Authentication

Authentication is a critical aspect of our platform, ensuring secure access to resources. Currently, there are two primary methods for authentication: the usage of JSON Web Tokens (JWT) through the giza users login command and the utilization of API keys.

What are JWT and API keys?

- JWT (JSON Web Token)
- : A JWT is a compact, URL-safe means of representing claims between two parties. In the context of our platform, it serves as a secure authentication token obtained through the giza users login command. This token is then used to establish and maintain a secure communication channel with the platform.
- API Key
- : An API key is a unique alphanumeric code generated by the platform that provides a secure way for applications or users to authenticate themselves. Once created, an API key serves as a credential to communicate with the platform, eliminating the need for repeated login procedures.
-

Key Differences

The primary distinction between JWT and API keys lies in their nature and usage:

- JWT is a token-based authentication mechanism that is time-sensitive and typically used for short-lived authentication sessions.
- API keys, on the other hand, are static credentials that persist and provide a more long-term solution for authentication without the need for frequent renewals.
-

How to authenticate

For information about using the CLI to authenticate yourself please refer to the users documentation.

Previous Installation Next Frameworks

Last updated18 days ago