NCP Secure Entry Client
Release Notes

Minor-Release: **13.19 r29720**
Datum: **September 2024**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 11, 64 Bit (ab Version 21H2 bis einschließlich Version 24H2)
- Windows 10, 64 Bit (ab Version 20H2 bis einschließlich Version 22H2, sowie Windows 10 Enterprise LTSC 2019 Version 1809)

HotSpot-Anmeldung
Für die korrekte Funktion der HotSpot-Anmeldung muss mind. die Version 101.0.1210.39 der Microsoft WebView2-Runtime installiert sein.

Neue Verzeichnisstruktur

Aus Gründen der Betriebssicherheit und der Kompatibilität zu Windows wurde die Verzeichnisstruktur des NCP Secure Clients ab der Version 12.0 geändert. Folgende Verzeichnisse die bei älteren Clientversionen im Installationsverzeichnis innerhalb `Programme\NCP\SecureClient\` waren sind in `ProgramData\NCP\SecureClient\` gewandert:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
Dabei handelt es sich um Konfigurationsdateien, Zertifikate oder Log-Dateien. Binaries oder Ressourcen verbleiben in `Programme\...`.
Während eines Updatevorganges wird die neue Verzeichnisstruktur automatisch angelegt und die Clientkonfiguration entsprechend übertragen. So werden Konfigurationspfade innerhalb der Zertifikatskonfiguration, welche die Variable `%InstallDir%` enthalten, in Pfade mit `%CertDir%` umgeschrieben. Dabei bezeichnet `%CertDir%` den Pfad `C:\ProgramData\NCP\SecureClient\certs`.
Anmerkung: Der Konfigurationseintrag `%CertDir%\client1.p12` ist gleichwertig zu `client1.p12`.

Ankündigung für das kommende Major-Release 14

Die Funktionen

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

werden ab dem künftigen Major-Release 14 nicht mehr im Funktionsumfang des NCP Secure Clients enthalten sein.

1. Neue Leistungsmerkmale und Erweiterungen

Tunnelvision / DHCP Filter

Die von der "Leviathan Security Group" entdeckte Schwachstelle namens „Tunnelvision“ (CVE-2024-3661) zielt auf via VPN angebundene Remotearbeitsplätze bzw. -netze ab. Der Angriff erfolgt hierbei nicht direkt auf einen vorhandenen VPN-Client, sondern auf das Routing im jeweiligen Betriebssystem. Der Angreifer imitiert im Netzwerk des Remote-Anwenders einen DHCP-Server, der mit Hilfe der DHCP-Option 121 die Routingtabelle auf dem Anwenderrechner manipuliert. Ziel dieser Manipulation ist, dass Daten nicht über die Standardroute durch den VPN-Tunnel versendet werden, sondern am VPN-Tunnel vorbei geleitet werden.
Mit dieser Version des NCP Secure Clients werden die DHCP-Optionen 121 und 249 standardmäßig im Netzwerkadapter ausgefiltert, so dass die Routingtabelle nicht geändert wird.
Dieses Verhalten kann durch Setzen eines Registry-Parameters deaktiviert werden:

```
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt
Valuename: AllowDHCPOption121and249
Valuetype: DWORD (32bit)
Value: 0 - off, 1 - on.    // Default 0
```

Des Weiteren wurde im Treiber bzw. Netzwerkadapter des NCP Secure Clients ein Fehler behoben, der während des ersten Bootvorganges nach der Installation in seltenen Fällen, einen Bluescreen verursachen konnte. Infolge dieser Anpassung wurde der Name und die Version des Netzwerkadapters von vormals

- „**NCP Secure Client Virtual NDIS6.20 Adapter**“ Version 12.1.2102.0

  zu
- „**NCP Secure Client Virtual NDIS Adapter**“ Version 13.1.2409.0

geändert.

Neues NCP-Logo

Das NCP-Logo wurde in der GUI durch die aktuelle Version ersetzt.

2. Verbesserungen / Fehlerbehebungen

Registrierung der Client-Firewall in Windows-Sicherheit

Sofern die Firewall des NCP Secure Clients aktiviert ist, konnte dies in Windows-Sicherheit nicht eingesehen werden. Dieses Problem wurde behoben.

Absturz des VPN-Dienstes „Problem mit Treiber-Schnittstelle (Mif32Init)“

Unter bestimmten Umständen stürzte der VPN-Dienst des NCP Secure Clients mit dem Hinweis auf ein Problem mit der Treiber-Schnittstelle ab. Dieses Problem wurde behoben.

PIN-Eingabe für SIM-Karte nicht möglich

Wurde der Rechner mit gesteckter SIM-Karte gestartet, so war die PIN-Eingabe unter bestimmten Umständen nicht möglich. Wurde die SIM-Karte erst nach dem Start des Rechners eingelegt, so konnte die PIN problemlos eingegeben und die SIM-Karte freigeschaltet werden. Dieses Problem wurde behoben.

Verbesserung der VPN-Verbindungsstabilität

Im Falle zweier oder mehr aktiver Verbindungsmedien konnte es unter bestimmten Umständen vorkommen, dass der VPN-Tunnel abgebrochen ist. Dieses Problem wurde behoben.

