LANCOM Release Notes
Advanced VPN Client macOS 4.61 Rel

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

Internet: http://www.lancom-systems.de

03.01.2022, CBuersch

Inhaltsübersicht

LANCOM Systems

1. Einleitung

Mit dem LANCOM Advanced VPN Client macOS 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 macOS Version 4.61 Rel sowie die Änderungen zur Vorversion.

2. Neue Features, Änderungen und Historie

Advanced VPN Client macOS Änderungen in Version 4.61 Rel Build 29053

Voraussetzungen

Apple macOS-Betriebssysteme

Folgende macOS-Betriebssysteme werden mit dieser Version auf Hardware mit Apple M1-Chip oder Intel-CPU unterstützt:

- macOS 11 Big Sur
- macOS 12 Monterey

Einschränkung in der Version 4.61 Rel

Diese Version des Clients enthält, im Gegensatz zu vorherigen Clientversionen, keine Firewallfunktionalität. Anwender, die diese Firewallfunktionalität nutzen möchten, sollten – sofern möglich – die Vorversion 4.0 des Clients nutzen.

Verbesserungen / Fehlerbehebungen

- **Split Tunneling**
  Es werden nun wieder alle Split Tunneling-Einträge korrekt vom Client ausgeführt.
- **IKEv1 Rekeying**
  Die Kompatibilität des Clients hinsichtlich des Rekeyings bei IKEv1 mit Fremdgateways wurde verbessert.

Bekannte Einschränkungen

- **Ablageort für Zertifikatsdateien**

Einhergehend mit Anpassungen für macOS Catalina können p12-Zertifikatsdateien im Client nicht von beliebigen Ablageorten genutzt werden. Im Falle der automatisch erzeugten Verzeichnisse im Home-Verzeichnis des Benutzers (z.B. Dokumente, Schreibtisch, Downloads etc.) erscheint der Fehler „Zugriff verweigert“. Werden die Zertifikatsdateien direkt in einem Verzeichnis unterhalb des Benutzer-Home-Verzeichnisses abgelegt, so funktioniert der Zugriff.

Advanced VPN Client macOS Änderungen in Version 4.60 Rel Build 29048

Voraussetzungen

Apple macOS-Betriebssysteme

Folgende macOS-Betriebssysteme werden mit dieser Version auf Hardware mit Apple M1-Chip oder Intel-CPU unterstützt:

- macOS 11 Big Sur
- macOS 12 Monterey

Einschränkung in der Version 4.60 Rel

Diese Version des Clients enthält, im Gegensatz zu vorherigen Clientversionen, keine Firewallfunktionalität. Anwender, die diese Firewallfunktionalität nutzen möchten, sollten – sofern möglich – die Vorversion 4.0 des Clients nutzen.

Neue Features

- **Unterstützung von macOS 11 Big Sur, macOS 12 Monterey sowie des Apple M1 Chip.**
  Der Client ist ab dieser Version kompatibel zum Apple M1 Chip. Als Betriebssystem werden macOS 11 Big Sur oder macOS 12 Monterey vorausgesetzt.

Verbesserungen / Fehlerbehebungen

- **Unterstützung von 250 Split-Tunnel-Netzen**
  Es werden nun für IPv4 und IPv6 bis zu 250 Split-Tunnel-Netze beim Import einer INI-Konfigurationsdatei unterstützt.
- **Unterstützung von DNS-Domains in der INI-Datei**
  DNS-Domains, die durch den VPN-Tunnel aufgelöst werden sollen, können nun auch per INI-Datei importiert werden.
- **MFA-Dialog wurde nicht vollständig angezeigt**
  Bei der Verwendung einer Multi-Faktor-Authentifizierung kam es zu Anzeigefehlern. Das bisherige Anzeigefenster war zu klein für besonders lange Texte.
- **Fehlerhaftes Caching von Domainnamen bei Profilwechsel**
  Domainnamen wurden fälschlicherweise nach Profilwechsel zwischengespeichert.
- **Konfiguration Split Tunneling: ‚Auch lokale Netze im Tunnel weiterleiten' hinzugefügt**
  Bisher war es nur im Windows-Client möglich, lokale Netze im Tunnel weiterzuleiten. Dies ist nun auch im macOS-Client möglich.
- **Ungewollte Proposal-Änderung (DH-Gruppe) nach Profilbearbeitung**
  Wurde in der INI-Konfigurationsdatei die DH-Gruppe ausschließlich in der Sektion IKEPOLICY konfiguriert, so wurde dieser Wert nach dem Bearbeiten des Profils im Client auf den Standardwert der DH-Gruppe gesetzt.
- **Konfigurationsänderung von IPv4 auf IPv6**
  Nach Umschalten im Profil von IPv4 auf IPv6 war unter Split Tunneling die IPv6-Tabelle nicht verfügbar.

