

DocuSign Authentication Overview

Service Integration

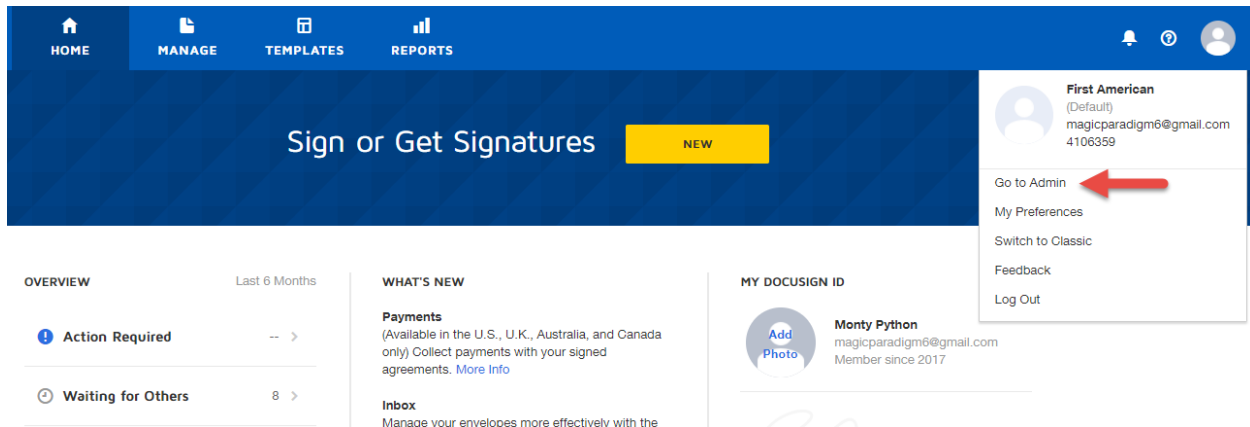
Requests to the DocuSign API must be authenticated. For applications that integrate to DocuSign without the direct involvement of senders, the use of a service integration is recommended. When a service integration is used, a one-time consent by the sender is all that is required. Once the one-time consent is given to the application (integrator key), it may make API calls by impersonating the sender. There are 2 types of consent that could be given to an application using a service integration:

User consent: An individual user with a DocuSign account can give consent that allows your application to use their account.

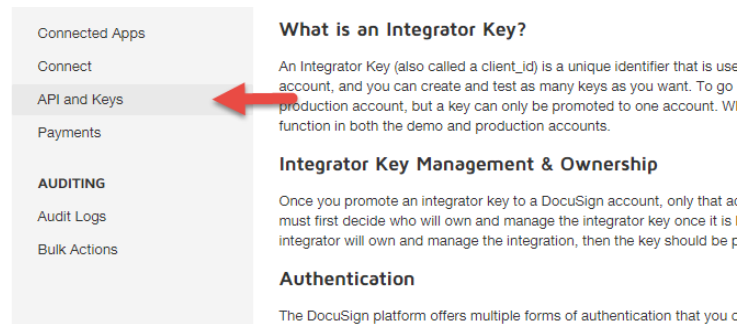
Admin consent: A domain administrator can give consent on behalf of *all* the users within the organization's email domain. See the [DocuSign Organization Administration guide](#) to learn more about authorizing an application

Getting your first service integration with user consent to work

1. Generate an integrator key for your application. The integrator key is used to uniquely identify your application to DocuSign. To generate an integrator, log into the DocuSign Web Application and select **Go To Admin** from the top menu on the right-hand side:



Select **API and Keys** from the menu at the left hand side of the screen:



Press the button labeled **ADD INTEGRATOR KEY** and a pop-up window will be displayed. In the pop-up window, put in a description for your application. The link to privacy policy and terms of use are optional fields that can be populated later.

Add API Integrator Key✕

App Description *

Link to Privacy Policy

Link to Terms of Use

☐ This is a mobile app.

