Export API token best practices

Last Modified on 03/18/2026 2:33 pm EDT

Here are a few best practices for using and rotating your Export API tokens:

- **Create separate tokens for separate data repositories or tools**
  This makes it easier to cut off access by deleting the token if the token is compromised or if you stop using the tool.

- **Share tokens between knowledge bases**
  The Export API tokens are generated for your account, which means they grant access to the Export API for all knowledge bases where the Export API has been enabled. If you're feeding multiple knowledge bases' Owl Analytics data into the same tool, you can use the same token for each knowledge base, just make sure you have separate calls for each `project_id`.

- **Avoid using export tokens directly in the URL for long-term use**
  While we provide you a copyable sample and instructions for this approach, exposing your export token in the URL is a higher security risk than passing it as a header in the call. We recommend using the URL approach only for quick tests and verification.

- **Rotate export tokens on a set schedule**
  Check with your security or IT teams to determine if you have internal policies on replacing and rotating API keys or tokens. Use those guidelines to determine when to create new tokens and delete the old ones.

- **Rotate export tokens as soon as you have any concerns about one being compromised**
  This is most relevant if you have reader tracking turned on, since the Readers report that you can export via the API includes email addresses, which are considered Personally Identifiable Information (PII). If you suspect a token has been compromised, delete it, create a new token, and update your API calls or integrations to use that new token.