RSA SecurID Access SAML Configuration for Zendesk BIME

Last Modified: April 14, 2016

BIME by Zendesk is a business analytic platform for sharing queries and dashboards and advanced visualization.

Before You Begin

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

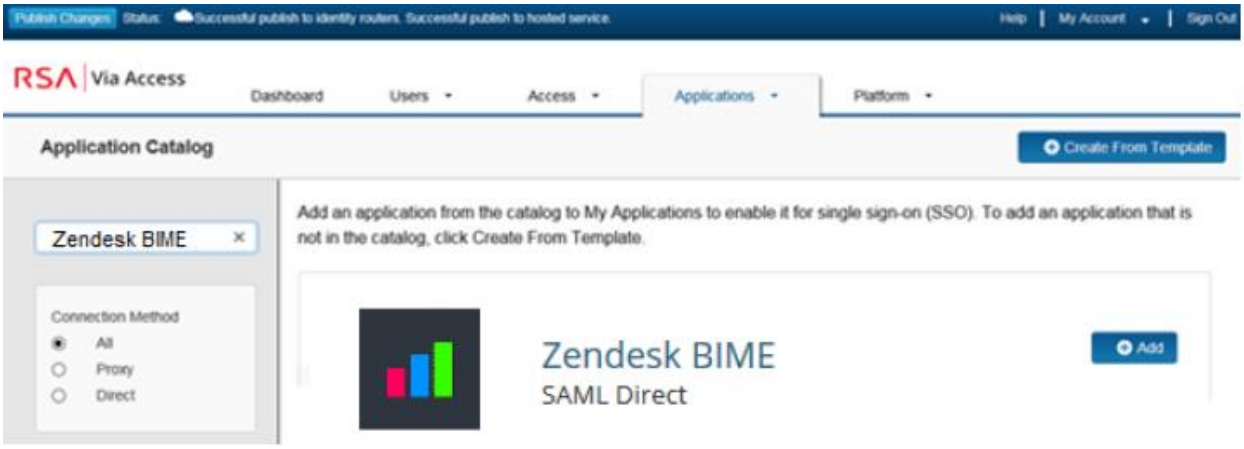
Procedure

1. Add the Application in RSA SecurID Access
2. Configure BIME 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 application that you wish to add. To add an application that is not in the list, click **+Create From Template**.

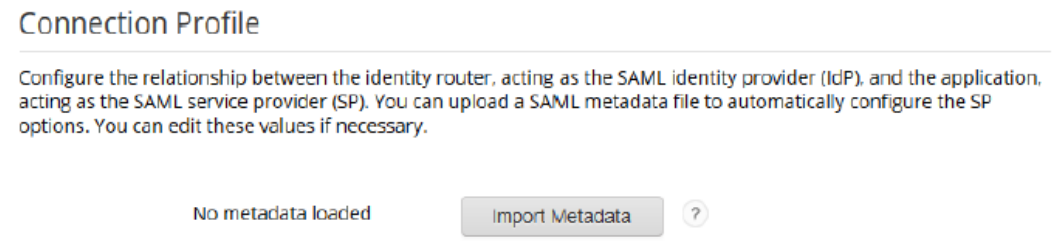


Copyright © 2016 EMC Corporation. All Rights Reserved.

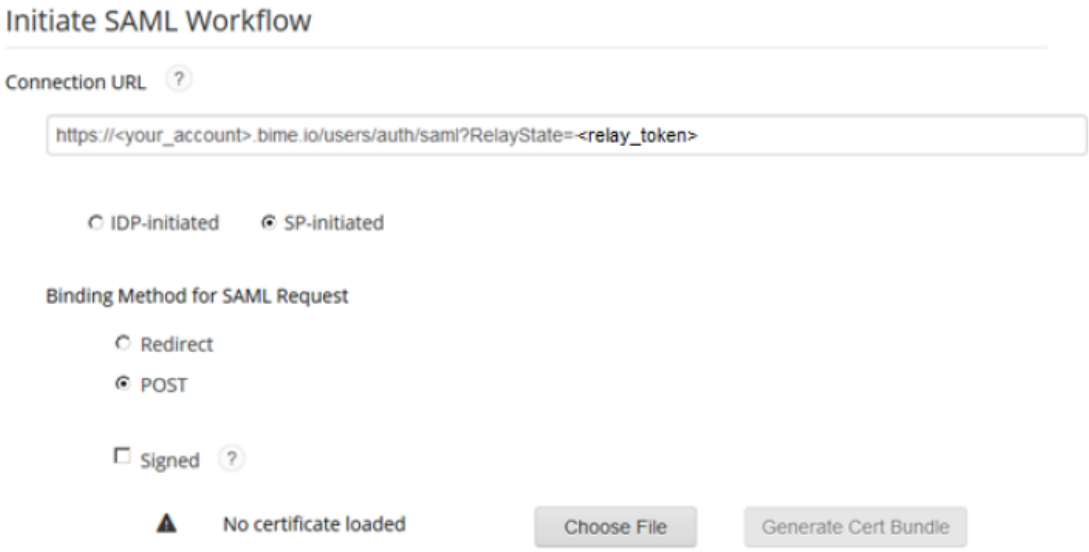
3. On the Basic Information page, specify the application name and click **Next Step**.

