Configure SSO with Active Directory Federation Services (AD FS)

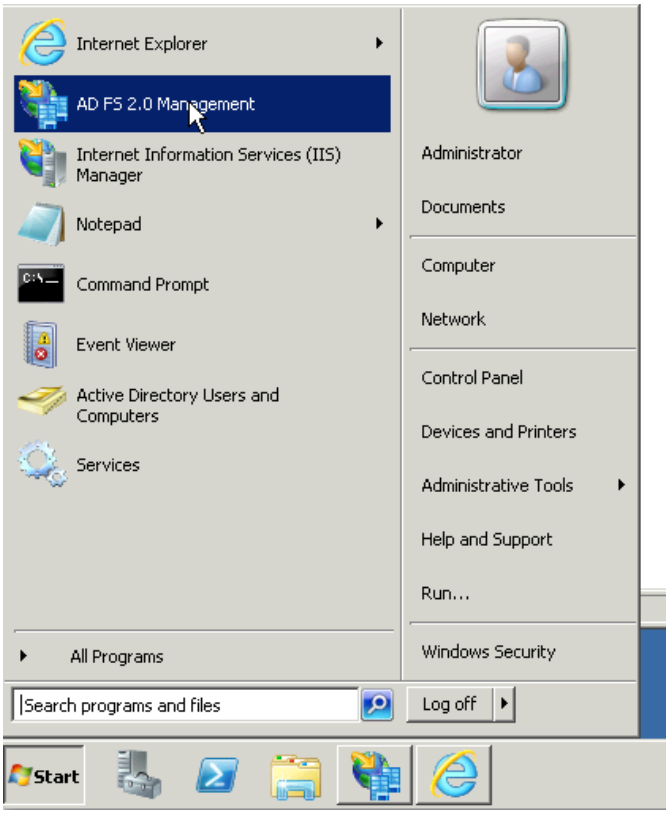
Last modified on 11/07/2026 12:01 pm EST

This tutorial will help walk you through setting up a an integration between AD FS and KnowledgeOwl using SAML 2.0. This feature is available on select plans.

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

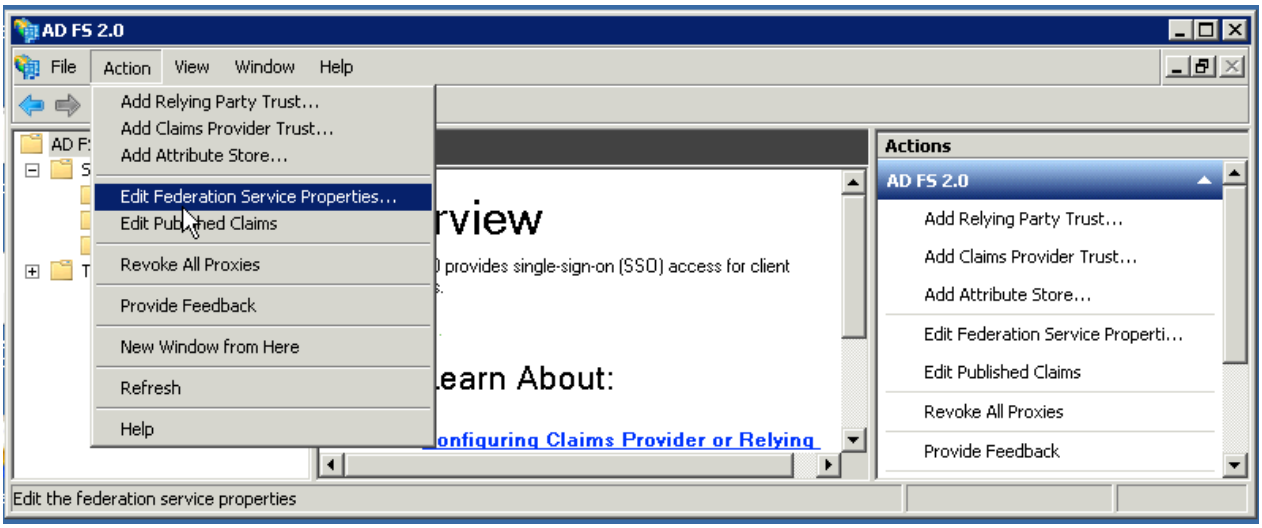
Step 1: Add your IdP info to KnowledgeOwl

