

AdobeSign Integration Walkthrough Guide

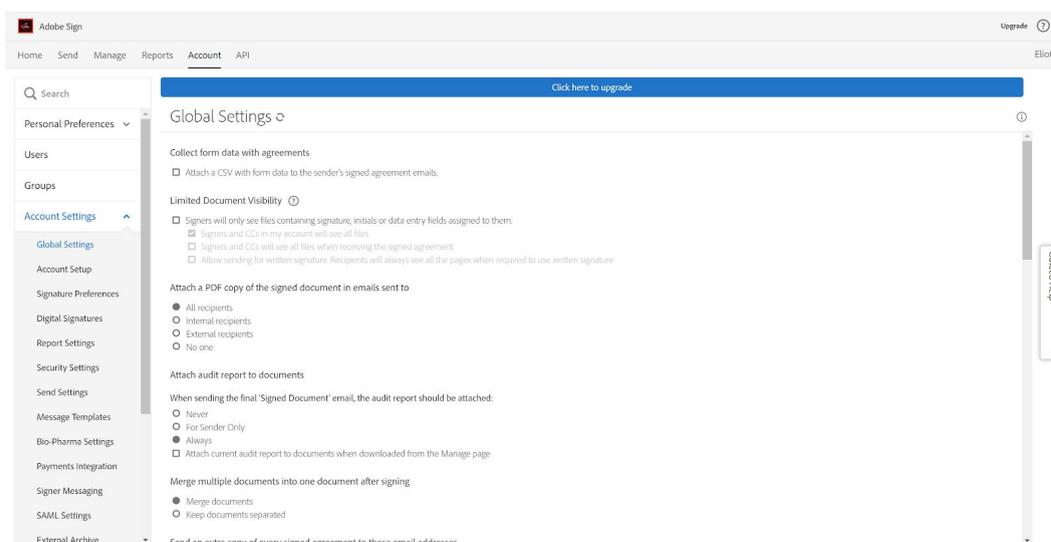
June 2020

This guide assumes you have an AdobeSign Enterprise account, which is needed to leverage any API integration with a third-party tool like Avvoka. You can test the AdobeSign API with Avvoka by creating an AdobeSign Developer account [here](#).

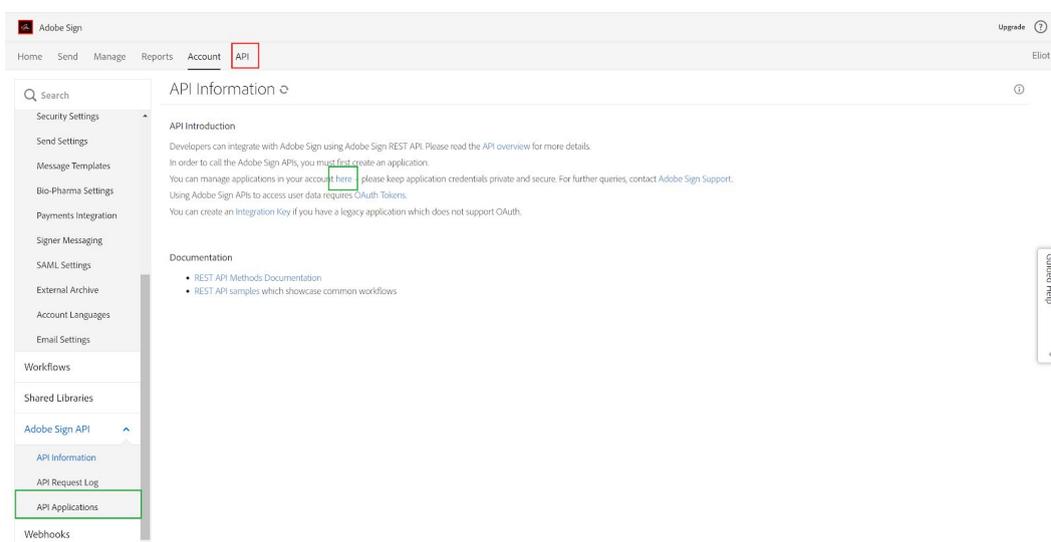
These steps are taken from the AdobeSign Developer Account but apply equally to Enterprise production Adobe Accounts.

