

Last Modified: February 9, 2015

Jive is a cloud based collaboration solution for businesses.

Before You Begin

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

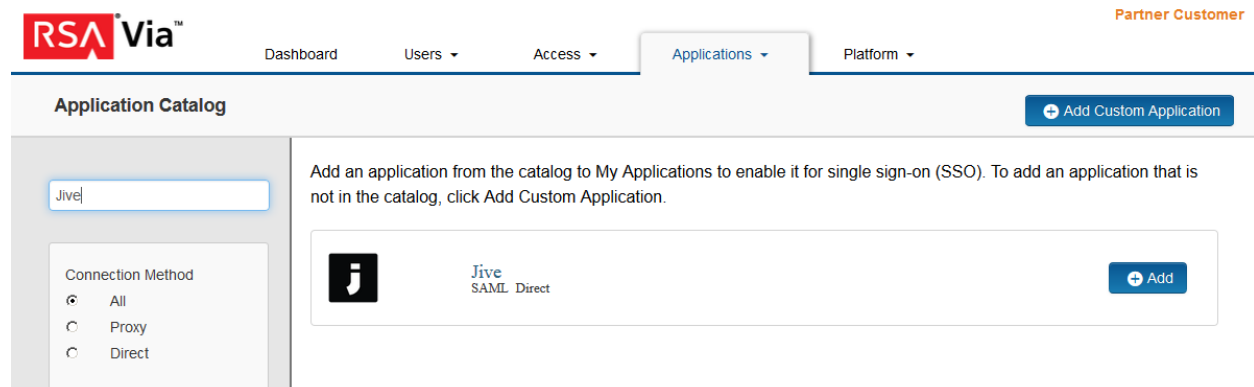
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Jive 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 SP-initiated configuration works for both IDP-initiated and SP-initiated connections.

4. In the **Connection URL** field enter your Jive login URL.
<https://<your instance>.jiveon.com>
5. Choose **SP -initiated** and **POST**.

Connection URL


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

6. Scroll down to the **SAML Identity Provider (Issuer)** section.
7. Take note of the Issuer Entity ID, it will be needed later when configuring Jive.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): jive

Override

- Click **Choose File** and upload the private key.
- Select **Include Certificate in Outgoing Assertion**, click **Choose File**, and upload the public key file **cert.pem**.

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

private key

Include Certificate in Outgoing Assertion

cert.pem

Certificate valid until: Sat Aug 05 19:11:46 UTC 2017

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


Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

- In the **Assertion Consumer Service (ACS) URL** field, replace <your_instance> with your company's Jive url. https://<your_instance>.jiveon.com/saml/sso
- In the **Audience (Service Provider Entity ID)** field, replace <your_instance> with your company's Jive url. https://<your_instance>.jiveon.com

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

 **Note:** Jive's default setting is to use "uid" for matching. Verify you have a "uid" value set on your Active Directory user's account.

User Identity

Name ID

Identifier Type

User Store

Property

- Click **Show Advanced Configuration**.








13. Scroll down to **Attribute Extension**.

 **Note:** Jive requires three attributes to be sent; email, first name, and last name.

14. Add **Attribute Name** for email, First name, and Last name.

Attribute Extension

Attribute Hunting Attribute Hunting Details

Attribute Source	Attribute Name	User Store	Property	Manage
User Store	email	PE_AD	mail	 
User Store	Firstname	PE_AD	givenName	 
User Store	Lastname	PE_AD	sn	 
 ADD				

15. Click **Next Step**.

16. 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

17. Click **Next Step**.

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

19. Click **Save and Finish**.

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

Publish Changes Status:  Changes Pending

Create the RSA SecurID Access Metadata file

1. Modify the example below with your environment information.
2. When inserting the cert.pem file do not include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----lines.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<EntityDescriptor xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="CHANGEME_TO_CONNECTOR_IDP_ENTITY_ID">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <!-- public saml cert -->
          <ds:X509Certificate>CHANGEME_TO_PUBLIC_SAML_CERT_CONTENT</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>

    <!-- Supported Name Identifier Formats -->
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</NameIDFormat>

    <!-- POST binding and location=idp url -->
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="CHANGEME_TO_IDP_URL" />

