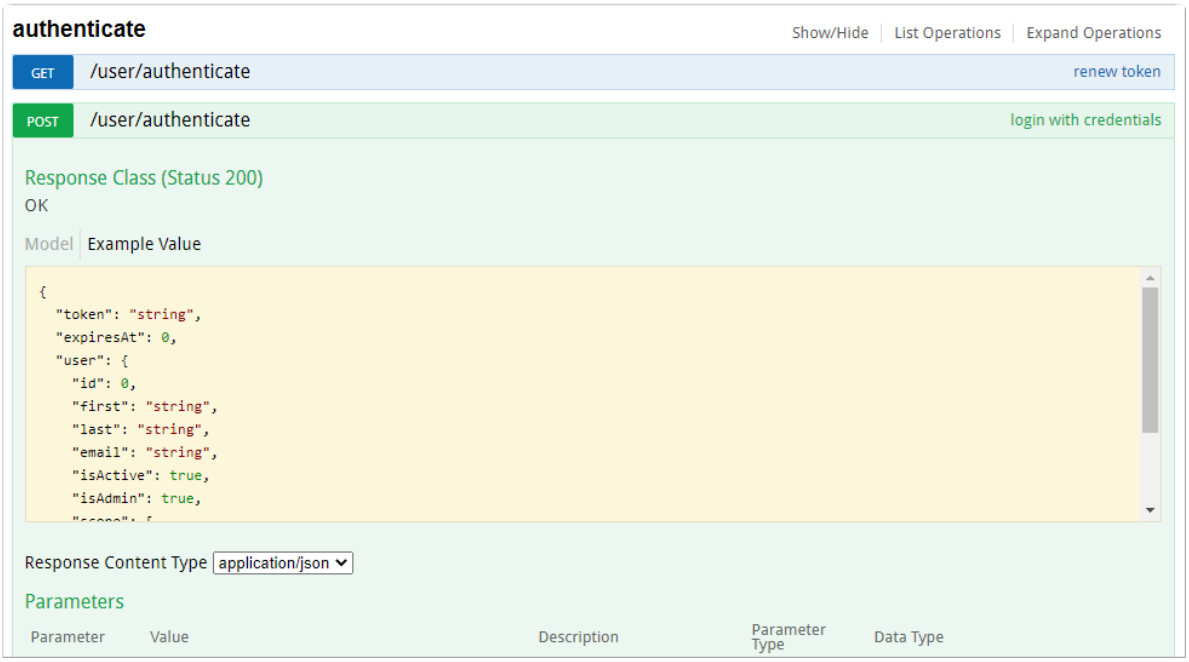
Session Token Overview

Last Modified on 02/26/2021 5:03 pm EST

- 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.