



Configure SSO with Active Directory Federation Services (AD FS)

Last Modified on 04/03/2024 12:49 pm EDT

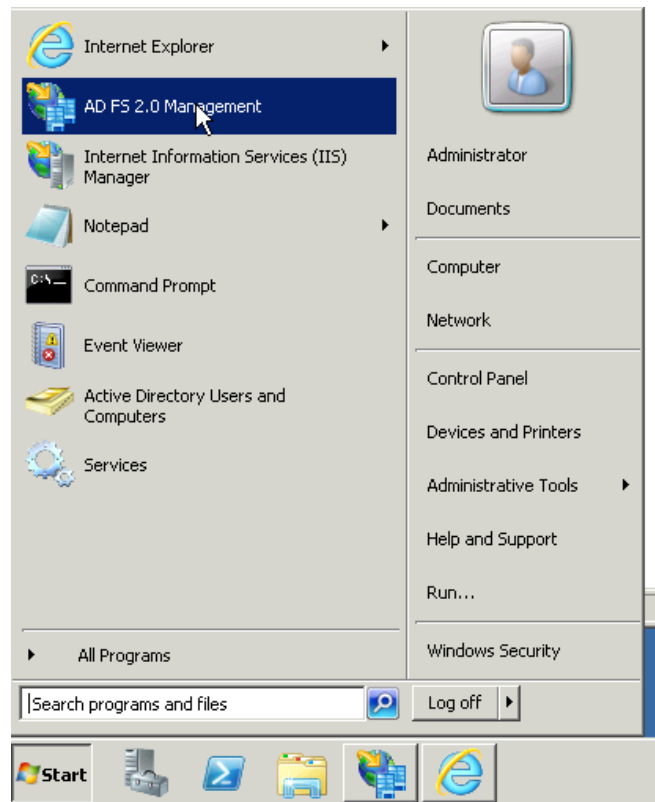
This tutorial will help walk you through setting up an integration between AD FS and KnowledgeOwl using SAML 2.0.



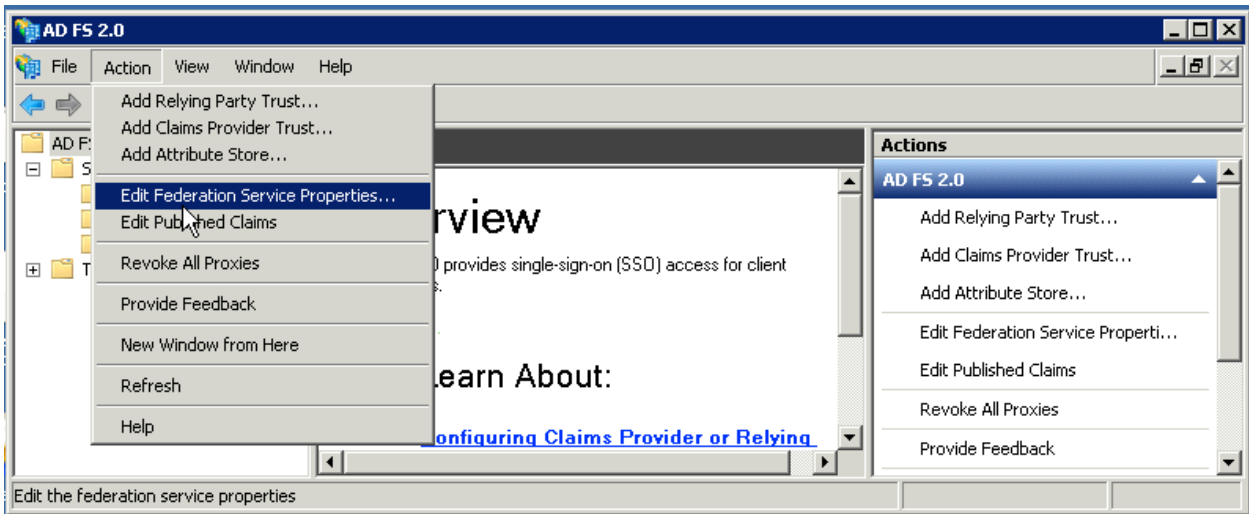
The screenshots below may not match your version of AD FS, but the steps to complete the integration should be the same.