ADD **CANCEL**

Add a redirect URL by pressing the **ADD URI** button. The redirect URI is the URL that the system will redirect to when you have granted consent.

After the URI has been added, add a secret key by pressing the **ADD SECRET KEY** button. For the purposes of the service integration authentication, you will not use the secret key again.

After adding the secret key, create an RSA keypair by pressing the **ADD RSA KEYPAIR** button. Be sure to save the private key to notepad or some other place that you can retrieve it again. After creating the RSA keypair, the private key will no longer be shown in the web application. It is important to note that private key begins after the line that reads:

-----BEGIN RSA PRIVATE KEY -----

And ends right before the line that reads:

-----END RSA PRIVATE KEY-----

2. Now that you have an integrator key set up, you must consent to giving it the rights to impersonate your sender to make API calls. Consent must be given only once and requires user interaction with DocuSign. Once consent has been given, the service integration does not need any further user interaction to make API calls.

To grant consent, enter in the following URL in a new browser session or ideally a separate browser from the one you used to log into your DocuSign account:

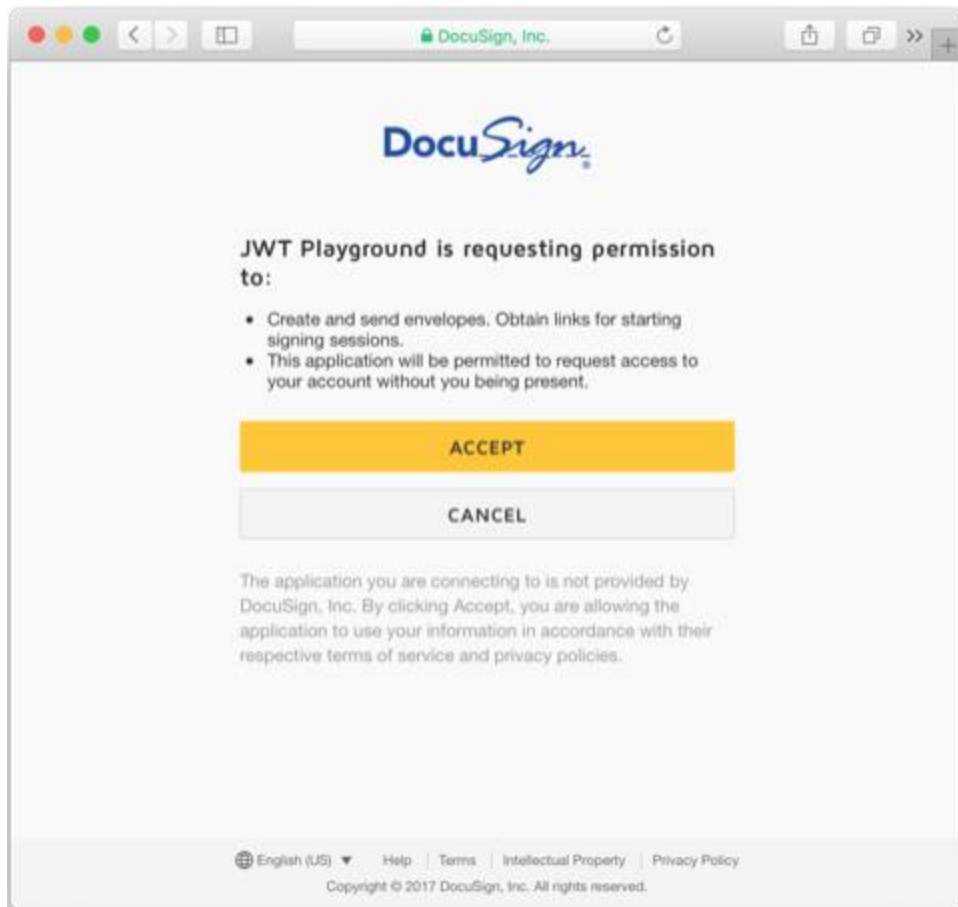
[https://account-d.docusign.com/oauth/auth?
response_type=code&scope=signature%20impersonation&client_id=\[integrator key\]
&\[redirect URI\]](https://account-d.docusign.com/oauth/auth?response_type=code&scope=signature%20impersonation&client_id=[integrator key]&[redirect URI])

