RSA SecurID Access SAML Configuration for DocuSign

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.

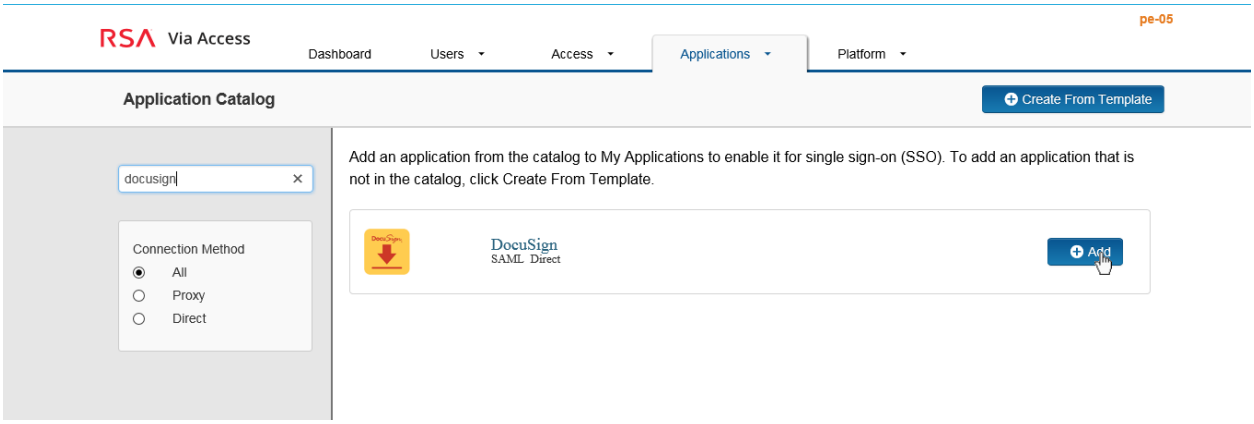
Procedure

1. Add the Application in RSA SecurID Access
2. Configure DocuSign to Use RSA SecurID Access as an Identity Provider

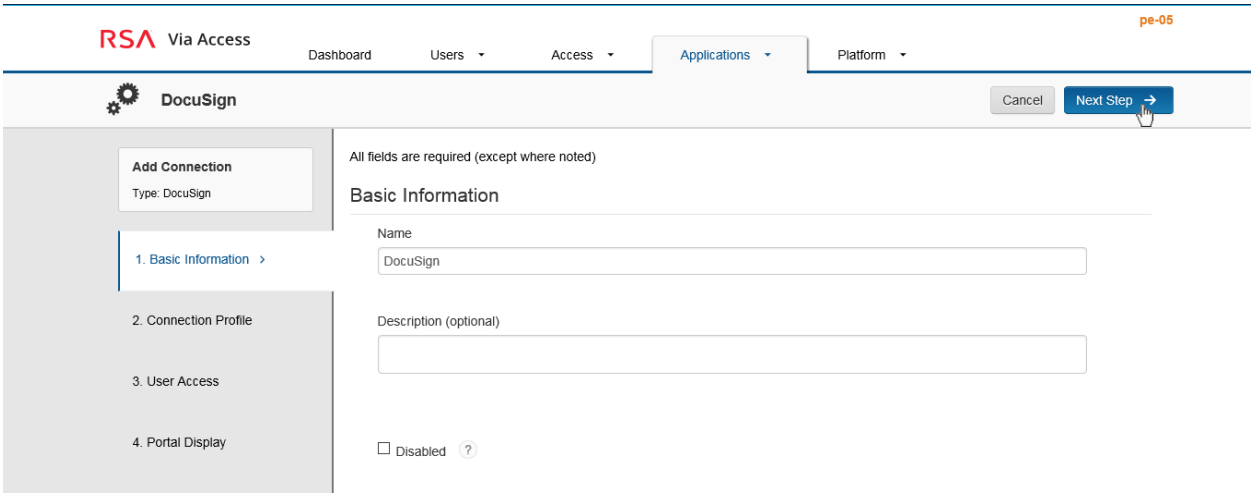
Add the Application in RSA SecurID Access

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**.