Problembehebung beim Profilwechsel von WLAN auf Mobilfunk

Ist die Option „Mobilfunk bei bestehender WLAN-Verbindung ausschalten“ gesetzt, so konnte beim ersten Verbindungsversuch nach einem Profilwechsel von WLAN auf Mobilfunk keine Verbindung aufgebaut werden. Dieses Problem wurde behoben.

Zertifikatshandling

Die Auswahl eines Benutzerzertifikates anhand der erweiterten Schlüsselverwendung schlug unter bestimmten Umständen fehl. Dieses Problem wurde behoben.

Erkennung eines angeschlossenen Chipkartenlesers

Wird im laufenden Betrieb ein Chipkartenleser angeschlossen, so wird er im NCP Client nicht korrekt erkannt. Ein Reboot des Computers oder ein Restart des „NCP Client VPN und Dialing Service“ ermöglichte die korrekte Erkennung des Chipkartenlesers. Dieses Problem wurde behoben.

Interne Optimierungen zur Performancesteigerung und Kompatibilität zu Drittherstellern

Log-Ausgabe bei Pre-Logon-Betrieb

Im Falle des Pre-Logon-Betriebes konnte es vorkommen, dass bei einer größeren Anzahl an Log-Ausgaben der Client-GUI, nicht alle Log-Meldungen in die Log-Datei geschrieben wurden. Dieses Problem wurde durch die Vergrößerung des internen Pufferspeichers behoben.

3. Bekannte Einschränkungen

Verbindungsprobleme via WLAN unter Windows 11 24H2

Mit der Einführung von Windows 11 24H2 ändert Microsoft die Vorgaben für Applikationen und damit auch für den NCP Secure Client um WLAN-Scans durchzuführen bzw. WLAN-Verbindungen aufzubauen. Hierfür ist nun Bedingung, dass die „Ortungsdienste“ auf dem Anwender-Rechner aktiviert sind (Einstellungen – Datenschutz und Sicherheit – Standort). Ist dies aus administrativen Gründen nicht möglich, so muss das WLAN-Handling mit Windows-Bordmitteln umgesetzt werden.

Verbindungsprobleme mit 5G-Modems

Bei einigen Endgeräten mit 5G-Modem kann es zu Verbindungsproblemen mit Mobilfunk kommen, sobald der NCP Secure Client auf dem Gerät installiert ist. Dabei wurden mit folgender Hardware Probleme festgestellt:

- Quectel RM520N – GL 5G M.2
- Snapdragon X62-5G (DW5932e)

Option: „Dialog für Verbindungsaufbau automatisch Öffnen“

Unter bestimmten Umständen funktioniert die Logon-Option „Dialog für Verbindungsaufbau automatisch Öffnen“ nicht.

Applikationsbasierte VPN Bypass Konfiguration

Die Konfiguration eines DNS innerhalb der VPN Bypass Konfiguration macht eine darin enthaltene applikationsbasierte Regel unwirksam.

PIN-Menüeinträge

Bei der Verwendung von Hardware-Zertifikaten sind die PIN-Menüeinträge „PIN eingeben/zurücksetzen/ändern“ / „Enter/Reset/Change PIN“ ohne Funktion, jedoch fälschlicherweise auswählbar.

Seamless Roaming

Unter bestimmten Umständen verbleibt der VPN-Tunnelstatus beim Wechseln von WLAN auf LAN auf „Tunnel logisch halten“ und eine funktionale Verbindung über LAN wird nicht aufgebaut. Dies muss durch manuelles Trennen und Verbinden geschehen.

Home Zone und IPv6

Ist in den Firewall-Einstellungen des VPN-Clients die vordefinierte Home Zone-Regel aktiv, so werden im definierten Home Zone-Netzwerk ausgehende IPv6-Pakete in das lokale Netzwerk verworfen.

Service-Release: **13.14 r29669**
Datum: **März 2023**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 11, 64 Bit (ab Version 21H2 bis einschließlich Version 22H2)
- Windows 10, 64 Bit (ab Version 20H2 bis einschließlich Version 22H2, sowie Windows 10 Enterprise LTSC 2019 Version 1809)

HotSpot-Anmeldung
Für die korrekte Funktion der HotSpot-Anmeldung muss mind. die Version 101.0.1210.39 der Microsoft WebView2-Runtime installiert sein.

Neue Verzeichnisstruktur

Aus Gründen der Betriebssicherheit und der Kompatibilität zu Windows wurde die Verzeichnisstruktur des NCP Secure Clients ab der Version 12.0 geändert. Folgende Verzeichnisse die bei älteren Clientversionen im Installationsverzeichnis innerhalb `Programme\NCP\SecureClient\` waren sind in `ProgramData\NCP\SecureClient\` gewandert:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
Dabei handelt es sich um Konfigurationsdateien, Zertifikate oder Log-Dateien. Binaries oder Ressourcen verbleiben in `Programme\...`.
Während eines Updatevorganges wird die neue Verzeichnisstruktur automatisch angelegt und die Clientkonfiguration entsprechend übertragen. So werden Konfigurationspfade innerhalb der Zertifikatskonfiguration, welche die Variable `%InstallDir%` enthalten, in Pfade mit `%CertDir%` umgeschrieben. Dabei bezeichnet `%CertDir%` den Pfad `C:\ProgramData\NCP\SecureClient\certs`.
Anmerkung: Der Konfigurationseintrag `%CertDir%\client1.p12` ist gleichwertig zu `client1.p12`.

