

NCP Exclusive Remote Access Client

Release Notes



Service Release: 12.20 r48591
Datum: Januar 2021

Voraussetzungen

Microsoft Windows Betriebssysteme:

Die folgenden Microsoft Windows Betriebssysteme werden mit diesem Release unterstützt:

- Windows 10, 32/64 Bit (bis einschließlich Version 20H2)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

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
- Client Configuration Plug-in: Version 12.20 oder neuer
- License Plug-in: Version 12.11 oder neuer
- Firewall Plug-in: Version 12.11

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

Neue Konfigurationsoption: DNS-Eingabe für VPN-Bypass

Mit dieser neuen Konfigurationsoption wird sichergestellt, dass für externe VPN-Bypass-Ziele die Namensauflösung durch den VPN-Tunnel nur durch die beiden konfigurierten DNS-Server erfolgt. Hierfür können in der VPN-Bypass-Konfiguration ein primärer und ein sekundärer DNS, wahlweise als IPv4 oder IPv6-Adresse, eingetragen werden. In diesem Release sind die konfigurierten DNS-Server ausschließlich für konfigurierte Webdomains wirksam. Konfigurierte Applikationen innerhalb der VPN-Bypass-Funktionalität werden aktuell noch nicht berücksichtigt.

Next Generation Network Access Technology



Bildschirmfreigabe über WLAN wird von der Client-Firewall nicht mehr geblockt

Die Bildschirmfreigabe über WLAN, z.B. zur Präsentation via Beamer über Miracast, wird von der Client-Firewall nicht mehr geblockt und ist nun möglich.

2. Verbesserungen / Fehlerbehebungen

Problembehebung bei Falscheingabe eines WLAN-Passwortes in der Pre-Logon-Phase

Wurde während der Pre-Logon-Phase bei der Anmeldung an einem WLAN ein falsches WLAN-Passwort eingegeben, so konnte dieses Passwort nicht mehr geändert werden. Mit dieser Freigabe wird das Passwort bei Falscheingabe erneut abgefragt und das neue WLAN-Profil erst nach einer erfolgreichen Anmeldung am WLAN erzeugt.

Problembehebung bei Reverse DNS-Anfragen

Es wurde ein Problem mit Reverse DNS-Anfragen (PTR-Anfragen) des Betriebssystems behoben.

Update auf OpenSSL Version 1.0.2u-8

Die im NCP Exclusive Remote Access Client verwendete OpenSSL-Version wurde auf 1.0.2u-8 angehoben. Damit wurde die OpenSSL-Sicherheitslücke CVE-2020-1971 geschlossen.

Bluescreen nach Update des NCP Exclusive Remote Access Clients

In seltenen Fällen stürzte der Anwender-Rechner während des ersten Neustarts nach einem Update des NCP Exclusive Remote Access Clients ab. Dieses Problem trat ausschließlich mit Windows 10 auf und wurde behoben.

FND-Erkennung schlägt bei installiertem Hyper-V fehl

Ist auf dem Anwender-Rechner Hyper-V installiert und dementsprechend ein virtueller Switch aktiv, so ist die FND-Funktionalität im NCP Exclusive Remote Access Client gestört. Dieses Problem wurde behoben.

Probleme in Verbindung mit mehreren IPv6-Adressen auf dem Adapter

Wurden dem NCP-Netzwerkadapter mehrere IPv6-Adressen zugewiesen so konnte in bestimmten Fällen der VPN-Verbindungsaufbau oder der Datentransfer durch den VPN-Tunnel gestört sein. Dieses Problem wurde behoben.

Kein Datentransport durch den VPN-Tunnel bei Juniper SRX Gegenstelle

In seltenen Fällen können in Verbindung mit einer Juniper SRX Gegenstelle keine Daten durch den VPN-Tunnel transportiert werden. Die äußert sich in einer falsch zugewiesenen IPv4-Adresse auf dem NCP-Adapter. Dieses Problem wurde behoben.