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

4. On the Connection Profile page, select Import Metadata. Select the file you downloaded from BIME on page 6 step 5.

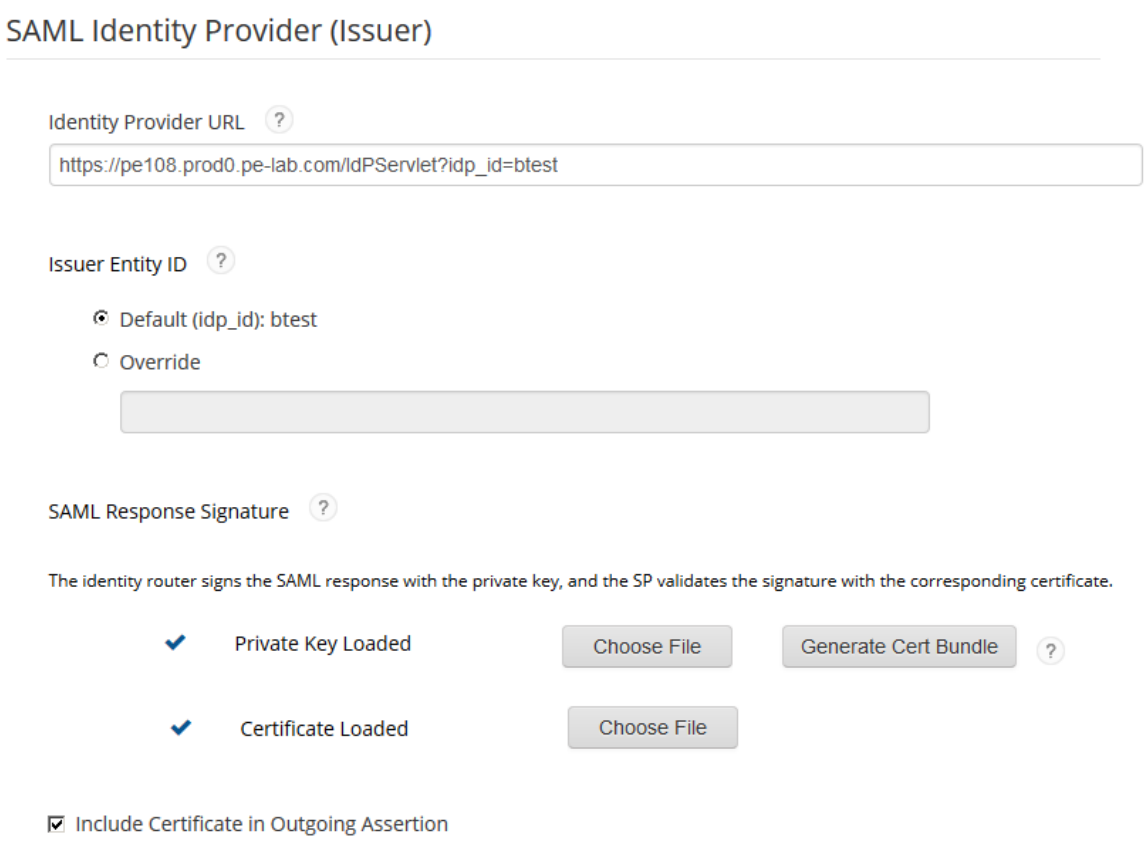


5. Click **Save** to import the metadata values.
6. In the Initiate SAML Workflow section, select **SP-initiated.**
7. Modify the **Connection URL** with your account name and relay token. Refer to page 7, How to determine the Relay Token.



