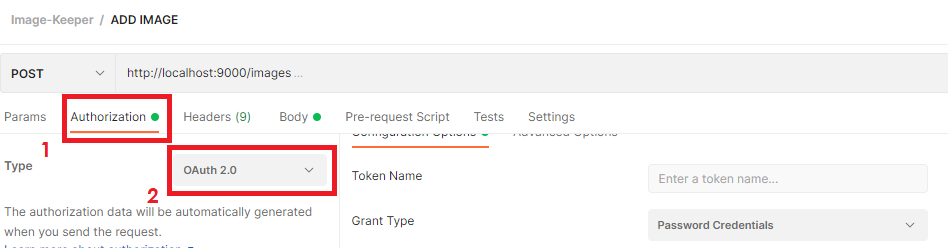
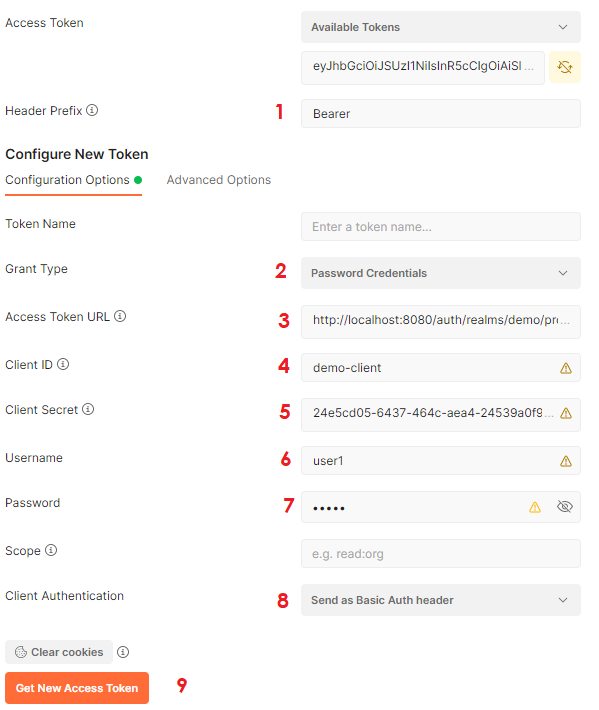
**Konfiguracja uwierzytelnienia OAuth 2.0 w Postman**

W parametrach przygotowywanego żądania należy wybrać zakładkę ‘Authorization’ a następnie z listy rozwijalnej wybrać pozycję OAuth 2.0

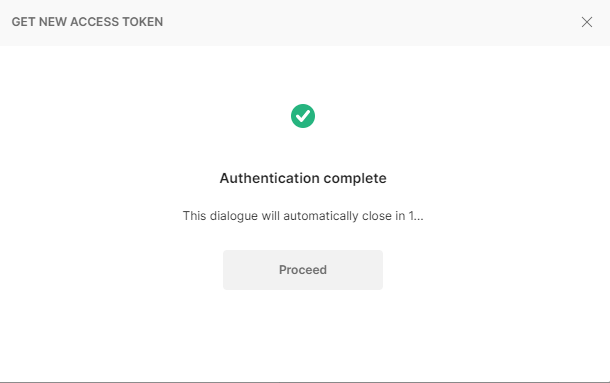


Korzystając z tej instrukcji należy skonfigurować pozostałe parametry uwierzytelnienia

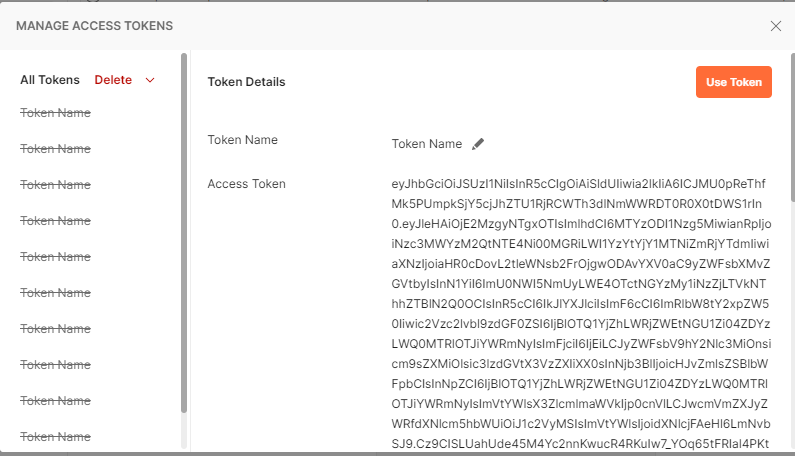


1. Header Prefix: Bearer
2. Grant Type: password Credentials
3. Adres do usługi Access Token: <http://localhost:8080/auth/realms/demo/protocol/openid-connect/token>
4. Client ID: demo-client (nazwa klienta skonfigurowana w Keycloak)
5. Client-Secret: 24e5cd05-6437-464c-aea4-24539a0f9902 (unikalny identyfikator klienta, potrzebny do uwierzytelnienia Postman w narzędziu Keycloack)
6. Username: user1 (w Keycloak dodanych jest dwóch użytkowników: user1 i user2)
7. Password: user1 (hasła użytkowników są takie same jak loginy)
8. Client Authentication: Send as Basic Auth header
9. Na koniec należy kliknąć Gen New Access Token – **WAŻNE aby przed każdym żądaniem na nowy endpoint wygenerować nowy Acccess Token**

Jeśli połaczenie z Keycloak uruchomionym w kontenerze Docker przebiegnie prawidłowo, wówczas ujrzymy obraz



Należy wówczas kliknąć ‘Proceed’ i przejdziemy do okna wyboru tokenu przy następnym uwierzytelnieniu



Na tym oknie należy kliknąć w przycisk ‘Use Token’

Dzięki temu Token został „załadowany” do Postman i zostanie przypisany do następnego żądania wychodzącego.