RSA SECURID® ACCESS
Implementation Guide

Lucidchart

Gina Salvalzo, RSA Partner Engineering
Last Modified: July 18, 2018

RSA READY

Solution Summary

Lucidchart is a solution for visual communication and cross-platform collaboration. Create professional flowcharts, process maps, UML models, org charts, and more. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows.

RSA SecurID Access Features	
Lucidchart	
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

The following supported use case of RSA SecurID Access with Lucidchart 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 – Lucidchart can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
Lucidchart 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 Lucidchart 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.

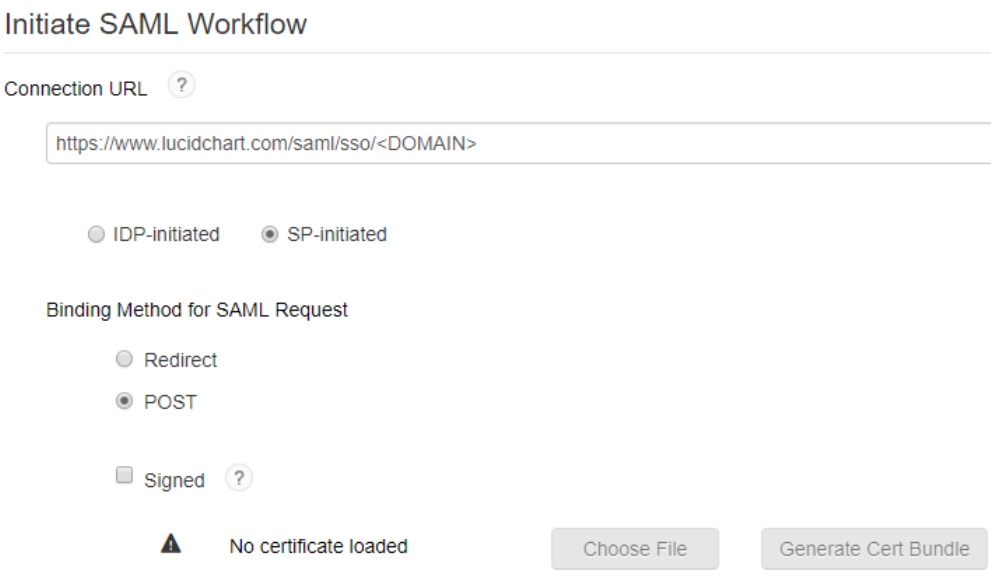
Configure RSA Identity Router SAML IdP

Procedure

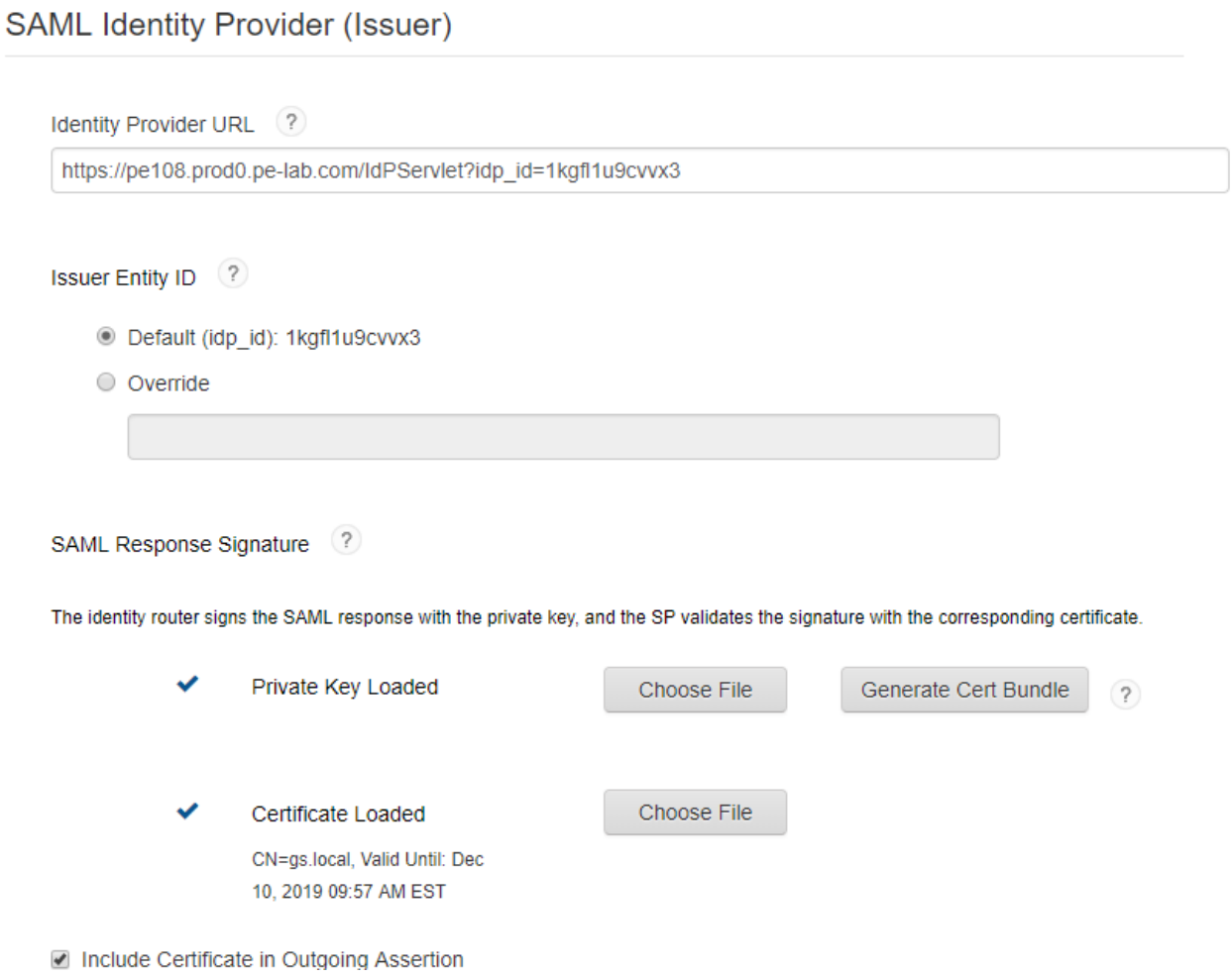
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for Lucidchart and click **+Add** to add the connector.

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 <DOMAIN> with your site domain.
   b. Choose **SP-initiated.**
   c. Select binding method **POST**.

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



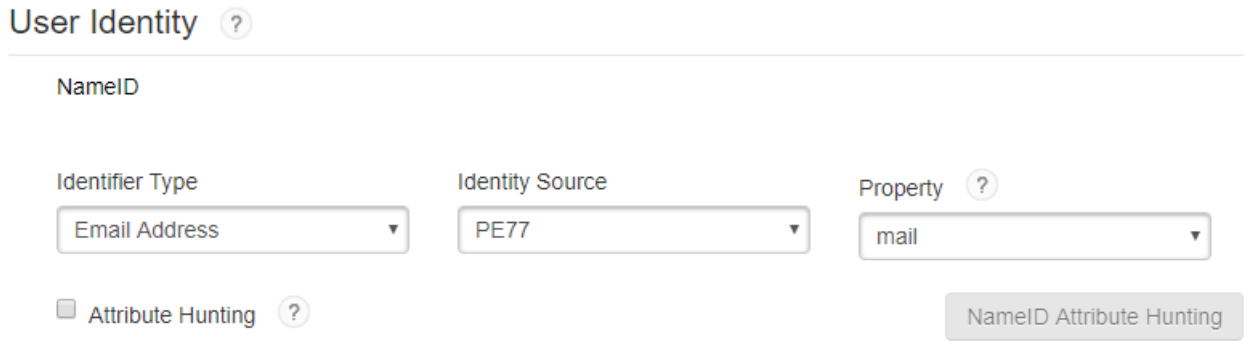
4. Scroll down to SAML Identity Provider (Issuer) section.



