



RSA SecurID Access Implementation Guide

Illumio

Gina Salvalzo, RSA Partner Engineering

Last modified: January 21, 2019

Table of Contents

Solution Summary	3
Use Case	3
Integration Types	3
Supported Features	4
Illumio integration with RSA Cloud Authentication Service	4
Illumio integration with RSA Authentication Manager	4
Configuration Summary	5
Known Issues	5
Integration Configuration	6
Relying Party	6
RSA Cloud Authentication Service	6
Illumio	11
SSO Agent - SAML	14
RSA Cloud Authentication Service	14
Illumio	18

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	Authentiacion 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

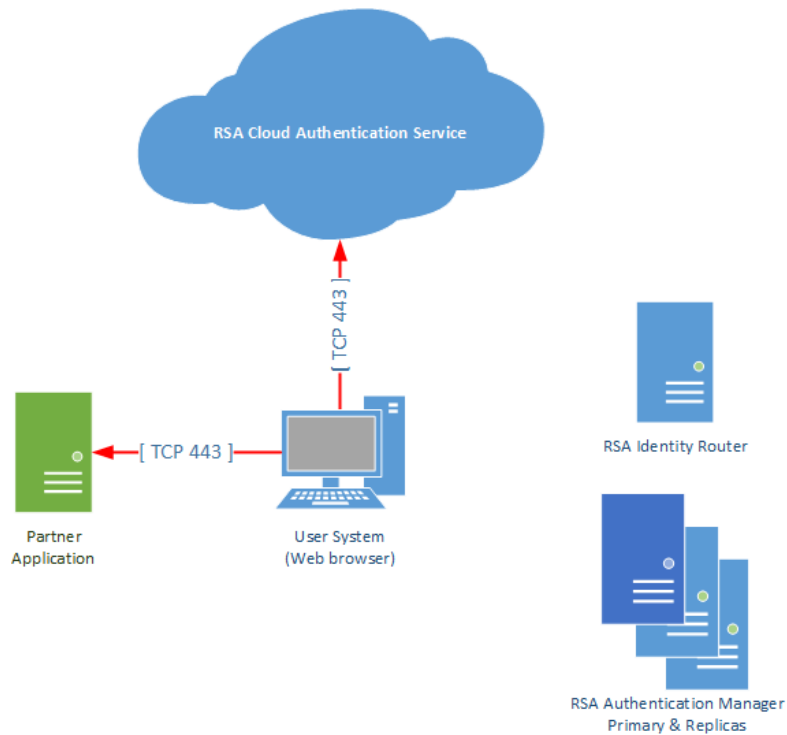
No known issues.

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

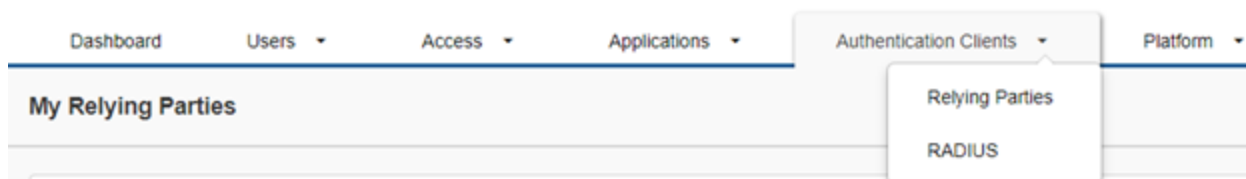


RSA Cloud Authentication Service

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

Procedure

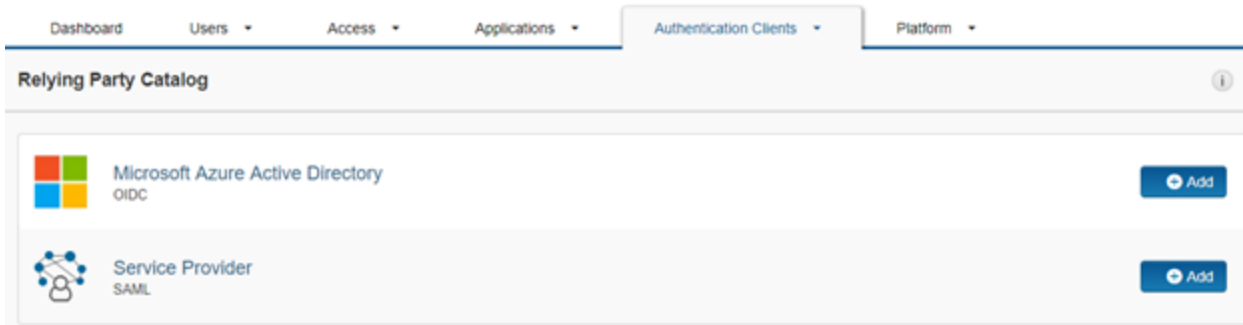
1. Logon to the **RSA Cloud Administrative Console** and browse to **Authentication Clients > Relying Parties** and click **Add a Relying Party**.



