RSA SecurID Access SAML Configuration for CA Flowdock

Last Modified: January 18, 2016

CA Flowdock (formerly Rally Flowdock) is your team's chat with a shared inbox. Teams using Flowdock stay up-to-date, react in seconds instead of days, and never forget anything.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and CA Flowdock.
- Obtain the ACS URL information from CA Flowdock.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

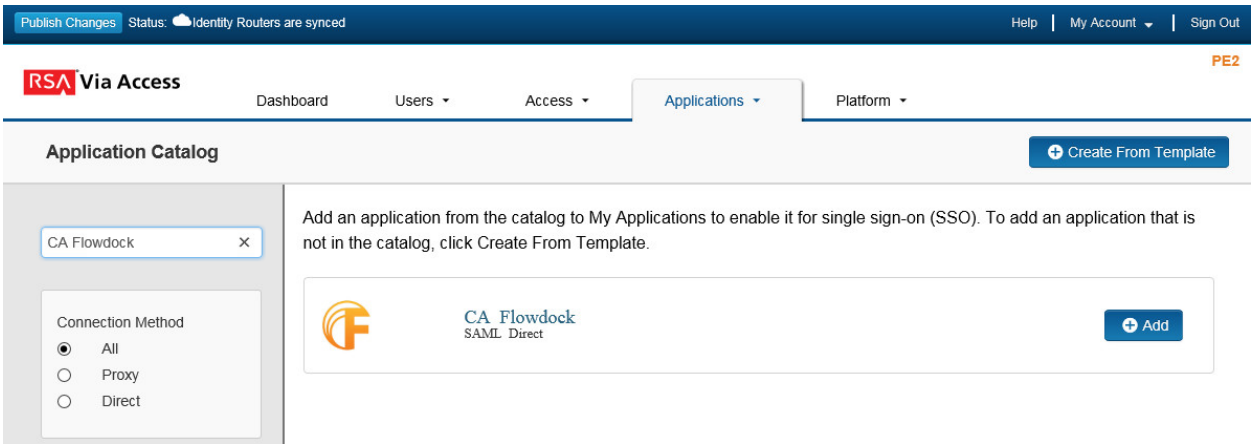
Procedure

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

Add the Application in RSA SecurID Access

Procedure

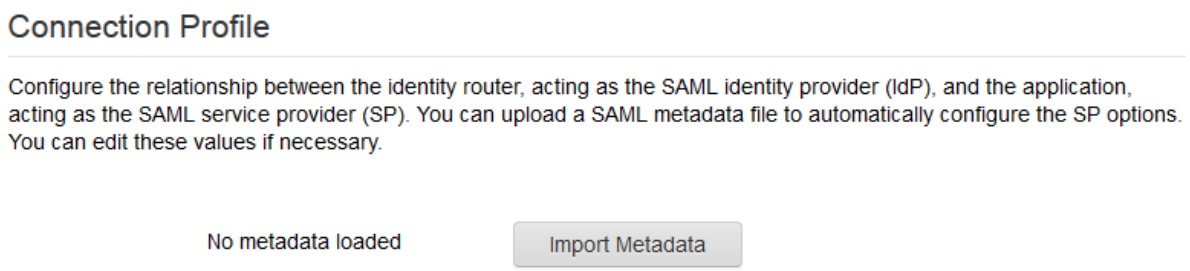
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.



