Release Notes

Advanced VPN Client Windows 6.23 Rel / 5.23 Rel

Inhaltsübersicht

1. Einleitung

Mit dem LANCOM Advanced VPN Client Windows können sich mobile Mitarbeiter jederzeit über einen verschlüsselten Zugang in das Unternehmensnetzwerk einwählen – ob im Home Office oder unterwegs, im Inland wie im Ausland.

Dieses Dokument beschreibt die Neuerungen der aktuellen LANCOM Advanced VPN Client Versionen 6.23 Rel und 5.23 Rel sowie die Änderungen zu den entsprechenden Vorversionen.

Der Client benötigt zur Aktivierung einen Lizenzschlüssel der gleichen Version. Eine Aktivierung bzw. Update-Installation mit altem Lizenzschlüssel ist nicht mehr möglich. Dies gilt fortan für jede kommende Major-Version.

2. Das Release-Tag in der Software-Bezeichnung

Release Candidate (RC)
Ein Release Candidate ist umfangreich von LANCOM getestet und enthält neue Betriebssystem-Features. Er dient als Praxistest und wird deshalb für den Einsatz in Produktivumgebungen nicht empfohlen.

Release-Version (Rel)
Das Release ist umfangreich geprüft und in der Praxis erfolgreich getestet. Es enthält neue Features und Verbesserungen bisheriger LANCOM Betriebssystem-Versionen und wird daher für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Ein Release Update dient zur nachträglichen Weiterentwicklung einer initialen Release-Version in Produktivumgebungen und enthält Detailverbesserungen, Security Fixes, Bug Fixes und kleinere Features.

Security Update (SU)
Enthält wichtige Security Fixes des jeweiligen LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard in Ihrer Produktivumgebung.

3. Voraussetzungen

Unterstützte Microsoft Windows Betriebssysteme

Eine Liste der unterstützten Betriebssysteme / Versionen können sie hier einsehen: https://knowledgebase.lancom-systems.de/pages/viewpage.action?pageId=37457108

HotSpot-Anmeldung

Für die korrekte Funktion der HotSpot-Anmeldung muss mindestens die Version 101.0.1210.39 der Microsoft WebView2-Runtime installiert sein.

Neue Verzeichnisstruktur

Aus Gründen der Betriebssicherheit und der Kompatibilität zu Windows wurde die Verzeichnisstruktur des LANCOM Advanced VPN Clients ab Version 5.0 geändert. Folgende Verzeichnisse, die bei älteren Clientversionen im Installationsverzeichnis innerhalb **Programme\LANCOM\Advanced VPN Client** waren, sind ab sofort in **ProgramData\LANCOM\Advanced VPN Client** beheimatet:

→ arls
→ cacerts
→ certs
→ config
→ crls
→ CustomBrandingOption
→ data
→ hotspot
→ log
→ statistics

Dabei handelt es sich um Konfigurationsdateien, Zertifikate oder Log-Dateien. Binaries oder Ressourcen verbleiben weiterhin im Pfad **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\LANCOM\Advanced VPN Client\certs**.

Hinweis:

Der Konfigurationseintrag **%CertDir%\client1.p12** ist gleichwertig zu **client1.p12**.

4. Historie Advanced VPN Client Windows Version 6.x

Advanced VPN Client Windows 6.23 Rel Build 30776

Korrekturen / Anpassungen

→ **Verbindungsprobleme mit 5G-Modems**

Bei einigen Endgeräten mit 5G-Modem konnte es zu Verbindungsproblemen mit dem Mobilfunk kommen, sobald der LANCOM Advanced VPN Client auf dem Gerät installiert wurde. Auffällig war dabei besonders die folgende Mobilfunk-Hardware:

- Quectel RM520N–GL 5G
- Snapdragon X62-5G (DW5932e)

Wiederherstellung der 5G-Konnektivität

Sofern bereits ein älterer Advanced VPN Client auf einem Windows-Rechner mit integriertem 5G Mobilfunk-Modem installiert wurde, kann mit nachfolgender Vorgehensweise das 5G-Verbindungsproblem behoben werden:

1. Installation des Advanced VPN Clients 6.23 Rel
2. Aufruf des Geräte-Managers ‚devmgmt.msc' im Administratormodus
3. Erweitern des Menüs ‚Netzwerkadapter' und Doppelklick auf das 5G-Modem
4. In den Modem-Eigenschaften ‚Erweitert' auswählen
5. In der Eigenschaftsliste alle nachfolgenden Einträge auf den Wert ‚Rx & Tx Enabled' setzen:
   - TCP-Prüfsummen-Offload (IPv4)
   - TCP-Prüfsummen-Offload (IPv6)
   - UDP-Prüfsummen-Offload (IPv4)
   - UDP-Prüfsummen-Offload (IPv6)
6. Bestätigen des Eigenschaftsdialogs mit ‚Ok' und Neustart des Rechners

→ **Routingtabelle wurde nicht korrekt gesetzt**

Waren beide nachfolgenden Bedingungen erfüllt, so wurde die Routing-Tabelle im Client nicht richtig gesetzt:

- Der Verbindungsaufbau erfolgte über ein Profil mit dem Medientyp ‚Mobilfunk'.
- Die Konfiguration des Split Tunneling war nicht Teil der Client-Konfiguration, sondern der Client bekam die entsprechende Konfiguration via IKE Config Mode vom VPN-Gateway.

Bekannte Einschränkungen

→ **Client zeigt keine Reaktion beim Verbindungsaufbau**
Es kann vorkommen, dass der Client nach einem Versions-Update keine Verbindung zum Gateway aufbauen kann. Dies kann durch eine Deinstallation und eine Neuinstallation des Clients behoben werden.

→ **GUI zeigt Verbindungsfehler**
Es kann vorkommen, dass der Client einen Verbindungsfehler anzeigt, obwohl der Tunnel steht. Dies kann auftreten, wenn der Computer aus einem Ruhezustand kommt oder das WiFi Signal kurzeitig verliert.

Advanced VPN Client Windows 6.22 Rel Build 30766

Korrekturen / Anpassungen

→ **VPN-Bypass-Konfiguration einer Applikation mit Wildcard**

Die Erstellung einer applikationsbasierten VPN-Bypass-Regel bedarf der Angabe des vollständigen Dateipfades der betreffenden Applikation. Für Firefox lautet dieser Dateipfad standardmäßig:
C:\Program Files\Mozilla Firefox\firefox.exe
Für Cloud-Applikationen kann es hilfreich sein, in deren Dateipfad ein Wildcard (gültig innerhalb einer Verzeichnisebene) mit aufzunehmen, da oft mit einem Applikationsupdate ein neuer Dateipfad angelegt wird. Nachfolgend ein Beispiel für Microsoft Teams:
C:\Program Files\WindowsApps\MSTeams_23285.3607.2525.937_x64__8wekyb3d8bbwe\ms-teams.exe
Hier empfiehlt sich die Konfiguration des Dateipfades wie folgt:
C:\Program Files\WindowsApps\MSTeams_*\ms-teams.exe
oder
C:\Program Files*\MSTeams_*\ms-teams.exe
Anmerkung: Im Gegensatz zu vorherigen Client-Versionen ist es nun NICHT mehr möglich, ausschließlich den Applikationsnamen, hier ‚ms-teams.exe', zu konfigurieren. Diese Konfiguration wird aus Sicherheitsgründen vom Client nicht ausgewertet.

→ **Signalisierung von IKEv2-Mobike**

Wurde dem Client über das Gateway signalisiert, dass kein IKEv2-Mobike unterstützt wird, so sendete der Client dennoch MOBIKE-Benachrichtigungen an das Gateway, was zu unerwünschten Effekten führen konnte.

→ **Seamless Roaming nach Standby**

Sofern ein WLAN-Adapter während eines Standby von Windows deaktiviert wurde, erfolgte nach dem Beenden des Standby kein automatischer VPN-Verbindungsaufbau.

→ **Absturz der Client GUI bei Lizenzaktivierung**

In seltenen Fällen konnte es während der Lizenzaktivierung im Advanced VPN Client vorkommen, dass die Client GUI abstürzte.

→ **Automatischer Modus mit zwei Mobilfunkkonfigurationen**
Wurde der automatische Modus konfiguriert und es waren zwei Mobilfunkkonfigurationen vorhanden, so wurde nur die erste Mobilfunkkonfiguration ausgewählt. War in diesem Fall die SIM-Karte des anderen Mobilfunkproviders gesteckt, so wurde die dazu passende Mobilfunkkonfiguration nicht verwendet. Dieses Problem wurde behoben.

