

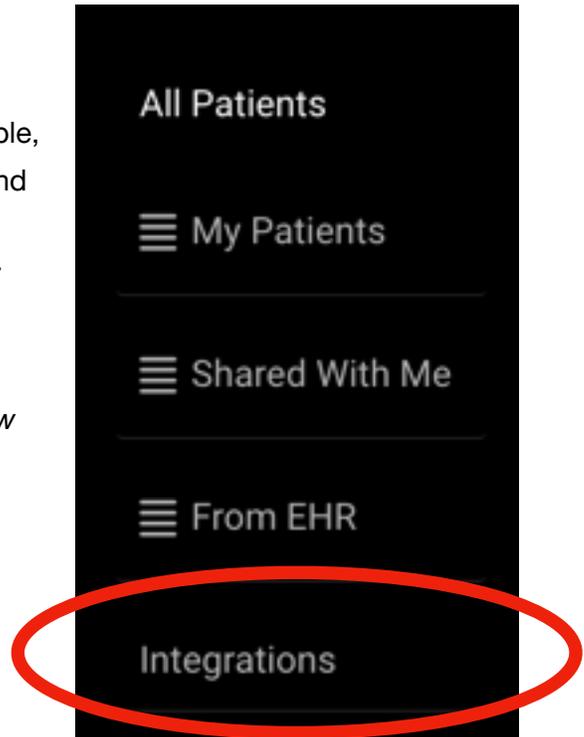
# Setting Up Eko Enterprise API Access

Once your institution has activated **Eko Enterprise API** features, the superadmin will see a link on the left hand sidebar of the **Eko** dashboard called “Integrations.” This is where API access keys are managed.

An **Integration** can be thought of as representing a single application that you wish to develop. For example, if you were planning on developing both an Android and an iOS application, you might want to distinguish between the two with separate sets of API keys rather than sharing them amongst different repositories.

To create a new **Integration**, you simply click the “*New Integration*” button at the upper right hand of the **Integrations** page. This will take you to a form with some fields to fill out.

*Application Name* should simply contain the name of your application.

A screenshot of a form titled 'Create New Integration'. It contains three input fields: 'APPLICATION NAME', 'BUNDLE OR PACKAGE ID', and 'DESCRIPTION'. Below the fields is a blue button labeled 'Create Enterprise Integration'.

*Bundle or Package ID* should be an identifier that is unique to your organization like an Apple Bundle ID or a Google Package. If you are developing a web application, then you should put a URL here instead. There are no hard formatting requirements on the value that you place into this field, but you cannot re-use these identifiers across multiple **Integrations**. They must be completely unique for each one.

*Description* is completely optional. If you'd like to add some notes to the **Integration** for internal housekeeping purposes, feel free to place them here.

Once you have filled out the two required fields, click “*Create Enterprise Integration*” to generate a new set of API keys.

This will take you back to the main **Integrations** management page where you will now see an actual **Integration** displaying both the values that you entered in the previous steps and two new fields called *Key* and *Secret*.



The *Key* is an identifier for this particular integration which does not need to be protected in any particular way, but the *Secret* is used to sign requests to the **Eko Enterprise API** and it should *never* be discoverable by anyone outside of your organization. If you place this *Secret* into a JavaScript file served via HTTP or a GitHub repository then other people will be able to sign requests as your organization and potentially cause significant problems which may result in the suspension of your API access.

Both the *Key* and the *Secret* need to be provided to the iOS SDK in order to sign requests. They can be easily copied to the clipboard by simply clicking on them on the **Integrations** page. An updated version of the iOS SDK will soon be shared which enables this functionality.