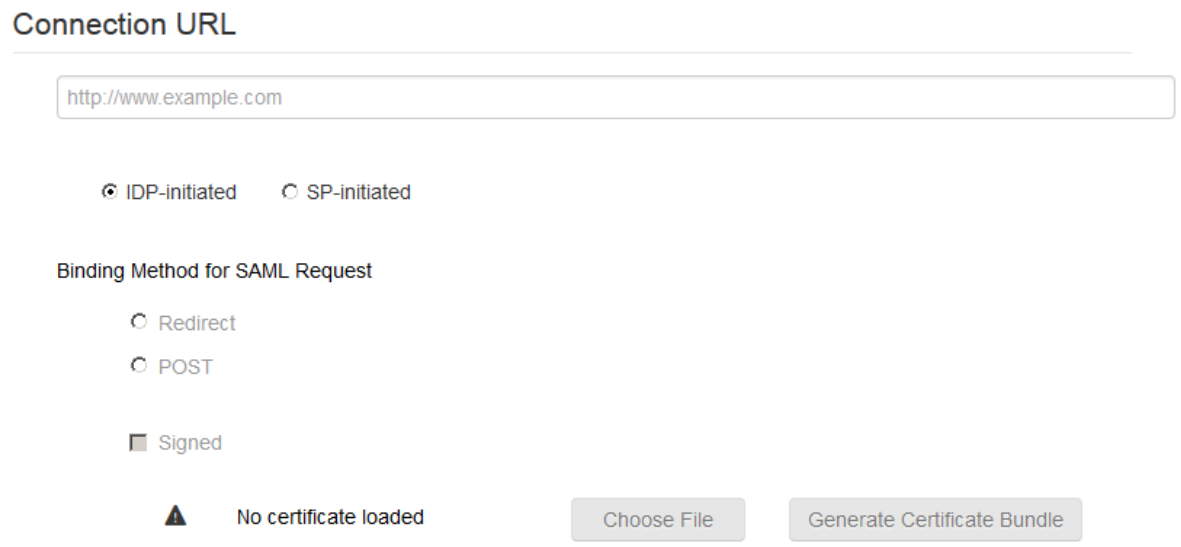
3. On the Basic Information page, specify the application name and click **Next Step**.

> **Note: The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.**

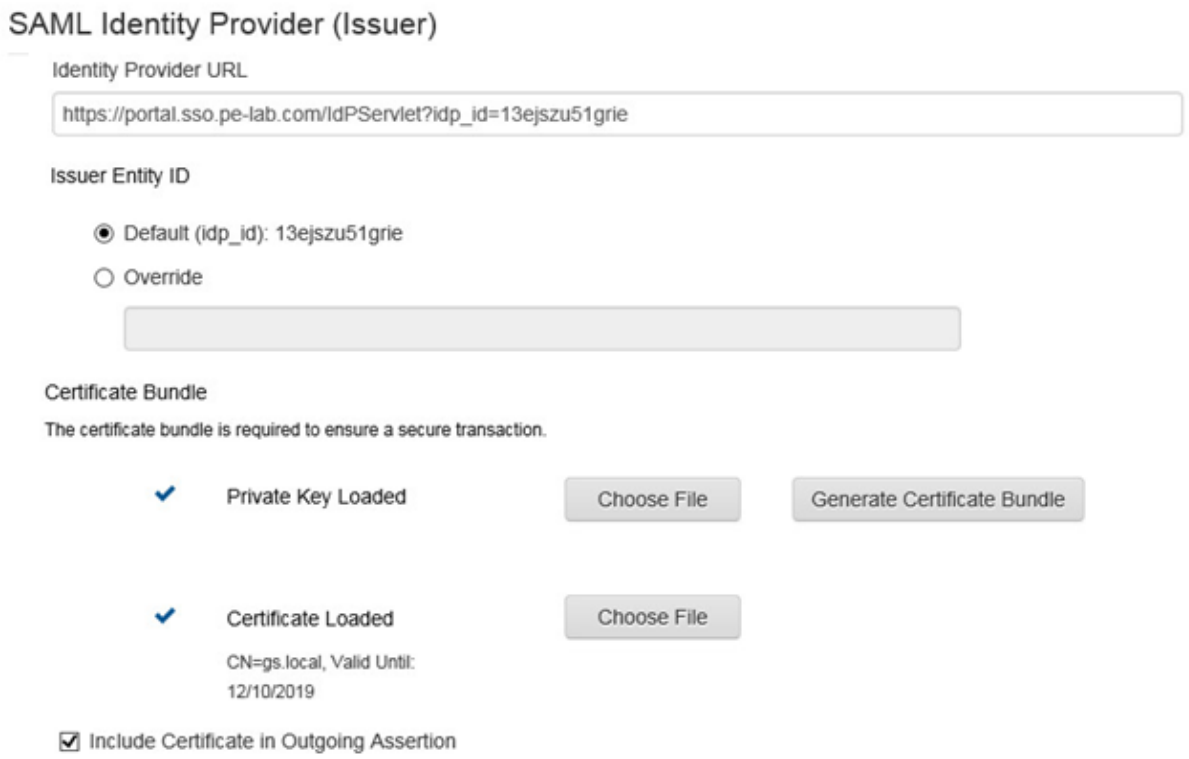
4. Click on **Import Metadata** and select the file you received from Flowdock. See page 7.