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

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Problembehebung: IKEv2 Rekeying funktionierte mit Juniper SRX Gateways nicht

Anpassung der PKCS#11-Modul-Konfiguration

Die Konfiguration eines PKCS#11-Moduls wurde angepasst um die Sicherheit im NCP Secure Client zu erhöhen. Aus diesem Grunde können mit dieser Clientversion nur noch PKCS#11-Dateien von folgenden Orten geladen werden: `WINDIR, PROGRAMFILES und PROGRAMFILES(x86)`
Alternativ kann in der Registry mit vorhandenen Admin-Rechten der folgende Pfad für das PKCS#11-Modul konfiguriert werden:
`"HKLM\\Software\\NCP engineering GmbH\\NCP Secure Client\\P11DllPath"`
In der Client-Konfiguration ist in jedem Fall immer die PKCS#11-DLL inklusiv dem kompletten Pfad anzugeben.

Problembehebung: VPN Bypass und Mobilfunk

Bei Verwendung eines Profils mit konfiguriertem Verbindungsmedium „Mobilfunk“ war eine über VPN Bypass konfigurierte Domain nicht erreichbar. Dieses Problem wurde behoben.

Problembehebung: Split-DNS mit Cisco ASA Gateway

Wurde gatewayseitig auf einer CISCO ASA Hardware Split-DNS konfiguriert, wird nur der erste DNS-Name für Split-DNS verwendet. Dieses Problem wurde behoben.

Problembehebung: Stateful Boot Option

Unter der Voraussetzung, dass alle nachfolgenden Bedingungen erfüllt sind,

- grundsätzlich nur Kommunikation durch den VPN-Tunnel oder innerhalb eines Friendly Nets gestattet ist
- Windows die Verbindungsmedien selbst verwaltet (der Medienwechsel wird nicht über den NCP Secure Client angestoßen)
- unmittelbar nach einem Windows-Systemstart Mobilfunk als Verbindungsmedium vom Windows-System gewählt wurde
- die Stateful Boot Option in den Firewalleinstellungen des Clients konfiguriert ist

konnte vom Rechner des Anwenders eine Verbindung ins Internet – ohne VPN-Tunnel – aufgebaut werden. Dieses Problem wurde behoben.

Problembehebung: Automatische Medienerkennung

In seltenen Fällen wechselte die im NCP Secure Client konfigurierte „automatische Medienerkennung“ fälschlicherweise auf WLAN obwohl das Gerät weiterhin mit LAN verbunden war. Dieses Problem wurde behoben.

Anpassung der IKEv2 Configuration Payload

Die Länge des IKEv2 Configuration Payload Attribute Types `INTERNAL_IP6_ADDRESS` wurde von 16 Bytes auf 17 Bytes geändert. Es wird demnach nun zusätzlich zur IPv6-Adresse auch das Prefix übertragen.

Unterstützung von RFC7383 (IKEv2 Message Fragmentation)

Mit der Unterstützung von RFC7383 wurde die Kompatibilität zu Gateways von Dritt-Herstellern verbessert.

Problembehebung: PIN-Symbol grün trotz nicht erfolgter PIN-Eingabe

Wurde der Anwender-Rechner mit einer gesteckten SmartCard gestartet, so wurde im NCP Secure Client die Statusanzeige für erfolgte PIN-Eingabe fälschlicherweise grün – entspricht PIN-Eingabe bereits erfolgt – angezeigt. Dieses Problem wurde behoben.

Verbesserung der Kompatibilität zur Juniper SRX innerhalb der Rekeying-Phase

Wurde das Rekeying vom Client gegen eine Juniper SRX initialisiert, so kam es zu einer Fehlersituation. Dieses Problem wurde behoben.

Update auf OpenSSL Version 1.0.2zg

Die im NCP Secure Client verwendete OpenSSL-Version wurde auf 1.0.2zg angehoben.

3. Bekannte Einschränkungen

Option: „Dialog für Verbindungsaufbau automatisch Öffnen“

Unter bestimmten Umständen funktioniert die Logon-Option „Dialog für Verbindungsaufbau automatisch Öffnen“ nicht.

Applikationsbasierte VPN Bypass Konfiguration

Die Konfiguration eines DNS innerhalb der VPN Bypass Konfiguration macht eine darin enthaltene applikationsbasierte Regel unwirksam.

PIN-Menüeinträge

Bei der Verwendung von Hardware-Zertifikaten sind die PIN-Menüeinträge „PIN eingeben/zurücksetzen/ändern“ / „Enter/Reset/Change PIN“ ohne Funktion, jedoch fälschlicherweise auswählbar.

Seamless Roaming

Unter bestimmten Umständen verbleibt der VPN-Tunnelstatus beim Wechseln von WLAN auf LAN auf „Tunnel logisch halten“ und eine funktionale Verbindung über LAN wird nicht aufgebaut. Dies muss durch manuelles Trennen und Verbinden geschehen.

Home Zone und IPv6

Ist in den Firewall-Einstellungen des VPN-Clients die vordefinierte Home Zone-Regel aktiv, so werden im definierten Home Zone-Netzwerk ausgehende IPv6-Pakete in das lokale Netzwerk verworfen.

