Antivirus Settings

Antivirus Settings

Admin path: **Content Checks > Antivirus Settings** (`view_antivirus_settings.cfm`, `inc/get_antivirus_settings.cfm`, `inc/antivirus_set_settings.cfm`, `inc/antivirus_add_whitelists.cfm`, `inc/antivirus_delete_entry.cfm`, `inc/generate_antivirus_configuration.cfm`, `inc/restart_clamav.cfm`).

This page configures the ClamAV antivirus engine that runs inside `hermes_mail_filter` and is called by Amavis on every message that clears the SMTP-time perimeter. Two cards: the main settings card (sixteen toggles that map to `clamd.conf` directives) and a Pro-only AV Signature Whitelist for suppressing known-bad-signature false positives. Refreshing third-party signature *feeds* (Sanesecurity, SecuriteInfo, MalwarePatrol, etc.) is configured separately on Malware Feeds; this page configures the engine itself.

Where antivirus sits in the flow

```
                +-----------------------------------+
inbound msg -->| Perimeter Checks pass              |
                +---------------+-------------------+
                                |
                                v
                +-----------------------------------+
                |  Postfix smtpd_proxy_filter       |
                |    -> hermes_mail_filter:10024    |
                +---------------+-------------------+
                                |
                                v
                +-----------------------------------+
                |  Amavis (hermes_mail_filter)      |
                |   - SpamAssassin scoring          |
                |   - ClamAV antivirus  <---- this page configures this engine
```

```
|   - banned-file checks            |
+--------------+------------------+
               |
               v
+----------------------------------+
|  Re-inject -> hermes_postfix_dkim:10026
+----------------------------------+
               |
               v
+----------------------------------+
|  OpenDKIM sign, ARC seal, deliver |
+----------------------------------+
```

Amavis calls ClamAV over the local socket; the verdict determines whether Amavis quarantines, blocks, or passes the message. Amavis's own action policy (the `final_*_destiny` settings — quarantine vs DSN vs discard) lives in Antispam Settings and the per-domain policy table, not on this page. This page is **engine knobs only**.

Container and socket placement

Component	Detail
Container	`hermes_mail_filter` (IPv4 `.105`)
Engine	`clamd` daemon, Unix socket inside the container
Daemon config	`/etc/clamav/clamd.conf` (volume-mounted from `./config/mail_filter/etc/clamav/clamd.conf`)
Signature dir	`/var/lib/clamav/` (Docker named volume `mail_filter_data_clamav`)
Signature whitelist	`/var/lib/clamav/local.ign2` (regenerated from `parameters2 WHERE module='clamav-bypass'` on every save)
Third-party feeds	`/etc/fangfrisch/fangfrisch.conf` + `/var/lib/fangfrisch/signatures/` (see Malware Feeds)
Base signature refresh	`freshclam` (official ClamAV CVD updates, default 1h)
Feed refresh	`fangfrisch refresh` on a 10-minute Ofelia job (`hermes-fangfrisch-refresh`)

The container exposes **no host ports** — Amavis is reached only by Postfix internally at `hermes_mail_filter:10024` and re-injects to `hermes_postfix_dkim:10026`.

ClamAV Antivirus Settings card

Sixteen toggles, each rendered from the `avSettings` array in `view_antivirus_settings.cfm` with an inline hint and a "Recommended" label on the safer default. Every toggle writes `parameters2.value2 = 'true' | 'false'` for `module = 'clamav'`; on save, `generate_antivirus_configuration.cfm` selects every active row and emits one `<directive> <value>` line per toggle into a temp file, substitutes the temp file into the `HERMES_ANTIVIRUS_SETTINGS_GO_HERE` placeholder of `clamd.conf.HERMES`, backs up the live config to `clamd.conf.HERMES`, and moves the rendered file into place.

