Häufig gestellte Fragen zu LANCOM Trusted Access (LTA)

LANCOM Trusted Access ist die vertrauenswürdige Network Access Security-Lösung für Unternehmensnetzwerke. Es ermöglicht einen sicheren und skalierenden Zugriff auf Unternehmensanwendungen für Mitarbeitende im Büro, zu Hause oder unterwegs. Dabei erhalten Benutzer wahlweise einen umfassenden Netzwerkzugriff (Cloud-managed VPN) oder ausschließlich Zugangsberechtigung auf Anwendungen, die ihnen zugewiesen wurden (Zero-Trust-Prinzip).

Welche Netzwerkkomponenten werden für die LANCOM Trusted Access-Lösung benötigt?

Für den Betrieb der LANCOM Trusted Access-Lösung benötigen Sie die folgenden drei LANCOM Komponenten sowie eine zentrale Benutzerdatenbank:

- → LANCOM Trusted Access Client (LTA-Client):
  Verfügbar als 1, 3 oder 5 Jahreslizenzen, Client-Lizenzierung erfolgt zentral über die LANCOM Management Cloud
- → LANCOM Management Cloud (LMC) (LTA-Controller):
  Konfiguration, Monitoring, Lizenzmanagement und Anbindung an Active Directory
- → LANCOM Trusted Access Gateway (LTA-Gateway):
  LANCOM VPN-Router oder LANCOM R&S®Unified Firewall
  Bei kleinen Installationen kann ein vorhandener VPN-Router für Standort-vernetzung und Remote Access eingesetzt werden. In größeren Szenarien empfiehlt sich eine Auslagerung z. B. der LTA-Gateway-Funktion auf ein Firewall HA-Cluster in einer DMZ.
- → Zentrale Benutzerdatenbank mit Microsoft Entra ID Connect (ehem. Azure AD Connect) zur Kopplung an vorhandenes Microsoft Active Directory. Alternativ steht für kleine Installationen ohne AD auch eine interne User-Verwaltung in der LMC zur Verfügung (LMC-interne Benutzertabelle).

Welche LANCOM Gateways unterstützen LTA?

- → Alle LCOS-basierten Router (Hardware oder vRouter) ab LCOS 10.80
- → Alle LCOS FX-basierten Firewalls (Hardware oder vFirewall) ab LCOS FX 10.13

Können LANCOM LTA-Gateways mit LANconfig konfiguriert werden?

- → Eine Konfiguration von LTA-Gateways mit LANconfig wird derzeit nicht unterstützt.

Auf welchen Betriebssystemen kann der LANCOM Trusted Access Client betrieben werden?

- → Microsoft Windows 10 / 11 (auf Intel x86 bzw. x86-64 Prozessorarchitektur)
- → MacOS (in Vorbereitung)

Was unterscheidet den LANCOM Trusted Access Client vom LANCOM Advanced VPN Client?

Features	Advanced VPN Client	Trusted Access Client
Betriebsart	Unmanaged	Cloud-managed
Inbetriebnahme	Manuelle Vorkonfiguration aller Zugangsparameter pro Client	Zero-touch / Auto-Konfiguration: Es ist keine Vorkonfiguration notwendig. Benutzer werden anhand ihrer E-Mail-Domäne automatisch dem richtigen Projekt zugeordnet. Die Client-Konfiguration und -Zuordnung erfolgt zentral über die LMC.
Monitoring	—	✓ Zentrales Monitoring-Dashboard in der LMC
Zugriffsrechte	Vollzugriff auf das Intranet	Einzelne Applikationen oder alternativ in kleineren Einsatzszenarien mit Vollzugriff auf das Intranet. Es wird jedoch empfohlen, den Zugriff pro Benutzergruppe auf die benötigten Anwendungen zu limitieren und die lokalen Anwendungen netzseitig voneinander zu trennen.
Lateraler Schutz (z. B. gegen Ransomware)	— Gesamtes Intranet erreichbar	✓ Bei Verwendung der Anwendungsfilterung in Verbindung mit Mikrosegmentierung (Private VLAN)
Endpoint Security	—	✓ Es kann Clients vorgegeben werden, dass Virenscanner und Firewall auf jedem Client aktiv sein müssen und es eine Mindestversion bzw. ein Patch-Level für das Betriebssystem gibt. Clients, die den Vorgaben nicht entsprechen, können automatisch blockiert werden.
Client-Konfiguration / Change-Management	Manuell pro Client	Automatisch / zentral via LMC
Zentrales User-Management	—	✓ Via Active Directory oder Benutzertabellen in der LMC
Zwei- oder Multi-Faktor-Authentifizierung (2FA / MFA)	—	✓ Nur bei Nutzung von Microsoft Active Directory; nicht in Verbindung mit lokaler Benutzertabelle
Lizenzierung	Lizenz muss pro Client manuell aktiviert werden	Lizenzierung erfolgt zentral über die LMC (pre-paid oder pay-per-use)
Regelmäßige Software-Updates	—	✓ Inkludiert über die gesamte Laufzeit

