



RSA SecurID Access Implementation Guide

Team

Gina Salvalzo, RSA Partner Engineering

Last modified: January 17, 2019

Teem

Table of Contents

Teem	2
Solution Summary	3
Use Case	3
Integration Types	3
Supported Features	4
Teem integration with RSA Cloud Authentication Service	4
Teem integration with RSA Authentication Manager	4
Configuration Summary	5
Known Issues	5
Integration Configuration	6
Relying Party	6
RSA Cloud Authentication Service	6
Teem	11
SSO Agent - SAML	15
RSA Cloud Authentication Service	15
Teem	19

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	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 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

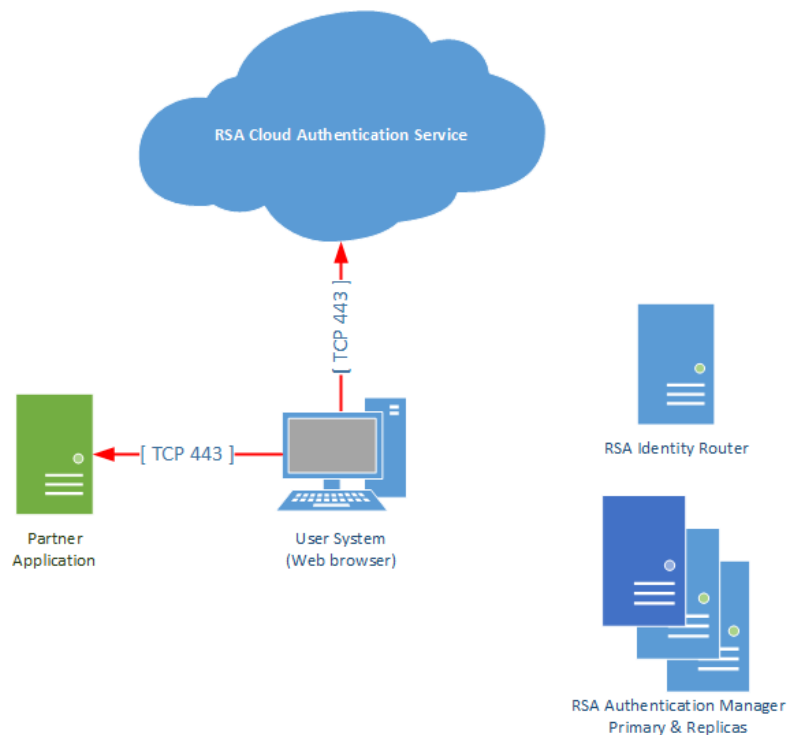
No known issues.

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

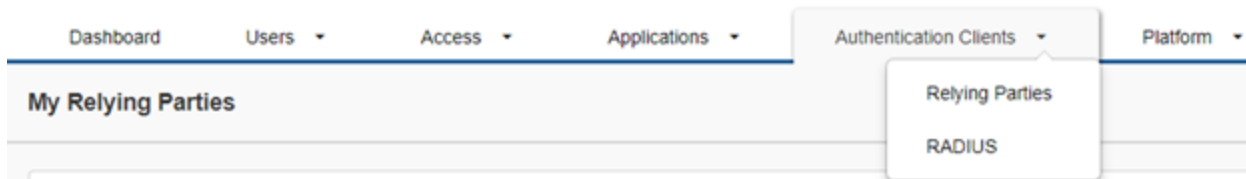


RSA Cloud Authentication Service

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

Procedure

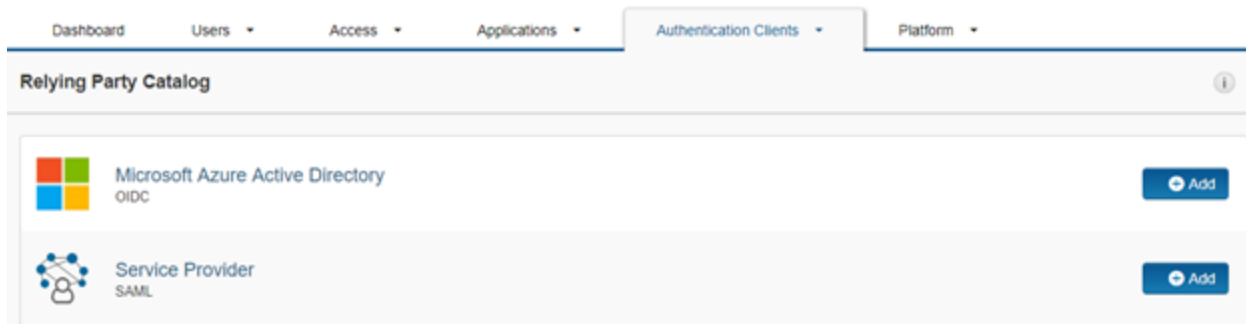
1. Logon to the **RSA Cloud Administrative Console** and browse to **Authentication Clients > Relying Parties** and click **Add a Relying Party**.
2. Browse to **Authentication Clients > Relying Parties** and click **Add a Relying Party**.