Step 1: Add your IdP info to KnowledgeOwl

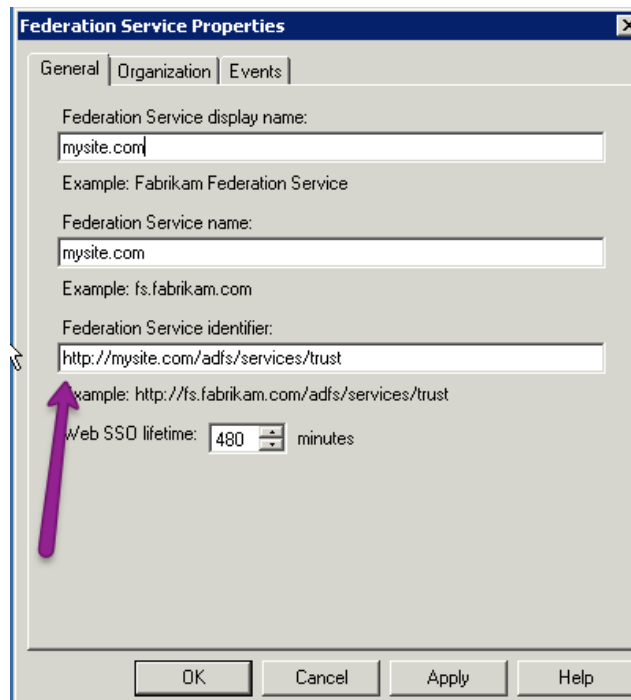
1. On your Windows server, find and open AD FS 2.0 Management (commonly found in the start menu under Administrative Tools).



2. Once you have opened AD FS Management, go to **Action > Edit Federation Service Properties**.



3. Copy the link that is displayed under **Federation Service identifier**.




4. In KnowledgeOwl, go to **Settings > SSO**.

5. Paste the link you copied in Step 3 into the field **iDP entityID**.

6. For most AD FS builds, the **Login URL** and the **Logout URL** will be the base URL of the iDP entityID with **"/adfs/ls/"** as the endpoint instead of **"/adfs/services/trust"**:

IdP entityID	<input type="text" value="https://mysite.com/adfs/services/trust"/>
IdP Login URL	<input type="text" value="https://mysite.com/adfs/ls"/>
IdP Logout URL	<input type="text" value="https://mysite.com/adfs/ls"/>