Insert your integrator key and redirect URI into the URL e.g., if your integrator key is *1a971ea6-780f-49fd-a622-d23232a01d52* and your redirect URI

<https://dsdemos.docusign.com/dsportals/finance/>, your URL would be:

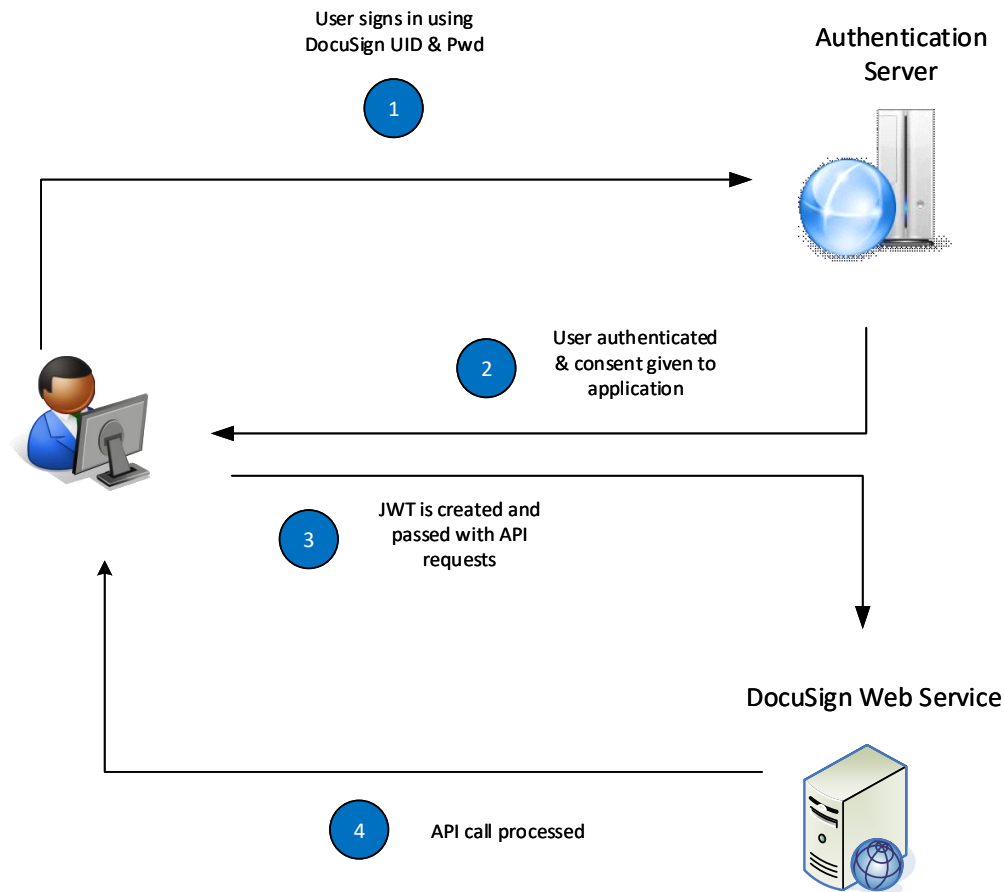
[https://account-d.docusign.com/oauth/auth?
response_type=code&scope=signature%20impersonation&client_id=ee91920b-8a4e-4726-
b87b-899aaf5bf060&redirect_uri=https://dsdemos.docusign.com/dsportals/finance/](https://account-d.docusign.com/oauth/auth?response_type=code&scope=signature%20impersonation&client_id=ee91920b-8a4e-4726-b87b-899aaf5bf060&redirect_uri=https://dsdemos.docusign.com/dsportals/finance/)

You should be presented with a DocuSign login screen. Log in the with your DocuSign account credentials and the following screen will be displayed:



Click *ACCEPT* and the screen will redirect to the redirect URI you specified. Your one time consent for the integrator key has been granted and you will not be prompted for your DocuSign credentials again when using this integrator key to make API calls.