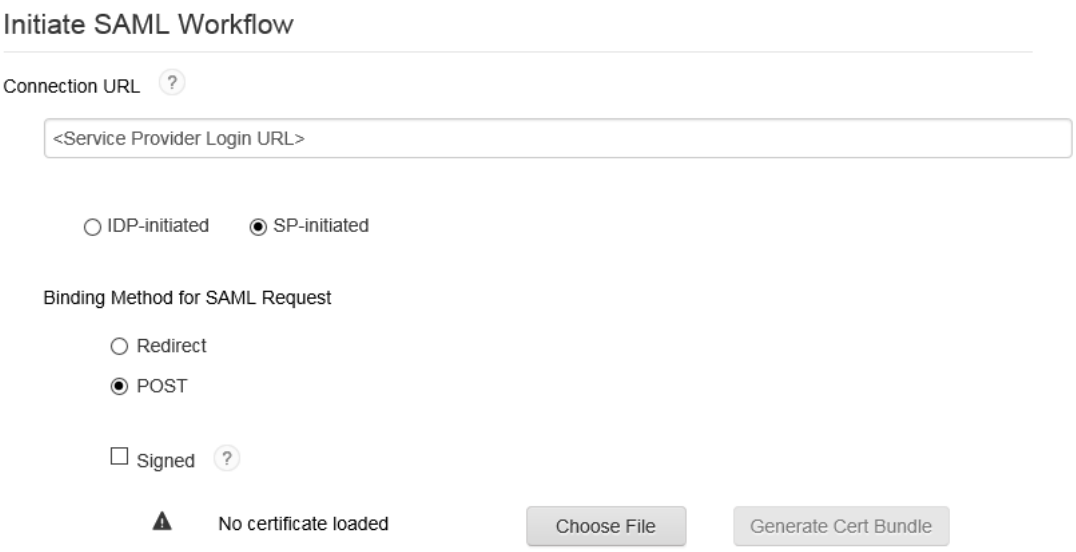


3. On the Basic Information page, specify the application name how you want to appear for users and click **Next Step**.



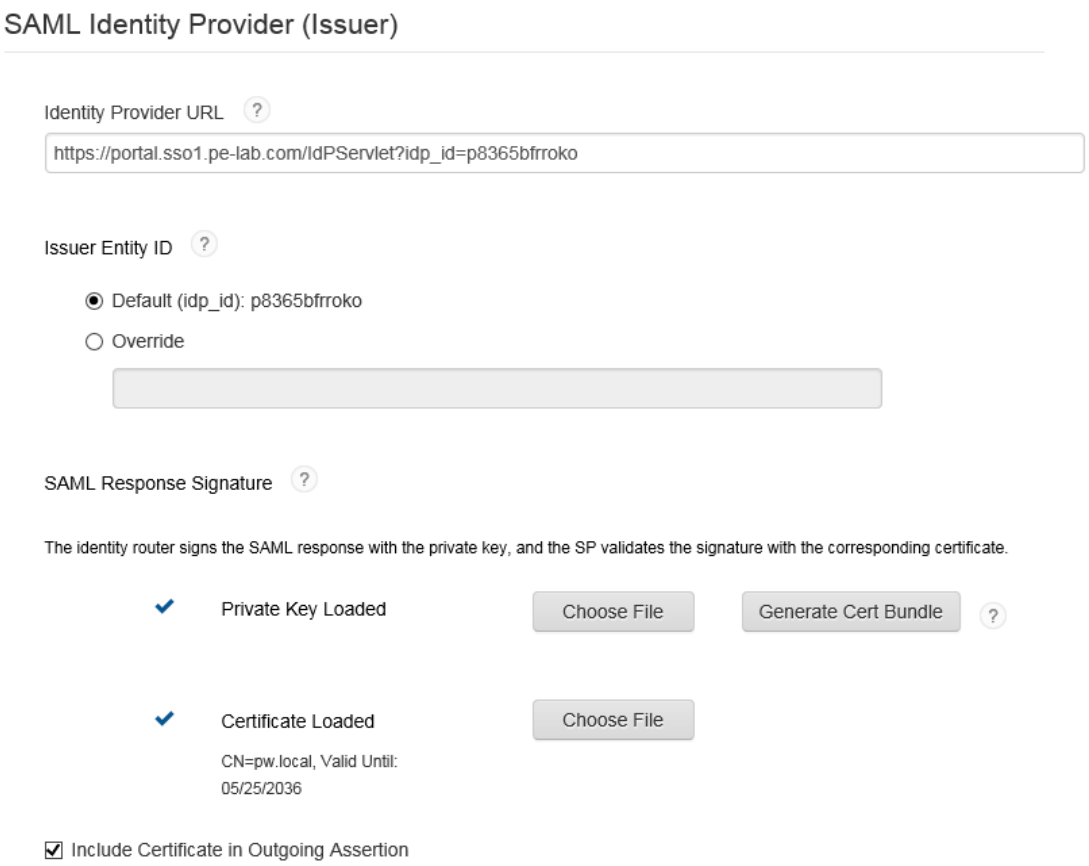
4. On the Connection Profile page configure the Initiate SAML Workflow settings and scroll down to the SAML Identity Provider (Issuer) section.

