Reader password security

Last Modified on 01/31/2024 4:27 pm EST

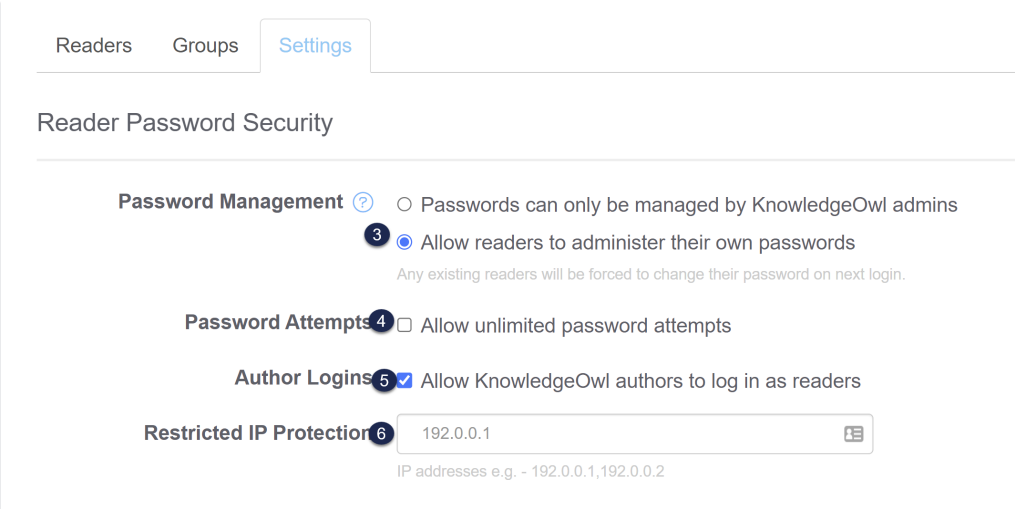
If you're using reader accounts in any of your knowledge bases, you'll need to set up your Reader Password Security. This helps to determine:

- 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 must be accessing 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. Click on your **profile icon/name** in the upper right.
2. Select **Readers** from the dropdown to access the Readers area of your account.
3. Open the **Settings** tab.
4. The Reader Password Security section will display at the top:



Reader Password Security in Your Account > Readers > Settings

5. **Password Management:** Choose whether you want to manage reader passwords or have them 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 **Settings > Security.** See What's the difference between admin managed and self-administered reader passwords? for more information.

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.

6. **Password Attempts:** Choose whether or not you want to allow unlimited password attempts. By default, reader accounts are locked for 20 minutes following 3 unsuccessful attempts.
7. **Author Logins:** Choose whether to allow KnowledgeOwl authors to log in as readers (recommended; on by default).
8. **Restricted IP Protection:** Optionally restrict reader logins to a specific IP address or list of IPs as a form of two-factor authentication (password AND IP address).
9. **Case insensitive Logins:** If using admin managed passwords, choose whether or not you want the usernames to be case-sensitive.
10. Click the **Save** button at the bottom of the screen to save your changes.