1. On your Windows server, find and open AD FS 2.0 Management (commonly found in **Start > Administrative Tools**).

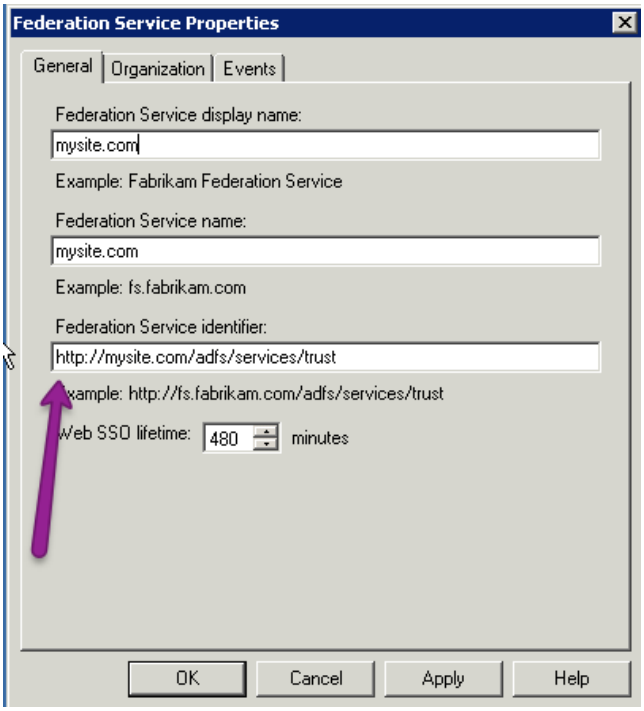


2. Once you have opened AD FS Management, go to **Action > Edit Federation Service Properties.**

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.



3. Copy the **Federation Service identifier** URL.



4. In KnowledgeOwl, go to **Security and access > Access & SSO**.

5. In the **Login methods** card, select **Set up** or **Manage** next to **SAML**.

6. Expand step 2, **Connect your identity provider**.

7. Paste the **Federation Service identifier** you copied as the **IdP entity ID**.

8. Enter your **IdP login URL** and **IdP logout URL**.

    a. If your AD FS build doesn't explicitly list these URLs, you can usually remove `/adfs/services/trust` from your **IdP entity ID URL** and replace it with `/adfs/ls/`. For example, if my **IdP entity ID URL** was

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

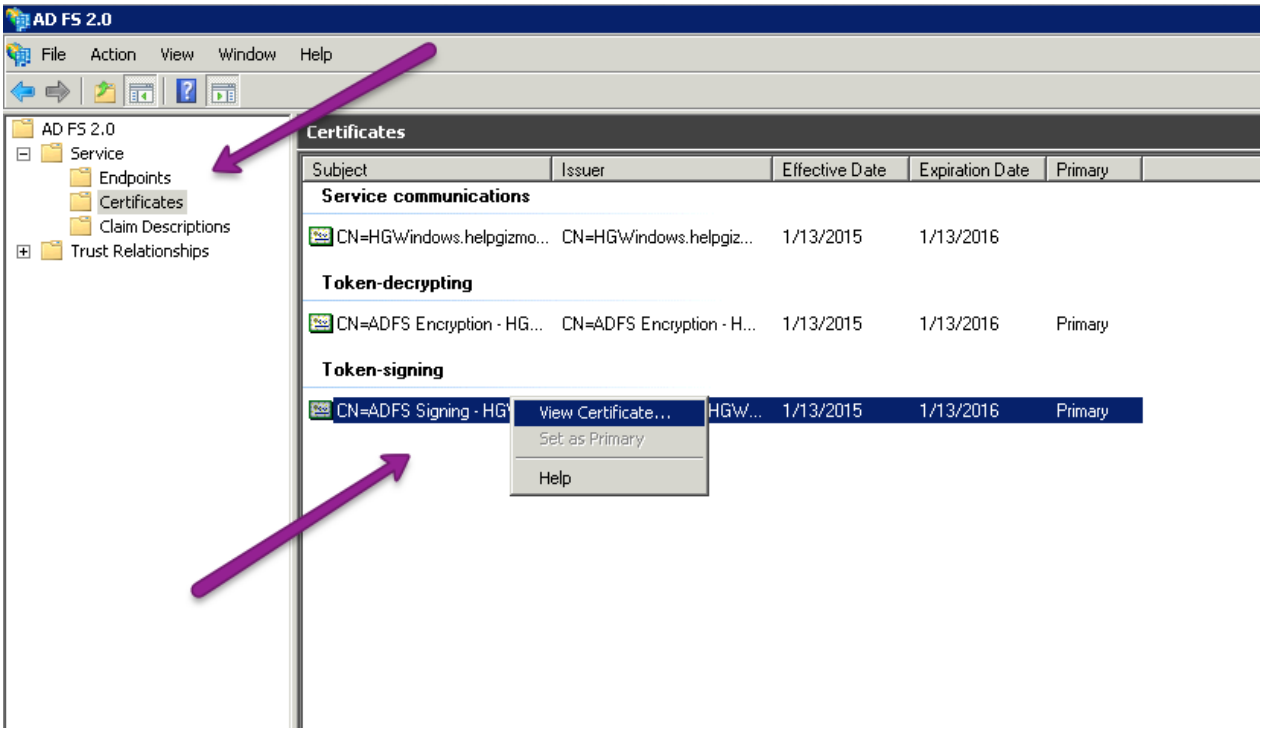
`https://mysite.com/adfs/services/trust`, **my IdP login URL and IdP logout URL are** `https://mysite.com/adfs/ls`.

9. Select **Save changes.**

Step 2: Upload the IdP certificate to KnowledgeOwl

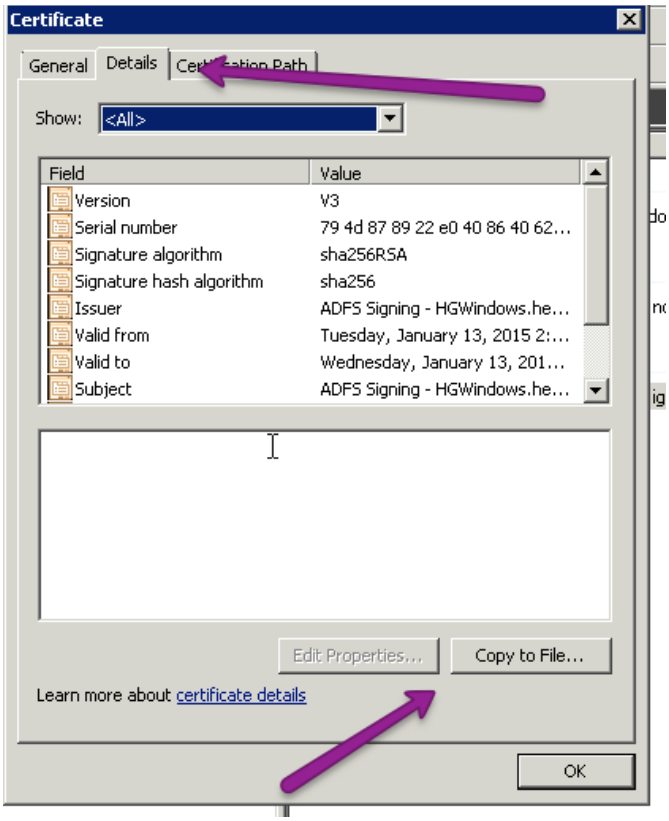
Next, export your AD FS cert into an x509 DER format to upload into KnowledgeOwl. To do so:

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. **Select View Certificate... in the right-click menu.**



4. **Open the Details tab.**
5. **Select Copy to File...**

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

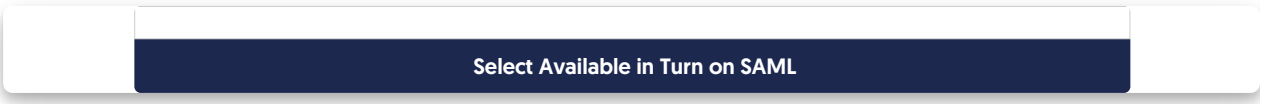


6. This opens a **Certificate Export Wizard**. In the wizard, choose Next until you get to the format page. On the format page, make sure that **DER encoded binary X.509** is selected and choose next.
7. Choose a filename and a location that you will remember for the cert and then finish the wizard.
8. In the KnowledgeOwl SAML setup, expand step 2, **Connect your identity provider**.
9. Under **IdP certificate**, drag the file you just created into the drop zone, or select **browse** to choose it. KnowledgeOwl accepts .crt, .pem, .cer, and .der files.
10. The certificate is saved as soon as you upload it, so there's no need to select **Save changes**. The **IdP certificate** section then displays the certificate's common name and the dates it's valid.

Step 3: Enable SAML SSO

Once you have entered the three IdP fields and have uploaded the IdP certificate into KnowledgeOwl, enable SAML SSO:

1. In the KnowledgeOwl SAML setup, expand step 5, **Turn on SAML**.
2. Select **Available**.



Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

3. Be sure to select **Save changes.**

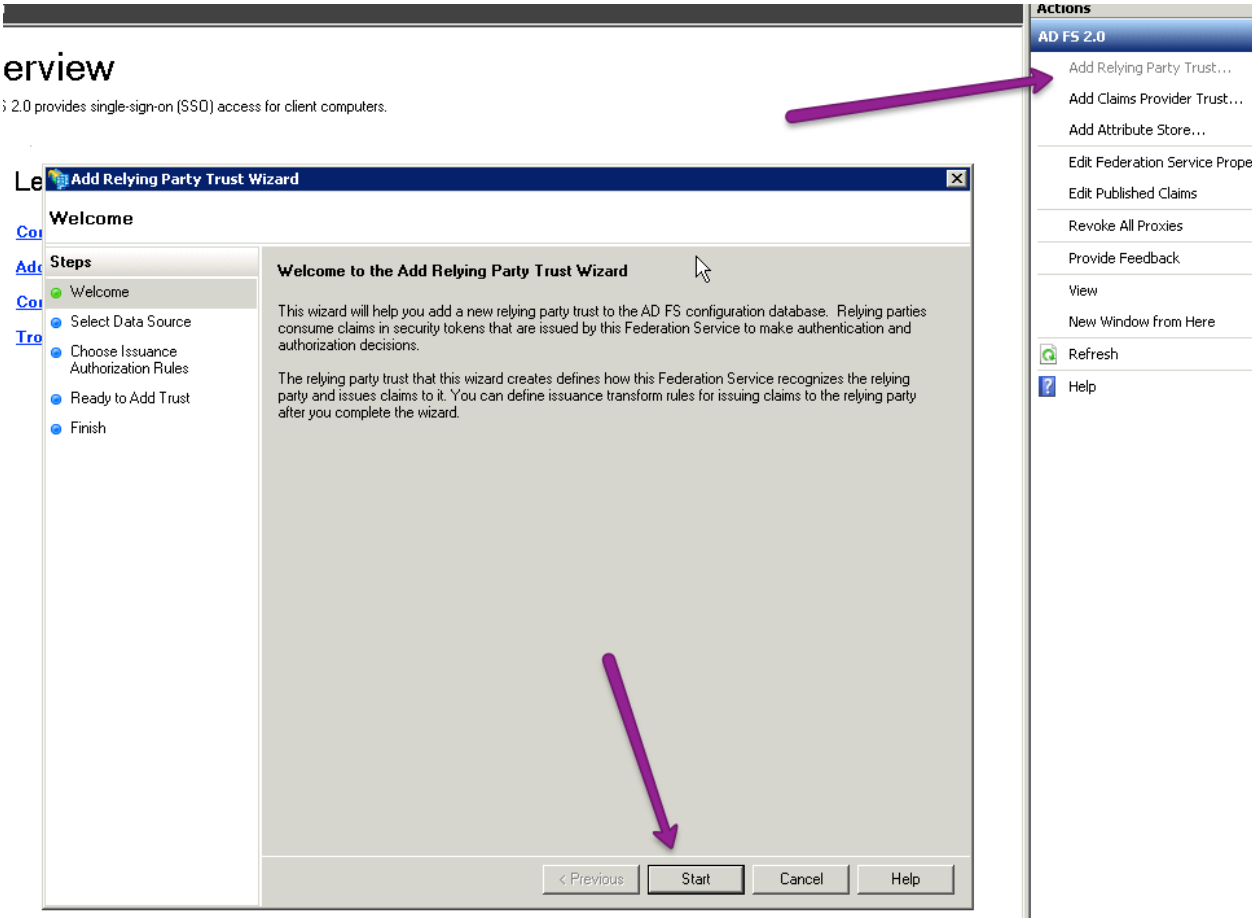
Step 4: Add the KnowledgeOwl SP info to your IdP

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

1. In the KnowledgeOwl SAML setup, expand step 1, **Give these details to your identity provider.**
2. Select **Download metadata.** KnowledgeOwl saves the metadata as `knowledgeowl-sp-metadata.xml` **. XML format is required for AD FS.**



3. In AD FS, select **Add Relying Party Trust....** The **Add Relying Party Trust Wizard** opens.
4. Select **Start** within that wizard.



5. On the next screen, select **Import data about the relying party from a file.**
6. **Browse to the** `knowledgeowl-sp-metadata.xml` **file you downloaded and choose Next.**

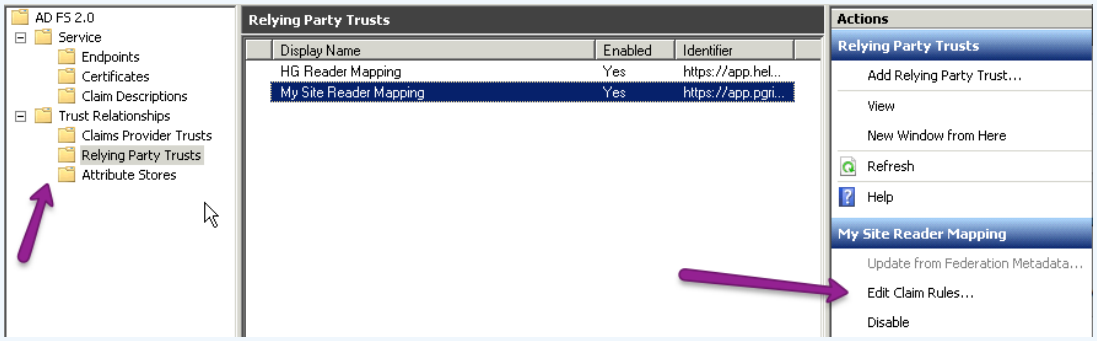
Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

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

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

I don't see Edit Claim Rules

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 just named, and click on **Edit Claim Rules...**.

