RSA SecurID Access SAML Configuration for Kintone

Last Modified: June 9, 2017

Kintone product is a social collaboration cloud service that provides communication, data, and business process management in one portal. The Kintone portal provides a single point of contact for a new generation of small and large businesses, where team members around the globe can share data and communications in one place.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Kintone.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	*https://<DOMAIN>.kintone.com/login*
ACS URL	*https://<DOMAIN>.kintone.com/saml/acs*
Service Provider Issuer ID	*https://<DOMAIN>.kintone.com*

Note: Replace <DOMAIN> with your account specific unique web domain.

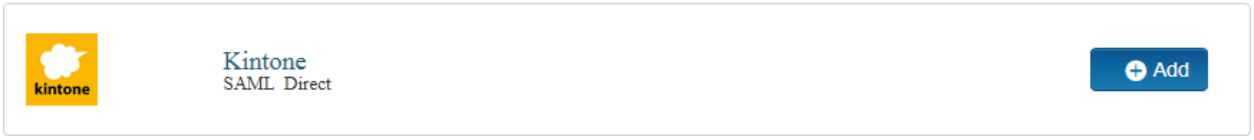
Procedure

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

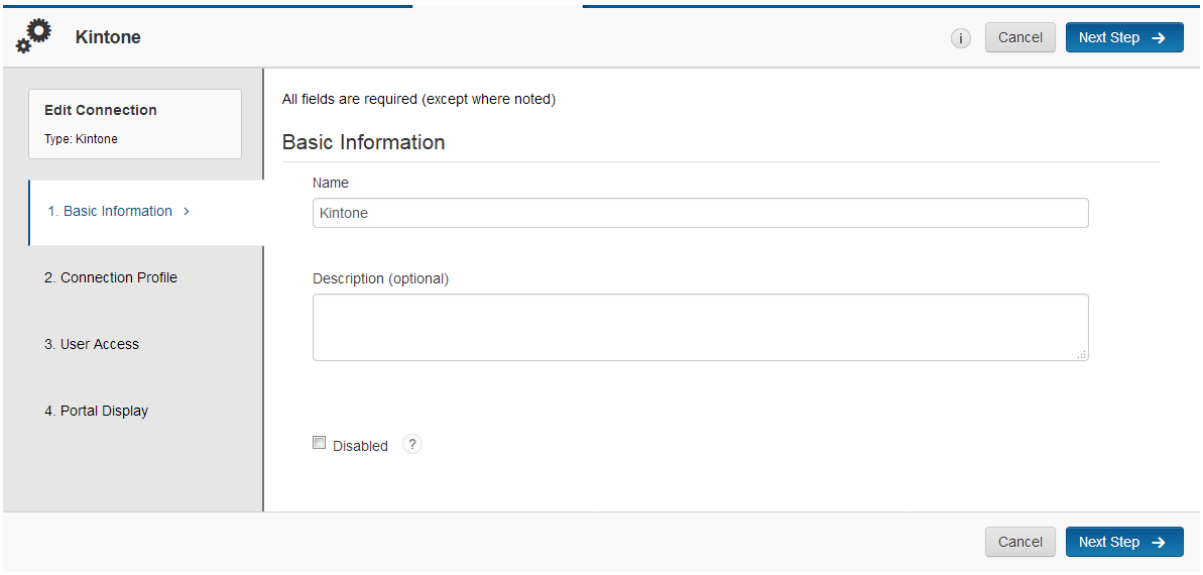
Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Kintone.

