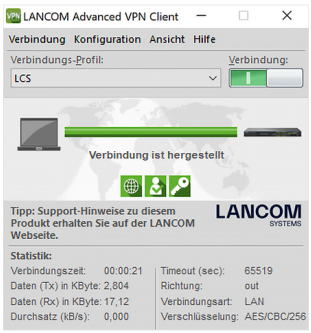
LANCOM SYSTEMS

lancom-systems.de

LANCOM Advanced VPN Client Windows

Universeller VPN-Software-Client für den sicheren Firmenzugang von unterwegs



Mit dem LANCOM Advanced VPN Client können sich mobile Mitarbeiter jederzeit über einen verschlüsselten Zugang in das Unternehmensnetzwerk einwählen – ob im Home Office oder unterwegs, im Inland wie im Ausland. Die Anwendung ist dabei denkbar einfach, denn nach einmalig erfolgter Konfiguration des VPN-Zugangs (Virtual Private Network) wird die sichere VPN-Verbindung intuitiv mit nur einem Klick über das beste verfügbare Verbindungsmedium aufgebaut. Für weiteren Schutz der Daten sorgt hierbei die integrierte Stateful Inspection Firewall, die Unterstützung aller IPSec-Protokollerweiterungen sowie weitere zahlreiche Sicherheitsfeatures.

- → IPSec-VPN-Client für Windows
- → Integrierte Stateful Inspection Firewall für sicheren Internetzugriff
- → Integrierter Mobilfunk-Dialer inklusive Budget-Manager für volle Kostenkontrolle
- → Priorisierung von Voice over IP-Daten
- → IPSec-over-HTTPS (basierend auf der NCP VPN Path Finder Technology)
- → Seamless Roaming – VPN-Verbindungen bleiben auch bei Medienwechsel bestehen
- → Unterstützung von IPv6-VPN

LANCOM SYSTEMS

lancom-systems.de

LANCOM Advanced VPN Client Windows

Sicherer Firmenzugang von unterwegs

Mit dem LANCOM Advanced VPN Client Windows kann der Nutzer über einen gesicherten VPN-Tunnel auf das Unternehmensnetzwerk zugreifen. Hierbei spielt es keine Rolle, ob der Anwender sich mobil unterwegs, im Home-Office oder auch im Ausland befindet – der LANCOM Advanced VPN Client bietet jederzeit und von überall einen sicheren Kanal zum Unternehmensnetzwerk. Perfekt für unterwegs: Dank Seamless Roaming bleibt der Kanal auch bei Medienwechsel bestehen.

Höchste Datensicherheit

Ausgerüstet mit einer Stateful Inspection Firewall erkennt der LANCOM Advanced VPN Client automatisch sichere und unsichere Netze für eine jederzeit abgesicherte Kommunikation. Zusammen mit weiteren Sicherheitsfunktionen wie der Unterstützung aller gängigen IPSec-Protokolle, digitaler Zertifikate und vielem mehr gewährleistet der Client optimalen Schutz, sodass alle Daten stets sicher übertragen werden.

Volle Kostenkontrolle

Der im Mobilfunk-Dialer integrierte Budget-Manager ermöglicht die Einstellung von Zeit- und Volumenkontingenten für eine volle Kostenkontrolle. Zudem bietet die Option "Kein Roaming zulassen" die Deaktivierung von Daten-Roaming, um zusätzliche Kosten zu vermeiden. Außerdem inklusive: Die automatische Verbindungssteuerung mit umfangreichen Kostenkontrollfunktionen sorgt jederzeit für einen aktuellen Überblick über Gebühren, Online-Zeiten und Transfervolumina.

Einfache und schnelle Konfiguration dank Installationsassistent und "1-Click-VPN"

Der in LANconfig integrierte Installationsassistent begleitet den Benutzer bei der schnellen und unkomplizierten VPN-Konfiguration. Mit der automatischen Medienerkennung muss der verwendete Anschluss nicht manuell festgelegt werden, sondern wird automatisch – abhängig von den verfügbaren Medien – ausgewählt. Nach einmaliger erfolgreicher Installation des VPN-Zugangs erfolgt die VPN-Verbindung intuitiv mit nur einem Klick.

LANCOM SYSTEMS

lancom-systems.de

LANCOM Advanced VPN Client Windows

Betriebssysteme	
Microsoft*	→ Windows 11 → Windows 10
Sprachen	Deutsch, Englisch
*) Hinweis	Auf Intel x86 bzw. x86-64 Prozessorarchitektur. Eine Übersicht zu älteren Advanced VPN Client Versionen finden sie auf unserer Knowledgebase unter https://support.lancom-systems.com/knowledge/x/1Iw7Ag

Kommunikation	
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. Always-on-Betrieb für Windows 11, 10 und 8.1, insbesondere Tablets
Verbindungsarten	VPN-Verbindung über bestehende IP-Verbindung (LAN / WLAN) oder direkte Steuerung von Analog- und DSL-Modems (PPPoE), ISDN-Adaptern (CAPI 2.0) sowie GPRS-, UMTS-und LTE-Karten mit Unterstützung der Mobile Broadband Schnittstelle ab Windows 7. 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

VPN/IPsec	
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: DH-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit) Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit Verschlüsselungsalgorithmen: AES mit 128, 192 und 256 Bit oder Triple DES
Verschlüsselung	AES-CBC/AES-CTR/AES-GCM (128, 192 oder 256 Bit), 3-DES (168 Bit), RSA (1024 oder 2048 Bit)
Hashes	SHA-512, SHA-384, SHA-256, SHA-1, MD-5
IKE Betriebsarten	IKE mit Pre-Shared Keys oder Zertifikaten, IKE Main oder Aggressive Mode, IKEv2, DH-Gruppen 1, 2, 5, 14-21, 25-30, 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.
Netzkopplung	Nutzung von IPv4 VPN über IPv4/IPv6 WAN-Verbindungen, Nutzung von IPv6 VPN über IPv4/IPv6 WAN-Verbindungen

