1.2 Activate Push Notifications

iOS iOS 5.2.x and earlier iOS 5.3.x iOS 5.4.x iOS 5.5.x iOS 5.6.x iOS 6.0.x iOS 6.1.x iOS - 6.3.x Latest version - 6.4.x

Enable Push Notifications in Xcode

1. In the project editor, choose a target and click **Capabilities**.
2. In the Push Notifications section, click the switch to turn it from `OFF` to `ON`.

Generate and export an APNS client TLS certificate from the Apple developer portal

Generate an APNS client TLS certificate

You need to generate a separate client TLS certificate for each app you distribute that uses push notifications including Development and Production versions.

It is important that you generate a Development (Sandbox) Push Notification certificate to use with a Development Provisioning Profile, and/or a Production Push Notification certificate to use with an Ad Hoc or Distribution Provisioning Profile. They will be used in 2 separate applications within Accengage Dashboard (see below) and it will be important that you respect this differentiation.

Generating the certificate fully enables push notifications for the associated App ID. In your developer account, you will notice that the Push Notifications service for the App ID changes automatically from Configurable to Enabled.

1. In your developer account, go to Certificates, Identifiers & Profiles and if necessary, choose the operating system from the pop-up menu on the left (for macOS apps, choose OS X).
2. Under Certificates, select All.
3. Click the Add button + in the upper-right corner.
4. Under Production, select the “Apple Push Notification service SSL (Sandbox & Production)” checkbox, then click Continue.
5. Choose an App ID from the App ID pop-up menu, and click Continue.
6. Choose the explicit App ID that matches your bundle ID.
7. Follow the instructions to create a certificate signing request on your Mac, and click Continue.
8. Click Choose File.
9. In the dialog that appears, select the certificate request file (a file with a `.certSigningRequest` file extension), and click Choose.
10. Click Continue.
11. Click Download and double-click the downloaded file (a file with a `.cer` file extension) to add the certificate to your keychain.
12. Click Done.

Create a certificate signing request

1. Launch Keychain Access located in `/Applications/Utilities`.
2. Choose Keychain Access > Certificate Assistant > Request a Certificate from a Certificate Authority.
3. In the Certificate Assistant dialog, enter an email address in the User Email Address field.
4. In the Common Name field, enter a name for the key (for example, Gita Kumar Dev Key).
5. Leave the CA Email Address field empty.
6. Choose “Saved to disk”, and click Continue.

Export the client TLS identity from your Mac

Export the identity from the keychain on the Mac where you created it, and copy it to the appropriate place on the server that runs the provider code and connects with the development or production version of APNs.

1. Launch Keychain Access.
2. In the Category section, select My Certificates.
3. Find the certificate you want to export and disclose its contents.
4. You’ll see both a certificate and a private key.
5. Select both the certificate and the key, and choose File > Export Items.
6. From the File Format pop-up menu, choose a file format that your server accepts.

7. Enter a filename in the Save As field, and click Save.
8. The certificate and key are saved to the location you specified as a text file in the Personal Information Exchange format (a file with a `.p12` file extension).