

# System Status

# System Status

Admin path: **System > System Status** (`index.cfm` — the post-login landing page; the sidebar entry points here, not to a separate `view_system_status.cfm`). Supporting includes: `inc/system_alerts.cfm`, `inc/check_system_update.cfm`, `inc/get_system_version_build.cfm`, `inc/get_system_uptime.cfm`, `inc/get_system_reboot_required.cfm`, `inc/get_system_resources.cfm`, `inc/get_system_cpu_usage.cfm`, `inc/get_system_memory_usage.cfm`, `inc/get_system_{root,data,vmail,nextcloud}_filesystem_usage.cfm`, `api/get_system_resources.cfm`, `api/get_message_stats.cfm`.

System Status is the operator's at-a-glance picture of the running gateway. It is the **default page after login** — every Authelia post-login redirect lands here — and the union of every "is anything broken right now" signal Hermes computes: license state, update availability, host OS reboot pending, fresh-install onboarding nudges, container resource usage, and live mail-processing volume.

The page is **graceful-degradation by design**: every widget catches its own errors, every external call has a fallback, and a single failed query (a missing setting row, an unreachable container, a malformed log file) does not blank the dashboard. If you log in to Hermes and the page renders at all, the page is doing its job.

## Page layout

|                                                         |                                           |                            |
|---------------------------------------------------------|-------------------------------------------|----------------------------|
| +-----+                                                 |                                           |                            |
| Top navbar                                              | [license / fresh-install / update badges] |                            |
| +-----+                                                 |                                           |                            |
| Alert callouts (priority <= 5)                          |                                           | rendered by top_navbar.cfm |
| * Templates Modified (priority 1)                       |                                           | from request.systemAlerts  |
| * License Revoked (priority 2)                          |                                           | (populated in              |
| * Placeholder hostname (priority 2)                     |                                           | inc/system_alerts.cfm)     |
| * Invalid / Pending / Grace-period expired (priority 3) |                                           |                            |
| * Self-signed cert (priority 3)                         |                                           |                            |
| * License Expired (priority 4)                          |                                           |                            |

```

|   * Offline Mode           (priority 5)           |
+-----+
| Welcome <user>   Last login: <timestamp>         |
+-----+
| System Info card                                     |
|   Version | Build | Edition | Uptime | Console IP/FQDN |
|   | License Status | OS Updates | Hermes Update |
+-----+
| Messages Processed card                             |
|   Donut chart + counts (Clean/Spam/Virus/Banned/   |
|   Bad Header/Other) over 15m / 1h / 8h / 12h / 24h |
+-----+
| System Resources card                               |
|   CPU | Memory | Root FS | Data FS | Vmail FS | Nextcloud FS |
|   (seven progress rings, auto-refresh every 10s)  |
+-----+

```

The two cards that show live data (Messages Processed and System Resources) poll their own JSON endpoints in the background; the rest of the page is rendered server-side once per load.

## Self-healing on first load

`index.cfm` is the **bootstrap convergence point** for several secrets that the rest of the app depends on. If any are missing on first load (fresh install, after a credential rotation, after a key file deletion), they are generated in-place before the dashboard renders:

| Missing artifact                                                    | Auto-generated by                                      |
|---------------------------------------------------------------------|--------------------------------------------------------|
| <code>/opt/hermes/keys/hermes.key</code> (AES-256 application key)  | <code>inc/generate_hermes_key.cfm</code>               |
| <code>encryption_settings.user.serverSecret</code> (Ciphermail)     | <code>inc/generate_ciphermail_server_secret.cfm</code> |
| <code>encryption_settings.user.clientSecret</code> (Ciphermail)     | <code>inc/generate_ciphermail_client_secret.cfm</code> |
| <code>encryption_settings.user.systemMailSecret</code> (Ciphermail) | <code>inc/generate_ciphermail_mail_secret.cfm</code>   |
| <code>/opt/hermes/scripts/container_ips.txt</code> (Fail2ban)       | <code>inc/generate_container_ips.cfm</code>            |

Each generator is idempotent — it checks "is the file/row empty?" before writing, so subsequent loads are no-ops. This is why the very first dashboard render on a fresh install is slightly slower than subsequent loads.