Ist die LTA-Lösung DSGVO-konform?

Ja, LANCOM Trusted Access unterliegt und entspricht als IT-Security-Lösung Made in Germany europäischen Rechtsstandards und ist somit DSGVO-konform. Der LANCOM Trusted Access Client sowie die LANCOM Management Cloud (LMC) werden in Deutschland entwickelt, und auch das Hosting sämtlicher Cloud-Daten erfolgt in Rechenzentren in Deutschland.

Für höchste Datensicherheit und höchsten Datenschutz erfolgt der Datenaustausch zur Benutzer-Authentifizierung ausschließlich über die LMC. Alle weiteren Nutzdaten verlaufen direkt zwischen LTA-Client und LTA-Gateway – ohne Auskopplung über eine externe Cloud.

Welche Lizenzen sind für den Betrieb von LTA erforderlich und wie erfolgt die Lizenzierung?

LANCOM Trusted Access Client

Die Lizenzen des LANCOM Trusted Access Clients können mit den Laufzeiten 1, 3 und 5 Jahren für verschiedene Benutzerzahlen (1, 10, 25, 100, 250 oder 1.000) käuflich erworben werden. Die Lizenzierung erfolgt pro Benutzer (d. h. nicht pro Endgerät). Mit einer LTA-Lizenz können pro Benutzer bis zu drei Endgeräte parallel genutzt werden.

Alle LTA-Lizenzen sind immer genau einem Projekt in der LANCOM Management Cloud (LMC) zugeordnet (wird bei der Bestellung abgefragt) und sind nicht übertragbar. Maßgeblich für die Benutzer-Zählung sind diejenigen Mitarbeitenden eines Unternehmens, die entweder in der lokalen Benutzerverwaltung hinzugefügt und aktiviert sind oder in der Primärgruppe der IdP-Benutzerverwaltung (geeignete Active Directory-Gruppe, z. B. „LTA User“) enthalten sind. Gegenstand der Lizenzierung sind somit jeweils alle potenziell berechtigten Benutzer.

Trusted Access Gateway (Router oder Firewall)

→ Alle LTA-Gateways müssen über eine aktive LMC-Lizenz verfügen.

→ Auf LCOS-basierten Gateways ist pro Benutzer ein freier VPN-Kanal notwendig. Content-Filtering für Web-Traffic steht nur in Verbindung mit Full Tunnel-Betrieb und mit der entsprechenden Software-Option LANCOM Content Filter zur Verfügung.

→ Auf LCOS FX-basierten Gateways ist eine aktive Basic- oder Full-Lizenz notwendig. Content-Filtering, IDS / IPS, Antivirus sowie SSL Inspection für Web-Traffic steht nur in Verbindung mit einer entsprechenden Full-Lizenz zur Verfügung.

Was passiert, wenn nicht genügend Lizenzen für ein Projekt aktiviert sind?

Falls Sie nicht ausreichende LTA-Lizenzen für die Anzahl der verwalteten LTA-Benutzer aktiviert haben, erhalten Sie entsprechende Hinweismeldungen. Nach einem mehrstufigen Mahnprozess werden alle Zugänge gesperrt. Um dies zu verhindern, lizenzieren Sie bitte frühzeitig nach.

Gibt es eine LTA-Testlizenz und wie erhalten Partner LTA-Demo-Lizenzen?

Es steht eine kostenfreie LTA-Starter-Lizenz zur Verfügung. Diese ermöglicht Ihnen den Test von LANCOM Trusted Access für maximal **30 Tage und 25 Benutzer**.

Die LTA-Starter-Lizenz wird einmalig in Ihrer Lizenzverwaltung unter „LTA-Benutzer-Lizenzen“ hinterlegt und nach der Konfiguration des ersten LTA-Benutzers bzw. einer Benutzergruppen-Aktivierung aus einem Active Directory automatisch aktiviert.

