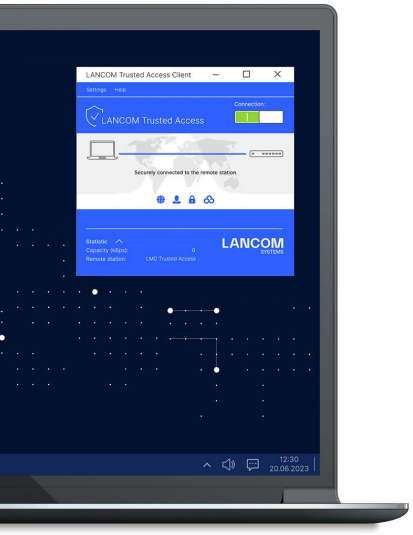
lancom-systems.com

LANCOM Trusted Access Client



Cloud-managed secure network access

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, protecting **modern hybrid working from anywhere, anytime**.

The LANCOM Trusted Access solution adapts to increasing security requirements in your organization and enables both **cloud-managed VPN client networking** for access to entire networks and the move to a **Zero Trust security architecture** for comprehensive network security. Based on granular access rights, users are only granted access to applications that have been assigned to them (Zero Trust principle). Existing systems for managing users and user groups (Active Directory) can be fully integrated into the LANCOM Management Cloud (LMC). For smaller networks, the LMC alternatively offers internal user management.

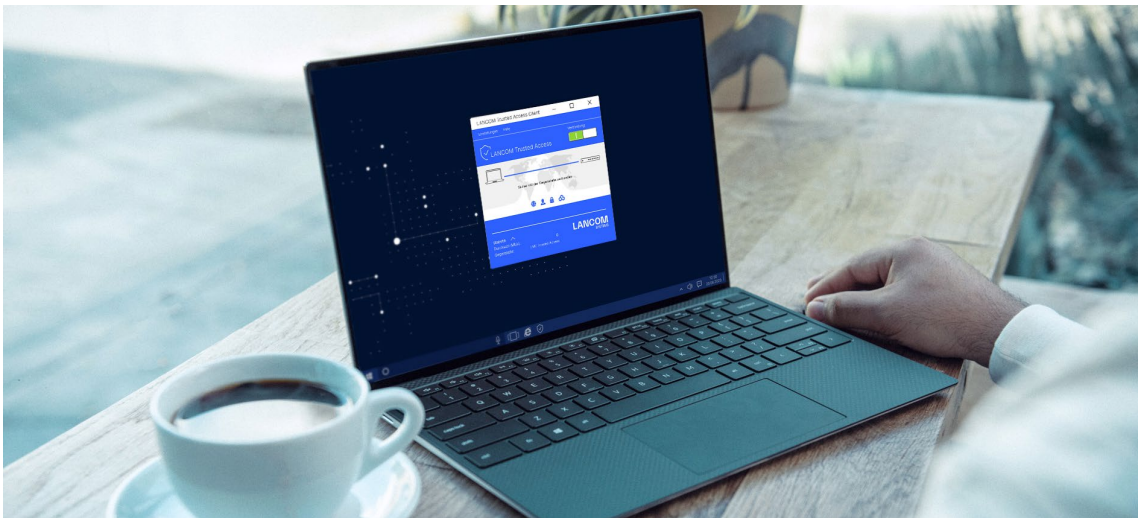
LANCOM Trusted Access 100% GDPR compliant and scales for small businesses as well as for very large networks with several thousand users.

Highlights

- → **Flexibly scalable secure network access solution** for enterprise networks, that adapts to increasing security requirements
- → **Choice of granular access control** to dedicated applications (Zero Trust principle) or entire networks (cloud-managed VPN client)
- → **Lateral protection** from internal spread of malware in connection with micro-segmentation
- → **Migrates seamlessly into existing installations** by integrating existing user databases in the company
- → **Endpoint security and multi-factor authentication** for a high level of security
- → **Easy access to external cloud applications** via single sign-on (SSO) without entering additional credentials
- → **Trusted Internet Access with Full Tunnel mode** for mobile working as secure as in the office
- → **Full integration into the LANCOM Management Cloud (LMC)** for zero-touch deployment and auto-configuration for easy and fast rollout of new remote access connections
- → **100% GDPR compliant** – data traffic runs without decoupling via an external cloud

lancom-systems.com

LANCOM Trusted Access Client



Granular access control to applications according to the Zero Trust principle

With access granted according to the Zero Trust principle **“as much as necessary, as little as possible“**, the LANCOM Trusted Access Client protects networks from threats and their spread. This means: No blind trust based on successful network access.

