RSA SecurID Access Implementation Guide

Illumio

Gina Salvalzo, RSA Partner Engineering

Last modified: January 21, 2019

Table of Contents

Solution Summary

Use Case

When integrated Illumio end users must authenticate with RSA SecurID Access to sign in. Illumio can integrate using **SAML SSO Agent** or **Relying Party**. Illumio does support JIT (just in time) user provisioning.

Integration Types

SSO Agent integrations use SAML 2.0 technologies to direct users' web browsers to RSA SecurID Access for authentication. SSO Agents also provide Single Sign-On to other applications using the RSA Application Portal.

Relying Party integrations use SAML 2.0 to direct users' web browsers to RSA SecurID Access for authentication.

Supported Features

This section shows all of the supported features by integration type and by RSA SecurID Access component. Use this information to determine which integration type and which RSA SecurID Access component your deployment will use. The next section in this guide contains the instruction steps for how to integrate RSA SecurID Access with Illumio using each integration type.

Illumio integration with RSA Cloud Authentication Service

Authentication Methods	Authentication API	RADIUS	Relying Party	SSO Agent
RSA SecurID	-	-	✔	✔
LDAP Password	-	-	✔	✔
Authenticate Approve	-	-	✔	✔
Authenticate Tokencode	-	-	✔	✔
Device Biometrics	-	-	✔	✔
SMS Tokencode	-	-	✔	✔
Voice Tokencode	-	-	✔	✔
FIDO Token	n/a	n/a	✔	✔

Illumio integration with RSA Authentication Manager

Authentication Methods	Authentiaction API	RADIUS	Authentication Agent
RSA SecurID	-	-	-
On Demand Authentication	-	-	-
Risk-Based Authentication	n/a	-	-

✔ Supported

- Not supported

n/t Not yet tested or documented, but may be possible.

n/a Not applicable

Configuration Summary

This section contains links to the sections that contain instruction steps that show how to integrate Illumio with RSA SecurID Access using all of the integration types.

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 RSA SecurID Access and Illumio components must be installed and working prior to the integration.

Links

Relying Party

SSO Agent

Known Issues

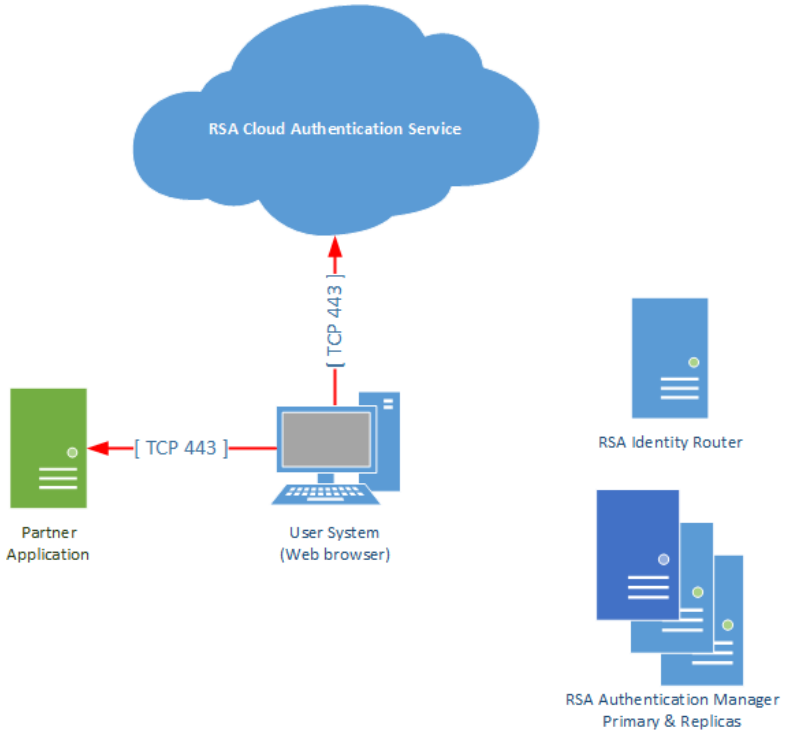
No known issues.

Integration Configuration

Relying Party

This section contains instructions on how to integrate RSA SecurID Access with Illumio using Relying Party. Relying party uses SAML 2.0 to integrate RSA SecurID Access as a SAML Identity Provider (IdP) to Illumio SAML Service Provider (SP).

Architecture Diagram

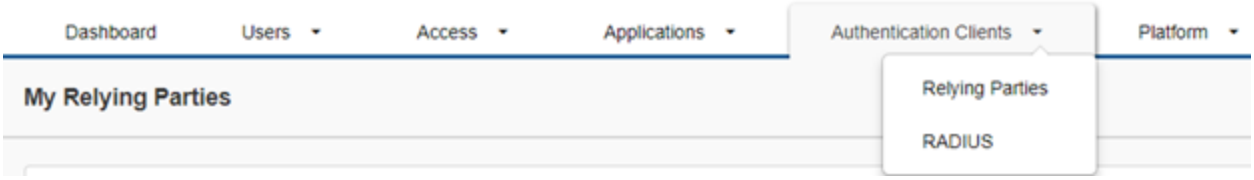


RSA Cloud Authentication Service

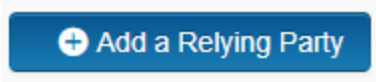
Follow the steps in this section to configure RSA Cloud Authentication Service as a Relying Party SAML IdP to Illumio .

Procedure

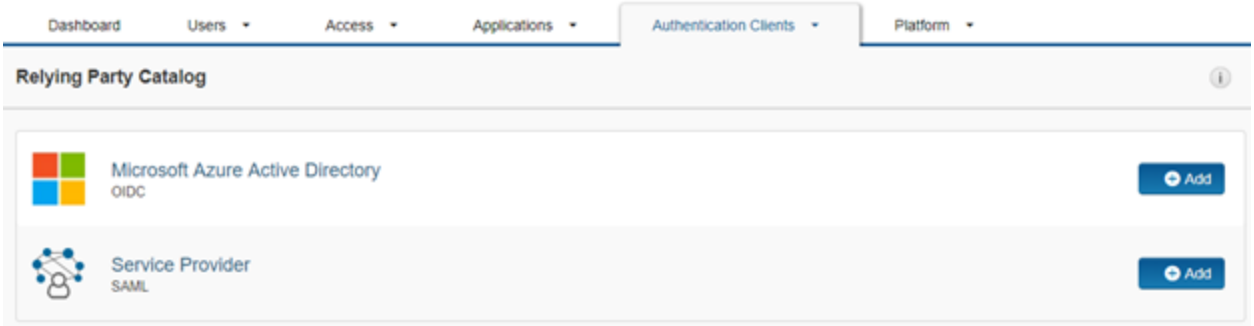
1. Logon to the **RSA Cloud Administrative Console** and browse to **Authentication Clients** > **Relying Parties** and click **Add a Relying Party**.



