RSA SecurID Access SAML Configuration for getAbstract

Last Modified: August 22, 2016

getAbstract is a Swiss and US-based corporation that creates abstracts of business books. This knowledge is delivered in summaries of the most relevant books. The summaries are available in multiple languages. To create its content business journalists are employed. Many of the world's largest companies offer their employees access to the getAbstract Library. The customer base spans the globe though getAbstract is not affiliated with any publishing house.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and getAbstract.
- Obtain the getAbstract Metadata from service provider.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	*https://www.getabstract.com/portal/emc*
ACS URL	*https://www.getabstract.com/ACS.do*
Service Provider Issuer ID	*getabstract*

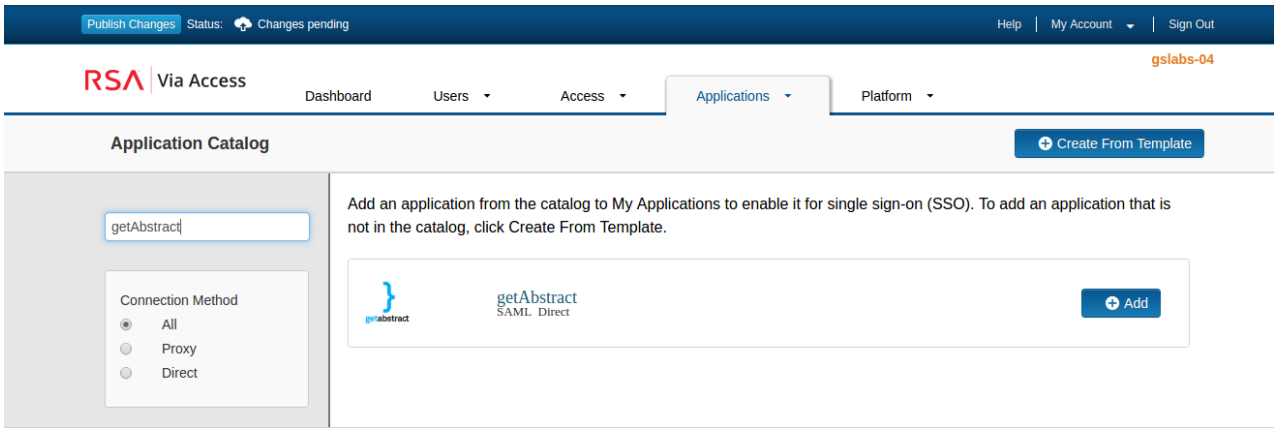
Procedure

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

Add the Application in RSA SecurID Access

Procedure

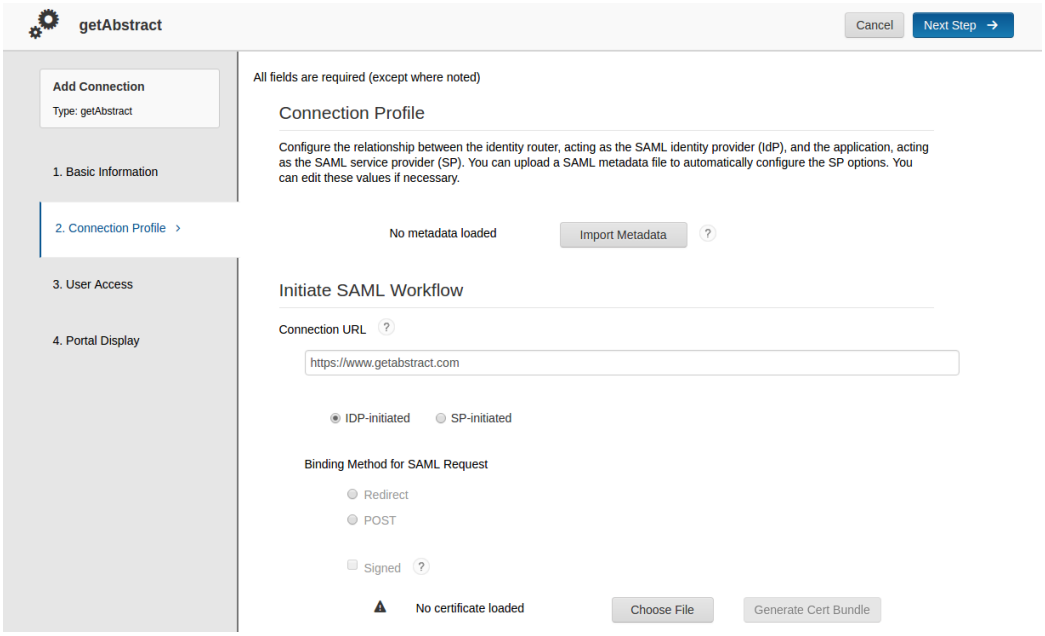
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for getAbstract.