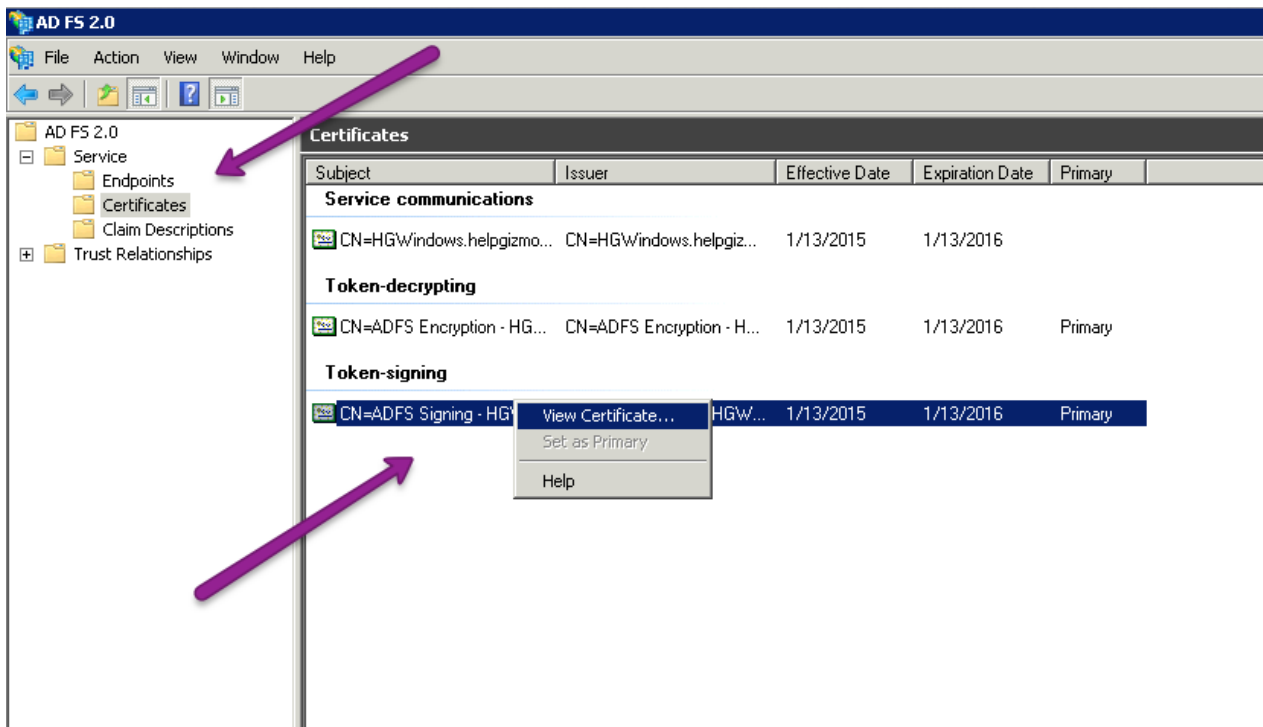
 If this is not true for your setup, you will need to locate the URL that your ADFS setup uses for authentication.

7. Be sure to Save your changes in KnowledgeOwl if you're not immediately continuing to Step 2.

Step 2: Upload the IdP certificate to KnowledgeOwl

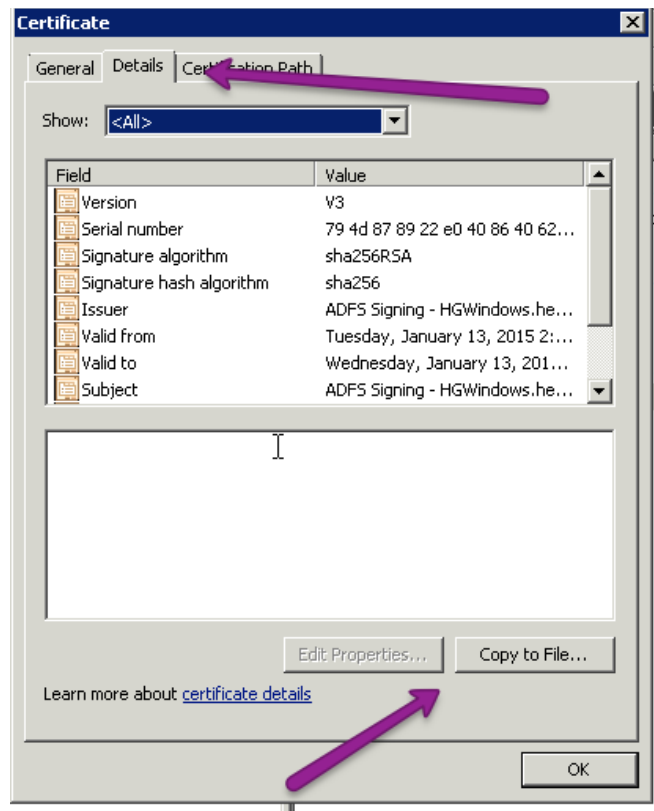
Next we will want to export our AD FS cert into a x509 DER format to upload into KnowledgeOwl. To do so:

1. In AD FS 2.0, go to **Service > Certificates**.
2. In the main pane, right-click on the certificate in the **Token-signing** section.
3. Click **View Certificate...** in the right-click menu.



