RSA SecurID Access SAML Configuration for Humanity

Last Modified: March 20, 2017

Humanity (formerly ShiftPlanning) is cloud-based Easy-To-Use Employee Scheduling Software company started in 2009. It is aim is to reduce the relying of businesses on pen and paper, excel spreadsheets and lots of headache medication to ensure scheduling of their staff. Add in shift trading and swapping, time and attendance functionality, training, learning management modules, vacation management tools, employee collaboration tools, document storage, payroll integration and other workforce management tools and voila are some of the best selling and successful features of Humanity.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Humanity.
- Obtain SP metadata details from the Service Provider.
- Obtain IdP metadata from IDR portal.

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

SP Login URL	*https://www.humanity.com/app/*
ACS URL	*https://rsa4.humanity.com/includes/saml/consume.php*
Service Provider Issuer ID	*https://rsa4.humanity.com/app/*

Procedure

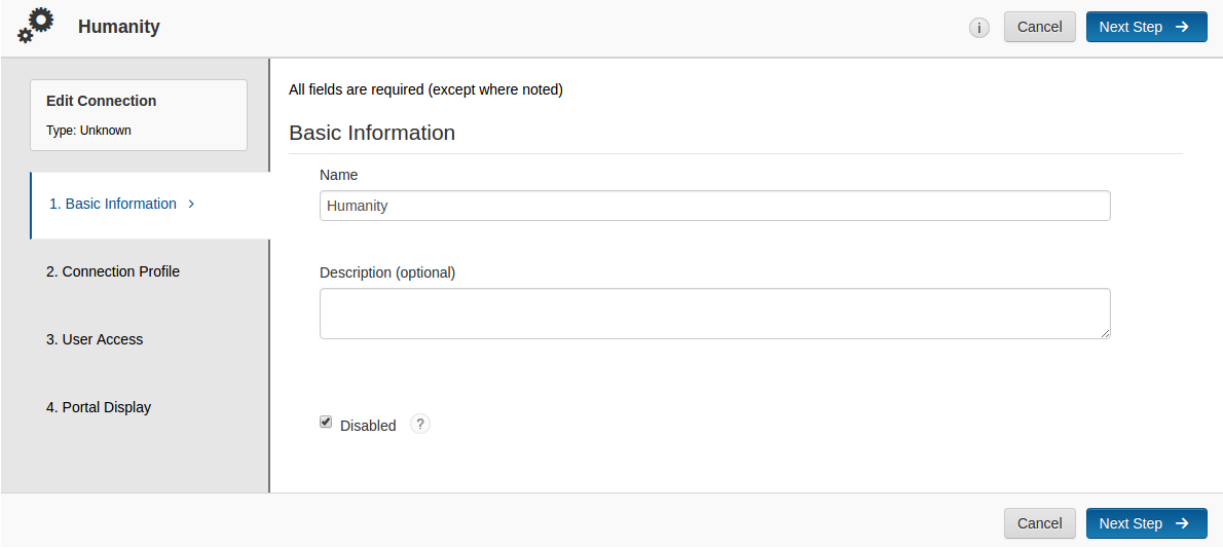
1. Add the Application in RSA SecurID Access
2. Configure Humanity to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

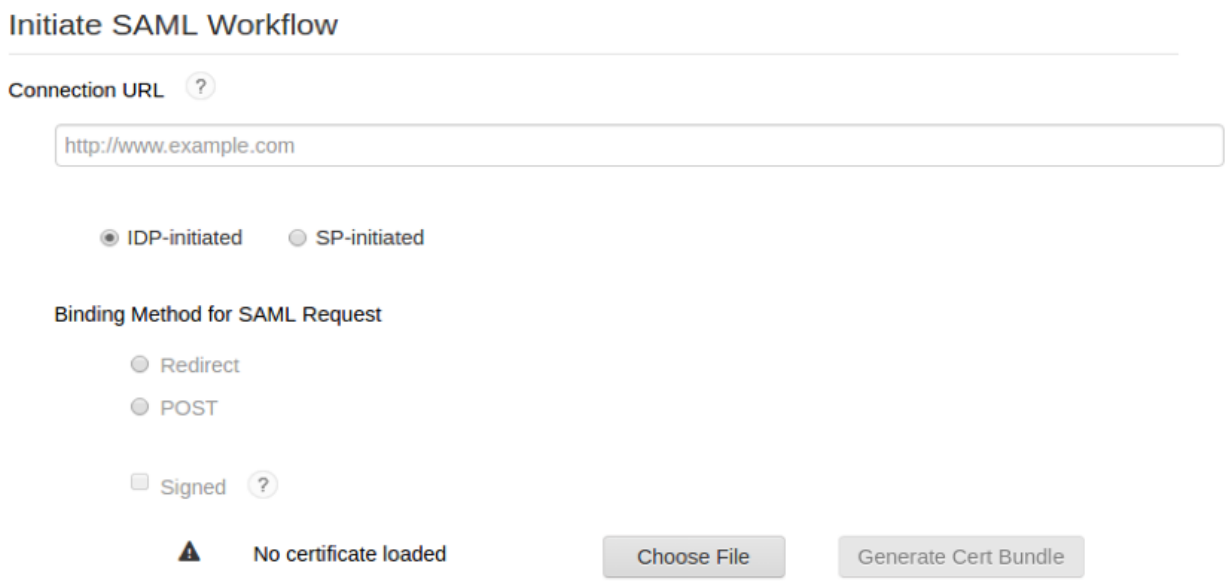
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Humanity.

