

AngularJS Firebase Authentication Providers

Learning Objectives

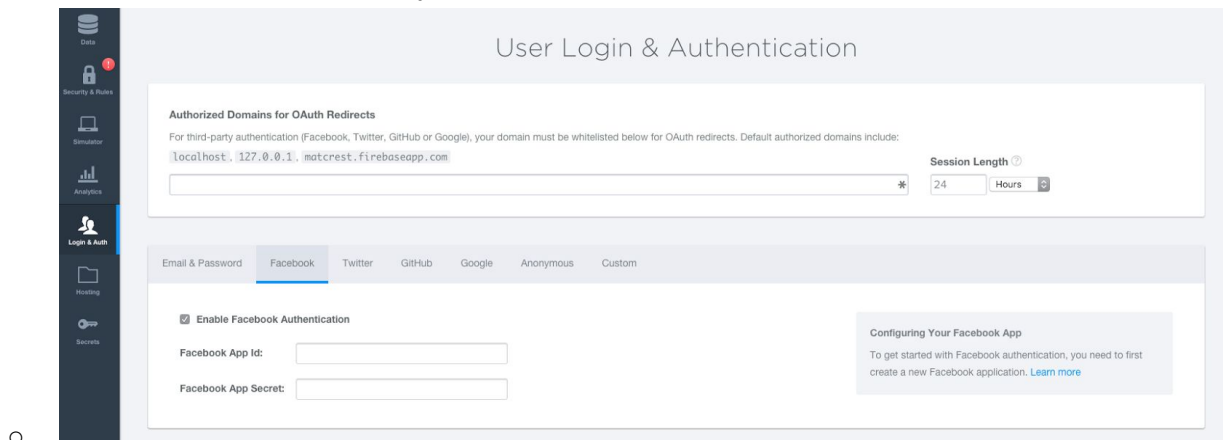
- Students will learn how to hook in 3rd party authentication.
- Students will create a sign up page supporting all 6 Firebase auth types (username, GitHub, Facebook, Twitter, Google, anonymous/guest).

Resources

- <https://www.firebase.com/docs/web/guide/user-auth.html>
- <https://www.firebase.com/docs/web/guide/login/facebook.html>
- <https://developers.facebook.com/apps>

Firebase Facebook Provider

- Providers all work in a similar fashion. Social providers require registering your app with the social site (e.g., Facebook).
- We will walk through setting up the Facebook provider.
- **Firebase documentation is excellent.** Students can rely heavily on it for other providers.
- **The following walkthrough follows the tutorial [here](#).**
- Enable Facebook authentication in your Firebase:



- Create a new Facebook web app here: <https://developers.facebook.com/apps>
 - From [Firebase tutorial](#): “To get started with Facebook authentication, you need to first create a new Facebook application. Click the Add a New App button in the top right of that page and select Website as your platform. Then choose an App

ID and click Create New Facebook App ID. Select your app's category and click Create App ID. In the top right, click Skip Quick Start.”

- Copy your app id and secret from the Facebook app page into the Firebase authentication page.
- Important: to the same page, add localhost to your list of authorized domains:

Authorized Domains for OAuth Redirects

For third-party authentication (Facebook, Twitter, GitHub or Google), your domain must be whitelisted below for OAuth redirects. Default authorized domains include:

