Okta SCIM provisioning for authors

Last Modified on 06/25/2026 1:52 pm EDT

This feature is an early access release
It's being rolled out slowly for early feedback before we release it to all customers. If you're interested in testing it out, please contact us at support@knowledgeowl.com and request to be added to our early adopter testing group.

KnowledgeOwl supports two forms of author account management, also known as author provisioning:

1. **Manual account management or provisioning**, in which you manually create, update, and delete authors in **Account > Authors**. Refer to Author management for more information.

2. **SCIM account management or provisioning**, in which your company's Identity Provider (IdP) handles the account creation, updates, and deletions. This page details how to set up SCIM provisioning for Okta. Refer to SCIM provisioning for authors generic instructions if you want to set up SCIM provisioning for another IdP.

Only available on some plans
This feature is available on select plans.

Before you begin

Before you begin setup, you'll want to make one key decision: what login type you want authors provisioned by SCIM to use.

You can use SCIM provisioning for KnowledgeOwl authors in two different ways:

- With the **Username and password** author **login type**: : In this setup, Okta creates, updates, and deletes author accounts in KnowledgeOwl but authors have a separate KnowledgeOwl password that is still reset and managed by KnowledgeOwl admins. Authors log in through app.knowledgeowl.com.
- With the **SAML SSO** author **login type**: In this setup, Okta creates, updates, and deletes author accounts in KnowledgeOwl and also handles the username and password processing. Authors log in through your SAML SSO login URL using their Okta account password. Refer to Set up SAML SSO for authors for more information on how this login type works and Author login type for more information on the types broadly.

Refer to the SCIM overview for a more detailed breakdown of the differences between these setups and for an introduction to SCIM overall.

How to set up Okta SCIM provisioning for authors

Setting up Okta SCIM provisioning for authors is a multi-step process.

> Only authors with **Full admin rights** can create and modify SCIM settings.

Step 1: Set up reader SAML SSO

Skip if using Username and password
If you plan to use SCIM for account provisioning but want to have KnowledgeOwl-specific passwords and still have your authors log in through app.knowledgeowl.com, skip this step.

If you plan to use your Okta SCIM provisioning as part of SAML SSO and want to use SAML SSO to log your authors in, you'll first need to Configure SAML SSO with Okta for readers.

Verify that setup is working before you move on to Step 2: Turn on SCIM author provisioning.

Step 2: Turn on SCIM author provisioning

First, you must enable SCIM author provisioning in KnowledgeOwl and copy some information:

1. Go to **Account > Authors** (or **Security and access > Authors**). The Authors page opens to the **Authors** tab.
2. Select the **SCIM** tab.
3. In the **SCIM author provisioning** section, check the box to **Enable for author provisioning:**
4. **Save.** Once you save, the page updates to include all the SCIM settings you'll need to get set up.
5. In the **SCIM settings** section, select **Generate token** to generate an app bearer token for SCIM provisioning.
6. Copy this token and save it somewhere. You'll need it later in the Okta setup process.

Now that SCIM is enabled, continue with Step 3: Set up your default provisioning profile in KnowledgeOwl.

Step 3: Set up your default provisioning profile in KnowledgeOwl

Next, set up your **Default provisioning profile**. This profile is used for all new authors coming in from Okta unless you set up **Group provisioning profiles** and they match one of those profiles.