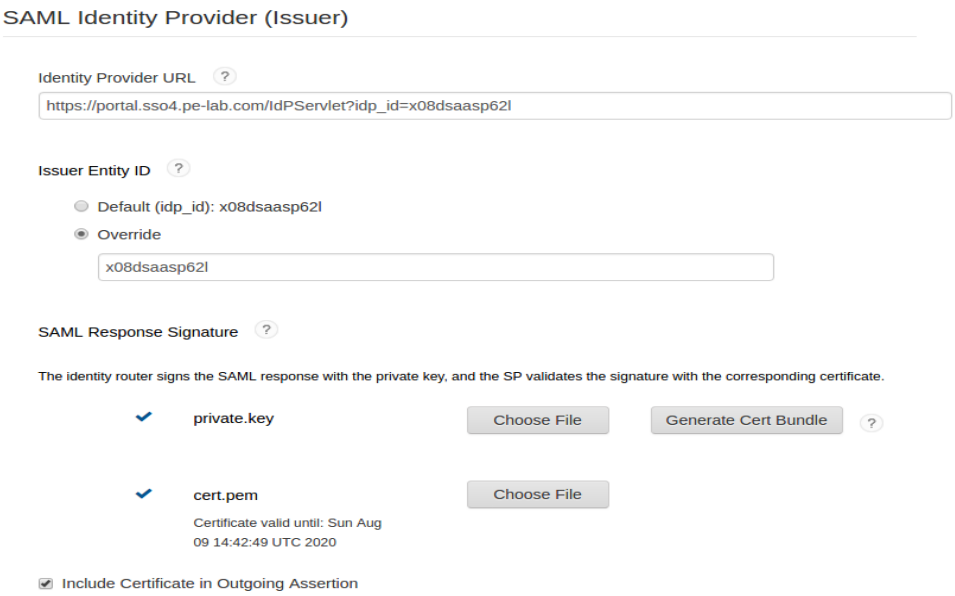
3. On the Basic Information page, specify the application name and click **Next Step**.

4. Navigate to **Initiate SAML Workflow** section**.**
   a) In the **Connection URL** field, type the getAbstract landing page URL. Portal users will be redirected to this page when they initiate SSO flow.
   For ex. https://www.getabstract.com/
   b) Choose **IDP –initiated**.

Note: The following IdP-initiated configuration works for SP-initiated getAbstract connections as well.



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

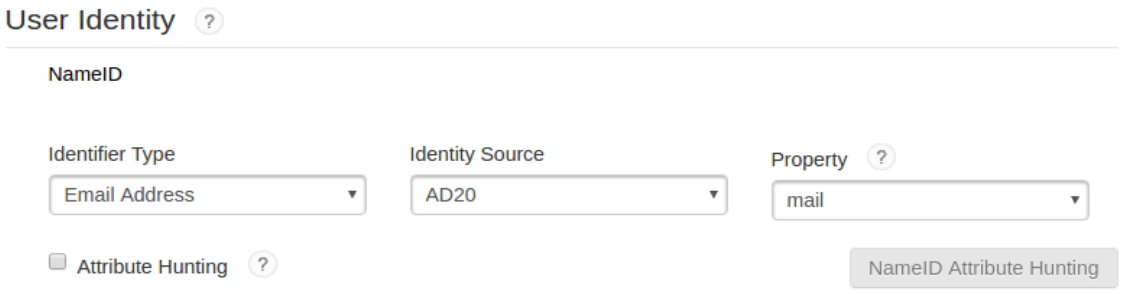


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Override** and enter a value for the **Issuer Entity ID** similar as mentioned in metadata details provided at service provider side.
c. Select **Choose File** and upload the private/public key. Select **Choose File** to locate and import a private key to sign the SAML assertion. The private key must correspond to the public signing certificate loaded in the SP application. If a private/public key pair is not readily available, you can click **Generate Certificate Bundle**.
d. Select the checkbox for **Include Certificate in Outgoing Assertion**.