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



- 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.



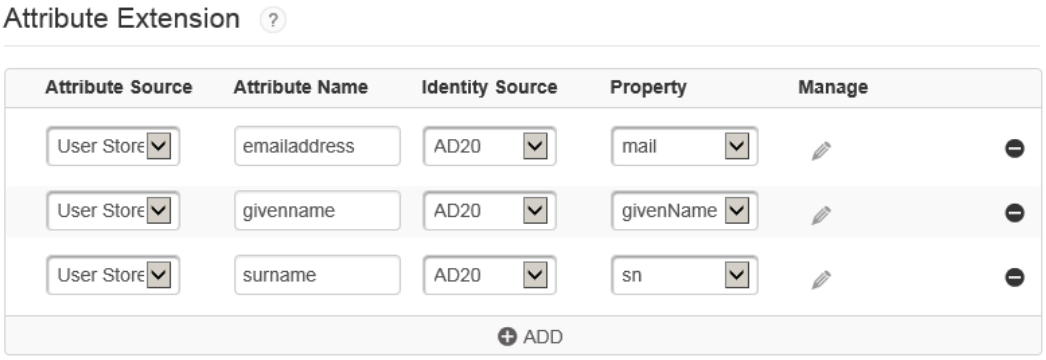
- Take note of the Identity Provider URL.
- Take note of the Issuer Entity ID.
- Select **Choose File** and upload the private key.
- Select **Choose File** and upload the public certificate.
- Mark the checkbox to **Include Certificate in Outgoing Assertion**.

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

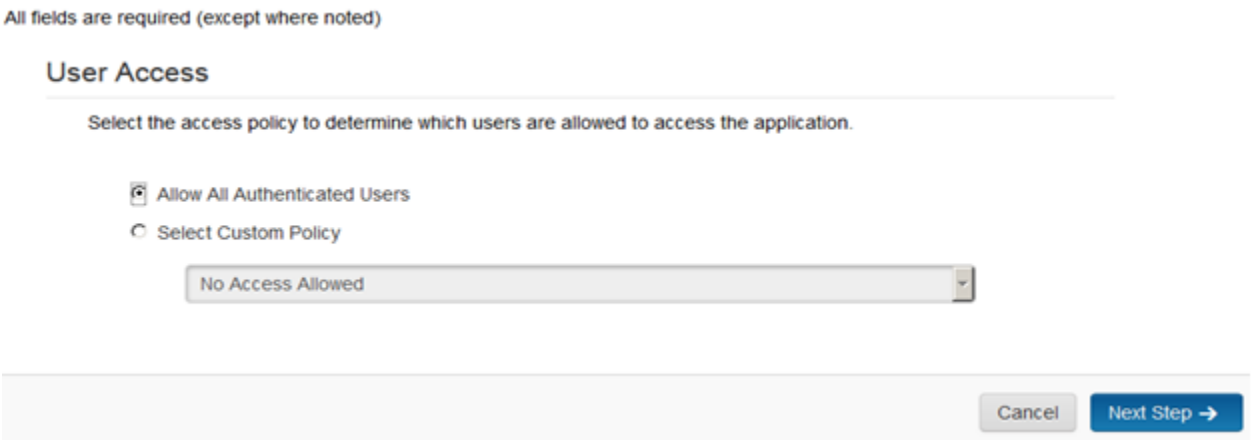
- Enter the Service Provider Assertion Consumer Service URL from the DocuSign SAML endpoints page ,found on page 10 step 12 into the **Assertion Consumer Service (ACS) URL** field.
- Enter the Service Provider Issuer URL from the DocuSign SAML endpoints page, found on page 10 step 12 into the **Audience (Service Provider Entity ID)** field.

7. Set **Identifier Type** to **persistent** and **Property** to the attribute in the identity source that contains the DocuSign username.