4. Open the **Details** tab.

5. Click on **Copy to File...**



6. This will bring up a **Certificate Export Wizard**. In the wizard, choose next until you get to the format page. On the format page make sure that **DER encoded binary X.509** is selected and choose next.
7. Choose a filename and a location that you will remember for the cert and then finish the wizard.
8. In KnowledgeOwl, upload the certificate you created by clicking the **Upload certificate** link in the **IdP Certificate** section:

IdP Certificate

 [Upload certificate...](#)

[View KnowledgeOwl SP Metadata](#)

9. Once you have selected the correct certificate, be sure to **Save** your changes.

Step 3: Enable SAML SSO

Once you have entered the 3 IdP fields and have uploaded the IdP certificate into KnowledgeOwl, make sure that the **Enable SAML SSO** checkbox is checked, and **Save** the SSO Settings page.

SAML SSO Settings

ⓘ Restrict Access to SSO will trump Public Default Access, requiring everyone to authenticate. Choose Restrict by Reader Logins as the Default Access to allow optional manual re

Enable SAML Enable SAML SSO — [View tutorial](#)
 Restrict Access to SSO
 Enable Debug Mode

Step 4: Add the KnowledgeOwl SP info to your IdP

Now that KnowledgeOwl has your information, you will need to grab some data from KnowledgeOwl to add into AD FS.

1. In KnowledgeOwl, click on the **View KnowledgeOwl SP Metadata** button underneath your IdP Certificate.


IdP Certificate

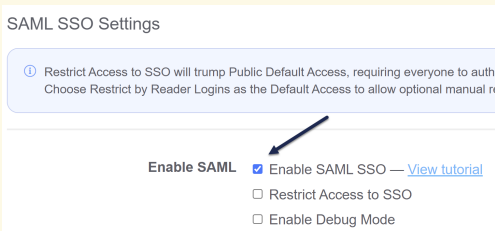
Common name: mysamlapp.com
Valid starting: 01/11/2017 3:23 pm EST
Valid until: 01/11/2027 3:23 pm EST

[Upload new certificate...](#)

[View KnowledgeOwl SP Metadata](#)

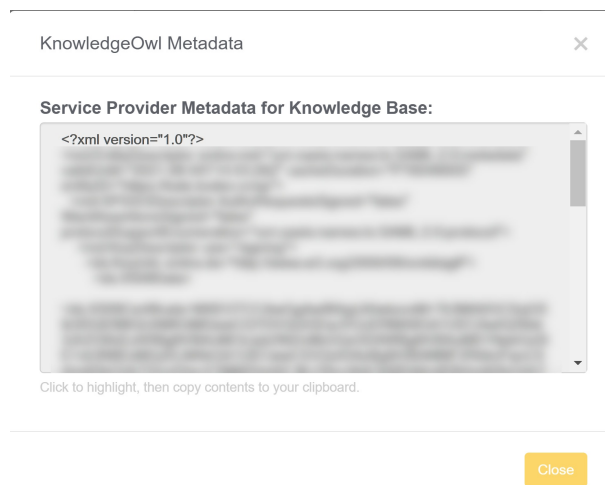
2. This will open up a pop-up with KnowledgeOwl XML metadata within it.

 If you aren't seeing any metadata, ensure that you've checked the box to "Enable SAML SSO" and saved. The metadata is only generated after this option is saved.

