Stack Overflow for Teams API v3

Access and update your SOE data with API v3.

Document generated 03/25/2024

PDF VERSION

Tags | **API** |

Applies to: Free Basic Business **Enterprise**

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

Overview

The Stack Overflow for Teams API enables you to interact with your Stack Overflow Enterprise (SOE) site programmatically with external scripts, reporting tools and automated workflows. We've also introduced the third version of our API, which builds on API v2 with new capabilities and an updated interface.

Read about general API v3 features in the all-product API v3 article.

API v3 now allows access to subject matter experts (SMEs), user groups, and Private Teams. With these new endpoints, you can:

- Get SMEs for a tag.
- Access data for private teams as well as the main site.

You'll access API v3 within your SOE instance at https://[your_site]/api/v3. API v2 is still available at https://[your_site]/api/docs, and you can use both APIs at the same time.

In addition to this document, https://[your_site]/api/v3 has interactive documentation with definitions for all API v3 methods and data models. This interactive documentation system (Swagger UI) allows you to test API calls and view returned data in a convenient web interface with no API implementation required. API v3 uses modern API design patterns, making it easy and familiar for both developers and end users.

Authentication and Authorization

The starting point for API v3 authentication is the API *access key*. This key functions like an API "application", authorizing the creation of API *access tokens* through an OAuth process. The resulting access token accompanies and authorizes each API v3 request. Access tokens that are read-only can read data only; read-write tokens allow API calls to read, update and delete data. Only users authenticated into SOE can create access keys and tokens.

***NOTE:** You can use the same API access tokens for API v2 and v3 requests. Each token's write permissions scope (read-only or read-write) applies to both APIs.*

In addition to its write permissions scope (read-only or read-write), each API v3 token has a private team or main site scope. If you specify a private team when creating a token, that token will be able to access only that team and not the main site data. Likewise, a main site token (no private team specified) can't access private team data. Only users who are part of a private team can use a private team token to access that team's data.

API v3 uses OAuth authentication to generate access tokens. This OAuth flow requires the access key to specify the domain of the application that will be accessing the API. If successful, the OAuth authentication process returns the resulting access token to the specified domain.

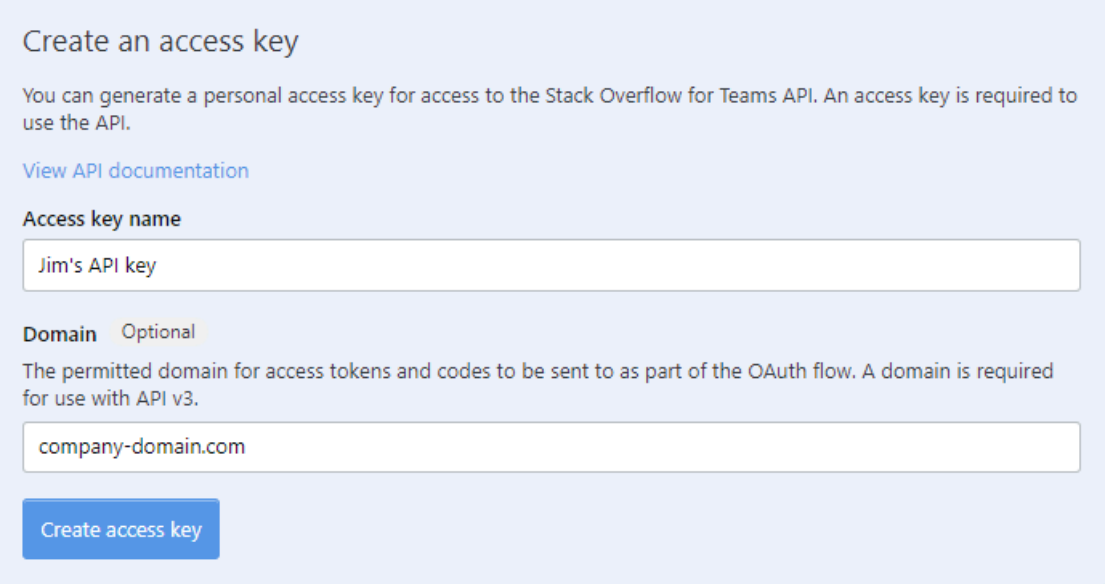
Learn more about access keys and tokens from your on-site API v2 documentation at https://[your_site]/api/docs/authentication.

User keys

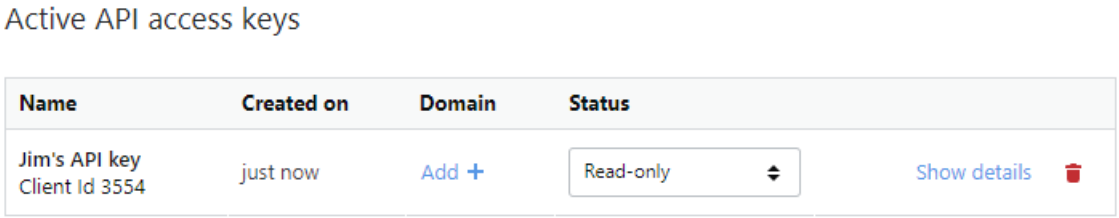
A user key and resulting token has access to the same data that you do. An access token with read-write permissions, for example, can update the same content (questions, answers, comments) that you can.