Voraussetzung dafür ist eine LMC-Organisation oder ein „Not-for-resale“-Projekt(NFR) in der LMC, welches kostenlos über das Partnerprogramm zur Verfügung gestellt wird. Zur Eigenverwendung sowie für Tests und Demos können dort kostenfrei Geräte durch die LANCOM Management Cloud betrieben werden.

LANCOM Gold- und Platinum-Partner können pro Jahr bis zu **10 LTA-NFR-Lizenzen** (CLA, projektgebunden, Laufzeit 1 Jahr) kostenfrei für Demo- und Testzwecke erhalten, Bronze- und Silver-Partner bis zu **5 LTA-NFR-Lizenzen**.

Ab Januar 2024 können in den NFR-Cloud-Projekten neben diesen LTA-NFR-Lizenzen auch kostenpflichtige LANCOM Trusted Access CLA-Lizenzen für den Eigenbetrieb eingesetzt werden.

Die nachfolgende Tabelle verdeutlicht, welche LTA-Lizenztypen in welchen LMC-Projekttypen funktionieren und wie viele Lizenzen pro Partnerstufe kostenlos verfügbar sind:

LTA-Lizenztyp	CLA-Projekt in der LMC	NFR-Projekt in der LMC	Bemerkung
30-Tage-LTA-Demo	✓	✓	Für bis zu 25 User pro LMC-Projekt
Kostenlose LTA-NFR-Lizenzen	–	✓	Anzahl der LTA-CLA-1Y-Lizenzen abhängig von Partnerstufe: Gold / Platinum = 10 Silver / Bronze = 5
CLA	✓	✓	

In welchen Varianten kann LTA implementiert werden?

Egal, ob Sie Cloud-managed VPN-Client-Vernetzung für weitreichende Netzwerkzugriffe benötigen oder den Schritt zu einer umfassenden Zero-Trust-Sicherheitsarchitektur gehen möchten – LANCOM Trusted Access bietet passende Ausbaustufen an.

Weitere Informationen dazu entnehmen Sie bitte dem Datenblatt des LANCOM Trusted Access Client. Bitte beachten Sie, dass LTA nicht für Private LMC zur Verfügung steht.

Wie erfolgt die Benutzerverwaltung?

Die Benutzerauthentifizierung nach dem Zero-Trust-Prinzip erfolgt bei LTA in der Regel über eine zentrale Benutzerdatenbank („Identity Provider“, z. B. ein Active Directory). Dies kann sowohl ein lokales Microsoft Active Directory sein (mit LMC-Anbindung über

Azure AD Connect), als auch ein Cloud-gehostetes Active Directory (Microsoft Entra ID, ehemals Azure AD). Für kleine Unternehmen ohne zentrale Benutzerdatenbank steht alternativ ein in die LANCOM Management Cloud integriertes Benutzer-Management zur Verfügung (LMC-interne Benutzertabelle).

Welche Redundanzfunktionen sind bei LTA möglich?

Geräteredundanz des LTA-Gateways

Die geräteseitige Redundanz muss manuell auf den Geräten in der LMC konfiguriert werden und kann als redundanter Einwahlpunkt für LTA-Clients über ein HA-Cluster (LCOS FX oder bei LCOS mit unterschiedlichen Einwahl-Pools und VRRP) realisiert werden.

Leitungsredundanz (redundante Anbindung der LTA-Gateways)

Die leitungsseitige Redundanz muss manuell auf den Geräten in der LMC konfiguriert werden. Dabei terminieren mehrere WAN-Verbindungen auf einem Gerät (bis zu 4 WAN-Verbindungen bei LCOS, bis zu 6 WAN-Verbindungen bei LCOS FX).

Controller-Redundanz (Cloud)

Die LANCOM Management Cloud (LMC) ist geo-redundant ausgelegt. Sie dient bei LTA nur als „Control Plane“, d. h. die Nutzdatenübertragung erfolgt nach Autorisierung direkt zwischen LTA-Client und LTA-Gateway.

LTA-Client – autarker Weiterbetrieb

Für einen aktiven, autorisierten Client ist ein Weiterbetrieb ohne LMC-Verbindung möglich, solange die jeweilige Session besteht.