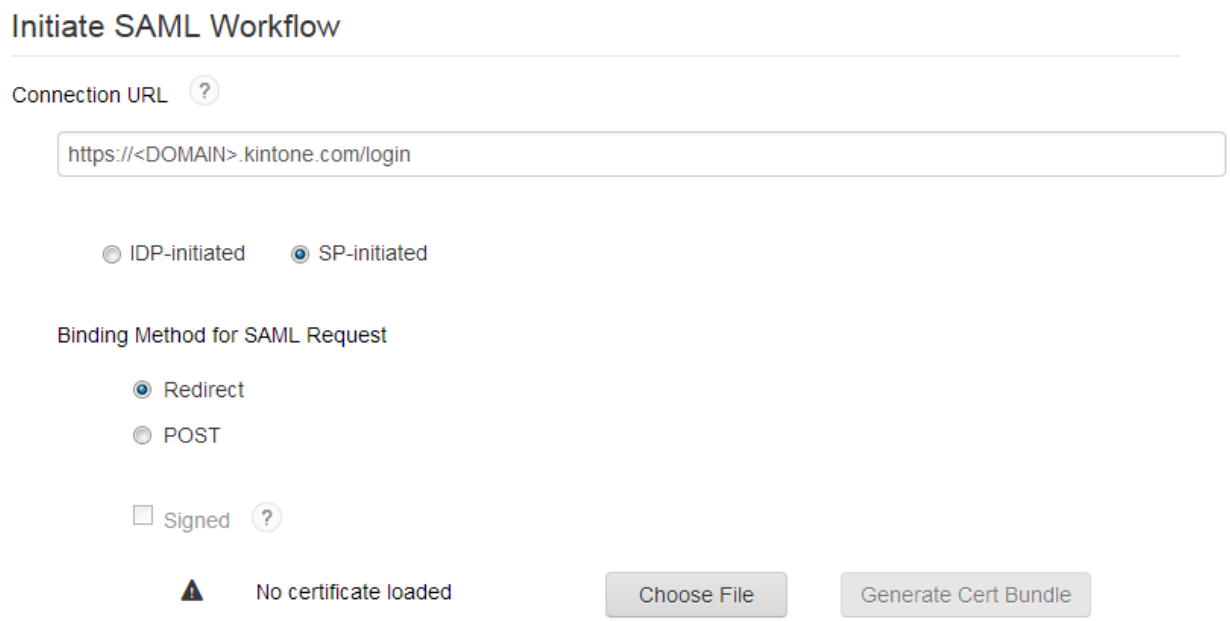


3. On the Basic Information page, specify the application name and click **Next Step**.

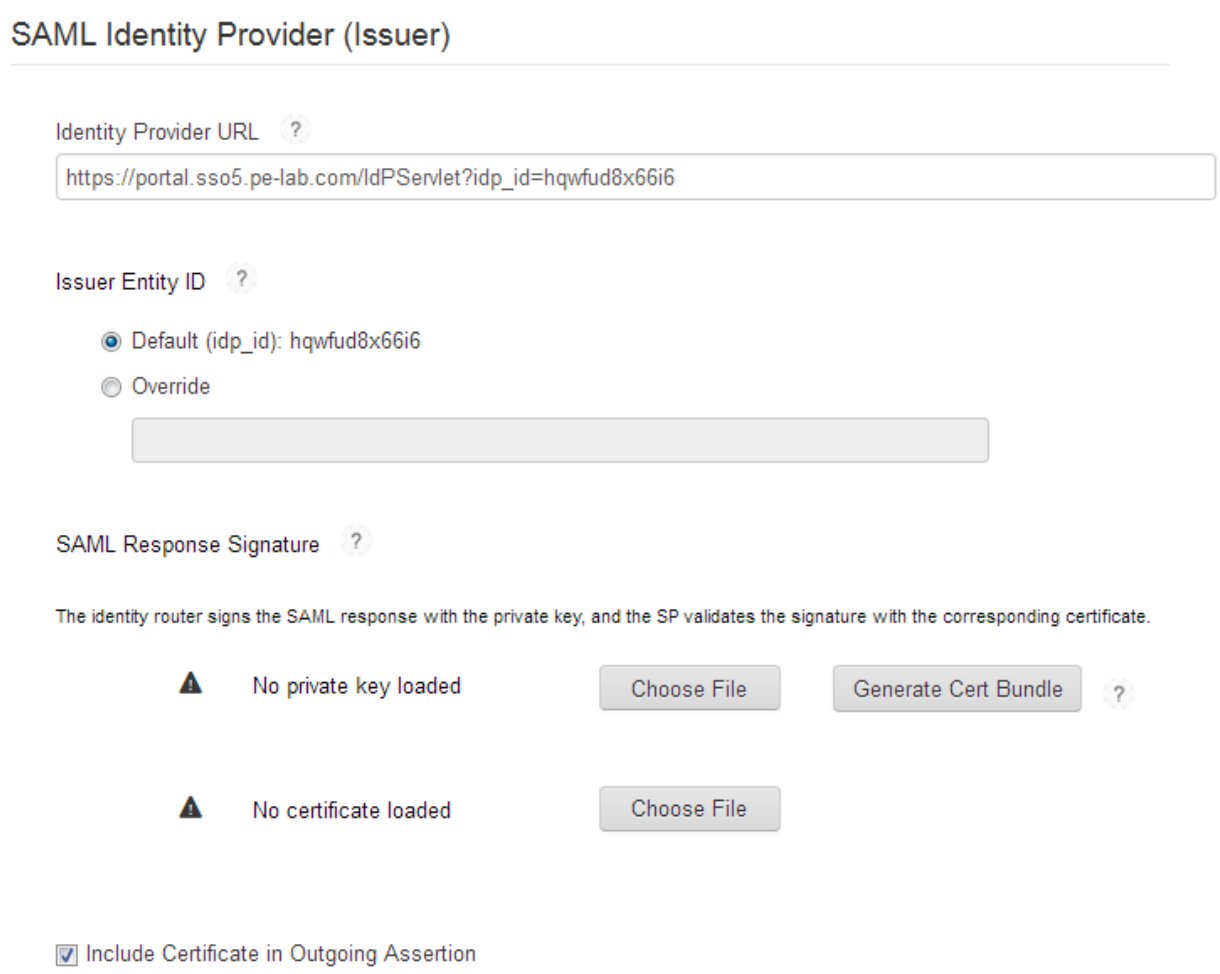


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, enter https://<DOMAIN>.kintone.com/login. Replace <DOMAIN> with your account specific unique web domain.
   b. Choose **SP-initiated.**
   c. Choose Binding Method for SAML Request as **Redirect.**

Note: Kintone application only supports SP-initiated SSO scenario and does not support auto-provisioning as of now.



