Frequently asked questions about LANCOM Trusted Access (LTA)

LANCOM Trusted Access is the trusted network access security solution for enterprise networks. It enables secure and scalable access to enterprise applications for employees in the office, at home, or on the road. Users can either be granted comprehensive network access (cloud-managed VPN) or access only to applications that have been assigned to them (Zero Trust principle).

Which network components are required for the LANCOM Trusted Access solution?

To operate the LANCOM Trusted Access solution, you need the following three LANCOM components and a central user database:

- → LANCOM Trusted Access Client (LTA client):
  Available as 1, 3, or 5-year licenses, client licensing is done centrally via the LANCOM Management Cloud.
- → LANCOM Management Cloud (LMC) (LTA controller):
  Configuration, monitoring, license management, and connection to Active Directory
- → LANCOM Trusted Access Gateway (LTA gateway):
  LANCOM VPN router or LANCOM R&S®Unified Firewall
  In small installations, an existing VPN router can be used for site networking and remote access. In larger scenarios, it is recommended to outsource the LTA gateway function to a firewall HA cluster in a DMZ, for example.
- → Central user database ith Microsoft Entra ID Connect (formely Azure AD Connect) for linking to existing Microsoft Active Directory. Alternatively, internal user management in the LMC is also available for small installations without AD.

Which LANCOM gateways support LTA?

- → All LCOS based routers (hardware or vRouter) as of LCOS 10.80
- → All LCOS FX based firewalls (hardware or vFirewall) as of LCOS FX 10.13

Can LANCOM LTA gateways be configured with LANconfig?

- → The configuration of LTA gateways with LANconfig is supported from version 10.80 RU8.

On which operating systems can the LANCOM Trusted Access Client be operated?

→ Microsoft Windows 10 / 11 (on Intel x86 or x86-64 processor architecture)

→ macOS Sequoia 15

→ macOS Sonoma 14

→ macOS Ventura 13

→ macOS Monterey 12

→ macOS Big Sur 11

What is the difference between the LANCOM Trusted Access Client and the LANCOM Advanced VPN Client?

Features	Advanced VPN Client	Trusted Access Client
Operating mode	Unmanaged	Cloud managed
Commissioning	Manual pre-configuration of all access parameters per client	Zero-touch / auto-configuration: No pre-configuration is required. Users are automatically assigned to the correct project based on their email domain. All client configuration and assignment is done centrally via the LMC.
Monitoring	–	✓ Central monitoring dashboard in the LMC
Access rights	Full access to the intranet	Individual applications or alternatively in smaller deployment scenarios with full access to the intranet. However, it is recommended to limit the access per user group to the required applications and to separate the local applications from each other on the network side.
Lateral protection (e. g. against ransomware)	– Entire intranet accessible	✓ When using application filtering in conjunction with micro-segmentation (Private VLAN)
Endpoint security	–	✓ Clients can be specified that virus scanners and firewalls must be active on each client and that there is a minimum version or patch level for the operating system. Clients that do not comply with the specifications can be blocked automatically.
Client configuration / change management	Manual per client	Automatic / central via LMC
Central user management	–	✓ Via Active Directory or user tables in the LMC
Two- or multi-factor authentication (2FA / MFA)	–	✓ Only when using Microsoft Active Directory; not in conjunction with local user table
Licensing	License must be activated manually per client	Licensing is carried out centrally via LMC (pre-paid or pay-per-use)
Regular software updates	–	✓ Included over the entire term

Is the LTA solution GDPR compliant?

Yes, LANCOM Trusted Access is subject to and complies with European legal standards as an IT security solution made in Germany and is therefore GDPR compliant. The LANCOM Trusted Access Client and the LANCOM Management Cloud (LMC) are developed in Germany, and all cloud data is also hosted in data centers in Germany.

For the highest level of data security and data protection, data exchange for user authentication takes place via the LMC. All other user data runs directly between the LTA client and the LTA gateway – without decoupling via an external cloud.

