RSA SECURID® ACCESS
Implementation Guide

Third Light

Gina Salvalzo, RSA Partner Engineering
Last Modified: August 22, 2018

RSA READY

Solution Summary

Third Light make digital media library software to help your team store, search and share media all in one place. Third Light supports multi-factor authentication through SAML 2.0 via the service-provider login page or the RSA identity provider portal. Third Light supports just in time user provisioning.

RSA SecurID Access Features	Third Light
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

Configuration Summary

All of the supported use cases of RSA SecurID Access with Third Light require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Third Light can be integrated with RSA Cloud Authentication Service in the following ways:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
Third Light SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Third Light in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

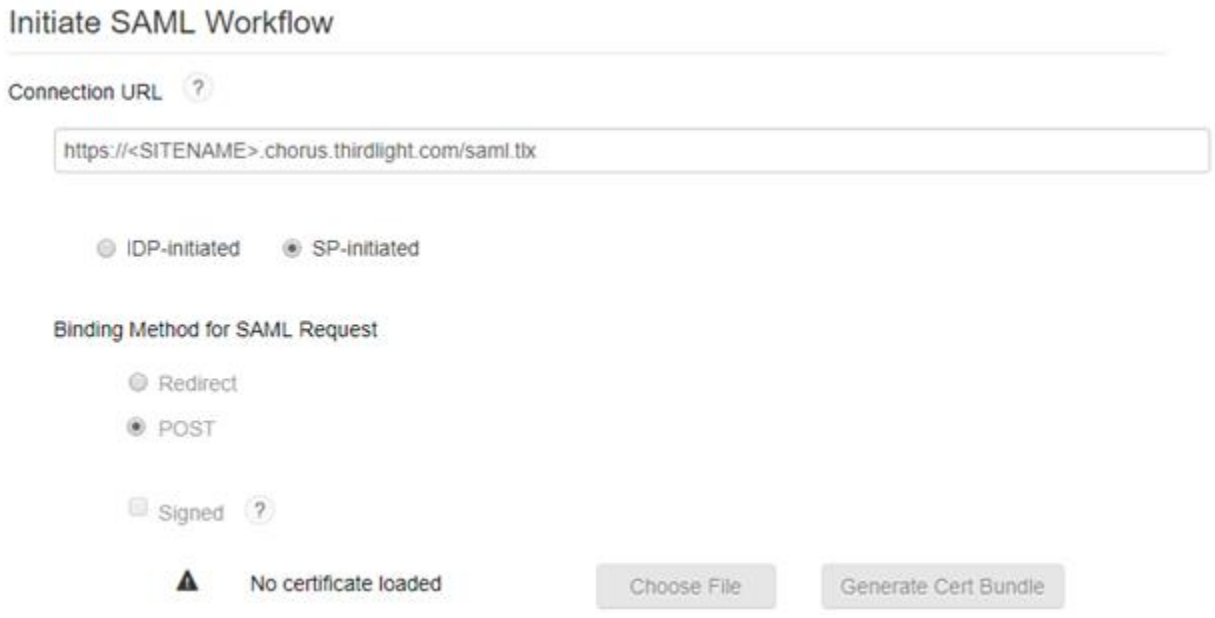
Configure RSA Identity Router SAML IdP

Procedure

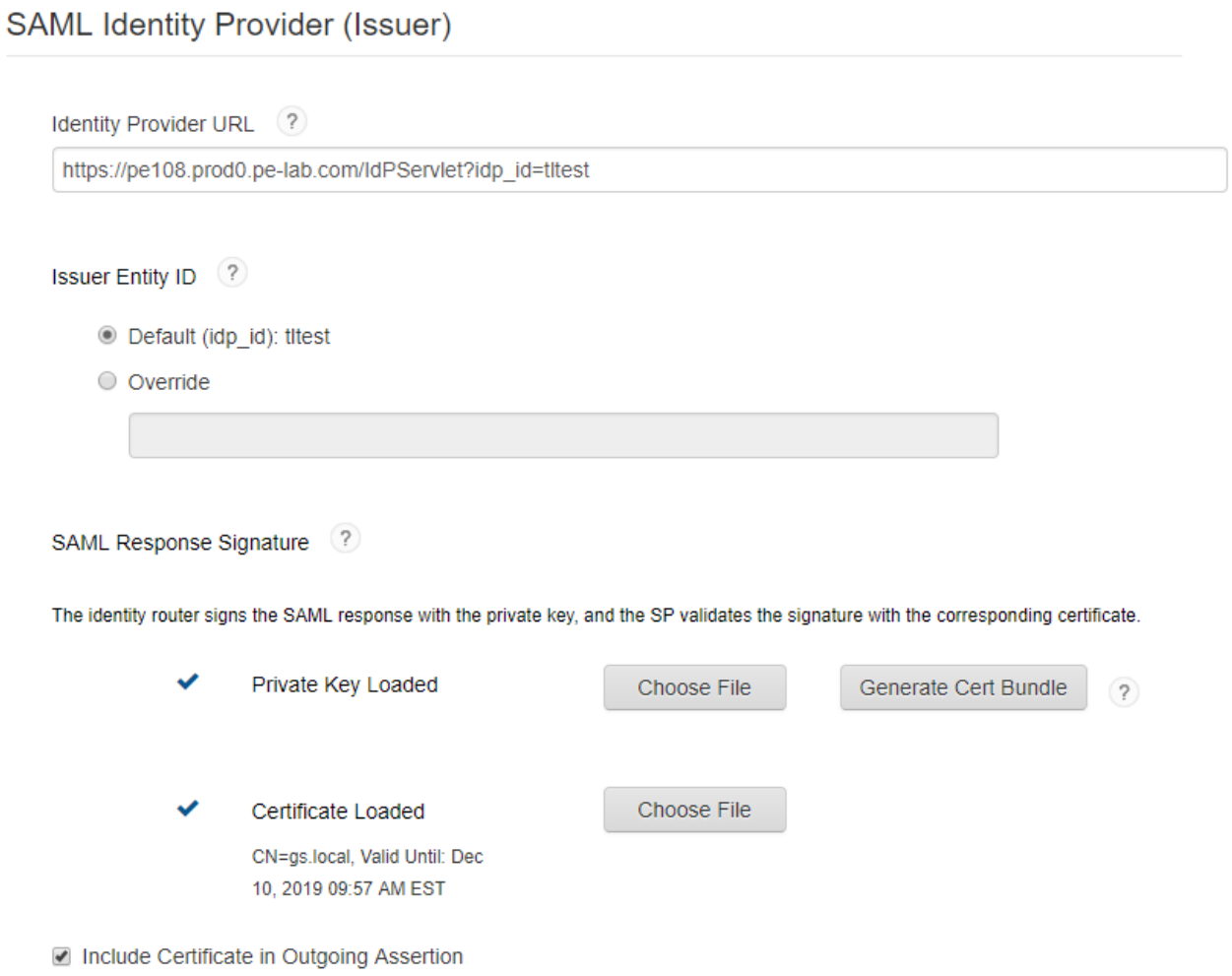
1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for Third Light and click **+Add** to add the connector.

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
   a. In the **Connection URL** field, replace <SITENAME> with your specific site name.
   b. Choose **SP-initiated** and binding method **POST**.

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



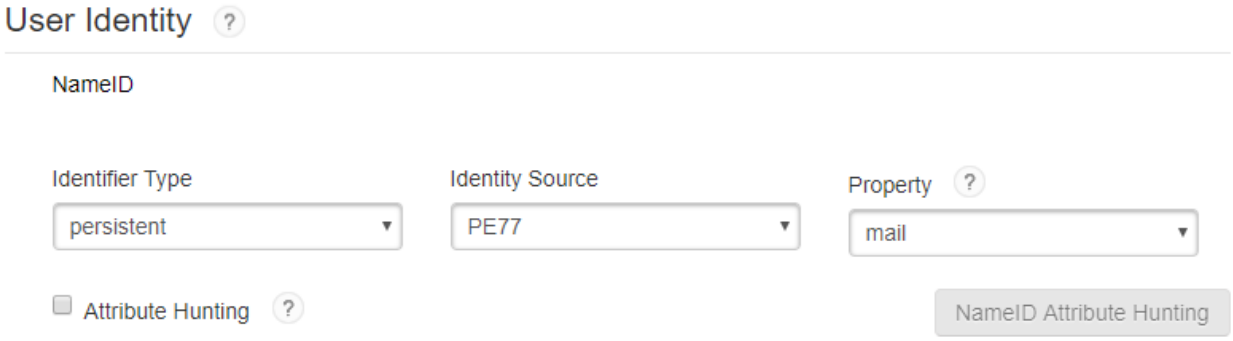
4. Scroll down to SAML Identity Provider (Issuer) section.