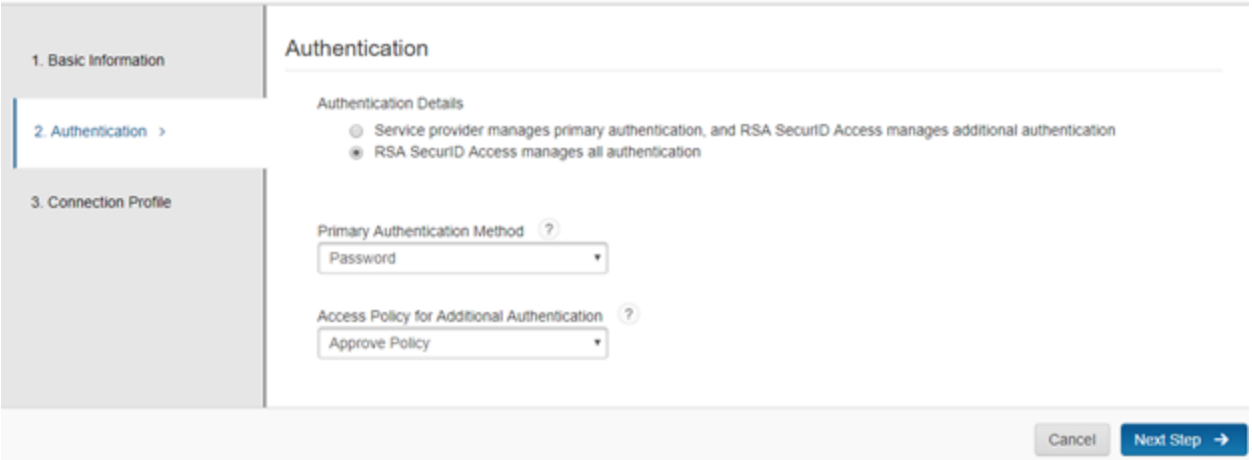
3. Click the **Add a Relying Party** button on the My Relying Parties page.



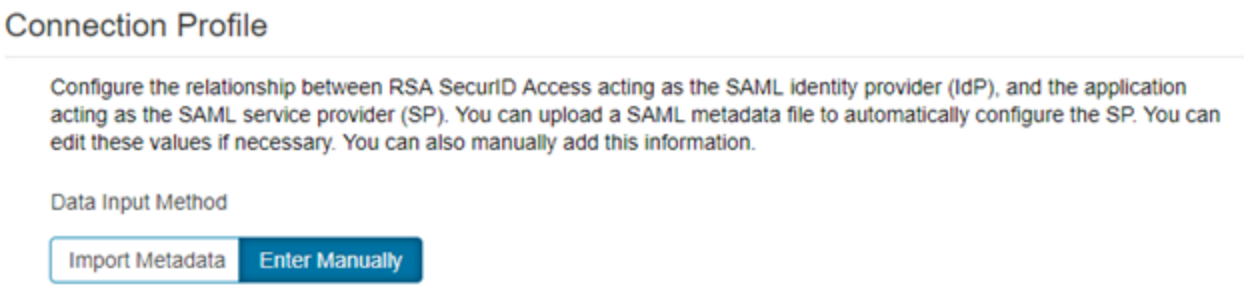
4. From the Relying Party Catalog select the **+Add** button for Service Provider SAML.



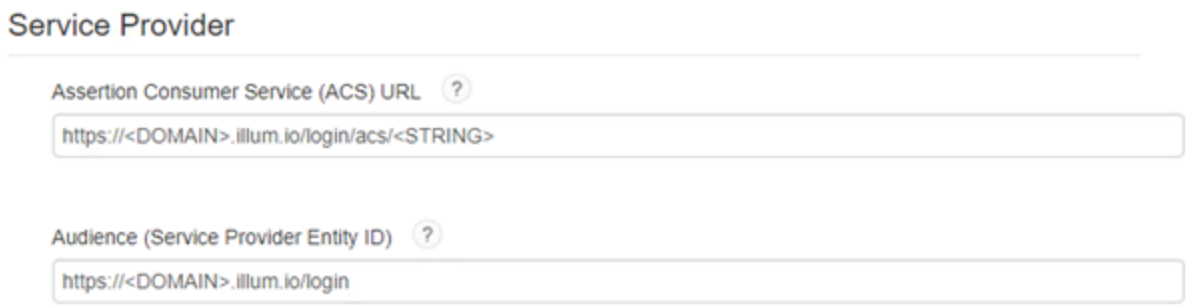
5. Enter a name for the Service Provider in the **Name** field on the Basic Information page.
6. Click the **Next Step** button.
7. On the Authentication page, select **RSA SecurID Access manages all authentication**.
8. From the Primary Authentication Method pulldown, select your desired login method either Password or SecurID.
9. From the Access Policy pulldown select a policy that was previously configured.



