Configure SAML SSO (generic instructions)

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

Below are instructions for setting up SAML SSO using a generic identity provider. This feature is available on select plans. We have specific instructions for our most popular identity providers:

- ADFS
- G Suite (Google Apps)
- Microsoft Entra ID
- Okta

If your identity provider supports OpenID Connect (OIDC), you can use that instead. Refer to Configure OpenID Connect SSO.

You'll do all of the KnowledgeOwl steps in the SAML setup. To open it, go to **Security and access > Access & SSO**. In the **Login methods** card, select **Set up** or **Manage** next to **SAML**. The SAML setup has five numbered steps, which match the KnowledgeOwl parts of the steps below. Select a step to expand it.

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.

- SP Entity ID
- SP Login URL: sometimes referred to as a "sign on URL" or ACS URL
- SP Logout URL: not all systems ask for this
- 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`.

To get the information for the SP Entity ID, SP Login URL, and SP Logout URL from KnowledgeOwl:

1. In the SAML setup, expand step 1, **Give these details to your identity provider.**
2. Select **Copy** next to each field you need (**SP entity ID, SP login (ACS) URL, SP logout URL**) and enter it in your IdP.



3. If your IdP can import SP metadata, or requires the KnowledgeOwl x509 certificate, select **Download metadata** to save the metadata as `knowledgeowl-sp-metadata.xml`. Or select **View metadata** to open the

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

KnowledgeOwl metadata modal, then select **Copy to clipboard** and paste it into a text editor or, if your IdP supports it, directly into a field within your IdP.

   a. Check your IdP's requirements for file format and how to upload the certificate.

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:

- IdP Entity ID
- IdP Login URL: sometimes referred to as a "sign on URL"
- IdP Logout URL: optional. It's needed to log readers out of your IdP when they log out of the knowledge base.

Add this information into the appropriate fields in KnowledgeOwl:

1. In the SAML setup, expand step 2, **Connect your identity provider**.
2. Enter the information into the **IdP entity ID**, **IdP login URL**, and **IdP logout URL** fields.



3. Select **Save changes**.

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.



Certificate file format
KnowledgeOwl accepts certificate files ending in .crt, .pem, .cer, or .der. If you are using Okta or another provider which saves the certificate as a .cert file, you'll need to rename it to .crt.

Once you have your certificate file:

1. In the SAML setup, expand step 2, **Connect your identity provider**.
2. Under **IdP certificate**, drag your certificate file into the drop zone, or select **browse** to choose it.
3. The certificate is saved as soon as you upload it, so there's no need to select **Save changes**. A message confirms "IdP certificate uploaded."
4. The **IdP certificate** section then displays the certificate's common name and the dates it's valid. Once the IdP fields and certificate are in place, the collapsed step 2 shows your IdP entity ID and the date the certificate is valid until.

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

Step 4: 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 step 3 of the SAML setup, **Map reader attributes**.



SSO ID and email address are required
To successfully log a reader in through SAML SSO, you must map 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 SAML is turned on and you don't have a mapping set up for the SSO ID, the SAML row in the **Login methods** card displays a warning: "No SSO ID mapped, so readers won't be created".

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 the SAML setup, expand step 3, **Map reader attributes**.
2. *Optional:* If your IdP is listed under **Identity provider**, select it and select its fill-in button to fill in the attribute names it usually sends. Check them against your IdP.
3. Paste the names of the outgoing IdP attributes into the **IdP attribute** column next to the matching **Reader field**. Refer to SAML attribute map for more details.
    - If you cannot directly map an IdP attribute to a KnowledgeOwl reader attribute, use Custom attribute map rules to do some mappings or logic for you.
4. Once you're done adding attribute mappings, select **Save changes**.

Step 5: Test your login

Use debug mode to check what your IdP sends:

1. In the SAML setup, expand step 4, **Test login**.
2. Check **Debug mode** and select **Save changes**.
3. Open a new incognito or private browser window and log in to your knowledge base by opening the **SP login (ACS) URL**. The login goes ahead as normal, and the attributes your IdP sent are kept for five minutes.

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

4. Back in step 4, select **Load last login attempt** to see the attributes your IdP sent. If any reader fields are wrong or missing, fix them in step 3: select the arrow at the right end of a field to pick from the attributes your IdP sent. Each one shows its value from that login. Then select **Save changes**.

5. When everything looks right, uncheck **Debug mode** and select **Save changes**.

Step 6: Turn on SAML

Once your login works, turn on SAML for your readers:

1. In the SAML setup, expand step 5, **Turn on SAML**.

2. Choose how readers can use SAML:

    - **Available**: Readers can log in with the login link or from your identity provider. Restricted content on a public knowledge base can send them here too.

    - **Required for all readers**: Anyone who isn't logged in is sent straight to SAML. This makes SAML SSO the main access method for your knowledge base. Other login methods set to **Available** still work through their login links. Refer to SSO options for different knowledge base setups for more information.

3. *Optional:* Copy the **Login link**. It sends readers straight to your IdP. Share it or add it to your site so readers can choose SAML alongside your other login methods.

4. Select **Save changes**.

Step 7: Optional settings

With your SAML SSO login working, you can now review a few additional options:

- If you'd like to use the SAML SSO as your primary reader authentication mechanism without requiring it, go back 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.
- To log readers out of your IdP when they log out of the knowledge base, check **Also log readers out of the IdP when they log out** in step 5, **Turn on SAML**. This needs an **IdP logout URL** in step 2.
- If you'd like to use SAML SSO for your authors, refer to Set up SAML SSO for authors.

Troubleshooting

If you try to open the **SP login (ACS) 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 your knowledge base **No Access** page:

1. In the SAML setup, expand step 4, **Test login**.

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

2. Check **Debug mode**.
3. Select **Save changes**.
4. Now open the **SP login (ACS) URL** again and log in.
5. Back in step 4, select **Load last login attempt**.
    - If you see "Login failed" with an error, or "No attributes were read, because the response was rejected first":
        - You may have an issue with the IdP certificate you uploaded, or
        - Your IdP may require one of the Advanced Options to be enabled.
    - If you see the attributes your IdP sent:
        - Make sure that the IdP attribute names listed match the values in step 3, **Map reader attributes**.
        - Make sure that the SSO ID and Username / email fields have values entered in step 3.
    - If you see "No login attempt in the last 5 minutes.", log in again and select **Load last login attempt** sooner.
6. Once you're done troubleshooting, be sure to uncheck **Debug mode** and select **Save changes**.
7. 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.

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