RSA SecurID Access SAML Configuration for Litmos

Last Modified: October 1, 2015

Litmos is a cloud platform for e-learning, also known as learning management system (LMS).

Before You Begin

- Acquire Litmos account.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the SecurID Access manual.

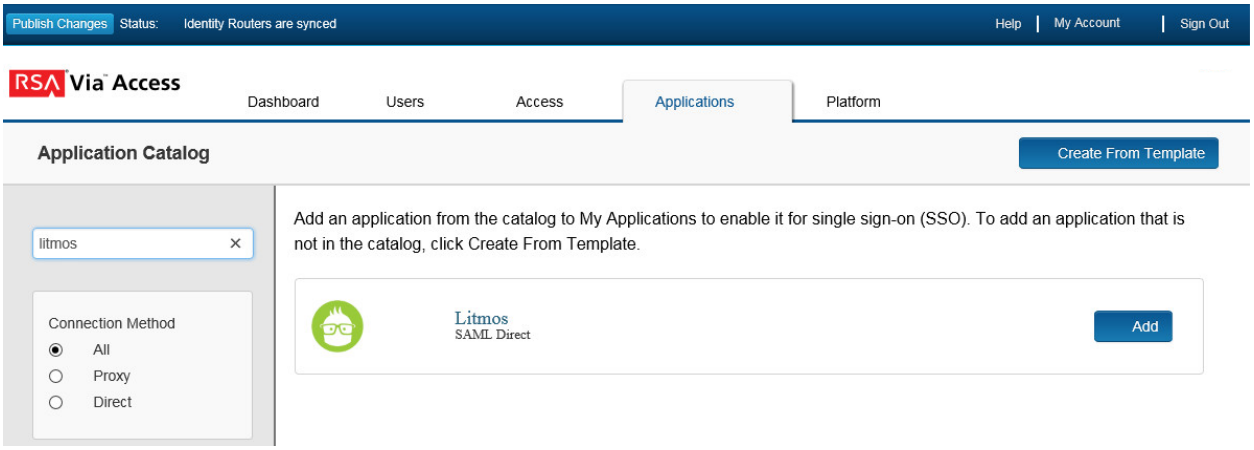
Procedure

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

Add the Application in RSA SecurID Access

Procedure

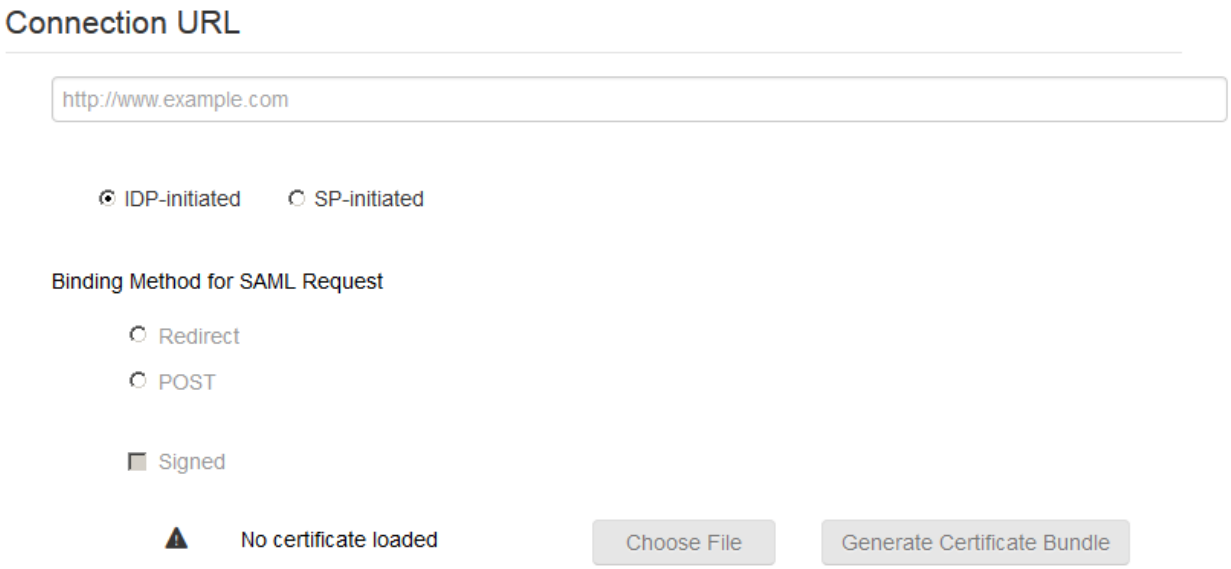
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, search for Litmos and click **+Add**.



