Settings (Developers)

Overview

The **Developers** section provides API credentials required for integrating the application with external systems, custom applications, or third-party services. It allows administrators and developers to securely access the application's APIs using generated authentication credentials.

Navigate to **Settings → Developers** to manage API credentials.

API Credentials

The **API Credentials** section contains the authentication details required for API access.

The following credentials are available:

Field	Description
API Key	A unique key used to identify and authenticate API requests.
API Token	A secure authentication token used to authorize API access.

These credentials are required when connecting external applications or services with the platform.

Generate API Token

Click **Generate API Token** to create a new API token.

A newly generated token can be used for secure API authentication. If an existing token is regenerated, the previous token may no longer be valid.

Manage API Credentials

Administrators can:

- View the existing API Key.
- Generate a new API Token.
- Use API credentials for application integrations.
- Authenticate API requests securely.

Best Practices

- Keep API credentials confidential.
- Do not share API Keys or API Tokens publicly.
- Regenerate the API Token if it is compromised.
- Use API credentials only in trusted applications and integrations.

> **Important:**
> The **API Key** and **API Token** are used to authenticate API requests. After generating a new API Token, ensure that all integrated applications are updated with the latest credentials.

Revision #2
Created 2026-07-13 05:07:34 UTC by Akshit Jain
Updated 2026-07-23 10:50:22 UTC by Akshit Jain