

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.

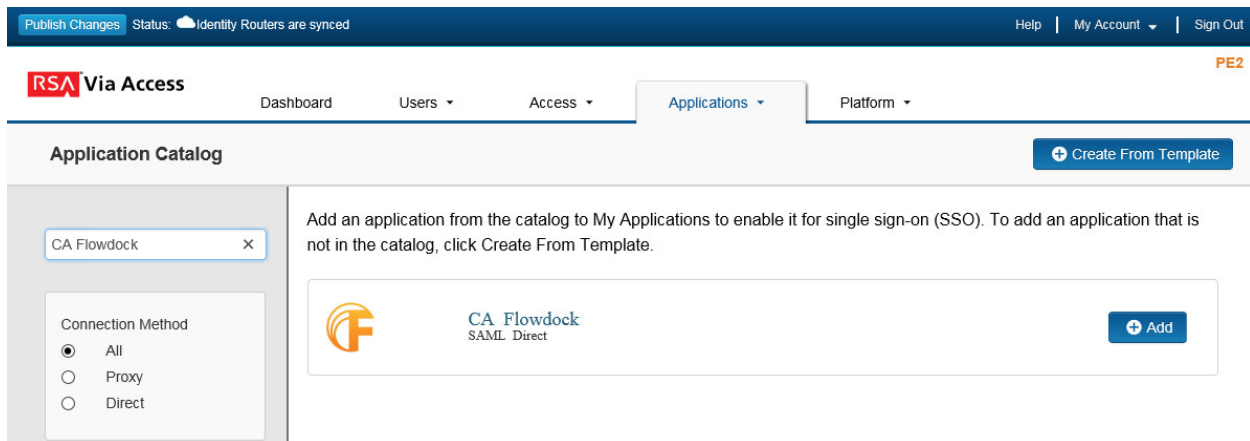
Procedure

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.



The screenshot shows the RSA SecurID Access Administration Console interface. At the top, there is a navigation bar with "Publish Changes", "Status: Identity Routers are synced", "Help", "My Account", and "Sign Out". Below this is the "RSA Via Access" header with navigation tabs for "Dashboard", "Users", "Access", "Applications", and "Platform". The "Applications" tab is selected, leading to the "Application Catalog" page. On the right side of the page, there is a "Create From Template" button. The main content area displays a search bar with "CA Flowdock" entered. Below the search bar, there are radio buttons for "Connection Method": "All" (selected), "Proxy", and "Direct". The search results show a card for "CA Flowdock SAML Direct" with an "Add" button.

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.

Connection Profile

Configure the relationship between the identity router, acting as the SAML identity provider (IdP), and the application, acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP options. You can edit these values if necessary.

No metadata loaded

Import Metadata

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.

Connection URL

http://www.example.com


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

Choose File

Generate Certificate Bundle

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

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): 13ejszu51grie

Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

Private Key Loaded

Certificate Loaded

CN=gs.local, Valid Until:
12/10/2019

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

- 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**.

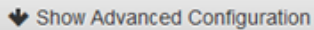
User Identity

Name ID

Identifier Type










User Store

Property



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**.

Attribute Extension

Attribute Source	Attribute Name	User Store	Property	Manage
<input type="text" value="User Store"/>	<input type="text" value="email"/>	<input type="text" value="nga2012"/>	<input type="text" value="mail"/>	 
<input type="text" value="User Store"/>	<input type="text" value="first_name"/>	<input type="text" value="nga2012"/>	<input type="text" value="givenName"/>	 
<input type="text" value="User Store"/>	<input type="text" value="last_name"/>	<input type="text" value="nga2012"/>	<input type="text" value="sn"/>	 
<input type="text" value="User Store"/>	<input type="text" value="full_name"/>	<input type="text" value="nga2012"/>	<input type="text" value="displayNam"/>	 
 ADD				

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

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response Assertion within response

Signature Algorithm rsa-sha1 ▼

Digest Algorithm sha1 ▼

Encrypt Assertion

 No certificate loaded

Choose File

Encryption Algorithm Triple DES ▼

Encryption Key Transport RSA15 ▼

Relay State URL Encoding

Receive Relay State URL - encoded by SP (in incoming request)

Send Relay State URL - encoded by IDP

Include Issuer NameID Format

NameID Format Unspecified ▼

14. Click **Next Step**.

15. 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 →


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.

Publish Changes

Status:  Changes Pending

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**.

The screenshot shows the Flowdock Account Admin interface. At the top, there is a navigation bar with the Flowdock logo and links for DOWNLOAD, INTEGRATIONS, HELP, ACCOUNT, LOG OUT, and a GO TO APP button. The main content area is divided into two sections. The left section is a sidebar menu with the following items: ACCOUNT, Profile, Login settings, Active Sessions, Authorizations, Developer Applications, API tokens, Export data, PE LAB (expanded), Subscription, Users, Flows, Admin, and Emoji. The right section is titled "Organization Admin Controls" and contains several settings: Single sign-on, Rename, Change ownership, User visibility, Flow-level admins, Remove integrations, Link organizations, and Delete. Below this is a section titled "Single Sign-On" with the heading "SSO is enabled." and a paragraph stating: "Your account is configured to use PE Lab SSO authentication. Currently, your organization has 0 user accounts that are not SSO enabled. To allow users to enable SSO, follow these instructions:" followed by two bullet points: "Existing users can connect their PE Lab SSO account with their Flowdock account by visiting the SSO migration page." and "New users can create SSO enabled Flowdock accounts simply by accessing Flowdock via PE Lab SSO. For direct access to Flowdock, the following link can be shared with new users: https://www.flowdock.com/auth/saml?uid=haEdZ6PRanqEvYdi-t5qSg".

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