

RSA SecurID Access SAML Configuration for SuccessFactors



Last Modified: December 7, 2015

SuccessFactors is an American multinational company headquartered in South San Francisco, California, providing cloud-based human capital management (HCM) software solutions using the Software as a service (SaaS) model.

Before You Begin

- Obtain the ACS URL and Audience information from SuccessFactors.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

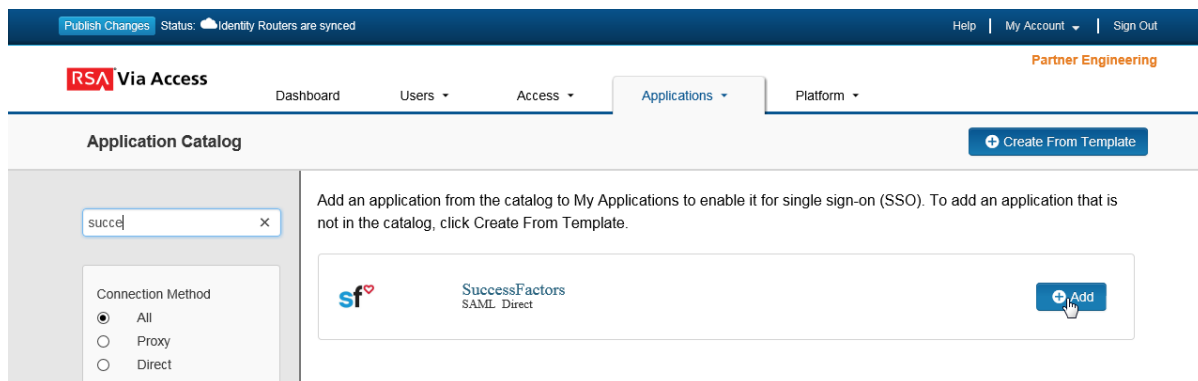
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Request SAML configuration for SuccessFactors](#)

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**.
4. On the Connection Profile page choose **IDP –initiated**.
5. Scroll down to SAML Identity Provider (Issuer) section.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): kfmnasw3s2mh

Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.



private.key

Choose File

Generate Certificate Bundle



cert.pem

Choose File

Certificate valid until: Mon May
06 19:17:04 UTC 2019

Include Certificate in Outgoing Assertion

- a. Take note of the **Identity Provider URL**.
- b. Take note of the **Issuer Entity ID**.
- c. Select **Choose File** and upload the private key.
- d. Select **Choose File** to locate and import a private key to sign the SAML assertion. The private key must correspond to the public signing certificate loaded in the SP application. If a private/public key pair is not readily available, you can click **Generate Certificate Bundle**.

6. Scroll down to the Service Provider section.

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

User Identity

Name ID

Identifier Type

User Store

Property

Attribute Hunting

- a. In the **Assertion Consumer Service (ACS) URL** field, enter the URL you obtained from SuccessFactors.
 - b. In the **Audience (Service Provider Entity ID)** field, enter the Audience / Entity ID you obtained from SuccessFactors.
7. Scroll down to the User Identity section. Set the Identifier Type to **unspecified** and the **Property** value to match the attribute in your user store which contains the SuccessFactors username.
 8. Click **Next Step**.

9. 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 →

10. Click **Next Step**.
11. On the **Portal Display** page, mark the **Display in Portal** checkbox.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

Next Steps

[Request SAML configuration for SuccessFactors](#)

Request SAML configuration for SuccessFactors

Open a support ticket with SuccessFactors to enable your SuccessFactors Sandbox with SSO via SAML 2.0. SuccessFactors will require the following information (at a minimum) in order to integrate with RSA SecurID Access IdP:

- Identity Provider URL
- Issuer Entity ID
- Signing Certificate