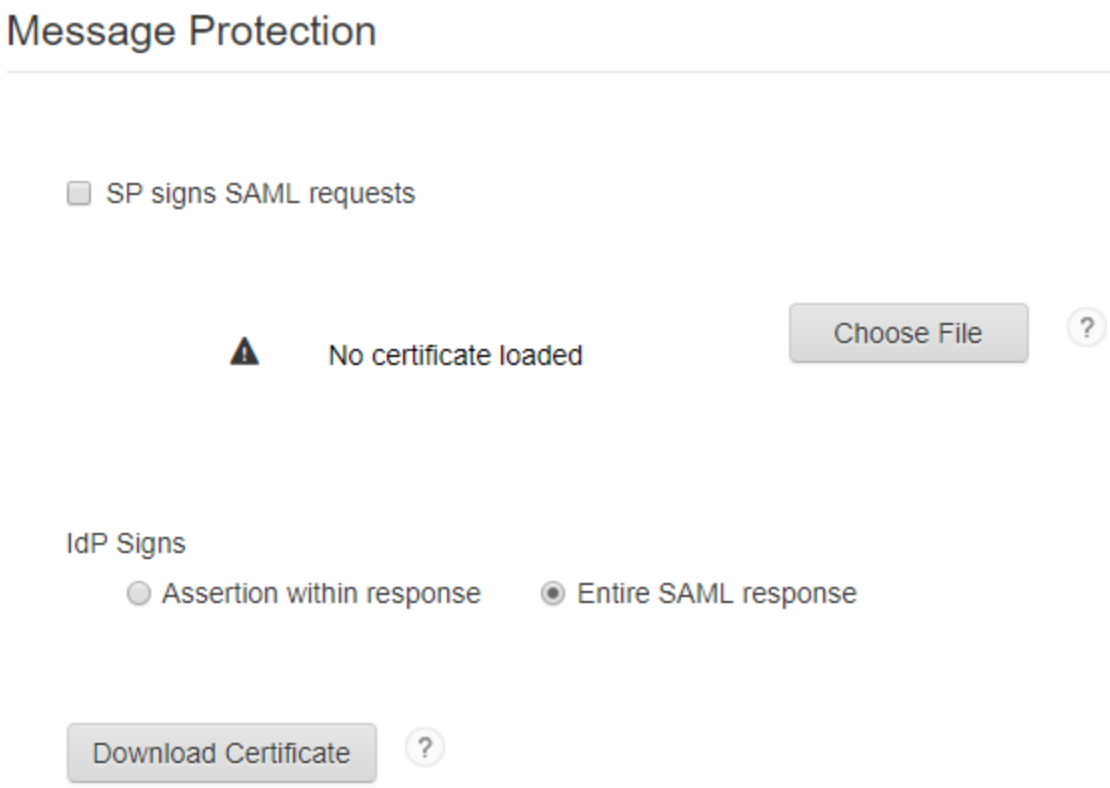
10. Select **Next Step**.
11. Select **Enter Manually**.



12. Enter the **Assertion Consumer Service (ACS) URL** found on the Illumio's Single Sign-On Configuration page.
13. Enter the **Illumio Issuer** in the Audience (Service Provider Entity ID) field.

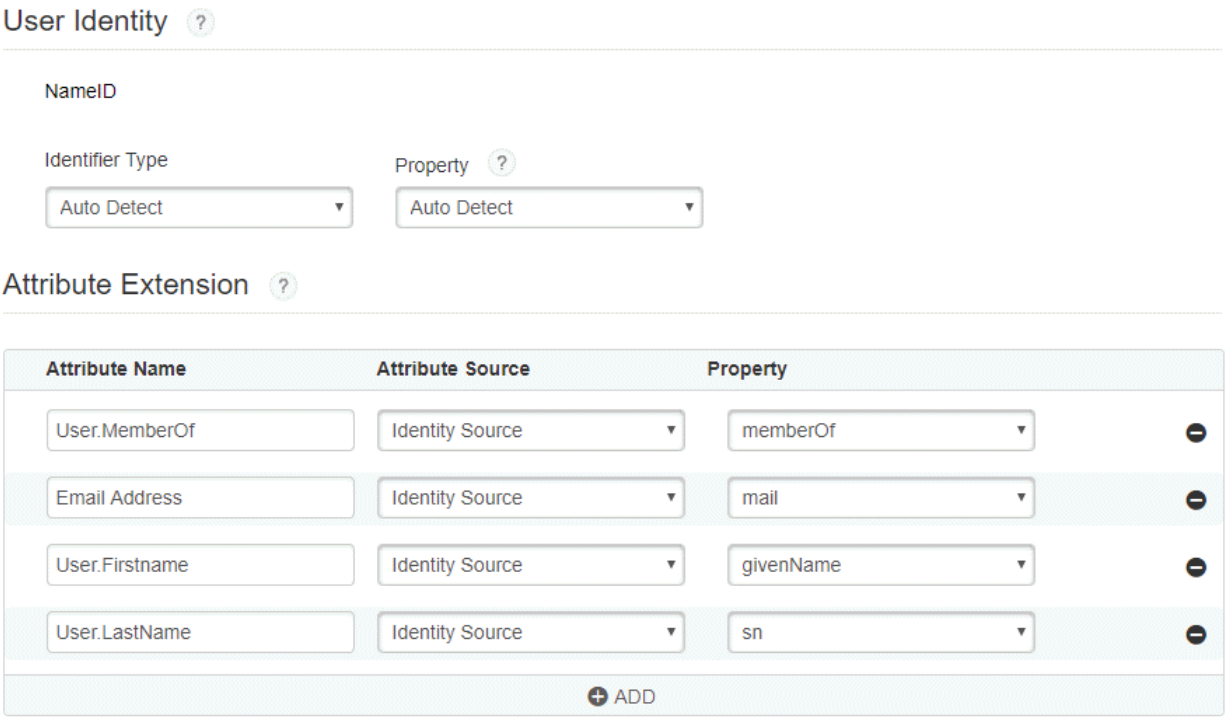


14. Under IdP Signs select **Entire SAML response**.



15. Select **Download Certificate.**

16. Select **Show Advanced Configuration**. Under Attribute Extension add attributes **Email Address, User.FirstName, User.LastName, and UserMemberOf**.



17. Select **Save and Finish**.

18. On the My Relying Parties page, select the **Edit** pulldown and select **View or Download IdP Metadata**.

19. View the metadata file to find the Cloud IDP URL. **Location=https://<company_id>.auth.securid.com/saml-fe/sso**. This is the Cloud IDP URL.

