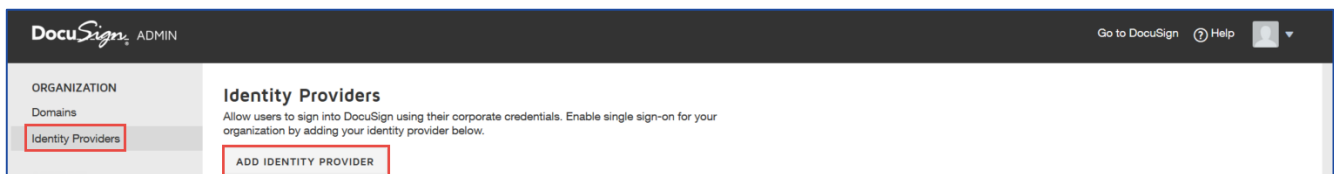


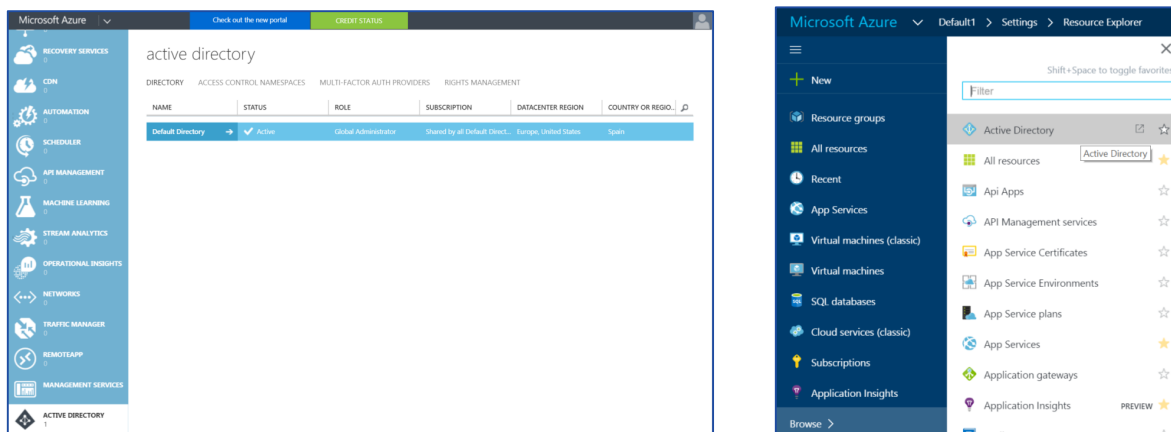
## Quick Guide

1. Pre-requisites:
  - a. DocuSign admin user.
  - b. Azure AD admin user.
2. Login to DocuSign Admin Portal
  - a. Demo: <https://admindemo.docusign.com/authenticate>
  - b. Production: <https://admin.docusign.com/authenticate>
3. Open the **Identity Provider** menu option and hit **ADD IDENTITY PROVIDER**
  - a. **Name:** Fill out the Name field with a unique name, such as {CompanyName}\_AzureAD
  - b. **Issuer:** Set this value as 'Test' or any other temporary value for the time being
  - c. **Login URL:** Set this value as 'Test' or any other temporary value for the time being
  - d. **Send AuthN Request:** Set this to POST. Also **uncheck** the **Sign AuthN Request** option
  - e. **Send Logout Request:** Set this to POST. Also **uncheck** the **Sign AuthN Request** option
  - f. Save the configuration. This will take you back to the Identity Providers panel.
  - g. Click on the **Actions** drop down button next to the Identity Provider you set up and hit the **Endpoints** link
    - i. You will need these values to configure Azure



Identity Providers admin console

4. Login to Azure and go to your Active directory.



Classic AZURE portal VS New AZURE portal

5. Go to Applications and hit **ADD**.
6. Select **Add an application my organization is developing**.

7. Complete the name (DocuSign Custom App) and select **Web application and/or web API**.
8. Complete the **App properties** with the information provided by DocuSign and save.
  - a. The **Log On URL** will be the **Service Provider Login URL** from the **DocuSign Identity Provider Endpoints**
  - b. The **App ID** will be the **Service Provider Issuer URI** from the **DocuSign Identity Provider Endpoints**
9. Hit **Next** and go to **Configure** in the menu. Find the textbox for **Reply URL** (this is under the single sign on section) and modify the value with the **Service Provider Assertion Consumer Service URL** from **DocuSign** (this URL ends with **/saml2/login**)

single sign-on

APP ID URI

REPLY URL

(ENTER A REPLY URL)

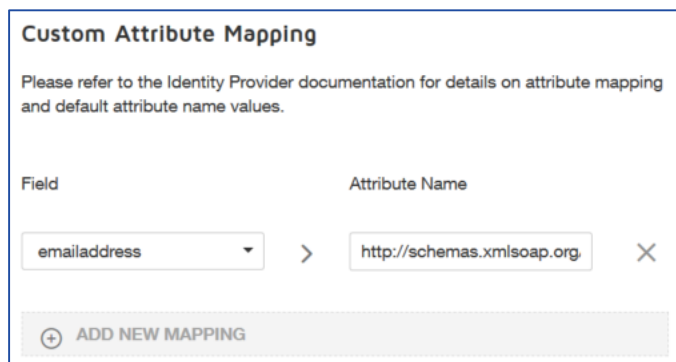
### Azure AD Application Configuration Panel – Single Sign On Settings

10. Hit **VIEW ENDPOINTS** and leave the popup open.
11. Open the URL listed for **Federation Metadata Document**. An XML file should show up, leave it open as well.

Endpoints and Federation Metadata Document

12. Go back to the **Identity Provider** you set up in DocuSign and click on **Actions -> Edit**
  - a. **Identity Provider Issuer**: set this to the value inside the **entityID** node from the **Federation Metadata Document** XML file opened above. It should look something like 'https://sts.windows.net/{GUID}/'
  - b. **Identity Provider Login URL**: Set this value to the **SAML-P Sign-On Endpoint** in the **App Endpoints** popup above.
  - c. **Identity Provider Logout URL**: Set this value to the **SAML-P Sign-Out Endpoint** in the **Federation Metadata Document** popup above.
  - d. **For the certificate**, from the **Federation Metadata Document** XML, copy the content of `<KeyInfo><X509Data><X509Certificate>`  
**Copy this only**  
`</X509Certificate></X509Data></KeyInfo>`  
 and paste it in a txt plain file. Save it as **.cert** and import it in DocuSign.

- e. Depending on your Active Directory configuration, you may need to configure a **Custom Attribute Mapping** in order to map the email of your users. Within the **Federation Metadata Document XML** search for the Uri of the field that contains the email, for example <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>. Usually, Azure AD sends over the email address in the 'name' property of the SAML assertion, therefore you will most likely have to map the emailaddress field to: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>



**Custom Attribute Mapping**

Please refer to the Identity Provider documentation for details on attribute mapping and default attribute name values.

Field	Attribute Name
emailaddress	http://schemas.xmlsoap.org.

+ ADD NEW MAPPING

*Custom Attribute Mapping for Email*

13. Go back to Azure, select your new custom app and hit **CONFIGURE**.
14. Configure **USER ASSIGNMENT REQUIRED TO ACCESS APP** as you need. If select YES, go to **USERS** and assign users accordingly.