RSA SecurID Access SAML Configuration for Small Improvements

Last Modified: November 15, 2016

Small Improvements is a tool that allows you to deploy a custom feedback process for your organization. It gives managers a place to capture 1:1 notes, mentor reports on objectives, or enable coworkers to congratulate on a job well done. All of these supplies will be available for reference simplifying everyone's life. It integrates with 3rd parties for your convenience. It easily tracks progress, sends nudges, and identify trouble areas, saving you valuable time.

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and Small Improvements.

> **Note: Contact Small Improvements support@small-improvements.com and request a subdomain be added to your account for SAML.**

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

SP Login URL	*https://gslab.small-improvements.com/dashboard?forceSaml=true*
ACS URL	*https://gslab.small-improvements.com/saml/consume?continueTo=dashboard*
SP Issuer ID	*https://www.small-improvements.com/*

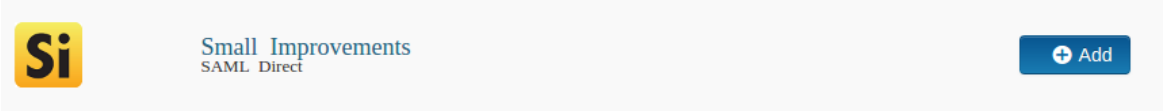
Procedure

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

Add the Application in RSA SecurID Access

Procedure

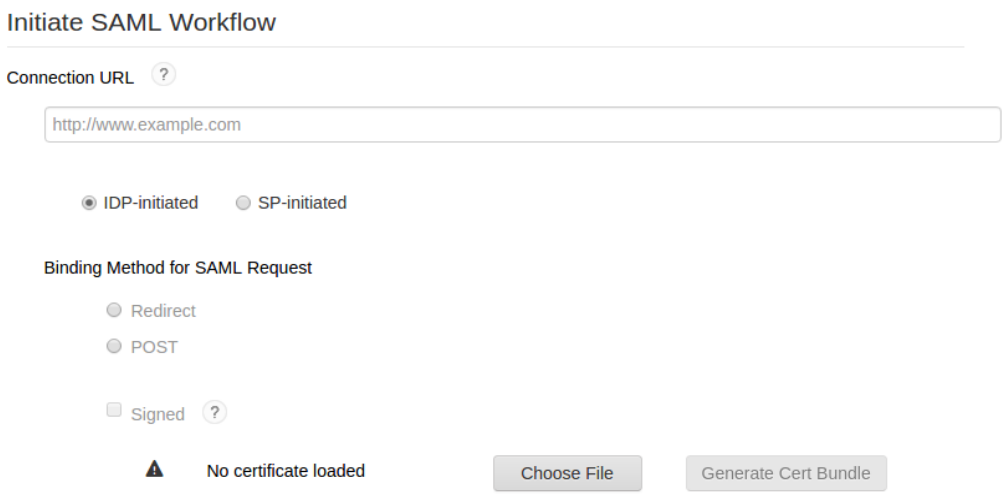
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for Small Improvements.



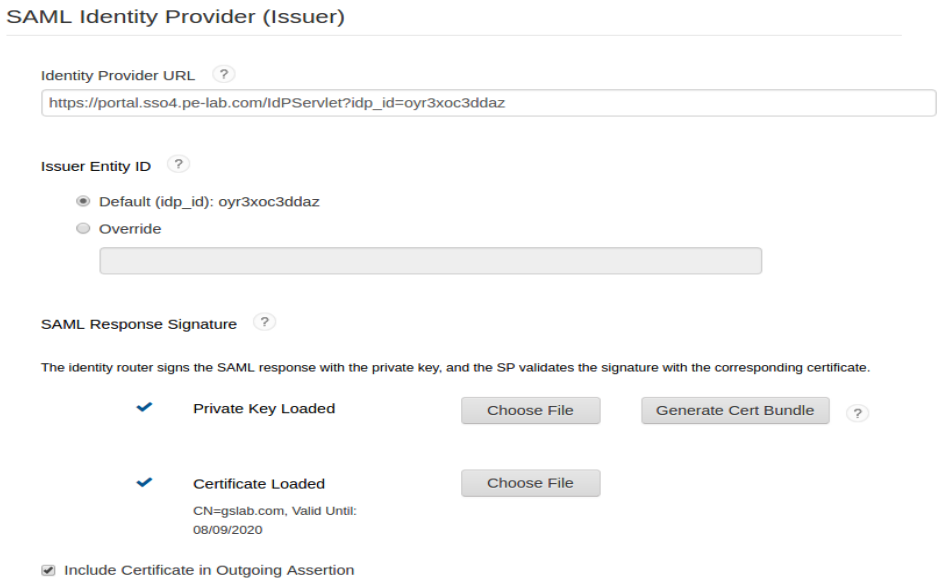
3. On the Basic Information page, specify the application name and click **Next Step**.

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 Small Improvements connections as well.



