Relay Host

Relay Host

Admin path: **Email Relay > Relay Host** (`view_relay_host.cfm`, `inc/get_relay_host_settings.cfm`, `inc/edit_relay_host_settings.cfm`, `inc/generate_sasl_password_transport.cfm`, `inc/generate_postfix_configuration.cfm`).

This page configures the **single global outbound relay host** that Postfix uses to deliver mail to the Internet — the smarthost an ISP, M365, SendGrid, or another upstream MTA supplies when direct delivery is blocked or undesirable. It controls the host/port pair, the optional SASL credentials, and the outbound TLS security level. Saving rewrites the relevant rows in the `parameters` table, regenerates `/etc/postfix/sasl_passwd`, and re-renders `/etc/postfix/main.cf` from the template so the new values take effect on the next message.

Pairs with Domains for the inbound half of the relay topology — Relay Host defines where outbound mail goes; Domains defines which inbound domains Hermes accepts and where each one is forwarded.

When you need a relay host

By default, Hermes attempts direct MX delivery for outbound mail. A relay host is required in any of these scenarios:

Scenario	Why direct delivery fails
Hermes is behind a firewall that blocks outbound TCP/25	Port 25 to the open Internet is filtered
ISP forbids outbound SMTP for residential/business links	Outbound TCP/25 is dropped at the ISP edge
Outbound IP has no PTR record or is on a blocklist	Recipients reject; deliverability tanks
Compliance requires all outbound mail to traverse a known SMTP gateway (M365 connector, SendGrid, on-prem hub)	Centralized policy/journaling/encryption point
Hermes sits on a non-routable internal network	No path to the Internet without a smarthost

If none of those apply and Hermes has a clean public IP with a PTR record, leave **Enable Relay Host** off and let Postfix do direct delivery.

How the relay host fits in the outbound path

```
local pickup / amavis re-inject (10025)
        |
        v
hermes_postfix_dkim (smtp client)
        |
        |  relayhost          = [smtp.example.com]:587   (from parameters)
        |  smtp_sasl_*        = enable + sasl_passwd map (from parameters + sasl_passwd)
        |  smtp_tls_security  = may | encrypt            (from parameters)
        |
        v
upstream smarthost  ──►  recipient MX
```

Only the upstream-bound TCP connection is affected. Inbound SMTP on port 25, the content-filter loop (Amavis on 10024/10026), and Dovecot LMTP delivery are untouched.

Configuration storage

Relay Host settings are spread across two tables. The host/port and SASL toggles live in the **`parameters`** table using the dual-row pattern (`child=2` parent name row, `child=1` value row). The SASL credentials themselves are encrypted at rest in **`system_settings`** to keep cleartext out of the directive table.

Setting	Storage	Notes
Enable Relay Host	`parameters.enabled` on `parameter='relayhost' AND child=2`	Master switch; disabling clears the child value and pushes `relayhost =` (empty) into `main.cf`
Relay Host Address	`parameters.name` on the `relayhost` child row	Bare FQDN/IP for display
Relay Host Port	Parsed from `parameters.parameter` (`[host]:port`)	Stored as the Postfix-formatted bracketed `[host]:port` literal
Outbound TLS Mode	`parameters.parameter` on `smtp_tls_security_level` child row (`""`, `may`, `encrypt`)	Empty value disables both parent and child; `may` = opportunistic STARTTLS; `encrypt` = mandatory TLS

Setting	Storage	Notes
Authentication required	`parameters.enabled` on `smtp_sasl_auth_enable` parent + `parameters.parameter` value `yes` / `no`	Flips the `smtp_sasl_password_maps` parent in lockstep
Relay Host Username	`system_settings.value` row `relay_host_username`	AES/Base64 encrypted with `/opt/hermes/keys/hermes.key`
Relay Host Password	`system_settings.value` row `relay_host_password`	AES/Base64 encrypted with the same key

> **By design.** The legacy schema kept the SASL username/password in plaintext on the `smtp_sasl_password_maps` child row's `name` column. The current code path encrypts both into `system_settings` and clears the legacy column on every save. The first read against a legacy install runs a one-shot migration in `get_relay_host_settings.cfm`: if `system_settings` is empty but the old `parameters.name` colon-delimited string is present, the values are encrypted forward and the plaintext column is cleared. No admin action is required.

Fields on the page

Enable Relay Host

Master switch. When off, all the other fields are hidden, the `relayhost` parent is set `enabled=0`, the child value is wiped, and the SASL parent/child rows + `system_settings` credentials are cleared in the same save. Postfix is then re-rendered with `relayhost =` empty so the next outbound message attempts direct delivery again.

