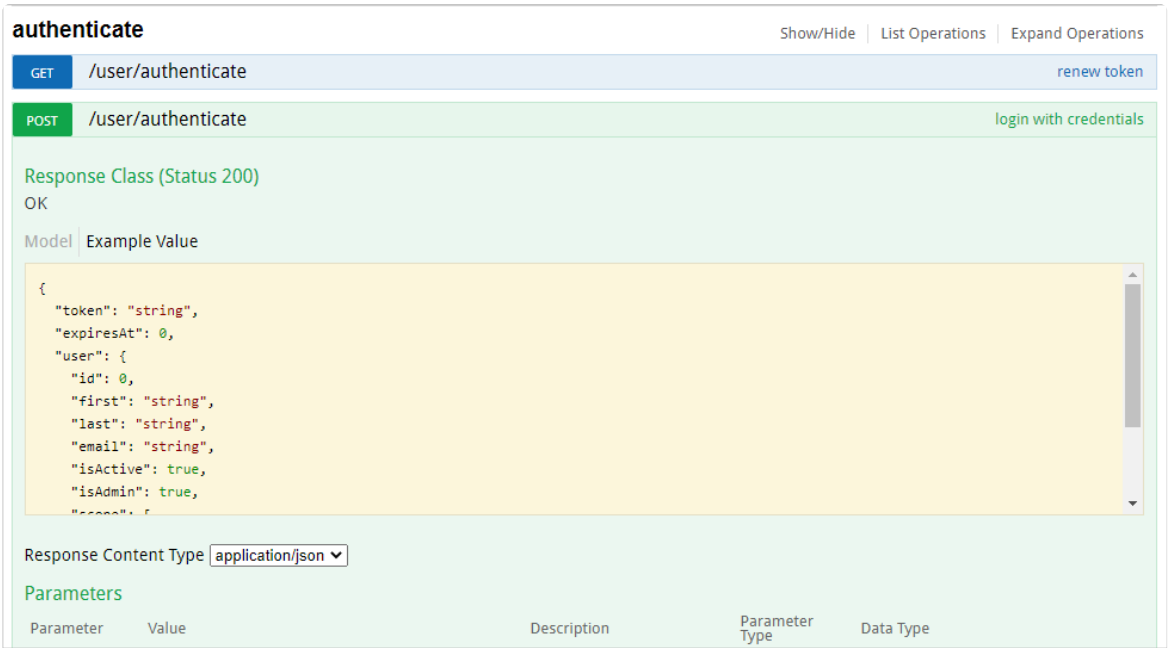
# Session Tokens

Last Modified on 05/28/2024 10:09 am EDT

## Important Notes

- These tokens are tied to the user's org account. This means that if a user doesn't have permission to perform an action in Core, they won't be able to do it through the API.
- Session tokens are valid for 15 minutes. To extend the session, the token must be refreshed **before** it expires. Tools that perform extended operations may require a child thread to guarantee the refresh window is not missed.
- Users must have a valid password. Because passwords expire based on the org's password policy, this method is not recommended for static integrations.
- When logging in via SSO, if a user is not already authenticated by their IdP (e.g., logged in through their corporate network), the login process depends on the IdP and therefore may need to be customized. For example, on ADFS and Azure, users outside the corporate network are generally redirected to a login web page. In this case, the integration must be customized to handle credential submission through the page as well as receiving and passing the IdP's response back to Core.




*The /user/authenticate call to create a session token.*

## Creating a Session Token

# Overview

Session tokens are required to authenticate an endpoint in order to receive the desired payload. you will receive a 403-authentication error, if an endpoint is not authenticated.

Resolver.
A KROLL BUSINESS

> ***Note:***
> *API Keys are the recommended method for endpoint authentication. For more information, refer to the* ***Create an API Key*** *article.*

## User Account Requirements

The user used to login must have Administrator permission to access Swagger Docs.