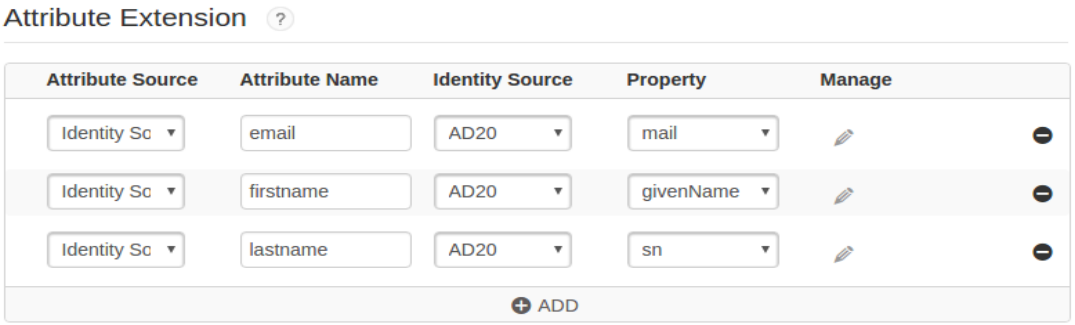
6. Scroll down to the **Service Provider** section.

a. In the **Assertion Consumer Service (ACS) URL** field, enter value that is received in SP Metadata details.
b. In the **Audience (Service Provider Entity ID)** field, enter value that is received in SP Metadata details.

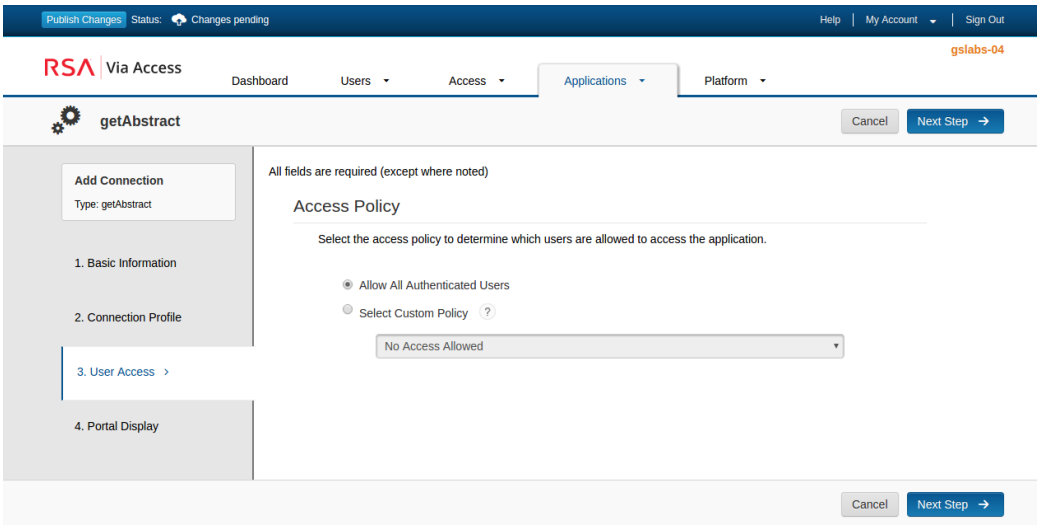
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



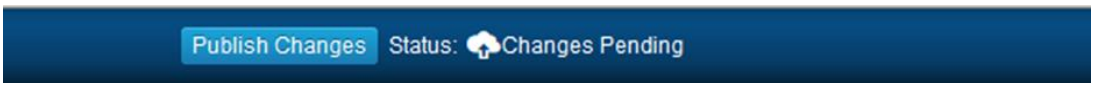
8. Moving next, select **Show Advanced Configuration.**
9. In the **Attribute Extension** section add **email**, **firstname** and **lastname**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.



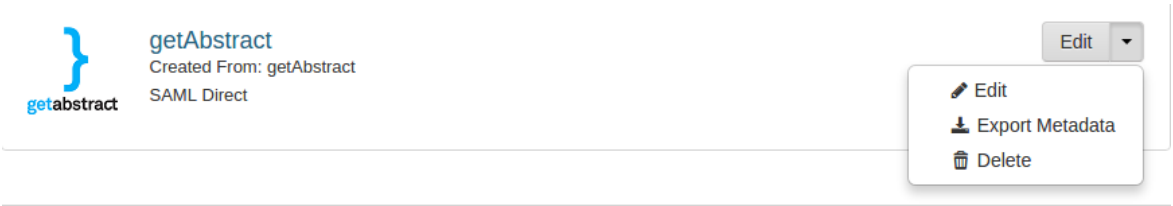
10. Click **Next Step**
11. On the **User Access page,** select the desired user policy from the drop down list.



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



16. Navigate to **Applications > My Applications**.
17. Locate getAbstract in the list and from the **Edit** pull down select **Export Metadata**.



Configure getAbstract to Use RSA SecurID Access as an Identity Provider

1. Contact getAbstract support at http://SSO.ITSupport@getAbstract.com and request that single sign-on be enabled.
2. Send getAbstract support the RSA metadata file downloaded from step 17 page 4.