Domains

Domains

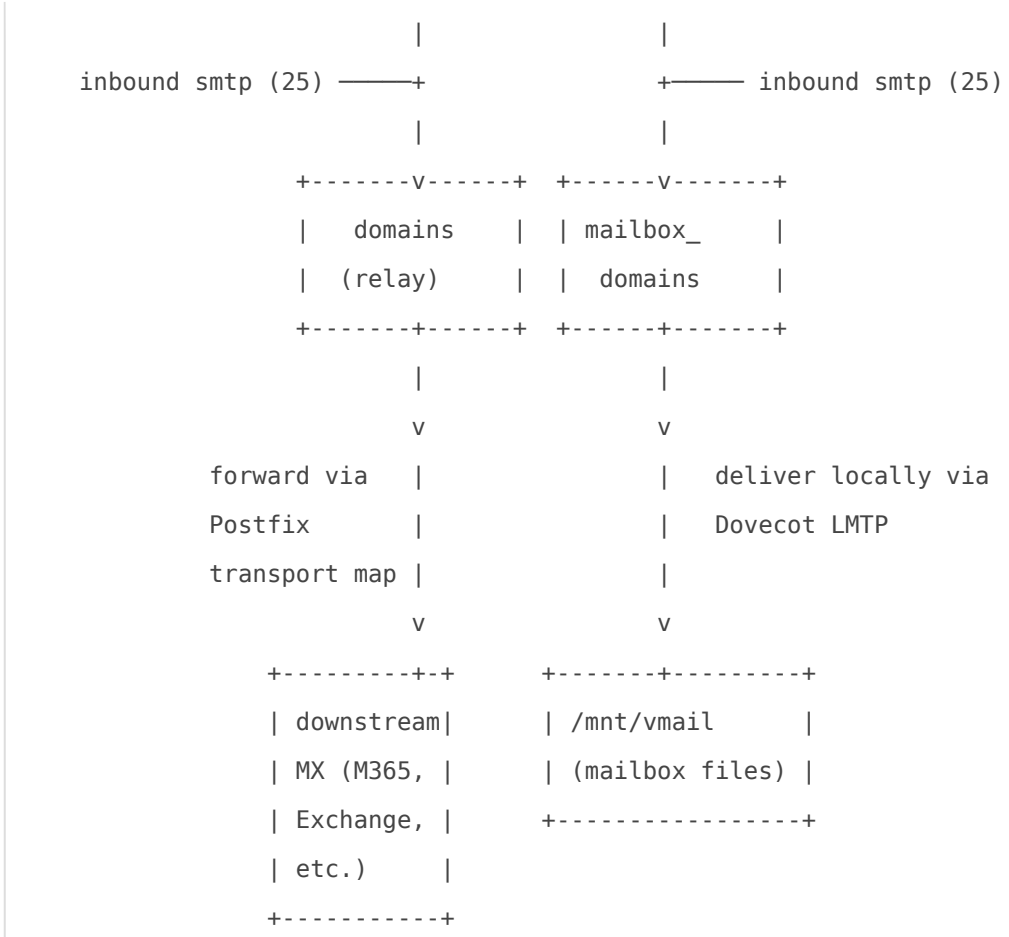
Admin path: **Email Relay > Domains** (`view_domains.cfm`, `inc/domain_add_action.cfm`, `inc/domain_edit_action.cfm`, `inc/domain_delete_action.cfm`, `inc/deletedomain.cfm`, `inc/get_domain_json.cfm`, `inc/generate_transports.cfm`, `inc/generate_relay_domains.cfm`, `inc/generate_sasl_password_transport.cfm`, `inc/generate_postfix_configuration.cfm`, `inc/add_domain_djigzo.cfm`, `inc/delete_domain_djigzo.cfm`).