## Related Information/Setup

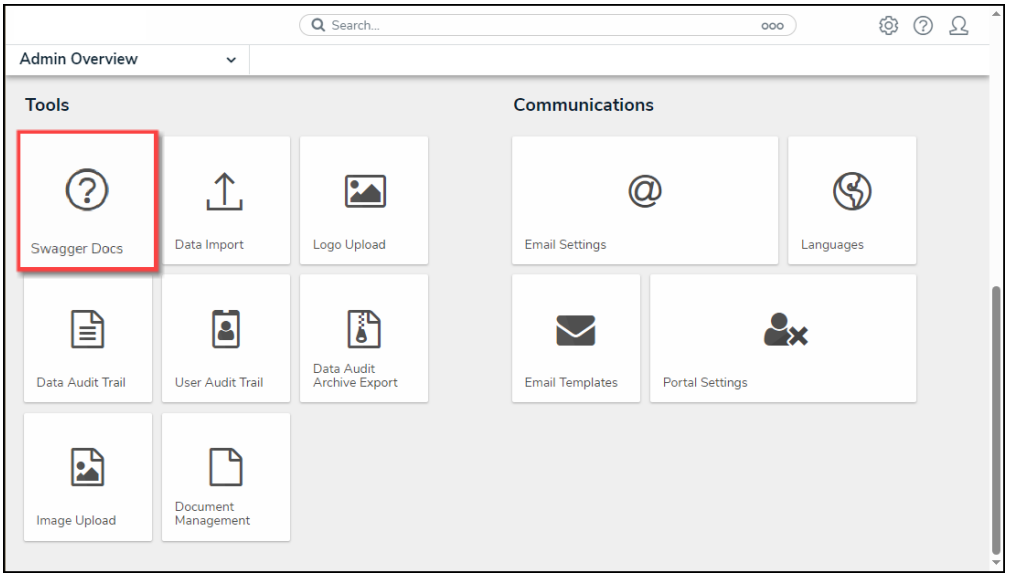
Please refer to the Locating an Org's ID article for further information on locating your org ID.