5. Click **Save** to accept the settings from the metadata file.
6. On the Connection Profile page, choose **IDP –initiated** and leave the URL blank.

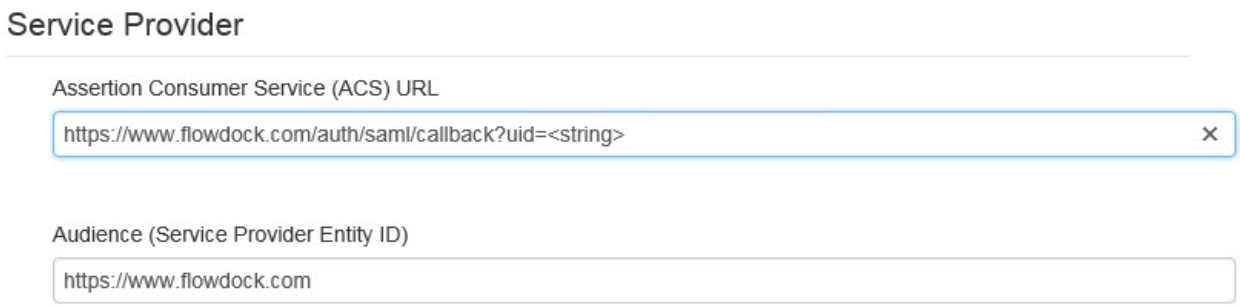


7. Scroll down to the **SAML Identity Provider (Issuer)** section.



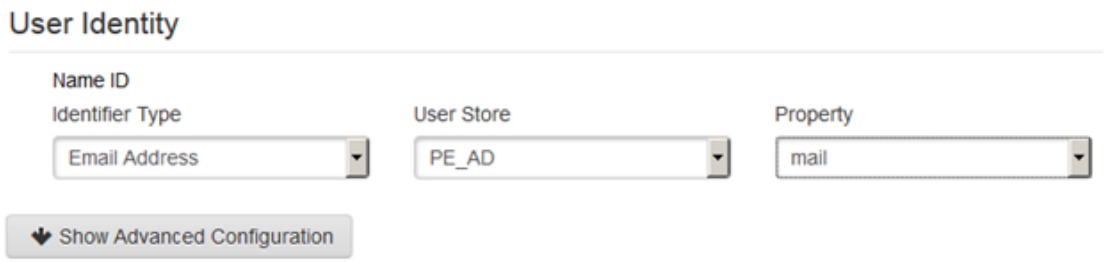
   a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the CA Flowdock.
   b. Select **Choose File** and upload the RSA SecurID Access private key.
   c. Select **Choose File** and upload the RSA SecurID Access public certificate.
   d. Check **Include Certificate in Outgoing Assertion**.