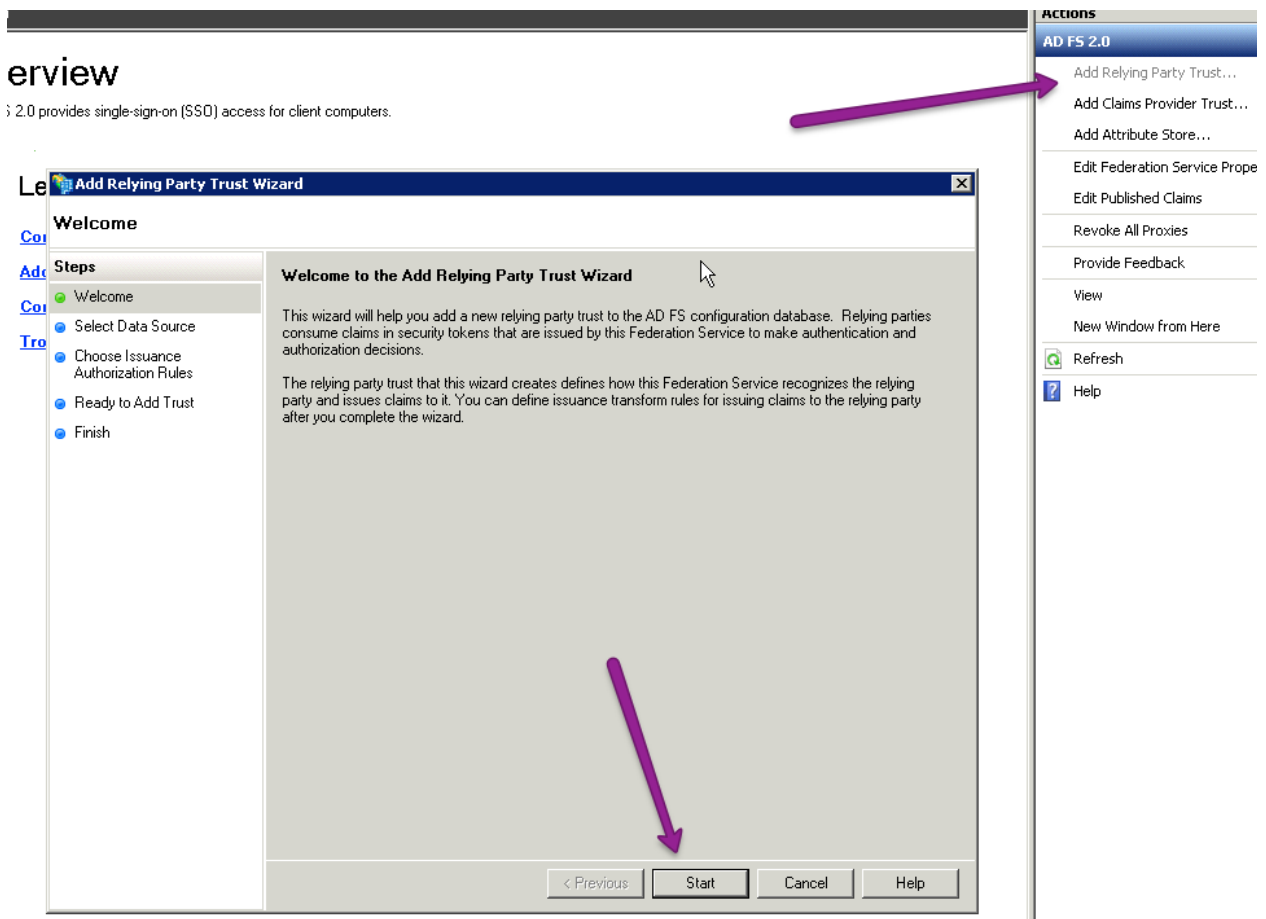


The screenshot shows the SAML SSO Settings page with the 'Enable SAML SSO' checkbox checked. A blue arrow points from the 'View KnowledgeOwl SP Metadata' button in the previous step to this checkbox.

3. Click anywhere in the **Service Provider Metadata for Knowledge Base** pop-up to highlight the full XML contents and copy it.



4. Open up a simple text editor of your choice (Notepad works well).
5. Paste the metadata text into Notepad.
6. Choose **File > Save as...**
7. Change the **Save as type:** to **All Files**. Save the file as **ko-metadata.xml** (the **.xml** extension is required!).
8. In AD FS, click on **Add Relying Party Trust...** which will open up the **Add Relying Party Trust Wizard**. Click on **Start** within that wizard.



9. On the next screen, select **Import data about the relying party from a file**.

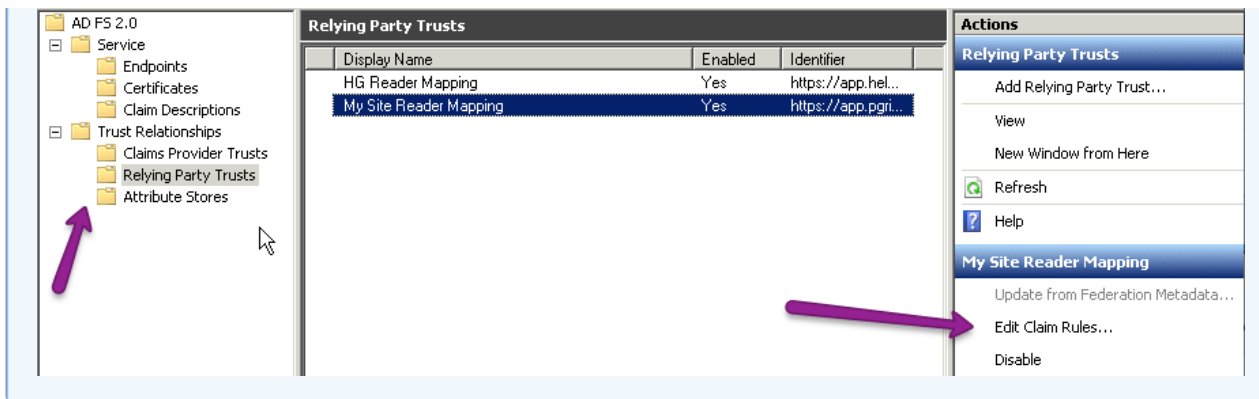
10. Browse to the XML metadata that we saved in Step 7 and choose **Next**.

11. Choose a name that makes sense, such as "KnowledgeOwl SSO", add whatever notes you would like, and click **Next**.

12. For most setups, you can click next until you finish this wizard, which should open up the **Edit Claim Rules** dialog.



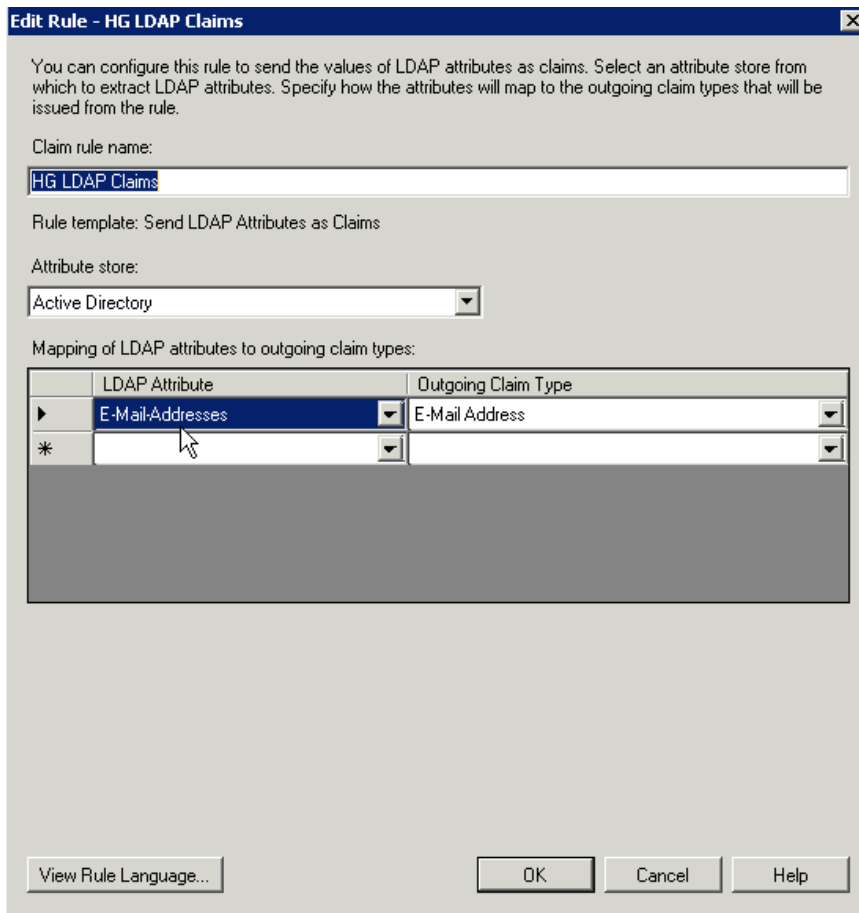
If the **Edit Claim Rules** dialog does not open automatically, you can navigate to it by going to **Trust Relationships > Relying Party Trusts**, select the trust identifier you created in Step 11, and click on **Edit Claim Rules....**