- **Unterstützung von PEM- und DER-Format unabhängig von der Datei-Endung**
  Bisher wurden nur Dateien mit .pem-Dateiendung als PEM-Format gelesen, alle anderen wurden ausschließlich im binären DER-Format gelesen. Nun werden auch für .cer- und .crt-Dateiendungen das DER- bzw. PEM-Format unterstützt.
- **Fehlende Menüleiste nach Start des Rechners**
  Nach dem Start des Rechners wurde unter bestimmten Umständen die Menüleiste des Clients trotz aktiver Client-GUI im Vordergrund nicht angezeigt.
- **Fehler beim Import der Konfigurationssperren**
  Das Importieren von Konfigurationssperren via INI-Konfigurationsdatei war fehlerhaft.
- **Update auf OpenSSL Version 1.0.2u-8**
  Die im NCP Secure Client verwendete OpenSSL-Version wurde auf 1.0.2u-8 angehoben. Damit wurde die OpenSSL-Sicherheitslücke CVE-2020-1971 geschlossen.
- **Optimiertes Handling von DNS-Requests**
  Einhergehend mit dem neu implementierten Netzwerkadapter konnte das Handling von DNS-Requests verbessert werden.
- **Verbesserungen bei VPN Path Finder in Verbindung mit einem konfigurierten Proxy**
  Wurde eine VPN-Verbindung mittels Pathfinder und einem Proxy für Pathfinder hergestellt, erfolgte keine Anfrage am Proxy-Server. Durch eine Verbesserung bei der dynamischen Konfigurationsübernahme ist dies nun möglich.
- **Fehlende Hilfe**
  Im LANCOM Advanced VPN Client wurde der Hilfetext für die Funktion ‚IPsec over HTTPS Proxy' nicht angezeigt.
- **Die Benutzerrechte für das Installationsverzeichnis wurden angepasst.**
- **Absturz des ncprwsmac-Dienstes**
  In seltenen Fällen kam es zum Absturz des ncprwsmac-Dienstes.

Bekannte Einschränkungen

- **Ablageort für Zertifikatsdateien**

Einhergehend mit Anpassungen für macOS Catalina können p12-Zertifikatsdateien im Client nicht von beliebigen Ablageorten genutzt werden. Im Falle der automatisch erzeugten Verzeichnisse im Home-Verzeichnis des Benutzers (z.B. Dokumente, Schreibtisch, Downloads etc.) erscheint der Fehler „Zugriff verweigert". Werden die Zertifikatsdateien direkt in einem Verzeichnis unterhalb des Benutzer-Home-Verzeichnisses abgelegt, so funktioniert der Zugriff.

Advanced VPN Client macOS Änderungen in Version 4.00 Rel Build 46079

Voraussetzungen

Apple macOS Betriebssysteme

Folgende Apple macOS Betriebssysteme werden mit dieser Version unterstützt:

- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13

Neue Features

- **Vollständiger Support von macOS Catalina 10.15**

  Der Client ist ab dieser Version vollständig kompatibel zu macOS Catalina 10.15.

  Bei der Installation muss die zu installierende Kernelextension explizit in den Einstellungen unter Sicherheit erlaubt werden.

- **Virtueller Netzwerkadapter**

  Der Client erhält nun einen eigenen Netzwerkadapter. Dies ermöglicht u.a. VoIP-Anwendungen die Kommunikation durch den VPN-Tunnel. Des Weiteren kann der Client dank dieses Netzwerkadapters auch ein IP-Protokoll innerhalb des VPN-Tunnels nutzen, obwohl es im tatsächlich verwendeten physischen Netzwerk nicht verwendet wird. Beispiel: Nutzung von IPv6 innerhalb des VPN-Tunnels, obwohl im angeschlossenen Netzwerk nur IPv4 vorhanden ist.

