System Settings

System Settings

Admin path: **System > System Settings** (`view_system_settings.cfm`, `inc/get_system_settings.cfm`, `inc/edit_system_settings.cfm`, `inc/add_serial_number.cfm`, `inc/update_system_email_addresses.cfm`, `inc/update_system_timezone.cfm`, `inc/update_system_update_check.cfm`, `inc/update_telemetry.cfm`, `inc/invalidate_user_sessions.cfm`).

This is the **catch-all configuration page** for the gateway's global identity. Three cards live here:

1. **General Settings** — postmaster + admin e-mail addresses, server timezone, daily update check, telemetry, and the Pro Edition serial number.
2. **Bot Protection (CAPTCHA)** — chooses the CAPTCHA provider used on public-facing forms (Forgot Password, etc.) and stores the per-provider keys.
3. **Session Management** — the "Force Logout All Users" red button.

Pairs with Console Settings (web-facing host / TLS cert) and Server Setup (mail-side host identity) — those define **where** Hermes lives; this page defines **who** runs it and which administrative addresses receive its automated traffic. The System Notifications page reads `admin_email` from this page when it sends Pushover or e-mail alerts.

Configuration storage

Every setting on this page lives in the `system_settings` table (`parameter` UNIQUE key, `value` VARCHAR(1024)). There are no `parameters2` rows in scope — that table is reserved for module-scoped config (`console`, `smtp`, etc.). The `parameter`/`value` shape is deliberately flat key/value; the seed in `config/database/hermes_install.sql` sets the defaults at install time and every edit on this page is a straight `UPDATE … WHERE parameter = '<key>'`.

Card	`system_settings.parameter`	Default	Notes
General	`postmaster`	`postmaster@domain.tld`	Must be a valid e-mail at a **domain that already exists in** `domains`
General	`admin_email`	`someone@otherdomain.tld`	Valid e-mail; no domain check

Card	`system_settings.parameter`	Default	Notes
General	`timezone`	`America/New_York`	Validated against the `timezones` table
General	`serial`	empty	Pro Edition serial; set via the **Add Serial Number** modal
General	`users`	`9999`	Set to `9999` automatically when a serial activates (legacy seat-cap field, no longer enforced)
General	`daily_update_check`	`2` (Disable)	`1` = enable, `2` = disable; controls the auto-update poll
General	`telemetry`	`1` (Enable)	`1` = enable, `2` = disable; anonymised usage data
General	`accepted`	`1`	Legacy AGPL acceptance flag; not surfaced in the UI
Release stamp	`version_no`	`Docker`	Sentinel that marks this as a Docker install
Release stamp	`build_no`	`v260119`	Current release tag
CAPTCHA	`captcha_provider`	`builtin`	One of `builtin`, `recaptcha`, `hcaptcha`, `turnstile`
CAPTCHA	`recaptcha_site_key` / `recaptcha_secret_key`	empty	reCAPTCHA v2
CAPTCHA	`hcaptcha_site_key` / `hcaptcha_secret_key`	empty	hCaptcha
CAPTCHA	`turnstile_site_key` / `turnstile_secret_key`	empty	Cloudflare Turnstile

The release-stamp rows (`version_no = 'Docker'`, `build_no = v<YYMMDD>`) are the canonical signal that this install is a Docker install rather than a legacy non-Docker one. They are surfaced read-only in the sidebar footer and in INSTALL_SUMMARY output; the schema-update orchestrator and several upgrade-path code paths gate on them.

General Settings — fields

Postmaster E-mail Address (required)

Where bounce notifications, postmaster-class mail, and several internal alerts originate from. `edit_system_settings.cfm` enforces three rules in sequence:

1. Must not be empty (`session.m = 2`)
2. Must validate as a real e-mail string (`session.m = 3`)
3. The **domain part must already exist in the `domains` table** (`session.m = 4`)

The third rule is the one that surprises people. A bare `postmaster@example.com` will not save unless `example.com` is already a recognised mailbox or relay domain on this gateway. If you are setting this up on a fresh install, add the domain first (Mailboxes > Domains or Email Relay > Relay Domains) and come back.