Relay Host Address

Accepts:

- **IPv4** — validated against a dotted-quad regex with 0–255 octet bounds
- **IPv6** — validated against a simplified colon/hex check
- **FQDN** — validated by the email-trick (`IsValid("email", "bob@<host>")`)

Trimmed before storage. The address is stored on its own (in `parameters.name`) and also formatted into the Postfix-required bracketed literal `[host]:port` (in `parameters.parameter`) so that Postfix skips MX lookups and connects directly. Brackets are always emitted for the relay host — round-robin via MX is not part of this page's model; if you need MX-driven relay distribution, configure

DNS upstream of the brackets.

Relay Host Port

1–65535. Default `25`. The page's helper text surfaces the three common values:

Port	Typical use
`25`	Inbound MX / unauthenticated relay
`587`	Submission with STARTTLS + SASL (most modern smarthosts)
`465`	Submission over implicit TLS (SMTPS) — Postfix needs `wrappermode` adjustments not exposed on this page; prefer `587` when the smarthost supports it

Outbound TLS Mode

Maps directly to Postfix's `smtp_tls_security_level` for client connections (not to be confused with the `smtpd_tls_*` server-side settings configured under SMTP TLS Settings).

UI value	`main.cf` value	Behavior
Disabled - No TLS	parent `enabled=0` (no directive emitted)	Plaintext only; STARTTLS not attempted
Opportunistic TLS (Recommended)	`smtp_tls_security_level = may`	STARTTLS used if offered; falls back to plaintext otherwise
Mandatory TLS	`smtp_tls_security_level = encrypt`	STARTTLS required; delivery fails if the upstream does not offer it. No certificate verification — use a TLS policy for that.

Pick **may** for port 587 with STARTTLS, **encrypt** if your smarthost contract requires confirmed encryption. For verified-peer TLS to a specific smarthost, layer on a TLS policy via SMTP TLS Settings.

Authentication

When toggled on, **Username** and **Password** become required. The password input is masked-and-replaceable: it is rendered blank with the first 4 characters of the stored value shown beneath as a hint (`abcd*****`), and a blank submit keeps the existing encrypted value. Set a new value to rotate.

The handler reads `/opt/hermes/keys/hermes.key`, encrypts both fields (`AES` / `Base64`), and writes the ciphertext into `system_settings`. The decryption path is symmetric — `generate_sasl_password_transport.cfm` reads, decrypts, and writes the `[host]:port  user:pass` line to `/etc/postfix/sasl_passwd` before postmapping it.

Save flow — the cascade

Clicking **Save Settings** posts `action=save`. The handler runs a strict sequence:

```
1. Validate Enable + (if enabled) host + port + (if auth) user/pass
2. edit_relay_host_settings.cfm
   - update parameters rows (relayhost, smtp_sasl_auth_enable,
     smtp_sasl_password_maps, smtp_tls_security_level)
   - if auth: encrypt creds, write to system_settings,
     clear legacy plaintext on parameters.name
   - if not auth or disabled: clear system_settings credentials,
     disable all SASL parameter rows
   - call generate_sasl_password_transport.cfm
     -> rewrites /etc/postfix/sasl_passwd
     -> docker exec hermes_postfix_dkim postmap /etc/postfix/sasl_passwd
3. generate_postfix_configuration.cfm
   - copies /etc/postfix/main.cf to main.cf.HERMES (write-time backup)
   - copies /opt/hermes/conf_files/main.cf.HERMES template -> main.cf
   - chown root:root via docker exec hermes_postfix_dkim
   - iterates enabled parameters rows, substitutes the directive name
     and value into main.cf
   - docker exec hermes_postfix_dkim postfix reload
4. cflocation back with session.m = 10 (success banner)
```

Validation failures short-circuit with `session.m` set to the matching error code (1–6) and a redirect — no partial DB writes land.

`sasl_passwd` generation — consolidated, not per-page

`generate_sasl_password_transport.cfm` is a **shared** generator called by both this page and the Domains Add/Edit/Delete handlers. It is the single source of truth for `/etc/postfix/sasl_passwd` and rebuilds the file from scratch each invocation:

```
# /etc/postfix/sasl_passwd  (regenerated on every save)
[smtp.example.com]:587    relayuser:relaypassword       <-- this page (relay host)
[mx1.partner.com]:25      partneruser:partnerpassword   <-- Domains page (per-domain auth)
[mx2.partner.com]:25      otheruser:otherpassword       <-- Domains page (per-domain auth)
```

The relay host entry is added if **all** of:

- `smtp_sasl_auth_enable` parent is enabled
- Decrypted username AND password from `system_settings` are non-empty
- `relayhost` child value is non-empty

Per-domain entries are added from `transport` rows where `authentication = 'YES'`. Postfix uses the bracketed `[host]:port` key on the relay host line to match its own bracketed `relayhost` directive — that exact-key match is why the brackets matter.

> **Operational consequence.** Disabling the relay host on this page wipes the relay-host row from `sasl_passwd` but does **not** touch per-domain entries from the Domains page. Conversely, deleting a domain with `authentication = YES` removes only that domain's entry. The two pages compose cleanly via the shared generator.