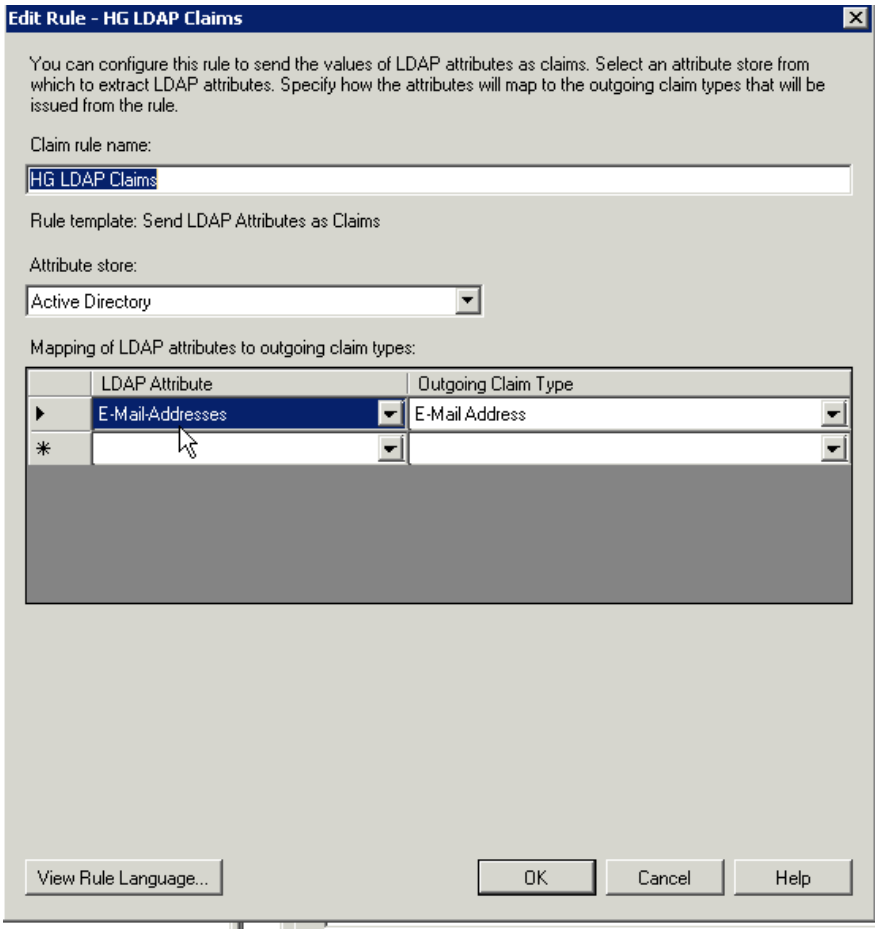


9. In the **Edit Claim Rules** dialog, select **Add Rule...**.

10. Choose the default **Send LDAP Attributes as Claims** and select **Next**.

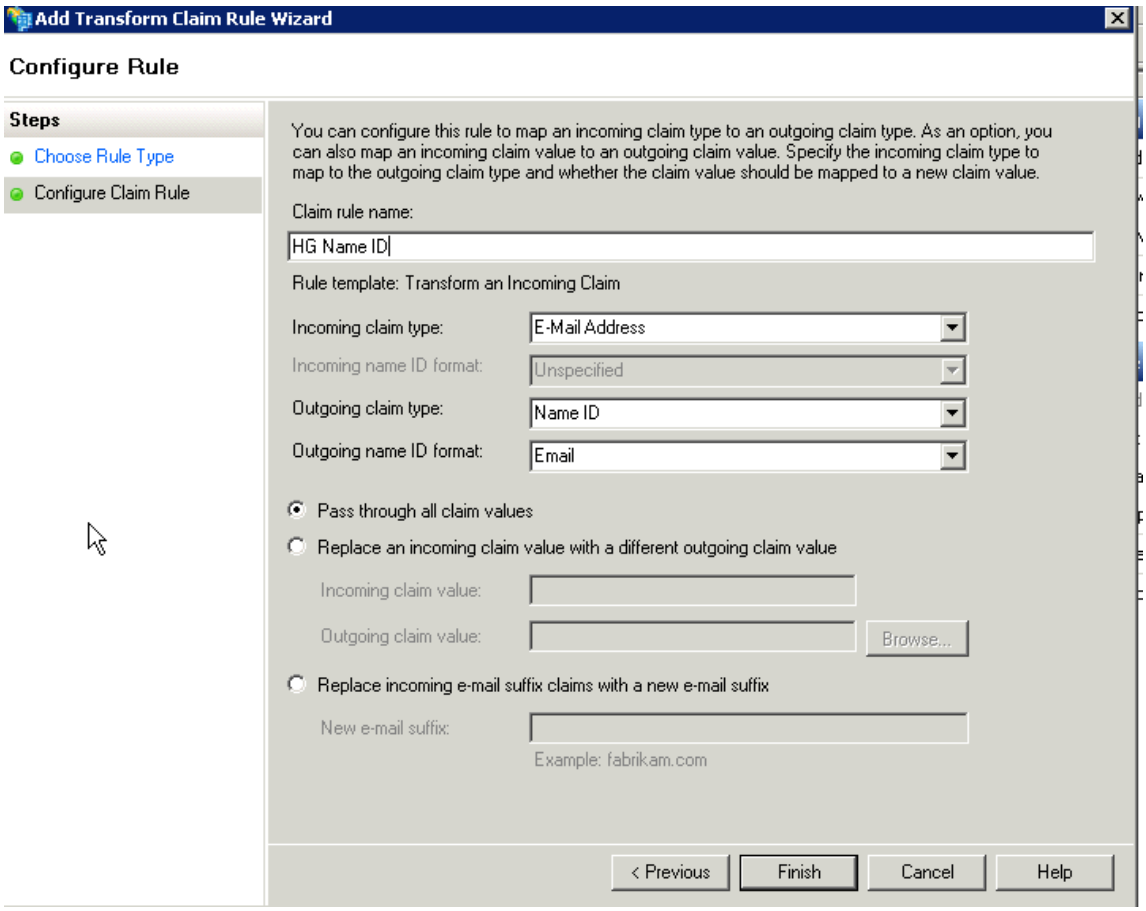
11. Here you can choose what information you want to send to KnowledgeOwl. At the very least you need to send the **E-Mail Addresses**.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.