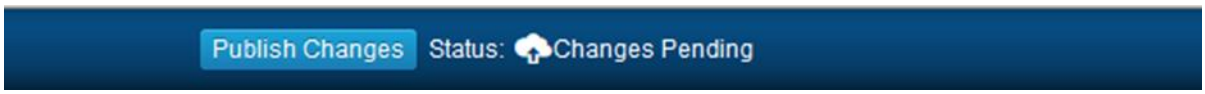
8. Expand the Advanced Configuration section, specify the attribute extensions as depicted in the following image and click **Next Step**.



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



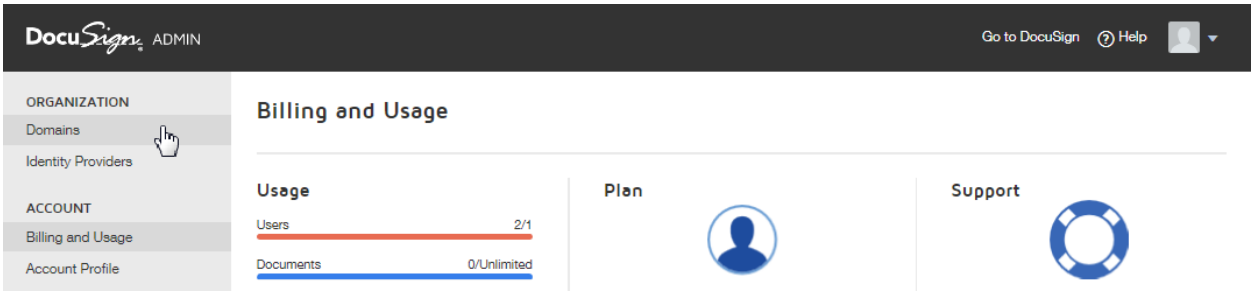
10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



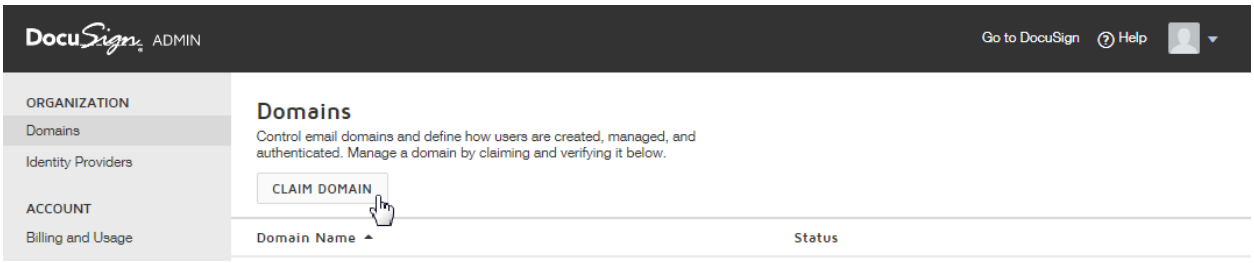
Configure DocuSign to Use RSA SecurID Access as an Identity Provider

Procedure

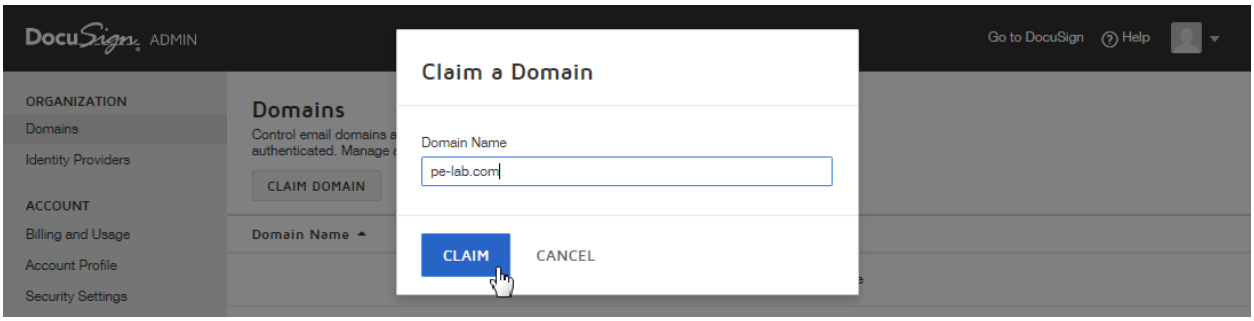
1. Logon to the DocuSign admin Web console and click on **Domains**.