- **Verbinden/Trennen-Menü im Dock-Icon**

  Verfügt der VPN-Client über ein konfiguriertes VPN-Profil, so kann die ausgewählte Verbindung durch Rechtsklick auf das Dock-Menü-Icon aufgebaut bzw. getrennt werden.

Verbesserungen / Fehlerbehebungen

- **Optimiertes Handling von DNS-Requests**

  Einhergehend mit dem neu implementierten Netzwerkadapter kann das Handling von DNS-Requests verbessert werden. Dabei sind folgende zwei Fälle zu unterscheiden:

  1. Kein Split Tunneling-Betrieb

  In diesem Betriebsmodus geschieht jegliche Kommunikation zu anderen IP-Adressen, die nicht innerhalb des aktuell verwendeten IP-Adressbereiches liegen, durch den VPN-Tunnel. Dies gilt demzufolge ebenso für DNS-Requests.

  2. Split-Tunneling Betrieb

  In diesem Betriebsmodus wird/werden innerhalb der Split-Tunneling-Konfiguration das oder die IP-Remotenetzwerk(e) definiert. Werden nun Ziele innerhalb des Remotenetzwerks adressiert, so fließen die Daten durch den VPN-Tunnel. Alle anderen Daten, insbesondere auch DNS-Requests fließen am VPN-Tunnel vorbei. Dadurch lassen sich Ziele im Remotenetzwerk zunächst nicht über ihren Domainnamen erreichen, denn typischerweise lösen allgemein erreichbare DNS-Server keine firmeninternen DNS-Namen auf.

Dieses Problem lässt sich durch die explizite Konfiguration der internen Domainnamen, die innerhalb des Remotenetzwerkes liegen, lösen.

So bewirkt der Eintrag ‚firma.local', dass entsprechende DNS-Requests, z.B. ‚intranet.firma.local', durch den VPN-Tunnel an firmeninterne DNS-Server fließen.

Durch diese Konfigurationsoption lässt sich der Datenverkehr durch den VPN-Tunnel und am VPN-Tunnel vorbei komplett trennen.

- **Neuer Verbindungsmodus**

  Der Verbindungsmodus „automatisch" wurde entfernt und dafür der Modus „immer" hinzugefügt. Ist „immer" konfiguriert, so versucht der Client zu jeder Zeit, einen VPN-Tunnel aufzubauen. Dies geschieht im Unterschied zum Modus „automatisch" ohne anliegende, zu versendende Daten.

Bekannte Einschränkungen

- **Ablageort für Zertifikatsdateien**

Einhergehend mit Anpassungen für macOS Catalina können p12-Zertifikatsdateien im Client nicht von beliebigen Ablageorten genutzt werden. Im Falle der automatisch erzeugten Verzeichnisse im Home-Verzeichnis des Benutzers (z.B. Dokumente, Schreibtisch, Downloads etc.) erscheint der Fehler „Zugriff verweigert". Werden die Zertifikatsdateien direkt in einem Verzeichnis unterhalb des Benutzer-Home-Verzeichnisses abgelegt, so funktioniert der Zugriff.

Advanced VPN Client macOS Änderungen in Version 3.20 Rel Build 43098

Voraussetzungen

Apple macOS Betriebssysteme

Folgende Apple macOS Betriebssysteme werden mit dieser Version unterstützt:

- macOS Mojave 10.14
- macOS High Sierra 10.13
- macOS Sierra 10.12

Ab dieser Version entfällt der Support für OS X Yosemite 10.10 und OS X El Capitan 10.11.

Neue Features

- **IPv6-Unterstützung**

  Der Client unterstützt nun den Dual Stack-Betrieb. Hierfür kann in der Konfiguration IPv4 only, IPv6 only oder beides ausgewählt werden. Des Weiteren kann die Split Tunneling-Konfiguration für beide Protokolle individuell erfolgen.

- **Dark Mode-Unterstützung**

  Die Client GUI unterstützt nun den mit macOS Mojave eingeführten Dark Mode.