  </IDPSSODescriptor>
</EntityDescriptor>
```

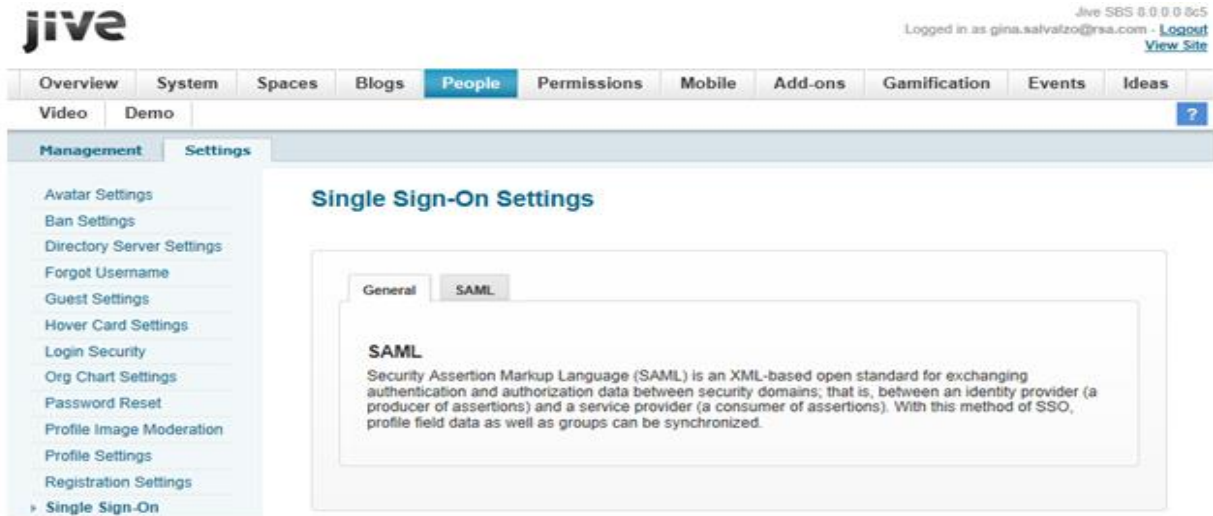
Next Steps

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

Configure Jive to Use RSA SecurID Access as an Identity Provider

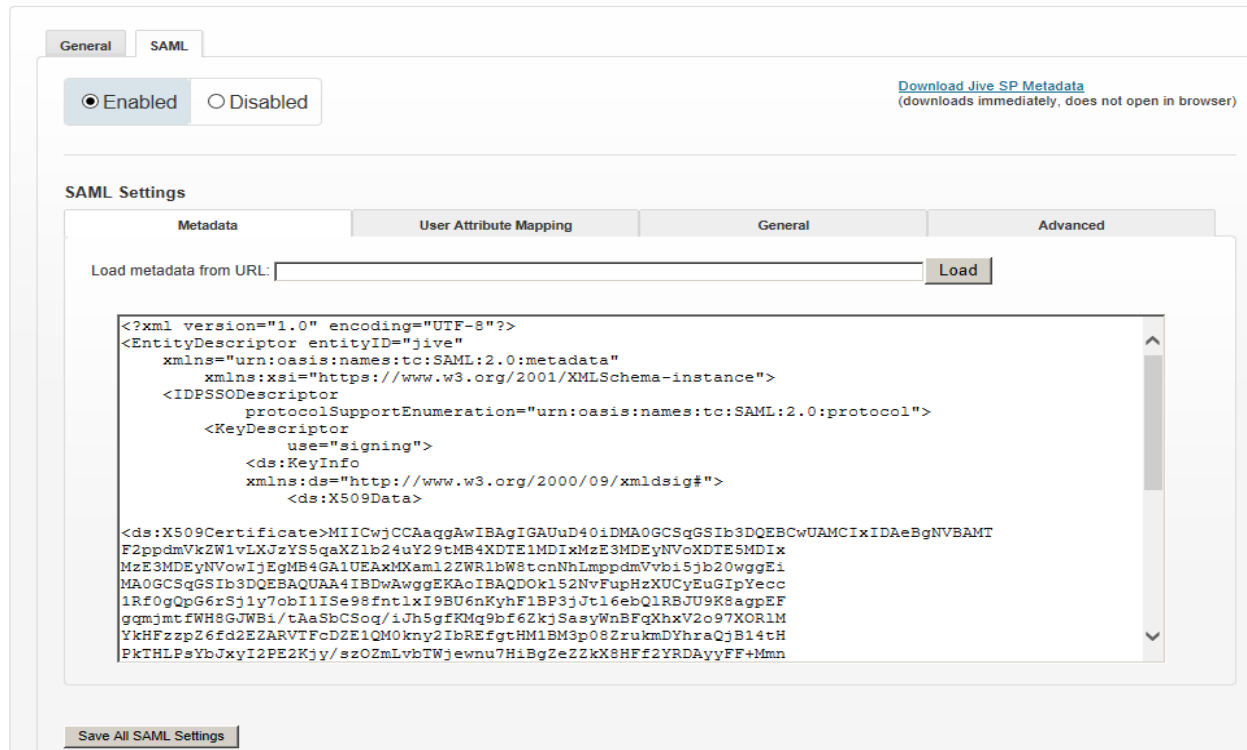
Procedure

1. Login into the Jive administration console.
http://<your_instance>.jiveon.com/admin/main.jsp
2. Navigate to **People >Settings >Single Sign-On.**



3. Select the **SAML** tab.
4. Select **Enabled**.
5. Paste your metadata file into the metadata window and click **Save All SAML Settings**.

Single Sign-On Settings



6. Select the **User Attribute Mapping** tab.
7. Enter the Identity Provider's attribute name for **Email**, **First Name**, and **Last Name** and check **Federated**.

SAML Settings

Metadata	User Attribute Mapping	General	Advanced																		
	<table border="1"> <thead> <tr> <th>Name</th> <th>Attribute Name</th> <th>Federated</th> </tr> </thead> <tbody> <tr> <td>External Identifier:</td> <td>Use Subject NameID or <input type="checkbox"/> Override with Assertion Attribute</td> <td></td> </tr> <tr> <td>Username:</td> <td>Use Subject NameID or <input type="checkbox"/> Override with Assertion Attribute</td> <td></td> </tr> <tr> <td>Email:</td> <td><input type="text" value="email"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>First Name:</td> <td><input type="text" value="Firstname"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Last Name:</td> <td><input type="text" value="Lastname"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Name	Attribute Name	Federated	External Identifier:	Use Subject NameID or <input type="checkbox"/> Override with Assertion Attribute		Username:	Use Subject NameID or <input type="checkbox"/> Override with Assertion Attribute		Email:	<input type="text" value="email"/>	<input checked="" type="checkbox"/>	First Name:	<input type="text" value="Firstname"/>	<input checked="" type="checkbox"/>	Last Name:	<input type="text" value="Lastname"/>	<input checked="" type="checkbox"/>		