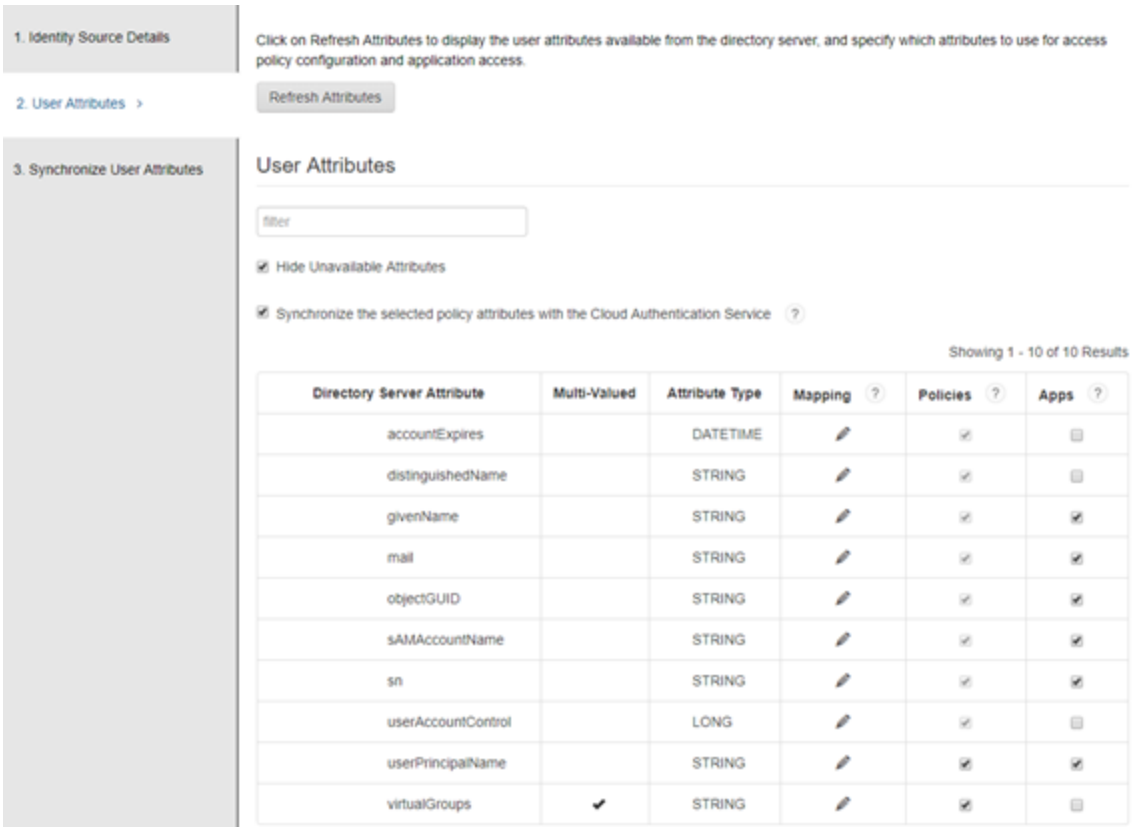
20. Navigate to **Users > Identity Sources**.

Note: Perform the following steps to all Identity Sources used in the policy.

21. Select **Edit** for the Identity Source used in the Policy.

22. On the User Attributes page, verify that the **Synchronize the selected policy attributes with the Cloud Authentication Servic**e is checked.

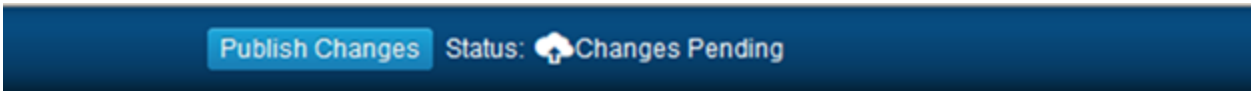
23. In the Policies column verify that attribute **mail, sn, givenName, and memberOf** are checked.



24. Click **Next Step**.

25. Click **Save and Finish**.

26. On the top menu click **Publish Changes**.



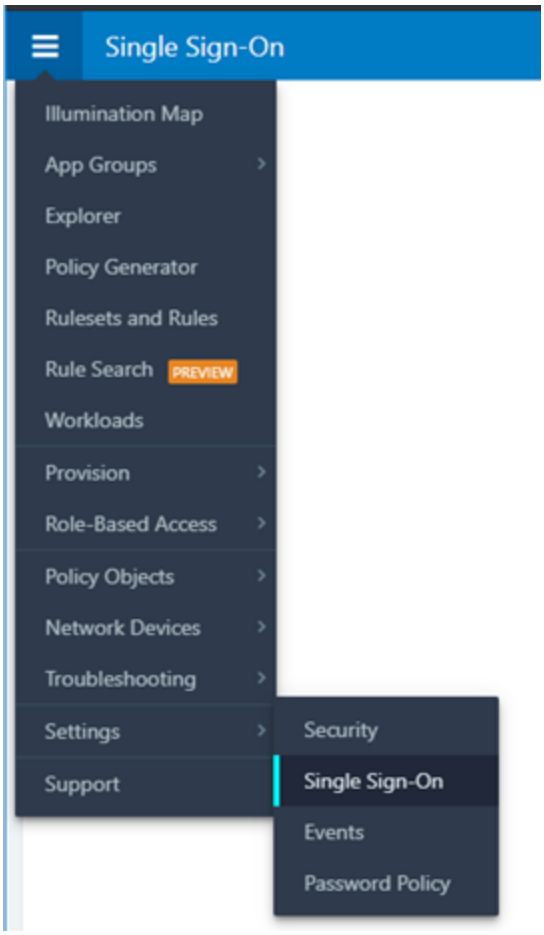
Illumio

Follow the steps in this section to configure Illumio as a Relying Party SAML SP to RSA Cloud Authentication Service.