5. Scroll down to **SAML Identity Provider (Issuer)** section.

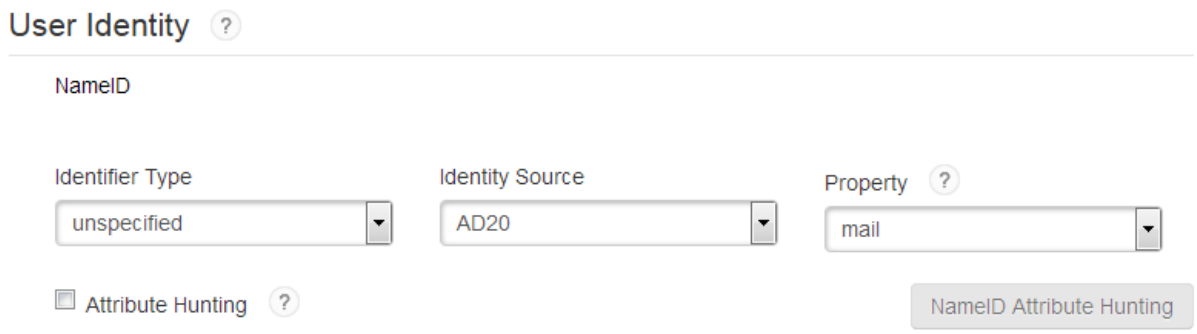


   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   b. Select **Default (idp_id)** for value for the **Issuer Entity ID**.
   c. Select **Choose File** and upload the private key.
   d. Select **Choose File** and import the public signing certificate.
   e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

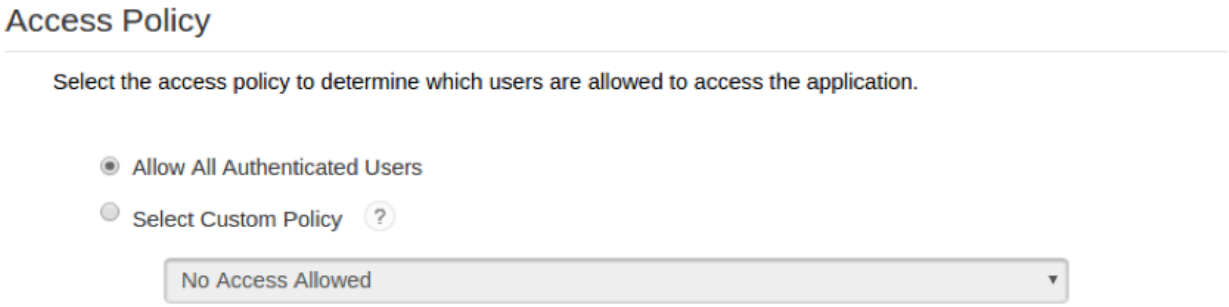
6. Scroll down to the **Service Provider** section.