The LANCOM Trusted Access Client allows access controls to be implemented at a very granular level (“software-defined perimeter“, SDP). This means that users can only access the applications and resources they need to perform their work, and that each access must be explicitly authorized.

What is “Zero Trust“?

Gartner defines Zero Trust as a security concept that focuses on the assumption that nothing and no one inside or outside the network can be trusted. Essentially, this means that any access to resources on the network – whether from outside or inside – must always be **authorized and authenticated** before it is allowed.

Compared to a classic VPN, the Zero Trust principle differs in that users or devices are **not granted access to entire networks**, but only to specific applications or network resources.

Such a **micro-segmentation** eliminates the need for enterprise servers to be interconnected in an intranet. This prevents the unhindered spread of ransomware throughout the intranet if one server is compromised. Thus, protection against so-called **lateral movement** is provided.

LANCOM Trusted Access Client

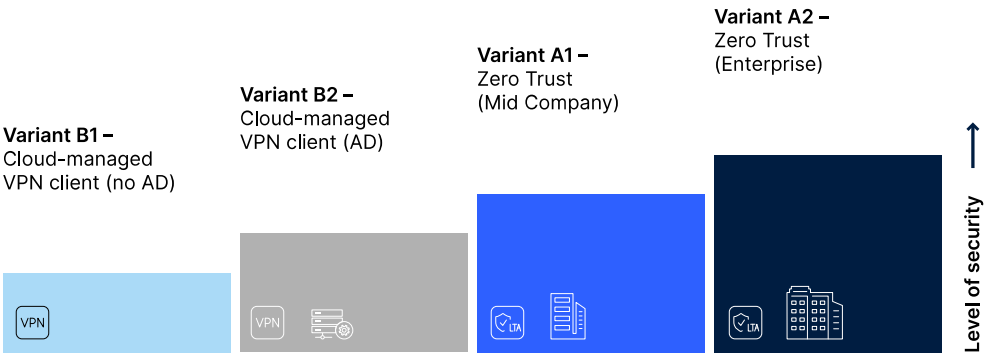
Network security tailored to your needs

Switching from classic VPN clients to a zero-trust model usually means a costly complete rebuild of a network's entire security architecture. However, this is not the case with LANCOM Trusted Access.

LANCOM Trusted Access allows a **direct transition to a Zero Trust security architecture**, because this solution grows with your security requirements. 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**.

Get started with LANCOM Trusted Access:
Which level of integration fits your use case?

Depending on user management, implementation of stricter security policies, and company size, four different variants are available:



You will find out how to optimally integrate LANCOM Trusted Access into your infrastructure at www.lancom-systems.com/lta-onboarding. By answering the interactive questionnaire and in just a few clicks you will receive your appropriate level and **access to tutorial videos**.

Usage as a cloud-managed VPN client

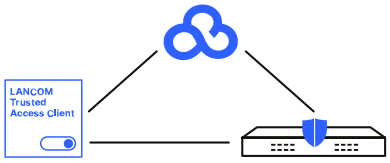
The LANCOM Trusted Access Client can optionally also be used as a cloud-managed VPN client, thus enabling the VPN connections of mobile employees to be managed securely and centrally. This means that configuration updates can be carried out easily and efficiently, or new users can be added or removed simply, without the need for an IT administrator or the end device to be physically on site. This convenient management coupled with transparent user monitoring via the LANCOM Management Cloud reduces your operating costs, as **all of your company's VPN clients are centrally accessible at a glance.**

lancom-systems.com

LANCOM Trusted Access Client

System architecture LANCOM Trusted Access

Everything you need to implement a LANCOM Trusted Access security architecture is a Trusted Access Gateway (router or firewall), the LANCOM Management Cloud (LMC), and the LANCOM Trusted Access Client.



Only the data exchange for user authentication takes place via the LMC (Control Plane). The subsequent data traffic takes place without decoupling via an external cloud (Data Plane).

Further information can be found in the tech paper LANCOM Trusted Access System architecture.

Trusted Internet Access: Mobile working as secure as in the office

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'.

Endpoint security and multi-factor authentication for a high level of security

Before a user is granted access, endpoint security can be verified (operating system version, anti-virus, local firewall). Each user must also have **their identity verified** before being granted access to an application or resource. Applications and resources are not made visible network-wide, making the network invisible to attackers. Additionally, two-factor or multi-factor authentication with fingerprint, facial recognition, or an authentication app on the smartphone may be required at login.

