Configure your KB access

Last Modified on 07/12/2023 1:43 pm EDT

This is one of the more important sets of features to think through: who has access to your knowledge base (KB), and how should they access it? (If you did the work on Purpose & audience, you have already begun answering these questions!)

First, let's start at a high level:

- Do you want any or all of your knowledge base content to be publicly available?
- Or would you prefer some or all of it to require a login of some kind?

In **Settings** > **Security**, you can set your knowledge base's **Default Access**. This will determine whether your knowledge base has any content that is publicly available (Default Access: Public) or whether it requires a login to view any content (any of the other Default Access options).

Your knowledge base may have been created with Default Access set to Public, so if you know you want to lock it down, now is a good time to do it!

Most of our customers opt for one of three options:

1. A totally public knowledge base
2. A public knowledge base with some private content
3. A totally private knowledge base

While you can change the default access at any time, knowing the core of how you want your knowledge base arranged can help determine which features you'll need to look at, so we'll explore each configuration in more detail below.

You can always change this access at a future date. Some authors will set their knowledge base as private initially while content is being built out, and then set it to public when it's launched. This can be a great way to encourage internal review and feedback before launching to a broader community.

Public KB

If you want your knowledge base accessible by anyone, you want a public knowledge base.

By default, all new knowledge bases are created with Default Access set to public, so if this option is what you need, you don't have to make any additional configuration changes.

But since it's going to be publicly available, you will want to review our SEO guide. You can choose to generate a sitemap (or prevent Google from indexing your knowledge base), and there are good tips about how to use features or metadata fields to get the best search performance.

Public KB with some private content

Sometimes, customers want a lot of their content to be publicly viewable, but then they might have a particular category or subcategory that they want available only to specific people. This setup works well for things like:

- **Support documentation**: a public section for prospect or current customers, with a private section for your support team
- **Product documentation**: a public section for prospects, but a private section for paying customers
- **Services or portfolio documentation**: a public section for free resources, but a private section for your staff or active clients

The way this works:

- The Default Access is set to public.
- All content without any Reader Group Restrictions will be available publicly.
- Content with Reader Group Restrictions will not be visible in any way to the public.
- Individuals will log in to reader accounts (which have membership to one or more reader groups) so they can see the private content.

For this configuration, you'll want to:

1. Keep the Default Access in **Settings > Security** set to Public. (Or set it to public if it was already set to something else.)

2. Create one or more Reader groups and restrict your private content to at least one of those reader groups.

3. Decide how you want your reader accounts created:

    - **KnowledgeOwl reader accounts**: accounts are created and administered within KnowledgeOwl directly. You'll manually assign readers to reader groups as you create them, or use Auto-assign groups by email rules. See Enable reader logins for setting this up.

    - **SAML Single Sign-On (SSO) integration**: Work with your IT team to integrate with an existing SSO provider your company already has, so people use the same login process for KnowledgeOwl as other tools. In this setup, the accounts are authenticated using your authentication provider and the KnowledgeOwl reader account is created/updated using info from that provider.

        - Sample SSO providers our customers have used include: Active Directory, Azure, Okta, Google SSO, Salesforce SSO, and more. If your provider isn't listed, the SAML SSO generic instructions should help your IT team get started.

        - For this mix of public and private, see more detailed configuration guidance in SSO options for different knowledge base setups.

- **Remote authentication**: Similar to SSO, use an existing authentication process to log people into KnowledgeOwl. Appropriate if you have a non-SAML SSO solution.

- For SSO and remote authentication, you'll want to talk to your IT team about passing over reader groups or setting up rules to assign reader groups in KnowledgeOwl to ensure your readers will be able to see the appropriate content.

Private KB

Some knowledge bases should never be publicly available in any way. If you're using your knowledge base for internal company documentation, or it contains proprietary information, this is a good setup.

For this configuration, you have two main options:

- Using reader logins (either KnowledgeOwl reader accounts or reader accounts created through a variety of integrations)
- Using a shared IP, password, or combination

Each is explained in more detail below, but the gist is that you set the Default Access to any option other than Public, and then configure it appropriately.

Restrict by reader logins

With this setup, anyone accessing your knowledge base must have an individual reader account. You can require a login to view any/all content, or you can further segregate content by creating reader groups, restricting content to specific reader groups and assigning those groups only to specific readers.

Pros:

- Individual readers can belong to different reader groups, which allows you to control what content they see.
- You can remove individual readers from your knowledge base when they leave your organization.
- You don't have to worry about everyone sharing a single account or password.
- You can integrate with an authentication method your employees or customers are already using.
- You can use KnowledgeOwl-only reader accounts, which you can set up and administer yourself without needing any IT expertise.

