LOADBALANCER

ADC PORTAL

The importance of keeping your organizational and private keys safe

Zero-trust architecture

The ADC Portal is based on the Zero Trust Security model, and utilizes end-to-end encryption (E2EE).

This ensures all data within the Portal is always encrypted, both at rest and in transit, meaning Loadbalancer.org can never see or read your data.

Key creation and encryption

The ADC Portal utilizes 4 established keys. These keys provide the ability to encrypt and decrypt data sent from the client to the Portal and back again, via the load balancer:

1. A public and private organization key
2. A public and private user key
3. A public and private organization intermediate key
4. A public and private Shuttle key

All of which are transmitted/sent over a TLS encrypted connection.

Organization key

An organization key, generated by the client, encrypts all organization-related data. Loadbalancer has no access to this key and is only aware of its existence.

User key

When a user is then invited by the organization to join an 'organization account', a unique pair of user keys are generated for that user.

Once the user has logged in and been verified, these ECC public and private PGP encrypted keys are then stored as a session by the client.

The user key then allows the user to encrypt a copy of the organization key, in order to read the organizational metadata.

Passwords and authentication

Unlike most SaaS solutions, user credentials never leave the user's device. Passwords are encrypted and a split remainder performed to later utilize for user authentication purposes by the Loadbalancer Portal.

Account recovery

Loadbalancer does not have access to the account or password data held by the client. **It is therefore very important that the client stores their organization and user keys securely.**

It is not possible for the client to simply assign a new password. However, you can assign a new password to your account assuming you use our recovery process and are happy to share your original keys with us.

It is therefore important to reiterate that when you create your account you must keep your keys saved somewhere safe, as these will give you the ability to recover your account.

> *In creating the ADC Portal, security has been paramount in our thinking. The development process has followed not only zero trust principles, but also, where possible, leveraged multiple layers of security.*
>
> *Such comprehensive security does however, place an onus on the user to safeguard their passwords, as well as their organizational and user keys!"*
>
> **Andrew Zak,**
> **Head of Development**