Bekannte Einschränkungen

→ **Unter bestimmten Umständen wird die Firewallkonfiguration im AVC nicht korrekt dargestellt.**

→ **Option: ‚Dialog für Verbindungsaufbau automatisch öffnen'**
Unter bestimmten Umständen funktioniert die Logon-Option ‚Dialog für Verbindungsaufbau automatisch öffnen' nicht.

Advanced VPN Client Windows 6.21 Rel Build 30745

Neue Features

→ **LANCOM Trusted Access Client**
Mit dieser Version wird der LANCOM Trusted Access Client eingeführt. Bei einer Neuinstallation wird der Benutzer innerhalb der Installationsroutine gefragt, ob der neue LANCOM Trusted Access Client (LTA Client) oder der LANCOM Advanced VPN Client (AVC) installiert werden soll. Im Falle eines Updates des Advanced VPN Clients wird dieser weiterhin ausgeführt. Der Betriebsmodus kann jeweils umgeschaltet werden.

→ **Neue GUI**
Die GUI des LANCOM Advanced VPN Client wurde überarbeitet.

→ **Die GUI-Skalierung wurde entfernt**
Der Menüpunkt ‚Ansicht / GUI-Skalierung' wurde entfernt.

→ **Anpassung des Software-Update-Dialogs für kostenpflichtige Updates**
Erkennt der VPN-Client innerhalb der Software Update-Prüfung eine neue, verfügbare Major Release, so weist er auf ein kostenpflichtiges Update hin.

Korrekturen / Anpassungen

→ **Aushandlung von IPv6-Selektoren**
Der Client handelt ab dieser Version nur noch IPv6-Selektoren aus, sofern ihm durch das Gateway eine IPv6-Adresse zugewiesen wird.

→ **Problembehebung: Bildschirmtastatur öffnet sich**
Ist die Bildschirmtastatur aktiviert, so trat sie bei bestimmten Aktionen im Menü des Clients in den Vordergrund.

→ **Problembehebung: Export eines VPN-Profils**
Beim Export eines Profils in eine INI-Datei werden nun auch IPv6-Adressen übernommen.

→ **Problembehebung: INI-Datei-Import bricht ab**
Der Profilimport via INI-Datei wurde überarbeitet, sodass jetzt bis zu 400 Profile importiert werden können.

→ **Problembehebung: Aktive PIN-Menüpunkte bei der Hardware-Zertifikaten**
Der VPN-Client zeigte trotz der Konfiguration von Hardware-Zertifikaten im Menü ‚Verbindung' fälschlicherweise die Menüpunkte ‚PIN eingeben / ändern / zurücksetzen' an.

→ **Problembehebung beim Export eines VPN-Profils mit PSK**

→ **Problembehebung: Absturz des VPN-Dienstes**
Unter bestimmten Konstellationen konnte der VPN-Dienst mit der Aktivierung des PKI-Logs abstürzen.

→ **Problembehebung: Support-Assistent sammelt nicht alle vorhandenen Log-Dateien ein**

→ **Verbesserung des PIN-Handlings in Verbindung mit SmartCard-Lesern mit PIN-Pad und konfigurierter PKCS#11**

→ **Problembehebung: Audit Log-Dateien wurden nicht (nach festgelegter Zeit) gelöscht.**

→ **Problembehebung: Löschen des verwendeten Zertifikats im Benutzer CSP**
Wurde das aktuell verwendete Benutzerzertifikat im Benutzer CSP gelöscht, so konnte der VPN-Client trotz vorhandener Alternativ-Zertifikate keine neue VPN-Verbindung aufbauen. Erst nach einem Wechsel des VPN-Profils auf ein anderes und wieder zurück konnte eine VPN-Verbindung aufgebaut werden.

→ **RFC 5685: IKEv2 Redirect-Unterstützung für IPv4/6 und FQDNs hinzugefügt**

→ **Optimierung in der Pro-Logon-Phase mit OTP**

→ **Update auf OpenSSL Version 1.0.2zi**

→ **Neuer Treiber bzw. Netzwerkadapter**
Der Treiber bzw. Netzwerkadapter des NCP Secure Clients wurde aufgrund eines möglichen Bluescreens angepasst. Dieser Bluescreen trat nach der Installation des NCP Secure Clients während des darauffolgenden Startvorganges auf. Betroffen waren nur vereinzelte Endgeräte mit der jeweils verwendeten Softwareumgebung.
Infolge dieser Anpassung wurde der Name des Netzwerkadapters geändert.