Name	Attribute Name	Federated																			
External Identifier:	Use Subject NameID or <input type="checkbox"/> Override with Assertion Attribute																				
Username:	Use Subject NameID or <input type="checkbox"/> Override with Assertion Attribute																				
Email:	<input type="text" value="email"/>	<input checked="" type="checkbox"/>																			
First Name:	<input type="text" value="Firstname"/>	<input checked="" type="checkbox"/>																			
Last Name:	<input type="text" value="Lastname"/>	<input checked="" type="checkbox"/>																			

8. Select the **Advanced** tab.

SAML Settings

Metadata	User Attribute Mapping	General	Advanced
	<input type="checkbox"/> Request Signed:		
	<input type="text" value="https://jivedemo-rsa.jiveon.com"/> Base metadata URL:		
	<input type="checkbox"/> Enable Username Confirmation for New Users:		
	<input type="checkbox"/> Enable Email Confirmation for New Users:		
	<input type="checkbox"/> Allow Federated Users to Change Name:		
	<input type="checkbox"/> External Identity is Case-Sensitive:		
	<input type="checkbox"/> Force Authentication:		
	<input type="checkbox"/> Enable Passive Authentication:		
	<input type="checkbox"/> Use Lenient mode for Passive Authentication:		
	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/> NameID Format:		
	<input checked="" type="checkbox"/> NameID Allow Create:		
	<input type="checkbox"/> Sign Metadata:		
	<input type="checkbox"/> IDP Want Response Signed		
	<input type="text"/> Requested AuthnContext:		
	<input type="text"/> Requested AuthnContext Comparison:		
	<input type="text" value="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/> RSA Signature Algorithm URI:		
	<input type="checkbox"/> Group Mapping Enabled:		
	<input type="checkbox"/> Require Valid Metadata		
	<input type="checkbox"/> Include Scoping:		
	<input type="text" value="2"/> Proxy Count:		
	<input checked="" type="checkbox"/> Validate InResponseTo		

9. Enter the **NameID Format**.
10. Click **Save All SAML Settings**.