NCP Secure Enterprise Client
Release Notes

Minor-Release: **13.10 r29617**
Datum: **August 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.

Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 5.30 oder neuer
- NCP Management Console: Version 5.30 oder neuer
- Client Configuration Plug-in: Version 13.10 oder neuer
- License Plug-in: Version 13.00 oder neuer
- Firewall Plug-in: Version 13.00 oder neuer
- Endpoint Policy Plug-in Version 6.20 oder neuer

Die folgenden Funktionen sind ab der Clientversion 13.x nicht mehr verfügbar:

- SMS Center
- Verbindungsmedium: Modem, xDSL, ext. Dialer

Vor dem Update auf diese neue Version 13 empfehlen wir im Fall des Rollouts via SEM zuerst die bereits am Anwenderrechner vorhandene Clientversion zu prüfen. Besitzt diese die Version 11.14 oder neuer, so kann das Update auf die Version 13 ohne weitere Maßnahmen durchgeführt werden. Ist die Clientversion älter, so wird dringend empfohlen einen Updateclient der Version 6.01 bis max. 7.01 zuerst via SEM zu verteilen. Er wird demnach an die erste Stelle in der Software-Update-Liste gestellt.
Bei einem Update von einer Version kleiner als 12.0 sind die Hinweise in „Neue Verzeichnisstruktur" zu beachten:

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`.

Zu beachten bei der Verwendung des NCP Secure Enterprise Managements:

Die NCP Secure Enterprise Clients lassen sich wie bisher auf die Version 13.x aktualisieren. Während des Updatevorganges wird die lokal vorgehaltene Konfiguration automatisch konvertiert. Bei der Zuweisung neuer Konfigurationen durch das NCP Management ist jedoch zu beachten, dass die zugewiesenen Konfigurationen bzw. die zugehörigen Vorlagen vor der Verteilung auf die neuen Pfade im Client umzuschreiben sind. Ebenso muss bei unterschiedlichen Clientversionen zwischen Konfigurationen ab der Version 12.x und älteren Versionen unterschieden werden. Die Verwendung absoluter Pfade wird von NCP nicht empfohlen.

1. Neue Leistungsmerkmale und Erweiterungen

Vorbereitung für die neue Benutzerauthentisierung via SAML-Protokoll

Die NCP-Lösung wird schrittweise eine neue Benutzerauthentisierung via SAML-Protokoll einführen. Die Anmeldung dazu geschieht mit dem am Rechner des Anwenders vorhandenen Standard-Webbrowser. Die Authentisierung erfolgt an einem Identitätsdienst wie Microsoft Azure AD oder Okta. Der noch in Entwicklung befindliche Authentication Server stellt die Schnittstelle zur NCP Lösung, dem NCP Secure Enterprise Management dar.

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.

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

Unterstützung des RFC 7296

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

Neuer Parameter „DNS_HOSTNAME“ innerhalb der Endpoint Policy-Prüfung

Der Parameter „DNS_HOSTNAME“ unterstützt im Gegensatz zum Parameter „COMPUTERNAME“ auch Namen länger als 15 Stellen sowie Groß-/Kleinschreibung.

2. Verbesserungen / Fehlerbehebungen

Software Update via Mobilfunk

Die Sperre von Software-Updates des Clients via Mobilfunk funktionierte nicht. Dieses Problem wurde behoben.

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 Rollout-Process mit INITUser und Zertifikatsverteilung

Problembehebung in der Client-API

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.

Erweiterung der Endpoint Policy um `WINDOWSDISPLAYVERSION`

Zur Bestimmung der korrekten Windows 10-Version wurde der Parameter `WINDOWSDISPLAYVERSION` für die Endpoint Policy-Prüfung implementiert.

Unterstützung von Windows 11 in der Endpoint Policy-Prüfung

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.

3. Bekannte Einschränkungen

Applikationsbasierte VPN Bypass Konfiguration

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

Kompatibilität des Update-Client

Der im NCP Secure Client enthaltene Update Client 8.0 ist nicht zu älteren Versionen des NCP Secure Clients kompatibel und kann dementsprechend nicht für diese Versionen via SEM-Update verteilt werden.