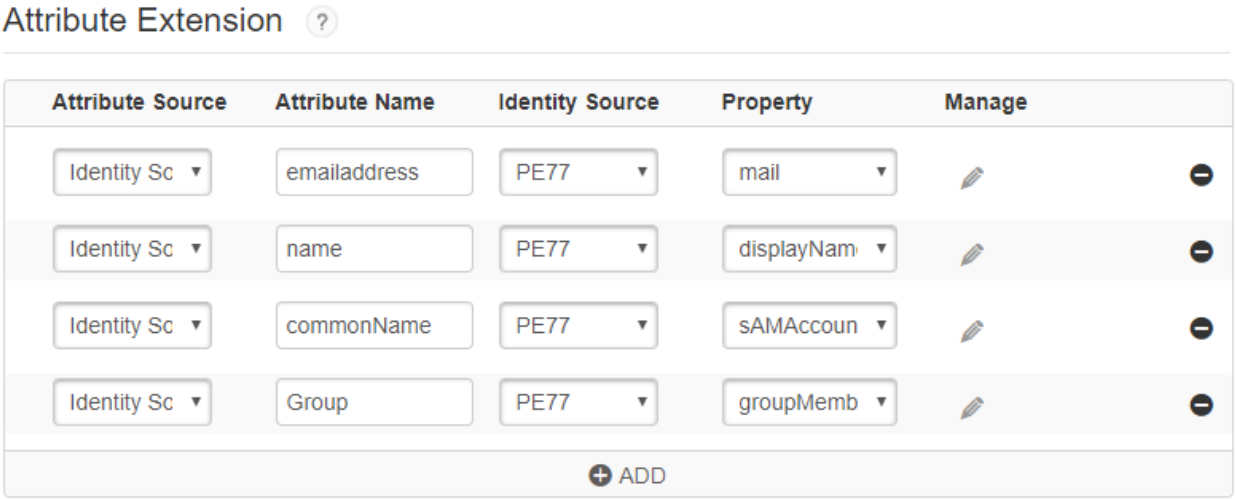
a. Take note of the **Identity Provider URL**.
b. Select **Choose File** and upload the private key.
c. Select **Choose File** to import the public signing certificate.
d. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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

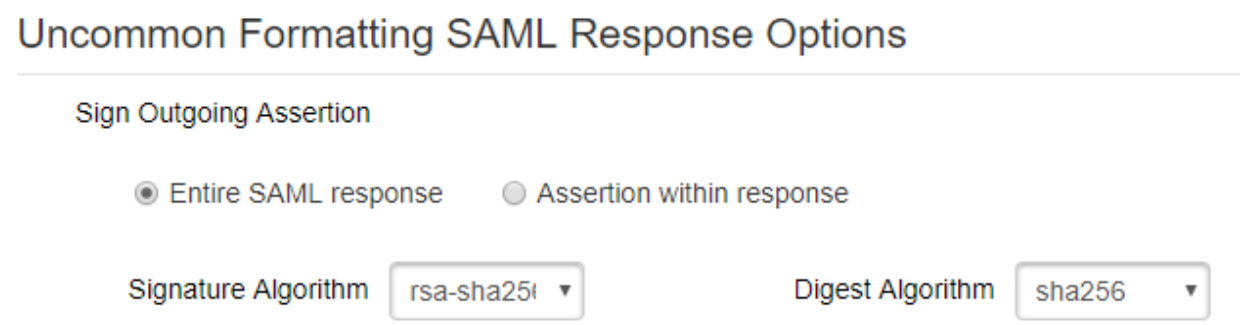
6. In the **Assertion Consumer Service (ACS) URL** field replace **<SITENAME>** and <**STRING>.** To find these values refer to the **SP metadata** file.
7. In the **Audience (Service Provider Entity ID)** field replace **<SITENAME>** with your site name.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the Identity Type is **persistent** and presented in **mail** format.



