

Last Modified: May 11, 2016

Aha! provides web-based product management tools and visual roadmap software for agile product managers.

Before You Begin

- RSA SecurID Access components including administrator and end user accounts must be in place.
- Acquire an Aha! administrator account and verify that SAML SSO is available.

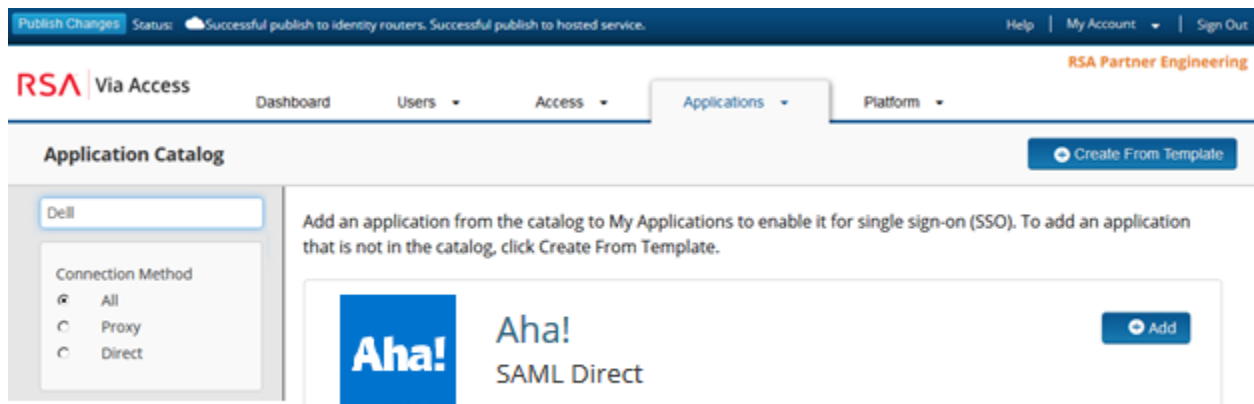
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Aha! 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 SP-initiated and IDP-initiated connections.

4. On the Connection Profile page, choose **IDP-initiated**.


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.

Identity Provider URL 

Issuer Entity ID 
 Default (idp_id): aha
 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.

<input checked="" type="checkbox"/>	Private Key Loaded	<input type="button" value="Choose File"/>	<input type="button" value="Generate Cert Bundle"/> 
<input checked="" type="checkbox"/>	Certificate Loaded	<input type="button" value="Choose File"/>	

CN=gs.local, Valid Until:
12/10/2019

Include Certificate in Outgoing Assertion


- Select **Choose File** and upload the private key.
- Select **Choose File** and upload the public certificate.
- Check **Include Certificate in Outgoing Assertion**.

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

Service Provider

Assertion Consumer Service (ACS) URL 

https://<myaccount>.aha.io/auth/saml/callback

Audience (Service Provider Entity ID) 

https://<myaccount>.aha.io/

- a. In the **Assertion Consumer Service (ACS) URL** field replace **<myaccount>** with your company's subdomain on Aha!.
- b. In the **Audience (Service Provider Entity ID)** field replace **<myaccount>** with your company's subdomain on Aha!.

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**.
9. In the Attribute Extension section, add **email**, **firstname** and **lastname**.

Attribute Extension

Attribute Source	Attribute Name	Identity Source	Property	Manage
User Store	email	DefaultId	mail	 
User Store	firstname	DefaultId	givenName	 
User Store	lastname	DefaultId	sn	 

 ADD

10. Click **Next Step**.

11. 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 →


12. Click **Next Step**.

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

14. Click **Save and Finish**.

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

Publish Changes

Status:  Changes Pending

16. Navigate to **Applications > My Applications**.

17. Locate Aha! in the list and from the **Edit** pulldown select **Export Metadata**.




Aha!

Created From: SAML 2 Generic Direct SP
SAML Direct

Edit

 Edit

 Export Metadata

 Delete

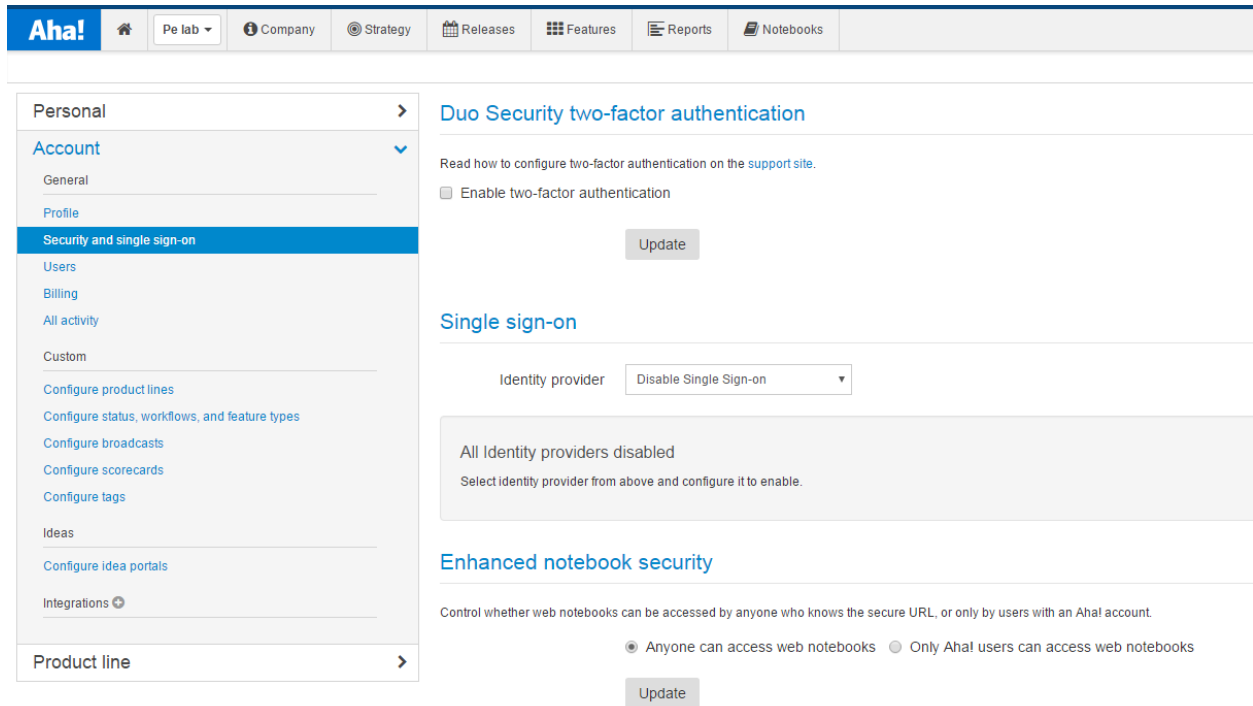
Next Steps

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

Configure Aha! to Use RSA SecurID Access as an Identity Provider

Procedure

1. Log in to your Aha! Administrator account. <https://<myaccount>.aha.io>
2. Navigate to **Account > Security and single sign-on**.



3. Select **SAML 2.0** from the Identity provider pull down.



4. Enter a name for the Identity Provider in the **Name** field.

Single sign-on

Identity provider

SAML 2.0 Configuration

Read how to configure SAML single sign-on on the [support site](#).

Name
Give this single sign-on provider a name that will be displayed to users.

Configure using Metadata URL Metadata file Manual settings

Metadata file Aha!-idp-metadata.xml
Upload a SAML configuration file in XML format.

SAML consumer URL
This is the URL that the identity provider will redirect users to after login.

SAML service provider metadata URL
This URL may be required by some identity providers.

SAML entity ID
Unique identifier for the service provider (Aha!).

5. From the **Configure using** options select **Metadata file** and upload the file RSA SecurID Access metadata file from step 17 page 4.
6. Select **Enable**.