RSA SecurID Access SAML Configuration for Jira

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.

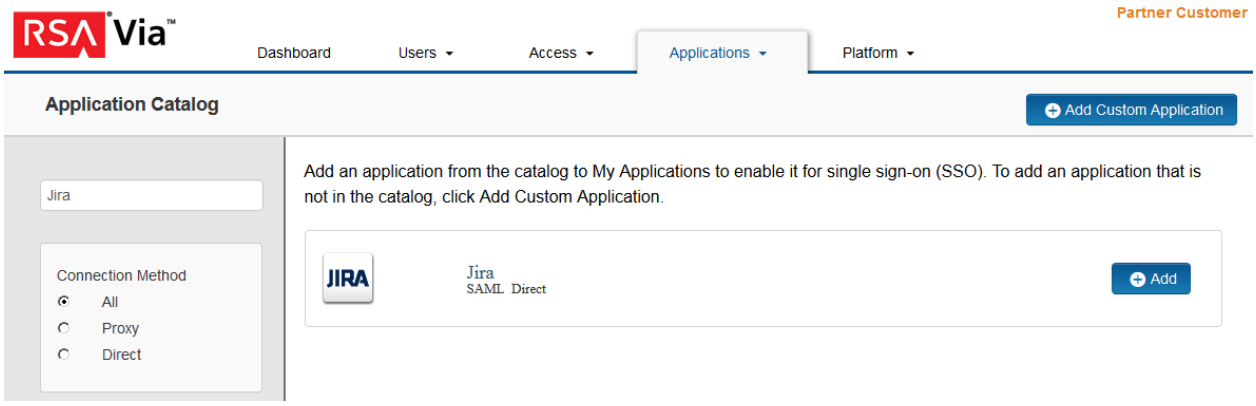
Procedure

1. Add the Application in RSA SecurID Access
2. Configure the Service Provider to Use RSA SecurID Access as an Identity Provider

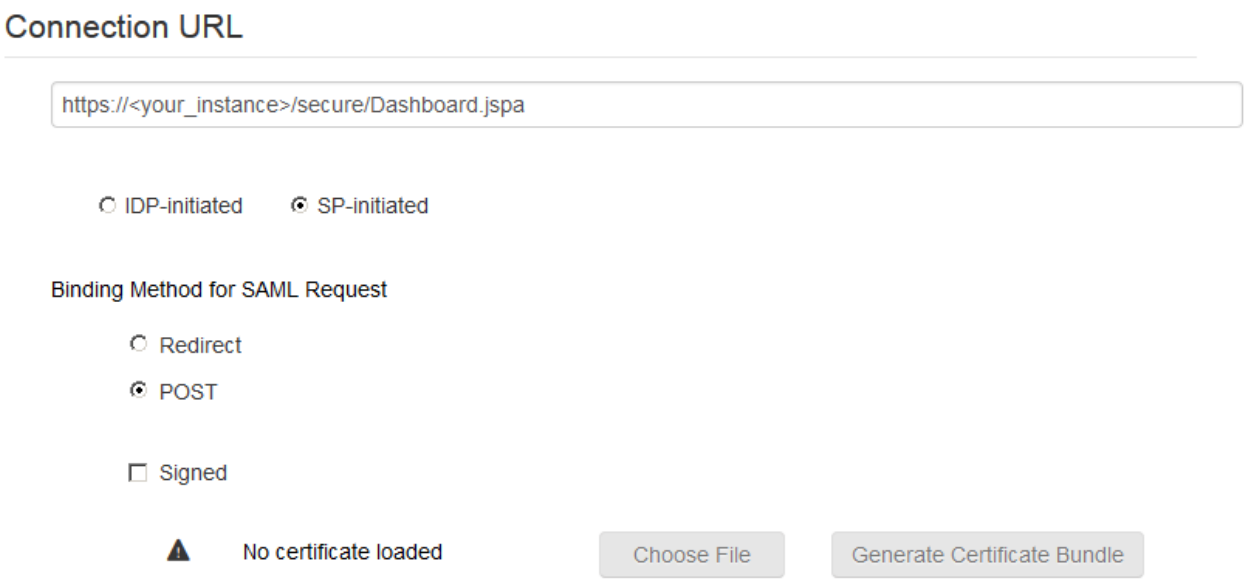
Add the Application in RSA SecurID Access

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.

