Release Notes

NCP Secure Entry Client

für Windows

Major-Release: 14.10 r32527
Datum: Juli 2026

Voraussetzungen

Microsoft Windows Betriebssysteme

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 11, 64 Bit (ab Version 23H2 bis einschließlich Version 25H2)
- Windows 10, 64 Bit (Version 22H2, sowie Windows 10 Enterprise LTSC 2021 Version 21H2)

HotSpot-Anmeldung

Für die korrekte Funktion der HotSpot-Anmeldung muss die Microsoft WebView2-Runtime installiert sein.

Ankündigung für künftige Clientversionen

Die Funktion

- *(dis)connect.bat nicht zulassen* (innerhalb der Verbindungsoptionen)

ist abgekündigt und wird in einer künftigen Clientversion entfernt.

Die aktive Medienauswahl für LAN, WLAN und Mobilfunk wird in einer künftigen Clientversion entfernt. Dies erfolgt aufgrund entsprechender Funktionalität in aktuellen Windows-Betriebssystemen. Clientfunktionen wie Seamless Roaming oder die Konfiguration von WLAN-SSIDs ist davon nicht betroffen und bleibt erhalten.

Die folgenden Funktionen sind ab der Clientversion 14.10 nicht mehr verfügbar:

Die folgenden Funktionen

- IEEE 802.1x-Authentisierung (EAP) unter dem Menüpunkt „Weitere Optionen/EAP“
- Quality of Service (QoS)
- GUI-Skalierung

sind ab dem Major-Release 14.10 nicht mehr im Funktionsumfang des NCP Secure Clients enthalten.

Die Funktion *Softzertifikatsauswahl aktivieren*, innerhalb der Benutzer-Zertifikatskonfiguration, ist in Verbindung mit der neuen GUI nicht nutzbar.

Die Auswahl des Installationsverzeichnisses bzw. -pfades innerhalb der Installationsroutine wurde entfernt. Der Client wird nur noch in das Standard-Installationsverzeichnis unter *c:\Programme* installiert. Im Falle eines Updates wird der ursprüngliche Pfad beibehalten.

1. Neue Leistungsmerkmale und Erweiterungen

Neue Client GUI

Die GUI des NCP Secure Clients wurde überarbeitet und präsentiert sich nach einer Neuinstallation im neuen Gewand mit Dark Mode-Unterstützung. Im Updatefall kann durch Auswahl des *Legacy Mode* in der Clientkonfiguration die GUI im bisherigen Design weiter genutzt werden.

FQDN-basiertes Split Tunneling

In der FQDN-basierten Split Tunneling-Konfiguration wird jeweils für IPv4 oder IPv6 das entfernte Ziel als Domainname eingetragen. Dieser Eintrag bewirkt, dass nur noch Daten an diese oder weitere konfigurierte Domainnamen oder Adressbereiche (gemäß Split Tunneling-Konfiguration) durch den VPN-Tunnel transportiert werden.

Beispiel: FQDN-Name: *EXCHANGE.DOMAIN.COM*

Durch den VPN-Tunnel werden ausschließlich Daten an *EXCHANGE.DOMAIN.COM* gesendet. Die zugehörige IP-Adresse ergänzt hierbei intern die Split Tunnel-Tabelle in der Client-Konfiguration. Der DNS-Server zur Auflösung des FQDN-Namens muss ebenso innerhalb eines konfigurierten Split-Tunnel Netzes erreichbar sein. Dieses sollte als erster Eintrag in der Tabelle stehen.

Neues FND-Protokoll

Mit dieser Clientversion wird ein neues, TLS-basiertes Protokoll zur Kommunikation mit dem FND-Server eingeführt. Voraussetzung zur Nutzung ist ein dafür konfigurierter FND-Server ab der Version 4.0.

