Securing the database

The security measures that concern the database of an Exponential site - where the credentials are kept and how to protect them, how the administration and the console mask secrets, passwords on command lines, network...

Source file: `doc/eng-us/help/database-administrators/securing-the-database.md` Last changed 2026-11-04
https://doc.exponential.earth/exphelp/viewer/help/database-administrators/securing-the-database.md

This page is for database administrators who review the security of an Exponential site's database. It answers: where the database credentials are, who can read them, where they could leak (command lines, debug output, backups), how to limit network access per engine, and what the application records. The general hardening of the site is on Security hardening and in chapter 13; this page is the database's part of it.

Contents

1. Where the credentials are
2. Protect the override files
3. What the application shows and hides
4. Passwords on command lines
5. Network exposure
6. The SQLite file
7. Debug output shows SQL
8. Backups are secrets
9. What is recorded
10. Checklist

Where the credentials are

File	What it holds
`settings/override/site.ini.append.php`	`[DatabaseSettings]` `User`, `Password`, and replica logins
`settings/override/file.ini.append.php` and `config.cluster.php`	the DFS cluster's database login, when clustering is used
`settings/override/ezoracle.ini.append.php`	Oracle connection settings (no password unless you put one there)
`settings/siteaccess/<name>/site.ini.append.php`	a siteaccess's own database, if any

Source: 13.3 Secrets in settings/override.

Protect the override files

- **Never commit** `settings/override/` to version control, and never copy it to a public place.
- Keep the files readable by the site's user only where nothing else needs them: `chmod 640`, owner the site's user or root, group the site's group.
- Back them up with the database, as secrets.
- Copy them with every move of the installation.

What the application shows and hides

One rule, `expSecretRule`, decides what is a secret for `exp:ini`, the settings pages, the audit log and **Setup > System information**:

- a value whose name contains password and similar words shows only "(set, hidden)" or `********`;
- **the database user is always hidden** in the System information report;
- the password inside an address is cut (`mysql://user:***@db/site`).

`exp:ini get` and `list` mask secrets unless `--show-secrets` is given (System information, what is never shown). Still, give the settings views (`setup/setup`) only to administrators.

Passwords on command lines

A password given as a command-line argument is visible to other users of the machine in the process list, and stays in the shell history. Prefer what each tool offers instead:

Tool	Safe way
`exp:install`	the environment variable `EXP_INSTALL_DB_PASSWORD`
`ora-grant.php`	`-` as the password and `ORACLE_NEW_PASSWORD` in the environment
`mysql`, `mysqldump`	`-p` without a value (prompt), or an option file readable by you only
`psql`, `pg_dump`	the prompt or a `.pgpass` file with mode 0600
`mongosh`, `mongodump`	`passwordPrompt()` or a URI without the password, so the tool asks
`ezsqldumpschema.php`, `ezsqlinsertschema.php`, `ezsqldiff.php`	they take `--password=` only: run them on a machine you control, or with a temporary password you change afterwards

Network exposure

Engine	Measure
PostgreSQL	`listen_addresses` only on the needed interface; `pg_hba.conf` lines only for the web servers, this database and this user, with a password method
MySQL, MariaDB	bind to the needed interface; the account's host part limited to the web servers
MongoDB	access control on; bind to the needed interface
Oracle	the listener reachable from the web servers only

Engine	Measure
All	a firewall that admits the database port from the web servers and cron hosts only; TLS where the database is on another machine, configured on the server and in the client library

Exponential has no setting of its own for client certificates or TLS options of MySQL or PostgreSQL connections; what the client library takes from its defaults applies. Verify encryption on the server side if your policy requires it.

The SQLite file

The database file must never be served over HTTP. Check on your own host; anything but `200` is right:

Shell

```
curl -sI https://www.example.com/var/storage/sqlite3/exponential.db | head -1
```

Keep the directory group-writable for the site's processes only, never world-writable (SQLite files, ownership and permissions).

Debug output shows SQL

`[DatabaseSettings] SQLOutput=enabled` puts every statement into the debug output. Turn debug output on only for your own address (`DebugByIP=enabled`, `DebugIPList[]`), never for everyone on a public site (12.4 Debug output).

Backups are secrets

A database dump holds every user's e-mail address and password hash. Encrypt backups at rest, keep them off the web server, limit who can read them, and delete old generations on schedule (Backups per engine, Log and data retention).

What is recorded

The audit trail records administrative actions; each run of the upgrade check and each download of its report is written as `system.upgrade.run` (The upgrade check, Audit). Statements you run directly against the database are not recorded by Exponential; use the engine's own auditing for that.

Checklist

- ☐ `settings/override/` is mode 640 and not in version control.
- ☐ No database password in a shell history, crontab or script.
- ☐ The database port is reachable from the web servers and cron hosts only.
- ☐ The SQLite file returns no `200` over HTTP.
- ☐ Debug output is limited to administrators' addresses.
- ☐ Backups are encrypted and access-controlled.

Related pages

- Database accounts and privileges
- Security hardening
- Hardening for hosts
- Free documentation: this page is free to copy, translate and improve under the GNU FDL 1.3.

> **Become an Exponential Partner**
>
> Partners share their information, provide funding, contribute back and develop the products with us, and that is how Exponential grows. A partner website and dashboard are planned for mid-2027: please become a partner today to speed up our growth rate and land new features faster.
>
> Partners: start here | How to apply

Exponential Copyright © 1998-2026 Exponential Foundation and 7x
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".
This documentation is free documentation, licensed under the GNU Free Documentation License 1.3 or later:
https://www.gnu.org/licenses/fdl-1.3.html.