This page manages the list of **inbound relay domains** — the SMTP domains for which Hermes accepts mail and forwards it to a downstream mail server (Microsoft 365, Exchange, Google Workspace, on-prem Postfix/Dovecot, an internal hub MTA, etc.). Each row in the `domains` table is paired with a `transport` row that tells Postfix where to forward, a `senders` row that flags the domain as a recognized sender, and a `recipients` row that gates whether the domain accepts mail for any address or only addresses on the Relay Recipients allowlist.

This is the inbound counterpart to Relay Host. The two pages together define the **relay topology** half of Hermes: inbound domains here, outbound smarthost there.

> **Not to be confused with Email Server > Domains.** That page is for the **mail-server topology** — domains where Hermes IS the destination MTA and delivers locally to Dovecot mailboxes. It writes to the `mailbox_domains` table, not the `domains` table. The two tables and the two admin pages are separate by design because Hermes supports three topologies (see Hermes topology overview below) and a single deployment can run any combination.

Hermes topology overview



Topology	`domains` rows	`mailbox_domains` rows	This page edits
Relay-only	one or more	none	Yes
Mail-server-only	none	one or more	No — use Email Server > Domains
Hybrid	one or more (forwarded)	one or more (delivered locally)	Yes, for the relay subset

`view_domains.cfm` filters its main query with `WHERE (d.type IS NULL OR d.type = '' OR d.type = 'relay')` so it only shows relay-mode rows. Add Domain writes `type='relay'` explicitly so the row is unambiguously routed to this page.

How a relay domain becomes Postfix config

A single Add Domain submission writes four database rows and regenerates four Postfix maps:

```
form submit  ──► domain_add_action.cfm
                     |
                     |  INSERT transport (domain, transport, dest, port, mx, auth, ...)
                     |  INSERT senders   (sender = domain, action = OK)
                     |  INSERT recipients(recipient = @domain, status = OK|"")
                     |  INSERT domains   (domain, transport_id, senders_id,
                     |                    recipients_id, type='relay')
                     |
                     |  --- regenerate ---
                     v
            generate_transports.cfm        -> /etc/postfix/transport
                                              + postmap (docker exec)
            generate_relay_domains.cfm     -> /etc/postfix/relay_domains
            sync_sasl_parameters.cfm
            generate_sasl_password_transport.cfm
                                           -> /etc/postfix/sasl_passwd
                                              + postmap (docker exec)
            generate_tls_policy.cfm        -> /etc/postfix/tls_policy
                                              + postmap (docker exec)
            generate_postfix_configuration.cfm
                                           -> /etc/postfix/main.cf
                                              + postfix reload (docker exec)
            add_domain_djigzo.cfm          -> registers domain in Ciphermail
                                              (encryption gateway)
```

The same pipeline runs on edit and delete (with the appropriate deletes substituted for inserts). The page deliberately does not expose a "dry-run" — every change to a domain is a config-changing save, and the cascade always runs to completion.

Configuration storage

Table	Role	Notes
`domains`	One row per relay domain	`type` column gates which admin page edits the row (`relay`, NULL/empty = relay; anything else = managed elsewhere). `id`, `transport_id`, `senders_id`, `recipients_id` are the join keys.

Table	Role	Notes
`transport`	One row per domain delivery target	`transport` column holds the Postfix-formatted string (`smtp:[host]:port` or `smtp:host:port` for MX-lookup mode, or `discard:Discard Email Silently`). `authentication = YES` toggles per-domain SASL. `authentication_username` / `authentication_password` are AES/Base64 encrypted with `/opt/hermes/keys/hermes.key`.
`senders`	One row per domain (sender = domain, action = `OK`)	Used by Postfix `smtpd_sender_restrictions` to recognise the domain as a known sender.
`recipients`	One row per domain (recipient = `@domain`, `domain='1'`)	`status = OK` = accept mail for any address (recipient_delivery = ANY). `status = ''` = require an entry in Relay Recipients (recipient_delivery = SPECIFIED). The default `spam_policies` policy is attached so Amavis applies SVF filtering.
`tls_policies`	Optional, one row per domain	Auto-managed: created with `method=encrypt` when **Enforce TLS** is on and Auth is YES; removed when either is turned off. Manually-added policies (different `description`) are untouched.
`dkim_sign`	Optional, one or more rows per domain	DKIM keys live separately; managed under the per-row **DKIM Keys** button (`edit_domain_dkim.cfm`). DKIM badge in the table reports `Active` / `Disabled` / `None` based on `enabled = '1'` counts.

