NCP Secure Enterprise Client
Release Notes

Service Release: **12.00 r45109**
Datum: **August 2019**

Voraussetzungen

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

- Windows 10, 32/64 Bit (bis einschließlich Version 1903)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

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 5.20 oder neuer
- NCP Management Console: Version 5.20 oder neuer
- Client Configuration Plug-in: Version 12.00 oder neuer
- License Plug-in: Version 12.00 oder neuer
- Firewall Plug-in: Version 12.00 oder neuer

Vor dem Update auf diese neue Version 12 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 12 ohne weitere Maßnahmen durchgeführt werden. Ist die Clientversion älter, so wird dringend empfohlen den Updateclient der Version 6.01 zuerst via SEM zu verteilen. Er wird demnach an die erste Stelle in der Software-Update-Liste gestellt. Des Weiteren sind die Hinweise unter Neue Verzeichnisstruktur zu beachten.

1. Neue Leistungsmerkmale und Erweiterungen

Quality of Service

Innerhalb des VPN-Tunnels können **vom Client ausgehende Daten** priorisiert werden. In der QoS-Konfiguration ist hierfür die Gesamtbandbreite des Datenkanals in Senderichtung einzutragen. Die konfigurierte Gesamtbandbreite ist statisch. Für den Einsatz im mobilen Umfeld ist die QoS-Funktionalität daher zum aktuellen Stand nur bedingt geeignet.

Zu priorisierende Daten können, gemäß ihres Ursprungs, in Form einer .exe-Datei (case sensitive) oder eines Verzeichnisses (ohne Unterverzeichnisse) angegeben werden. Diese Datenquellen können gruppiert und jeder Gruppe eine Minimalbandbreite zugewiesen werden. Zu sendende Daten die keiner Gruppe zugeordnet werden können werden gemäß der verbleibenden Restbandbreite begrenzt. Ist eine konfigurierte Gruppe nicht in Benutzung, so erhöht sich die Restbandbreite um den reservierten Durchsatz dieser inaktiven Gruppe. Die in Senderichtung auftretenden Durchsatzraten der konfigurierten Gruppen können unter dem Menüpunkt Verbindung/Verbindungsinformationen/Quality of Service eingesehen werden.

Temporäre Home Zone

Es wurde eine neue Option „Home Zone nur temporär setzen“ hinzugefügt. Bisher hat der NCP Secure Client eine einmal gesetzte Home Zone zu einem späteren Zeitpunkt wiedererkannt. Eine gesetzte Home Zone wird bei gesetzter Option nach einem Neustart, Stand-by oder einem Wechsel des Verbindungsmediums vergessen und muss bei Bedarf neu gesetzt werden.

IPv4 / IPv6 Dual Stack-Unterstützung

Innerhalb des VPN-Tunnels wird sowohl das IPv4 und IPv6 Protokoll unterstützt. Die Split Tunneling Funktionalität kann getrennt für IPv4 und IPv6 konfiguriert werden.

Erweitertes Verbindungs-Management

Das Verbindungsmanagement des NCP Secure Clients wurde um zwei Verbindungsoptionen erweitert:
„Mobilfunk bei gestecktem LAN-Kabel ausschalten“ und
„Mobilfunk bei bestehender WLAN Verbindung ausschalten“

Die Entrust-PKI Unterstützung wurde entfernt

Erweiterung des Support-Assistenten

Der Support-Assistent sammelt ab dieser Version immer alle verfügbaren Log-Dateien zur Weitergabe an den Support. Die Dateien `setup.msilog`, `ncpdrvinst.log`, `ncpdrvupd.log` und `rwsrsu.log` wurden neu in den Support-Assistenten aufgenommen.

2. Verbesserungen / Fehlerbehebungen

Neue Verzeichnisstruktur

Aus Gründen der Betriebssicherheit und der Kompatibilität zu Windows wurde die Verzeichnisstruktur des NCP Secure Clients geändert. Folgende Verzeichnisse die bisher 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 12.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. Weitere Informationen zur Umstellung auf die neue Verzeichnisstruktur entnehmen Sie bitte der Datei `Lies_Mich.pdf`.

Verhaltensänderung der Firewallfunktion nach Ende des Testzeitraumes

Nach der Installation und dem Beginn des Testzeitraumes besitzt der NCP Secure Client für 30 Tage die volle Funktionalität. Nach Ablauf des Testzeitraumes konnte kein VPN-Tunnel aufgebaut werden und die Firewall hatte keine Funktionalität.
Dieses Verhalten wurde für die Firewallfunktionalität geändert. Nach dem Ende des Testzeitraumes verliert die Firewall ihre Funktion nicht mehr, d.h. der Rechner wird durch die Firewall weiterhin geschützt.

Erweitertes Status-Fenster „Verbindungsinformationen“

Im Statusfenster „Verbindungsinformationen“ werden die für die aktuelle VPN-Verbindung ausgehandelten Algorithmen innerhalb der IKE-Verhandlung und des IPsec-Protokolls angezeigt.

