Configure SAML SSO (generic instructions)

Last Modified on 04/18/2024 11:37 am EDT

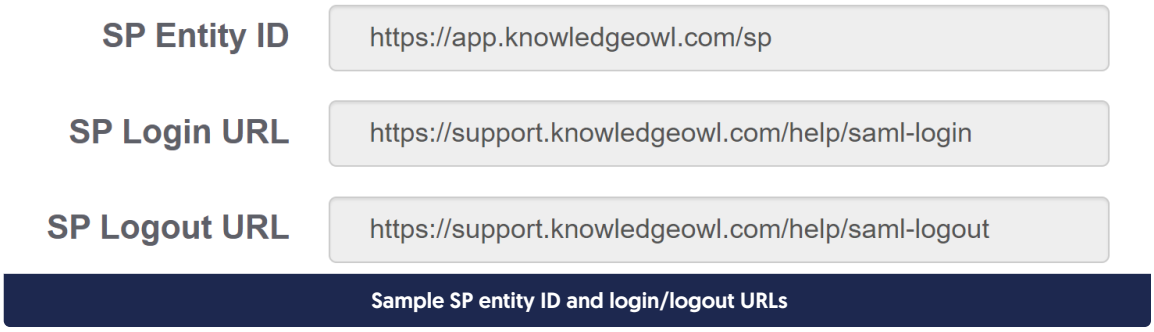
Below are instructions for setting up SAML SSO using a generic identity provider. We have specific instructions for our most popular identity providers:

- ADFS
- G Suite (Google Apps)
- Azure AD

Step 1: Add the KnowledgeOwl SP info to your IdP

Generally speaking, when adding an SP to your IdP, there are four pieces of information that you need about the SP.

1. SP Entity ID
2. SP Login URL — sometimes referred to as a "sign on URL"
3. SP Logout URL — some systems do not ask for this
   All three of these fields can be found in your knowledge base in **Settings > SSO** in the **SAML Settings** tab:



Sample SP entity ID and login/logout URLs

4. Name ID Format — some systems do not ask for this. If yours needs it, you should set it to "**Unspecified**" or, if you need the long version: "**urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**"

Step 2: Add your IdP info to KnowledgeOwl

Once you have entered those pieces of information into your IdP, the IdP should provide you with the same three pieces of information as above, but for the IdP side of the connection:

1. IdP Entity ID

2. IdP Login URL — sometimes referred to as a "sign on URL"

3. IdP Logout URL — if the IdP does not provide this, use the login URL

Add this information into the appropriate fields in KnowledgeOwl, located just under the SP fields in **Settings > SSO** in the **SAML Settings** tab:

Be sure to **Save** your changes if you aren't ready to upload your certificate yet.

Step 3: Upload the IdP certificate to KnowledgeOwl

The IdP should also provide a public certificate. You will need to download the certificate and then upload it into KnowledgeOwl.

KnowledgeOwl expects a file formatted as .crt. If you are using Okta or another provider which saves the certificate as a .cert file, you'll need to resave it as .crt.

Once you have your certificate in .crt format:

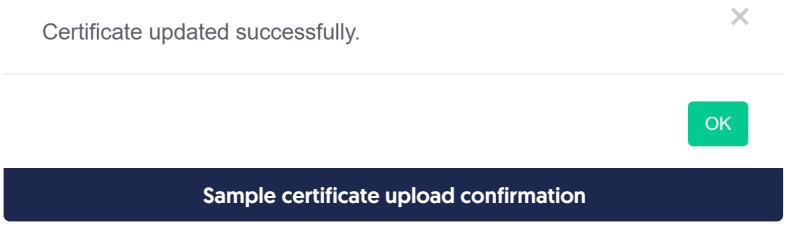
1. Go to **Settings > SSO**.

