

RSA SECURID[®] ACCESS

Implementation Guide

ScaleFT

Gina Salvazo, RSA Partner Engineering
Last Modified: November 2, 2018

Solution Summary

ScaleFT is an access management platform that offers cloud-native Zero Trust security solution. ScaleFT supports multi-factor authentication through SAML 2.0 via the service-provider login page or the RSA identity provider portal.

SAML 2.0 integrations have two specific use cases:

1. When integrated with Identity Router (IDR IDP), RSA provides single sign-on authentication and multi-factor authentication to ScaleFT via SP or IDP initiated login. JIT provisioning is supported.
2. When integrated with Cloud IDP/ Relying Party, RSA provides both the primary authentication and the multi-factor authentication to protect the ScaleFT login page. JIT provisioning is supported.

RSA SecurID Access Features	
ScaleFT	
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

All of the supported use cases of RSA SecurID Access with ScaleFT 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 – ScaleFT can be integrated with RSA Cloud Authentication Service in the following ways:

SAML via RSA Identity Router (IdP)

[Cloud Authentication Service – Identity Router IdP Configuration
ScaleFT SAML Configuration](#)

SAML via RSA Cloud (IdP)

[Cloud Authentication Service – Cloud IdP Configuration
ScaleFT 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 ScaleFT 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 ScaleFT and click **+Add** to add the connector.



ScaleFT
SAML Direct

+ Add

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 ScaleFT connections as well.

Initiate SAML Workflow

Connection URL ?

http://www.example.com

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): sctest

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. Select **Override** and paste the Identity Provider URL into the Issuer Entity ID field.
- c. Select **Choose File** and upload the private key.
- d. Select **Choose File** to import the public signing certificate.
- e. 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. Verify the [Assertion Consumer Service \(ACS\) URL](#) field.
7. In the [Audience \(Service Provider Entity ID\)](#) field replace **<TEAM>** with your team name.
8. Scroll down to the User Identity section and select **persistent** from the Identifier Type pulldown. 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 **FirstName**, **LastName**, **Email**, and **Login** with the correlating value from your Active Directory.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
<input type="text" value="Identity Sc"/>	<input type="text" value="FirstName"/>	<input type="text" value="PE77"/>	<input type="text" value="givenName"/>	
<input type="text" value="Identity Sc"/>	<input type="text" value="LastName"/>	<input type="text" value="PE77"/>	<input type="text" value="sn"/>	
<input type="text" value="Identity Sc"/>	<input type="text" value="Login"/>	<input type="text" value="PE77"/>	<input type="text" value="mail"/>	
<input type="text" value="Identity Sc"/>	<input type="text" value="Email"/>	<input type="text" value="PE77"/>	<input type="text" value="mail"/>	
ADD				

- Under Uncommon Formatting SAML Response Options, set Signature Algorithm to **rsa-sha256** and Digest Algorithm to **sha256**.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response Assertion within response

Signature Algorithm

Digest Algorithm

- 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

Next Steps

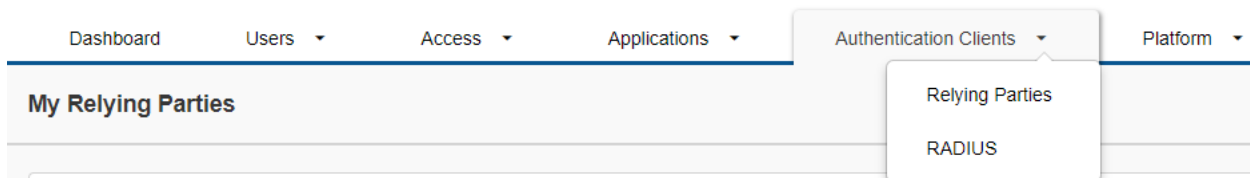
[ScaleFT SAML Configuration](#)

SAML via RSA Cloud (IdP)

To configure a SAML Service Provider in RSA Cloud IdP, you must add a Service Provider 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.

