RSA SecurID Access Implementation Guide

Teem

Gina Salvalzo, RSA Partner Engineering

Last modified: January 17, 2019

Teem

Table of Contents

Solution Summary

Use Case

When integrated Teem end users must authenticate with RSA SecurID Access to sign in. Teem can integrate using SAML SSO Agent or Relying Party. Teem 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 Teem using each integration type.

Teem 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	✔	✔

Teem 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 Teem 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 Teem components must be installed and working prior to the integration.

Links

Relying Party

SSO Agent

Known Issues

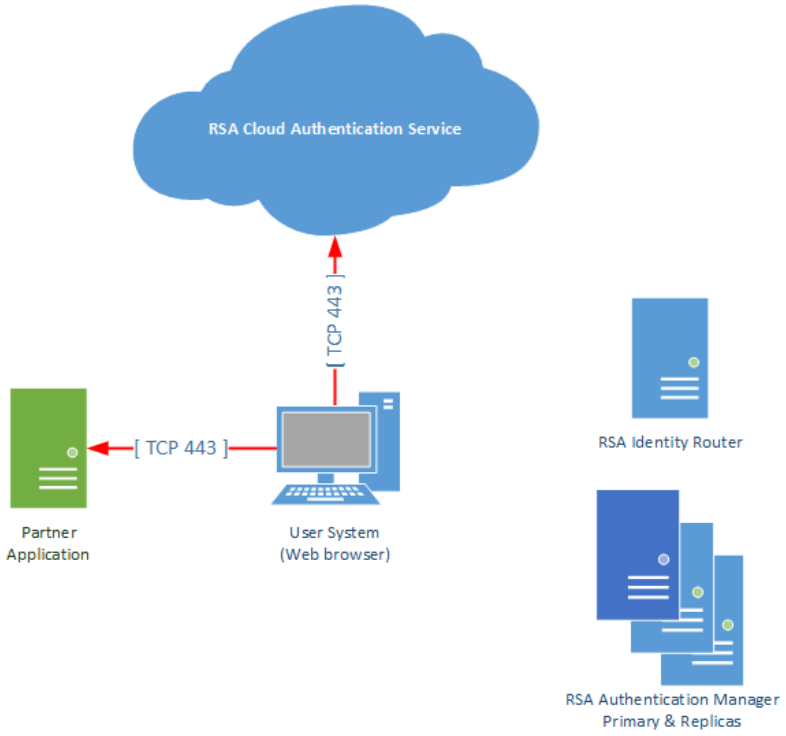
No known issues.

Integration Configuration

Relying Party

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

Architecture Diagram



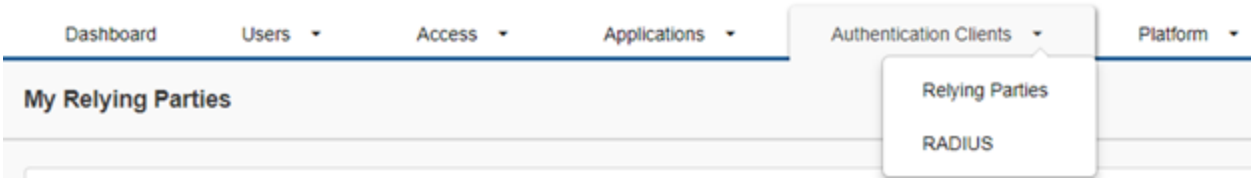
RSA Cloud Authentication Service

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

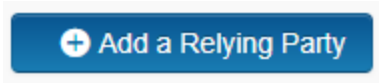
Procedure

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

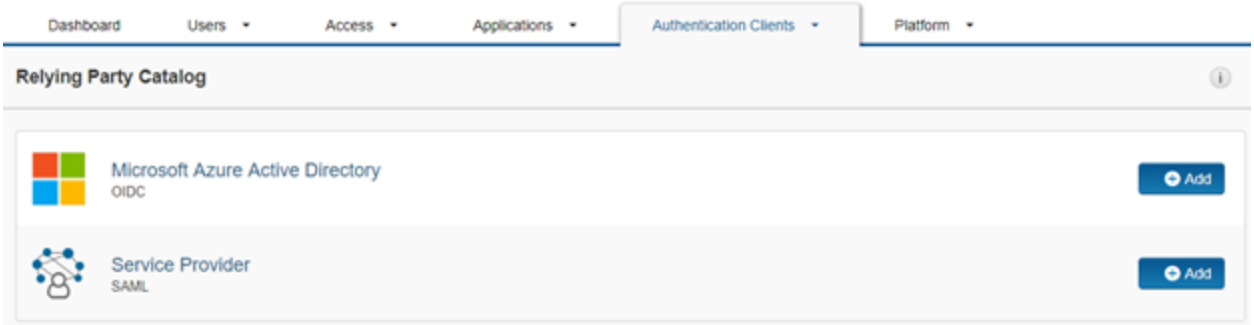
2. Browse to **Authentication Clients** > **Relying Parties** and click **Add a Relying Party**.



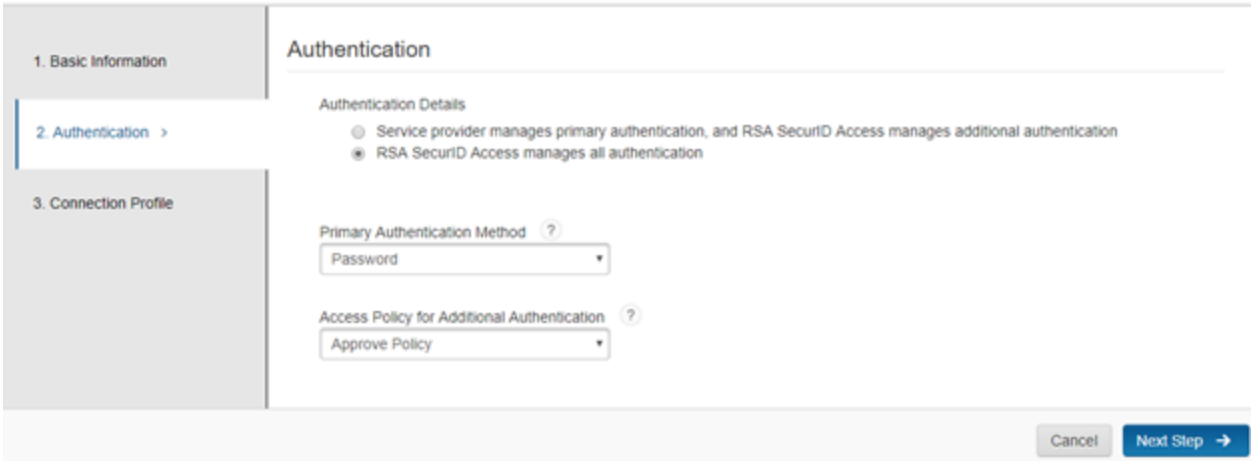
3. Click the **Add a Relying Party** button on the My Relying Parties page.



