RSA SecurID Access SAML Configuration for Bonusly

Last Modified: June 2, 2017

Bonusly provides the easiest way to recognize and reward employees. It supports employee engagement and retention.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Bonusly Enterprise account.
- Obtain SP metadata details from the Service Provider.

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

SP Login URL	https://bonus.ly/users/sign_in_start
ACS URL	https://bonus.ly/saml/ecd-at-emc/consume
Service Provider Issuer ID	ecd-at-emc

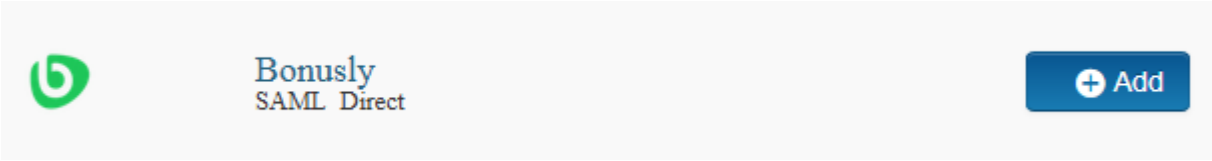
Procedure

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

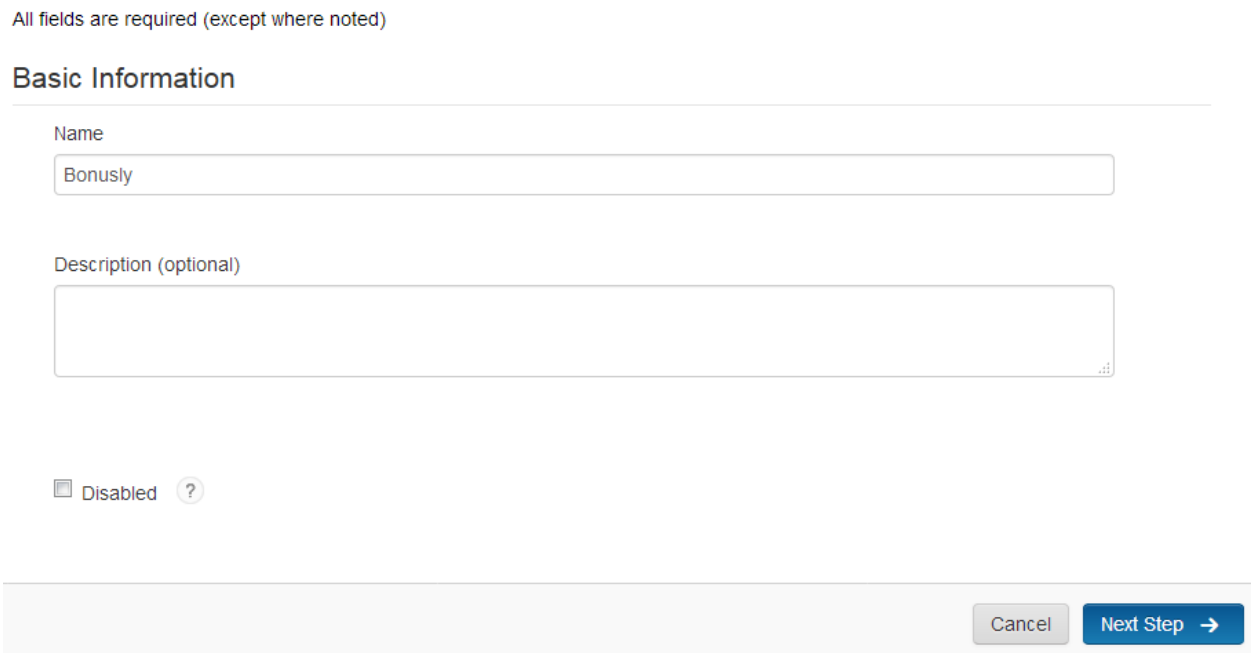
Add the Application in RSA SecurID Access