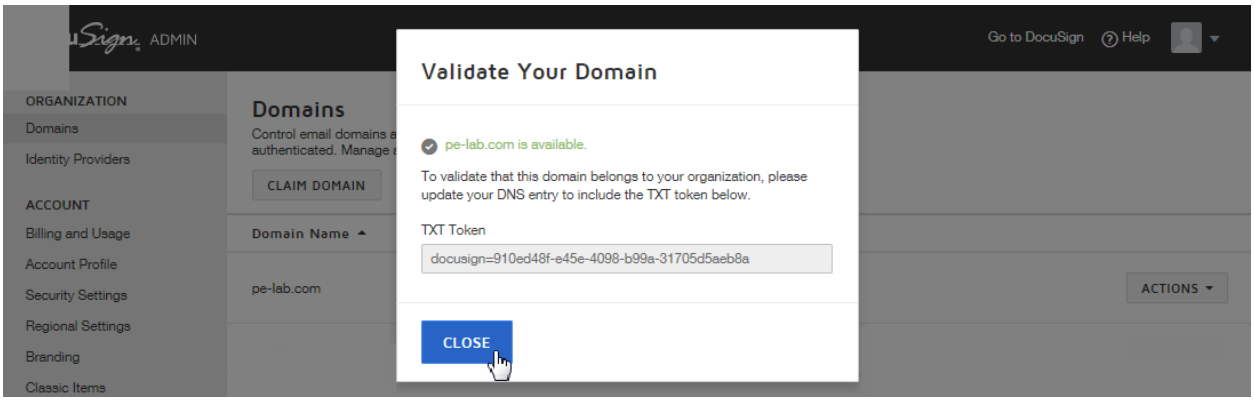
2. Click **CLAIM DOMAIN**.



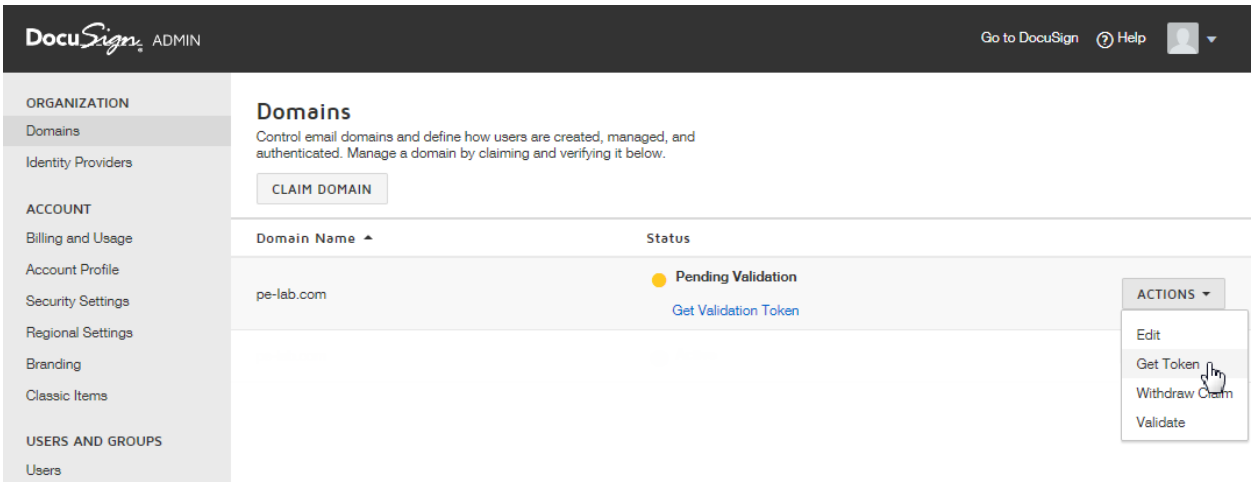
3. Enter the **Domain Name** and click **CLAIM**.