Seamless Roaming und IKEv2

Für den Fall, dass ein Gateway bei Verwendung von IKEv2 kein MOBIKE unterstützt, führt der NCP Secure Client ein ReKeying aus. Dadurch wird eine Seamless Roaming-Funktionalität wie bei IKEv1 auch mit IKEv2, jedoch ohne MOBIKE-Unterstützung bereitgestellt.

Padding-Verfahren gemäß RFC 7427

Die Konfiguration innerhalb der Experten-Konfiguration unter *Erweiterte IPsec-Optionen* wurde um zwei Optionen erweitert:

- *Erlaube RSA Authentisierung mit PKCS#1 V1.5 Padding*
- *Erlaube RSA Authentisierung mit SHA-1 Hash*

2. Verbesserungen / Fehlerbehebungen

Update auf OpenSSL 3.5.6 – 3rd-Party-Pakete

Mit dem Update auf OpenSSL 3.5.6 wurden die folgenden Sicherheitslücken geschlossen: 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

Des Weiteren wurden die verwendeten Open Source 3rd-Party-Pakete aktualisiert.

Verbindungsprobleme mit 5G-Modems

Bei einigen Endgeräten mit 5G-Modem konnte es zu Verbindungsproblemen mit Mobilfunk kommen, sobald der NCP Secure Client auf dem Gerät installiert wurde. Ursache des Problems war ein Fehler im Hardware-Treiber des Modems.

Mit dieser Clientversion wurde der NCP Secure Client entsprechend modifiziert, um auch mit diesen Treibern einen reibungslosen Betrieb zu ermöglichen.

Optimierung des Datendurchsatzes

Bei eingeschalteter Client-Firewall waren Einbußen beim Datendurchsatz bemerkbar. Dieses Problem wurde behoben.

Neue Version des Netzwerktreibers: 14.1.2603

Deinstallation des NCP-Treibers

War die Vorgängerversion des NCP Secure Clients 13.19 bereits auf dem Gerät installiert, so konnte bei einer Deinstallation einer nachfolgend durch Update aufgespielten 13-er Version, der NCP-Treiber nicht vollständig entfernt werden. Dieses Problem wurde behoben.

Standardwert der DH-Gruppe

Beim Neuanlegen eines VPN-Profils wurde die DH-Gruppe für den IKEv2-Schlüsselaustausch und die PFS-Gruppe von 14 auf 19 angehoben.

Split-DNS – externe DNS-Requests

Im Falle eines konfigurierten Split-DNS-Funktionalität werden keine DNS-Request für die konfigurierte, interne Domäne, nach extern bzw. am VPN-Tunnel vorbei, kommuniziert.

Lokale Netze im Tunnel weiterleiten

Wurde der die Funktion *Auch lokale Netze im Tunnel weiterleiten* im Client deaktiviert, so wurde dies erst nach einem Neustart des Betriebssystems wirksam. Dieses Problem wurde behoben.

Überarbeitung der Barrierefreiheit

Mit der Einführung der neuen GUI wurde die Barrierefreiheit überarbeitet und mit den Screen Readern JAWS und Microsoft Narrator überprüft.

Windows Pre-Logon

Bei konfigurierter Profileinstellung „*immer*“ in den Verbindungsoptionen und aktiviertem Credential Provider, kann der Anwender durch ausschließliches Klicken auf den Credential Provider innerhalb des Anmeldebildschirmes, eine automatische Windows-Anmeldung ohne weiteres Zutun durchführen.

Problembehebung: Deinstallationsroutine entfernt nicht alle Dateien / Ordner

PIN-Menüpunkte

Fälschlicherweise wurden die Menüpinkte *PIN eingeben / PIN zurücksetzen* bei der Verwendung eines Hardware-Zertifikates angezeigt. Dieses Problem wurde behoben.

Problembehebung: Falsche Windows-Version im *Client-Info-Center*

Support-Assistent

Der Support-Assistent sammelt im Bedarfsfall alle relevanten Log-Dateien in einer ZIP-Datei ein. Fälschlicherweise wurden Pre-Logon-Logs sowie Log-Dateien aus dem Verzeichnis *log_system* nicht mit in die *NCPSupport.zip* aufgenommen. Dieses Problem wurde behoben.