Integration of existing user databases

User authentication is performed via a central user database ("identity provider", e.g. an Active Directory such as Microsoft Entra ID (formerly Azure AD)). User groups taken over from the identity provider can be provided with individual access rights to the permitted applications. The validity period of an authentication can be set, and clients can also be blocked manually or automatically. For small companies without a central user database, user management integrated into the LANCOM Management Cloud is available as an alternative.

lancom-systems.com

LANCOM Trusted Access Client

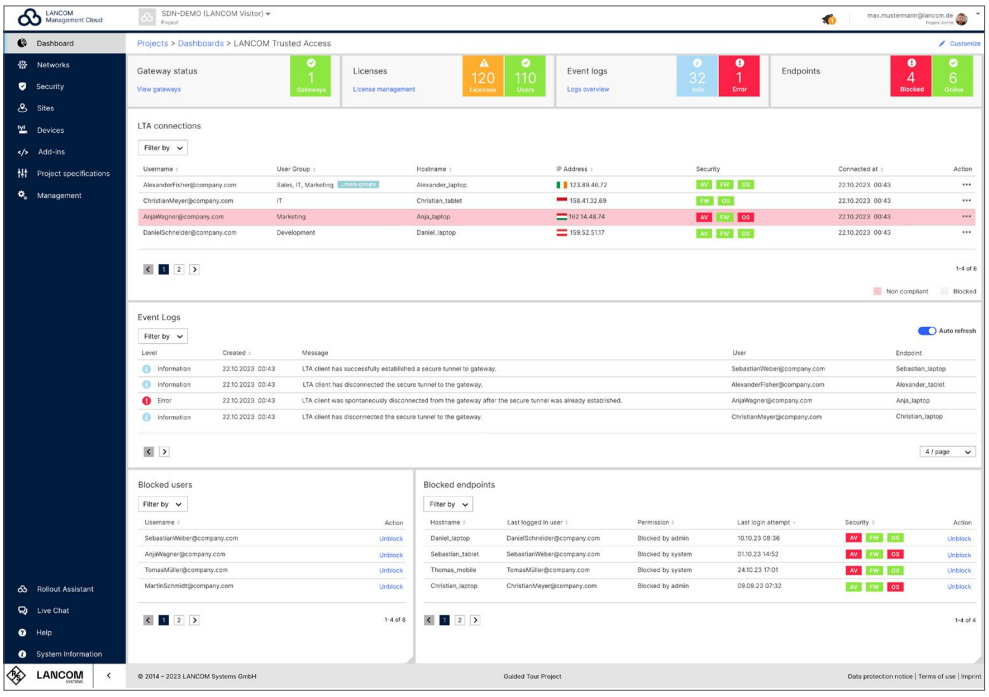
Easy access to external cloud applications via single sign-on (SSO)

The LANCOM Trusted Access Client handles the login processes for password-protected applications: Via single sign-on (SSO), users can access external web applications conveniently and securely after logging on once to the Active Directory – without having to re-enter their credentials. This ensures particularly **user-friendly and fast work processes.**

Seamless integration into the LANCOM Management Cloud

The LANCOM Management Cloud (LMC) provides **fully integrated management** of all LANCOM network components (routers / gateways, firewalls, switches, and access points) including the LANCOM Trusted Access Client. The management of the underlying security policies for all users in the network is also carried out centrally via the LMC.

A LANCOM Trusted Access **Real-Time Dashboard** is available to administrators for comprehensive diagnostics and troubleshooting. The dashboard displays active connections with user name, IP address, device name, and user group, and provides additional information such as compliance status and last login. Furthermore, clients can be blocked both manually and automatically, information on the number of users and blocked connection requests is available, as well as central license management and monitoring.