To set up your **Default provisioning profile:**

1. In the **SCIM** tab, scroll to the **Default provisioning profile** section:

2. If you want your default profile to grant any type of **Admin rights**, check the box(es) to grant the appropriate rights:
    a. **Full account admin**: Check this box to give authors with this profile the ability to manage **Billing**, **Authors**, **Readers**, **API Keys**, and so on.
    b. **Admin access to readers**: Check this box to give authors with this profile the ability to manage **Readers** but no other account admin functions. Choose whether they **Can purge readers**, too.
    c. Refer to Author permissions for a more detailed explanation of these admin rights settings.
3. Choose the **Login type** you want to use with this profile:
    a. Choose **Username and password** if you want your authors to log in through app.knowledgeowl.com using a password stored within KnowledgeOwl. This will mean authors log in with a password separate from their Okta account.
    b. Choose **SAML SSO** if you've already set up Okta reader SAML SSO and you want to use that integration to handle their login and password. Authors will log in through the **SAML KB** you select using their Okta password.
        i. Use the **SSO ID source** to choose which ID field contains the Okta ID you want to tie to.
        ii. If you used our default setup in Configure SAML SSO with Okta, use **Author email (most common)**.
    c. Refer to SCIM overview for more information about the differences between these setups.
4. Choose the **KB access** you want this profile to have:
    a. Choose the **Knowledge base** and **Role**.
    b. Editor and Writer are default roles built into all knowledge bases; refer to Default author roles for more information on what permissions each role grants.
    c. All other roles listed here are custom author roles. Refer to your **Account > Authors > Roles** to review those permissions in more detail.
    d. Repeat for any additional knowledge bases you want to grant access to.
5. Be sure to **Save** your changes.

Now that you have the basic required setup in KnowledgeOwl complete, continue with Step 4: Add the KnowledgeOwl Author Provisioning app in Okta.

Step 4: Add the KnowledgeOwl Author Provisioning app in Okta

Next, head over to Okta and add the KnowledgeOwl Author Provisioning app:

1. In Okta, go to **Applications > Applications**.
2. Select **Browse App Catalog**.
3. Search for `KnowledgeOwl Author Provisioning`.
4. Select the **KnowledgeOwl Author Provisioning with SCIM 2.0** app.
5. Select **+ Add Integration**. The app's **General Settings** tab opens:

6. If desired, edit the **Application label**.
7. Select **Done**. The app opens to the **Assignments** tab.

Now that you've added the KnowledgeOwl Author Provisioning app in Okta, continue with Step 5: Set up your Okta app's provisioning.

Step 5: Set up your Okta app's provisioning

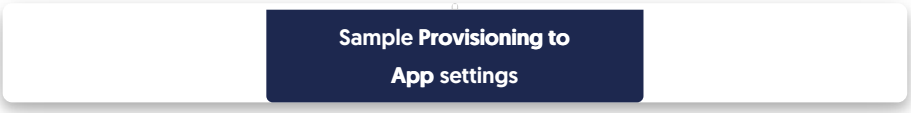
Once your Okta SCIM 2.0 app opens to the **Assignments** tab, provision the app to get it connected to your KnowledgeOwl account and set up what it can do:

1. In your Okta app, select the **Provisioning** tab.
2. Select **Configure API integration**:
3. Check the box to **Enable API integration**. Additional fields display.
4. Paste the **Bearer token** you copied from KnowledgeOwl in Step 1 into the **API Token** field.
5. Select **Test API Credentials** to verify that the bearer token works.
6. Once you have confirmation that the credentials worked, be sure to **Save** your changes.
7. The app settings are saved and you'll be automatically taken to the app's **Provisioning** settings for **To App**.
8. Select **Edit**, then use these settings:
    a. **Create Users**: Set to **Enable**. The app won't be able to create new author accounts if you don't enable this.
        i. Uncheck the **Set password when creating new users** box so it is not enabled.

b. **Update User Attributes:** Set to **Enable**.

c. **Deactivate Users:** Set to **Enable**. This will do the clean-up of removing KnowledgeOwl author accounts when their Okta account is unassigned from this app or deactivated.

d. Your settings should look like this:



9. **Save** your changes.

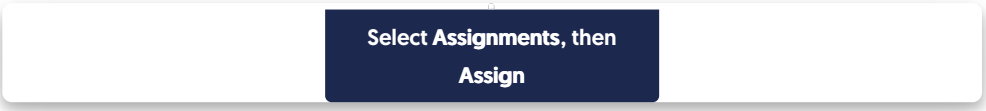
Now that you've set up your Okta app's authentication and provisioning, continue with Step 6: Assign your Okta app to users or groups.