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

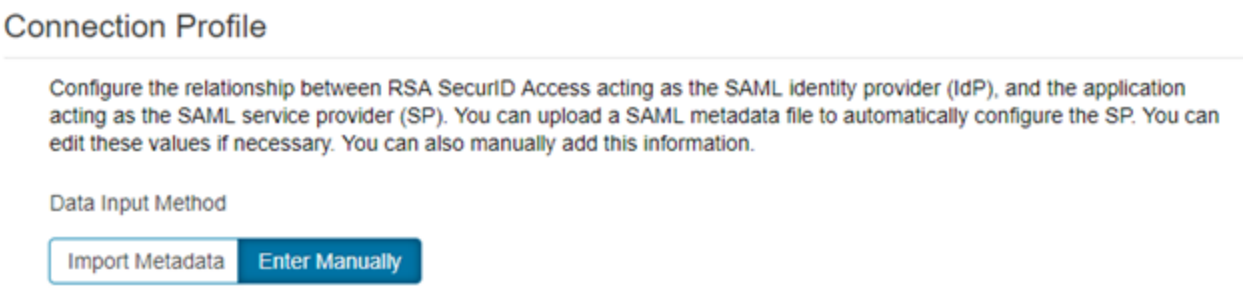


5. Enter a name for the Service Provider in the **Name** field on the Basic Information page.
6. Click the **Next Step** button.
7. On the Authentication page, select **RSA SecurID Access manages all authentication**.
8. From the Primary Authentication Method pulldown, select your desired login method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



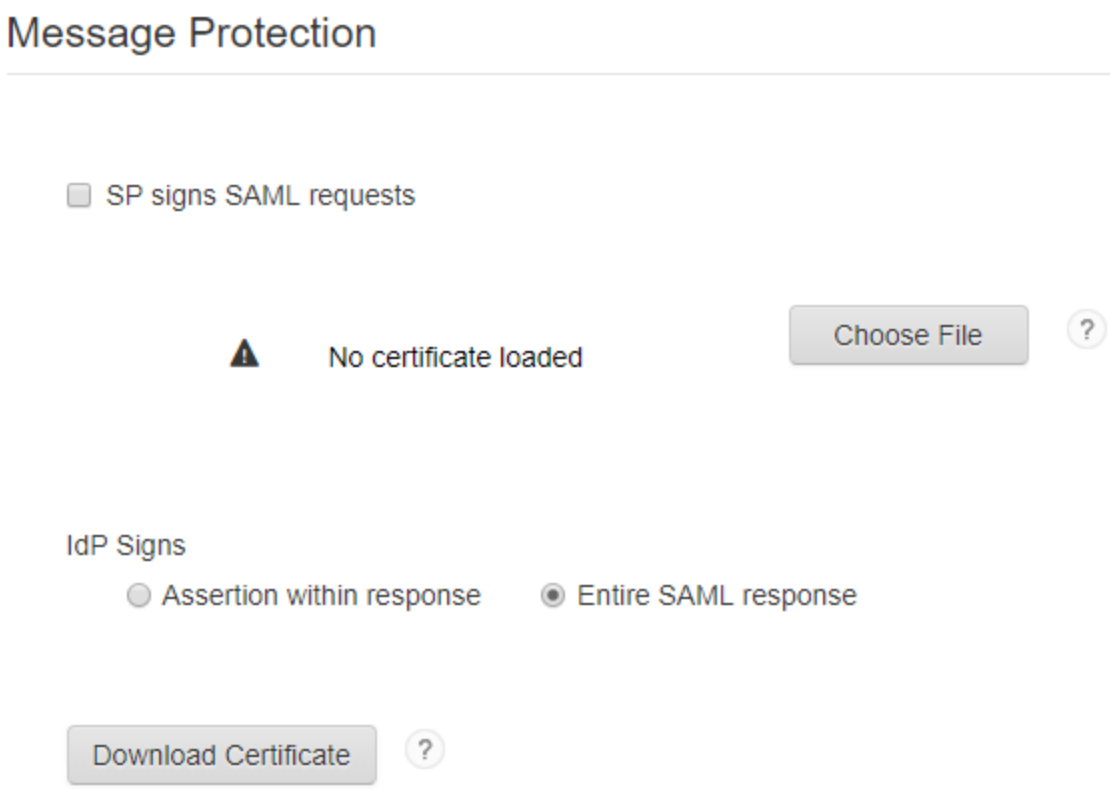
10. Select **Next Step**.

11. Select **Enter Manually**.



12. Enter the **Assertion Consumer Service (ACS) URL**. https://app.teem.com/sso/complete/saml/
13. Enter the **Service Provider Entity ID (Audience)** field. https://teem.com

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



15. Click **Download Certificate**.

16. Select **Show Advanced Configuration**.

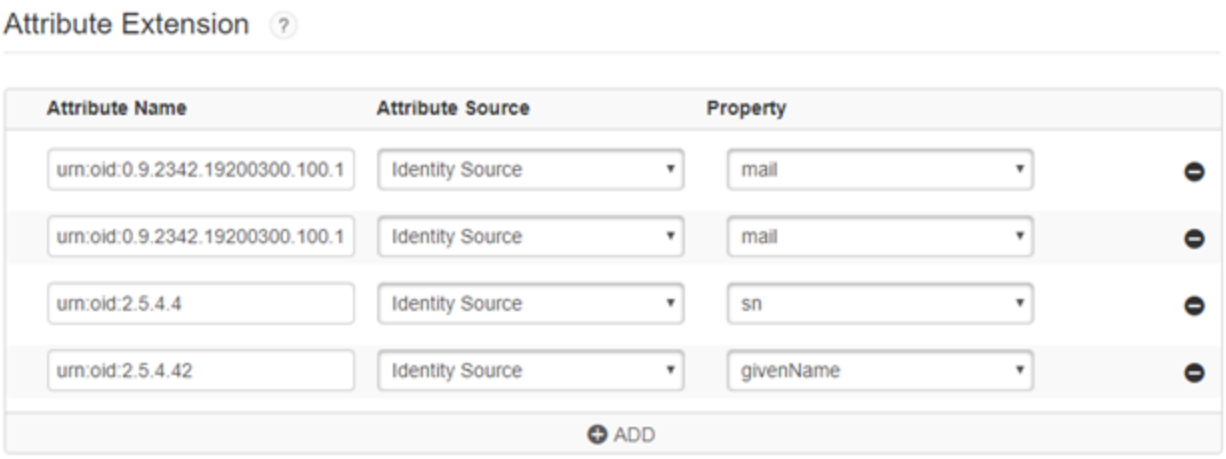
17. Under Attribute Extension enter the following attributes:

urn:oid:0.9.2342.19200300.100.1.1 set to property **mail**

urn:oid:0.9.2342.19200300.100.1.3 set to property **mail**

urn:oid:2.5.4.4 set to property last name, **sn**

urn:oid:2.5.4.42 set to property first name, **givenName**



18. Select **Save and Finish**.

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

20. 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.

