RSA SecurID Access SAML Configuration for Changepoint

Last Modified: January 21, 2016

Changepoint is a Business Execution Management™ company, with leading solutions to help organizations better connect corporate strategy with cross-enterprise work planning and management. More than 1,000 organizations worldwide use Changepoint to improve agility, performance, and business outcomes every year.

Before You Begin

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

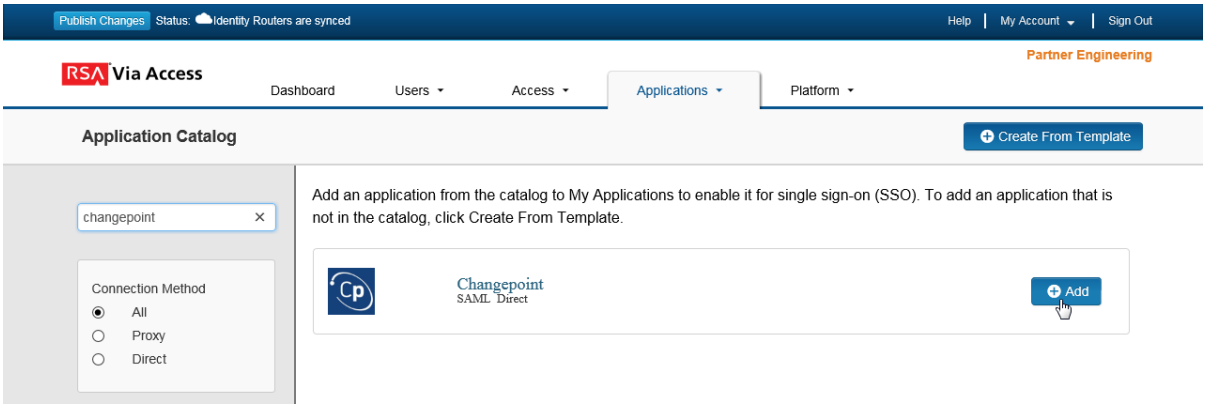
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Changepoint 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.

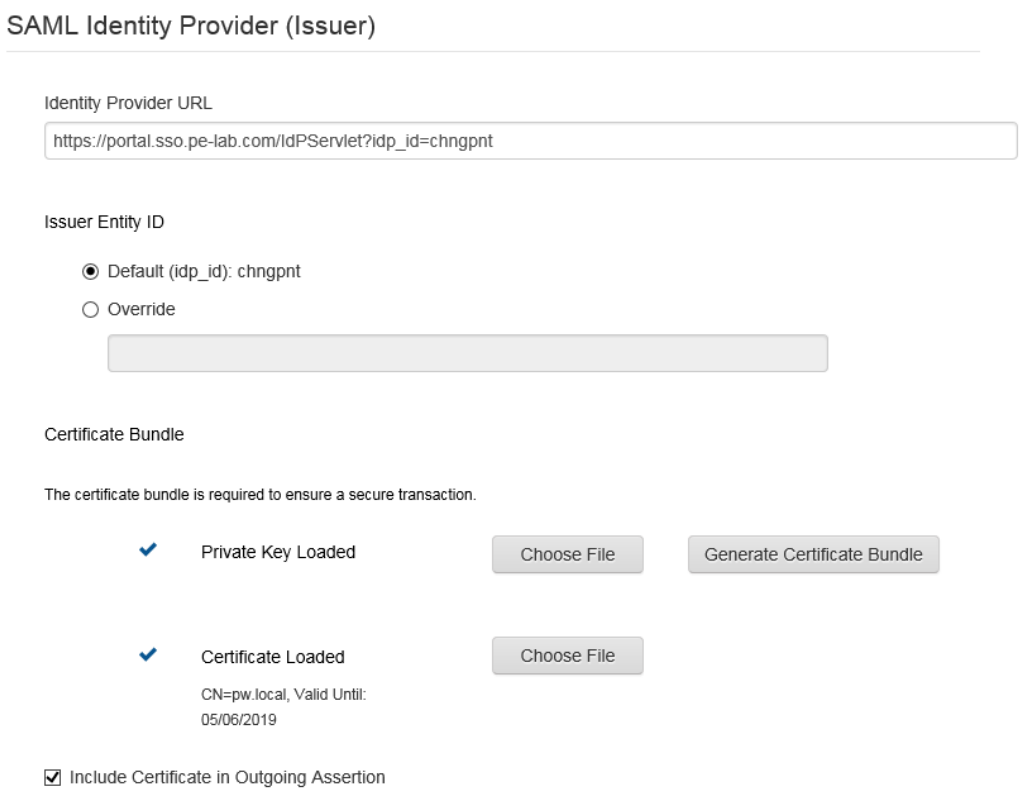


Copyright © 2016 EMC Corporation. All Rights Reserved.

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.**

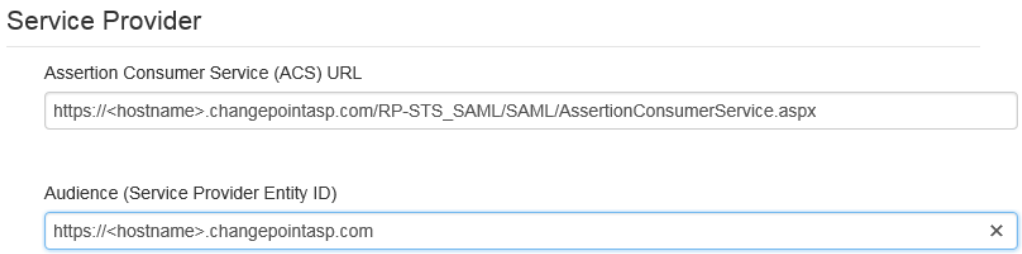
4. On the Connection Profile page choose **IDP –initiated**.
5. Scroll down to **SAML Identity Provider (Issuer)** section.



