Mailboxes

Mailboxes

Admin path: **Email Server > Mailboxes** (`view_mailboxes.cfm`, `add_mailbox.cfm`, `inc/add_mailbox_action.cfm`, `inc/edit_mailbox_action.cfm`, `inc/edit_mailbox_encryption_action.cfm`, `inc/edit_mailbox_access_control_action.cfm`, `inc/delete_mailbox_action.cfm`, `inc/get_mailbox_json.cfm`, `inc/ldap_add_user_mailbox.cfm`, `inc/ldap_add_user_mailbox_remoteauth.cfm`, `inc/ldap_add_user_groups_mailbox.cfm`, `inc/ldap_delete_user_mailbox.cfm`, `inc/nextcloud_provision_user.cfm`, `inc/signature_regen_map.cfm`, `inc/send_mailbox_welcome_email.cfm`, `inc/send_mailbox_welcome_email_remoteauth.cfm`, `inc/admin_resend_mobile_setup_action.cfm`, `inc/rotate_nc_password_action.cfm`).

This page manages **individual mailboxes** inside the mail-server topology — one row per address in the `mailboxes` table, joined to a `recipients` row that carries the per-recipient policy stack (SVF policy, encryption flags, S/MIME certs, PGP keyrings, 2FA enforcement, auth type). A mailbox is the local-delivery counterpart to a Relay Recipient — same `recipients` row shape, different `recipient_type` column value (`'mailbox'` vs `'relay'`) and a sibling row in `mailboxes` that gives Dovecot a userdb entry.

This is the **per-mailbox** half of the mail-server topology. Pairs with Domains (the domains those mailboxes live under and inherit defaults from), Settings (global Dovecot config and quota warning thresholds), and the per-address feature pages: Aliases, Shared Mailboxes, Mailbox Rules, and per-mailbox app passwords.

Mailbox vs Alias vs Shared Mailbox vs Relay Recipient

Four address concepts share the namespace under a mailbox domain; keep them straight:

Concept	Stored in	Has Dovecot mailbox?	Local sign-in?

Mailbox (this page)	`mailboxes` (`mailbox_type='user'`) + `recipients` (`recipient_type='mailbox'`)	Yes — Dovecot LMTP delivery to `/mnt/vmail/<domain>/<user>/`	Yes — IMAP/POP3/Submission, web portal, Nextcloud
Alias	`mailbox_aliases`	No — forwards to one or more mailboxes (or silently discards)	No
Shared Mailbox	`mailboxes` (`mailbox_type='shared'`) + `shared_mailbox_permissions`	Yes — but accessed via Dovecot ACL from owner mailboxes	No direct login — owners reach it from their own session
Relay Recipient	`recipients` (`recipient_type='relay'`)	No — forwarded to a downstream MX	Yes for web portal / Submission (via app passwords)

See Aliases and Shared Mailboxes for the alias and shared variants, and Email Relay > Relay Recipients for the relay-topology equivalent.

What a Mailbox row carries

```
mailboxes table  (Dovecot userdb-driving row)
├── id, domain_id          -> joins to domains where type='mailbox'
├── username               full email (e.g. jsmith@company.com)
├── name                   display name
├── quota                  per-mailbox quota in BYTES (DB stores bytes;
│                          UI shows GB)
├── active                 1/0 — Dovecot rejects auth when 0
├── nextcloud_enabled      per-mailbox Nextcloud flag
├── mailbox_type           'user' | 'shared'
└── first_name, last_name, title, phone, mobile, department
                           (Pro Personal Information for signature
                            substitution)

recipients table  (paired row, recipient_type='mailbox')
├── recipient              same as mailboxes.username
├── policy_id              -> spam_policies (SVF policy)
├── auth_type              'local' | 'remote'
├── remoteauth_domain      NULL if local; mapping key if remote
├── enforce_mfa            0 | 1 (admin policy)
├── pdf_enabled / smime_enabled / pgp_enabled / digital_sign
└── (cert + keyring slots populated lazily by cert_generation_queue)
```

Side tables linked at create-time or lazily:

Table	Role
`user_settings`	`report_enabled` (quarantine notifications), `train_bayes`, `download_msg`, `timezone`, `ldap_username`
`maddr`	Amavis address index — required for the user portal session machinery
`sender_login_maps`	Postfix `smtpd_sender_login_maps` entry — permits the mailbox owner to send AS their own address from Submission
`app_passwords`	Per-mailbox application passwords (Argon2-hashed) for IMAP/SMTP/CalDAV/CardDAV/Nextcloud. The Add flow creates an initial `Hermes System` app password used by the Nextcloud Mail auto-profile.
`recipient_certificates`, `recipient_keystores`	S/MIME cert + PGP keyring slots (lazy — populated by the queue)
`cert_generation_queue`	Async S/MIME + PGP generation jobs
`mailbox_aliases`	If any aliases exist pointing at the mailbox
`shared_mailbox_permissions`	If the mailbox is granted access to any shared mailbox

Add Mailbox — `add_mailbox.cfm`

Single-mailbox page (not a bulk form). The admin selects a target domain, fills in the address local-part + display name + quota + auth mode + per-recipient stack (policy, notifications, encryption flags), and submits. `add_mailbox_action.cfm` then runs the full creation pipeline:

```
form submit  ──► add_mailbox_action.cfm
                    |
                    |  validate domain + email + auth mode
                    |  duplicate-check against recipients, mailboxes,
                    |     mailbox_aliases, virtual_recipients
                    |
                    |  --- write DB ---
                    |  INSERT recipients   (recipient_type='mailbox', policy,
                    |                       auth_type, remoteauth_domain,
                    |                       enforce_mfa, encryption flags)
                    |  INSERT maddr        (Amavis address index)
                    |  INSERT user_settings(notifications, train_bayes,
                    |                       download_msg, timezone)
```

```
|  INSERT mailboxes    (domain_id, username, name,
|                       quota, active=1, nextcloud_enabled)
|  INSERT sender_login_maps (permits send-as)
|
|  --- LDAP ---
|  auth_type=local  : ldap_add_user_mailbox.cfm
|                     (random userPassword, will be reset)
|  auth_type=remote : ldap_add_user_mailbox_remoteauth.cfm
|                     (no userPassword; seeAlso pointer to
|                     upstream DN, associatedDomain set to
|                     remoteauth_domain)
|  ldap_add_user_groups_mailbox.cfm
|    -> cn=mailboxes,ou=groups,dc=hermes,dc=local
|    -> cn=one_factor OR cn=two_factor (per enforce_mfa)
|  if NC enabled:
|    -> cn=nextcloud,ou=groups,dc=hermes,dc=local
|
|  --- Nextcloud (if NC enabled) ---
|  nextcloud_provision_user.cfm
|    -> occ user:add with RANDOM internal password
|       (not the user's real password — they reach NC
|        via OIDC; the internal password is defense-in-depth)
|    -> occ user:setting to pre-fill email + display name
|    -> create initial Hermes System app password
|       (used by the Mail app account profile)
|    -> create Nextcloud Mail account profile
|       (IMAP+SMTP credentials pre-wired)
|
|  --- lazy cert / keyring queue ---
|  if smime_enabled : INSERT cert_generation_queue (smime)
|  if pgp_enabled   : INSERT cert_generation_queue (pgp)
|
|  --- send welcome ---
|  local  : send_mailbox_welcome_email.cfm
|           (password-reset link, 30-min expiry)
|  remote : send_mailbox_welcome_email_remoteauth.cfm
|           (sign-in with organization password)
|
|  --- signature map ---
|  if Pro: signature_regen_map.cfm
```

```
                    |    -> rebuild body milter signature_by_sender map
                    |    -> rebuild sender_data.json
                    |
                    v
            cflocation -> view_mailboxes.cfm with session.m = 1
```

Dovecot mailbox directories on `/mnt/vmail/<domain>/<user>/` are NOT pre-created. Dovecot auto-creates the directory tree on first LMTP delivery or first IMAP login. The mailbox row alone is enough.

Password handling

Local-auth mailboxes:

- The admin enters a password on the Add form (12-char minimum, no special chars, checked against the HIBP "Have I Been Pwned" k-anon range API).
- The same password is stored in three places, each hashed by its consuming subsystem: OpenLDAP `userPassword` (Argon2id via `slappasswd -o module-load=argon2.la -h {ARGON2}`), `app_passwords` initial `Hermes System` row (Argon2id), and the Nextcloud internal user password (only on the NC side, set by `occ user:add` — but immediately replaced with a random value by `nextcloud_provision_user.cfm`, see Phase 1 of #197).
- Argon2id hashing uses the canonical `docker run --rm authelia/authelia:<version> authelia crypto hash generate argon2 --password <value>` pattern. No host-side `argon2` binary required.

