

Last Modified: January 18, 2016

BamboHR is an online human resources (HR) software service for small and mid-sized businesses. BamboHR provides a cloud-based business management solution for managers and employees, streamlining employee profiles, time-off requests & approvals, and recruitment & applicants.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and BamboHR.
- Obtain the ACS URL information from BamboHR.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

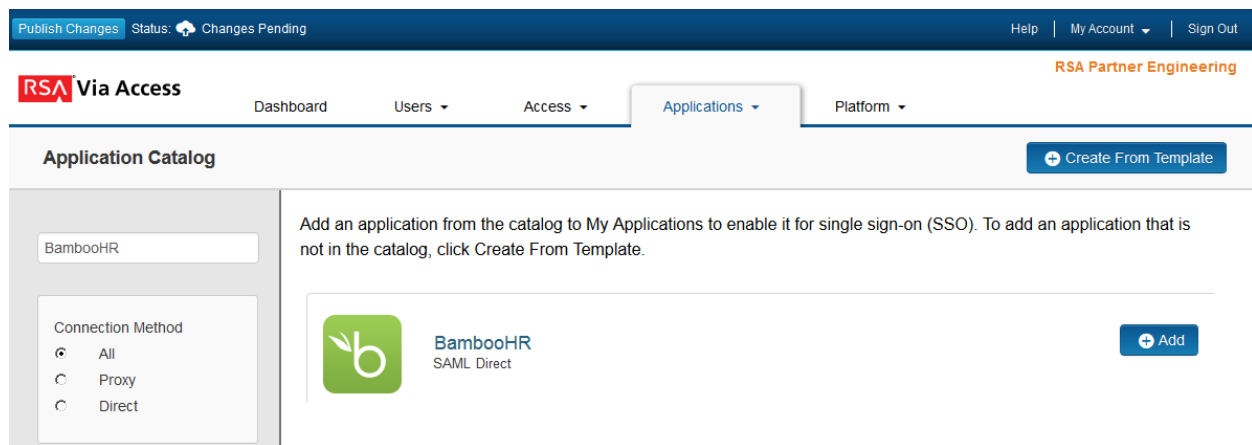
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure BamboHR 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 the SAML application that you wish to add.



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

 **Note:** The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.

4. On the Connection Profile page, choose **IDP –initiated** and leave the URL blank.

Connection URL


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

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

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): btest

Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

Private Key Loaded

Certificate Loaded

CN=salesforce_saml, Valid
Until: 08/05/2017

Include Certificate in Outgoing Assertion

- a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the BambooHR.
- b. Select **Choose File** and upload the RSA SecurID Access private key.
- c. Select **Choose File** and upload the RSA SecurID Access public certificate.

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

Service Provider

Assertion Consumer Service (ACS) URL

https://<your_instance>.bamboohr.com/saml/consume.php

Audience (Service Provider Entity ID)

https://<your_instance>.bamboohr.com/saml/consume.php

- a. In the **Assertion Consumer Service (ACS) URL** field, enter your subdomain in place of **<your_instance>**. https://<your_instance>.bamboohr.com/saml/consume.php
 - b. In the **Audience (Service Provider Entity ID)** field, enter your subdomain in place of **<your_instance>**. https://<your_instance>.bamboohr.com/saml/consume.php
7. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email** and **Property** to **mail**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

Show Advanced Configuration

8. Click **Show Advanced Configuration** and scroll down to **Uncommon Formatting SAML Response Options**, select **Assertion within response**.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response Assertion within response

Signature Algorithm rsa-sha1

Digest Algorithm sha1

Encrypt Assertion

No certificate loaded

Choose File

Encryption Algorithm Triple DES

Encryption Key Transport RSA15

Relay State URL Encoding

Receive Relay State URL - encoded by SP (in incoming request)

Send Relay State URL - encoded by IDP

Include Issuer NameID Format

NameID Format Unspecified

9. Click **Next Step**.

10. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

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

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


11. Click **Next Step**.

12. On the **Portal Display** page, select **Display in Portal**.

13. Click **Save and Finish**.

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

Publish Changes

Status:  Changes Pending

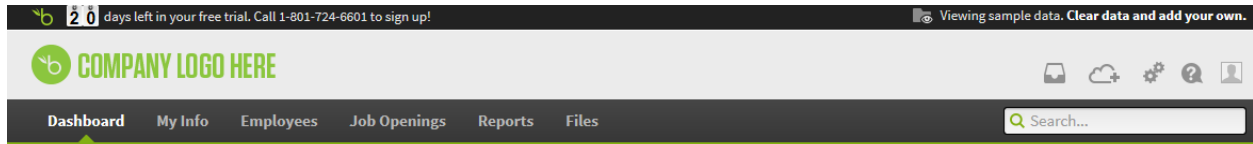
Next Steps

[Configure BambooHR to Use RSA SecurID Access as an Identity Provider](#)