Copyright © 2016 EMC Corporation. All Rights Reserved.

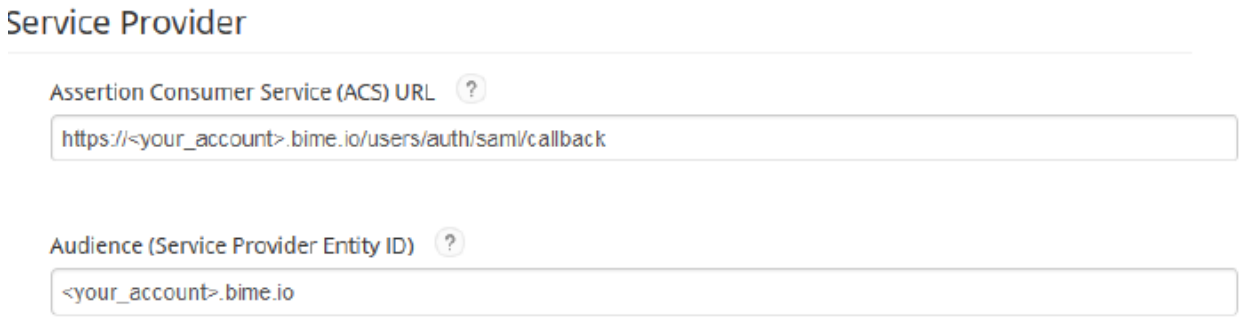
8. Scroll down to the **SAML Identity Provider** section.



a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the BIME.
b. Select **Choose File** and upload the RSA Via Access private key.
c. Select **Choose Fil**e and upload the RSA Via Access public certificate.
d. Select the checkbox for **Include Certificate in Outgoing Assertion**.

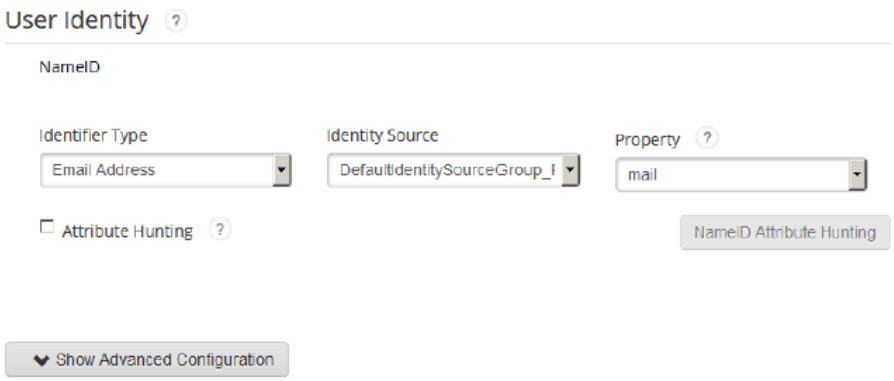
Copyright © 2016 EMC Corporation. All Rights Reserved.

9. Scroll down to the Service Provider section.



   a. Modify the Assertion Consumer Service (ACS) URL with your account name.
   b. Modify the Audience (Service Provider Entity ID) with your account name.