- **macOS Schlüsselbund-Unterstützung**

  Ein Benutzerzertifikat lässt sich innerhalb der Computer-Zertifikats-Konfiguration zur Verwendung im macOS Schlüsselbund konfigurieren. Dazu ist der vorherige Import des Zertifikates in den System-Schlüsselbund erforderlich. Für den im Zertifikat enthaltenen privaten Schlüssel ist der Zugriff durch den NCP-Dienst ncprwsmac im Verzeichnis /Library/Application Support/NCP/Secure Client/ freizugeben.

Korrekturen / Anpassungen

- **Anpassung der Deinstallationsroutine in macOS Mojave**

  Bei der Deinstallation wurde vom Benutzer ggf. die Erlaubnis zum Zugriff auf das Adressbuch, Kalender und Fotos erfragt. Wenngleich die Deinstallationsroutine nie auf die genannten Daten zugegriffen hat, so wurde dieses Verhalten nun behoben. Ebenso wird das Applikations-Icon nach der Deinstallation korrekt aus dem Dock entfernt.

Advanced VPN Client macOS Änderungen in Version 3.10 Rel Build 40218

Neue Features

- **Biometrische Authentisierung (Fingerabdruck-Erkennung) vor VPN-Verbindungsaufbau**

  Zur Absicherung vor einem VPN-Verbindungsaufbau durch nicht autorisierte Dritte wurde im Advanced VPN Client eine biometrische Authentisierung integriert. Direkt nach dem Klick auf den „Verbinden"-Button in der Client-GUI erfolgt die Aufforderung zur Benutzerauthentisierung. Der VPN-Verbindungsaufbau wird daraufhin erst nach positiver Authentisierung gestartet. Voraussetzung für die biometrische Authentisierung ist macOS Sierra 10.12.1 oder neuer. Sofern keine Apple-Hardware mit integriertem Fingerabdrucksensor verwendet wird, wird bei aktivierter Option das Benutzerpasswort abgefragt.

Korrekturen / Anpassungen

- **OTP-Funktionalität**

  Die Dialogbox zur Eingabe des OTP-Passcodes wurde nicht angezeigt. Dieser Fehler wurde behoben.

- **Zertifikats-Fingerprint**

  In der Zertifikatsansicht wurde der Fingerprint eines Zertifikates nicht angezeigt. Ein Abgleich des Fingerprints zur Überprüfung eines Zertifikates konnte nicht stattfinden. Dieser Fehler wurde behoben.

Bekannte Einschränkungen

- Unter OS X Yosemite 10.10 kann der FIPS-Modus nicht eingeschaltet werden.

Advanced VPN Client macOS Änderungen in Version 3.00 RU1 Build 38902

Korrekturen / Anpassungen

- **Optimierter Start der Systemdienste**
  Eine hohe Anzahl an verbauten Netzwerkadaptern konnte dazu führen, dass der Start des VPN Clients fehlschlug.

Advanced VPN Client macOS Änderungen in Version 3.00 Rel Build 37856

Neue Features

- **Unterstützung von macOS High Sierra 10.13**
  Das Apple-Betriebssystem macOS High Sierra 10.13 wird nun umfänglich unterstützt.
- **Unterstützung für IKEv2 und IKEv2 Redirect**
  Der Client unterstützt ab dieser Version IKEv2 und IKEv2 Redirect. Mittels IKEv2 Redirect ist es möglich, den Advanced VPN Client auf ein anderes Gateway umzuleiten. Ideal für eine effiziente Lastverteilung in Umgebungen, in denen mehrere Gateways eingesetzt werden.
- **Unterstützung des FIPS-Modus**
  Der Client kann innerhalb der Installationsroutine FIPS-konform installiert werden. FIPS (Federal Information Processing Standard) ist die Bezeichnung für öffentlich bekanntgegebene Sicherheitsstandards der Vereinigten Staaten, deren Erfüllung erforderlich ist, sofern der Client dort eingesetzt wird. Ist der FIPS-Modus aktiviert, werden alle Verbindungen mit Algorithmen aufgebaut, die den FIPS-Standard erfüllen.
- Modernisierung der grafischen Oberfläche des Clients

Korrekturen / Anpassungen

- **Verbesserung der DPD-Funktionalität**
  Die Dead-Peer-Detection zur Verbindungsüberwachung von VPN-Verbindungen wurde allgemein verbessert.

