NCP Exclusive Remote Access Client
Release Notes

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 Exclusive Remote Access Management

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

- NCP Exclusive Remote Access 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 NCP Management 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 NCP Management 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\Exclusive Remote Access Client\` waren sind in `ProgramData\NCP\Exclusive Remote Access Client\` 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\Exclusive Remote Access Client\certs`.
Anmerkung: Der Konfigurationseintrag `%CertDir%\client1.p12` ist gleichwertig zu `client1.p12`.
Zu beachten bei der Verwendung des NCP Exclusive Remote Access Client:
Die NCP Exclusive Remote Access 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 Exclusive Remote Access 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 der WPA3-Verschlüsselung

Der im NCP Exclusive Remote Access 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%".

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

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.

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.

Neu importierte Zertifikate in Computer CSP wurden nicht übernommen

In seltenen Fällen kam es bei der Verwendung des NCP Exclusive Remote Access 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 Exclusive Remote Access 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 Exclusive Remote Access 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 Exclusive Remote Access Client enthaltene Update Client 8.0 ist nicht zu älteren Versionen des NCP Exclusive Remote Access 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 Exclusive Remote Access Client

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der NCP-Website. Mehr Information zum NCP Exclusive Remote Access Client finden Sie hier:
https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/

5. Leistungsmerkmale

Betriebssysteme	Microsoft Windows (64 Bit): Windows 11, Windows 10 x86-64 Prozessorarchitektur
Juniper SRX/vSRX OS	Junos OS 15.1X49-D80 oder höher vorausgesetzt
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)
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)
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 (inkl. HSCSD), GPRS, UMTS, LTE, HSDPA
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 GPRS/UMTS und WLAN, bei GPRS/UMTS 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),
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); 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 Management-Server Version 5.30 und folgende Plugins ab der genannten Version benötigt: • License Plugin: Version 13.00 • Client Configuration Plugin: Version 13.00 • 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/

Weitere Informationen zum NCP Exclusive Remote Access Client:
https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/

FIPS 140-2 Inside

NCP PATH FINDER