→ **Problembehebung beim Profilwechsel von WLAN auf Mobilfunk**
Ist die Option ‚Mobilfunk bei bestehender WLAN-Verbindung ausschalten' gesetzt, so konnte beim ersten Verbindungsversuch nach einem Profilwechsel von WLAN auf Mobilfunk keine Verbindung aufgebaut werden.

→ **Zertifikatsbehandlung**
Die Auswahl eines Benutzerzertifikates anhand der erweiterten Schlüsselverwendung schlug unter bestimmten Umständen fehl.

→ **Interne Optimierungen zur Performance-Steigerung**

→ **Log-Ausgabe bei Pre-Logon-Betrieb**
Im Falle des Pre-Logon-Betriebs konnte es vorkommen, dass bei einer größeren Anzahl an Log-Ausgaben der Client GUI nicht alle Log-Meldungen in die Log-Datei geschrieben wurden.

→ **Verbindungsaufbau über Mobilfunk**
Beim Verbindungsaufbau über Mobilfunk in Verbindung mit Seamless Roaming konnte in bestimmten Fällen kein funktionaler VPN-Tunnel aufgebaut werden.

→ **INI-Profil-Import auf DH-Gruppe 30 erweitert**
Innerhalb des INI-Profil-Imports konnten bisher DH-Gruppen bis einschließlich DH-Gruppe 26 importiert werden. Die Importfunktion wurde auf die DH-Gruppen bis 30 erweitert.

Bekannte Einschränkungen

→ **Unter bestimmten Umständen wird die Firewallkonfiguration im AVC nicht korrekt dargestellt**

→ **Option: ‚Dialog für Verbindungsaufbau automatisch Öffnen'**
Unter bestimmten Umständen funktioniert die Logon-Option ‚Dialog für Verbindungsaufbau automatisch Öffnen' nicht.

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

→ **PIN-Menüeinträge**
Bei der Verwendung von Hardware-Zertifikaten sind die PIN-Menüeinträge ‚PIN eingeben / zurücksetzen / ändern' 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 Wieder-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.

Advanced VPN Client Windows 6.14 Rel Build 29669

Korrekturen / Anpassungen

→ **Anpassung der PKCS#11-Modul-Konfiguration**
Um die Sicherheit des LANCOM Advanced VPN Clients zu erhöhen, können ab dieser Clientversion nur noch PKCS#11-Dateien von folgenden Orten geladen werden: WINDIR, PROGRAMFILES und PROGRAMFILES(x86).

→ **Verbesserung: VPN Bypass und Mobilfunk**
Bei Verwendung eines Profils mit konfiguriertem Verbindungsmedium ‚Mobilfunk' ist die über VPN Bypass konfigurierte Domain nun wieder zuverlässig nutzbar.

→ **Verbesserung: Automatische Medienerkennung**
Die ‚automatische Medienerkennung' wählt nun wieder zuverlässig LAN als Verbindungsmedium aus, wenn das Gerät mit dem LAN verbunden ist.

→ **Verbesserung: Stateful Boot-Option**

→ **Verbesserung: Statusanzeige (PIN-Symbol) im Zusammenhang mit Smartcards**

→ **Anpassung der IKEv2 Configuration Payload**
Die Länge des IKEv2 Configuration Payload Attribute Typs INTERNAL_IP6_ADDRESS wurde von 16 Bytes auf 17 Bytes geändert. Es wird demnach nun zusätzlich zur IPv6-Adresse auch das Prefix übertragen.

→ **Unterstützung von RFC7383 (IKEv2 Message Fragmentation)**

→ **Update auf OpenSSL Version 1.0.2zg**

Bekannte Einschränkungen

→ **Option: ‚Dialog für Verbindungsaufbau automatisch öffnen'**
Unter Umständen funktioniert die Logon-Option ‚Dialog für Verbindungsaufbau automatisch Öffnen' nicht zuverlässig.

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

→ **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.

Advanced VPN Client Windows 6.11 Rel Build 29631

Neue Features

→ **Neue Option: DNS Domains im Tunnel auflösen**
Die Split-DNS-Funktionalität lässt sich mit Hilfe der neuen Option ‚DNS Domains im Tunnel auflösen' 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.