8. Scroll down to the **Service Provider** section.

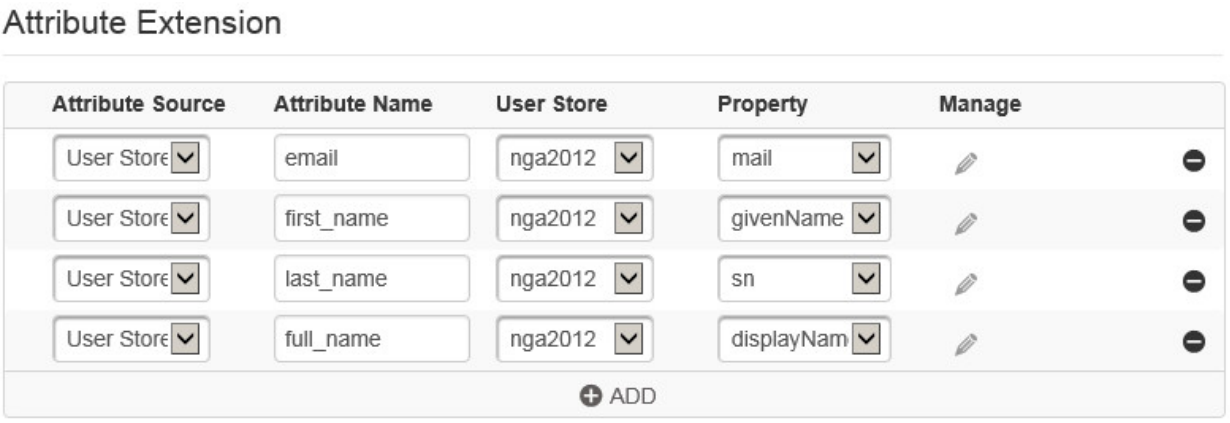


   a. In the **Assertion Consumer Service (ACS) URL** field, replace **<string>** with your uid value. Example: https://www.flowdock.com/auth/saml/callback?uid=haEdZ6PRanqEvYdi-t5aSg
   b. In the **Audience (Service Provider Entity ID)** field, enter https://www.flowdock.com.

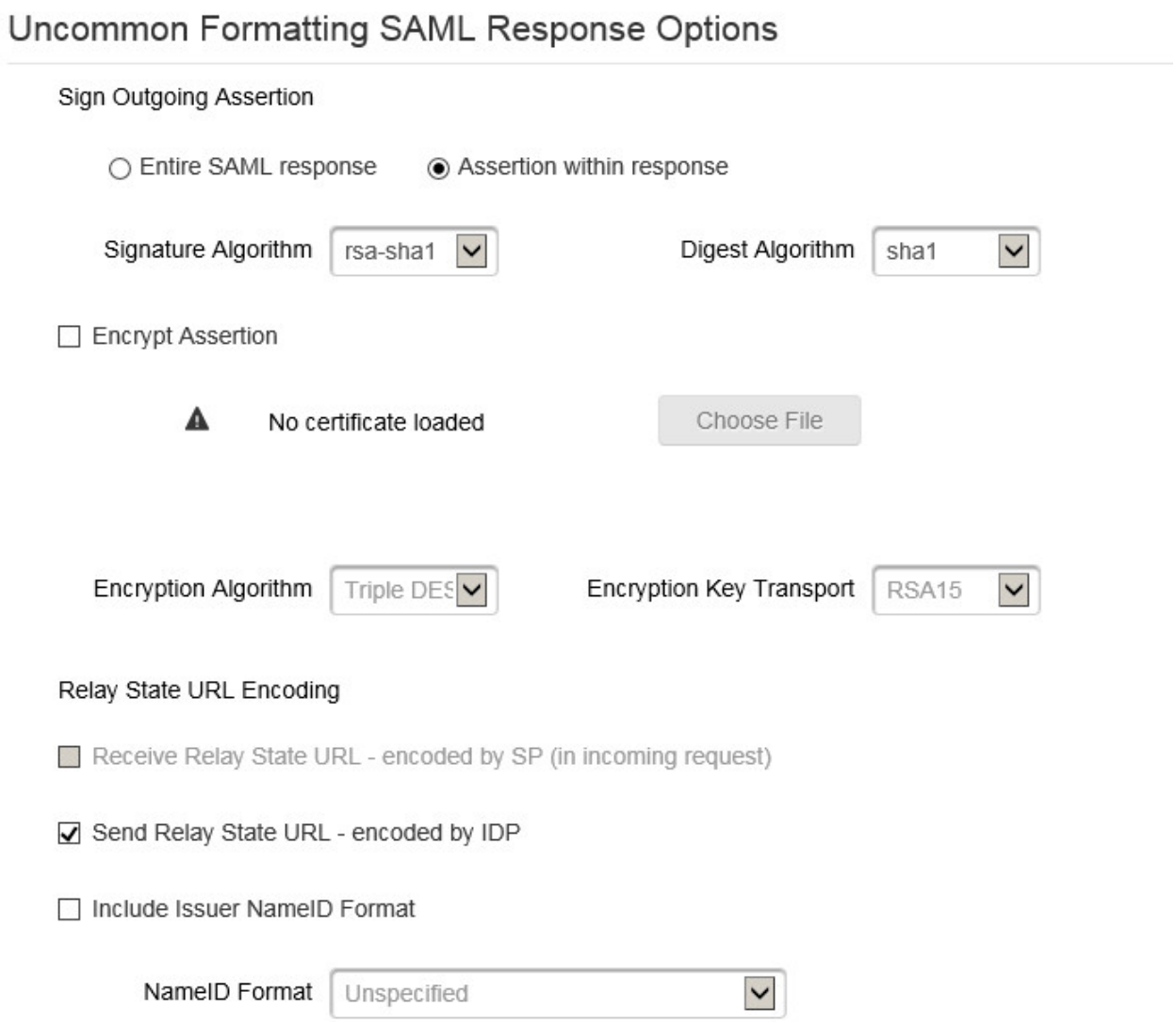
9. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email** and **Property** to **mail**.