Fields on the page

Add Domain card

Field	Default	Notes
Domain Name	(empty)	Trimmed, lower-cased, validated by the email-trick. Uniqueness checked against `domains.domain` — duplicates rejected with error 12. Stored as-is on the row.

Field	Default	Notes
Delivery Method	`SMTP (Recommended)`	`smtp` forwards via the destination address; `discard` writes `discard:Discard Email Silently` into the transport row and accepts mail only to drop it. Useful for honeypot or sunset domains.
Recipient Delivery	`ANY`	`OK` = accept any recipient at the domain. `""` = SPECIFIED — only addresses listed under Relay Recipients are accepted; everything else is rejected at SMTP time with `relay_recipient_maps`.
Destination Address	`smtp.<domain>` (placeholder)	FQDN or IP of the downstream MX/smarthost. Lower-cased. Required when method = `smtp`.
Port	`25`	Free-text but validated as integer. No range cap on this page (vs. Relay Host's explicit 1–65535) but Postfix will reject out-of-range.
MX Lookup	`NO`	`NO` writes a bracketed transport `smtp:[host]:port` (Postfix skips MX, connects directly). `YES` writes unbracketed `smtp:host:port` (Postfix resolves MX records). MX mode is **automatically forced off** when Auth = YES, because authenticated submission with MX rotation rarely makes sense.
Auth	`NO`	When `YES`, the username/password and Enforce TLS fields reveal.
Destination Username / Password	(empty)	Required when Auth = YES. Encrypted with `/opt/hermes/keys/hermes.key` before write. On Edit, blank password keeps the existing ciphertext.
Enforce TLS	checked	When Auth = YES, auto-inserts a `tls_policies` row with `method=encrypt` and `description='Auto-added: domain requires authentication'`. Manages itself on subsequent edits — turning either off deletes the auto-added row but leaves manually-added TLS policies alone.

Domains table

Sortable, searchable, exportable (copy/CSV/Excel/PDF/print via the DataTables Buttons extension; `stateSave: true` so column ordering and page-size choices persist across reloads). Columns:

Column	Source	Badge logic
Domain	`domains.domain`	Plain text
Delivery	`transport.method`	`Discard` (warning) or `SMTP` (success)
Destination	`transport.destination`	Dash for discard rows
Port	`transport.port`	Dash for discard
MX	`transport.mx`	Dash for discard
Recipients	`recipients.status`	`Any` (info) when `OK`, `Specified` (secondary) otherwise
Auth	`transport.authentication`	`YES` (warning) or `NO` (secondary)
DKIM	aggregated from `dkim_sign`	`Active` when any enabled key, `Disabled` when keys exist but all disabled, `None` when no keys
TLS	derived from `tls_policies.domain` join	`YES` (success) when a policy exists for the domain, `NO` (secondary) otherwise
Actions	—	Edit (opens modal), DKIM Keys (→ `edit_domain_dkim.cfm`), Delete (opens confirm modal)

Edit Domain modal

Opens via `openEditModal(id)` which fetches `./inc/get_domain_json.cfm` over AJAX, hydrates the form fields, then reveals the modal body. **Domain Name is read-only on edit** — changing a domain name across `domains` / `transport` / `senders` / `recipients` / `dkim_sign` / `tls_policies` is risky enough that the page enforces add-and-delete instead. Every other field is editable.

Blank password keeps the existing ciphertext (the masked hint beneath the input shows `Current: abcd*****` when a stored value exists).