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

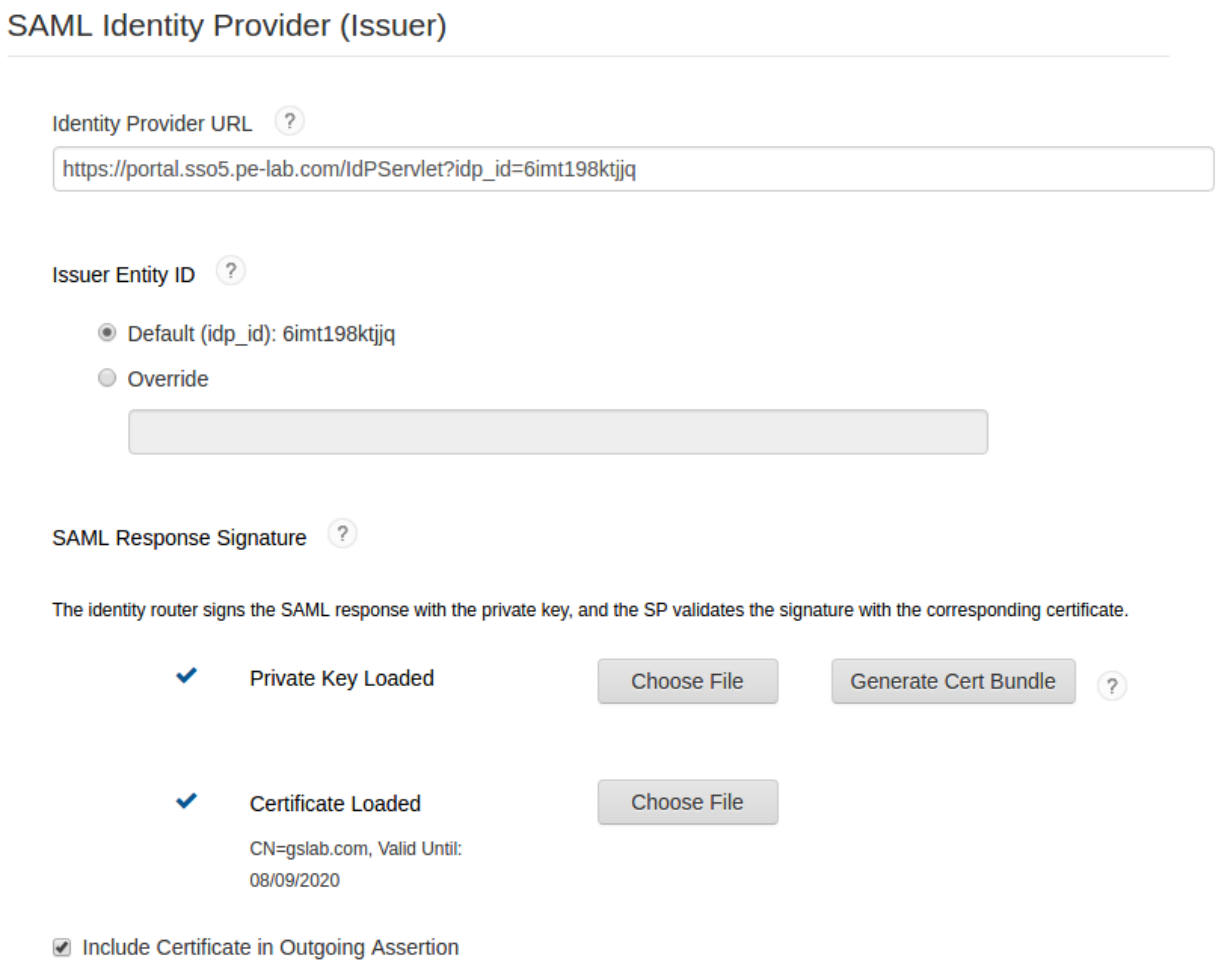


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP–initiated**.

