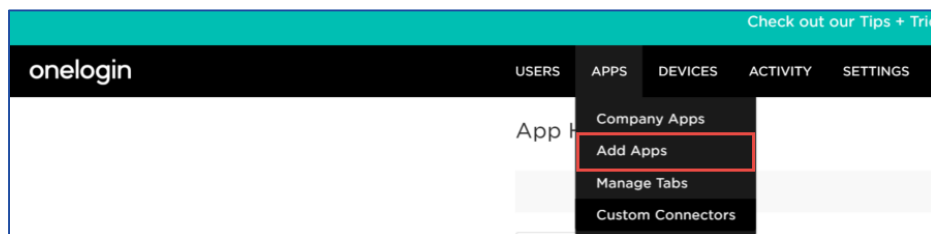
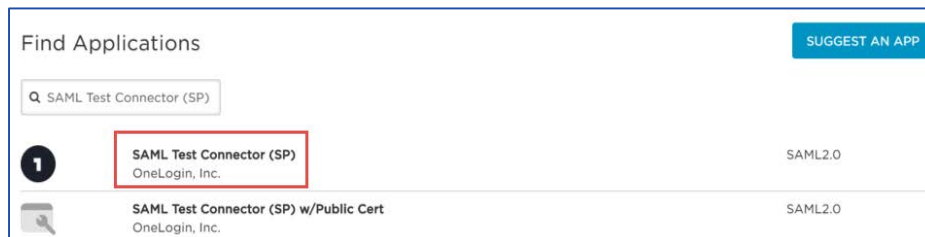


Quick Guide

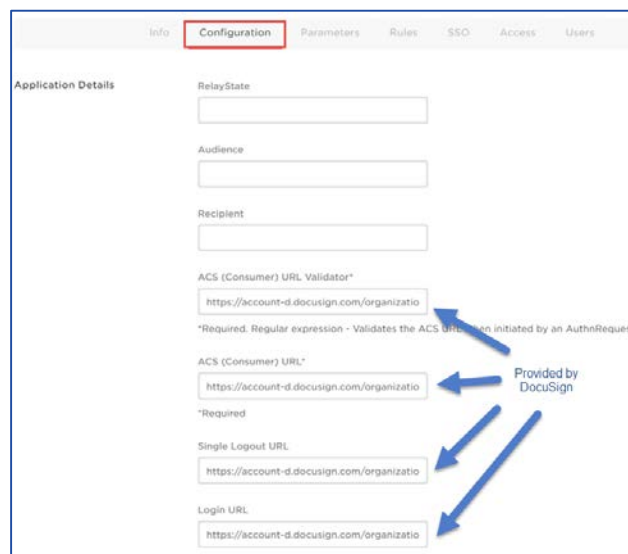
1. Pre-requisites:
 - a. DocuSign admin user.
 - b. OneLogin admin user.
 - c. DNS admin user.
2. Login to OneLogin and go to **APPS** -> **Add Apps**.



3. Search for **SAML Test Connector (SP)**.



4. Update the **Display Name**, for example DocuSign, and the icon. Then hit **SAVE**.
5. Go to **Configuration** and complete the fields as follows:



6. Go to **Parameters** and configure the following mappings:

Parameters		
SAML Test Connector (SP) Field	Value	
Email	Email	
emailaddress	Email	custom parameter
givenname	First Name	custom parameter
surname	Last Name	custom parameter

⇒ Check the flag **Include in SAML assertion** for all of them.

7. Go to **SSO**. Download the certificate and save Issuer URL, SAML 2.0 Endpoint and SLO Endpoint.

Info	Configuration	Parameters	Rules	SSO	Access	Users
------	---------------	------------	-------	------------	--------	-------

Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)
[Change](#) [View Details](#)

Issuer URL

SAML 2.0 Endpoint (HTTP)

SLO Endpoint (HTTP)

8. Login to DocuSign Admin Portal.

- Demo: <https://admindemo.docusign.com/authenticate>
- Production: <https://admin.docusign.com/authenticate>

9. Open the **Domains** menu option.

- Hit **CLAIM DOMAIN**.
- Complete your domain. Without http:// for example *docusign.com* and hit **CLAIM**.
- Update your DNS entry to include the TXT token.
- Once your DNS entry is created, hit **ACTIONS** and then **Validate**.

DocuSign ADMIN		Go to DocuSign	Help	
----------------	--	----------------	------	--

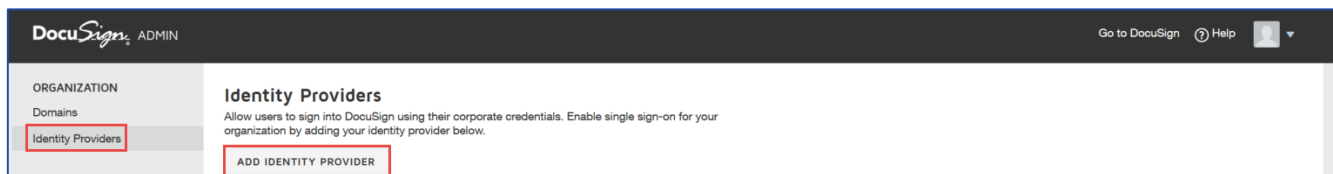
ORGANIZATION	Domains		
Domains	Control email domains and define how users are created, managed, and authenticated. Manage a domain by claiming and verifying it below.		
Identity Providers	CLAIM DOMAIN		
ACCOUNT			
Billing and Usage			
Account Profile			
Security Settings			

Domain Name	Status	
.com	Active	ACTIONS

- e. Hit EDIT and mark the options that you need.¹

- ☐ Always require login when opening envelopes
☐ Prevent unmanaged signups
☐ Require all users to authenticate with Identity Provider

10. Open the **Identity Provider** menu option and hit **ADD IDENTIFY PROVIDER** if it has not been created by DocuSign yet. Otherwise, hit **ACTIONS** and then **Edit**. Complete the fields as follows:
- Identity Provider Issuer:** use the **Issuer URL** from section 7.
 - Identity Provider Login URL:** use the **SAML 2.0 Endpoint (HTTP)** from section 7.
 - Identity Provider Logout URL:** use the **SLO Endpoint (HTTP)** from section 7.
 - Upload the **certificate** from section 7.



11. Go back to OneLogin and assign users to the new Connector to meet your internal policies.