

Last Modified: June 22, 2016

DocuSign is a San Francisco- and Seattle-based company that provides electronic signature technology and Digital Transaction Management services for facilitating electronic exchanges of contracts and signed documents. DocuSign’s features include authentication services, user identity management and workflow automation.

Before You Begin

- RSA SecurID Access components including administrator and end user accounts must be in place.
- Acquire a DocuSign Enterprise account and verify that SAML SSO is available.

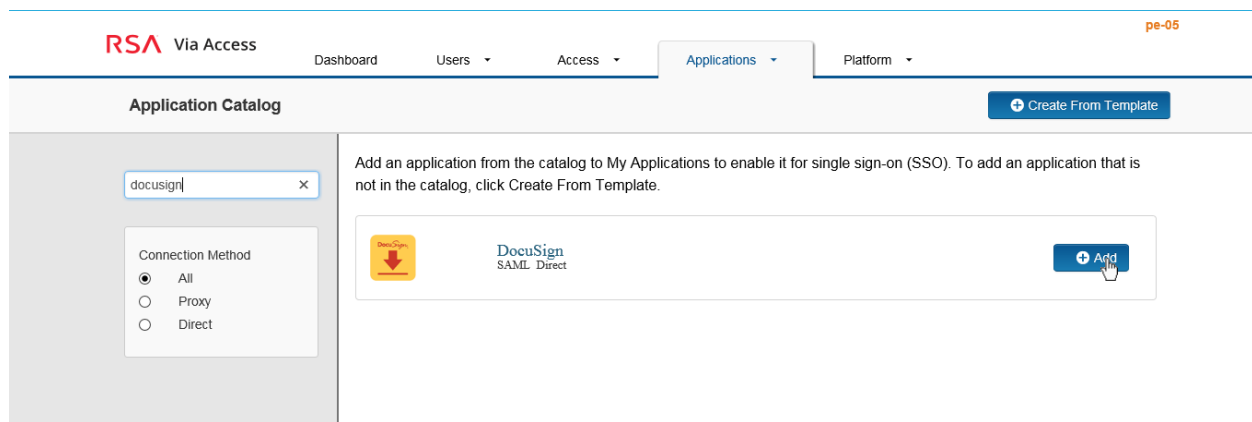
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure DocuSign to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. Locate DocuSign SAML Direct from the list of applications and click **+Add**.



3. On the Basic Information page, specify the application name how you want to appear for users and click **Next Step**.

The screenshot shows the 'DocuSign' configuration page in the 'Applications' section of the RSA Via Access interface. The page title is 'DocuSign' and the user is logged in as 'pe-05'. The 'Basic Information' section is active, showing a form with the following fields: 'Name' (containing 'DocuSign'), 'Description (optional)', and a 'Disabled' checkbox. A 'Next Step' button is highlighted with a mouse cursor. A sidebar on the left shows a navigation menu with '1. Basic Information' selected, and other options: '2. Connection Profile', '3. User Access', and '4. Portal Display'. A message at the top states 'All fields are required (except where noted)'.

4. On the Connection Profile page configure the Initiate SAML Workflow settings and scroll down to the SAML Identity Provider (Issuer) section.

 **Note: The following SP-initiated configuration works for both SP-initiated and IDP-initiated work flows.**

Initiate SAML Workflow

The screenshot shows the 'Initiate SAML Workflow' configuration page. The 'Connection URL' field is set to '<Service Provider Login URL>'. The 'IDP-initiated' radio button is unselected, and the 'SP-initiated' radio button is selected. The 'Binding Method for SAML Request' section has 'Redirect' unselected, 'POST' selected, and 'Signed' unselected. At the bottom, there is a warning icon and the text 'No certificate loaded', along with 'Choose File' and 'Generate Cert Bundle' buttons.

- Enter the Service Provider Login URL from the DocuSign SAML endpoints page into the **Connection URL** field.
- Select **SP-initiated**.
- Set the binding method to **POST**.

