Authentication Methods via REST API

There are two methods to authenticate over REST API:

1) Using a dedicated API Username and Password (provided by Bullhorn Support)
2) Using REST-backed custom components where a user's session is used, along with a Client ID/Secret, to obtain an authorization code

Marketplace, developer and SI partners should leverage the 1st method.

Utilizing REST-backed custom components is less stable and may cause issues with refresh_tokens expiring, requiring a user to re-authenticate to obtain an up-to-date token to allow for API calls to be successful again. Because an expired token is outside our control due to a number of reasons including the user changing their password, network connectivity issues, etc, the best practice is to use a dedicated API Username and Password for your integration.

For each customer activating the integration, you will be able to obtain an API Username and Password from Bullhorn Support for authenticating. This provides you with control over the authentication should the refresh_token expire for any reason.

Please see the Guide on using a dedicated API Username and Password as well as using refresh_tokens to best leverage this method

Note that the only difference between the two methods is the inclusion of the *&username={API Username}&password={API Password}* in the initial OAuth authorization call.