

Last Modified: November 21, 2014

Jira is an issue tracking system.

Before You Begin

- Host your own instance of Jira.
- Acquire an administrator account to RSA SecurID Access.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the RSA SecurID Access manual.

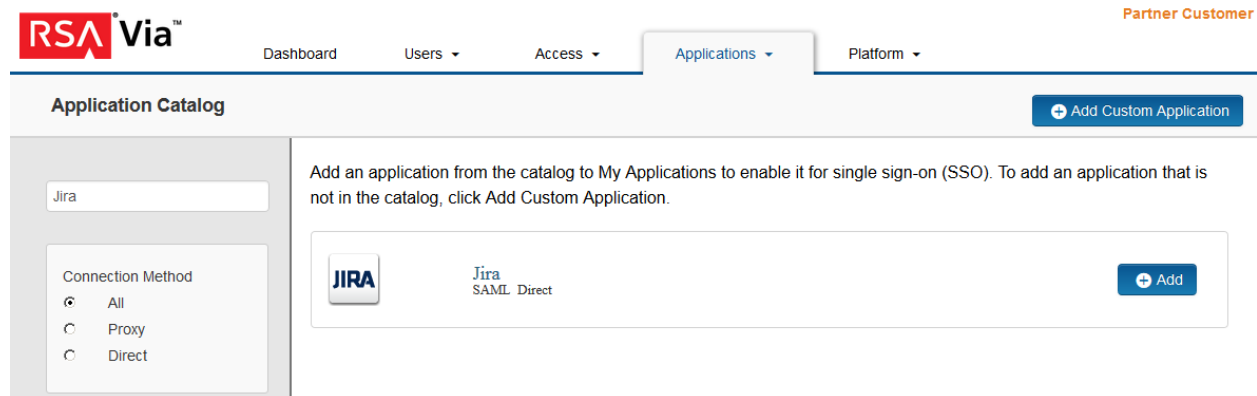
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure the Service Provider 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**.
4. In the **Connection URL** field, enter the URL to the Jira home page.
5. Choose **SP -initiated** and binding method **POST**.

Connection URL

https://<your_instance>/secure/Dashboard.jspa


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. Select **Override** and copy and paste the Identity Provider URL in to the field.

SAML Identity Provider (Issuer)

Identity Provider URL

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

Issuer Entity ID

Default (idp_id): jiratest

Override

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

8. Click **Choose File** and upload the private key.

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.



private.key

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion



No certificate loaded

Choose File

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

Service Provider

Assertion Consumer Service (ACS) URL

http://x.x.x.x:8080/plugins/servlet/samlss0

Audience (Service Provider Entity ID)

http://x.x.x.x:8080/plugins/servlet/samlss0

- a. In the **Assertion Consumer Service (ACS) URL** field, enter the URL you obtained from the plugin metadata file from page 7 step 8. The ACS URL is the Location URL in the metadata file.
- b. In the **Audience (Service Provider Entity ID)** field, enter the Entity ID you obtained from the plugin metadata file from page 7 step 8.

10. Scroll down to the **User Identity** section. Set the **Identifier Type** to **unspecified** and **Property** to **mail**.

User Identity

Name ID

Identifier Type

unspecified

User Store

PE_AD

Property

mail

⌵ Show Advanced Configuration

11. Click **Show Advanced Configuration**.
12. Scroll down to **Uncommon Formatting SAML Response Options**.
13. Under Sign Outgoing Assertion, select **Assertion within response**.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

Entire SAML response Assertion within response

Signature Algorithm rsa-sha1

Digest Algorithm sha1

Encrypt Assertion

⚠ No certificate loaded

Choose File

14. Click **Next Step**.

15. 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 →


16. Click **Next Step**.

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

18. Click **Save and Finish**.

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

Publish Changes

Status:  Changes Pending

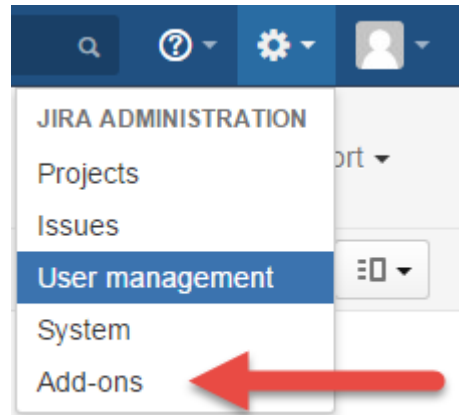
Next Steps

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

Configure Jira to Use RSA SecurID Access as an Identity Provider


Procedure

1. Login to Jira with the administrator account.
2. Under the gear icon, select **Add-ons**.



3. Search for **SAML SingleSignOn for JIRA**.

SAML Search results All categories Paid or free




SAML SingleSignOn for JIRA
resolution Reichert Network Solutions GmbH • Vendor supported
DASHBOARD GADGETS

★★★★ (4)
430 downloads
Paid via Atlassian

[Buy now](#)
[Manage](#)

With SAML Single Sign-On, the user authentication is delegated to a SAML 2.0 Identity Provider. Users already authenticated at the IdP are not asked again for their credentials.

4. Install the add-on.
5. Select **Manage Add-ons**.
6. Expand add-ons and click **Configure**.

▼  **SAML SingleSignOn for JIRA**

SAML 2.0 based Single Sign On for JIRA

Your trial is expiring on 24/May/15. Buy a license (unknown price) for this add-on.

[Configure](#) [Buy now](#) [Uninstall](#) [Disable](#)

7. The SAMLSSO plugin configuration window will open.

SAMLSSO plugin configuration

Configure the SSO settings here

Show Metadata

Opens a new browser window with SAML metadata for the Identity Provider configuration

IdP URL

SAML Identity provider URL. For ADFS this is usually https://<your-adfs-server>/adfs/ls

Redirect login requests

Check to redirect login requests to this plugin instead of the login page. If unchecked, SSO is working using the plugin url /plugins/servlet/samlssso only.

IdP Certificate (Base64)

Base64 encoded IdP Token Signing Certificate including the BEGIN and END CERTIFICATE lines. Leave empty to disable certificate validation.

8. Click **SAML Metadata**; copy the entityID and Location URLs need to configure the SecurID Access Service Provider fields on page 3 step 9.
9. Enter the SecurID Access Identity URL in the **IdP URL** field.
10. Paste the SecurID Access public certificate file in the **Idp Certificate** file, including the Begin and End statement.
11. Click **Show advanced settings**.
12. Add the user group you want to enable SAML for.

Groups

Groups to add user to on first login. Separate group names with ';', e.g. 'jira-users,jira-developers'.

 **Note:** User groups can be found under the User Management menu.

13. Select **Save settings**.

AN