5. Configure the SAML Identity Provider settings and scroll down to the Service Provider section.

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): p8365bfroko

Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded

?

Certificate Loaded

CN=pw.local, Valid Until:
05/25/2036

Include Certificate in Outgoing Assertion

- Take note of the Identity Provider URL.
- Take note of the Issuer Entity ID.
- Select **Choose File** and upload the private key.
- Select **Choose File** and upload the public certificate.
- Mark the checkbox to **Include Certificate in Outgoing Assertion**.

- Configure the Service Provider settings and scroll down to the User Identity section.

Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

- Enter the Service Provider Assertion Consumer Service URL from the DocuSign SAML endpoints page, found on page 10 step 12 into the **Assertion Consumer Service (ACS) URL** field.
 - Enter the Service Provider Issuer URL from the DocuSign SAML endpoints page, found on page 10 step 12 into the **Audience (Service Provider Entity ID)** field.
- Set **Identifier Type** to **persistent** and **Property** to the attribute in the identity source that contains the DocuSign username.

User Identity ?

NameID

Identifier Type: persistent

Identity Source: AD20

Property: sAMAccountName

Attribute Hunting ? NameID Attribute Hunting

- Expand the Advanced Configuration section, specify the attribute extensions as depicted in the following image and click **Next Step**.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
User Store <input type="text"/>	emailaddress	AD20 <input type="text"/>	mail <input type="text"/>	
User Store <input type="text"/>	givenname	AD20 <input type="text"/>	givenName <input type="text"/>	
User Store <input type="text"/>	surname	AD20 <input type="text"/>	sn <input type="text"/>	
+ ADD				

9. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy


No Access Allowed

Cancel

Next Step →

10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.

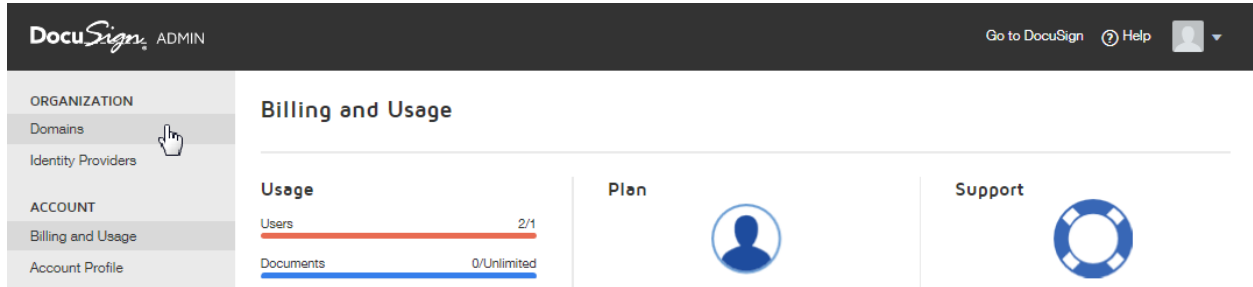
Publish Changes

Status:  Changes Pending

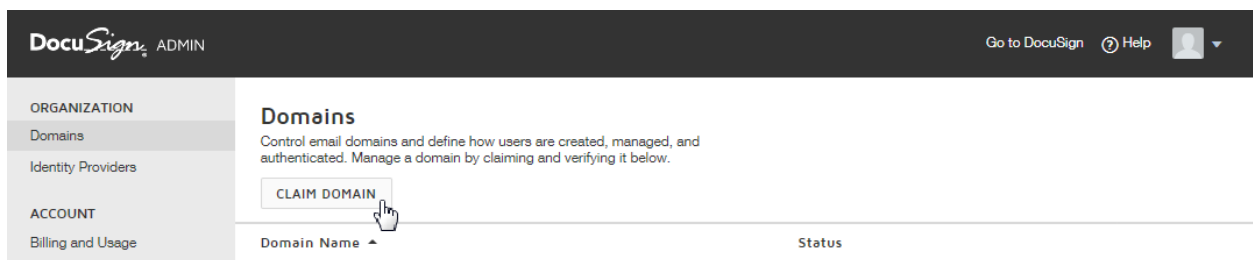
Configure DocuSign to Use RSA SecurID Access as an Identity Provider