Service-Release: **13.11 r29631**
Datum: **September 2022**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 11, 64 Bit (bis einschließlich Version 21H2)
- Windows 10, 64 Bit (bis einschließlich Version 21H2)

HotSpot-Anmeldung
Für die korrekte Funktion der HotSpot-Anmeldung muss mind. die Version 101.0.1210.39 der Microsoft WebView2-Runtime installiert sein.

Neue Verzeichnisstruktur

Aus Gründen der Betriebssicherheit und der Kompatibilität zu Windows wurde die Verzeichnisstruktur des NCP Secure Clients ab der Version 12.0 geändert. Folgende Verzeichnisse die bei älteren Clientversionen im Installationsverzeichnis innerhalb `Programme\NCP\SecureClient\` waren sind in `ProgramData\NCP\SecureClient\` gewandert:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
Dabei handelt es sich um Konfigurationsdateien, Zertifikate oder Log-Dateien. Binaries oder Ressourcen verbleiben in `Programme\...`.
Während eines Updatevorganges wird die neue Verzeichnisstruktur automatisch angelegt und die Clientkonfiguration entsprechend übertragen. So werden Konfigurationspfade innerhalb der Zertifikatskonfiguration, welche die Variable `%InstallDir%` enthalten, in Pfade mit `%CertDir%` umgeschrieben. Dabei bezeichnet `%CertDir%` den Pfad `C:\ProgramData\NCP\SecureClient\certs`.
Anmerkung: Der Konfigurationseintrag `%CertDir%\client1.p12` ist gleichwertig zu `client1.p12`.

1. Neue Leistungsmerkmale und Erweiterungen

Neue Option: „DNS Domains im Tunnel auflösen“

Die Split-DNS-Funktionalität lässt sich mit Hilfe der neuen Option „DNS Domains im Tunnel auflösen“ / „DNS domains to be resolved in the tunnel“ konfigurieren. Dabei werden im Falle von konfiguriertem Split Tunneling die DNS-Requests der konfigurierten Domains in den VPN-Tunnel gesendet. Alle anderen DNS-Requests gehen am VPN-Tunnel vorbei.

Unterstützung des RFC 7296

Der VPN-Client unterstützt nun RFC 7296 zur Verteilung von Split Tunneling-Konfigurationen seitens des VPN-Gateways.

2. Verbesserungen / Fehlerbehebungen

Neue Rechtestruktur innerhalb `C:\ProgramData\NCP\`

Ein Benutzer hatte innerhalb des Verzeichnisses `C:\ProgramData\NCP\` Schreibrechte. Diese wurden auf ein Minimum begrenzt. Beispielsweise kann ein Benutzer nun keine CA-Zertifikate mehr im dafür vorgesehenen Verzeichnis ablegen. Ebenso wurde die Verzeichnis- und Rechtestruktur so umgebaut, dass keine Anwendung im User- und System-Kontext in das gleiche Verzeichnis schreibt. Das Problem wurde behoben.

Verbesserungen beim serverseitig konfigurierten Split-DNS

Automatische Windows-Anmeldung

Wurde innerhalb der Logon-Optionen die Option „Automatisch mit konfigurierten Anmeldedaten durchführen“ ausgewählt, so funktionierte die Windows-Anmeldung nicht. Ebenso gab es ein Problem in Verbindung mit 2-Faktor-Authentisierung via TOTP. Dieses Problem wurde behoben.

Problembehebung bei Seamleass Roaming und IPv6-Zieladressen

VPN-Benutzername aus Cache

Nach dem Update einer Vorversion wurde u.U. der zwischengespeicherte VPN-Benutzername im Anmeldedialog nicht korrekt angezeigt. Dieses Problem wurde behoben.

Falsche Statusanzeige nach Profilwechsel

Nach einem Profilwechsel von einem zertifikatsbasierten Profil mit erfolgreicher PIN-Eingabe auf ein Profil mit Pre-Shared-Key wurde die eingegebene PIN nicht gelöscht und das PIN-Icon nicht aus der Client-GUI entfernt. Dieses Problem wurde behoben.

PKI-Error beim Profilwechsel

Beim Profilwechsel von einem zertifikatsbasierten Profil mit *.p12-Datei auf ein Profil mit SmartCard-Reader wurde ein PKI-Error angezeigt. Dieses Problem wurde behoben.

Update auf zlib Version 1.2.12

Die im VPN-Client verwendete zlib-Version wurde auf 1.2.12 angehoben. Damit wurde die zlib-Sicherheitslücke [CVE-2018-25032] geschlossen.

OpenSSL Sicherheitspatch

Die Sicherheitslücken [CVE-2022-0778] und [CVE-2020-1971] wurden in OpenSSL behoben.

Umstellung auf TLS 1.2

Die TLS-Versionen 1.0 und 1.1 werden mit dieser Clientversion nicht mehr unterstützt.

Update auf cURL-Library 7.84.0

Die im VPN-Client verwendete cURL-Version wurde auf 7.84.0 angehoben. Damit wurden die cURL-Sicherheitslücken [CVE-2022-27776], [CVE-2022-27775], [CVE-2022-27774], [CVE-2022-22576], [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207] und [CVE-2022-32208] geschlossen.