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

Korrekturen / Anpassungen

→ **Neue Rechtestruktur innerhalb C:\ProgramData\NCP**
Die Schreibrechte innerhalb des Verzeichnisses ‚C:\ProgramData\NCP\' wurden auf ein Minimum begrenzt. Beispielsweise kann ein Benutzer nun keine CA-Zertifikate mehr im dafür vorgesehenen Verzeichnis ablegen. Ebenso wurde die Verzeichnis- und Rechte-Struktur so umgebaut, dass keine Anwendung im User- und System-Kontext in das gleiche Verzeichnis schreibt.

→ **Verbesserungen beim serverseitig konfigurierten Split-DNS**

→ **Die automatische Windows-Anmeldung funktioniert wieder.**

→ **Seamless Roaming funktioniert nun auch mit IPv6-Zieladressen.**

→ **Gespeicherte VPN-Benutzernamen werden nach einem AVC-Update wieder korrekt angezeigt.**

→ **Verbesserung der Kompatibilität zu Fremdgateways bei der Adressierung via IPv6**

→ **Die Kompatibilität zu Fremdgateways in Verbindung mit der 2-Faktor-Authentisierung / Tokeneingabe wurde verbessert**

→ **Diverse GUI-Optimierungen**

→ **Update auf zlib Version 1.2.12**

→ **CVE-2022-0778 und CVE-2020-1971 wurden in der OpenSSL behoben.**

→ **Umstellung auf TLS 1.2 (TLS 1.0 und 1.1 werden ab sofort nicht mehr unterstützt)**

→ **Update auf cURL-Library 7.84.0**

- → **Änderungen der DNS-Einträge in der VPN-Bypass-Konfiguration funktionieren wieder ordnungsgemäß.**
- → **Verbesserung der Funktion ‚Verbindungsaufbau vor Windows-Anmeldung'**
- → **Die Weitergabe der Split-DNS-Konfiguration durch das Gateway (RFC 8598) wird nun unterstützt.**
- → **Die Netzwerkverbindung funktioniert nach einer Client-Installation wieder ordnungsgemäß.**
- → **Allgemeine Verbesserungen beim INI-Datei-Import**
- → **Implementierung des RFC8598 (https://datatracker.ietf.org/doc/html/rfc8598)**

Bekannte Einschränkungen

- → **Option: ‚Dialog für Verbindungsaufbau automatisch Öffnen'**
  Unter bestimmten Umständen funktioniert die Logon-Option ‚Dialog für Verbindungsaufbau automatisch öffnen' nicht.
- → **Applikationsbasierte VPN-Bypass-Konfiguration**
  Die Konfiguration eines DNS innerhalb der VPN-Bypass-Konfiguration macht eine darin enthaltene applikationsbasierte Regel unwirksam.
- → **PIN-Menüeinträge**
  Bei der Verwendung von Hardware-Zertifikaten ist der PIN-Menüeintrag ‚PIN eingeben/zurücksetzen/ändern' 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.

Advanced VPN Client Windows 6.04 Rel Build 29378

Neue Features

→ **Überarbeitete Hotspot-Anmeldung**

Ab dieser Version 6.0 des LANCOM Advanced VPN Client 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

→ **INI-Datei-Import für max. 250 Split-Tunneling-Netzwerke**

Sowohl für IPv4 als auch für IPv6 können jeweils bis zu 250 Split-Tunneling-Konfigurationen via INI-Datei in den Client importiert werden.

→ **INI-Datei-Import: Neuer Split-DNS-Parameter**

Die gezielte Umleitung von DNS-Requests in den VPN-Tunnel kann nun durch Setzen des Parameters ‚DomainInTunnel' mit einer max. Länge von 1023 Zeichen in der Import-Datei konfiguriert werden.

→ **Unterstützung der WPA3-Verschlüsselung**

Der im LANCOM Advanced VPN 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. Diese Funktion wird ab dieser Client-Version unterstützt.

→ **Erweiterung des VPN-Status in der Windows-Registry**

Bisher ließ sich der Verbindungsstatus des LANCOM Advanced VPN 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)

Korrekturen / Anpassungen

→ **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.

→ **‚Network Location Awareness' bei aktiver 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'.

→ **Automatische Anmeldung via Credential-Provider**

Bei Verwendung der Logon-Option mit konfigurierten User Credentials konnte ein gesperrter Windows-Arbeitsplatz durch Auswahl des Credential-Providers entsperrt werden.

→ **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.

→ **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.

→ **Überarbeitete Installationsroutine**
In seltenen Fällen wurde nach Ende des Installationsvorganges und vor dem Rechner-Neustart die Netzwerkverbindung komplett getrennt. Desweiteren wurde innerhalb des MSI-Installationsvorganges die ‚Programm reparieren‘-Funktionalität entfernt.

