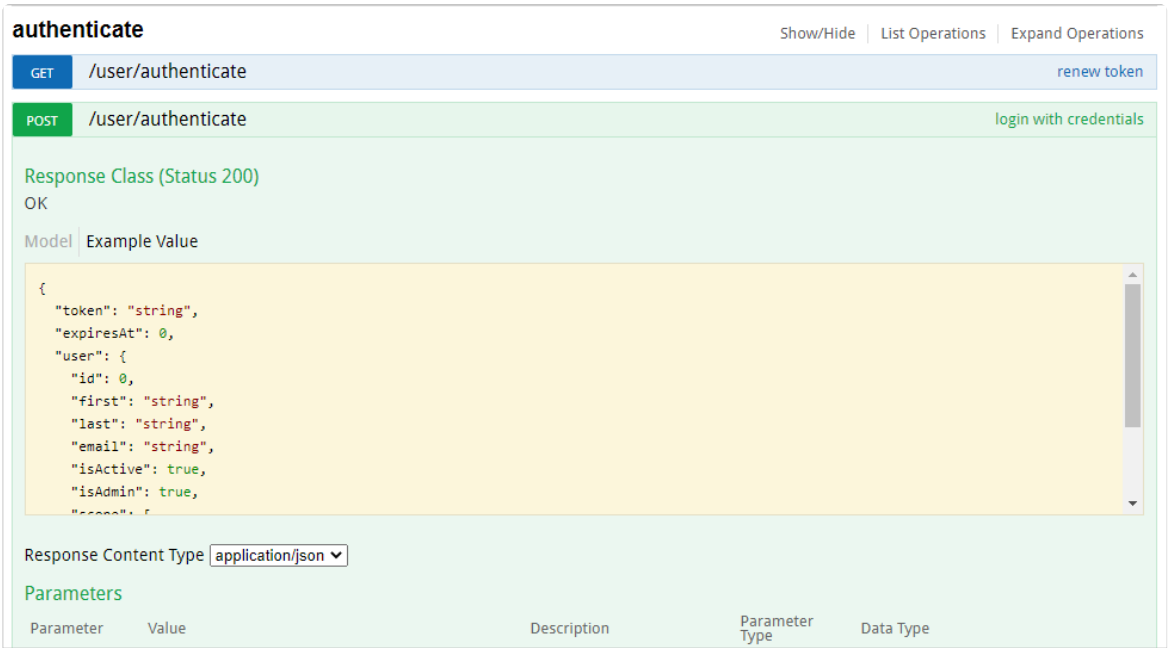
Session Tokens

Last Modified on 01/23/2024 2:22 pm EST

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.

Create a Token

To create a session token:

1. Log into Core as an administrator.
2. Navigate to **Admin > Swagger Docs.**
3. Click any endpoint to launch Swagger.

4. Scroll down to the **authenticate** endpoint to expand it.
5. Click **POST /user/authenticate**.
6. Click the **Example Value** box to populate the template in the **body** text box, then enter your login credentials and the org ID in the request body. Org IDs can be obtained using
7. Click **Try it out!** 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.
8. 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.