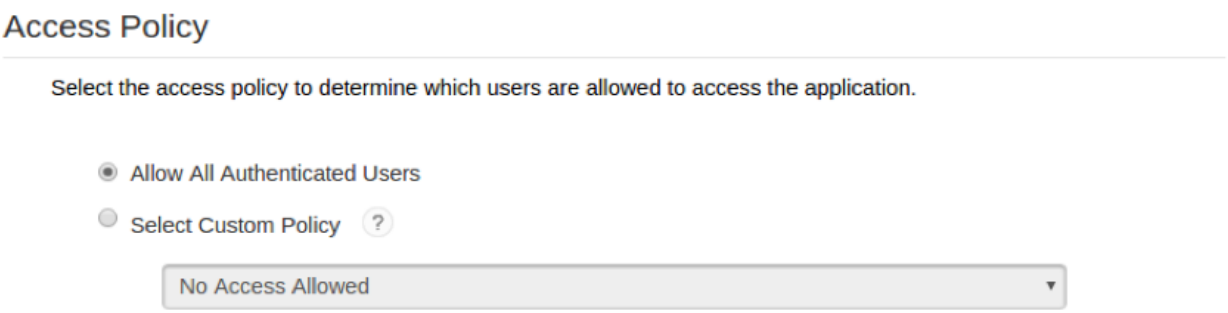
9. Click **Show Advanced Configuration**.
10. Under Attribute Extension, enter attributes for **emailaddress, name, commonName,** and **Group** with the correlating value from your Identity source.



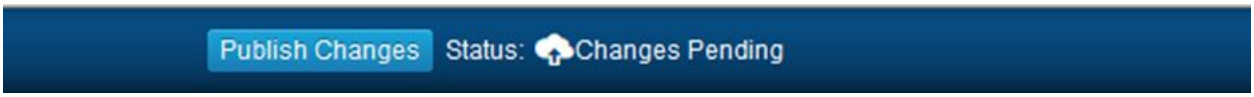
11. Under Uncommon Formatting SAML Response Options, select Signature Algorithm **rsa-sha256** and Digest Algorithm **sha256**.



12. Click **Next Step**.
13. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.



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



Next Steps

[Third Light SAML Configuration]

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Third Light with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

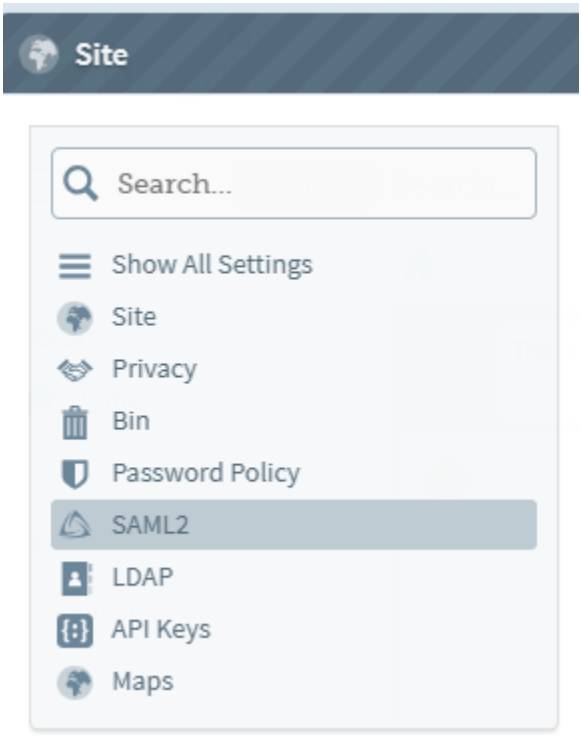
All Third Light components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Third Light SAML Configuration

