SCIM provisioning for authors (generic instructions)

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. Follow the instructions on this page if you want to set up SCIM author provisioning and we don't have a provider-specific set of instructions.

Generic instructions only
This page provides instructions for setting up SCIM author provisioning using a generic identity provider. This feature is available on select plans. We have specific instructions for our most popular identity provider, Okta, and will add more for other providers based on your requests.

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, your SCIM IdP 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, your SCIM IdP 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 IdP 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 SCIM provisioning for authors

Setting up SCIM provisioning for authors is a multi-step process, but it generally includes 5-6 steps, outlined below.

> 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 SCIM IdP as part of SAML SSO and want to use SAML SSO to log your authors in, you'll first need to Set up SAML SSO for readers.

Verify that setup is working before you continue.

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, copy the **SCIM base URL** and save it somewhere. You'll need it later in the setup process.
6. Select **Generate token** to generate an app bearer token for SCIM provisioning.
7. Copy this token and save it somewhere. You'll need it later in the setup process.

Step 3: Set up your default provisioning profile in KnowledgeOwl

With SCIM enabled, set up your **Default provisioning profile.** This profile is used for all new authors coming in from your IdP 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 the profile the ability to manage Billing, Authors, Readers, API Keys, and so on.
    b. **Admin access to readers**: Check this box to give the 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 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 login with a password separate from their IdP account.
    b. Choose **SAML SSO** if you've already set up 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 IdP password.
    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.
5. Be sure to **Save** your changes.

Step 4: Create a SCIM provisioning app in your IdP

Next, go to your IdP and create a SCIM provisioning app. Most IdPs have this as an app type option. Follow instructions provided by your IdP to set up the SCIM provisioning app.

As you create your app, you'll need to use these settings:

1. KnowledgeOwl SCIM uses a **bearer token** authorization type. Enter the **bearer token** you generated and copied in Step 2 as the API key or bearer token.
2. Enter the **SCIM base URL** you copied in Step 2 as the API **endpoint URL**, or whatever your IdP app calls this

field.

3. Some IdPs will require you to **map attributes** from your IdP to KnowledgeOwl fields. Match what you did with your reader SAML SSO setup.

4. Set which **actions** the auto-provisioning SCIM app can do. These settings go by different names in different apps; here are the broad permission categories you should look for:
    a. Create new users
    b. Update existing users
    c. Deprovision users unassigned from the app
    d. Delete or deprovision deactivated or deleted users
    e. Some IdPs also have a day or time selector for deprovisioning (for example: wait 7 days after deactivation before deprovisioning)
    f. Add or assign push groups

5. **Assign** specific users or groups to the provisioning app. This may include selecting or setting **push groups**.

At this point, you can either set up group provisioning profiles if you want to use them, or jump straight to testing your SCIM setup.

Step 5: Set up your group provisioning profile in KnowledgeOwl (optional)

If your IdP supports push groups and you're using them, once your IdP pushes those groups to KnowledgeOwl, the groups will appear in the **Group provisioning profiles** section.

Configure the profile for each group:

1. In the **SCIM** tab, in the **Group provisioning profiles** section, look for any groups with a **Status** of **Not configured**.

2. Select the gear cog icon in that group's row:

    The **Edit group** modal opens.

3. 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. The first profile that matches is the one that will be applied to users.

4. Set up the rest of the group provisioning profile in the same way you set up the default provisioning profile.

5. Be sure to **Save** your group profile once you're done making changes.

Step 6: 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.