RSA SecurID Access SAML Configuration for RightScale

Last Modified: September 7, 2016

RightScale is a SaaS-based cloud computing management solution for managing cloud infrastructure across multiple IaaS providers. It enables organizations to easily deploy and manage applications in the cloud.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and RightScale.
- Obtain the RightScale SP details 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://login.rightscale.com/login/session/new*
ACS URL	*https://login.rightscale.com/login/saml2/consume*
Service Provider Issuer ID	*https://login.rightscale.com/login/saml2/metadata*

Procedure

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

Add the Application in RSA SecurID Access

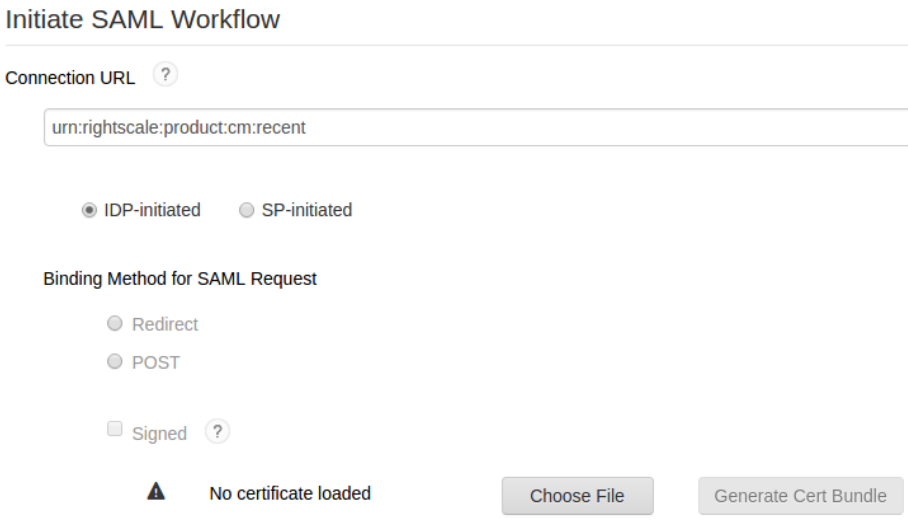
Procedure

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

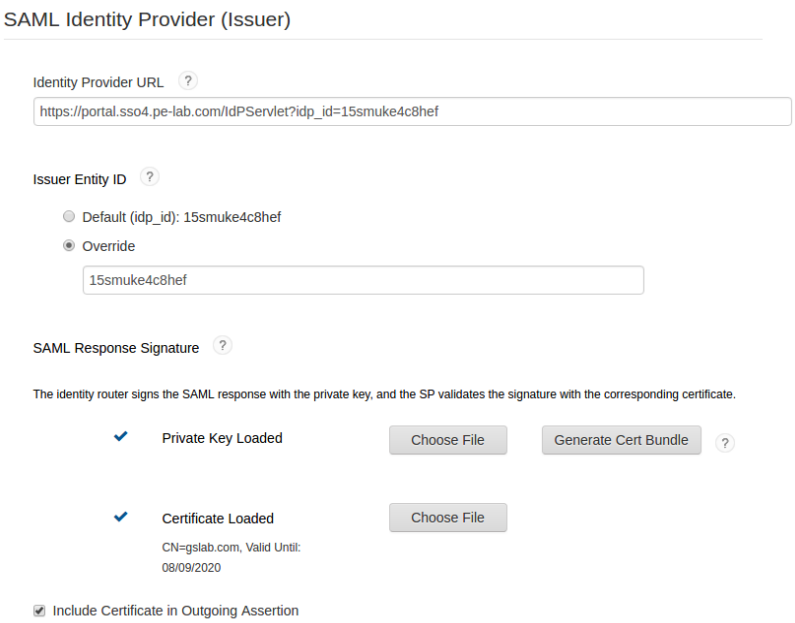
3. On the Basic Information page, specify the application name and click **Next Step**.

4. Navigate to **Initiate SAML Workflow** section**.**
   a) In the **Connection URL** field, type the RightScale landing page URL. Portal users will be redirected to this page when they initiate SSO flow.
   For ex. **urn:rightscale:product:cm:recent**
   b) Choose **IDP –initiated**.