Step 6: Assign your Okta app to users or groups

With your Okta app's provisioning set up, assign your Okta app to users or groups. These users or groups will have author accounts in KnowledgeOwl, so you may want to create a separate Okta group and just assign that group:

1. In your Okta app, select the **Assignments** tab.

2. Select **Assign**, then select the type of assignment you'd like to complete:



a. Select **Assign to People** if you want to assign individual users. Refer to Okta's Assign application to users documentation for detailed instructions.

b. Select **Assign to Groups** to assign to one or more existing groups. Refer to Okta's Assign an app integration to a group for more information.

3. Locate the user or group you wish to assign, select it, then select **Assign**.

4. Repeat for any other users or groups you wish to assign.

If you plan on having different groups of authors coming in from Okta and you want to assign them different permissions, continue with Step 7: Add Push Groups to your Okta app. If you don't need to set up different groups of authors, jump to Step 9: Test your SCIM setup.

Step 7: Add Okta Push Groups to your Okta app (optional)

If you want to assign multiple groups to your Okta app for KnowledgeOwl provisioning, you may want to handle permissions for those groups differently. For example, maybe you want to have separate groups for KnowledgeOwl admins and for KnowledgeOwl authors, granting full admin rights to the admins group and no

admin rights to the second.

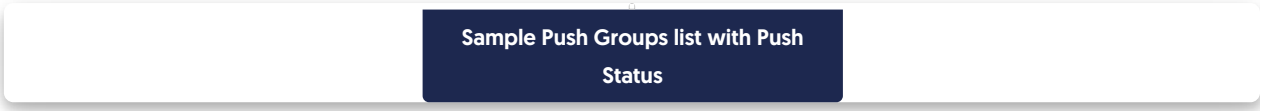
For this type of setup, add the separate Okta groups as **Push Groups** in your Okta app. Once those groups have been pushed to KnowledgeOwl, set up group provisioning profiles in KnowledgeOwl to handle their permissions. Refer to Okta's App assignments and Group Push documentation for more information on Push Groups.

To set up the Push Groups in your Okta app:

1. In your Okta app, select the **Push Groups** tab.
2. Once the tab opens, select **+ Push Groups**:

3. Use the appropriate action to find the group you want (**by name** or **by rule**).
4. Check the box to **Push group memberships immediately**:

5. Then **Save** (or, if you want to add more groups, **Save and Add Another**).
6. After you save, the Push Groups tab updates and shows a **Push Status** for the group:



Once the Okta app lists the Push Group with a **Push Status** of **Active**, the group exists in KnowledgeOwl. Continue to Step 8: Set up KnowledgeOwl group provisioning profiles.

Step 8: Set up KnowledgeOwl group provisioning profiles (optional)

Once the Okta app lists the Push Group with a **Status** of **Active**, the groups exist in KnowledgeOwl.

Set up group provisioning profiles in KnowledgeOwl so that your authors get the correct permissions:

1. In KnowledgeOwl, go to **Account > Authors** (or **Security and access > Authors**). The Authors page opens to the **Authors** tab.
2. Select the **SCIM** tab.
3. In the **Group provisioning profiles** section, look for any groups with a **Status** of **Not configured**.
4. Select the gear cog icon in that group's row:

The **Edit group** modal opens.

5. If you have multiple groups, use the **Priority** field to determine the order in which group provisioning profiles are applied. Priority of 0 is the first applied, followed by 1, 2, and so on.
    a. Authors will get the provisions in the first profile that matches.
    b. Authors who don't match any of the groups will get the **Default provisioning profile**.
6. Set up the rest of the group provisioning profile in the same way you set up the default provisioning profile.
7. Be sure to **Save** your group profile once you're done making changes.

With your group provisioning profiles set up, continue to Step 9: Test your SCIM setup.

Step 9: Test your SCIM setup

Test logging into the knowledge base as one of the assigned users or groups:

- If you used the **SAML SSO login type**, you should have received an author SAML SSO welcome email after you assigned the author to the IdP SCIM app. Open the knowledge base SAML SSO login URL in that email and test logging in with your IdP credentials. Make sure the account gets the permissions you expect.
- If you used the **Username and password** login type, you should have received an author welcome email with a temporary KnowledgeOwl password after you assigned the author to the IdP SCIM app. Open app.knowledgeowl.com and test logging in with the temp password. Make sure the account gets the permissions you expect.