

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.

The screenshot displays the RSA SecurID Access Administration Console interface. At the top, there is a navigation bar with 'Publish Changes', 'Status: Identity Routers are synced', 'Help', 'My Account', and 'Sign Out'. Below this is the 'RSA Via Access' header with navigation tabs for 'Dashboard', 'Users', 'Access', 'Applications', and 'Platform'. The 'Applications' tab is active, showing the 'Application Catalog' page. On the left, there is a search box containing 'Socialcast' and a 'Connection Method' filter with radio buttons for 'All', 'Proxy', and 'Direct'. The main content area shows a card for 'Socialcast SAML Direct' with an '+ Add' button. A blue button labeled 'Create From Template' is also visible in the top right of the application catalog area. Below the card, there is instructional text: 'Add an application from the catalog to My Applications to enable it for single sign-on (SSO). To add an application that is not in the catalog, click Create From Template.'

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**.

Connection Profile

Define the SAML connection for this application.

Connection URL

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

Choose File

Generate Certificate Bundle

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.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID


Default (idp_id): sctest

Override

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

Certificate Bundle


The certificate bundle is required to ensure a secure transaction.

 Private Key Loaded

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion

 No certificate loaded

Choose File

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.**

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

- 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**.

User Identity

Name ID

Identifier Type


Email Address

User Store

PE_AD

Property

mail

 Show Advanced Configuration

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.

Attribute Extension

Attribute Hunting Attribute Hunting Details

Attribute Source	Attribute Name	User Store	Property	Manage
User Store	FirstName	PE_AD	sAMAccount	
User Store	LastName	PE_AD	sn	
User Store	Email	PE_AD	mail	

+ ADD

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

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

- Allow All Authenticated Users
 Select Custom Policy

No Access Allowed

Cancel

Next Step →

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.

Publish Changes

Status: Changes Pending

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**.

Single Sign-On Settings

General Settings

SSO Error Resource URL

Set an optional URL for the error page users see after a SSO error.

SSO Provision New Users
SSO values can be used to provision new users.

SSO Provision Reactivates Users
SSO can reactivate accounts that were deprovisioned.

Save

Cancel

SAML Configurations

Enabled	Name	IdP SSO Target URL	IdP Certificate Expiration
New SAML Configuration			

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

New SAML Configuration

Import Options

Import from IdP Metadata URL

Available file types are XML or SAML.

or

Upload a file from your computer

Available file types are XML or SAML.

No file selected.

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.

Configuration Settings

Enabled

Name

IdP SSO Target URL

Set this value by using the 'Import' feature above

IdP Certificate

Set this value by using the 'Import' feature above

IdP Certificate Fingerprint

Set this value by using the 'Import' feature above

IdP Certificate Expiration

Set this value by using the 'Import' feature above

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**.

First Name Field

Use commas to specify a fallback field in case the original field is blank

Last Name Field

Use commas to specify a fallback field in case the original field is blank

E-mail Field

Use commas to specify a fallback field in case the original field is blank

Location Field

Use commas to specify a fallback field in case the original field is blank

Allowed clock drift

Allow the clock of the IDP to drift ahead (in seconds, must be between 0 and 3600)

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.

SAML Configurations

Enabled	Name	IdP SSO Target URL	IdP Certificate Expiration	
<input checked="" type="checkbox"/>	Via	https://pe110.pe-lab.com/Id...	Sat, 05 Aug 2017 15:11:46 -0400	

[New SAML Configuration](#)

- Test
- View SP Descriptor
- Edit
- Delete

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>
```