



The enterprise mail platform you own, end to end.

Whitemail is a high-availability mail and groupware platform that runs entirely on your infrastructure — mail, calendars, contacts, chat, security filtering, and a full web administration console. No per-mailbox cloud fees, no external dependencies, air-gap ready.

15,000+

accounts per cluster

5 tiers

every layer redundant

3x

data replication on
distributed storage

100%

on-premises · air-gap
capable

WHY WHITEMAIL

Full ownership, zero cloud lock-in

Every component runs on your servers or private cloud. The signed offline installer bundles all packages — nothing is pulled from the internet, so fully air-gapped sites install and update the same way as connected ones.

High availability by design

Every tier is redundant: floating VIPs, health-checked frontends, mailbox backends sized to absorb node loss, replica-3 distributed storage, and a synchronous database cluster. A single node failure is a non-event.

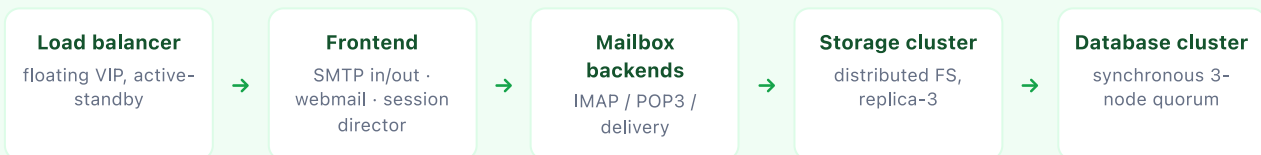
Complete groupware, one login

Webmail, shared calendars and tasks, contacts, in-org chat, file sharing, and mobile sync via Microsoft ActiveSync — plus public folders, notes, and shared address books across the organisation.

One control plane for everything

The Web Admin console manages domains, accounts, services, queues, quarantine, tracking, reports, and logs across every node — with role-based access, two-factor login, and an append-only audit trail.

ARCHITECTURE AT A GLANCE



A session director pins each user to one mailbox backend, eliminating concurrent-access corruption on shared storage. Authentication integrates with Active Directory / LDAP, with local accounts alongside. Full detail on page 3.

Everything a mail platform should do, in one product

● Core mail

- ✓ **Full protocol suite**
SMTP, submission, IMAP4, POP3 — all TLS-secured
- ✓ **Modern webmail**
Responsive web client with native mobile screens
- ✓ **Server-side rules**
Per-user filtering, vacation replies, forwarding (Sieve)
- ✓ **Full-text search**
Indexed search across message bodies and attachments
- ✓ **Mail objects**
Aliases, distribution lists, quotas, forwards, catch-alls
- ✓ **Acceptance & routing rules**
Domain-level policy applied at SMTP time and in-message

● Groupware & collaboration

- ✓ **Calendars & tasks**
Shared scheduling via open CalDAV standard
- ✓ **Contacts**
Personal and shared address books (CardDAV)
- ✓ **Mobile sync**
Microsoft ActiveSync push for iOS and Android
- ✓ **In-org chat**
Instant messaging native to the webmail, data stays in-house
- ✓ **File & folder sharing**
Share files and grant colleagues access to mail folders
- ✓ **Public resources**
Org-wide folders, notes, calendars and address books

● Security & filtering

- ✓ **Layered scanner chain**
Antivirus and anti-spam run independently, in order — third-party engines slot in alongside
- ✓ **BEC / impersonation filter**
Flags executive-name spoofing from outside senders
- ✓ **Quarantine**
Admin review, release, and per-user handling of held mail
- ✓ **DNSBL & geo blocking**
Blocklists and country-level connection filtering
- ✓ **Message encryption**
Per-account PGP, admin-enabled; S/MIME signing support
- ✓ **Internal zero-trust PKI**
Mutual TLS between all internal components

● Administration

- ✓ **Web Admin console**
Full control plane: domains, accounts, services, every node
- ✓ **Domain lifecycle automation**
Add or retire a domain across the whole stack in one action
- ✓ **Account profiles**
One settings profile applied to many mailboxes at once
- ✓ **Message tracking & queue**
Trace any message end to end; hold, release, requeue safely
- ✓ **Reports & email templates**
Usage reporting plus branded system notifications
- ✓ **RBAC · 2FA · audit**
Role-based access, two-factor login, append-only audit trail

● Identity & self-service

- ✓ **Directory integration**
Active Directory / OpenLDAP auth — read-only, passwords stay in your directory
- ✓ **Hybrid identity**
Local accounts and directory-imported users side by side
- ✓ **User self-service**
Vacation, rules, forwarding and quota view — no ticket needed
- ✓ **Single sign-on console**
One login across admin, monitoring and dashboards
- ✓ **AI assistant access (MCP)**
Connect Claude Desktop to your own mail, calendar and notes via a read-only MCP gateway — admin-gated, off by default