Procedure

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

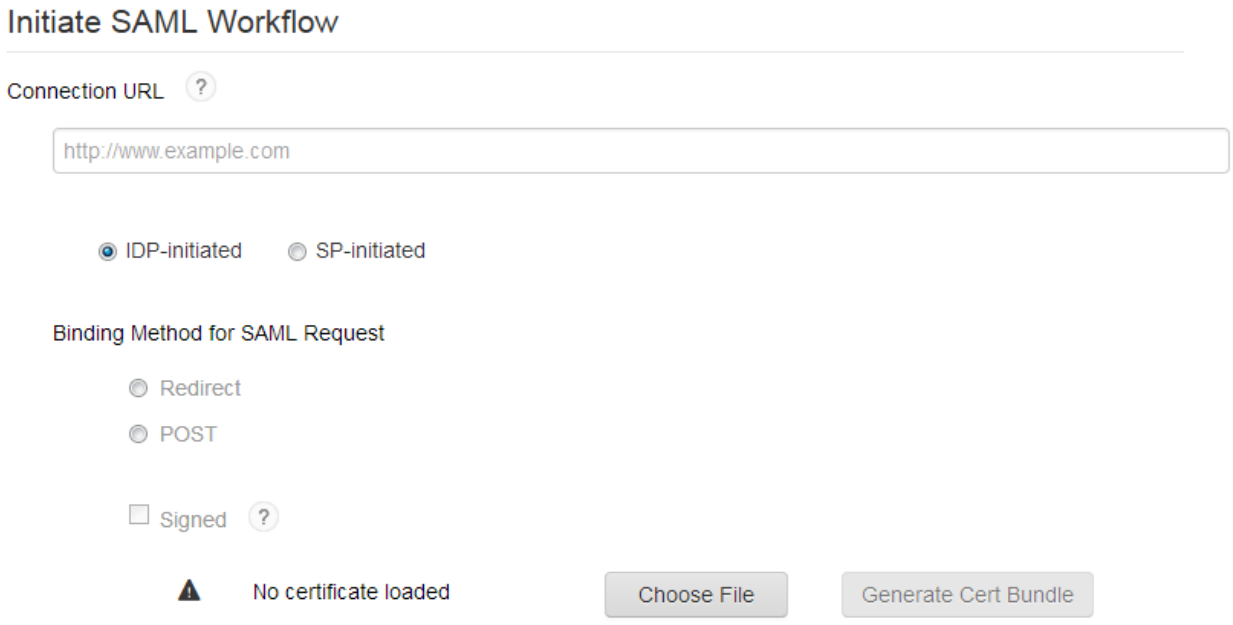


3. On the Basic Information page, specify the application name and click **Next Step**.

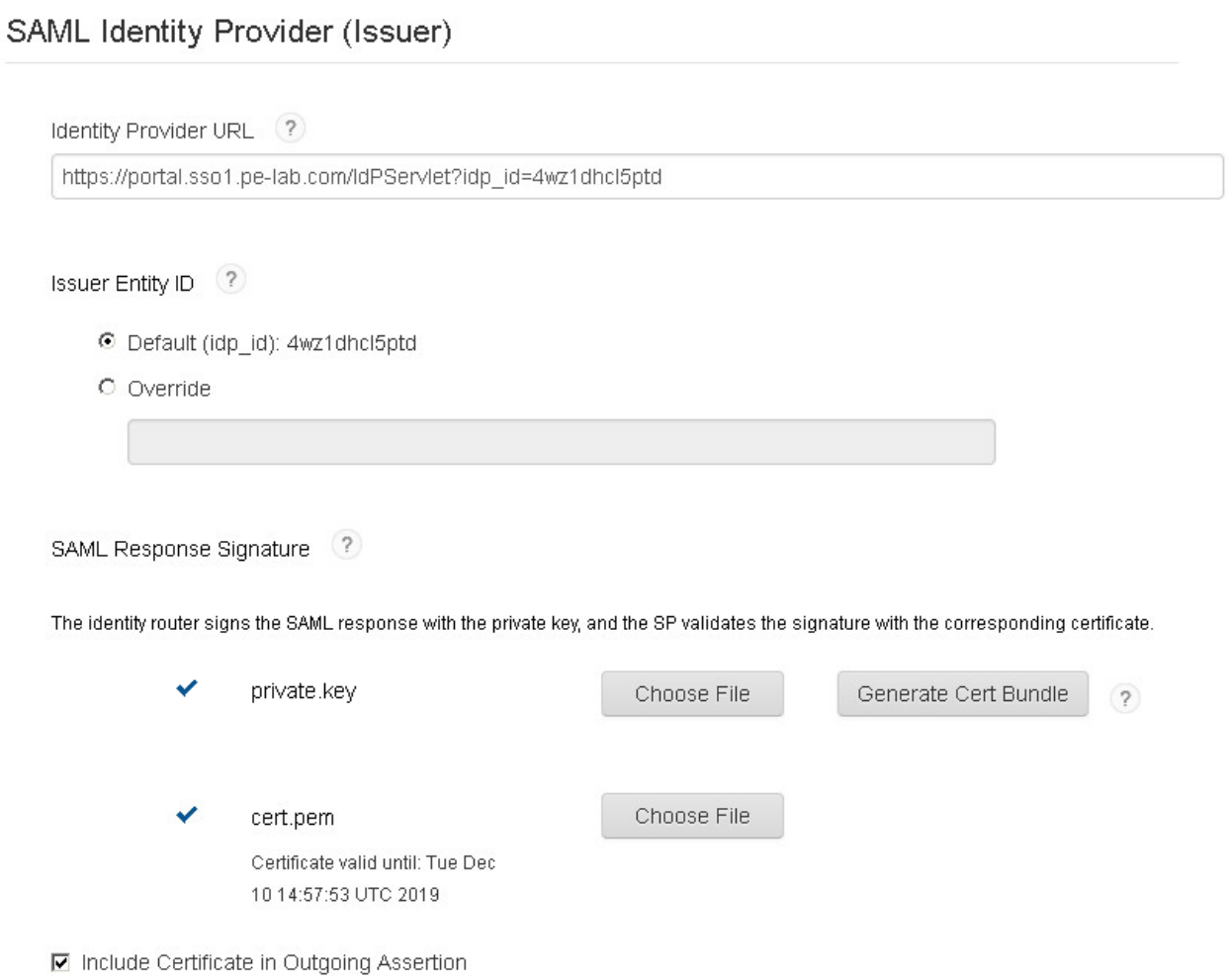


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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

