RSA SecurID Access SAML Configuration for Socialcast

Last Modified: September 1, 2015

Socialcast is the premier enterprise social networking platform that connects people to the knowledge, ideas and resources they need to work more effectively.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Socialcast.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

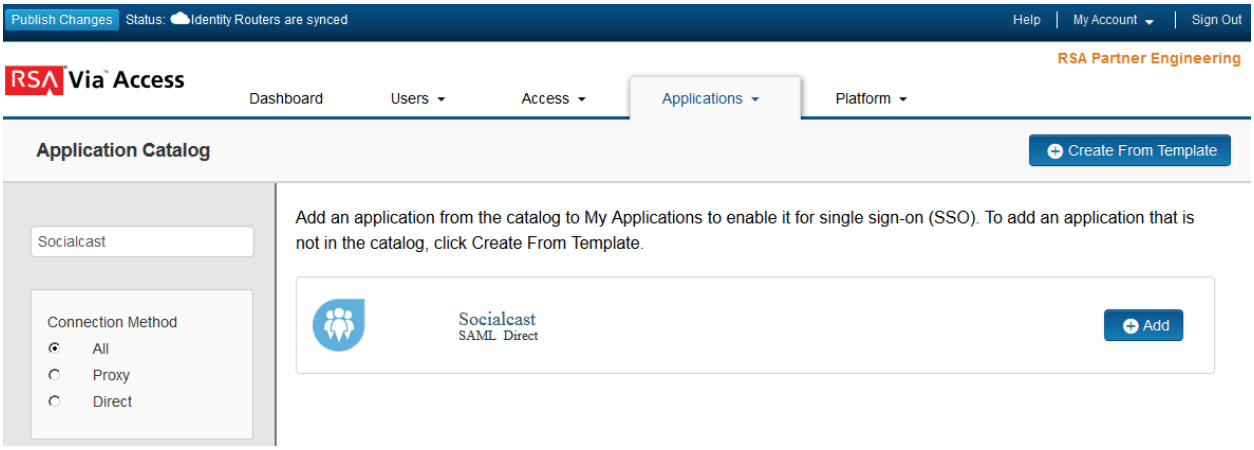
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Socialcast to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

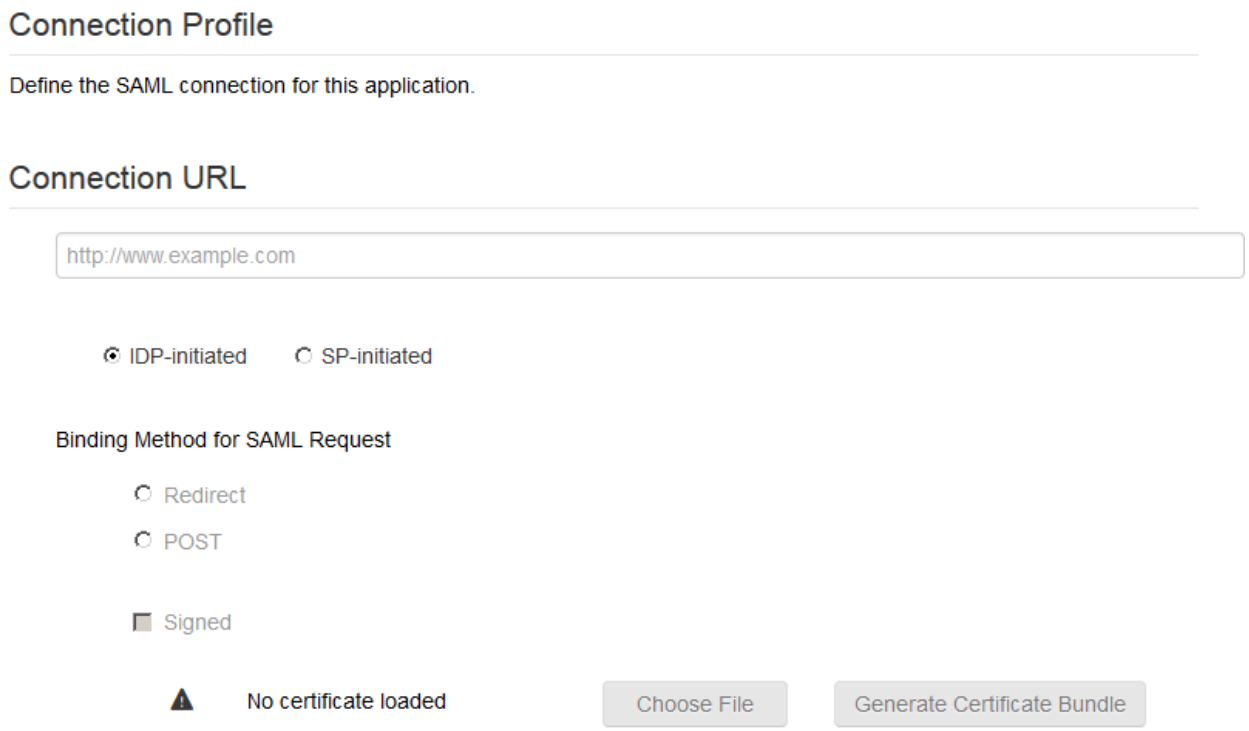
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the application that you wish to add.



