

RSA SECURID[®] ACCESS

Implementation Guide

Lucidchart

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

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.**


Initiate SAML Workflow

Connection URL 

IDP-initiated
 SP-initiated

Binding Method for SAML Request

Redirect
 POST
 Signed 

 No certificate loaded

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): 1kgfl1u9cvvx3

Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

Private Key Loaded

?

Certificate Loaded

CN=gs.local, Valid Until: Dec 10, 2019 09:57 AM EST

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

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.

User Identity ?

NameID

Identifier Type

Identity Source

Property ?

Attribute Hunting ?

NameID Attribute Hunting

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

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc ▼	<input type="text" value="Email"/>	PE77 ▼	mail ▼	⊖
Identity Sc ▼	<input type="text" value="First Name"/>	PE77 ▼	givenName ▼	⊖
Identity Sc ▼	<input type="text" value="Last Name"/>	PE77 ▼	sn ▼	⊖
+ ADD				

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

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

Entire SAML response
 Assertion within response

Signature Algorithm
 Digest Algorithm

Encrypt Assertion ?

▲ No certificate loaded

Encryption Algorithm
 Encryption Key Transport

Relay State URL Encoding

Send encoded URL in outgoing assertion ?

Include Issuer NameID Format

NameID Format

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

Access Policy

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy ?

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

Publish Changes
Status: Changes Pending

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

Lucidchart
 Created From: Lucidchart
 SAML Direct

Edit

Export Metadata

Delete

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.

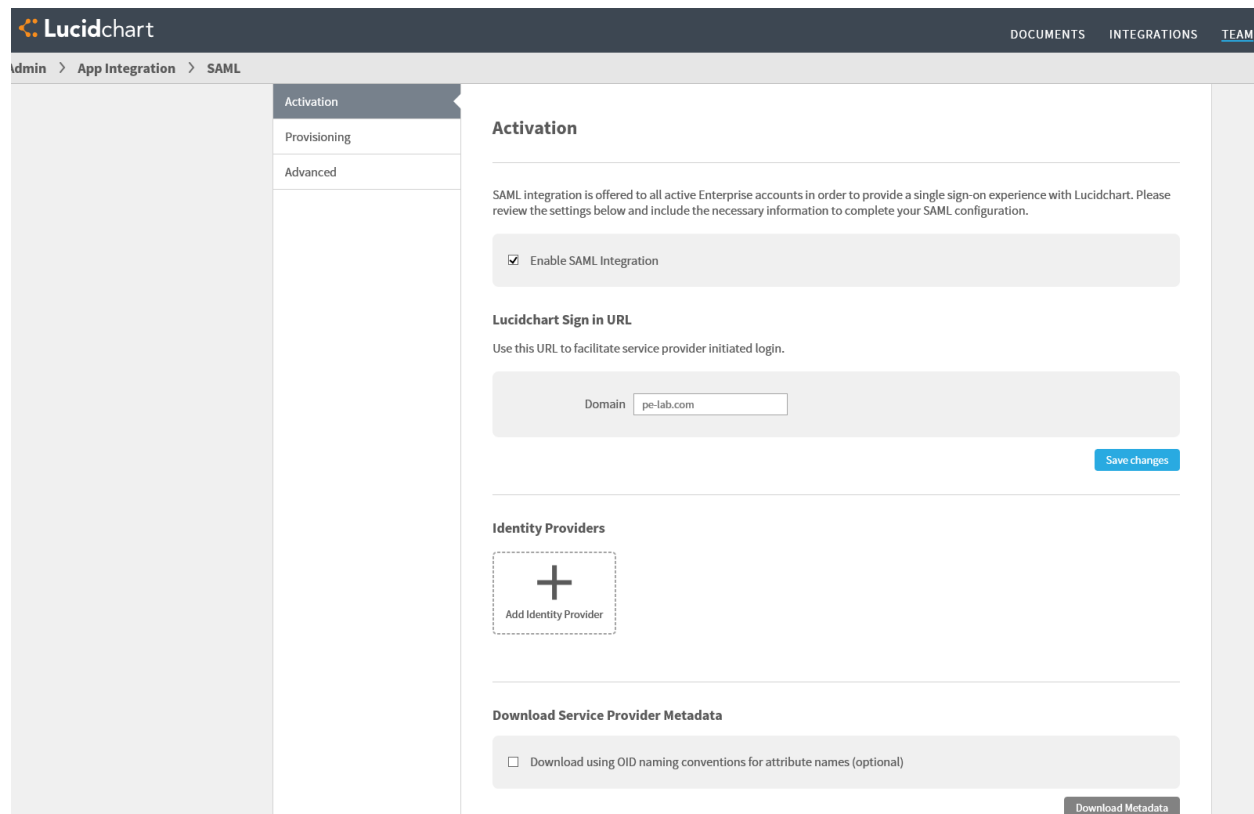
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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**.

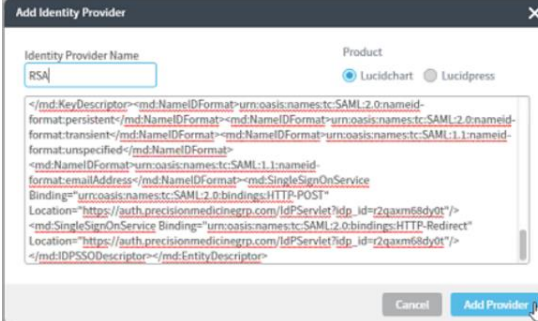


The screenshot shows the Lucidchart user interface for SAML configuration. The breadcrumb trail is 'admin > App Integration > SAML'. On the left, a sidebar menu has 'Activation' selected, with 'Provisioning' and 'Advanced' below it. The main content area is titled 'Activation' and contains the following sections:

- Enable SAML Integration:** A checkbox labeled 'Enable SAML Integration' is checked.
- Lucidchart Sign in URL:** A section with the heading 'Lucidchart Sign in URL' and the instruction 'Use this URL to facilitate service provider initiated login.' Below this is a 'Domain' input field containing 'pe-lab.com' and a 'Save changes' button.
- Identity Providers:** A section with the heading 'Identity Providers' and a dashed box containing a plus sign and the text 'Add Identity Provider'.
- Download Service Provider Metadata:** A section with the heading 'Download Service Provider Metadata' and a checkbox labeled 'Download using OID naming conventions for attribute names (optional)'. A 'Download Metadata' button is located at the bottom right of this section.

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**.



Identity Provider Name: RSA

Product: Lucidchart Lucidpress

```
</md:KeyDescriptor><md:NameIDFormat-urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat><md:NameIDFormat-urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat><md:NameIDFormat-urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat><md:NameIDFormat-urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat><md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://auth.precisionmedicinegrp.com/IdPServlet?idp_id=r2qaxm68dy0t"/><md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://auth.precisionmedicinegrp.com/IdPServlet?idp_id=r2qaxm68dy0t"/></md:IDPSSODescriptor></md:EntityDescriptor>
```

Buttons: Cancel, Add Provider

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