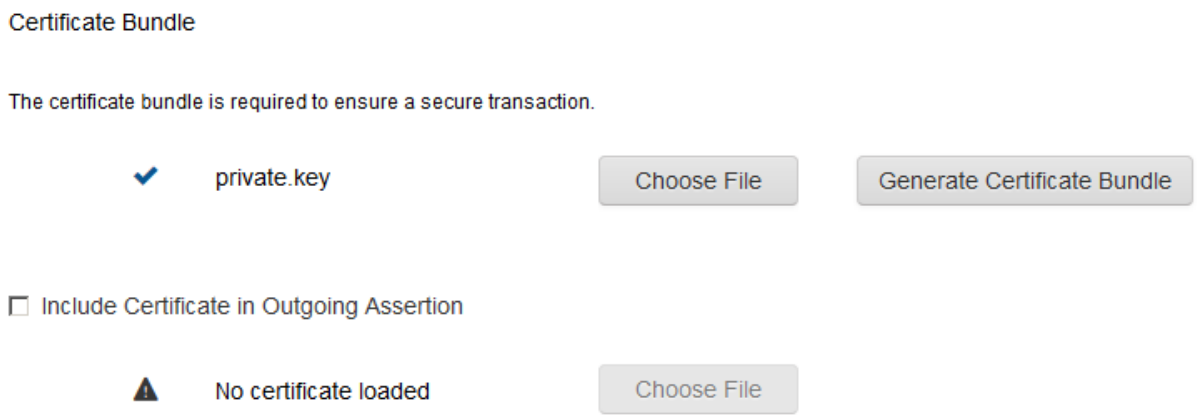


3. On the Basic Information page, specify the application name and click **Next Step**.
4. In the **Connection URL** field, enter the URL to the Jira home page.
5. Choose **SP -initiated** and binding method **POST.**



6. Scroll down to **SAML Identity Provider (Issuer)** section.
7. Select **Override** and copy and paste the Identity Provider URL in to the field.

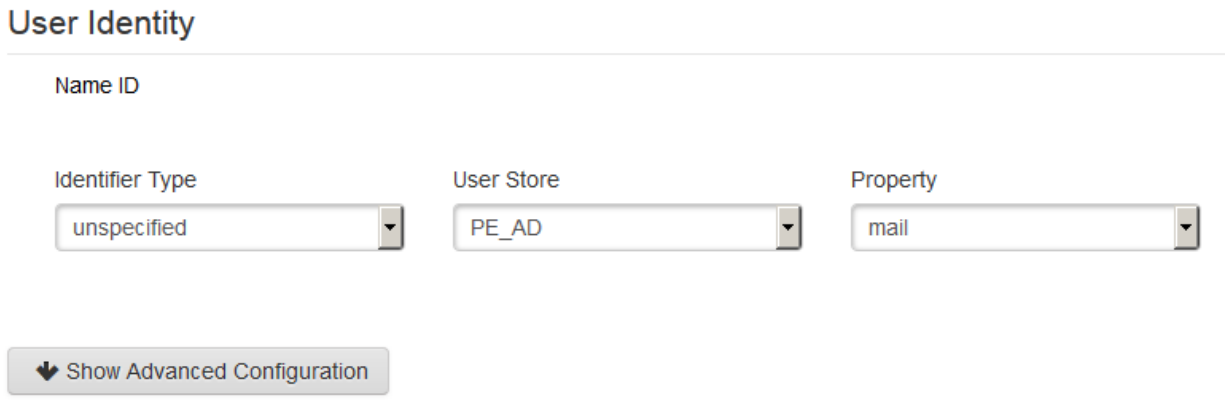
8. Click **Choose File** and upload the private key.



