Libraesva Admin Support Account

This article describes why having a Libraesva support administrative account on customer Virtual Appliances hosted on the Libraesva cloud is not optional, but a fundamental part of the cloud service. This document also describe how access to these accounts is strictly controlled, highly secure, and used only by highly qualified and secured employees at Libraesva.

Libraesva provides its solutions only as a **partially-managed cloud solution** OR on-premise solution.

When the End User opt for the **partially-managed cloud solution** and sign the End User Libraesva Cloud Service Activation Form and License Agreement, the End User grants Libraesva the following:

1. Provision the service
2. Run the service
3. Ensure, preserve, update the service
4. Facilitate availability, integrity, and performance of the solution

These tasks cannot be satisfied without the privilege of technical access to the solution involved.

It would, in fact, be contradictory to make use of the service and deny us administrative access.

Nature of the Libraesva Support Account

The Libraesva support account is:

- **Owned by the provider** (not a customer account)
- **Only used for specific purposes** (support, maintenance, security, incident response)
- **Non-interactive by default**
- **Heavily restricted and monitored**

It is not a shared or generic account, neither accessible by ordinary personnel.

Extremely Restricted Human Access

Only a **very small, elite subset of Libraesva employees** may ever access cloud customers' VMs.

These individuals:

- Are senior engineers and certified security specialists
- Are formally authorized and vetted
- Are contractually bound by strict confidentiality obligations
- Operate under internal security policies exceeding standard industry practices

There is **no anonymous, automated, or casual access**.

Bastion Host Enforcement

All support connections **must go through a dedicated bastion host**.

The bastion host:

- Acts as the single controlled entry point
- Terminates and re-establishes encrypted sessions
- Enforces strong authentication at multiple layers
- Validates user identity, role, and authorization in real time
- Rejects all connections that fail any verification step

There is **no direct access** to cloud customers VMs under any circumstance.

End-to-End Encryption

All connections are:

- Encrypted in transit
- Protected against interception and tampering
- Established using modern cryptographic standards

No plaintext access paths exist at any layer.

Auditing, Accountability, and Traceability

Every support session is:

- Logged
- Attributed to a specific individual
- Subject to internal review

This ensures **full accountability and non-repudiation**.

Why This Protects the Customer

Rather than increasing risk, Libraesva's support access account ensure:

- **Reduces downtime and guarantee contractual service levels**
- **Enables rapid incident response to zero-day threats**
- **Prevents security escalation**
- **Ensures service continuity during outages**
- **Protects customer data and reputation**