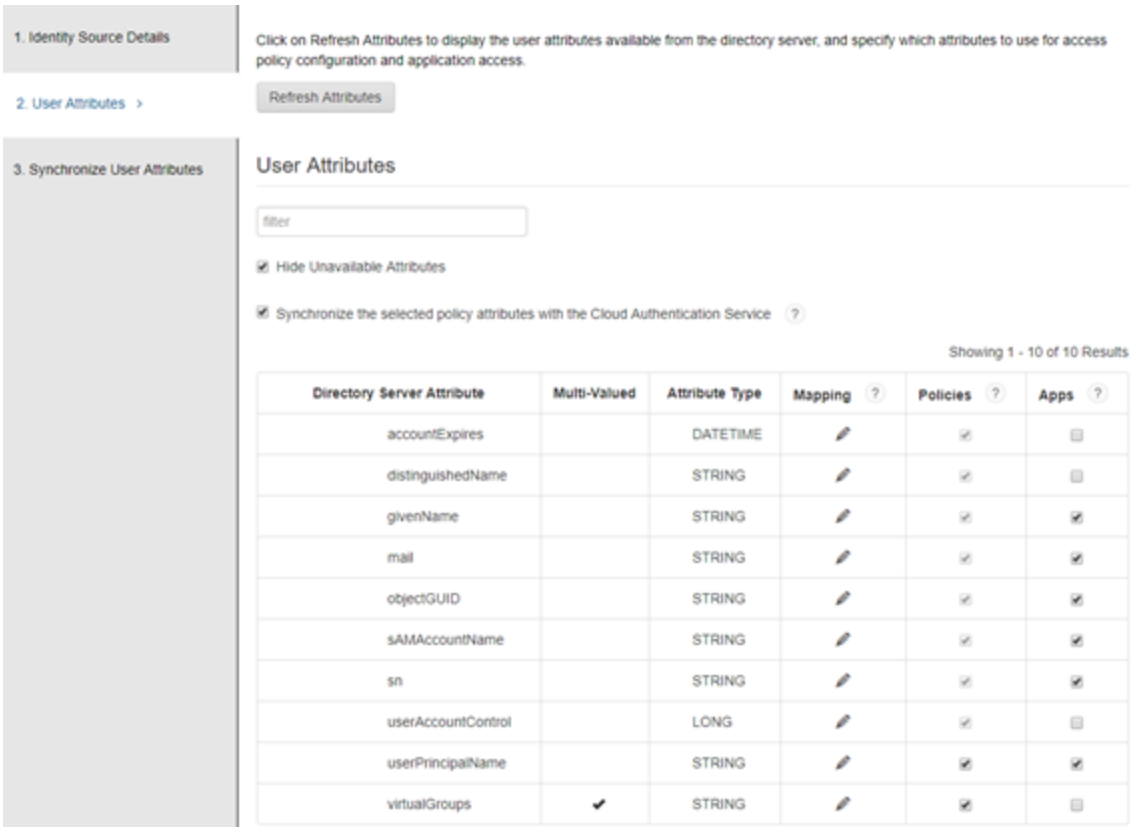
21. Navigate to **Users > Identity Sources**.

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

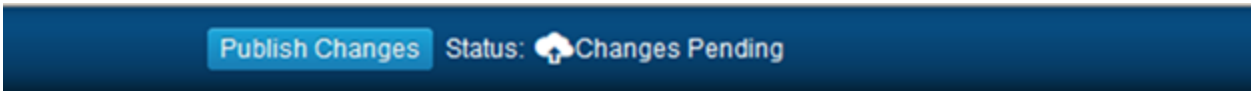
22. Select Edit for the Identity Source used in the Policy.

23. On the User Attributes page, verify that the **Synchronize the selected policy attributes with the Cloud Authentication Service** is checked.