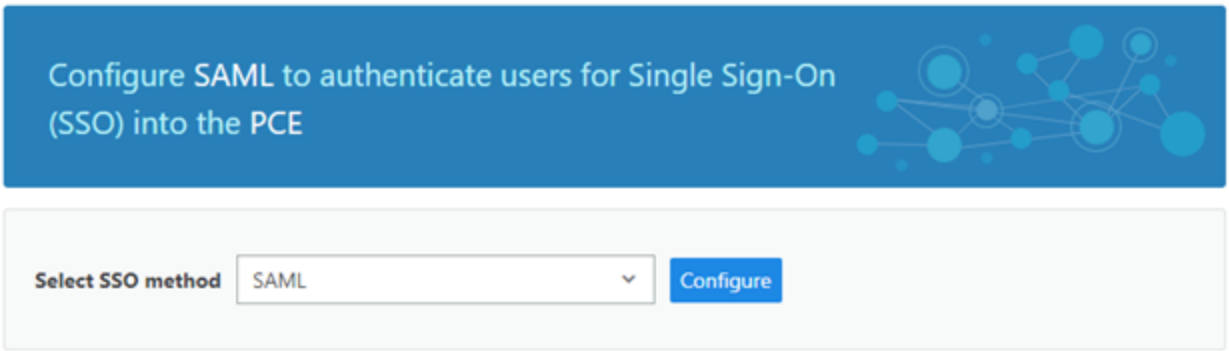
Procedure

1. Login into the Illumio administration console.

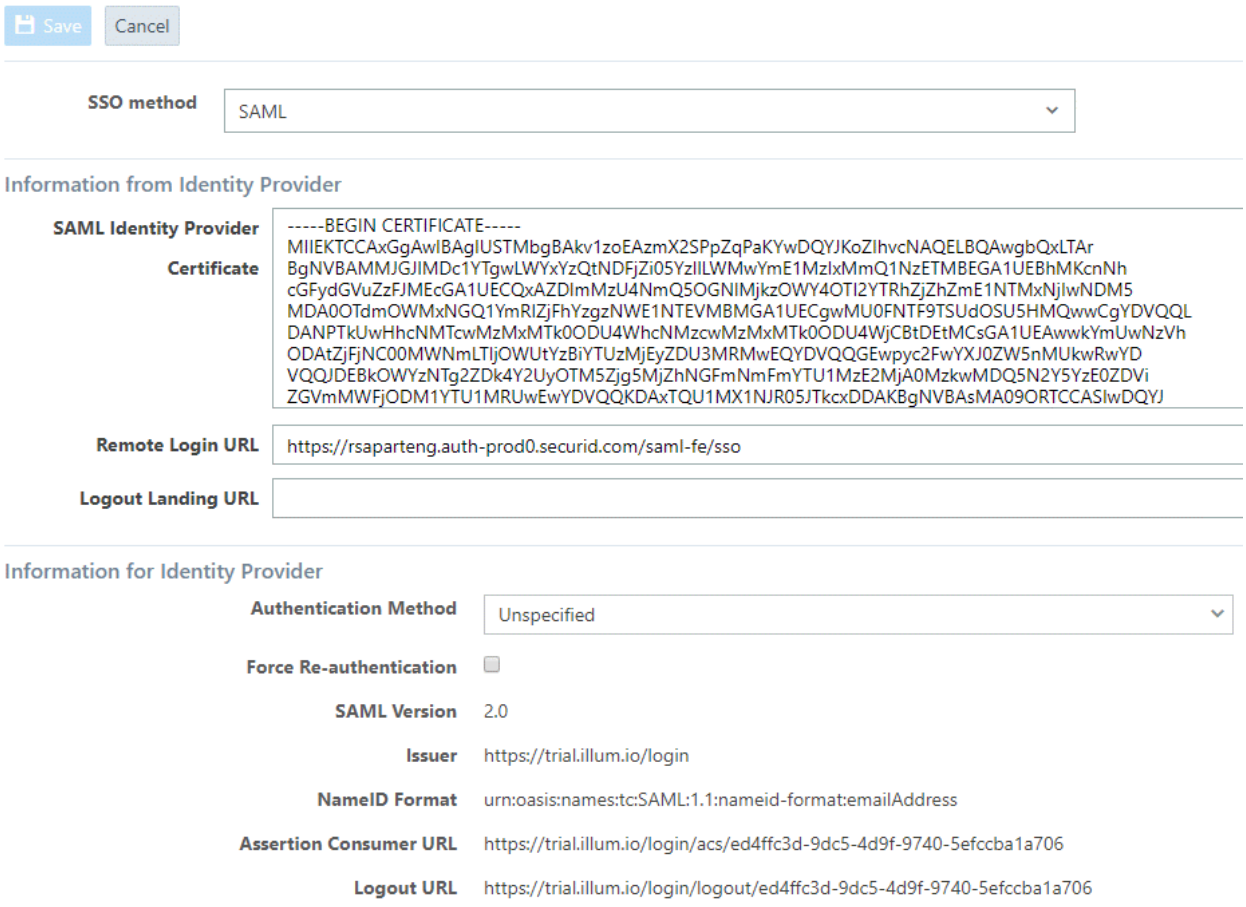
2. Navigate to **Settings > Single Sign-On**



3. Select **SAML** from the pulldown and then click **Configure**.



4. Click **Edit.**



5. Paste the Cloud certificate in the SAML Identity Provider Certificate field.
6. Enter the Cloud IDP URL in the Remote Login URL field.
7. Enter a Logout Landing URL (optional).
8. Click **Save**.

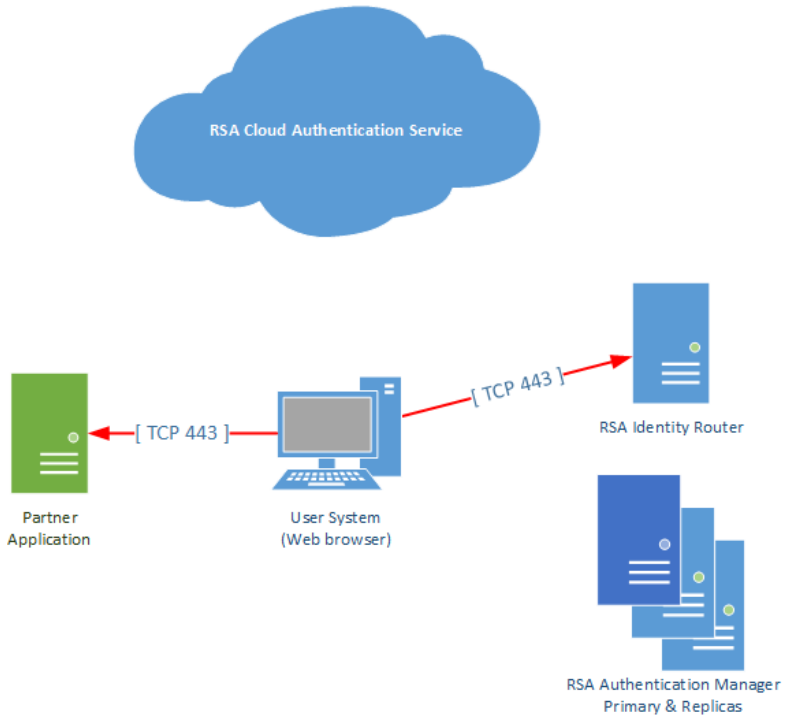
Configuration is complete.