# System Info card

The columns and what they mean:

| Column             | Source                                                                                                     | Notes                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version            | <code>system_settings.version_no</code>                                                                    | Always <code>Docker</code> in the Docker era. Hyphenated legacy values (e.g. <code>2024-08</code> ) belong to bare-metal installs that have not yet been migrated.                                                                                                                                                                                           |
| Build              | <code>system_settings.build_no</code>                                                                      | Current release tag ( <code>vYYMMDD</code> ). This is the single value the update orchestrator compares against to decide what to apply. See <a href="#">System Update</a> .                                                                                                                                                                                 |
| Edition            | <code>session.edition</code>                                                                               | <code>Community</code> or <code>Pro</code> . Community shows an <code>ENTER SERIAL</code> link to <a href="#">System Settings</a> ; Pro shows the edition with state suffixes ( <code>Pro (Templates Modified)</code> , <code>Pro (Validation Required)</code> ) when the license is in a non-VALID state.                                                   |
| Uptime             | <code>/opt/hermes/scripts/get_uptime.sh</code> via <code>cfexecute</code>                                  | Host uptime in days, not container uptime.                                                                                                                                                                                                                                                                                                                   |
| Console IP or FQDN | <code>parameters2.console.host</code>                                                                      | The value bound on <a href="#">Console Settings</a> .                                                                                                                                                                                                                                                                                                        |
| License Status     | <code>session.license</code> + <code>session.licenseexpires</code>                                         | One of <code>VALID</code> , <code>EXPIRED</code> , <code>REVOKED</code> , <code>INVALID</code> , <code>TAMPERED</code> , <code>PENDING_VALIDATION</code> , <code>VIOLATION</code> , <code>N/A</code> . Community shows <code>N/A</code> . The status text resolves through the same license-evaluation logic documented in <code>inc/setsession.cfm</code> . |
| OS Updates         | <code>/var/run/reboot-required</code> (file exists?)                                                       | <code>REBOOT REQUIRED</code> when the kernel/glibc-class update on the host needs a reboot. Hermes does not reboot the host — the admin does, via SSH.                                                                                                                                                                                                       |
| Hermes Update      | <code>inc/check_system_update.cfm</code> (reads <code>/opt/hermes/updates/check_system_update.txt</code> ) | <code>UPDATE BUILD vYYMMDD FOUND</code> (clickable, opens GitHub release notes modal), <code>LATEST VERSION</code> , <code>UPDATE CHECK PENDING</code> , or <code>UPDATE CHECK UNAVAILABLE</code> . The cache file is written by the daily <code>schedule/check_for_update.cfm</code> job; see <a href="#">System Update § Daily update check</a> .          |

The Hermes Update cell never makes a network call. It reads the cache file written by the Ofelia-scheduled CFML job, so the page renders fast and works offline.

“ **By design.** The dashboard never calls the GitHub Releases API at page-render time. All network IO for "is there an update" happens in the once-a-day Ofelia job. If the cache file is missing (first load after install, before the first scheduled run) you see `UPDATE CHECK PENDING`, never a hang.

## Release-notes modal

Clicking `UPDATE BUILD vYYMMDD FOUND` opens a modal that fetches the release body from the GitHub Releases API:

```
GET https://api.github.com/repos/deeztek/Hermes-Secure-Email-Gateway/releases/tags/<vYYMMDD>
```

The response's `body` field (Markdown) is converted client-side to HTML and rendered in the modal. If the fetch fails (rate limit, offline, release deleted) the modal degrades to a "View Release on GitHub" button. The GitHub release page is canonical; the modal is a convenience.

The tag passed to the URL is the build number **as-is**. Earlier revisions of this code prepended `build-` to match the legacy update-server file-name convention; that prefix was removed during the [#218](#) release-engineering pivot because GitHub release tags do not carry it.

## Alert callouts

`inc/system_alerts.cfm` builds a priority-ordered array of alerts each page load. The array is sorted ascending by priority (lower number = more urgent), then split:

| Priority | Surface                                                                             |
|----------|-------------------------------------------------------------------------------------|
| 1-5      | Full-width callout banner under the navbar, rendered by <code>top_navbar.cfm</code> |
| 6+       | Compact badge next to the user/edition pill in the navbar                           |

Every Hermes page that includes `top_navbar.cfm` participates — the callouts are not exclusive to System Status — but System Status is where an admin is most likely to be looking when they appear.

# License-state alerts

| Alert                | Priority | Trigger                                                                                                  |
|----------------------|----------|----------------------------------------------------------------------------------------------------------|
| Templates Modified   | 1        | <code>session.license = TAMPERED</code>                                                                  |
| License Revoked      | 2        | <code>session.license = REVOKED</code>                                                                   |
| Invalid License      | 3        | <code>session.license = INVALID</code>                                                                   |
| Validation Required  | 3        | <code>session.license = PENDING_VALIDATION</code><br>(no offline baseline yet)                           |
| Grace Period Expired | 3        | <code>session.license = GRACE_PERIOD_EXPIRED</code>                                                      |
| License Expired      | 4        | <code>session.license = EXPIRED</code>                                                                   |
| Offline Mode         | 5        | <code>VALID</code> + <code>validationMode = cached</code> ;<br>includes remaining grace-period day count |
| Expires in <N> days  | 10       | <code>VALID</code> + <code>licensevaliddays &lt;= 30</code><br>(badge only, never a callout)             |