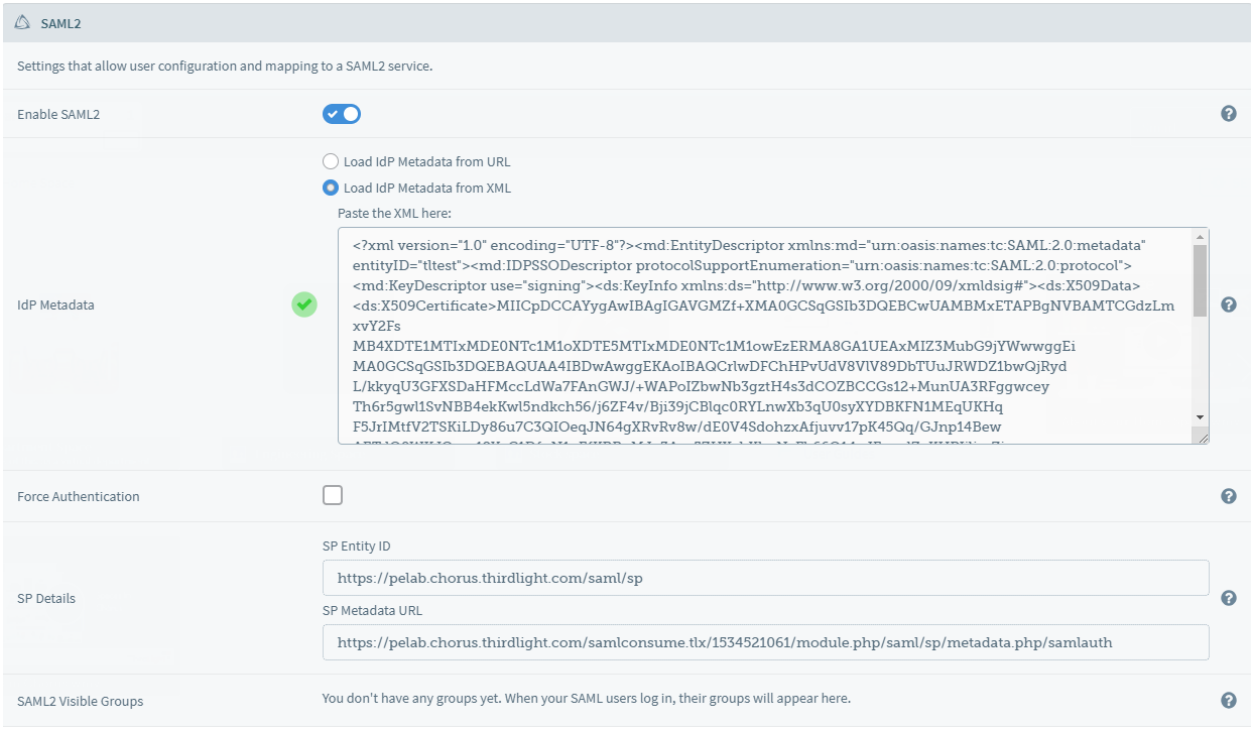
Complete the steps in this section to integrate Third Light with RSA SecurID Access using SAML authentication protocol.

Procedure

1. Login into the Third Light administration console. **https://<SITENAME>.chorus.thirdlight.com**
2. Under Admin select **Setting > Site**.
3. Select **SAML2.**



4. Select the checkbox **Enable SAML2**.
5. Choose **Load IdP Metadata from XML**.
6. Paste the metadata file into the IdP Metadata file window.
7. Click **Save**.
8. Once the save is complete the **SP Details** fields will populate.
9. In a browser copy the **SP Metadata URL,** right click on the data and select **Save as**.



10. Return to the RSA's application setup and import the metadata file retrieved from the SP Metadata URL page. The import will update the **Assertion Consumer Service URL and Audience (Service Provider Entity ID)** fields.
11. Click **Save** and **Publish Changes**.