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.



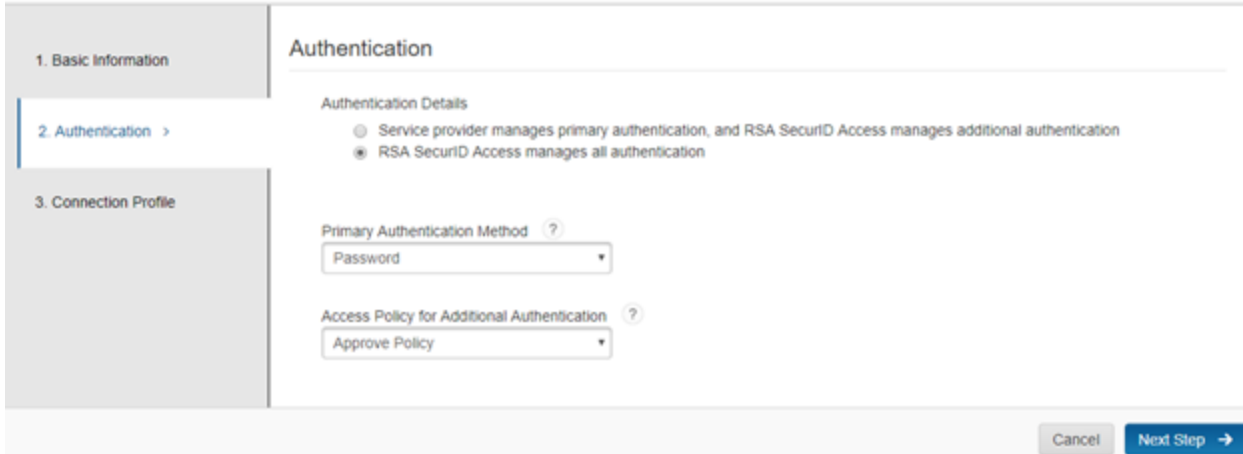
5. Enter a name for the Service Provider in the **Name** field on the Basic Information page.

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**.

Connection Profile

Configure the relationship between RSA SecurID Access acting as the SAML identity provider (IdP), and the application acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP. You can edit these values if necessary. You can also manually add this information.

Data Input Method

Import Metadata

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.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.illum.io/login/acs/<STRING>

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.illum.io/login

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

Message Protection

SP signs SAML requests



No certificate loaded

Choose File



IdP Signs

Assertion within response

Entire SAML response

Download Certificate



15. Select **Download Certificate**.

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

User Identity ?

NameID

Identifier Type

Auto Detect

Property ?

Auto Detect

Attribute Extension ?

Attribute Name	Attribute Source	Property	
User.MemberOf	Identity Source	memberOf	⊖
Email Address	Identity Source	mail	⊖
User.Firstname	Identity Source	givenName	⊖
User.LastName	Identity Source	sn	⊖
+ ADD			

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 Service** is checked.

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

1. Identity Source Details

Click on Refresh Attributes to display the user attributes available from the directory server, and specify which attributes to use for access policy configuration and application access.

2. User Attributes >

Refresh Attributes

3. Synchronize User Attributes

User Attributes

filter

Hide Unavailable Attributes

Synchronize the selected policy attributes with the Cloud Authentication Service ?

