



. . . 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)

### Universeller VPN Software Client

- Hochsicherer, verschlüsselter Firmenzugang von unterwegs
- Integrierte Stateful-Inspection Firewall
- Integrierter UMTS-Dialer
- Priorisierung von Voice over IP
- IPSec over HTTPS (basierend auf der NCP VPN Path Finder Technology)
- Universeller IPSec VPN Client für Windows XP, Windows Vista, Windows 7 (32 und 64 Bit)

### Neu in Version 2.23:

- FIPS inside
  - Das eingebettete Kryptografiemodul ist nach FIPS 140-2 zertifiziert (Zertifikat #1051)
- Erweiterung der Konfiguration für die Hotspot-Anmeldung
- Datenübertragung via UMTS unter Windows 7, auch ohne Nutzung des integrierten UMTS-Dialers

### **Mehr Sicherheit.**

Ideal auf die LANCOM VPN Gateways abgestimmt, bietet der LANCOM Advanced VPN Client umfangreichste Security-Funktionen, die ihn optimal in jedes Szenario einfügen: IPSec Verschlüsselung mit AES oder 3-DES, IPCOMP Datenkompression, erweiterte Authentifizierungen (X.auth, EAP), Unterstützung digitaler Zertifikate und Hardware-Tokens, eine integrierte Stateful Inspection Firewall mit situationsabhängigen Firewallregeln und „Friendly Net Detection“ für eine automatische Erkennung von sicheren und unsicheren Netzen.

### **Mehr Komfort.**

Mit den integrierten Installations-Assistenten gelingt die VPN-Integration einfach und schnell. Zur Einwahl stehen verschiedene Profile bereit. Mit der automatischen Medienerkennung muss der verwendete Anschluss nicht mehr manuell festgelegt werden, sondern wird automatisch - abhängig von den verfügbaren Medien - ausgewählt. Hierbei übernimmt der Client auf Wunsch auch die Einwahl-Steuerung für Analog- oder DSL-Modems, ISDN-, GPRS oder UMTS-Karten. In Verbindung mit der Dynamic DNS-Funktion der LANCOM VPN-Gateways können auch VPN-Einwahlzugänge an Standard-DSL-Anschlüssen mit dynamischer IP-Adresse genutzt werden.

### **Mehr Leistung.**

Seine vielfältigen Möglichkeiten machen den LANCOM Advanced VPN Client zum idealen mobilen Begleiter für Geschäftsreisende: Vom 0900er Dialer-Schutz, der automatischen Kanalbündelung bis hin zur verschiedenen Start-Optionen, die den Client auch direkt beim Betriebssystem-Start in das Windows-Login integrieren können. Die automatische Verbindungssteuerung bietet umfangreiche Kostenkontrollfunktionen und jederzeit einen aktuellen Überblick über Gebühren, Online-Zeiten und Transfervolumina. Die Möglichkeit Voice over IP Datenströme zu priorisieren ermöglicht eine optimale Integration in bestehende LANCOM VoIP Infrastrukturen.

### **Mehr Kontrolle.**

Seit der Version 2.1 wird der integrierte UMTS-Dialer um den Budget-Manager ergänzt. Dieser hilft bei der Einhaltung eines festgesetzten Zeit- oder Volumenkontingents bspw. über UMTS-Verbindungen und trägt daher zur persönlichen Kostenkontrolle bei. Der Budget-Manager misst und überwacht die voreingestellte Online- Dauer oder das Datenvolumen während einer bestimmten Zeitspanne und warnt bei einer Überschreitung. Die Voreinstellungen im Budget-Manager können vom Anwender oder auch vom Administrator vorgenommen werden.