3. For an application to use a service integration to authenticate with DocuSign, it requires a JSON Web Token (JWT). The process to perform the service integration follows the workflow shown below:



To create the JWT requires 3 components: a header, payload and signature.

The header will always be:

```
{
  "typ": "JWT",
  "alg": "RS256"
}
```

The payload consists of the following data:

```
{
  "iss": "[integrator key]",
  "sub": "[DocuSign user ID]" (not the account ID),
  "iat": [the issued at time],
  "exp": [the expiration time] (the value will be clipped at IAT + 3600 seconds)
  "aud": "account-d.docusign.com", (the address for the DocuSign auth service)
  "scope": "signature impersonation"
}
```

For the signature, the JWT is signed by the RSA private key created earlier and 64-bit encoded.

To create the JWT, it is recommended that a JWT toolkit be utilized. To see a fully working example written in C# and .NET, please refer to the reference application.

Utilizing the reference application

The *ServiceIntegration* application allows users to interactively test out their integrator keys with a service integration. To use the application, follow these steps:

1. Follow step 1 above to generate an integrator key for your application
2. Follow step 2 above to grant consent for your application to make API calls using your identity
3. Now that you have an integrator key, private key and DocuSign user ID, you can use the *ServiceIntegration* application to test your integrator key:
 - a. Enter in the values for your integrator key, DocuSign user ID and private key. Press *Next* to continue

DocuSign Authentication Examples

Home

Help

For demonstration purposes only.

Service Integration Authentication Example

Integrator Key (client ID)

1e971ee6-780f-49fd-a622-d23232a01d52

User ID (sub)

