LANCOM Advanced VPN Client macOS

Universal VPN Software Client for secure corporate network access when traveling

The LANCOM Advanced VPN Client provides mobile employees with encrypted access to the company network, whether they are at their home office, on the road, or even abroad. The application is extremely easy to use; once VPN access (virtual private network) has been configured, a click of the mouse is all it takes to establish a secure VPN connection. Further data protection comes with the integrated stateful inspection firewall, support of all IPSec protocol extensions, and numerous other security features.

> IPSec VPN Client for macOS
> Integrated stateful inspection firewall for secure internet access
> Prioritization of Voice over IP
> IPSec over HTTPS (based on NCP VPN Path Finder Technology)
> Support of IKEv2
> Biometric authentication

LANCOM
Systems

LANCOM Advanced VPN Client macOS

Secure company network access when traveling

The LANCOM Advanced VPN Client for macOS provides users with a secure VPN tunnel to access the company network. No matter whether the user is mobile on the road, in the home office, or even abroad — the LANCOM Advanced VPN Client provides a secure channel to the company network, anytime and anywhere.

Maximum data security

Equipped with a stateful inspection firewall, the LANCOM Advanced VPN Client automatically detects secure and unsecure networks for protected communication at all times. Together with other security features such as the support of all current IPSec protocols, digital certificates, and many more, the client ensures that all data are securely transmitted at all times.

Fast and easy configuration thanks to the Setup Wizard and "1-Click-VPN"

The integrated Setup Wizard in LANconfig supports the user with fast and easy VPN configuration. Once the VPN connection is established intuitively with a single click.

LANCOM
Systems

LANCOM Advanced VPN Client macOS

Operating systems	
Apple	> macOS Mojave 10.14 > macOS High Sierra 10.13 > macOS Sierra 10.12 > OS X El Capitan 10.11 > OS X Yosemite 10.10 > OS X Mavericks 10.9 (up to version 2.05 RU1) > OS X Mountain Lion 10.8 (up to version 2.05 RU1) > Mac OS X Lion 10.7 (up to version 2.05 RU1) > Mac OS X Snow Leopard 10.6 (up to version 2.05 RU1) > Mac OS X Leopard 10.5 (up to version 2.05 RU1)
Languages	German, English

Communication	
Connection management	Communication only via secured VPN tunnel or with simultaneous unsecured Internet access. Manual or automatic connection establishment, adjustable hold-times with automatic connection establishment, time and connection limit with warning.
Connection types	VPN connection over existing IP connection (LAN / WLAN)
Protocols	All IP-based protocols

VPN/IPsec	
Standards	Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header)
FIPS inside	The IPSec client integrates an cryptographic algorithm conformant to the FIPS standard. The embedded cryptographic module is certified according to FIPS 140-2 (Certificate #1051). FIPS conformance will always be maintained when any of the following algorithms are used for establishment and encryption of the IPsec connection: Diffie Hellman Group: Group 2 or higher (DH starting from a length of 1024 bits) Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES
Encryption	AES-CBC/AES-CTR/AES-GCM (128, 192 or 256 bit), 3-DES (168 bit), RSA (1024 or 2048 bit)
Hashes	SHA-512, SHA-384, SHA-256, SHA-1, MD-5
IKE operating modes	IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, IKEv2, DH groups 1, 2, 5, 14-21, 25-30, Re-keying after adjustable transfer volumes or time. In combination with LANCOM VPN remote sites, an IKE extension enables separate pre-shared keys to be used for each user in Aggressive Mode as well.

Additional functions	
IPSec over HTTPS	To overcome VPN filter (e.g. port 500 blocking for IKE). LANCOM VPN router and gateways with LCOS 8.0 or higher needed. IPSec over HTTPS is based on the NCP VPN Path Finder Technology.
XAUTH	For authentication by username/password
IKE config mode	For assignment of IP parameters (local IP address, DNS and WINS server) to the client
IPCOMP	IPCOMP data compression (LZS and Deflate) for optimal bandwidth exploitation
Dead-Peer-Detection	Dead-peer detection (DPD) for connection monitoring
IKE redirect	Support for IKE redirect according to RFC 5685
NAT-Traversal	NAT-Traversal (NAT-T) to overcome routers not capable of IPSec masking, or when using AH
RAS user template	Configuration of all VPN client connections in IKE ConfigMode via a single entry in the LANCOM VPN gateway
EAP-MD5	For extended authentication of layer-2 devices such as switches or WLAN access points
Biometric authentication	Secure against unauthorised access by third parties via biometric authentication (fingerprint detection).

PKI	
Certificates	Public Key Infrastructure according to X.509v3, Entrust SmartCards: PKCS#11, TCOS 1.2 and 2.0 over CT-API or PC/SC Soft certificates: PKCS#12
Certificate extension	Control of, and notice about, a certificate's validity period
Certificate revocation lists (CRL)	Control of the CRL and ARL (Certificate and/or Authority Revocation List)
One-Time Password	Convenient entry through separated PIN and password

LANCOM
Systems

LANCOM Advanced VPN Client macOS

Firewall	
Stateful inspection Firewall	Stateful inspection firewall for IPv4 and IPv6, direction-dependant packet filter with IP- and port ranges per protocol, LAN-adapter protection to protect PCs with active VPN connections from attacks from other LAN users, IP broadcast and NetBIOS/IP filter
Installation	
Wizards	Tailor-made Setup Wizards are available for all types of connection
Administration	
Password protection	Password protection for configuration and profile management, configuration rights can be defined for each function area, display/hide parameter fields
Network diagnostics	Easy checking of internet accessibility through PING and DNS request
Activation / Deactivation	
Online/offline activation	After installation, the software will function for a period of 30 days. Activation must take place within these 30 days. This can be conducted either directly online (requiring Internet access from the corresponding computer) or offline (requiring Internet access from any other computer). Activation is anonymous. No user-specific data of any kind is transmitted.
License	The licenses for the LANCOM Advanced VPN Client are single-device licenses and may only be activated and operated on one system at a time.
Updates	
Update	An update to a later version is generally available for free and can be carried out without purchasing a new license key. An update provides all of the previous bugfixes from earlier versions.
Upgrade	With an upgrade to the current version, users of older versions can take advantage of the new features in the current version. An upgrade is subject to a fee and requires a new upgrade license key to be purchased, along with a new activation. Upgrades are only possible with a maximum of 2 software versions between the version that was activated originally and the current version. Please visit www.lancom-systems.com/avc-mac for details.
Support	
Support	Support via Internet
Service	30-day demo version from www.lancom-systems.com
Package content	
Manual	Printed Quick Installation Guide (DE/EN)
Key	Printed license key
Item numbers	
Item no. 61606	LANCOM Advanced VPN Client macOS
Item no. 61607	LANCOM Advanced VPN Client macOS (10 Bulk)
Options	
Item no. 61608	LANCOM Upgrade Advanced VPN Client macOS (for activating the new functions up to two major releases)
Item no. 61609	LANCOM Upgrade Advanced VPN Client macOS (10 bulk) (for activating the new functions up to two major releases)