Procedure

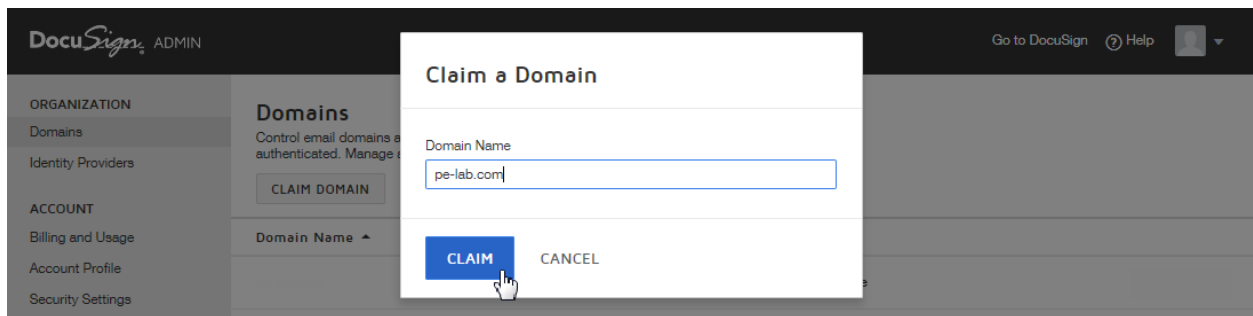
1. Logon to the DocuSign admin Web console and click on **Domains**.



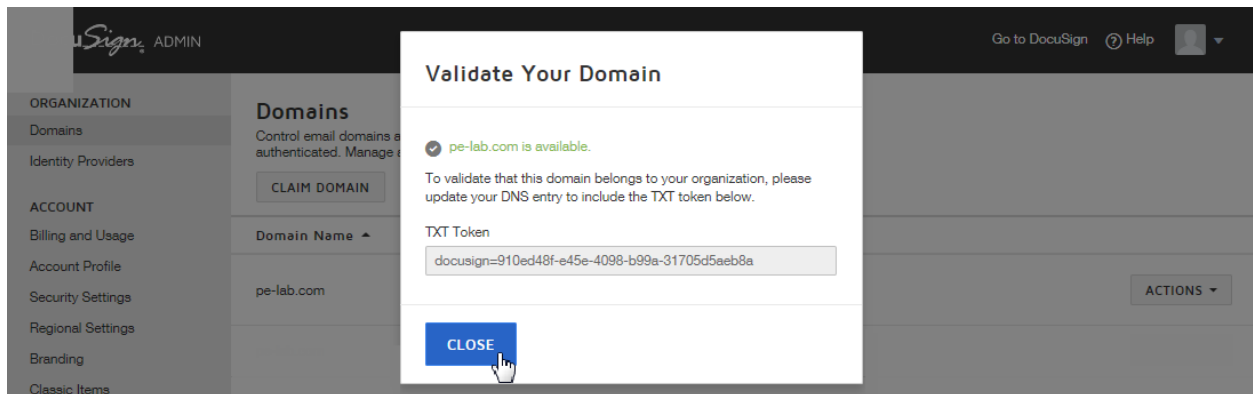
2. Click **CLAIM DOMAIN**.