12. Select **Add Rule...** again.
13. This time under **Claim rule template:** choose **Transform an Incoming Claim** and select Next.
14. Set the **Claim rule name** to KO Name ID or something similar.
15. Set the **Incoming claim type** to E-Mail Address.
16. Set the **Outgoing claim type** to Name ID.
17. Set the **Outgoing name ID format** to Email.
18. Be sure the option to **Pass through all claim values** is selected. Your configuration should look a bit like this:

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.



19. Select **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 the KnowledgeOwl SAML setup, expand step 4, **Test login**, and check the box next to **Debug mode**.
2. Select **Save changes**.
3. In a private browser window or in an incognito tab, copy and paste the **SP login (ACS) 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. Debug mode doesn't stop the login; the attributes AD FS sent are kept for five minutes.
4. Back in step 4, select **Load last login attempt**. You'll then see the IdP attributes that AD FS is sending over.
5. Once you're done with Step 6, be sure to uncheck **Debug mode** and select **Save changes**.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

Step 6: Map SAML attributes to fields in KnowledgeOwl

With the attributes from your test login loaded, you can now map SAML attributes to fields in KnowledgeOwl. To do so:

1. In the KnowledgeOwl SAML setup, expand step 3, **Map reader attributes**.
2. *Optional:* Under **Identity provider**, select **AD FS**, then select **Fill in AD FS settings**. This fills in the standard AD FS claim names for SSO ID, Username / email, First name, Last name, and Reader groups. AD FS only sends the claims your claim rules include, so check them against what AD FS sent.
3. In the attributes from your test login, locate the attribute that contains your email address, and copy its name exactly as it appears.
4. Paste that attribute name into the fields for **SSO ID** and **Username / email** in step 3. You can also select the arrow at the right end of the field and pick it from the attributes your IdP sent.
5. To map additional fields, repeat this process. Refer to SAML attribute map for more information.
    - If you cannot directly map an IdP attribute to a KnowledgeOwl reader attribute, use Custom attribute map rules.
6. Once you're done mapping fields, uncheck **Debug mode** in step 4.
7. Select **Save changes**.
8. In a private browser window, open the **SP login (ACS) URL** to log in through AD FS again. If everything was successful, you'll log into your knowledge base. If so, congratulations! You now have a working SAML SSO integration with AD FS.

The SSO ID is a required mapping. If you don't set it up, the SAML row in the **Login methods** card of **Security and access > Access & SSO** displays a warning: "No SSO ID mapped, so readers won't be created".

Step 7: Optional settings

With your AD FS SAML SSO login working, review three additional options:

- To make it so that SAML SSO is the main access method for your knowledge base, select **Required for all readers** in SAML step 5, **Turn on SAML**, and select **Save changes**. Anyone who isn't logged in is sent straight to SAML. This overrides the **Who can read this knowledge base?** selection in **Security and access > Access & SSO**. Other login methods set to **Available** still work through their login links. Refer to SSO options for different knowledge base setups for more information.
- If you'd like to use the SAML SSO as your primary reader authentication mechanism without requiring it, go to **Security and access > Access & SSO**. In the **Login methods** card, set **Send readers who aren't logged in to** to **SAML login** and select **Save changes**. (This option isn't shown when **Who can read this knowledge base?** is set to **Logged-in readers only**.) Refer to SSO options for different knowledge base setups for more information.
- If you'd like to use SAML SSO for your authors, refer to Set up SAML SSO for authors.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.

Copyright © 2015 – 2025 Silly Moose, LLC. All rights reserved.
Powered by KnowledgeOwl knowledge base software.