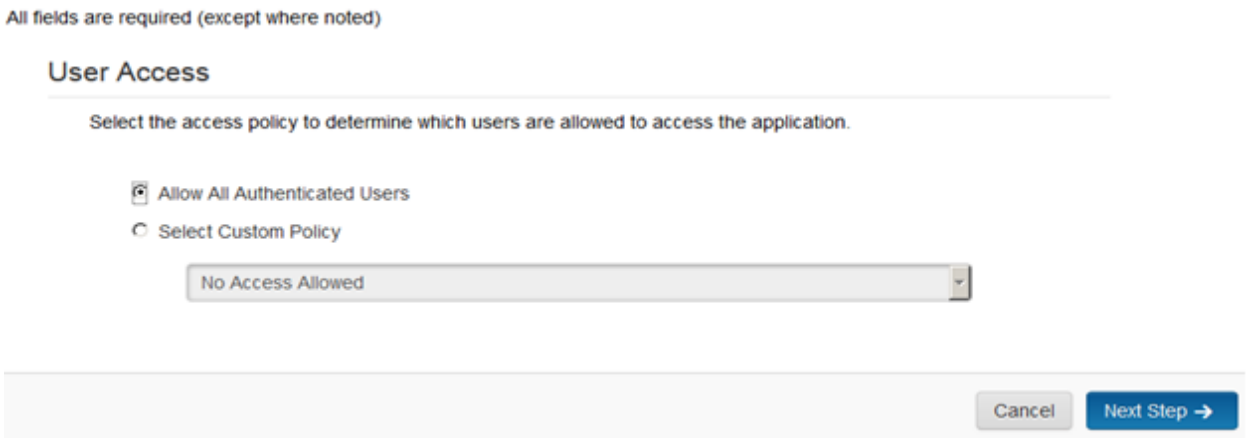
10. Scroll down to the User Identity section. Set the Identifier Type to Email Address and Property to mail.



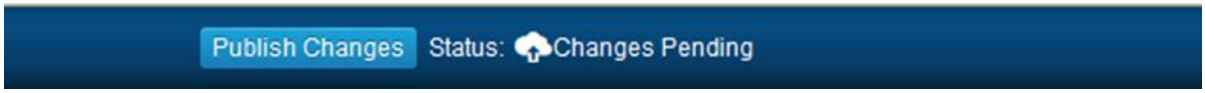
11. Click **Next Step**.

Copyright © 2016 EMC Corporation. All Rights Reserved.

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



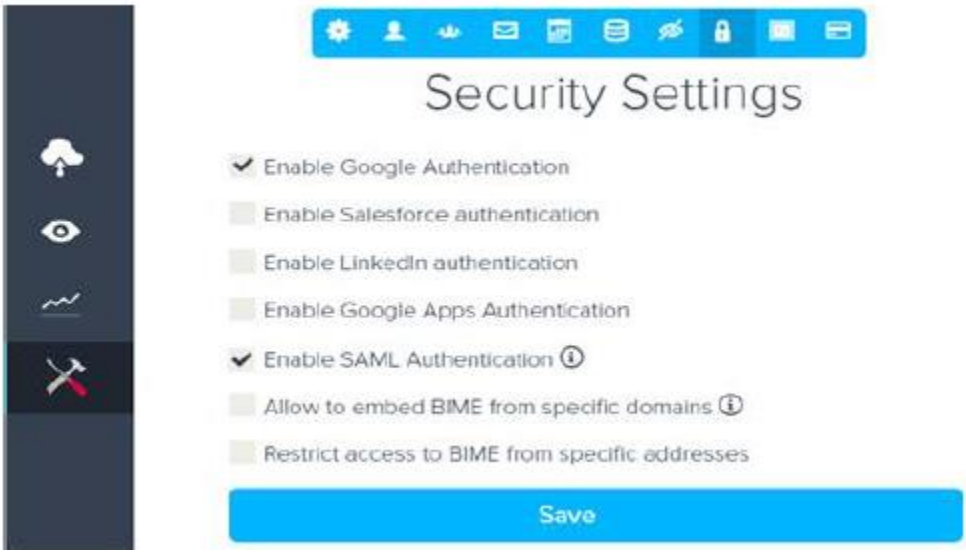
13. Click **Next Step**.
14. On the **Portal Display** page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**. Your application is now enabled for SSO.