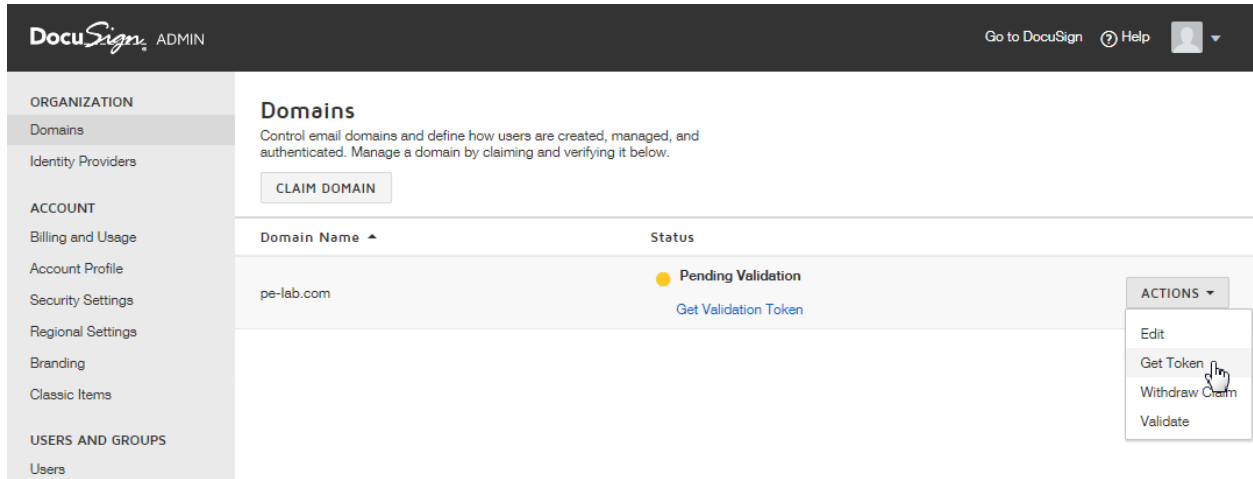
3. Enter the **Domain Name** and click **CLAIM**.



4. Update your DNS entry with a TXT record with the value shown on the screen.



5. After the TXT record has propagated, click **ACTIONS** > **Get Token**.



DocuSign ADMIN

Go to DocuSign Help

ORGANIZATION

- Domains
- Identity Providers

ACCOUNT

- Billing and Usage
- Account Profile
- Security Settings
- Regional Settings
- Branding
- Classic Items

USERS AND GROUPS

- Users

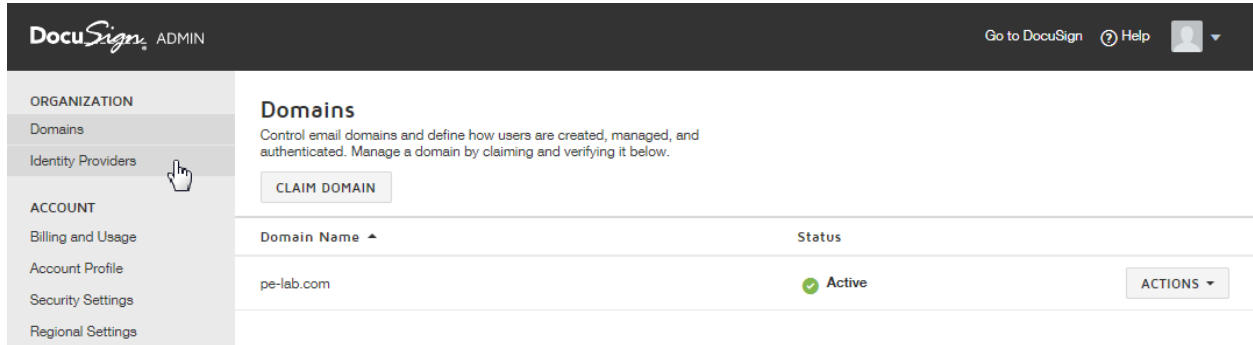
Domains

Control email domains and define how users are created, managed, and authenticated. Manage a domain by claiming and verifying it below.