Anzeige der Software Update Liste

Die Software Update Liste wird häufiger angezeigt, obwohl im Secure Enterprise Management Server eingestellt ist, dass der Anwender „nur bei vorhandenen Updates“ informiert wird. Dies liegt in der Einführung des Audit-Logs im VPN-Client begründet, welches mind. einmal täglich an das zentrale Management übertragen wird.

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.

Programmwartung / Programm ändern

Wird über die klassische Systemsteuerung „Programm ändern“ der VPN-Client dazu veranlasst die Programmwartung durchzuführen, so erfolgt mit dem Treiber-Update ein Rollback der Installation. Nach dem "Fertig stellen" der Aktion erscheint die Nachricht "Schwerwiegender Fehler bei Installation". Der VPN-Client ist nach dem Schließen aller Dialoge wieder uneingeschränkt funktionsfähig.

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

Minor-Release: **13.05 r29388**
Datum: **Mai 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)

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 5.30 oder neuer
- NCP Management Console: Version 5.30 oder neuer
- Client Configuration Plug-in: Version 13.00 oder neuer
- License Plug-in: Version 13.00 oder neuer
- Firewall Plug-in: Version 13.00 oder neuer

Die folgenden Funktionen sind ab dieser Clientversion nicht mehr verfügbar:

- SMS Center
- Verbindungsmedium: Modem, xDSL, ext. Dialer

Vor dem Update auf diese neue Version 13 empfehlen wir im Fall des Rollouts via SEM zuerst die bereits am Anwenderrechner vorhandene Clientversion zu prüfen. Besitzt diese die Version 11.14 oder neuer, so kann das Update auf die Version 13 ohne weitere Maßnahmen durchgeführt werden. Ist die Clientversion älter, so wird dringend empfohlen einen Updateclient der Version 6.01 bis max. 7.01 zuerst via SEM zu verteilen. Er wird demnach an die erste Stelle in der Software-Update-Liste gestellt.

Bei einem Update von einer Version kleiner als 12.0 sind die Hinweise in „Neue Verzeichnisstruktur“ zu beachten:

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

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`.
Zu beachten bei der Verwendung des NCP Secure Enterprise Managements:
Die NCP Secure Enterprise Clients lassen sich wie bisher auf die Version 13.x aktualisieren. Während des Updatevorganges wird die lokal vorgehaltene Konfiguration automatisch konvertiert. Bei der Zuweisung neuer Konfigurationen durch das NCP Management ist jedoch zu beachten, dass die zugewiesenen Konfigurationen bzw. die zugehörigen Vorlagen vor der Verteilung auf die neuen Pfade im Client umzuschreiben sind. Ebenso muss bei unterschiedlichen Clientversionen zwischen Konfigurationen ab der Version 12.x und älteren Versionen unterschieden werden. Die Verwendung absoluter Pfade wird von NCP nicht empfohlen.

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Der NCPRWSNT-Dienst reagiert nicht mehr

In seltenen Fällen, vorrangig auf neuer Hardware kam es zu sporadischen Abstürzen des NCPRWSNT-Dienstes. Dieses Problem, welches auf einem „HP ZBook Firefly 14 G8 Mobile Workstation“ auftrat, wurde behoben.

Smartcard via CSP: Probleme mit PIN-Eingabe

Bei der Verwendung eines SmartCard-Lesers mit Ansteuerung via CSP wurde der PIN-Eingabedialog nicht automatisch beim Zugriff auf die SmartCard angezeigt. In dieser Situation musste der Anwender die PIN-Eingabe manuell aufrufen. Dieses Problem wurde behoben.

Logon-Optionen: Problem mit der automatischen Windows-Anmeldung und TOTP

Innerhalb der Logon-Optionen kann der Client so konfiguriert werden den VPN-Benutzernamen und das VPN-Passwort an die Windows-Anmeldung durchzureichen. Dies funktionierte bisher nicht für den Fall einer 2-Faktor-Authentisierung mit der Eingabe eines weiteres Passcodes. Dieses Problem wurde behoben.