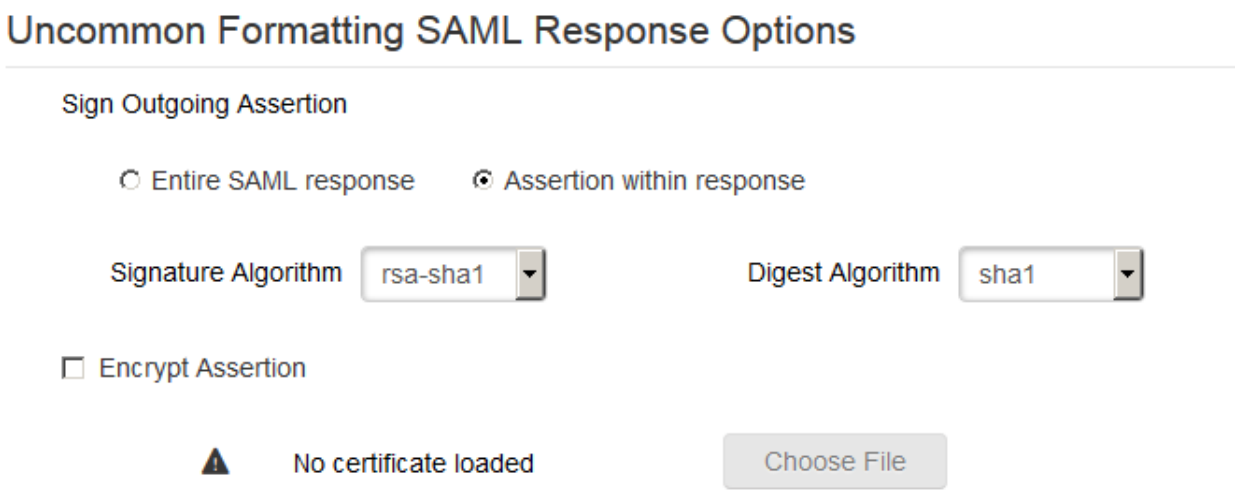
9. Scroll down to the **Service Provider** section.

   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**.