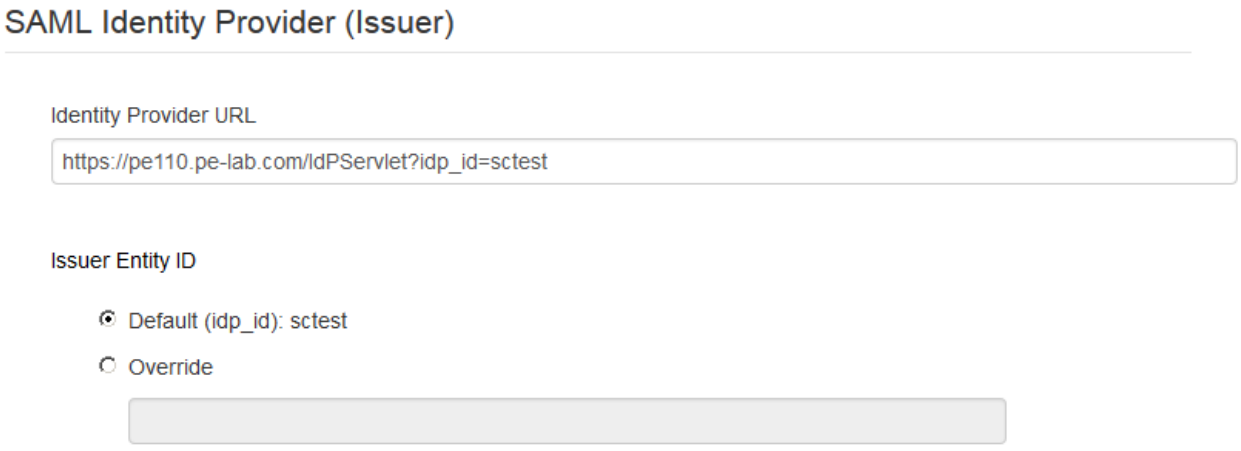
3. On the Basic Information page, specify the application name and click **Next Step**.