Update auf OpenSSL Version 1.0.2u-12

Die im NCP Secure Client verwendete OpenSSL-Version wurde auf 1.0.2u-12 angehoben. Damit wurde die OpenSSL-Sicherheitslücke CVE-2022-0778 geschlossen.

Nach dem Ziehen und Stecken einer SmartCard wird diese im Client nicht mehr erkannt

Bei der Verwendung eines SmartCard-Lesers und Ansteuerung über CSP – Microsoft Smart Card Key Storage Provider – wurde die SmartCard nach mehrmaligen Ziehen und Stecken nicht mehr erkannt. Dieses Problem wurde behoben.

Falsche Anzeige des PIN Icons

Bei der Nutzung des Credential Providers (Windows Pre-Logon) wurde der PIN-Status bei aktivierter Option „Pin-Eingabe bei jedem Verbindungsaufbau“ falsch gesetzt. Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Anzeige des PIN- und SmartCard-Leser-Status

Sind im NCP Secure Client sowohl VPN-Profile mit und ohne Zertifikatskonfiguration vorhanden, so kann unter bestimmten Umständen der Status des PIN-Icons oder SmartCard-Lesers in der Client-GUI falsch angezeigt werden. Die Nutzung eines Profils ohne Zertifikatskonfiguration kann unter Umständen erst nach dem Neustart des PKI-Dienstes möglich sein.

Applikationsbasierte VPN Bypass Konfiguration

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

Kompatibilität des Update-Client

Der im NCP Secure Client enthaltene Update Client 8.0 ist nicht zu älteren Versionen des NCP Secure Clients kompatibel und kann dementsprechend nicht für diese Versionen via SEM-Update verteilt werden.

Option: „Dialog für Verbindungsaufbau automatisch Öffnen“

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

Major-Release: **13.04 r29374**
Datum: **März 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)

Voraussetzung für den Betrieb mit dem NCP Secure Enterprise Management (SEM)

Um diese Client-Version zentral verwalten zu können, bedarf es der folgenden zentralen Komponenten:

- NCP Secure Enterprise Management: Version 5.30 oder neuer
- NCP Management Console: Version 5.30 oder neuer
- Client Configuration Plug-in: Version 13.00 oder neuer
- License Plug-in: Version 13.00 oder neuer
- Firewall Plug-in: Version 13.00 oder neuer

Die folgenden Funktionen sind ab dieser Clientversion nicht mehr verfügbar:

- SMS Center
- Verbindungsmedium: Modem, xDSL, ext. Dialer

Vor dem Update auf diese neue Version 13 empfehlen wir im Fall des Rollouts via SEM zuerst die bereits am Anwenderrechner vorhandene Clientversion zu prüfen. Besitzt diese die Version 11.14 oder neuer, so kann das Update auf die Version 13 ohne weitere Maßnahmen durchgeführt werden. Ist die Clientversion älter, so wird dringend empfohlen einen Updateclient der Version 6.01 bis max. 7.01 zuerst via SEM zu verteilen. Er wird demnach an die erste Stelle in der Software-Update-Liste gestellt.
Bei einem Update von einer Version kleiner als 12.0 sind die Hinweise in „Neue Verzeichnisstruktur“ zu beachten:

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`.

Zu beachten bei der Verwendung des NCP Secure Enterprise Managements:
Die NCP Secure Enterprise Clients lassen sich wie bisher auf die Version 13.x aktualisieren. Während des Updatevorganges wird die lokal vorgehaltene Konfiguration automatisch konvertiert. Bei der Zuweisung neuer Konfigurationen durch das NCP Management ist jedoch zu beachten, dass die zugewiesenen Konfigurationen bzw. die zugehörigen Vorlagen vor der Verteilung auf die neuen Pfade im Client umzuschreiben sind. Ebenso muss bei unterschiedlichen Clientversionen zwischen Konfigurationen ab der Version 12.x und älteren Versionen unterschieden werden. Die Verwendung absoluter Pfade wird von NCP nicht empfohlen.

