NCP Secure Entry Client
Release Notes

Service Release: **12.11 r48297**
Datum: **August 2020**

Voraussetzungen

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

- Windows 10, 32/64 Bit (bis einschließlich Version 2004)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

1. Neue Leistungsmerkmale und Erweiterungen

Auswahl des Zertifikats für 802.1x-Authentisierung am WLAN

Innerhalb der WLAN-Konfiguration des NCP Secure Clients kann unter Profile/Verschlüsselung über den Button „Zertifikatsauswahl“ ein Windows-Dialog zur Auswahl eines im Zertifikatsspeicher vorhandenen Zertifikates aufgerufen werden. Dieses Zertifikat wird anschließend für die 802.1x-Authentisierung an einem WLAN mit konfigurierter SSID verwendet.

Unterstützung des Cookie Challenge-Mechanismus

Der Cookie Challenge-Mechanismus dient der Abwehr von DoS-Attacken auf ein VPN-Gateway. Der NCP Secure Client unterstützt dieses Verfahren ab dieser Version und ist damit auch zu VPN-Gateways von Fremdherstellern kompatibel. Dieses Verfahren ist im Client nicht konfigurierbar.

Erweiterung der Parametersperre für Profil sichern/wiederherstellen

Die Parametersperre zur Profilsicherung wurde durch zwei neue Parametersperren ersetzt. Dabei wird nun zwischen der Sicherung und der Wiederherstellung eines Profils unterschieden.

2. Verbesserungen / Fehlerbehebungen

Umstellung auf TLS 1.2 innerhalb der FND-Verhandlung

Innerhalb der Verhandlung mit dem NCP Friendly Net Detection Server wurde auf TLS 1.2 umgestellt. Voraussetzung dafür ist die Verwendung des NCP Friendly Net Detection Server 3.01 oder neuer.

IPv6-Priorisierung bei DNS-Auflösung des VPN-Tunnelendpunkts

Ist der VPN-Tunnelendpunkt als Domainname konfiguriert, kann ein DNS-Server eine IPv6- als auch eine IPv4-Adresse zurückgeben. In diesem Fall wählt der NCP Secure Client zuerst die IPv6-Adresse aus. Im Falle des Scheiterns des Verbindungsaufbaus wird anschließend die IPv4-Adresse versucht. Gleiches Verfahren gilt bei der Auswahl eines Gateways beim Load Balancing-Verfahren.

Ausführung der `(dis)connect.bat`-Batchdatei bei Verbindungsaufbau/-abbau

Die Batchdatei `(dis)connect.bat` wurde nicht ausgeführt. Dieses Problem wurde behoben.

Eingabefenster für Benutzername und Passwort beim Verbindungsaufbau

Ist in der Clientkonfiguration bei Verwendung von IKEv1/XAUTH kein VPN-Benutzername oder Passwort eingetragen, so erscheint beim Verbindungsaufbau ein separates Eingabefenster. Bei der Verwendung von IKEv2/EAP erschien dieses Fenster nicht. Dieses Problem wurde behoben.

Auslesen von `%username%` für die ID der lokalen Identität

Analog zur Eingabe der Umgebungsvariable `%username%` für den VPN-Benutzernamen, kann dieser Eintrag nun auch in der ID der lokalen Identität vorgenommen werden. Beim erstmaligen Einlesen der Konfiguration durch die Client-GUI wird der entsprechende Wert von `%username%` fest in die Konfiguration übernommen.

Anzeige der verfügbaren WLAN-SSIDs

Verfügbare WLAN-SSIDs wurden in der WLAN-Konfiguration des NCP Secure Clients nicht vollständig angezeigt. Dieses Problem wurde behoben.

Verbesserung der Kompatibilität zu CISCO ASA

Die Kompatibilität zu CISCO ASA-Gateways in Verbindung mit IKEv2 wurde verbessert. Des Weiteren wurde die Kompatibilität zu weiteren Fremd-Gateways in Hinblick auf ReKeying verbessert.

Optimierungen der Client-GUI im Aufruf „erweiterte Log-Einstellungen“

Optimierung der Funktionalität „OTP-Token“

Optimierung der Funktionalität „Logon-Optionen“

Wurde der NCP Secure Client außerhalb des c:\Programme-Verzeichnisses installiert, so wurde der NCP Credential Provider bei der Windows-Anmeldung nicht korrekt angezeigt. Dieses Problem wurde behoben.

