Enable API Access Tokens

Contents:

For secure and flexible access to the REST APIs of the Trifacta® platform, you can enable access tokens. Each request via API requires some form of authentication. By using API access tokens, you can ensure that transfer of authentication information is minimized and obscured, and you can control the lifespan of these tokens.

> **Tip:** Access tokens are the recommended method for managing access to the REST APIs.

- For more information on all supported forms of authentication via API, see *API Authentication*.
- For more information on how to use access tokens, see *Manage API Access Tokens*.

Enable

Steps:

1. You apply this change through the *Workspace Settings Page*. For more information, see *Platform Configuration Methods*.
2. Locate the API Access Token setting, and set it to `true`.
3. Save changes and restart the platform.

Create and Use

Via UI

You can create and delete tokens for personal use through the Settings area in the Trifacta application. For more information, see *Access Tokens Page*.

Via API

You can manage your access tokens through a specified set of REST APIs. See *Manage API Access Tokens*.

Disable

To disable this feature, please set the above setting to `false`.

> **NOTE:** Disabling this feature prevents all API users from using their tokens to access any endpoints.