Verbindungsabbrüche nach ReKeying

In speziellen Fällen konnte es nach dem ReKeying zu Verbindungsabbrüchen kommen. Dieses Problem wurde behoben.

VPN Bypass-Konfiguration

Innerhalb der VPN Bypass-Konfiguration war die Verwendung von Wildcards im Dateipfad unwirksam. Dieses Problem wurde behoben.

Pre-Logon mit 2-Faktor Authentisierung

Im Falle eines konfigurierten Pre-Logons mit 2-Faktor Authentisierung via TOTP konnte es beim Sperren des Bildschirmes und folgender Unterbrechung des VPN-Tunnels, zu einer Fehlersituation beim Wiederverbinden des VPN-Tunnels kommen. Dieses Problem wurde behoben.

DNS Domains im Tunnel auflösen

Mit dieser Version des NCP Secure Clients ist die Eingabe einer Domain innerhalb der Funktion „DNS / Management“ / *DNS Domains im Tunnel auflösen* case insensitive.

IKEv2-Signature Authentication

Um die Sicherheit bei der IKEv2-Signature Authentication zu erhöhen, lassen sich innerhalb der Experten-Konfiguration die veralteten Algorithmen *PKCS#1 V1.5 Padding* und *SHA-1 Hash* sperren.

Absturz der Client GUI

In sehr seltenen Fällen konnte die GUI des NCP Secure Clients nach längerer Benutzung beim Abspeichern eines Profils abstürzen. Dieses Problem wurde behoben.

Gesetzter Registry-Eintrag: *fMinimizeConnections*

Wurde der Registry-Eintrag: *fMinimizeConnections* auf einem Windows-System unter

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

durch einen Administrator auf einen anderen Wert als „*0*“ gesetzt, so wurde dieser Wert durch den Start des *ncprwsnt*-Dienstes wieder auf „*0*“ zurückgesetzt. Dieses Problem wurde behoben.

Log-Meldung: `MD5 invalid challenge response length received`

In seltenen Fällen kam es innerhalb der Kommunikation mit dem FND-Server zu folgendem Fehler:
`MD5 invalid challenge response length received`

Dieses Problem wurde behoben.

Problembehebung: Fälschlicherweise wurde die PIN bei Verwendung eines Hardware-Zertifikates abgefragt

Verbesserung der Kompatibilität zu Telekom SIM-Karten mit *internet.v6.telekom* APN

Virtuelle SmartCards

Der NCP Secure Client ist ab dieser Version zu virtuellen SmartCards kompatibel.

Medienwechsel von Mobilfunk auf WLAN

Trotz eines ausschließlich für Mobilfunk konfigurierten Profils, versuchte der NCP Secure Client, bei gleichzeitigem Vorhandensein einer Mobilfunk- und WLAN-Verbindung, den VPN-Tunnel über WLAN fortzuführen. Dieser Versuch blieb jedoch erfolglos. Dieses Problem der fälschlicherweise durchgeführten Medienumschaltung im NCP Secure Client wurde behoben.

WLAN-Probleme mit eingespieltem Windows Update KB5077181

Bei eingespieltem Windows Update KB5077181 und im Profil konfiguriertem Medium WLAN, konnte es mit bestimmter Intel Wi-Fi-Hardware zu Verbindungsproblemen kommen. Ebenso konnte es bei eingespieltem Windows Update KB5077181 zu Problemen beim WLAN-Scan kommen. Diese Probleme wurden behoben.