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



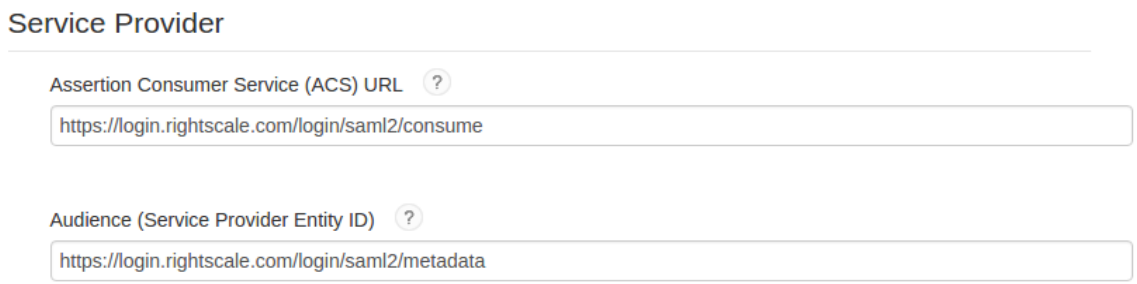
5. Scroll down to **SAML Identity Provider (Issuer)** section.



   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.

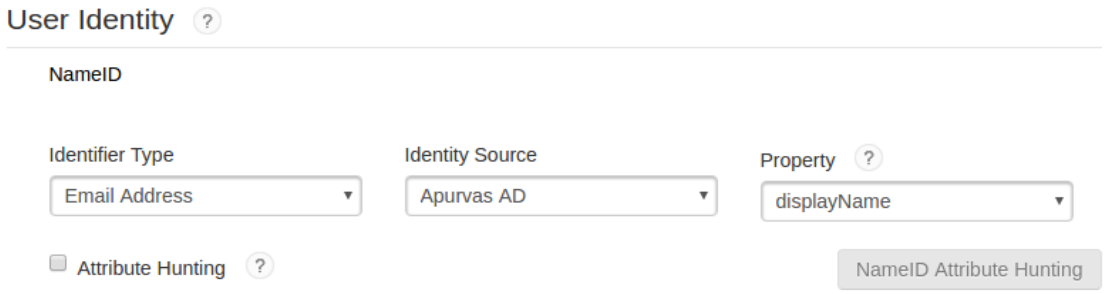
b. Select **Choose File** and upload the private/public key. Select **Choose File** to locate and import a private key to sign the SAML assertion. The private key must correspond to the public signing certificate loaded in the SP application. If a private/public key pair is not readily available, you can click **Generate Certificate Bundle**.
c. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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



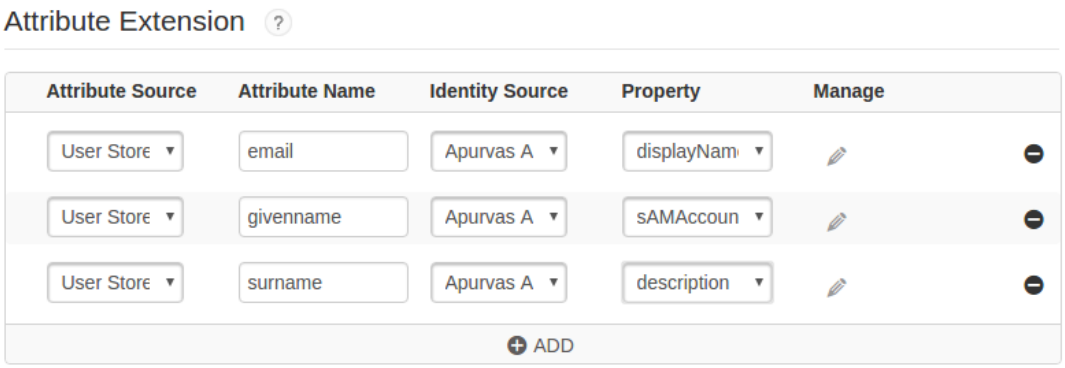
a. In the **Assertion Consumer Service (ACS) URL** field, enter value that is received in SP details.
b. In the **Audience (Service Provider Entity ID)** field, enter value that is received in SP details.

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.