2. Be sure you're in the **SAML Settings** tab.

3. Select the **Upload certificate** option in the **IdP Certificate** section, which is located just under the IdP URL fields:

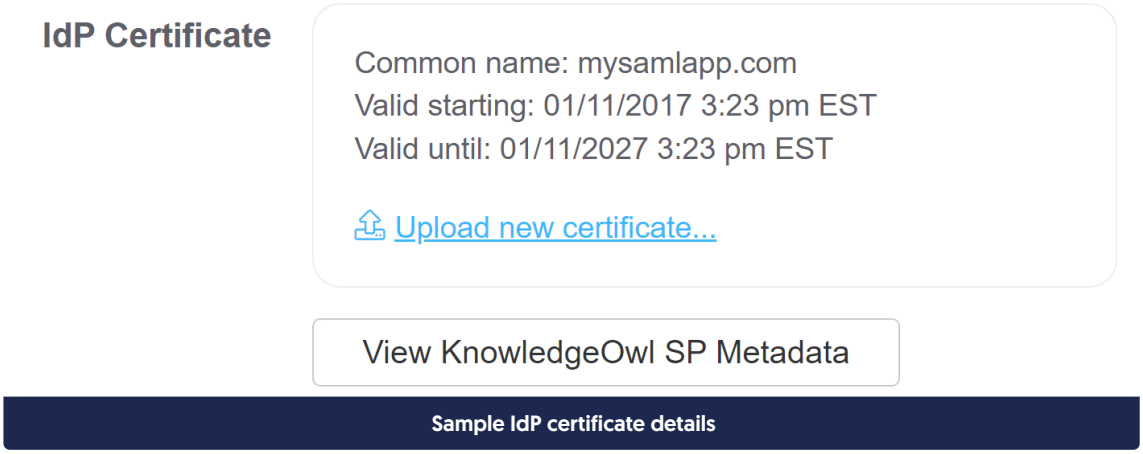
Select the Upload certificate option

4. The link will open a file browsing window where you can select the .crt file to upload. Once you upload, a pop-up will appear to confirm if the certificate was updated successfully:



Sample certificate upload confirmation

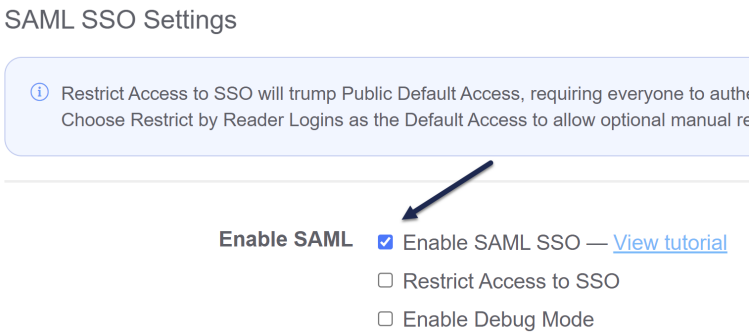
5. **Once you select OK to close that pop-up, the IdP Certificate section should update to display the certificate's details. For example:**



Sample IdP certificate details

Step 4: Enable SAML SSO

Once you have entered the three 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.



Step 5: Add the KnowledgeOwl x509 certificate to your IdP

If your IdP requires it, you can access the x509 certificate in KnowledgeOwl:

1. **Go to Settings > SSO.**
2. **In the SAML Settings tab, select the View KnowledgeOwl SP Metadata button. 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.

3. This will open a pop-up with your x509 certificate information in it.

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

5. Then copy the text and paste where necessary (you may need to put in a text editor to save this as a .crt file, an .xml file, or some other format--check your IdP's requirements).

