3. Scope

*Part of the **More Security** manual — see also 1. Introduction, 2. What's New, 4. Setup, 5. Usage, 6. Troubleshooting.*

Reference only — see 4. Setup for how to configure each of these.

3.1 Assets, management & administration items

- The **Setup > General** configuration screen gains a new "More Security" section for all of the above settings
- The **Central dashboard** includes a new "More Security" dashboard with attack-trend cards
- The admin menu gains a new **Security log** item for searching and auditing attempt history
- **User profiles** gain a new permission that controls who can view the security log
- Nothing else in GLPI is modified — all data the plugin needs lives in its own tables

3.2 Automatic actions

- Monthly automatic update of the GeoIP database for geoblocking
- Weekly automatic cleanup of old, resolved security-log entries

A scheduled task runs automatically (once a month) to download the latest DB-IP Lite database, keeping geoblocking country data current.

Another scheduled task runs automatically (roughly once a week, overnight) to clean up old, resolved entries from the security log, so the log doesn't grow forever. Only entries that are no longer blocking anyone are removed; anything still actively blocked — including a permanent block

— is kept. How long an entry is kept before cleanup is configurable from **Setup > Automatic actions**.

Actually blocking and unblocking happens instantly when an attempt occurs — only the log cleanup and database updates run on a schedule.

See 4.2 Configuration.

3.3 Notifications

None — no emails are sent. A blocked user simply sees an error message on the login or password-reset page itself, right when they try again.

3.4 Rules

Not applicable — no GLPI rules engine integration.

3.5 Permissions

- Changing the More Security settings requires the same permission as changing any other general GLPI setting — no separate right to manage.
- Viewing the security log is controlled by its own dedicated permission, which can be given to specific profiles independently of other rights. This log is read-only for everyone: even a profile with full rights can view entries but never edit or delete them.
- The trusted-network whitelist is configured alongside other settings in the More Security configuration tab, using the same permission as other general GLPI settings.

See 4.3 Permissions.

> Generated for **More Security 2.0.0** on GLPI 11.0.8 — 2026-08-24.

Revision #18
Created 2026-08-24 08:26:20 UTC by Óscar Beiro
Updated 2026-08-24 12:24:07 UTC by Óscar Beiro