Give FiveM staff limited txAdmin access

txAdmin has its own staff accounts and permissions. A CloudExa game-panel subuser, an ESX group, a QBCore permission and a txAdmin administrator are separate access systems. Granting one does not automatically grant the others. Use a separate named account for each staff member so actions can be traced and access removed individually.

Check which control surface you have

txAdmin is bundled with FXServer, but your service must actually run it and provide an authorised management address. Use only the address supplied for your service. A normal game connection port is not automatically the txAdmin web port. If no txAdmin address is supplied, ask support about availability rather than exposing extra ports or changing startup arguments yourself.

Before changing an established staff setup, save a private backup of the txAdmin profile and access configuration through the tools available to you. Keep it away from public downloads: account and authentication information is sensitive. If you are also changing framework permissions, take the corresponding files and database backup before that separate change.

Create a role around real duties

Open txAdmin's Admin Manager as the owner or an administrator authorised to manage accounts. Give a moderator the specific player actions their job requires. For example, viewing the player list and warnings does not require permission to change server settings or execute arbitrary console commands. Select actions individually using the installed version's permission descriptions.

In particular, `console.write`, `server.cfg.editor`, `commands.resources` and `control.server` are operational powers. Treat `manage.admins` as permission to grant access to others. The `all_permissions` role is owner-level access, not a convenient default for ordinary staff. Protect the master account and avoid distributing its password.

Check web and in-game access separately

1. Have the staff member sign in using their own account in a separate browser session. Confirm the permitted pages and actions work.
2. Check an action outside their role is unavailable. Do not run a destructive action just to test its denial; inspect the controls or use a harmless, controlled test.
3. If they need the in-game menu, attach their correct Cfx.re or Discord identifier to their txAdmin account. A display name alone is not the identifier.
4. After joining, test `/tx` or `/txadmin`. If permissions were recently changed, the documented `/txAdmin-reauth` command can retry authentication.

Remove access cleanly

When someone leaves, remove their txAdmin account and separately review game-panel, database and framework permissions. If they knew shared secrets, rotate those secrets through the appropriate service. Review txAdmin action logs around unexplained restarts or configuration changes before assuming the hypervisor failed.

If menu authentication fails, record the exact error and account identifier type privately. Do not turn off source-IP checks or other authentication safeguards as a first fix. A reverse proxy or unusual hosting layout needs support to check its trusted network path. Successful staff access means both the allowed action works and owner-only actions remain restricted.

Related guides

- Understand ACE permissions and principals
- Collect useful resource error evidence

Further reading

- txAdmin permission system
- txAdmin in-game menu
- txAdmin project and setup

Looking for another game? Browse game server setup and troubleshooting guides.

Revision #2
Created 2026-11-09 09:21:20 UTC by CloudExa Hosting Admin
Updated 2026-11-09 09:21:21 UTC by CloudExa Hosting Admin