LANCOM
Systems

Information regarding

LANCOM Advanced VPN Client macOS 3.10 Rel

Copyright (c) 2002-2018 LANCOM Systems GmbH, Wuerselen (Germany)

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

Mac and macOS are trademarks of Apple Inc. registered in the U.S. and other countries.

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

23.07.2018, CBuersch

Table of Contents

1. Preface

This document describes the innovations within the LANCOM Advanced VPN Client macOS 3.10 Rel, as well as the improvements since the previous version.

2. New features, improvements, and history

Improvements version 3.00 RU1 Build 38902 ► 3.10 Rel Build 40218

New features

› Biometric authentication (fingerprint recognition) before VPN connection establishment
For protection against a VPN connection establishment by unauthorized third parties a biometric authentication has been added to the Advanced VPN Client. Immediately after pressing the "Connect" button in the client GUI there is a prompt for user authentication. The VPN connection is only established after a positive authentication. Required for biometric authentication is macOS Sierra 10.12.1 or later. If this option is enabled but no Apple hardware with integrated fingerprint sensor is used, the user password is required instead.

Bugfixes / improvements

› OTP functionality
The dialogue box for entering the OTP pass code was not displayed. This bug has been fixed.
› Certificate fingerprint
The fingerprint of a certificate was not displayed within the certificate view. A comparison of the fingerprint for certificate checking could not happen. This bug has been fixed.

Known issues

› Under OS X Yosemite 10.10 the FIPS mode cannot be activated.

Improvements version 3.00 Rel Build 337856 ► 3.00 RU1 Build 38902

Bugfixes / improvements

> Optimized start of system services
> A bigger amount of installed network adapters could cause a failure when trying to start the VPN client.

Improvements version 2.05 RU1 Build 32167 ► 3.00 Rel Build 37856

New features

> Support for macOS High Sierra 10.13
> The Apple operating system macOS High Sierra 10.13 is now fully supported.
> Support for IKEv2 and IKEv2 Redirect
> As from this version, the client supports IKEv2 and IKEv2 Redirect. Using IKEv2 Redirect, it is now possible to forward the Advanced VPN Client to another gateway. Ideal for efficient load balancing in environments where multiple gateways are deployed.
> Support for FIPS mode
> The client can be installed with Federal Information Processing Standard (FIPS) conformity using the installation routine. FIPS is the term used to describe publicly disclosed United States security standards that are required to be enforced if the client is used in the U.S. With activated FIPS mode all connections are established with algorithms obeying the FIPS standard.
> Modernized graphical user interface of the client

Bugfixes / improvements

> Improved DPD functionality
> The Dead-Peer-Detection for VPN connection monitoring has been generally improved.

Improvements version 2.05 Rel Build 23310 ► 2.05 RU1 Build 32167

New features

> Support for macOS Sierra 10.12

Known issues

> An online activation is not possible if the 30-day test period has been exceeded. The activation has to be done offline in that case.
> (see: https://www.lancom-systems.com/service-support/registrations/software/activation/)

Improvements version 2.05 Rel Build 14711 ▶ 2.05 Rel Build 23310

New features

> Compatibility improvements for OS X Yosemite 10.10

Bugfixes / improvements

> The NCP service is also started again at system startup.

Improvements version 2.02 Rel Build 0014 ▶ 2.05 Rel Build 14711

New features

> Support for OS X Mavericks (10.9) (minimum requiremets OS X Mountain Lion 10.8)
>

Bugfixes / improvements

> If the smartcard is removed during operation, an existing VPN tunnel is not disconnected.

Improvements version 2.02 Rel Build 0011 ▶ 2.02 Rel Build 0014

New features

> DNS requests for a domain can be resolved through a VPN tunnel independent from split tunneling.

Bugfixes / improvements

> Improved profile selection on the client user interface
> When using external xAUTH authentication the dialogues for central site password query are displayed correctly.

Improvements version 2.01 Rel Build 0047 ▶ 2.02 Rel Build 0011

Bugfixes / improvements

> The LANCOM Advanced VPN Client can be used under OS X Lion 10.7.
> Path extension to 250 characters for the PKCS#11 module

Improvements version 1.01 Rel Build 0010 ▶ 2.01 Rel Build 0047

New features

> The LANCOM Advanced VPN Client shows usage examples and configuration hints.
> By clicking the information additional details will be displayed in a browser.
> The LANCOM Advanced VPN Client can be minimized permanently.
> EAP support (Extensible Authentication Protocol) for 802.1x authentication in a LAN
> Each VPN profile can be configured to either use the providers DNS server or the one accessible through the VPN tunnel.
> Automatic WEB proxy server recognition without password authentication during online activation when using OS X

Bugfixes / improvements

> Solved problems when importing profiles

Improvements version 1.00 Rel Build 0078 ▶ 1.01 Rel Build 0010

Bugfixes / improvements

> The firewall of the LANCOM Advanced VPN client remains active even after a long-lasting system boot (e.g. due to deleting the system cache).
> An internet connection established by OS X via PPPoE (e.g. UMTS) can be used for VPN connection establishment.
> LANCOM Advanced VPN Client can only be started once at a time on the same computer. This avoids overwriting settings of the first user on quick user changes. The VPN connection remains established.
> Fixed the IP address assignment when importing profiles.
> If the LANCOM Advanced VPN Client is used behind a NAT device, the IKE keepalive packets do not avoid link disconnection by manually configured timeouts.
> The firewall log is continued, even if a network adapter is removed or a PPP connection is terminated.
> Reworked error messages in the log window
> A certificate connection which was initialized after application start can be established even if the preset profile was not changed before.