## Fresh-install onboarding nudges

Two universal nudges fire when the gateway is still using seed defaults. Both apply to every install regardless of topology (relay-only, mail-server-only, hybrid) and they live here precisely **because** they are topology-agnostic.

| Nudge                | Priority | Trigger                                                                                                                                                | Fix link                            |
|----------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Placeholder hostname | 2        | <code>parameters.myhostname = 'hermes.domain.tld'</code> (Postfix seed) OR<br><code>parameters2.console.host = 'smtp.domain.tld'</code> (console seed) | <a href="#">Server Setup</a>        |
| Self-signed cert     | 3        | Every row in <code>system_certificates</code> is flagged <code>system = 1</code> (only bootstrap cert exists)                                          | <a href="#">System Certificates</a> |

Earlier iterations of this list included three more topology-specific nudges (no relay domains, no relay networks, no recipients-or-mailboxes). They were removed because they fired noisily on installs that legitimately don't have those things — a relay-only install has zero mailboxes and that is the correct configuration. Topology-specific onboarding guidance lives in [docs/install/get-started-docker.md](#) instead, where it is read deliberately rather than nagged about every page load.

# Other alerts (placeholders)

`system_alerts.cfm` includes guarded blocks for **Reboot Required** (when `session.rebootRequired = true`) and **Cert Expiring** (when `session.certExpiringSoon = true`). Neither flag is currently populated by any code path — they are reserved for future widgets that compute the values and stash them in the session.

# Messages Processed card

Polls `api/get_message_stats.cfm` on initial load and every 60s. The period selector reloads with the new window value but does not otherwise change the polling cadence.

| Bucket     | Color                           |
|------------|---------------------------------|
| Clean      | Green ( <code>#28a745</code> )  |
| Spam       | Yellow ( <code>#ffc107</code> ) |
| Virus      | Red ( <code>#dc3545</code> )    |
| Banned     | Gray ( <code>#6c757d</code> )   |
| Bad Header | Dark ( <code>#343a40</code> )   |
| Other      | Cyan ( <code>#17a2b8</code> )   |

The endpoint reads from the `msgs` table (Amavis-fed; covered in more detail under [System Logs](#)) filtered to the selected window. A 10,000-row hard cap is applied to keep page-load fast on busy installs; when the cap is hit, the total is suffixed with `+` and a small "Showing most recent 10,000 messages" note appears under the breakdown.

# System Resources card

Seven progress rings, auto-refreshing every 10s via `api/get_system_resources.cfm`:

| Ring                 | Source                                                                             |
|----------------------|------------------------------------------------------------------------------------|
| CPU Utilization %    | <code>/opt/hermes/scripts/get_cpu_usage.sh</code>                                  |
| Memory Utilization % | <code>/opt/hermes/scripts/get_memory_usage.sh</code>                               |
| Root FileSystem %    | <code>df</code> on <code>/</code> (host root)                                      |
| Data FileSystem %    | <code>df</code> on the Data tier mount (see <a href="#">Storage Topology</a> )     |
| Archive FileSystem % | <code>df</code> on the Archive tier mount ( <code>#260</code> ; Amavis quarantine) |

| Ring                   | Source                                      |
|------------------------|---------------------------------------------|
| Vmail FileSystem %     | <code>df</code> on the Vmail tier mount     |
| Nextcloud FileSystem % | <code>df</code> on the Nextcloud tier mount |

Each ring color-codes by threshold (`get_system_*_usage.cfm` returns a hex color alongside the value). The rings degrade independently — a missing tier mount renders that ring at 0 rather than failing the whole card.

Tiers that share a host path (a smaller install where Archive, Vmail, and Nextcloud are pinned to the same disk as Data) will show the same percentage on multiple rings. That is the correct behavior; the underlying `df` reading is the same.

