

# How to configure your App Service application to use Google login

2 minutes to  
read

Contributors    

This topic shows you how to configure Azure App Service to use Google as an authentication provider.

To complete the procedure in this topic, you must have a Google account that has a verified email address. To create a new Google account, go to [accounts.google.com](https://accounts.google.com).

## Register your application with Google

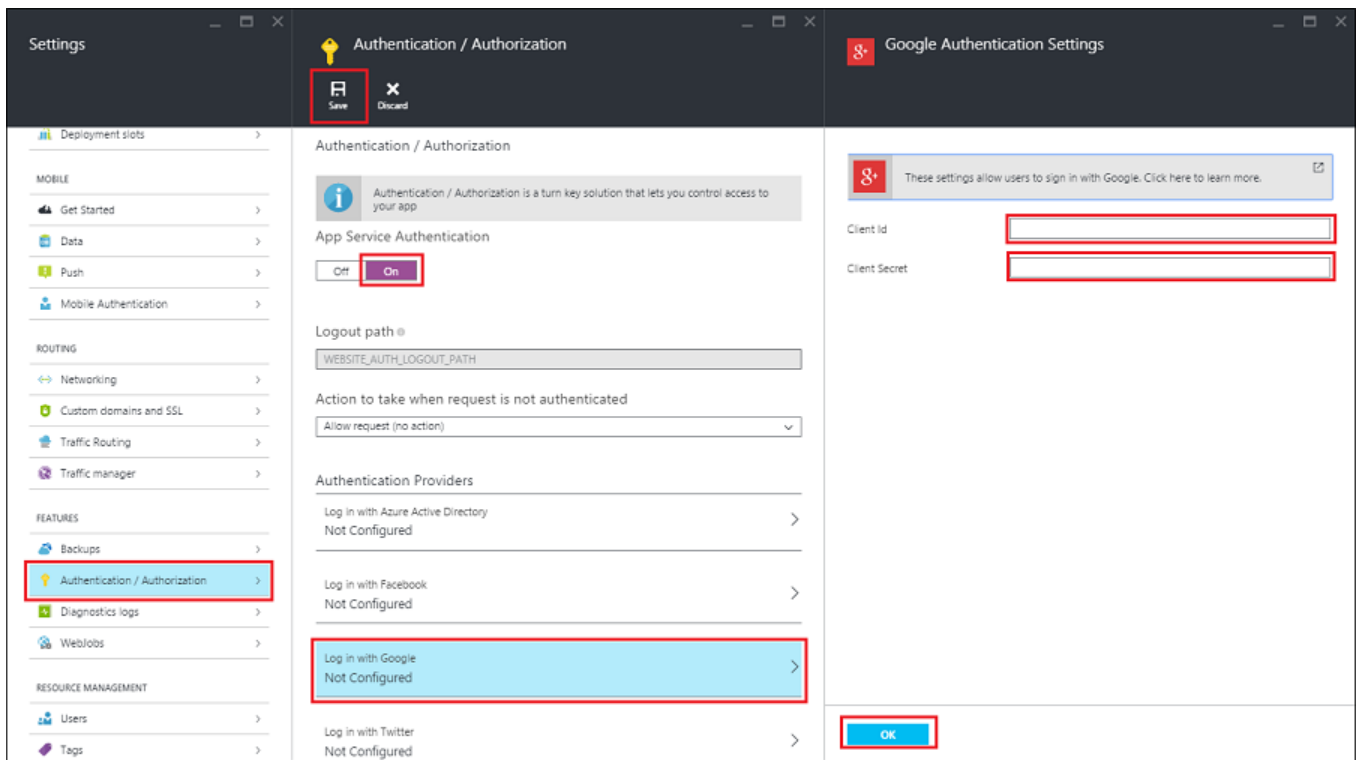
1. Log on to the [Azure portal](#), and navigate to your application. Copy your **URL**, which you use later to configure your Google app.
2. Navigate to the [Google apis](#) website, sign in with your Google account credentials, click **Create Project**, provide a **Project name**, then click **Create**.
3. Once the project is created, select it. From the project dashboard, click **Go to APIs overview**.
4. Select **Enable APIs and services**. Search for **Google+ API**, and select it. Then click **Enable**.
5. In the left navigation, **Credentials** > **OAuth consent screen**, then select your **Email address**, enter a **Product Name**, and click **Save**.
6. In the **Credentials** tab, click **Create credentials** > **OAuth client ID**.
7. On the "Create client ID" screen, select **Web application**.
8. Paste the App Service **URL** you copied earlier into **Authorized JavaScript Origins**, then paste your redirect URI into **Authorized Redirect URI**. The redirect URI is the URL of your application appended with the path, `/.auth/login/google/callback`. For example, `https://contoso.azurewebsites.net/.auth/login/google/callback`. Make sure that you are using the HTTPS scheme. Then click **Create**.
9. On the next screen, make a note of the values of the client ID and client secret.

### Important

The client secret is an important security credential. Do not share this secret with anyone or distribute it within a client application.

## Add Google information to your application

1. Back in the [Azure portal](#), navigate to your application. Click **Settings**, and then **Authentication / Authorization**.
2. If the Authentication / Authorization feature is not enabled, turn the switch to **On**.
3. Click **Google**. Paste in the App ID and App Secret values which you obtained previously, and optionally enable any scopes your application requires. Then click **OK**.



By default, App Service provides authentication but does not restrict authorized access to your site content and APIs. You must authorize users in your app code.

- (Optional) To restrict access to your site to only users authenticated by Google, set **Action to take when request is not authenticated** to **Google**. This requires that all requests be authenticated, and all unauthenticated requests are redirected to Google for authentication.
- Click **Save**.

You are now ready to use Google for authentication in your app.

## Related Content

- [App Service Authentication / Authorization overview](#)
- Add authentication to your Mobile App: [iOS](#), [Android](#), [Windows Universal](#), [Xamarin.Android](#), [Xamarin.iOS](#), [Xamarin.Forms](#), [Cordova](#)  
Learn how to add App Service authentication to your mobile app.

## Feedback

We'd love to hear your thoughts. Choose the type you'd like to provide:

Product feedback



Sign in to give documentation feedback



Our new feedback system is built on GitHub Issues. Read about this change in [our blog post](#).

Loading feedback...



