

Databricks Personal Access Token Page

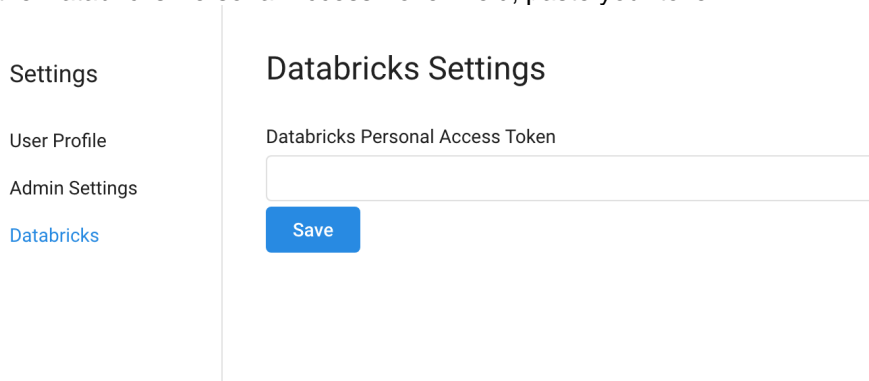
Each user of the Trifacta® platform must insert their personal access token into their User Settings page. This configuration enables the user to authenticate using the Azure Databricks REST APIs, which enables the execution of jobs and, if enabled, access to a Databricks connection.

NOTE: Each user must apply a personal access token to their User Profile. Users that do not provide a personal authentication token cannot run jobs on Azure Databricks, including transformation, sampling, and profiling jobs.

NOTE: When you reset your personal access token, your personal cluster is no longer valid, and a new cluster must be created for you. This new cluster is created when you first request access to the Azure Databricks cluster. The next time that you use interfaces that require the cluster, such as the relational browser, may take some time to load.

Steps:

1. Acquire your Azure Databricks personal access token. For more information, see <https://docs.azuredatabricks.net/api/latest/authentication.html#requirements>.
2. Login to the application. From the menu bar, select **Settings menu > Settings**.
3. Click **Databricks**.
4. In the Databricks Personal Access Token field, paste your token.



The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes 'Settings', 'User Profile', 'Admin Settings', and 'Databricks' (which is highlighted in blue). The main content area is titled 'Databricks Settings' and contains a form with a label 'Databricks Personal Access Token' above a text input field. Below the input field is a blue 'Save' button.

Figure: Databricks user configuration

5. Click **Save**.

Azure Databricks personal access tokens are saved in the Azure key vault.