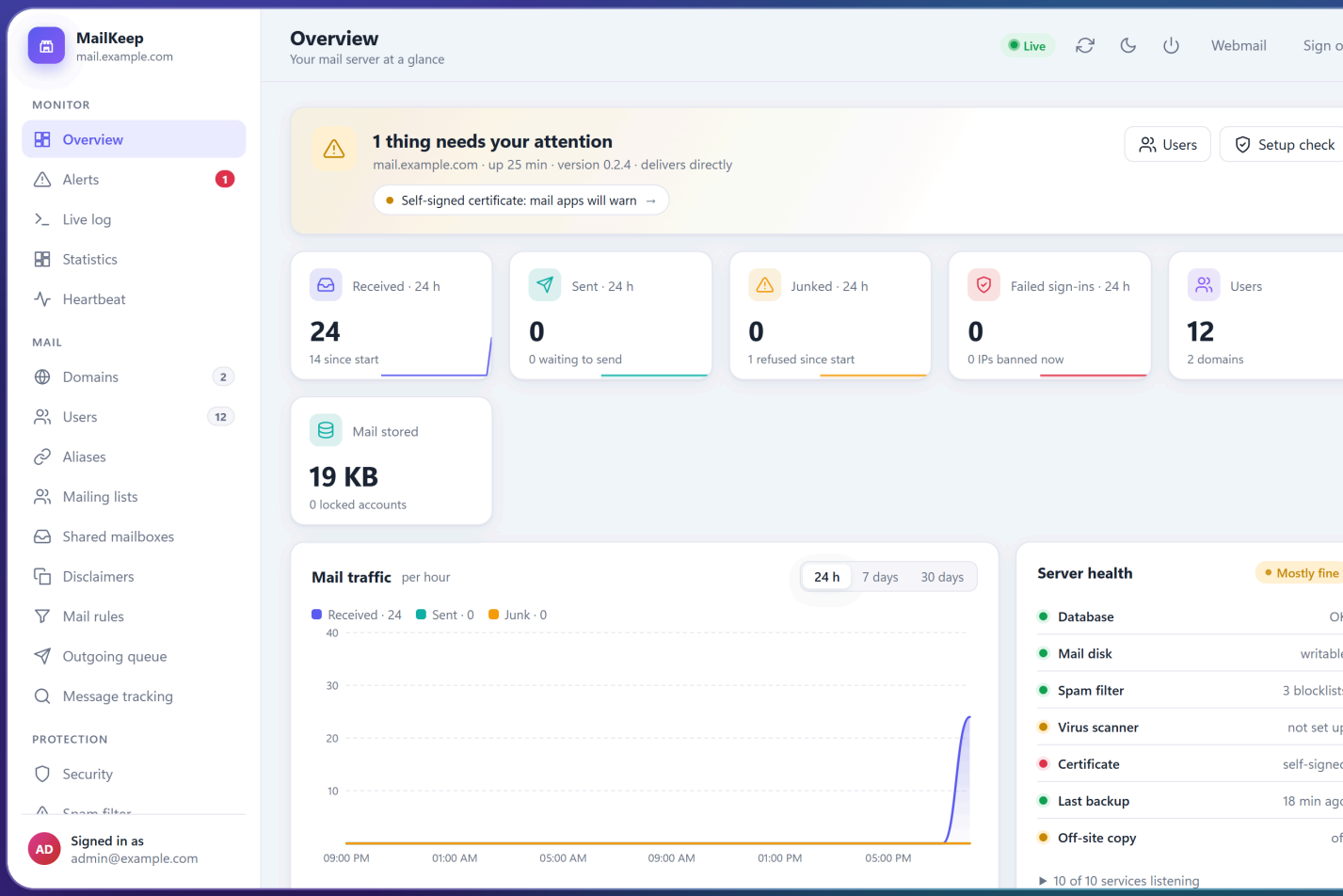
USER & ADMINISTRATOR MANUAL

MailKeep MX

The all-in-one mail server for Windows and Linux: e-mail, webmail, calendars and contacts, spam and virus protection, and a complete admin console.



Version 0.2.33 · November 2026

Contents

Chapters 1–4 get the server running, 5–19 cover every feature and page of the admin console, 20 is for the people who use the mail, and 21–23 are reference.

1 Introduction 4

What is MailKeep? · Features at a glance · Who this manual is for · Conventions in this manual

2 How MailKeep works 7

The big picture · Ports and services · The path of an incoming message · The path of an outgoing message · Where things are stored · Instant push

3 Installing MailKeep 11

Before you start · Installing on Windows: the setup wizard · Upgrading and uninstalling on Windows · Installing on Windows from the command line · Installing on Linux (systemd) · Installing with Docker · The first-time setup in the admin console · Setting up from the command line instead · After installing: a checklist

4 DNS, certificates and the network 18

The DNS records each domain needs · Certificates · A server with several IP addresses · Sharing ports 80/443 with IIS websites

5 The admin console 25

Opening the console · Finding your way around · The Overview page · Changing settings

6 Domains and DKIM 31

The Domains page · Adding and removing a domain · Disabling a domain · DKIM signing · Sending a domain's mail through its own relay · A domain's own look in webmail · Your logo in recipients' inboxes (BIMI)

7 Users and mailboxes 35

The Users page · Creating a mailbox · Invite links: people create their own mailbox · Adding many mailboxes from a spreadsheet · Everyday tasks · When someone leaves · Out-of-office and forwarding for a user · Paused sending

8 Aliases and catch-all addresses 40

What an alias is · Adding and removing aliases · Catch-all addresses · Several people for one address?

9 Mailing lists 42

How lists work · Creating a list and adding people · List settings · The list's special addresses · Moderation · Daily digests · The web archive · Outside senders and DMARC

10 Shared mailboxes 46

What a shared mailbox is · Access levels · Creating a shared mailbox · From the command line · How people use it

11 Disclaimers 50

Setting up a disclaimer · What gets changed

12 Sending mail and the outgoing queue 52

How sending works · Retries and bounces · The Outgoing queue page · Sending through a relay · Mail rules (server-wide) · Protection against hacked accounts

13 Spam, viruses and the quarantine 56

The spam score · The learning filter · The Newsletters folder · Allow and block lists · The spam settings · Warnings about mail from outside · Virus scanning with ClamAV · The quarantine

14 Security and sign-in protection 63

Layers of protection · The Security page · Blocking an address for good · Who is behind an address, and reporting it · Two-factor sign-in · Recent sign-ins and "sign out everywhere" · Alerts to users · Country rules · Who may use the admin console

15 Archive, legal hold and folder clean-up 70

Journaling · Searching and exporting the archive · Legal hold · Automatic folder clean-up

16 Monitoring, alerts and the setup check 72

Alerts · The daily summary · Heartbeat: being told when the whole server is down · Message tracking · Statistics · Storage · Blocklists · DMARC and TLS reports · The live log · The setup check · Health and metrics for monitoring tools

17 Administrators and delegation 84

Two kinds of administrator · Making someone a domain administrator · What a domain administrator sees · The management API and API keys

18 Backups and maintenance 88

What a backup contains · The Backups page · Copies off the server · Restoring · Updating MailKeep · Routine maintenance

19 Moving in from another server 94

The Move in page · From MailEnable · From any IMAP server · Is everything here? Compare · Switching over without losing mail

20 For users: webmail, mail apps and phones 98

Webmail · The calendar · Tasks · Setting up a mail app · Calendars and contacts · Mail rules · Shared mailboxes

21 Settings reference 106

General · [listeners] — services and ports · [limits] · [security] — sign-in security · [tls] — certificates · [outbound] — sending to other domains · [spam] — spam and viruses · [admin] — console, backups, alerts and heartbeat · [archive] — journaling · [retention] — folder clean-up · [reports] — DMARC/TLS reports and MTA-STS · [offsite] — off-site backup copies · [directory] — company directory · An example settings file

22 Command-line reference 121

mailserver setup · mailserver init · mailserver serve · mailserver service · mailserver release-key · mailserver domain · mailserver user · mailserver alias · mailserver list · mailserver shared · mailserver queue · mailserver dkim · mailserver dns · mailserver checkup

23 Troubleshooting and FAQ 136

Where to look first · Receiving mail · Sending mail · Signing in · The server · Frequently asked questions · Glossary

CHAPTER 1

Introduction

What MailKeep is, what it can do, and how to use this manual.

What is MailKeep?

MailKeep is a complete mail system in a single program. It receives mail for your domains, delivers your users' mail to the rest of the world, and gives your users everything they expect from a modern mail service: mail on every device with instant push, webmail, calendars and contacts that sync with phones, shared team mailboxes, and strong protection against spam, viruses and hacked accounts.

It runs on Windows (as a service) and on Linux (under systemd or in Docker). Everything is managed from a web-based **admin console**, and every task can also be done from the **command line**. There's nothing else to install: no separate database server, web server or spam filter.

Features at a glance

Mail for all your domains

Any number of domains (international names too), mailboxes with size limits, invite links, aliases and catch-all addresses, DKIM signing, and each domain's own look and logo.

Every kind of mail app

IMAP with instant push (IDLE), POP3, SMTP submission, JMAP, and automatic setup for Outlook, Thunderbird, iPhone and Android.

Webmail

An Outlook-style webmail with conversations, previews, undo send, send later, snooze, templates, push notifications, shared mailboxes, out-of-office, passkeys and two-factor sign-in, and an app-style layout on phones.

Calendars, meetings and contacts

A calendar with meeting invitations, free/busy, meeting rooms and shared calendars; tasks; a company directory; all synced with phones, Outlook and Thunderbird over CalDAV and CardDAV.

Spam and virus protection

SPF, DKIM, DMARC, blocklists, content rules, a learning filter per user, allow/block lists per user, domain or server, attachment blocking, ClamAV virus scanning with a test button, warnings about outside and impostor mail, and a quarantine.

Security

Bans for password guessing, permanently blocked addresses and ranges, account lockouts, passkeys, two-factor sign-in with app passwords, country rules, hacked-account detection, an outgoing spam check and a full audit log.

Team features

Mailing lists with moderation, digests and web archives; shared mailboxes with per-folder permissions; per-domain disclaimers; server-wide mail rules; hand-over when someone leaves; domain administrators with their own dashboard.

Compliance

Journaling of all mail, archive search and export, legal hold, and automatic clean-up of old Junk and Trash.

Operations

Let's Encrypt certificates, scheduled backups with encrypted off-site copies (Backblaze B2, S3 or a network share), alerts that resolve themselves, a heartbeat to outside monitors, a daily summary, statistics, storage and blocklist pages, DMARC/TLS reports, MTA-STS and DANE, message tracking, versioned updates from the console, and a setup checker.

Moving in

Direct import from MailEnable (passwords included) and from any IMAP server, one mailbox or hundreds at a time.

Who this manual is for

If you are…	Read
Installing the server for the first time	Chapters 2, 3 and 4, then the setup check in chapter 16
The administrator running it day to day	Chapters 5 to 19 — one per area of the admin console
Moving from MailEnable or another server	Chapter 19
A person who uses the mail	Chapter 20: webmail, mail apps, phones, calendars, shared mailboxes
Looking up a setting or command	Chapters 21 and 22
Fixing a problem	Chapter 23

Conventions in this manual

- Settings → Certificate means: in the admin console, open *Settings* and go to the *Certificate* section.
- `mailserver user add` is a command you type in a terminal (PowerShell on Windows, opened as administrator). On Windows the installer makes `mailserver` work in any new terminal window, and it finds the installed settings by itself. Elsewhere, run it in the folder that holds `mailserver.toml`, or add `--config <path>`.
- `[outbound] relay` means the `relay` setting in the `[outbound]` section of `mailserver.toml`.
- The examples use **example.com** and the server name **mail.example.com**. Replace them with your own.

✓ **Tip**

Green boxes like this one give a shortcut or a good habit.

Note

Blue boxes explain something worth knowing.

Important

Yellow boxes warn about something that can cause trouble if it's overlooked.

CHAPTER 2

How MailKeep works

The parts of the server, the ports it uses, the path a message takes, and where everything is stored.

The big picture

MailKeep is one program that listens on several network ports. Each port serves one kind of client: other mail servers deliver to port 25, mail apps send through port 587 or 465 and read mail over IMAP or POP3, and browsers use the web ports for webmail and the admin console. Behind those doors, every message passes through the same security guard, spam filter and mail rules before it's stored.

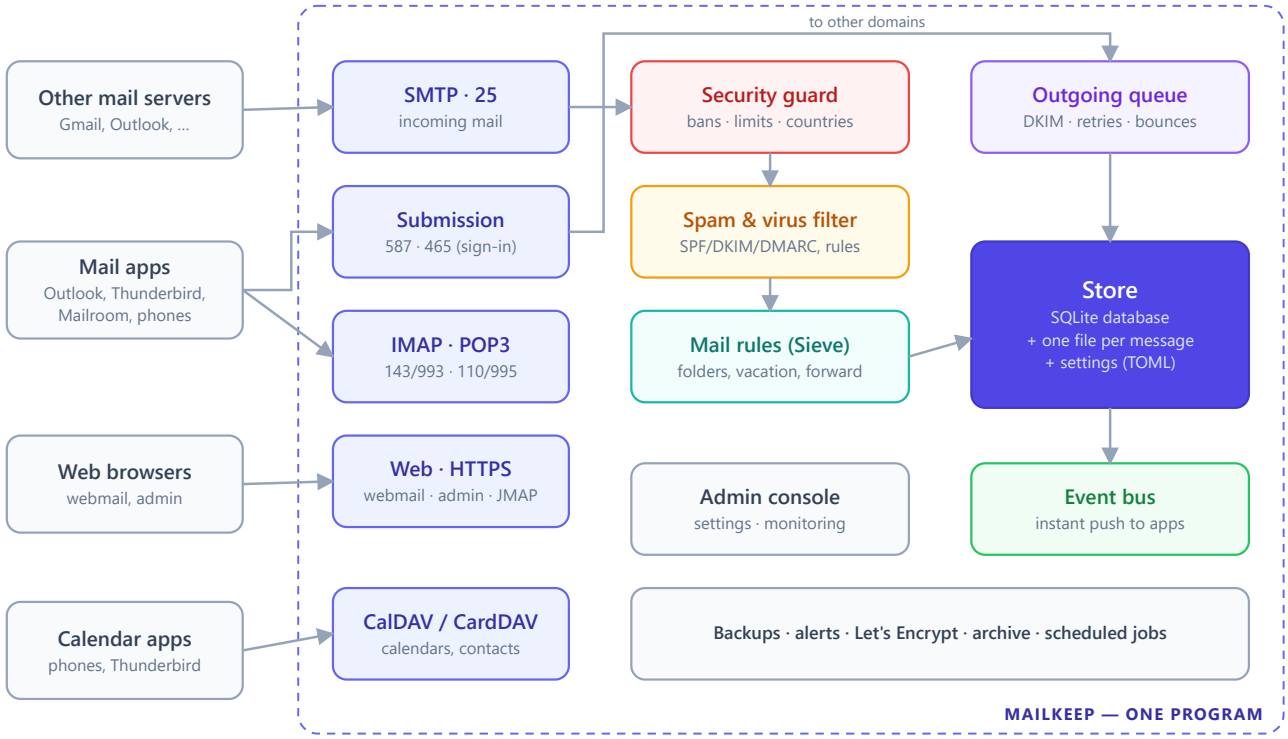


Figure 2.1 — The parts of MailKeep and who talks to them.

Ports and services

Port	Service	Used by
25	SMTP — incoming mail (STARTTLS offered)	Other mail servers delivering to your domains
587	Submission (STARTTLS, sign-in required)	Mail apps sending mail
465	Submission over TLS	Mail apps sending mail (encrypted from the start)
143 / 993	IMAP (STARTTLS) / IMAP over TLS, with instant push	Mail apps reading mail

Port	Service	Used by
110 / 995	POP3 (STLS) / POP3 over TLS	Older mail apps that download mail
4190	ManageSieve	Mail apps editing server-side mail rules
443	HTTPS	Webmail, admin console, calendars and contacts, JMAP, auto-setup
80	HTTP	Let's Encrypt checks, auto-setup, redirect to HTTPS

Every port can be moved or turned off under **Settings → Services and ports** (see chapter 21).

The path of an incoming message

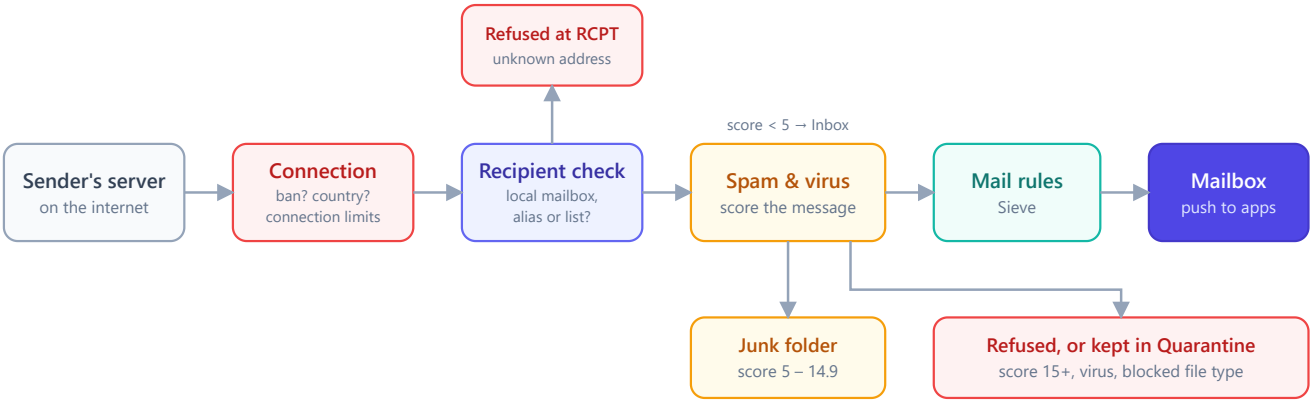


Figure 2.2 — From the sender's server to the user's mailbox.

1. **Connection.** The security guard drops banned addresses, countries you've blocked, and anyone with too many connections open.
2. **Recipient check.** Mail for an address that doesn't exist is refused straight away, so the sender gets the error and no bounce is ever sent to a forged address.
3. **Spam and virus filter.** The message gets a score from authentication checks (SPF, DKIM, DMARC), blocklists, content rules and the user's learning filter. Below 5 it goes to the Inbox, from 5 to Junk, and from 15 it's refused or kept in the quarantine. Viruses and dangerous attachments are never delivered.
4. **Mail rules.** The user's own rules (Sieve) can file the message, reply while they're away, or forward it.
5. **Mailbox.** The message is stored, and every connected mail app, webmail tab and phone is told at once.

The path of an outgoing message

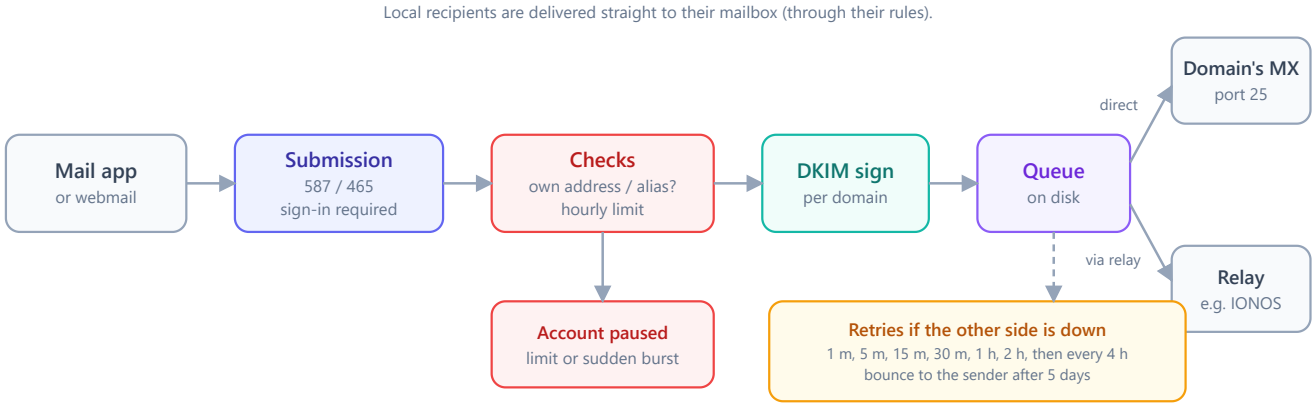


Figure 2.3 — From a mail app to the recipient's server.

Users must sign in to send. The server checks that the From address is theirs (their own address, one of their aliases, or a shared mailbox they may send as) and that they're within their hourly limit. The message is signed with the domain's DKIM key and placed in the queue, which delivers it to the recipient's mail server directly or through a relay. If the other side is unavailable, the queue retries for up to five days before returning the message to the sender with an explanation.

Where things are stored

What	Where
Settings	`mailserver.toml`. Saving in the admin console keeps the previous five versions as `.bak` files next to it.
Accounts, folders, message index, rules, calendars, contacts, lists, keys	The SQLite database `mailserver.db` in the data folder
Messages	One `.eml` file per message under `data/mail/`
Certificates	`data/tls/` (self-signed) and `data/tls/acme/` (Let's Encrypt)
Outgoing queue	`data/queue/` plus the database
Backups	`backups/` next to the data folder, or `[admin] backup_dir`
Log	The console window, and `log_file` if set (the Windows service always writes `logs\mailserver.log`)

> *i* **Relative paths**
> Paths in `mailserver.toml` are relative to the folder the settings file is in, so it doesn't matter where the server is started from.

Instant push

An internal event bus connects every part of the server. When a message arrives, is flagged, moved or deleted — over any protocol, by any client — every IMAP client waiting in IDLE, every open webmail tab, every JMAP client and every browser with notifications turned on is told within a moment. Phones with push (IMAP IDLE) show new mail as it arrives, without polling.

CHAPTER 3

Installing MailKeep

Requirements, installing on Windows, Linux or Docker, and the first-time setup wizard.

Before you start

You need	Why
A server with a fixed public IP address	Other mail servers must be able to find and reach it. Windows 10/11 or Windows Server, or any modern 64-bit Linux.
A name for the server, e.g. **mail.example.com**	Your MX records point at it, mail apps connect to it, and the certificate is issued for it.
Access to your domain's DNS	To publish the MX, SPF, DKIM and DMARC records (chapter 4).
Reverse DNS (PTR) for the IP address	Set by your hosting company or ISP to the server name. Gmail and Outlook refuse mail without it.
Port 25 open in both directions	Incoming mail arrives on 25, and outgoing delivery uses 25. If your provider blocks outgoing 25, use a relay (chapter 12).
Disk space	About the size of all mailboxes plus room to grow, and the same again for backups.

Installing on Windows: the setup wizard

Double-click `mailserver.exe`. Windows asks for administrator rights (the usual "Do you want to allow this app to make changes?"), and the setup wizard opens in its own window. It's a Microsoft Edge app window without an address bar or tabs, served by the program itself to this computer only. Without Edge it opens in your default browser instead.

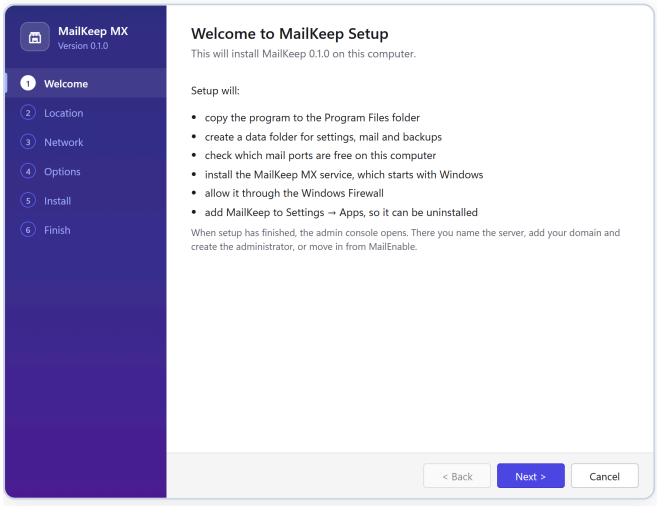


Figure 3.1 — Step 1: what setup will do.

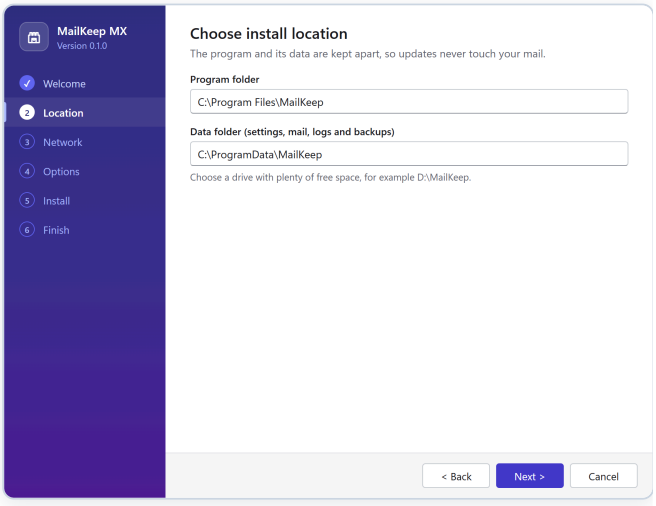


Figure 3.2 — Step 2: where the program and the data go.

1. **Welcome** — what setup will do. The steps are listed on the left and ticked off as you go; **Back**, **Next** and **Cancel** are at the bottom right.
2. **Location** — the **program folder** (default `C:\Program Files\MailKeep`) and the **data folder** for settings, mail, logs and backups (default `C:\ProgramData\MailKeep`). Pick a drive with plenty of room for the data, e.g. `D:\MailKeep`. If the data folder already holds a MailKeep settings file, it's kept along with the mail.
3. **Network and ports** — every service with its port, checked live: *free* or *in use*. When another program has a port — MailEnable on the mail ports, IIS on 80/443 — setup suggests a free one (8088 and 8443 for the web, 2525 for SMTP), or you can turn that service off. On a computer with several IP addresses, you can listen on just one, so another mail server keeps running on the other (chapter 4).
4. **Options** — optionally the server's internet name, and whether to open the Windows Firewall for MailKeep (on by default).
5. **Install** — a progress bar, and each step is shown as it happens: copy the program, write the settings, install the **MailKeep MX** service, open the firewall, add MailKeep to **Settings → Apps**, start it, and wait until it answers.
6. **Finish** — **Open admin console** takes you to the first-time setup wizard below.

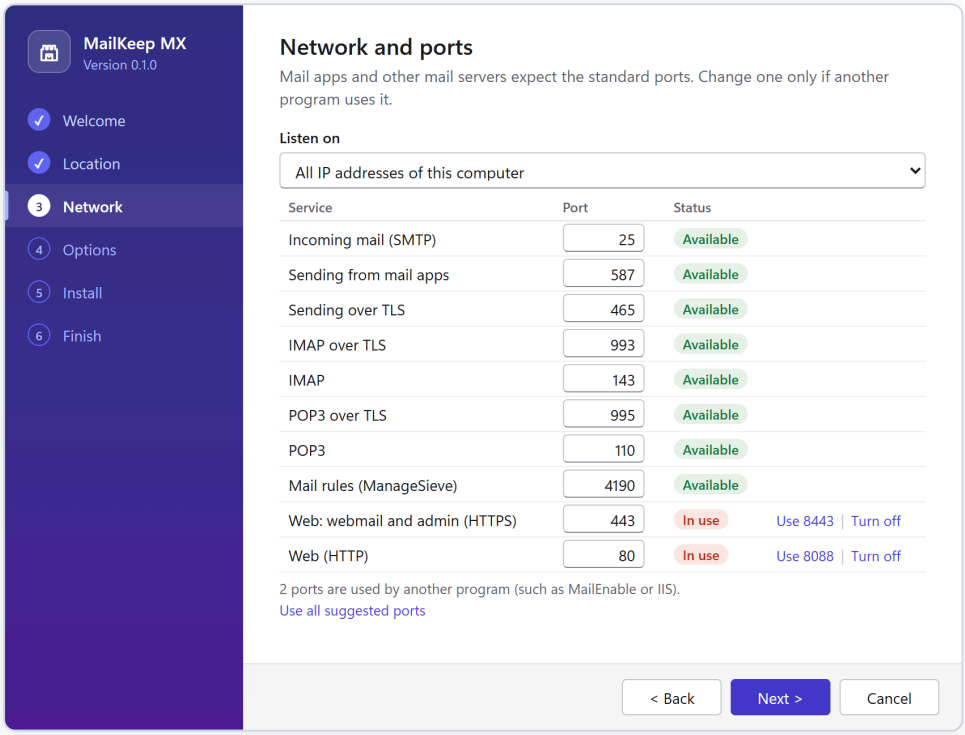


Figure 3.3 — Step 3: ports 80 and 443 are taken by another program; setup suggests 8088 and 8443.

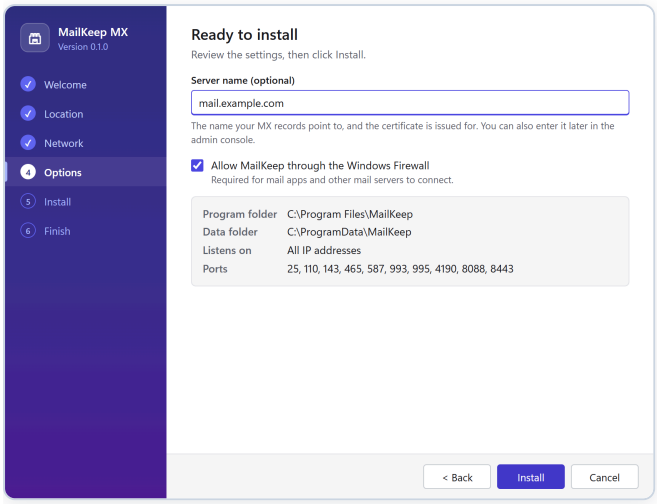


Figure 3.4 — Step 4: ready to install.

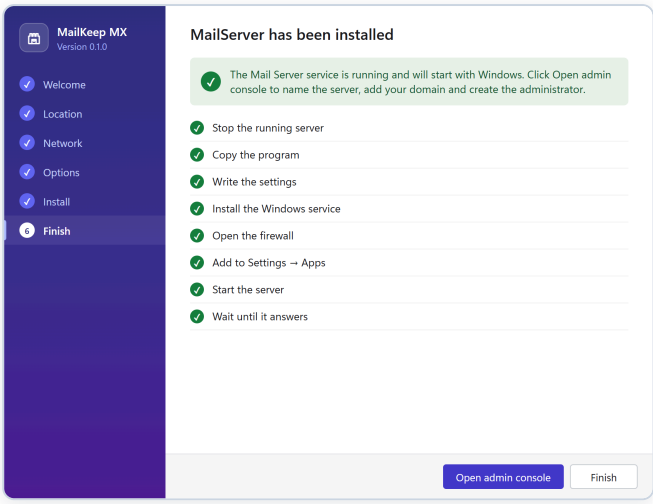


Figure 3.5 — Step 6: finished.

The service runs as LocalSystem, starts at boot without anyone signed in, and restarts itself after 5, 30 and 60 seconds if it ever fails. It logs to `logs\mailserver.log` in the data folder.

> **Keep the small window open**
>
> Double-clicking also opens a small console window that says where the wizard is. Leave it open until setup has finished; closing it cancels setup. Both windows close by themselves when you click **Finish** in the wizard.

> **Trying it out first**
>
> `mailserver setup --test C:\SetupTest` runs the whole wizard without changing the computer: files go under `C:\SetupTest`, and the service, firewall and Apps entry are only listed.

Upgrading and uninstalling on Windows

Upgrading: double-click the new `mailserver.exe`. Setup finds the installed copy and offers **Upgrade**: it stops the service, replaces the program, and starts it again. Settings and mail are kept, and mail that arrives in those few seconds is simply retried by the sending servers. Double-clicking the installed copy itself shows that it's installed, with buttons to open the admin console or uninstall it.

Uninstalling: Settings → Apps → MailKeep → Uninstall (or `mailserver setup --uninstall`). It removes the service, the firewall rule, the Apps entry and the program. **Mail and settings are kept** unless you tick *Also delete all mail, settings and backups* and type DELETE to confirm.

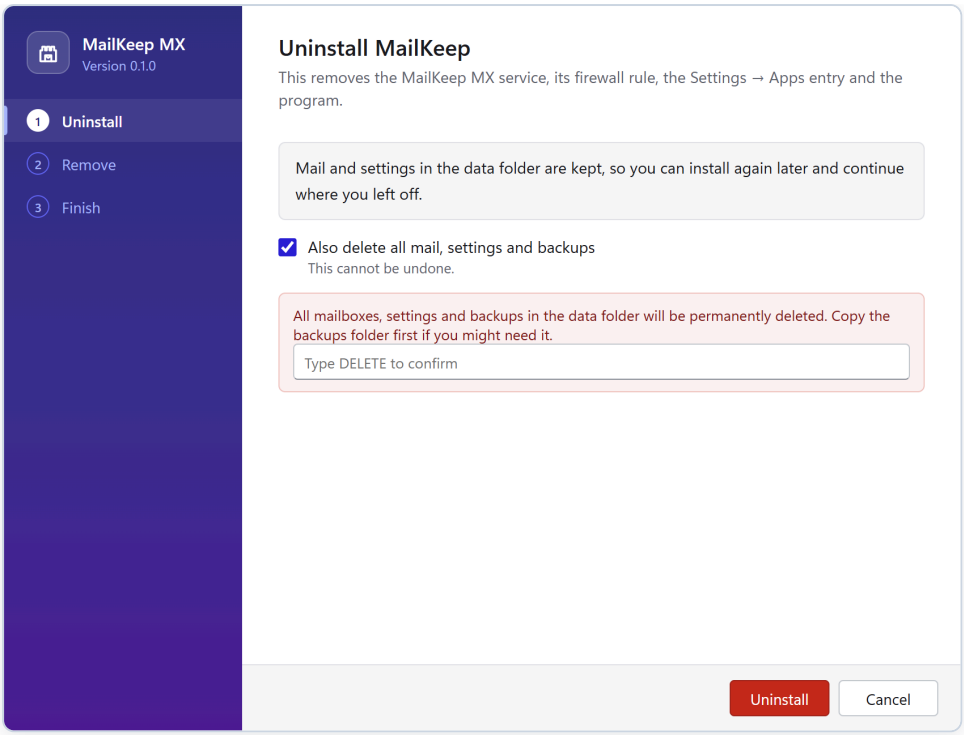


Figure 3.6 — Uninstalling: mail is kept unless you choose otherwise.

