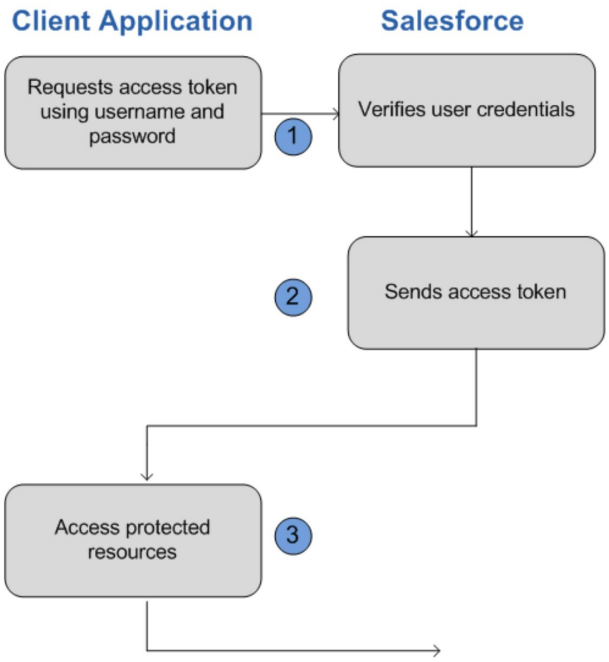

1.) The application uses the user's username and password to request an access token. This is done via an out-of-band POST request to the appropriate Salesforce token request endpoint, such as https://login.salesforce.com/services/oauth2/token. These request fields are required:

    a.) Grant_type - Must be password for this authentication flow.
    b.) Client_id - The Consumer Key from the connected app definition.
    c.) Client_secret - The Consumer Secret from the connected app definition. Required unless the Require Secret for Web Server Flow setting is not enabled in the connected app definition.
    d.) Username - End-user's username.
    e.) Password - End-user's password.

2.) Salesforce verifies the user credentials, and if successful, sends a response to the application with the access token. This response contains the following values:

    a.) Access_token - Access token that acts as a session ID that the application uses for making requests. This token should be protected as though it were user credentials.
    b.) Instance_url - Identifies the Salesforce instance to which API calls should be sent.
    c.) Id - Identity URL that can be used to both identify the user as well as query for more information about the user. Can be used in an HTTP request to get more information about the end user.
    d.) Issued_at - When the signature was created, represented as the number of seconds since the Unix epoch (00:00:00 UTC on 1 January 1970).
    e.) Signature - Base64-encoded HMAC-SHA256 signature signed with the client_secret (private key) containing the concatenated ID and issued_at value. The signature can be used to verify that the identity URL wasn't modified because it was sent by the server.

3.) The application uses the provided access token to access protected user data.