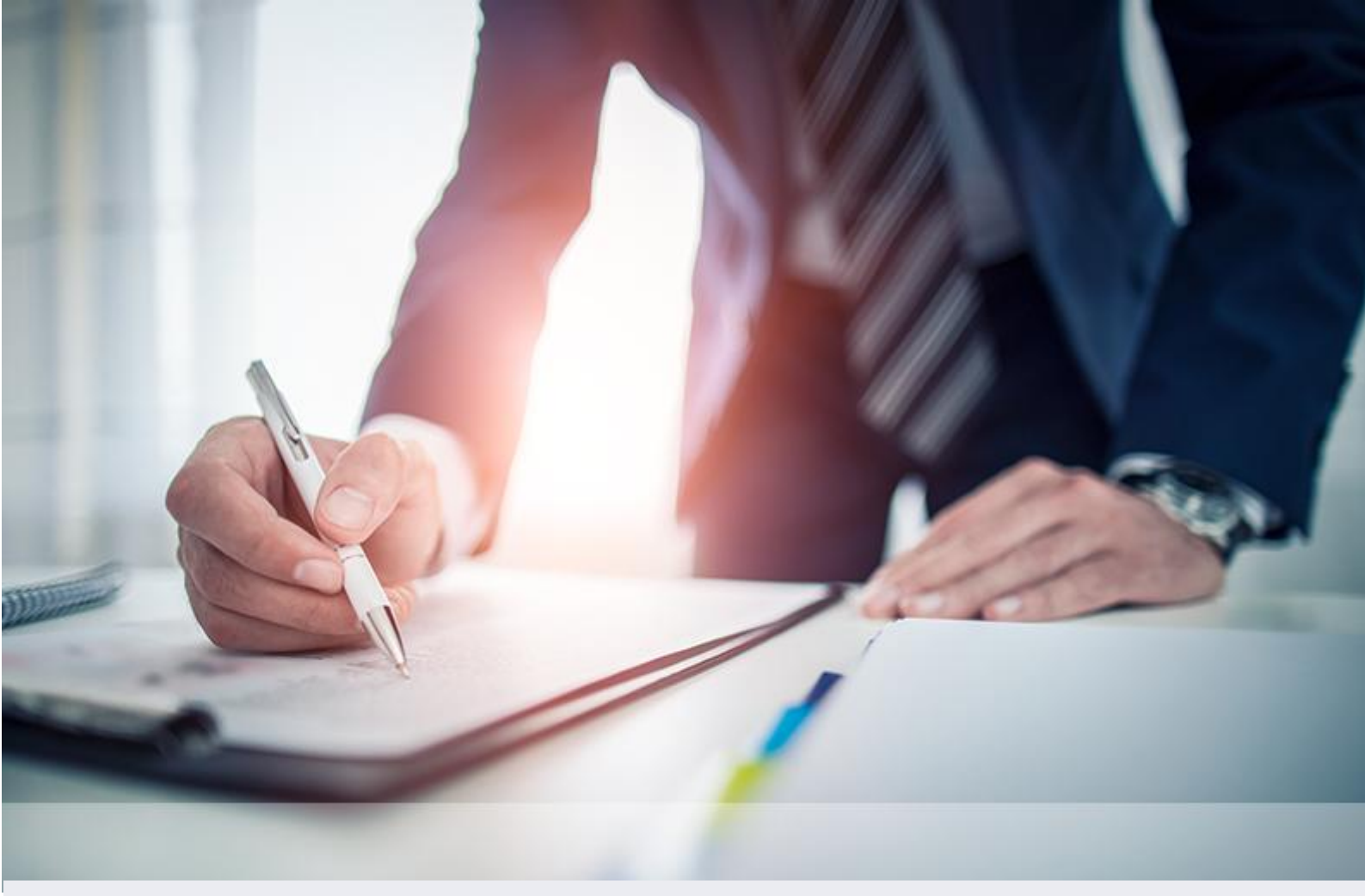
3. Bekannte Einschränkungen

Keine.

4. Hinweise zum NCP Secure Enterprise Client

Weitere Informationen zum letzten Stand der Entwicklung des NCP Secure Entry Clients erhalten Sie auf der Website:

https://www.ncp-e.com/de/produkte/ipsec-vpn-client-suite



NCP engineering GmbH
Dombühler Str. 2
90449 Nürnberg
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