Entfernung nicht mehr relevanter Konfigurationsparameter

Die folgenden Konfigurationsparameter wurden aus der Konfiguration entfernt, da sie aktuell nicht mehr relevant sind:

Internet-Einwahl	ISDN
Verbindungssteuerung	IP-Addr. halten bei manuellem Verbindungsaufbau
Verbindungssteuerung	Dynamische Linkzuschaltung
Verbindungssteuerung	Schwellwert für Linkzuschaltung
Rückruf	
Eingehende Rufe	
Link-Einstellungen	Logon am Netzwerk
Link-Einstellungen	MAC-Adresse
DNS / Management	1. und 2. WINS-Server
Erweiterte IPsec-Optionen	Ziel-Adresse für IPsec-Gateway
Link Firewall	nur noch im Expertenmodus konfigurierbar

Unterstützung der Gemalto IDPrime 830 SmartCard

Das PIN-Handlich in Verbindung mit einer via Microsoft Smart Card Key Storage Provider (CSP) konfigurierten Gemalto IDPrime 830 SmartCard wurde optimiert.

Optimierung des NCP Filtertreibers

Der NCP Filtertreiber wurde hinsichtlich Datendurchsatz optimiert.

Optimierung der Anmeldung via Time-based OTP

Fehlerbehebung innerhalb der GUI-Skalierung

Bei Nutzung der GUI-Skalierung konnte es zu einer fehlerhaften Darstellung innerhalb von Konfigurationsdialogen kommen. Dieses Problem wurde behoben.

Fehlerbehebung innerhalb des INIT-Rolloutprozesses

Die INIT-Benutzerauthentisierung mittels der Umgebungsvariablen %USERNAME% für den Benutzernamen und %HOMEPATH% für den Authentisierungscode war ab Windows 10 Version 1803 nicht möglich. Dieses Problem wurde behoben.

Überarbeitung der Parametersperre im WLAN-Manager

Die Option „automatisch verbinden“ wird über die Parametersperre gesperrt, d.h. sie wird auch durch das manuelle Trennen einer WLAN-Verbindung nicht deaktiviert.

Überarbeitete Meldung nach Ablauf der Testversion

Die nach dem Ende des Testzeitraumes erscheinende Meldung *„Testversion abgelaufen. Bitte lizenzieren oder deinstallieren Sie die Software.“* wurde durch die folgende Meldung ersetzt: *„Die Inbetriebnahme des Secure Clients ist noch nicht vollständig abgeschlossen. Bitte bauen Sie eine VPN-Verbindung zu Ihrem Firmennetz auf um den Vorgang abzuschließen.“*

3. Bekannte Einschränkungen

Temporäre Home Zone

Sind zwei Netzwerkadapter verfügbar, so wird die Home Zone bei gesetzter Option nur auf einem Adapter vergessen.

SMS-Center: Kein Empfang von SMS möglich

Der NCP Secure Client bietet bei Vorhandensein einer Mobilfunkhardware die Option des SMS-Versands und -Empfangs an. Der SMS-Empfang funktioniert in dieser Clientversion 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:

http://www.ncp-e.com/de/downloads/download-vpn-client/versionsinformationen.html

Weitere Informationen zum NCP Secure Enterprise Client (Win32/64) finden Sie hier:

http://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/managed-vpn-client-suite.html

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

http://www.ncp-e.com/de/unternehmen/kontakt.html

5. Leistungsmerkmale

Betriebssysteme	Windows (32 und 64 Bit): Windows 10 Version 1903, Windows 8.x, Windows 7
Security Features	Unterstützung aller IPsec Standards nach RFC
Personal Firewall Firewall Configuration	Stateful Packet Inspection; IP-NAT (Network Address Translation); 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; differenzierte Filterregeln bezüglich: Protokolle, Ports, Applikationen und Adressen, Schutz des LAN-Adapters; IPv4- und IPv6-Unterstützung; zentrale Administration
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 2048 Bits; Seamless Rekeying (PFS); Hash Algorithmen: SHA-1, SHA-256, SHA-384, SHA-512, MD5, DH Gruppe 1,2,5,14-21, 25, 26
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
Standards **PKI Enrollment**	PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); Smart Card Betriebssysteme: TCOS 1.2, 2.0 und 3.0; Smart Card ReaderInterfaces: PC/SC, CT-API; PKCS#12 Interface für Private Schlüssel in Soft Zertifikaten; CSP zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher 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, 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, vollständiger WWAN-Support (Wireless Wide Area Network, Mobile Broadband ab Windows 7)
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/3G/4G) 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 (Voraussetzung: NCP Secure Enterprise Server 8.0)
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, analoges Fernsprechnetz

Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; 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
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 Secure Enterprise VPN Server)
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, PPP over Ethernet, LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
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 5.20 und folgende Plugins ab der genannten Version benötigt: • License Plugin: Version 12.00 • Client Configuration Plugin: Version 12.00 • Firewall Plug-in: Version 12.00 • Update Client: Version 7.0

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

**) Voraussetzung: NCP Secure Enterprise VPN Server / Optional: NCP Secure Enterprise Management

Weitere Informationen zum NCP Secure Enterprise Client (Win32/64):

FIPS 140-2 Inside

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

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