# What is NOT on this page

System Status is intentionally a "snapshot" page, not an investigation tool. It surfaces alerts and current resource state. It does not surface:

| Want to see                                                       | Go here instead                                                         |
|-------------------------------------------------------------------|-------------------------------------------------------------------------|
| Mail queue contents / deferred messages                           | <a href="#">Mail Queue</a>                                              |
| Per-message processing history                                    | <a href="#">System Logs</a>                                             |
| Detailed cert / SAN status                                        | <a href="#">System Certificates</a> , <a href="#">SMTP TLS Settings</a> |
| Container health ( <code>docker ps</code> output, restart counts) | Host shell — Hermes does not surface raw Docker state in the web UI     |
| Scheduled-job last-run / next-run                                 | <a href="#">Scheduled Tasks</a>                                         |
| Fail2ban bans in effect                                           | <a href="#">Intrusion Prevention</a>                                    |
| Past update history                                               | The git log on the host ( <code>git log --oneline -- updates/</code> )  |

# Failure semantics

| What breaks                                                             | What happens                                                                                      |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <code>/opt/hermes/updates/check_system_update.txt</code> does not exist | <code>hermesupdate = "UPDATE CHECK PENDING"</code> ; cell renders cleanly                         |
| Ofelia job has been failing for days (cache stale or shows old build)   | Page still renders; the <b>Hermes Update</b> cell reflects whatever the last successful run wrote |

| What breaks                                                                        | What happens                                                                                                                    |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| GitHub API rate-limited or unreachable when an admin clicks the release-notes link | Modal falls back to a "View Release on GitHub" button                                                                           |
| <code>df</code> on a tier mount fails                                              | That ring renders at 0 with default color; other rings render normally                                                          |
| <code>get_uptime.sh</code> exits non-zero                                          | Page short-circuits to the error template — uptime is treated as critical because its absence usually means a broken commandbox |
| <code>system_settings.build_no</code> / <code>version_no</code> row missing        | Empty value in the matching cell; license cells will display <code>N/A</code>                                                   |
| <code>inc/generate_*</code> first-load generator fails                             | Logged; affected feature degrades downstream (Ciphemail mail crypto disabled, etc.) — the dashboard itself still renders        |

# Files and containers touched

| Path                                                                                                                    | Owner                                                          | Role                                                                         |
|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------------------------|
| <code>config/hermes/var/www/html/admin/2/index.cfm</code>                                                               | <code>hermes_commandbox</code>                                 | Page                                                                         |
| <code>config/hermes/var/www/html/admin/2/inc/system_alerts.cfm</code>                                                   | <code>hermes_commandbox</code>                                 | Alert array builder (license + nudges + future widgets)                      |
| <code>config/hermes/var/www/html/admin/2/inc/check_system_update.cfm</code>                                             | <code>hermes_commandbox</code>                                 | Cache-file reader (Docker path)                                              |
| <code>config/hermes/var/www/html/admin/2/inc/get_system_*.cfm</code>                                                    | <code>hermes_commandbox</code>                                 | Per-widget data fetchers                                                     |
| <code>config/hermes/var/www/html/admin/2/api/get_system_resources.cfm</code>                                            | <code>hermes_commandbox</code>                                 | JSON endpoint for progress-ring auto-refresh                                 |
| <code>config/hermes/var/www/html/admin/2/api/get_message_stats.cfm</code>                                               | <code>hermes_commandbox</code>                                 | JSON endpoint for message-stats card                                         |
| <code>/opt/hermes/scripts/get_uptime.sh</code> ,<br><code>get_cpu_usage.sh</code> ,<br><code>get_memory_usage.sh</code> | <code>hermes_commandbox</code>                                 | Shell helpers invoked via <code>cfexecute</code>                             |
| <code>/opt/hermes/updates/check_system_update.txt</code>                                                                | <code>hermes_commandbox</code>                                 | Cache file written by <code>schedule/check_for_update.cfm</code> ; read here |
| <code>/var/run/reboot-required</code>                                                                                   | host filesystem (mounted into <code>hermes_commandbox</code> ) | Ubuntu's standard "kernel upgrade pending" sentinel                          |
| <code>/opt/hermes/keys/hermes.key</code>                                                                                | <code>hermes_commandbox</code>                                 | Created on first load if missing                                             |
| <code>encryption_settings</code> table                                                                                  | <code>hermes_db_server</code> ( <code>hermes</code> DB)        | Ciphemail secrets populated on first load if empty                           |

# Related

- [System Update](#) — the page System Status's "Hermes Update" cell links to; covers the daily update check and the orchestrator that consumes the cache file
- [System Settings](#) — where the Pro serial number is entered to lift Community to Pro
- [System Certificates](#) — the page the "Self-signed cert" nudge links to
- [Server Setup](#) — the page the "Placeholder hostname" nudge links to
- [System Logs](#) — drill-down for the message-volume numbers shown in the Messages Processed card
- [Storage Topology](#) — explains the five tiers the resource-usage rings reflect
- [Release and Update Methodology](#) — methodology behind the version stamp this page surfaces

---

Revision #64

Created 2026-05-31 12:52:06 UTC by Dino Edwards

Updated 2026-08-22 11:48:32 UTC by Dino Edwards