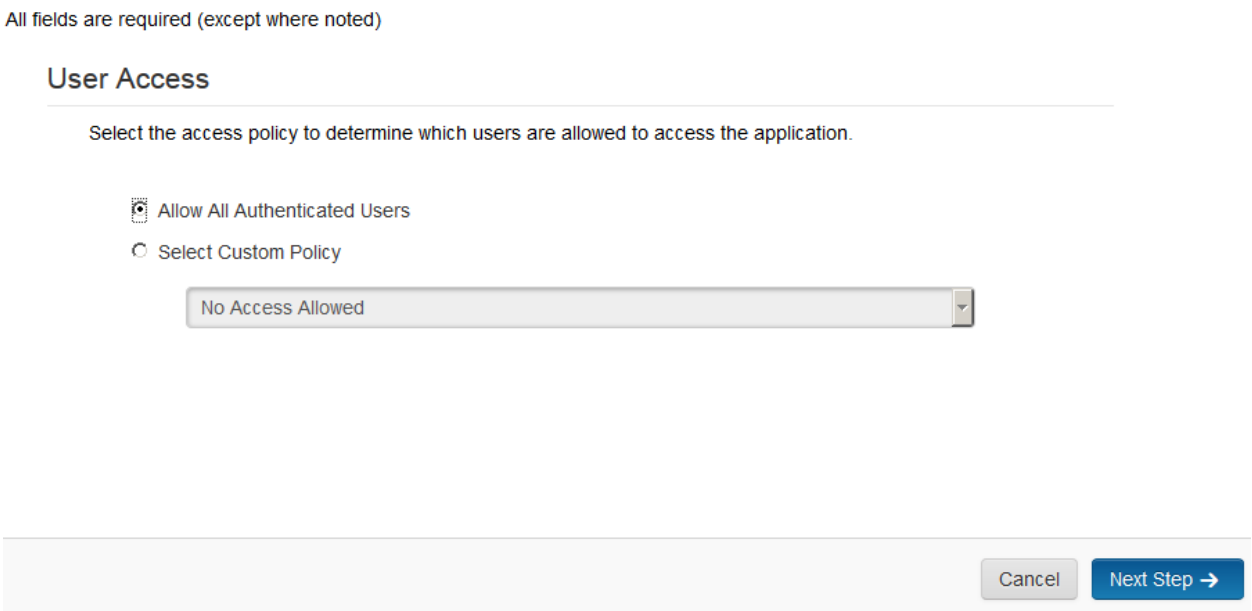


11. Click **Show Advanced Configuration**.
12. Scroll down to **Uncommon Formatting SAML Response Options**.
13. Under Sign Outgoing Assertion, select **Assertion within response**.

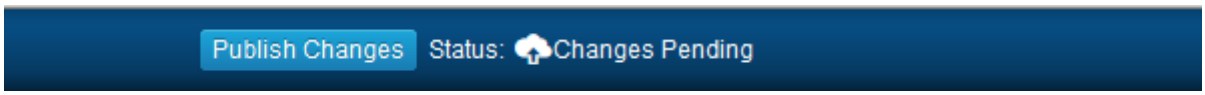


14. Click **Next Step**.

15. On the **User Access** page, select the desired user policy from the drop down list.



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.



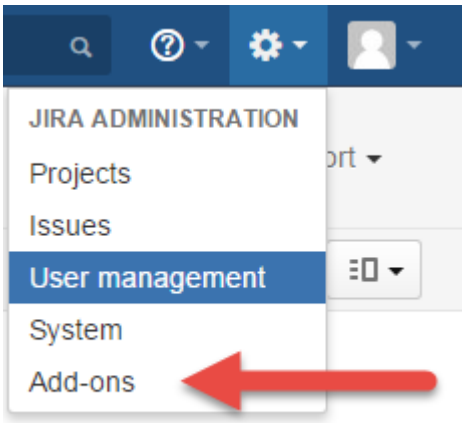
Next Steps

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

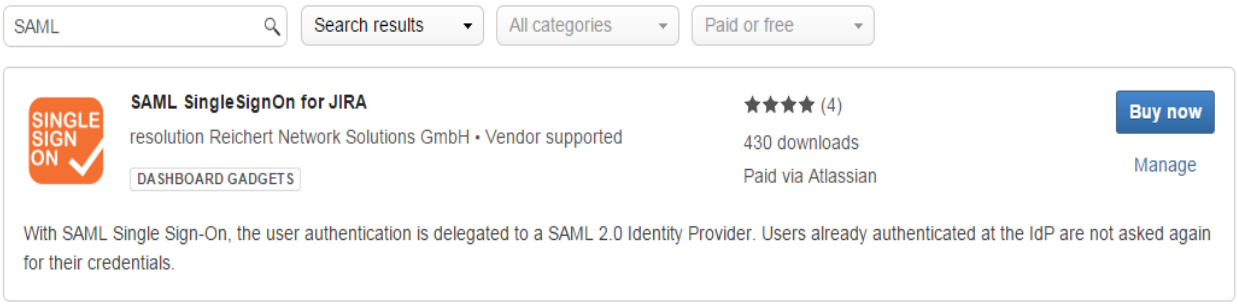
Configure Jira to Use RSA SecurID Access as an Identity Provider

Procedure

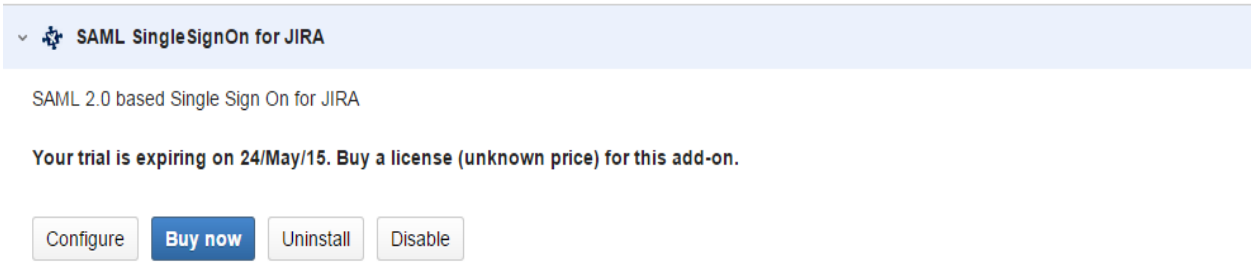
1. Login to Jira with the administrator account.
2. Under the gear icon, select **Add-ons**.