RemoteAuth mailboxes (`auth_type='remote'`):

- No password is captured. The local LDAP entry has no `userPassword`; bind goes through the OpenLDAP remoteauth overlay to the upstream AD/LDAP per the `remoteauth_domain` mapping (see LDAP RemoteAuth).
- `app_passwords` still issues Hermes-side credentials for IMAP/SMTP/DAV — these remain Hermes-owned regardless of upstream password rotation.

The Mailboxes table

Single DataTable with 21 columns and an optional Domain filter dropdown above (populated only when ≥1 domain has mailboxes). Per-row columns:

Column	Source	Notes

Actions	—	Dropdown: Edit Options, Edit Encryption, Reset 2FA Devices, Manage App Passwords (→ `view_mailbox_app_passwords.cfm`), Send Mobile Setup Profile, Rotate NC Internal Password (only if NC enabled), Delete
S/MIME	link to `view_recipient_certificates.cfm?type=1&id=...`	Per-mailbox cert manager
PGP	link to `view_recipient_keyrings.cfm?type=1&id=...`	Per-mailbox keyring manager
Email	`mailboxes.username`	Full address
Display Name	`mailboxes.name`	
Domain	join on `domains.domain`	
Quota	`mailboxes.quota / 1024 / 1024 / 1024`	Rendered in GB
Auth	`recipients.auth_type`	`LOCAL` badge or `REMOTE` badge (tooltip shows `remoteauth_domain`)
2FA	LDAP `cn=two_factor` + `enforce_mfa`	Two independent pills — see Two-pill 2FA column
Policy	`spam_policies.policy_name`	
Notifications, Train Bayes, Download Msgs	`user_settings.*`	`YES` (success) / `NO` (secondary)
PDF / S/MIME / PGP Encrypt, Sign All	`recipients.*`	`YES` / `NO`
S/MIME Cert, PGP Keyring	join against `recipient_certificates`, `recipient_keystores`	`YES` (green) if a cert/keyring exists; spinner badge if a job is `pending` / `processing` in `cert_generation_queue`
Nextcloud	`mailboxes.nextcloud_enabled`	`YES` / `NO`
Status	`mailboxes.active`	`Active` (success) / `Inactive` (danger) — Dovecot rejects auth when `active=0`

The query filters `WHERE m.mailbox_type = 'user'` so shared mailboxes do not appear here — they have their own page at Shared Mailboxes.

Two-pill 2FA column

Same two-orthogonal-states model as Email Relay > Relay Recipients § Two-pill 2FA column. Admin enforcement (`recipients.enforce_mfa`) and user enrollment (`cn=two_factor` LDAP membership) are

decoupled, so the cell can show **Enrolled**, **Required**, both, or em-dash.

The page pulls all `cn=two_factor` group members in a single `ldapsearch` (via `docker exec hermes_ldap ldapsearch -Y EXTERNAL`) once per render, then each row checks for its DN substring in the result — avoids an N+1 LDAP roundtrip storm.

Edit Options modal — AJAX pre-fill

Opens via `loadEditModal(mailboxId)`, hits `inc/get_mailbox_json.cfm` over AJAX, hydrates every field with the mailbox's current values. Unlike the Relay Recipients bulk-edit foot-gun, this modal is **always single-mailbox** — there is no bulk Edit Options on this page.

Fields:

Section	Notes
Email Address	Read-only
Display Name	`mailboxes.name`
Personal Information *(collapsible, Pro only)*	`first_name`, `last_name`, `title`, `phone`, `mobile`, `department`. Used by signature placeholder substitution (`{{user.first_name}}`, `{{user.title}}`, etc.) and by department-based signature resolution. Department field uses a typeahead datalist built from the domain's existing departments via `inc/get_dept_options.cfm`. Community inputs are HTML-disabled and the action handler skips the UPDATE on Community so values survive a Pro→Community downgrade.
Mailbox Quota (GB)	Per-mailbox override of the domain default
Status	`Active` / `Inactive`
SVF Policy	Populated from `spam_policies` where `custom='1' OR default_policy='1'`
Quarantine Notifications	`user_settings.report_enabled`
Train Bayes Filter	`user_settings.train_bayes` — with prominent warning that improperly-trained Bayes affects ALL recipients
Download Messages from User Portal	`user_settings.download_msg` — with malware-risk warning
Nextcloud Webmail	`mailboxes.nextcloud_enabled`. **Enabling for an existing user requires a new password** (NC needs the password to provision the Mail app profile) — error 51 if the admin enables NC without setting a password. **Disabling** shows a `Keep Nextcloud account data` checkbox that gates whether the NC user account and data are preserved or permanently deleted.