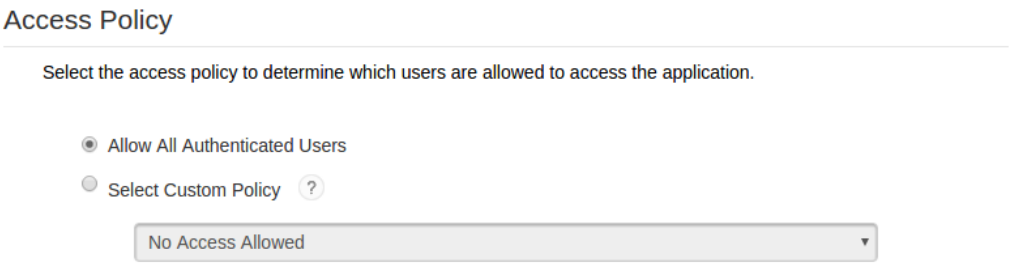


8. Next, select **Show Advanced Configuration.**

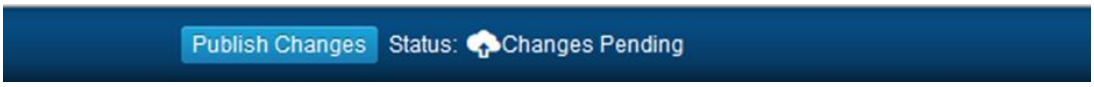
9. In the **Attribute Extension** section, add **email**, **givenname** and **surname**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.



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

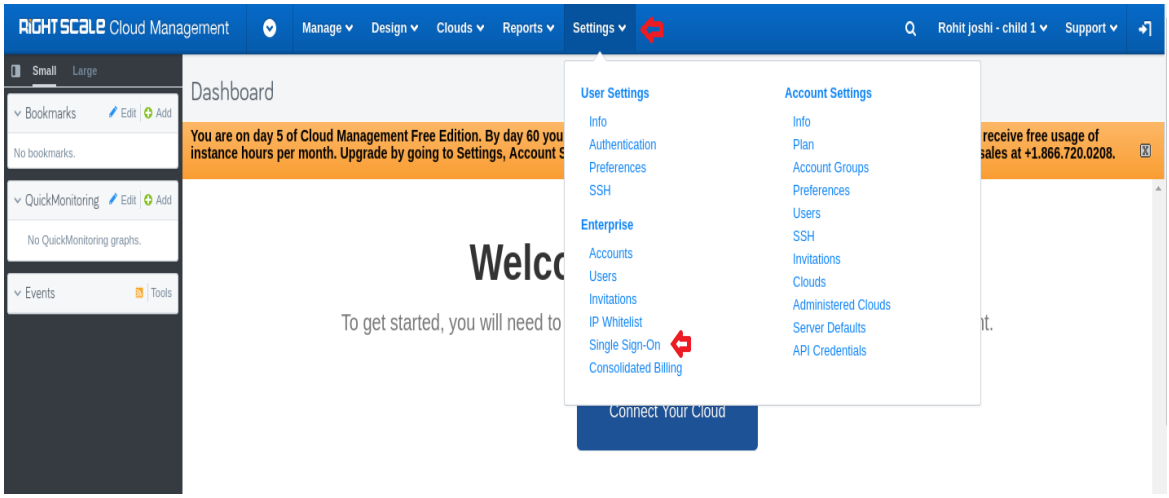


12. Click **Next Step**.
13. On the **Portal Display** page, select **Display in Portal**.
14. Click **Save and Finish**.
15. Click **Publish Changes**. Your application is now enabled for SSO.

