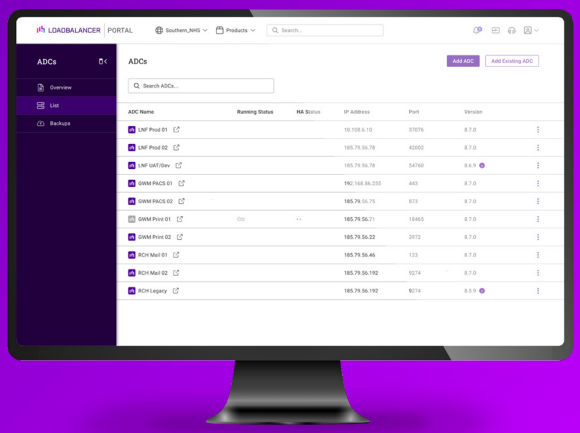
LOADBALANCER

The ADC Portal



State-of-the-art cryptographic technology for smarter end-to-end enterprise security and protection.

What is the Loadbalancer ADC Portal?

The ADC Portal is an ultra-secure, cloud-based subscription service (SaaS).

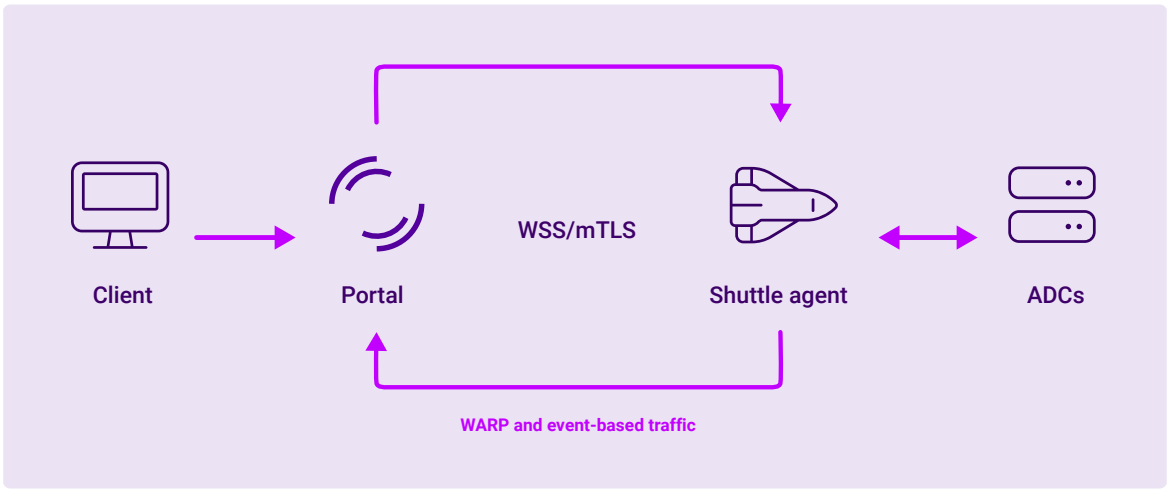
Zero trust protection

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.

Passwords and authentication

User passwords are never transmitted over the internet so, unlike most SaaS solutions, user credentials never leave the user's device.



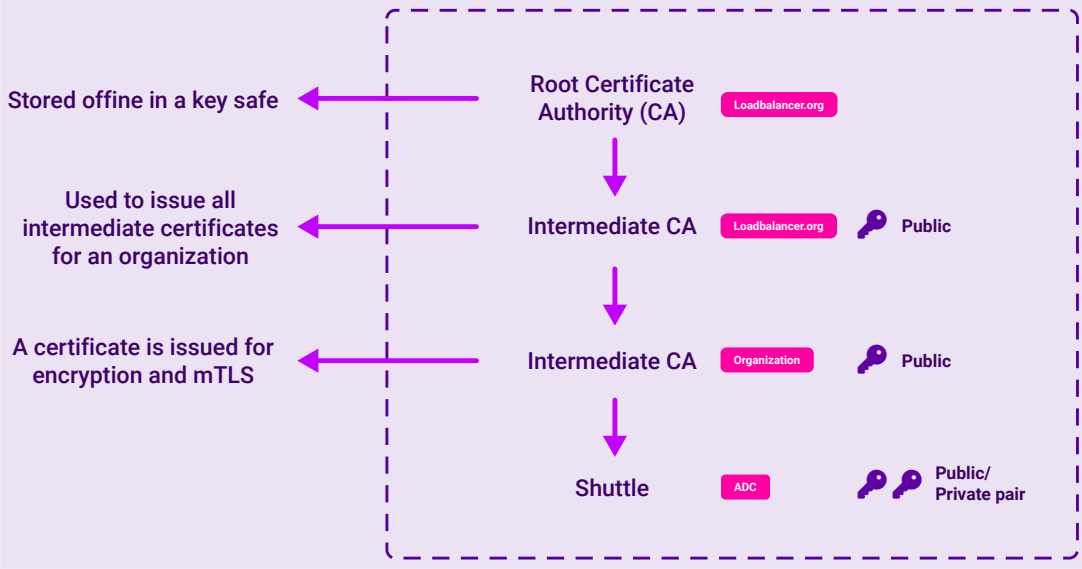
Secure WebSocket Security

All communication takes place via a secure WebSocket protocol (WSS) with mTLS.

This double layer of authentication provides an additional layer of protection against impersonation attacks.

Once the two-way authentication process has taken place and a secure connection established, two methods of communication then occur within the encrypted WSS channel:

1. Remote HTTP proxy
2. Event-driven requests



PGP encryption

In addition to secure WebSocket Security (WSS) with mTLS, the Portal also contains a second, additional layer of security called PGP encryption, which allows for multiple levels of encryption using a series of public, intermediary, and private keys.

Once the initial mTLS handshake has been completed, a Loadbalancer.org sidecar agent called the Shuttle creates its own PGP keys, which are then used for communication and verification with the ADCs.

This Certificate Chain enables the receiver to verify that the sender and all Certificate Authorities are trustworthy.

Governance and compliance

The Loadbalancer Portal leverages an advanced cloud authentication and network communications model that has been built for the highest levels of privacy, security and trust.

Loadbalancer.org is an ISO 13485 and ISO 9001 certified company, actively working towards ISO 27001. We hold our Quality Management System (QMS) in high regard and carry out regular security audits and penetration tests internally and with independent third-parties.

We also adhere to the SOC2 principles of security, availability, processing integrity, confidentiality, and privacy.

Features

Example features include:

Zero trust architecture

- All data encryption/decryption occurs within the client's environment using unique 256-bit ECC Account Keys.

Single sign-on (SSO)

- Offered through Google and Microsoft Azure ADC.

Multi-factor authentication

- Two-factor authentication is available via SMS or an authenticator app.

We needed a secure, single pane of glass to equip us with the tools to better manage and protect our diverse ADC estate. Because the Loadbalancer ADC Portal is vendor-agnostic, this gave us maximum visibility and control for a far greater return on investment."

IT Director
Medical imaging vendor