Section	Notes
Two-Factor Authentication	`recipients.enforce_mfa`. When enabled, the user's web portal access becomes restricted to Account Settings, My App Passwords, Set Up Your Devices, and Webmail & Apps until they enroll. Email/calendar/contacts keep working throughout — only the web portal is gated. The 0→1 transition triggers an LDAP group move from `cn=one_factor` to `cn=two_factor` so Authelia challenges them on next sign-in.
Timezone	`user_settings.timezone` (Java `ZoneId` list). Used for the vacation auto-reply schedule and dashboard timestamps.
Authentication Type	Read-only — `local` or `remote`
Change Password *(local auth only)*	Optional. Minimum 12 chars, no special chars, HIBP-checked. Blank keeps the current password.

Edit Encryption modal

Per-mailbox encryption flags (`pdf_enabled`, `smime_enabled`, `digital_sign`, `pgp_enabled`) plus the cert/keyring generation parameters (CA, validity, key size, algorithm, PGP key length). Submit queues async cert + keyring generation into `cert_generation_queue` if a flag flips on and no existing cert/keyring is present — same lazy-queue pattern as Relay Recipients.

Reset 2FA Devices modal

Single-purpose modal that clears Authelia TOTP and WebAuthn device registrations via `docker exec hermes_authelia authelia storage user totp delete` and `... webauthn delete --all`. Two modes:

Mode	What it does
Default	Deletes TOTP + WebAuthn devices. User stays under 2FA enforcement and re-registers on next sign-in. "User lost their phone" recovery.
Nuclear *(checkbox)*	Also moves the user from `cn=two_factor` back to `cn=one_factor`. Admin override; if `enforce_mfa` is still 1 the next Edit Options save will reverse the LDAP move.

> **Does not affect Duo Push.** Duo enrollments live on Duo's cloud servers. Use the Duo Admin Console.

Send Mobile Setup Profile

Per-mailbox action that emails the user a signed iOS / iPadOS mobileconfig profile pre-wired with IMAP + Submission + CalDAV + CardDAV + the appropriate account name and email. The link in the email expires in 30 minutes and works only once.

Handler is `inc/admin_resend_mobile_setup_action.cfm`. The mobileconfig generator itself is shared with the user-portal Setup Your Devices wizard.

Rotate NC Internal Password

Visible only when `mailboxes.nextcloud_enabled = 1`. Generates a new random local password for the Nextcloud user via `docker exec hermes_nextcloud occ user:resetpassword` and the displayed value is **never shown** — it is purely defense-in-depth.

Background: the Nextcloud internal password was historically set to the user's real password, which silently allowed CalDAV/CardDAV to accept the org password and defeat the app-password isolation boundary (closed in #197 Phase 1). The internal password is now random and unused by anything user-facing — users reach NC via OIDC, and DAV/IMAP go through app passwords. This admin action lets the admin re-randomize on demand without touching the user's actual credentials.

Delete

Cascading delete that mirrors the create pipeline in reverse, with the same cleanup discipline as Relay Recipients (the goal is zero-orphan rows). Per mailbox:

```
For the selected mailbox ID:
1. Read mailboxes row + user_settings (for ldap_username)
2. Remove LDAP from cn=mailboxes  (before delete_internal_recipients
                                   runs ldap_delete_user_relay)
3. (If NC enabled) Remove from cn=nextcloud LDAP group
4. delete_internal_recipients.cfm
     - docker exec hermes_authelia authelia storage user totp delete
     - docker exec hermes_authelia authelia storage user webauthn delete --all
     - LDAP user entry delete
     - cert_generation_queue cancel + recipient_certificates clear
     - recipient_keystores + Ciphermail keystore clear
```

```
     - wblist, mailaddr, password_reset_requests cancel
5. DELETE mailboxes WHERE id = <id>
6. DELETE sender_login_maps WHERE login_user = <email>
7. DELETE user_settings (if not already cleared by step 4)
8. Re-sync any shared mailbox vfile ACLs the user was a member of
   (so the deleted user vanishes from sharer lists)
9. DELETE app_passwords WHERE username = <email>
10. (If NC enabled AND admin did NOT check "Keep Nextcloud data")
    docker exec hermes_nextcloud occ user:delete <user>
11. signature_regen_map.cfm (rebuild body milter map without this user)
```

The Nextcloud user/data preservation is opt-in via the `Keep Nextcloud account data` checkbox surfaced when toggling NC off in Edit Options — deletion from this page asks the same question.