What licenses are required to operate LTA and how is licensing carried out?

LANCOM Trusted Access Client

The LANCOM Trusted Access Client licenses can be purchased with terms of 1, 3, and 5 years for various numbers of users (1, 10, 25, 100, 250, or 1,000). Licensing is per user (i. e. not per end device). With one LTA license, up to three end devices can be used in parallel per user.

All LTA licenses are always assigned to exactly one project in the LANCOM Management Cloud (LMC) (will be requested when ordering) and are not transferable. Decisive for the user count are those employees of a company who are either added and activated in the local user management or are included in the primary group of the IdP user management (suitable Active Directory group, e. g. „LTA User“). The object of licensing is thus in each case all potentially authorized users.

Trusted Access gateway (router or firewall)

- → All LTA gateways must have an active LMC license.
- → On LCOS based gateways, a free VPN channel per user is required. Content filtering for web traffic is only available in conjunction with full-tunnel operation and ith the corresponding software option LANCOM Content Filter.
- → On LCOS FX based gateways, an active Basic or Full license is required. Content filtering, IDS / IPS, Anti-Virus, as well as SSL inspection for web traffic is only available in conjunction with a corresponding full license.

What happens if not enough licenses are activated for a project?

If you have not activated sufficient LTA licenses for the number of managed LTA users, you will receive corresponding notification messages. After a multi-stage reminder process, all accesses will be blocked. To prevent this, please re-license early.

Is there an LTA test license and how do partners obtain LTA demo licenses?

A free LTA starter license is available. This allows you to test LANCOM Trusted Access for a maximum of **30 days and 25 users**.

The LTA starter license is stored once in your license management under "LTA user licenses" and is automatically activated after the configuration of the first LTA user or a user group activation from an Active Directory.

The requirement for this is an LMC organization or an "not-for-resale" (NFR) project in the LMC, which is provided free of charge via the partner program. Devices can be operated there free of charge by the LANCOM Management Cloud for personal use, tests, and demos.

LANCOM Gold and Platinum partners can receive up to **10 LTA NFR licenses** (CLA, project-bound, 1 year term) per year free of charge for demo and test purposes, Bronze and Silver partners up to **5 LTA NFR licenses**.

From January 2024, in addition to these LTA NFR licenses, paid LANCOM Trusted Access CLA licenses can also be used in NFR cloud projects for self-operation.

The following table shows which LTA license types work in which LMC project types and how many licenses are available free of charge per partner level:

LTA license typ	CLA project in the LMC	NFR project in the LMC	Remark
30-day LTA demo	✓	✓	For up to 25 users per LMC project
Free LTA-NFR licenses	–	✓	Number of LTA-CLA-1Y licenses depending on partner level: Gold / Platinum = 10 Silver / Bronze = 5
CLA	✓	✓	

In which variants can LTA be implemented?

Whether you need cloud-managed VPN client networking for wide-ranging network access or want to take the step to a comprehensive Zero Trust security architecture, LANCOM Trusted Access offers exactly the right configuration levels.

For more information, please refer to the LANCOM Trusted Access Client datasheet.

Please note that LTA is not available for Private LMC.

How is the user management carried out?

With LTA, user authentication according to the Zero Trust principle is usually performed via a central user database (“identity provider“, e. g. an Active Directory). This can be both a local Microsoft Active Directory (with LMC connection via Azure AD Connect) and a Cloud-hosted Active Directory (Microsoft Entra ID, formerly Azure AD). For small companies without a central user database, user management integrated into the LANCOM Management Cloud is available as an alternative.

Which redundancy functions are possible with LTA?

Device redundancy of the LTA gateway (router or firewall)

The device-side redundancy must be configured manually on the devices in the LMC and can be implemented as a redundant dial-in point for LTA clients via an HA cluster (LCOS FX or for LCOS with different dial-in pools and VRRP).