Steps

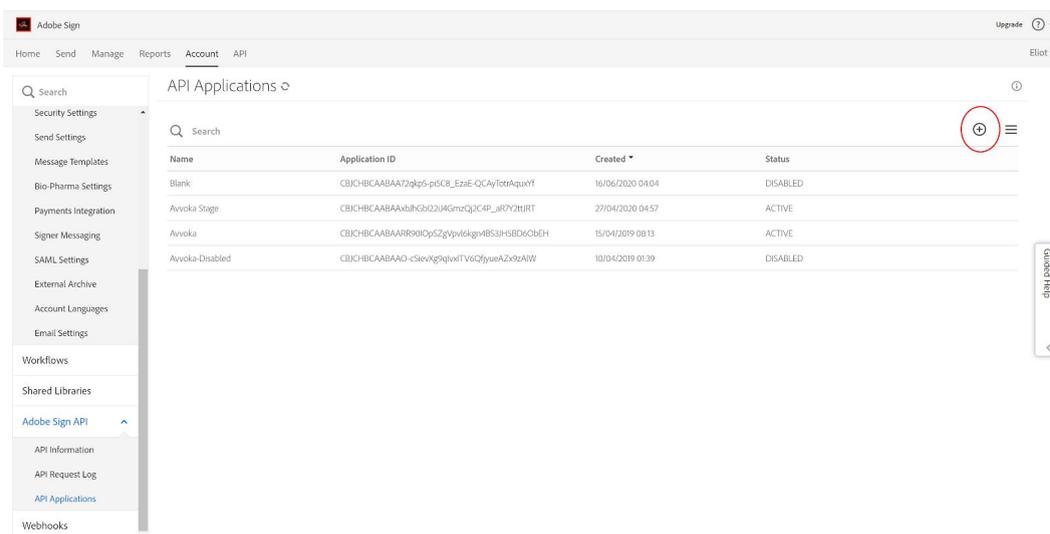
1. Login to your Adobe account and access the administrator settings.



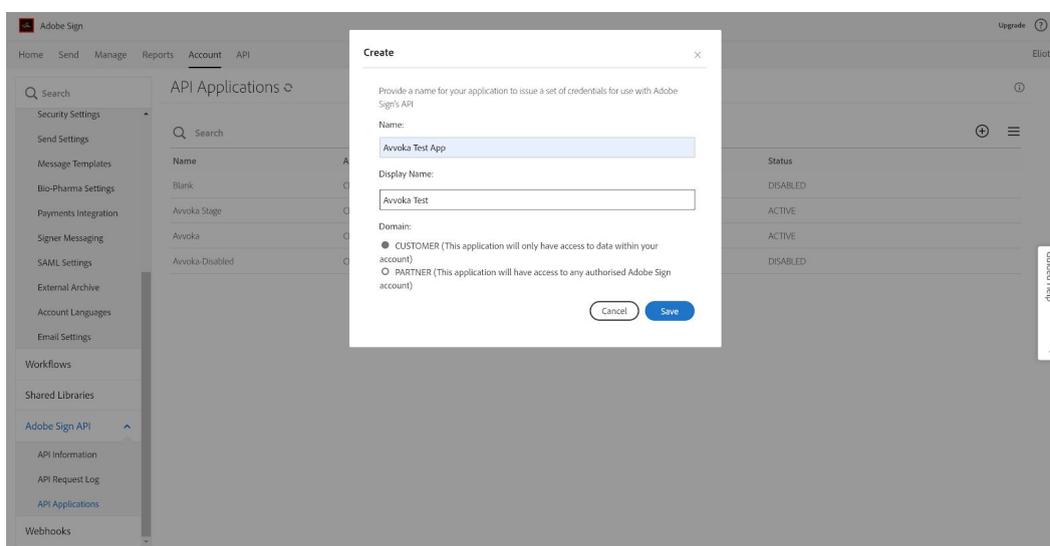
2. Navigate to the API page. You will be notified that in order to use the API, you must create an application first. Navigate to either green box (below) in order to access the Applications page