localhost, 127.0.0.1, matcrest.firebaseio.com

localhost * Session Length 24 Hours

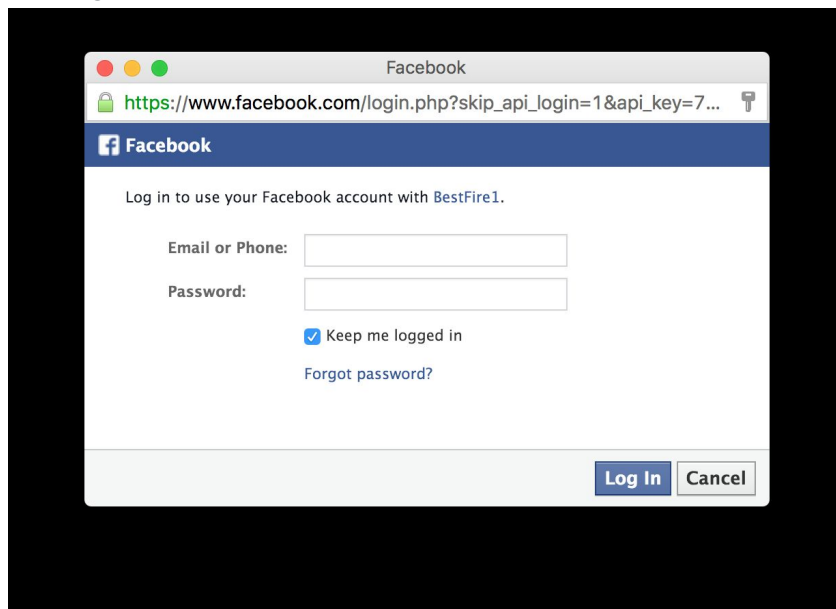
- If you run your html page from WebStorm, it will be served on localhost.
- “In your Facebook app configuration, click on the Settings tab on the left-hand navigation menu. Then go to the Advanced tab at the top and scroll down to the Security section. At the bottom of that section, add `https://auth.firebase.com/v2/<YOUR-FIREBASE-APP>/auth/facebook/callback` to your Valid OAuth redirect URIs and click Save Changes at the bottom of the page.”
 - E.g., for Firebase “matcrest”, URL will be <https://auth.firebase.com/v2/matcrest/auth/facebook/callback>
 - Yours may look like the default that firebase assigned: `https://auth.firebase.com/v2/vivid-fire-7010/auth/facebook/callback`

Once setup is complete, this complete code example may be run:

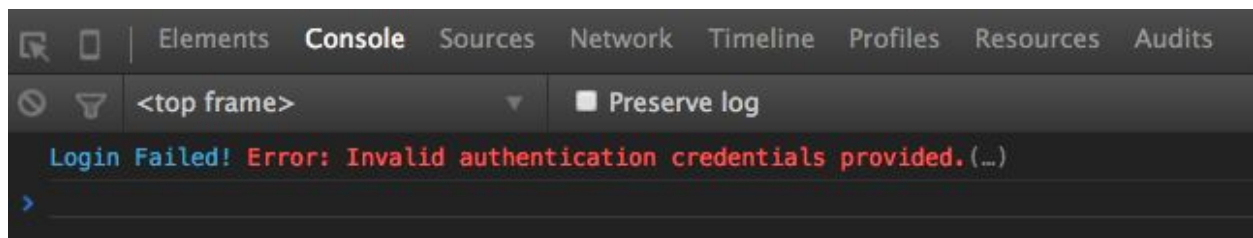
All-in-one example: <https://github.com/MountainlandWEB/firebase/blob/master/facebook.html>

Hosted version: <http://dolthead.github.io/firebase/facebook.html>

Clicking the button will present the user with a Facebook authorization modal:



Clicking Cancel calls the error callback:



Authorizing provides a token to the success callback:



Exercise

Students can follow the other guides in the documentation to set up applications with other social services:

1. <https://www.firebase.com/docs/web/guide/login/twitter.html>
2. <https://www.firebase.com/docs/web/guide/login/github.html>
3. <https://www.firebase.com/docs/web/guide/login/google.html>
4. <https://www.firebase.com/docs/web/guide/login/anonymous.html> (requires no additional setup, just add the code snippet to a click handler).

Once students have set up these various authentication methods, user authentication may be used to interact with rules and permissions (covered tomorrow). This will allow us to lock down data based on login (e.g., allowing a user to delete only their own records).

LocalStorage Follow-Up

Simple example: <http://embed.plnkr.co/o4w3VGqmp8opfrWzvsJy/>