Security

Redis Enterprise Cloud provides a number of ways to secure subscriptions and databases.

As a Redis Cloud user, here are a few things to consider when thinking about security:

- The admin console
- Your databases
- The Redis Cloud API

Before digging into all the details, you should review our shared responsibility model for security.

Admin console security

The admin console is the web application you use to manage your Redis Cloud deployments.

Secure access to the admin console by:

- Assigning appropriate roles to team members with access
- Enabling multi-factor authentication

Database security

You have several options when it comes to securing your Redis Cloud databases. These include:

- encryption at rest
- role-based access control
- network security
- TLS
- network security using VPC peering and CIDR whitelist

API security

The Redis Enterprise Cloud API allows you to programatically administer your subscriptions and database deployments. This API is disabled by default. When you enable the API, you can then manage the API keys for all owners of your Redis Cloud account. For an overview of the security features of the API, see the API authentication documentation.

Updated: January 12, 2022