Configure SAML SSO with Okta

Last Modified on 06/17/2026 5:08 pm EDT

This tutorial will walk you through setting up an SSO SAML 2.0 Okta app integration with KnowledgeOwl. This feature is available on select plans.

Always defer to Okta instructions
If you have questions on setting up your Okta app, refer to Okta's Application Integration Wizard SAML field reference documentation, as it's more comprehensive than the steps below.

Step 1: Create your Okta SAML 2.0 app

To begin, create a SAML 2.0 app in Okta:

1. Sign in to the Okta Admin Console.
2. Go to **Applications > Applications**.
3. Select **Create App Integration**. The **Create a new app integration** modal opens.
4. Select **SAML 2.0** as the **Sign-in method**. The **Create SAML Integration** page opens to the **General Settings** tab.
5. Enter an **App name**. This app name will be displayed at the top of the knowledge base's login page when a user isn't logged in, so you may want to use the name of your knowledge base.
6. Add your knowledge base logo, if desired. This logo is also displayed on the Okta login page for your knowledge base. Here's where the logo and name show up on the login page by default:

   Sample Okta login. App logo and name display at the top with the "Connecting to [logo] Sign in with your account to access [App name]" text

   If you're feeling very KnowledgeOwl festive, you're welcome to use this version of Linus:

7. Select **Next**. The app's **Configure SAML** tab loads and you can move on to Step 2.

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

Step 2: Add the KnowledgeOwl SP info to your Okta app

Now that your Okta app exists, add the KnowledgeOwl Service Provider (SP) information into it. Keep your Okta app open to the **Configure SAML** tab. Then:

1. In KnowledgeOwl, go to **Security and access > Single sign-on**. The **SAML settings** tab loads.
2. From the **Service provider metadata** section, copy the **SP login URL**.
3. Paste this into your Okta app as the **Single sign-on URL**. Leave the box to **Use this for Recipient URL and Destination URL** checked.
4. In KnowledgeOwl, copy the **SP entity ID**.
5. Paste this into your Okta app as the **Audience URI (SP Entity ID)**.
6. Leave the **Default RelayState** blank.
7. Leave **Name ID format** as **Unspecified**.
8. Set the **Application username** to **Email**.
9. Leave **Update application username on** set to **Create and update**. So your completed screen should look something like this:

10. Select **Next**. The **Feedback** tab opens. No actions are required on this page, though if you feel thorough, copy the URL for this page and add it to the **Did you find SAML docs for this app?** textbox.
11. Select **Finish**. The page updates to display the **General** tab of your application details.
12. If you named your app after your knowledge base, **Edit** the **App Settings** to add **Application notes for admins** to note that this app is `For KnowledgeOwl SAML for [knowledge base name]`. **Future Okta admins will thank you.**

You can now continue with Step 3: Add your Okta IdP details into KnowledgeOwl.

If you have questions on setting any of the Okta app fields, refer to Okta's Application Integration Wizard SAML field reference documentation.

Step 3: Add your Okta IdP details into KnowledgeOwl

Now that the KnowledgeOwl info is in Okta, we need to add the Okta details into KnowledgeOwl.

For this step, in KnowledgeOwl in **Security and access > Single sign-on > SAML settings**, go to the **Identity provider metadata** section:

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

Sample initial Identity provider metadata section

From your Okta application details:

1. Open the **Sign On** tab.
2. In the SAML 2.0 card, select **More details**.
3. Copy the **Sign on URL**.
4. In KnowledgeOwl, in **Security and access > Single sign-on > SAML settings > Identity provider metadata**, paste the Sign on URL you copied into the **IdP login URL**.
5. Copy the Okta **Sign out URL** and paste it into KnowledgeOwl as the **IdP logout URL**.
6. Copy the Okta **Issuer** and paste it into KnowledgeOwl as the **IdP entityID**.

Sample **More details** section in Okta**Sign On** tab

7. In Okta, **Download** the **Signing Certificate**.
8. Find the certificate in your downloads and use your preferred method to change the file extension from .cert to .crt. (in many cases, if you show the file extension in the name, renaming it from .cert to .crt works).
9. In KnowledgeOwl, still in the **Identity provider metadata** section, select the **Upload certificate** option in the **IdP certificate** subsection, located just under the IdP URL fields:

Select **Upload certificate...** under **IdP certificate**

10. A file browsing window opens where you can select the .crt file to upload. Once you upload, a modal confirms if the certificate was updated successfully.
11. Once you select **OK** to close that modal, the **IdP certificate** section displays the certificate's details. For example:

Sample Okta Identity provider metadata configuration, including certificate

Proceed with Step 4: Enable SAML SSO in KnowledgeOwl.