Credential rotation

To rotate the relay host password without changing anything else:

1. Open **Email Relay > Relay Host**.
2. Type the new password into the **Password** field.
3. Click **Save Settings**.

The handler encrypts the new value into `system_settings`, `generate_sasl_password_transport.cfm` rewrites `sasl_passwd` with the decrypted new value, `postmap` rebuilds the `.db`, and Postfix picks up the change on the next outbound connection (no daemon restart needed — Postfix re-reads hash maps lazily).

Rotating the encryption key itself (`/opt/hermes/keys/hermes.key`) is handled by `rotate_db_credentials.sh` — see that script for the full re-encryption sweep across `system_settings`

and the `transport` table.

Failure semantics

What breaks	What happens
Host fails IPv4/IPv6/FQDN validation	`session.m = 2`, redirect, no DB write
Port empty or non-integer or out of range	`session.m = 3` or `4`, redirect, no DB write
Auth enabled, username blank	`session.m = 5`, redirect, no DB write
Auth enabled, password blank AND `system_settings.value` empty	`session.m = 6`, redirect, no DB write
Auth enabled, password blank but cached cipher present	Cached value is decrypted and reused; no error
Postfix template substitution fails (`generate_postfix_configuration.cfm`)	The error include surfaces the message; the **previous** `main.cf` has already been overwritten with the template copy at that point — recovery is to restore from `main.cf.HERMES` (the write-time backup the same script creates) and re-save
`docker exec hermes_postfix_dkim postfix reload` fails	The next inbound delivery attempt re-reads `main.cf`; no immediate user-facing symptom unless directives changed
`docker exec hermes_postfix_dkim postmap` fails	The new `sasl_passwd` is on disk but the `.db` lags; outbound auth uses the stale `.db` until the next successful postmap

Files and containers touched

Path	Owner	Role
`config/hermes/var/www/html/admin/2/view_relay_host.cfm`	`hermes_commandbox`	Page
`config/hermes/var/www/html/admin/2/inc/get_relay_host_settings.cfm`	`hermes_commandbox`	Load handler + legacy-cred migration
`config/hermes/var/www/html/admin/2/inc/edit_relay_host_settings.cfm`	`hermes_commandbox`	Save handler
`config/hermes/var/www/html/admin/2/inc/generate_sasl_password_transport.cfm`	`hermes_commandbox`	Consolidated `sasl_passwd` generator (shared with Domains page)
`config/hermes/var/www/html/admin/2/inc/generate_postfix_configuration.cfm`	`hermes_commandbox`	Template-to-`main.cf` renderer + `postfix reload`
`/opt/hermes/conf_files/main.cf.HERMES`	`hermes_commandbox`	Postfix template Hermes renders from
`/etc/postfix/main.cf`	`hermes_postfix_dkim` (volume-mounted)	Live Postfix config (regen target)

Path	Owner	Role
`/etc/postfix/main.cf.HERMES`	`hermes_postfix_dkim` (volume-mounted)	Write-time backup created on every regen
`/etc/postfix/sasl_passwd`	`hermes_postfix_dkim` (volume-mounted)	Plain-text credentials file (regen target)
`/etc/postfix/sasl_passwd.db`	`hermes_postfix_dkim`	postmap-built hash database
`/opt/hermes/keys/hermes.key`	`hermes_commandbox`	Symmetric key for AES/Base64 cred encryption
`system_settings` rows `relay_host_username`, `relay_host_password`	`hermes_db_server`	Encrypted credential storage
`parameters` rows: `relayhost`, `smtp_sasl_auth_enable`, `smtp_sasl_password_maps`, `smtp_tls_security_level` (each as `child=2` parent + `child=1` value)	`hermes_db_server`	Postfix directive driver rows

Every shell-out uses `docker exec hermes_postfix_dkim ...` per the standard Hermes pattern; nothing on this page touches the host's own Postfix (there is none).

Related

- Domains — companion page for inbound relay-mode domains. The two pages share `generate_sasl_password_transport.cfm` and together define the entire relay topology.
- Relay Networks — `mynetworks` (which clients are allowed to relay outbound without authentication). Independent of this page but part of the same outbound story.
- Relay Recipients — recipient validation for inbound relay-mode domains; complements Domains.
- SMTP TLS Settings — outbound TLS policy per destination (peer verification, cipher pinning). The TLS Mode dropdown on this page sets the *default* level; per-destination policies override.
- Server Setup — Postfix `myorigin` / `myhostname` and host IP. Defines the identity the relay host sees in EHLO/MAIL FROM.

Revision #14
Created 2026-05-31 12:52:10 UTC by Dino Edwards
Updated 2026-06-13 12:30:10 UTC by Dino Edwards