

LANCOM Advanced VPN Client Mac OS X

Universal VPN Software Client

- High-security, encrypted corporate network access when travelling
- Integrated stateful inspection firewall
- Support of all IPsec protocol extensions
- IPsec over HTTPS (based on NCP Path Finder Technology)



LANCOM Advanced VPN Client Mac OS X

Mac OS 10.5 Elepard	Operating systems	
Mac OS 10.5 Show's Lepard	Microsoft Windows	
LANCOM Advanced VPN Client Version 2.05 Mac OS 10.3 Mountain Lion Mac OS 10.11 El Capatan Connection management Communication connection stabilishment, adjustable hold-times with automatic connection establishment. VPN Lonnection over existing IP connection All IP-based protocols All IP-based protocols Standards Standard Conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) Encryption 3-DES (168 bit), AES (178, 192 or 256 bit), Blowfish (128 bit), SAS (1024 or 2048 bit) Hashes MD-5, SIA-1, SIA-256, SIA-384 and SIA-512 IKE operating modes IKE with precibared keys or certificates, KK Main or Aggressive Mode, DH groups 1, 2, 5, and 14. Be-keying after adjustable transfer volumes of time. In combination with LANCOM VPN remotes sites, an IKE extension enables separate pre-shared keys to be used for each user in Aggressive Mode as well. Additional functions IPSec over HTITS To overcome VPN filter (e.g. port 500 blocking for IKE). LANCOM VPN recuter and gateways with LCOS 8.0 or higher needed PSec over HTITS is based on the ICV VPN Path Finder Technology. Kauth For authentication by username/password IKE config mode For authentication by username/password For authentication by username/password For authentication by username/password For extended authentication of layer-2 devices such as switches or WLAN access points PKI Certificate retrepiate Configuration of all VPN client connection monitoring NAI-Traversal (NAI-T) to overcome routers not capable of IPSec mask		Mac OS 10.6 Snow Leopard
# Mac OS 10.9 Maverrics # Mac OS 10.1 Wosemite # Mac OS 10.1 El Capitan # Mac O		
* Mac OS 10.1 Bl Capitan * Mac OS 10.1 Bl Capitan * Mac OS 10.1 Bl Capitan * Mac OS Sierra German and English Communication Commection management Communication only via secured VPN tunnel or with simultaneous unsecured Internet access. Manual or automatic connection establishment. Connection types VPN connection over existing IP connection VPN WIPSec Standards Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-S, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes WK with preshared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. Re-keying after adjustably transfer volumes of time. In combination with LANCOM VPN remote sites, an IKE extension enables separate pre-shared key to be used for each user in Aggressive Mode as well. Additional functions IPSec over HTIPS 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 HTIPS is based on the NCP VPN Path Finder Technology. X auth For authentication by username/password KE config mode For assignment of IP parameters (local IP address, DNS and WINS server) to the client IPCOMP IPCOMP data compression (LZS) for optimal bandwidth exploitation Dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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-NDS For extended authentication of layer-2 devices such as switches or WLAN access points PKK Certificate extension Control of, and notice about, a certificate's validity period Certificate revocation lists (CRL) Control of the CRL and ARL (Certificate andior Authority Revocation List) One-Time Password Convenient entry through separated PI		Mac OS 10.8 Mountain Lion
anguages Germa and English Communication Connection management Communication only via secured VPN tunnel or with simultaneous unsecured Internet access. Manual or automatic connection stabilishment, adjustable hole-times with automatic connection establishment. VPN connection very existing IP connection Protocols All IP-based protocols All IP-based protocols Standards Standard conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) Standards Standards Standard conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) Bencyption 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes WE with preshared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. Re-keying after adjustable transfer violumes or time. In combination with ILAN COM 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 remote sites, an IKE extension enables separate pre-shared keys to be used for each user in Aggressive Mode as well. X. auth For authentication by username/password For authentication by username/password For authentication by username/password For authentication by username/password KE config mode For assignment of IP parameters (local IP address, DNS and WINS server) to the client IPCOMP IPCOMP IPCOMP Pach-peer detection (DPD) Dead-peer detection (DPD) De		
Communication Connection management Communication only via secured VPN tunnel or with simultaneous unsecured Internet access. Manual or automatic connection stablishment. VPN connection vere visiting IP connection Protocols All IP-based protocols All IP-based protocols Standards Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) Encryption 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. PSec 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. X auth For authentication by username/password KE config mode For assignment of IP parameters (local IP address, DNS and WINS server) to the client IPCOMP IPCOMP (IPCOMP data compression (LZS) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 For extended authentication of layer-2 devices such as switches or WLAN access points PXI Certificate sevenation (St (RL) Control of, and notice about, a certificate's validity period Certificate extension Control of, and notice about, a certificate's validity period Convenient entry through separated PIN and password Firewall Stateful inspection firewall, direction-dependant packet filter with IP- and port tranges per pr		