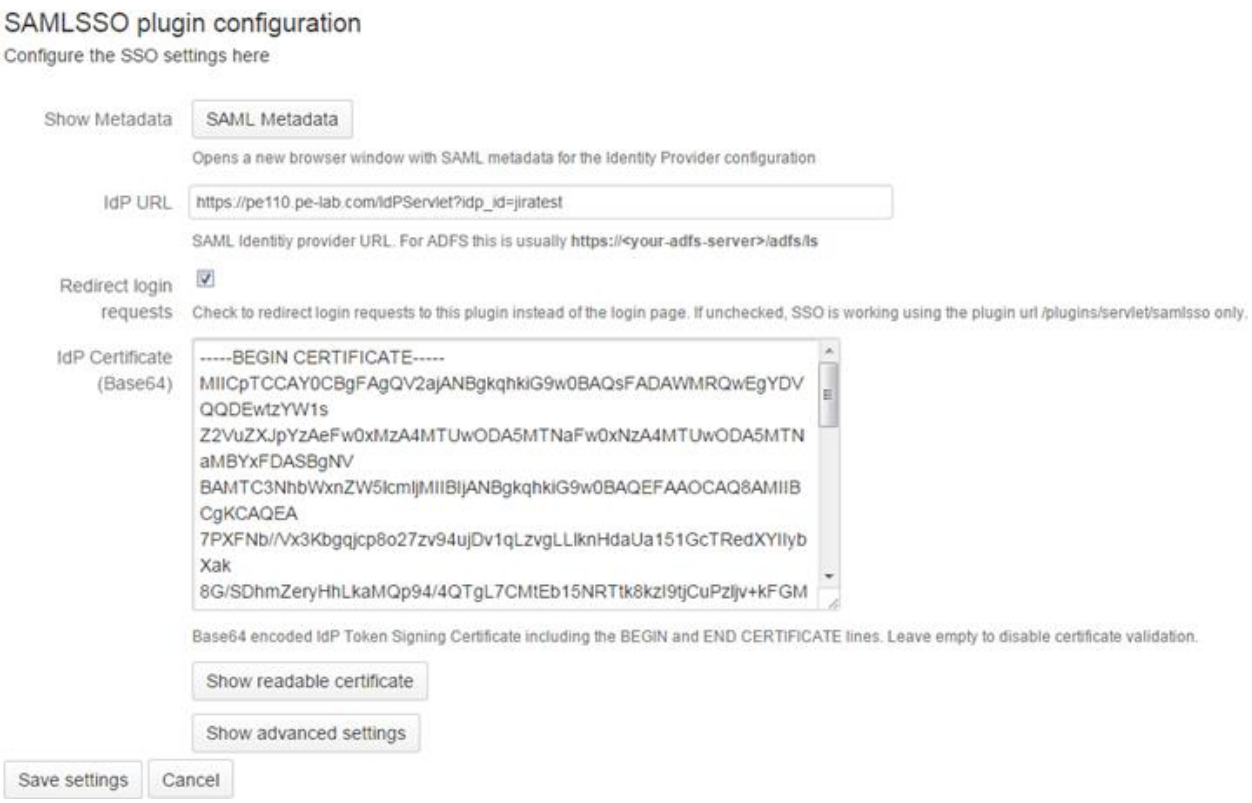
3. Search for **SAML SingleSignOn for JIRA**.



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



7. The SAMLSSO plugin configuration window will open.



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.

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

13. Select **Save settings**.

AN