Showing 1 - 10 of 10 Results

Directory Server Attribute	Multi-Valued	Attribute Type	Mapping ?	Policies ?	Apps ?
accountExpires		DATETIME		<input checked="" type="checkbox"/>	<input type="checkbox"/>
distinguishedName		STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>
givenName		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
mail		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
objectGUID		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
sAMAccountName		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
sn		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
userAccountControl		LONG		<input checked="" type="checkbox"/>	<input type="checkbox"/>
userPrincipalName		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
virtualGroups	<input checked="" type="checkbox"/>	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>

24. Click **Next Step**.

25. Click **Save and Finish**.

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

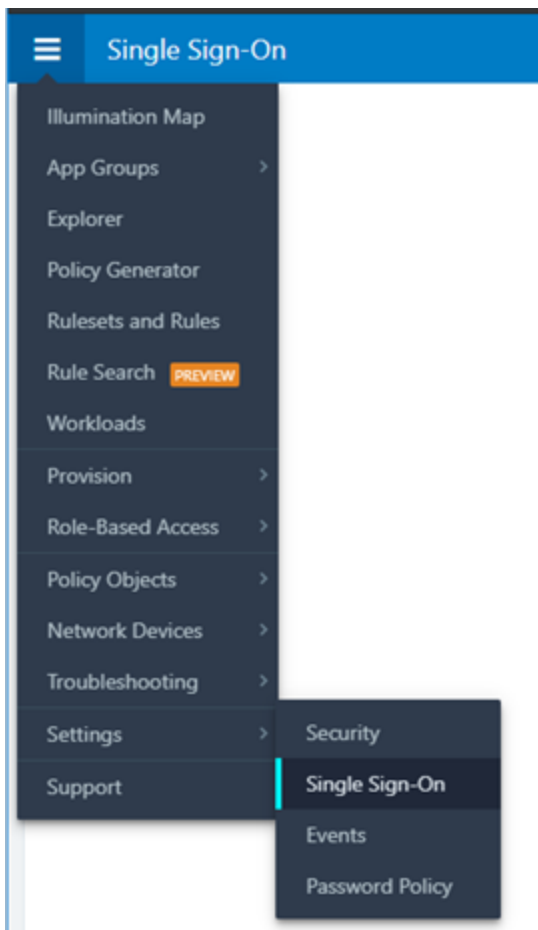
Publish Changes Status: Changes Pending

Illumio

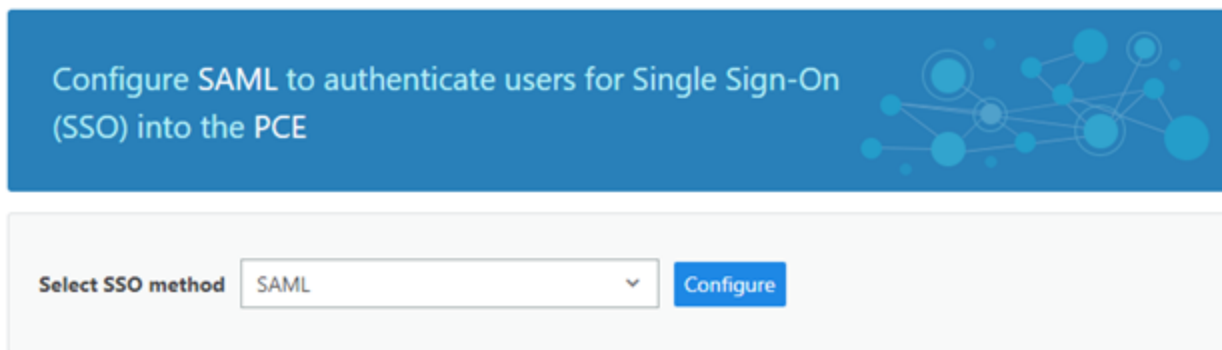
Follow the steps in this section to configure Illumio as a Relying Party SAML SP to RSA Cloud Authentication Service.

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**.