13. In the **Edit Claim Rules** dialog click on **Add Rule...**

14. Choose the default **Send LDAP Attributes as Claims** and click **Next**.

15. Here you can choose what information you want to send to KnowledgeOwl. At the very least you need to send the **E-Mail Addresses**.



16. Click on **Add Rule...** again.

17. This time under **Claim rule template**: choose **Transform an Incoming Claim** and click **Next**.

18. Set the **Claim rule name** to **KO Name ID** or something similar.
19. Set the **Incoming claim type** to **E-Mail Address**.
20. Set the **Outgoing claim type** to **Name ID**.
21. Set the **Outgoing name ID format** to **Email**.
22. Be sure the option to **Pass through all claim values** is selected. Your configuration should look a bit like this:

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The 'Steps' pane on the left shows 'Choose Rule Type' and 'Configure Claim Rule' as completed steps. The main area contains the following configuration:

- Claim rule name:** HG Name ID
- Rule template:** Transform an Incoming Claim
- Incoming claim type:** E-Mail Address
- Incoming name ID format:** Unspecified
- Outgoing claim type:** Name ID
- Outgoing name ID format:** Email
- Options:**
 - Pass through all claim values
 - Replace an incoming claim value with a different outgoing claim value
 - Incoming claim value:** [Empty text box]
 - Outgoing claim value:** [Empty text box]
 - Replace incoming e-mail suffix claims with a new e-mail suffix
 - New e-mail suffix:** [Empty text box]
 - Example: fabrikam.com

At the bottom of the dialog are buttons for '< Previous', 'Finish', 'Cancel', and 'Help'.

23. Click **Finish**.

Step 5: Enable debug mode

AD FS may send the attribute claims over in a way that you are not expecting.

In order to view how AD FS is sending the claims, in Knowledgeowl:

1. In **Settings > SSO** in the **SAML Settings** tab, check the box next to **Enable debug mode**.
2. **Save**.
3. In a private browser window or in an incognito tab, copy and paste the **SP Login URL** into the address bar. If the

above steps were done correctly, you should be asked to log into your AD server where you will be redirected back to your knowledge base.

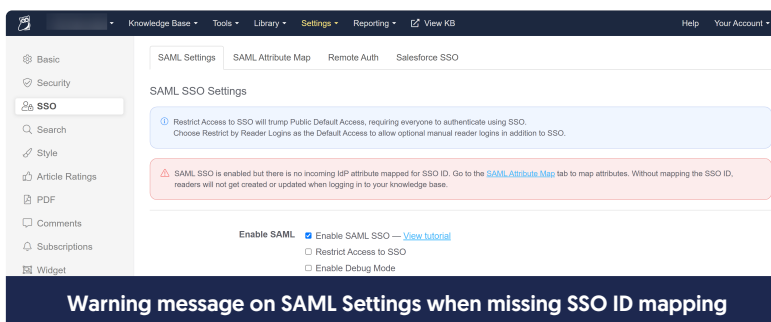
4. In debug mode, you'll then see a list of the IdP attributes that ADFS is sending over.
5. Keep this window open while you work on Step 6. Once you're done with Step 6, be sure to uncheck the box next to **Enable debug mode** and re-save the settings.