Zusatzfunktionen	
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

LANCOM SYSTEMS

lancom-systems.de

LANCOM Advanced VPN Client Windows

Zusatzfunktionen	
IKE Config-Mode	Zur Zuweisung von IP-Parametern (lokale IP Adresse, DNS und WINS Server) an den Client
IPCOMP	IPCOMP-Datenkompression (LZS und Deflate) für optimale Bandbreitenausnutzung
Dead-Peer-Detection	Dead-Peer-Detection (DPD) zur Verbindungsüberwachung
IKEv2-Redirect	Unterstützung von IKEv2-Redirect nach RFC 5685
IKEv2 Split-DNS	Split-DNS ermöglicht die DNS-Auflösung bestimmter interner Domänen, z. B. "*.firma.de" über den VPN-Tunnel, während für alle anderen DNS-Anfragen ein öffentlicher DNS-Server verwendet wird.
IKEv2 Cookie Challenge	Der IKEv2 Cookie Challenge-Mechanismus dient der Abwehr von DoS-Attacken auf ein VPN-Gateway.
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
Seamless Roaming	VPN-Verbindungen bleiben auch bei Änderung des Verbindungsmediums (LAN / WLAN / Mobilfunk) bestehen, so dass keine neue Session aufgebaut werden muss (in Verbindung mit LANCOM Routern ab LCOS-Version 8.6)
Biometrische Authentisierung	Absicherung vor einem VPN-Verbindungsaufbau durch eine biometrische Authentisierung (z.B. Fingerabdruck- oder Gesichtserkennung)
Windows-Zertifikatsspeicher (CSP)	Zur Verwendung von Benutzerzertifikaten im Windows-Zertifikatsspeicher
PKI	
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
Firewall	
Stateful Inspection Firewall	Stateful Inspection Firewall für IPv4 und IPv6, 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
Installation	
Assistenten	Für alle Verbindungsarten stehen angepasste Setup-Assistenten zur Verfügung

LANCOM SYSTEMS

lancom-systems.de

LANCOM Advanced VPN Client Windows

Administration	
Passwort-Schutz	Passwort-Schutz für Konfiguration und Profil-Management, Konfigurations-Berechtigung pro Funktionsbereich einstellbar, Ein- und Ausblenden von Parameterfeldern
Netzwerkdiagnose	Einfache Überprüfung der Internetverfügbarkeit durch Ping und DNS-Abfrage
Automatisches Softwareupdate	Software kann in definierbaren Zeitabständen nach neuen Versionen suchen
MSI Installer	Software-Verteilung über MSI Installer
Aktivierung / Deaktivierung	
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 entwender direkt online (Internet Zugang von dem entsprechenden Computer aus erforderlich) oder offline (Internet Zugang auf einem anderen Computer erforderlich) durchgeführt wird. Die Aktivierung erfolgt anonym. Es werden keine benutzerspezifischen Daten übermittelt.
Deaktivierung	Die Lizenzen für den LANCOM Advanced VPN Client sind Einzelplatz-Lizenzen und dürfen zeitgleich nur auf einem System aktiviert und verwendet werden. Die Deaktivierungs-Funktion des Advanced VPN Client bietet Ihnen eine komfortable Möglichkeit, eine Lizenz auf einem nicht mehr genutzten System zu deaktivieren, um diese auf einem neuen System wieder aktivieren zu können. (ab Version 2.32, Build 128)
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 2 Softwaresprünge 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 www.lancom-systems.de/avc
*) Hinweis	Ab Version 3.10 wird für die Aktivierung des Advanced VPN Clients zwingend ein Lizenzschlüssel der gleichen Version benötigt. Eine Aktivierung mit altem Lizenzschlüssel ist damit nicht mehr möglich. Dies gilt fortan für jede kommende Major-Version. Entscheidend dafür, ob Sie eine Neulizenzierung oder Upgrade-Lizenz benötigen, sind die ersten beiden Ziffern Ihrer Version. Haben Sie z.B. die Version 3.10 im Einsatz, so können Sie auf die Version 3.11 kostenlos updaten.
Support	
Support	Support über Internet
Service	30-Tage Demoversion unter www.lancom-systems.de
Lieferumfang	
Handbuch	Gedruckter Quick Installation Guide (DE/EN)
Schlüssel	Gedruckter Lizenzschlüssel

lancom-systems.de

LANCOM Advanced VPN Client Windows

Artikelnummern	
Art.-Nr. 61600	LANCOM Advanced VPN Client Windows
Art.-Nr. 61601	LANCOM Advanced VPN Client Windows (10er Bulk)
Art.-Nr. 61602	LANCOM Advanced VPN Client Windows (25er Bulk)

Optionen	
Art.-Nr. 61603	LANCOM Upgrade Advanced VPN Client Windows (ermöglicht ein Upgrade über maximal zwei Major-Versionen)
Art.-Nr. 61604	LANCOM Upgrade Advanced VPN Client Windows (10er Bulk) (ermöglicht ein Upgrade über maximal zwei Major-Versionen)
Art.-Nr. 61605	LANCOM Upgrade Advanced VPN Client Windows (25er Bulk) (ermöglicht ein Upgrade über maximal zwei Major-Versionen)

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
www.lancom-systems.de