Die Kompatibilität zu Fremdgateways in Verbindung mit 2-Faktor-Authentisierung / Tokeneingabe wurde verbessert

Falsche Statusanzeige: Chipkarte

Unter bestimmten Umständen wurde bei einem Profil mit 2-Faktor-Authentisierung fälschlicherweise ein Chipkartensymbol angezeigt. Beim Wechsel auf ein Profil mit Chipkarte wurde eine Fehlermeldung angezeigt, dass die Chipkarte nicht richtig initialisiert sei. Dieses Problem wurde behoben.

Problembehebung nach Änderung der DNS-Einträge in der VPN Bypass-Konfiguration

Problembehebung beim Aufruf der HotSpot-Anmeldung

Die HotSpot-Anmeldung wurde nicht korrekt aufgerufen, wenn die Autostart-Option „Icon im System Tray“ ausgewählt war. Dieses Problem wurde behoben.

Problembehebung einer fälschlicherweise angezeigten PIN-Abfrage

Bei der Verwendung des CSP Benutzerzertifikatsspeichers wurde u.U fälschlicherweise eine PIN abgefragt. Dieses Problem wurde behoben. Ebenso wurde die Option zur PIN-Abfrage im Falle des CSP Benutzerzertifikatsspeichers im Client Plug-in entfernt.

Verbesserung der Kompatibilität zu Fremdgateways bei der Adressierung via IPv6

PAP/CHAP-Fehler beim Verbindungsaufbau

Unter bestimmten Umständen zeigt der VPN-Client beim IKEv2-Verbindungsaufbau einen PAP/CHAP-Fehler an. Dieser lässt sich durch den Anwender durch Öffnen des VPN-Profils und Bestätigen mit „Ok“ beheben. Dieses Problem wurde behoben.

Überarbeitung der Funktion „Verbindungsaufbau vor Windows-Anmeldung“

Um einer möglichen Priviledge Escalation vorzubeugen, wurde die Funktion „Verbindungsaufbau vor Windows-Anmeldung“ überarbeitet. Hierbei konnte ein Standard-Benutzer, sofern diese Funktion nicht über die Konfigurationssperren deaktiviert war, sich Administratorrechte, z.B. über eine konfigurierte CMD-Shell, erschleichen. Mit dieser Änderung können nur vom Administrator im Verzeichnis `C:\ProgramData\NCP\SecureClient\scripts\` angelegte Batch-Dateien ausgewählt werden.

Verbesserung der Kompatibilität zu Juniper SRX-Gateways im Falle der ReKeying-Phase

Unterstützung von RFC 8598

In RFC 8598 ist die Weitergabe der Split-DNS-Konfiguration durch das VPN Gateway an den VPN Client definiert. Dieses RFC wird ab dieser Clientversion unterstützt.

Netzwerkverbindung nach Installation dauerhaft getrennt

Nach der Installation des Clients war die Netzwerkverbindung dauerhaft getrennt. Erst nach dem Reboot des Rechners war wieder eine Netzwerkkommunikation möglich. Dieses Problem wurde behoben.

Problem beim Importieren eines zuvor exportierten Profils

Der Import eines exportierten Profils in einen 13-er Client schlug fehl. Dieses Problem wurde behoben.

Allgemeine Verbesserungen beim INI- oder PCF-Datei-Import

Verbesserung der Kompatibilität zu Fremdgateways hinsichtlich IP-Adresszuweisung

Wurde dem VPN Client während des Verbindungsaufbaus eine IP-Adresse, endend mit `.255`, zugewiesen, so war kein Routing durch den VPN-Tunnel möglich. Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Option: „Dialog für Verbindungsaufbau automatisch Öffnen“

Unter bestimmten Umständen funktioniert die Logon-Option „Dialog für Verbindungsaufbau automatisch Öffnen“ nicht.

Applikationsbasierte VPN Bypass Konfiguration

Die Konfiguration eines DNS innerhalb der VPN Bypass Konfiguration macht eine darin enthaltene applikationsbasierte Regel unwirksam.

PIN-Menüeinträge

Bei der Verwendung von Hardware-Zertifikaten sind die PIN-Menüeinträge „PIN eingeben/zurücksetzen/ändern“ / „Enter/Reset/Change PIN“ ohne Funktion, jedoch fälschlicherweise auswählbar.

Seamless Roaming

Unter bestimmten Umständen verbleibt der VPN-Tunnelstatus beim Wechseln von WLAN auf LAN auf „Tunnel logisch halten“ und eine funktionale Verbindung über LAN wird nicht aufgebaut. Dies muss durch manuelles Trennen und Verbinden geschehen.

Home Zone und IPv6

Ist in den Firewall-Einstellungen des VPN-Clients die vordefinierte Home Zone-Regel aktiv, so werden im definierten Home Zone-Netzwerk ausgehende IPv6-Pakete in das lokale Netzwerk verworfen.