> **Note: The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.**

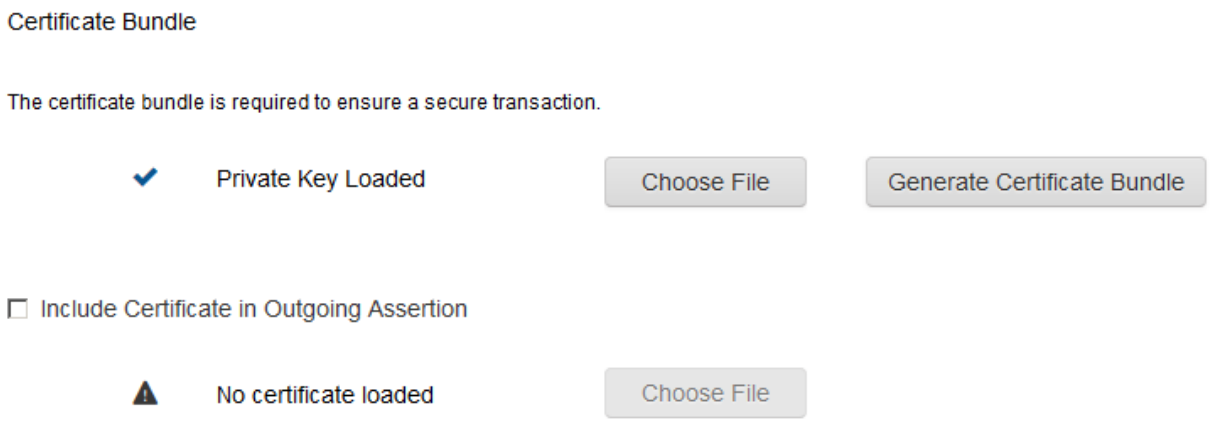
4. On the Connection Profile page, leave the URL blank and select **IDP -initiated**.



5. Scroll down to **SAML Identity Provider (Issuer)** section.
6. Take note of the Issuer Entity ID it will be needed to create the RSA SecurID Access metadata file.

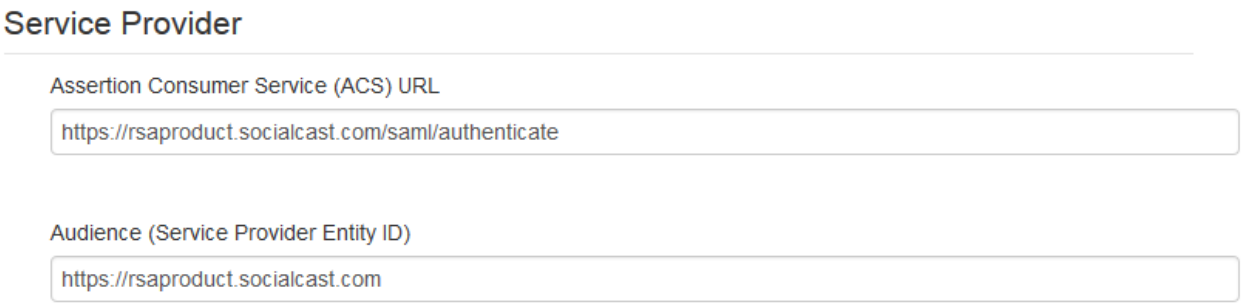


7. Click **Choose File** and upload the private key.



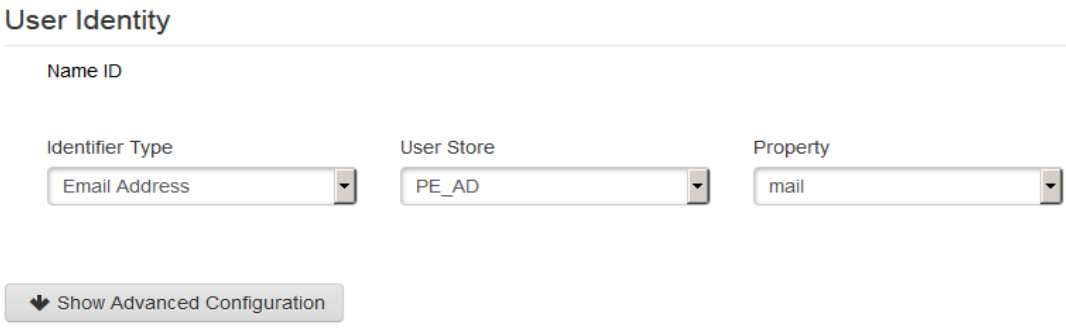
8. Scroll down to the **Service Provider** section.

