02. Configuration

- Authentik Security

Authentik Security

For optimum security you can create Captchas at Authentik’s public enrollment flow, since that’s where people create the shared account. Authentik supports CAPTCHA—including hCaptcha and Cloudflare Turnstile—in flows. goauthentik.io

1. In Authentik, create a CAPTCHA stage and configure it with your provider’s site/public key and secret/private key. For Turnstile, use its documented script and verification URLs; for hCaptcha, use its corresponding URLs. goauthentik.io
2. Edit the Enrollment flow used for sign-up and add the CAPTCHA stage before the stage that writes/creates the user.
3. Add email verification to that flow too, so sign-ups must prove access to the address they provide. Authentik enrollment flows can include both CAPTCHA and email verification stages. goauthentik.io
4. Add rate limiting at the reverse proxy in front of Authentik’s enrollment flow as well. CAPTCHA can deter automated sign-ups, while rate limiting slows repeated attempts; neither alone stops a botnet using many IP addresses.
5. Keep newly enrolled users out of the ten BookStack applications by default, or give them only low permissions. Grant access through Authentik groups or policies rather than automatically allowing every registrant into every wiki.

Test registration from a private browser window after changing the flow, including that failed CAPTCHA and unverified email submissions don’t create usable accounts.