Search Token Authentication

Search tokens are special JSON web tokens (see https://jwt.io/) which can be used to execute queries and send usage analytics events as a specific user. They are intended to be used in JavaScript code running in a web browser, typically along with the Coveo JavaScript Search Framework (see Coveo JavaScript Search Framework Home).

By default, a search token automatically expires after 24 hours (see the validFor property).

You can generate search tokens in server-side code by calling a REST service exposed through the Coveo Cloud platform (see Requesting a Search Token).

Typically, you will want to use search token authentication when your search page users are authenticated and some (or all) items in your index are secured. In this scenario, each end user gets a unique search token, allowing the search interface to securely return only items that the user is allowed to see (see Sample Usage Workflow).

Sample Usage Workflow

Here is a typical workflow demonstrating the use of search tokens:

A user requests a search page from a web server.

The web server executes server-side code that eventually renders the HTML response (PHP, ASP.NET, etc.).

Server-side code authenticates the user who is making the request.

Server-side code calls a REST service exposed through the Coveo Cloud platform to get a search token for the authenticated user (see Requesting a Search Token).

The search token is used to generate the JavaScript code that initializes the Coveo JavaScript Search Framework in the search page (see JavaScript Search Framework Home).

The server sends the generated HTML to the client.

The JavaScript code initializes the search page and executes the first query, using the provided search token.

The Coveo Cloud platform executes the query as the user impersonated by the search token.

Results are displayed to the user.