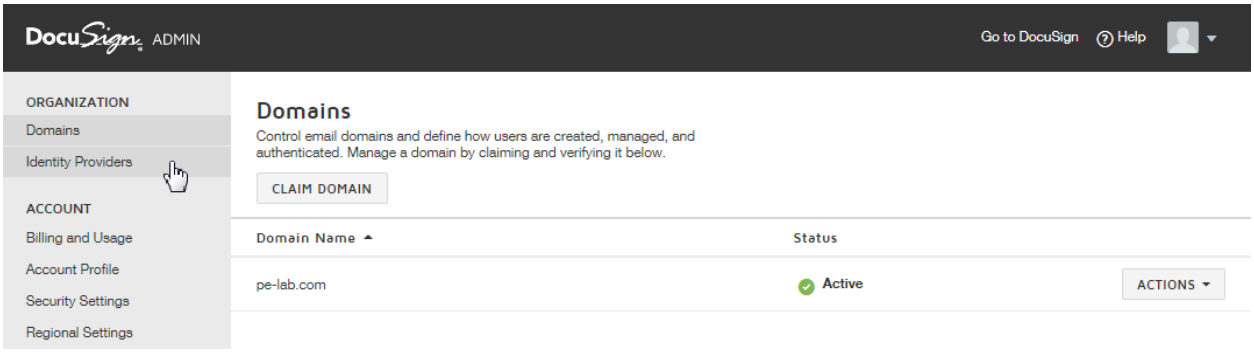
4. Update your DNS entry with a TXT record with the value shown on the screen.



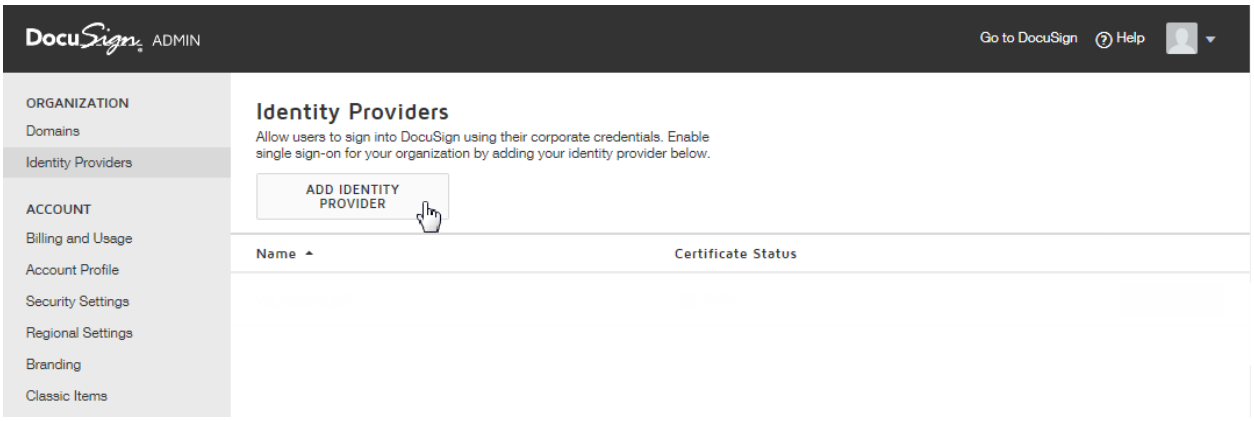
5. After the TXT record has propagated, click **ACTIONS** > **Get Token**.