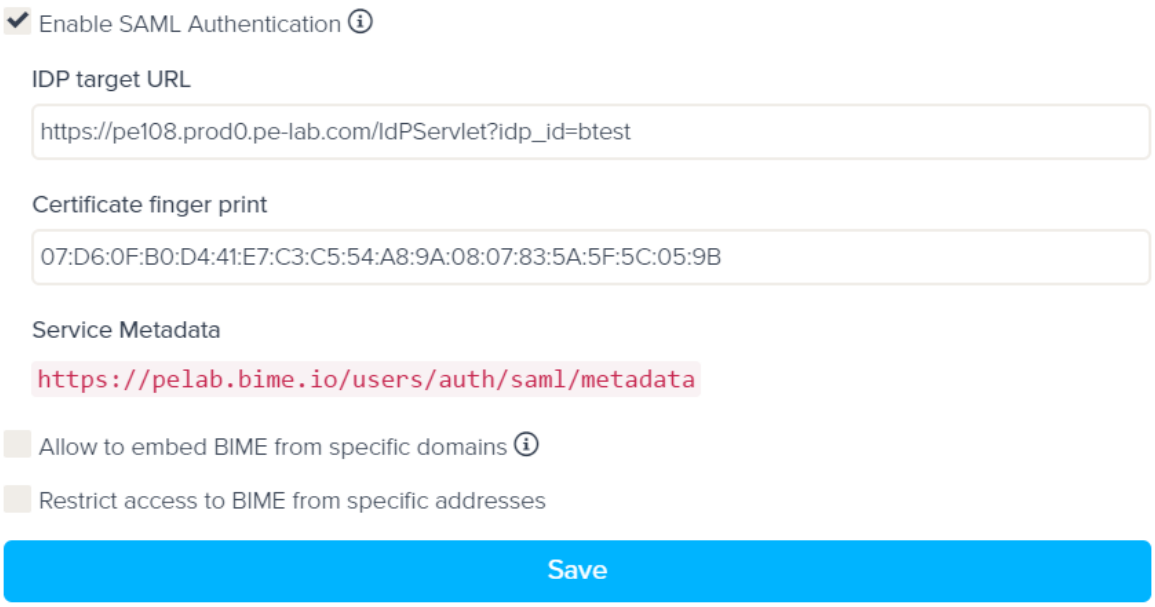
Copyright © 2016 EMC Corporation. All Rights Reserved.

Configure BIME to Use RSA SecurID Access as an Identity Provider

1. Login into the BIME administration console; https://<your_account>.bime.io
2. Select the Admin tool icon from the left menu.
3. Select the Security lock icon from the top menu.
4. On the Security page, select **Enable SAML Authentication**.



5. In the **IDP target URL** field, enter the RSA Via Access Identity Provider URL from page 3 step a.



6. Enter the **Certificate finger print**. Refer to the next section, How to Create a SHA1 fingerprint.
7. Click **Save**.

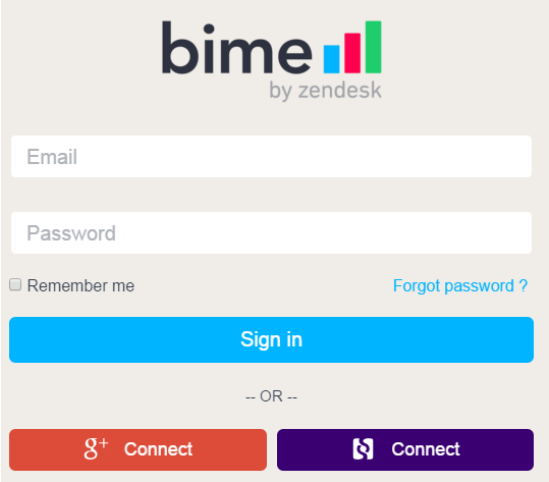
Copyright © 2016 EMC Corporation. All Rights Reserved.

How to Create a SHA1 fingerprint

1. To generate a SHA1 fingerprint of your SAML certificate you must use **openssl**.
2. Open your terminal or command prompt and navigate to the file location in which your RSA Via Access cert.pem file resides.
3. Enter the following command in a terminal or command prompt to obtain your SHA1 fingerprint: **openssl x509 -sha1 -noout -fingerprint -in cert.pem**.
4. After entering the above command, your terminal or command window will display, SHA1 Fingerprint= <your_SHA1_Fingerprint_string>.

How to determine the Relay Token

1. Once you have enable SAML in BIME you will see a purple **Connect** button on the Login page.



2. Right click the **Connect** button and copy the link. It should look similar to this, https://pelab.bime.io/users/auth/saml?RelayState=ghEoMujD5KFoAWTLr%2FByLw%3D%3D.
3. Copy the URL into a URL decoder, such as http://meyerweb.com/eric/tools/dencoder/.
4. Select **decode**. The Connection URL should look similar to this, https://pelab.bime.io/users/auth/saml?RelayState=ghEoMujD5KFoAWTLr/ByLw==.

GLS

Copyright © 2016 EMC Corporation. All Rights Reserved.