> **Note: Obtain the ACS URL and the Service Provider Entity ID from the Socialcast metadata file. See page 10, step 12.**



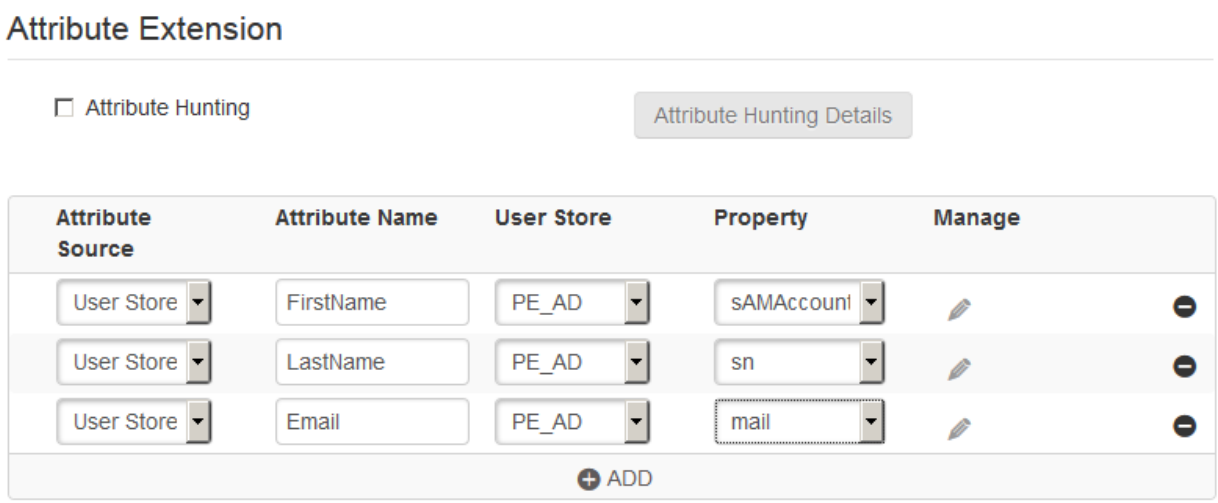
   a. In the **Assertion Consumer Service (ACS) URL** field, enter https://<your_instance>.socialcast.com/saml/authenticate
   b. In the **Audience (Service Provider Entity ID)** field, enter https://<your_instance.socialcast.com.

9. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

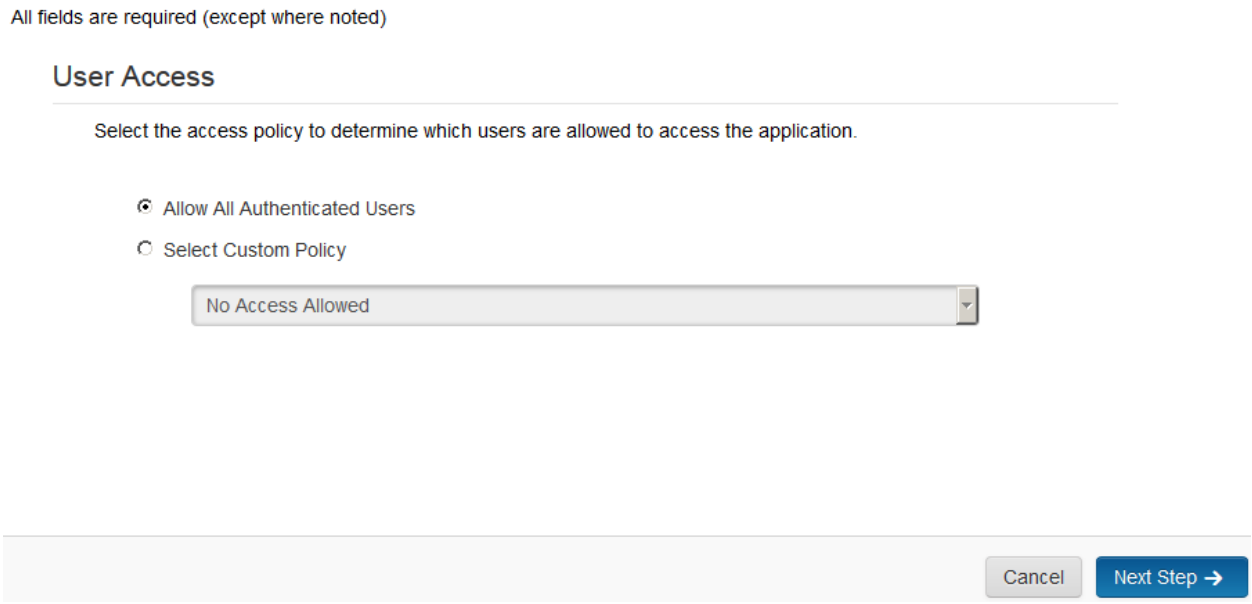


10. Click **Show Advanced Configuration**.

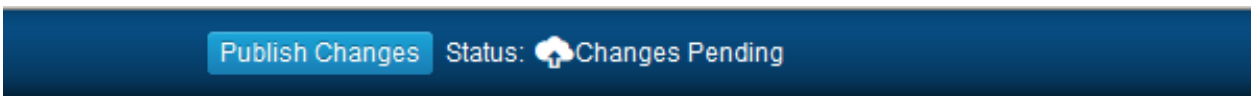
11. Scroll down to the **Attribute Extension** section.
12. Under the **Attribute Source** select **User Store**.
13. Add Attribute Names **FirstName**, **LastName**, and **Email** and its associated property.



14. Click **Next Step**.
15. On the **User Access** page, select the desired user policy from the drop down list.



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



Create the RSA SecurID Access Metadata file

1. Modify the example below with your environment information.
2. When inserting the cert.pem file do not include the -----BEGIN CERTIFICATE---- and ----END CERTIFICATE----lines.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<EntityDescriptor xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
   xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
   entityID="CHANGE_ME_TO_ENTITY_ID">
 <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   <KeyDescriptor use="signing">
     <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       <ds:X509Data>
         <!-- public saml cert -->
<ds:X509Certificate>CHANGE_ME_TO_PUBLIC_SAML_CERT_CONTENT<ds:X509Certificate>
       </ds:X509Data>
     </ds:KeyInfo>
   </KeyDescriptor>

   <!-- Supported Name Identifier Formats -->
   <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</NameIDFormat>
   <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName</NameIDFormat>

   <!-- POST binding and location=idp url -->
   <SingleSignOnService
     Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
     Location="CHANGE_ME_TO_IDP_URL"/>

