1. Introduction

*Part of the **More Security** manual — see also 2. What's New, 3. Scope, 4. Setup, 5. Usage, 6. Troubleshooting.*

1.1 What More Security does

More Security protects the GLPI login page and the "forgotten password" form against automated password-guessing attacks. If someone — or some script — keeps trying wrong passwords against an account, or keeps requesting password resets, More Security notices and temporarily locks that account, that email address, or the attacker's network address, so the attack simply stops working. It also supports geoblocking: restricting logins to specific countries or blocking entire regions based on where the client's IP address is located.

1.2 Pain points it addresses

Login pages on the public internet are attacked constantly. Without protection, an attacker can sit and guess passwords or spam the "forgotten password" form for as long as they like, and GLPI itself won't stop them — it has no built-in defense against this. That's a real risk: a compromised account can mean exposed tickets, assets, and client data. More Security closes that gap: it slows attackers to a crawl and locks out repeated failures automatically, with no ongoing effort from IT staff, and no change to how legitimate users log in.

1.3 Features

- Locks an account after too many wrong password attempts, for a duration you choose — or until an administrator manually unlocks it
- Automatically forgets old failed attempts after a quiet period, so a genuine user who mistypes their password once isn't punished

- Blocks a single network address after too many failed attempts, whether it's guessing one account or many — stopping a broad attack even if it never fully locks one account
- Recognises a coordinated attack that spreads guesses across many different addresses to avoid triggering the usual limits, and locks the targeted account anyway
- Understands when GLPI sits behind a company firewall or load balancer, so the real attacker's address is blocked — not the office's shared address
- Lets you mark trusted networks (like your own office) as exempt from blocking, so staff working from a known location are never accidentally locked out
- Restricts logins to specific countries or blocks entire regions, using the client IP's geographic location for access control
- Keeps a read-only log of every login/reset attempt for security auditing
- Displays attack trends on the Central dashboard: the top attacking IP addresses and most-targeted user accounts, broken down by time range (24 hours, 7 days, 30 days)

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

Revision #18
Created 2026-08-24 08:26:19 UTC by Óscar Beiro
Updated 2026-08-24 12:24:05 UTC by Óscar Beiro