

Last Modified: August 27, 2015

Brainshark is a business presentation solution provider, enabling companies to increase sales productivity, train more effectively or reach new audiences.

Before You Begin

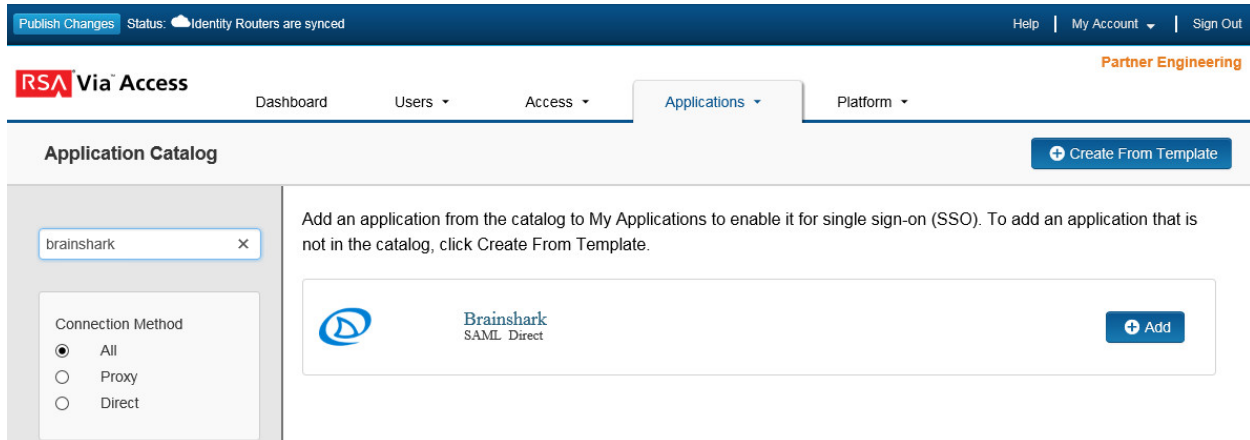
- Acquire an administrator account to RSA SecurID Access.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.
- Contact Brainshark support for single sign-on enablement.

 **Note:** Brainshark will send you a SSO questionnaire and will request your metadata file.

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 shows 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 right side of the page, there is a "Create From Template" button. The main content area displays a search box with "brainshark" entered. Below the search box, there are radio buttons for "Connection Method": "All" (selected), "Proxy", and "Direct". To the right of the search results, there is a card for "Brainshark SAML Direct" with a blue "+ Add" button.

3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, select **SP –initiated** and binding method **POST**.

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

5. In the Connection URL field enter your domain single sign-on login URL.
For 'staging' (test) environments: https://staging.brainshark.com/<your_instance>
For Production environments: https://www.brainshark.com/<your_instance>

Connection URL


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

6. Scroll down to **SAML Identity Provider (Issuer)** section.
7. Under the Issuer Entity ID, select **Override** and paste the URL from the Identity Provider URL field in the Override field.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): brainsharktest

Override

8. 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

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

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

- a. In the **Assertion Consumer Service (ACS) URL** field, enter the ACS URL.
For 'staging' (test) environments: <https://ssostg.brainshark.com/sp/ACS.saml2>
For Production environments: <https://sso.brainshark.com/sp/ACS.saml2>
- b. In the **Audience (Service Provider Entity ID)** field, enter Entity ID.
For 'staging' (test) environments: **brainshark:staging:saml2**
For Production environments: **brainshark:default:saml2**

10. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Subject** and **Property** to **mail**.

User Identity

Name ID

Identifier Type

User Store

Property

⏴ Show Advanced Configuration

11. Click **Show Advance Configuration**.

- Under Attribute Extension, use the **Attribute Source** pull down and select **User Store** and add attributes: **firstname**, **lastname**, **username**, **ssokey**, **email**, and **profilename**.

Attribute Extension

Attribute Hunting Attribute Hunting Details

Attribute Source	Attribute Name	User Store	Property	Manage
User Store	firstname	PE_AD	givenName	
User Store	lastname	PE_AD	sn	
User Store	username	PE_AD	sAMAccount	
User Store	ssokey	PE_AD	mail	
User Store	email	PE_AD	mail	
User Store	profilename	PE_AD	ou	

+ ADD

- Click **Next**.

- 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 →

- 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

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.
3. When modifying the Extended Attributes enter the mapping used on page 4 step 12.

```
<?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>CHANGEME_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"/>

        <!--Extended Attributes ->
        <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          firstname="givenname"/>
        <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" username="SMAAccountName"/>
        <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          lastname="sn"/>
        <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" email="mail"/>
        <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" ssokey="mail"/>
        <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" profile="ou"/>

      </IDPSSODescriptor>
    </EntityDescriptor>
```