Cons:

- Individual accounts can cause more administrative overhead (creating, resetting passwords, updating reader group membership)
- To integrate with an existing authentication method, you'll need help from your IT team to get things set up properly

Full configuration steps for each of these options are pretty detailed; rather than try to cover them all here, you can visit the links below for more details:

- **KnowledgeOwl reader accounts**: accounts are created and administered within KnowledgeOwl directly. You'll manually assign readers to reader groups as you create them, or use Auto-assign groups by email rules. See Enable reader logins for setting this up.

- **SAML Single Sign-On (SSO) integration**: Work with your IT team to integrate with an existing SSO provider your company already has, so people use the same login process for KnowledgeOwl as other tools. In this setup, the accounts are authenticated using your authentication provider and the KnowledgeOwl reader account is created/updated using info from that provider.
    - Sample SSO providers our customers have used include: Active Directory, Azure, Okta, Google SSO, Salesforce SSO, and more. If your provider isn't listed, the SAML SSO generic instructions should help your IT team get started.
- **Remote authentication**: Similar to SSO (but not using SAML), use an existing authentication process to log people into KnowledgeOwl.
- A combination of KO reader accounts and SSO. See the links above for information on KO readers and SSO, and see SSO options for different knowledge base setups on a few extra details for this exact setup.

Restrict by IP address or shared password

We generally see this option used when you want to make your entire knowledge base available to a group of people, without segregating content in any way, and you don't ever have to worry about removing someone's access. (For example: if someone leaves your organization, they no longer have access to the VPN, and therefore don't meet an IP address requirement.) Some of our customers who create one knowledge base per customer use this option for their individual customer's knowledge bases, too.

Pros:

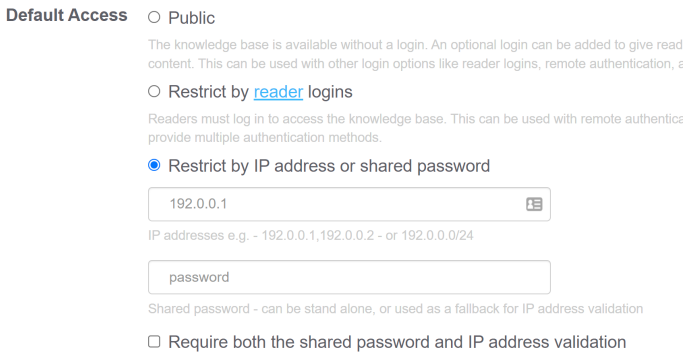
- You can set this once and forget it
- You don't have to administer individual reader accounts, or deal with password resets, etc.
- You don't generally need anyone from your IT department to help you

Cons:

- There's no way to segregate content via reader groups--everyone has access to everything
- Aside from the IP address or shared password, you have no way to remove someone's access (so, for example, if the password is compromised, you have to reset the password and then communicate to everyone what the new password is)

To set this option:

1. Go to **Settings > Security**.
2. Select the option next to **Restrict by IP address or shared password**.



3. Add whichever fields are appropriate (IP address or password). If you'd like to require both, check the box to "Require both the shared password and IP address validation". See notes below for more details on each.

4. **Save** your changes.

There are four basic options here:

1. **IP address** - add an IP address or range to the IP addresses field
   This setting is great for internal office knowledge bases. If you can track down the IP addresses that your office uses, you can paste the comma separated list into the box and ensure that no one trying to access your knowledge base from outside of your office can get in.

   
   You can also use the /24 subnet mask for a range of IP addresses; at this time, we only support the /24 subnet mask.

2. **Restrict by shared password** - add a password to the Shared password field
   This one is great if you need to restrict access to your knowledge base but you aren't sure of your office's IP addresses or if your readers are going to be spread out. Creating a single password that you can give to everyone will allow you to control who gets in but will allow for more flexibility.

3. **IP-based Restriction OR Shared Password** - enter both an IP address and a shared password, but leave "Require both the shared password and IP address validation" unchecked
   This means that someone either needs to be accessing the knowledge base from an approved IP address or they will need to enter the shared password. So, for example, while someone is in your office, on an approved IP address, they won't have to worry about logging in because they are accessing the knowledge base from an approved IP address. If they work from home one day and have a different IP, they will be asked for the shared password to log in.

4. **IP-based Restriction AND Shared Password** - enter both an IP address and a shared password and check the box for "Require both the shared password and IP address validation"
   This basically enforces a two-factor authentication: someone must be on an approved IP address AND enter that shared password.