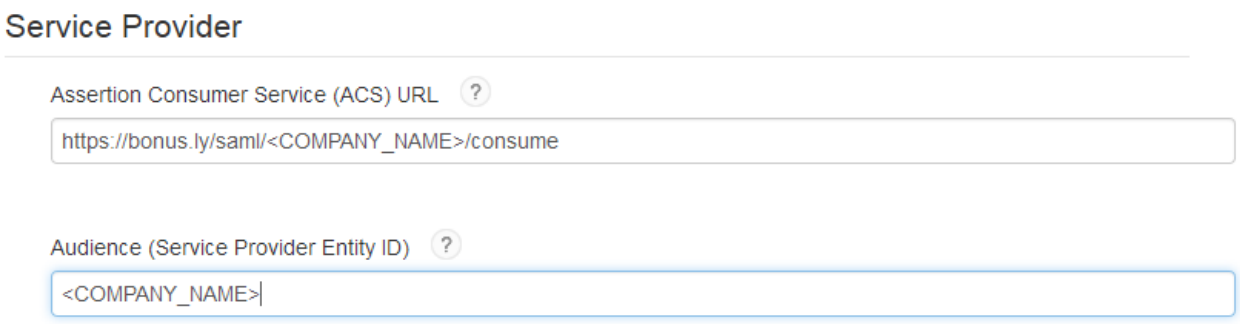


5. Scroll down to **SAML Identity Provider (Issuer)** section.

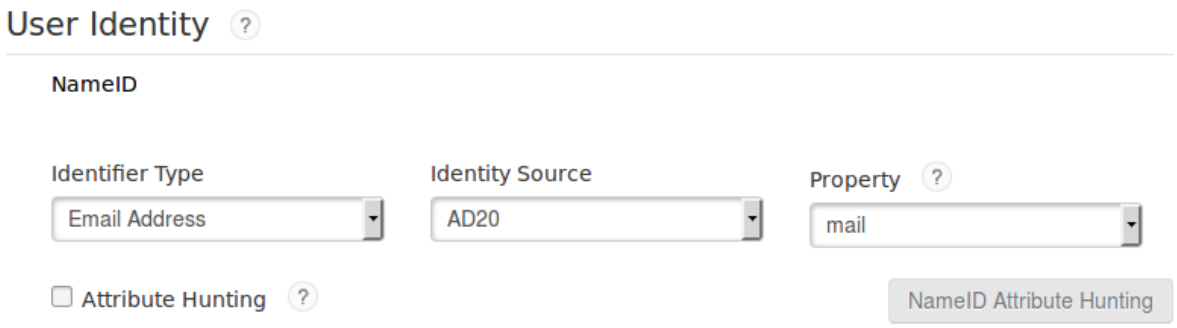


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** 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**.