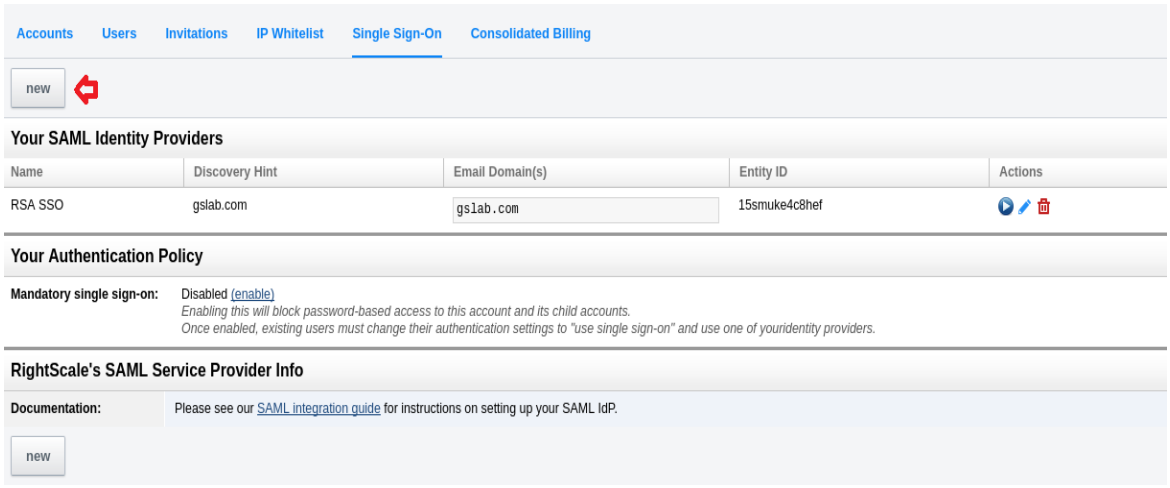


Configure RightScale to Use RSA SecurID Access as an Identity Provider

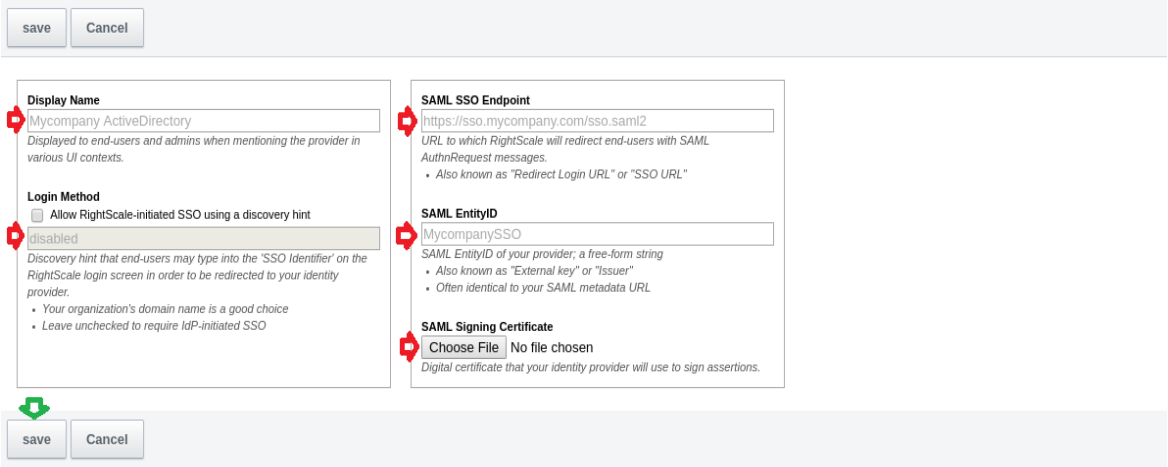
1. Login to your RightScale account. (https://login.rightscale.com/login/session/new)
2. Following page will be displayed. Select **Single Sign-On** option available under **Settings** tab.



3. Following UI will be displayed. Select **new** option to configure IdP SAML settings.



4. Following pop-up will appear.



Provide below details here –

a) **Display Name :** Provide your organization name here as per convenience.
For ex. RSASSO.
b) **Login Method :** Select **Checkbox** and enter value of 'Discovery Hint' in **Textfield** that will be used for SP-initiated SSO scenario. Organization name will be the best choice for this. If left blank and un-checked, SP-initiated SSO won't be available to use.
c) **SAML SSO Endpoint :** Provide IdP endpoint URL value. This value can be obtained from portal. It is of following format –
https://<Your_Portal_URL>/IdPServlet?idp_id=<Unique_IdP_ID>
d) **SAML EntityID :** Provide unique IdP entity id from portal.
e) **SAML Signing Certificate :** Provide IdP public certificate that is obtained from portal.

Once confirmed all details, click on **Save** button.

5. That's it! Your RightScale account is now configured for SAML SSO authentication.

Things to Note :

1. To use SAML authentication, you must add 'Domain authority' of your Email domain at RightScale. Once valid domain is configured, only then you can perform SAML SSO.
For ex. If your corporate email id is abc@example.com, then confirm RightScale that you own example.com domain.

How to do this?

Write an email to support@rightscale.com saying that you owns the domain and ask them to authorize the same for the sake of SAML authentication. On completion, the RightScale support team will make an entry of domain for your account and make it available for you to use.

RJ