> **Dovecot mailbox data on disk is NOT deleted.** `/mnt/vmail/<domain>/<user>/` survives the delete. If you intend to permanently retire the mailbox, remove the directory from the host after the delete completes. This matches the per-domain behavior on Domains.

Local-auth vs RemoteAuth — the credential split

Identical model to relay recipients. See Email Relay > Relay Recipients § Local-auth vs RemoteAuth and Authentication Settings for the full four-credential architecture.

For mailboxes specifically: app passwords are always Hermes-issued regardless of `auth_type`. RemoteAuth mailbox users' upstream directory password is exposed only to the web gate (via the LDAP overlay's pass-through bind) — never to Dovecot or the Nextcloud Mail profile.

> **Known forward-looking gap (#102).** RemoteAuth mapping deletion validation in `view_remoteauth.cfm` and `edit_remoteauth_mapping.cfm` currently only checks `system_users` and `recipients`. When RemoteAuth-for-mailboxes activity grows, the validation must add a third query against `mailboxes` so an in-use mapping cannot be stranded. See LDAP RemoteAuth § Deletion validation.

Failure semantics

What breaks	What happens
Quota not a positive number	`session.m = 15`, redirect, no DB write
Missing required form fields	`session.m = 20`, redirect, no DB write
Mailbox not found (Edit/Delete)	`session.m = 21`, redirect, no DB write
Password under 12 characters	`session.m = 22`, redirect, no DB write
Password found in HIBP breach	`session.m = 99`, redirect, no DB write
HIBP API unavailable	`session.m = 100`, warning banner, mailbox still rejected (fail-closed)
Enabling NC for existing user without setting a password	`session.m = 51`, redirect, no DB write
Mobile setup profile email failed but profile staged	`session.m = 83`, warning banner, link still works
Duplicate email (against recipients / mailboxes / aliases / virtual_recipients)	redirect to `add_mailbox.cfm` with appropriate alert
LDAP add fails after DB inserts succeed	DB row exists; subsequent IMAP/SMTP login fails until the LDAP entry is created (admin can re-save Edit Options or delete and re-add)
Nextcloud `occ user:add` fails	Mailbox creation succeeds; NC toggle effectively becomes a no-op until re-toggled
`cert_generation_queue` row stuck in `processing`	Surfaces in the Add Recipient / Add Mailbox alert banner via Pending S/MIME or PGP generation; retry via the same Retry Failed Jobs button on the Relay page

Files and containers touched

Path	Owner	Role
`config/hermes/var/www/html/admin/2/view_mailboxes.cfm`	`hermes_commandbox`	Main page + Edit Options / Edit Encryption / Reset 2FA / Delete modals
`config/hermes/var/www/html/admin/2/add_mailbox.cfm`	`hermes_commandbox`	Add page (single mailbox, full per-recipient stack)
`config/hermes/var/www/html/admin/2/inc/add_mailbox_action.cfm`	`hermes_commandbox`	Add handler — orchestrates DB + LDAP + NC + cert queue + welcome email
`config/hermes/var/www/html/admin/2/inc/edit_mailbox_action.cfm`	`hermes_commandbox`	Edit Options handler