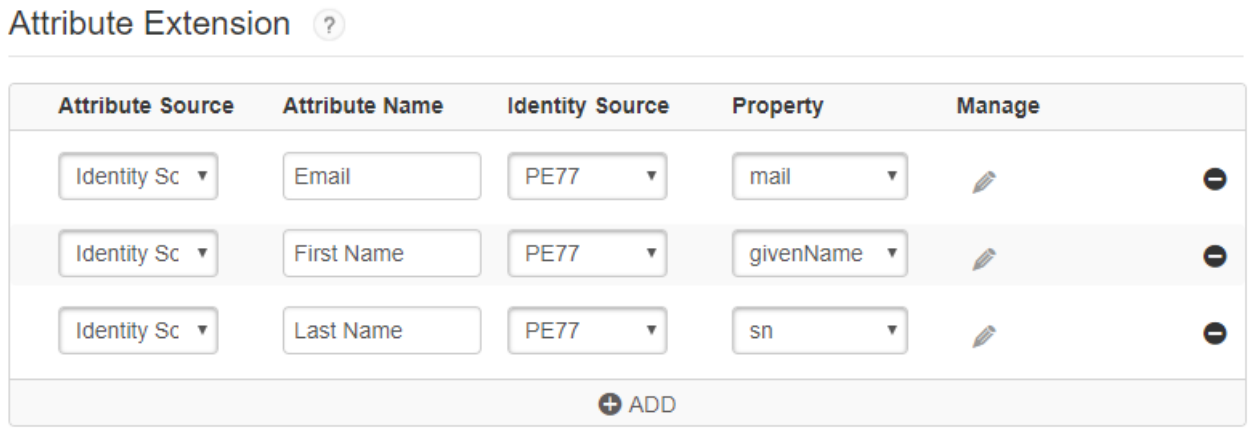
a. Select **Choose File** and upload the private key.
b. Select **Choose File** to import the public signing certificate.
c. Select the checkbox for **Include Certificate in Outgoing Assertion**.

5. Scroll down to the Service Provider section.

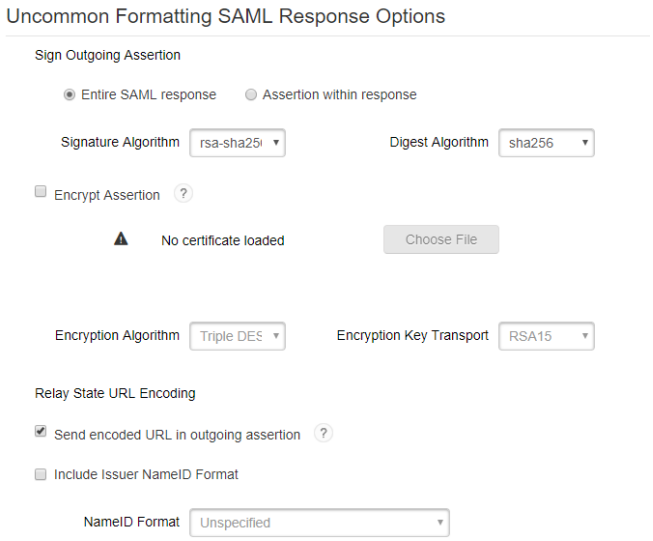
6. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your site domain.
7. Verify the **Audience (Service Provider Issuer ID)** field.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



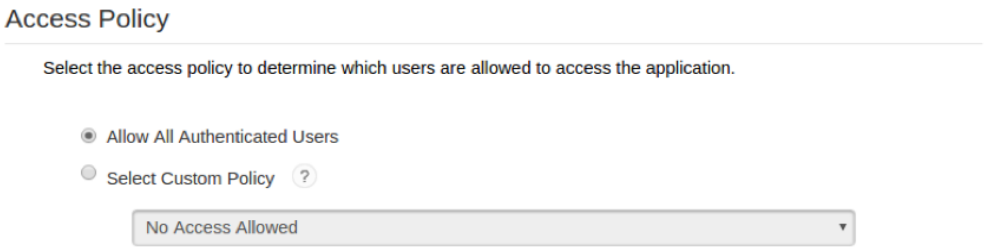
9. Click **Show Advanced Configuration**.
10. Under Attribute Extension, enter attributes **Email, First Name, Last Name** with the correlating value from your Identity source.



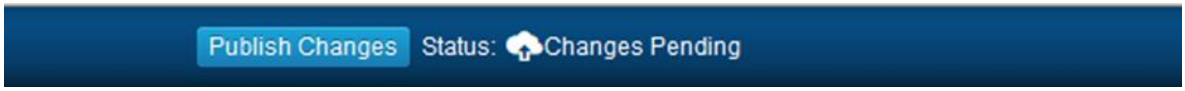
11. Under Uncommon Formatting SAML Response Options, verify that the Signature Algorithm rsa-sha256 and Digest Algorithm sha256 are correct for your environment.



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.



18. Navigate to **Applications > My Applications**.
19. Locate Lucidchart in the list and from the **Edit** option, select **Export Metadata**.

