Informationen zum

Advanced VPN Client macOS 3.10 Rel

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Würselen
Germany

Internet: http://www.lancom.de

23.07.2018, CBuersch

Inhaltsübersicht

1. Einleitung

Dieses Dokument beschreibt die Neuerungen des LANCOM Advanced VPN Client macOS Version 3.10 Rel sowie die Änderungen zur Vorversion.

2. Neue Features, Änderungen und Historie

Änderungen von Version 3.00 RU1 Build 38902 ► 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.

Änderungen von Version 3.00 Rel Build 37856 ► 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.

Änderungen von Version 2.05 RU1 Build 32167 ► 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.

Änderungen von Version 2.05 Rel Build 23310 ► 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/)

Änderungen von Version 2.05 Rel Build 14711 ► 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.

Änderungen von Version 2.02 Rel Build 0014 ► 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.

Änderungen von Version 2.02 Rel Build 0011 ► 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.

Änderungen von Version 2.01 Rel Build 0047 ► 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.

Änderungen von Version 1.01 Rel Build 0010 ► 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.

Änderungen von Version 1.00 Rel Build 0078 ► 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.