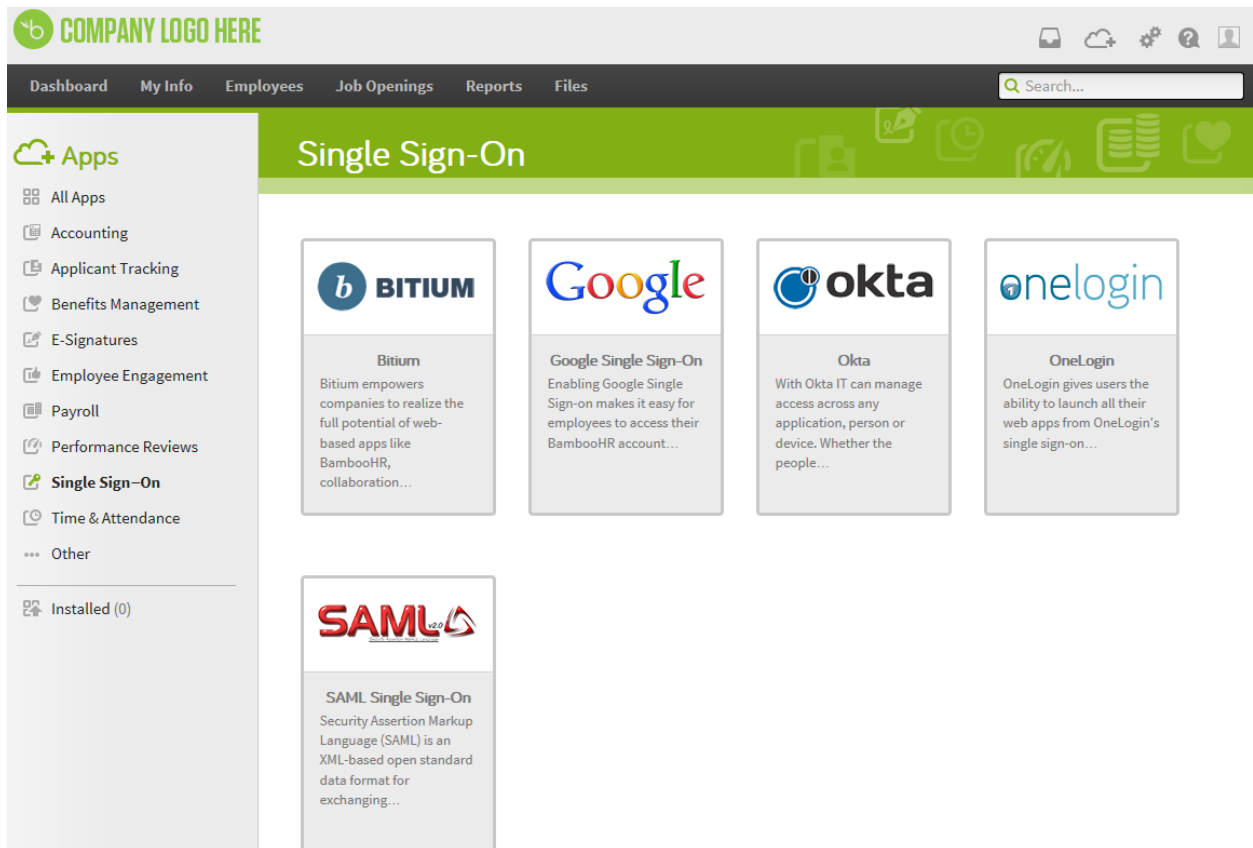
Configure BambooHR to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to your instance of BambooHR. <https://<your instance>.BambooHR.com>
2. Click on the **Cloud+** symbol in the right upper corner.



3. The Apps page will open.
4. Select **Single Sign-On** from the menu list.



5. Click on **SAML Single Sign-On**.

6. Click **Install**.

← App Info

SAML Single Sign-On



Settings

SSO Login URL *

https://portal.sso.pe-fab.com/IDPServlet?idp_id=btest

x.509 Certificate *

```
-----BEGIN CERTIFICATE-----
MIICpDCCAYygAwIBAgIGAVGMZf+XMA0GCSqGSIb3DQEBCwUAMBAMxETAPBgNVBAMT
CGdzLmxxvY2FwMB4XDTE1MTIxMDE0NTc1M1oXDTE1MTIxMDE0NTc1M1owEzERMA8G
A1UEAxMIz3MubG9jYXVwYyEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCx
lWDFChHPvUdV8VlV89DbTUuJRWD21bwQjRydL/kkyqU3GFXSDaHFMccLdWa7FAnG
WJ/+WAPoIZbwNb3gztH4s3dCOZBCCGs12+MunUA3RFggwceyTh6r5gw118vNBB4e
kKw15ndkch56/j62F4v/Bji39jCBlqc0RYLnwXb3qU0syXYDBKFN1MEqUKHqF5Jr
IMtFV2TSKiLDy86u7C3QIOeqJN64gXRvRv8w/dE0V48dohzxAfjuvv17pK45Qq/G
Jnp14BewAETdO0WKJQvr+19YqC1DfnN1pEfKRRqMJg3Arp5ZHXchXhoNxFb66O14
pJEpgcl2xKHPiJlirxZjAgMBAAEwDQYJKoZIhvcNAQELBQADggEBADb2P8zcYC6T
m0oLi1gr2wOLKOEu63WY0KaF/010Mx91ifgOXLSPyryIjJ95RqQle1shUWMSwC
PEFGXCDL1nd5v034t60FC13ke70iyjCQRByI51z0908MEv5GI+qVUH+C7sJvwy7b
HK06dCpPW2+jbfnTawDoh5HkeZMDbl9t4GaHrgYa4cvbLDWKg9g7fsCNcWg3fr9W
XVfFEVGqK3fYC1zU7Q7xRVhkMUyW/Z8aqCjpdTmho5peceqDdz21Y9D6ZualZAt9
XI8OP0uB6s+axwRnAJTqXa48/2i8QbP2V8SLe5113TVwG5L48wCpxwBeoLbMOI5r
```

Save

Cancel

7. Enter the RSA SecurID Access Identity Provider URL from step 5 page 2 in the **SSO Login URL** field.
8. Paste the RSA SecurID Access public certificate in the x.509 window.
9. Click **Save**.
10. Click the gear icon in the upper right corner.
11. From the top menu select Employees.

COMPANY LOGO HERE



Dashboard My Info Employees Job Openings Reports Files

Search...

12. Click **Add Employee**.
13. Enter the user's required information and verify that the **Email** address matches the single sign-on user account.