Advanced VPN Client macOS Änderungen in Version 2.05 RU1 Build 32167

Neue Features

- Unterstützung von macOS Sierra 10.12

Bekannte Einschränkungen

- Eine Online-Aktivierung ist nicht möglich, wenn der 30-tägige Testzeitraum überschritten wurde. Die Aktivierung muss in diesem Fall offline durchgeführt werden.
  (siehe: https://www.lancom-systems.de/service-support/registrierungen/software/aktivierung/)

Advanced VPN Client macOS Änderungen in Version 2.05 Rel Build 23310

Neue Features

- Verbesserung der Kompatibiltät zu OS X Yosemite 10.10

Korrekturen / Anpassungen

- Der NCP Dienst wird beim Systemstart wieder mitgestartet.

Advanced VPN Client macOS Änderungen in Version 2.05 Rel Build 14711

Neue Features

- Unterstützung vom OS X Mavericks 10.9 (Mindestvoraussetzung OS X Mountain Lion 10.8)

Korrekturen / Anpassungen

- Wird die SmartCard während des Betriebs entfernt, wird der bestehende VPN-Tunnel nicht mehr getrennt.

Advanced VPN Client macOS Änderungen in Version 2.02 Rel Build 0014

Neue Features

- DNS-Anfragen für eine Domäne können unabhängig von Split-Tunneling durch den VPN-Tunnel aufgelöst werden.

Korrekturen / Anpassungen

- Die Profilauswahl in der Client-Oberfläche wurde verbessert.
- Beim Einsatz einer externen xAUTH Authentisierung werden die Dialoge zur zentralseitigen Passwortabfrage richtig angezeigt.

Advanced VPN Client macOS Änderungen in Version 2.02 Rel Build 0011

Korrekturen / Anpassungen

- Der LANCOM Advanced VPN Client kann unter OS X Lion 10.7 verwendet werden.
- Die Pfadangabe für das PKCS#11 Modul wurde auf 250 Zeichen erweitert.

Advanced VPN Client macOS Änderungen in Version 2.01 Rel Build 0047

Neue Features

- Im LANCOM Advanced VPN Client werden Konfigurationstips und Anwendungsbeispiele gezeigt. Mit einem Mausklick in dieses Feld werden weitere Informationen im Browser angezeigt.
- Der LANCOM Advanced VPN Client kann dauerhaft in die Menüleiste minimiert werden.
- Für die 802.1x Authentisierung im LAN unterstützt der LANCOM Advanced VPN Client EAP (Extensible Authentication Protocol).
- Im VPN-Profil kann hinterlegt werden, ob die DNS-Auflösung durch den Tunnel oder über den DNS-Server des Providers geschieht.
- Wird im OS X ein WEB Proxy-Server ohne Passwort-Authentisierung verwendet, wird dies bei der Online-Aktivierung erkannt.

Korrekturen / Anpassungen

- Probleme beim Import von Profilen wurden behoben.

Advanced VPN Client macOS Änderungen in Version 1.01 Rel Build 0010

Korrekturen / Anpassungen

- Auch nach einem lang andauernden Systemstart (z.B. durch Löschen des System Caches) bleibt die Firewall des LANCOM Advanced VPN Clients weiterhin aktiv.
- Eine vom OS X aufgebaute Internetverbindung über PPPoE (z.B. UMTS) kann für den VPN Verbindungsaufbau genutzt werden.
- Der LANCOM Advanced VPN Client kann nur einmal auf einem Rechner gestartet werden. So wird verhindert, dass bei einem schnellen Benutzerwechsel Einstellungen des ersten Benutzers überschrieben werden. Die VPN Verbindung bleibt beim schnellen Benutzerwechsel bestehen.
- Die Zuordnung der IP-Adressen bei einem Profilimport wurde korrigiert.
- Wird der LANCOM Advanced VPN Client hinter einem NAT-Gerät genutzt, verhindern die IKE Keepalive Pakete nicht den Abbau der Verbindung durch den manuell konfigurierten Timeout.
- Das Firewall-Log wird auch dann weiter geführt, wenn ein Netzwerkadapter entfernt bzw. eine PPP-Verbindung beendet wurde.
- Die Fehlermeldungen im Log-Fenster wurden überarbeitet.
- Eine nach dem Programmstart initiierte Zertifikatsverbindung kann auch dann aufgebaut werden, wenn zuvor das voreingestellte Profil nicht gewechselt wurde.

LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems