RSA SECURID® ACCESS
Implementation Guide

ScaleFT

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

RSA READY

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.

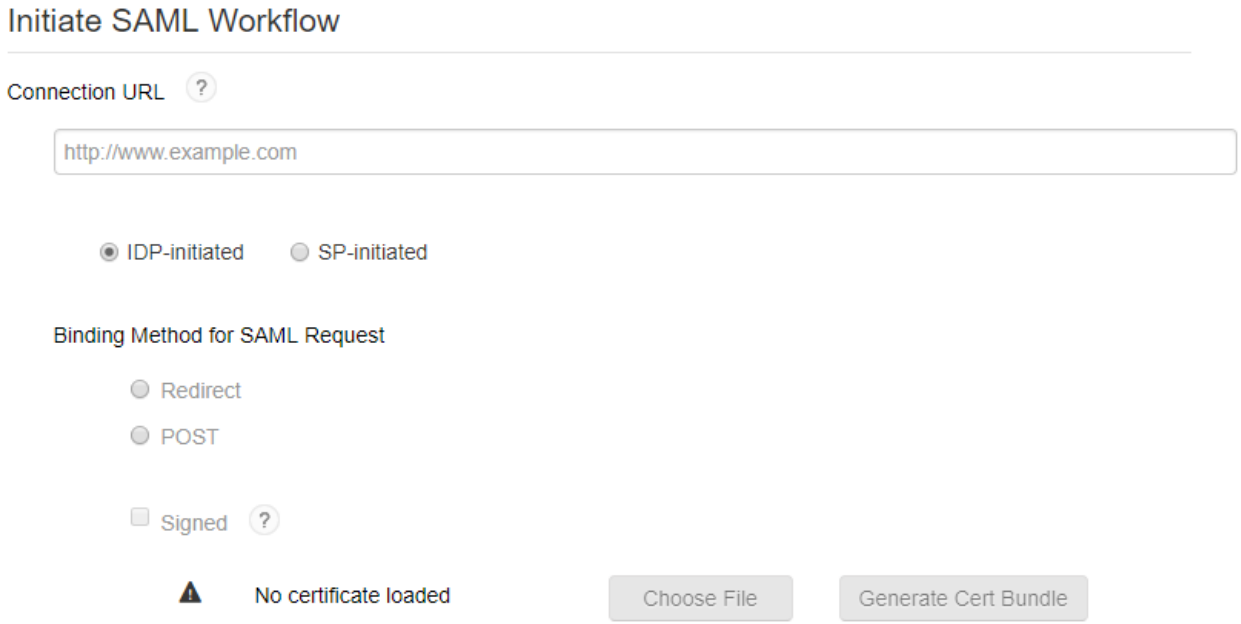
Configure RSA Identity Router SAML IdP

Procedure

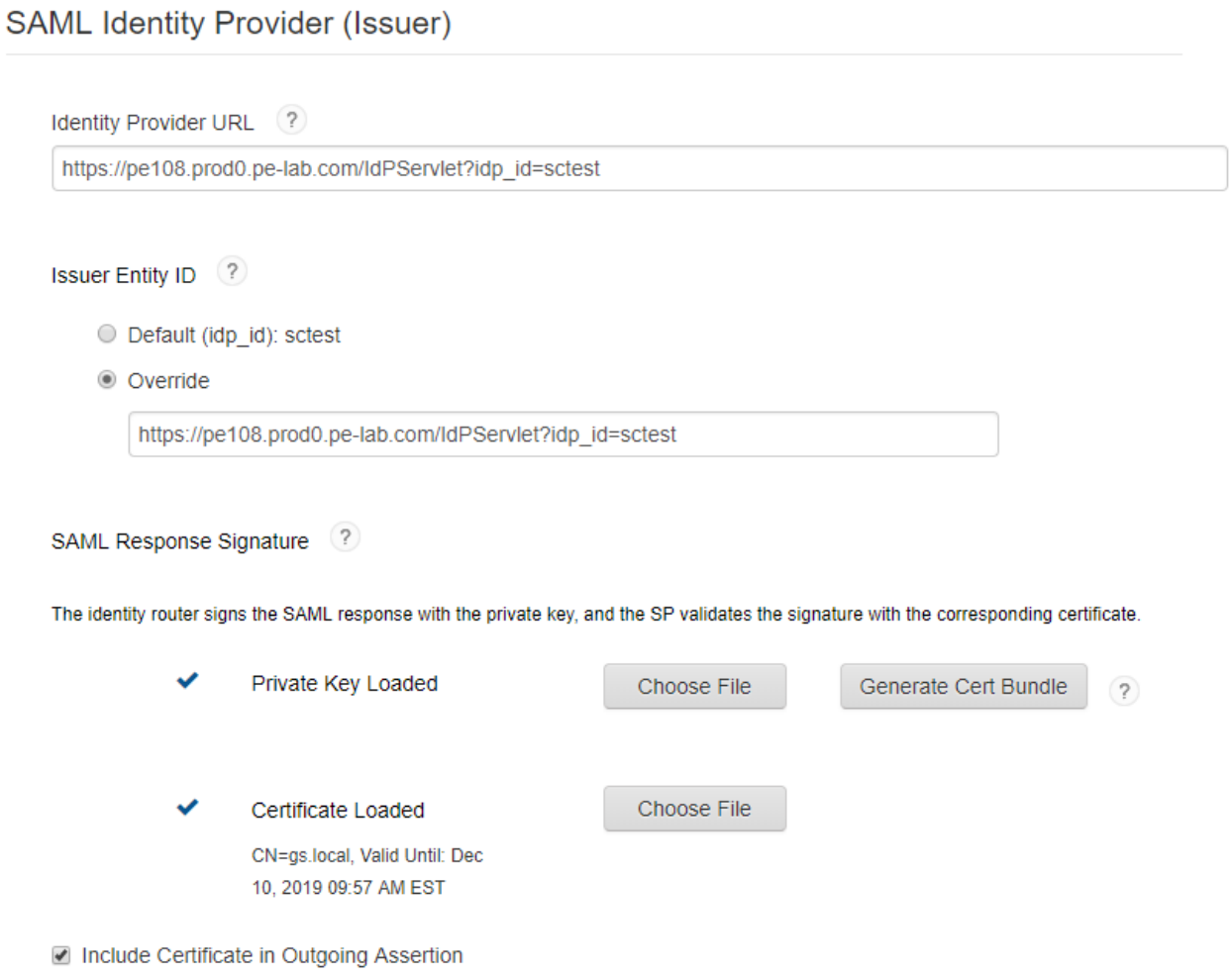
1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for ScaleFT and click **+Add** to add the connector.

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.



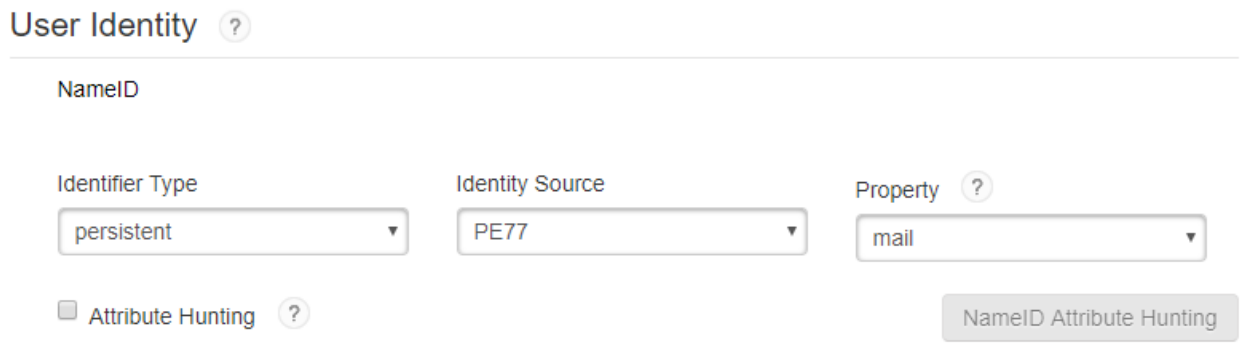
4. Scroll down to SAML Identity Provider (Issuer) section.



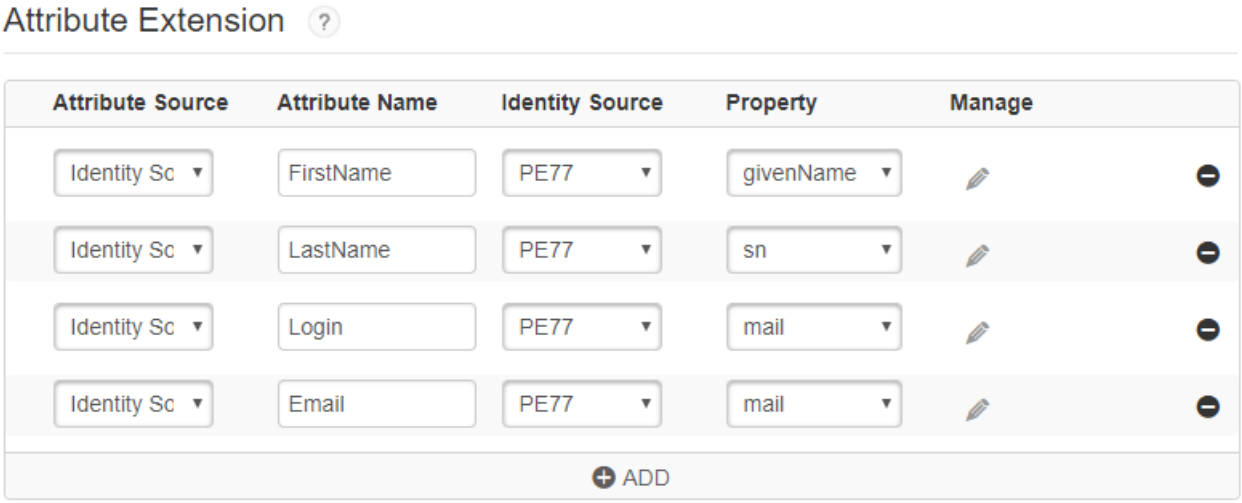
a. Take note of the **Identity Provider URL**.
b. Select **Override** and paste the Identity Provider URL into the Issuer Entity ID field.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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

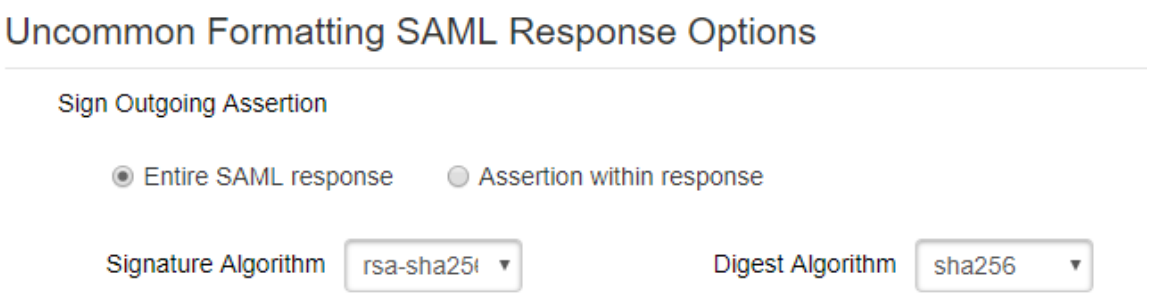
6. Verify the **Assertion Consumer Service (ACS) URL** field.
7. In the **Audience (Service Provider Entity ID)** field replace **<TEAM>** with your team name.
8. Scroll down to the User Identity section and select **persistent** from the Identifier Type pulldown. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



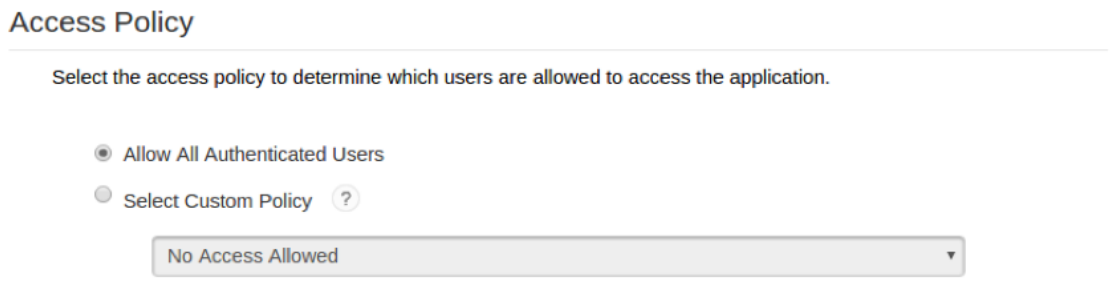
9. Click **Show Advanced Configuration**.
10. Under Attribute Extension, enter attributes **FirstName, LastName, Email,** and **Login** with the correlating value from your Active Directory.



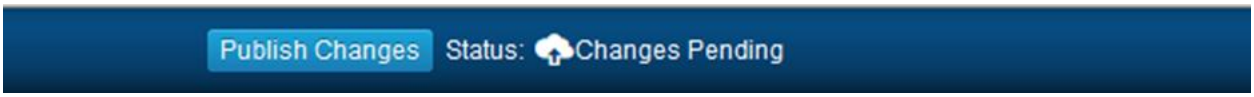
11. Under Uncommon Formatting SAML Response Options, sent Signature Algorithm to **rsa-sha256** and Digest Algorithm to **sha256**.



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



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



Next Steps

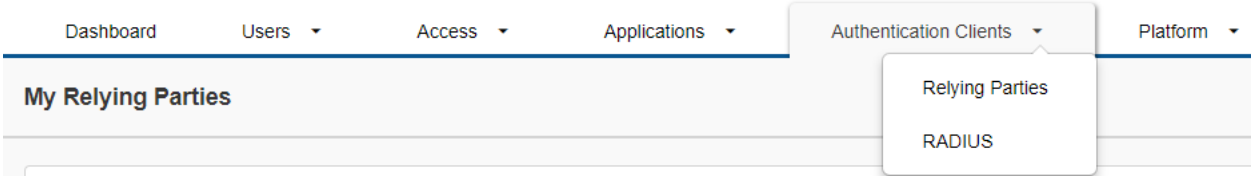
[ScaleFT SAML Configuration]

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.

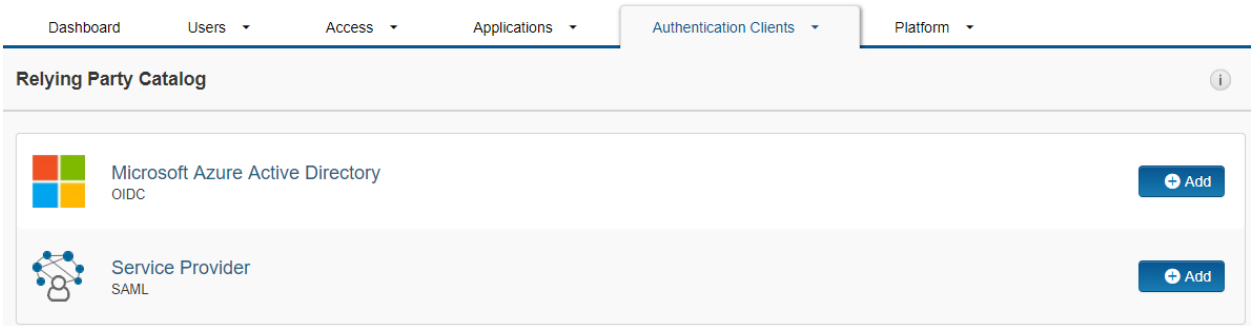
Procedure

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.



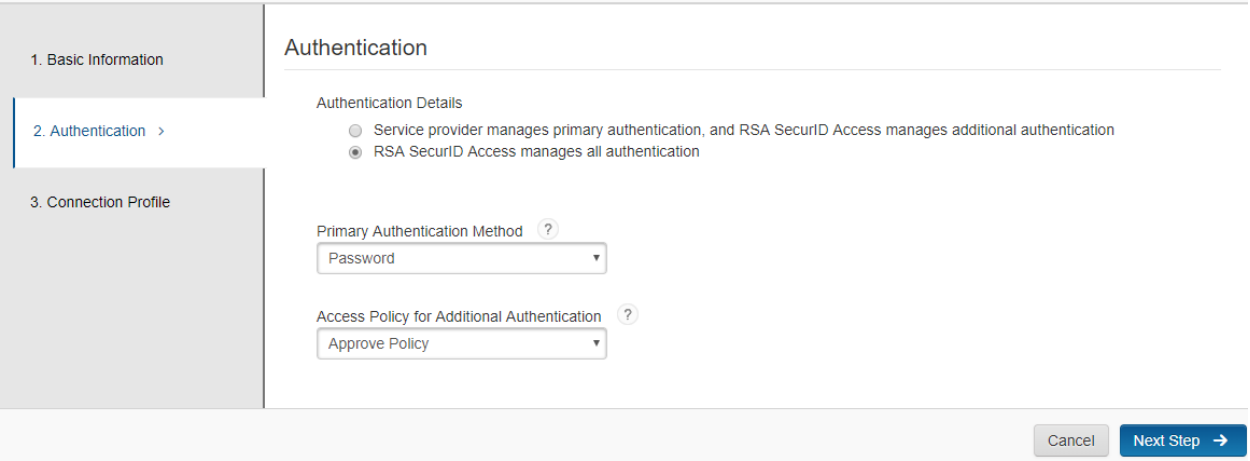
3. Click the **Add a Relying Party** button on the My Relying Parties page.

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

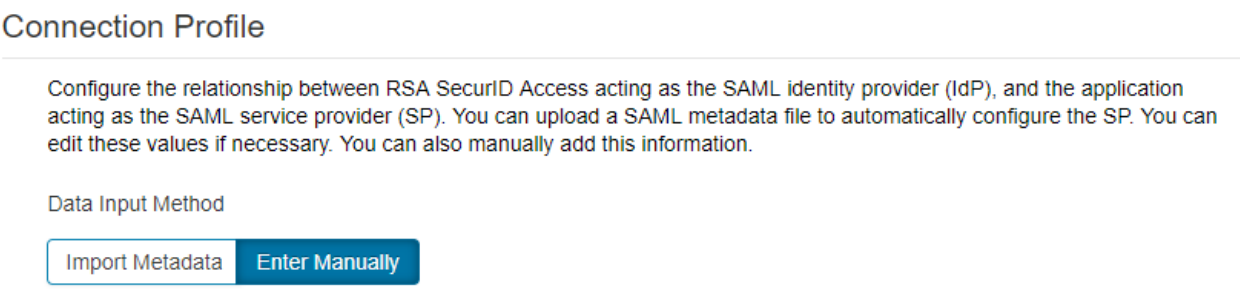


5. Enter a name for the Service Provider in the **Name** field on the Basic Information page.
6. Click the **Next Step** button.

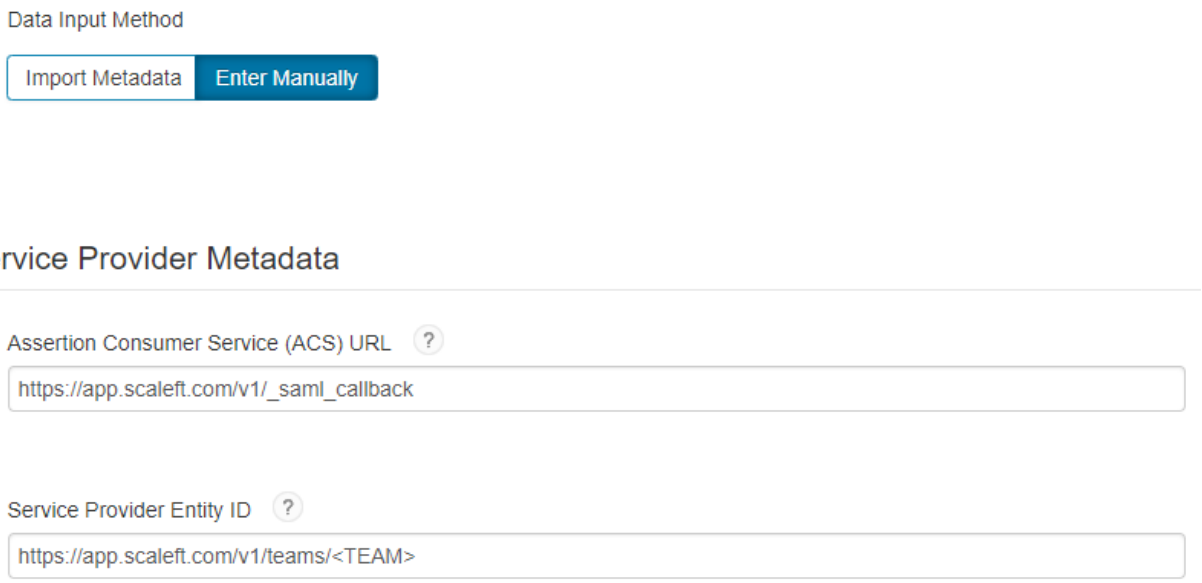
7. On the Authentication page, select **RSA SecurID Access manages all authentication**.
8. From the Primary Authentication Method pulldown, select your desired login method either Password or SecurID.
9. From the Access Policy pulldown select a policy that was previously configured.



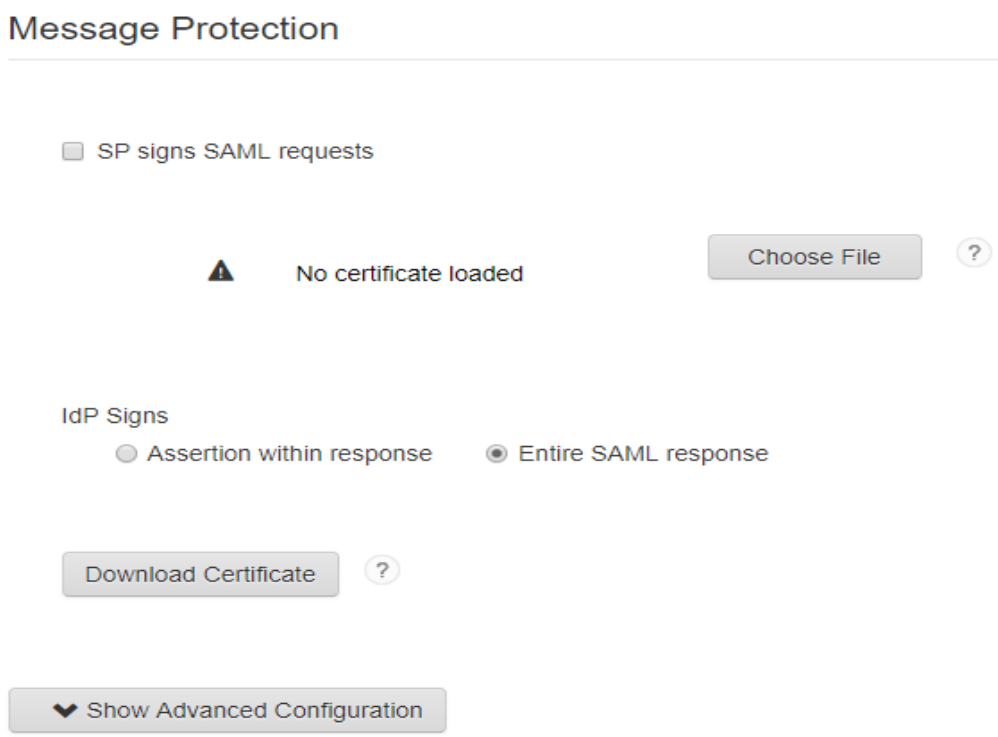
10. Select **Next Step**.
11. Select **Import Metadata** and use the file you download in step 1 page 8.



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.

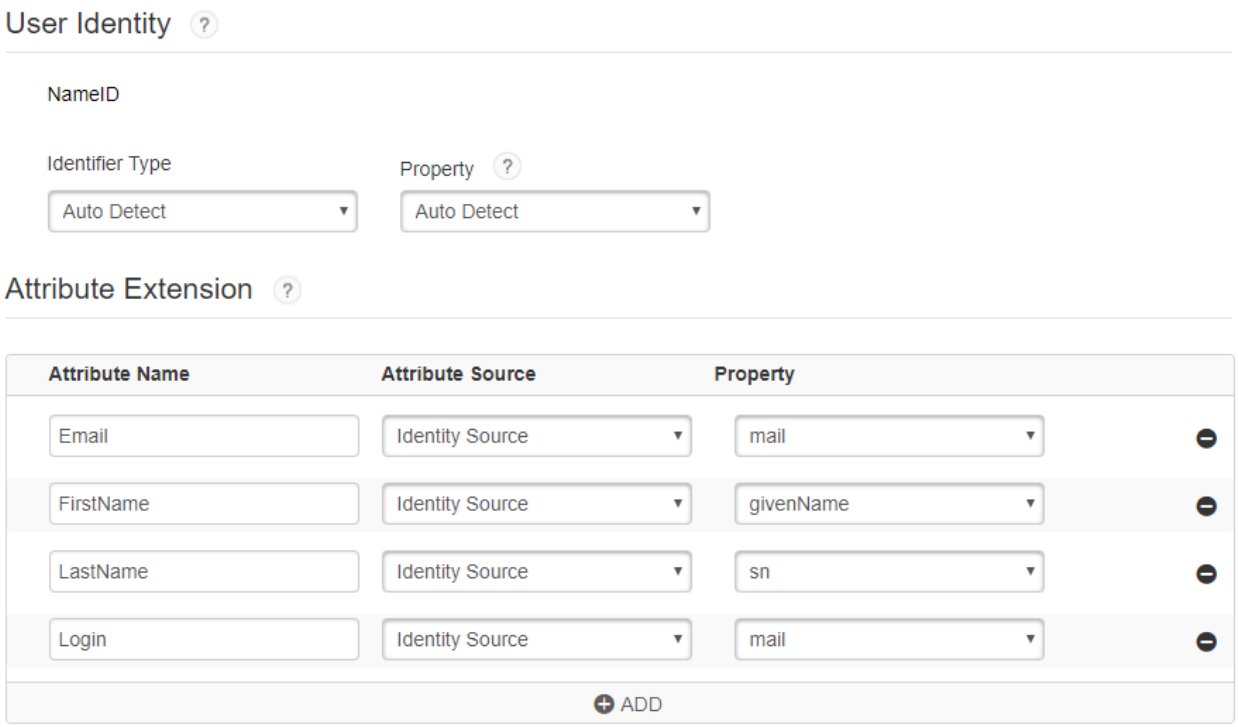


14. Select IdP Signs **Entire SAML response**.
15. Click **Download Certificate**.



16. Click **Show Advanced Configuration**.

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

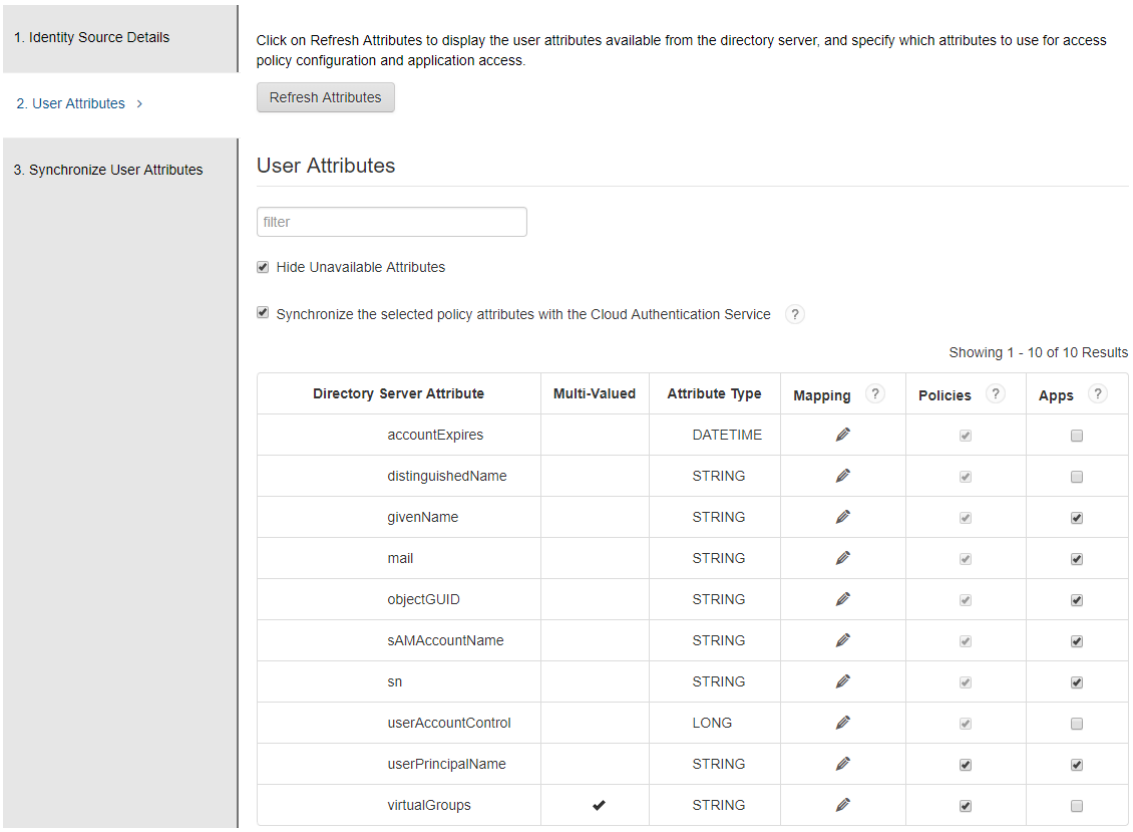


18. Select **Save and Finish.**
19. On the My Relying Parties page, select the **Edit** pulldown and select **View or Download IdP Metadata**.
20. View the metadata file to find the Cloud IDP URL. **Location=https://<company_id>.auth.securid.com/saml-fe/sso.** This is the Cloud IDP URL.

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 **sAMAccountName** or **uid** is checked.



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

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.

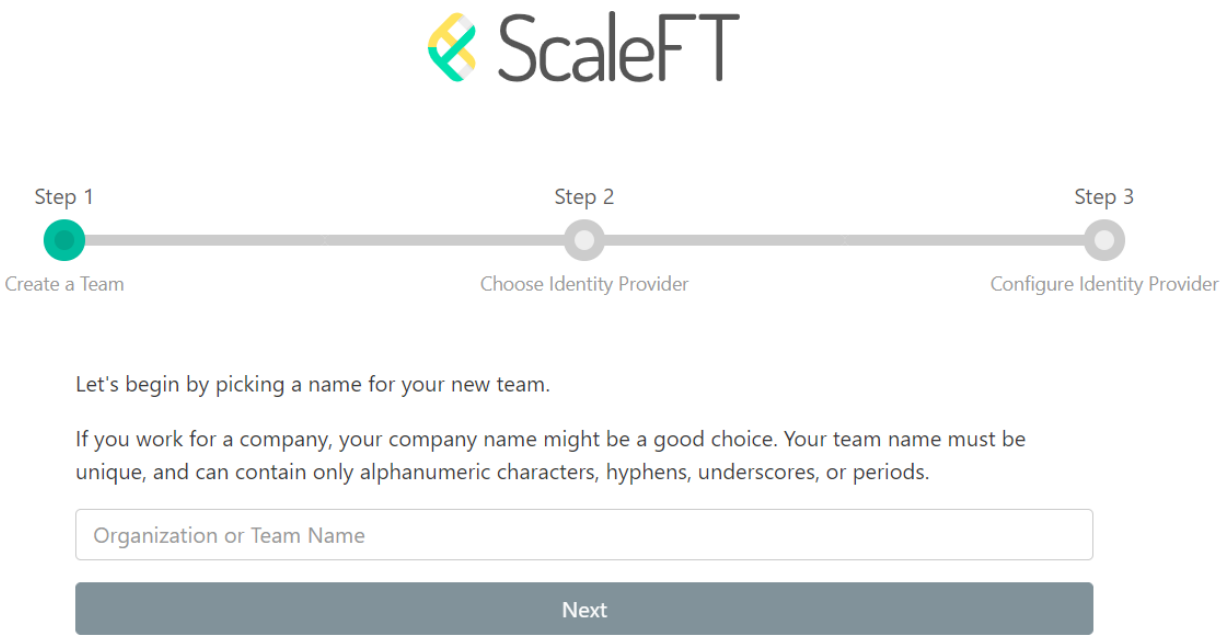
All ScaleFT components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

ScaleFT SAML Configuration

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

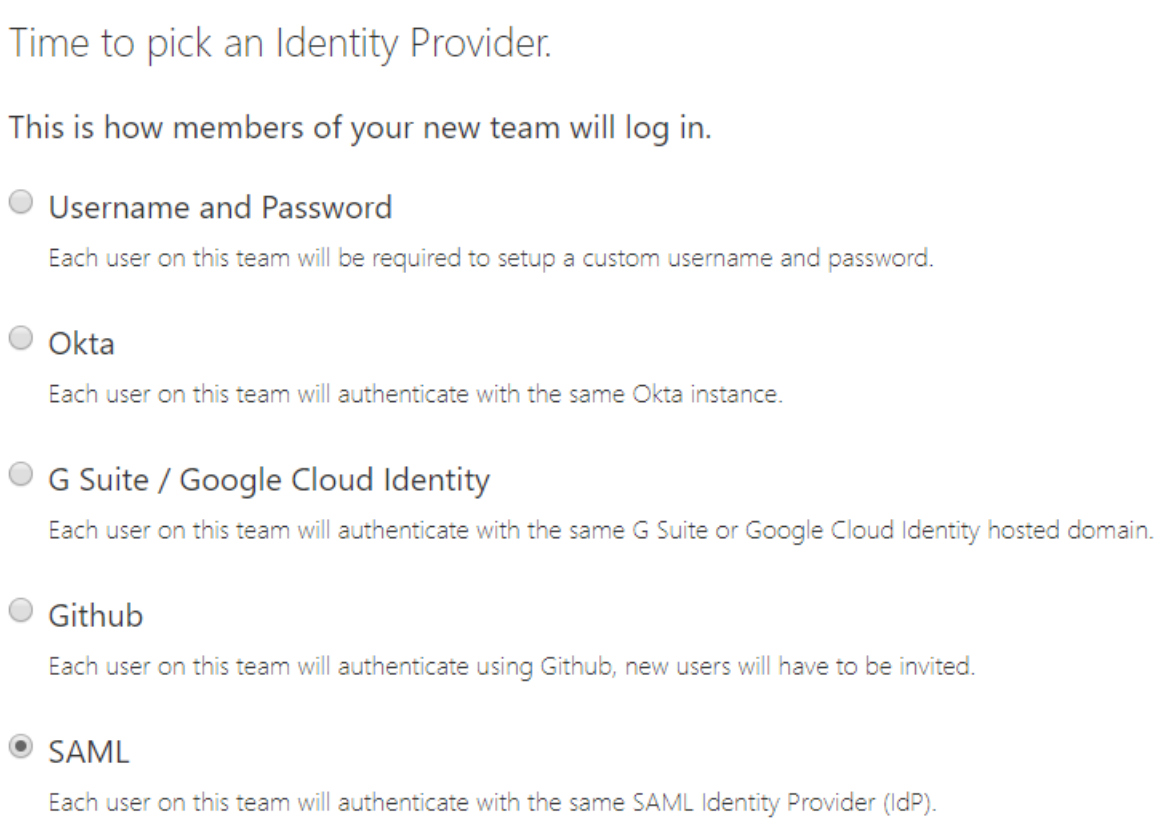
Procedure

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

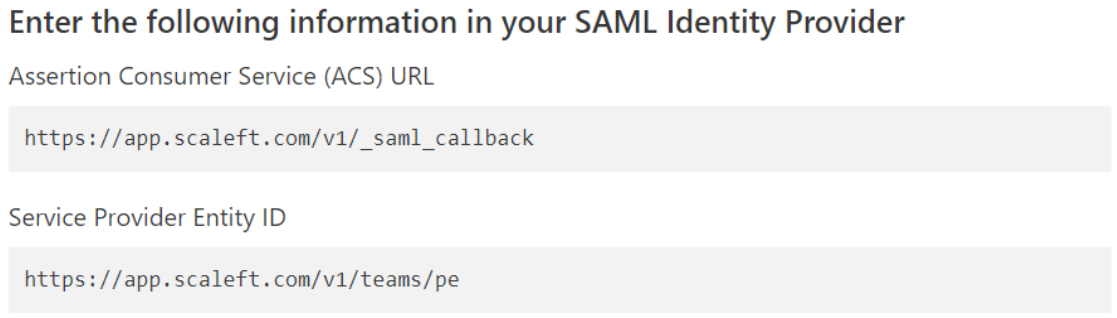


3. Select **Next**.

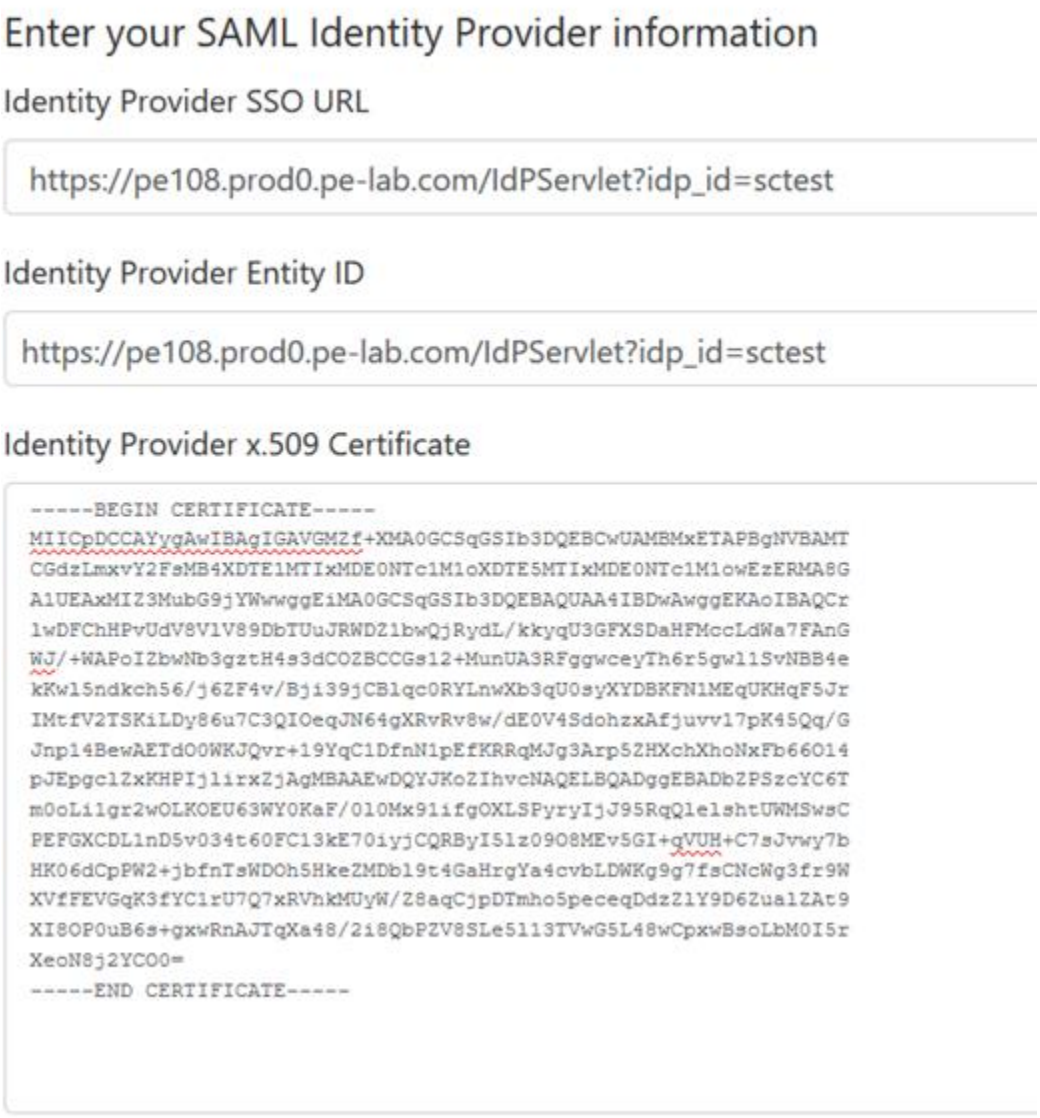
4. Select **SAM**L.



