

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

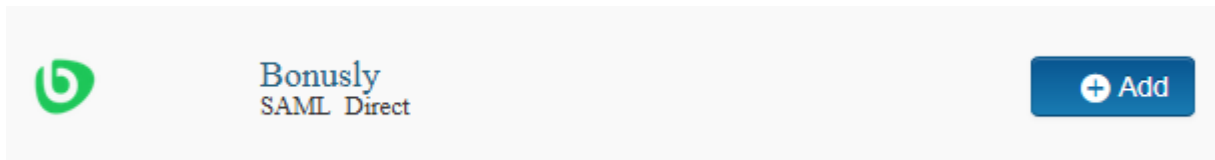
Procedure

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**.

All fields are required (except where noted)

Basic Information

Name

Bonusly


Description (optional)

Disabled ?

Cancel

Next Step →

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

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

Initiate SAML Workflow

Connection URL ?

http://www.example.com

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?



No certificate loaded


Choose File

Generate Cert Bundle

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


SAML Identity Provider (Issuer)

Identity Provider URL 

Issuer Entity ID 

Default (idp_id): 4wz1dhcl5ptd

Override

SAML Response Signature 

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

private.key



cert.pem

Certificate valid until: Tue Dec
10 14:57:53 UTC 2019

Include Certificate in Outgoing Assertion

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

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

Service Provider

Assertion Consumer Service (ACS) URL ?

https://bonus.ly/saml/<COMPANY_NAME>/consume

Audience (Service Provider Entity ID) ?

<COMPANY_NAME>|

- 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.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

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

Access Policy

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy ?

No Access Allowed

10. Click **Next Step**.

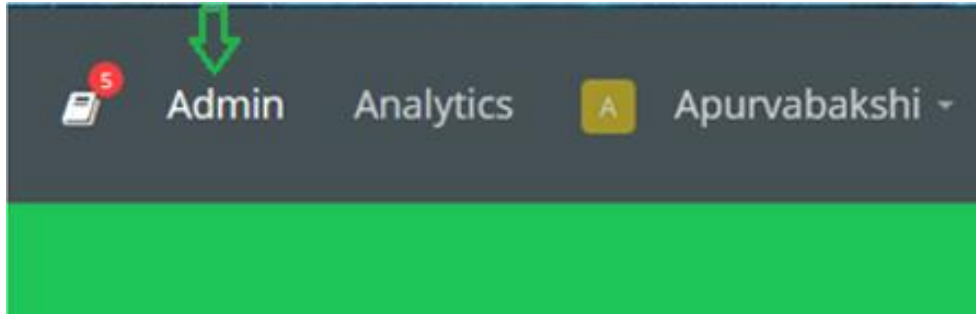
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



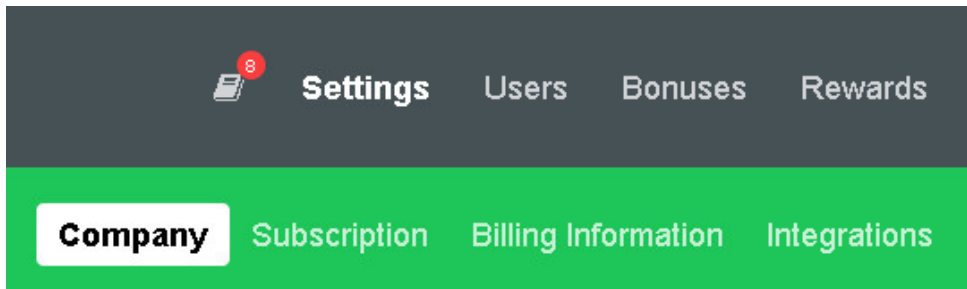
Configure Bonusly to Use RSA SecurID Access as an Identity Provider

Procedure

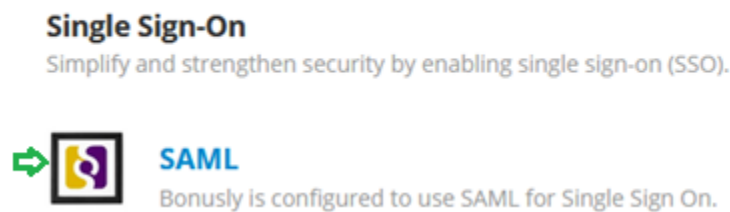
1. Login to your Bonusly application web account. (https://bonus.ly/users/sign_in_start)
2. In the top right corner of the homepage, click on **Admin** option.



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.

SAML Integration

Metadata: [Download](#)

Consumer URL `https://bonus.ly/saml/ecd-at-emc/consume`

App ID `ecd-at-emc`

Automatically Configure from Metadata Simply provide your IdP Metadata URL & Issuer, we'll do the rest

IdP Metadata URL
URL for your IdP metadata, e.g. `https://generic_saml.com/saml/metadata/XYZ`

IdP Issuer (Entity ID)
IdP Issuer Entity ID. Often a URL, e.g. `http://generic_saml.com/exk90p7vamTeckRdV0h7`

IdP SSO target URL
Target for receiving SAML Assertions, e.g. `https://generic_saml.com/trust/saml2/http-post/sso/XYZ`

X.509 Cert

OPTIONAL: Provide X.509 Cert *OR* Fingerprint

Cert Fingerprint
OPTIONAL: Provide X.509 Cert *OR* Fingerprint

Disable user mgmt Turn off manual user management (users can be provisioned via API)

- In the field *IdP Issuer*, enter [IDP Issuer Id](#) obtained from IDR.
- Keep *IdP Metadata URL* field blank.
- In *IdP SSO target URL* field, enter [IDP URL](#).
- Leave the optional *X.509 Cert* field blank.
- In the *Cert Fingerprint* section, enter fingerprint of the [certificate](#) you have imported to IDP.
- Click on **Save**.

6. Following UI will be displayed.

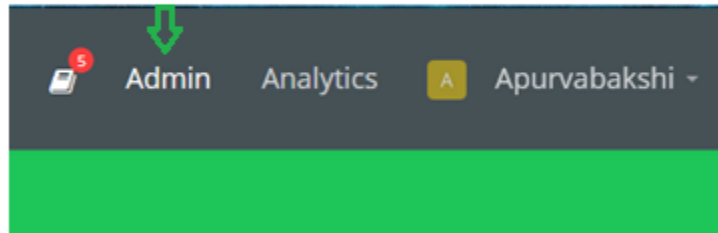
SAML Integration

Metadata: [Download](#)
App ID: ecd-at-emc
Consumer URL: https://bonus.ly/saml/ecd-at-emc/consume
SP Issuer: bonusly
IdP Issuer: 4wz1dhcl5ptd
IdP Target URL: https://portal.sso5.pe-lab.com/IdPServlet?idp_id=4wz1dhcl5ptd
IdP Cert Fngprnt: dd 5b d8 b5 28 d4 63 bc 7f 32 05 18 11 e0 15 a3 57 91 79 0a
Name Id Fmt: emailAddress
userName: Email
Authn Context: PasswordProtectedTransport

[Edit](#) [Delete](#)

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.

Allow Auto Join Allow users with email addresses in the domains above to automatically join your account

Login Methods **Restrict to Single Sign On** Web Login Google LinkedIn Chatter

[Hide advanced settings](#)

[Save Settings](#)

11. Click on **Save Settings**.