

# Authentication using Azure Databricks personal access tokens

07/09/2020 • 2 minutes to read •  

## In this article

[Requirements](#)

[Generate a personal access token](#)

[Revoke a personal access token](#)

[Use a personal access token to access the Databricks REST API](#)

To authenticate to and access Databricks REST APIs, you can use Azure Databricks personal access tokens or Azure Active Directory (Azure AD) tokens.

This article discusses how to use Azure Databricks personal access tokens. For Azure AD tokens, see [Authentication using Azure Active Directory tokens](#).

### Important

Tokens take the place of passwords in an authentication flow, and like passwords, they should always be treated with care. To protect tokens, Databricks recommends that you store tokens in:


- **Secrets** and retrieve tokens in notebooks using the **Secrets utilities**.
- A local key store and use the **Python keyring** package to retrieve tokens at runtime.

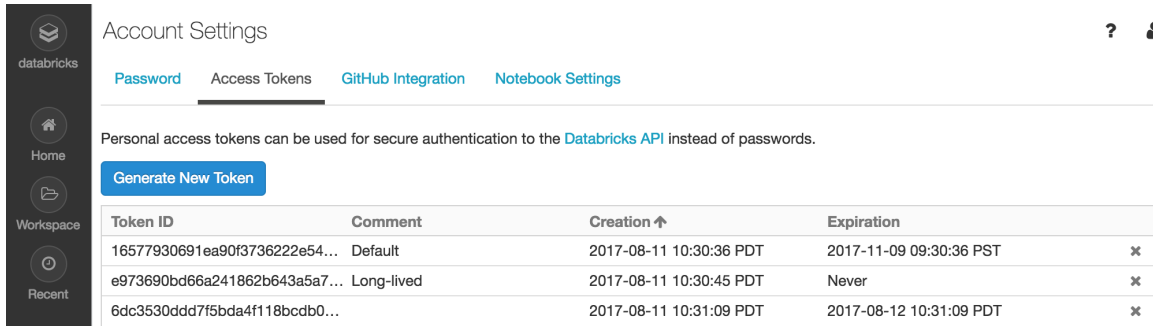
## Requirements

Token-based authentication is enabled by default for all Azure Databricks accounts launched after January 2018. If it is disabled, your administrator must enable it before you can perform the tasks described in this article. See [Manage personal access tokens](#).

## Generate a personal access token

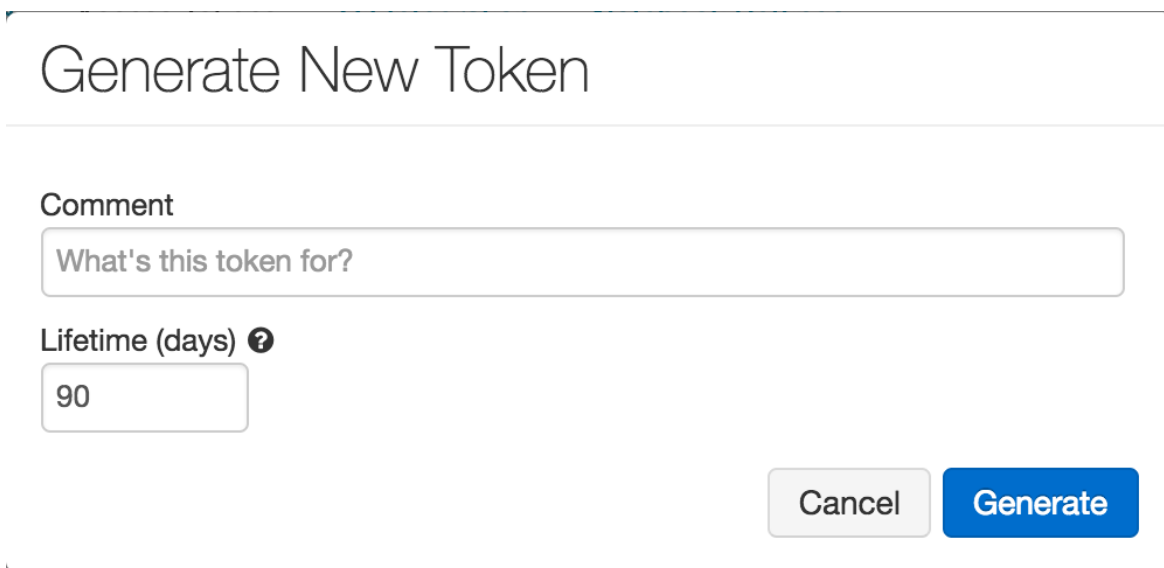
This section describes how to generate a personal access token in the Azure Databricks UI. You can also generate and revoke tokens using the [Token API](#).

1. Click the user profile icon  in the upper right corner of your Azure Databricks workspace.
2. Click **User Settings**.
3. Go to the **Access Tokens** tab.



Token ID	Comment	Creation ↑	Expiration
16577930691ea90f3736222e54...	Default	2017-08-11 10:30:36 PDT	2017-11-09 09:30:36 PST
e973690bd66a241862b643a5a7...	Long-lived	2017-08-11 10:30:45 PDT	Never
6dc3530ddd7f5bda4f118bcd0...		2017-08-11 10:31:09 PDT	2017-08-12 10:31:09 PDT


4. Click the **Generate New Token** button.
5. Optionally enter a description (comment) and expiration period.



6. Click the **Generate** button.
7. Copy the generated token and store in a secure location.

## Revoke a personal access token

This section describes how to revoke personal access tokens using the Azure Databricks UI. You can also generate and revoke access tokens using the [Token API](#).

1. Click the user profile icon  in the upper right corner of your Azure Databricks workspace.


2. Click **User Settings**.
3. Go to the **Access Tokens** tab.
4. Click **x** for the token you want to revoke.
5. On the Revoke Token dialog, click the **Revoke Token** button.

## Use a personal access token to access the Databricks REST API

You can store a personal access token in `.netrc` and use in `curl` or pass it to the `Authorization: Bearer` header.

### Store token in `.netrc` file and use in `curl`


Create a `.netrc` file with `machine`, `login`, and `password` properties:

ini	 Copy
<pre>machine &lt;databricks-instance&gt; login token password &lt;personal-access-token&gt;</pre>	

where:

- `<databricks-instance>` is the `adb-<workspace-id>.<random-number>.azuredatabricks.net` domain name of your Azure Databricks deployment.
- `token` is the literal string `token`
- `<personal-access-token>` is the value of your personal access token.

To invoke the `.netrc` file, use `-n` in your `curl` command:

Bash	 Copy
<pre>curl -n -X GET https://&lt;databricks-instance&gt;/api/2.0/clusters/list</pre>	

### Pass token to Bearer authentication

You can include the token in the header using `Bearer` authentication. You can use this approach with `curl` or any client that you build. For the latter, see [Upload a big file into DBFS](#).

Bash

 Copy

```
curl -X GET -H 'Authorization: Bearer <personal-access-token>'
https://<databricks-instance>/api/2.0/clusters/list
```

---

Is this page helpful?

 Yes  No

---