Secure API Token Generation Using OAuth with PKCE

How to use OAuth Authorization Code Flow with Proof Key for Code Exchange (PKCE) to generate secure API tokens.

Document generated 12/06/2024

PDF VERSION

Tags | **API** | **Authentication** |

Applies to: Free Basic Business **Enterprise**

ADMIN PRIVILEGES REQUIRED

*This documentation is for **Stack Overflow for Teams Enterprise**. Free, Basic, and Business users can access their documentation here. Find your plan.*

Overview

Stack Overflow for Teams Enterprise API v3 and API v2.3 (write access) use OAuth authentication to generate access tokens. OAuth's implicit flow authentication exposes bearer tokens in URLs, which can make them susceptible to interception and impersonation. For better security, we recommend using OAuth's Authorization Code Flow with Proof Key for Code Exchange (PKCE) instead. This method generates a code verifier string, hashes it, and provides the hash during the authentication process. This ensures secure validation and exchange of tokens, mitigating the risk of impersonation and unauthorized access.

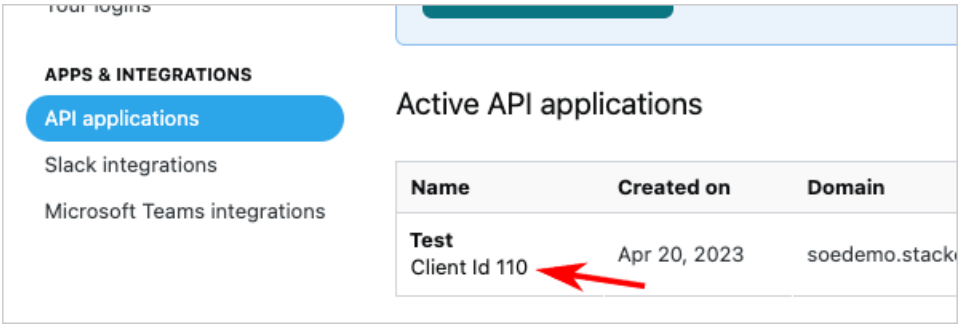
This guide explains how to generate a Stack Overflow for Teams Enterprise (SOE) API token using the Authorization Code Flow with PKCE method. You'll find it helpful to have a text file or other working document open to copy/paste values as you walk through the process.

Obtain a Client ID

1. On your SOE site, click on your avatar (profile pictures) to access your user profile.
2. Click **Settings** in the left-hand menu.
3. Click **API applications** (under the "APPS & INTEGRATIONS" heading).

Use an existing API application

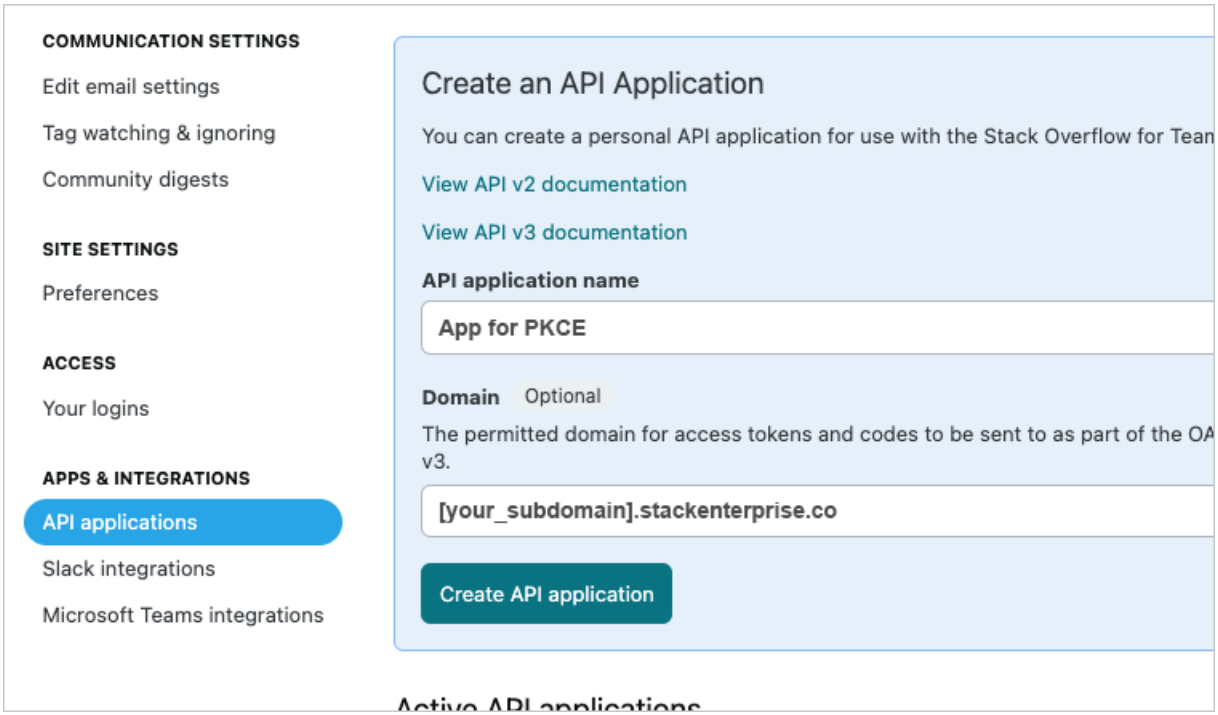
If you see an application already listed under the "Active API Applications" heading, copy the **Client ID** number (for example: 110) to your working document.