Installing on Windows from the command line

For scripted installations, or if you prefer a terminal. In PowerShell opened with **Run as administrator**:

```
cd C:\MailKeep
.\mailserver.exe init                                  # writes mailserver.toml
notepad mailserver.toml                                # set hostname (and ports if needed)
.\mailserver.exe serve                                 # try it; Ctrl+C to stop
.\mailserver.exe --config C:\MailKeep\mailserver.toml service install
.\mailserver.exe service start
```

Then allow the mail ports through Windows Firewall for `mailserver.exe` (25, 587, 465, 993, 995, 143, 110, 4190, 443, 80 — whichever you use).

```
mailserver service status      # no administrator needed
mailserver service stop
mailserver service uninstall   # mail, users and settings are kept
```

✓ **Everyday commands while the service runs**

Commands such as `user add`, `queue list` and `backup` work while the service is running. Only `restore` needs it stopped. Open PowerShell as administrator and type them as shown (for example `mailserver dns example.com`): the installer adds MailKeep to the command line, and the commands find the installed settings themselves. Open a new window after installing so it notices. On a server installed before version 0.2.29 that hasn't been updated yet, give the full paths instead:

```
& "C:\Program Files\MailKeep\mailserver.exe" --config
"C:\ProgramData\MailKeep\mailserver.toml" dns example.com
```

Installing on Linux (systemd)

```
sudo useradd --system --home /var/lib/mailserver --shell /usr/sbin/nologin mailserver
sudo install -m 755 mailserver /usr/local/bin/
sudo install -d -o mailserver -g mailserver /etc/mailserver /var/lib/mailserver /var/log/mailserver
sudo -u mailserver mailserver --config /etc/mailserver/mailserver.toml init
```

In `/etc/mailserver/mailserver.toml` set `hostname`, `data_dir = "/var/lib/mailserver"` and `log_file = "/var/log/mailserver/mailserver.log"`. Then install and start the unit that comes with MailKeep:

```
sudo cp packaging/linux/mailserver.service /etc/systemd/system/
sudo systemctl daemon-reload
sudo systemctl enable --now mailserver
journalctl -u mailserver -f
```

The unit runs as the unprivileged `mailserver` user. It may only open ports below 1024, sees the system as read-only, and may write only to its own folders. Run admin commands as that user so file ownership stays right: `sudo -u mailserver mailserver --config /etc/mailserver/mailserver.toml user add …`

Installing with Docker

```
docker compose run --rm mailserver init          # writes ./data/mailserver.toml
# edit ./data/mailserver.toml: hostname, certificate
docker compose run --rm mailserver domain add example.com
docker compose run --rm mailserver user add bob@example.com
docker compose up -d
docker compose logs -f
```

Everything — settings, database, mail, certificate and logs — lives in `./data`. Back it up with `docker compose run --rm mailserver backup`, or copy the folder with the container stopped.

The first-time setup in the admin console

When setup finishes it opens the admin console (or open **http://localhost/admin/** in a browser **on the server itself**). While there is no administrator yet, a second, short wizard asks three questions. For safety it only works from the server machine.

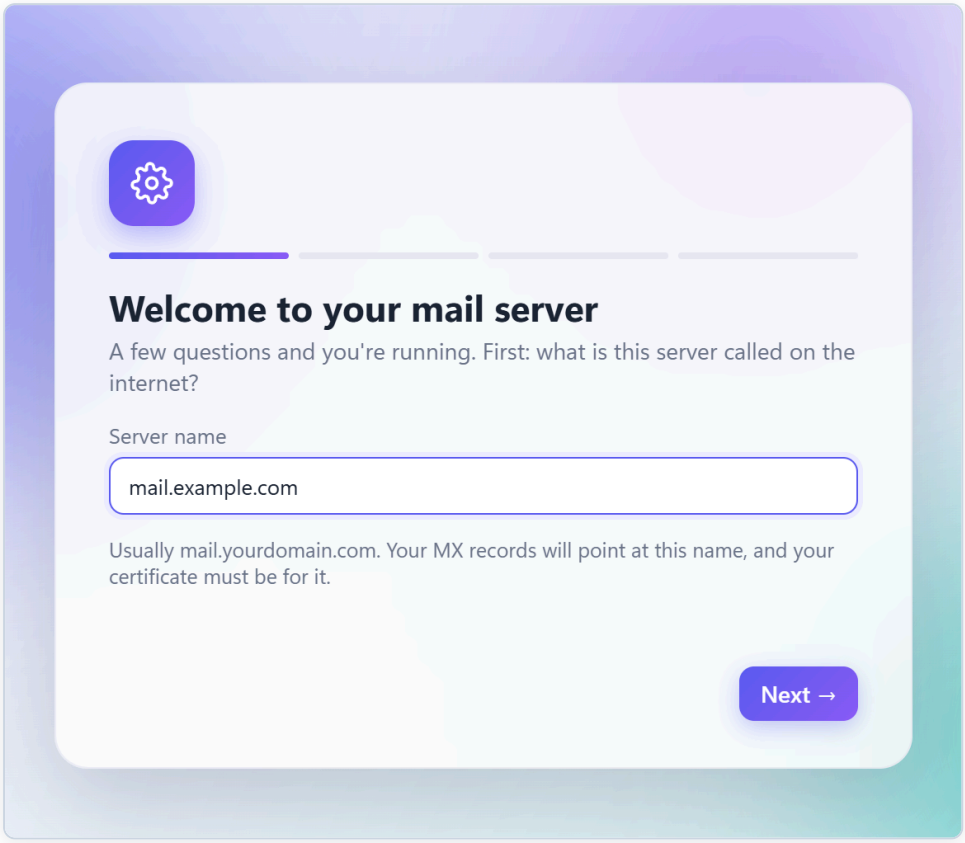


Figure 3.7 — Step 1: the server's name on the internet.

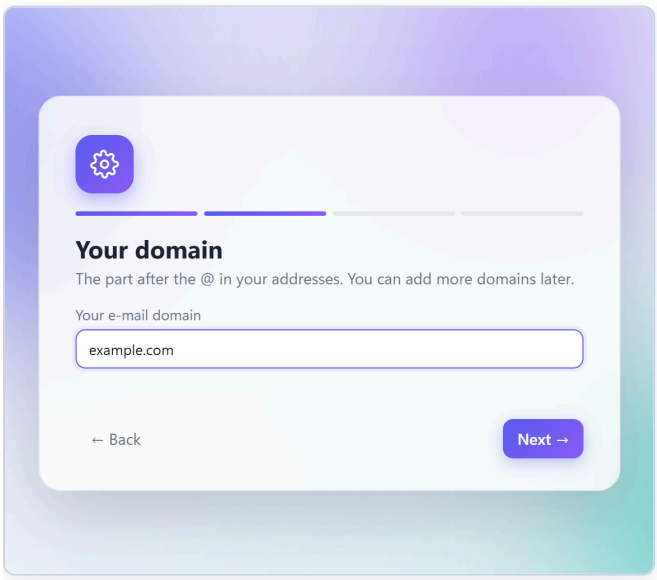


Figure 3.8 — Step 2: your first e-mail domain.

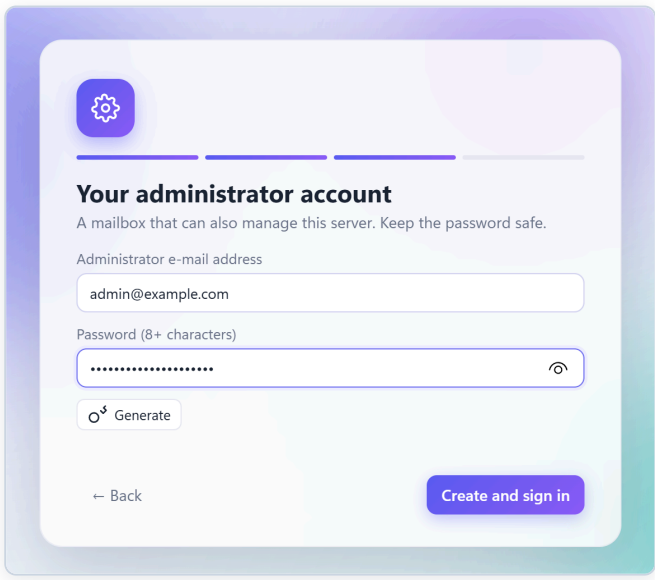


Figure 3.9 — Step 3: the administrator's mailbox and password.

After **Create and sign in** the wizard offers three next steps: move in from MailEnable, review the settings, or go to the dashboard. If you changed the server name, restart once from **Settings → Restart server**.

Setting up from the command line instead

```
mailserver init                                  # writes mailserver.toml
mailserver domain add example.com
mailserver user add bob@example.com --quota-mb 2048
mailserver alias add sales@example.com bob@example.com
mailserver admin add bob@example.com             # may use the admin console
mailserver serve
```

After installing: a checklist

1. Publish the DNS records for each domain (chapter 4, `mailserver dns example.com`).
2. Get a real certificate with Let's Encrypt (chapter 4).
3. Run **Setup check** and fix everything it flags (chapter 16).
4. Turn on scheduled backups with an off-site copy, and alerts (chapters 16 and 18).
5. Add a heartbeat service, so you hear about it if the whole server goes down (chapter 16).
6. Install ClamAV and press **Test the virus scanner** (chapter 13).
7. Turn on two-factor sign-in or passkeys for every administrator, and add your own address to *Never ban these IPs* (chapter 14).
8. Create the users, or move them in from your old server (chapters 7 and 19).

CHAPTER 4

DNS, certificates and the network

The records other mail servers check, getting a free certificate, servers with several IP addresses, and sharing ports 80/443 with IIS.

The DNS records each domain needs

Other mail servers decide whether to accept your mail by looking at DNS. Every hosted domain needs the records below; the server name needs an A record and reverse DNS.

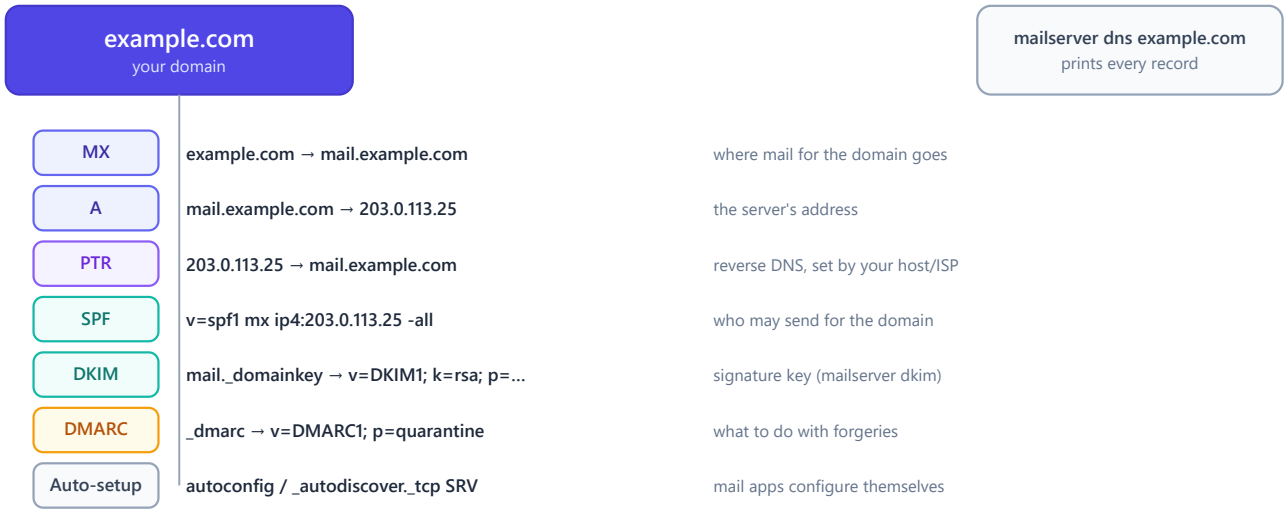


Figure 4.1 — The records for example.com, served by mail.example.com at 203.0.113.25.

You don't have to write them yourself. **Domains → DNS records** in the admin console, or this command, prints every record with its exact value:

```
mailserver dns example.com
```

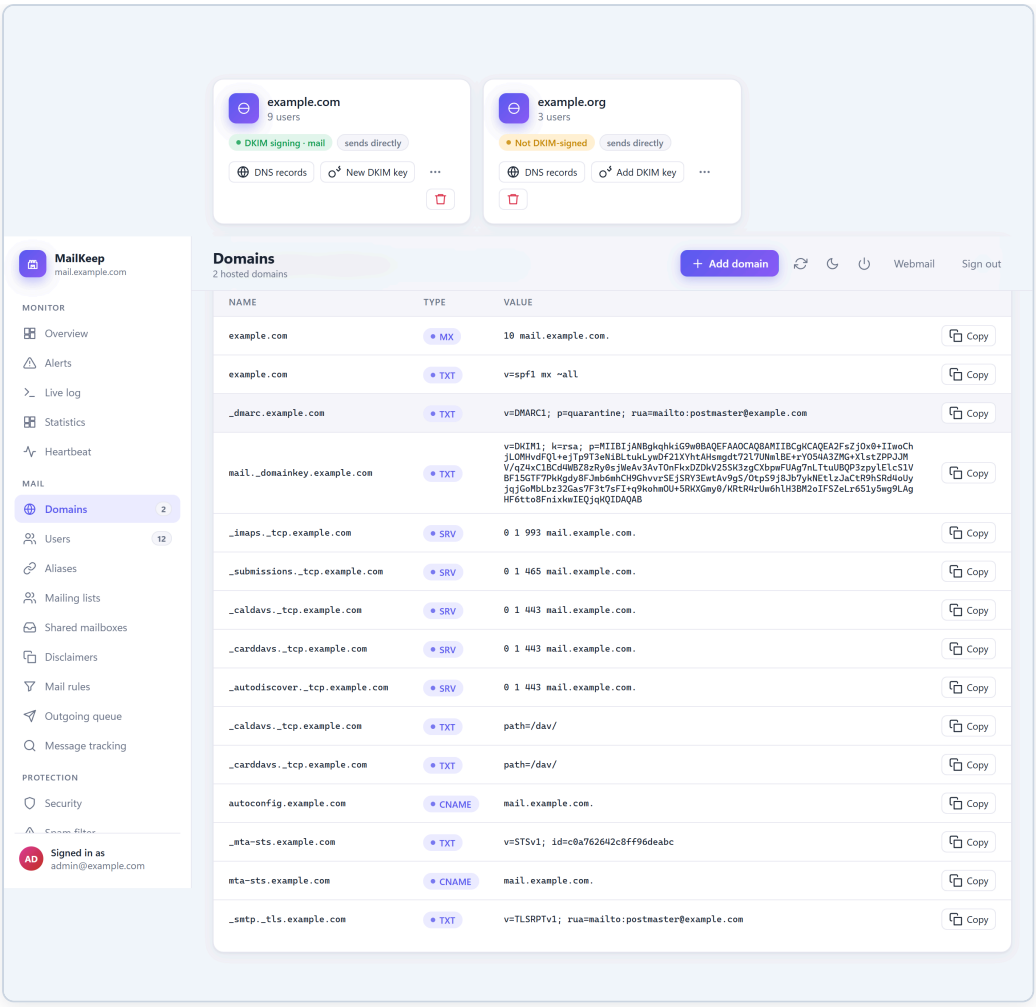


Figure 4.2 — The DNS records for a domain, each with a Copy button.

Record	Purpose	Notes
MX	Where mail for the domain is delivered	Points at the server name, never at an IP address
A	The server name's IP address	One A record for the server name, shared by all domains
PTR (reverse DNS)	The IP address's name	Set by the owner of the IP (hosting company, ISP), not in your DNS zone. Must equal the server name.
SPF (TXT)	Which servers may send for the domain	Include every server and relay that sends mail as the domain
DKIM (TXT)	The public key for signatures	Created with **Add DKIM key** or `mailserver dkim generate`
DMARC (TXT)	What receivers do with mail that fails SPF and DKIM	Start with `p=quarantine` (or `p=none` to only watch), with `rua=mailto:postmaster@<domain>` so reports reach the Reports page; move to `reject` once only your own senders appear there and pass
MTA-STS (TXT + a web page)	Other servers must deliver to you encrypted, with a valid certificate	Optional; see below

Record	Purpose	Notes
TLS reports (TXT)	Other servers report delivery problems to you	Optional: `_smtp._tls.<domain>`
BIMI (TXT)	Your logo next to your mail	Optional (chapter 6)
Auto-setup	Mail apps configure themselves	`autoconfig.<domain>` and `_autodiscover._tcp.<domain>` SRV (chapter 20)

> *i* **One server name for every domain**
>
> Users of every hosted domain set their mail app to the server's own name (e.g. `mail.example.com`), and every domain's MX points at it, so only that name needs to be on the certificate. For Outlook's automatic setup, publish `_autodiscover._tcp.<domain> SRV 0 1 443 mail.example.com.` instead of an `autodiscover.<domain>` record; the SRV route needs no certificate for the customer's domain.

Certificates

Every encrypted connection — mail apps, webmail, other servers — uses the server's certificate. Until you set one up, MailKeep makes a **self-signed** certificate in `data/tls/`; mail is still encrypted, but mail apps and browsers warn about it.

Free certificates from Let's Encrypt

1. Make sure the server name's A record points at this server and **port 80 reaches it from the internet**. Let's Encrypt checks ownership by fetching a file over HTTP.
2. Open **Settings → Certificate**, turn on **Free certificate from Let's Encrypt**, optionally add an e-mail for expiry warnings, and save.
3. Click **Restart now**, then **Get certificate now**.

The certificate is stored in `data/tls/acme/`, renewed automatically 30 days before it expires, and takes effect immediately without a restart. Use **Test mode** (`acme_staging`) while you are still testing port 80; the test service has much higher rate limits.

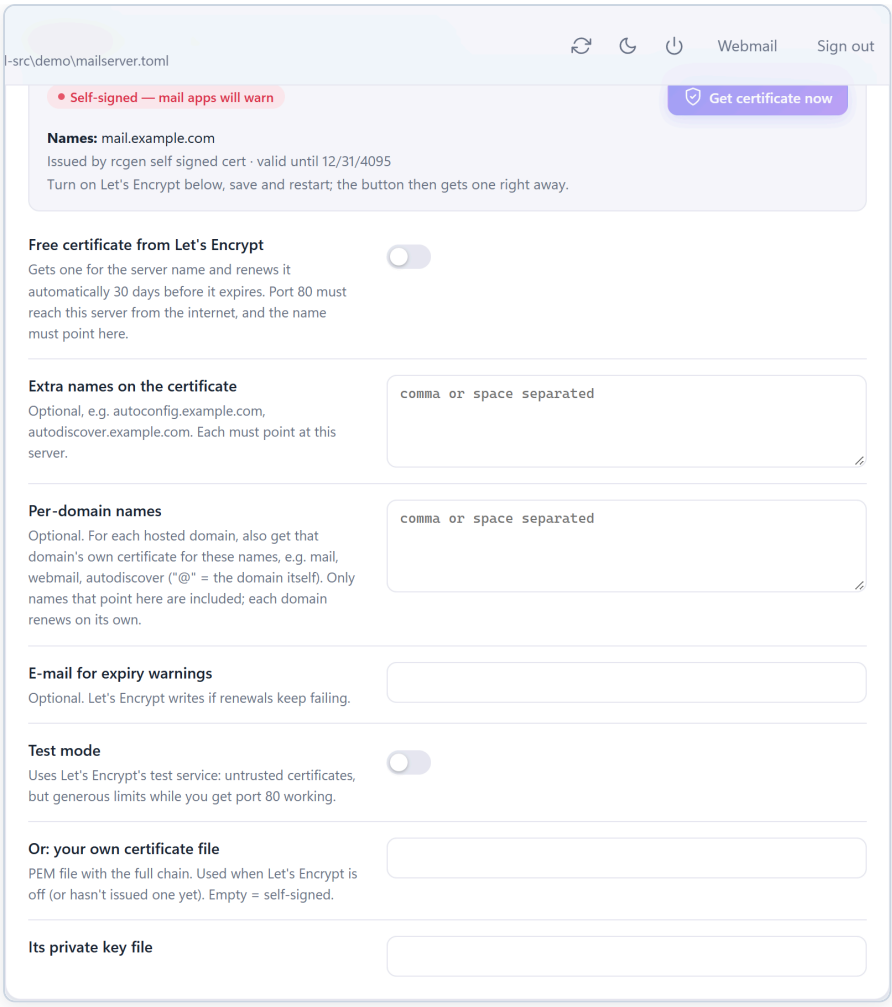


Figure 4.3 — Settings → Certificate.

Customers' own names

To let each hosted domain use its own names — `mail.customer.com` in mail apps, `webmail.customer.com`, or `autodiscover.customer.com` — list the prefixes under **Per-domain names**:

```
[tls]
acme_domain_names = ["mail", "webmail", "autodiscover"]   # "@" = the domain itself
```

Each domain then gets its own certificate, and the server presents the right one for whatever name a client connects to, falling back to the main certificate. Only names whose DNS already points at this server are requested, so one customer's DNS problem never affects another.

MTA-STS

MTA-STS tells other mail servers to deliver to your domain only over an encrypted connection with a valid certificate. It has two parts, and both must work:

1. The **policy page** at `https://mta-sts.<domain>/.well-known/mta-sts.txt`, which MailKeep serves itself. Point `mta-sts.<domain>` at this server (a CNAME to the server name), add `mta-sts` under **Per-domain names** (above) so it's on a certificate, and make sure MailKeep answers on port 443.

2. The **TXT record** `_mta-sts.<domain>` with the value Setup check shows. Publish it last, once the page works.

Choose `testing` or `enforce` in the Reports page's Settings (**Your MTA-STS policy**). If Setup check says *the TXT record is there but the policy can't be fetched*, the page isn't reachable yet: fix step 1, or remove the TXT record until it works.

Your own certificate

If you already have a certificate (for example from your hosting company, or issued by win-acme in IIS), set **Or: your own certificate file** and **Its private key file** to PEM files: the full chain and the key.

Plain http:// goes to https://

Someone who types `http://mail.example.com/webmail/` is sent on to the same address over https (a permanent `308` redirect, to the https port if it isn't 443), so passwords never cross the network unencrypted. Pages served over https also tell the browser to use https for that name from now on (`Strict-Transport-Security`, for a year).

A few addresses keep answering over plain HTTP, because the services that use them can't follow the redirect: Let's Encrypt's checks (`/.well-known/acme-challenge/`), mail-app auto-setup (`/mail/config-v1.1.xml`, `/autodiscover/…`), and `/health` and `/metrics` for monitoring tools. This machine itself (`http://localhost`) is never redirected.

Both follow **Settings → Security → Passwords only over encrypted connections** (on by default). Turn that off only on a test server without a certificate.

A server with several IP addresses

When the machine has more than one public address, mail must leave from the address receivers check: the one your server name points to, whose reverse DNS is that name, and which your SPF records list. Otherwise Windows picks one, and mail from the wrong address fails SPF and the reverse-DNS check.

Set **Settings → Sending to other domains → Send from address**, or:

```
[outbound]
source_ip = "203.0.113.25"
```

After a restart the log says `outbound mail is sent from 203.0.113.25`. If the address has a typo or isn't one of this machine's, mail waits in the queue and the log warns, instead of going out from another address. The setup check warns when it differs from the address your server name points to.

You can also listen on just one address by giving the address in each listener, e.g. `smtp = "203.0.113.25:25"`. That lets two mail servers run side by side on one machine, each on its own address (see chapter 19).

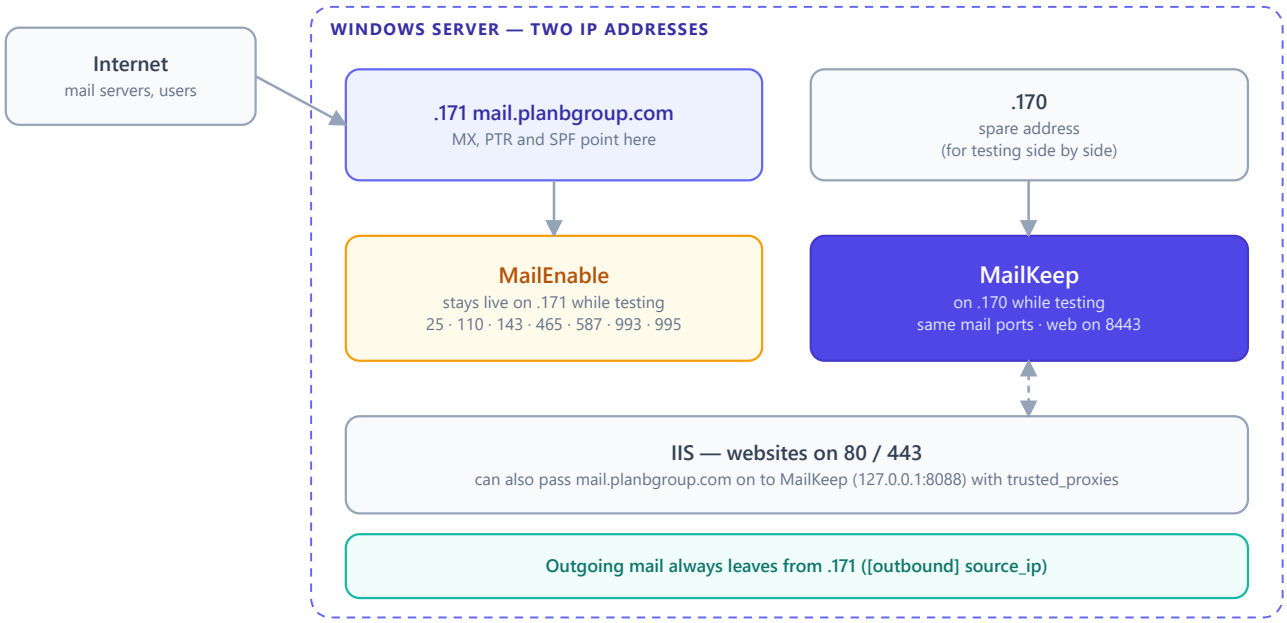


Figure 4.4 — A Windows server with two addresses, during the move from MailEnable: each mail server on its own address, IIS keeping 80/443.

Sharing ports 80/443 with IIS websites

Mail apps and other mail servers never go through IIS: the mail ports stay with MailKeep. Only the web side (webmail, admin, calendars, auto-setup) is affected. There are two ways.

A. Webmail on its own port

Set `https = "0.0.0.0:8443"` and use `https://mail.example.com:8443/webmail/`. Nothing changes in IIS. For the certificate, either let IIS pass only `/.well-known/acme-challenge/` on to MailKeep's HTTP port, or issue the certificate in IIS and point `[tls] cert` / `key` at exported PEM files.

B. Webmail at plain https:// through IIS

1. In IIS, install **URL Rewrite** and **Application Request Routing**. In ARR's *Server Proxy Settings* tick **Enable proxy**, keep "Preserve client IP in X-Forwarded-For" on, and set the response buffer threshold to 0.
2. Add a site for `mail.example.com` with HTTP and HTTPS bindings and a certificate for that name.
3. Add a *Reverse Proxy* rule to `http://127.0.0.1:8088/{R:1}`. Under *Server Variables*, allow `HTTP_X_FORWARDED_PROTO` and set it to `https` on the HTTPS binding.
4. In `mailserver.toml`:

```
[listeners]
http = "127.0.0.1:8088"   # only IIS reaches it

[security]
trusted_proxies = ["127.0.0.1"]
```

C. IIS on one address, MailKeep on the other

On a server with two public addresses, the cleanest arrangement is to give IIS one address (for your websites) and MailKeep the other, each with the normal ports 80 and 443. Windows' web layer (HTTP.sys, which IIS uses) claims ports 80 and 443 on **every** address by default, so tell it which one to use:

1. Point every website's DNS A record at the IIS address (in this example 203.0.113.26), and the mail names (`mail.example.com` and the like) at MailKeep's address (203.0.113.25).
2. In IIS Manager, change each site's bindings from *All Unassigned* to 203.0.113.26.
3. In an administrator PowerShell:

   ```
   netsh http add iplisten ipaddress=203.0.113.26
   ```

   then restart the machine (stopping the HTTP service by hand often hangs).
4. Check with `netstat -ano | findstr /c:":80 " /c:":443 "`: IIS (process 4) should listen only on `203.0.113.26`.
5. In MailKeep's **Settings → Services and ports**, set **Web (HTTPS)** to `203.0.113.25:443` and **Web (HTTP)** to `203.0.113.25:80`, save and restart.

Webmail and the console are then at `https://mail.example.com/` without a port, Let's Encrypt reaches MailKeep directly, and no IIS rewrite rule is needed. Calendar and contacts accounts set up with the old port need setting up again.

> **!** **Always set trusted_proxies behind IIS**
>
> Without it, everyone coming through IIS looks like the server itself. The "local network only" admin console and the first-time setup would be open to the internet, and one password guesser would get everybody banned. With it, MailKeep reads the visitor's real address from X-Forwarded-For — only from IIS, and in a way visitors can't fake — so sign-in limits, bans, the audit log and the admin console's local-network rule apply to the real visitor. Never list an address that visitors can connect from directly.

CHAPTER 5

The admin console

Signing in, finding your way around, the Overview page, and how settings are saved.

Opening the console

The admin console is at **https://mail.example.com/admin/**. If the web service listens on another port than 443 (for example `8443` while another web server still holds 443), add it: **https://mail.example.com:8443/admin/**. Sign in with the e-mail address and password of an account that's been made an administrator (the one from the setup wizard, or any account given admin rights later). If two-factor sign-in is on for the account, the console also asks for the 6-digit code; an administrator who has added a **passkey** can use Sign in with a passkey instead (chapter 14).

> ! **Local network only, by default**
> The console only answers from the server itself and from private (local-network) addresses. To use it from the internet, turn on Settings → This console → Allow the console from the internet, and turn on two-factor sign-in (or passkeys) for every administrator first. On a remote server, sign in over Remote Desktop or a VPN instead. To open it to the internet but only from your own addresses, fill in Admin console only from as well (chapter 14).

Installing the console as an app

In Edge or Chrome, open the console and choose ⋯ → Apps → Install MailKeep Admin (in Chrome: ⋮ → Cast, save and share → Install page as app), or click the install icon at the right of the address bar. The console then opens in its own window with the MailKeep icon, gets a taskbar and Start menu entry, and can be pinned. It's the same console with the same sign-in and rules (network, allowlist, two-factor), just without the browser around it. To remove it, use ⋯ → Uninstall in the app's own window, or Windows Settings → Apps. The install option only appears over https, or on `http://localhost`.

Finding your way around

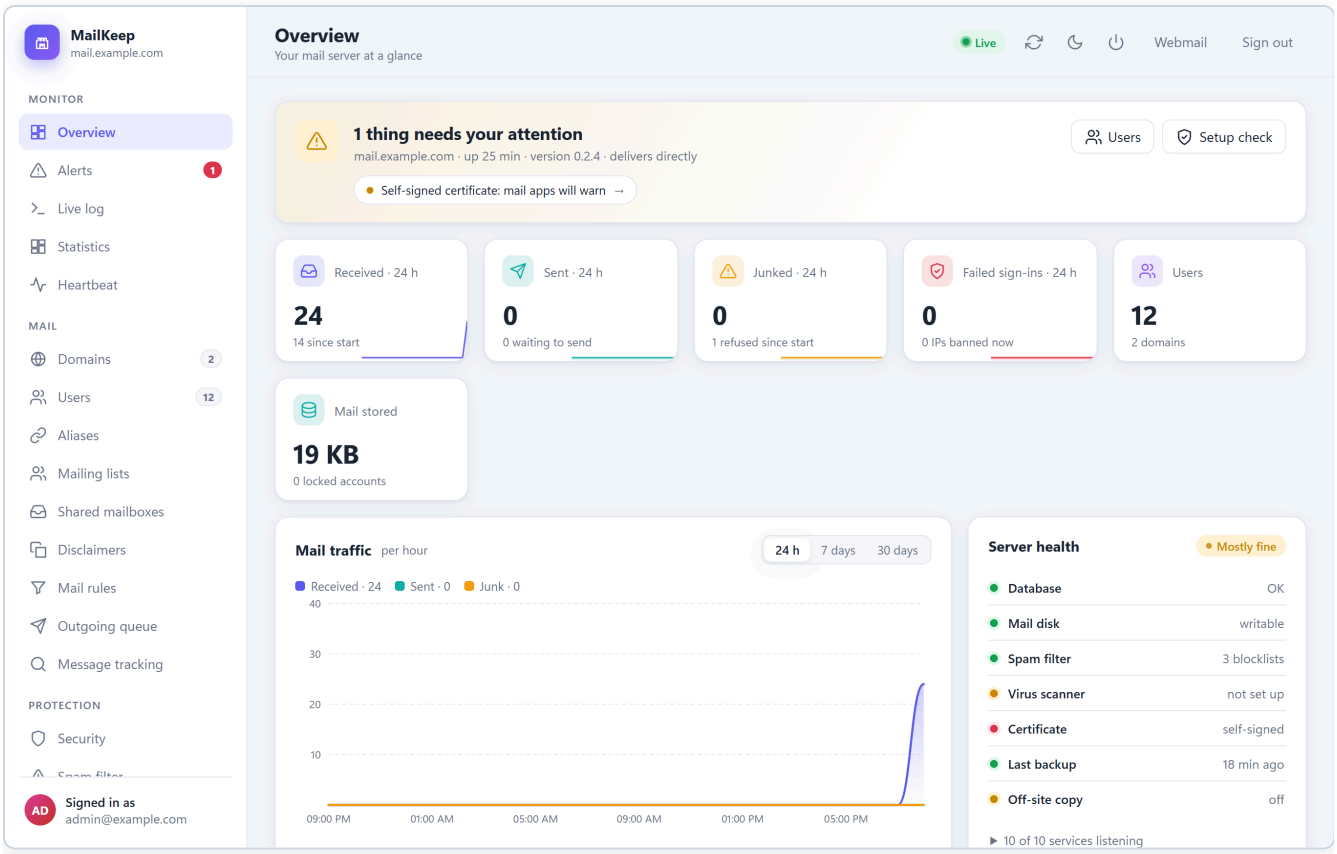


Figure 5.1 — The admin console: the menu on the left, the page on the right.

The menu on the left groups the pages:

Group	Page	What it's for	Chapter
Monitor	Overview	What needs you, traffic, and the health of every service	5
	Alerts	Problems the server warned about (dismiss, resolved), where alerts go, the daily summary	16
	Live log	The server's log as it happens	16
	Statistics	Mail in and out, spam and sign-ins, day by day	16
	Heartbeat	Outside services that tell you when the whole server is down	16

Group	Page	What it's for	Chapter
Mail	Domains	Hosted domains, DKIM, DNS records, relays, logos and branding	6
	Users	Mailboxes, invite links, leavers, admin rights	7
	Aliases	Extra addresses and catch-alls	8
	Mailing lists	Lists, members, moderation	9
	Shared mailboxes	info@, support@ and who may open them	10
	Disclaimers	Text added under outgoing mail, per domain	11
	Mail rules	Server-wide rules: refuse, redirect, copy, tag	12
	Outgoing queue	Mail waiting to be delivered, and why	12
	Message tracking	What happened to each message	16
Protection	Security	Bans, blocked addresses, locked accounts, paused senders, audit log, sign-in protection	14
	Spam filter	Allow and block lists, the main spam settings, the virus scanner test	13
	Quarantine	Held mail: view, release, delete	13
	Archive	Journaled mail and legal holds	15
	Reports	DMARC and TLS reports, your MTA-STS policy	16
	Blocklists	Is this server's address on the lists big providers use?	16
Server	Setup check	DNS, reverse DNS, certificate, ports, per-domain records	16
	Backups	Backups, schedule, off-site copies, restoring	18
	Storage	What uses the disk, and each mailbox's size	16
	Settings	The server-wide settings	21
	Move in	Import from MailEnable or any IMAP server, compare, and the switch-over checklist	19
	Update	Install a new version, and the update history	18
API keys	Keys for other software (billing, control panels, scripts) to use the management API	17	

At the top right: **Live** shows the page refreshes itself, the arrows refresh now, the moon switches between light and dark mode, the **power button** restarts the server (it asks first), **Webmail** opens your own mailbox, and **Sign out**. The numbers next to pages in the menu (Security, Alerts, Outgoing queue…) follow every

refresh and every action such as Unban. Your account is shown at the bottom left. Every page opens at its top, whichever page you came from.

Long lists (users, the audit log, message tracking…) show 50 rows at a time. The bar under the list moves a page forward or back and offers 100 or 250 rows per page; your choice is remembered in that browser.

On **Users**, **Aliases**, **Quarantine**, **Message tracking** and the **Audit log**, the server does the searching, sorting and paging and sends only the page you see, so these pages stay quick with thousands of mailboxes. Boxes that ask for a mailbox (an alias's target, Someone is leaving…, shared mailboxes, the archive, legal holds, Move in) suggest matching addresses as you type instead of listing everyone.

Any IP address shown in the console (in the audit log, the Overview, message tracking…) can be clicked. A panel shows its reverse DNS name, the network it belongs to and its abuse contact, country (by name, such as *Russia (RU)*, when a country database is set; chapter 14), whether it's on blocklists, its sign-in history and the mail it sent here, with buttons to Ban now (for the ban length), Block permanently (chapter 14), show Its mail, and draft an Abuse report… (chapter 14). Banning or blocking from this panel updates the page behind it straight away. The server's own addresses are marked *this server: can't be banned or blocked* and get none of these buttons.

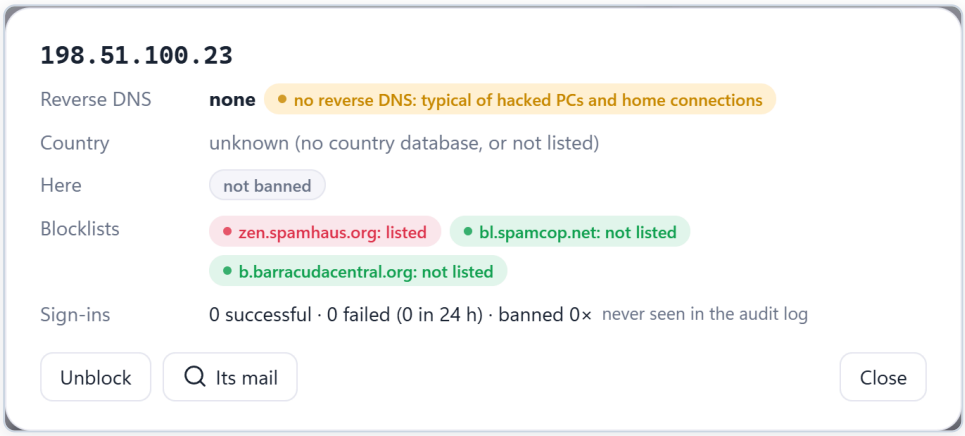


Figure 5.2 — The panel for an IP address.

> ✓ **Keyboard shortcuts**
>
> **1**–**9** jump to the pages in menu order, **r** refreshes, **/** jumps to the page's search box, and **Esc** closes menus and dialogs.

The Overview page

The Overview is the console's home page. It refreshes itself every 30 seconds.

- **At the top**, a verdict: *all good*, or the things that need you (an expiring certificate, a failed backup, the virus scanner not answering, a paused sender…). Each line is a link to the page where it's fixed.
- **Counters**: mail received, sent and junked in the last 24 hours, failed sign-ins, users and domains, and the mail stored, with small trend lines.
- **Mail traffic**: received, sent and junk mail per hour, for 24 hours, 7 days or 30 days.
- **Server health**: the database, the disk, the spam filter, the virus scanner (asked live: red when ClamAV doesn't answer), the certificate and every listening service, each green, amber or red.

- Further down: sign-ins and failures, the addresses trying hardest to guess passwords, the largest mailboxes, recent security events, and the backups with a **Back up now** button.

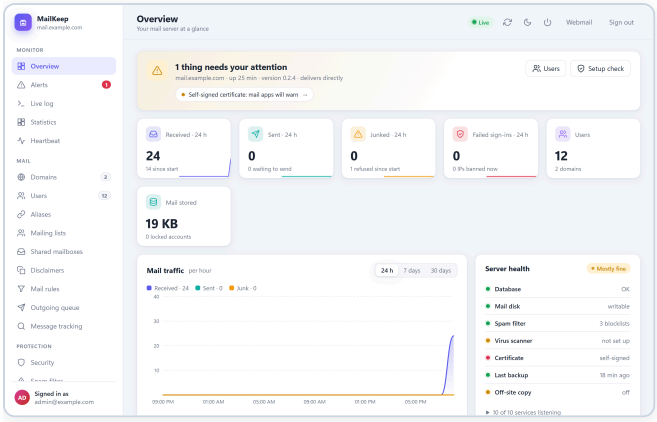


Figure 5.3 — Light mode.



Figure 5.4 — Dark mode.

Changing settings

Settings live where you use them. The pages with their own settings show a **Settings** panel at the bottom:

Page	Its settings
Security	Bans, lockouts, the never-ban list, countries, password rules (all sign-in protection)
Spam filter	Filter on/off, junk and refuse scores, blocklists, greylisting, learning filter, outgoing check, outside-mail warning
Quarantine	Quarantine instead of refusing, how long to keep, the users' daily summary
Archive	Journaling, which domains, an extra copy address, how long to keep
Alerts	Alerts on/off, an outside address, phone push, the low-disk limit, the daily summary
Reports	Reading and sending DMARC/TLS reports, your MTA-STS policy
Blocklists	Which lists to watch, how often
Backups	Schedule, how many to keep, the folder, the off-site copy
Heartbeat	How often the services are called (applies at once)

Everything else (server name, ports, certificate, sending, limits, the console, the company directory, folder clean-up and the technical spam options) is on the **Settings** page: one section at a time, picked from the list on the left. Its search box finds **every** setting, including the ones on other pages, with a button that takes you there.

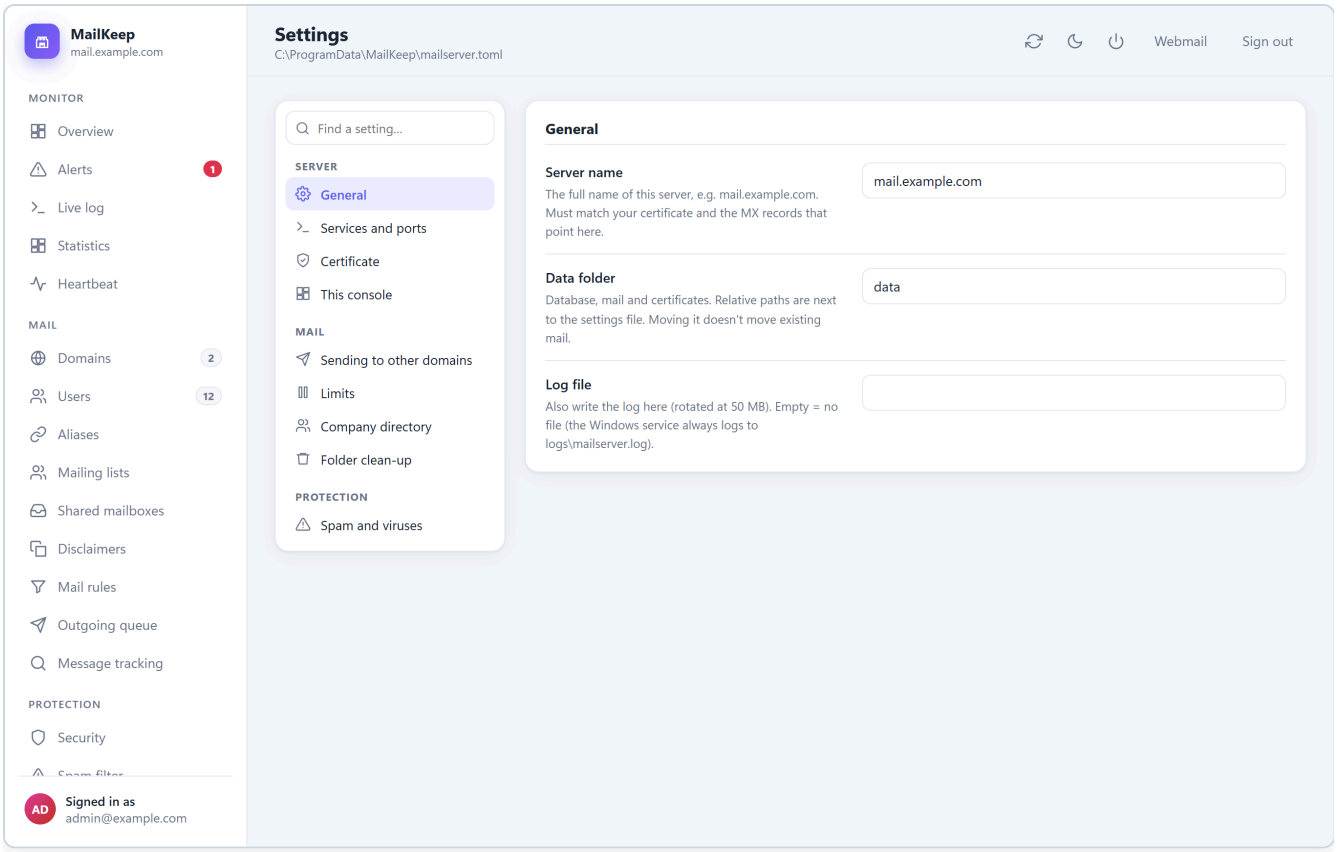


Figure 5.5 — The Settings page.

As soon as you change something, a bar floats at the bottom of the screen, wherever you've scrolled: Discard or Save changes. Leaving the page with unsaved changes asks first. Saving checks the values (for example that no port is used twice), keeps the previous file as a `.bak` (the last five are kept), and a banner at the top of **every page** says a restart is needed, with Restart now. The banner stays in view under the top bar however far you scroll, and the power button in the top bar shows an orange dot until the server has restarted. Restarting applies the changes in about a second, without stopping the Windows service. Everyone stays signed in, and mail apps reconnect by themselves.

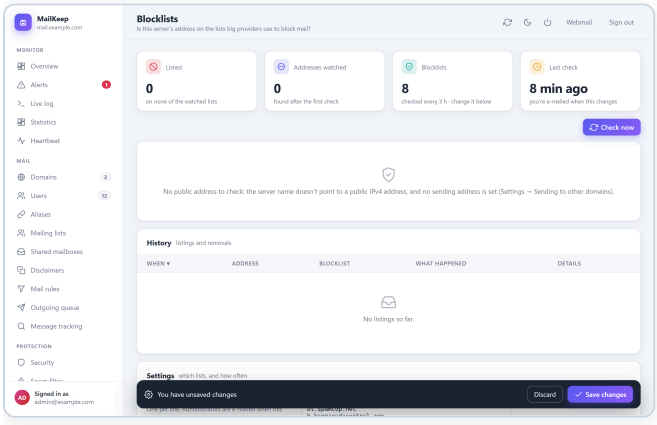


Figure 5.6 — An unsaved change: the floating save bar.

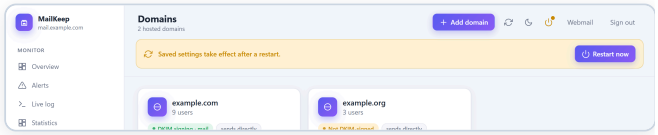


Figure 5.7 — Saved: the restart banner on every page.

Chapter 21 lists every setting with its default and meaning.

CHAPTER 6

Domains and DKIM

Adding the domains you receive mail for, signing their mail, sending a domain's mail through its own relay, and giving each domain its own look and logo.

The Domains page

Each hosted domain has a card showing its number of users, whether its mail is DKIM-signed, and how its mail leaves the server (directly, or through a relay). A disabled domain's card is greyed out and tagged *disabled · mail deferred* (or *refused*); point at the tag to see since when and who disabled it.

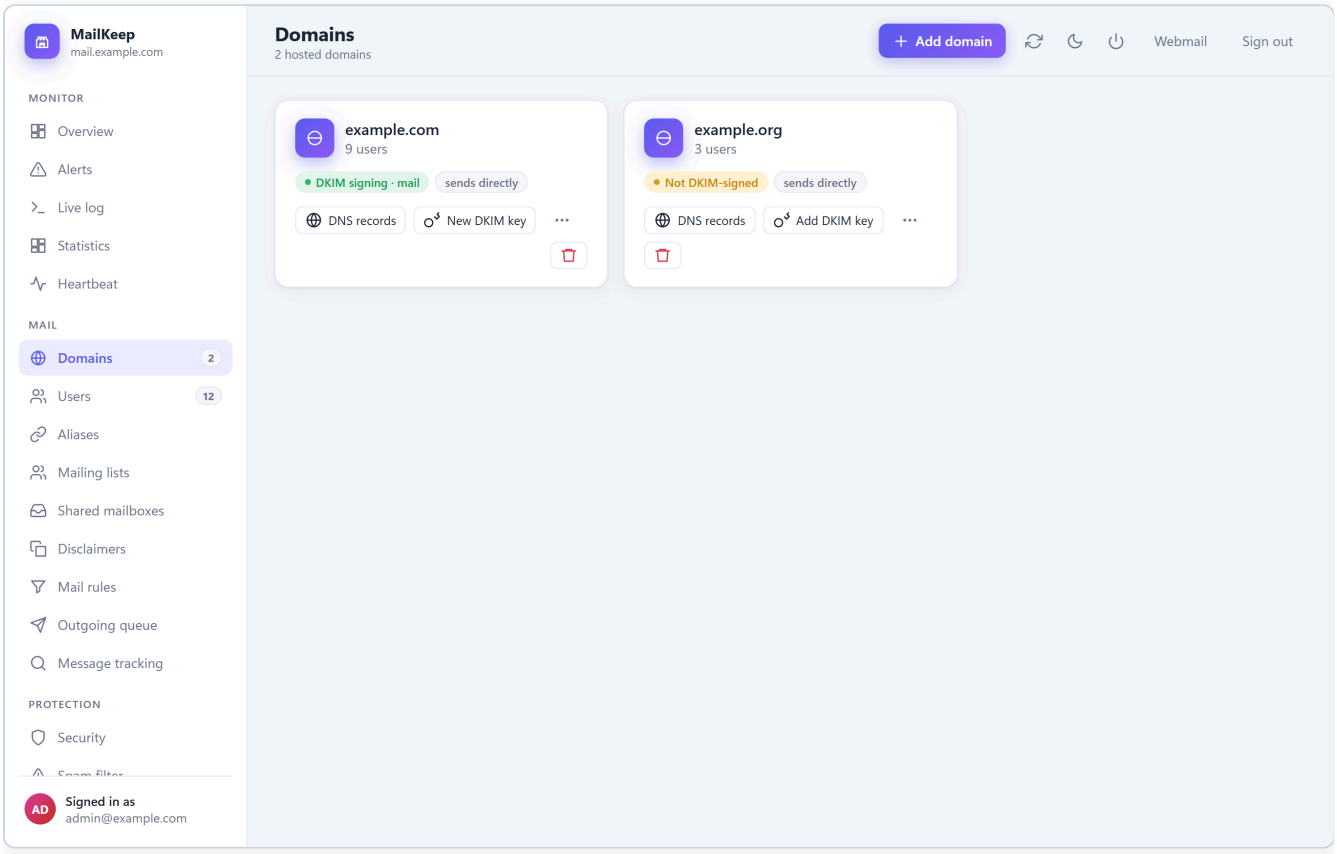


Figure 6.1 — The Domains page.

Adding and removing a domain

1. Click **Add domain** and type the domain, e.g. `example.com`. International names such as `müller.de` work too: they're shown as typed and handled as `xn--mller-kva.de` in DNS and mail, as the internet requires.
2. Click **Add DKIM key** on its card.
3. Click **DNS records** and publish every record shown at your DNS host (chapter 4).
4. Run the **Setup check** once the records are live.

```
mailserver domain add example.com
mailserver domain list
mailserver domain remove example.com
```

> ! **Removing a domain deletes its mail**
> Removing a domain deletes every user of that domain and all their mail. It can't be undone. A domain with an account on legal hold can't be removed. To stop a domain without losing anything, disable it instead (below).

Disabling a domain

For a customer who stopped paying, a domain being retired, or one sending spam while you look into it: ⋯ → **Disable domain…** switches the whole domain off without deleting anything. You choose what happens to mail sent to it:

- **Try again later (nothing lost)**: sending servers are told to retry, and keep doing so for a few days. If you enable the domain in that time, the mail still arrives.
- **Refuse it**: senders get a bounce straight away. For a domain that isn't coming back.

While it is disabled:

- its users are signed out and can't sign in anywhere (webmail, IMAP, POP3, phones, passkeys) or send. Mail apps that are already connected are turned away the next time they connect;
- its aliases, mailing lists and shared mailboxes stop receiving, and so do its mailboxes when mail reaches them through an alias on another domain;
- your other domains' users who write to it from webmail are told it is switched off;
- its users' *send later* mail waits, and fetching from their outside accounts pauses;
- Message tracking shows each deferred or refused message with the reason.

⋯ → **Enable domain** brings everything back as it was: mailboxes, mail, aliases, DKIM keys and settings are untouched. Both steps are in the audit log.

> *i* **Who can disable a domain**
> Only full administrators, and not the domain their own account is in (that would lock them out). Domain administrators can't disable domains. DNS isn't changed: the MX record still points here, and this server answers "not now" or "no".

DKIM signing

DKIM adds a digital signature to every message a domain sends, so receivers can tell it really came from you and wasn't changed on the way. Gmail, Outlook.com and Yahoo expect it.

- **Add DKIM key** (or `mailserver dkim generate example.com`) creates a 2048-bit key with the selector `mail` and shows the TXT record to publish at `mail._domainkey.example.com`.
- From then on, all mail from the domain is signed — from mail apps, webmail, lists and forwards.

- New DKIM key replaces the key. Mail is signed with the new key at once, so update the DNS record straight away.

```
mailserver dkim generate example.com [--selector mail] [--bits 2048]
mailserver dkim show example.com       # the DNS record again
mailserver dkim remove example.com
```

Sending a domain's mail through its own relay

Some domains are also hosted somewhere that only relays mail for its own domains, such as IONOS. Mail from such a domain can leave through that provider while other domains are unaffected. Use the ⋯ menu on the domain's card, then Send through a relay…, and enter:

Field	Example
Relay server (host:port)	`smtp.ionos.com:587`
Encryption	STARTTLS (port 587), TLS (port 465), or None
User name and password	A mailbox of the same domain at that provider

Saving tests the relay straight away. Test the relay signs in again later without sending anything, and Stop using the relay removes it. Restart the server to start using a new relay. Publish the provider's SPF include (e.g. `include:_spf-eu.ionos.com`) in the domain's SPF record.

```
[outbound.sender_relays."example.com"]
relay = "smtp.ionos.com:587"
security = "starttls"
user = "mailbox@example.com"
password = "…"
```

```
mailserver check-relay --domain example.com
```

A domain's own look in webmail

When several companies share the server, each can see its own name, colour and logo in webmail. Use the ⋯ menu on the domain's card:

- Webmail look…: the **company name** and an **accent colour** (such as `#1a73e8`) for the top bar and buttons.
- Webmail logo…: a PNG, JPEG or WebP picture of at most 300 KB (no SVG, for safety).
- Back to the standard look removes both.

The **sign-in page** takes its look from the address it's opened on: `mail.acme.com/webmail/` shows Acme's look when acme.com is a hosted domain. Once signed in, the look follows the user's own domain.

> **Each domain's sign-in page is for its own people**
>
> On an address that belongs to one hosted domain (such as `mail.mlmview.com`), webmail only signs in that domain's users. Someone from another domain is told "*This is the sign-in page for MLM View. Sign in at mail.innoventions.io instead*", with a link. The server's own name, plain IP addresses and the admin console accept everyone, so an administrator is never locked out. Mail apps (IMAP, SMTP) aren't affected.

Your logo in recipients' inboxes (BIMI)

BIMI shows your logo next to your mail in Yahoo, AOL, Apple Mail, Fastmail and others. Use ⋯ → **BIMI logo…** and upload the logo as an **SVG Tiny PS** file (square, solid background, no scripts). MailKeep hosts it at `https://mail.example.com/bimi/example.com.svg` and shows the DNS record to publish:

```
default._bimi.example.com   TXT   "v=BIMI1; l=https://mail.example.com/bimi/example.com.svg"
```

- BIMI only works with a DMARC policy of `quarantine` or `reject` (chapter 4).
- Gmail and Apple also want a paid certificate for the logo (a VMC, which needs a registered trademark, or a CMC). Without one, the logo shows at Yahoo, AOL and Fastmail only.
- Setup check shows whether BIMI is set up for each domain.

CHAPTER 7

Users and mailboxes

Creating mailboxes, passwords and size limits, turning accounts off, and admin rights.

The Users page

Every mailbox is listed with its status, the storage it uses (and its limit), whether two-factor sign-in is on, and when it last signed in. Search with the box at the top (address or name), or filter with **Active**, **Disabled**, **Admins**, **2FA on** and **Nearly full** (90% of the size limit or more). Each button shows how many users match the search. Click a column title to sort.

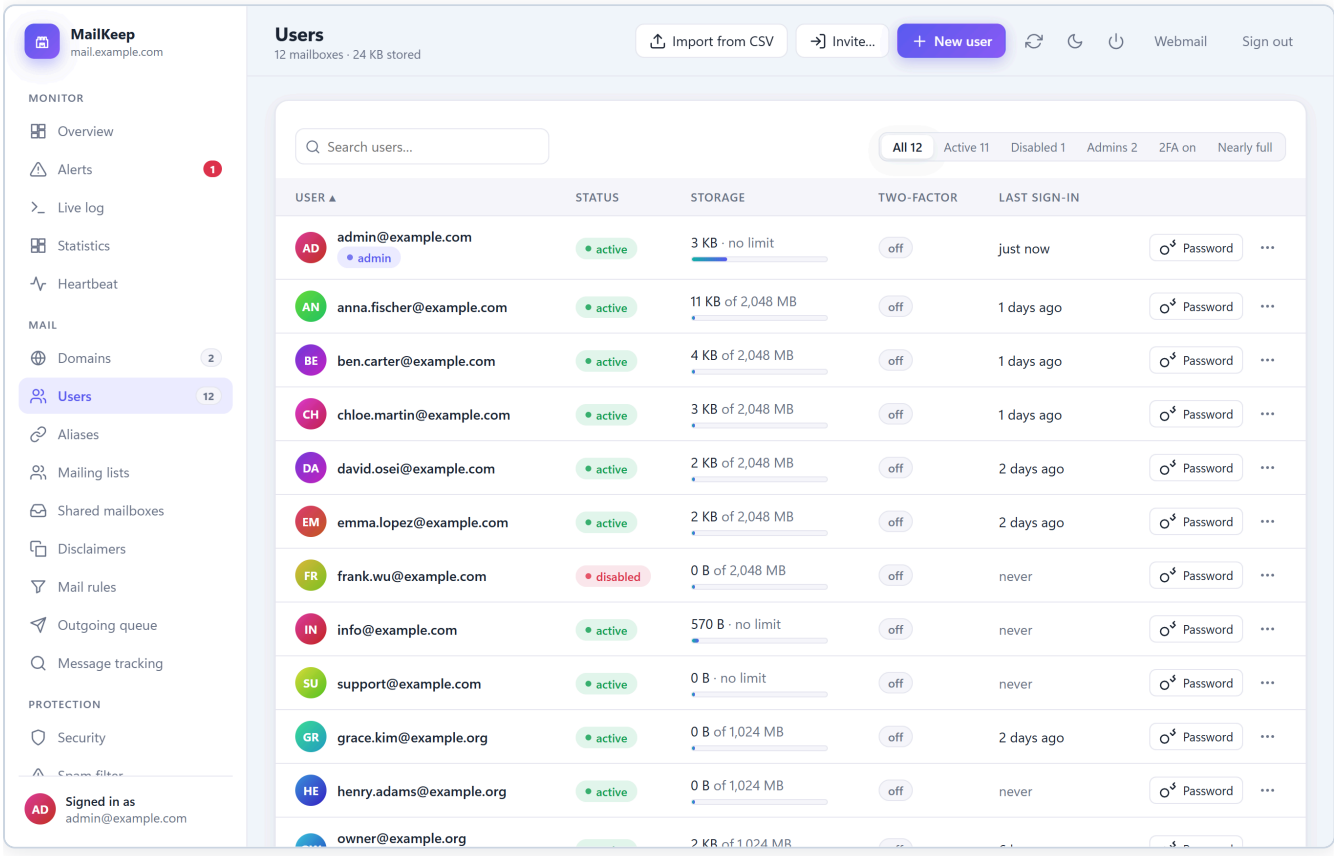


Figure 7.1 — The Users page.

Creating a mailbox

Click **New user**. Type the name part of the address and pick the domain from the list next to it (a domain administrator with one domain sees it filled in). Pasting a whole address such as `john@example.com` into the name box splits it for you. Then enter a password at least as long as the server's minimum (8 by default; shown on the box; chapter 14) (**Generate** makes a strong one) and optionally a size limit in MB (0 = no limit). The mailbox starts with the folders Inbox, Sent, Drafts, Trash and Junk.

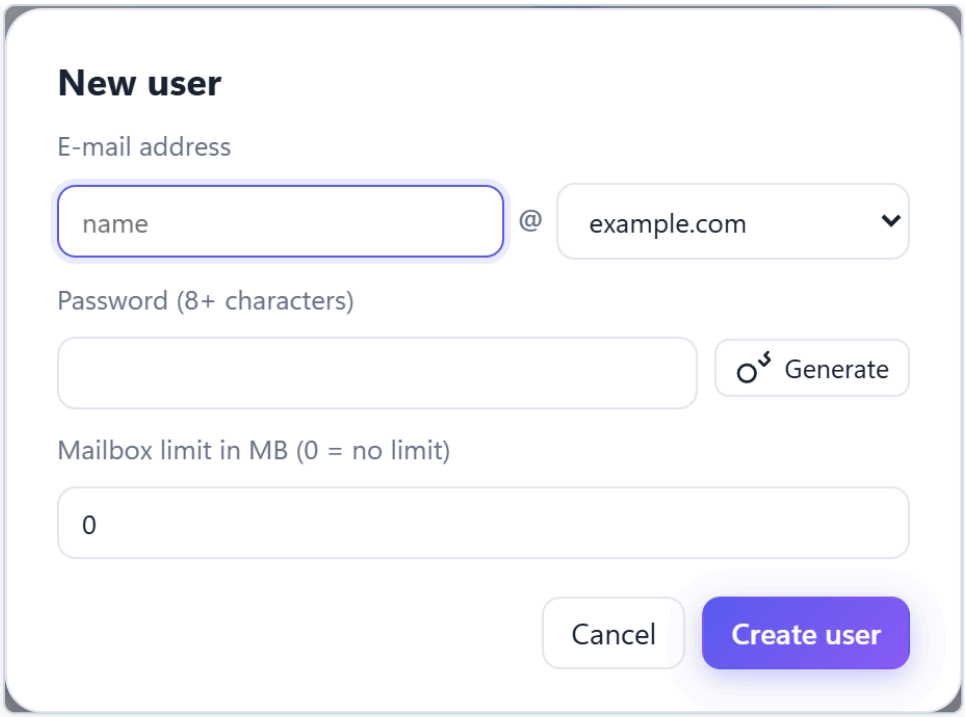


Figure 7.2 — Creating a mailbox.

```
mailserver user add bob@example.com --quota-mb 2048     # asks for the password
mailserver user add bob@example.com --password "…"
mailserver user list
```

Invite links: people create their own mailbox

Instead of choosing someone's password for them, send them a one-time link. Click **Invite…** on the Users page and choose:

- **Domain**, and optionally the **address** (empty = they choose the name themselves);
- how long **the link works** (for example 7 days), and the mailbox size limit.

Copy the link and send it to the person (by text message, or to their private address). Opening it shows a short sign-up page where they pick their address and password; they can also set up two-factor sign-in straight away. Each link works once. Links not used yet are listed under **Open invite links**, where you can cancel them. Nobody can create a mailbox without a link from an administrator.

Adding many mailboxes from a spreadsheet

For a new office or a move from another system, list the mailboxes in a spreadsheet and save it as CSV. One mailbox per line:

```
address,password,quota
liam.novak@example.com,,500
mia.rossi@example.com,Sunny-Harbour-27,2 GB
```

- Only the address is needed. An **empty password** gets a random one; the size limit can be in MB (`500`) or GB (`2 GB`), and empty means no limit.
- A first line of column names is skipped. Commas, semicolons (Excel in many countries) and tabs all work, and "quoted, values" too.
- The domains must already exist (chapter 6). Mailboxes that already exist are left alone, unless you tick **Also change the password and limit of mailboxes that already exist**.

1. On the Users page, click **Import from CSV**, then **Choose File**, or paste the lines into the box.
2. Click **Trial run**. Every line is checked and you see what would happen, without anything changing.
3. Fix any lines marked *Problem*, then click **Import**.
4. If any mailbox got a made-up password, click **Download passwords (CSV)** straight away: they aren't shown again.

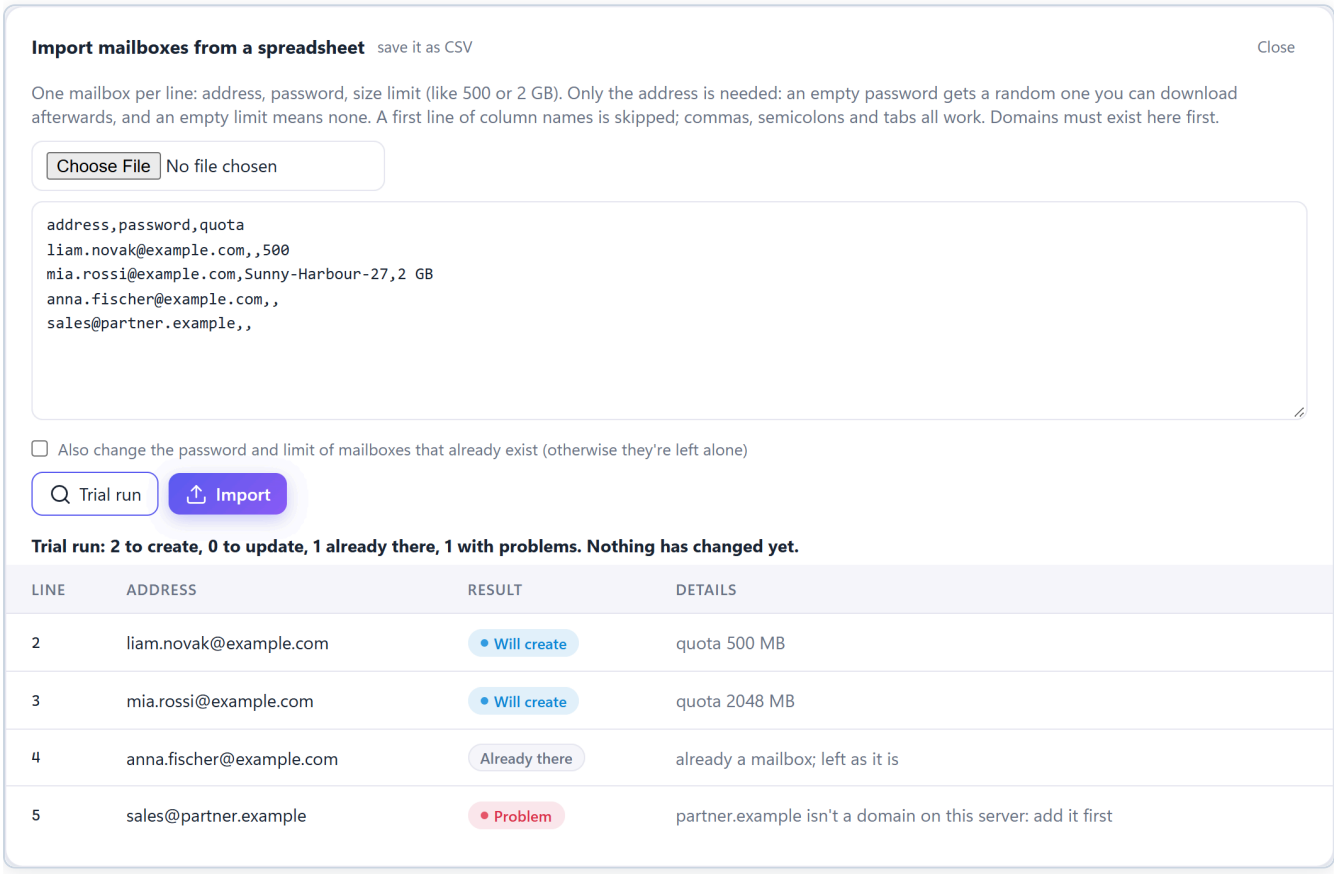


Figure 7.3 — A trial run: two mailboxes to create, one that already exists, one for a domain that isn't on this server.

