

Accountability: Making Every Action Traceable

Fri, Aug 7, 9:00 AM EDT · <https://scottslab.io/posts/accountability-and-session-management>

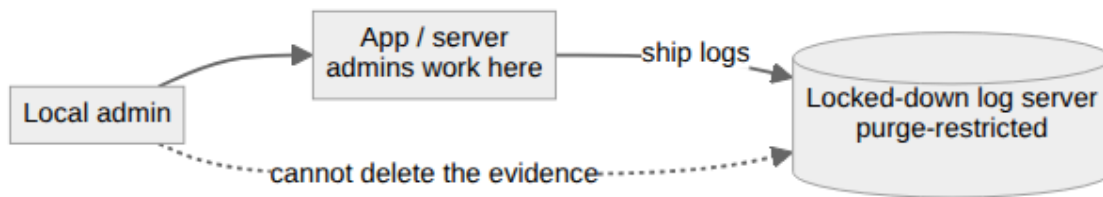


TL;DR

Accountability means every action ties back to one real person, and it collapses the moment you allow shared accounts: everyone can blame everyone. It rests on unique identification plus strong authentication, logs shipped to a separate locked-down server the local admins can't purge, and session controls (idle timeouts, re-auth for sensitive actions, lock screens) so an abandoned session can't be inherited.

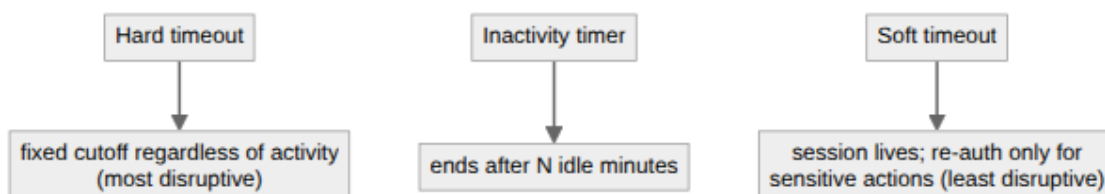
Accountability is the quiet fourth 'A', the one that only matters after something has already gone wrong, and it has a single requirement: every action has to trace back to exactly one human. The instant that chain breaks, your logs stop being evidence and become an argument. And the classic way it breaks isn't a hacker. It's a shared "ops" login three people use, so when something destructive happens at 2am, each of them can point at the other two. Plausible deniability is the enemy here, and shared accounts manufacture it for free.

So accountability stands on the two steps before it: unique identification (real per-person usernames, never a generic account) and authentication strong enough that a logged action really was that person. Without both, "the logs say Scott did it" means nothing; maybe it was whoever knew Scott's reused password.



Then there's a subtler failure: who can edit the evidence. If the logs live on the same box as the activity, an admin who does something they shouldn't can also delete the record of it: the fox auditing the henhouse. That's why logs get shipped off to a separate, locked-down log server whose database restricts purging, so even a local admin can't quietly rewrite history. Most orgs centralize logging for exactly this reason; it's not about storage, it's about tamper-resistance.

Sessions are the other place accountability leaks. An authenticated session left open is an unlocked door with your name on it. Whatever happens next is attributed to you. The blunt tool is a hard timeout: a fixed cutoff regardless of activity, like a two-hour VPN disconnect. Effective, and genuinely annoying. Gentler is an inactivity timer that ends the session after, say, ten idle minutes. Gentlest, and my favorite, is the soft timeout: the session stays alive but sensitive actions demand a fresh re-authentication, so routine work is never interrupted while the dangerous stuff stays gated.



And the smallest habit that carries the most weight: locking the screen. A screensaver lock doesn't log you out. It just requires re-authentication to resume, but it closes the "walked away from my desk" gap that no server-side timeout can see. It's cheap, and it's the whole difference between a session being yours and a session being whoever sits down next.