Release Notes

NCP Secure Entry Client

for Windows

Major release: 14.10 r32527
Date: July 2026

Prerequisites

Microsoft Windows Operating Systems

The following Microsoft Operating Systems are supported with this release:

- Windows 11, 64 bit (from version 23H2 up to and including version 25H2)
- Windows 10, 64 bit (Version 22H2, as well as Windows 10 Enterprise LTSC 2021 version 21H2)

HotSpot login

For the correct function of the HotSpot login the Microsoft WebView2 Runtime must be installed.

Notice Regarding Future Client Versions

The feature

- *Deny the start of the (dis)connect.bat* (in the Link options)

has been deprecated and will be removed in a future client version.

The active media selection for LAN, Wi-Fi, and cellular networks will be removed in a future version of the client. This change is being made because current Windows operating systems already provide this functionality. Client features such as seamless roaming and the configuration of Wi-Fi SSIDs are not affected by this change and will remain available.

The following features are no longer available starting with client version 14.10:

The following features

- IEEE 802.1x authentication (EAP) under the *Other Options/EAP* menu item
- Quality of Service (QoS)
- GUI scaling

are no longer included in the feature set of the NCP Secure Client as of major release 14.10.

The *Enable Certificate Selection* feature, found within the *User Certificate* configuration, cannot be used in conjunction with the new GUI.

The option to select the installation directory or path within the installation routine has been removed. The client is now installed only in the default installation directory at *c:\Program Files*\. In the event of an update, the original path is retained.

1. New features and enhancements

New Client GUI

The NCP Secure Client GUI has been redesigned and now features a new look with Dark Mode support after a fresh installation. If you're updating, you can continue using the GUI in its previous design by selecting *Legacy Mode* in the client configuration.

FQDN-Based Split Tunneling

In the FQDN-based split tunneling configuration, the remote destination is entered as a domain name for either IPv4 or IPv6. This entry ensures that only data destined for this domain name—or other configured domain names or address ranges (as specified in the split tunneling configuration)—is transmitted through the VPN tunnel.

Example: FQDN: *EXCHANGE.DOMAIN.COM*

Only data destined for *EXCHANGE.DOMAIN.COM* is sent through the VPN tunnel. The corresponding IP address is automatically added to the split tunnel table in the client configuration. The DNS server used to resolve the FQDN must also be accessible within a configured split-tunnel network. This should be the first entry in the table.

New FND Protocol

This client version introduces a new, TLS-based protocol for communicating with the FND server. To use this protocol, you must have an FND server configured for it, version 4.0 or later.

Seamless Roaming and IKEv2

If a gateway does not support MOBIKE when using IKEv2, the NCP Secure Client performs a rekeying. This provides seamless roaming functionality similar to IKEv1, even with IKEv2, but without MOBIKE support.

Padding Method According to RFC 7427

The configuration within the *Expert Mode* under *Advanced IPsec Options* has been expanded to include two options:

- *Allow RSA authentication with PKCS#1 V1.5 padding*
- *Allow RSA authentication with SHA-1 hash*

2. Improvements / Problems Resolved

Update to OpenSSL 3.5.6 – Third-Party Packages

The update to OpenSSL 3.5.6 addressed the following security vulnerabilities:
NCPVE-2025-1015, CVE-2025-11187, CVE-2025-15467, CVE-2026-28386, CVE-2026-28387, CVE-2026-28388, CVE-2026-28389, CVE-2026-31789, CVE-2026-31790, CVE-2026-31791

In addition, the open-source third-party packages used have been updated.

Connection Issues with 5G Modems

Some devices equipped with 5G modems experienced connection issues with cellular networks once the NCP Secure Client was installed on the device. The problem was caused by a bug in the modem's hardware driver.

In this client version, the NCP Secure Client has been modified accordingly to ensure smooth operation even with these drivers.

Data Throughput Optimization

When the client firewall was enabled, a noticeable drop in data throughput occurred. This issue has been resolved.