Step 6: Map SAML attributes to fields in KnowledgeOwl

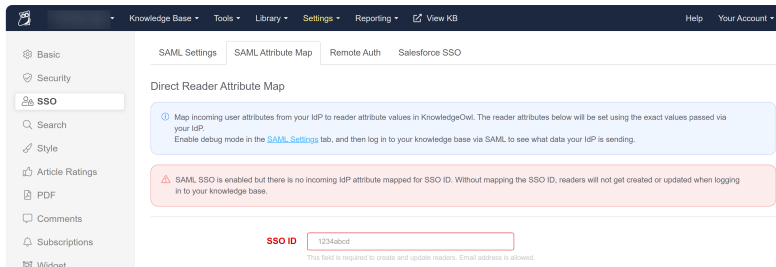
With your debug window open, you can now map SAML attributes to fields in KnowledgeOwl. To do so:

1. In KnowledgeOwl, go to **Settings > SSO**.
2. Open the **SAML Attribute Map** tab.
3. In your debug output, locate the **attribute value** that contains your email address, and copy the **Attribute Name** exactly as it appears after the colon.
4. On the SAML Attribute map tab of KnowledgeOwl, paste that attribute name into the fields for **SSO ID** and **Username / Email**.
5. To map additional fields, repeat this process. See [Direct Reader Attribute Map](#) for more information.
 - If you cannot directly map an IdP attribute to a KnowledgeOwl reader attribute, you can use [Custom Attribute Map Rules](#) to do some mappings or logic for you. See the help page on those rules for more info.
6. Once you're done mapping fields, uncheck the **Enable debug mode** checkbox.
7. **Save all your changes.**
8. In the tab or window that contained the debug information, click on the **Re-login to see any changes** link at the top to log in through AD FS again. If everything was successful, you will be logged into your knowledge base and you will now have a working SAML SSO integration with AD FS.

The SSO ID is a required mapping. If you don't set it up, you'll see [warning messages](#) in **Settings > SSO** in both the **SAML Settings** tab and the **SAML Attribute Map** tab:



The screenshot shows the KnowledgeOwl interface with the SAML Settings tab selected. The left sidebar contains navigation options: Basic, Security, SSO (selected), Search, Style, Article Ratings, PDF, Comments, Subscriptions, and Widget. The main content area displays 'SAML SSO Settings' with a warning message: 'SAML SSO is enabled but there is no incoming IdP attribute mapped for SSO ID. Go to the SAML Attribute Map tab to map attributes. Without mapping the SSO ID, readers will not get created or updated when logging in to your knowledge base.' Below the warning, there are checkboxes for 'Enable SAML' (checked), 'Enable SAML SSO' (checked), 'Restrict Access to SSO' (unchecked), and 'Enable Debug Mode' (unchecked). A dark blue banner at the bottom of the screenshot reads 'Warning message on SAML Settings when missing SSO ID mapping'.



Warning message on SAML Attribute Map when missing SSO ID mapping

Step 7: Optional settings

With your AD FS SAML SSO login working, you can now review two additional options:

- To make it so that SAML SSO is the **only** access method for your knowledge base, check the **Restrict Access to SSO** box in **Settings > SSO** and **Save**. This will override the **Default Access** selection in **Settings > Security**.
- If you'd like to use the AD FS SAML SSO as your **only** or **primary** reader authentication mechanism, set the **Default Login Page** in **Settings > Security** to **SAML Login URL** and **Save**.

See [SSO options for different knowledge base setups](#) for more information.