Return to the main page for more certification related information.

SSO Agent - SAML

This section contains instructions on how to integrate RSA SecurID Access with Illumio using a SAML SSO Agent.

Architecture Diagram



RSA Cloud Authentication Service

Follow the steps in this section to configure RSA Cloud Authentication Service as an SSO Agent SAML IdP to Illumio.

Procedure

1. Logon to the RSA Cloud Administration Console and browse to **Applications** > **Application Catalog**, search for **illumio** and click **+Add** to add the connector.

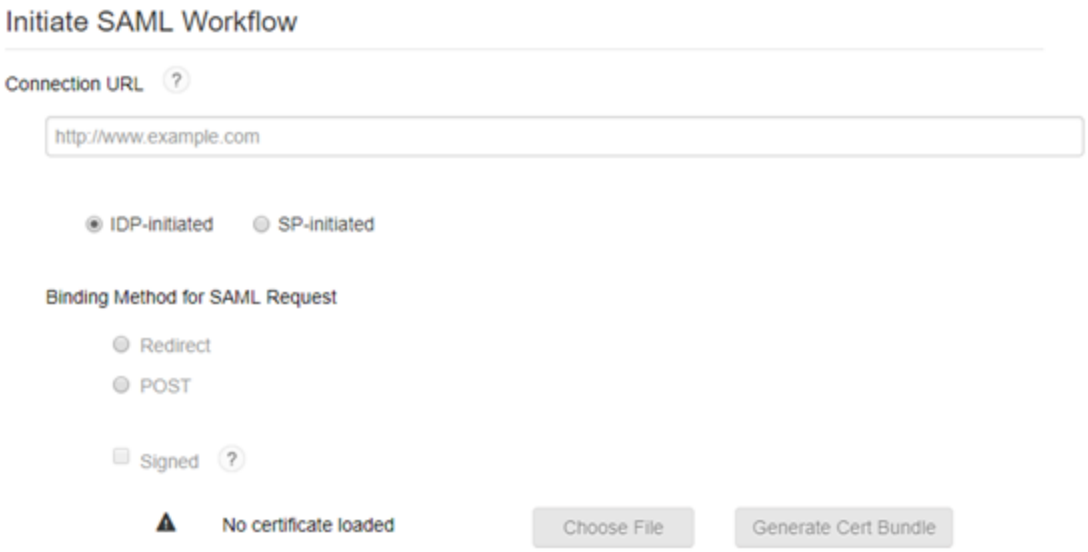
2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.

3. Navigate to Initiate SAML Workflow section.

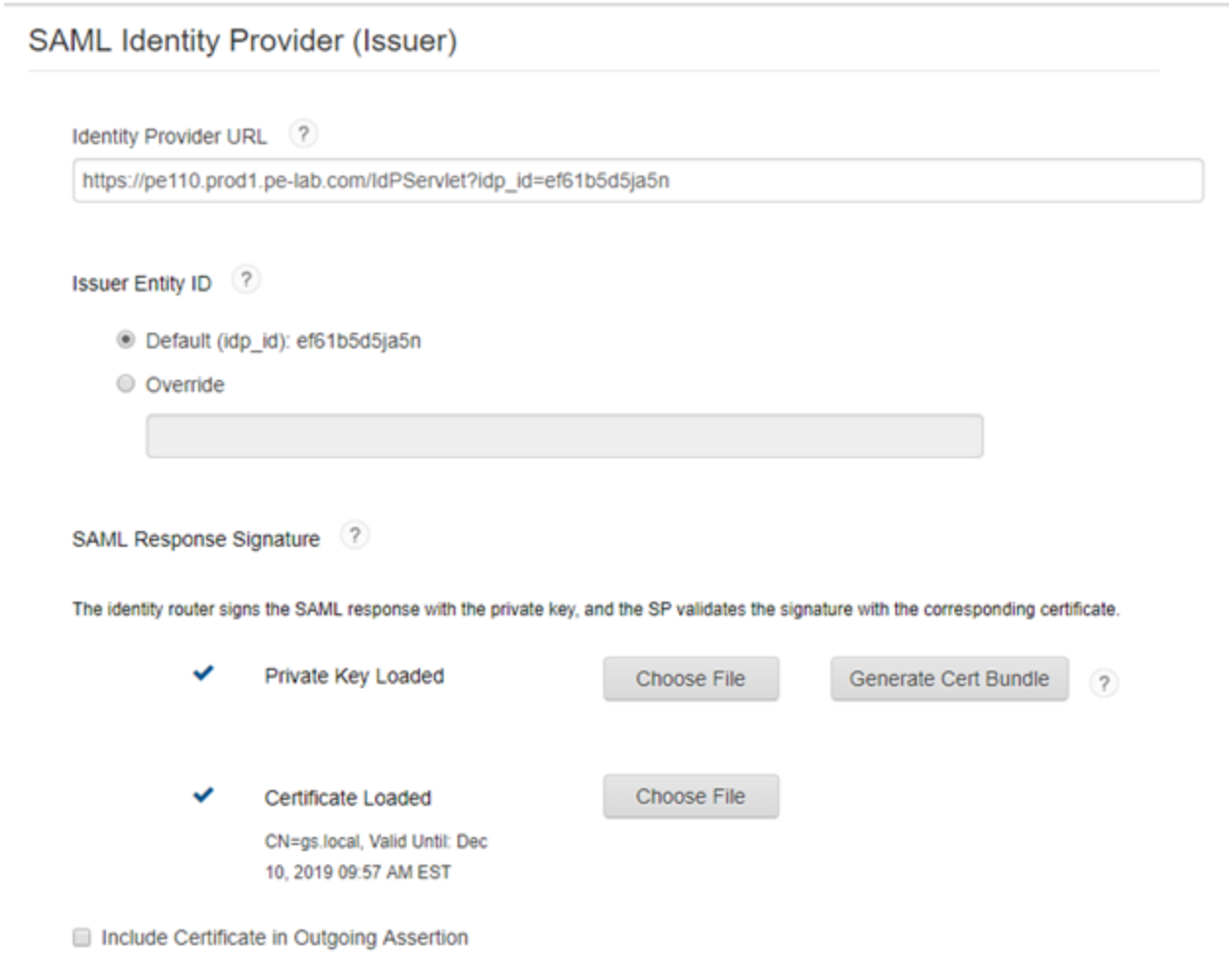
a. Leave the **Connection URL** field blank.