New network driver version: 14.1.2603

Uninstalling the NCP Driver

If the previous version of NCP Secure Client 13.19 was already installed on the device, uninstalling a version 13 that was subsequently installed via an update might not have completely removed the NCP driver. This issue has been resolved.

Default Value of the DH Group

When creating a new VPN profile, the DH group for the IKEv2 key exchange and the PFS group have been increased from 14 to 19.

Split DNS – External DNS Requests

If Split DNS functionality is configured, no DNS requests for the configured internal domain are routed externally or bypass the VPN tunnel.

Forward Local Networks Through the Tunnel

If the *Full Local Network Enclosure Mode* feature was disabled in the client, the change did not take effect until the operating system was restarted. This issue has been resolved.

Accessibility Revisions

With the introduction of the new GUI, accessibility features were revised and tested with the screen readers JAWS and Microsoft Narrator.

Windows Pre-Logon

If the “Always” profile setting is configured in the connection options and the credential provider is enabled, the user can automatically log on to Windows without any further action simply by clicking the credential provider on the logon screen.

Troubleshooting: Uninstallation routine does not remove all files/folders

PIN Menu Items

The “Enter PIN” and “Reset PIN” menu items were incorrectly displayed when using a hardware certificate. This issue has been resolved.

Troubleshooting: Incorrect Windows version in the *Client Info Center*

Support Assistant

The Support Assistant collects all relevant log files into a ZIP file when necessary. Previously, pre-logon logs and log files from the *log_system* directory were mistakenly not included in the *NCPSupport.zip* file. This issue has been resolved.

Connection Disconnections After ReKeying

In certain cases, connection disconnections could occur after rekeying. This issue has been resolved.

VPN Bypass Configuration

Within the VPN bypass configuration, the use of wildcards in the file path was ineffective. This issue has been resolved.

Pre-Logon with Two-Factor Authentication

If pre-logon with two-factor authentication via TOTP was configured, locking the screen and subsequently interrupting the VPN tunnel could cause an error when reconnecting the VPN tunnel. This issue has been resolved.

Resolving DNS Domains in the Tunnel

With this version of the NCP Secure Client, entering a domain within the *“DNS / WINS / Management” / DNS Domains to be resolved in the tunnel* feature is case-insensitive.

IKEv2 Signature Authentication

To enhance security for IKEv2 signature authentication, the outdated *PKCS#1 V1.5 Padding* and *SHA-1 Hash* algorithms can be disabled in the expert configuration.

Client GUI Crash

In very rare cases, the NCP Secure Client GUI could crash while saving a profile after prolonged use. This issue has been resolved.

Set Registry Entry: *fMinimizeConnections*

If the registry entry *fMinimizeConnections* on a Windows system under

`HKLM\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\Local`

to a value other than *"0"*, this value was reset to *"0"* when the *ncprwsnt* service was started. This issue has been resolved.

Log message: `MD5 invalid challenge response length received`

In rare cases, the following error occurred during communication with the FND server:

```
MD5 invalid challenge response length received
```

This issue has been resolved.

Troubleshooting: The PIN was incorrectly requested when using a hardware certificate

Improved compatibility with Telekom SIM cards using the *internet.v6.telekom* APN

Virtual SmartCards

Starting with this version, the NCP Secure Client is compatible with virtual SmartCards.

Media Switch from Mobile Network to Wi-Fi

Despite a profile configured exclusively for mobile networks, the NCP Secure Client attempted to continue the VPN tunnel over Wi-Fi when both a mobile network and a Wi-Fi connection were available simultaneously. However, this attempt was unsuccessful. This issue of the NCP Secure Client incorrectly switching media has been resolved.

Wi-Fi Issues with Windows Update KB5077181 Installed

When Windows Update KB5077181 was installed and Wi-Fi was configured as the medium in the profile, connection issues could occur with certain Intel Wi-Fi hardware. Additionally, problems with the Wi-Fi scan could occur when Windows Update KB5077181 was installed. These issues have been resolved.