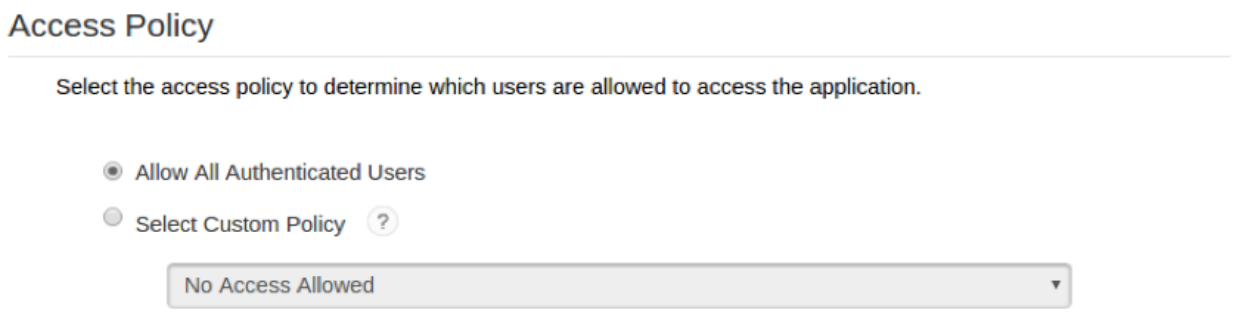
6. Scroll down to the **Service Provider** section.



   a. In the **Assertion Consumer Service (ACS) URL** field, replace <COMPANY_NAME> value with your organization name value.
   b. In the **Audience (Service Provider Issuer ID)** field, provide value as per received from service provider.
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.

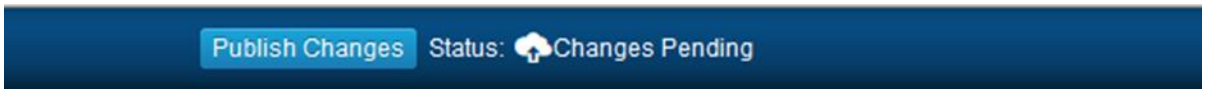


8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users** user policy from the available options.



10. Click **Next Step**.

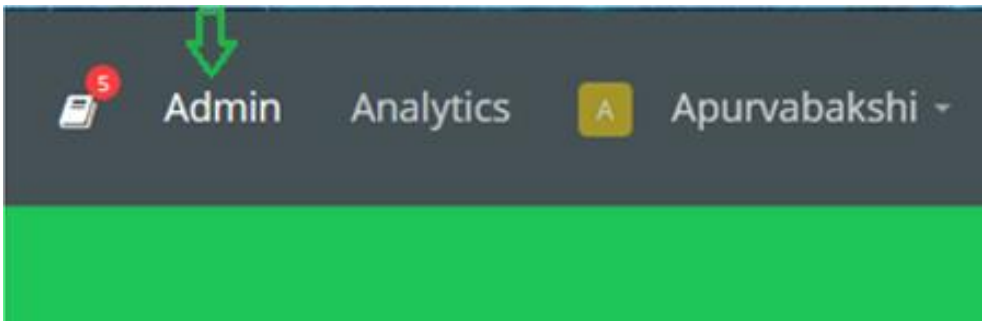
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



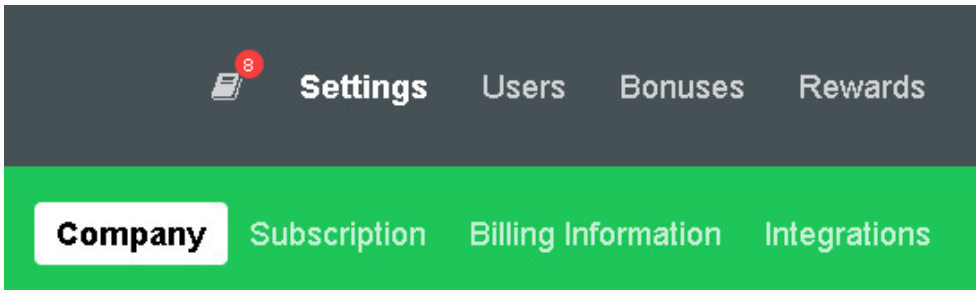
Configure Bonusly to Use RSA SecurID Access as an Identity Provider

Procedure

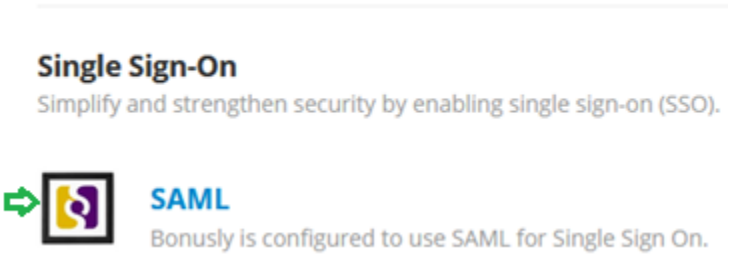
1. Login to your Bonusly application web account. (https://bonus.ly/users/sign_in_start)
2. In the top right corner of the homepage, click on **Admin** option.