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



25. Click **Next Step**.
26. Click **Save and Finis**h.
27. On the top menu click **Publish Changes**.

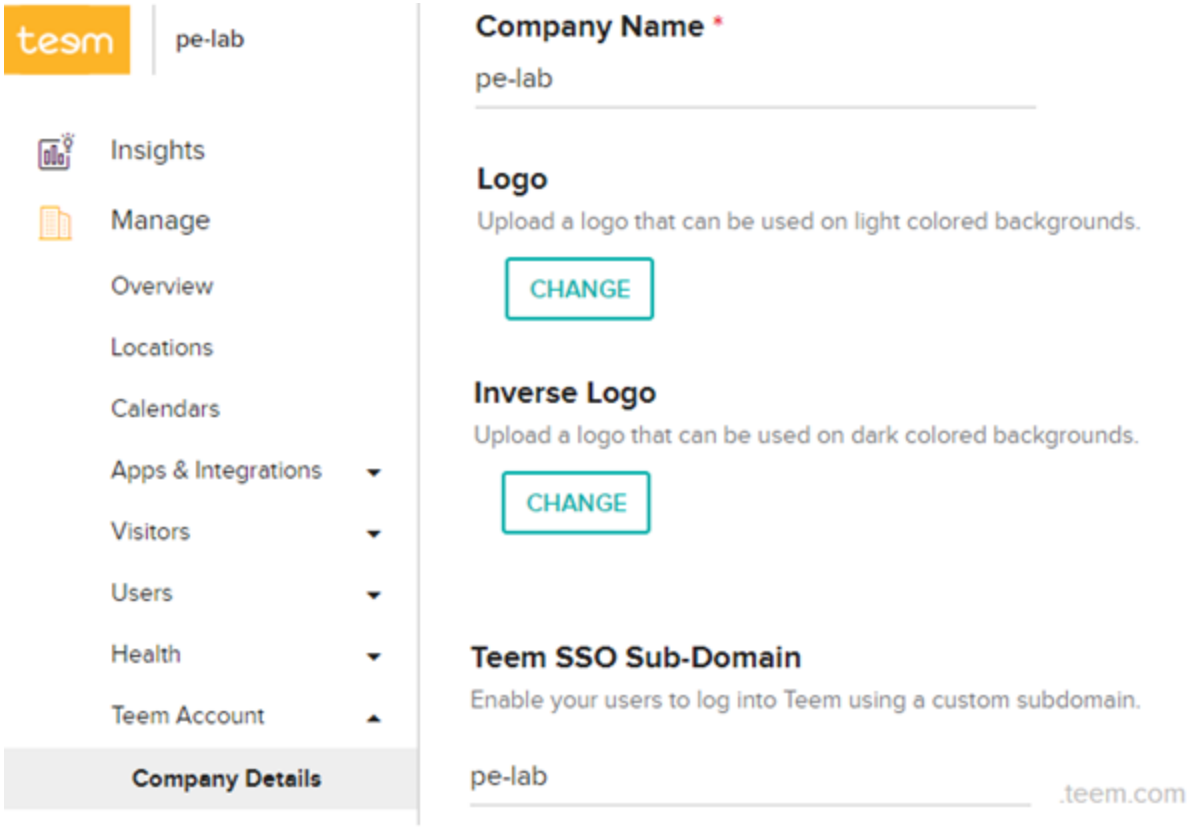


Teem

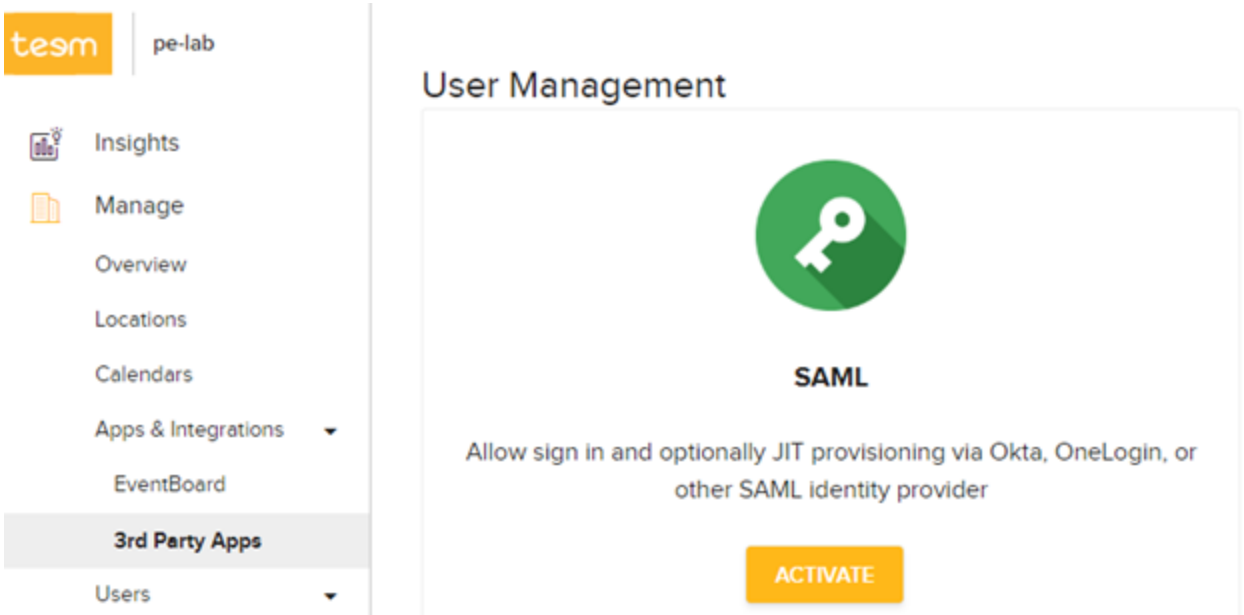
Follow the steps in this section to configure Teem as a Relying Party SAML SP to RSA Cloud Authentication Service.

Procedure

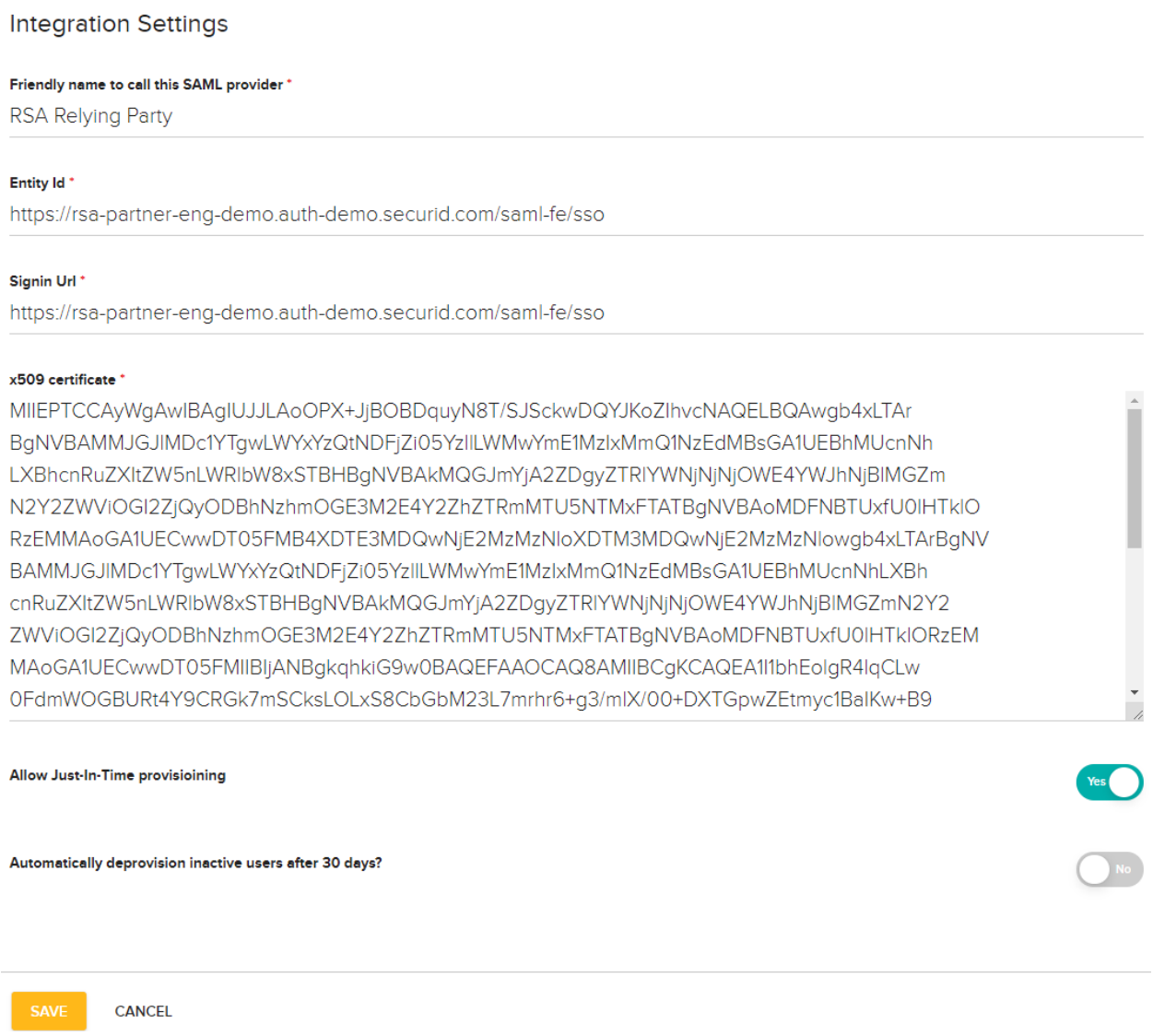
1. Login into the Teem administration console. https://app.teem.com.
2. Create your Teem SSO sub-domain. Navigate to **Manage > Teen Account >Company Details**.
3. Scroll down to **Teem SSO Sub-Domain** and enter a custom subdomain.



