

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.

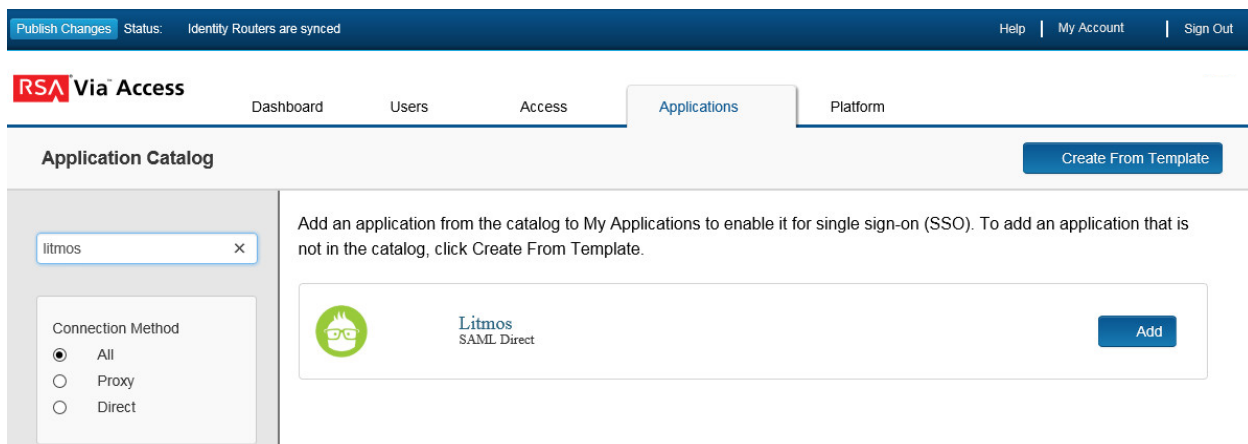
Procedure

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.

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

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

SAML Identity Provider (Issuer)

Identity Provider URL

https://pe110.pe-lab.com/IdPServlet?idp_id=litmostest

Issuer Entity ID


Default (idp_id): litmostest

Override

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

Certificate Bundle


The certificate bundle is required to ensure a secure transaction.

 Private Key Loaded

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion

 No certificate loaded

Choose File

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

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

- In the **Assertion Consumer Service (ACS) URL** field, replace <your_instance> with your specific subdomain.
https://<your_instance>.litmos.com/integration/samllogin
 - In the **Audience (Service Provider Entity ID)** field, replace <your_instance> with your specific subdomain.
https://<your_instance>.litmos.com/integration/samllogin
- Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

User Identity

Name ID

Identifier Type


Email Address

User Store

PE_AD

Property

mail

 Show Advanced Configuration

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**.

Attribute Extension

Attribute Hunting Attribute Hunting Details

Attribute Source	Attribute Name	User Store	Property	Manage
User Store	Email	PE_AD	mail	
User Store	FirstName	PE_AD	sAMAccount	
User Store	LastName	PE_AD	sn	
ADD				

15. Click **Next Step**.
16. 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 →

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.

Publish Changes

Status: Changes Pending

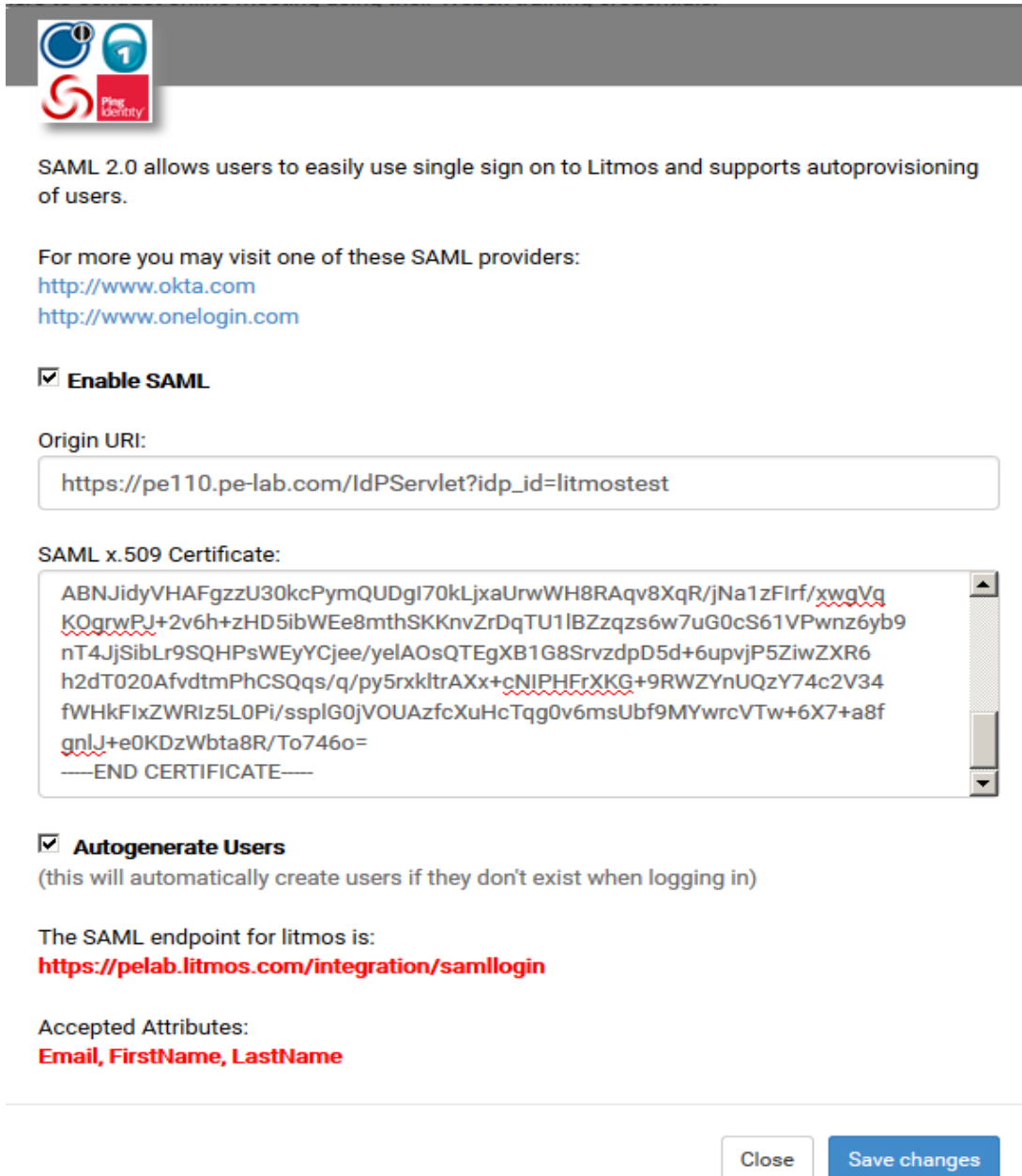
Next Steps

[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**.



SAML 2.0 allows users to easily use single sign on to Litmos and supports autoprovisioning of users.

For more you may visit one of these SAML providers:
<http://www.okta.com>
<http://www.onelogin.com>

Enable SAML

Origin URI:

SAML x.509 Certificate:

Autogenerate Users
(this will automatically create users if they don't exist when logging in)

The SAML endpoint for litmos is:
<https://pelab.litmos.com/integration/samllogin>

Accepted Attributes:
[Email](#), [FirstName](#), [LastName](#)