A domain administrator can only import mailboxes for their own domains. From the command line:

```
mailserver user import staff.csv --dry-run      # check only
mailserver user import staff.csv                # made-up passwords are printed at the end
mailserver user import staff.csv --update       # also change existing mailboxes
```

Everyday tasks

Task	In the console	Command
Set a new password	**Password** on the user's row. Their other sessions are signed out; mail apps ask for the new password.	`user passwd bob@example.com`
Change the size limit	··· → **Change quota**	`user quota bob@example.com 4096`
Turn an account off	··· → **Disable account**: no sign-ins, mail to it is refused; nothing is deleted	`user disable bob@example.com`
Turn it back on	··· → **Enable account**	`user enable bob@example.com`
Reset two-factor	··· → **Reset two-factor** (when someone lost their phone)	`user 2fa disable bob@example.com`
Admin rights	··· → **Make administrator** / **Remove admin rights**	`admin add` / `admin remove`
Which services it may use, its own sending limit	··· → **Services and sending limit…**: switch off for example POP3 or webmail for this account, or give a shared or newsletter account a different hourly limit	
Name, job title and phone; meeting rooms	··· → **Name, title and phone…**: shown in the company directory (chapter 20), or hide the account from it. *This mailbox is: A meeting room* makes it a room that accepts invitations when free and declines when booked.	
Download the whole mailbox	··· → **Download mailbox (.zip)**: one `.mbox` file per folder, which Thunderbird, Apple Mail and archive tools open	
Delete a mailbox	··· → **Delete user**: deletes the account and all its mail, calendars and contacts	`user remove bob@example.com`

> *i* **Mailbox full**
>
> When a mailbox reaches its limit, new mail for it is refused with a "mailbox full" error so the sender knows, and mail apps can't add more. The storage bar turns red above 85%.

When someone leaves

··· → **Someone is leaving…** does the usual hand-over in one step:

- **Give a colleague full access** to the mailbox (they can also send as this address); optionally **also forward new mail** to that colleague.
- An **automatic reply** tells senders who to write to instead.
- **Signing in** is switched off, so the person who left can't get in any more; mail keeps arriving.
- The account is **hidden from the company directory**.

Download the mailbox as a .zip first if you need a copy for your records. Later, when nobody needs the mail any more, delete the user.

Out-of-office and forwarding for a user

Users normally set these themselves in webmail (chapter 20). An administrator can set them from the command line:

```
mailserver user vacation bob@example.com --message "I'm away until Monday." [--subject "Out of
office"] [--days 7]
mailserver user vacation bob@example.com --off
mailserver user forward bob@example.com bob@gmail.com          # keeps a copy
mailserver user forward bob@example.com bob@gmail.com --no-copy
mailserver user forward bob@example.com --off
```

Automatic replies go to each sender at most once every *days* days, and never to mailing lists, robots, bounces or Bcc copies.

Paused sending

If an account suddenly sends far more than usual — typically because its password was stolen — its sending is paused automatically. Its row shows **sending paused**. See chapter 12 for how to resume it.

CHAPTER 8

Aliases and catch-all addresses

Extra addresses that deliver to an existing mailbox.

What an alias is

An alias is an address without a mailbox of its own: mail to it is delivered to a mailbox you choose. Use aliases for role addresses that one person handles (`sales@`, `billing@`) or for old addresses someone should keep receiving. The person can also **send** from their aliases — the server allows a signed-in user to use their own address and any alias that delivers to them.

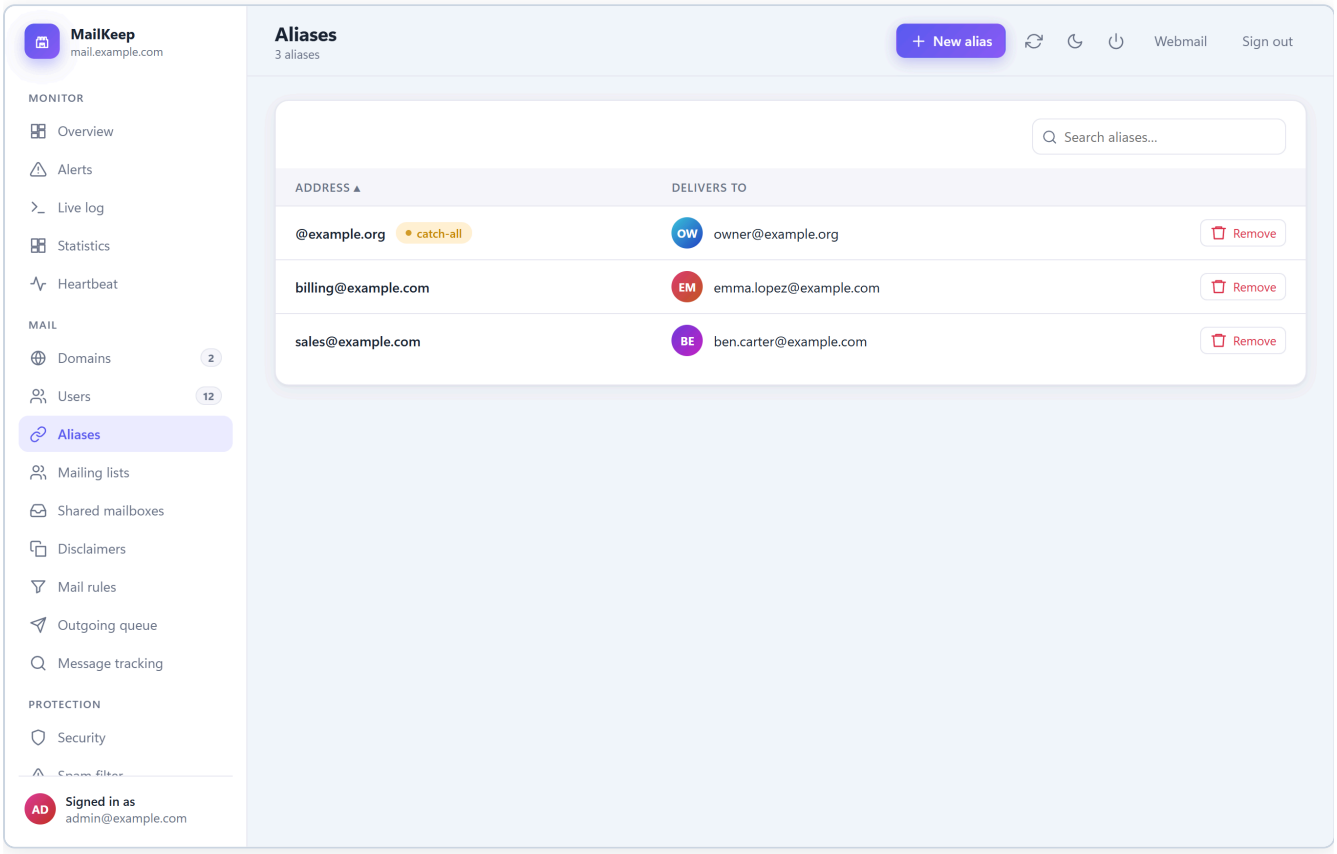


Figure 8.1 — The Aliases page.

Adding and removing aliases

Click New alias, type the name and pick the domain, then enter the mailbox it delivers to. Remove on its row deletes it; mail to the address is refused from then on.

```
mailserver alias add sales@example.com ben.carter@example.com
mailserver alias list
mailserver alias remove sales@example.com
```

Catch-all addresses

An alias written as `@example.com` catches mail to **any** address at that domain that has no mailbox, alias or list of its own. In the New alias dialog, leave the name empty and pick the domain; MailKeep asks you to confirm before creating a catch-all.

```
mailserver alias add @example.com owner@example.com
```

> ! **Catch-alls attract spam**
>
> Spammers send to made-up addresses at every domain they find; a catch-all accepts all of it. Use one only while moving in or when you really need it. Specific addresses always win over the catch-all, so as soon as a mailbox such as `info@` exists, its mail goes there instead.

Several people for one address?

An alias delivers to one mailbox. For an address that several people should receive or work on together, use either:

- a **mailing list** (chapter 9) when everyone should get their own copy, or
- a **shared mailbox** (chapter 10) when the team should work from one inbox, seeing who has read and handled what.

CHAPTER 9

Mailing lists

One address that reaches every member, with moderation, daily digests and a web archive.

How lists work

Mail sent to a list address (e.g. `team@example.com`) is delivered to every member as their own copy. Each copy is DKIM-signed and carries standard list headers, including a one-click unsubscribe link that Gmail and Yahoo show as an *Unsubscribe* button. Whether someone may post is checked while the mail is still arriving, so refused senders get an error from their own server and no bounce is ever sent to a forged address.

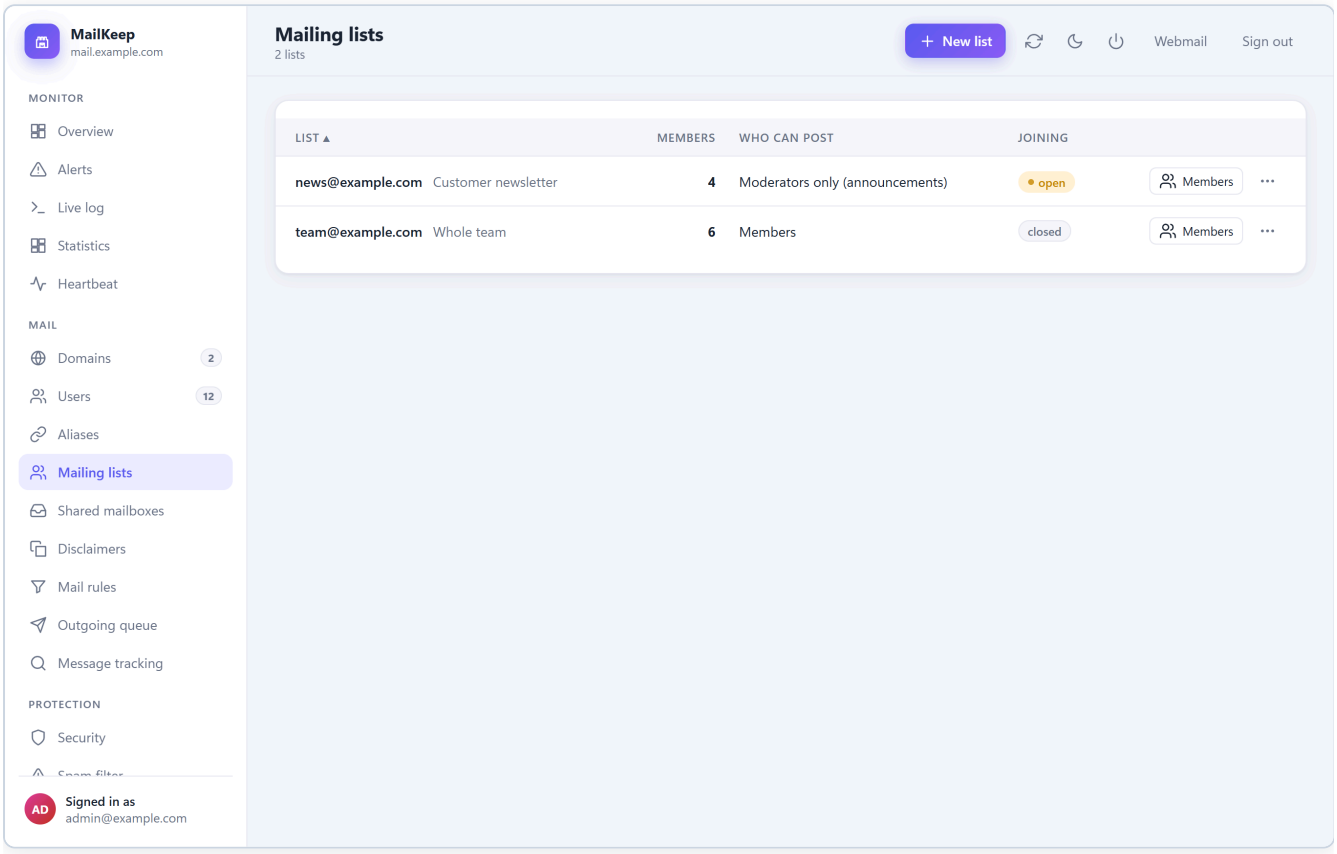


Figure 9.1 — The Mailing lists page.

Creating a list and adding people

1. Click **New list**, type the name part of the list address and pick its domain, then give it a name, e.g. *Our team*.
2. Click **Members** on its row, then **Add people**. Paste any number of addresses (separated by commas, spaces or new lines) and choose *Members* or *Moderators*.
3. Open ⋯ → **Settings** to choose who may post and how the list behaves.

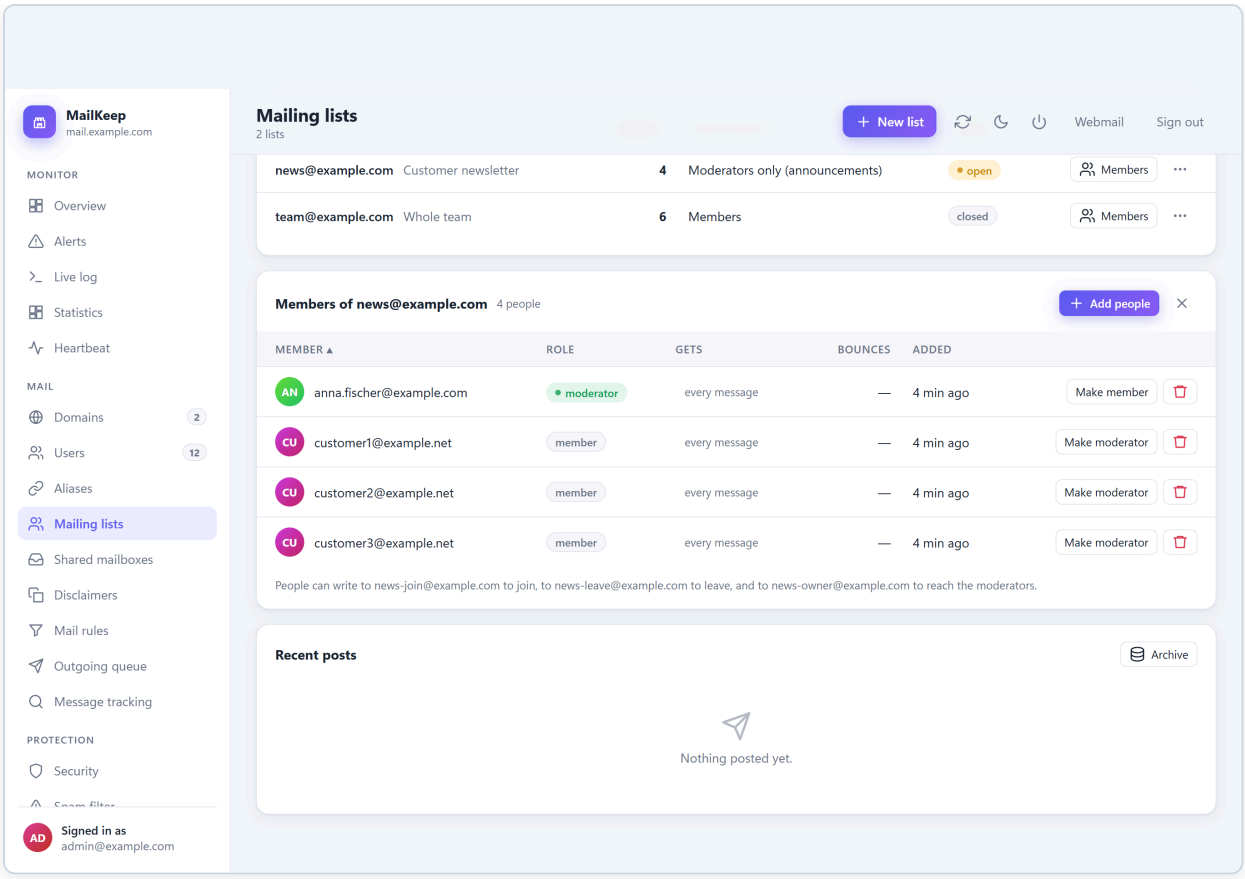


Figure 9.2 — A list's members, recent posts and special addresses.

```
mailserver list add team@example.com --name "Our team"
mailserver list subscribe team@example.com anna@example.com ben@example.com
mailserver list subscribe team@example.com boss@example.com --moderator
mailserver list members team@example.com
mailserver list unsubscribe team@example.com ben@example.com
```

List settings

Setting	Choices
Who can post	**Members** (default), **Anyone**, or **Moderators only** — an announcement list such as a newsletter
Joining	**Only admins add people** (closed), or **Anyone may join**, confirmed by e-mail
Replies go to	The whole list, or just the sender
Posts from people who may not post	**Refuse them**, **Hold for a moderator**, or **Hold every post for a moderator**
Archive of past posts	Members can read it (signed in to webmail), anyone can read it (sender names only), or no archive
Subject prefix	Put in front of every subject, e.g. `[team]`
Footer	Text added under every message

Setting	Choices
Description	Sent to new members

```
mailserver list set team@example.com --post members --subscribe closed --reply-to list \
    --prefix "[team]" --moderation hold --archive members
```

The list's special addresses

Every list gets a few extra addresses automatically. For `team@example.com`:

Address	What it does
`team-join@example.com`	Asks to join. On an open list a confirmation e-mail is sent; on a closed list the moderators are told.
`team-leave@example.com`	Leaves the list, after confirming by e-mail or link.
`team-owner@example.com`	Reaches the list's moderators.
`team-bounces@example.com`	Collects bounces. Each member's bounces are counted and shown on the Members page.

Moderation

When a post is held, the moderators get an e-mail with a link to a page where they can approve or reject it; the link page shows a button, so a link scanner opening it doesn't decide anything. Held posts also appear in the **Waiting for approval** panel on the list's Members page, and are deleted after 14 days if nobody decides. At most 10 posts per list wait at a time.

```
mailserver list held team@example.com     # shows each held post with its number
mailserver list approve 42
mailserver list reject 42
```

Daily digests

A member can get one e-mail a day with all the day's posts instead of every message. Click **every message** / **daily digest** in the member's *Gets* column to switch, or:

```
mailserver list digest team@example.com anna@example.com on
```

The web archive

With the archive on, past posts can be read at `https://mail.example.com/lists/archive/team@example.com/`. A members-only archive asks the visitor to sign in to webmail first. The **Archive** button on the Recent posts panel opens it.

Outside senders and DMARC

When someone from another domain posts to a list, their domain's DMARC policy could make receivers reject the copies, because the list re-sends their mail. MailKeep therefore rewrites the From line of such posts to "*Their Name via Our team*" at the list's own address, with Reply-To set to them. Posts from your own domains keep their From line.

CHAPTER 10

Shared mailboxes

Team inboxes such as info@ and support@, and letting people open other people's folders.

What a shared mailbox is

A shared mailbox is an address several people read and answer together. Nobody signs in to it directly; instead you give people access, and it appears in their own mail app under **Shared**. Everyone sees the same messages, and read/unread state and flags are shared, so the team can see what's been handled.

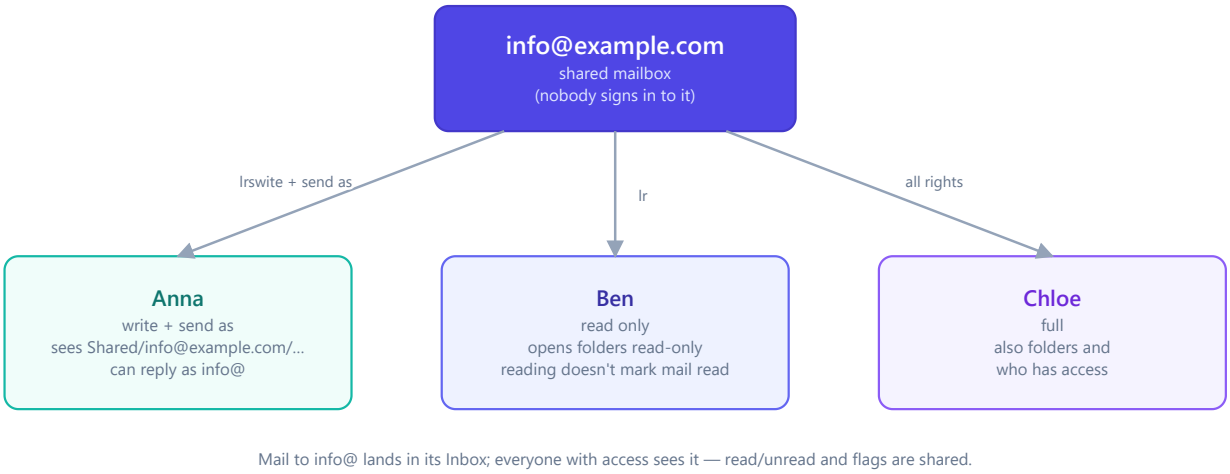


Figure 10.1 — One shared mailbox, three people with different access.

Any ordinary mailbox can be shared the same way — for example, an assistant given access to a manager's Inbox.

Access levels

Level	The person can…	Technical rights
Read only	See the folders and read mail. Folders open read-only, and reading doesn't mark mail as read for everyone else.	`lr`
Read and change	Also mark read/unread, flag, delete, move mail out, and file or copy mail in.	`lrswite`
Full	Also create and delete folders, and decide who else has access.	`lrswipkxtea`
Send as (extra)	Send mail with the shared address as the From address. Only with access to all folders.	—

Access can be given to the whole mailbox or to one folder. A grant on a folder also covers its subfolders, and the most specific grant wins.

Creating a shared mailbox

1. Open **Shared mailboxes** and click **New shared mailbox**.
2. Type the name part of the address (e.g. `info`), pick the domain, and give it a name (e.g. *Info desk*). If the address already exists as a mailbox — for example one moved in from MailEnable — it becomes a shared one and keeps its mail.
3. Click **Give access** on its panel for each person: choose the person, all folders or one folder, the access level, and whether they may send as the address.

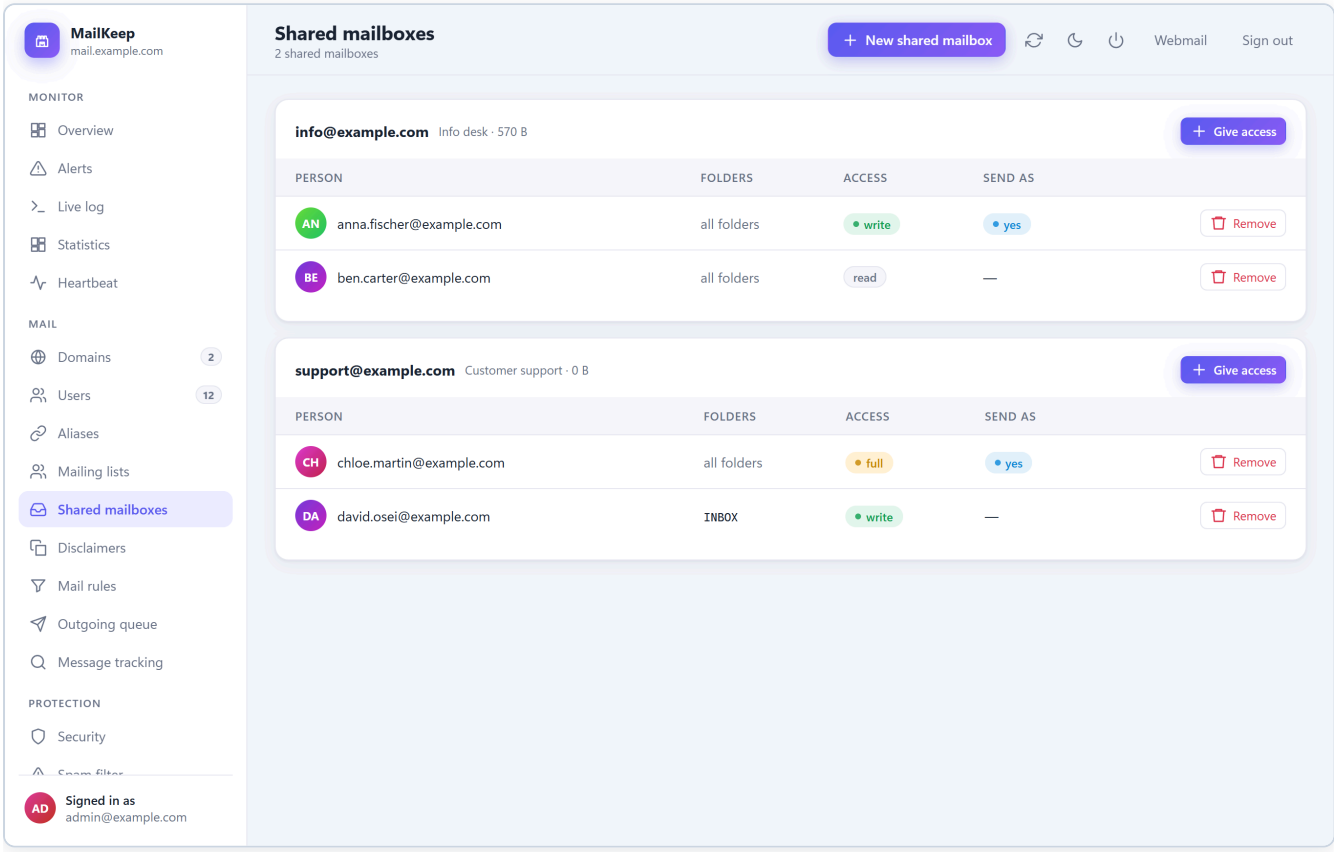


Figure 10.2 — The Shared mailboxes page, with who has access to each.

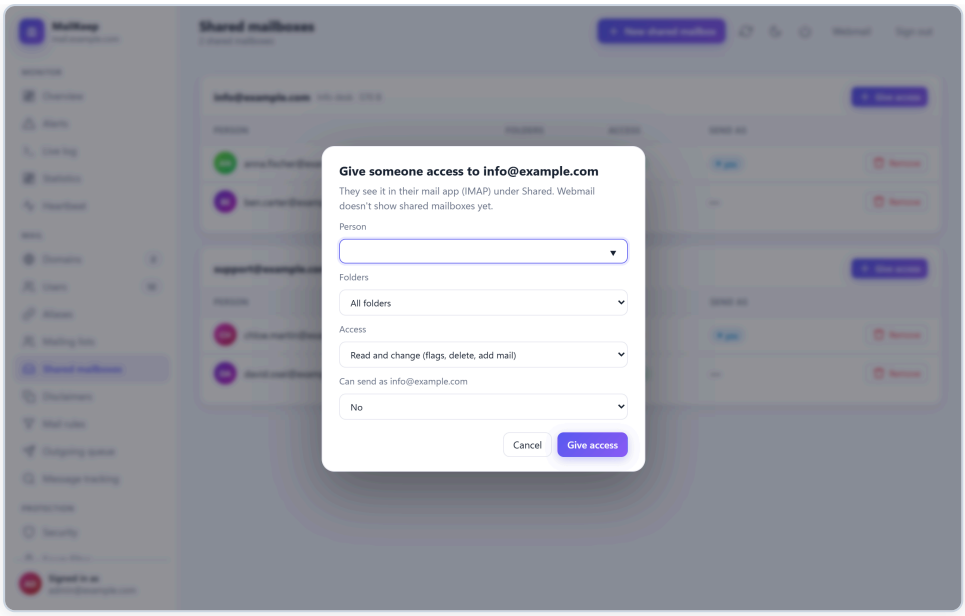


Figure 10.3 — Giving someone access.

To change someone's access, use **Give access** again with the same person and folder; the new level replaces the old one. **Remove** on their row takes it away — the folders disappear from their mail app at its next refresh.

From the command line

```
mailserver shared add info@example.com --name "Info desk"
mailserver shared mark old-sales@example.com           # an existing mailbox becomes shared
mailserver shared grant info@example.com anna@example.com --level write --send-as
mailserver shared grant info@example.com ben@example.com --level read --folder INBOX
mailserver shared list
mailserver shared revoke info@example.com ben@example.com --folder INBOX
```

How people use it

In any IMAP mail app — Outlook, Thunderbird, Apple Mail, phones, Mailroom — the mailbox appears as a folder tree:

```
Shared
 └ info@example.com
    ├ INBOX
    ├ Sent
    └ …
```

Shared and *info@example.com* are headings only (shown greyed out in some apps); open the folders under them. Some apps only show shared folders after you refresh or "show all folders". Mail filed into a shared mailbox counts against its own size limit, not the person's.

Webmail

In webmail, each shared mailbox appears below your own folders under its address, and someone with "send as" can pick it as the From address (chapter 20). Webmail only offers what the access level allows: with *Read*, there is no Delete or Move.

For mail-app users and administrators

Apps that support the IMAP ACL extension can also show and change access themselves (MYRIGHTS, GETACL, SETACL, DELETEACL, LISTRIGHTS). Only the owner, or someone with full access, can change who has access, and only people with a mailbox on this server can be given access.

CHAPTER 11

Disclaimers

Text added under every message a domain's users send.

Setting up a disclaimer

Each domain can have its own disclaimer: a company signature, address, or confidentiality notice added under every message its users send.

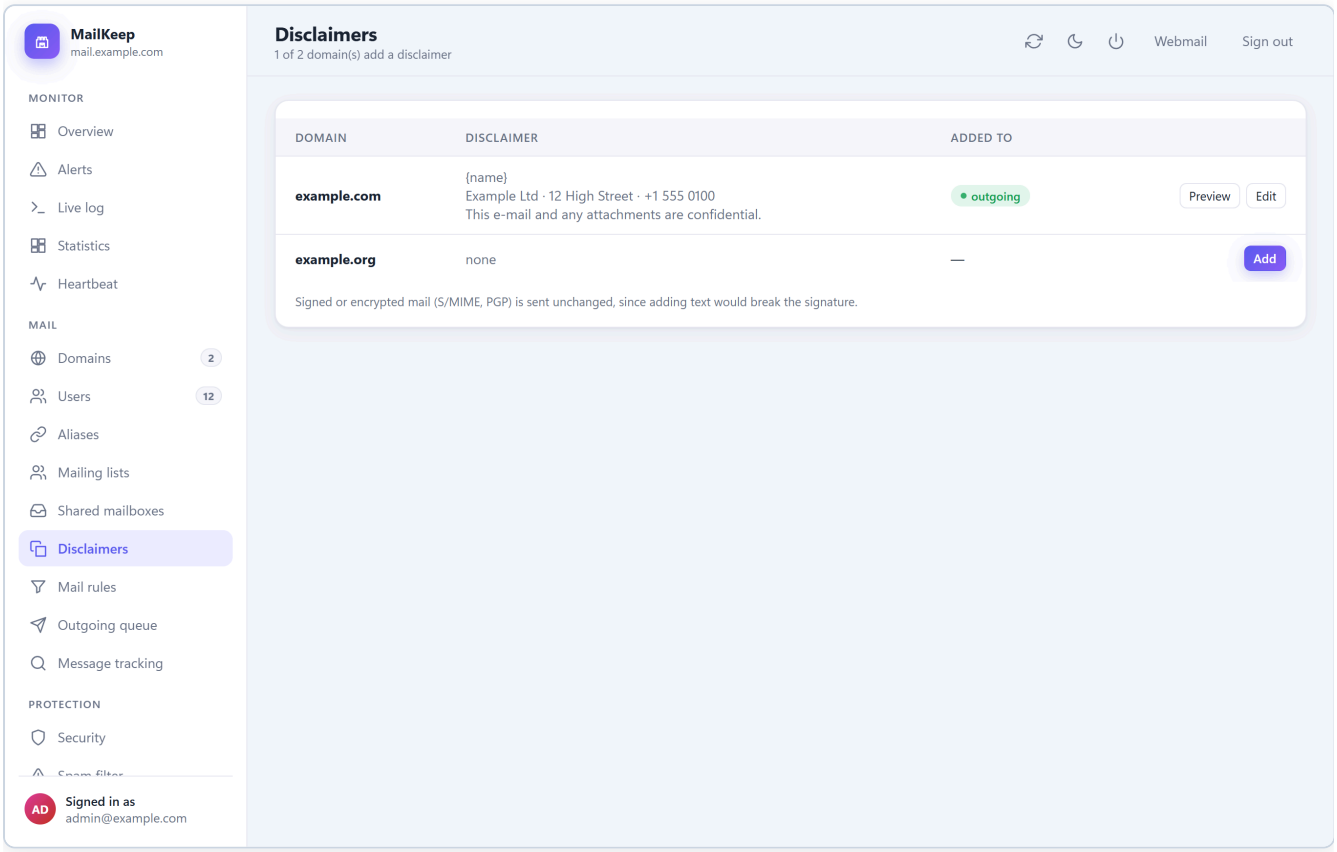


Figure 11.1 — The Disclaimers page.

1. Open **Disclaimers** and click **Add** next to the domain.
2. Write the **Text**. `{name}`, `{address}` and `{domain}` are filled in for each sender.
3. Optionally write an **HTML version** for formatted mail. Without one, the text is used in HTML mail too.
4. Choose **Add it to**: *Mail to other domains* (outgoing only), or *All mail, also inside the company*.
5. Set the **Status** to On, and save. **Preview** shows how a message from the domain will look.

```
{name}
Example Ltd · 12 High Street · +1 555 0100
This e-mail and any attachments are confidential.
```

What gets changed

- Plain-text and HTML parts each get their own version; attachments are untouched.
- Messages are re-encoded correctly whatever character set or encoding they used.
- **Signed or encrypted mail** (S/MIME, PGP) is sent unchanged, since adding text would break the signature.
- Setting the Status to Off keeps the text for later. Clearing the text removes the disclaimer.

CHAPTER 12

Sending mail and the outgoing queue

How mail reaches other domains, relays, the queue, and protection against hacked accounts.

How sending works

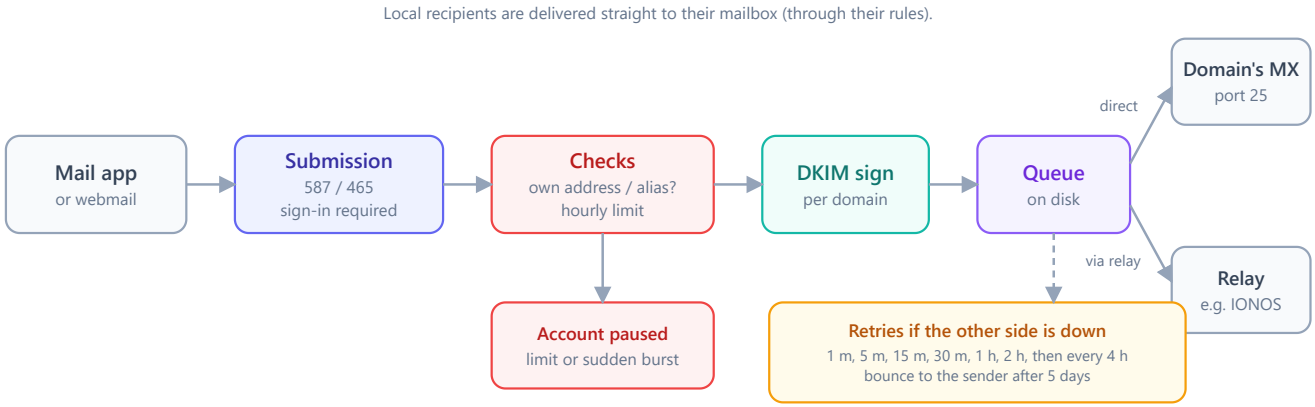


Figure 12.1 — The path of an outgoing message.