UI Toggle	`clamd.conf` directive	Recommended	Notes
Scan Email Attachments	`ScanMail`	Enabled	Master switch for inbound attachment scanning
Scan Archives	`ScanArchive`	Enabled	Recurse into ZIP, RAR, 7z, etc. Without this, only the archive wrapper is scanned
Mark Encrypted Archives as Viruses	`ArchiveBlockEncrypted`	Disabled	Aggressive; commonly false-positives on legitimate password-protected files
Scan Portable Executables	`ScanPE`	Enabled	Windows PE format; required for decompression of UPX / FSG / Petite packers
Scan OLE2 Files	`ScanOLE2`	Enabled	MS Office `.doc/.xls/.ppt` and `.msi`
Block OLE2 VBA Macros	`OLE2BlockMacros`	Disabled	Blocks ALL macro-enabled documents regardless of intent (detected as `Heuristics.OLE2.ContainsMacros`); useful in strict environments, breaks legitimate macros otherwise
Scan PDF Files	`ScanPDF`	Enabled	PDF embedded JS, exploit detection
Scan HTML/JavaScript Content	`ScanHTML`	Enabled	HTML normalization + JavaScript/ScriptEncoder decryption; phishing + script-exploit detection
Algorithmic Detection	`AlgorithmicDetection`	Enabled	Engine-level heuristics for complex malware and graphic-file exploits
Scan ELF Files	`ScanELF`	Enabled	Linux/Unix executable format

UI Toggle	`clamd.conf` directive	Recommended	Notes
Phishing Signature Detection	`PhishingSignatures`	Enabled	ClamAV's phishing signature DB
Scan Email URLs for Phishing	`PhishingScanURLs`	Enabled	URL extraction + phishing URL DB lookup
Block SSL Mismatches in URLs	`PhishingAlwaysBlockSSLMismatch`	Disabled	False-positives on CDN and redirect URLs
Block Cloaked URLs	`PhishingAlwaysBlockCloak`	Disabled	False-positives on URL shorteners and marketing-tracker links
Detect Potentially Unwanted Applications	`DetectPUA`	Enabled	Adware, dialers, non-malicious-but-unwanted software
Heuristic Scan Precedence	`HeuristicScanPrecedence`	Enabled	When on, heuristic hits stop the scan immediately (saves CPU). When off, scanning continues so a signature-based hit can override a heuristic match

> **Operational consequence — disabling `ScanMail`.** This effectively turns off antivirus for inbound mail. Amavis will still consult ClamAV for ban-pattern decisions but the engine will skip the attachment scan. Leave on except for very short-term diagnostics.
>
> **Operational consequence — `OLE2BlockMacros` = true.** Every macro-enabled Office document is blocked as `Heuristics.OLE2.ContainsMacros`, including documents from your own users. Most organizations get better results with macro-blocking enforced at the endpoint (Microsoft 365 Protected View, Group Policy) rather than at the gateway. Turn on only after warning users and ensuring you have a release workflow.

AV Signature Whitelist card (Pro)

When ClamAV produces a false positive on a known-safe file, the admin enters the exact ClamAV signature name (e.g. `Heuristics.OLE2.ContainsMacros`) and Hermes appends it to `/var/lib/clamav/local.ign2`. ClamAV reads `local.ign2` at engine start and suppresses any detection whose signature name matches a line in the file.

Storage: `parameters2 WHERE module = 'clamav-bypass'` (one row per signature name, `parameter` column holds the signature string). On every save and on every delete,

`generate_antivirus_configuration.cfm` rewrites the whole `local.ign2` from the table, runs `dos2unix` to scrub line endings, backs up the current file to `local.ign2.HERMES`, and moves the new file into place. ClamAV is then restarted via `restart_clamav.cfm` to pick up the change.