● Operations

- ✓ **Monitoring & central logs**
Cluster-wide metrics, dashboards, live log search and tail
- ✓ **Health checks & auto-recovery**
Failed services detected and restarted automatically
- ✓ **Mail backup & restore**
Back up and restore at the mail level — per message and mailbox
- ✓ **Log retention & SIEM**
Policy-based retention with forwarding to your SIEM
- ✓ **Rolling upgrade & patch**
Node-by-node updates with the service staying up

Built so that one failure changes nothing

Whitemail separates the mail path into five independent tiers. Each tier is clustered, health-checked, and sized to keep full service when a node is lost — not merely in steady state.

THE FIVE TIERS

1 · Load balancer Active-standby pair with a floating service IP. Clients see one address, always.

2 · Frontend SMTP inbound/outbound, webmail, and the session director that pins each user to one backend.

3 · Mailbox backend IMAP, POP3 and delivery. Sized so the survivors carry the full connection count when a node is gone.

4 · Storage A distributed file system keeps three replicas of every mailbox across three nodes.

5 · Database A three-node synchronous cluster holds configuration, groupware data, and the audit trail.

A groupware tier (calendar / contacts / mobile sync) and a webmail tier are added as the deployment grows; the control plane spans additional nodes without redesign. Sits cleanly behind an existing mail-security gateway.

WHAT HAPPENS WHEN A NODE FAILS

FAILURE	BEHAVIOUR
Load balancer	Service IP moves to the standby in seconds. No client change.
Frontend	Health checks route around it; sessions reconnect transparently.
Mailbox backend	The director re-maps its users onto the survivors, which are sized to hold the whole load.
Storage node	Two replicas keep serving; the third re-replicates in the background.
Database node	The cluster keeps quorum with two of three and continues writing.

Mail delivery is atomic — a message is written, synced, then published, so a crash mid-delivery never leaves a corrupt mailbox. Undeliverable mail queues rather than bounces during maintenance.

Guarded control plane

Every service action from the console runs through a policy engine that refuses any operation that would drop a cluster below quorum. Node agents accept only an allowlisted set of commands — there is no general shell.

Scale by adding nodes

From a compact 13-VM cluster to multi-tier deployments serving 15,000+ accounts: capacity grows by enrolling nodes into a tier, not by re-architecting. Reference build sheets cover each size.

Storage that grows with you

Mailbox storage expands online by adding disks or nodes. Tiered mailbox layout and index optimisation keep IMAP fast on both distributed and NAS-backed storage.

Defence in depth, evidence on record

- **Ordered, pluggable scanning**

Virus scanning runs independently of the spam engine, in a defined order. Commercial third-party scanners attach through the standard milter interface — no engine is a hidden dependency of another.

- **Business email compromise filter**

Messages whose display name impersonates an executive but arrive from outside the organisation are flagged or held before they reach the inbox.

- **Quarantine & safe queue control**

Held mail is reviewed and released from the console. Queue operations are reversible by design, and destructive actions require explicit, named scope — never a silent bulk delete.

- **Recoverable encryption at scale**

Server-managed per-account PGP keeps stored and transmitted mail as ciphertext while staying recoverable, searchable and scannable at 15,000+ accounts. Enabled per account by the administrator.

- **Zero-trust internals**

An internal certificate authority issues per-node certificates; all east-west traffic is mutually authenticated TLS. Management traffic runs on a separate network segment.

- **Audit trail & SIEM forwarding**

Every change and service action is recorded append-only — who, what, when, before and after. Logs retain on policy and forward to your SIEM.

MIGRATION & DEPLOYMENT

Moving in is a managed process, not a leap

Mail migration, from the console

Mailboxes copy in live from any IMAP server. A trial run — connect, authenticate, count, write nothing — is the default. During cutover the console answers the question that matters: who is left.

Groupware comes along

Contacts and calendars import from standard .vcf and .ics exports of the old system, with per-user counts reported as the record of what moved.

Offline-first installer

The whole platform ships as a verified, self-contained bundle — every package pinned by checksum. Installation adds no third-party repositories and works identically on air-gapped networks.

See Whitemail on your own infrastructure.

Ask for a guided evaluation or a proof-of-concept build sized to your organisation. Partner and reseller programmes available worldwide.

WhiteMail Inc.

BELLE FLURI, 4007 ZX, Netherlands
whitemail.io · sales@whitemail.io