 </IDPSSODescriptor>
</EntityDescriptor>
```

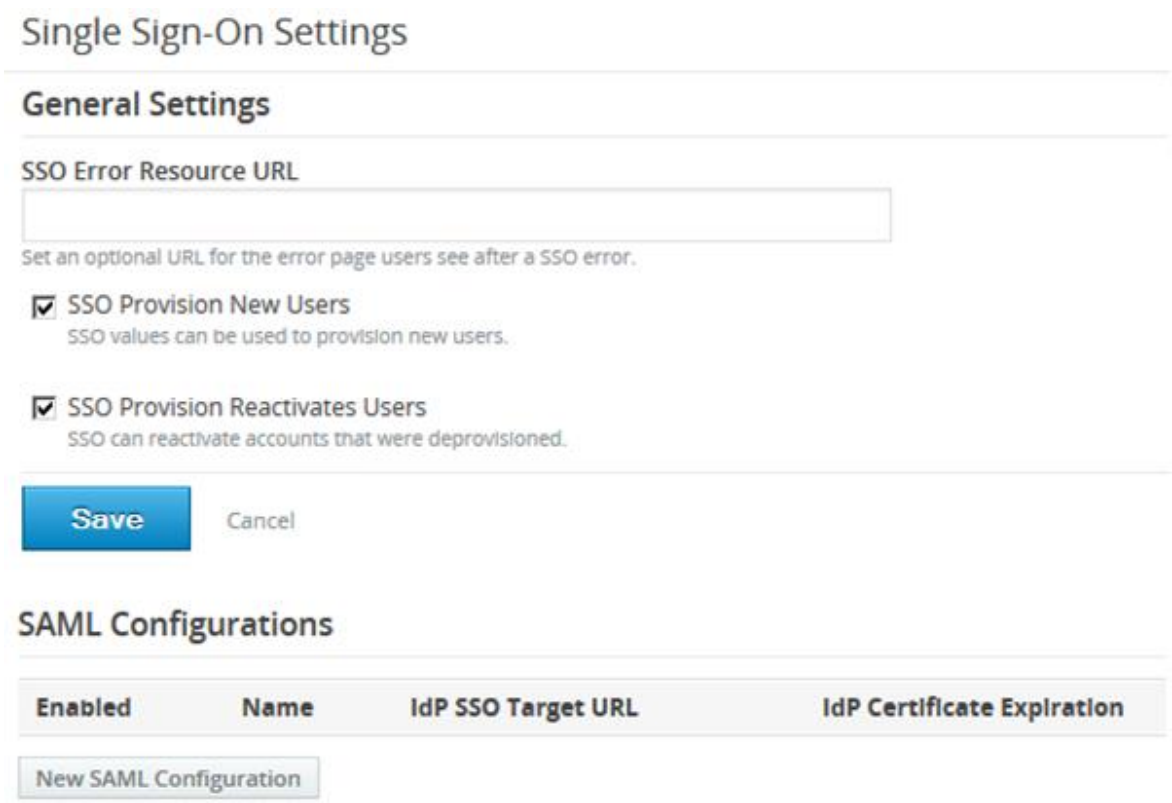
Next Steps

Configure Socialcast to Use RSA SecurID Access as an Identity Provider

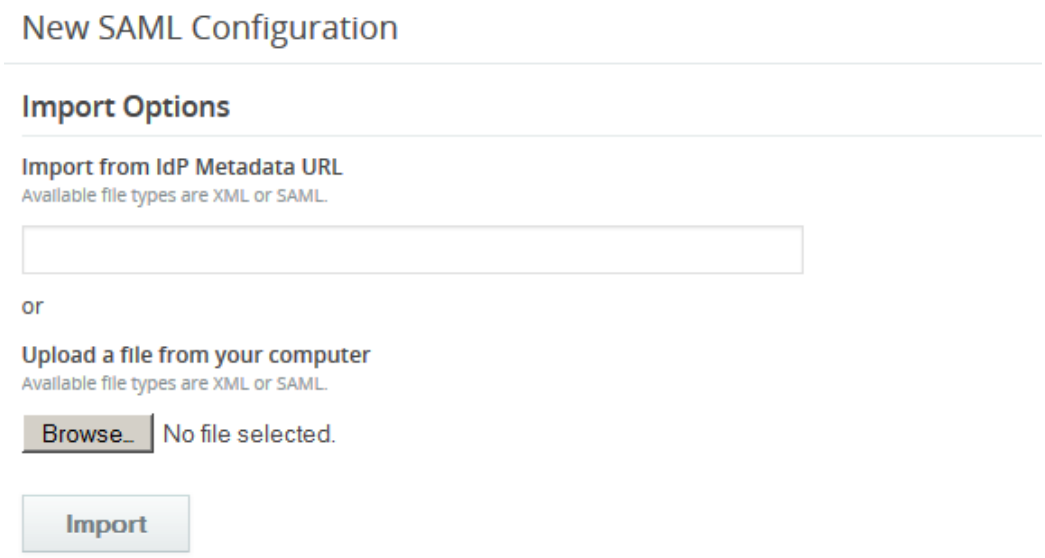
Configure Socialcast to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login into the Socialcast administration console. https://login.socialcast.com/sso/new
2. Under the gear icon navigate to **Admin Settings** > **Security** > **SSO Configuration**, and click **New SAML Configuration**.

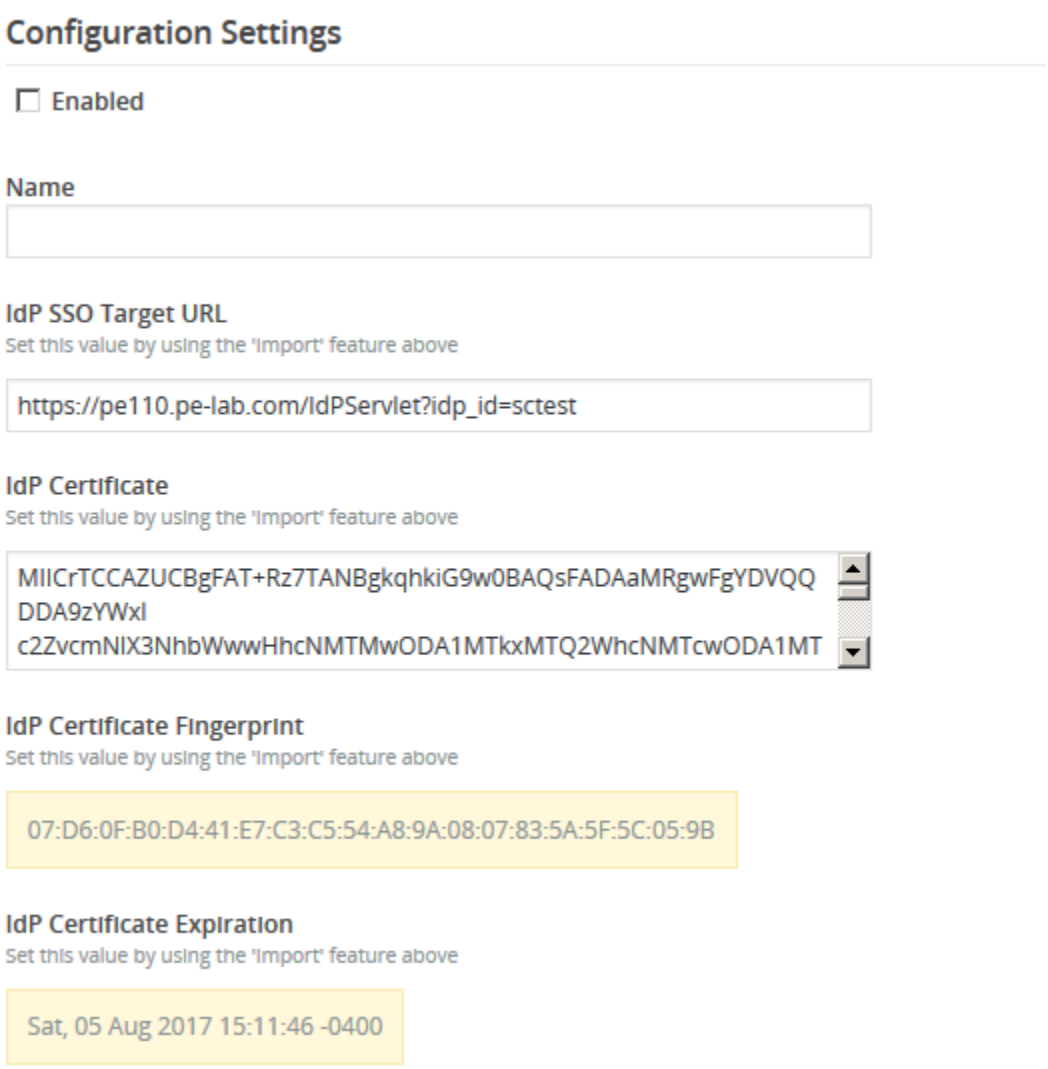


3. The New SAML Configuration page will open, click **Browse** to select the RSA SecurID Access metadata file.

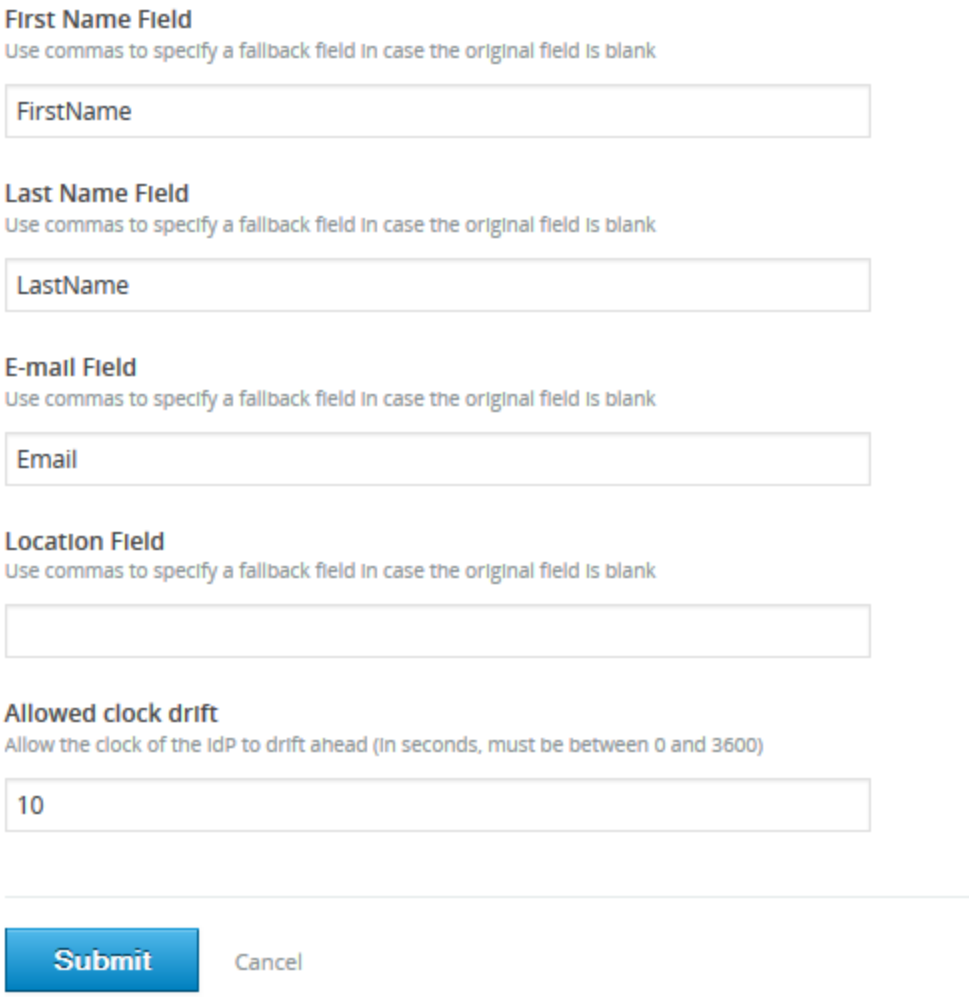