Connection management Connection management Connection types VPN connection establishment, adjustable hold-times with automatic connection establishment. VPN connection were stisting IP connection Protocols All IP-based protocols All IP-based protocols Standard's Standard's Standard's Standard's Standard's Standard's Standard'-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. PSec over HTIPS 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 HTIPS is based on the N.CP VPN Path finder Technology. X. auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection of all VPN client connection monitoring NA1-Traversal NA1-Traversal (NA1-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 FAP-MD5 For extended authentication of layer-2 devices such as switches or WLAN access points With Control of, and notice about, a certificate's validity period 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	Languages	German and English
connection types VPN connection over existing IP connection Protocols All IP-based protocols All IP-based protocols Standards Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) Encryption 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SIHA-1, SIHA-256, SIHA-384 and SIHA-512 IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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 HITPS 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 HITPs is based on the NCP VPN Path Finder Technology. X. auth For authentication by username/password For assignment of IP parameters (local IP address, DNS and WINS server) to the client IPCOMP IPCOMP data compression (LZS) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring NAT-Traversal NAT-Traversal (NAT-1) to overcome routers not capable of IPSec masking, or when using AH Configuration of all VPN client connections in IKE ConfigMode via a single entry in the LANCOM VPN gateway EAP-MDS For extended authentication of layer-2 devices such as switches or WLAN access points PKI Certificate extension Control of, and notice about, a certificate's validity period Certificate revocation lists (CRI) Control of the CRI and ARL (Certificate and/or Authority Revocation List) One-Time Password Convenient entry through separated PIN and password Firewall Stateful inspection firewall, 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 Net6/OS/IP filter Installation	Communication	
Protocols All IP-based protocols VPN/IPSec Standards Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. X auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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-MDS For extended authentication of layer-2 devices such as switches or WLAN access points PKI 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 Firewall Stateful inspection firewall, 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	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.
Standards Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) Standards Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. X.auth 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 (IZS) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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-MDS For extended authentication of layer-2 devices such as switches or WLAN access points PKI Certificate Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support Certificate extension Control of, and notice about, a certificate's validity period Control of, and notice about, a certificate's validity period Control of, one-Time Password Convenient entry through separated PIN and password Firewall Stateful inspection firewall, direction-dependant packet filter with IP- and port ranges per protocol, LAN-adapter protection to protect PCs with active VPN connections from attacks	Connection types	VPN connection over existing IP connection
Standards Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header) 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. PSec 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. X. auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support Certificate revocation lists (CRL) Control of the CRL and ARL (Certificate and/or Authority Revocation List) One-Time Password Control of and notice about, a certificate's validity period Control of protect PCs with active VPN connections from attacks from other LAN users, IP broadcast and NetBiOS/IP filter Installation	Protocols	All IP-based protocols
Encryption 3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit) Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. PSec 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 [PSec over HTTPS is based on the NCP VPN Path Finder Technology. X. auth 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) for optimal bandwidth exploitation Dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificate Public Key Infrastructure according to X.509v3, PKCS#12 Support Certificate extension Control of, and notice about, a certificate's validity period Control of, and notice about, a certificate's validity period Control of the CRL and ARL (Certificate and/or Authority Revocation List) One-Time Password Convenient entry through separated PIN and password Firewall Stateful inspection firewall, 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	VPN/IPSec	
Hashes MD-5, SHA-1, SHA-256, SHA-384 and SHA-512 IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. PSec 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. X. auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificate Public Key Infrastructure according to X.509v3, PKCS#12 Support Certificate extension Control of, and notice about, a certificate's validity period Control of the CRL and ARL (Certificate and/or Authority Revocation List) One-Time Password Convenient entry through separated PIN and password Firewall Stateful inspection firewall, 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	Standards	Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header)
