Manage API Access Tokens

Contents:

This section provides some workflow information for how to use API access tokens as part of your API projects in Trifacta®. An **access token** is a hashed string that enables authentication when submitted to any endpoint. Access tokens limit exposure of clear-text authentication values and provide an easy method of managing authentication outside of the browser.

Notes:

- An access token is linked to its creator and can be generated by submitting a username/password combination or another valid token from the same user.
  - If a token is created for userA, userB can be provided the token to impersonate userA.
  - You cannot create access tokens for users without their authentication credentials.
  - Changes to passwords do not affect tokens.
- After a token has been created, it cannot be modified or extended.
  - You can create an unlimited number of tokens.
- Access tokens can be used for authentication with any supported version of the APIs.

Enable

This feature must be enabled in your instance of the platform. For more information, see *Enable API Access Tokens*.

Enable individual access

When access tokens are enabled, by default only administrators are permitted to generate tokens. Optionally, workspace administrators can enable individual users in the workspace to generate and use their own API access tokens. For more information, see *Workspace Settings Page*.

Generate New Token

API access tokens must be created.

> **NOTE:** The first time that you request a new API token, you must submit a separate form of authentication to the endpoint. To generate new access tokens after you have created one, you can use a valid access token if you have one.

Via API

For more information, see *https://api.trifacta.com/ee/8.2/index.html#operation/getApiAccessToken*

Via UI

Tokens can be generated from the web application.

Steps:

1. Login to the Trifacta application.
2. From the left nav bar, select **User menu > Preferences > Access Tokens**.
3. Click **Generate New Token**.
4. Specify the number of days for how long the token should live.

   > **Tip:** Depending on how your environment is configured, you may be able to enter `-1` to create a non-expiring token.

5. Add a user-friendly description if desired.
6. Click **Generate**.

> **NOTE:** Copy the value of the token to the clipboard and store it in a secure location for use with your scripts. For security reasons, the token value itself cannot be retrieved from the application after it has been created.

> **Tip:** If you wish to manage your token via the APIs, you should copy the Token ID value, too. The Token ID can always be retrieved from the Trifacta application.

For more information, see *Access Tokens Page*.

Use Token

After a token has been acquired, it must be included in each request to the server, for as long as it is valid.

> **NOTE:** After a token has been created, it cannot be extended or modified.

> **NOTE:** API access tokens are not used by users through the Trifacta application.

> **NOTE:** When using the APIs in SSO environments, API access tokens work seamlessly with platform-native versions of SAML and LDAP-AD. They do not work with the reverse proxy SSO methods. For more information, see *https://api.trifacta.com/ee/8.2/index.html#section/Authentication*

After you have acquired the token, you submit it with each API request to the platform.

Example - cURL:

The following example returns a JSON version of the list of available REST API endpoints for your environment:

```
curl http://tri.example.com:3005/v4/open-api-spec -X GET -H "Authorization: Bearer (tokenValue)"
```

- `(tokenValue)` is the value returned for the token when it was created.

Example - REST client:

If you are submitting your API calls through a REST client, the Authorization header must be specified as follows:

```
Authorization: Bearer (tokenValue)
```

List Tokens

> **NOTE:** For security reasons, you cannot acquire the actual token through any of these means.

> **Tip:** You can see all of your current and expired tokens through the Trifacta application. See *Access Tokens Page*.

Endpoint	Description
https://api.trifacta.com/ee/8.2/index.html#operation/listApiAccessTokens	List all access tokens for your user account.
https://api.trifacta.com/ee/8.2/index.html#operation/getApiAccessToken	List your access token for the specified token ID.

Renew Token

New tokens can be acquired at any time.

> **NOTE:** It is the responsibility of the user to acquire a new API token before the current one expires. If a token is permitted to expire, a request for a new token must include userId and password information.

- See *https://api.trifacta.com/ee/8.2/index.html#operation/createApiAccessToken*
- See *Access Tokens Page*.

Delete Token

- **Via API:** Acquire the `tokenId` value for the token and use the delete endpoint. See *https://api.trifacta.com/ee/8.2/index.html#operation/deleteApiAccessToken*
- **Via UI:** In the Access Tokens page, select **Delete Token...** from the context menu for the token listing. See *Access Tokens Page*.