→ **Standby-Zustand in Verbindung mit IPv6**
Nach dem Standby-Zustand des PCs kam es mit IPv6 zu Verbindungsproblemen.

→ **Installation mit certmgr.exe**
Bei der Installation des LANCOM Advanced VPN Clients wurde die von Microsoft erstellte Datei ‚certmgr.exe‘ zur Installation des Herstellerzertifikates verwendet. Diese Datei wurde als nicht signiert erkannt. Ab dieser Version wird anstatt ‚certmgr.exe‘ die neuere ‚certutil.exe‘ verwendet.

→ **Dynamische Zertifikatsauswahl**
Die Zertifikatsauswahl wurde verbessert, zudem werden künftig nur gültige Zertifikate importiert.

→ **Fehlerbehebung im ESP-Header für IPv6**

→ **Überarbeitete Parameter-Sperren in der Client-GUI**
In der Client-GUI wurden Maßnahmen getroffen, damit gesperrte Schaltflächen sich nicht durch bestimmte Tools aktivieren lassen und dadurch gesperrte Funktionen zur Verfügung gestellt werden.

→ **Behebung eines Fehlverhaltens beim Verbindungsaufbau mit der HTTPS-Encapsulation und 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.

→ **Verbesserung der VPN-Bypass-Kompatibilität zu MS Teams**

Bekannte Einschränkungen

→ **Option ‚Dialog für Verbindungsaufbau automatisch öffnen'**

Unter bestimmten Umständen funktioniert die Logon-Option ‚Dialog für Verbindungsaufbau automatisch öffnen' nicht.

5. Historie Advanced VPN Client Windows Version 5.x

Advanced VPN Client Windows 5.23 Rel Build 48767

Korrekturen / Anpassungen

→ **Unvollständige Log-Dateien**
Es konnte sporadisch zu fehlerhaften Schreibzugriffen auf die Client-Log-Dateien kommen, welche dazu führten, dass das Client-Log unvollständig war.

→ **Überarbeitete Installationsroutine**
In seltenen Fällen wurde nach Ende des Installationsvorganges vor dem Rechner-Neustart die Netzwerkverbindung komplett getrennt.

→ **Behebung von CVE-2021-41793**
Innerhalb des MSI-Installationsvorganges wurde die ‚Programm reparieren'-Funktionalität entfernt und damit CVE-2021-41793 beseitigt.

Advanced VPN Client Windows 5.20 Rel Build 48591

Neue Features

→ **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.

→ **Bildschirmfreigabe über WLAN**

Die Bildschirmfreigabe über WLAN, z.B. zur Präsentation via Beamer über Miracast, ist nun möglich.

Korrekturen / Anpassungen

→ **Problembehebung bei Reverse DNS-Anfragen**

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

→ **Update der integrierten OpenSSL-Version**

Die im LANCOM Advanced VPN Client verwendete OpenSSL-Version wurde auf die neueste Version aktualisiert.

→ **Probleme in Verbindung mit mehreren IPv6-Adressen auf dem Adapter**

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

→ **DNS-Fehlerbehebung**

Unter bestimmten Umständen wurden DNS-Anfragen durch den VPN-Tunnel nicht richtig aufgelöst oder lieferten einen Fehler.

→ **Support-Assistent**

Der Ausgabepfad zur Ablage der ZIP-Datei mit den gesammelten Protokolldateien wird nun berücksichtigt.

→ **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.

→ **Fehlerbehebung im Bereich der VPN-Bypass-Funktionalität**

→ **Diverse Stabilitätsverbesserungen**

Bekannte Einschränkungen

→ **Netzwerkverbindung bleibt nach Installation/Update getrennt**
Nach dem Installations-/Updatevorgang des Advanced VPN Client bleibt die Netzwerkverbindung inaktiv und kann erst nach einem Neustart des Rechners genutzt werden.

→ **Dialog bei 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.

Advanced VPN Client Windows 5.11 Rel Build 48297

Neue Features

→ **Auswahl des Zertifikats für IEEE 802.1X-Authentisierung am WLAN**
Innerhalb der WLAN-Konfiguration des LANCOM Advanced VPN 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 IEEE 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. Die Funktion 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.