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

Unterstützung für max. 250 Split Tunneling Remote Netzwerke

Sowohl für IPv4 als auch für IPv6 können jeweils bis zu 250 Split Tunneling Konfigurationen via IKEConfigMode vom NCP Secure Enterprise VPN Server an den Client kommuniziert werden. Voraussetzung dafür ist ein NCP Secure Enterprise VPN Server ab der Version 13.0.

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 = Verbindung hergestellt aber nur Kommunikation mit dem NCP Management Server möglich (Lizenzierung)

Auswertung von Windows-Umgebungsvariablen in der Zertifikatskonfiguration

Der Client unterstützt in der Zertifikatskonfiguration "CSP Benutzer-Zertifikatsspeicher" die Eingabe von Windows Umgebungsvariablen, z.B. `%userdnsdomain%`, `%userdomain%` oder `%computername%`. Diese werden beim Einlesen der cnf-Konfiguration im zugrundeliegenden Betriebssystem abgefragt und deren Rückgabewerte statisch in die Konfiguration übernommen. Eine Kombination mit zusätzlichen Zeichen ist möglich, z:B:
„`%computername%.%userdnsdomain%`".

2. 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.

Unterstützung der NCP Secure VPN GovNet Box entfernt

Die zum Betrieb der NCP Secure VPN GovNet Box notwendigen, internen Firewall-Regeln wurden entfernt.

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

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

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.

Neu importierte Zertifikate in Computer CSP wurden nicht übernommen

In seltenen Fällen kam es bei der Verwendung des NCP Secure Client 12.20 zu Verbindungsfehlern, wenn durch Entrust ein neues Zertifikat verteilt wurde. 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.

Einlesen einer `ncpphone.cnf` via `ncpclientcmd.exe` vor Benutzeranmeldung

Ab der Version 12.x des NCP Secure Clients konnte mit den CLI-Tools `rwscmd.exe` und `ncpclientcmd.exe` keine cnf-Konfiguration vor der Benutzeranmeldung eingelesen werden. Dieses Problem wurde behoben.

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

3. Bekannte Einschränkungen

Kompatibilität des Update-Client

Der im NCP Secure Client enthaltene Update Client 8.0 ist nicht zu älteren Versionen des NCP Secure Clients kompatibel und kann dementsprechend nicht für diese Versionen via SEM-Update verteilt werden.

Option: „Dialog für Verbindungsaufbau automatisch Öffnen“

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

4. Hinweise zum NCP Secure Enterprise 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/

Weitere Informationen zum NCP Secure Enterprise Client finden Sie hier:

https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/

Weitere Unterstützung bei Fragen zum Enterprise Client, erhalten Sie über die Mail-Adressen auf folgender Seite:

https://www.ncp-e.com/de/unternehmen/kontakt/

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

5. Leistungsmerkmale

Betriebssysteme	Microsoft Windows (64 Bit): Windows 11, Windows 10 x86-64 Prozessorarchitektur
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall **Firewall Configuration**	Stateful Packet Inspection; IP-NAT (Network Address Translation); differenzierte Filterregeln bezüglich: Protokolle, Ports, Applikationen und Adressen, Schutz des LAN-Adapters; IPv4- und IPv6-Unterstützung; zentrale Administration 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; Home Zone;
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	IKEv1 (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, 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
PKI Enrollment	CMP* (Certificate Management Protocol)
Network Access Control	**Endpoint Policy: Überprüfung Aktualität des Virenscanners, vorhandene Hotfixes/Service Packs, gestartete Dienste, etc.
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)
Netzwerkprotokolle	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
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)
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; Konfigurations- und Profil-Management mit Passwortschutz, Konfigurationsparametersperre
Update mit SEM	Um ein Update auf diese Client-Software durchführen zu können, werden die SEM-Version 5.30 und folgende Plugins ab der genannten Version benötigt: • License Plugin: Version 13.00 • Client Configuration Plugin: Version 13.10 • Firewall Plug-in: Version 13.00 • Update Client: Version 8.00

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

Weitere Informationen zum NCP Secure Enterprise Client:
https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/

FIPS 140-2 Inside

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