3. *Configure company* page will get displayed. In the top right corner, click on **Integrations** option.



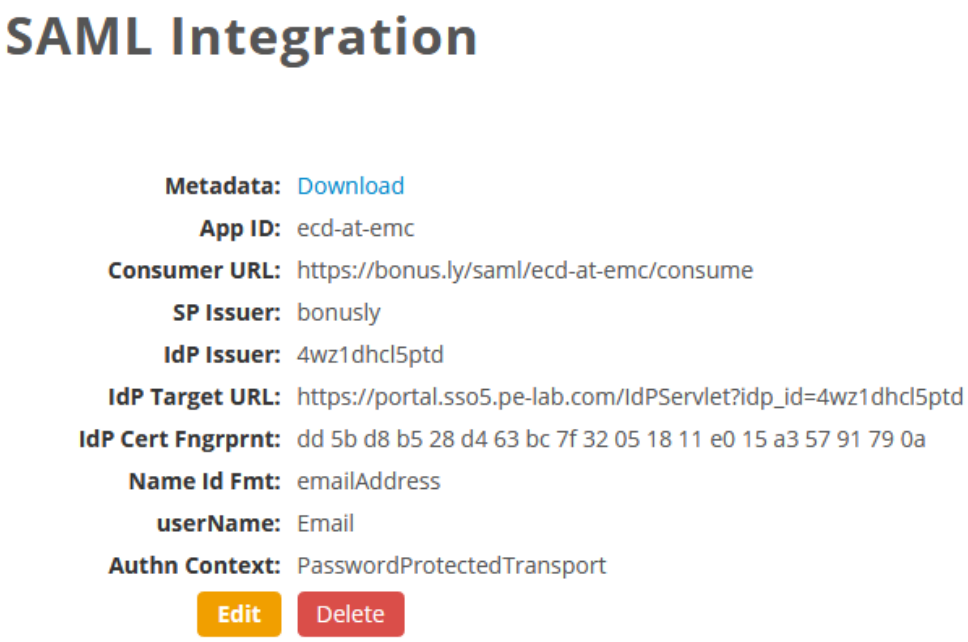
4. On the *Integrations* page, go to **Single Sign On** section. Click on **SAML** icon as shown below.



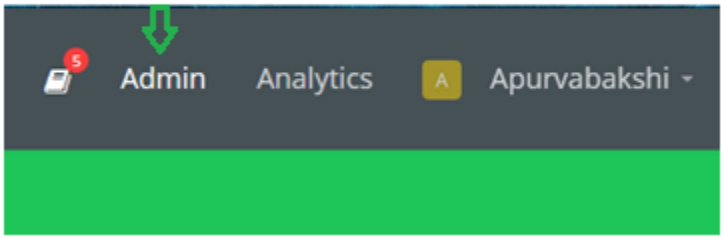
5. **SAML Integration** page will get displayed.

a. In the field *IDP Issuer,* enter IDP Issuer Id obtained from IDR.
b. Keep *IDP Metadata URL* field blank.
c. In *IDP SSO target URL* field, enter IDP URL.
d. Leave the optional *X.509 Cert* field blank.
e. In the *Cert Fingerprint* section, enter fingerprint of the certificate you have imported to IDP.
f. Click on **Save**.

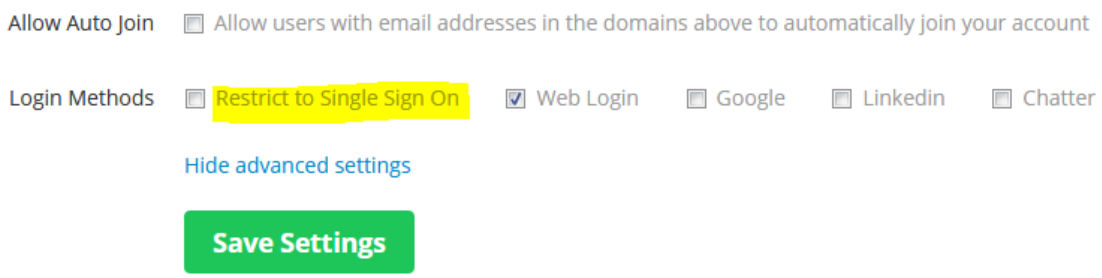
6. Following UI will be displayed.



7. Your Bonusly account is now enabled for SAML authentication.
8. To enable SP initiated SSO from Bonusly, click on **Admin** on top right corner of the homepage.



9. In the bottom of the page, click on *Show advanced settings* option.
10. In *Login Methods* field, check the option **Restrict to Single Sign On** as shown below.



11. Click on **Save Settings**.

AB