Step 4: Enable SAML SSO in KnowledgeOwl

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

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

1. Go to **Security and access > Single sign-on**.
2. Be sure you're in the **SAML Settings** tab.
3. In the **SAML settings** section, select **Enable SAML SSO reader logins**.

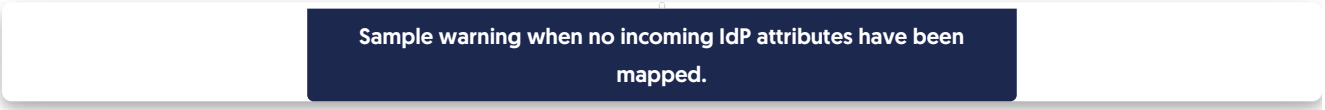
Select Enable SAML SSO reader logins

4. Be sure to **Save** your changes.

SAML won't work yet since we have no SAML attribute maps, but this leaves us perfectly positioned to test it once we do!

If you don't have a mapping set up for the SSO ID, a warning displays above the tabs of **Security and access > Single sign-on** warning you that:

> 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.



Sample warning when no incoming IdP attributes have been mapped.

In steps 5 and 6, we'll do the work to remove this warning and finish SAML SSO configuration.

Step 5: Select Okta attributes to pass to KnowledgeOwl

Select which attributes you want to pass from Okta over to KnowledgeOwl:

1. In Okta, go to your application detail's **Sign On** tab.
2. In the **Attribute statements** section, select **Add expression**. The **Add expression** modal opens.
3. Enter a **Name** for your expression, like `email`.
4. Enter an expression for your attribute, like `user.profile.email`.
5. Be sure to **Save** your changes.

Refer to your Okta Admin Console **Directory > Profile Editor > User** to view a list of all user attributes and how to reference them.

For a standard Okta setup, we recommend passing along these attributes or their equivalent as a minimum:

Name	Expression

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

Name	Expression
email	user.profile.email
firstName	user.profile.firstName
lastName	user.profile.lastName

You may want to pass along additional attributes if you're using reader signup custom fields. Refer to Add custom fields to the reader signup form for more information on using custom fields.

Step 6: Map Okta SAML attributes to fields in KnowledgeOwl

Now that you've made these user profile attributes available to your Okta KnowledgeOwl SAML app, map these attributes to the correct fields in KnowledgeOwl:

1. In KnowledgeOwl, go to **Security and access > Single sign-on**.
2. Open the **SAML attribute map** tab.
3. Map the fields in your Okta attribute list to the corresponding fields in KnowledgeOwl using the exact same names you used in Okta. For example, if you used the default setup above, enter `email` for both **SSO ID** and **Username / email**, `firstName` for **First name**, and `lastName` for **Last name**.

   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.

   a. 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. Be sure to **Save** your changes.

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**. Once you do this, check **Account > Readers** to be sure that the reader account attributes all came through properly to the knowledge base and that different readers are coming in under different accounts.

If you run into any issues, refer to the Troubleshooting section below.

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

Step 7: Optional settings

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

1. To make it so that SAML SSO is the only access method for your knowledge base:
    a. Go to **Security and access > Single sign-on > SAML settings tab**.
    b. Select **Require all readers to log in via SAML SSO**.
    c. **Save**.
    This overrides the **Content authentication** selection in **Security and access > Security settings**.

2. If you'd like to use the SAML SSO as your only or primary reader authentication mechanism:
    a. Go to **Security and access > Security settings**.
    b. In the **Unauthenticated access behavior** subsection, select **Redirect them to your SAML login URL**.
    c. **Save**.
    This sets your SAML login URL as the URL all unauthenticated readers will be directed to.

Refer to SSO options for different knowledge base setups for more information.

Troubleshooting

If you try to open the **SP Login URL** and the page doesn't load, make sure that the **IdP Login URL** is correct, that it uses HTTPS, and that you can resolve the page by going to the IdP login URL directly.

For all other issues, including if you can successfully log into your IdP but you get redirected to your knowledge base **No Access** page:

1. Go to **Security and access > Single sign-on**.
2. In the **SAML settings** tab, in the **SAML settings** section, select **Enable debug mode to troubleshoot issues**.
3. **Save** those settings.
4. Now open the **SP Login URL** again.
    - If you receive 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 receive 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 on the **SAML Attribute Map** tab.

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

- Make sure that the **SAML Attribute Map** tab has values entered for the **SSO ID** and **Username / Email** fields. SAML SSO won't work without these entries.

5. Once you're done troubleshooting, be sure to uncheck the **Enable debug mode to troubleshoot issues** 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.

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