Note: The following IdP-initiated configuration works for SP-initiated Humanity connections as well.

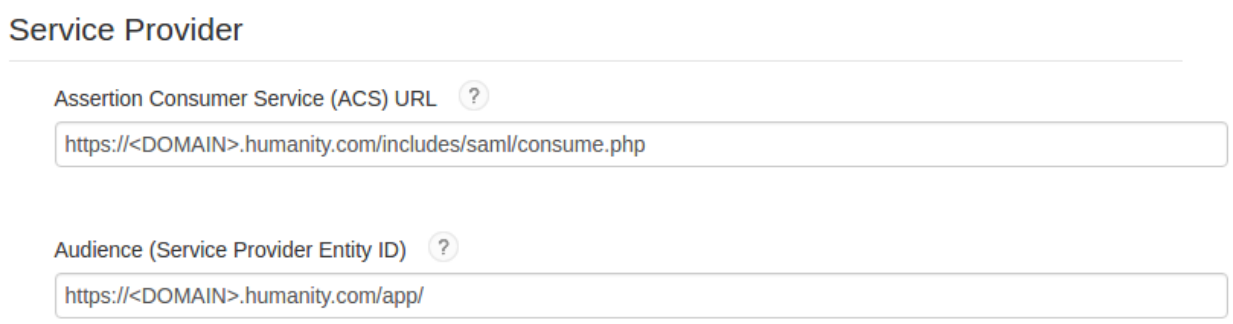


5. Scroll down to **SAML Identity Provider (Issuer)** section.

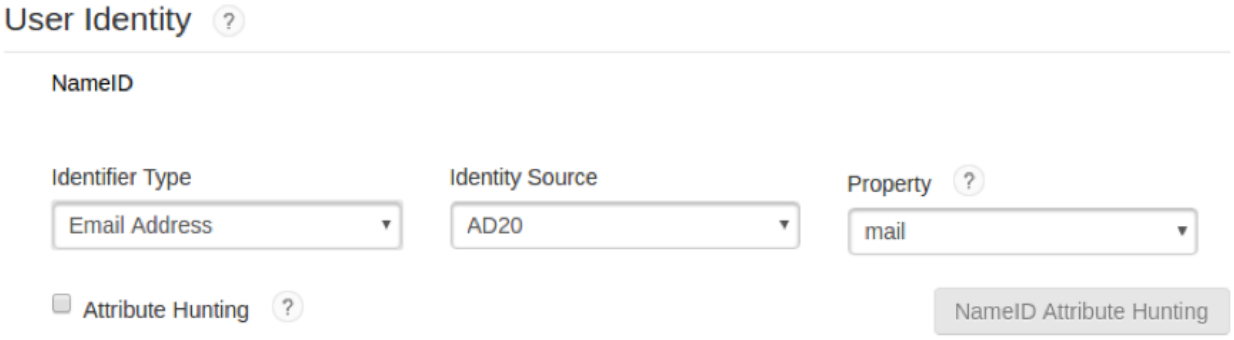


   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
   c. Select **Choose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

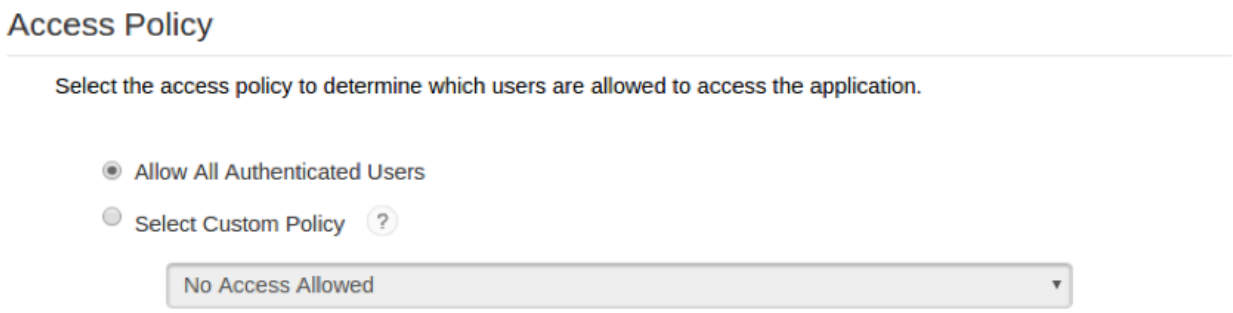
6. Scroll down to the **Service Provider** section.