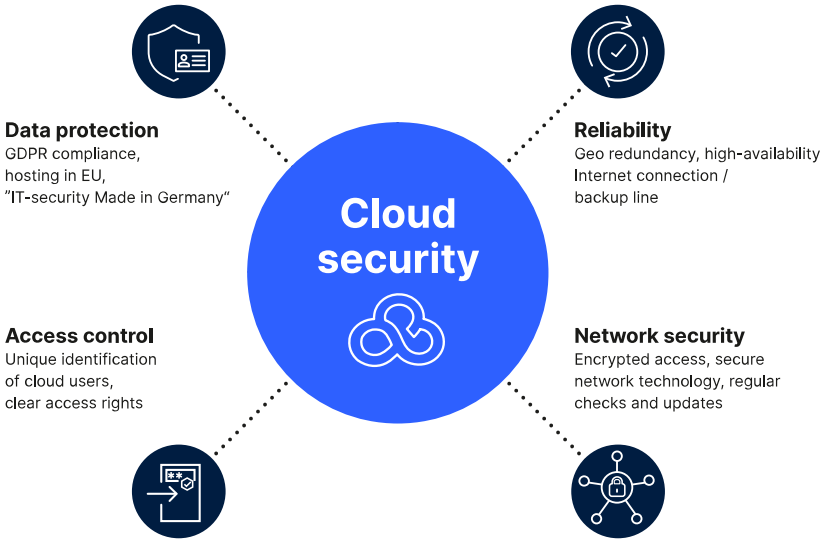


LANCOM Trusted Access Client

100% Digital Sovereignty, 100% 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.

Only the data exchange for user authentication takes place via the LMC; all other user data runs directly between the LANCOM Trusted Access Client and the LANCOM Trusted Access Gateway – without decoupling via an external cloud. The LANCOM Trusted Access Client thus stands for the **highest level of data security and data protection**. It is subject to and complies with European legal standards, is therefore DSGVO compliant, and is a convincing **IT security solution engineered in Germany**.



For more information, please refer to the Infopaper LMC (Public) Data Protection and Data Security.

LANCOM Trusted Access Client

LANCOM Trusted Access level of integration

Attributes / Application scenarios	Variant B1 – Cloud-managed VPN client (no AD)	Variant B2 – Cloud-managed VPN client (AD)	Variant A1 – Zero Trust (Mid Company)	Variant A2 – Zero Trust (Enterprise)
Deployment recommendation	Small and medium-sized enterprises	Small and medium-sized companies	Medium-sized companies	Large Enterprises
Requirements and technical expertise	→ Experience with the LMC	→ Experience with the LMC → Experience with Microsoft Entra ID (formerly Azure AD) and if necessary Microsoft Entra ID Connect	→ Experience with the LMC → Experience with Microsoft Entra ID (formerly Azure AD) and if necessary Microsoft Entra ID Connect	→ Experience with the LMC → Experience with Microsoft Entra ID (formerly Azure AD) and if necessary Microsoft Entra ID Connect
User administration	→ Locally via the LMC	→ Active Directory	→ Active Directory	→ Active Directory
Access rights	→ Full access intranet → (Alternative: Dedicated application approval	→ Full access intranet → (Alternative: Dedicated application approval)	→ Dedicated application approval	→ Dedicated application approval → Subdivision into microsegments (Private VLAN)
Core functions	→ Cloud-managed VPN client → Endpoint security check (software updates, antivirus)	→ Cloud-managed VPN client → Endpoint security check (software updates, antivirus) → Connection to Active Directory → Single sign-on	→ Cloud-managed VPN client → Endpoint security check (software updates, antivirus) → Connection to Active Directory → Single sign-on → Application approval for user groups	→ Cloud-managed VPN client → Endpoint security check (software updates, antivirus) → Connection to Active Directory → Single sign-on → Application approval for user groups → Micro-segmentation
Complexity	Low	Medium	High	Very high

LANCOM Trusted Access Client

Features	
Zero-touch auto-configuration	→ Easily and quickly roll out new remote access connections via zero-touch auto-configuration. Note: → This means that the user can connect an installed client (freely downloadable or alternatively installed by central IT via a software distribution such as Baramundi) to the target applications simply by entering the access data. → Administrator rights are required to install the client on a computer. → The user name must include the domain (e.g. via the e-mail address) so that the LANCOM Management Cloud (LMC) can find the matching project with the domain.
Connection of existing AD users or LMC-internal users	→ Seamless integration of existing user databases (via Microsoft Entra ID (formerly Azure AD)) → Alternative user management within the LANCOM Management Cloud (without AD) Note: → In the case of an AD connection, it must be ensured that a suitable group structure or affiliation is stored in the AD, which is then used by the LMC to activate the application releases for the user groups. → When using the LMC-internal LANCOM Trusted Access (LTA) user management (i.e. without AD), the following functions are not available, as they are based on Microsoft Entra ID functions: single sign-on and multifactor authentication
Software-defined perimeter	Central and dynamic control of access rights and profile deployments. Client access takes place at the application or service level. The associated enforcement takes place through the LTA gateways, which implement the corresponding application and service releases through connection targets based on URLs, IP addresses, ports, and protocols. Further functions: → LMC internal PKI (fully automatic) → Micro-segmentation (Private VLAN) through manual port isolation of switches on the LAN → SSO agent (via Microsoft Entra ID)
Central user monitoring	→ LTA dashboard in the LANCOM Management Cloud → Display of the accessing remote endpoints → Display of active connections with user name, IP address, device name, user group, and further information (compliance status, last login) → Display of the license status → The LTA dashboard can only be viewed by IT administrators.
Endpoint security	→ Compliance enforcement (preventing LTA clients with missing operating system updates from dialing in) → Conditional access by checking security parameters such as activated system firewall, anti-virus status, or operating system updates → Blocking of LANCOM Trusted Access users (directly from the LMC, independent of the AD status of the user)
Protective mechanisms	→ Multi-factor authentication (via Microsoft Entra ID)
Highest encryption standards	→ Integrated certificate management (PKI) → State-of-the-art cryptography according to BSI TR 02-102 (recommendation of the German Federal Office for Information Security)
Software and security updates	All general software and security updates of the LANCOM Trusted Access Client, the LMC, and the LANCOM Trusted Access Gateways are included over the licensed client lifetime

LANCOM Trusted Access Client

MSI installer	The MSI installer can provide additional information during the installation via command line option (for software management systems): → LANCOM_PRODUCT_TYPE=AVC → LANCOM_PRODUCT_TYPE=LTA → MGMCLOUD_URL=cloud.lancom.de → MGMCLOUD_DOMAIN=mycompany.com
Operation mode	→ Split tunneling: Internet traffic is decoupled directly at the LTA client. → Full tunneling: All traffic is always routed via the LTA gateway. In combination with security functions such as Anti Virus or Content Filter activated on the LTA gateway (LCOS or LCOS FX), the operating mode is called ‚Trusted Internet Access'.
Supported gateways	VPN routers / gateways or Unified Firewalls (hardware or vRouter / vFirewall) with the following operating system versions: → LCOS as from 10.80 → LCOS FX as from 10.13
Supported Identity Provider (IdP)	→ Microsoft Entra ID (formerly Azure AD) → The connection to local AD servers is done via Microsoft Entra ID Connect (formerly Azure AD Connect). → Alternatively, an integrated local user table is available in the LMC for small installations.
Supported operating systems	→ Microsoft Windows 10 / 11 (on Intel x86-64 processor architecture) → MacOS (in preparation, different functionality possible)

Licenses Up to three devices can be used in parallel per user. A separate pay-per-use license model is available for LANCOM partners with a Service Provider License Agreement.		**Item no.**
LANCOM LTA-CL-1Y 1 License	License for 1 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 1 year runtime	50400
LANCOM LTA-CL-1Y 10 Licenses	License for 10 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 1 year runtime	50401
LANCOM LTA-CL-1Y 25 Licenses	License for 25 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 1 year runtime	50402
LANCOM LTA-CL-1Y 100 Licenses	License for 100 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 1 year runtime	50403
LANCOM LTA-CL-1Y 250 Licenses	License for 250 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 1 year runtime	50404
LANCOM LTA-CL-1Y 1000 Licenses	License for 1000 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 1 year runtime	50405
LANCOM LTA-CL-3Y 1 License	License for 1 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 3 years runtime	50410

LANCOM Trusted Access Client

LANCOM LTA-CL-3Y 10 Licenses	License for 10 LANCOM TrustedAccess users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 3 years runtime	50411
LANCOM LTA-CL-3Y 25 Licenses	License for 25 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 3 years runtime	50412
LANCOM LTA-CL-3Y 100 Licenses	License for 100 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 3 years runtime	50413
LANCOM LTA-CL-3Y 250 Licenses	License for 250 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 3 years runtime	50414
LANCOM LTA-CL-3Y 1000 Licenses	License for 1000 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 3 years runtime	50415
LANCOM LTA-CL-5Y 1 License	License for 1 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 5 years runtime	50420
LANCOM LTA-CL-5Y 10 Licenses	License for 10 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 5 years runtime	50421
LANCOM LTA-CL-5Y 25 Licenses	License for 25 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 5 years runtime	50422
LANCOM LTA-CL-5Y 100 Licenses	License for 100 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 5 years runtime	50423
LANCOM LTA-CL-5Y 250 Licenses	License for 250 LANCOM Trusted Access-Users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC-Project-ID and email adress for receipt, 5 years runtime	50424
LANCOM LTA-CL-5Y 1000 Licenses	License for 1000 LANCOM Trusted Access users in the LANCOM Management Cloud, secure remote access (zero-trust principle or cloud-managed VPN), order only possible under specification of LMC project ID and e-mail address for receipt, 5 years runtime	50425

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