4. Click **Import** to upload the metadata file.

5. The metadata will automatically populate the **IdP SSO Target URL**, **IdP Certificate**, **IdP Certificate Fingerprint**, and **IdP Certificate Expiration** fields.



6. Enter a name for this configuration in the **Name** field.
7. Map the **First Name Field**, **Last Name Field**, and **Email Field** to the attribute names configured under the RSA SecurID Access Attribute Extension section.
8. Click **Submit**.



9. Under the gear icon, select **Test** to confirm you can access the RSA SecurID Access portal.
10. Once successful select **Enabled**.
11. Under the gear icon, select **View SP Descriptor** to download the SP metadata file.

12. Open the SP metadata file and locate the **entityID** and **ACS URL**. This information will be needed to configure RSA SecurID Access.

```
<?xml version='1.0' encoding='UTF-8'?>
<md:EntityDescriptor xmlns:md='urn:oasis:names:tc:SAML:2.0:metadata'
entityID='https://<your_instance>.socialcast.com'>
 <md:SPSSODescriptor
protocolSupportEnumeration='urn:oasis:names:tc:SAML:2.0:protocol'
AuthnRequestsSigned='false' WantAssertionsSigned='true'>
  <md:AssertionConsumerService
Binding='urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'
Location='https://<your_instance>.socialcast.com/saml/authenticate'
isDefault='true' index='0'/>
 </md:SPSSODescriptor>
</md:EntityDescriptor>
```

GLS