Convert a private knowledge base to mixed public and private

Last Modified on 01/07/2025 1:58 pm EST

After having a private knowledge base for a while, you may want to make part of that knowledge base public.

This is a good problem: you're seeing uses for the knowledge base beyond what you originally thought.

If you're in this position, here are the steps we suggest to convert your existing totally-private knowledge base to a mixed public knowledge base.

Identify your current login option(s)

Before you begin, make sure you know all the ways your readers are logging in to your knowledge base, as it impacts the next steps.

There are a few options, and some of these you can use in combination:

- **KnowledgeOwl reader accounts** (KO readers)
  To check if you're using KO readers:
  1. Go to **Security and access > Readers** (or **Account > Readers**).
  2. In the dropdown at the top of the page, select **Non-SSO Readers**.
  3. If you have more than a couple test accounts listed here, your knowledge base is using KO Readers.
  4. Refer to KO Readers below for detailed instructions.
- **SAML Single Sign-On** (SAML SSO)
  To check if you're using SAML SSO:
  1. Go to **Security and access > Single sign-on**.
  2. In the **SAML settings** tab, is the **Enable SAML SSO reader logins** box checked? If so, your knowledge base is using SAML SSO.
  3. Refer to SAML SSO or Remote Auth below for detailed instructions.
- **Salesforce Single Sign-On** (Salesforce SSO)
  To check if you're using Salesforce SSO:
  1. Go to **Security and access > Single sign-on** and open the **Salesforce SSO** tab.

2. Under **Enable Salesforce SSO**, is the box to **Allow readers to log in through your Salesforce SSO integration** checked? If so, your knowledge base is using Salesforce SSO.

Unsupported
Salesforce SSO can't be used in a mixed public/private knowledge base setup. You'll need to create a second knowledge base for your public content, either with standalone or synced content.

- **Remote authentication** (remote auth)
  To check if you're using remote auth:
  1. Go to **Security and access > Single sign-on** and open the **Remote authentication** tab.
  2. Are the **Remote login URL** and **Remote logout URL** populated? If so, you might be using Remote Auth. You can fully confirm this a few ways:
     a. Go to **Security and access > Security settings**. If **Content authentication** is set to **Remote authentication**, you're definitely using remote auth.
     b. Go to **Security and access > Security settings**. If the **Unauthenticated access behavior** is set to **Redirect them to your remote auth login URL**, you're most likely using remote auth.
     c. Check with whomever set up your knowledge base originally to see if they set up a remote auth script.
  3. Refer to SAML SSO or Remote Auth below for detailed instructions.

KO Readers

Follow these steps if your knowledge base is using KnowledgeOwl readers alone or in combination with other auth types:

1. Create a new reader group for your KO readers.
2. Use Edit readers in bulk to assign all your current KO readers to that reader group.
3. For future KO reader accounts:
   a. If all your readers are coming from the same domain (like knowledgeowl.com), use Auto-assign groups by email rules to assign future readers to this group.
   b. If your readers come from different domains, you can either:
      i. Manually assign current and future readers to the group. Edit readers in bulk is a good tool for this.
      ii. Set up one Auto-assign groups by email rules for each domain your readers are coming from.

4. Confirm that all current KO readers are assigned to the new reader group.
5. Once all KO readers are assigned to the new group, you can start restricting categories (or articles) that should only be available to logged in readers.
    a. Readers won't notice anything since you're just updating permissions on the back-end and they will continue to have access to the same content.

Pro tip: Use your content organization
It's easiest if you can organize your content by categories, as then you just need to update the top-level categories that need to be behind the login.

6. Make sure the theme has the reader login/logout button enabled. Once you make it public, your readers will need a way to log in again, since the login page won't open by default.
7. In **Security and access > Security settings** in the **Reader security options** section, if the **Image / file security** box to **Require authentication** is checked, no images or files will load for public readers. If you plan to have any files displayed in your public content, you must uncheck this box. Refer to Requiring login to view files/images for more information.
8. In **Security and access > Security settings**, update the **Content authentication** to **Public**.

Look before you leap
Once you make this change and save, any content not restricted to your reader group will be publicly available!

9. In **Security and access > Security settings**, update the **Unauthenticated access behavior** to **Redirect them to the reader login page**.
    a. UNLESS you're using KO readers and SAML SSO or Remote Auth, then you may want to use one of the other login pages as the default, or update the reader login page so that it includes a link to your other login page.
10. Be sure to **Save** your changes.
11. Immediately test to make sure everything is working. You can always switch back while troubleshooting! This is a good thing to do during a slow day/time.

SAML SSO or Remote Auth

Follow these steps if your knowledge base is using SAML SSO, Remote authentication, or both:

1. Create a new reader group for people who log in via SSO.
2. Update SSO to automatically assign all readers to the new group.
    a. If you're using SAML SSO, you can do this as a custom attribute map rule. To assign all readers to the same group, use a **Default rule**.
    b. If you're using remote authentication, the remote auth login script will need to be updated to automatically assign all readers to the group.
3. Confirm that all readers are now being given access to the new group.
4. Once all SSO readers are being assigned to the new group, you can start restricting categories (or articles) that should only be available to logged in readers.
    a. Readers won't notice anything since you're just updating permissions on the back-end and they'll continue to have access to the same content.

Pro tip: Use your content organization
It's easiest if you can organize your content by categories, as then you just need to update the top-level categories that need to be behind the login.

5. Make sure the theme has a login/logout button or link somewhere. Once you make it public, people who use SSO will need a way to log in again (it won't go there by default).
6. In **Security and access > Security settings** in the **Reader security options** section, if the **Image / file security** box to **Require authentication** is checked, no images or files will load for public readers. If you plan to have any files displayed in your public content, you must uncheck this box. Refer to Requiring login to view files/images for more information.
7. In **Security and access > Security settings**, update the **Content authentication** to **Public**.

Look before you leap
Once you make this change and save, any content not restricted to your reader group will be publicly available!

8. In **Security and access > Security settings**, update the **Unauthenticated access behavior**:
    a. If you're using SAML SSO, update it to **Redirect them to your SAML login URL.**
    b. If you're using remote auth, update it to **Redirect them to your remote auth login URL.**
    c. If you're using both SAML SSO and remote auth, you'll need to pick one of these as the default, but you may want to update that login page to include a link to the other.

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

10. Immediately test to make sure everything is working. You can always switch back while troubleshooting! This is a good thing to do during a slow day/time.