DNS Fehler

Unter bestimmten Umständen wurden DNS-Anfragen durch den VPN-Tunnel nicht richtig aufgelöst bzw. lieferten einen Fehler. Ursache war eine falsch vergebene Metrik auf dem NCP Netzwerkadapter. Dieses Problem wurde behoben.

Support-Assistent

Der Ausgabepfad zur Ablage der ZIP-Datei mit den gesammelten Protokolldateien wurde ignoriert. Dieses Problem wurde behoben.

Kein Datendurchsatz im VPN-Tunnel

In seltenen Fällen konnten beim Einsatz von Seamless Roaming nach dem Medienwechsel keine Daten durch den VPN-Tunnel transportiert werden. Ursache war, dass die DHCP-Verhandlung für den NCP-Netzwerkadapter in einen Timeout lief und dadurch die IP-Adresse nicht korrekt zugewiesen wurde. Dieses Problem wurde behoben.

Fehlerbehebung im Bereich der VPN-Bypass-Funktionalität

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.



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

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
- Client Configuration Plug-in: Version 12.11 oder neuer
- License Plug-in: Version 12.11 oder neuer
- Firewall Plug-in: Version 12.11

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

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.

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. Der Eintrag `%ncpusername%` bewirkt das Auslesen des zugehörigen Wertes von `%username%` für jeden Start der Client-GUI.

Anzeige der verfügbaren WLAN-SSIDs

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

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

Einlesen der Initialkonfiguration

Beim Einlesen der Initialkonfiguration vom NCP Exclusive Remote Access Management konnte es vorkommen, dass die Client-GUI nicht korrekt dargestellt wurde. Dieses Problem wurde behoben.

Software-Update via NCP Exclusive Remote Access Management

Beim Software-Update via NCP Exclusive Remote Access Management wurde der Download-Zähler im NCP Exclusive Remote Access Management nicht erhöht. Dieses Problem wurde behoben.

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



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.

NCP Exclusive Remote Access 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 1909)
- Windows 8.x, 32/64 Bit
- Windows 7, 32/64 Bit

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 5.0 oder neuer
- NCP Management Console: Version 5.0
- Client Configuration Plug-in: Version 12.00 oder neuer
- License Plug-in: Version 12.00 oder neuer
- Firewall Plug-in: Version 12.00

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

Next Generation Network Access Technology



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 Exclusive Remote Access 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 Exclusive Remote Access 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 Exclusive Remote Access Clients geändert. Folgende Verzeichnisse die bisher 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 Managements:

Der NCP Exclusive Remote Access Client lässt 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 Exclusive Remote Access 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 Exclusive Remote Access Clients ist noch nicht vollständig abgeschlossen. Bitte bauen Sie eine VPN-Verbindung zu Ihrem Firmennetz auf um den Vorgang abzuschließen.*“

3. Bekannte Einschränkungen

Keine.

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	Windows (32 und 64 Bit): Windows 10, Windows 8.x, Windows 7; x86 bzw. 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: <ul style="list-style-type: none">▪ 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

NCP Exclusive Remote Access Client

Release Notes



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, <i>vorm. CRL</i>), CARL (Certification Authority Revocation List, <i>vorm. ARL</i>), OCSP
PKI Enrollment	CMP* (Certificate Management Protocol)
Networking Features	LAN Emulation: Virtual Ethernet-Adapter mit NDIS-Interface, integrierter WLAN- (Wireless Local Area Network) 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

Next Generation Network Access Technology

NCP Exclusive Remote Access Client

Release Notes



	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); 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: <ul style="list-style-type: none">• License Plugin: Version 12.11• Client Configuration Plugin: Version 12.11• Firewall Plug-in: Version 12.11 mind.• Update Client: Version 7.01

*) NCP FND-Server kann kostenlos als Add-On hier heruntergeladen werden:

<https://www.ncp-e.com/de/service/download-vpn-client.html>

Weitere Informationen zum on NCP Exclusive Remote Access Client:

<https://www.ncp-e.com/en/exclusive-remote-access-solution/vpn-client/>



FIPS 140-2 Inside

NCP PATH FINDER

Next Generation Network Access Technology