The postmaster address is also the `From:` on every notification e-mail the gateway sends (see System Notifications § Email path), so it must be a deliverable address from the gateway's perspective — which is exactly what the domain-existence check guarantees.

Admin E-mail Address (required)

The destination address for every automated alert and notification e-mail. Validates as a normal e-mail string (`session.m = 5` empty, `session.m = 6` malformed) but has no domain-existence check — it is deliberately allowed to be an external address (your monitoring inbox, a shared mailbox at a different provider) so the gateway can still reach you when its own mail flow is broken.

The System Notifications page reads this value at every send.

TimeZone (required)

Free-text autocomplete backed by `inc/gettimezones.cfm` against the `timezones` table. The submitted value is checked back against the table before save (`session.m = 7` empty, `session.m = 8` unknown). Drives every timestamp that Lucee renders in the UI plus the schedule times shown on Scheduled Tasks.

> **The Lucee server's own timezone is set elsewhere.** Changing this field rewrites the application's display timezone; it does **not** change the container's `TZ` env var or the OS clock. If the two diverge you will see UI timestamps in one zone and log files in another.

Serial Number (read-only here)

Display-only on the General card. To set or change a serial, use the **Add Serial Number** button at the top of the page — that opens a modal that POSTs to `inc/add_serial_number.cfm`.

The activation flow (only triggered when a serial is entered, not on every page load):

```
Modal POST  serial_number + tos
      │
      ▼
  add_serial_number.cfm
      │  validate non-empty / alphanumeric-only / TOS accepted
      │  generate per-request token (customtrans3)
      │  read host UUID via dmi_decode.cfm
      │  RSA-encrypt "<UUID>@<serial>" with /opt/hermes/ssl/public.pem
      ▼
  POST https://activate.hermesseg.io  (TCP/443, no SSL interception)
      │
      ▼
  Server returns "<hash>@<expires>" on success
                 or  INVALID / ALREADY_ACTIVATED / EXPIRED / REVOKED / ERROR
      │
      ▼
  On success: UPDATE system_settings SET value=<serial> WHERE parameter='serial'
              updateRetentionPolicy("VALID", expires, serial, hash)  (cache the result)
              session.license = "VALID"
```

Every login after this point re-validates against `https://validate.hermesseg.io` and falls back to the cached `<hash>@<expires>` if the validation endpoint is unreachable (the "offline mode" path). The page itself never re-runs validation — that is the job of `inc/setsession.cfm` at login.

`session.license` value visible after this page	Meaning
`VALID` + `session.edition = "Pro"`	Activation succeeded; Pro features available
`EXPIRED`	Cached license past expiry; renew at the vendor portal and re-login
`REVOKED`	Vendor revoked the serial; contact support
`INVALID`	Serial not recognised; double-check the value
`TAMPERED`	Pro template files don't match the signed fingerprint; reinstall the release
`PENDING_VALIDATION`	Cached license exists but no signed fingerprint baseline; reach the internet and re-login
`N/A`	No serial configured — Community Edition

The two activation-server error paths (`session.m = 12` / `session.m = 13`) both render the same root-cause hint: Hermes must reach `activate.hermesseg.io` over HTTPS **without SSL interception**. Inline-decrypt proxies will break activation because they re-sign the RSA-encrypted payload.

> **By design.** Deleting the serial value from `system_settings` instantly demotes the install to Community Edition. The next login sees `session.license = N/A` and stops attempting remote validation.

Daily Update Check / Telemetry

Two boolean (1 = enable, 2 = disable) selects. Daily Update Check is the toggle for the auto-update poll that watches for new releases. Telemetry is the anonymised usage-data feed; the in-card warning callout links to the public privacy doc. Defaults are: Telemetry = enabled, Daily Update Check = disabled.

Save flow

Save Settings posts `action = edit`, which runs `edit_system_settings.cfm` as a strict 5-step sequence (postmaster → admin_email → timezone → update_check → telemetry). Each validation failure short-circuits with `cflocation` back to `view_system_settings.cfm` and `session.m` set to the matching alert code — no partial state lands. On the final step, four small update includes write to `system_settings` one parameter at a time (`update_system_email_addresses.cfm`, `update_system_timezone.cfm`, `update_system_update_check.cfm`, `update_telemetry.cfm`).

