RSA SecurID Access SAML Configuration for Birst

Last Modified: October 23, 2015

Birst is a cloud solution that delivers business intelligence and analytics to thousands of organizations.

Before You Begin

- Acquire Birst account.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the SecurID Access manual.

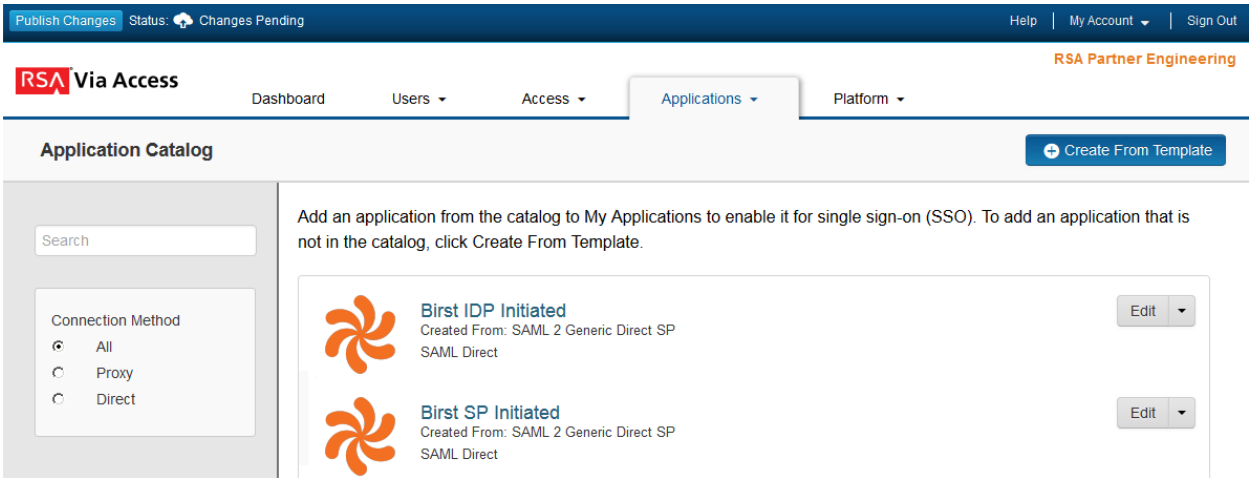
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Birst 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, search for Birst and click **+Add**.

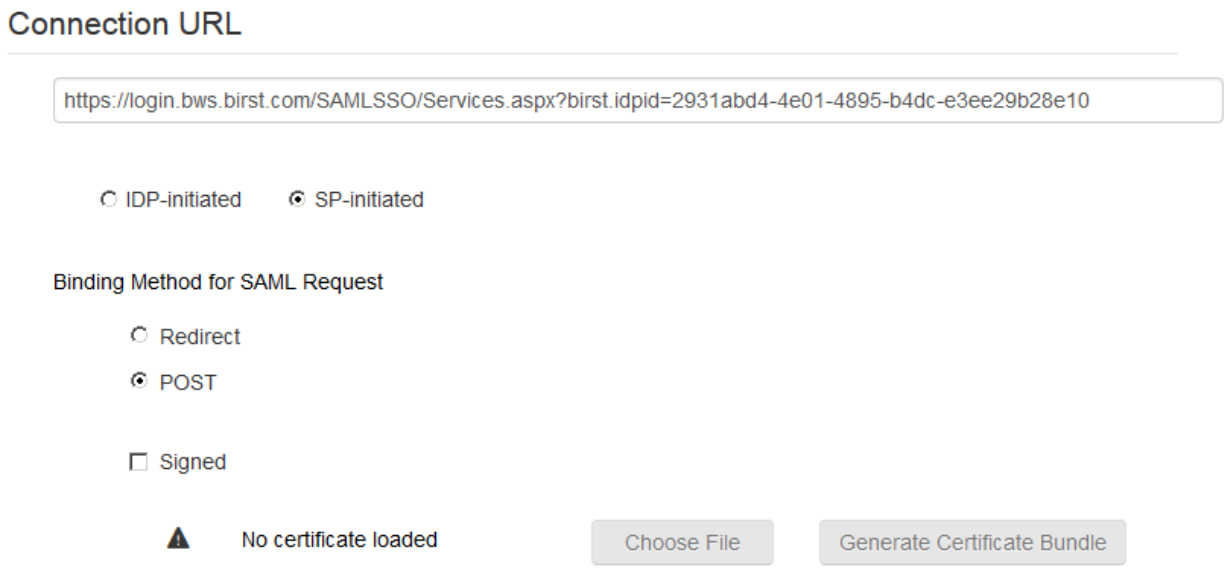


3. On the Basic Information page, specify the application name and click **Next Step**.
4. In the Connection URL field, choose **IDP-initiated** if the user will be connecting to the RSA SecurID Access portal to access the application or **SP-initiated** if the user will be connecting from the Service Provides site.