## Navigation

1. From the ***Home*** screen, click the **System** icon.

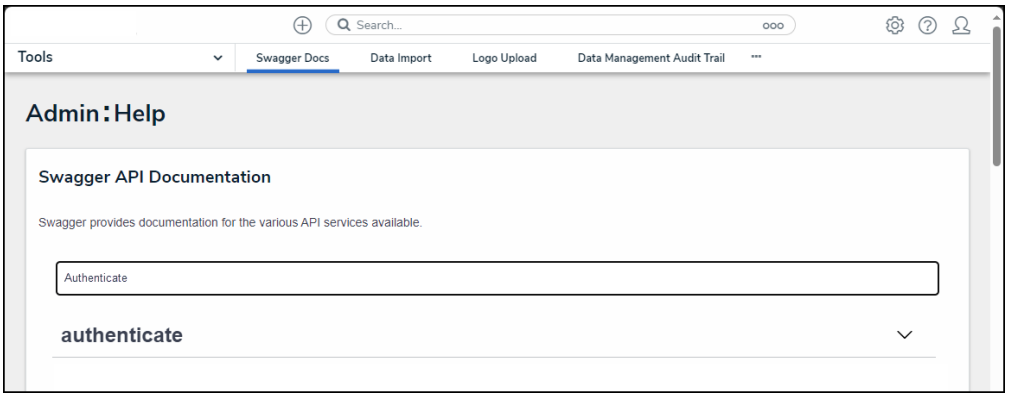

*System Icon*

2. From the ***Admin Overview*** screen, click the **Swagger Docs** tile under the **Tools** section.



*Swagger Docs Tile*

3. From the ***Admin: Swagger*** screen, enter authenticate in the **Search** field.

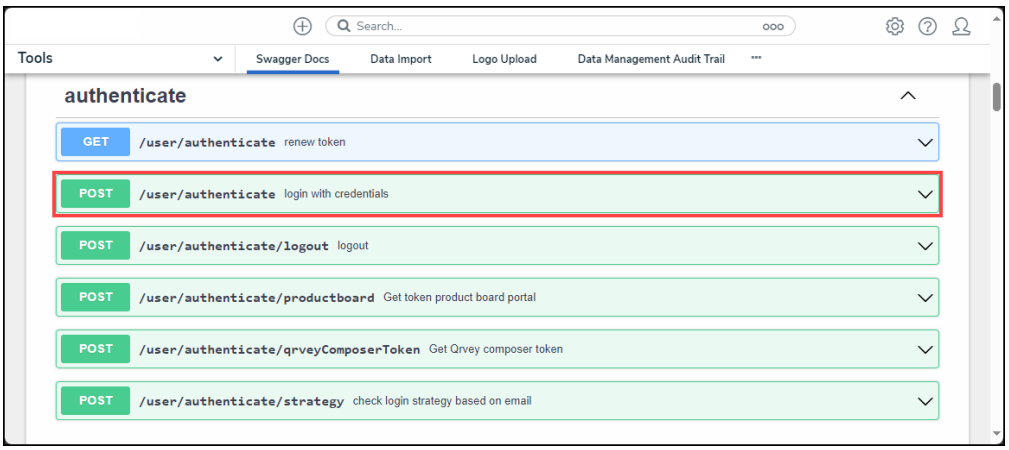



*Search Field*

4. Click the **Authenticate** endpoint.

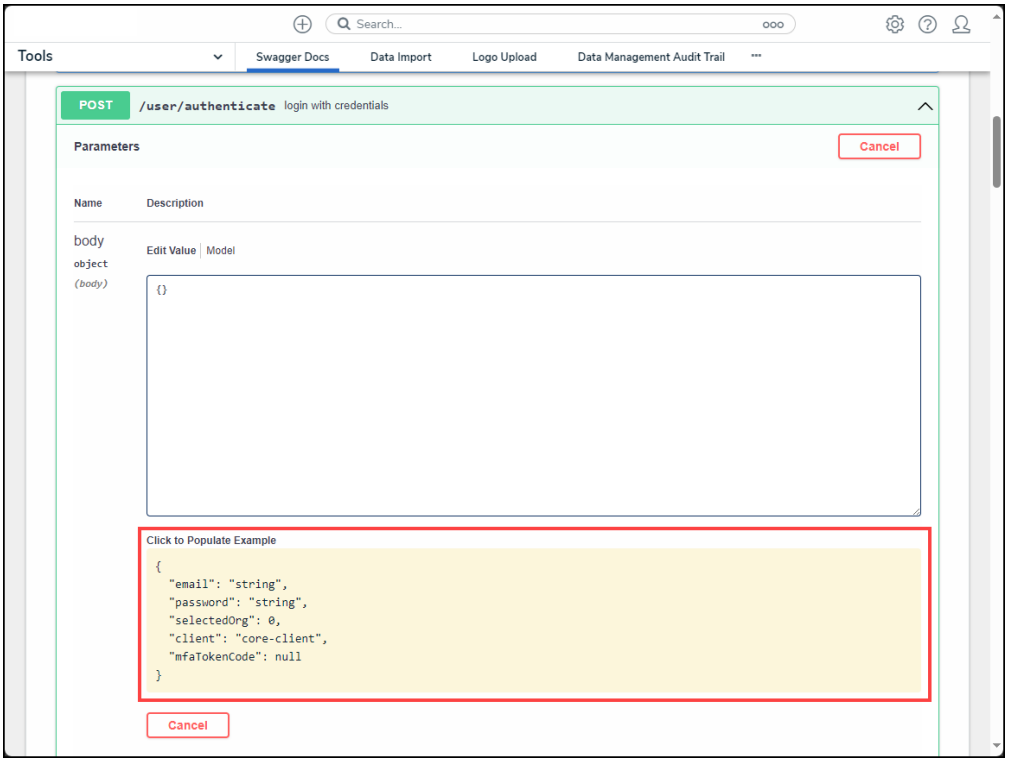
# Creating a Session Token

1. From under the **Authenticate** endpoint, click **POST /user/authenticate.**



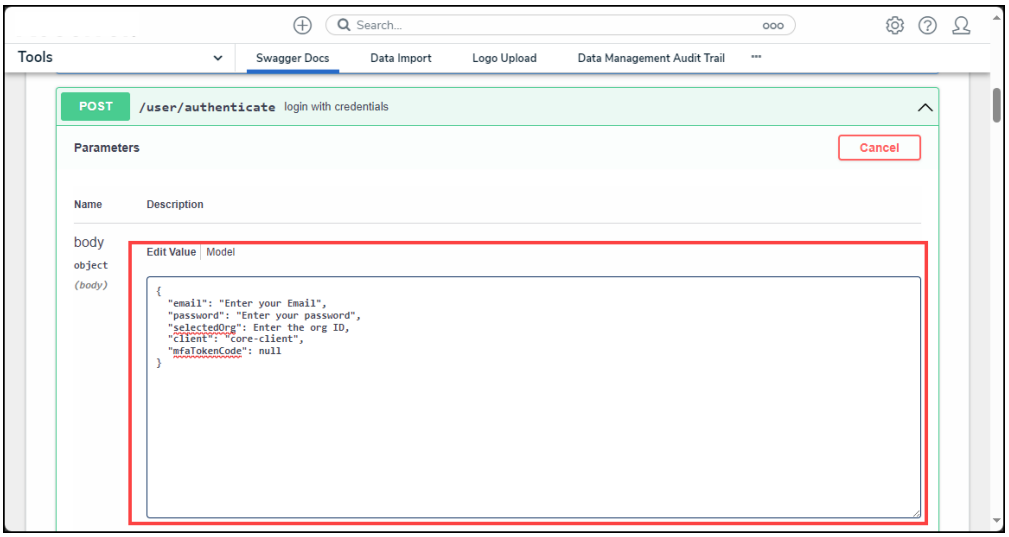

*POST/user/authenticate*

2. Click the **Example Value** box to populate the template in the **body** text box.




*Example Value*

3. Enter your login credentials (email and password) between the quotation marks (e.g., "23145") in the request body.
4. Enter the org ID (selectedOrg), Org IDs can be obtained using your browser's dev tools. For further information, see the Locating an Org's ID article.