3. From the Applications page, create a new application (see red circle below)

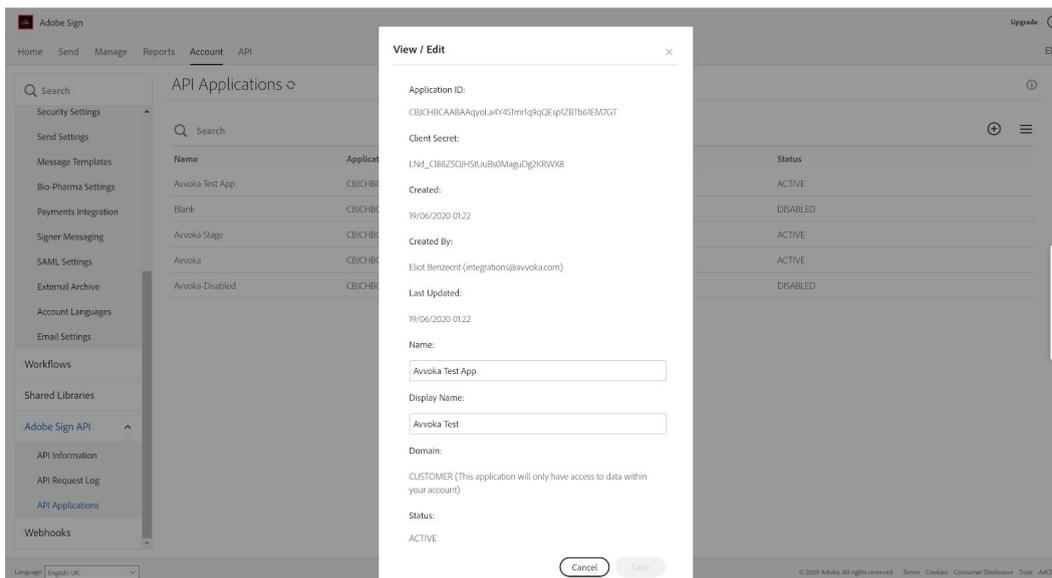


4. Name your application (this can be anything) and opt for the 'Customer' option.

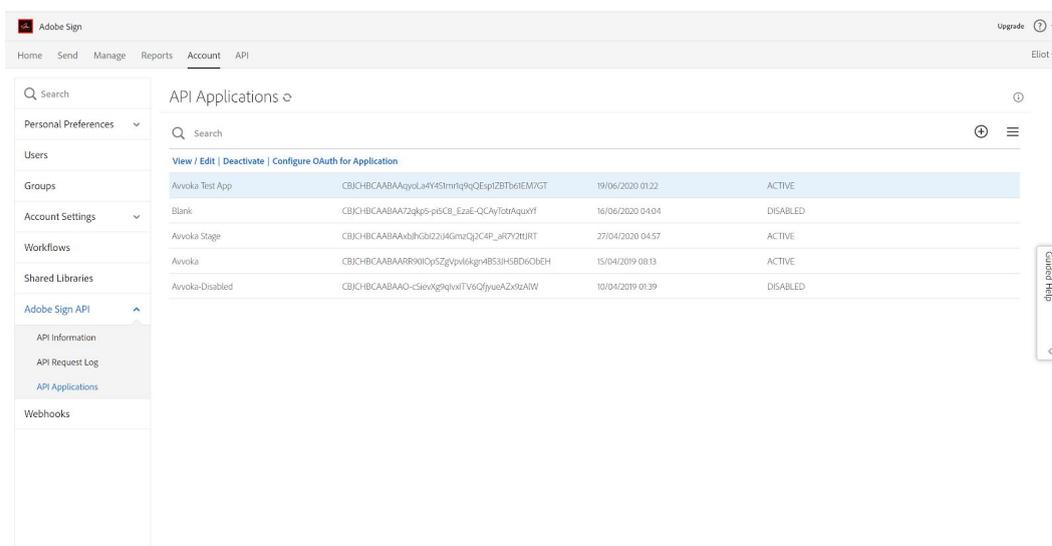


5. After you have named your application, you will be navigated back to the Application main page. Click on the application, you have just created, choose 'View / edit' and make a note of the Application ID and Client Secret (you will need these in Avvoka later).