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

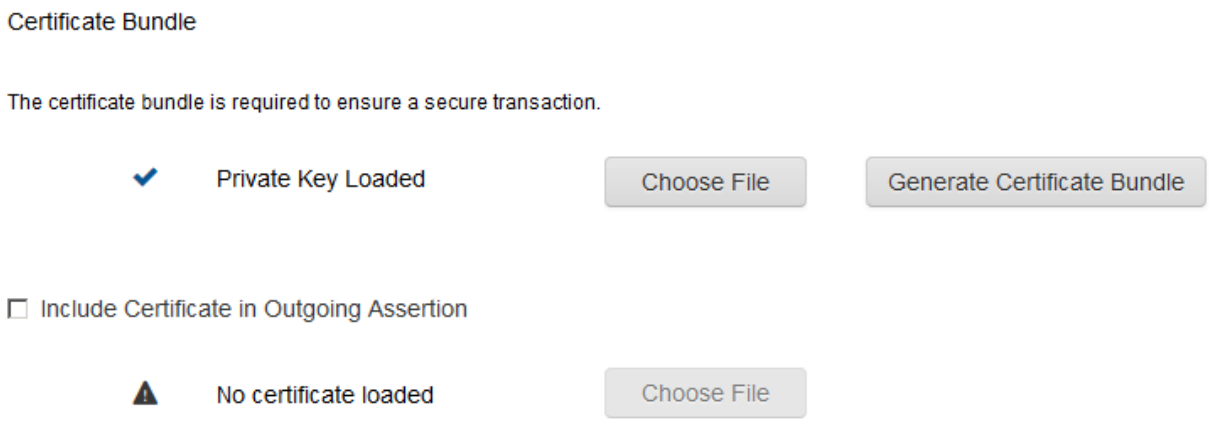
> **Note: Litmos only supports IDP initiated sessions.**

4. In the Connection URL field, select **IDP –initiated** and leave the connection URL blank.

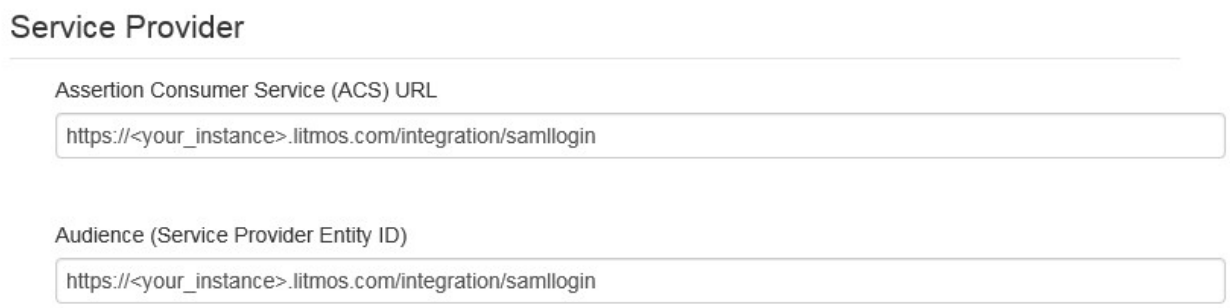


5. Scroll down to **SAML Identity Provider (Issuer)** section.
6. Take note of the Identity Provider URL; it will be needed to configure Litmos.