Note: In ACS URL and SP ID, replace <DOMAIN> with your account specific unique web domain.

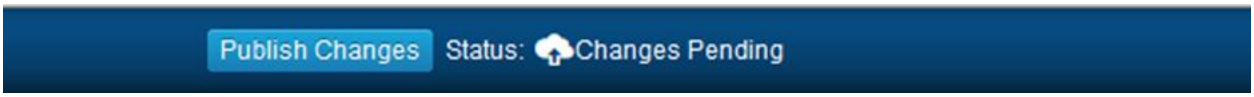
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users.**



10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.

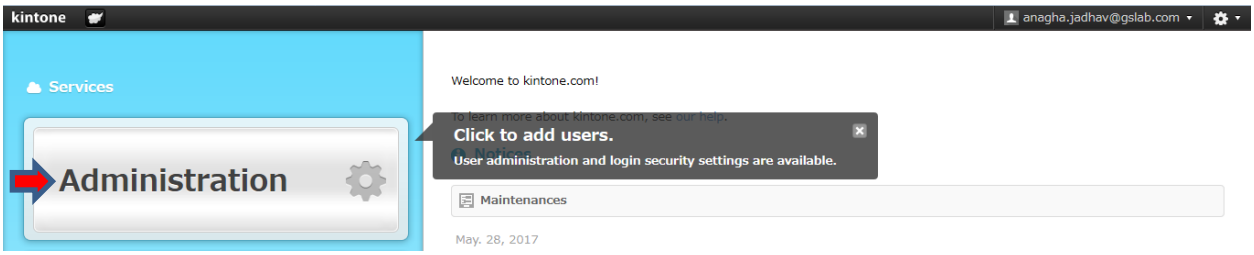


Configure Kintone to Use RSA SecurID Access as an Identity Provider

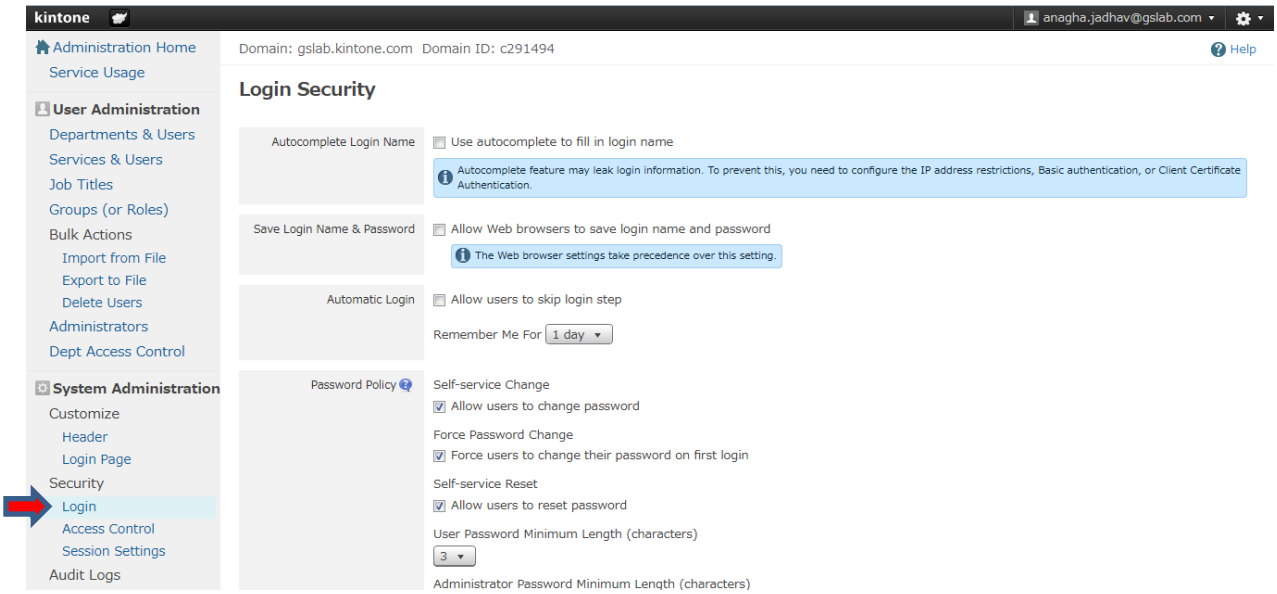
Procedure

1. Login to your Kintone application web account. (https://<DOMAIN>.kintone.com/login and replace <DOMAIN> with your account specific unique web domain.)

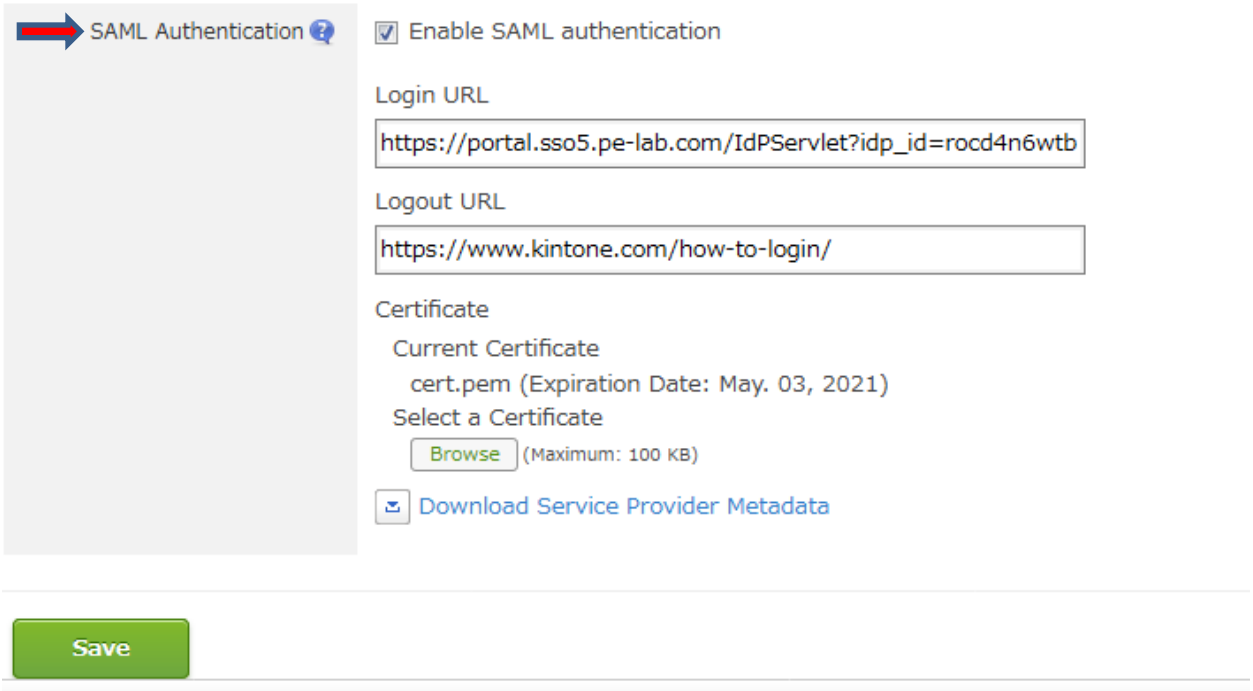
2. Following UI will be displayed. Click *Administration*.



3. Navigate to *System Administration->Security->Login.* Following UI will be displayed.



4. At the bottom of page, you will get following section.



   a. Select **Enable SAML authentication** checkbox.
   b. In **Login URL**, enter IDP URL.
   c. Enter a **Logout URL**.
   d. In **Certificate** section, upload certificate which is the public certificate used when configuring the RSA IDR.
   e. Click on **Save** button to complete configuration changes.

5. Your Kintone account is now enabled for SAML SSO authentication.

AJ