

Last Modified: August 31, 2015

Blue Jeans is a cloud-based video conferencing service that enables you to connect with your colleagues, customers, partners, suppliers and social network any time, any place, and from any device.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Blue Jeans.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

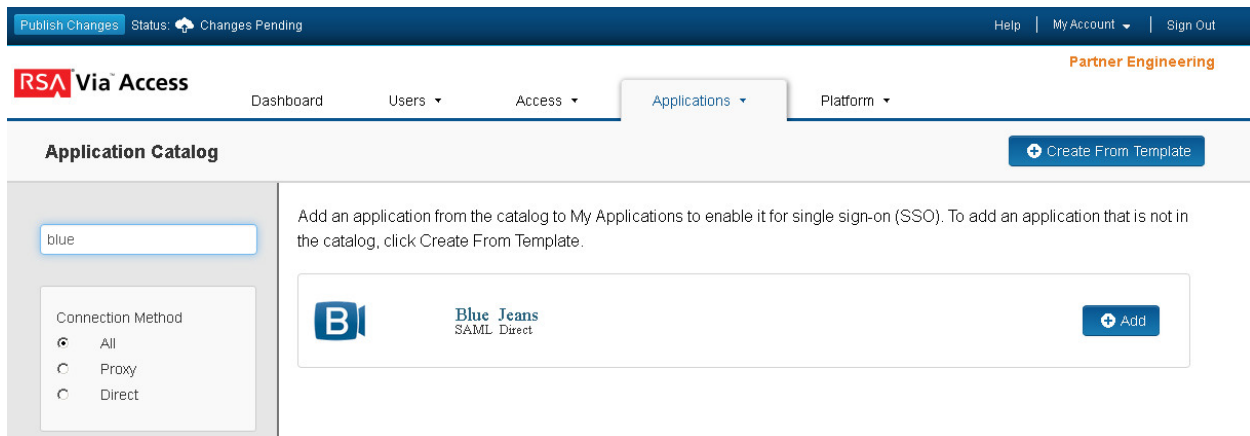
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Blue Jeans 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.



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. In the **Connection URL** field, enter the value from page 7 step 14 of the Blue Jeans configuration.

Connection URL

eyJncm91cCI6Njk4OCwibW9kZSI6ImF1dGgifQ==

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed



No certificate loaded

Choose File

Generate Certificate Bundle

6. Scroll down to the **SAML Identity Provider ("Issuer")** section. Take note of the Issuer Entity ID default value. This is need on page 6 step 9 of the Blue Jeans configuration.

SAML Identity Provider (Issuer)

Identity Provider URL

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

Issuer Entity ID

Default (idp_id): bluejeanstest

Override

7. Select **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

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

Service Provider

Assertion Consumer Service (ACS) URL

<https://bluejeans.com/sso/saml2/>

Audience (Service Provider Entity ID)

<http://samlsp.bluejeans.com>

- a. In the **Assertion Consumer Service(ACS) URL** field, enter <https://bluejeans.com/sso/saml2/>
 - b. In the **Audience (Service Provider Entity ID)** field, enter <http://samlsp.bluejeans.com>.
9. 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

nga2012dc

Property

mail

10. Click **Show Advanced Configuration**.

11. Scroll down to **Uncommon Formatting SAML Response Options**.
12. Under **Sign Outgoing Assertion** and select **Assertion within response**.

Uncommon Formatting SAML Response Options


Sign Outgoing Assertion


- Entire SAML response Assertion within response

Signature Algorithm

Digest Algorithm

- Encrypt Assertion

 No certificate loaded

 Encryption Algorithm

Encryption Key Transport

Relay State URL Encoding

- Receive Relay State URL - encoded by SP (in incoming request)

- Send Relay State URL - encoded by IDP

- Include Issuer NameID Format

NameID Format

13. Click **Next Step**.

14. 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 →


15. Click **Next Step**.

16. On the **Portal Display** page, select **Display in Portal**.

17. Click **Save and Finish**.

18. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

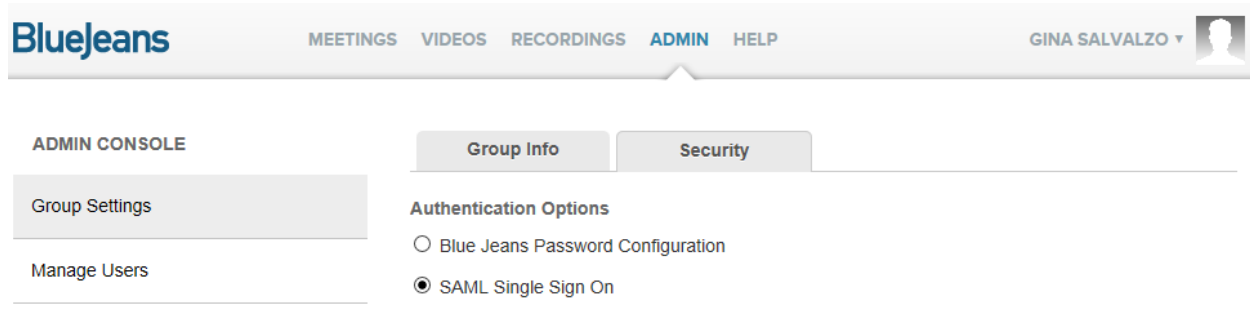
Next Steps

[Configure Blue Jeans to Use RSA SecurID Access as an Identity Provider](#)

Configure Blue Jeans to Use RSA SecurID Access as an Identity Provider

Procedure

1. Contact Blue Jeans support and ask for a "Custom Landing Page" for single sign-on.
2. Login with your admin account.
3. Navigate to the **ADMIN** page.
4. Choose the **Security** tab.
5. Select **SAML Single Sign On**.



6. Choose **Enable automatic preference**.
7. Select **Choose File** and upload the RSA SecurID Access public certificate.

The following configuration will allow you to setup Single Sign On for your group. For more information on Single Sign On, please visit our [Help Page](#)

Enable automatic provisioning

Certificate Path

Currently: [sso/certs/6988/cert.pem](#)

Change:

8. In the **Login URL** field, enter the Identity Provider URL from step 6 of the RSA SecurID Access configuration.
9. In the **Password Change URL** field, enter your Custom Login Page URL.

Login URL

URL for signing into the remote authentication system

Password Change URL

URL to allow users to change their password

10. In the **Logout URL** field, enter a URL to redirect user to on logout.
11. In the **Custom Error Page URL** field, enter a URL to redirect a user to on an error.

Logout URL

URL to which a user is redirected to on logout

Custom Error Page URL

URL to which a user is redirected to on an error

12. Copy the **Relay State** and enter it in the Connection URL field in step 5 of the RSA SecurID Access configuration.
13. Select **Pick User ID from <saml2:NameID> element**.
14. In the Email field, type **Email**.

RelayState

For IdP initiated SSO, configure your IdP with the following RelayState

[Copy to clipboard](#)

Pick User Id from <saml2:NameID> element

Email *

Username

First Name

Last Name

Title

Phone

Company

15. Click **Save Changes**.