Delete Domain modal

Confirms the destructive action. The handler (`deletedomain.cfm`) runs four dependency checks before allowing the delete:

Check	If it returns rows →
Relay Recipients still pointing at the domain (`recipients.recipient LIKE '%domain%' AND domain IS NULL`)	Error 1, abort

Check	If it returns rows →
Virtual Recipients referencing the domain (`virtual_recipients.virtual_address LIKE '%domain%'`)	Error 2, abort
Postmaster address using the domain (`system_settings.postmaster LIKE '%domain%'`)	Error 3, abort
DKIM keys for the domain (`dkim_sign.domain LIKE '%domain%'`)	Error 4, abort

If all four pass, the handler deletes from `domains`, `transport`, `senders`, and `recipients` (the four rows linked at creation), clears the `tls_policies` row for the domain, removes the Ciphermail registration, and regenerates all Postfix maps.

> **Operational consequence.** The dependency checks force a bottom-up cleanup. To remove a domain you must first delete its recipients, its DKIM keys, and reassign the system postmaster. This is intentional — Hermes will not silently strand referencing rows, and the order also prevents you from losing in-flight mail for active recipients.

Per-domain auth vs. relay host auth

Per-domain authentication on this page is **separate from and additive to** the global Relay Host SASL on the Relay Host page. Both pages write into the same `/etc/postfix/sasl_passwd` file via the shared `generate_sasl_password_transport.cfm` generator:

```
# /etc/postfix/sasl_passwd  (regenerated on every save on either page)
[smtp.upstream-isp.com]:587  globaluser:globalpass    <-- Relay Host page
[mx.partner-a.com]:25        partner_a_user:secret1   <-- Domains page (per-domain)
[mx.partner-b.com]:25        partner_b_user:secret2   <-- Domains page (per-domain)
```

A domain with per-domain auth will use **its own** credentials when Postfix forwards to its destination. The global relay host credentials are used only when a message has no matching per-domain transport (typical for outbound mail to arbitrary recipients).

> **By design.** The error code 15 (`Cannot enable Destination Authentication when Relay Host is enabled`) is reserved in the page's alert table but not currently raised by the action handlers — historically the two auth modes were considered mutually exclusive, but the consolidated SASL generator handles both cleanly, so the constraint was relaxed. The alert is kept in case a future tightening reintroduces the rule.

Discard delivery

Setting Delivery Method to `discard` writes `discard:Discard Email Silently` into the transport. Postfix accepts mail for the domain (passing SMTP-time checks and the content filter), then drops it on the floor — no NDR, no bounce, no forwarding attempt. Useful for:

- Sunset domains that should not generate backscatter
- Honeypot domains for spam-trap analysis
- Catching mail to a domain you control while migration is in progress and you don't want it bouncing

The destination/port/MX/auth/TLS fields are hidden in the UI when discard is selected because none of them apply.

Failure semantics

What breaks	What happens
Domain name empty	`session.m = 10`, redirect, no DB write
Domain name fails email-trick validation	`session.m = 11`, redirect, no DB write
Domain name already exists in `domains`	`session.m = 12`, redirect, no DB write
Delivery method not in `smtp,discard`	`session.m = 20`, redirect, no DB write
Destination address blank when method = smtp	`session.m = 13`, redirect, no DB write
Port not an integer	`session.m = 14`, redirect, no DB write
Auth = YES but username blank	`session.m = 16`, redirect, no DB write
Auth = YES but password blank AND no cached cipher	`session.m = 17`, redirect, no DB write
Delete blocked by dependency check	One of `session.m = 1..4` per the table above, redirect, no DB write

What breaks	What happens
`postmap` of `transport` / `sasl_passwd` / `tls_policy` fails	New map file is on disk but `.db` lags; next mail flow uses stale data until next successful postmap
`postfix reload` fails	Live config keeps the previous values; reload error is in container logs
`add_domain_djigzo.cfm` errors during Ciphermail registration	Domain row is already in the DB; encryption gateway will not know about the domain until the next manual sync. Re-saving the domain triggers a fresh registration attempt.