4. Navigate to **Manage > Apps & Integrations > 3rd Party Apps**.
5. Scroll down to User Management. Click **ACTIVATE** for the SAML app.



6. The configuration page will open.
7. Enter the name for your SAML Provider.
8. Enter the Cloud IDP URL in the **Entity Id**.
9. Enter the Cloud IDP URL in the **Signin Url** field.
10. Paste the Cloud certificate in the x509 field. Do not include the ---BEGIN and ---END CERTIFICATE markers.
11. Select **Allow Just-In-Time provisioning**.



12. Click **Save.**

Note: SP initiated login URL is https://<domain>.teem.com/login

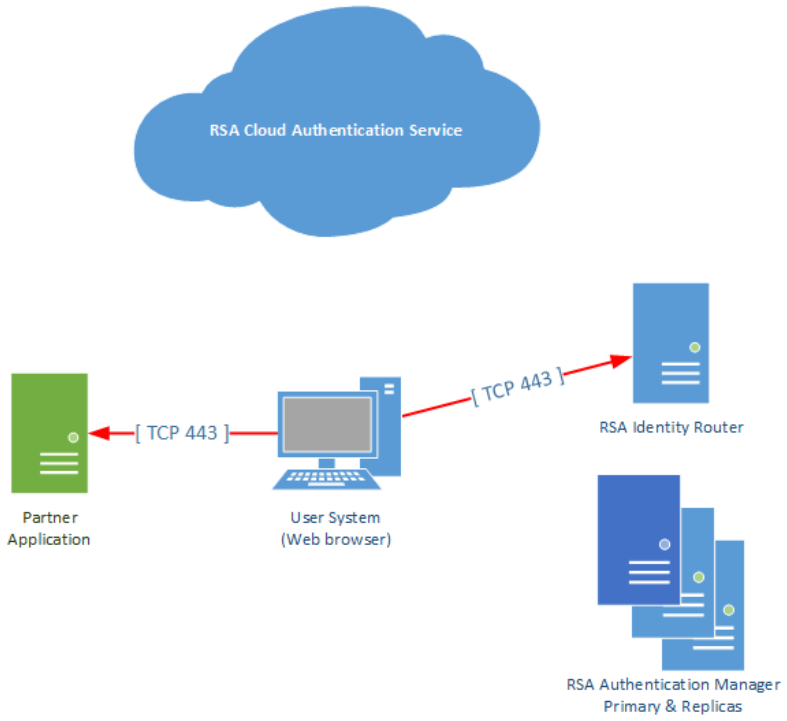
Configuration is complete.

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 Teem Teem 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 Teem.

Procedure

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

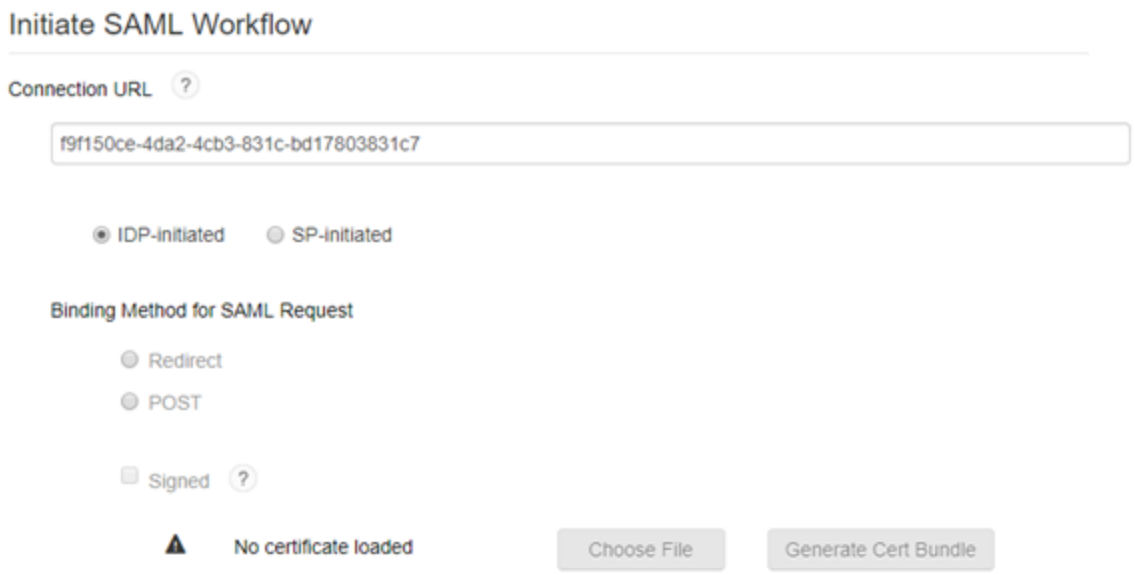
2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.