Save
Cancel

SSO method SAML

Information from Identity Provider

SAML Identity Provider	-----BEGIN CERTIFICATE-----
Certificate	MIIEKTCcAxGgAwIBAgIUStMbgBAkv1zoEAzmX2SPpZqPaKYwDQYJKoZIhvcNAQELBQAwgBQxLTArBgNVBAMMJGJIMDc1YTgwLWYxYzQtNDJiZi05YzllLWwYmE1MzlxMmQ1NzETMBEGA1UEBHMKcnNh cGFydGVuZzFJMEcGA1UECQxhZDlmMzU4NmQ5OENIMjkzOWY4OTI2YTRhZjZlZmE1NTMxNjJwNDM5 MDA0OTdmOWMxNGQ1YmRlZjFhYzgzNWE1NTEVMBMGA1UECgwMU0FNTF9TSUdOSU5HMQwwwCgYDVQQQL DANPTkUwHhcNMTCwMzMTk0ODU4WWhcNMzcwMzMTk0ODU4WjCBtDEtMCsGA1UEAwwkYmUwNzVh ODAtZjFjNC00MWNmLTljOWUtYzBiYTUzMTk0ODU4WjZDU3MRMwEQYDVQGEwpcyc2FwYXJ0ZW5nMUkwRwYD VQJDEBkOWYzNTg2ZDk4Y2UyOTM5Zjg5MjZlZjZlZmE1NTEVMBMGA1UECgwMU0FNTF9TSUdOSU5HMQwwwCgYDVQQL ZGVmMWFjODM1YTU1MRUwEwYDVQQKDAxTU1MX1NJR05JTkcxDDAKBgNVBAsMA09ORTCCASlwDQYJ
Remote Login URL	https://rsaparteng.auth-prod0.securid.com/saml-fe/sso
Logout Landing URL	

Information for Identity Provider

Authentication Method	Unspecified
Force Re-authentication	<input type="checkbox"/>
SAML Version	2.0
Issuer	https://trial.illum.io/login
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion Consumer URL	https://trial.illum.io/login/acs/ed4ffc3d-9dc5-4d9f-9740-5efccba1a706
Logout URL	https://trial.illum.io/login/logout/ed4ffc3d-9dc5-4d9f-9740-5efccba1a706

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**.

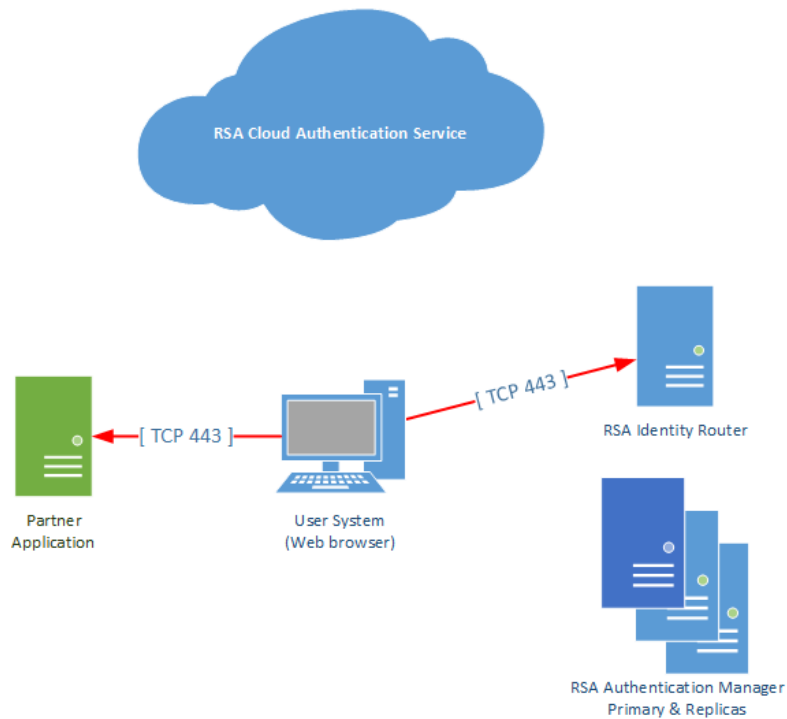
Configuration is complete.

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

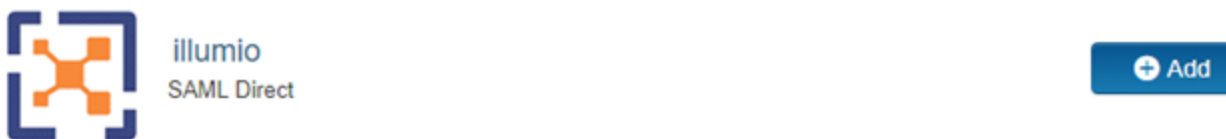


RSA Cloud Authentication Service

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.

Initiate SAML Workflow

Connection URL ?

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?



No certificate loaded

Choose File

Generate Cert Bundle

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

- Default (idp_id): ef61b5d5ja5n
- 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. 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.

Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

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**.

User Identity ?

NameID

Identifier Type

Identity Source

Property ?

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Show Advanced Configuration**.
10. Under Attribute Extension add attributes **Email Address, User.FirstName, User.LastName, User.MemberOf** with their correlated property.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc	Email Address	DefaultIde	mail	
Identity Sc	User.FirstName	DefaultIde	givenName	
Identity Sc	User.LastName	DefaultIde	sn	
Identity Sc	User.MemberOf	DefaultIde	memberOf	
+ ADD				

11. Click **Next Step**.
12. 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 ?

No Access Allowed

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.

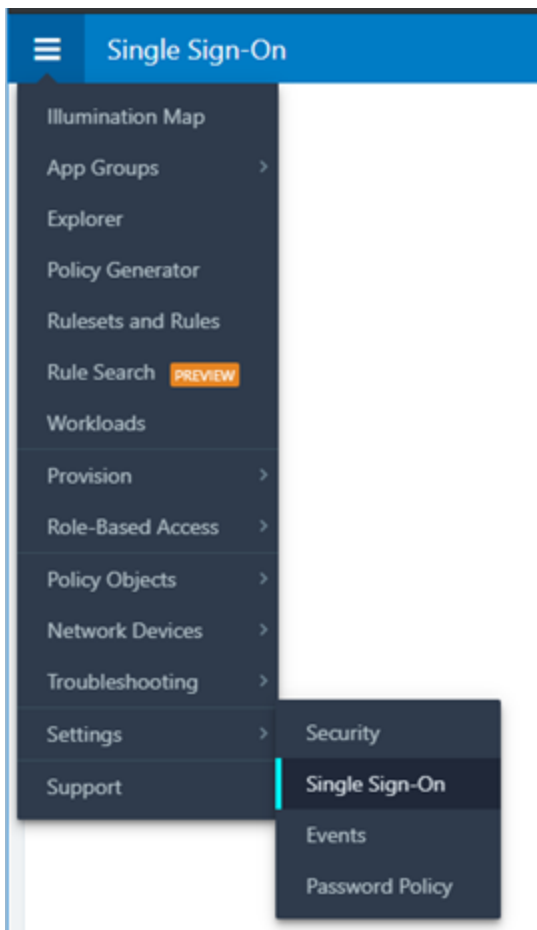
Publish Changes Status:  Changes Pending

Illumio

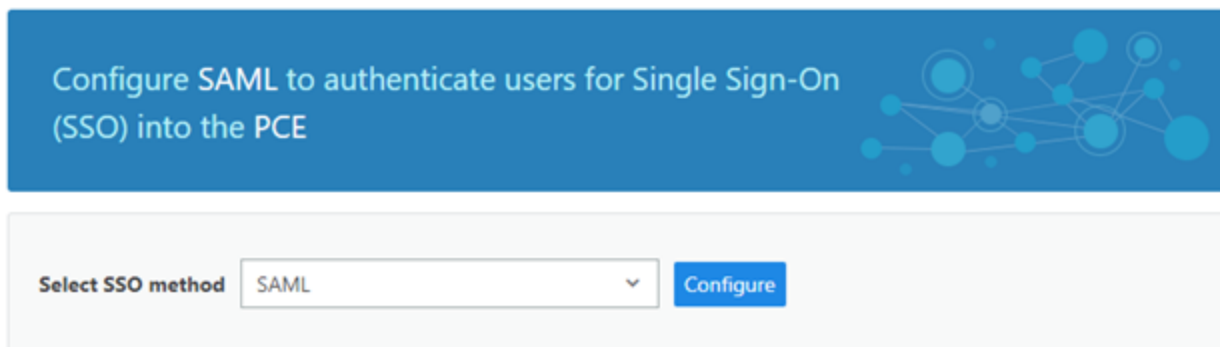
Follow the steps in this section to configure Illumio as an SSO Agent SAML SP to RSA Cloud Authentication Service.

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**.

The screenshot shows a configuration window with a 'Save' button and a 'Cancel' button. Below them is a dropdown menu for 'SSO method' set to 'SAML'. A section titled 'Information from Identity Provider' contains a text area for 'SAML Identity Provider Certificate' with a public certificate key, and two text input fields for 'Remote Login URL' and 'Logout Landing URL'.

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.