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

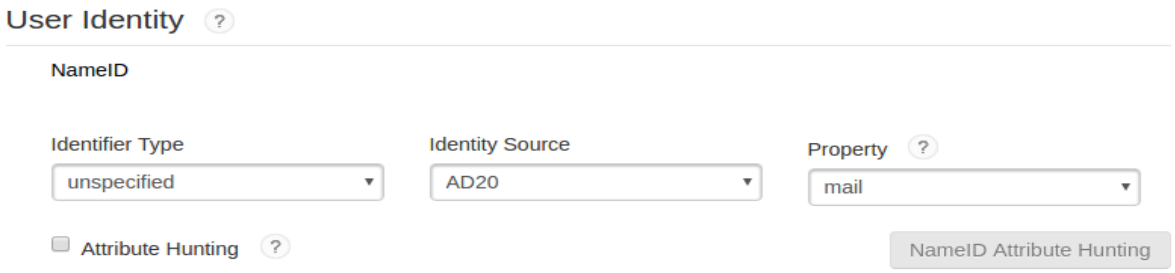


   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   b. Select **Choose File** and upload the private key.
   c. Select **Choose File** to import the public signing certificate.
   d. Select the checkbox for **Include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

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

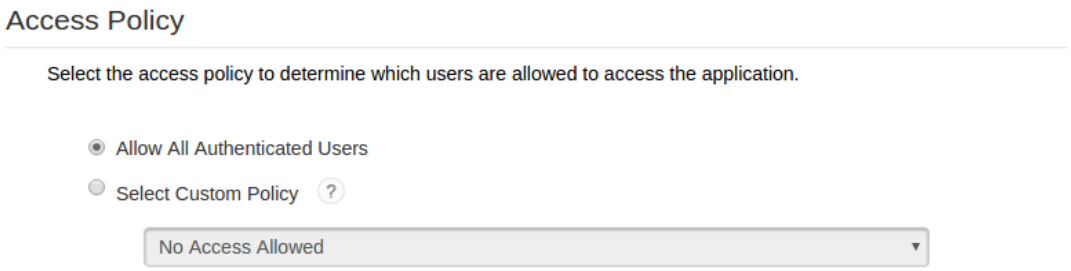
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your customer domain.
   b. In the **Audience (Service Provider Entity ID)** field, enter value that is configured inside Small Improvements account.

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**.

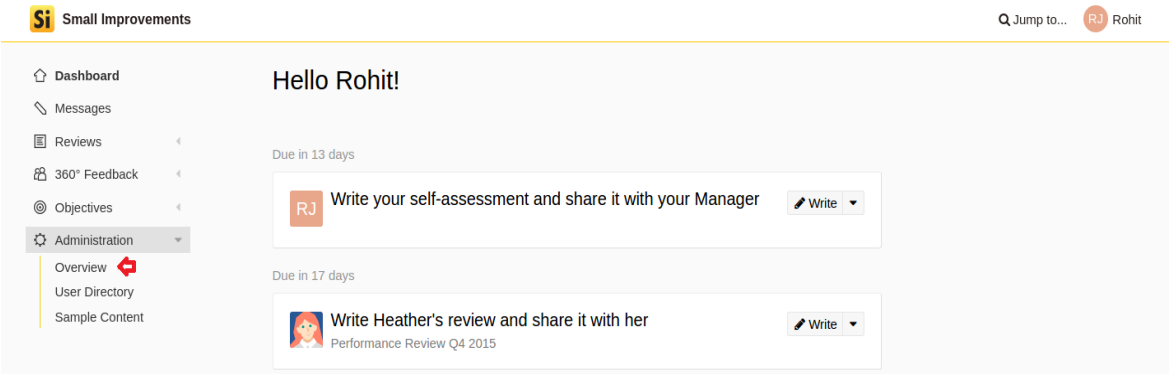
9. On the **User Access page,** select **Allow All Authenticated Users** option from drop down list.



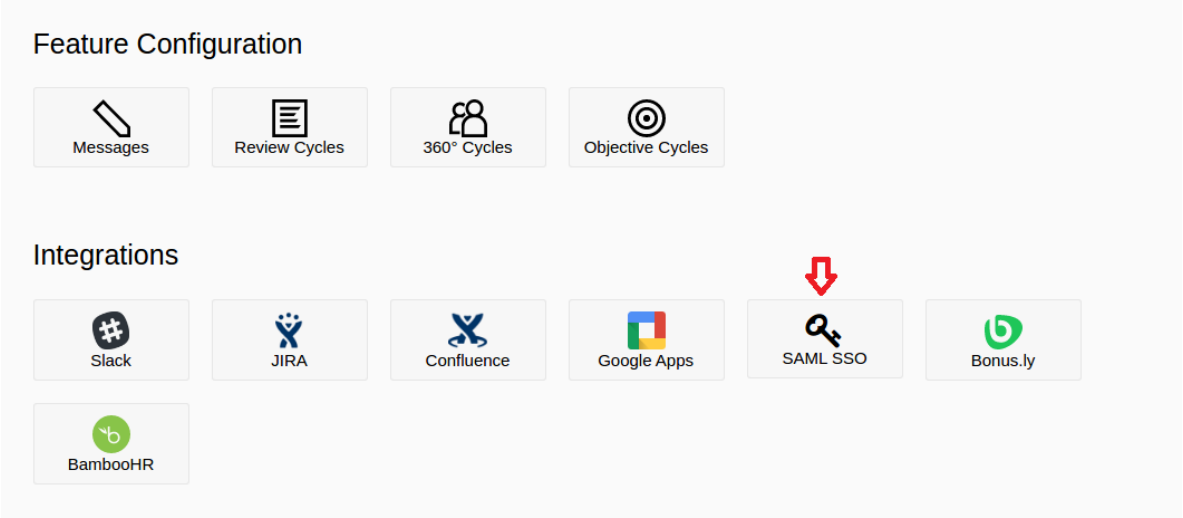
10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.

