

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.

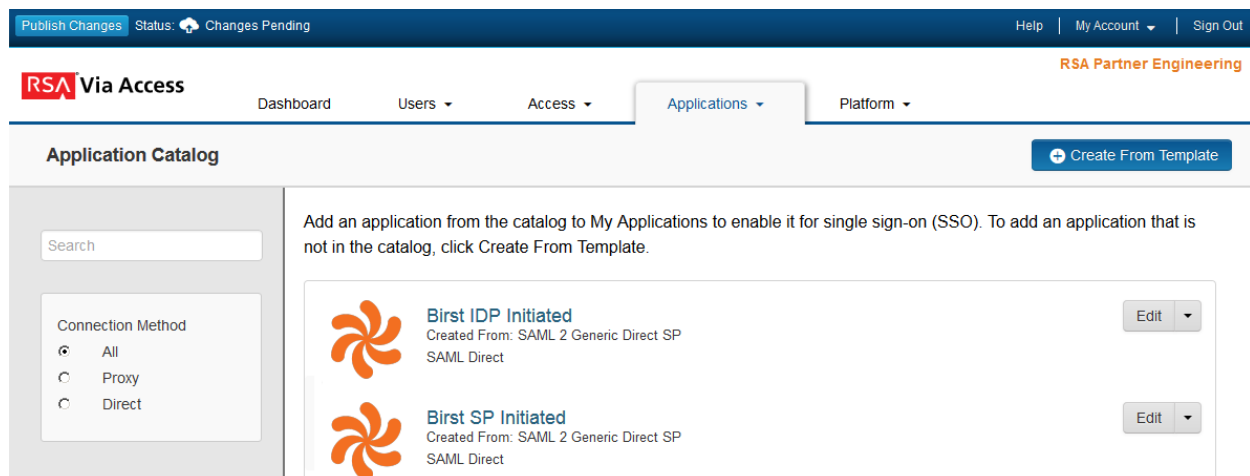
Procedure

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.

Connection URL

`https://login.bws.birst.com/SAMLSSO/Services.aspx?birst.idpid=2931abd4-4e01-4895-b4dc-e3ee29b28e10`


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

Choose File

Generate Certificate Bundle

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

SAML Identity Provider (Issuer)

Identity Provider URL

https://pe110.prod1.pe-lab.com/IdPServlet?idp_id=birsttest

Issuer Entity ID

Default (idp_id): birsttest

Override

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

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

✓ Private Key Loaded

Choose File

Generate Certificate Bundle

✓ Certificate Loaded

Choose File

CN=stage.sde.birst.com, Valid

Until: 08/10/2019

Include Certificate in Outgoing Assertion

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

Service Provider

Assertion Consumer Service (ACS) URL

<https://login.bws.birst.com/SAMLSSO/Services.aspx>

Audience (Service Provider Entity ID)

<https://www.birst.com>

- 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**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

↓ Show Advanced Configuration

12. Click **Next Step**.

13. 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 →


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.

Publish Changes

Status:  Changes Pending

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.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): birsttest

Override

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