Procedure

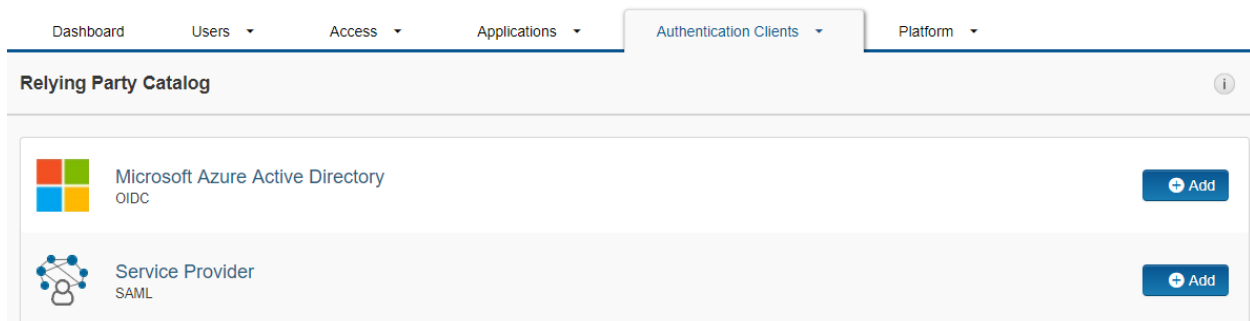
1. Log in to the RSA SecurID Access Administration Console.
2. Select the **Authentication Clients > Relying Parties** menu item at the top of the page.



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

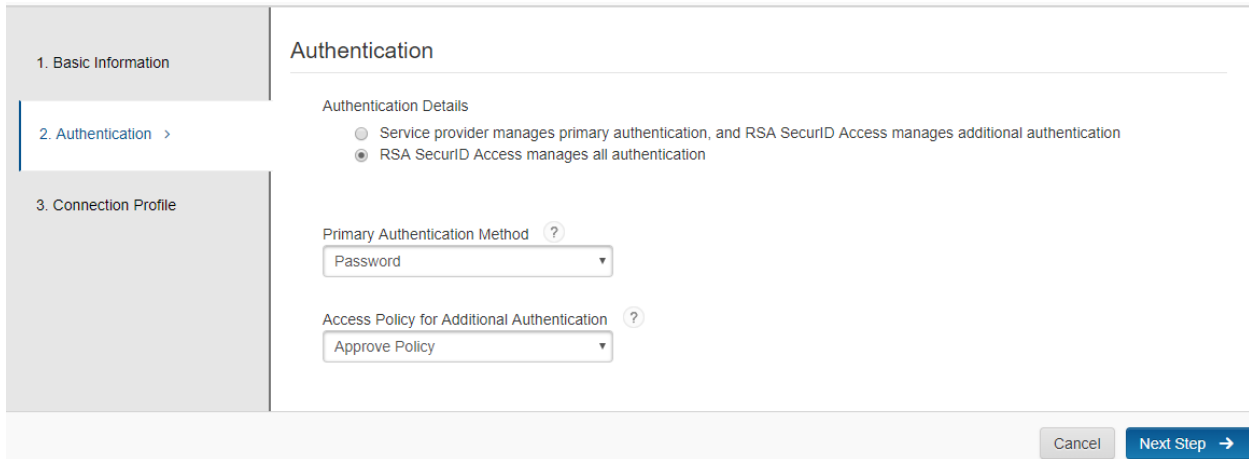


4. From the Relying Party Catalog select the **+Add** button for Service Provider SAML.



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.



1. Basic Information

2. Authentication >

3. Connection Profile

Authentication

Authentication Details

Service provider manages primary authentication, and RSA SecurID Access manages additional authentication

RSA SecurID Access manages all authentication

Primary Authentication Method ?

Password

Access Policy for Additional Authentication ?