Major-Release: **13.04 r29378**
Datum: **April 2022**

Voraussetzungen

Microsoft Windows Betriebssysteme:
Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 11, 64 Bit (bis einschließlich Version 21H2)
- Windows 10, 64 Bit (bis einschließlich Version 21H2)

Die folgenden Funktionen sind ab dieser Clientversion nicht mehr verfügbar:

- Verbindungsmedium: Modem, xDSL, ext. Dialer

Neue Verzeichnisstruktur

Aus Gründen der Betriebssicherheit und der Kompatibilität zu Windows wurde die Verzeichnisstruktur des NCP Secure Clients ab der Version 12.0 geändert. Folgende Verzeichnisse die bei älteren Clientversionen im Installationsverzeichnis innerhalb `Programme\NCP\SecureClient\` waren sind in `ProgramData\NCP\SecureClient\` gewandert:
`arls, cacerts, certs, config, crls, CustomBrandingOption, data, hotspot, log, statistics`
Dabei handelt es sich um Konfigurationsdateien, Zertifikate oder Log-Dateien. Binaries oder Ressourcen verbleiben in `Programme\...`.
Während eines Updatevorganges wird die neue Verzeichnisstruktur automatisch angelegt und die Clientkonfiguration entsprechend übertragen. So werden Konfigurationspfade innerhalb der Zertifikatskonfiguration, welche die Variable `%InstallDir%` enthalten, in Pfade mit `%CertDir%` umgeschrieben. Dabei bezeichnet `%CertDir%` den Pfad `C:\ProgramData\NCP\SecureClient\certs`.
Anmerkung: Der Konfigurationseintrag `%CertDir%\client1.p12` ist gleichwertig zu `client1.p12`.

1. Neue Leistungsmerkmale und Erweiterungen

Überarbeitete Hotspot-Anmeldung

Ab dieser Version 13.0 des NCP Secure Clients wird der Chrome-basierte Microsoft Edge-Webbrowser mittels WebView2-Runtime aufgerufen und ausschließlich für den Zweck der Anmeldung an einem Hotspot verwendet. Voraussetzung hierfür ist die installierte WebView2-Runtime (ab der Version 94.0.992.31 oder neuer) innerhalb des Betriebssystems.

Die WebView2-Runtime kann hier heruntergeladen werden:
https://developer.microsoft.com/en-us/microsoft-edge/webview2/#download-section

INI-Datei-Import für max. 250 Split Tunneling Remote Netzwerke

Sowohl für IPv4 als auch für IPv6 können jeweils bis zu 250 Split Tunneling Konfigurationen via INI-Datei in den Client importiert werden.

Neuer Split-DNS-Parameter

Die gezielte Umleitung von DNS-Requests in den VPN-Tunnel kann durch Setzen des Parameters `DomainInTunnel` in der INI-Datei mit einer max. Stringlänge von 1023 konfiguriert werden. Der String enthält, via Komma separiert, die aufzulösenden Domainnamen:

`google.com` – alle Domains die `google.com` enthalten werden verwendet, z.B. `www.test-google.com`

`.google.com` – alle Domains die `.google.com` enthalten werden verwendet, z.B. `news.google.com`

`news.google.com` – alle Domains die `news.google.com` enthalten werden verwendet

Unterstützung der WPA3-Verschlüsselung

Der im NCP Secure Client integrierte WLAN-Manager kann nun auch mit WPA3 verschlüsselte WLANs verwalten.

Unterstützung von RFC 7296

In RFC 7296 ist die Weitergabe von Split Tunneling-Remote Netzwerken durch das VPN Gateway an den VPN Client definiert. Dieses RFC wird ab dieser Clientversion unterstützt.

Erweiterung des VPN-Status in der Windows-Registry

Bisher ließ sich der Verbindungsstatus des NCP Clients in der Registry unter "`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP RWS/GA\6.0`" für den Parameter `SecClCsi` mit den Werten

0 = nicht verbunden

und

1 = verbunden

auslesen. Ab dieser Version speichert der Client weitere Zustände unter folgendem Ort in der Windows-Registry ab:
`HKEY_LOCAL_MACHINE\SOFTWARE\NCP engineering GmbH\NCP Secure Client`
bzw.
`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NCP engineering GmbH\NCP Secure Client`
Der zugehörige Parameter `ConnectState` kann dabei die folgenden Werte annehmen:

0 = Verbindung ist getrennt

1 = Verbindung wird aufgebaut

2 = Verbindung ist erfolgreich aufgebaut
3 = Internetverbindung ist unterbrochen, VPN-Verbindung wird gehalten

4. Verbesserungen / Fehlerbehebungen

Überarbeitetes Datei-Handling der ncp.db

In seltenen Fällen wurde die Datei `ncp.db` während des Betriebes unbrauchbar, wodurch der Client seine Lizenz verloren hatte. Dieses Problem wurde behoben.

„Network Location Awareness“ bei aktiver NCP-Firewall nicht verfügbar

Bei aktivierter Client-Firewall ist die “Network Location Awareness” des Windows Betriebssystems nicht verfügbar. Für den Fall der ausschließlich gewünschten Friendly Network Detection-Funktionalität kann durch Konfigurieren einer Client-Firewall-Regel „jeden Netzwerkverkehr bidirektional zulassen“ und Setzen eines Registry-Keys die “Network Location Awareness” des Windows Betriebssystems genutzt werden. Hierzu ist in der Registry innerhalb `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ncprwsnt` der Parameter `RegDw "WscIntegration"=0` zu konfigurieren. Der Standardwert dieses Parameters ist `1`.