- **Signing in is required.** Port 25 accepts mail only for your own domains; nobody can use the server to send elsewhere without signing in (no "open relay").
- **Only your own addresses.** A signed-in user may send as their own address, their aliases, and shared mailboxes they have "send as" on. Anything else is refused.
- **Tidy messages.** A missing Date or Message-ID is added, Bcc lines are removed, and the message is DKIM-signed.
- **Local recipients** are delivered straight away, through their own mail rules.
- **Other domains**: the queue looks up the domain's mail servers (MX records), tries them in order with encryption (STARTTLS) whenever offered, and records the result.
- **Strict encryption where the other side asks for it.** If the receiving domain publishes an **MTA-STS** policy, or **DANE** (TLSA records signed with DNSSEC), mail goes to it only over an encrypted connection with the right certificate, so nobody in between can read or redirect it. Both are on by default (**Follow other domains' MTA-STS policies**, **Follow other domains' DANE records**).

Retries and bounces

If the other side is down or says "try later", the message stays in the queue and is retried after 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, and then every 4 hours. After 5 days (**Give up after**, `max_queue_hours` = 120) — or straight away when the other side refuses permanently — the sender gets a delivery report explaining what went wrong. A crash or restart never loses queued mail.

No bounces to forged senders

Spam nearly always carries a made-up sender address. Sending a delivery report ("bounce") back to it hits an innocent stranger or a throwaway domain, and servers that do this a lot (*backscatter*) end up on blocklists. So MailKeep avoids bouncing mail from outside:

- **Full mailboxes are refused at the door.** When a mailbox is already over its quota, the other server is told `552 mailbox full` for that recipient during the conversation, and it tells its own sender. The other recipients still get the message. Message tracking shows *mailbox full*.
- **Bounces go only to senders that check out.** When something fails after a message from outside was accepted (it didn't fit in the mailbox, or a user's mail rule rejects it), a bounce is sent only if the sending server passed SPF for the sender's domain and the message doesn't look like spam. Otherwise the failure is only written to the log.
- Your own users (signed in, or on the local network) always get their bounces, as above.

Mail the server writes itself (out-of-office replies, bounces, alert and journal e-mails) is DKIM-signed with the key of the sender's domain, or of the hosted domain the server's name belongs to (`mail.example.com` → `example.com`). With an empty envelope sender, that signature is what lets Gmail and Yahoo accept it. A TXT record `v=spf1 a ~all` on the server's name gives it a passing SPF check too.

Items with an empty sender in the queue are messages the server itself sends: bounces, and the daily DMARC and TLS reports (chapter 16). The page tags them *bounce* either way; the subject tells them apart (*Report Domain:* … for a report).

The Outgoing queue page

Lists every message waiting, with its sender, size, age, and for each recipient the number of attempts, the next attempt and the last error.

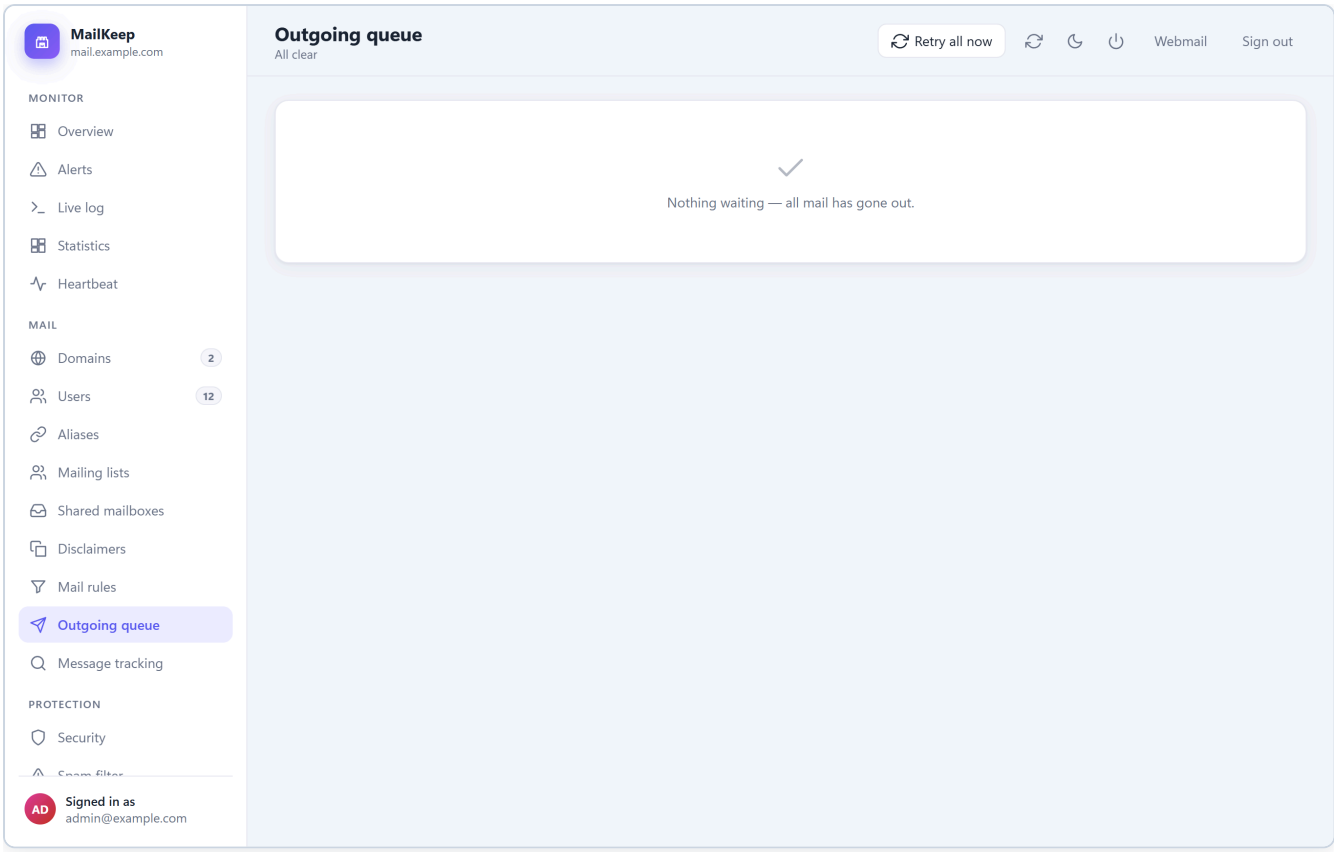


Figure 12.2 — The Outgoing queue (empty when everything is delivered).

- Retry all now tries every waiting message straight away, for example after fixing a network problem.
- Delete drops a message without delivering or bouncing it.

```
mailserver queue list
mailserver queue retry
mailserver queue delete 17
```

To follow one message from the queue to the other server (or to its bounce), search for it under Message tracking (chapter 16).

Sending through a relay

A relay (or "smart host") sends your mail on for you. Use one when your provider blocks outgoing port 25, or when your IP address has a poor reputation.

- **One relay for everything**: Settings → Sending to other domains → Relay server, with user name, password and encryption.
- **A relay for one domain**: Domains → ⋯ → Send through a relay… (chapter 6). Other domains are unaffected.
- **A fixed server for a recipient domain**: `[outbound.routes]`, e.g. `"partner.com" = "mx.partner.com:25"`.

```
mailserver check-relay                    # signs in to the relay without sending
mailserver check-relay --domain example.com
mailserver check-mx gmail.com             # can this machine reach port 25 out?
```

On a server with several IP addresses, set **Settings → Sending to other domains → Send from address** (`source_ip`) so mail leaves from the address your SPF and reverse DNS describe (chapter 4). Setup check warns when the sending address, the server name and its reverse DNS don't match.

Mail rules (server-wide)

The **Mail rules** page holds rules that apply to everyone, like Exchange's mail flow rules. Each rule has:

- **Direction**: mail coming in from outside, mail your users send out, or both.
- **Conditions**: the sender, a recipient, the subject, an attachment's name or type, any header, or the size.
- **An action**: refuse the message, redirect it, send a copy to someone, add a header, or tag the subject (such as `[Invoice]`).

Rules run before each user's own rules (chapter 20). Typical uses: a copy of all mail mentioning "invoice" to the accounts department, refusing `.zip` attachments from outside, or tagging mail over 20 MB.

Protection against hacked accounts

A stolen password is usually used to send spam as fast as possible. MailKeep watches every account's sending:

- **Hourly limit**: at most **Recipients per user per hour** (500) recipients.
- **Sudden bursts**: more than 10 times the account's busiest hour of the past two weeks, counted from 100 recipients an hour, so a quiet account's normal newsletter isn't caught.

MailKeep also runs the **spam content checks on outgoing mail** (**Check outgoing mail for spam**, on by default). A message to other domains that scores as spam is refused with a clear message to the sender, and the administrators get an alert: a hacked account sending spam is stopped before it harms your server's reputation.

When either limit is hit, the account's sending is **paused**: new mail from it is refused, mail it already queued is held, and the user and every administrator get a notice. Nothing is lost. Its row on the Users page shows *sending paused*.

Change the password first (and check the account's forwarding rules), then resume sending under **Security → Sending paused**: **Resume and send** delivers the held mail, **Discard and resume** deletes it. If **Pause accounts that hit the limit** is off, the limit simply refuses mail for the rest of the hour.

CHAPTER 13

Spam, viruses and the quarantine

How mail from the internet is checked, how users train the filter, and how to rescue mail that was held.

The spam score

Every message arriving from the internet gets a score. Mail from signed-in users isn't scored.

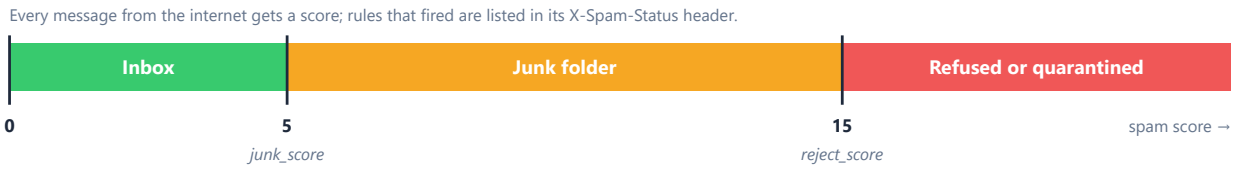


Figure 13.1 — What happens at each score.

The score is the sum of everything the checks found. Each message carries an `X-Spam-Status` header listing the rules that fired, and an `Authentication-Results` header with the SPF, DKIM and DMARC results — useful when someone asks why a message went to Junk.

Check	What it looks at
SPF, DKIM, DMARC, reverse DNS	Whether the sending server may send for the domain, the signature, and the domain's own policy. DMARC `p=reject` is refused, `p=quarantine` goes to Junk.
Blocklists	The sender's address on Spamhaus ZEN, SpamCop and Barracuda (by default). Adds to the score, or refuses outright if you choose.
Content rules	Missing headers, shouting subjects, servers lying about their name, outsiders using your own domain, lookalike and punycode domains, links whose text shows a different site, numeric-IP and shortener links, spam phrases, HTML-only mail, macro attachments.
Dangerous attachments	Programs and scripts (exe, scr, js, vbs, iso, lnk, …), including double extensions like `invoice.pdf.exe` and disguised Windows programs. Never delivered.
Viruses	With ClamAV installed, every message is scanned. Infected mail is never delivered.
Learning filter	Each user's own filter, trained by their Junk decisions (below).
Greylisting (optional)	Unknown senders are asked to try again a few minutes later; most spam programs never do.

The learning filter

Each user has their own learning filter. It learns when they:

- move mail **into** Junk (this is spam), or **out of** Junk to anywhere but Trash (this is fine),

- press **Junk** / **Not junk** in webmail, or the Junk buttons in Thunderbird and Apple Mail.

Changing your mind un-learns the old decision. A user's filter starts voting once it has seen 20 messages of each kind. The Spam filter page shows how far each user's filter has been trained.

The Newsletters folder

Bulk mail from real companies (newsletters, marketing, notifications sent through mailing services) isn't spam, but it crowds the Inbox. With Newsletters folder on (the default, in the Spam filter page's Settings), it goes to a folder called **Newsletters** instead, a little like Gmail's Promotions tab. Nothing is refused and nothing goes to Junk.

A message counts as bulk mail when it has an unsubscribe header, a "bulk" marker, or the fingerprints of a big mailing service. Replies in a conversation always stay in the Inbox, even from a mailing list.

It learns per sender, from the user's own moves (in webmail or any mail app):

- moving a message from Newsletters back to the **Inbox** keeps that sender in the Inbox from then on,
- moving one from the Inbox **into** Newsletters sends that sender there from then on.

A choice covers the sender's whole domain, so teaching `news.example.com` also covers `mail.example.com`. Each user can turn the folder off for themselves in webmail (⚙ Settings → Writing, under Reading); the server setting is only the default.

Allow and block lists

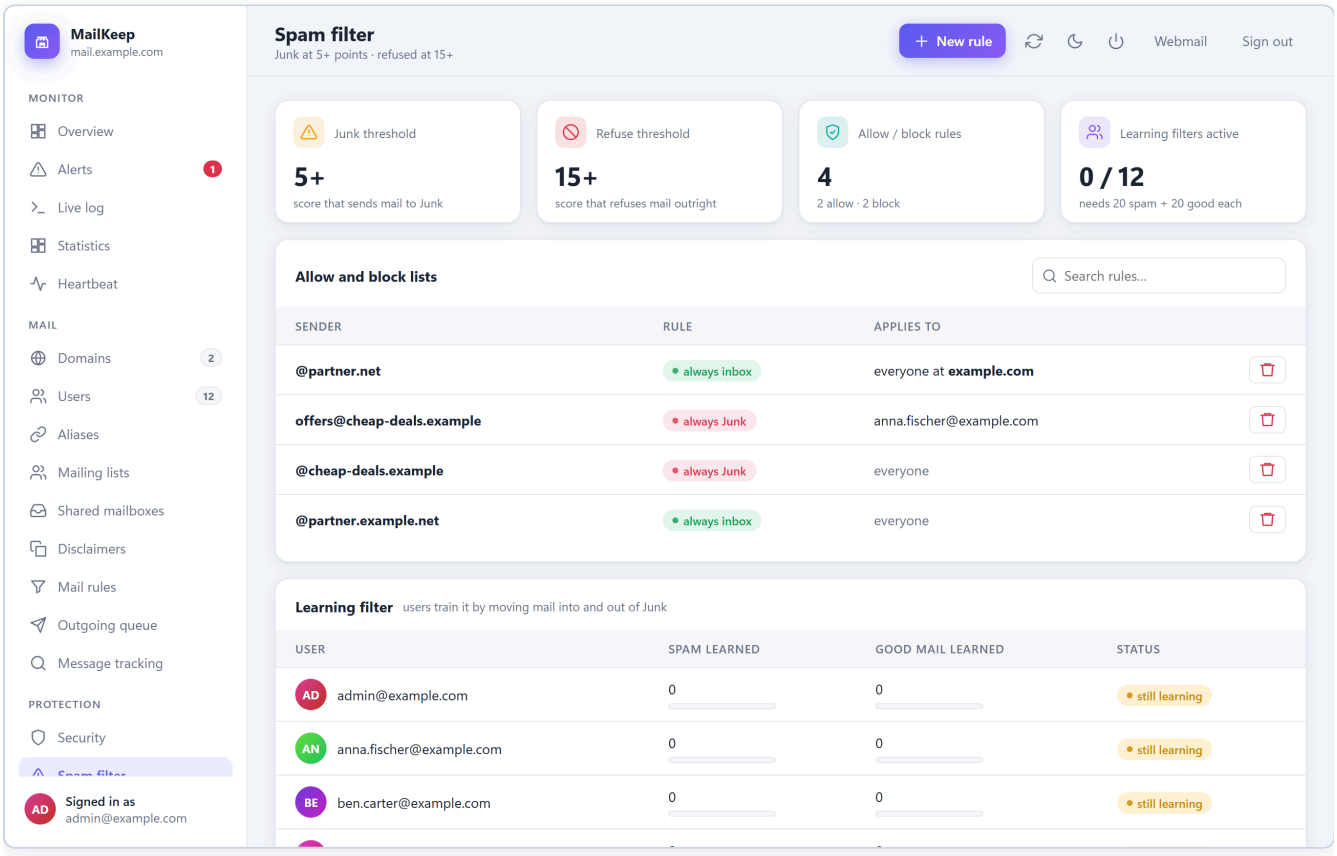


Figure 13.2 — The Spam filter page: allow/block lists, training, the virus scanner and the main settings.

An **allow** entry always delivers mail from an address or domain to the Inbox; a **block** entry always sends it to Junk. Under **For**, an entry applies to:

- **everyone** on the server (leave it empty),
- **everyone in one domain**: `@example.com`, shown as *everyone at example.com*,
- or **one mailbox**: `anna@example.com`.

A mailbox's own entry wins over its domain's, and the domain's over everyone's. Domain administrators see and add entries for their own domains and mailboxes only.

```
mailserver spam allow partner.com                          # for everyone
mailserver spam block offers@cheap.example --user anna@example.com
mailserver spam list
mailserver spam remove partner.com
mailserver spam stats                                      # training per user
mailserver spam check message.eml --ip 203.0.113.5         # why did it score that?
```

The spam settings

The main switches are in the **Settings** panel at the bottom of the Spam filter page: the filter on or off, the **Junk** and **Refuse** scores, the blocklists (and whether a listing refuses mail outright), greylisting, the learning filter, the check of outgoing mail, and the **outside-mail warning** (below). The technical options (SPF/DKIM checks, attachment types, ClamAV's address, link blocklists, reverse DNS, server names, ARC sealing) are in Settings → Spam and viruses.

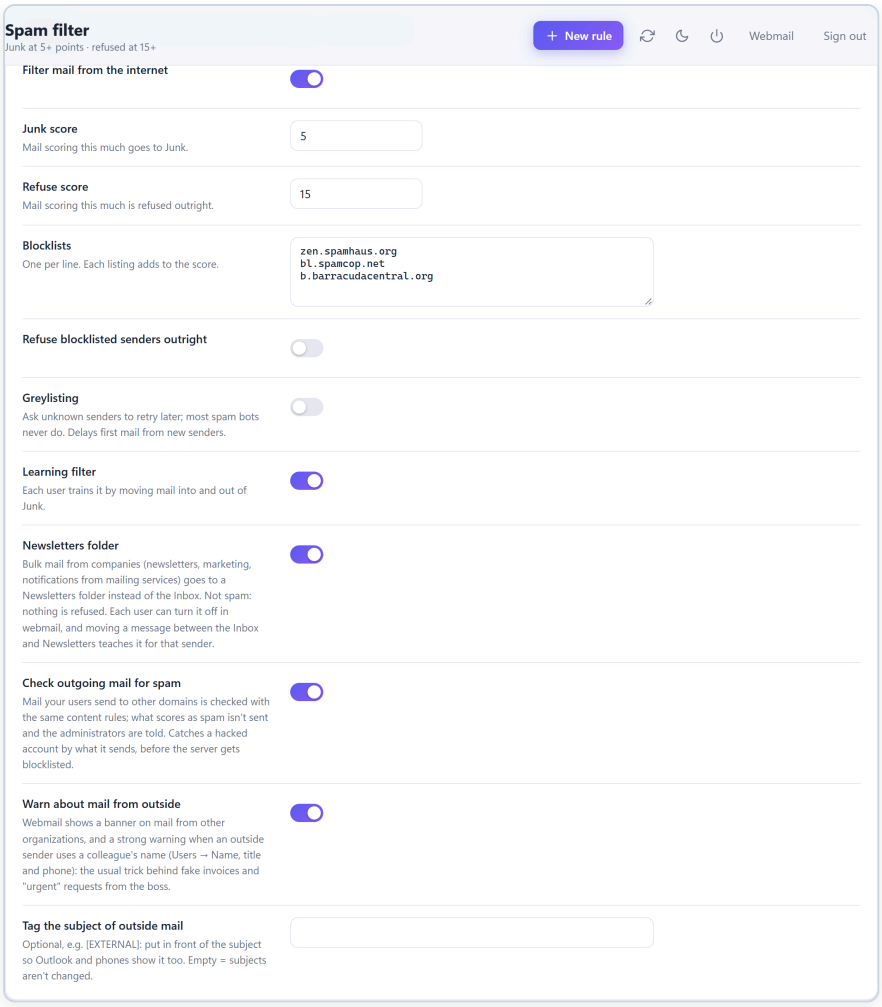


Figure 13.3 — The Spam filter page's Settings panel.

Warnings about mail from outside

With **Warn about mail from outside** on, webmail shows a banner on mail from outside your organization. Mail from outside that **uses a colleague's name** (the usual "CEO fraud" and fake-invoice trick) gets a red *Be careful* warning instead; once the sender is saved in the user's contacts, it stops. **Tag the subject of outside mail** also adds a tag such as `[EXTERNAL]` to the subject, for Outlook and phones.

Users can press **Report phishing** on a suspicious message in webmail: it moves to Junk and the administrators get an alert with the sender and subject, so they can block it for everyone.

Virus scanning with ClamAV

MailKeep checks attachments with **ClamAV**, the free open-source virus scanner. Install it on the server:

1. Download the Windows installer from **clamav.net** → **Downloads**: the file whose name contains **x64** and ends in **.msi** (not arm64 or win32), and install it to `C:\Program Files\ClamAV`.
2. In an administrator PowerShell, copy the two example settings files:

```
cd "C:\Program Files\ClamAV"
copy .\conf_examples\freshclam.conf.sample .\freshclam.conf
copy .\conf_examples\clamd.conf.sample .\clamd.conf
```

In **both** files delete the line that just says `Example`. In `clamd.conf` make sure these lines have no `#` in front:

```
TCPSocket 3310
TCPAddr 127.0.0.1
```

3. Download the virus definitions and install both services:

```
.\freshclam.exe
.\freshclam.exe --install-service
.\clamd.exe --install-service
net start clamd
net start freshclam
Set-Service clamd -StartupType Automatic
Set-Service freshclam -StartupType Automatic
```

The first download is about 110 MB. clamd uses about 1–1.5 GB of memory; freshclam updates the definitions by itself several times a day.

4. In Settings → Spam and viruses → ClamAV virus scanner, enter `127.0.0.1:3310`, save and restart.
5. On the **Spam filter** page, press Test the virus scanner.

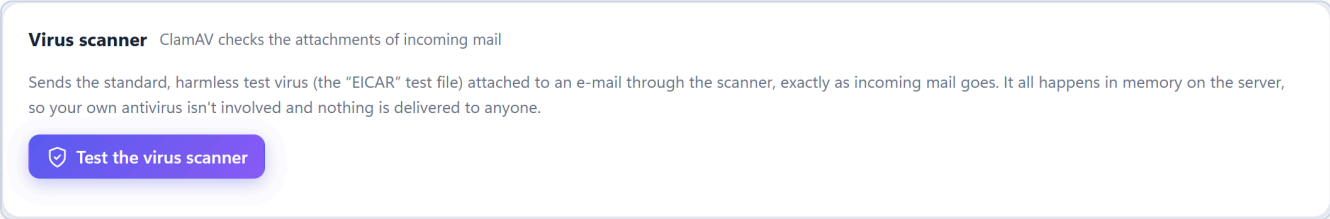


Figure 13.4 — The test sends the standard harmless test virus (EICAR) through the scanner, in memory, as incoming mail goes.

The test answers *Caught* (all fine), *Not caught* (the definitions are missing: run `freshclam.exe` and restart clamd), *Didn't answer* (start the clamd service), or *not set up*. Your own antivirus isn't involved and nothing is delivered. Choose what happens if the scanner is down: Deliver if the virus scanner is down (default), or ask senders to retry later.

The Overview's *Virus scanner* line asks ClamAV live and turns red when it doesn't answer; an alert is sent if it stays down. After a reboot, MailKeep gives clamd 5 minutes to load its signatures before it counts as down.

Viruses caught

The **Spam filter** page's Viruses caught card counts infected messages stopped in the last 24 hours and the last 30 days (a message to several people counts once), and lists the viruses found, most common first. Show them opens Message tracking filtered to *Viruses*, with each message's sender, recipients, the sending server's

address and whether it was refused or held. A domain administrator sees only mail to their own domains. Each virus is also written to the Live log as a warning.

> **Testing by e-mail**
>
> The test string pasted into a message body isn't flagged: ClamAV recognises the EICAR test only as an exact 68-byte attachment, and mail providers and desktop antivirus usually refuse to send it anyway. Use the test button instead.

The quarantine

With **Quarantine instead of refusing** on, mail that would be refused — high spam scores, viruses, blocked attachments, blocklisted senders — is kept in the quarantine instead, so nothing important is lost by mistake.

Held mail is listed newest first, a page at a time. The search box looks through sender, recipients, subject and reason as you type. Tick messages to release or delete several at once; ticks are kept when you move between pages.

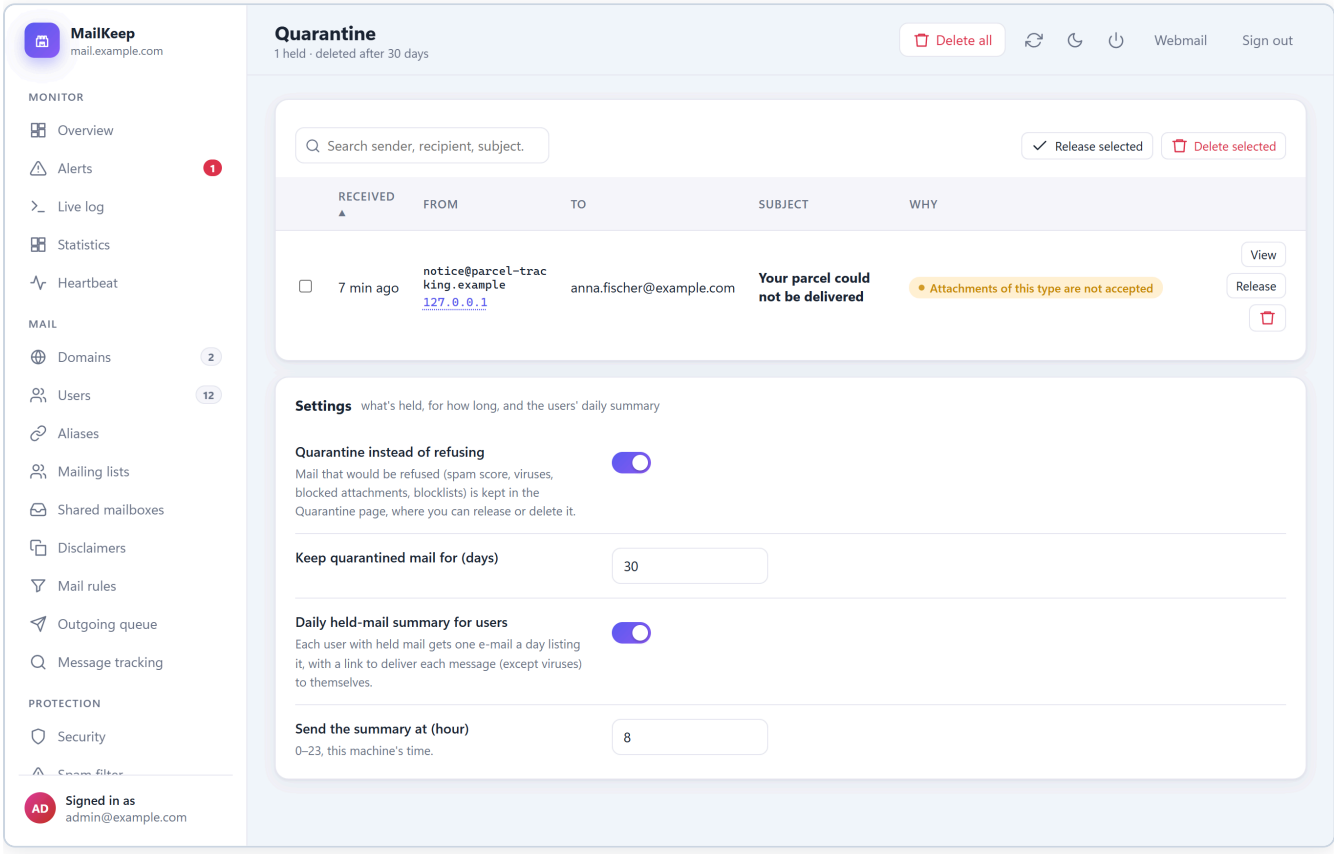


Figure 13.5 — The Quarantine page, with the reason each message was held.

- **View** shows the headers, the text and the attachments' names (never the HTML, and attachments are not opened). **Download** saves the original.
- **Release** delivers it to the recipient's Inbox; you can also allow the sender from now on. Messages with a virus can't be released to users.
- **Delete**, or select several and use **Release selected** / **Delete selected**.
- Held mail is deleted after **Keep quarantined mail for** days (30).

The quarantine's settings are in the **Settings** panel at the bottom of the Quarantine page. Domain administrators see and release only held mail whose recipients are all in their own domains.

The daily held-mail e-mail for users

With **Daily held-mail summary for users** on (the default when the quarantine is on), each user who had mail held gets one e-mail a day, at the chosen hour, listing it with a **Release** link per message. The link opens a page with a button — so link scanners can't release anything — and delivers the message to their Inbox. Viruses are never offered for release.

CHAPTER 14

Security and sign-in protection

How the server keeps out password guessers and intruders, blocking addresses for good, two-factor sign-in and passkeys, country rules and the audit log.

Layers of protection

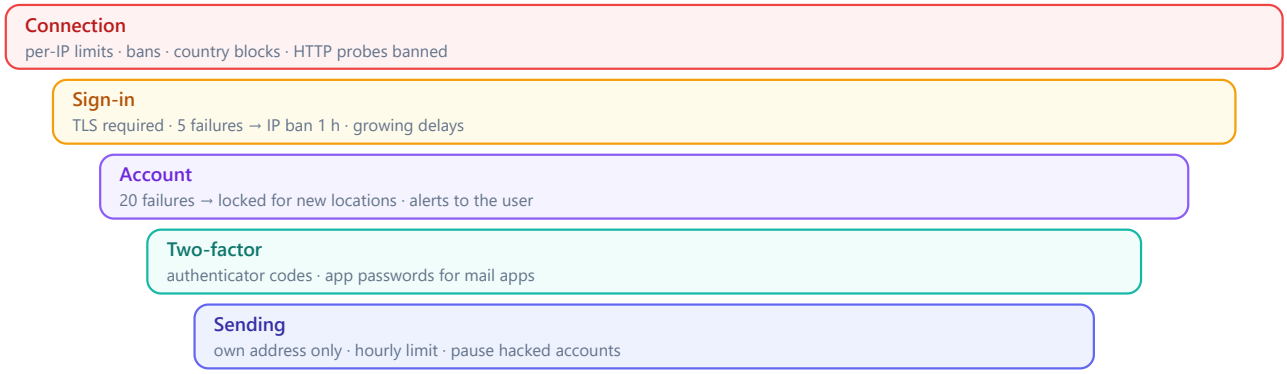


Figure 14.1 — Each layer stops a different kind of attack.

Protection	Default	Setting
Passwords only over encrypted connections (the server itself is exempt)	on	`require_tls_for_auth`
Failed sign-ins from one address before it's banned	5 in 10 minutes	`max_auth_failures`
Ban length	1 hour	`ban_secs`
Growing delay after each failed sign-in	always	—
Failures to one account (from any addresses) before it's locked for new locations	20 in an hour	`max_user_failures`
Alert: different addresses trying one mailbox	5 in 10 minutes	`attack_ips`
Alert: one network trying different accounts	10 in 15 minutes	`spray_accounts`
Account lock length	30 minutes	`user_lock_secs`
Signing in to an account that can't exist (no @domain, or a domain not hosted here)	banned at once	`ban_unknown_accounts`
Signing in to a mailbox that doesn't exist on one of your domains	banned on the 2nd try	`ban_unknown_accounts`
Connections per address / in total	20 / 2000	`[limits]`
Disconnect after unknown commands	10	`max_bad_commands`

Protection	Default	Setting
Web requests on mail ports (a sign of scanning)	banned	—

> **Lockouts that can't lock out the real user**
> When an account is locked after many failures, only **new** locations are locked out. Devices and places the account has signed in from before keep working, so an attacker can't lock someone out of their own mail. The user gets an e-mail telling them about it.

> **Guessing at accounts that don't exist**
> Attacks often come from hundreds of addresses, each trying only once or twice with names like `support`, `admin` or addresses at domains you don't even host, so the normal limit of 5 failures never bans them. MailKeep bans such an address straight away. A mailbox name on one of your own domains could be a typo, so that is forgiven once and banned on the second try. Addresses that have signed in successfully before, and those on *Never ban these IPs*, are never banned this way: a typo in the office counts as an ordinary failure. Turn it off with **Ban guessing at accounts that don't exist** in the Security page's Settings.

All these settings are in the **Settings** panel at the bottom of the Security page.

What each failed sign-in was

A failed sign-in isn't always a password guess. The audit log records each kind separately, and only some of them count towards locking the account:

In the audit log	What happened	Counts towards
Wrong password	The password was checked and was wrong.	banning the address, locking the account
No such account	The name isn't a mailbox here.	banning the address (faster, see above)
Refused: country rule	Refused by *Only allow sign-ins from* **before** any password was checked: nothing was learned.	banning the address only
Refused: account locked	The account is locked for new locations.	banning the address, locking the account
Stopped by two-factor	The **right** password, but no code or app password. The user gets an e-mail.	banning the address, locking the account

The **Failed sign-ins** card on the Security page and the daily summary break the total down the same way. With a country rule in place, most failures usually show as *refused by the country rule*: no password was ever tried.