e602a60e-5ac0-44a5-9e2c-01e251ddf116

Private Key

MIIEpAIBAAKCAQEAljJkwo7rErqLOKgzqOja9RlNKupSTxbtH4wYzYqRcbk/c0
dKYTHX+xmJkGs0k82mXqXYXWSYj97IDUaZDuxRLuoBGItG9uetpVKp/62Hicq
GlcwS3wLXpYa+zFPW4eOpJC8F26an4tdgLiXyJIRjykr4TcBywav3kWGmVJ+w6rs
X0j/WhAw40R3TlydM4yEh+Aws61sGihFeH5cc7Rq/lxalRQYmohsuqGa8WRReJgyO
rZw/Vh3S2p/9WayKe78yQ/18xhJsM3DWIrX/DKvX0KfQ5iqm4MVPZm91RVnaa3On
fw89VhtLcyF3nzoCqkYOAi1FBj0WbaP1TvDOQIDAQAABAB158IEOBmTYHAPt
bgU8R4P1uHterLB4qJL5coVStJA6zoJr7gUB9NM9Pa3gXawzMQg5JY3N7eEgaJH
dvohnkThSszBuBooRIUFDmkyowlEsaavgSFnuS4MYsJUbQPlxy+BmC3g+uKQMSW
9GblI4aS2MX/bZG2dUZYdeSeGvsDgpY8G8ISjzjISwm/0t6yuKdgybV/Ga6tQV2
RDLYe4cYYnaqAyoQ9GfpmSakiGLV/btk4OmPLieY2vAc5McLOdypASTIOa2awR
XT6Ge7vTfPQe9os1A8u2tmzA47EAixDQJjhaT06c95fKksORM7d5lhN0+HSL8h
gYMHMF0CgYEA08DWPXfjgCB4T5rGMFDMYqmioSk71EvJef4V16axP/VLbX54Gwu
89lgmDwOEBAS4S18IwvHQ1TgtngsZiQZm5vZNs9XwzIN5nB7e+psWAHhgS7NkMBx
bo4lsRnuMMDSkJ2FWxWjb0mcmK4mRY26UyJVD/VXChJ+YiwGF7Cox8CgYEArdS
IF5bDaFib2W6mFwWlb4eYzoFMvMGeadmaCBuZLxmEMP0s2epNFZLTraCYeZp63LC
HBpY5nyHkqNyCnuNLf3dEz7U4G4EM4k3PNUM9mv1fp7xo3cGVqEkKui5VhWwMXj
ChpraA/OBLwM7ta4SN18XXgtKuv0I92AV0bZqcCgYEAxbl9Jx+FYyxH1+rj9dml
cxnVdkfjPhXGQWtwFXmv1ymnDMFHq3Ncll4XKQail0dhTukl6LFCEkXxIKIRzbOOY
kCQJg413Pt1IMDeHS/a8fM+LonAoYUE/0GksxRS6DYRnh4foR3JtWla7dWCWRfT
QxSnm8CfnvFmIDUe97LVa9kCgYEAzAmGsLs+cUjB9nINN4AcvFulsF1QKlelu+926h
j+XxgH0wtPapu2A7h+RKTmVvDMCj3WpFq9hWfSyc2Yz7z78AGIT2w3rE1+9jtug
Ndvl4GKH27Os3v30C+yU7wFihFXKeHCFv2xVXhyEV/vavZ4P+kTIDBUNhC85i2S
6ZIK/V8CgYAUwJPD2KuhFieMasLaY4Qv9dCeMgX5+pp/ct/gXrEsYcJHtdq8u+Pk
Oehwqd523P+pyTS23cm7b9yPrmthf3KXvm/XG031gFDVYRTEmu+Zi28Ys7NBgu
xkldwDlkc2yH0eVhfmMgM6rqWZOxyuotcAGT1MsIYGIAPAMd0bvY6Q

Next

- b. The JWT that is created will be used to create an envelope with a certified delivery recipient. From the *Accounts* dropdown list, select the account from the envelope should be sent. Enter in the recipient name and email address. Lastly, upload a PDF that you want to send as part of the envelope by browse to a file and selecting *Upload*. When you are finished entering all the data, click *Submit* to continue:

DocuSign Authentication Examples Home Help

For demonstration purposes only.

Service Integration Authentication Example

Primary Account Holder

Account
First American

First Name
Warren

Last Name
Buffet

Email Address
magicparadigm@live.com

Envelope Information

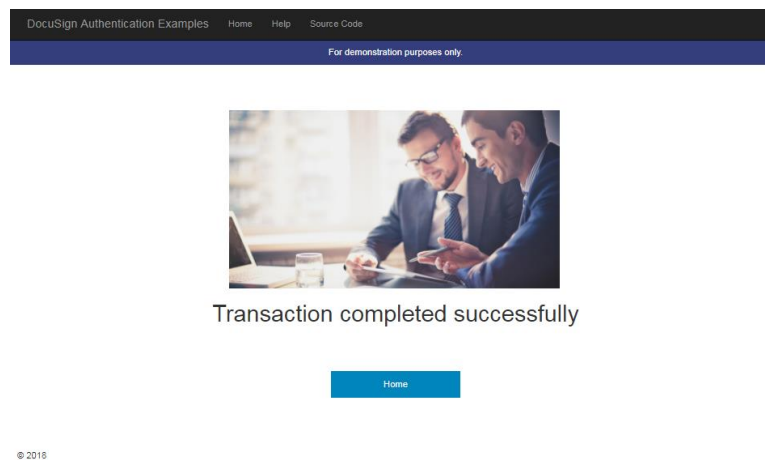
[Choose File](#) No file chosen

Upload

Upload File
samplecontract.pdf

Submit

- c. Once you see the confirmation screen, check the email account to which you sent the envelope:



To access the source code for the reference application, click the *Source Code* link on the top menu