Partner Product Configuration

Before You Begin

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

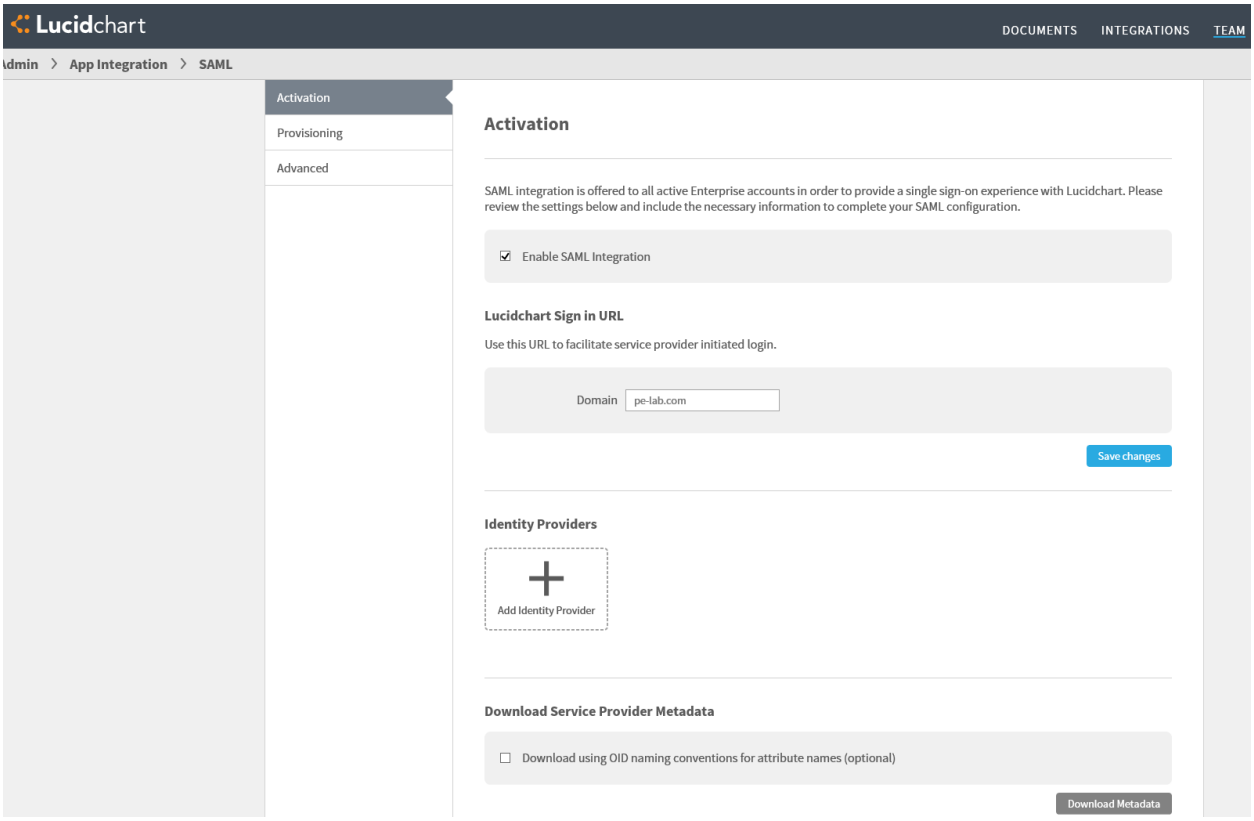
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Lucidchart SAML Configuration

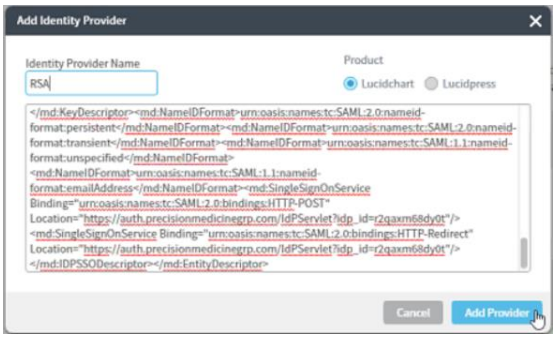
Procedure

1. Login to Lucidchart as an administrator.
2. Navigate to **TEAM > App Integration > SAML > Activation**.



3. Select the **Enable SAML Integration** checkbox.
4. Enter your site domain and select **Save changes**.

5. Select **Add Identity Provider**.
6. Enter a name for the Identity Provider.
7. Copy and paste the Identity Provider metadata file into the window and click **Add Provider**.



8. To login to your site via SP initiated browse to **https://www.lucidchart.com/saml/sso/<DOMAIN>.**