Anzeige der Verbindungsinformationen

Nach der Trennung einer VPN-Verbindung und dem Wiederaufbau wurden die angezeigten IP-Adressen nicht aktualisiert. Dieses Problem wurde behoben.

Optimierung der FND-Erkennung bei zwei aktiven LAN-Adaptern

Wegfall der Verzeichnisauswahl für Firewall-Log-Dateien

Verbesserung der Kompatibilität zu Gemplus USB Key Smart Card Readern

Fehlerbehebung bei der Bearbeitung von Zertifikaten mit darin enthaltenen Zertifikatsketten die größer als 8 kByte sind

Fehlerbehebung im Suchpfad einer PKCS#11-DLL unter Windows 10

Verbesserung der Kompatibilität zu ReinerSCT cyberJack®-Kartenlesern

Fehlerbehebung im Support-Assistenten

Beim Aufruf des Support-Assistenten zum Sammeln der Log-Dateien fehlen die Dateien des PKI-Log. Dieses Problem wurde behoben.

Fehlerbehebung beim Lizenzhandling

In seltenen Fällen konnte es vorkommen, dass die NCP-Lizenzdatei beschädigt wurde. Es erschien die Fehlermeldung: „Lizenzdaten konnten nicht gelesen werden“. Dieses Problem wurde behoben.

Anpassung der Fehlermeldung wenn kein VPN-Gateway erreicht wird

Fehlerbehebung innerhalb der Friendly Net Detection

Nach Zuweisung einer neuen IP-Adresse durch den DHCP-Server, wegen Ablauf der DHCP Lease Time, funktionierte die Friendly Net Detection nicht korrekt. Dieses Problem wurde behoben.

Fehlerbehebung innerhalb der Split Tunneling-Konfiguration

Unterstützung von CertReqWithData=1 in ini-Importdatei

Der Parameter CertReqWithData bewirkt, dass der Client im Falle von IKEv1 einen Zertifikatsrequest, welcher das Subject der lokal vorhandenen CA-Zertifikate enthält, an das VPN-Gateway sendet. Ist dieser Parameter nicht gesetzt so wird ein „leerer“ Zertifikatsrequest gesendet. Durch die Unterstützung dieses Parameters wird die Kompatibilität zu Fremdgateways verbessert.

3. Bekannte Einschränkungen

Silent-Installation unter Windows 7

Seit der Umstellung der Software-Signatur von SHA-1 auf SHA-256 innerhalb Windows 7, werden generell zwei Windows-Sicherheitsdialoge zur Bestätigung der Treiberinstallation während der Clientinstallation eingeblendet. Dieser Effekt tritt nicht unter Windows 8.x oder Windows 10 auf.

Option: „Dialog für Verbindungsaufbau automatisch Öffnen“

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

Client Info Center: Status des NCP Virtual Secure Client Adapters wird falsch angezeigt

Der NCP Virtual Secure Client Adapter wird im Client Info Center fälschlicherweise als deaktiviert angezeigt.

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 1909)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

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.

Expertenmodus

Innerhalb der Clientkonfiguration wurde eine Expertenkonfiguration hinzugefügt. Diese

Konfiguration enthält neben den bisherigen Konfigurationsoptionen weitere, selten genutzte oder experimentelle Optionen.

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“

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 Client 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`.
Weitere Informationen zur Umstellung auf die neue Verzeichnisstruktur entnehmen Sie bitte der Datei `Lies_Mich.pdf`.

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:

Verbindungsmedium	ISDN
ISDN	Dynamische Linkzuschaltung
ISDN	Schwellwert für Linkzuschaltung
IPsec-Adresszuweisung	1. und 2. WINS-Server
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.

3. Bekannte Einschränkungen

Temporäre Home Zone

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

4. 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

5. Leistungsmerkmale

Betriebssysteme	Windows (32 und 64 Bit): Windows 10, Windows 8.x, Windows 7; x86 bzw. 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/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
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); 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.html

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

Weitere Informationen zum NCP Secure Entry Client (Win32/64) finden Sie hier:
https://www.ncp-e.com/de/produkte/ipsec-vpn-client-suite/entry-clients.html
Eine kostenlose 30-Tage Vollversion können Sie hier herunterladen:
https://www.ncp-e.com/de/service/download-vpn-client.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