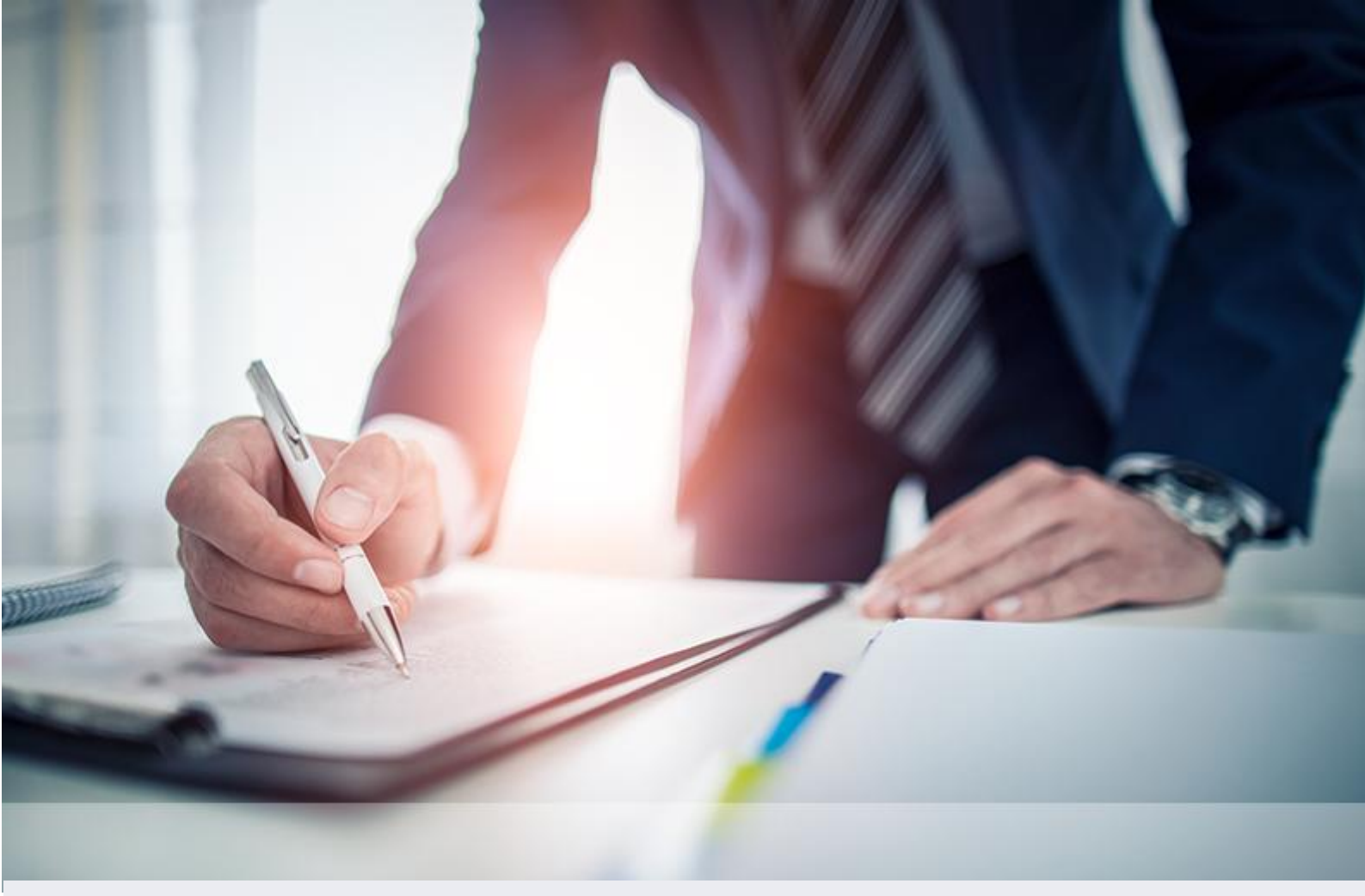
3. Known Issues

None.

4. Getting Help for the NCP Secure Enterprise VPN Server

For more information on the latest developments regarding the NCP Secure Entry Client, please visit the website:

https://www.ncp-e.com/en/products/ipsec-vpn-client-suite



NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Deutschland

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com