Attacks spread over many addresses

Some attacks use hundreds of addresses, each staying under the ban limit. Every five minutes MailKeep looks at the audit log for two patterns and tells the administrators (at most once a day each):

- **Many addresses trying one mailbox**: **Alert when this many addresses try one mailbox** (5 within 10 minutes). Only real mailboxes count. The alert goes to the full administrators and to the mailbox's domain administrators, with the addresses, countries and what kind of failures they were.
- **One network trying many accounts** (password spraying): **Alert when one network tries this many accounts** (10 within 15 minutes, a network being a /24, or a /48 for IPv6), across all your domains. Full administrators only.

These are alerts only. The bans and locks above keep doing the blocking, and nothing locks an account because of them, so an attacker can't use them to lock anyone out. 0 turns either one off. If one network keeps coming back, block its range permanently (below), but only if none of your own users sign in from there.

Password length and strength

New and changed passwords must be at least **Shortest password allowed** long (8 by default), and an administrator's at least **...for administrators** (12 by default); both can be set from 8 to 64 under **Settings → Security**. With **Refuse weak passwords** on, a password also can't be one of the most common ones or contain the user's name or domain. Existing passwords keep working: the rules apply when a password is set, in the console, in webmail, on invitation and reset pages and with `mailserver user add` / `user passwd`. The password boxes show the minimum. Current advice is 15 characters where an account has no two-factor sign-in, and no forced symbols or regular changes, which only lead to weaker passwords.

Passwords are stored as Argon2id hashes. The server answers the same way whether or not an address exists, so attackers can't find out which accounts are real.

The Security page

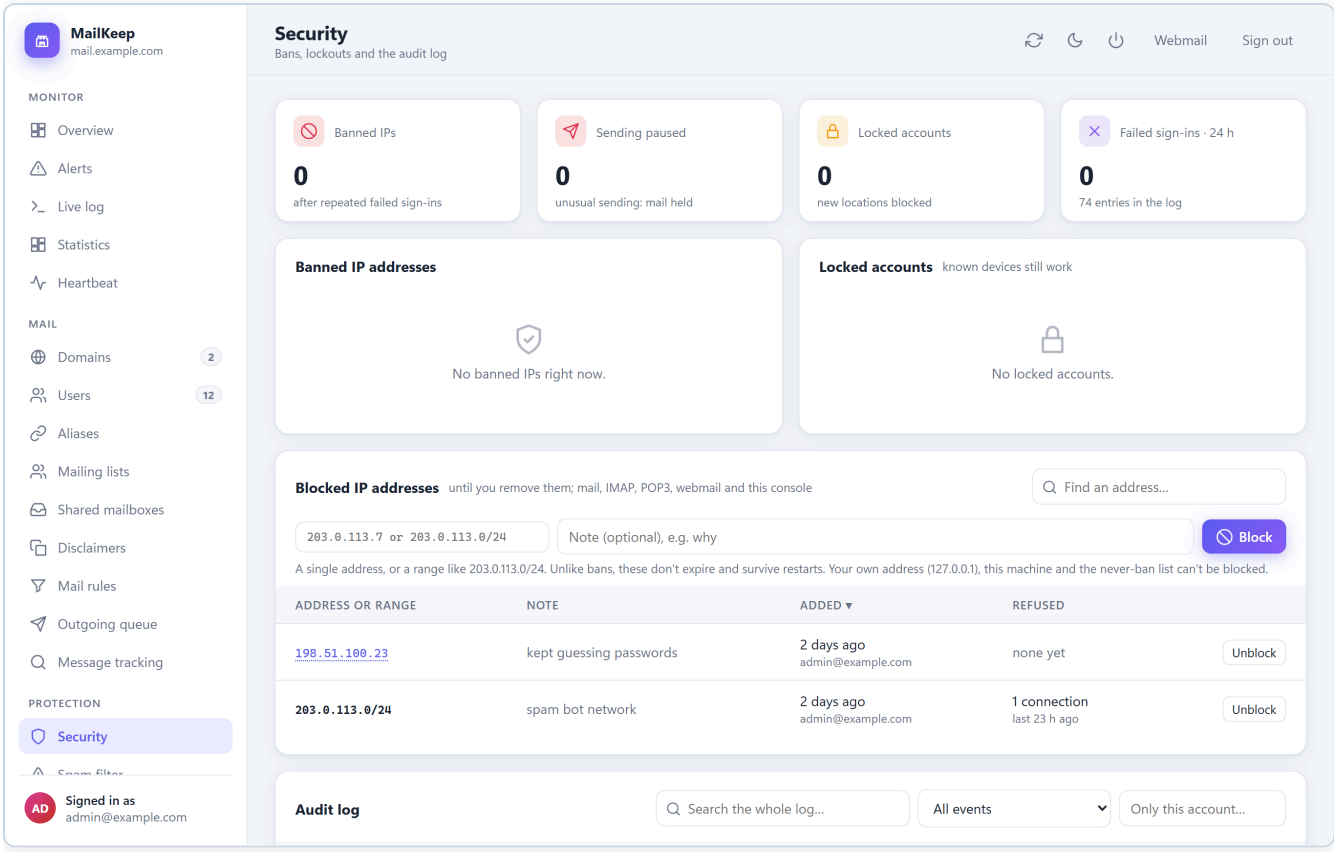


Figure 14.2 — Bans, locked accounts, blocked addresses, paused senders and the audit log.

- **Banned addresses** with the time left and how many connections were refused from each since it was banned; Unban removes one.
- **Blocked IP addresses**: addresses and ranges blocked until you remove them (below).
- **Locked accounts**; Unlock lifts the lock.
- **Sending paused**: accounts stopped for sending too much (chapter 12), with Resume and send or Discard and resume.
- **Audit log**: every sign-in (method, address, country), failure, lockout, ban and administrative change. Search the whole log (accounts, addresses, details), pick one kind of event, or enter an account and press Enter; page through it at the bottom. The card at the top counts failed sign-ins in the last 24 hours, with the most common kinds.

```
mailserver audit                      # the latest 50 entries
mailserver audit --user bob@example.com --limit 200
```

Blocking an address for good

A ban lasts for the ban length. Bans are kept in the database, so a restart or an update doesn't lift them: they carry on with the time they had left. Unban lifts one for good. To keep an address or a whole network out **until you remove it**, use **Blocked IP addresses** on the Security page:

- Enter a single address (`203.0.113.7`) or a range (`203.0.113.0/24` ; IPv6 works too), an optional note such as *spam bot network*, and press **Block**.
- Or click the address anywhere in the console and choose **Block permanently**.
- Blocks apply to every service (incoming mail, sending, IMAP, POP3, webmail and the console), are kept in the database, and survive restarts. The list shows how many connections each one has refused and when it last tried. **Unblock** lifts one at once.
- Your own current address, the server itself (also by its public address) and the never-ban list can't be blocked or banned, not even inside a range, and ranges wider than `/8` are refused, so you can't lock yourself out by accident.

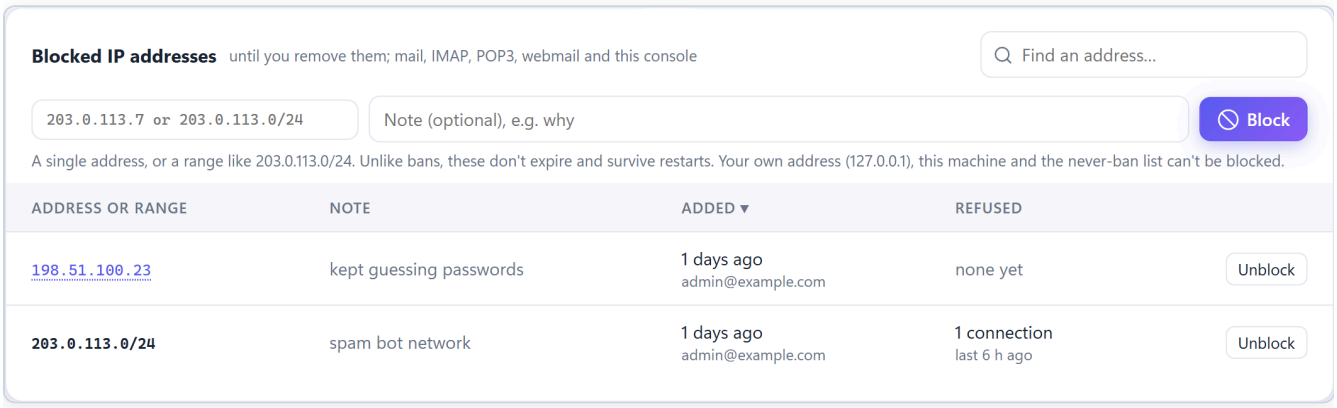


Figure 14.3 — Blocked IP addresses.

> ✓ **Never ban your office**
> Add your office's or your own fixed address to **Never ban these IPs** (`allowlist`). Addresses on it are never banned or throttled.

Who is behind an address, and reporting it

The panel for an IP address (click any address in the console) has a **Network** row: who the network is registered to, its name and range, the AS number where the registry gives one, and its published **abuse contact**. MailKeep asks the regional internet registry (ARIN, RIPE, APNIC, LACNIC or AFRINIC, through RDAP) only when you open the panel, never while someone signs in, and remembers the answer for a week. It never contacts anything else for this, and private addresses aren't looked up. If the lookup fails, the row says *unavailable* and why.

For an address with failed sign-ins, **Abuse report…** writes a draft to that abuse contact:

- only facts from the audit log: the times (in UTC), how many attempts of each kind, the services, and how many mailboxes were tried, with the names shortened (`s***t@example.com`);
- a statement that there's no evidence any account was accessed, and a request to look into it;
- a warning before you send if the address has also signed in successfully, because it may be one of your own users.

Edit it as you like, choose the **From** address and press **Send**, then **Yes, send** to confirm. It goes out through the normal outgoing queue, DKIM-signed, with a copy in that address's Sent folder so the provider's reply threads with it. Nothing is ever sent without that confirmation.

- **From** lists the addresses you may send as. `abuse@` your main domain comes first once it's yours: add it as an alias of your own mailbox on the Aliases page, so replies reach you.
- One report per address every 30 days (the view then says when it was sent), and at most 20 a day. Only full administrators can send, never to an address hosted here, and every report sent is in the audit log.
- Copy, Download and Open in mail app are there too, to send it some other way.

Providers act on reports to different degrees; a ban or a permanent block protects you either way.

Failed sign-ins recorded before version 0.2.17 were all of one kind. On the first start of 0.2.18 they are sorted into the kinds above from what their details say, once, so old country refusals don't show as wrong passwords.

Two-factor sign-in

With two-factor sign-in, signing in also needs a 6-digit code from an authenticator app (Microsoft or Google Authenticator, 1Password, Authy, ...), so a stolen password alone isn't enough. Turn it on for every administrator.

- **Users turn it on themselves** in webmail: ⚙ Settings → Two-factor sign-in (chapter 20).
- **An administrator** can turn it on from the command line:

```
mailserver user 2fa enable bob@example.com           # shows a QR code to scan
mailserver user 2fa confirm bob@example.com 123456   # with the code the app shows
mailserver user 2fa disable bob@example.com          # if the phone was lost
```

Passkeys

A **passkey** signs in with Windows Hello, Face ID or Touch ID, a phone or a security key, with no password to type or steal and no code needed. A passkey only works on the site it was made for, so a fake sign-in page can't use it. Users add one in webmail under ⚙ Settings → Security → Passkeys, then choose Sign in with a passkey on the sign-in page; it works for the admin console too. If someone loses the device, an administrator turns their passkeys off on the Users page.

App passwords

Mail apps can't ask for a code, so once two-factor is on, each mail app signs in with its own **app password**: a long random password used only by that app, revocable on its own. Alternatively, the account password followed directly by the current 6-digit code works too.

```
mailserver user app-password add bob@example.com "iPhone Mail"   # shown once
mailserver user app-password list bob@example.com
mailserver user app-password revoke bob@example.com "iPhone Mail"
```

Recent sign-ins and "sign out everywhere"

Each user sees their own **recent sign-ins** (when, from where, and through which service: webmail, phone, mail app) in webmail under ⚙ Settings → Security. If something looks unfamiliar, they change their

password and press **Sign out everywhere**, which ends every webmail session of the account, including the current one.

Alerts to users

With **E-mail users about new locations and lockouts** on, users get an e-mail when they sign in from a country they haven't used before, when their account gets locked, and when someone knew their password but was stopped by two-factor.

Country rules

1. Download a free country database: MaxMind GeoLite2-Country or DB-IP Lite Country (an `.mmdb` file).
2. Set **Country database (.mmdb)** to its path.
3. Then either **block countries** (two-letter codes like `XX`), which drops all their connections — on port 25 only if you also tick **Also block them for incoming mail** — or **allow sign-ins only from** a list of countries.

The audit log then shows each sign-in's country, the panel for an IP address shows the country's name with its code (*Russia (RU)*), and users are alerted about sign-ins from new countries. A sign-in from a country that isn't allowed is refused before the password is even checked, so guessing from there gets nowhere.

Who may use the admin console

- Only accounts marked as administrator. Full administrators can do everything; domain administrators only see and manage their own domains (chapter 17). On the Security page they see their own users' sign-ins, locked accounts and paused senders, but not bans or blocked addresses.
- By default, only from the server itself and the local network. **Allow the console from the internet** lifts that; use two-factor sign-in if you do.
- **Only from chosen addresses:** **Settings → This console → Admin console only from** takes addresses and ranges, one per line (`203.0.113.7`, `203.0.113.0/24`, `2001:db8::/32`). Everyone else is turned away before any sign-in, even with the right password, and the audit log shows *Refused: admin IP rule* (once an hour per address). Webmail and mail apps aren't affected; calls with an API key follow the list too. The server itself is always allowed, so a mistake can be fixed on it (Remote Desktop, `http://localhost/admin/`), and the console won't save a list that leaves out the address you're saving from. If your address at home changes now and then, list your provider's range, or add the new address from the server.
- **Two-factor for administrators:** with **Administrators must use two-factor sign-in** on, an administrator or domain administrator who has neither an authenticator app nor a passkey can still sign in to webmail, but the console refuses them with a link to turn one on (**⚙ Settings → Security** in webmail). The console won't turn this on until your own account has one. The Users page's **Two-factor** filter shows who still needs it. API keys aren't affected (they're made in the console, which already needed it).
- Behind IIS or another web front end, set `trusted_proxies` so these rules see the real visitor (chapter 4).

CHAPTER 15

Archive, legal hold and folder clean-up

Keeping a copy of all mail for compliance, preserving a mailbox for legal reasons, and deleting old Junk and Trash automatically.

Journaling

With journaling on, the server keeps a copy of every message sent and received in the **archive**, separate from users' mailboxes. Users can't change or delete it.

- **Keep a copy of all mail**, in the Settings panel at the bottom of the **Archive** page, turns it on.
- **Only for these domains** limits it to some domains.
- **Also send each copy to** forwards every copy, wrapped in a journal report, to an outside archiving service.
- **Delete archived mail after** days (0 = keep forever).

Searching and exporting the archive

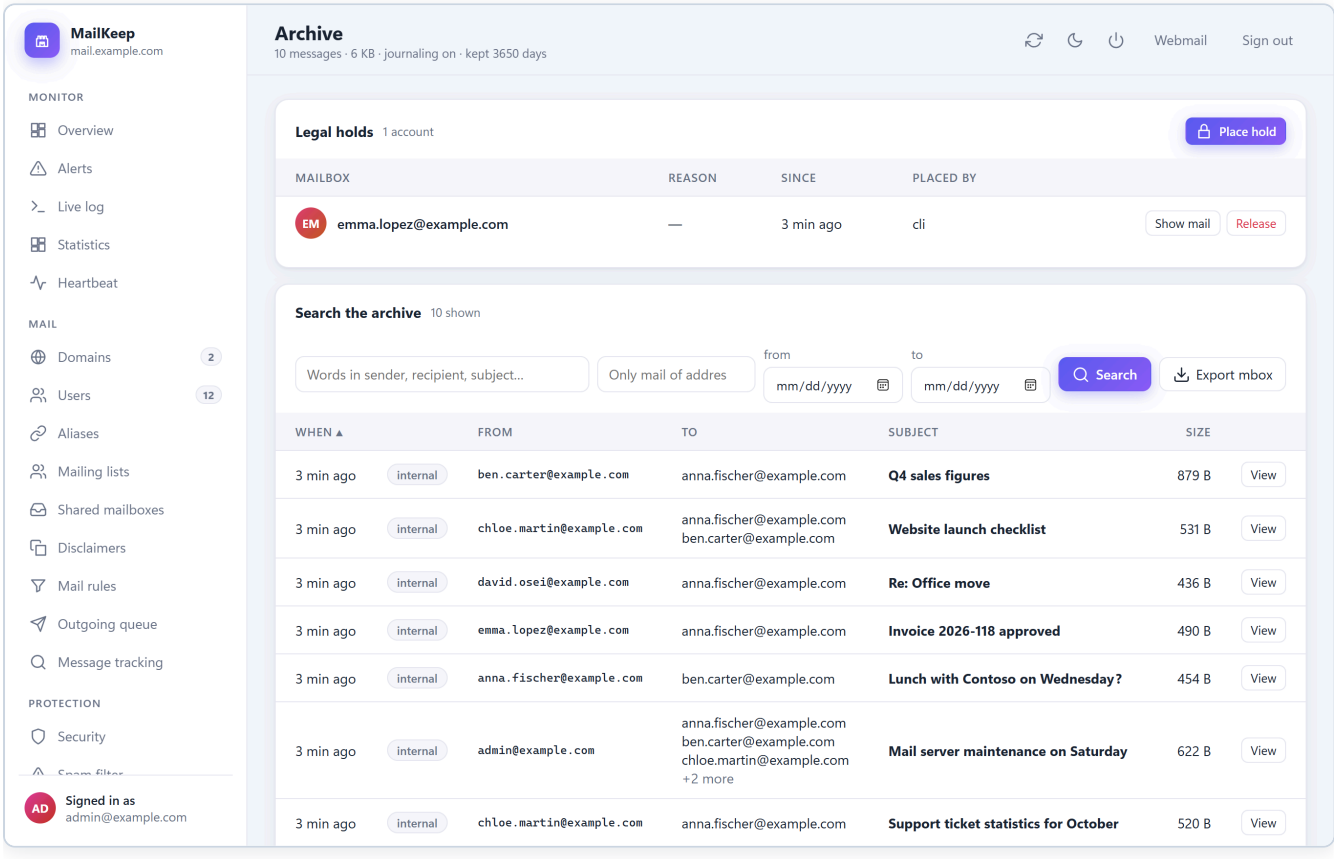


Figure 15.1 — The Archive page: search, legal holds and export.

Search by words in the sender, recipients, subject or Message-ID, by address, and by date range. **View** shows a message as text, **Download** saves it, and **Export mbox** writes all matches to one mbox file that any mail program can open.

```
mailserver archive search "invoice" --address emma@example.com --since 2026-01-01 --until 2026-06-30
mailserver archive search --address emma@example.com --export emma-2026.mbox
```

Legal hold

Putting a mailbox on **legal hold** preserves everything in it, for example during a dispute or investigation:

- All its existing mail is copied into the archive.
- Whatever the user deletes — messages, folders — is archived first.
- The account, and its domain, can't be removed while the hold lasts.
- Archive retention and folder clean-up never delete its mail.

```
mailserver archive hold emma@example.com
mailserver archive holds
mailserver archive release emma@example.com
```

Holds are listed on the Archive page, where **Release** lifts one.

Automatic folder clean-up

Settings → Folder clean-up deletes old mail from every user's folders once an hour. It's off by default.

- **Empty Junk after** days, and **Empty Trash after** days (0 = keep).
- More folders by name in `mailserver.toml`:

  ```
  [retention]
  junk_days = 30
  trash_days = 30
  folders = { "Newsletters" = 90 }
  ```

Mail of accounts on legal hold is archived before it's removed.

CHAPTER 16

Monitoring, alerts and the setup check

Knowing the server is healthy, being told when it isn't (even when it's down), the statistics, storage, blocklist and report pages, and checking everything other mail servers judge you by.

Alerts

With **E-mail admins about problems** on (the default), the server watches itself and warns the full administrators about:

Backups
A scheduled backup failed.

Disk space
Less than **Low-disk alert below** GB (2) or 5% free on the mail disk.

Blocklists
The server's address appeared on a blocklist.

Stuck mail
Mail waiting in the queue for more than a day.

Certificate
Expiring within 14 days.

Virus scanner
ClamAV stopped answering.

Services
A service couldn't start, or the data folder isn't writable.

Hacked accounts
An account's sending was paused.

Delivery problems
Other providers refusing your mail for a reason this server can fix (below).

Attacks
Many addresses trying one mailbox, or one network trying many accounts (chapter 14).

Domain administrators don't get these server-wide alerts, which would show them other domains' accounts and the server's state. They hear about their own mailboxes instead: sending paused, outgoing mail refused as spam, a mailbox 95% full, a phishing report, an account locked after repeated failures, and attacks on one of their mailboxes.

At most one alert per kind per day, unless the problem went away and came back. This holds across updates and restarts too: a restart doesn't send the same alert again, and a dismissed alert counts as sent. Alerts go to administrators' inboxes, and optionally:

- **Also e-mail alerts to** an outside address, so you hear about problems even when this server's mail is down;
- **Push alerts to your phone**: an ntfy topic URL (`https://ntfy.sh/your-topic`) or a Discord, Slack or Teams incoming-webhook URL.

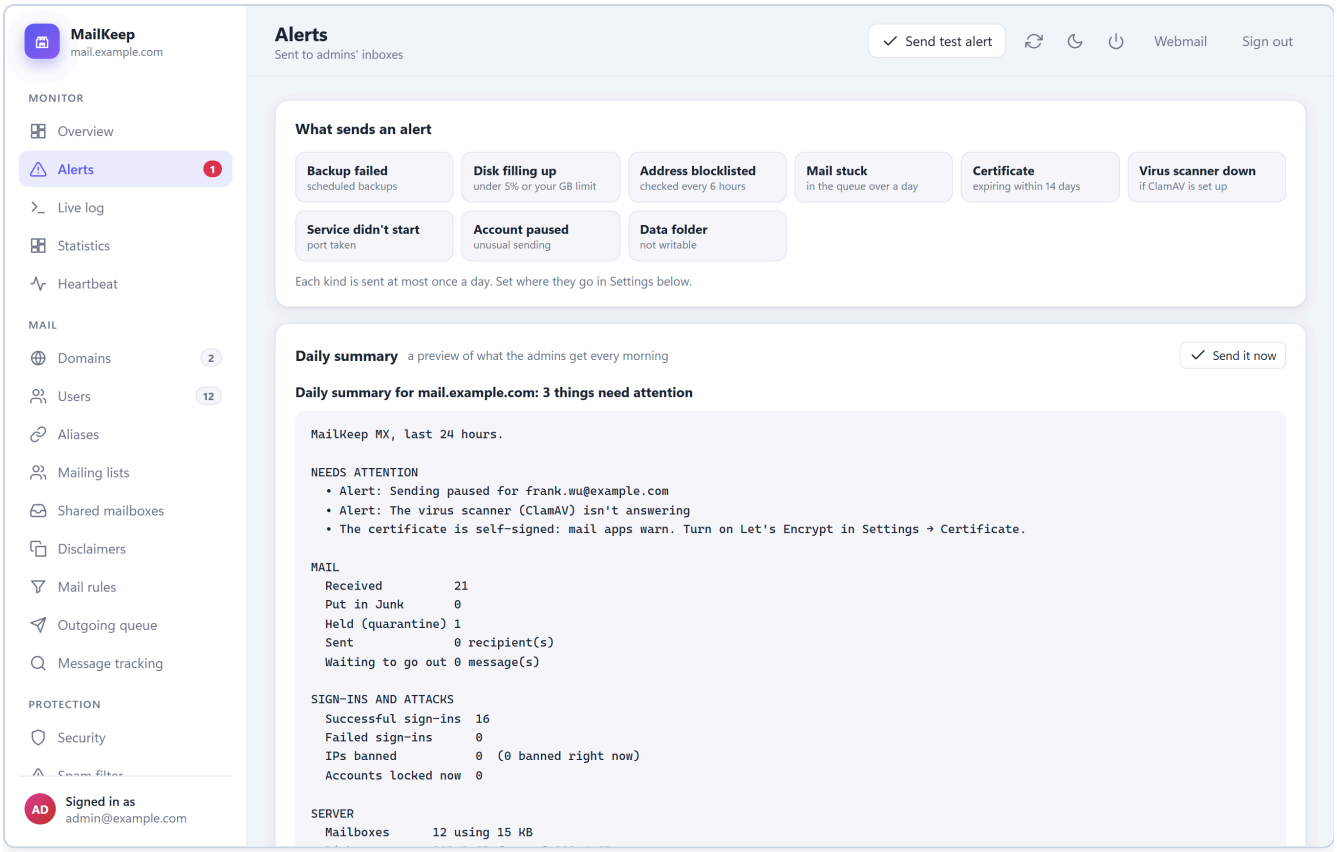


Figure 16.1 — The Alerts page: what sends an alert, the daily summary and the history, with a test button.

Send test alert checks that alerts reach you everywhere you set up. Where alerts go is set in the **Settings** panel at the bottom of the Alerts page.

When other providers refuse your mail

When Gmail, Yahoo, Microsoft or another provider refuses mail from this server, its answer says why, and the reasons follow known patterns. Every five minutes MailKeep reads the last six hours of refusals in Message tracking and sorts them:

What the receivers said	Likely cause	Alert after
Gmail 5.7.26, Yahoo 5.7.9, "unauthenticated", DKIM/SPF/DMARC	The mail isn't authenticated: DKIM or SPF missing or failing	2 messages
Spamhaus, SpamCop, "listed", "blocked using"	This server's address is on a blocklist	2 messages
"PTR", "reverse DNS", 5.7.25	Reverse DNS missing or not matching the server name	2 messages
"must issue a STARTTLS", 5.7.10	The receiver requires encryption that couldn't be made	2 messages
"spam", 5.7.350	The content was judged to be spam	3 messages
4.7.28, "rate limit", "try again later"	Too much at once: the receiver is slowing mail down	3 messages

Refusals about one recipient (no such mailbox, mailbox full) are left out, and a message retried many times counts once. When a pattern repeats, the full administrators get one alert (at most once a day per cause) that names the providers, explains the likely cause and what to fix, lists the sending domains affected, adds the matching Setup check results with their fixes (for example *✗ DKIM (example.com): …*), and quotes what the receiving servers said. It also shows under **Needs attention** on the Overview. MailKeep changes nothing by itself. A new alert goes out only for refusals newer than the last one reported, and the alert resolves itself once the matching Setup check items are green and nothing new has been refused for 30 minutes.

Dismissed and resolved alerts

The red number next to Alerts in the menu counts alerts from the last day that are still **open**. An alert stops counting when:

- you press Dismiss on it (or Dismiss all): it stays in the history, marked *dismissed by* you;
- or its cause goes away by itself: ClamAV answers again, the next backup or off-site copy works, disk space or the queue is back to normal, the certificate is renewed, a blocklist drops the address, a heartbeat service answers again, a paused sender is resumed. The alert is then marked *resolved … later*.

The **History** shows the last 30 days; Show older goes back 90. The same alert repeated is shown once, tagged with how often it came (*3 times since 11/12/2026*). Each alert shows what happened; why, what to do and the details open under Details.

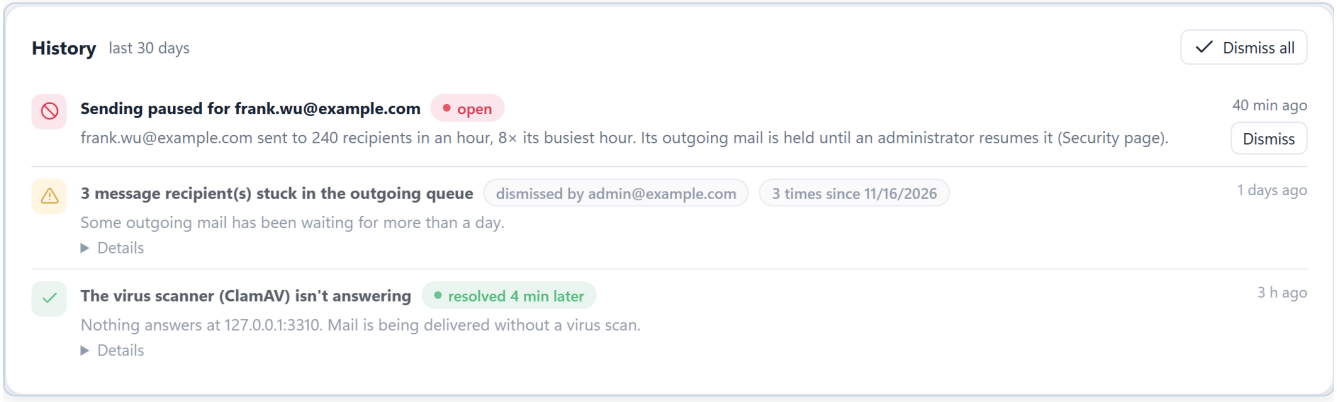


Figure 16.2 — The alert history: open, dismissed and resolved alerts, with repeats grouped.

The daily summary

Every morning (at 7 by default) each full administrator gets a short e-mail about the last 24 hours, also sent to Also e-mail alerts to if set:

- **Needs attention**, first: alerts, mail waiting more than an hour to go out, accounts with sending paused, a certificate that is self-signed or expires within 14 days, no backup in two days, a failed backup, a disk over 90% full. With nothing to report, the subject ends in *all good*.
- **Mail**: received, put in Junk, held in the quarantine, sent, waiting to go out.
- **Sign-ins and attacks**: successful and failed sign-ins (broken down by kind: wrong password, no such account, refused by the country rule, and so on), IPs banned, locked accounts, the most-tried accounts and the busiest attacking addresses.
- **Server**: mailboxes and storage, free disk, certificate, last backup and version.

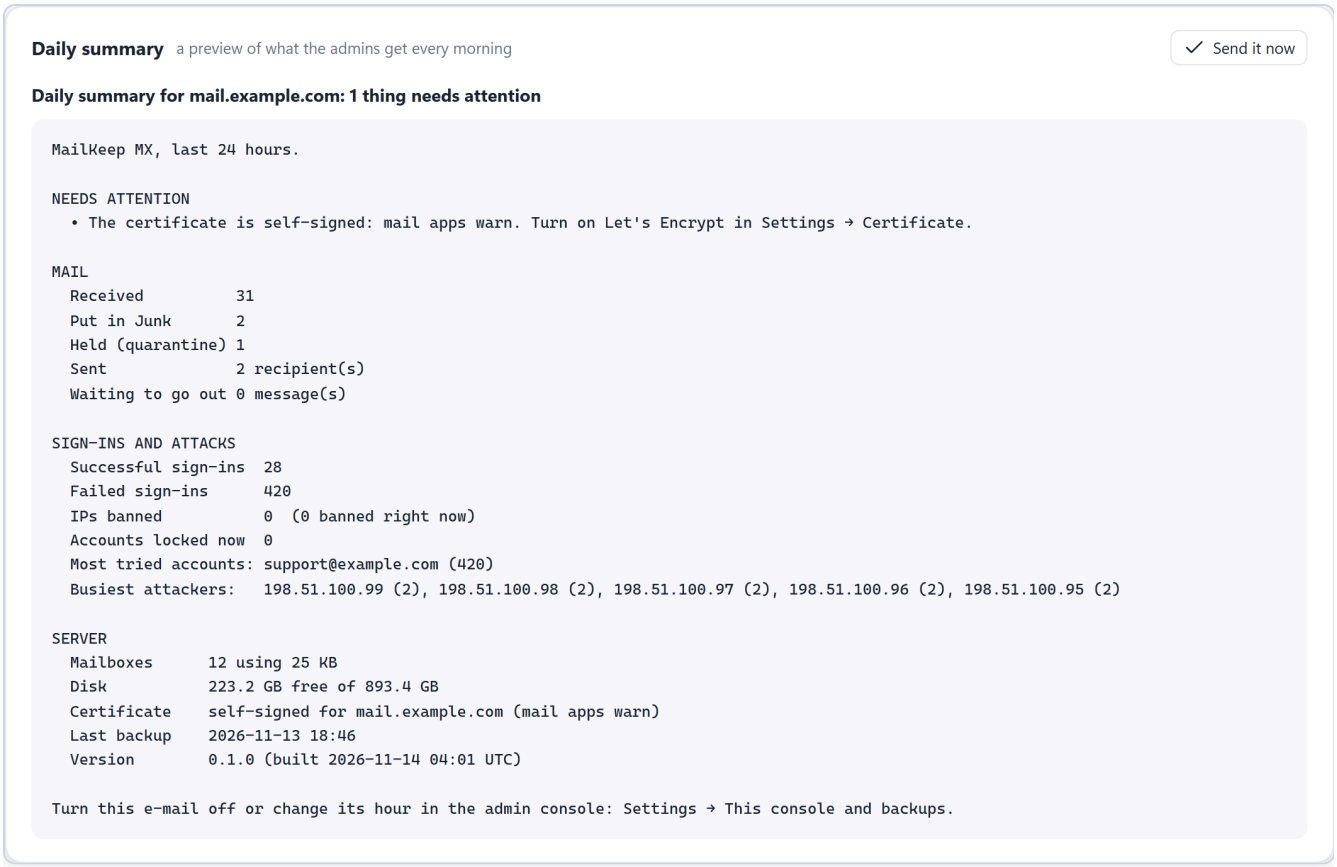


Figure 16.3 — The preview on the Alerts page, with *Send it now*.

Each **domain administrator** gets their own summary at the same hour, about their domains only: what needs their attention (paused, locked or nearly full mailboxes, held mail, other servers failing DMARC as their domain), their mail, their users' sign-ins and their mailboxes. Nothing about other domains or the server itself. They can turn it off on their Overview page (Daily summary).

The Alerts page shows a preview of today's summary; Send it now sends it at once. Turn it off, or change the hour, in the Alerts page's Settings (`[admin] daily_summary` , `summary_hour`).

Heartbeat: being told when the whole server is down

If the server is off, Windows hangs or the network is down, the server can't send an alert itself. A **heartbeat** solves that: MailKeep calls an outside monitoring service every few minutes, and when the calls stop, *that service* alerts you.

1. Sign up at a heartbeat service such as **healthchecks.io** (free), Better Stack, Cronitor or UptimeRobot (heartbeat monitors), with an e-mail address that is **not** on this server.
2. Create a check that expects a call every 5 minutes, with a few minutes' grace, and copy its ping URL.
3. On the Heartbeat page, paste the URL, optionally give it a name, and press Add. The first call goes out straight away.
4. Add a second service the same way if you want a backup.

