2022-27774], [CVE-2022-22576], [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207], and [CVE-2022-32208].

Improved compatibility with third-party gateways in conjunction with 2-factor authentication / token entry.

Incorrect status display: smart card

Under certain circumstances, a profile with 2-factor authentication incorrectly displayed a smart card icon. When switching to a profile with a smart card, an error message was displayed stating that the smart card was not initialized correctly. This problem has been fixed.

Problem solved after changing DNS entries in VPN Bypass configuration.

Problem solved when calling HotSpot login

The HotSpot login was not called correctly if the autostart option "Icon in system tray" was selected. This problem has been fixed.

Troubleshooting an incorrectly displayed PIN request

When using the CSP user certificate store, a PIN was sometimes incorrectly prompted. This problem has been fixed. Likewise, the PIN query option in the case of the CSP user certificate store has been removed in the client plug-in.

Improved compatibility with third-party gateways when addressing via IPv6

PAP/CHAP error during connection setup

Under certain circumstances, the VPN client displays a PAP/CHAP error when establishing an IKEv2 connection. This can be resolved by the user by opening the VPN profile and confirming with "Ok". This problem has been fixed.

Revision of the "Connection setup before Windows logon" function

To prevent possible privilege escalation, the "Connect before Windows logon" function has been revised. In this case, a standard user, if this function was not deactivated via the configuration locks, could sneak administrator rights, e.g. via a configured CMD shell. With this change, only batch files created by the administrator in the `C:\ProgramData\NCP\SecureClient\scripts\` directory can be selected.

Improve compatibility with Juniper SRX gateways in case of ReKeying phase.

Support for RFC 8598

RFC 8598 defines how the VPN gateway passes the split DNS configuration to the VPN client. This RFC is supported as of this client version.

Network connection permanently disconnected after installation

After installing the client, the network connection was permanently disconnected. Only after rebooting the computer, network communication was possible again. This problem has been fixed.

Problem importing a previously exported profile

Importing an exported profile into a client with version 13 failed. This problem has been fixed.

General improvements in INI or PCF file import.

Improved compatibility with third-party gateways regarding IP address assignment.

If the VPN client was assigned an IP address ending with `.255` during connection establishment, routing through the VPN tunnel was not possible. This problem has been fixed.

3. Known Issues

Option: “Automatically open dialog for connection establishment”

Under certain circumstances, the Logon option "Automatically open dialog for connection establishment" does not work.

Application-based VPN bypass configuration

Configuring a DNS within the VPN Bypass configuration will invalidate an application-based rule contained within it.

PIN menu entries

When using hardware certificates, the PIN menu entries “Enter/Reset/Change PIN” without function can be selected incorrectly.

Seamless roaming

Under certain circumstances, the VPN tunnel status remains at "Keep tunnel logical" when switching from WLAN to LAN and a functional connection via LAN is not established. This must be done by manually disconnecting and connecting.

Home Zone and IPv6

If the predefined Home Zone rule is active in the firewall settings of the VPN client, outgoing IPv6 packets to the local network are dropped in the defined Home Zone network.

Major release: **13.04 r29378**
Date: **April 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)

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

- Connection medium: modem, xDSL, ext. dialer

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 `Program Files\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 `Program Files\...`.
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`.

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

INI file import for max. 250 split tunneling remote networks

For IPv4 as well as for IPv6 up to 250 split tunneling configurations each can be imported into the client via INI file.

New Split DNS parameter

The targeted redirection of DNS requests into the VPN tunnel can be configured by setting the `DomainInTunnel` parameter in the INI file with a max. string length of 1023.The string contains the domain names to be resolved, separated by commas:

`google.com` – all domains containing `google.com` are used, e.g. `www.test-google.com`

`.google.com` – all domains containing `.google.com` are used, e.g. `news.google.com`

`news.google.com` – all domains containing `news.google.com` are used

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

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.

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

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.

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.

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

Option: “Automatically open dialog for connection establishment”

Under certain circumstances, the Logon option "Automatically open dialog for connection establishment" does not work.

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 (64 bit): Windows 11, Windows 10 x86-64 platform
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 (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
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, 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

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

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
Networking Features	LAN emulation: Ethernet adapter with NDIS interface, full WLAN (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/mobile data connection) 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)
VPN Path Finder**	NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500 respectively UDP encapsulation is not possible
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, GPRS, LTE, 5G, 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 mobile data connection and Wi-Fi, in case of mobile data connection separated administration of roaming abroad) Connection Modes: automatic, manual, variable (reconnection dependent on how previous disconnect invoked)
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 (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, import of the file formats:*.ini, *.pcf, *.wgx and *.spd,
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 (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; Display of connection status; Integrated support of Mobile Connect Cards; 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

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

*) 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 VPN Path Finder Technology on the Gateway is required

More information on NCP Secure Entry Client is available on the Internet at:
https://www.ncp-e.com/en/products/ipsec-vpn-client-suite/vpn-clients-for-windows-10-8-7-macos/

You can test a free, 30-day full version of Secure Entry Client (Win32/64) here:
https://www.ncp-e.com/en/service-resources/download-vpn-client/#c28622

FIPS 140-2 Inside