Approve Policy

Cancel Next Step →

10. Select **Next Step**.
11. Select **Import Metadata** and use the file you download in step 1 page 8.

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. In the **Assertion Consumer Service (ACS) URL** enter https://app.scaleft.com/v1/_saml_callback.
13. In the **Service Provider Entity ID** enter <https://app.scaleft.com/v1/teams/<TEAM>> where <TEAM> is your specific team name when the site was created.

Data Input Method

Import Metadata

Enter Manually

Service Provider Metadata

Assertion Consumer Service (ACS) URL ?

Service Provider Entity ID ?

14. Select IdP Signs **Entire SAML response**.
15. Click **Download Certificate**.

Message Protection

 SP signs SAML requests


No certificate loaded

Choose File



IdP Signs

 Assertion within response

 Entire SAML response



16. Click **Show Advanced Configuration**.

- Enter Attributes **Email, FirstName, LastName, and Login** with the correlating value from your Active Directory.

User Identity ?

NameID

Identifier Type

Property ?

Attribute Extension ?

Attribute Name	Attribute Source	Property	
<input type="text" value="Email"/>	<input type="text" value="Identity Source"/>	<input type="text" value="mail"/>	⊖
<input type="text" value="FirstName"/>	<input type="text" value="Identity Source"/>	<input type="text" value="givenName"/>	⊖
<input type="text" value="LastName"/>	<input type="text" value="Identity Source"/>	<input type="text" value="sn"/>	⊖
<input type="text" value="Login"/>	<input type="text" value="Identity Source"/>	<input type="text" value="mail"/>	⊖
+ ADD			

- Select **Save and Finish**.
- On the My Relying Parties page, select the **Edit** pulldown and select **View or Download IdP Metadata**.
- 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 **sAMAccountName** or **uid** is checked.

1. Identity Source Details

2. User Attributes >

3. Synchronize User Attributes

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.

[Refresh Attributes](#)

User Attributes

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

Next Steps

[ScaleFT SAML Configuration](#)

Partner Product Configuration

Before You Begin

This section provides instructions for configuring ScaleFT 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.

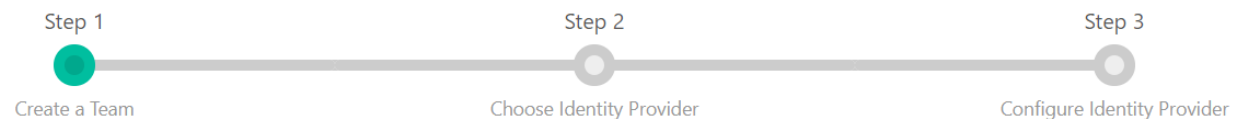
All ScaleFT components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

ScaleFT SAML Configuration

Complete the steps in this section to integrate ScaleFT with RSA SecurID Access using SAML authentication protocol.

Procedure

1. Enroll for a ScaleFT account.
2. Enter your **Team Name**.



Let's begin by picking a name for your new team.

If you work for a company, your company name might be a good choice. Your team name must be unique, and can contain only alphanumeric characters, hyphens, underscores, or periods.

Next

3. Select **Next**.

4. Select **SAML**.

Time to pick an Identity Provider.

This is how members of your new team will log in.

Username and Password

Each user on this team will be required to setup a custom username and password.

Okta

Each user on this team will authenticate with the same Okta instance.

G Suite / Google Cloud Identity

Each user on this team will authenticate with the same G Suite or Google Cloud Identity hosted domain.

Github

Each user on this team will authenticate using Github, new users will have to be invited.

SAML

Each user on this team will authenticate with the same SAML Identity Provider (IdP).

5. Take note of the Assertion Consumer (ACS) URL for this much match what is configured on the identity provider.
6. Take note of the Service Provider Entity ID for this much match what is configured on the identity provider.