# LANCOM Advanced VPN Client (WIN)

<b>Betriebssysteme</b>	
Microsoft Windows	Windows XP, Windows Vista und Windows 7, jeweils 32 und 64 Bit
Sprachen	Deutsch und Englisch
<b>Kommunikation</b>	
Verbindungssteuerung	Kommunikation nur über gesicherten VPN-Tunnel oder mit gleichzeitigem ungesichertem Internetzugang. Manueller oder automatischer Verbindungsaufbau, einstellbare Haltezeit mit automatischem Verbindungsabbau, Gebühren-, Zeit- und Verbindungs-Limit mit Vorwarnung, ISDN Kanalbündelung bei einstellbarem Schwellwert
Verbindungsarten	VPN-Verbindung über bestehende IP-Verbindung (LAN / WLAN) oder direkte Steuerung von Analog- und DSL-Modems (PPPoE), ISDN-Adapttern (CAPI 2.0), GPRS- oder UMTS-Karten. Alternativ Direkteinwahl ohne Verschlüsselung (z.B. ISDN) Unterstützung von bis zu 5 entfernten Netzen pro Zugangsprofil
Protokolle	Alle IP-basierten Protokolle sowie NetBIOS/IP (Windows Networking), PPP, PPPoE und PPTP
<b>VPN/IPSec</b>	
Standards	Standard-konformes IPSec mit ESP (Encapsulation Security Payload) und/oder AH (Authentication Header)
FIPS inside	Der IPsec Client verfügt über einen kryptografischen Algorithmus nach FIPS-Standard. Das eingebettete Kryptografiemodul ist nach FIPS 140-2 zertifiziert (Zertifikat #1051). Die FIPS Kompatibilität ist immer gegeben, wenn die folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: <ul style="list-style-type: none"> <li>• DH-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit)</li> <li>• Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit</li> <li>• Verschlüsselungsalgorithmen: AES mit 128, 192 und 256 Bit oder Triple DES</li> </ul>
Verschlüsselung	3-DES (168 Bit), AES (128, 192 oder 256 Bit), Blowfish (128 Bit), RSA (1024 oder 2048 Bit)
Hashes	MD-5, SHA-1, SHA-256, SHA-384 und SHA-512
IKE Betriebsarten	IKE mit Pre-Shared Keys oder Zertifikaten, IKE Main oder Aggressive Mode, DH-Gruppen 1, 2, 5 und 14. Re-Keying nach einstellbarem Transfervolumen oder Zeitraum In Verbindung mit LANCOM VPN-Gegenstellen können durch eine IKE-Erweiterung auch bei Aggressive Mode Verbindungen pro Benutzer separate Pre-Shared Keys verwendet werden
<b>Zusatzfunktionen</b>	
IPSec over HTTPS	Zur Überwindung von VPN-Filtern (z. B. bei Sperrung von Port 500 für IKE). Setzt die Unterstützung von IPSec over HTTPS auf dem VPN Gateway (Gegenstelle) voraus. LANCOM VPN Router und Gateways benötigen dazu LCOS 8.0 oder höher. IPSec over HTTPS basiert auf der NCP VPN Path Finder Technology.
XAUTH	Zur Authentisierung per Username/Passwort
IKE Config-Mode	Zur Zuweisung von IP-Parametern (lokale IP Adresse, DNS und WINS Server) an den Client
IPCOMP	IPCOMP-Datenkompression (LZS) für optimale Bandbreitenausnutzung
Dead-Peer-Detection	Dead-Peer-Detection (DPD) zur Verbindungsüberwachung
NAT-Traversal	NAT-Traversal (NAT-T) zur Überwindung von nicht-IPSec-maskierungsfähigen Routern oder bei Verwendung von AH
RAS User Template	Konfiguration aller VPN-Client-Verbindungen im IKE Config-Mode über einen Eintrag im LANCOM VPN Gateway
EAP-MD5	Zur erweiterten Authentisierung gegenüber Layer-2-Geräten wie Switches oder WLAN Access Points
<b>PKI</b>	
Zertifikate	Public Key-Infrastruktur nach X.509v3, Entrust SmartCards: PKCS#11, TCOS 1.2 und 2.0 über CT-API oder PC/SC, Soft-Zertifikate: PKCS#12
Zertifikatsverlängerung	Überprüfung und Hinweis zur Gültigkeitsdauer eines Zertifikates
Certificate Revocation List (CRL)	Überprüfung der CRL und ARL (Certificate bzw. Authority Revocation List)
One Time Password	Komfortable Eingabe durch Trennung von PIN und Passwort
<b>Firewall</b>	
	Stateful Inspection, richtungsabhängige Paketfilter mit IP- und Port-Bereichen je Protokoll, LAN-Adapter-Schutz zum Schutz des PCs bei aktiver VPN-Verbindung vor Zugriffen anderer LAN-Benutzer, IP Broadcast und NetBIOS/IP Filter
<b>Installation</b>	
Assistenten	Für alle Verbindungsarten stehen angepasste Setup-Assistenten zur Verfügung
<b>Administration</b>	
Passwort-Schutz	Passwort-Schutz für Konfiguration und Profil-Management, Konfigurations-Berechtigung pro Funktionsbereich einstellbar, Ein- und Ausblenden von Parameterfeldern
<b>Aktivierung</b>	
Online- / Offline-Aktivierung	Nach der Installation der Software ist das Produkt zunächst für 30 Tage lauffähig*.  Innerhalb dieser 30 Tage muss eine Aktivierung erfolgen, die entweder direkt online (Internet Zugang von dem entsprechenden PC aus erforderlich) oder offline (Internet Zugang auf einem anderen PC erforderlich) durchgeführt wird. Die Aktivierung erfolgt anonym. Es werden keine benutzerspezifischen Daten übermittelt.
Hinweis	* Dies gilt auch für eine bereits lizenzierte Vollversion (kleiner v1.30), die aktualisiert wurde.