Create a new API application

If you don't see an application listed, you'll need to create a new one with the following steps.

1. Enter an application name into the **API Application Name** field. This name can be anything you want, but it should be descriptive so you can easily identify it later.
2. Enter your site's URL into the **Domain** field in this format: [your_subdomain].stackenterprise.co (no https://).
3. Click **Create API application**.



4. Copy the new API application's **Client ID** number to your working document.

Generate a code verifier and code challenge

Before you can generate a token, you need to create a code verifier and code challenge. The code verifier is a random string, and the code challenge is a hashed version of the code verifier.

Ping has a helpful tool for generating these values: https://developer.pingidentity.com/en/tools/pkce-code-generator.html.

Use the Ping tool (or any other PKCE code generator) to generate the code verifier and code challenge strings, and copy both to your working document.

Generate an authorization code

Next, you'll use the client ID, code verifier, and code challenge to generate a token.

Modify and enter the following URL into your web browser to generate a token:

https://YOUR_SUBDOMAIN.stackenterprise.co/oauth?client_id=YOUR_CLIENT_ID&redirect_uri=https://YOUR_SUBDOMAIN.stackenterprise.co/oauth/login_success&code_challenge=YOUR_CODE_CHALLENGE&code_challenge_method=S256&state=YOUR_STRING&scope=YOUR_SCOPE

Using your working document:

- Replace **YOUR_SUBDOMAIN** with your SOE subdomain.
- Replace **YOUR_CLIENT_ID** with the client ID of your API application.
- Replace **YOUR_CODE_CHALLENGE** with the code challenge.
- Replace **YOUR_STRING** with any random string or word. This is used to prevent cross-site request forgery (XSRF) attacks.
- Replace **YOUR_SCOPE** with the scope(s) you want to grant. See below for the most common scopes.

Scopes

- **no_expiry** The token will not expire. If you don't specify this scope, the token will expire after 24 hours.
- **write_access** The token will have write access to the API. If you don't specify this scope, the token will only have read access.

Combine multiple scopes into a comma-separated list, with no spaces (for example: scope=no_expiry,write_access).

Authorize the application

After you visit this URL, you'll be prompted to log in to your SOE account and authorize the application. The site will then redirect you to a page that includes an authorization code in the URL.

The URL will look something like this: https://YOUR_SUBDOMAIN.stackenterprise.co/oauth/login_success?code=YOUR_AUTHORIZATION_CODE&state=YOUR_STRING.

Copy the authorization code (identified with "code=" in the URL) to your working document.

Generate a token

You'll use the authorization code to generate a token. One of the best ways to do this is with curl, modifying and entering the following command:

```
bash
curl -X POST https://YOUR_SUBDOMAIN.stackenterprise.co/oauth/access_token/json \
```

```
  -H "Content-Type: application/x-www-form-urlencoded" \
  -d "client_id=YOUR_CLIENT_ID" \
  -d "code=YOUR_AUTHORIZATION_CODE" \
  -d "code_verifier=YOUR_CODE_VERIFIER" \
  -d "redirect_uri=https://YOUR_SUBDOMAIN.stackenterprise.co/oauth/login_success"
```

Using your working document:

- Replace **YOUR_SUBDOMAIN** with your SOE subdomain.
- Replace **YOUR_CLIENT_ID** with the client ID of your API application.
- Replace **YOUR_AUTHORIZATION_CODE** with the authorization code.
- Replace **YOUR_CODE_VERIFIER** with the code verifier.

After you run the curl command, you should receive a response that includes your access token. You can then use this token to authenticate your requests to the Stack Overflow for Teams Enterprise API.