RSA SecurID Access SAML Configuration for Aha!

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.

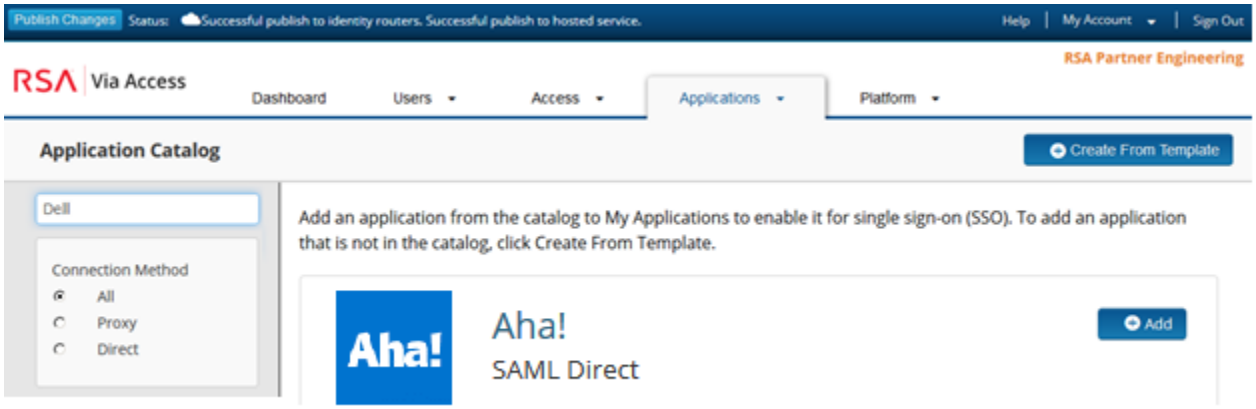
Procedure

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

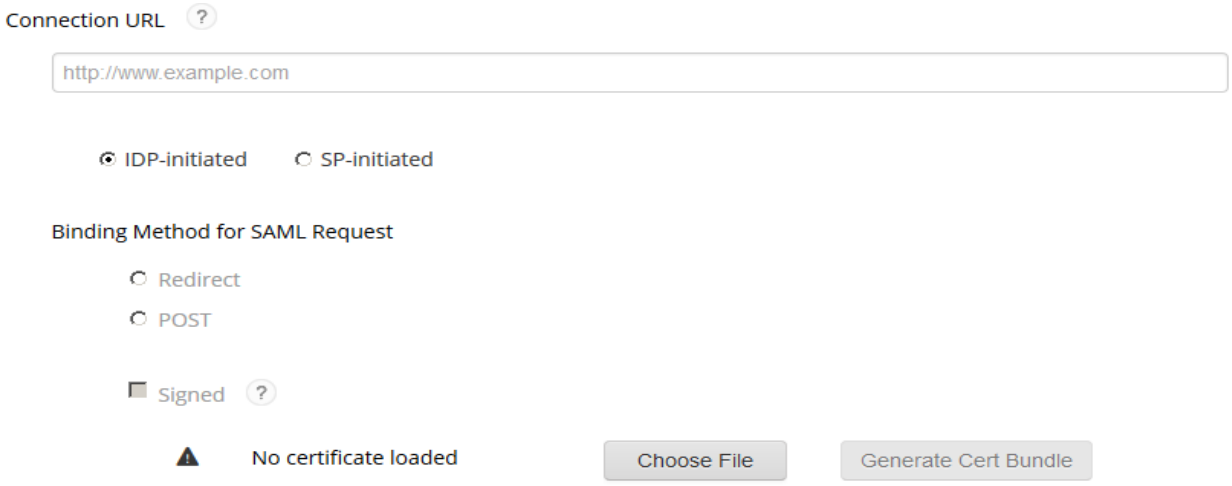
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.



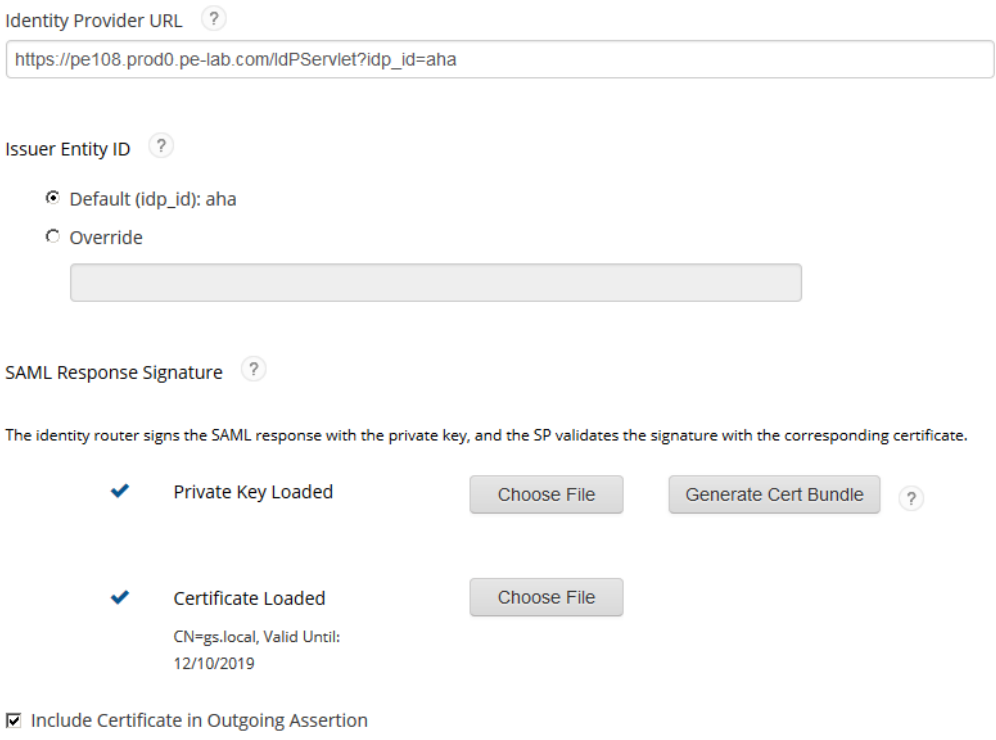
3. On the Basic Information page, specify the application name and click **Next Step**.

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

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



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

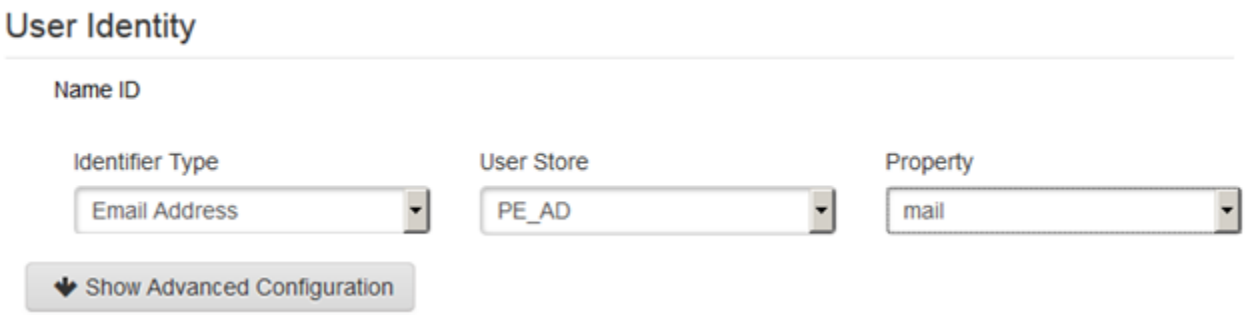


- Select **Choose File** and upload the private key.
- Select **Choose File** and upload the public certificate.
- Check **Include Certificate in Outgoing Assertion**.

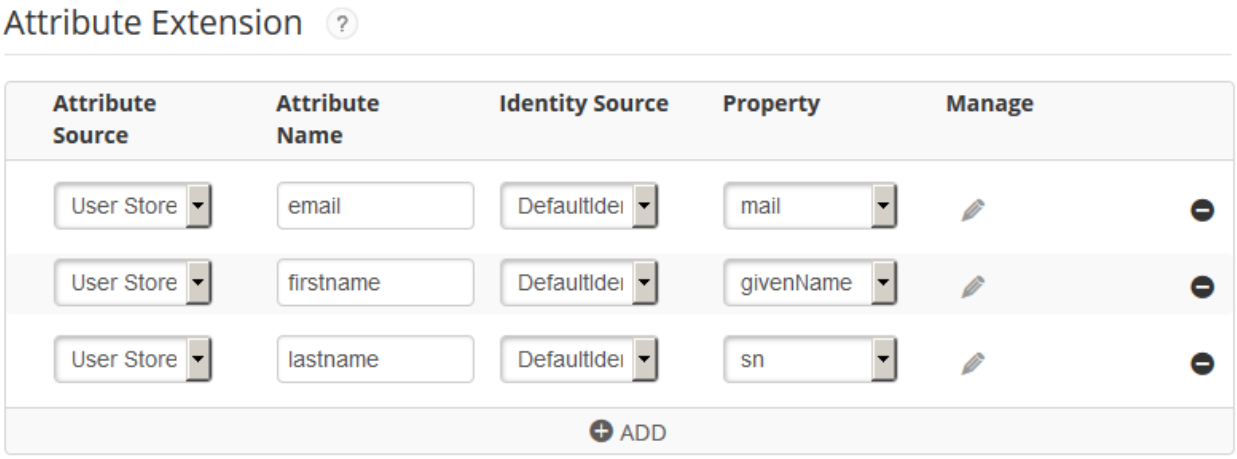
6. Scroll down to the **Service Provider** section.

   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**.

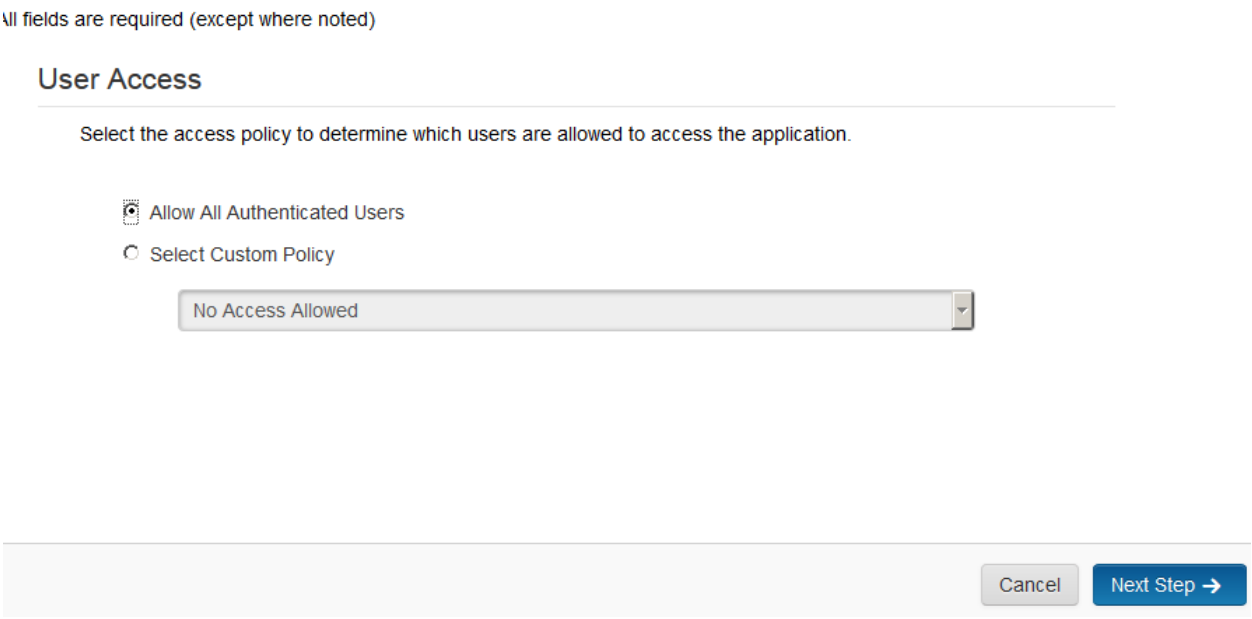


8. Click **Show Advanced Configuration**.
9. In the Attribute Extension section, add **email**, **firstname** and **lastname**.



10. Click **Next Step**.

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



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.

16. Navigate to **Applications > My Applications**.
17. Locate Aha! in the list and from the **Edit** pulldown select **Export Metadata**.

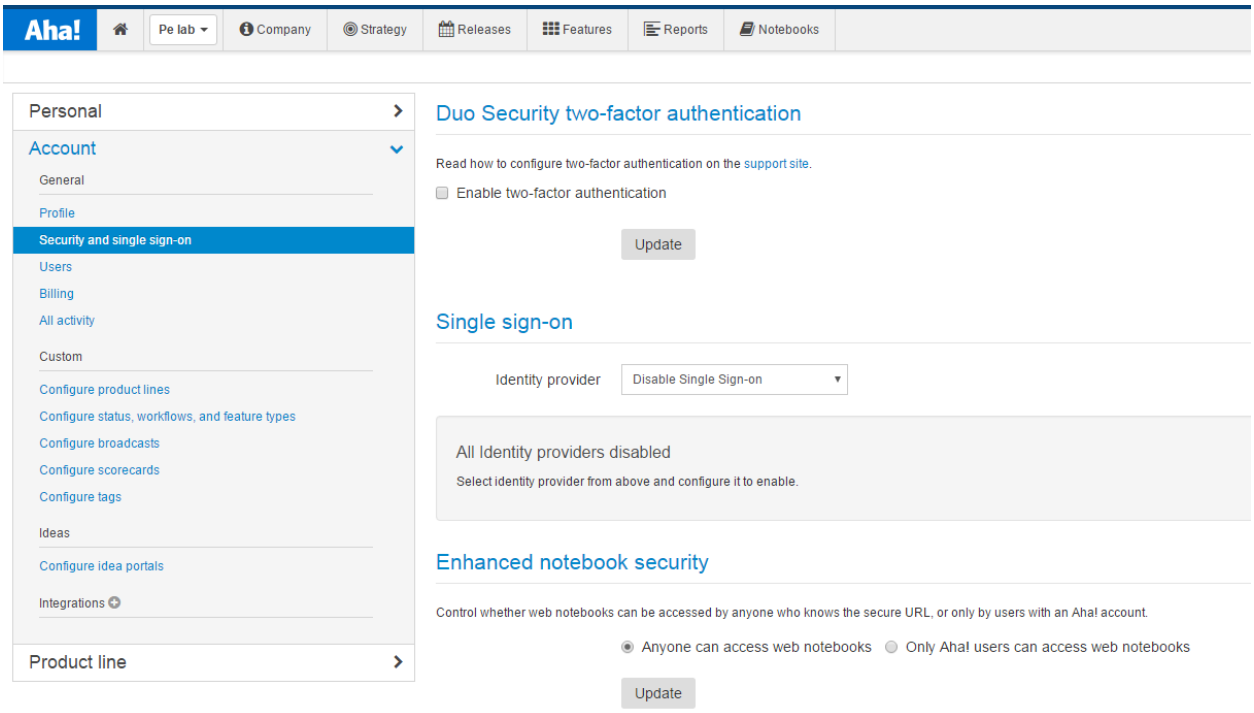
Next Steps

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

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

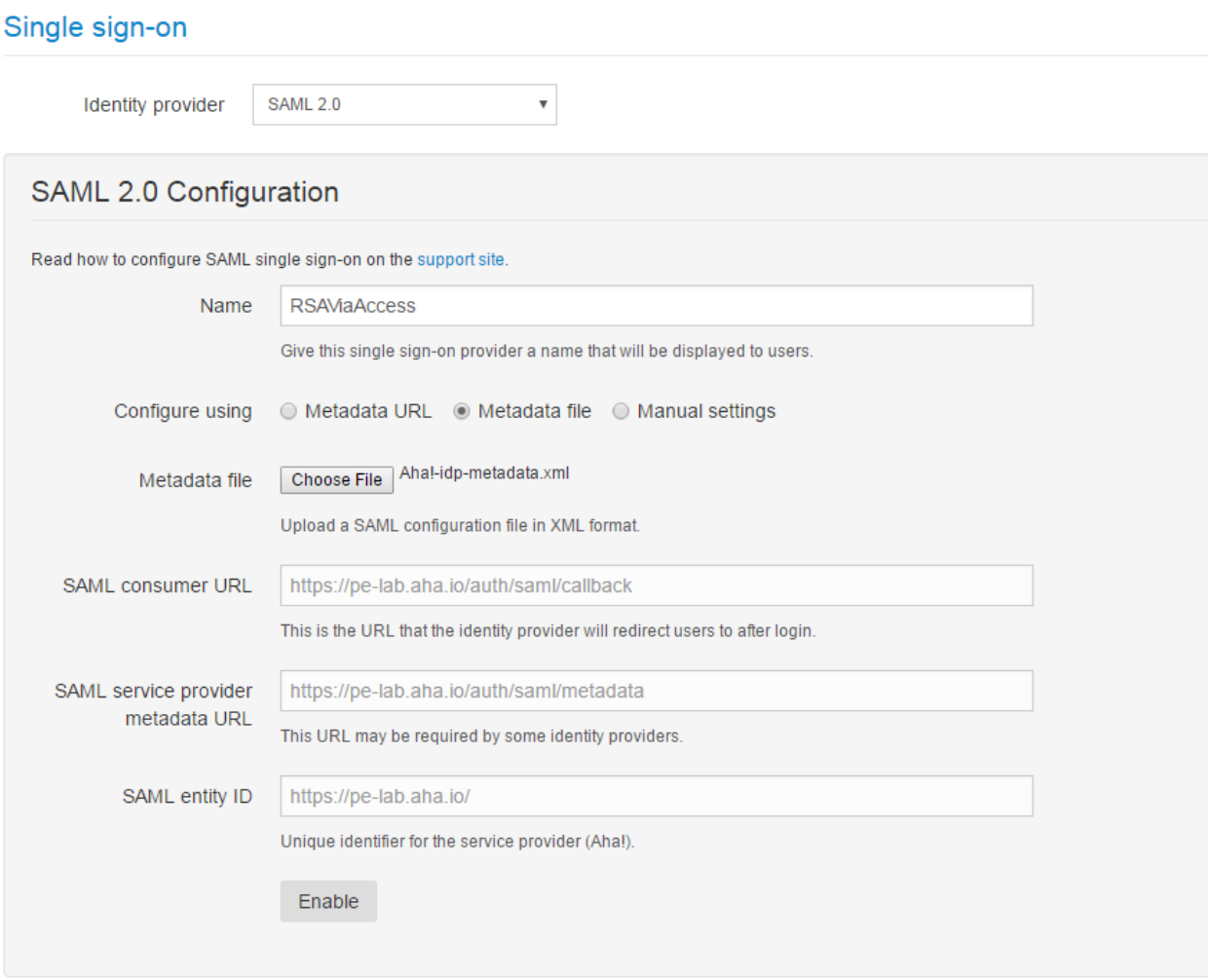
Procedure

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.



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**.

GLS