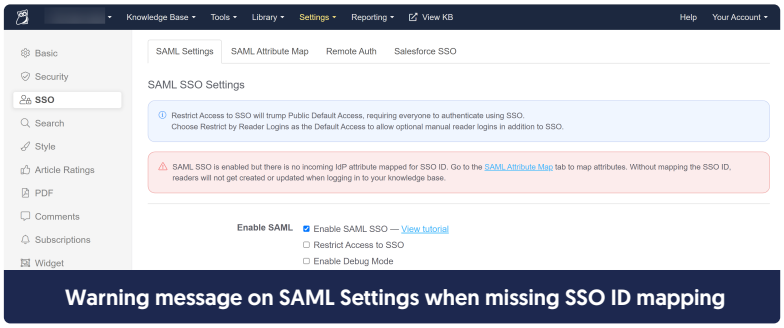
Step 6: Map SAML attributes to fields in KnowledgeOwl

Now that the IdP URLs have been added to your knowledge base settings and vice versa with the SP URLs into your IdP, you will need to configure your IdP to pass over identifying information about the readers logging in so that we can create / update them within your KnowledgeOwl account.

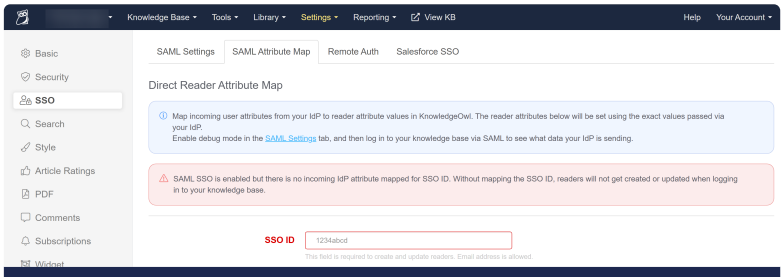
These mappings are configured in **Settings > SSO** in the **SAML Attribute Map** tab.

The minimum required information needed to successfully log a reader in through SAML SSO is a unique ID (SSO ID) and an email address. The reader's email address can be used as both the SSO ID and their email address if this is preferred.

If you don't have a mapping set up for the SSO ID, you'll see warnings in **Setting > SSO** in the **SAML Settings** tab and the **SAML Attribute Map** tab:



Warning message on SAML Settings when missing SSO ID mapping



Warning message on SAML Attribute Map when missing SSO ID mapping

In the IdP, there should be a mechanism to add outgoing attributes where you can choose a name and select the appropriate field from the IdP's database.

Add the reader's email and any other information you would like to the outgoing attributes. Choose names that make sense for these attributes, such as "email", "firstName", and so on.

1. In KnowledgeOwl, go to **Settings > SSO**.
2. Select the **SAML Attribute Map** tab.
3. Paste the names of the outgoing IdP attributes that correspond to the KnowledgeOwl reader attributes in the Direct Reader Attribute Map section.
    - 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.
4. Once you're done adding attribute mappings, **Save**.

If everything has been done correctly up to this point, you should be able to open a new incognito or private browser window and log into your knowledge base by accessing the **SP Login URL**.

Step 7: Optional settings

With your 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 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.

Troubleshooting

If you try to open the **SP Login URL** and the resulting page does not resolve, make sure that the **IdP Login URL** is correct, that it is using HTTPS, and that you can resolve the page by going to the IdP login URL directly.

If you are able to successfully log into your IdP but you get redirected to the "No Access" page with your knowledge base:

1. Go to **Settings > SSO**.
2. Check the box next to **Enable Debug Mode** near the top of the SAML Settings tab
3. **Save** those settings.
4. Now open the **SP Login URL** again.
    - If you see an error on the resulting debug page after logging in:
        - You may have an issue with the IdP certificate you uploaded, or
        - Your IdP may require one of the Advanced Options to be enabled in the **SAML Settings** tab.

- If you don't see an error on the debug page after logging in:
  - Make sure that the IdP attribute names listed on the debug page match the values listed when you click on the **SAML Attribute Map** tab.
  - Make sure that the SSO ID and Username / Email fields have values entered in the **SAML Attribute Map** tab.

5. Once you're done troubleshooting, be sure to uncheck the **Enable Debug Mode** box and **Save** the SAML Settings.
6. If you're still having trouble after trying all of the above steps, contact our support team and we will try to help figure out what the issue is.