# LANCOM Advanced VPN Client (WIN)

Aktualisierung	
Update	Ein Update auf neuere Softwareversionen ist generell kostenlos und kann ohne Erwerb eines neuen Lizenzschlüssels durchgeführt werden. Ein Update stellt alle verfügbaren Bugfixes zu früheren Versionen bereit.
Upgrade	Mit einem Upgrade auf die aktuelle Version kann der Anwender einer älteren Version zusätzlich die neuen Features der aktuellen Version freischalten. Das Upgrade ist kostenpflichtig und erfordert den Erwerb eines neuen Upgrade-Lizenzschlüssels sowie eine neue Aktivierung. Ein Upgrade ist nur dann möglich, wenn nicht mehr als <b>2 Softwaresprünge</b> zwischen der ursprünglich aktivierten Version und der aktuellen Version liegen. Eine Übersichtstabelle, aus der Sie entnehmen können, ob Sie bei einer vorhandenen älteren Version des LANCOM Advanced VPN Clients ein Upgrade benötigen oder eine Neulizenzierung durchführen sollten, finden Sie auf <a href="http://www.lancom.de/avc">www.lancom.de/avc</a>
Support	
Support	Support über Hotline und Internet
Service	30-Tage Demoversion unter <a href="http://www.lancom.de/avc">www.lancom.de/avc</a> sowie auf der LANCOM CD
Lieferumfang	
Handbuch	Gedruckter Quick Installation Guide (DE/EN)
CD	CD mit Software
Schlüssel	Gedruckter Lizenzschlüssel
Artikelnummern	
	LANCOM Advanced VPN Client (WIN), für Windows XP, Windows 7 und Vista <span style="float: right;">Art.-Nr. 61600</span>
	LANCOM Advanced VPN Client (WIN, 10 Bulk), für Windows XP, Windows 7 und Vista <span style="float: right;">Art.-Nr. 61601</span>
	LANCOM Advanced VPN Client (WIN, 25 Bulk), für Windows XP, Windows 7 und Vista <span style="float: right;">Art.-Nr. 61602</span>
Optionen	
	LANCOM Upgrade Advanced VPN Client (WIN), für Windows XP, Windows 7 und Vista (ermöglicht ein Upgrade über maximal zwei Major-Versionen) <span style="float: right;">Art.-Nr. 61603</span>
	LANCOM Upgrade Advanced VPN Client (WIN, 10 Bulk), für Windows XP, Windows 7 und Vista (ermöglicht ein Upgrade über maximal zwei Major-Versionen) <span style="float: right;">Art.-Nr. 61604</span>
	LANCOM Upgrade Advanced VPN Client (WIN, 25 Bulk), für Windows XP, Windows 7 und Vista (ermöglicht ein Upgrade über maximal zwei Major-Versionen) <span style="float: right;">Art.-Nr. 61605</span>

LANCOM, LANCOM Systems und LCOS sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Änderungen vorbehalten. Keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen. 07/10