AVVOKA LIMITED



- After completing step 5, click cancel on the pop-up and click on your application again, this time choosing 'Configure OAuth for Application'.



- From the next page, in the URI redirect box, add the following URI: [https://app.\[stage\].avvoka.com/as_callback](https://app.[stage].avvoka.com/as_callback) [Note: if you are connecting to a different Avvoka server, update the square-bracketed area accordingly. For clients with whitelabel domains, then replace the 'app' part with your whitelabel].
- Below this, in the Enabled Scopes section, make sure the following settings are configured and then press Save:

AVVOKA LIMITED

Enabled Scopes

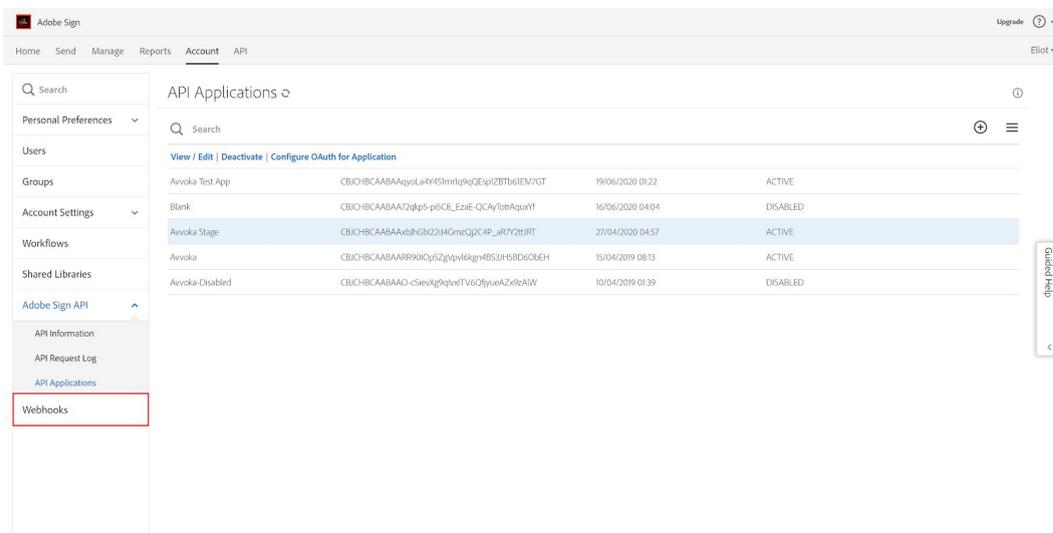
You must enable the scopes that you intend to request through the OAuth protocol. Please limit the scopes that you enable to the minimum set necessary for your application, which is one of the requirements for Certification.

Please [contact support](#) if you need to change which scopes are enabled for your application.

