Re-sign an App

You will occasionally need to re-sign an app that was already signed. Some common scenarios include:

- An app is expired or due to expire.
- An app was signed with third-party or development credentials.
- After you apply policies to an app.

The process for re-signing an app is technically the same as signing an app the first time (you can use the Portal or the signing package). All the same prerequisites and tasks still apply. For instructions, see Sign an App (Admin Portal) and Sign an App (Signing Package).

However, there are some additional best practices to consider.

Use the Same Credentials

When you re-sign an app that was already installed on any of your users' devices, it is important that you sign it with the same signing credentials used to previously sign it.

iOS and Android do not allow a user to install an update of an app if the update is signed with credentials that differ from the currently installed version.

> ⓘ   For iOS, when you renew a distribution provisioning profile it is still technically the same profile with an updated certificate and expiration date.

Back to Top

Notify Users

After you re-sign an app you'll want to inform your users that they need to download a new version of the app.

- When you re-sign an iOS app through the Admin Portal, you can select the "Notify users about the update" option to send a Push Notification to the devices of all users who have already installed the app.
- If you are signing an app that was previously distributed to any users, you can mark the update as mandatory to ensure users install the new app file created when you re-sign it. For more information, see Managing Application Updates.

Back to Top