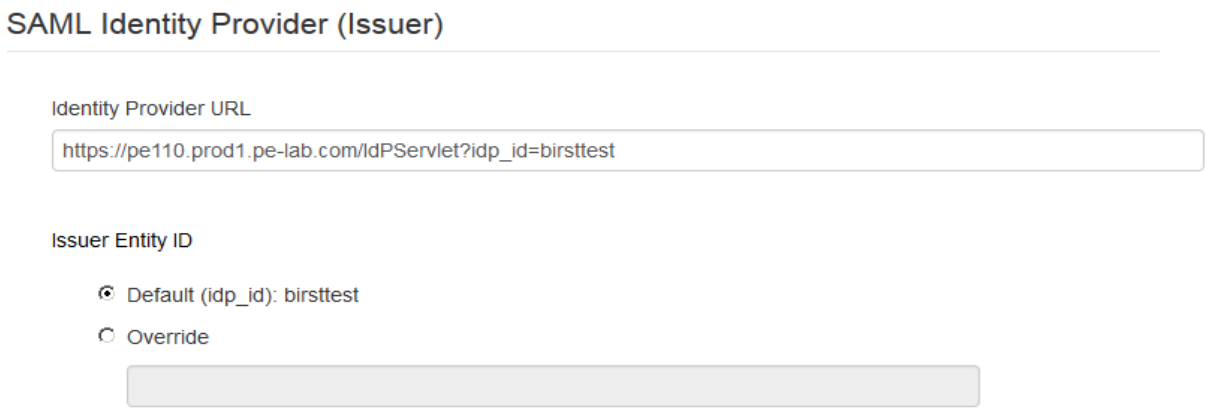
> **Note: The SP-initiated configuration works for both SP-initiated and IDP- initiated connections.**

> **Note: When configuring for IDP- initiated leave the Connection URL blank. When configuring for SP- initiated enter the connection URL provided to you by Birst. The connector URL provided by Birst will be needed to go directly to your Birst site login page.**

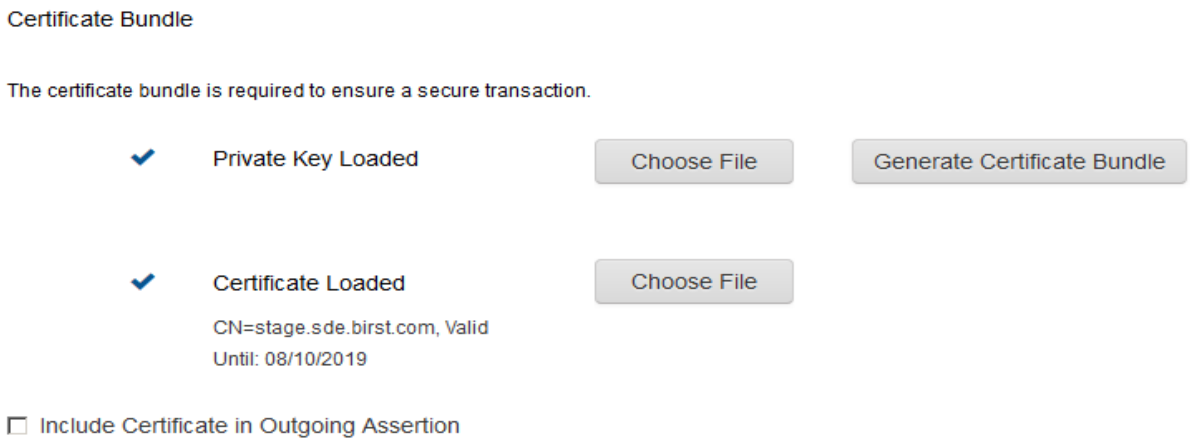
5. In this SP initiated example replace the trailing digits with your assigned birst.idpid value.



