

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/ |

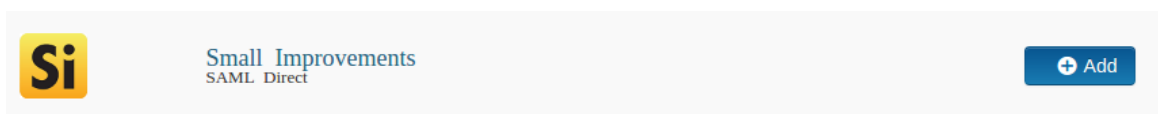
Procedure

- [Add the Application in RSA SecurID Access](#)
- [Configure Small Improvements to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access


Procedure

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




- 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.

Initiate SAML Workflow

Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect


POST


Signed 

 No certificate loaded

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


SAML Identity Provider (Issuer)

Identity Provider URL 


Issuer Entity ID 

Default (idp_id): oyr3xoc3ddaz


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 Loaded



 Certificate Loaded

CN=gslab.com, Valid Until:
08/09/2020

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.small-improvements.com/saml/consume?continueTo=dashboard

Audience (Service Provider Entity ID) ?

https://www.small-improvements.com

- 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.

User Identity ?

NameID

Identifier Type

unspecified

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** option from drop down list.

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**.

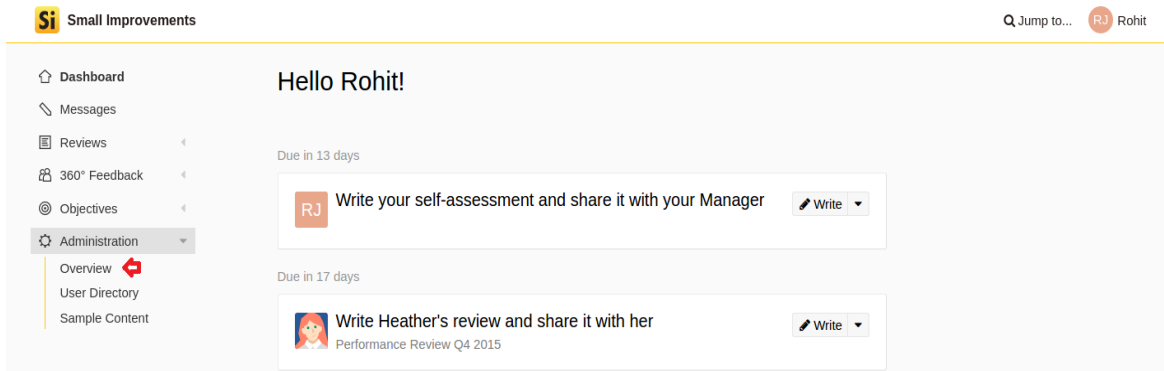
13. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

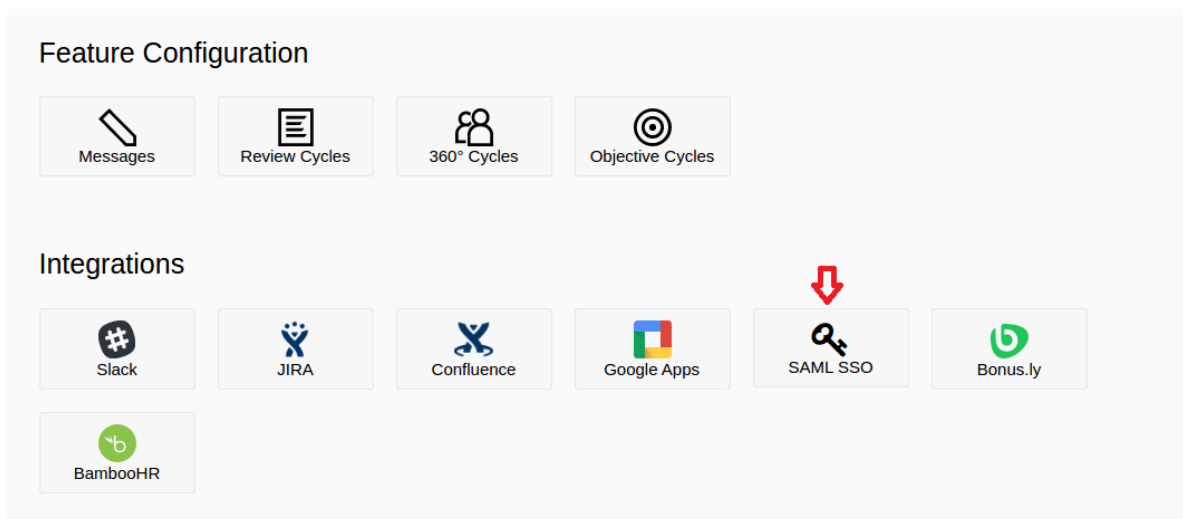
Status:  Changes Pending

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 –

SAML Integration

Small Improvements integrates with SingleSignOn-providers using SAML.

Enable SAML **Enable SAML for SSO**

Application Issuer URL

HTTP Endpoint

x.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIICPjCCAY6gAwIBAgI GAVgp4T9kMA0GC SsqGSib3DQEB CwUAMBQxEJAOBGNVBAMT
CWdz bGFILmNvbTAeFw0xNjExMDMxMTA5MzdaFw0yMDExMDMxMTA5MzdaMBQxEJAO
BgNVBAMTCWdz bGFILmNvbTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJoUHRNu+TFz94saWXzKjVbSzhkYw8dGAOAPi6Cm7do1ID/AIRUJJPzcca+7dkU
nBizdSIbm5OGG06AbQfsbFPezHHie2EZSRn5HTJhm831VO/33Hwz94U/kpl.bEgg
TF2G60JL9z66lrW0fbjhQAFg7eU/9h2CD4eEafGlvkq1YerweQGwYMs8z7ZoDRnrR
EGkT+GW8Qo0PsRsiHL8yzQYODqk4XypwXn9Rz2+b6wdJ9MyD/JJ912rqzpzZrXeB
HeOF1lbZ1wml/N5VshaWBr5yFTGK5Q6Zilsxsei+opLPXOSZc4z2InMkFzxzbiKs
ACpZzdoVfpyKssLYxnqjMBMCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEASVErg9WL
fk5eEUDzuiDEu7O3yBSyym0RqfZMOal0kN86emizCBEIe4GGtZ93od6NJJF31Hna
v2QuRCuThoojyNtk+ppTd8i6NvCPTZVdp7/h+jDneTNZuvzbGySoE3EL6VZ88aD
RgqkRZncIM+F2jaPSSwqrJasNxEIF4Sqz8sHXjPuhp7gzGN4WLM+ixZaFnlHX
QNXrlo+JGX6+JD1VgjkRofElpcAVm0T1ssehfGef8uHeIN+GT1uKv0b60u0WJ
2LNB5xezV459GOnkyL+qv2Wj2lODMMCbje2QR+x56fQfrRNPg8QHwCoxpTaFdG
iFoD7W0nrC1EaA=
-----END CERTIFICATE-----
```

Allow access via login-form as well **Enable access via login/password too.**
Useful if you have guest accounts who are not in your SSO-Provider user base. If you tick this checkbox, then users accessing your subdomain will not automatically get logged in with SAML, but also see an option to log in via username/password. Those who want to proceed with SSO login can simply click a button, while the others can provide their credentials.

SAML Prompt:

Those users who want to log in via SAML will see a little button. It defaults to "Log in via SAML", but you can change this to mention your specific SAML provider, making it more obvious to users.

- 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 activate the account.