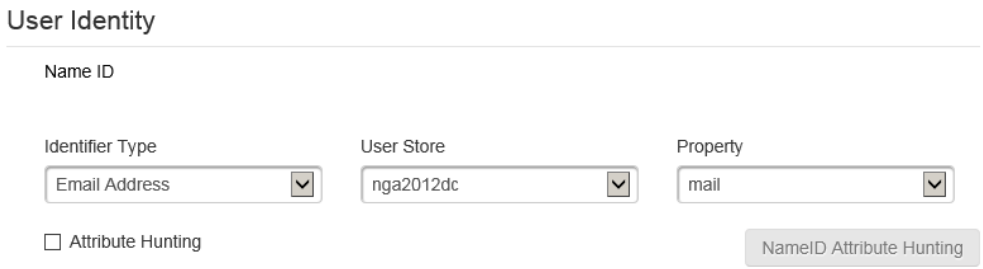
a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Service Provider configuration.
b. Take note of the **Issuer Entity ID**.
c. Select **Choose File** and upload the private key. Select **Choose File** to locate and import a private key to sign the SAML 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**.
d. Mark the checkbox to **Include Certificate in Outgoing Assertion**.

Copyright © 2016 EMC Corporation. All Rights Reserved.

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



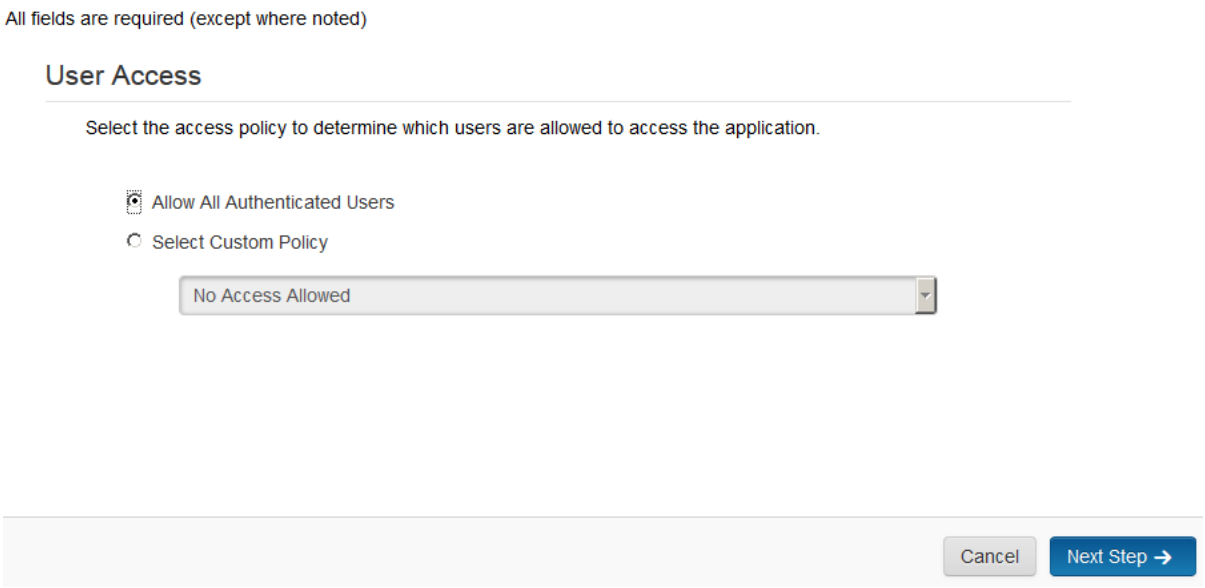
   a. In the **Assertion Consumer Service (ACS) URL** field, enter the URL you obtained from Changepoint.
   b. In the **Audience (Service Provider Entity ID)** field, enter the Entity ID you obtained from Changepoint.
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be in presented in email format and the user account will be validated again the User Store selected.



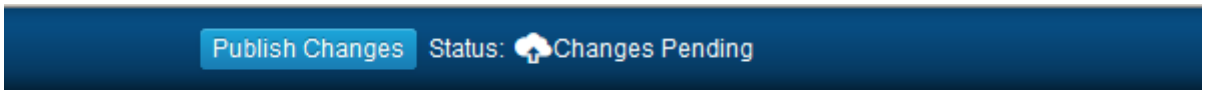
8. Click **Next Step**.

Copyright © 2016 EMC Corporation. All Rights Reserved.

9. On the **User Access** page, select the desired user policy from the drop down list.



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



Next Steps

[Configure Changepoint to Use RSA SecurID Access as an Identity Provider]

Copyright © 2016 EMC Corporation. All Rights Reserved.

Configure Changepoint to Use RSA SecurID Access as an Identity Provider

Procedure

1. Logon to the root of your Changepoint website using SFTP.
2. Navigate to /Enterprise/RP-STS_SAML/ and open the web.config file for editing.
3. Set the SAMLIdentityProvider value to match the RSA Identity Provider URL:
   Example:
   <add key="SSO.SAMLIdentityProvider" value="https://portal.sso.pe-lab.com/IdPServlet?idp_id=chngpnt" />
4. Set the SAMLIdentityProviderType value to match the RSA Issuer Entity ID.
   Example:
   <add key="SSO.SAMLIdentityProviderType" value="chngpnt" />
5. Save and close the file.

Copyright © 2016 EMC Corporation. All Rights Reserved.