CLAIM DOMAIN

Domain Name	Status	ACTIONS
pe-lab.com	● Pending Validation Get Validation Token	<ul style="list-style-type: none">EditGet TokenWithdraw ClaimValidate

6. Note status is **Active**, then click **Identity Providers**.



DocuSign ADMIN

Go to DocuSign Help

ORGANIZATION

- Domains
- Identity Providers**

ACCOUNT

- Billing and Usage
- Account Profile
- Security Settings
- Regional Settings

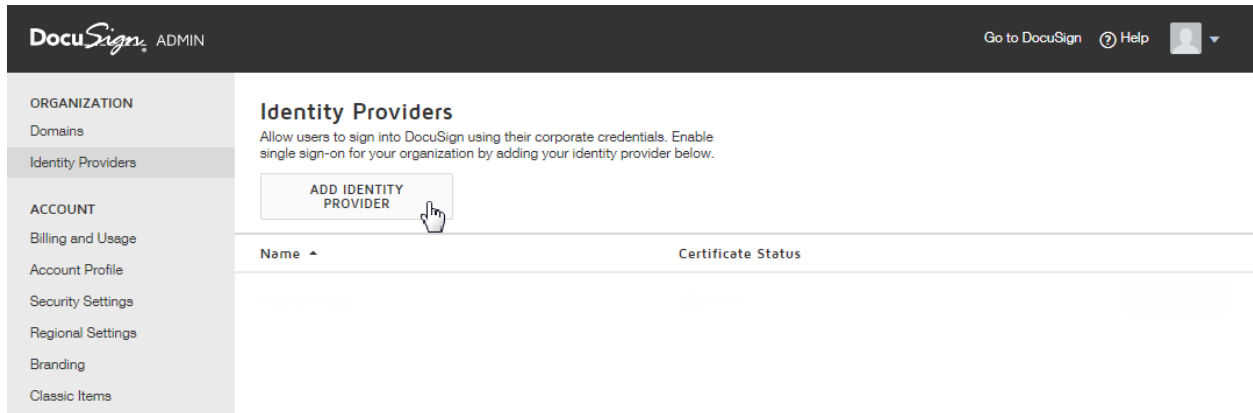
Domains

Control email domains and define how users are created, managed, and authenticated. Manage a domain by claiming and verifying it below.

CLAIM DOMAIN

Domain Name	Status	ACTIONS
pe-lab.com	● Active	

7. Click **ADD IDENTITY PROVIDER**.



DocuSign ADMIN

Go to DocuSign Help

ORGANIZATION

- Domains
- Identity Providers

ACCOUNT

- Billing and Usage
- Account Profile
- Security Settings
- Regional Settings
- Branding
- Classic Items

Identity Providers

Allow users to sign into DocuSign using their corporate credentials. Enable single sign-on for your organization by adding your identity provider below.

ADD IDENTITY PROVIDER

Name	Certificate Status
------	--------------------

8. Configure the Identity Provider Settings and click **Save**.

DocuSign ADMIN Go to DocuSign Help

Identity Provider List > Identity Provider Settings

Identity Provider Settings

SAVE CANCEL

SSO Protocol: **SAML 2.0**

Name *

Identity Provider Issuer *

Identity Provider Login URL *

Identity Provider Logout URL

Identity Provider Metadata URL

Sign AuthN request
 Sign logout request

Send AuthN request by: GET POST
Send logout request by: GET POST

Custom Attribute Mapping

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

Field	Attribute Name
<input type="button" value="ADD NEW MAPPING"/>	

SAVE CANCEL

English | Powered by DocuSign | Terms of Use | Privacy | Intellectual Property | Copyright © 2016 DocuSign, Inc. All rights reserved.

- Enter a **Name**.
- Enter Identity Provider Entity ID (from step 5 in the previous section) into the **Identity Provider Issuer** field.
- Enter the Identity Provider URL (from step 5 in the previous section) into the **Identity Provider Login URL** field.
- Set **Send AuthN request by** to **POST**.