How to find a signature name

The in-card info box gives admins the lookup steps:

1. From **Message History**, find the blocked message (Type column shows `Virus` or `Banned`)
2. Grep the mail-filter log for the message ID: `docker logs hermes_mail_filter 2>&1 | grep <mail_id>`
3. The log line shows the signature in parentheses, e.g. `Blocked INFECTED (Heuristics.OLE2.ContainsMacros)`
4. Or scan a file directly: `docker exec hermes_mail_filter clamscan /path/to/file`

> **Operational consequence — whitelisting is by signature name, not by file hash.** If you whitelist `Heuristics.OLE2.ContainsMacros`, you have effectively turned off macro detection globally. Prefer narrow signature names (specific malware family) over heuristic families when possible.

Signature refresh

Two independent refresh loops keep the engine current:

Source	Mechanism	Cadence	Database
Official ClamAV (`main.cvd`, `daily.cvd`, `bytecode.cvd`)	`freshclam` daemon inside `hermes_mail_filter`	Default 1h (configurable in `/etc/clamav/freshclam.conf`)	`/var/lib/clamav/`
Third-party feeds (Sanesecurity, SecuriteInfo, MalwarePatrol, etc.)	`fangfrisch refresh` via Ofelia job `hermes-fangfrisch-refresh`	Every 10 minutes (only feeds whose own publish cycle has elapsed actually re-download)	`/var/lib/fangfrisch/signatures/` then linked into `/var/lib/clamav/` by `setup-clamav-sigs`

`fangfrisch` is the small Python tool that handles auth, cadence control, and integrity verification for third-party feeds; the feed list and per-feed enable/disable lives on Malware Feeds. Enabling premium feeds (SecuriteInfo paid, MalwarePatrol paid) requires Pro licensing — the feed list itself is gated on the same page.

Resource footprint

Loading the full signature database into RAM costs roughly 1.5–2 GB of memory. If `hermes_mail_filter` is under-provisioned (e.g. shared host with 4 GB total), `clamd` will fail to start, mail will queue behind Amavis, and the only sign in the UI is a quiet rise in deferred queue depth. Plan for at least 4 GB dedicated to the `hermes_mail_filter` container on systems with all third-party feeds enabled.

The default ClamAV file-size cap is 25 MB (`MaxFileSize 25M` in `clamd.conf`). Messages larger than this are passed without scan and flagged with a `Heuristics.Limits.Exceeded` indicator. Raising the cap requires editing `clamd.conf.HERMES` directly; the UI does not expose it because raising it disproportionately increases RAM and CPU per scan.

Save flow

```
1. View page submits action="AV Settings" (sixteen booleans),
                       action="Add AV Whitelist" (textarea),
                       action="Delete Entry" (id list)
2. view_antivirus_settings.cfm validates every avFields entry exists and is true|false
   (any failure -> error.cfm + cfabort)
3. antivirus_set_settings.cfm UPDATEs parameters2.value2 for each toggle
   (16 UPDATEs, module='clamav')
4. generate_antivirus_configuration.cfm:
     a. SELECT active='1' rows from parameters2 module='clamav' -> temp avsettings file
     b. dos2unix the temp file
     c. Substitute into clamd.conf.HERMES placeholder HERMES_ANTIVIRUS_SETTINGS_GO_HERE
     d. Back up /etc/clamav/clamd.conf -> clamd.conf.HERMES, move new file into place
     e. Rebuild /var/lib/clamav/local.ign2 from parameters2 module='clamav-bypass'
     f. dos2unix, back up local.ign2 -> local.ign2.HERMES, move new file into place
     g. cfinclude restart_clamav.cfm (docker container restart hermes_mail_filter ClamAV
process)
5. session.m = 9 -> green "Antivirus Settings were saved successfully" alert
```

`generate_antivirus_configuration.cfm` also runs on whitelist add/delete — every change to either card triggers the same full regen + ClamAV restart cycle. The page does not return until the restart has completed (timeout per `cfexecute`).