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.



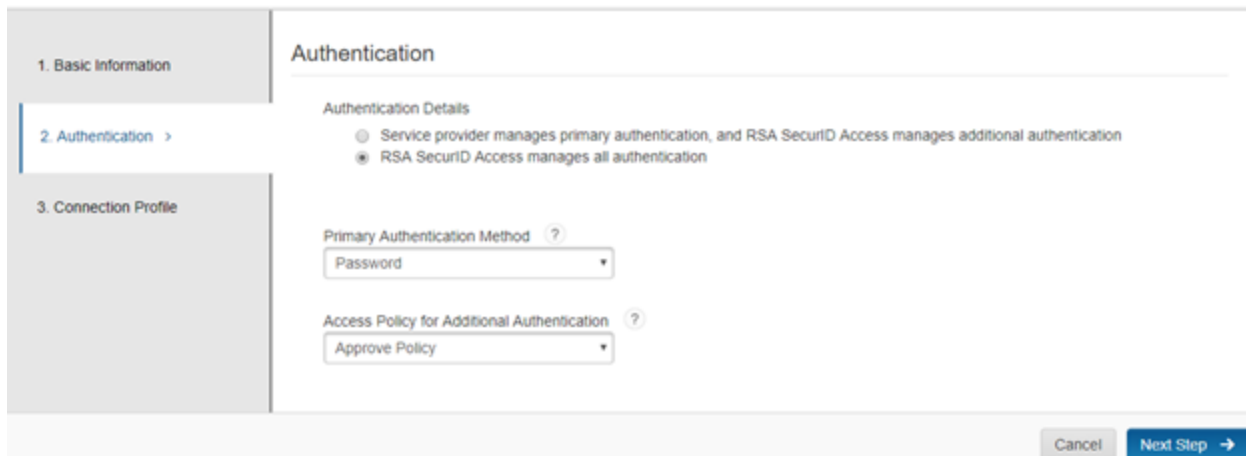
5. Enter a name for the Service Provider in the **Name** field on the Basic Information page.

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**.

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**. <https://app.teem.com/sso/complete/saml/>
13. Enter the **Service Provider Entity ID (Audience)** field. <https://teem.com>

Service Provider Metadata

Assertion Consumer Service (ACS) URL ?

Service Provider Entity ID ?

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. 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**

Attribute Extension ?

Attribute Name	Attribute Source	Property	
urn:oid:0.9.2342.19200300.100.1	Identity Source	mail	⊖
urn:oid:0.9.2342.19200300.100.1	Identity Source	mail	⊖
urn:oid:2.5.4.4	Identity Source	sn	⊖
urn:oid:2.5.4.42	Identity Source	givenName	⊖
+ ADD			

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.

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"/>

25. Click **Next Step**.

26. Click **Save and Finish**.

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

Publish Changes Status: Changes Pending

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.

The screenshot shows the Teem user interface. On the left is a navigation menu with the 'teem' logo and 'pe-lab' text. The menu items are: Insights, Manage, Overview, Locations, Calendars, Apps & Integrations (with a dropdown arrow), Visitors (with a dropdown arrow), Users (with a dropdown arrow), Health (with a dropdown arrow), and Teem Account (with an up arrow). The 'Company Details' item is highlighted in a grey bar. The main content area is titled 'Company Name *' and shows 'pe-lab' in a text input field. Below this is the 'Logo' section with the instruction 'Upload a logo that can be used on light colored backgrounds.' and a 'CHANGE' button. The 'Inverse Logo' section has the instruction 'Upload a logo that can be used on dark colored backgrounds.' and another 'CHANGE' button. The 'Teem SSO Sub-Domain' section has the instruction 'Enable your users to log into Teem using a custom subdomain.' and shows 'pe-lab' in a text input field followed by '.teem.com'.

4. Navigate to **Manage > Apps & Integrations > 3rd Party Apps**.

5. Scroll down to User Management. Click **ACTIVATE** for the SAML app.

The screenshot shows the Teem user interface with the '3rd Party Apps' menu item highlighted in the left navigation bar. The main content area is titled 'User Management' and features a large green circular icon with a white key symbol. Below the icon is the text 'SAML'. Underneath, it says 'Allow sign in and optionally JIT provisioning via Okta, OneLogin, or other SAML identity provider'. At the bottom of this section is a yellow 'ACTIVATE' button.