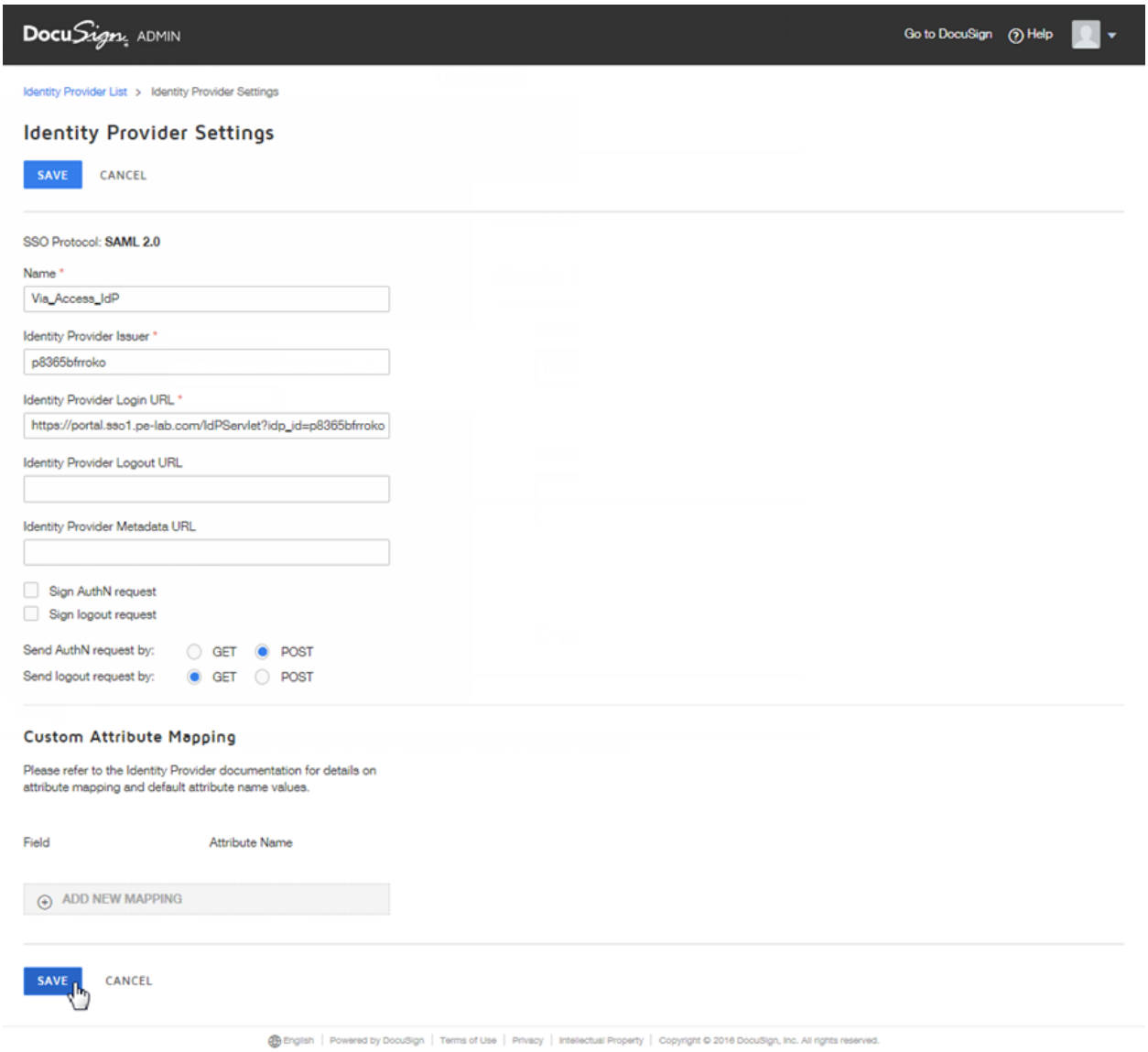
6. Note status is **Active**, then click **Identity Providers**.