Failure semantics

Failure	Behavior
Toggle form missing a required boolean field	`m = "Antivirus Settings: form.<f> does not exist"`, `error.cfm`, cfabort
Toggle value not in `true,false`	`m = "Antivirus Settings: form.<f> is not true or false"`, `error.cfm`, cfabort
Delete clicked with no selection	session.m = 11
Add Whitelist with empty textarea	session.m = 13
`dos2unix` failure on the temp avsettings or local.ign2 file	`error.cfm` + cfabort with the failing path in the message
`cp /etc/clamav/clamd.conf -> .HERMES` failure	`error.cfm` + cfabort
`mv <tmp>_clamd.conf -> /etc/clamav/clamd.conf` failure	`error.cfm` + cfabort
`restart_clamav.cfm` failure	Surfaces as cfcatch from the docker restart step

The save is **not** transactional across the steps — if the SQL updates succeed but the ClamAV restart fails, the DB state has already advanced. The next save will re-render and re-apply because every save regenerates the entire file from the current row state (no incremental writes).

Files and containers touched

Path	Owner	Role
`config/hermes/var/www/html/admin/2/view_antivirus_settings.cfm`	`hermes_commandbox`	The page
`config/hermes/var/www/html/admin/2/inc/antivirus_*.cfm`	`hermes_commandbox`	Validate / save / regenerate / restart
`config/hermes/var/www/html/admin/2/inc/get_antivirus_settings.cfm`	`hermes_commandbox`	Loads current `parameters2 module='clamav'` values
`config/hermes/opt/hermes/conf_files/clamd.conf.HERMES`	`hermes_commandbox` (read) -> `hermes_mail_filter` (live `/etc/clamav/clamd.conf`)	Canonical template with `HERMES_ANTIVIRUS_SETTINGS_GO_HERE` placeholder
`config/mail_filter/etc/clamav/clamd.conf`	`hermes_mail_filter` (live config, bind-mounted)	Read by `clamd` at start
`/var/lib/clamav/local.ign2`	`hermes_mail_filter` (Docker named volume `mail_filter_data_clamav`)	Signature whitelist; rewritten on every save
`/var/lib/clamav/*.cvd`, `*.cld`, `*.ndb`, etc.	`hermes_mail_filter`	Signature databases (official + third-party)
`parameters2` table, `module='clamav'`	`hermes_db_server` (`hermes` DB)	Source of truth for the sixteen toggles

Path	Owner	Role
`parameters2` table, `module='clamav-bypass'`	`hermes_db_server` (`hermes` DB)	Source of truth for the AV Signature Whitelist
`malware_databases` table	`hermes_db_server` (`hermes` DB)	Third-party feed list (configured on Malware Feeds)
`ofelia_jobs` row `hermes-fangfrisch-refresh`	`hermes_db_server`	10-minute feed refresh scheduler
`hermes_mail_filter` container	—	`clamd`, `freshclam`, `fangfrisch`, Amavis, SpamAssassin

Related

- Malware Feeds — the third-party signature feed configuration (Sanesecurity, SecuriteInfo, MalwarePatrol, etc.) that Fangfrisch refreshes every 10 minutes
- Perimeter Checks — every check on this page runs only after a connection clears the SMTP-time perimeter
- Anti-Spam Settings — runs in the same Amavis pass; a virus verdict overrides any spam score
- Score Overrides — per-rule weight changes for SpamAssassin
- Email Policies > Disclaimers — body modification that runs after Amavis re-injection; never conflicts with ClamAV because it happens post-scan
- ARC Settings — seals over the body Amavis passed, so a virus verdict naturally pre-empts everything downstream
- DNS Resolver — URL phishing lookups (`PhishingScanURLs`) and signature-feed downloads (Fangfrisch) all resolve through `hermes_unbound`
- Email flow — full pipeline diagram

Revision #48
Created 2026-05-31 12:52:20 UTC by Dino Edwards
Updated 2026-06-20 13:33:11 UTC by Dino Edwards