Für höchste Resilienz ist optional ein autarker Weiterbetrieb der LTA-Clients einstellbar, so dass ein einmal authentisierter LTA-Client innerhalb eines definierten Zeitraums auch ohne Verbindung zur LMC bzw. nach Neustart des Clients oder Rechners eine Verbindung zu den zugewiesenen Zielen aufbauen kann.

Was ist Trusted Internet Access?

Mit LANCOM Trusted Access (LTA) verwalten Sie die Zugriffsrechte und Netzwerkverbindungen für mobile Mitarbeitende sicher und zentral über die LANCOM Management Cloud. Dabei wird den mobilen Benutzern der normale Internetverkehr grundsätzlich erlaubt (Split Tunnel). Um zusätzlich den gesamten Internetverkehr angebundener LTA-Clients abzusichern, aktivieren Sie den ‚Full Tunnel‘-Betrieb. Damit wird der gesamte Datenverkehr durch das zentrale LTA-Gateway (Unified Firewall oder SD-WAN Gateway) geleitet. Der Vorteil: Risiken durch unbefugte Zugriffe, Malware, Phishing und andere Cyberangriffe werden minimiert und können zusätzlich über aktivierte Sicherheitsfunktionen auf dem Gateway wie Anti-Virus oder Content Filter auch bei externen Web- / Cloudbasierten Anwendungen überprüft werden. Wir nennen diesen Betriebsmodus ‚Trusted Internet Access‘.

Was ist der Unterschied zwischen Split Tunnel & Full Tunnel?

LANCOM Trusted Access kann mit verschiedenen Tunnel-Modi verwendet werden. Dieser legt fest, ob der gesamte Netzwerkverkehr der LTA-Benutzer über den Tunnel zum Gateway geleitet wird (Full Tunnel) oder nur selektiv (Split Tunnel). Sie finden die Einstellungsmöglichkeiten in der LANCOM Management Cloud unter ‚Sicherheit / LANCOM Trusted Access / Client-Konfiguration'. Die Sicherheitseinstellung für die LTA-Benutzer nehmen Sie hingegen im Profil ‚LTA users' unter ‚Sicherheit / Profile' vor.

Split Tunnel:

Selektiver Netzwerkverkehr wird vom LTA-Client durch den sicheren Tunnel zum Gateway geleitet. Die Selektion erfolgt im LTA-Client auf Basis der ‚getunnelten Netze'. Diese Einstellung ermöglicht eine effizientere Nutzung der Gateway-Ressourcen oder eine gezielte Steuerung bestimmter Datenverbindungen über das LTA-Gateway.

Full Tunnel:

Jeglicher Netzwerkverkehr wird vom LTA-Client durch den sicheren Tunnel zum Gateway geleitet und kann auf dem Gateway durch Sicherheitsfunktionen überprüft werden. Die Sicherheitseinstellung für die LTA-Benutzer werden im Profil ‚LTA users' im Tab ‚Profile' vorgenommen. Die Kombination aus Full Tunnel-Betrieb und Sicherheitsmechanismen auf dem LTA-Gateway wird ‚Trusted Internet Access' genannt.

An wen kann ich mich für LTA-Support wenden?

Der LANCOM Service & Support steht Ihnen mit Rat und Tat zur Seite, sofern Sie Unterstützung bei Software-Problemen benötigen oder technische Informationsanfragen haben.

Welche Voraussetzungen dafür gelten, erfahren Sie im Infopaper Support-Leistungen LANCOM Trusted Access.

Ist ein Trade-in-Programm für LANCOM Advanced VPN Client-Lizenzen verfügbar?

Ein generelles Trade-in-Programm für erst kürzlich erworbene LANCOM Advanced VPN Client-Lizenzen gibt es derzeit nicht. Für eine individuelle Beratung wenden Sie sich als Partner bitte an Ihre zuständige Ansprechperson im LANCOM Vertrieb.

Wie kann Trusted Access eingerichtet werden?

LANCOM Systems bietet ein umfangreiches Trusted Access Onboarding-Programm an, bei dem Schritt-für-Schritt-Anleitungen und Trainingsvideos sowie weiterführende Informationen für unterschiedliche Szenarien und thematische Schwerpunkte (Sales, Technik) angeboten werden.

Dieses Programm wendet sich an LANCOM Partner, die Trusted Access bei sich im Unternehmen und / oder bei ihren Kunden einrichten wollen.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de