IKE operating modes IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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. X. auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	Encryption	3-DES (168 bit), AES (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024 or 2048 bit)
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. X. auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	Hashes	MD-5, SHA-1, SHA-256, SHA-384 and SHA-512
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. X. auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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-MDS For extended authentication of layer-2 devices such as switches or WLAN access points PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	IKE operating modes	IKE with pre/shared keys or certificates, IKE Main or Aggressive Mode, DH groups 1, 2, 5, and 14. 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.
IPSec over HTTPS is based on the NCP VPN Path Finder Technology. X. auth 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) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	Additional functions	
IKE config mode For assignment of IP parameters (local IP address, DNS and WINS server) to the client IPCOMP IPCOMP data compression (LZS) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	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.
IPCOMP data compression (LZS) for optimal bandwidth exploitation dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	X.auth	For authentication by username/password
dead-peer detection (DPD) Dead-peer detection (DPD) for connection monitoring 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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	IKE config mode	For assignment of IP parameters (local IP address, DNS and WINS server) to the client
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 PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	IPCOMP	IPCOMP data compression (LZS) for optimal bandwidth exploitation
RAS user template Configuration of all VPN client connections in IKE ConfigMode via a single entry in the LANCOM VPN gateway For extended authentication of layer-2 devices such as switches or WLAN access points PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	dead-peer detection (DPD)	Dead-peer detection (DPD) for connection monitoring
For extended authentication of layer-2 devices such as switches or WLAN access points PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	NAT-Traversal	NAT-Traversal (NAT-T) to overcome routers not capable of IPSec masking, or when using AH
PKI Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	RAS user template	Configuration of all VPN client connections in IKE ConfigMode via a single entry in the LANCOM VPN gateway
Certificates Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support 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 Firewall Stateful inspection firewall, 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	EAP-MD5	For extended authentication of layer-2 devices such as switches or WLAN access points
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 Firewall Stateful inspection firewall, 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	PKI	
Certificate revocation lists (CRL) Control of the CRL and ARL (Certificate and/or Authority Revocation List) Convenient entry through separated PIN and password Firewall Stateful inspection firewall, 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	Certificates	Public Key Infrastructure according to X.509v3, PKCS#11, PKCS#12 Support
One-Time Password Convenient entry through separated PIN and password Firewall Stateful inspection firewall, direction-dependent 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	Certificate extension	Control of, and notice about, a certificate's validity period
Stateful inspection firewall, 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	Certificate revocation lists (CRL)	Control of the CRL and ARL (Certificate and/or Authority Revocation List)
Stateful inspection firewall, 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	One-Time Password	Convenient entry through separated PIN and password
to protect PCs with active VPN connections from attacks from other LAN users, IP broadcast and NetBIOS/IP filter Installation	Firewall	
		Stateful inspection firewall, 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
Wizards Tailor-made Setup Wizards are available for all types of connection	Installation	
	Wizards	Tailor-made Setup Wizards are available for all types of connection
Administration	Administration	
Password protection Password protection for configuration and profile management, configuration rights can be defined for each function area, display/hide parameter fields	Password protection	Password protection for configuration and profile management, configuration rights can be defined for each function area, display/hide parameter fields

LANCOM, LANCOM Systems and LCOS are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. Subject to change without notice. No liability for technical errors and/or omissions.

LANCOM Advanced VPN Client Mac OS X

Activation	
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 Mac) or offline (requiring Internet access from any other MaC). Activation is anonymous. No user-specific data of any kind is transmitted.
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.
Support	
Support	Support via hotline and Internet
Service	30-day demo version from www.lancom.de
Package content	
Manual	Printed Quick Installation Guide (DE/EN)
CD	Software CD
Key	Printed license key
Item numbers	
Item no. 61606	LANCOM Advanced VPN Client Mac, for Mac OS 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11 and 10.12
Item no. 61607	LANCOM Advanced VPN Client Mac (10 Bulk), for Mac OS 10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11 and 10.12