Korrekturen / Anpassungen

→ **IPv6-Priorisierung bei DNS-Auflösung des VPN-Tunnelendpunktes**
Ist der VPN-Tunnelendpunkt als Domänenname konfiguriert, kann ein DNS-Server sowohl eine IPv6- als auch eine IPv4-Adresse zurückgeben. In diesem Fall wählt der LANCOM Advanced VPN Client zuerst die IPv6-Adresse aus. Im Falle des Scheiterns des Verbindungsaufbaus wird anschließend die IPv4-Adresse versucht.

→ **Eingabefenster für Benutzername und Passwort beim Verbindungsaufbau IKEv2/EAP**
Ist in der Clientkonfiguration bei Verwendung von IKEv2/EAP kein Benutzername oder Passwort eingetragen, so erscheint beim Verbindungsaufbau nun ein separates Eingabefenster.

→ **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 LANCOM

Advanced VPN Client nicht vollständig angezeigt.

→ **Optimierungen der Client-GUI im Aufruf ‚erweiterte Log-Einstellungen'**

→ **Optimierung der Funktionalität ‚OTP-Token'**

→ **Optimierung der Funktionalität ‚Logon-Optionen'**
Wurde der LANCOM Advanced VPN Client außerhalb des ‚C:\Programme'-Verzeichnisses installiert, so wurde der NCP Credential Provider bei der Windows-Anmeldung nicht korrekt angezeigt.

→ **Anzeige der Verbindungsinformationen**
Nach der Trennung einer VPN-Verbindung und deren Wiederaufbau wurden die angezeigten IP-Adressen nicht aktualisiert. Dieses Problem wurde behoben.

→ **Wegfall der Verzeichnisauswahl für Firewall-Log-Dateien**

→ **Verbesserung der Kompatibilität zu Gemplus USB Key SmartCard Lesegeräten**

→ **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 fehlten die Dateien des PKI-Log. Dieses Problem wurde behoben.

→ **Fehlerbehebung beim Lizenz-Handling**
In seltenen Fällen konnte es vorkommen, dass die Lizenzdatei des LANCOM Advanced VPN Client 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 Split Tunneling-Konfiguration**

Bekannte Einschränkungen

→ **Silent Installation unter Windows 7**
Seit der Umstellung der Software-Signatur von SHA-1 auf SHA-256 innerhalb von Windows 7 werden generell zwei Windows-Sicherheitsdialoge zur Bestätigung der Treiberinstallation während der Client-Installation 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.

Advanced VPN Client Windows 5.00 Rel Build 45109

Neue Features

→ **Quality of Service**

Innerhalb des VPN-Tunnels können vom Client ausgehende Daten nun 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.

→ **IPv4 / IPv6 Dual Stack-Unterstützung**

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

→ **Temporäre Home Zone**

Es wurde eine neue Option „Home Zone nur temporär setzen“ hinzugefügt. Bisher hat der Advanced VPN 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 nun vergessen und muss bei Bedarf neu gesetzt werden.

→ **Expertenmodus**

Innerhalb der Clientkonfiguration wurde eine Expertenkonfiguration hinzugefügt.

→ **Erweitertes Verbindungs-Management**

Das Verbindungsmanagement des Advanced VPN 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.

Korrekturen / Anpassungen

→ **Neue Verzeichnisstruktur**

Aus Gründen der Betriebssicherheit und der Kompatibilität zu Windows wurde die Verzeichnisstruktur des Advanced VPN Client geändert. Verzeichnisse, die bisher im Installationsverzeichnis innerhalb „\Programme\LANCOM\Advanced VPN Client\“ erstellt wurden, sind in „\ProgramData\LANCOM\Advanced VPN Client\“ verschoben worden. Weitere Informationen zur Umstellung auf die neue Verzeichnisstruktur entnehmen Sie bitte der Datei Liesmich.txt.

→ **Erweitertes Status-Fenster „Verbindungsinformationen“**

Im Status-Fenster „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-Handling in Verbindung mit einer via Microsoft Smart Card Key Storage Provider (CSP) konfigurierten Gemalto IDPrime 830 SmartCard wurde optimiert.

→ **Optimierung des Filtertreibers**

Der Advanced VPN Filtertreiber wurde hinsichtlich des Datendurchsatzes optimiert.

→ **Optimierung der Anmeldung via Time-based OTP (one-time passwords)**

→ **Fehlerbehebung innerhalb der GUI-Skalierung**

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

6. Allgemeine Hinweise

Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de