Collect txAdmin logs for support without exposing player data

txAdmin logs can explain a failed resource start, unexpected restart or staff action, but a full export may expose player identifiers, chat and typed commands. Send support a focused copy while preserving the original evidence privately. You need authorised access to the service's logs; do not change permissions across the host to obtain them.

Identify the right time and profile

Write down the incident time, timezone, service name and exact symptom. Include whether a player saw it once or repeatedly. Compare the panel clock with your own clock before choosing an excerpt. A five-minute timezone mistake can make a useful log look unrelated.

The official log reference distinguishes admin events, FXServer console output and server activity. Choose the stream that answers your question. An administrative restart belongs in a different investigation from a resource stack trace or a player chat dispute.

Find the configured log location

Use the panel's available log viewer or file manager. Older layouts commonly place logs below a txData profile, but check the actual installation. The current environment documentation describes `TXHOST_DATA_PATH` and notes changes from older convars. On hosted services, ask support when the data path is outside your accessible files; do not edit startup settings to make it visible.

1. Confirm the profile belongs to the affected service. A familiar folder name alone is not enough if several test profiles exist.
2. Copy the relevant log files to a private local folder. Keep original names and timestamps, and record which period each covers.

3. Extract the incident window with a few minutes of context before the first failure. Include the first error, not only the last repeated line.
4. Make a second copy for redaction. Keep the untouched original restricted in case support later needs to verify sequence or correlation.
5. Review the whole excerpt for credentials, webhooks, database URLs, session tokens, chat and player addresses. Replace sensitive values consistently, such as `[PLAYER-A]`, while preserving useful error structure.

Send a reproducible report

Include the resource version, artifact and txAdmin version, steps that triggered the issue and the expected result. Attach the redacted excerpt through your private support ticket. Avoid publicly accessible paste sites for raw console logs, and do not send an entire txData directory when a short excerpt answers the question.

If you suspect a staff-account compromise, preserve the full originals and tell support privately before changing retention. Deleting log files does not necessarily remove related records elsewhere, and it can destroy evidence of the original sequence.

Verify and retain appropriately

Open the submitted attachment to confirm it is readable and covers the incident. Check that redaction did not remove the resource name, time or stack-trace line needed to investigate. Keep a record of the support ticket and original file location.

This is an export workflow, not a retention-policy change. If logs rotate before incidents can be investigated, agree suitable retention with support and your privacy obligations. Do not increase every log to unlimited retention or enable verbose credential-bearing debug output indefinitely. Remove only your temporary working copies when the case and your agreed retention policy permit it.

Related help

- Give FiveM staff limited txAdmin access
- Trace FiveM script errors and measure resource performance

Revision #1
Created 2026-11-09 10:42:42 UTC by CloudExa Hosting Admin
Updated 2026-11-09 10:42:42 UTC by CloudExa Hosting Admin