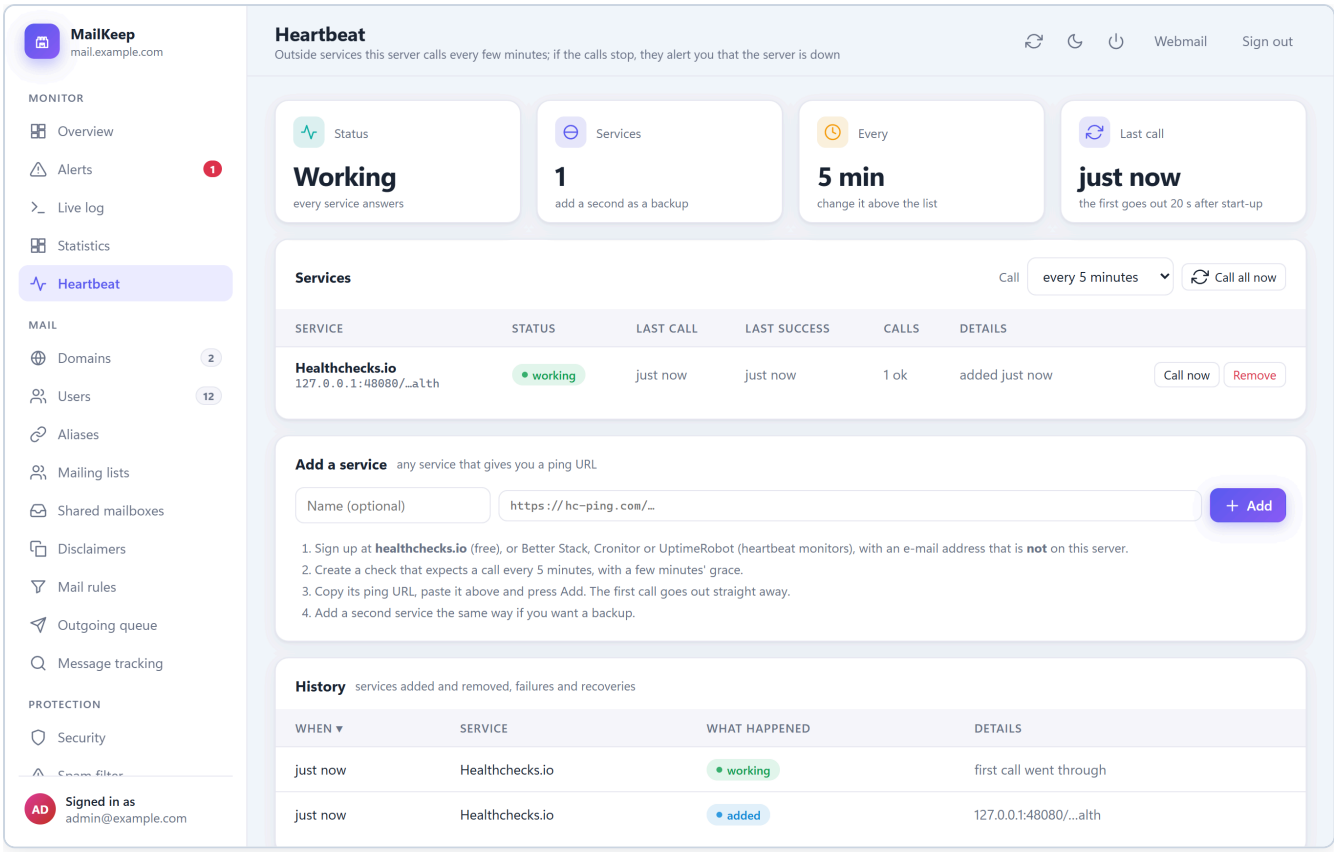


Figure 16.4 — The Heartbeat page: each service's status, last call and history.

The page shows each service's status, last call and last success, call counts and a history of failures and recoveries; **Call now** and **Remove** are on each row, and the interval (1 to 60 minutes) is chosen above the list. Changes apply at once. If a mail service fails to start, MailKeep stops calling on purpose, so the outside service raises the alarm. If calls to a service fail three times in a row, the administrators get an alert. For a check from outside that the mail ports answer, add a port monitor at UptimeRobot (ports 25 and 443).

Message tracking

"I sent you an e-mail yesterday — did you get it?" **Mail → Message tracking** answers that. Every step of every message is recorded, one line per recipient:

What happened	Meaning
Delivered	Stored in the mailbox; the details show the folder and the spam score.
Put in Junk	Stored, but in Junk because of its spam score.
Held	Held in the quarantine (chapter 13), with the reason.
Refused	Turned away, with why: no such mailbox, refused by the spam filter, too big, a mail loop… The sending server tells its user.
Try later	Greylisted or a temporary problem; the sending server tries again.
To list	Handed to a mailing list.

What happened	Meaning
Queued	Your user's mail is waiting to go out; its id (`Q...`) follows it through the next steps.
Sent	The other domain's mail server took it.
Retrying	The other server couldn't take it yet; the details say why and when the next try is.
Bounced	Given up; a bounce went back to the sender, with the other server's answer.

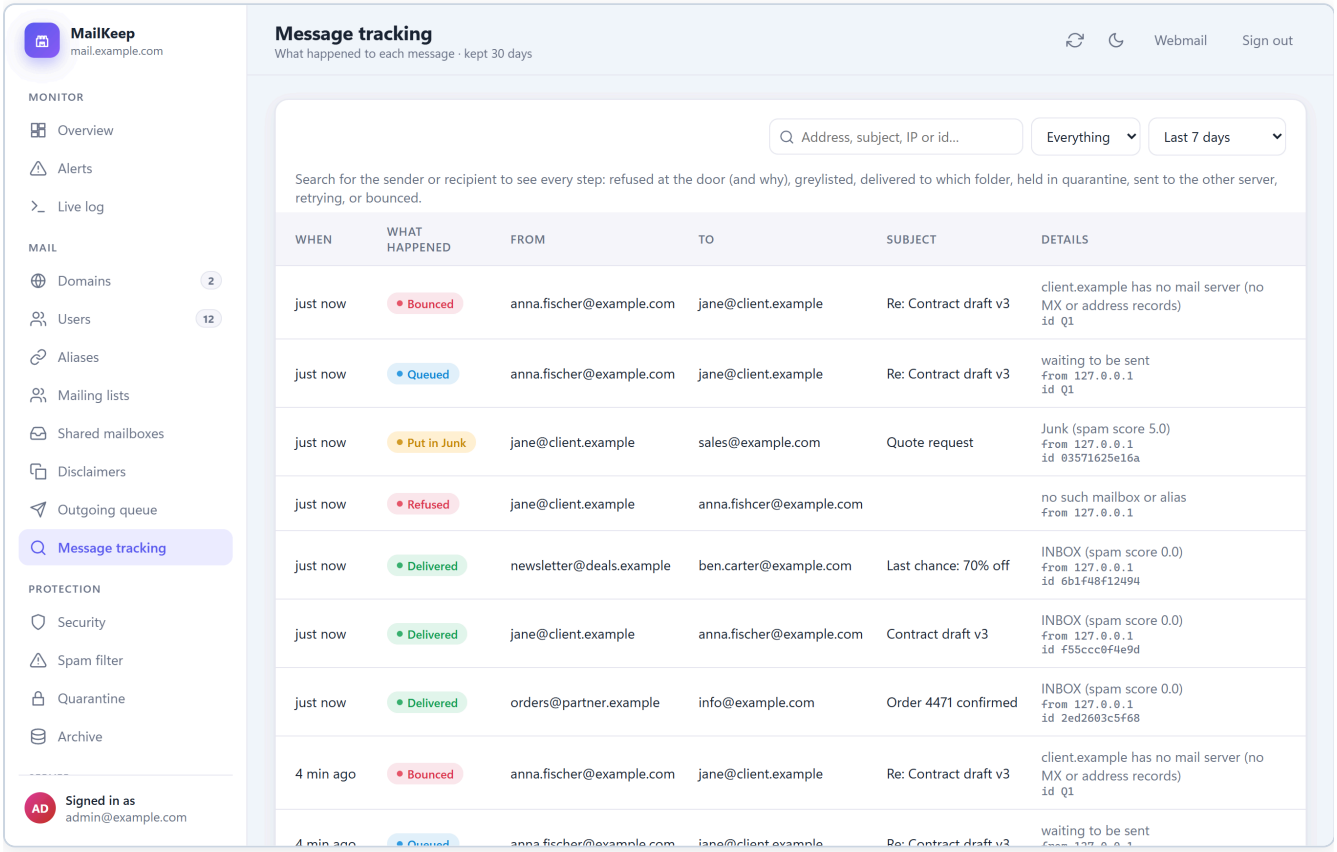


Figure 16.5 — Message tracking: a bounce, a queued message, mail put in Junk, a typo refused at the door, and deliveries.

Search for a sender, recipient, subject, IP address or id, narrow it to one kind of step (or to *Viruses*: mail refused or held because the virus scanner found one), and choose how far back to look. The log keeps 30 days (`[limits] tracking_days`). It records mail from the moment this feature was installed, not before. Domain administrators see only mail sent from or to their own domains.

Mail the server writes itself is tracked too, with what it is in brackets: out-of-office replies (*INBOX (automatic reply)*), alerts, daily summaries, security notices to users, storage warnings, quarantine digests, bounces, journal reports and mail rules forwarding to another mailbox here. Going to another domain it shows as *Queued* first (*automatic reply, waiting to be sent*), then as Sent, Retrying or Bounced like any other mail. Out-of-office replies and bounces have an empty envelope sender; the From column shows the mailbox or `MAILER-DAEMON@` the server's name they come from.

Statistics

Statistics shows mail received, put in Junk, refused, held, sent and bounced, and sign-ins, day by day for 30 days, 90 days or a year, with the busiest senders and inboxes, where your mail goes, and why mail was refused. Daily totals are kept for a year, even after the mail itself is deleted; the lists come from the message log. Domain administrators see the figures for their own domains.

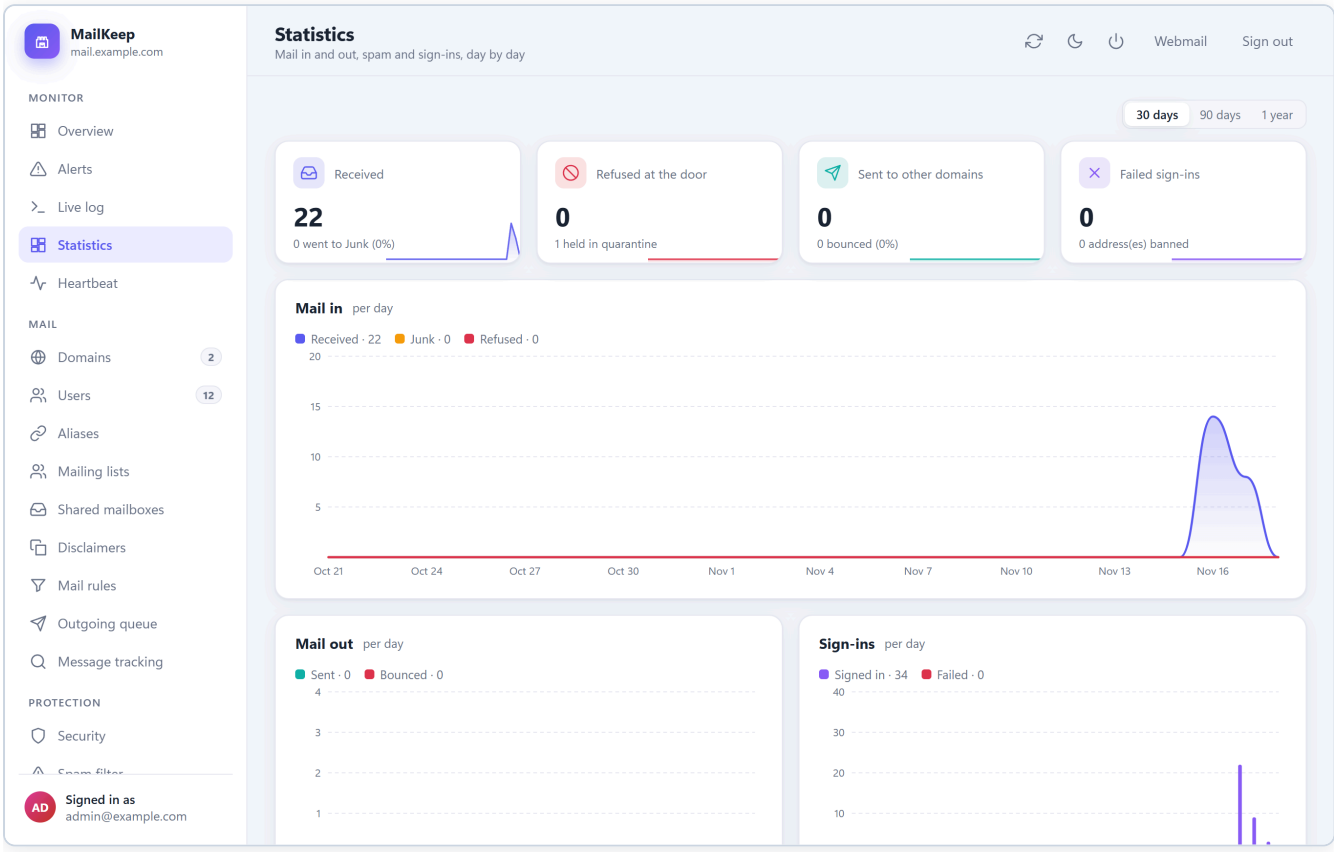


Figure 16.6 — Statistics.

Storage

Storage shows the free disk, what uses it (mailboxes, archive, quarantine, files shared by link, the queue, backups), how fast mail grows and when the disk would be full at that rate, and every mailbox with its size, quota and growth over 30 days. Search for a mailbox with the box above the list; click one to see its folders and biggest messages. An alert is sent when the disk will be full within 30 days.

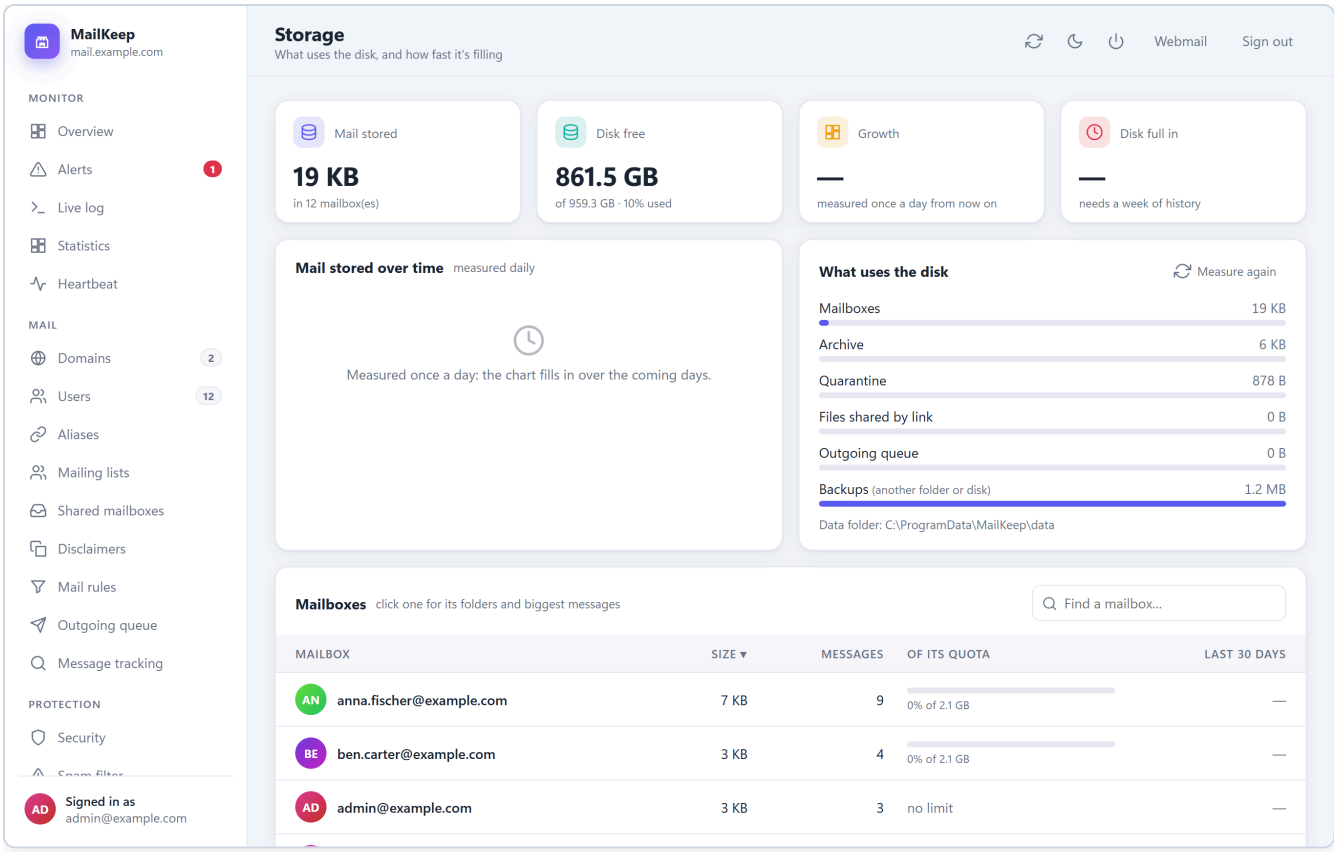


Figure 16.7 — Storage.

Blocklists

Blocklists checks whether this server's addresses are on the lists big providers use to refuse mail (Spamhaus, SpamCop, Barracuda and others), every few hours, and alerts you when one appears or is removed. Each listing has a link to the list's own page with the reason and the removal form. Which lists and how often are set in the page's Settings.

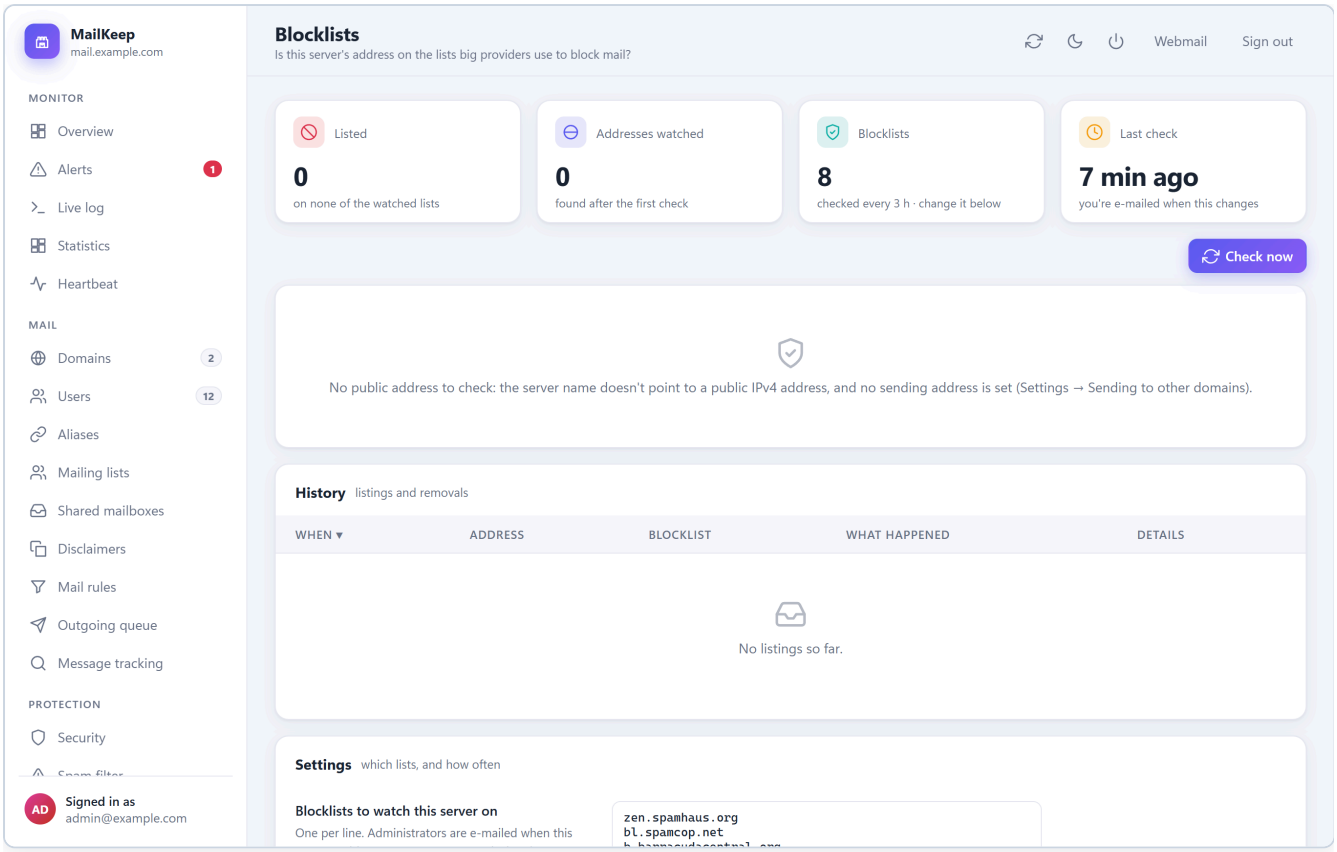


Figure 16.8 — Blocklists.

> **Spamhaus and public DNS**
>
> Spamhaus refuses lookups that come through big public DNS services such as 8.8.8.8. If its lines say *couldn't check*, give the server your hosting provider's DNS resolver, or run your own.

DMARC and TLS reports

Gmail, Microsoft, Yahoo and others send each domain a daily report listing every server that sent mail as it, and whether it passed SPF, DKIM and DMARC. Reports reads them as they arrive and shows, per domain, who sends as you and how much passes, and flags **failing senders** that aren't this server: someone forging your domain, or a service of yours (a website form, a newsletter tool) that still needs SPF or DKIM. TLS reports show whether other servers could deliver to you encrypted.

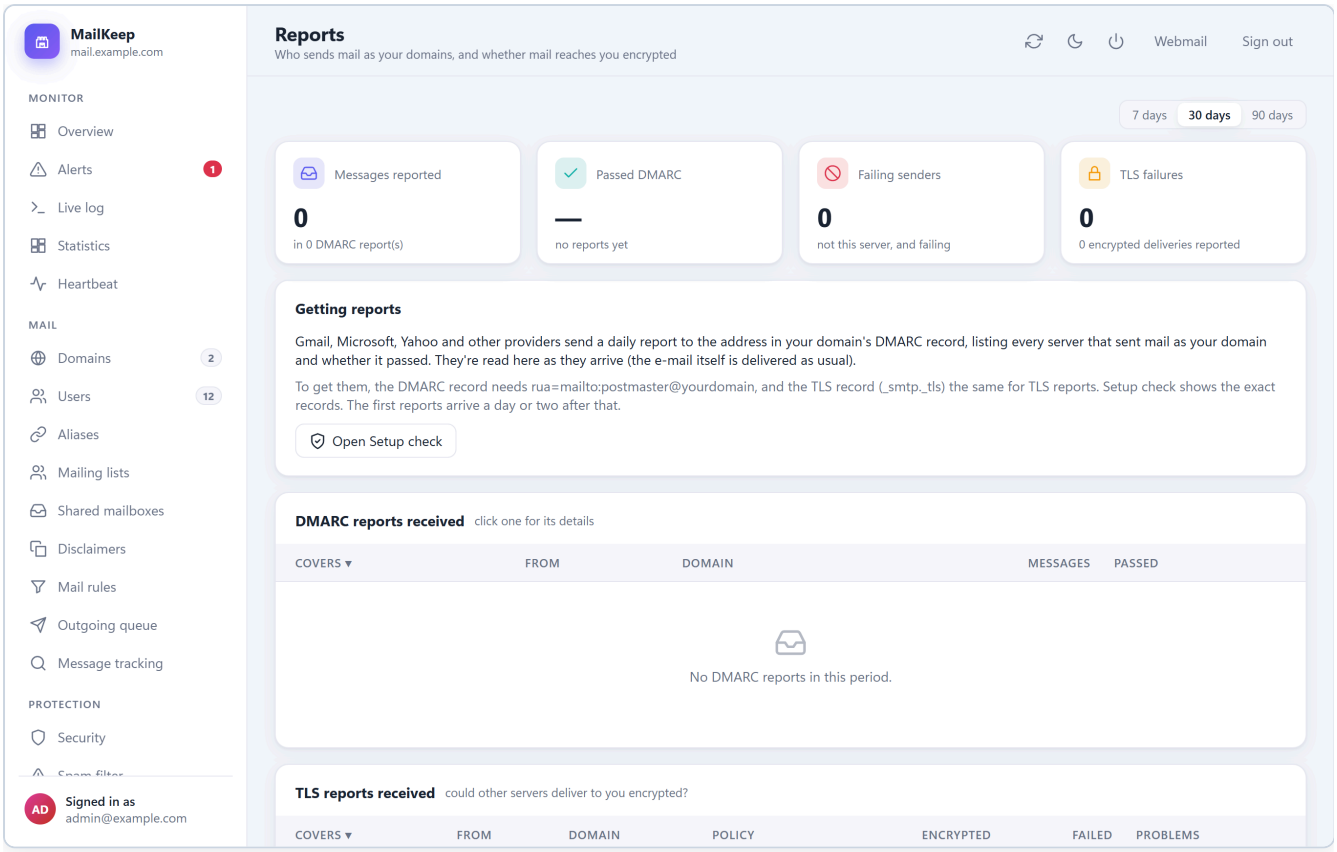


Figure 16.9 — Reports, before the first reports have arrived.

To receive them, the domain's DMARC record needs `rua=mailto:postmaster@yourdomain` (and `postmaster@` must exist as a mailbox or alias), and the TLS record `_smtp._tls` the same. Setup check shows the exact records. MailKeep also **sends** DMARC and TLS reports to other domains that ask, and serves your **MTA-STS** policy (chapter 4); both are set in the Reports page's Settings.

A DMARC report goes out once a day, and only to a domain that had at least one message delivered **outside Junk** that day. Spam domains often publish a DMARC record asking for reports, and their servers rarely answer; they get none. To stop sending reports altogether, turn off Send DMARC reports.

> ✓ **Which DMARC policy?**
>
> Start with `p=quarantine`, watch the Reports page for two to four weeks until only your own senders appear and pass, then change to `p=reject`. With `reject`, mail that fails is refused outright by Gmail and others.

The live log

Live log shows the server's log as it's written: sign-ins, deliveries, refusals and errors. It's the first place to look when something doesn't work. Set the environment variable `RUST_LOG=debug` before starting the server for much more detail.

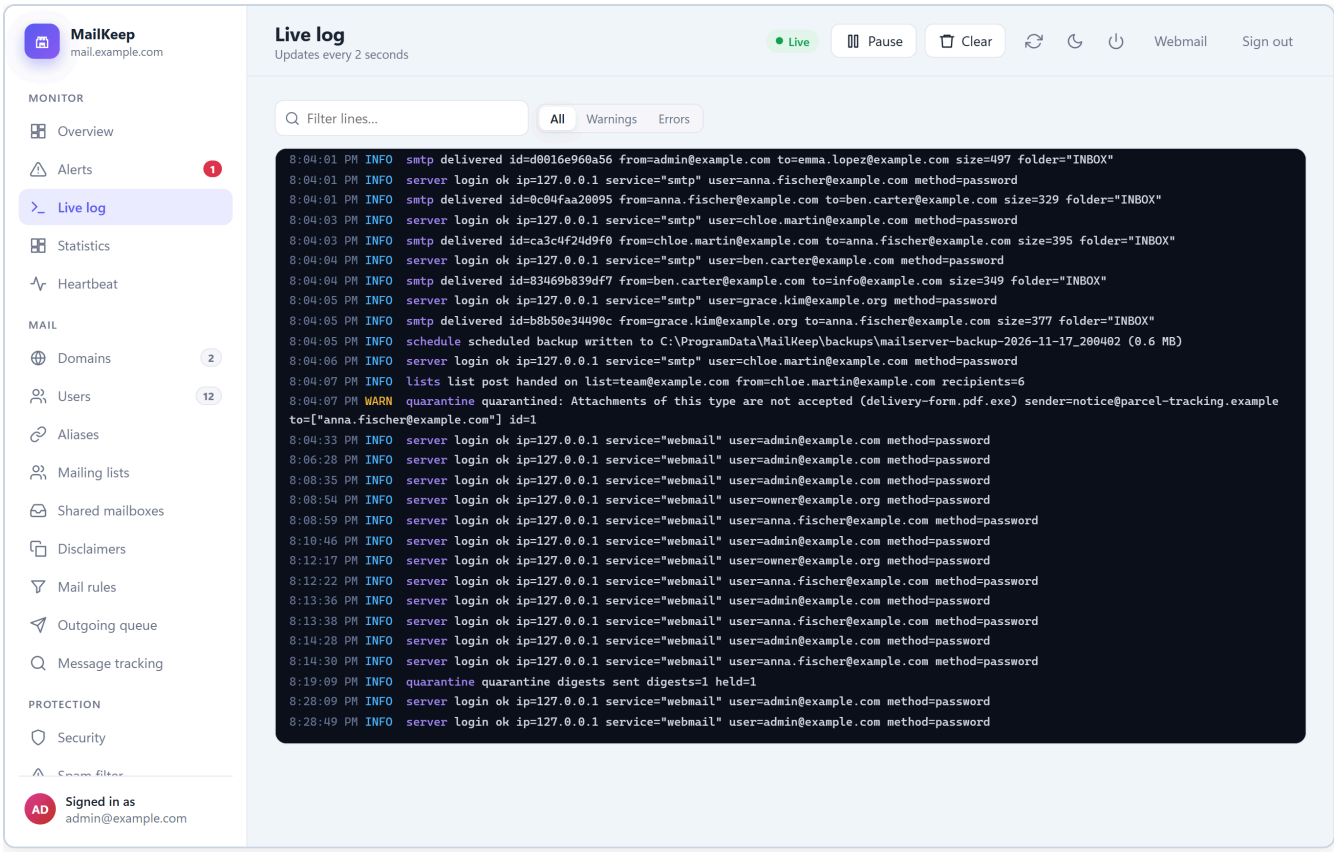


Figure 16.10 — The live log.

The setup check

Setup check (or `mailserver checkup`) looks at everything other mail servers judge you by, and says how to fix each problem, with the exact DNS record and a Copy button:

- the server name's A record, and the reverse DNS (PTR) of its address;
- the send-from address, when set;
- blocklists, and the certificate (trusted? expiring?);
- outgoing port 25, or the relay;
- the heartbeat services;
- for every domain: MX, SPF, DKIM, DMARC, MTA-STS, TLS reports, BIMI, and the auto-setup records.

Domain administrators see their own domains' checks only.

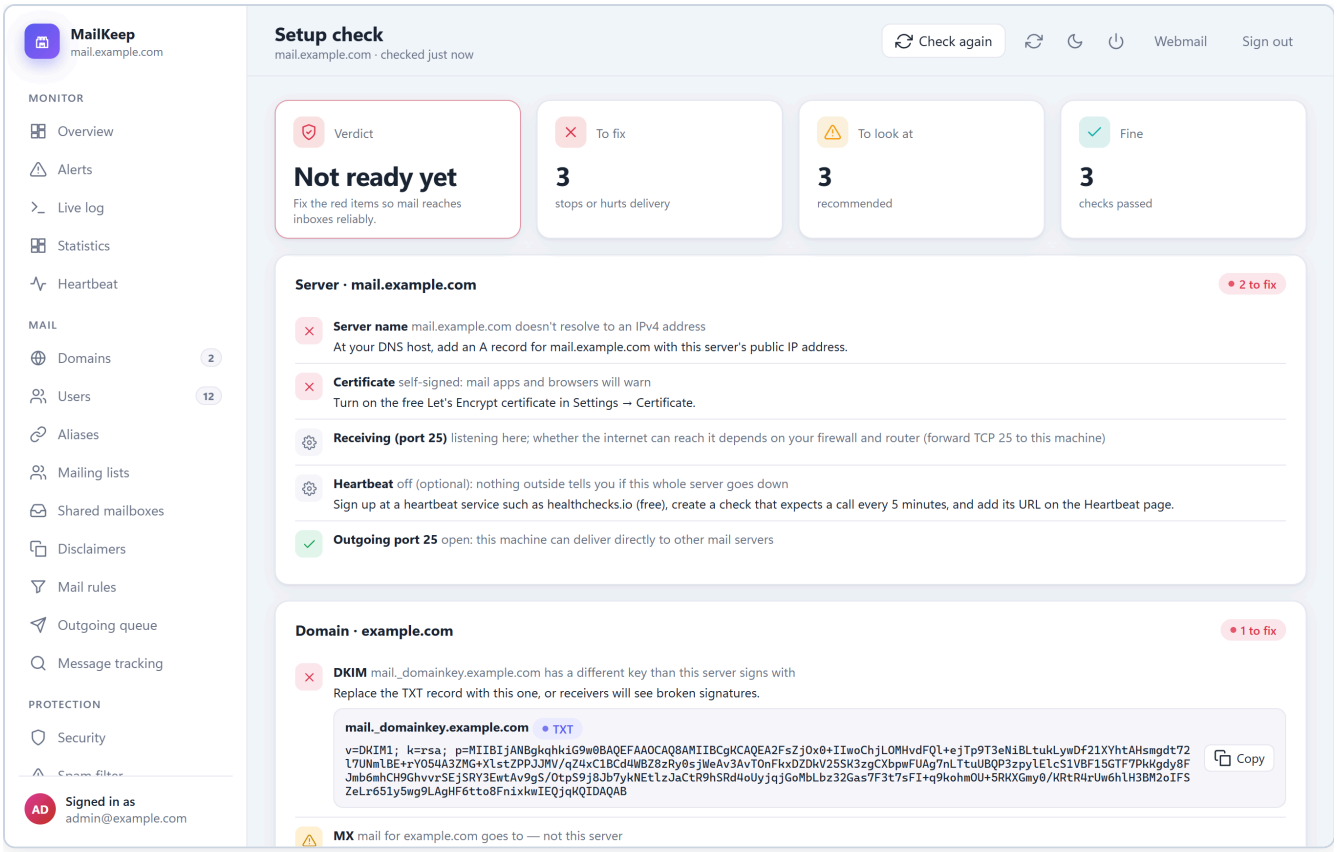


Figure 16.11 — The setup check on a test server: what's fine, what to look at, what to fix.

