6. Troubleshooting

*Part of the **More Security** manual — see also 1. Introduction, 2. What's New, 3. Scope, 4. Setup, 5. Usage.*

Troubleshooting

Accounts or IPs become stuck blocked

Check the More Security tab on Setup > General. If an account or IP is still listed under "Active blocks" but should no longer be blocked, use the "Unblock" button next to the entry or select multiple entries and use "Unlock selected" to clear them.

The temporary block duration depends on the configuration:

- **Login account blocks** expire after the "Login block duration" setting (default 5 minutes)
- **Password reset blocks** expire after the "Password reset block duration" setting (default 10 minutes)
- **IP blocks** expire after the "IP block duration" setting (default 15 minutes)

Permanent blocks (marked "Permanent" instead of a time duration) never expire automatically and require manual unblock.

Legitimate users getting blocked

If regular users report login failures or repeated password reset rejections, check:

1. **Configuration** — Review the attempt limits on the More Security tab:
   - "Number of login attempts before block" — lower values block faster
   - "Number of password reset attempts before block" — separate limit for password resets
   - "Attempts counting window" — the time period over which attempts are counted
2. **Shared IP addresses** — If multiple users share a single IP (corporate office, hosting provider, school network), the per-IP limit "Number of attempts before IP block" may block the entire group after a few combined failed attempts. Check the "Active blocks" section to see if the IP is blocked, and use "Unblock" if needed. Configure "Trusted proxies" if users connect through reverse proxies or load balancers.
3. **Password reset abuse** — Users sometimes trigger many failed password-reset attempts while trying to recover a forgotten password. This is independent of login blocking — check the "Password reset block duration" and attempt limits separately.

Cannot access the More Security configuration

The More Security tab on Setup > General requires the same permission as any other general GLPI setting. If a user can't see the tab, check with an administrator that their profile has permission to edit general setup.

IP whitelist entries

A whitelisted network address is never blocked, no matter how many failed attempts come from it — useful for a trusted office network or monitoring service. CIDR notation (e.g. `203.0.113.0/24`) is supported for whitelisting an entire range at once.

At the moment, there is no page in GLPI where an administrator can add or remove whitelist entries themselves — this needs to be set up by your technical support/development contact. If you need a new address whitelisted, ask them directly rather than looking for it on the More Security tab.

The full attempts log appears empty

A more detailed "Attempts" table (visible to administrators with GLPI's debug mode turned on) shows every login/password-reset attempt, including failed ones that haven't triggered a block yet. If it appears empty:

1. **Trigger an attempt** — have someone try to log in or reset their password to generate test data
2. **Check filters** — the table may have filters applied; clear them to see all attempts
3. **Verify the plugin is active** — if the plugin was recently updated or restarted, the table may not appear until GLPI's cache is cleared

Blocked accounts shown with missing display names

The "Active blocks" table shows the account login, email, and IP. If the login field contains only a username with no full name or profile link, the account exists but may have been deleted since the block was created. The block record itself persists until manually unblocked or the temporary duration expires.

Geoblocking doesn't seem to be blocking anything

Geoblocking relies on a downloaded country database (DB-IP Lite) that must be fetched by the plugin's "update GeoIP database" automatic action before geoblocking can work. If that action hasn't run yet (e.g. right after install, or on a fresh environment), the database file won't exist and geoblocking **fails open** — logins are allowed through regardless of country, rather than being blocked.

To check:

1. **Run the automatic action** — go to Setup > Automatic actions, find the GeoIP database update task for More Security, and run it manually (or wait for its normal schedule).
2. **Check GLPI's Events log** — a failed lookup due to a missing or corrupt database logs an entry there ("GeoIP lookup failed ... database unavailable"). If you see this, the database hasn't downloaded successfully.
3. **Confirm outbound network access** — the automatic action downloads from db-ip.com; if the server has no outbound internet access or is behind a restrictive proxy/firewall, the download will keep failing silently until network access is fixed.

Until the database is present, treat geoblocking as effectively disabled — no logins will be rejected on country grounds, even if a mode and country list are configured.

"Too many attempts" error when trying to log in

This means the login or password-reset request was rejected because the account, address, or email hit its attempt limit — technically shown as an HTTP 429 error if you check your browser's network tools. This is expected: the protection is working as intended. Wait for the block duration to expire (default: 5 minutes for login, 10 minutes for password reset) or ask an administrator to unblock it early from the More Security tab.

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

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