b. Choose **IDP-initiated**.

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

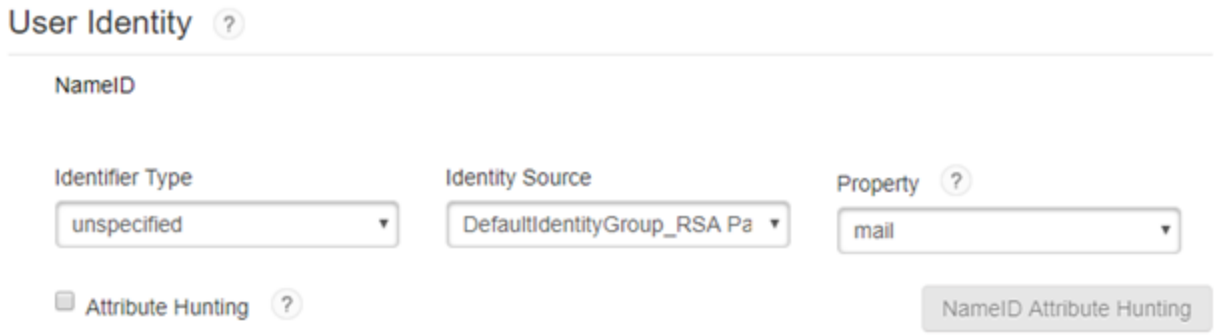
c. Select **Choose File** to import the public signing certificate.

5. Scroll down to the Service Provider section.

6. Enter the **Assertion Consumer Service (ACS) URL** found on Illumio's Single Sign-On Configuration page.

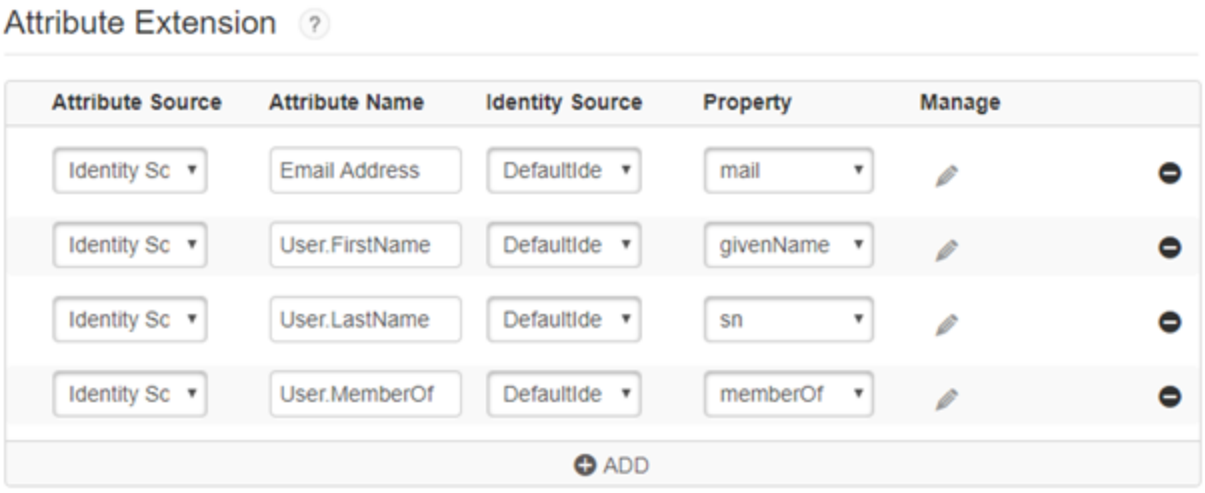
7. Enter the **Illumio Issuer** in the Audience (Service Provider Entity ID) field.

8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the NameID is set to format **unspecified** with the value of **mail**.



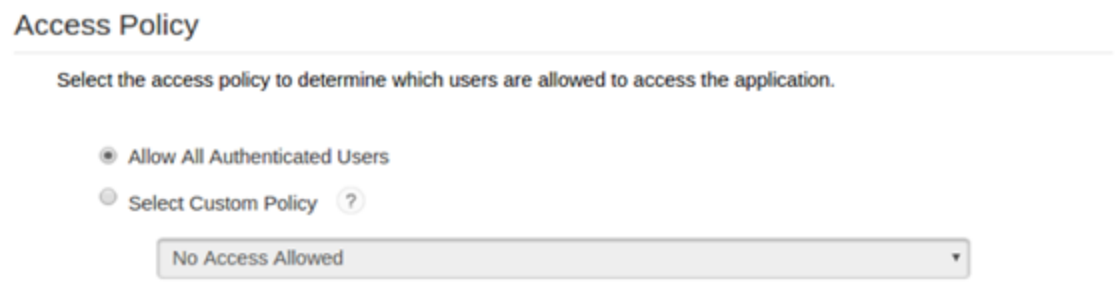
9. Click **Show Advanced Configuration**.

10. Under Attribute Extension add attributes **Email Address, User.FirstName, User.LastName, User.MemberOf** with their correlated property.