3. Navigate to Initiate SAML Workflow section.

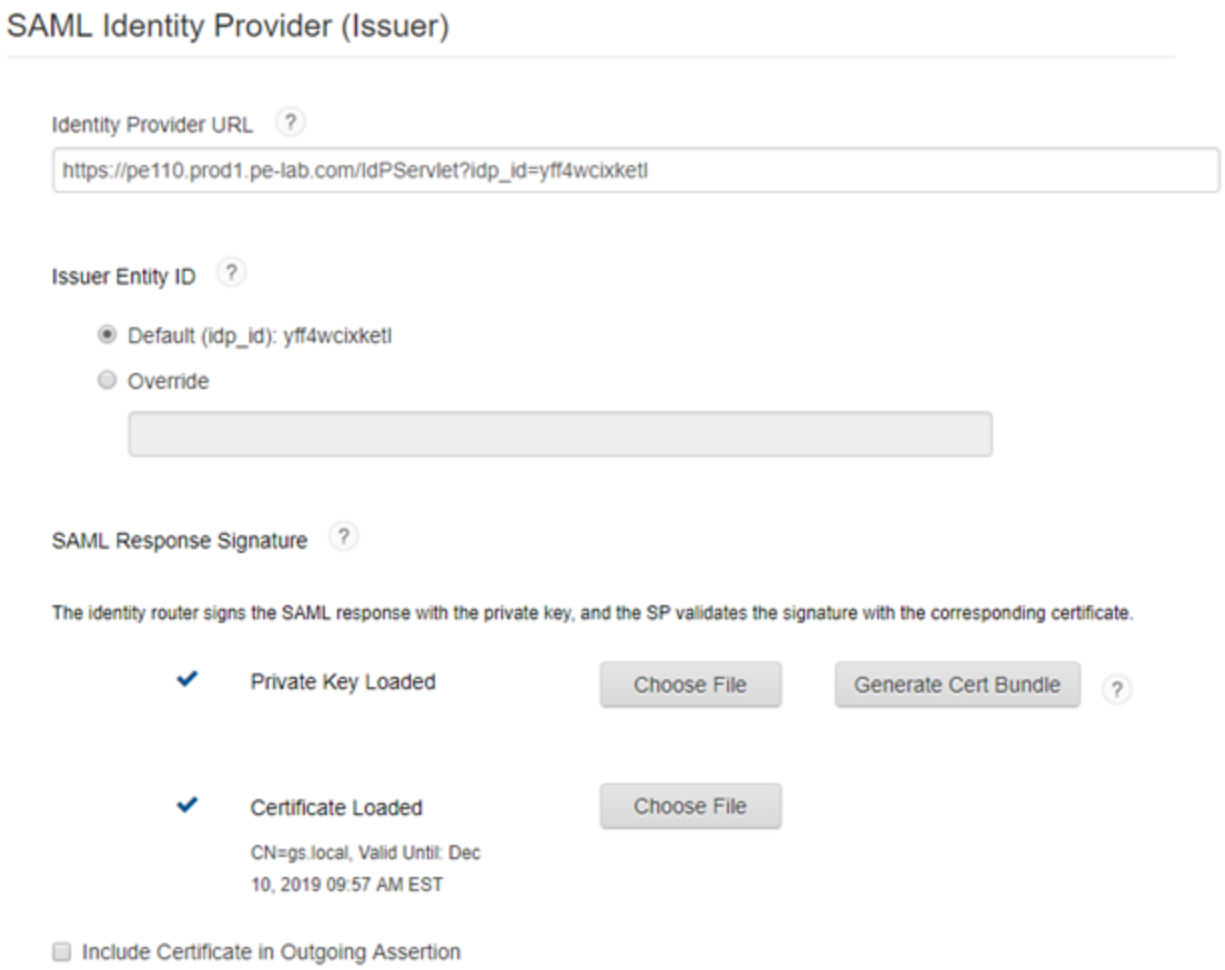
a. In the **Connection URL** field, enter **Uuid** string from the Teem SAML app page.

b. Choose **IDP-initiated**.

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



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



a. Take note of the Identity Provider URL.

b. Take note of the Issuer Entity ID.

b. Select **Choose File** and upload the private key.

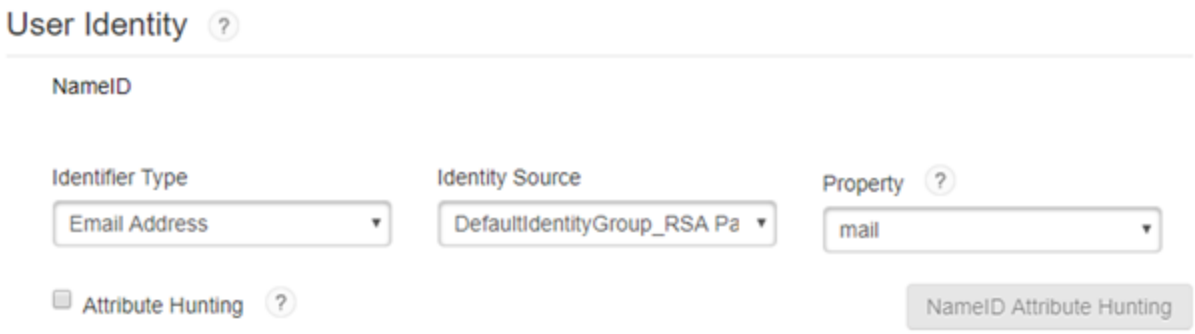
c. Select **Choose File** to import the public signing certificate.

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

6. Verify the **Assertion Consumer Service (ACS) URL**.

7. Verify the **Audience (Service Provider Entity ID)**.

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 **Email Address** with the value of **mail**.