Path	Owner	Role
`config/hermes/var/www/html/admin/2/inc/edit_mailbox_encryption_action.cfm`	`hermes_commandbox`	Edit Encryption handler + cert/keyring queue insertion
`config/hermes/var/www/html/admin/2/inc/edit_mailbox_access_control_action.cfm`	`hermes_commandbox`	Reset 2FA Devices handler (TOTP + WebAuthn clear + optional nuclear move)
`config/hermes/var/www/html/admin/2/inc/delete_mailbox_action.cfm`	`hermes_commandbox`	Delete cascade
`config/hermes/var/www/html/admin/2/inc/get_mailbox_json.cfm`	`hermes_commandbox`	AJAX hydrator for Edit Options
`config/hermes/var/www/html/admin/2/inc/get_dept_options.cfm`	`hermes_commandbox`	Per-domain department datalist (typeahead)
`config/hermes/var/www/html/admin/2/inc/ldap_add_user_mailbox.cfm` / `ldap_add_user_mailbox_remoteauth.cfm`	`hermes_commandbox`	Local / remote LDAP entry creation
`config/hermes/var/www/html/admin/2/inc/ldap_add_user_groups_mailbox.cfm`	`hermes_commandbox`	Group assignment: `cn=mailboxes`, `cn=one_factor` / `cn=two_factor`, `cn=nextcloud`
`config/hermes/var/www/html/admin/2/inc/ldap_delete_user_mailbox.cfm`	`hermes_commandbox`	LDAP entry removal on delete
`config/hermes/var/www/html/admin/2/inc/nextcloud_provision_user.cfm`	`hermes_commandbox`	NC user creation, random internal password, Mail app profile, initial app password
`config/hermes/var/www/html/admin/2/inc/rotate_nc_password_action.cfm`	`hermes_commandbox`	On-demand NC internal password rotation
`config/hermes/var/www/html/admin/2/inc/admin_resend_mobile_setup_action.cfm`	`hermes_commandbox`	Mobile setup profile generation + email
`config/hermes/var/www/html/admin/2/inc/send_mailbox_welcome_email.cfm` / `send_mailbox_welcome_email_remoteauth.cfm`	`hermes_commandbox`	Welcome email (local: reset link; remote: org-password instructions)
`config/hermes/var/www/html/admin/2/inc/signature_regen_map.cfm`	`hermes_commandbox`	Body milter `signature_by_sender` map + `sender_data.json` rebuild
`mailboxes`, `recipients`, `user_settings`, `maddr`, `sender_login_maps`, `app_passwords`, `recipient_certificates`, `recipient_keystores`, `cert_generation_queue`, `mailbox_aliases`, `shared_mailbox_permissions`, `wblist`, `password_reset_requests`	`hermes_db_server`	The mailbox row group
`cn=<user>,ou=users,dc=hermes,dc=local`	`hermes_ldap`	Per-mailbox LDAP entry (with `userPassword` Argon2id hash for local-auth or `seeAlso` for remote)

Path	Owner	Role
`cn=mailboxes`, `cn=one_factor` / `cn=two_factor`, `cn=nextcloud` in `ou=groups`	`hermes_ldap`	Group memberships set at create-time
`/mnt/vmail/<domain>/<user>/`	`hermes_dovecot` (mounted)	Mailbox directory tree — auto-created on first LMTP delivery / IMAP login; NOT removed on delete
Authelia `totp_configurations` + `webauthn_devices`	`hermes_authelia` storage backend	Cleared on delete + Reset 2FA Devices
`hermes_nextcloud` container	—	`occ user:add` / `user:delete` / `user:resetpassword` / `group:add` (the latter from Domains)

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

Related

- Domains — mailbox-domain registration. A mailbox is meaningless without a domain row of `type='mailbox'`. Domain defaults (default quota, Nextcloud enabled, 2FA required) pre-fill the Add Mailbox form for new mailboxes; toggling the per-domain default does NOT cascade to existing mailboxes.
- Settings — global Dovecot config: TLS profile, compression, encryption at rest, quota warning thresholds. The warning thresholds measure against the per-mailbox quota set here.
- Aliases — alias addresses that resolve to mailboxes (with optional silent-discard mode). Add aliases AFTER the target mailbox exists.
- Shared Mailboxes — shared-namespace mailboxes with per-user ACLs. Distinct from regular mailboxes — they live in the same `mailboxes` table but with `mailbox_type='shared'` .
- Mailbox Rules — server-side Sieve rules per mailbox. Sieve is always-on at the protocol level via Settings.
- SAN Management — SAN prefixes that gate client auto-discovery for every mailbox domain.
- Authentication Settings — Authelia config, OIDC, the four-credential architecture (web vs IMAP/SMTP vs DAV vs Nextcloud) that mailbox app passwords slot into.
- LDAP RemoteAuth — required prerequisite for `auth_type='remote'` mailboxes. The Add form surfaces only mappings with `enabled=1`.
- Password Resets — admin-driven password reset for local-auth mailboxes (the user-facing flow uses the link in the welcome email).

- System Users — distinct from mailboxes; covers console admins / readers, which use the `system_users` table rather than `mailboxes`.
- Email Relay > Relay Recipients — the relay-topology equivalent. Mailbox users are delivered locally; relay recipients are forwarded downstream. Don't confuse the two.
- Organizational Signatures *(Pro)* — consumer of the Personal Information fields on the Edit Options modal (plus the domain's Organization Information fields).

Revision #48
Created 2026-05-31 12:52:15 UTC by Dino Edwards
Updated 2026-06-20 13:33:08 UTC by Dino Edwards