Line redundancy (redundant connection of the LTA gateways)

Line-side redundancy must be configured manually on the devices in the LMC. Multiple WAN connections terminate on one device (up to 4 WAN connections with LCOS, up to 6 WAN connections with LCOS FX).

Controller redundancy (cloud)

The LANCOM Management Cloud (LMC) is geo-redundant. In the case of LTA, it only serves as a “control plane“, i. e. after authorization, the user data is transferred directly between the LTA client and the LTA gateway.

LTA client – autonomous continued operation

For an active, authorized client, continued operation without an LMC connection is possible as long as the respective session exists.

For highest resilience, an autonomous continued operation of the LTA clients can optionally be set, so that a once authenticated LTA client can establish a connection to the assigned targets within a defined period of time even without connection to the LMC or after restarting the client or computer.

What is Trusted Internet Access?

With LANCOM Trusted Access (LTA), you can manage access rights and network connections for mobile employees securely and centrally via the LANCOM Management Cloud. Mobile users are always allowed normal Internet traffic (Split Tunnel). To additionally secure the entire Internet traffic of connected LTA clients, activate ‘Full Tunnel’ operation. This means that all data traffic is routed through the central LTA gateway (Unified firewall or SD-WAN gateway). The advantage: Risks from unauthorized access, malware, phishing and other cyber attacks are minimized and can also be checked for external web/cloud-based applications via activated security functions on the gateway such as Anti-Virus or Content Filters. We call this operating mode ‘Trusted Internet Access’.

What is the difference between Split Tunnel & Full Tunnel?

LANCOM Trusted Access can be used with different tunnel modes. This determines whether all network traffic of the LTA users is routed to the gateway via the tunnel (Full Tunnel) or only selectively (Split Tunnel). You can find the setting options in the LANCOM Management Cloud under ‘Security / LANCOM Trusted Access / Client configuration‘. The security settings for the LTA users, on the other hand, are made in the ‘LTA users’ profile under ‘Security / Profiles‘.

Split Tunnel:

Selective network traffic is routed from the LTA client through the secure tunnel to the gateway. The selection is made in the LTA client based on the ‘tunneled networks’. This setting enables more efficient use of gateway resources or targeted control of certain data connections via the LTA gateway.

Full Tunnel:

All network traffic is routed from the LTA client through the secure tunnel to the gateway and can be checked on the gateway using security functions. The security settings for the LTA users are made in the ‘LTA users’ profile in the Profiles tab. The combination of full tunnel operation and security mechanisms on the LTA gateway is called ‘Trusted Internet Access’.

Who can I contact for LTA support?

LANCOM Service & Support is available to provide you with advice and assistance if you need support with software problems or have technical information requests.

You can find out about the requirements for this in the Infopaper support services LANCOM Trusted Access.

Is a trade-in program available for LANCOM Advanced VPN Client licenses?

Yes, there is a trade-in promotion for recently purchased LANCOM Advanced VPN Client (AVC) licenses.

You can either take advantage of an additional discount of 20% (in addition to the partner discount and, if applicable, deal registration) on the list price when purchasing new LTA licenses or benefit from up to 77% off the former AVC purchase price. The following conditions of participation apply in both cases:

- Advanced VPN client licenses purchased after January 1, 2020 are entitled to the discount.
- Additional discount only applies to new purchases of LTA licenses
- The LANCOM partner must have undergone LTA onboarding.
- The promotion is limited until December 31, 2024.
- Processing takes place via a project credit when purchasing the LTA licenses.

For individual advice on this topic, you as a partner can get in touch with your responsible contact person in LANCOM Sales.

How can Trusted Access be set up?

LANCOM Systems offers a comprehensive Trusted Access onboarding program, providing step-by-step instructions and training videos as well as further information for different scenarios and thematic focuses (sales, technology).

This program is aimed at LANCOM partners who want to set up Trusted Access in their company and / or at their customers.

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