9. Click **Show Advanced Configuration**.

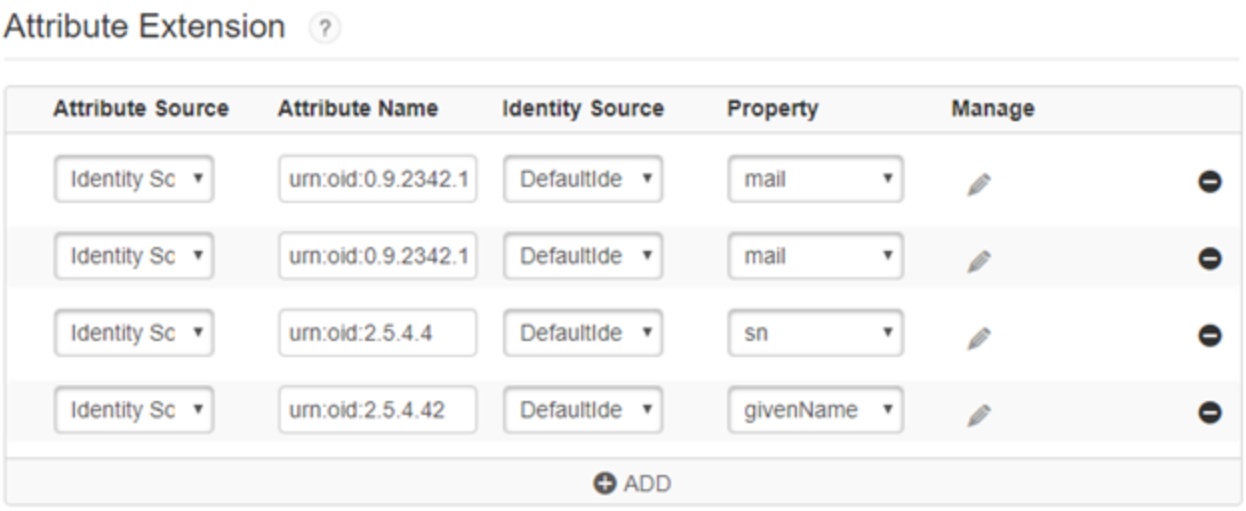
10. Under Attribute Extension enter the following attributes:

urn:oid:0.9.2342.19200300.100.1.1 set to property **mail**

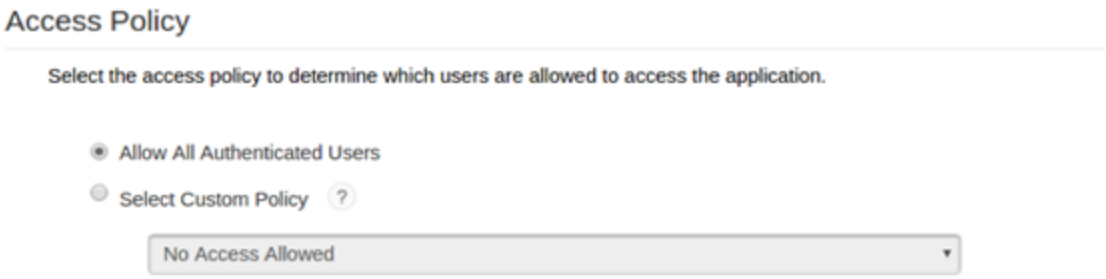
urn:oid:0.9.2342.19200300.100.1.3 set to property **mail**

urn:oid:2.5.4.4 set to property last name, **sn**

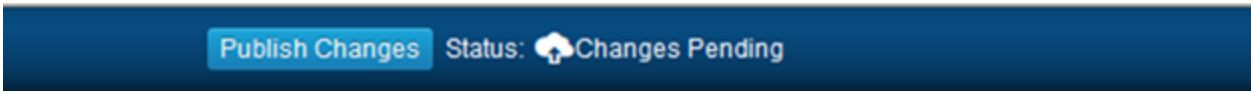
urn:oid:2.5.4.42 set to property first name, **givenName**



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.