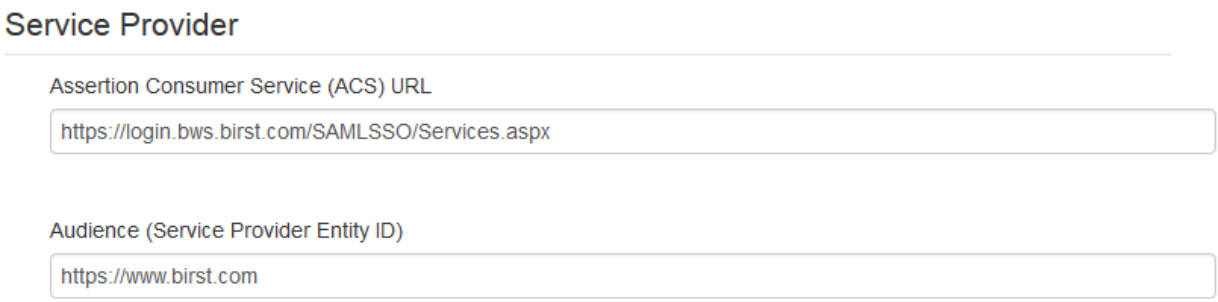
6. Scroll down to **SAML Identity Provider (Issuer)** section.
7. Take note of the Identity Provider Entity ID; it must be provided to Birst.



8. Click **Choose File** and upload the private key.
9. Click **Choose File** and upload the public certificate.



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

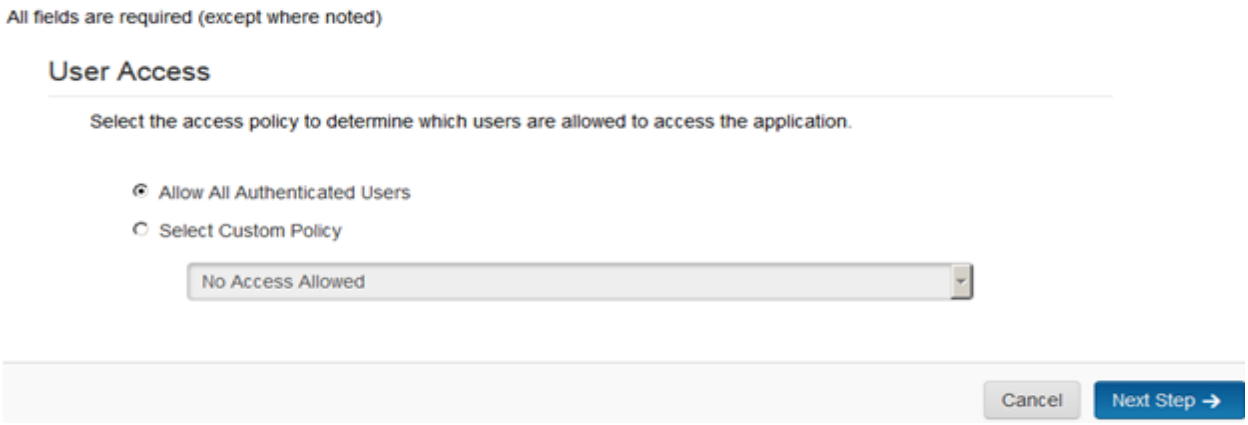


   a. In the **Assertion Consumer Service (ACS) URL** field, enter https://login.bws.birst.com/SAMLSSO/Services.aspx

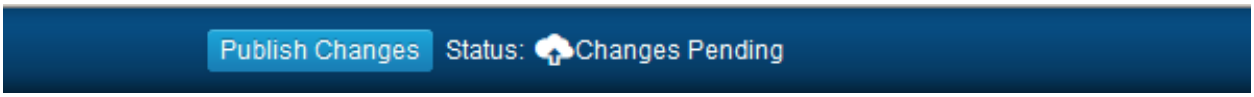
   b. In the **Audience (Service Provider Entity ID)** field, enter https://www.birst.com

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

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



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



Next Steps

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

Configure Birst to Use RSA SecurID Access as an Identity Provider

1. Contact Birst and provided them with the RSA SecurID Access Default (idp_id), found on page 3 step 5.

2. Also provide the public certificate, **cert.pem** file used on page 3 step 8.

GLS