



. . . c o n n e c t i n g y o u r b u s i n e s s . . .

LANCOM Advanced VPN Client (WIN)

Universal VPN Software Client for secure corporate network access when traveling

- IPsec VPN Client for Windows XP, Windows Vista, Windows 7 (32 and 64 Bit)
- Integrated stateful inspection firewall for secure internet access
- Integrated UMTS-Dialer with budget manager for full cost control
- Prioritization of Voice over IP
- IPsec over HTTPS (based on NCP VPN Path Finder Technology)
- FIPS inside: The highly secure cryptographic module is certified according to FIPS 140-2

New features in version 2.30:

- Seamless Roaming – VPN connections stay uninterrupted even when the media changes (in conjunction with LANCOM routers as of LCOS 8.6)
- Windows 7 Mobile Broadband support for high-performance cellular networks (LTE)
- Improved handling of firewall rules
- Easy internet connection check with PING and DNS tests

The LANCOM Advanced VPN Client provides field staff with high-security encrypted access to the company network—nationwide and abroad. Once configured, the VPN connection can be established with only one click using the best available connection media. The Client also includes a stateful-inspection firewall and it supports all IPsec protocol extensions. VoIP data is prioritized. The integrated UMTS dialer as features an integrated Budget Manager that offers adjustable time and volume limits for full cost control. A list of approved UMTS network operators can be set up and roaming can be limited. Automatic login to LANCOM and T-Mobile HotSpots can be set up in advance.

More Security.

Optimally tuned for LANCOM VPN gateways, the LANCOM Advanced VPN Client offers highly comprehensive security functions that are suited to any scenario: IPsec encryption with AES or 3-DES, IPCOMP data compression, extended authentication (X.auth, EAP), support of digital certificates and hardware tokens, an integrated stateful inspection firewall with situation-dependant firewall rules, and “friendly net detection” which automatically identifies secure and unsecure networks.

More Convenience.

Installation Wizards are included which enable quick and easy VPN integration. Dial-in functions are supported by a range of profiles. Automatic media detection means that the connection type does not have to be defined manually; it is selected automatically depending on the available medium. If preferred, the client can handle the dial-in procedure for analog or DSL modems, and for ISDN, GPRS, UMTS or LTE cards. The dynamic DNS function in the LANCOM VPN gateways enable even standard DSL connections with dynamic IP addresses to be used for VPN dial-in access.

More Performance.

The versatility of the LANCOM Advanced VPN Client makes it the ideal mobile companion for business travelers: This includes the 0900er dialer protection, automatic channel bundling, or the various start-up options that the client can integrate directly into the Windows login. The automatic connection-establishment tools offer wide-ranging cost-control functions and a constant overview of charges, online time, and transfer volumes. The option of prioritizing VoIP data traffic facilitates an optimal integration into existing LANCOM VoIP infrastructure.

More Control.

The integrated UMTS dialer offers a Budget Manager which helps to stick to time- and volume quotas. Connection costs can easily be controlled. The Budget Manager measures and monitors defined online times or data volumes during a certain time span and warns the user when these are exceeded. Users and administrators can easily change the default settings of the Budget Manager.

LANCOM Advanced VPN Client (WIN)

Operating systems	
Microsoft Windows	Windows XP, Windows Vista und Windows 7, 32- und 64 Bit
Languages	German, English and French
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, charges, time and connection limit with warning, ISDN channel bundling with adjustable threshold value
Connection types	VPN connection over existing IP connection (LAN /WLAN) or direct management of analog and DSL modems (PPPoE), ISDN adapters (CAPI 2.0) as well as GPRS, UMTS and LTE cards with support of the Mobile Broadband interface of Windows 7. Alternative direct dial-in without encryption (e.g. ISDN), supports up to 5 remote networks per access profile
Protocols	All IP-based protocols, NetBIOS/IP (Windows Networking), PPP, PPPoE and PPTP
VPN/IPSec	
Standards	Standard-conform IPSec with ESP (Encapsulation Security Payload) and/or AH (Authentication Header)
FIPS inside	The IPSec client integrates a 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: <ul style="list-style-type: none"> • 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	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, 14 and 15-18. 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
Seamless Roaming	VPN connections stay uninterrupted even when the media (LAN, WLAN, cellular networks) changes and no new session has to be started (in conjunction with LANCOM routers with LCOS 8.6)
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
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
Automatic software updates	Software can search for new versions in definable time intervals

LANCOM Advanced VPN Client (WIN)

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 PC) or offline (requiring Internet access from any other PC). Activation is anonymous. No user-specific data of any kind is transmitted.
Notice	* This also applies when updating full versions (earlier than v1.30) which are licensed already.
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 for details.
Support	
Support	Support via hotline and Internet
Service	30-day demo version from www.lancom.de/avc or on the LANCOM CD
Package content	
Manual	Printed Quick Installation Guide (DE/EN)
CD	Software CD
Key	Printed license key
Item numbers	
	LANCOM Advanced VPN Client (WIN), for Windows XP, Vista and Windows 7 Item no. 61600
	LANCOM Advanced VPN Client (WIN, 10 Bulk), for Windows XP, Vista and Windows 7 Item no. 61601
	LANCOM Advanced VPN Client (WIN, 25 Bulk), for Windows XP, Vista and Windows 7 Item no. 61602
Options	
	LANCOM Upgrade Advanced VPN Client (WIN) for Windows XP, Vista and Windows 7 (for activating the new functions up to two major releases) Item no. 61603
	LANCOM Upgrade Advanced VPN Client (WIN, 10 bulk), for Windows XP, Vista and Windows 7 (for activating the new functions up to two major releases) Item no. 61604
	LANCOM Upgrade Advanced VPN Client (WIN, 25 bulk), for Windows XP, Vista and Windows 7 (for activating the new functions up to two major releases) Item no. 61605

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. 07/10