9. Click **Add New Certificate**.

DocuSign ADMIN

Go to DocuSign Help

ORGANIZATION

- Domains
- Identity Providers

ACCOUNT

- Billing and Usage
- Account Profile
- Security Settings
- Regional Settings
- Branding

Identity Providers

Allow users to sign into DocuSign using their corporate credentials. Enable single sign-on for your organization by adding your identity provider below.

ADD IDENTITY PROVIDER

Name	Certificate Status
Via_Access_IdP	No Valid Certificates Add New Certificate

ACTIONS

10. Scroll to the bottom of the page and click **ADD CERTIFICATE**.

Identity Provider Certificates

ADD CERTIFICATE

Certificate Issuer	Thumbprint	Expires
--------------------	------------	---------

SAVE CANCEL

English | Powered by DocuSign | Terms of Use | Privacy | Intellectual Property | Copyright © 2016 DocuSign, Inc. All rights reserved.

11. Browse to the certificate file and click **Save**.

Note: This certificate must match the certificate uploaded on page 2, step 5.

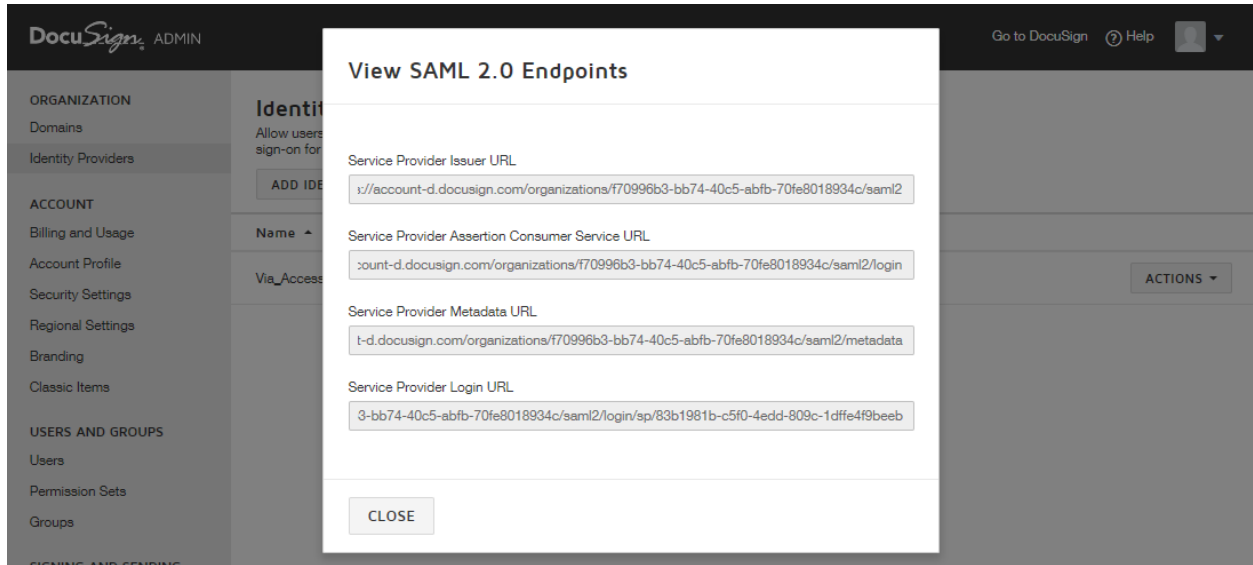
Identity Provider Certificates

ADD CERTIFICATE

Certificate Issuer	Thumbprint	Expires
CN=pw.local, OU=PE, O=PE, L=Bedford, S=MA, C=US	328F9900A8763D493CEB54961F1A303AD160D60F	May 25, 2036 4:18:56 PM

SAVE CANCEL

12. Click **ACTIONS** > **Endpoints** to view the logon, assertion consumer service and service provider entity ID URLs.



PEW