

Reader password security

Last Modified on 09/24/2025 5:12 pm EDT

If you're using reader accounts in any of your knowledge bases, you'll need to set up your **Reader Password Security**. This helps to determine:

- Whether readers will administer their own passwords or if one of your admins will manage them
- How many failed password attempts are allowed
- Whether [authors](#) can log in as readers
- If readers can only access your knowledge base from a specific list of IP addresses

These settings are account-wide across all of your knowledge bases, though you have some options to override them in individual knowledge bases.

To review and set up these settings:

1. Go to **Account > Readers**. The Readers page opens to the Readers tab.
2. Open the **Settings** tab.
3. Use the **Reader Password Security** section to adjust any settings you need. Options include:
 - a. **Password Management:** Choose whether you want your knowledge base admins to manage reader passwords or have readers manage their own. Self-administered passwords are the default password management option. We recommend self-administered passwords because few people have time to deal with forgotten password issues. This is an account-wide setting but can be overwritten on individual knowledge bases for accounts with multiple knowledge bases under **Security and access > Security settings**. Refer to [What's the difference between admin managed and self-administered reader passwords?](#) for more information.



Related settings

If you're using self-administered passwords, you'll also want to review the [Self-Administered Reader Options](#), the [Reader Welcome Email](#), and the [Reader Password Reset](#) email settings.

- b. **Password Attempts:** By default, reader accounts are locked for 20 minutes following 3 unsuccessful attempts. If you'd like to allow unlimited password attempts, check the box to **Allow unlimited password attempts**.
- c. **Author Logins:** Choose whether to allow KnowledgeOwl authors to log in as readers (recommended, on by default).

- d. **Restricted IP Protection:** If your readers should all be on a VPN or on a specific range of IP addresses, add a comma-separated list of IP addresses here to enforce that restriction in addition to the **Default access options** in **Security and access > Security settings**.
- e. **Case insensitive Logins:** If using admin managed passwords, choose whether or not you want the usernames to be case-sensitive.

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