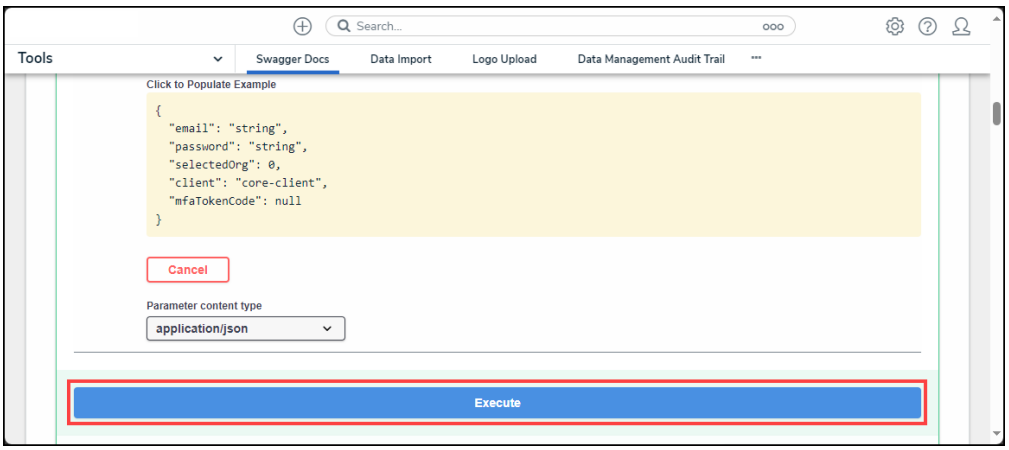



*Request Body*

5. Click the **Execute** button to return one of the following responses:

- **401 Unauthorized:** The login credentials are incorrect.
- **404 Not Found: The user is not an active member of any orgs.**

- **200 Success:** The user was successfully authenticated.




*Execute Button*

5. If successful, copy the bearer token to your clipboard. This token is valid for 15 minutes and must be entered in the authorization header of each request.

# Renew a Token

## To maintain the current session:

1. From Swagger, scroll down to the **authenticate** endpoint.
2. Click **GET /user/authenticate (Renew token)**.
3. Enter the bearer token that's about to expire in the authorization header.
4. Click **Try it out!** to return a new token, which is valid for 15 minutes.
5. Copy the new token to your clipboard and use it for any subsequent calls.