Bot Protection (CAPTCHA)

CAPTCHA gates the public-facing forms that an unauthenticated visitor can hit — primarily the Forgot Password flow on `/user-auth/` and `/admin-auth/`. The provider is chosen here; the form templates check the same `system_settings` keys at render and validation time. Four providers are supported:

Provider	What it needs
Built-in (math)	No keys. Renders a "what is 7 + 3?" style challenge. Default; works offline.
Google reCAPTCHA v2	Site key + secret key. Pick the "*I'm not a robot*" *Checkbox* flavour at the reCAPTCHA admin.
hCaptcha	Site key + secret key. Privacy-focused reCAPTCHA alternative.
Cloudflare Turnstile	Site key + secret key. Usually invisible — no user interaction in the happy path.

`save_captcha` POSTs validate that the provider is one of the four allowed values and that the matching pair of keys is non-empty when a non-builtin provider is selected. All seven values are

written on every save regardless of which provider is active — this lets the admin switch providers back and forth without re-entering keys.

> **Failure mode.** A misconfigured external provider (bad keys, domain mismatch) breaks Forgot Password silently for the end user — the form renders, the CAPTCHA widget loads, but the server-side `siteverify` call fails and the request is rejected. Test the provider end-to-end on `/user-auth/forgot_password.cfm` after every change.

Session Management — Force Logout All Users

The red button at the bottom of the page flushes the **entire Authelia session store** in one call. Every user (admin, mailbox, relay recipient — and the operator clicking the button) is redirected to the login page on their next request. There is no per-user logout on this page; that happens automatically when a user's password is changed, their account is deactivated, or their account is deleted, because Authelia's session cookie is encrypted and only Authelia can invalidate one. The bulk-flush button is the only way to forcibly log people out from the admin UI.

Use this when:

- A shared admin credential has been rotated and you want every inherited session gone
- You suspect a compromised session token
- You have just changed Console Settings and want every old hostname-scoped cookie cleared at once

The action runs `inc/invalidate_user_sessions.cfm` with `targetSessionUser = "*"` and surfaces `session.m = 36` on return.

Edition badge — Pro vs Community

Although this page **stores** the serial number, the Pro / Community edition badge that appears in the sidebar header and in System Status is rendered from `session.edition` / `session.license` — both of which are set during login by `inc/setsession.cfm`. Changing the serial here updates the row in `system_settings`; the badge updates on the **next** login. Use **Force Logout All Users** above if you need the change to be visible to other admins immediately.

Files and tables touched

Path / table	Role
`system_settings`	Every setting on this page (key/value rows)
`domains`	Read at postmaster save to validate the domain part
`timezones`	Read at timezone autocomplete and save
`config/hermes/var/www/html/admin/2/view_system_settings.cfm`	Page
`config/hermes/var/www/html/admin/2/inc/edit_system_settings.cfm`	General-card save handler
`config/hermes/var/www/html/admin/2/inc/add_serial_number.cfm`	Serial activation against `activate.hermesseg.io`
`config/hermes/var/www/html/admin/2/inc/invalidate_user_sessions.cfm`	Force-logout call into Authelia
`config/hermes/var/www/html/admin/2/inc/setsession.cfm`	Reads serial + edition at login; this page's read-only Pro Edition state comes from here
`https://activate.hermesseg.io`	One-time serial activation endpoint
`https://validate.hermesseg.io`	Per-login Pro Edition re-validation endpoint

Related

- Console Settings — web console host + TLS cert
- Server Setup — mail-side host identity (Postfix `myhostname` / `myorigin`)
- System Notifications — consumes `admin_email` + `postmaster` from this page; also the home of Pushover settings
- System Status — surfaces the same Pro / Community badge plus the dashboard-alert stream
- System Update — when Daily Update Check is enabled, it is this page that drives the poll
- Password Resets — the public form that CAPTCHA actually protects

---

Revision #14
Created 2026-05-31 12:52:05 UTC by Dino Edwards
Updated 2026-06-13 12:30:08 UTC by Dino Edwards