Salesforce Sales Cloud - Resolving 401 Errors

Last Modified on 03/17/2021 11:47 am EDT

Salesforce returns 401 errors when a Salesforce Sales Cloud session expires. Expired sessions are commonly caused by the following:

- The user revoked access rights.
- The session expired. Access tokens have a limited lifetime specified by the session timeout in Salesforce.
- The instance is using the Username-Password OAuth Authentication method which does not allow the use of refresh tokens. For sessions that don't expire, you may wish to switch to token based authentication for your instances.
- Too many uses of the same credentials to authenticate. Currently, Salesforce has a limit of 5 concurrent sessions. A sixth session could invalidate a previous instance.

The most common solution is to re-authenticate the instance. If the expired instance belongs to your customer, they will be prompted to enter their credentials the next time they attempt to use the connector.

To re-authenticate via the user interface:

1. Navigate the instance.
2. Hover over your instance and click "Edit".
3. In the lower-right corner of the next page, click "RE-AUTHENTICATE" which will allow you to re-authenticate your instance using the Salesforce login page.

To re-authenticate using the API:

1. Navigate to your instance's custom OAuth url (this is found by making a GET request to https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2/elements/23/oauth/url?apiKey={yourApiKey}&apiSecret={yourApiSecret}&callbackUrl={yourCallbackUrl})
2. Enter your Salesforce login credentials. You should then receive a new code which can be used to re-authenticate your instance.

For more information regarding the OAuth process for Salesforce Sales Cloud, see the documentation here.