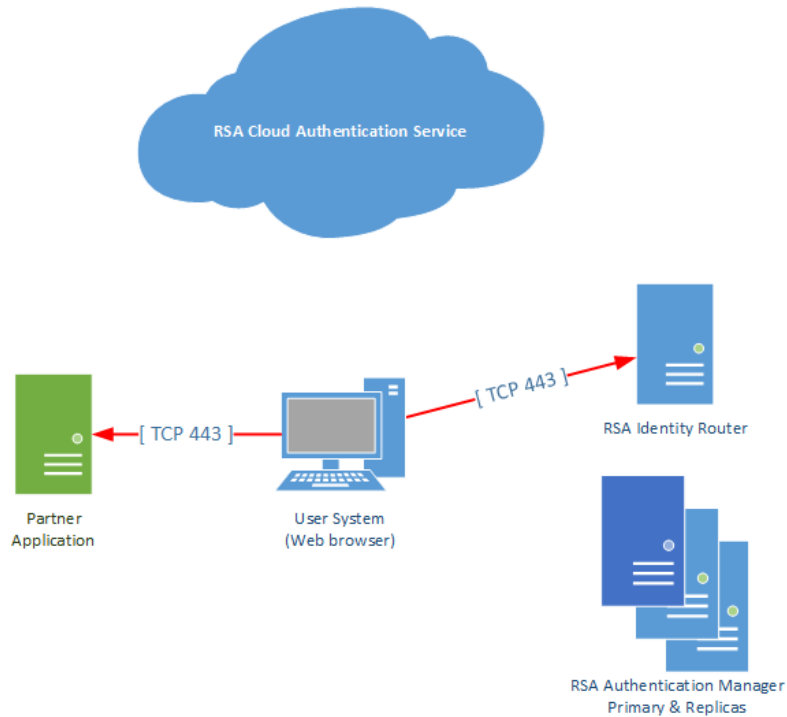
Configuration is complete.

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.

Initiate SAML Workflow

Connection URL ?

f9f150ce-4da2-4cb3-831c-bd17803831c7

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 ?

https://pe110.prod1.pe-lab.com/IdPServlet?idp_id=yff4wcixketl

Issuer Entity ID ?

Default (idp_id): yff4wcixketl

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

Choose File

Generate Cert Bundle

?

Certificate Loaded

Choose File

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. 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.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://app.teem.com/sso/complete/saml/

Audience (Service Provider Entity ID) ?

https://teem.com

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**.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

DefaultIdentityGroup_RSA Pa

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

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**

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc ▾	urn:oid:0.9.2342.1	DefaultIde ▾	mail ▾	 
Identity Sc ▾	urn:oid:0.9.2342.1	DefaultIde ▾	mail ▾	 
Identity Sc ▾	urn:oid:2.5.4.4	DefaultIde ▾	sn ▾	 
Identity Sc ▾	urn:oid:2.5.4.42	DefaultIde ▾	givenName ▾	 

 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.



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.

The screenshot shows the Teem user interface. On the left is a navigation menu with the 'teem' logo and 'pe-lab' text. The menu items are: Insights, Manage, Overview, Locations, Calendars, Apps & Integrations (with a dropdown arrow), Visitors (with a dropdown arrow), Users (with a dropdown arrow), Health (with a dropdown arrow), and Teem Account (with an up arrow). The 'Company Details' item is highlighted in a grey bar. The main content area on the right has the following sections:

- Company Name ***: A text input field containing 'pe-lab'.
- Logo**: A section with the instruction 'Upload a logo that can be used on light colored backgrounds.' and a teal 'CHANGE' button.
- Inverse Logo**: A section with the instruction 'Upload a logo that can be used on dark colored backgrounds.' and a teal 'CHANGE' button.
- Teem SSO Sub-Domain**: A section with the instruction 'Enable your users to log into Teem using a custom subdomain.' and a text input field containing 'pe-lab' followed by '.teem.com'.

4. Navigate to **Manage > Apps & Integrations > 3rd Party Apps**.

5. Scroll down to User Management. Click **ACTIVATE** for the SAML app.

The screenshot shows the Teem user interface with the '3rd Party Apps' menu item highlighted in the left navigation bar. The main content area is titled 'User Management' and features a large green circular icon with a white key symbol. Below the icon, the text reads 'SAML' and 'Allow sign in and optionally JIT provisioning via Okta, OneLogin, or other SAML identity provider'. At the bottom of this section is a prominent yellow 'ACTIVATE' button.

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.