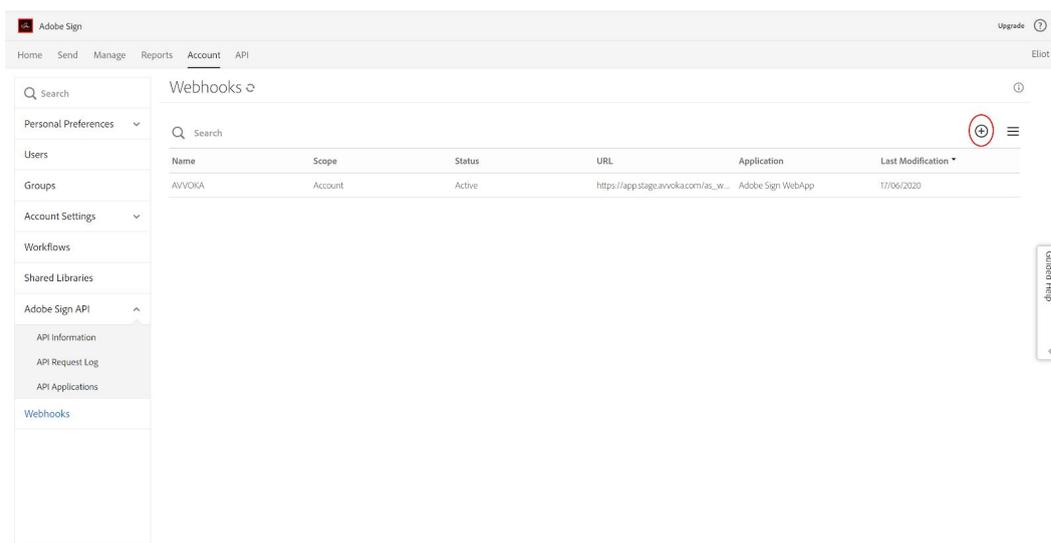
Note that only Group Admins can approve OAuth requests that use the ':group' scope modifier, and only Account Admins can approve OAuth requests that use the ':account' scope modifier.

Enabled?	Scope	Modifier	Description
<input type="checkbox"/>	user_read	account	View users in your account
<input type="checkbox"/>	user_write	account	Create or manage users within your account
<input checked="" type="checkbox"/>	user_login	account	Login on behalf of any user in your account
<input checked="" type="checkbox"/>	agreement_read	account	Access documents & data on behalf of any user in your account
<input checked="" type="checkbox"/>	agreement_write	account	Manage the status of documents on behalf of any user in your account
<input checked="" type="checkbox"/>	agreement_send	account	Send documents on behalf of any user in your account
<input type="checkbox"/>	widget_read	account	View web forms on behalf of any user in your account
<input type="checkbox"/>	widget_write	account	Create, edit or publish web forms on behalf of any user in your account
<input type="checkbox"/>	library_read	account	View templates and document library on behalf of any user in your account
<input type="checkbox"/>	library_write	account	Manage the templates and document library on behalf of any user in your account
<input type="checkbox"/>	workflow_read	account	View workflows on behalf of any user in your account
<input type="checkbox"/>	workflow_write	account	Create workflows on behalf of any user in your account
<input type="checkbox"/>	webhook_read	account	View webhooks on behalf of any user in your account
<input type="checkbox"/>	webhook_write	account	Create or edit webhooks on behalf of any user in your account
<input type="checkbox"/>	webhook_retention	account	Permanently delete webhooks on behalf of any user in your account

9. From the API Applications page, navigate to 'Webhooks'.



10. User the + icon to create a new webhook setting:



11. In the pop-up that appears, You can call the webhook setting what you wish and choose 'scope' as 'Account'.
12. The URL should be set as: https://app.stage.avvoka.com/as_webhook. **[Note: if you are connecting to a different Avvoka server, update the square-bracketed area accordingly. For clients with whitelabel domains, then replace the 'app' part with your whitelabel].**
13. In the 'Events' box, click the dashed lines next to the text box and choose 'Agreement' and 'Agreement all events' only from the dropdown menus.
14. Finally, In the 'Notification parameters', tick the following only:
 - Agreement Info
 - Agreement Document Info
 - Agreement Participant Info
 - Agreement Signed Document
15. As an Organisation Admin:
 - Log into Avvoka, paste the details you collected in Item 5 into the AdobeSign box on the Organisation Admin Settings page for your Organisation.
 - i. The Client ID corresponds to the Application ID from AdobeSign, you will also need the Client Secret.
 - Set the Authorization URL as [https://secure.\[eu1\].echosign.com](https://secure.[eu1].echosign.com). **[Note, depending on where you are in the world, the square-bracketed part of the Adobe URL will change to reflect your local Adobe datacentre. You can work out which three characters to include, by following the Adobe guidance [here](#)]**
 - Click save, after which you will be redirected to AdobeSign to authenticate your account.