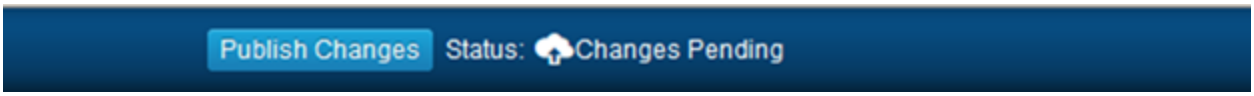


11. Click **Next Step**.

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



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

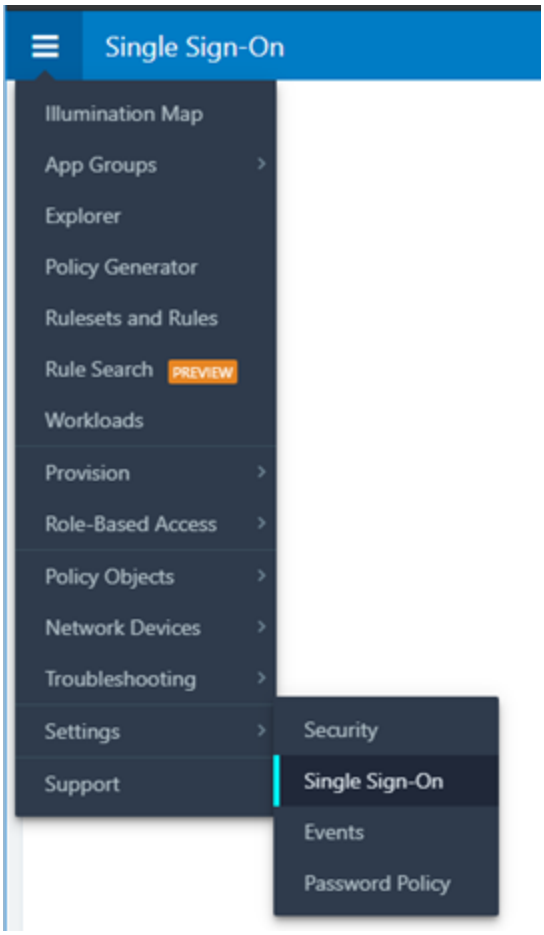


Illumio

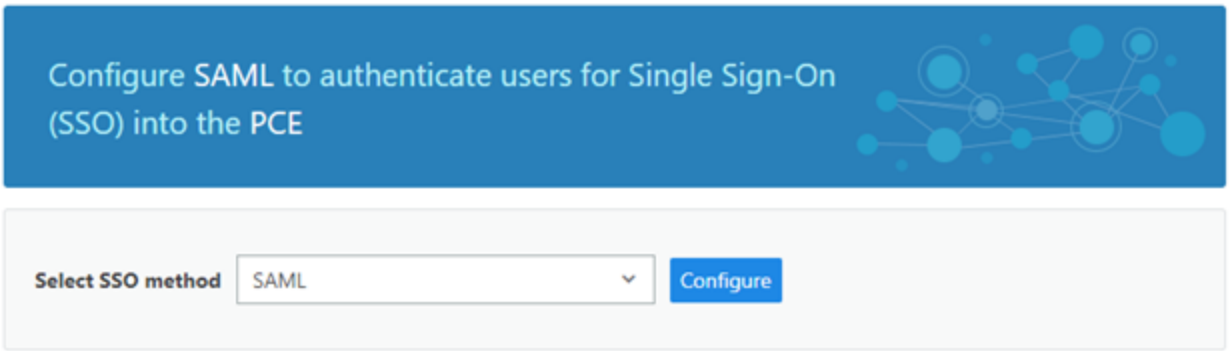
Follow the steps in this section to configure Illumio as an SSO Agent SAML SP to RSA Cloud Authentication Service.

Procedure

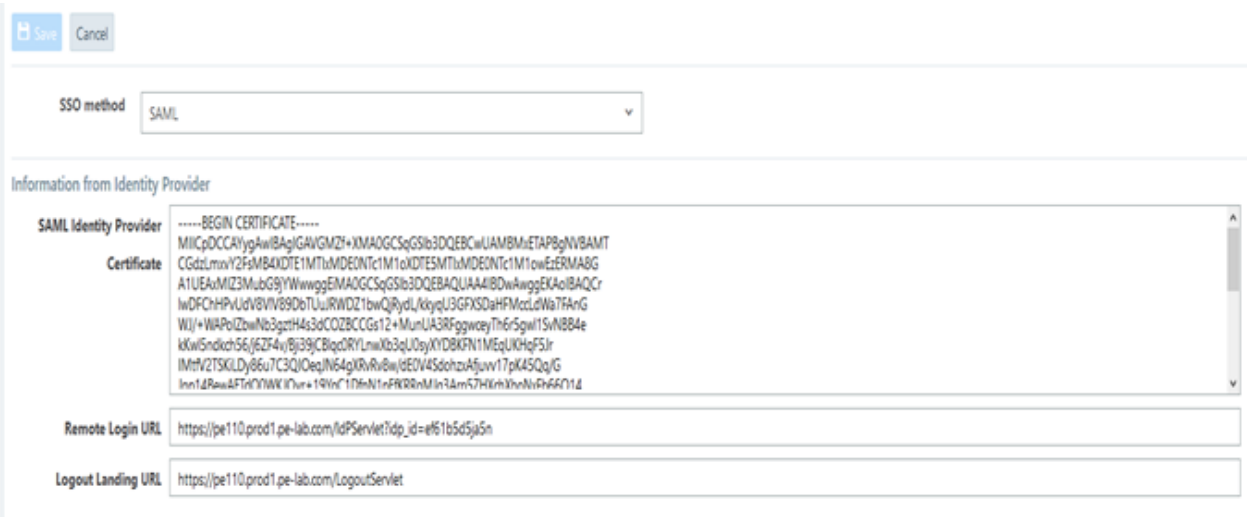
1. Login into the Illumio administration console.
2. Navigate to **Settings > Single Sign-On**.



3. Select **SAML** from the pulldown and then click **Configure**.



4. Click **Edit**.



5. Paste the public certificate in the SAML Identity Provider Certificate field.
6. Enter the **Identity Provider URL** in the **Remote Login URL** field.
7. Enter the **Logout Landing URL**.
8. Click **Save.**

Configuration is complete.

Return to the main page for more certification related information.