10. Click **Show Advanced Configuration** and scroll down to **Attribute Extension**.
11. Add Attributes and their Property fields for **email**, **first_name**, **last_name**, and **full_name**.

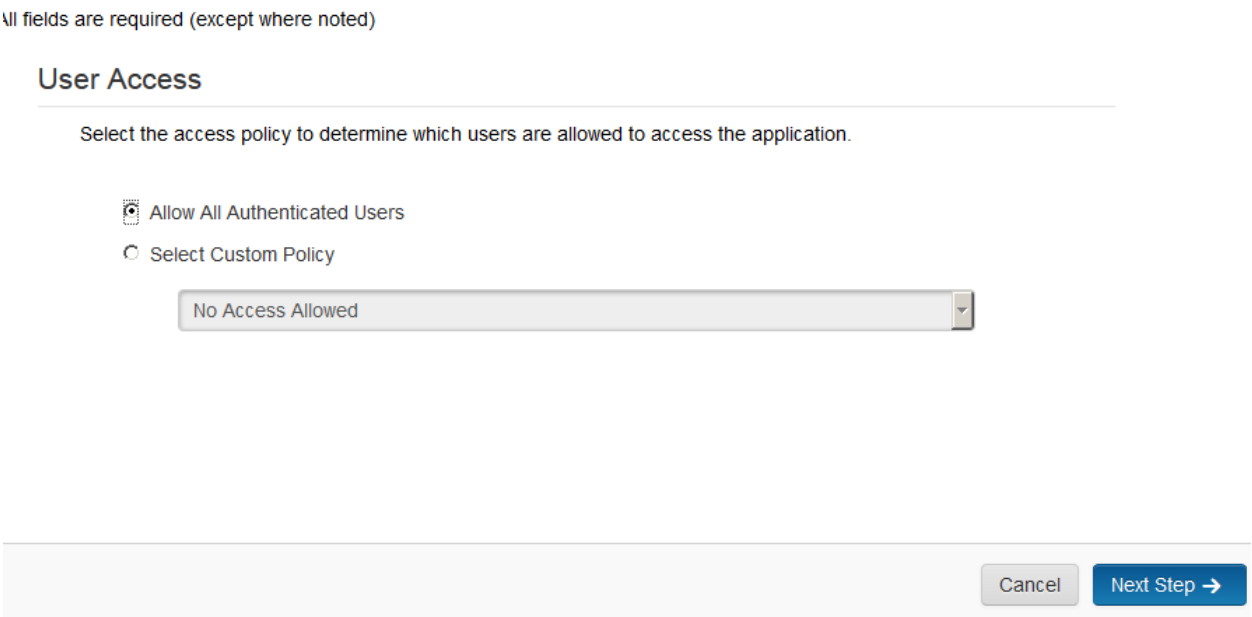


12. Scroll down to **Uncommon Formatting SAML Response Options**.
13. Under Sign Outgoing Assertion, select **Assertion within response**.

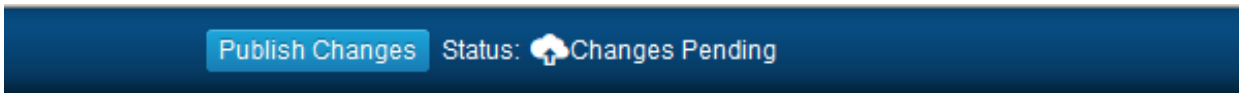


14. Click **Next Step**.

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



16. Click **Next Step**.
17. On the **Portal Display** page, select **Display in Portal**.
18. Click **Save and Finish**.
19. Click **Publish Changes**. Your application is now enabled for SSO.