To access the user API key management page, click your avatar (profile picture) at the top of the page. Click **Settings**, then **API access keys** (under the "APPS & INTEGRATIONS" heading).

The API access keys page has two parts: an upper section to create new keys, and a table of existing keys below. To create a new user API key, enter an **Access key name** and your site's **Domain**. Click **Create access key**.



Your new key will appear in the "Active API access keys" table.



To change the permissions of a key, click the select menu in that key's **Status** column. When you enable write access, you'll be prompted to enter or confirm the domain of the application that will be accessing the API. To delete a key, click the trash can button. The API will reject any future calls that use the deleted key.

The API key table on the admin settings page allows control over user access keys as well as service keys. Admins can change the read-only/read-write scope of a user key, update its domain, and delete it.

Create access tokens

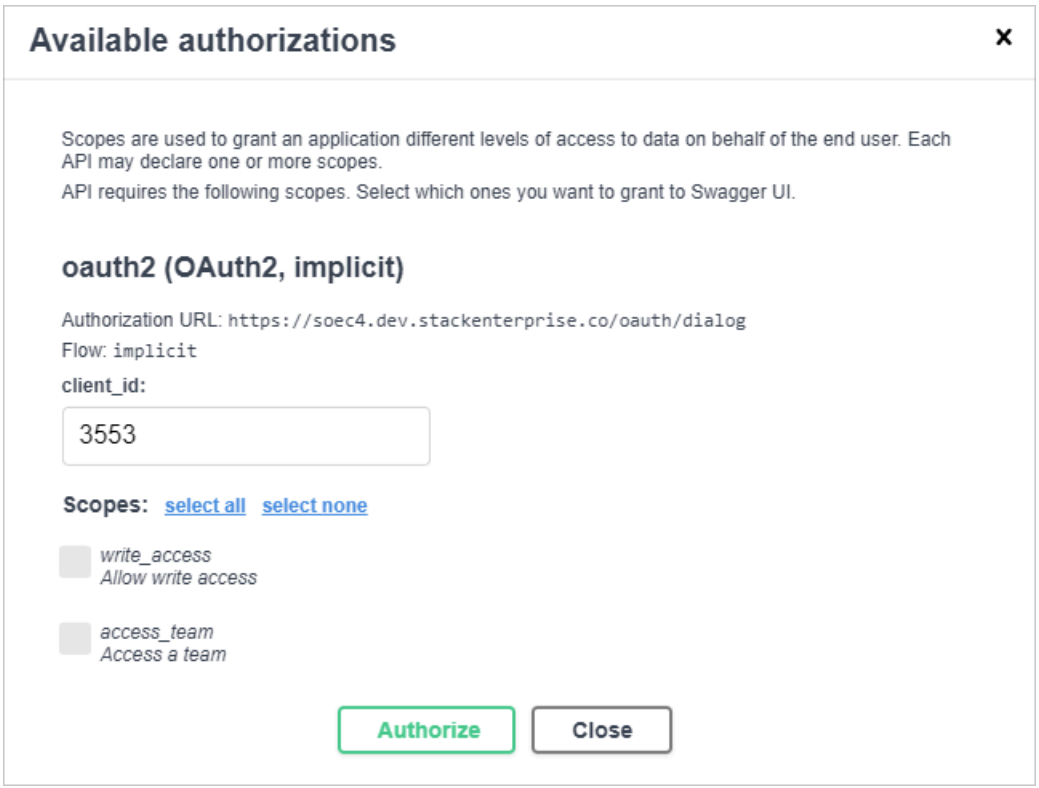
Standard OAuth process
API v3 uses the same OAuth process as API v2 to create access tokens from access keys. Go to https://[your_site]/api/docs, and follow the instructions in the "Authentication" section. Choose the explicit or implicit grant flow based on your application. To generate read-only tokens, omit "write_access" from the scopes list. To create a token for private team access, include the "access_team" scope.

Swagger UI process
The Swagger UI interface functions as an API application with full access to API v3 as the authenticated user. When authorized, Swagger UI uses its access key to create an access token. You can also use this token for API calls outside of Swagger UI, which may be useful for temporary API application development or testing. An access token created through Swagger UI expires after 24 hours.

NOTE: *If you already have an active Swagger UI access token, first delete this token so you can make changes and reset the 24-hour expiration window. Do this by clicking* ***Authorize****, then* ***Logout****, then* ***Authorize*** *again.*

To authorize Swagger UI and create a new access token:

- Go to https://[your_site]/api/v3.
- Click **Authorize**. An implicit OAuth flow popup will appear.
- Leave **Client ID** unchanged.
- Check **write_access** if the token should have write permissions.
- Check **access_team** if the token is for a private team and not the main site. Choose the private team and click **Continue**.
- Click **Approve**.



When you use Swagger UI to access API v3, Swagger UI reveals the access token as part of the underlying API call. You can find the access token in the "Curl" section of the Swagger UI execution output. Look for the following line:

```
-H 'Authorization: Bearer [access_token]'
```

If you need further support or have questions, contact your site administrator.