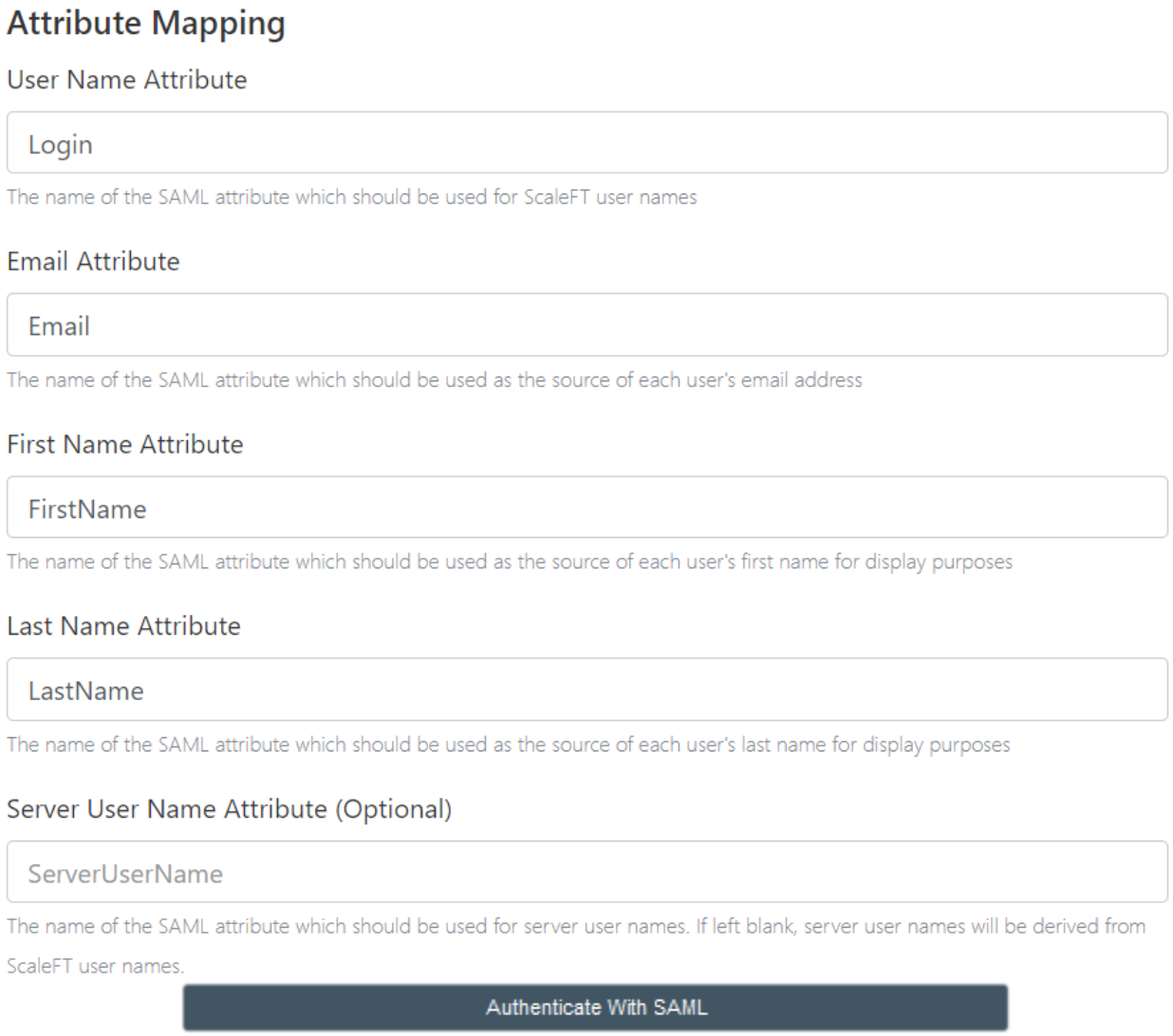
5. Take note of the Assertion Consumer (ACS) URL for this much match what is configured on the identity provider.
6. Take note of the Service Provider Entity ID for this much match what is configured on the identity provider.



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.



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.



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