Option „WLAN bei gestecktem LAN-Kabel ausschalten“: Problem mit Hyper-V

Bei genutzter Hyper-V-Funktionalität wurde der WLAN-Adapter bei gesetzter „WLAN bei gestecktem LAN-Kabel ausschalten“-Option fälschlicherweise deaktiviert. Dieses Problem wurde behoben.

Automatische Anmeldung via Credential Provider

Bei Verwendung der Logon-Option mit konfigurierten User-Credentials konnte ein gesperrter Windows-Arbeitsplatz durch Auswahl des NCP Credential Providers entsperrt werden. Dieses Problem wurde behoben.

Problembehebung bei mehreren Zertifikaten mit gleichem Issuer und Subject im Windows-Zertifikatsspeicher

Sind im Windows-Zertifikatsspeicher Zertifikate mit identischem Issuer und Subject enthalten, wurde unter Umständen das falsche, abgelaufene Zertifikat vom Client verwendet und mit der Meldung „unable to get issuer certificate“ quittiert. Dieses Problem wurde behoben.

Geänderter Standardwert in den FND-Optionen

Der Standardwert für die Option „Auf bekannte Netze periodisch prüfen“ wurde von 0 Sek. auf 3600 Sek. geändert.

Unvollständige Log-Dateien

Unter bestimmten Umständen kam es zu fehlerhaften Schreibzugriffen auf die Client-Log-Dateien, so dass im schlechtesten Fall Log-Einträge fehlten. Dieses Problem wurde behoben.

Überarbeitete Installationsroutine

In seltenen Fällen wurde nach Ende des Installationsvorganges, vor dem Rechner-Neustart, die Netzwerkverbindung komplett getrennt. Dieses Problem wurde behoben. Des Weiteren wurde innerhalb des MSI-Installationsvorganges die „Programm reparieren“-Funktionalität entfernt.

Fehler nach dem Standby-Zustand in Verbindung mit IPv6 behoben

Nach dem Standby-Zustand des PCs kam es mit IPv6 zu Verbindungsproblemen. Dieser Fehler wurde behoben.

Problem bei der Installation mit `certmgr.exe`

Bei der Installation des NCP Secure Clients wurde die von Microsoft erstellte Datei `certmgr.exe` zur Installation des NCP-Herstellerzertifikates verwendet. Diese Datei wurde als nicht signiert erkannt. Ab dieser Version wird anstatt `certmgr.exe` die neuere `certutil.exe` verwendet. Das Problem wurde dadurch behoben.

Dynamische Zertifikatsauswahl

Die Zertifikatsauswahl wurde entscheidend verbessert, zudem werden künftig nurmehr gültige Zertifikate importiert.

Fehlerbehebung im ESP-Header für IPv6

Überarbeitete Parametersperren in der Client-GUI

In der Client-GUI wurden Maßnahmen getroffen, dass gesperrte Schaltflächen sich nicht durch bestimmte Tools aktivieren lassen und dadurch gesperrte Funktionen zur Verfügung gestellt werden.

Behebung eines Problems beim Verbindungsaufbau mit VPN Path Finder via IPv6

Verbesserung der FND-Kompatibilität zu Netzwerk-Switches

Optimierung des Aufbaus einer IKEv2-Verbindung mit EAP

In bestimmten Situationen konnte der Aufbau des VPN-Tunnels mit IKEv2 und EAP ungewöhnlich lang dauern. Dieses Problem wurde behoben.

Verbesserung der VPN-Bypass-Kompatibilität zu MS Teams

5. Bekannte Einschränkungen

Option: „Dialog für Verbindungsaufbau automatisch Öffnen“

Unter bestimmten Umständen funktioniert die Logon-Option „Dialog für Verbindungsaufbau automatisch Öffnen“ nicht.

6. Hinweise zum NCP Secure Entry Client (Win32/64)

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/service/download-vpn-client/versionsinformationen.html

Weitere Unterstützung bei Fragen zum Enterprise, erhalten Sie über die Mail-Adressen auf folgender Seite:
https://www.ncp-e.com/de/unternehmen/kontakt.html

E-Mail: support@ncp-e.com

7. Leistungsmerkmale

Betriebssysteme	Microsoft Windows (64 Bit): Windows 11, Windows 10; x86-64 Prozessorarchitektur
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); differenzierte Filterregeln bezüglich: Protokolle, Ports, Anwendungen und Adressen, Schutz des LAN-Adapters; IPv4 und IPv6 Unterstützung Friendly Net Detection (Automatische Umschaltung der Firewall-Regeln bei Erkennung des angeschlossenen Netzwerkes anhand des IP-Adressbereiches oder eines NCP FND-Servers*); FND-abhängige Aktion starten; Secure Hotspot Logon; Homezone;
VPN Bypass	Die VPN-Bypass-Funktion gestattet Anwendungen festzulegen, die trotz deaktiviertem Split Tunneling außerhalb der VPN-Konfiguration direkt ins Internet kommunizieren dürfen. Alternativ ist es möglich, Domänen bzw. Zieladressen zu bestimmen, zu denen die Datenkommunikation am VPN-Tunnel vorbei stattfinden soll.
Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; IPsec-Proposals können determiniert werden durch das IPsec -Gateway (IKEv1/IKEv2, IPsec Phase 2); Event log; Kommunikation nur im Tunnel; MTU Size Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Tunnel Mode
Verschlüsselung (Encryption)	Symmetrische Verfahren: AES 128, 192, 256 Bits; Blowfish 128, 448 Bits; Triple-DES 112, 168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 8192 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1, 2, 5, 14-21, 25-30
FIPS Inside	Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747). Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: ▪ Diffie Hellman-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit) ▪ Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit ▪ Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES

Authentisierungsverfahren	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKEv2 IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse aus dem internen Adressbereich (private IP); PFS; PAP, CHAP, MS CHAP V.2; IEEE 802.1x: EAP-MD5 (Extensible Authentication Protocol): erweiterte Authentifikation gegenüber Switches und Access Points (Layer 2); EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): erweiterte Authentifikation gegenüber Switches und Access Points auf Basis von Zertifikaten (Layer 2); Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens und Zertifikate mit ECC-Technologie; Multi-Zertifikatskonfiguration; Pre-Shared Secrets; One-Time Passwords und Challenge Response Systeme (u.a. RSA SecurID Ready)
Starke Authentisierung	X.509 v.3 Standard; Biometrische Authentisierung ab Windows 8.1 PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2, 2.0 und 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 für Private Schlüssel in Soft Zertifikaten; CSP zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher CSP zur Verwendung von SmartCards via API des Herstellers PIN-Richtlinie; administrative Vorgabe für die Eingabe beliebig komplexer PINs; Revocation: EPRL (End-entity Public-Key Certificate Revocation List, vorm. CRL), CARL (Certification Authority Revocation List, vorm. ARL), OCSP
Networking Features	LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface, integrierter WLAN- (Wireless Local Area Netzwork) und WWAN-Support (Wireless Wide Area Network, Mobile Broadband)
Netzwerkprotokoll	IPv4 / IPv6 Dual Stack
Dialer	NCP Internet Connector oder Microsoft RAS Dialer (für ISP-Einwahl mittels Einwahl-Script)
Seamless Roaming	Automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium (LAN/WLAN/Mobilfunk) ohne IP-Adresswechsel, so dass über den VPN-Tunnel kommunizierende Anwendungen nicht beeinflusst werden, bzw. die Anwendungs-Session nicht getrennt wird Voraussetzung: NCP Secure Enterprise VPN Server
VPN Path Finder**	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist
IP Address Allocation	DHCP (Dynamic Host Control Protocol); DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server
Übertragungsmedien	Internet, LAN, WLAN, GSM, GPRS, LTE, 5G
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; WLAN-Roaming (Handover);

	Timeout (zeit- und gebührengesteuert); Budget Manager (Verwaltung von Verbindungszeit und/oder -volumen für Mobilfunk und WLAN, bei Mobilfunk getrennte Verwaltung für Roaming im Ausland) Verbindungsmodi: automatisch, manuell, wechselnd (Der Verbindungsaufbau ist davon abhängig wie die Trennung zuvor stattgefunden hat)
APN von SIM Karte	Der APN (Access Point Name) definiert den Zugangspunkt eines Providers für eine mobile Datenverbindung. Die APN-Daten werden bei einem Providerwechsel automatisiert aus der jeweiligen SIM-Karte in die Client-Konfiguration übernommen
Datenkompression	IPCOMP (lzs), Deflate (nur für IKEv1)
Quality of Service	Priorisierung konfigurierter Datenströme innerhalb des VPN-Tunnels in Senderichtung
Weitere Features	Automatische Mediatyp-Erkennung, UDP-Encapsulation; WISPr-Support (T-Mobile Hotspots); IPsec-Roaming bzw., WLAN-Roaming (Voraussetzung: NCP (Virtual) Secure Enterprise VPN Server); Importfunktion der Dateiformate:*.ini, *.pcf, *.wgx und *.spd
Point-to-Point Protokolle	PPP over GSM, PPP over Ethernet; MLP, CCP, CHAP
Internet Society RFCs und 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, IKEv2-Authentisierung nach RFC 7427 (Padding-Verfahren)
Client Monitor **Intuitive, grafische Benutzeroberfläche**	Mehrsprachig (Deutsch, Englisch, Spanisch, Französisch); Client Info Center; Konfiguration, Verbindungssteuerung und -überwachung, Verbindungsstatistik, Log-Files (farbige Darstellung, einfache Copy&Paste-Funktion); Test-Werkzeug für Internet-Verfügbarkeit; Trace-Werkzeug für Fehlerdiagnose; Anzeige des Verbindungsstatus; Integrierte Unterstützung von Mobile Connect Cards; Individuell gestaltbares Textfeld; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre; Automatische Prüfung auf neue Version

*) NCP FND-Server kann kostenlos als Add-On hier heruntergeladen werden:
https://www.ncp-e.com/de/service/download-vpn-client/

**) Voraussetzung: NCP VPN Path Finder Technology am VPN Gateway erforderlich

Weitere Informationen zum NCP Secure Entry Client finden Sie hier:
https://www.ncp-e.com/de/produkte/ipsec-vpn-client-suite/vpn-clients-fuer-windows-10-8-7-macos/
Eine kostenlose 30-Tage Vollversion können Sie hier herunterladen:
https://www.ncp-e.com/de/service/download-vpn-client/#c28557