Enter the following information in your SAML Identity Provider

Assertion Consumer Service (ACS) URL

```
https://app.scaleft.com/v1/_saml_callback
```

Service Provider Entity ID

```
https://app.scaleft.com/v1/teams/pe
```

7. In the Identity Provider SSO URL field paste the [Identity Provider URL](#) when configuring for IDR IDP. When configuring Cloud IDP use the [Cloud IDP URL](#) in this field.
8. In the Identity Provider Entity ID field paste the [Issuer Entity ID](#) when configuring for IDR IDP. When configuring Cloud IDP use the [Cloud IDP URL](#) in this field.
9. In the Identity Provider x.509 Certificate field paste the [public certificate](#) when configuring for IDR IDP. Paste the [IdP sign SAML assertion certificate](#) when configuring for Cloud IDP.

Enter your SAML Identity Provider information

Identity Provider SSO URL

https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=sctest

Identity Provider Entity ID

https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=sctest

Identity Provider x.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIICpDCCAYYqAwIBAgIGAVGMZf+XMA0GCSqGSIb3DQEBCwUAMBxETAPBgNVBAMT
CGdzLmxxvY2FzMB4XDTE1MTIxMDE0NTc1M1oXDTE1MTIxMDE0NTc1M1owEzERMA8G
A1UEAxMIZ3MubG9jYWwwgqEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCx
lwDFChHPvUdV8V1V89DbTUuJRWDZ1bwQjRydL/kkyqU3GFXSdaHFMccLdWa7FAnG
WJ/+WAPoI2bnNb3gztH4s3dCOZBCCGs12+MunUA3RfggwceyTh6r5gw115vNBB4e
kKw15ndkch56/j6ZF4v/Bji39jCB1qc0RYLnwXb3qU0eyXYDBKFN1MEqUKHqF5Jr
IMtFV2TSKiLDy86u7C3QIOeqJN64gXRvRv8w/dEOV4SdohzxAfjuvv17pK45Qq/G
Jnp14BewAETd00WKJQvr+19YqC1DfnNipEfKRRqMJg3Aarp52HXchXhoNxFb66014
pJEpgclZxKHPIj11rxZjAgMBAAEwDQYJKoZIhvcNAQELBQADggEBADbZPSzcYC6T
m0oLi1gr2wOLKOEu63WY0KaF/010Mx91ifgOXLSPyryIjJ95RqQle1shtUWMSwsc
PEFGCDLlnD5v034t60FC13kE70iyjCQRByIS1z0908MEv5GI+qVUH+C7sJvvy7b
HK06dCpPW2+jbfnTsWDOh5HkeZMDb19t4GaHrgYa4cvbLDWKg9g7fsCNCwq3fr9W
XVfFEVgqK3fYC1rU7Q7xRVhkMUyW/Z8aqCjpdTmho5peceqDdz21Y9D6Zual2At9
XI8OP0uB6s+gxwRnAJTqXa48/2i8QbPZV8SLe5113TVwG5L48wCpxwBsoLbM0I5r
XeoN8j2YCO0=
-----END CERTIFICATE-----
```

10. In the Attribute Mapping section, enter **Login** for the User Name Attribute.
11. Enter **Email** for the Email Attribute field.
12. Enter **FirstName** for the First Name Attribute field.
13. Enter **LastName** for the Last Name Attribute field.
14. Leave the Server User Name Attribute field blank.

Attribute Mapping

User Name Attribute

The name of the SAML attribute which should be used for ScaleFT user names

Email Attribute

The name of the SAML attribute which should be used as the source of each user's email address

First Name Attribute

The name of the SAML attribute which should be used as the source of each user's first name for display purposes

Last Name Attribute

The name of the SAML attribute which should be used as the source of each user's last name for display purposes

Server User Name Attribute (Optional)

The name of the SAML attribute which should be used for server user names. If left blank, server user names will be derived from ScaleFT user names.

Authenticate With SAML

15. Click **Authenticate With SAML** to complete and validate your configuration.