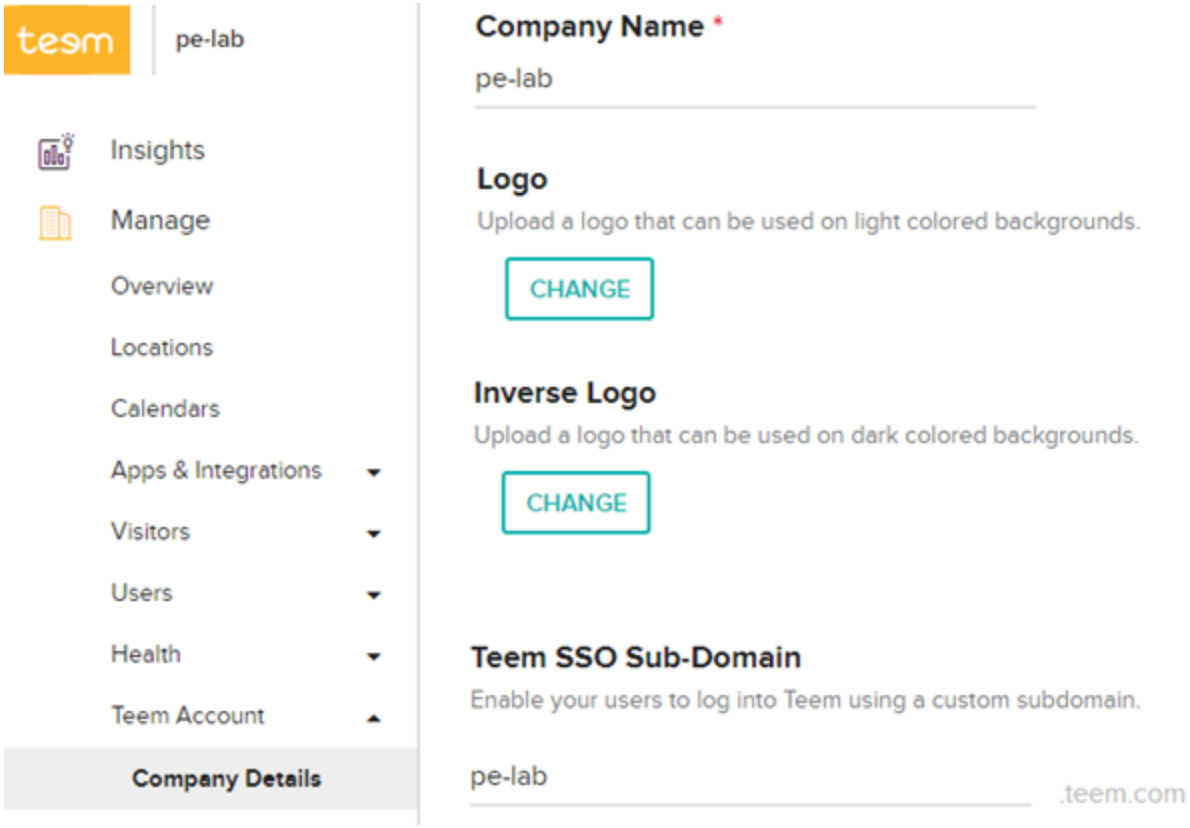


Teem

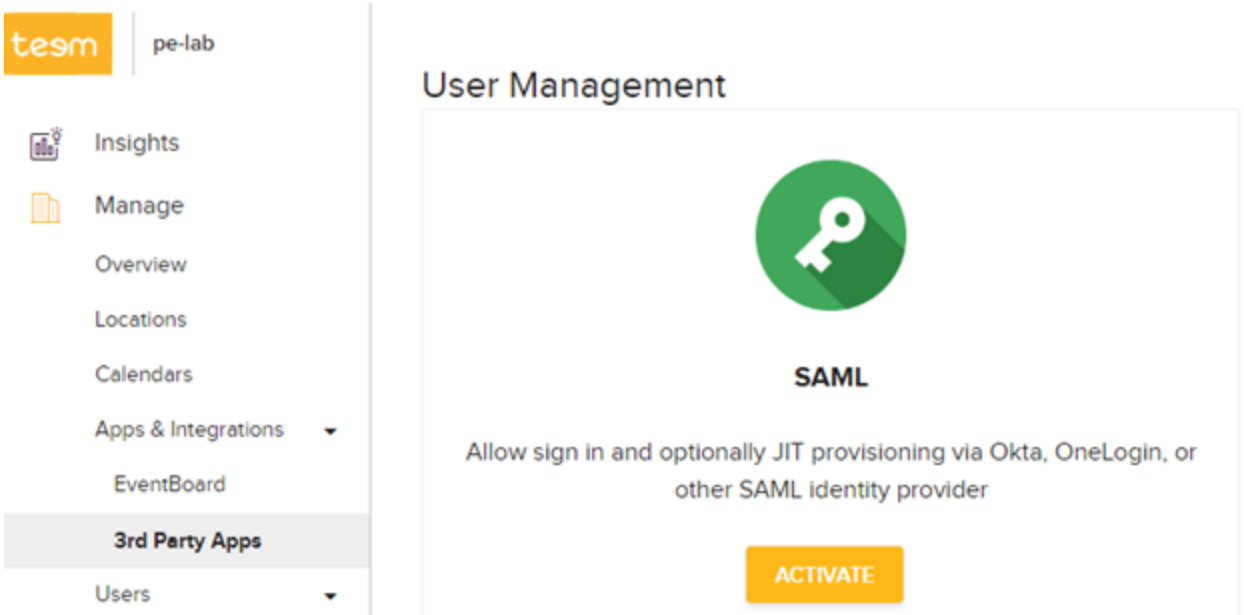
Follow the steps in this section to configure Teem as an SSO Agent SAML SP to RSA Cloud Authentication Service.

Procedure

1. Login into the Teem administration console. https://app.teem.com.
2. Create your Teem SSO sub-domain. Navigate to **Manage > Teen Account >Company Details**.
3. Scroll down to **Teem SSO Sub-Domain** and enter a custom subdomain.



4. Navigate to **Manage > Apps & Integrations > 3rd Party Apps**.
5. Scroll down to User Management. Click **ACTIVATE** for the SAML app.



6. The configuration page will open.

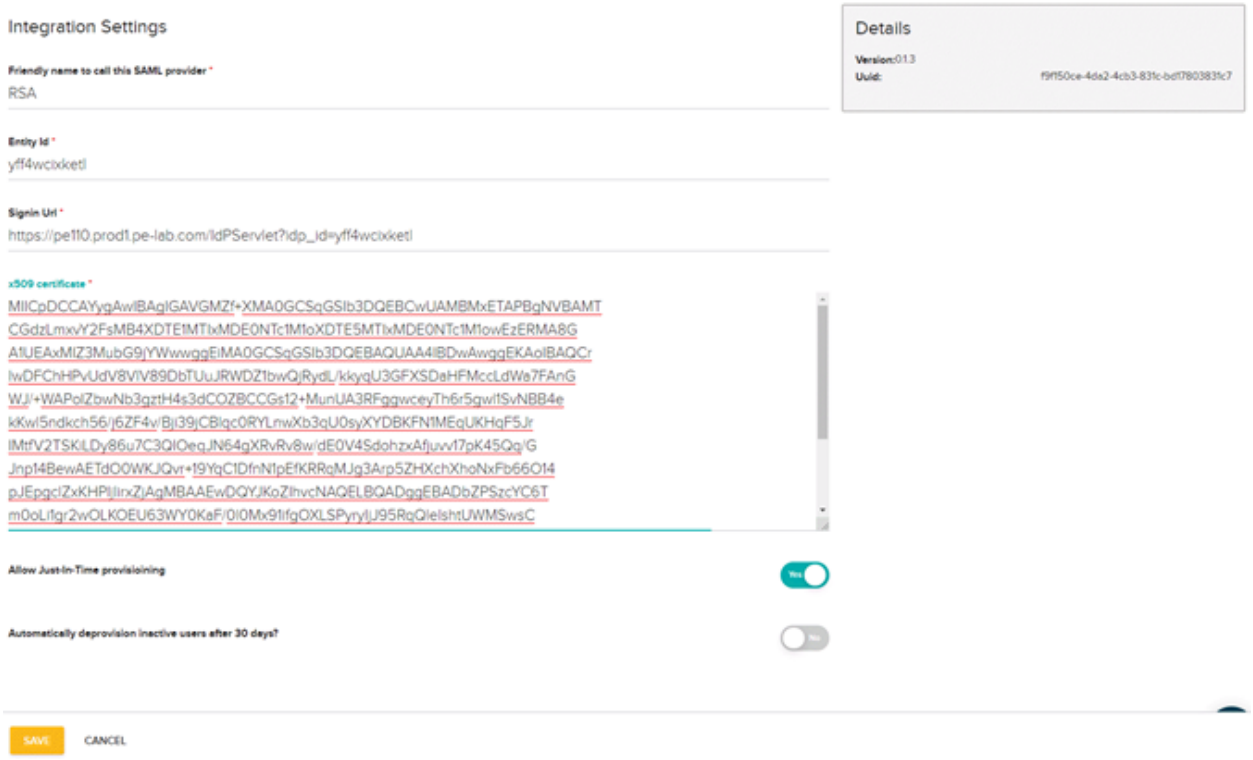
7. Enter the name for your SAML Provider.

8. Enter the Issuer Entity ID in the **Entity Id.**

9. Enter the Identity Provider URL in the **Signin Url** field.

10. Paste the public certificate in the x509 field. Do not include the ---BEGIN and ---END CERTIFICATE markers.

11. Select **Allow Just-In-Time provisioning**.



12. Click **Save.**

13. Copy the **Uuid** string from the Details window. Paste the Uuid into the RSA Connection URL field.

Configuration is complete.

Return to the main page for more certification related information.