Create a private knowledge base

Last modified on 11/07/2026 12:01 pm EST

You can choose to make your knowledge completely private, meaning that no one will be able to access it without some type of login, password, or shared IP.



Best use cases
Internal documentation of any kind: Employee handbooks, Support/troubleshooting team info, HR policies, Marketing resources, Multi-department knowledge bases



Worst use cases
Any type of documentation you'd want to share publicly

You can make your knowledge base private by choosing one of our available security options. Most of them are in **Security and access > Access & SSO**, under **Who can read this knowledge base?**:

- **Logged-in readers only**
  Readers will be required to log in with a username and password created and maintained within KnowledgeOwl. Authors with full account admin access can set up readers, reader groups, and reader settings under **Security and access > Readers**. Learn more in our Reader Management guide. Configure this in **Security and access > Access & SSO**.
- **Allowed IP addresses or a shared password**
  Readers will need to be coming from a specified IP address or enter a shared password to access the site. You can also choose to require both an approved IP address and a password to log in. Configure this in **Security and access > Access & SSO**.
- **Your own login system (remote authentication)**
  Readers will be required to log in through a 3rd party site, such as your own website or application. You can use this option to automatically log in readers from your software. You'll need to configure remote authentication first: in **Security and access > Access & SSO**, under **Login methods**, select **Set up** next to **Remote authentication**.
- **SAML SSO (single sign-on)**
  Readers will be required to log in through your specified identity provider, such as ADFS, Okta, Microsoft Entra ID, or Google Workspace. Set up SAML in **Security and access > Access & SSO** by selecting **Set up** next to **SAML**, then set it to **Required for all readers**. Refer to Single sign-on (SSO) for more information.
- **OpenID Connect SSO (single sign-on)**
  Readers will be required to log in through an OpenID Connect identity provider, such as ClassLink, Clever, Microsoft Entra ID, Google Workspace, or Okta. Set up OpenID Connect in **Security and access > Access & SSO** by selecting **Set up** next to **OpenID Connect (OIDC)**, then set it to **Required for all readers**. Refer to OpenID Connect (OIDC) SSO overview for more information.

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

- **Salesforce SSO (single sign-on)**
  Readers will only be able to log in through your Salesforce account. Set up Salesforce SSO in **Security and access > Access & SSO** by selecting **Set up** next to **Salesforce SSO**, then check the box to **Require readers who aren't logged in to log in through Salesforce**. See our Salesforce SSO Configuration guide.

When SAML, OpenID Connect, or Salesforce SSO is required, the **Who can read this knowledge base?** section shows which method readers who aren't logged in are sent to, instead of the list of options. Refer to Access & SSO page overview for more on how these settings work together.

Additional considerations

By default, all files stored in KnowledgeOwl can be publicly accessed by their URL. For fully private knowledge bases, you may want to lock this down so the files also require logging in to be viewed. Refer to Require login to view files/images for instructions on restricting your files.

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