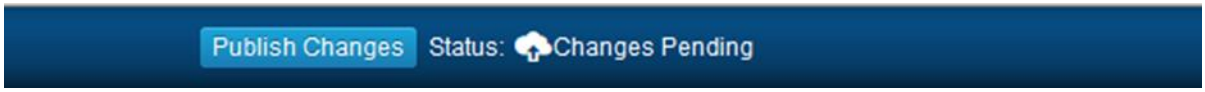
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> name with your organization sub-domain value.
   b. In the **Audience (Service Provider Entity ID)** field, replace <DOMAIN> name with your organization sub-domain value.
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be in 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** user policy from the available options.

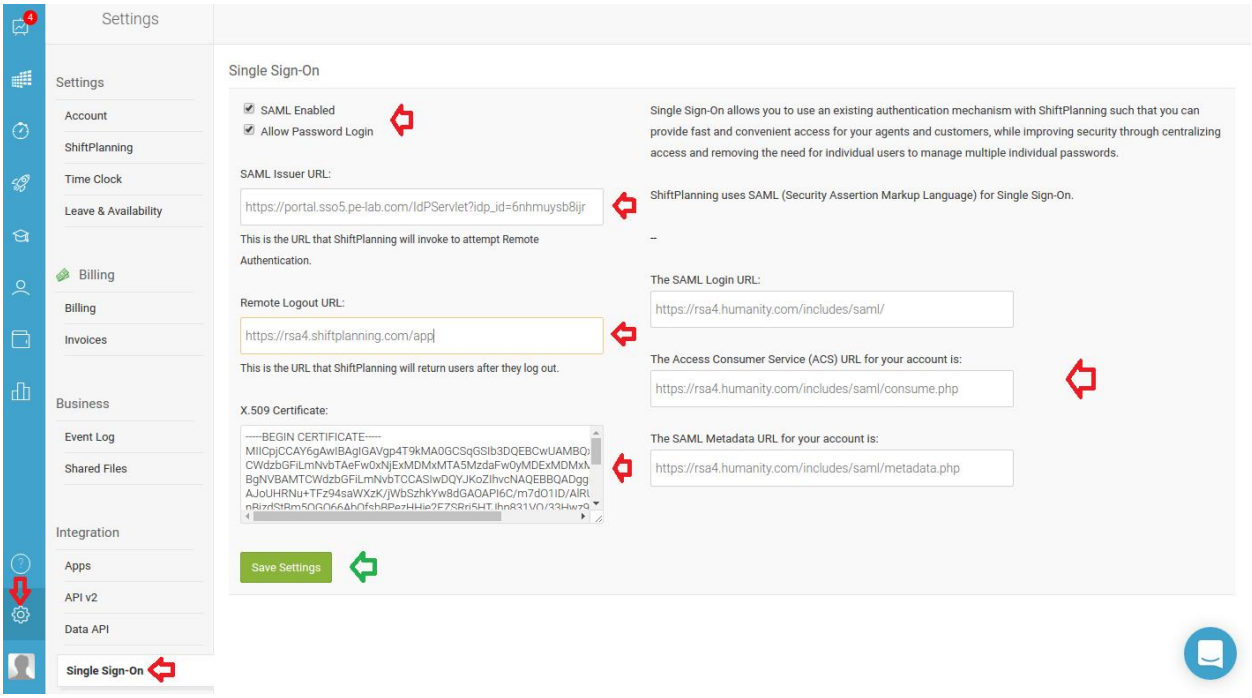


10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



Procedure

1. Login to your Humanity application web account. (https://www.humanity.com/app/)
2. Following UI will be displayed. Click on **geared symbol** available at left-bottom of the page followed by *Single Sign-On* option appears inside list that pop-ups.



   a. Click on **SAML Enabled** checkbox.
   b. Click on **Allow Password Login** checkbox so that in case of SAML failures, user will not be blocked to access account manually.
   c. **SAML Issuer URL** : Enter the Identity Provider URL found on page 2 step 5. It is of following format : https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>
   d. **Remote Logout URL** : Provide URL of your choice to where user will get redirected after logging out from the account.
   e. **X.509 Certificate** : Paste the RSA SecurID Access IdP public certificate here.
   f. Make a note of Service Provider specific details which will be handy while performing Identity Provider side SAML configurations.
   g. Once sure of all the details provided, click on **Save Settings** button.

3. Your Humanity account is now enabled for SAML authentication.
4. Add a user and active the user account.

RJ