Comment spam protection and security

Last Modified on 04/02/2025 2:57 pm EDT

Comments have some built-in security measures to prevent issues such as spam, abusive comments, or private information from being posted for all to see:

- **All comments require approval** before they're displayed publicly, unless you override this setting to auto-approve and display them. This lets you review comments for appropriateness and decide whether to approve or delete them.
- **Public commenters must pass your spam protection to submit a comment.** Keep reading for more information.

Comments spam protection

Spam is mostly a concern with comments on public knowledge bases, those that don't require login to view content.

To combat spam, if you have the **Restrict commenters** box to **Only allow logged in readers and authors to leave comments** unchecked, we apply your knowledge base's **Spam protection** method to the comments form.

Public readers on knowledge bases using honeypot won't see anything different.

Logged-in readers and authors won't ever have to pass honeypot logic or a reCAPTCHA test.

Public readers on knowledge bases using reCAPTCHA will need to check an "I'm not a robot" box to submit their comment:

> A public reader is prompted for their name and email. If reCAPTCHA spam protection is used, they'll also have to pass the I'm not a robot test.

If you're using reCAPTCHA with a private domain, you must upload your own reCAPTCHA V2 key and secret to properly prevent spam comment submissions. Refer to **Add reCAPTCHA** for more detailed instructions.