Configure Small Improvements to Use RSA SecurID Access as an Identity Provider

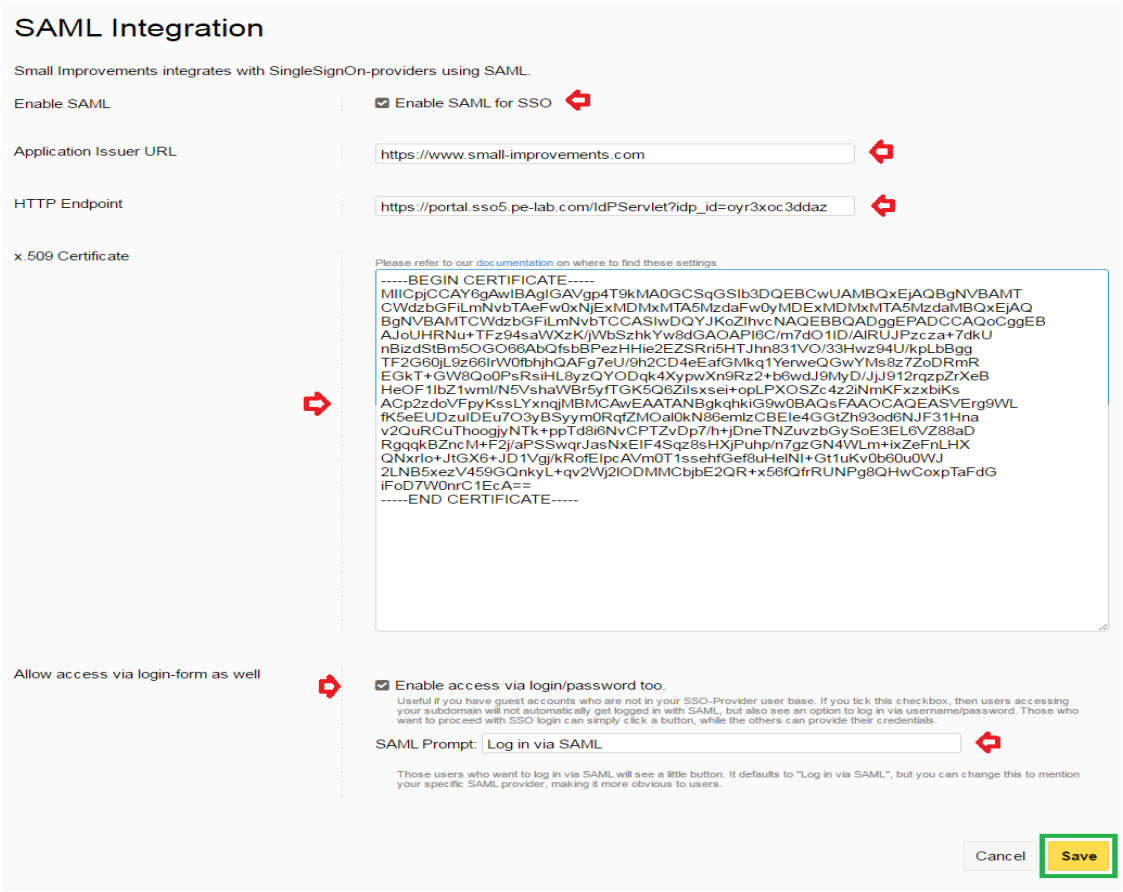
1. Login to your Small Improvements account. (https://www.small-improvements.com/login)
2. Select **Overview** option available under **Administration** tab located at left side of the page.



3. Following UI will be displayed. Select **SAML SSO** option available under **Integrations** section to add new SAML configurations.



4. Following UI will be displayed –



a) Click on Checkbox **Enable SAML for SSO** to make account enable for SAML authentication.
b) **Application Issuer URL** – Enter the SP entity ID of your choice.
c) **HTTP Endpoint** – 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) **x.509 Certificate** – Paste the RSA SecurID Access IdP public certificate here.
e) Click on Checkbox **Enable access via login/password too** to allow manual logins also to verify failures or issues in SAML authentication.
f) In the **SAML Prompt** field enter the text that will appear on the login page.
g) Click **Save**.

5. From the left side menu go to **Administration > User Directory**.
6. Select **+Add users**.
7. Enter First name, Last name, and email address for the user.
8. Select **Create Users**. An email will be sent to user's email address to active the account.

RJ