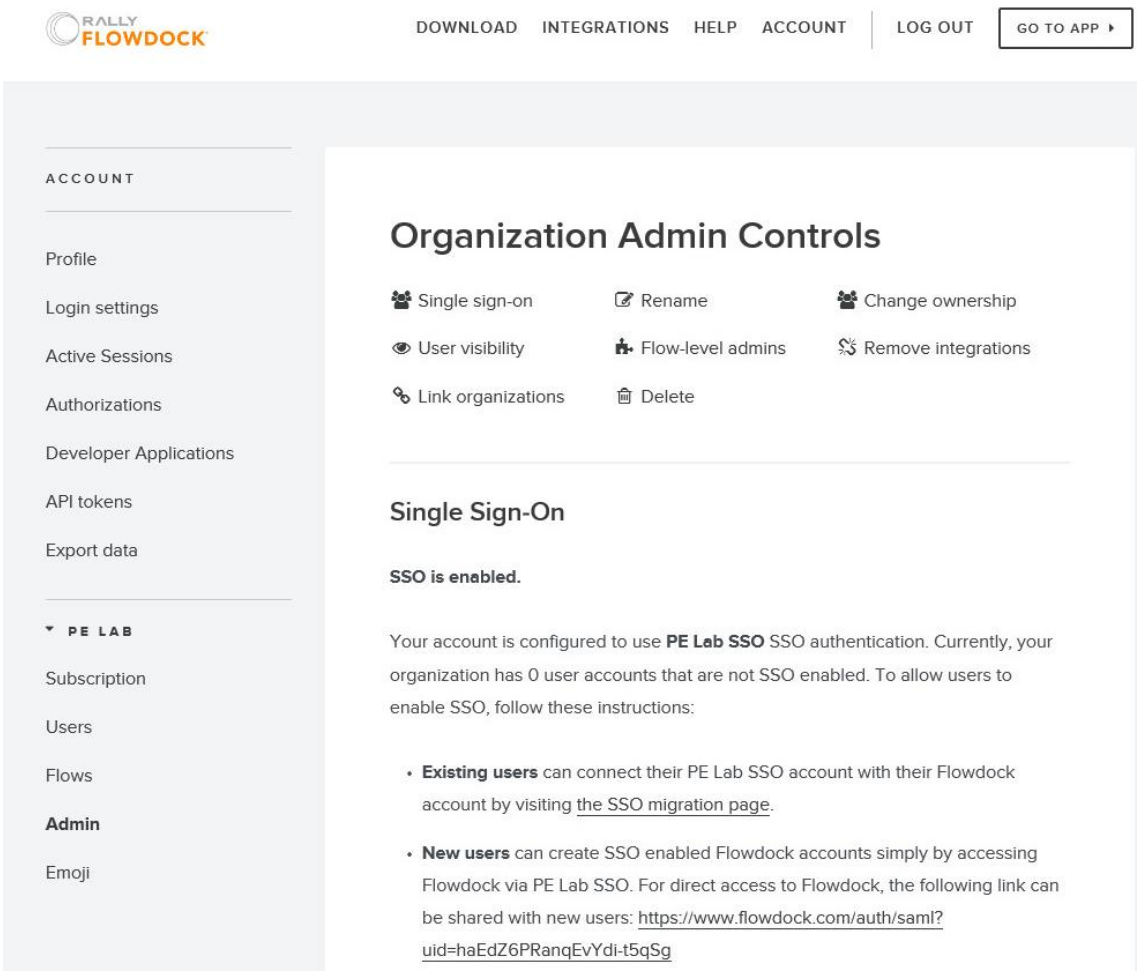
Next Steps

[Configure CA Flowdock to Use RSA SecurID Access as an Identity Provider]

Configure CA Flowdock to Use RSA SecurID Access as an Identity Provider

Procedure

1. Contact Flowdock support and request single sign-on be enabled.
2. They will ask you for the following information, which can be found from step 5 on page 2.
    - SSO Endpoint, also known as the Identity Provider URL
    - RSA Access Entity ID
    - RSA Access public certificate
3. Once SSO is enabled on your organization, support will provide you with the following:
    - Issuer URL, which is the Audience URL
    - Service Provider Single Sign On URL, also known as ACS URL
    - link to metadata URL, https://www.flowdock.com/auth/saml/metadata?uid=<string>
4. Browse to the metadata URL and save it to a file, metadata.xml. Use this for step 4 on page 2.
5. Login to CA Flowdock with an admin account.
6. Select the pulldown arrow next to the username.
7. Navigate to **Account > Admin**.
8. Select **Single sign-on**.



9. Use the **New user URL** provided on this page to add new SSO users with the same email domain.

GLS