7. Click **ADD IDENTITY PROVIDER**.

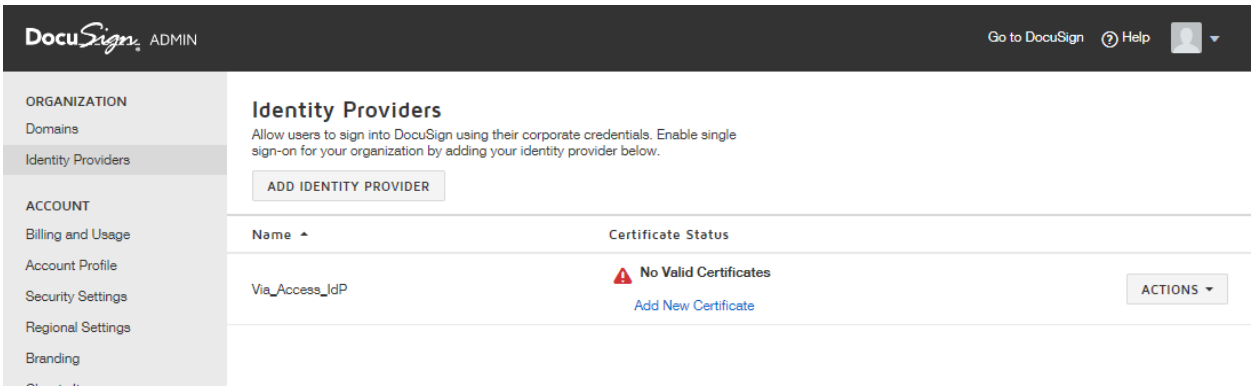


8. Configure the Identity Provider Settings and click **Save**.

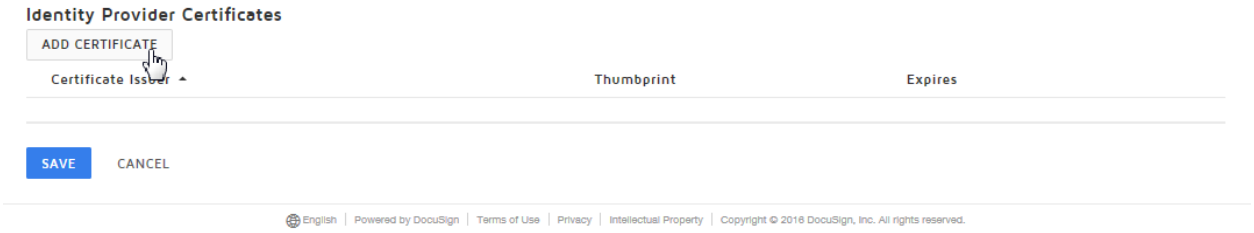


- Enter a **Name**.
- Enter Identity Provider Entity ID (from step 5 in the previous section) into the **Identity Provider Issuer** field.
- Enter the Identity Provider URL (from step 5 in the previous section) into the **Identity Provider Login URL** field.
- Set **Send AuthN request by** to **POST**.

9. Click **Add New Certificate**.

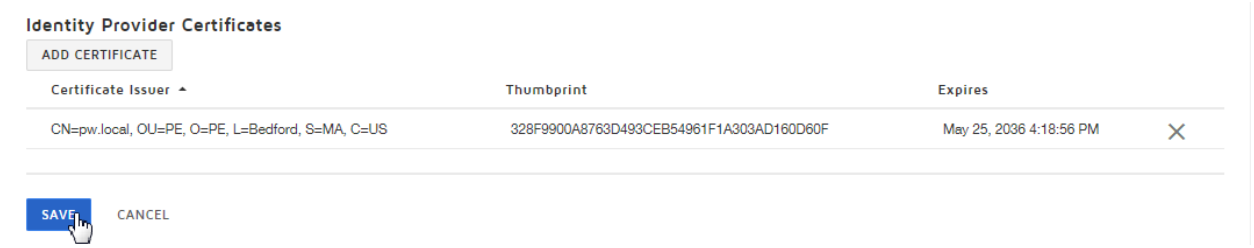


10. Scroll to the bottom of the page and click **ADD CERTIFICATE**.

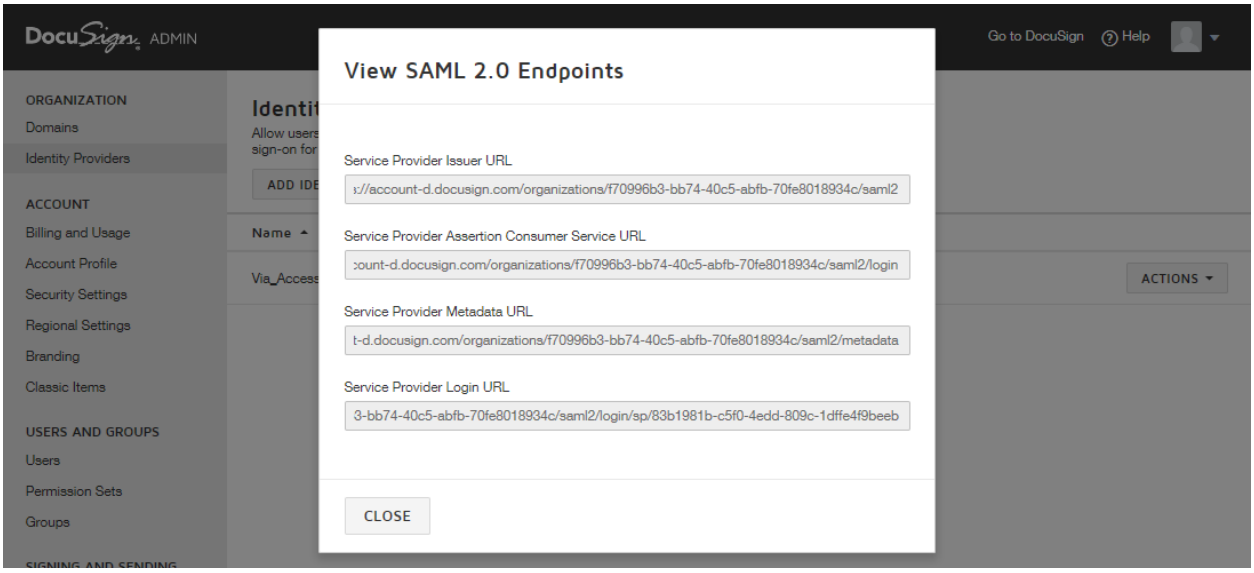


11. Browse to the certificate file and click **Save**.

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



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



PEW