Use Google Sign-In with IT Apps

The following is a checklist of steps to take when using Google Sign-In with work accounts for a custom-developed IT application. If you are developing a mobile app, refer to the best practices for mobile as well.

Note: If your application supports only SAML for authentication, refer to the Google Apps Administrator Help Center for instructions on setting up a custom SAML app.

1. Include your Google for Work domain in your OpenID Connect request so the Google authentication service will only display accounts in that domain. This is done using the `hd` parameter with the REST endpoint, the `hosted_domain` parameter with the JavaScript API, the `setHostedDomain` builder method on Android, and the `hostedDomain` property on iOS.
2. When you get an OpenID Connect assertion from Google, double check that the Google authentication service has confirmed it is an account controlled by the administrators of that domain name. This check is done server side by evaluating the `hd` field in the token to verify the domain is what you expected. See Authenticate with a backend server for details.
3. Optional, but strongly recommended: whitelist the application so that your users will not see a confirmation screen when they sign in. This step, combined with the previous steps, ensures that users of your IT application can automatically sign in. To whitelist your app:
    a. Open the Google Apps Admin Console.
    b. Click the Security icon, then click **Show More > Advanced Settings > Manage API client access**.
    c. Enter the OAuth client ID you registered for the application. A client ID is normally a string of letters and numbers followed by `.apps.googleusercontent.com`.
    d. In the **API Scopes** field, type the following string:

    ```
    https://www.googleapis.com/auth/plus.me,https://www.googleapis.com/auth/userinfo.email
    ```

    If your app needs to request additional scopes to access Google APIs, specify them here as well.
    e. Click **Authorize**. The whitelisting will take effect in about 30 minutes.

    Note: The whitelisting will not work if the app starts the OAuth/Open ID Connect flow and includes the parameters `offline` or `prompt`. These parameters are generally not needed for IT apps.

Last updated December 18, 2015.