Files and containers touched

Path	Owner	Role
`config/hermes/var/www/html/admin/2/view_domains.cfm`	`hermes_commandbox`	Page + Add/Edit/Delete modals
`config/hermes/var/www/html/admin/2/inc/domain_add_action.cfm`	`hermes_commandbox`	Add handler
`config/hermes/var/www/html/admin/2/inc/domain_edit_action.cfm`	`hermes_commandbox`	Edit handler
`config/hermes/var/www/html/admin/2/inc/domain_delete_action.cfm`	`hermes_commandbox`	Delete dispatch (thin wrapper)
`config/hermes/var/www/html/admin/2/inc/deletedomain.cfm`	`hermes_commandbox`	Delete handler with dependency checks
`config/hermes/var/www/html/admin/2/inc/get_domain_json.cfm`	`hermes_commandbox`	AJAX hydrator for the Edit modal
`config/hermes/var/www/html/admin/2/inc/generate_transports.cfm`	`hermes_commandbox`	Rewrites `/etc/postfix/transport` + postmap
`config/hermes/var/www/html/admin/2/inc/generate_relay_domains.cfm`	`hermes_commandbox`	Rewrites `/etc/postfix/relay_domains`
`config/hermes/var/www/html/admin/2/inc/generate_sasl_password_transport.cfm`	`hermes_commandbox`	Shared `sasl_passwd` generator (also used by Relay Host)
`config/hermes/var/www/html/admin/2/inc/generate_tls_policy.cfm`	`hermes_commandbox`	Rewrites `/etc/postfix/tls_policy` + postmap
`config/hermes/var/www/html/admin/2/inc/generate_postfix_configuration.cfm`	`hermes_commandbox`	Template-to-`main.cf` renderer + `postfix reload`
`config/hermes/var/www/html/admin/2/inc/add_domain_djigzo.cfm` / `delete_domain_djigzo.cfm`	`hermes_commandbox`	Ciphermail (djigzo) domain registration
`/etc/postfix/transport` + `.db`	`hermes_postfix_dkim`	Per-domain transport map (regen target)
`/etc/postfix/relay_domains`	`hermes_postfix_dkim`	List of domains Postfix accepts mail for (regen target)

Path	Owner	Role
`/etc/postfix/sasl_passwd` + `.db`	`hermes_postfix_dkim`	Consolidated SASL credentials (regen target)
`/etc/postfix/tls_policy` + `.db`	`hermes_postfix_dkim`	Per-destination TLS policy (regen target)
`/etc/postfix/main.cf`	`hermes_postfix_dkim`	Live Postfix config (re-rendered on every save)
`/opt/hermes/keys/hermes.key`	`hermes_commandbox`	Symmetric key for AES/Base64 cred encryption
`domains`, `transport`, `senders`, `recipients`, `tls_policies`, `dkim_sign`	`hermes_db_server`	The relay-domain row group

Every shell-out uses `docker exec hermes_postfix_dkim ...` per the standard Hermes pattern.

Related

- Relay Host — outbound smarthost; the page's twin. Shares the `sasl_passwd` generator and is part of the same relay topology.
- Relay Recipients — recipient allowlist used when a domain's Recipient Delivery is set to `SPECIFIED`. Required reading if you tighten recipient validation for a domain.
- Virtual Recipients — alias and catch-all mappings (`alias@dom → real@dom`). Independent of this page but domain deletes block when virtual rows reference the domain.
- Relay Networks — `mynetworks` (which clients may relay outbound without authentication). The networks that hold the per-domain submission clients live here.
- SMTP TLS Settings — manages per-destination TLS policies (the Enforce TLS checkbox on this page is a shortcut into the same table).
- Email Server > Domains — the separate page for mail-server-topology domains, backed by `mailbox_domains`. **Do not confuse with this page.**

Revision #8
Created 2026-05-31 12:52:09 UTC by Dino Edwards
Updated 2026-05-31 14:01:11 UTC by Dino Edwards