7. Click **Choose File** and upload the private key.



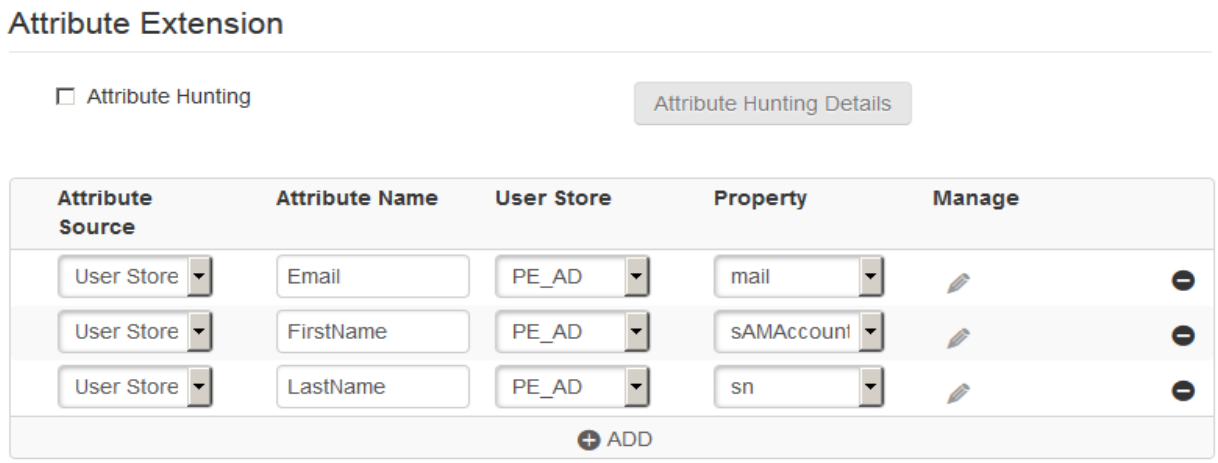
8. Scroll down to the **Service Provider** section.



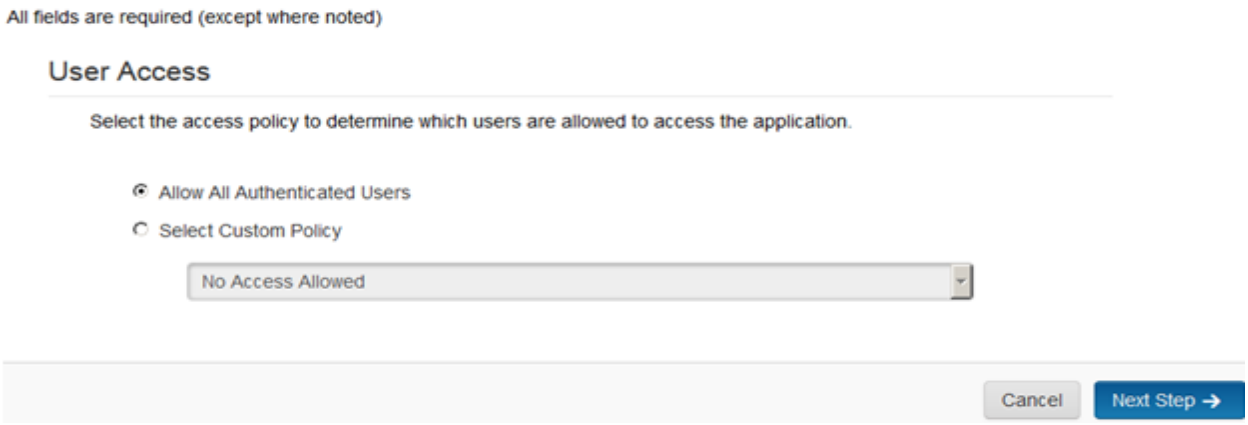
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <your_instance> with your specific subdomain.
   https://<your_instance>.litmos.com/integration/samllogin
   b. In the **Audience (Service Provider Entity ID)** field, replace <your_instance> with your specific subdomain.
   https://<your_instance>.litmos.com/integration/samllogin

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

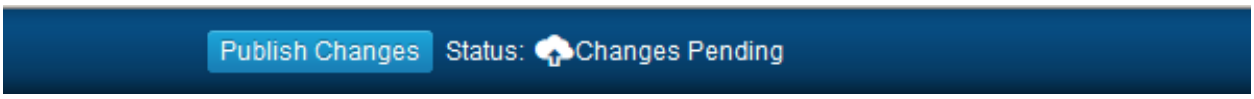
10. Click **Show Advanced Configuration**.
11. Scroll down to Attribute Extension and select your Attribute Source and User Store.
12. Add attribute **Email** with property **mail.**
13. Add attribute **FirstName** with property **sAMAccount**.
14. Add attribute **LastName** with property **sn**.



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



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



Next Steps

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

Configure Litmos to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to Litmos. https://<your_instance>.Litmos.com
2. From the left side tool bar select the **Account**'s icon then select the **Integrations** tab.
3. Scroll down and click on **SAML 2.0 (Single Sign On)**.
4. Enter the RSA SecurID Access Identity Provider URL found on page 2 step 6 in the **Origin URL** field.
5. Copy and paste the RSA SecurID Access public certificate in the SAML x.509 window.
6. Check the **Enable SAML** box.
7. Check the **Autogenerate Users** box.
8. Click **Save changes**.