> ✓ **Before and after every big change**
>
> Run the setup check before you switch your MX records over, and again after. Fix every red item; amber items are recommendations.

Health and metrics for monitoring tools

Address	Returns	Who may ask
`/health`	200 with `{"status":"ok"}` when the database and disk are fine, 503 otherwise; also the queue size and uptime	Anyone (no sign-in), for uptime monitors
`/metrics`	Prometheus counters: mail received, sent, junked, refused, sign-ins, queue, users, bans	The local network, or anyone with `Authorization: Bearer <metrics_token>`

CHAPTER 17

Administrators and delegation

Full administrators, and domain administrators who manage only their own domains.

Two kinds of administrator

	Full administrator	Domain administrator
Sees	Everything	Only their domains
Domains page	Add, remove, DKIM, DNS, relays	Their domains: DKIM, DNS records, the domain's relay (no adding or removing domains)
Users, aliases, lists, shared mailboxes, disclaimers	All	Only addresses in their domains
Other administrators' accounts	Can change them	Can't reset their passwords, open their mailboxes or change them
Admin rights	Can grant and limit them	Can't make anyone an administrator
Overview, Statistics, Storage	The whole server	Their domains: their mailboxes, their mail and sign-ins, what needs them
Message tracking, Reports, Setup check	All domains	Mail from or to their domains; their domains' reports and DNS checks
Security	Everything	Their users' sign-ins, locked accounts (Unlock) and paused senders (Resume); no bans or blocked addresses
Spam filter	Everything	Allow/block entries for their mailboxes and domains, their users' learning filters; no filter settings
Quarantine	All held mail	Held mail whose recipients are all in their domains
Settings, Queue, Archive, Alerts, Live log, Heartbeat, Blocklists, Backups, Move in, Update, Restart	Yes	No — these concern the whole server

Every request a domain administrator makes is checked on the server, not just hidden in the console. Each address or domain in the request must be one of theirs, and a refused request is recorded in the audit log as *admin_denied*.

Making someone a domain administrator

1. Open **Users**, find the account, and choose ⋯ → **Make administrator**.

2. Choose ⋯ → **Admin of which domains…**, pick *Only these domains*, and list the domains, separated by commas.

Their row then shows **admin of example.org**. Choosing *Everything* makes them a full administrator again.

```
mailserver admin add jane@acme.com --domain acme.com
mailserver admin add pat@acme.com --domain acme.com --domain acme.org
mailserver admin add jane@acme.com           # without --domain: full administrator again
mailserver admin list                        # each admin and their domains
mailserver admin remove jane@acme.com
```

What a domain administrator sees

When they sign in, the console shows only the pages they may use and says *Domain administrator* at the bottom left. Their **Overview** is their own dashboard: their mailboxes, mail received and sent in the last day, failed sign-ins, a **Needs your attention** list (locked accounts, paused senders, held mail, mailboxes over 90% full, each a link to where it's fixed) and their largest mailboxes. In the dialogs for new users, aliases, lists and shared mailboxes, their domain is filled in.

They get e-mail about their own domains only: alerts about their mailboxes (sending paused, spam refused, nearly full, phishing reported, an account locked, an attack on a mailbox) and a **daily summary** of their domains, which they can turn off with the switch at the bottom of their Overview. The server-wide alerts and summary go to full administrators only.

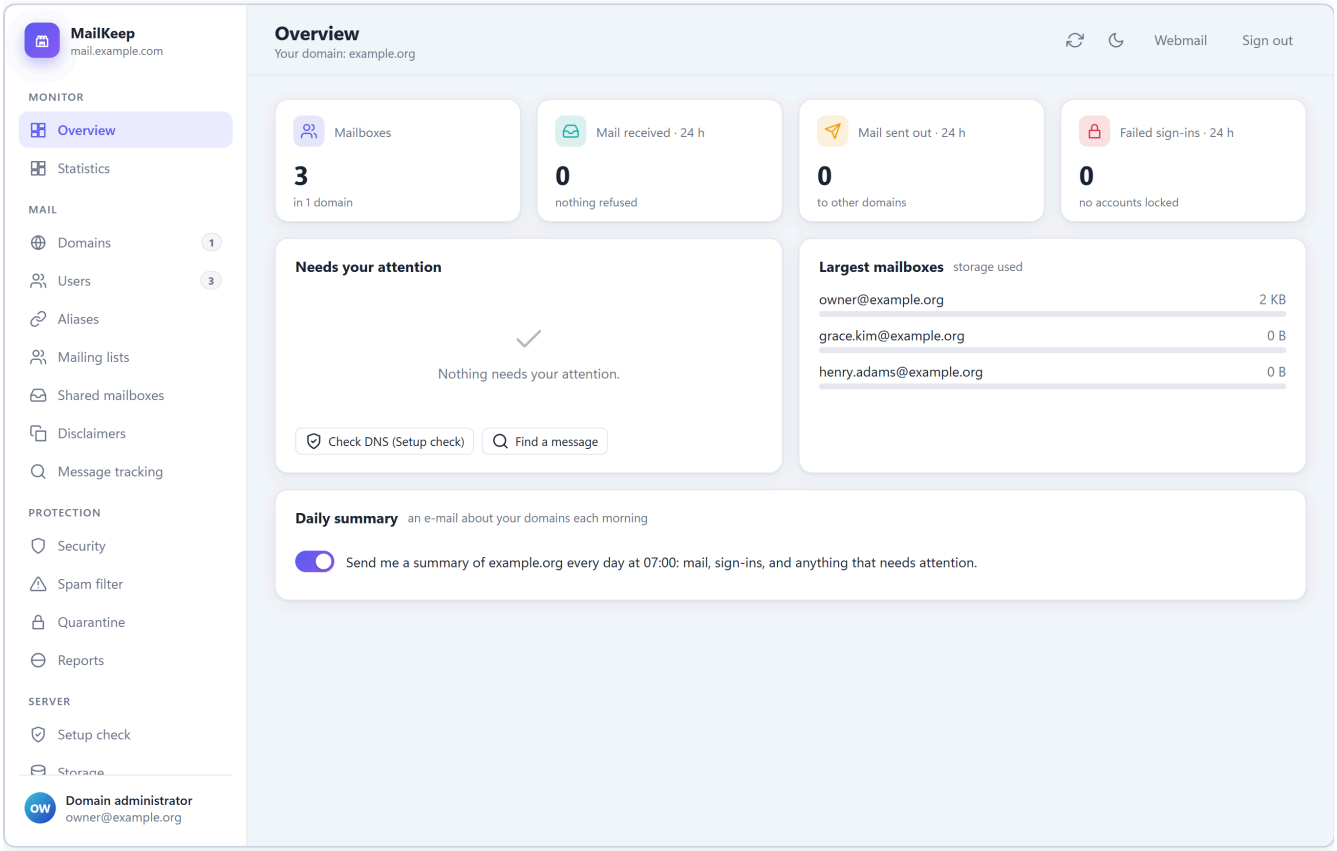


Figure 17.1 — The Overview as the domain administrator of example.org sees it.

✓ **Good practice**

Keep at least two full administrators, with two-factor sign-in on. You can't limit or remove your own admin rights from the console, so you can't lock yourself out by accident.

The management API and API keys

Other software, such as a billing system, a control panel or your own scripts, can manage MailKeep through the **management API**: the same calls the admin console makes, at `https://mail.example.com/admin/api/…`, signed in with an **API key** instead of a password.

1. Open Server → API keys and press New API key (full administrators only).
2. Name it after what will use it. Optionally list **only these domains**, and choose **read only** if it only needs to look.
3. Copy the key (`mk_…`): it's shown once and can't be looked up later. Keep it as safe as a password.

```
curl -H "Authorization: Bearer mk_…" https://mail.example.com/admin/api/users
curl -H "Authorization: Bearer mk_…" -H "Content-Type: application/json" \
     -d '{"address":"anna@example.com","password":"a long passphrase","quotaMb":2048}' \
     https://mail.example.com/admin/api/users
```

- A key **acts as the administrator who made it**, never more. A key narrowed to some domains acts like a domain administrator of those; a read-only key can only read. If its owner loses their admin rights or is turned off, the key stops.
- Some things are only possible in the console: making keys, granting admin rights, changing settings, restarting and installing updates. A leaked key can't take over the server.
- Calls need https, follow the console's network rule (*Allow the console from the internet*), and a wrong key counts as a failed sign-in, so guessing gets the address banned.
- Every change made with a key is in the audit log as … *(by admin@example.com via API key "Billing")*. The page shows when and from where each key was last used; Revoke stops a key at once.

Call	Body or query	What it does
`GET domains`		The domains
`POST domains`	`{name}`	Add a domain
`GET domains/dns`	`?domain=`	The DNS records it needs
`GET users`		Mailboxes with storage and status
`POST users`	`{address, password, quotaMb?}`	Add a mailbox
`POST users/password`	`{address, password}`	Set a password
`POST users/quota`	`{address, quotaMb}`	Storage limit in MB (0 = none)
`POST users/enable`	`{address, enabled}`	Turn a mailbox off or on

Call	Body or query	What it does
`POST users/remove`	`{address}`	Delete a mailbox and its mail
`GET aliases` / `POST aliases`	`{source, target}`	Extra addresses and catch-alls
`GET tracking`	`?q=&days=`	Message tracking
`GET stats`, `GET overview`		Statistics and dashboard numbers

Answers are JSON; errors are `{"error": "…"}` with status 400, 401 (no valid key) or 403 (not allowed for this key). The full list of calls is in `docs/API.md`.

CHAPTER 18

Backups and maintenance

Backing up while the server runs, copies off the server, restoring, updating the program, and keeping it healthy.

What a backup contains

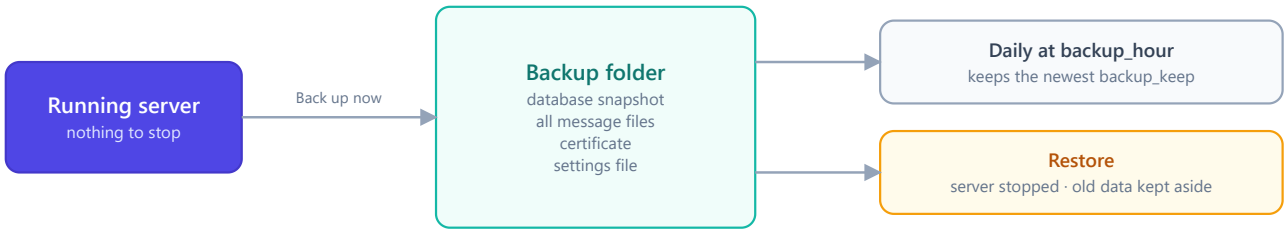


Figure 18.1 — A backup is one folder with everything needed to rebuild the server.

Each backup is a folder named `mailserver-backup-<date-time>` holding a consistent snapshot of the database (accounts, folders, rules, calendars, contacts, lists, DKIM keys), every message file, the certificate and the settings file. It's taken while the server runs; nobody notices.

The Backups page

Server → Backups has everything about backups in one place: the last backup and the schedule, the backups kept on this server, the off-site copies, how to bring a backup back, and the settings.

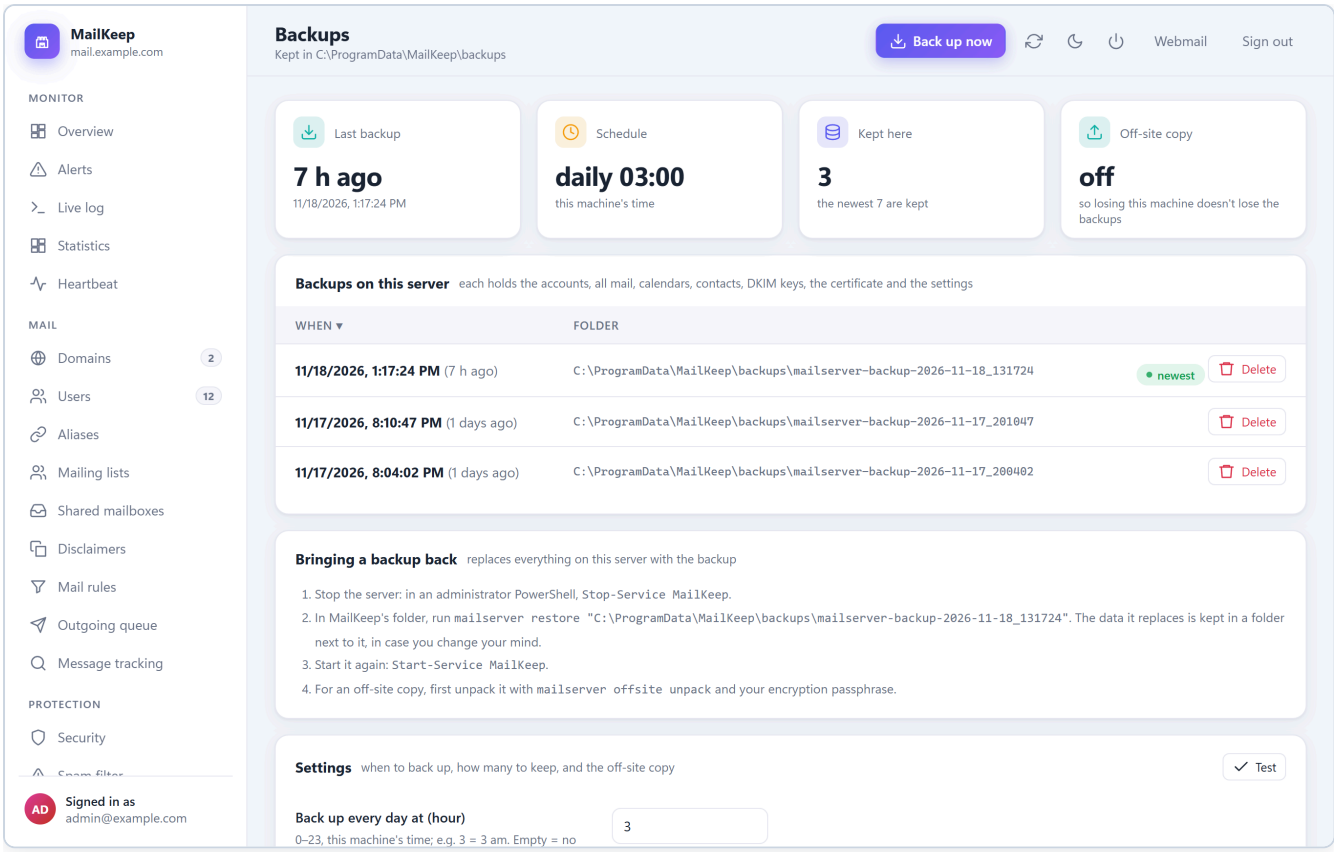


Figure 18.2 — The Backups page.

- **Now**: Back up now at the top of the page (also on the Overview), or `mailserver backup` (optionally `--to D:\Backups`).
- **Every day**: in the page's Settings, Back up every day at (an hour, 0–23). A server that was off at that hour catches up when it starts.
- **Before an update**: Server → Update makes one first (see "Updating MailKeep" below).
- **How many**: Backups to keep (7). After **every** backup (daily, Back up now, or before an update) the older ones beyond this number are deleted. After Back up now, the message says how many were removed.
- **Where**: Backup folder (`backup_dir`), by default `backups` next to the data folder. Another disk is better.

To remove one backup by hand, press Delete on its row under **Backups on this server** and confirm. It's gone from this server for good; its off-site copy (below) is not touched. Only full administrators can delete backups. Deleting the folders in Windows Explorer works too; MailKeep keeps no other record of them.

Copies off the server

Backups on the same machine don't help if the machine is lost. MailKeep copies **every** backup (scheduled or Back up now) to a second place by itself. In the Backups page's Settings, set Copy each backup to:

- **Another disk or network share**: a folder such as `E:\MailBackups` or `\\nas\backups`. Each backup folder is copied there as it is.
- **S3-compatible storage**: Backblaze B2, Wasabi, Amazon S3, MinIO and others. Each backup is packed into one file, compressed and **encrypted with your passphrase** before it leaves the server.

Setting up Backblaze B2 (or another S3 service)

1. At Backblaze, create a **private** bucket (for example `MailKeepBackup`), and set its Lifecycle Settings to *Keep only the last version of the file*, so copies MailKeep deletes don't stay billed as hidden versions.
2. Under Application Keys, create a key with **Read and Write** access to that bucket. Note the **keyID** and the **applicationKey**; the second is shown only once.
3. In MailKeep's Backups Settings, choose *S3-compatible storage* and fill in:

Field	Example
Storage address	`https://s3.us-west-004.backblazeb2.com` (the bucket's Endpoint, with https://)
Region	`us-west-004` (the part of the endpoint between `s3.` and `.backblazeb2.com`)
Bucket	`MailKeepBackup` (capitals as shown)
Folder in the bucket	`mailkeep`
Access key / Secret key	the keyID / the applicationKey
Encryption passphrase	12+ characters. **Keep a copy away from this server**: without it the copies can't be opened.
Copies to keep there	`14`

4. Press Save changes, then Test in the Settings header (it uses the saved settings), then Restart now.
5. Press Back up now. The message ends with *copying it off-site now*, and the **Off-site copy** card turns to *working*. Show copies lists what's stored there.

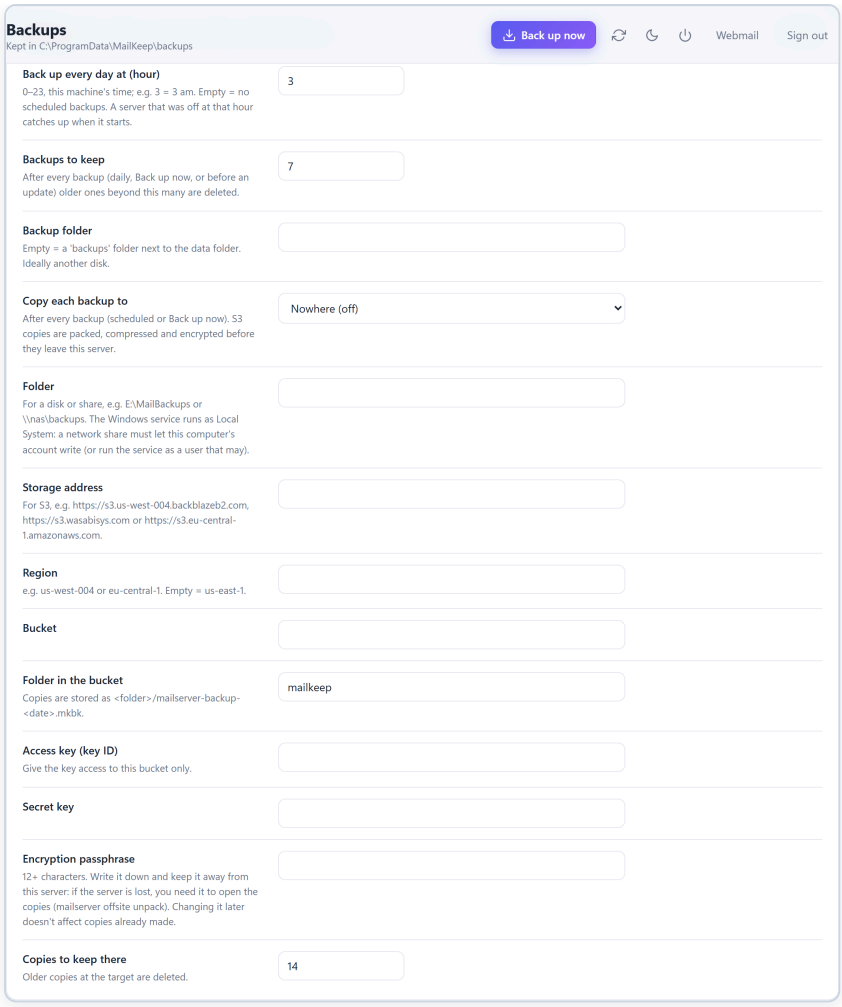


Figure 18.3 — The Backups page's Settings, with the off-site copy.

If a copy fails, the card turns red and the administrators get an alert. Once a year or so, try bringing a copy back on another machine (below), to know it works before you need it.

Restoring

The Backups page shows these steps with the exact command for your newest backup.

1. Stop the server: in an administrator PowerShell, `Stop-Service MailKeep` (or `mailserver service stop`).
2. In MailKeep's folder, restore: `mailserver restore "C:\ProgramData\MailKeep\backups\mailserver-backup-2026-11-12_030000"`. The current data is kept aside, not deleted.
3. Start the server again: `Start-Service MailKeep`.

For an **off-site copy** in S3 storage, bring it back as a backup folder first (the passphrase comes from the settings, or is asked for), then restore that folder:

```
mailserver offsite list                                  # the copies at the target, newest first
mailserver offsite get mailserver-backup-2026-11-12_030000.mkbk
mailserver offsite unpack D:\Downloads\mailserver-backup-2026-11-12_030000.mkbk   # a file you downloaded yourself, e.g. on a new machine
```

To move the server to a new machine: install MailKeep there, restore the latest backup, and change the DNS A record (and reverse DNS) to the new address.

Updating MailKeep

A new version comes as a new `MailKeep-Setup-<version>.exe`, for example `MailKeep-Setup-0.2.5.exe`; each release has its own number, shown on the Update page and in the program's file properties. Nothing needs uninstalling: settings, mail, users, certificates and DKIM keys stay where they are, and the database is brought up to date when the new version starts. There are two ways to install it.

From the admin console (Server → Update)

1. Open **Update**, click **Choose File**, pick the new `MailKeep-Setup-….exe` and click **Upload and check**.
2. The page shows the installed version and the new one (each with the time it was built). Leave **Back up mail and settings first** ticked.
3. Click **Install now**. Mail apps and webmail are disconnected for about half a minute; mail from other servers simply arrives a few minutes later. The page reconnects by itself and shows the new version.

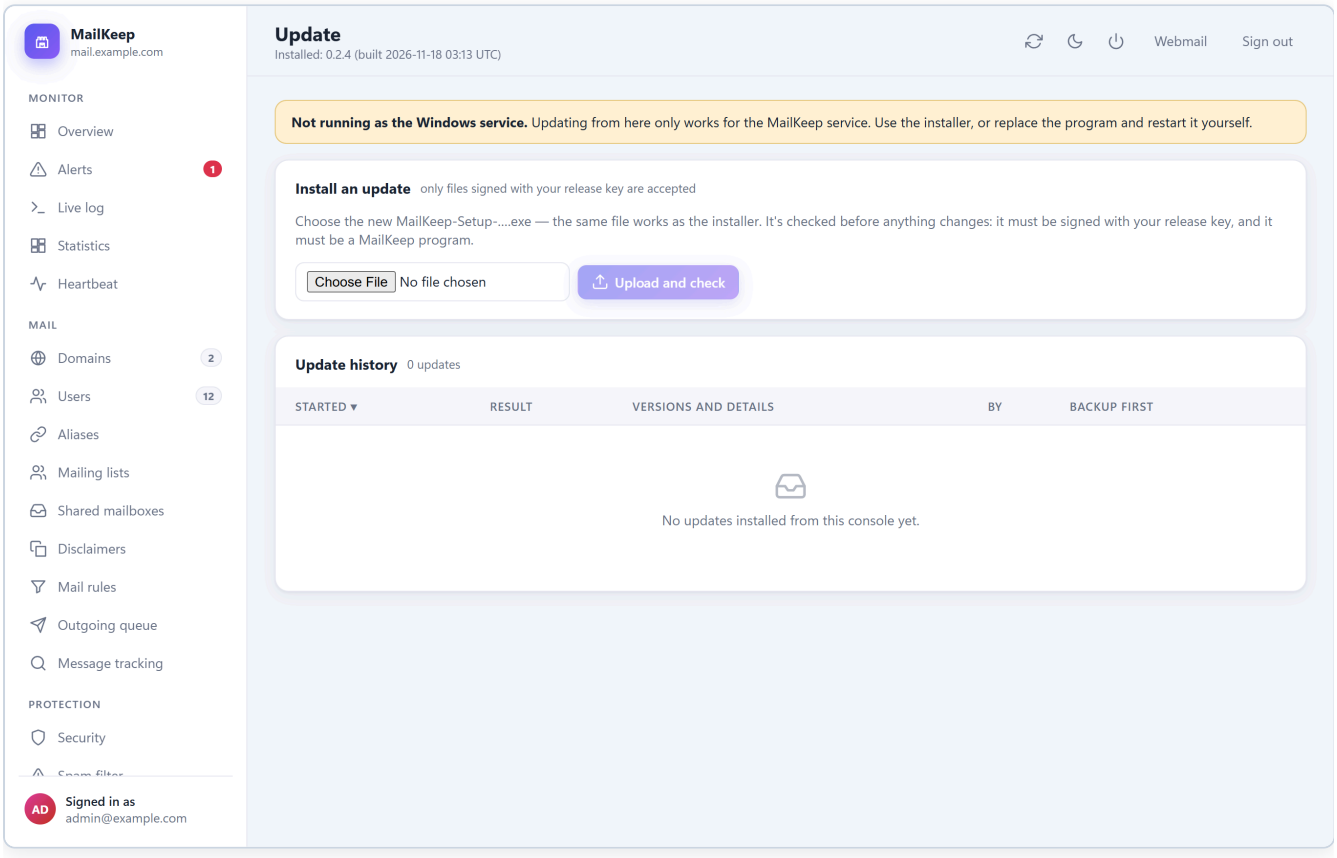


Figure 18.4 — The Update page and its history.

> **Only your own releases are accepted**
>
> Every release is signed with a release key, and the console only accepts files signed with the key the running copy was built with. An unsigned or altered file is refused before anything changes. Without this, anyone who found out an administrator's password could put their own program on the server. The private half of the key stays on the machine that builds releases; keep a copy of it somewhere safe.

If the new version doesn't start, or doesn't answer within 90 seconds, the previous version is put back automatically and an alert says why. The **Update history** on the same page lists every update with its date, the versions before and after, who started it, the backup made first, and whether it worked; the outcome is also in the audit log. The previous program is kept as `mailserver.old.exe` next to the new one.

With the installer

Copy the same file to the server and double-click it. Setup recognises the existing installation and offers Upgrade. Use this the first time, if the console isn't running as the Windows service, or if the server can't be reached from your browser.

On Linux, or from the command line: stop the service, replace the program, start the service.

A new program typically takes about 15 seconds to start the first time on Windows while Defender scans it.

Routine maintenance

How often	Task
Daily (automatic)	Backup, the administrators' daily summary, quarantine digest, list digests, certificate renewal check, alerts
Through the day (automatic)	Folder clean-up (hourly), archive retention, quarantine expiry, message-tracking clean-up, and the watchdog: disk space, blocklists, stuck mail, certificate
Weekly	Glance at the Overview and Alerts; check the off-site copy card on the Backups page
Monthly	Run the Setup check; review the audit log for administrator changes; check disk space
Yearly	Consider a new DKIM key (publish the new record first); review who is an administrator

CHAPTER 19

Moving in from another server

Importing from MailEnable or any IMAP server, and switching over without losing a message.

The Move in page

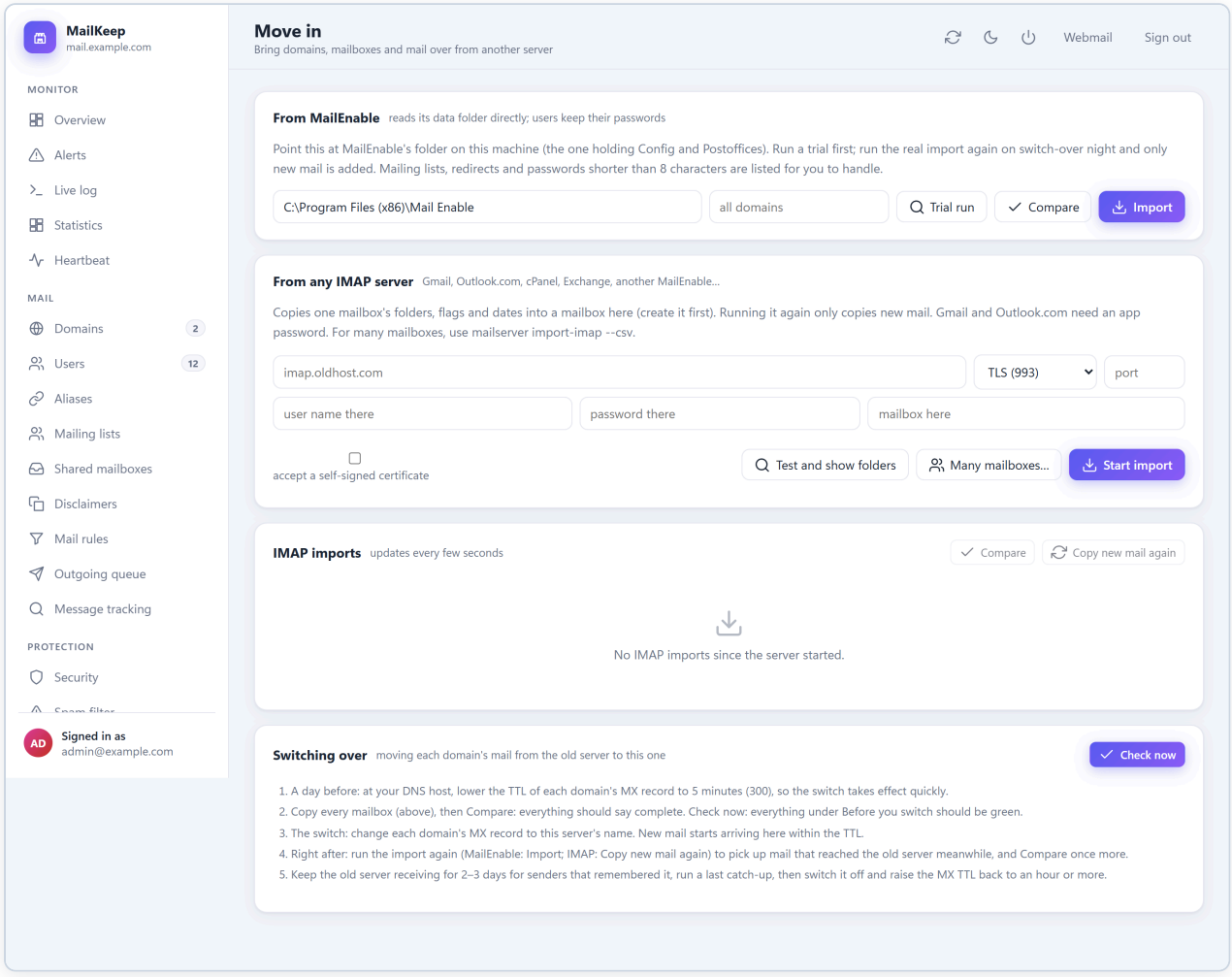


Figure 19.1 — Move in: from MailEnable or any IMAP server, Compare and Copy new mail again, and the Switching over checklist.

From MailEnable

The importer reads MailEnable's data folder directly (`Config\` and `Postoffices\`), so **users keep their passwords** and nothing has to be exported. Tested with MailEnable Standard (free) 10.48.

Comes over	Handled by hand
• Domains (post offices) • Mailboxes with their passwords, quotas, and disabled state • Every extra address as an alias; `*@domain` as a catch-all • The active DKIM key and selector, so the DNS record stays valid • All folders, including nested ones; Inbox, Sent Items, Drafts, Deleted Items and Junk E-mail become INBOX, Sent, Drafts, Trash and Junk • Every message with its read and flag state and received date	• Mailing lists: recreate them (chapter 9) • Redirects • Passwords shorter than 8 characters: those accounts get a random password; set a new one The importer lists all of these at the end.

1. Enter MailEnable's folder (usually `C:\Program Files (x86)\Mail Enable`) and optionally one domain.
2. Click **Trial run**. It shows what would come over, without changing anything.
3. Click **Import**. Check a few mailboxes in webmail or a mail app.
4. Run it again any time: only new mail is added.

```
mailserver import-mailenable "C:\Program Files (x86)\Mail Enable" --dry-run
mailserver import-mailenable "C:\Program Files (x86)\Mail Enable" [--only example.com]
```

From any IMAP server

Gmail, Outlook.com, cPanel, Exchange, another MailEnable... Any server that offers IMAP can be copied from: folders, flags and dates. Create the mailbox here first. Gmail and Outlook.com need an app password.

1. Enter the server, its security (TLS on 993, STARTTLS or none on 143), the user name and password there, and the mailbox here.
2. **Test and show folders** signs in and lists the folders with their message counts.
3. **Start import** runs it in the background; progress appears under *IMAP imports*.

Many mailboxes... imports a list, one after another. Paste one line per mailbox: `remote user,remote password,local address`. A password may contain commas.

```
mailserver import-imap --host imap.oldhost.com --user old@example.com --to bob@example.com
mailserver import-imap --host imap.oldhost.com --csv mailboxes.csv
mailserver import-imap --host old.example.com --security starttls --insecure --user … --to …   #
self-signed
```

Running an import again copies only new mail, so import early and top up on switch-over night.

Is everything here? Compare

Before switching, and again after, check that every message came over:

- **MailEnable**: **Compare** next to Import reads MailEnable's folder and checks every mailbox, folder by folder, against the import's own record of the files it copied. Each mailbox shows *complete*, *N missing*

with the folders concerned, or *no mailbox here*. It changes nothing.

- **IMAP**: Compare on the *IMAP imports* panel signs in to the old server again for each mailbox imported since the server started and compares the number of messages in each folder there and here. Mail that arrived here since doesn't hide anything missing.

To copy what's missing, run the import again: Import for MailEnable, or Copy new mail again on the *IMAP imports* panel, which reruns every IMAP import since start-up. Only new mail is copied.

> *i* **After a restart**
>
> IMAP passwords are kept in memory only, never on disk, so Compare and Copy new mail again cover the IMAP imports started since the server last started. After a restart, start those imports again: they still copy only what's new.

Switching over without losing mail

The **Switching over** panel at the bottom of the Move in page does the checking for you. Check now runs the Setup check and sorts what matters into three lists, each item with its fix:

- **Before you switch**: the server's name, reverse DNS, send-from address, certificate, port 25 in and out, blocklists, and DKIM, SPF and DMARC for each domain. A banner says *Ready* once nothing here is red.
- **The switch**: where each domain's MX points now (an MX under the domain's own name, such as `mail.customer.com`, counts as here when it points at this server's address).
- **Copying mail**: how the IMAP imports since start-up went.

The panel also lists the steps: lower the MX record's TTL to 5 minutes a day before; copy and Compare; change each domain's MX to this server; run the imports once more and Compare again; keep the old server receiving for two or three days, then a last catch-up, and switch it off.

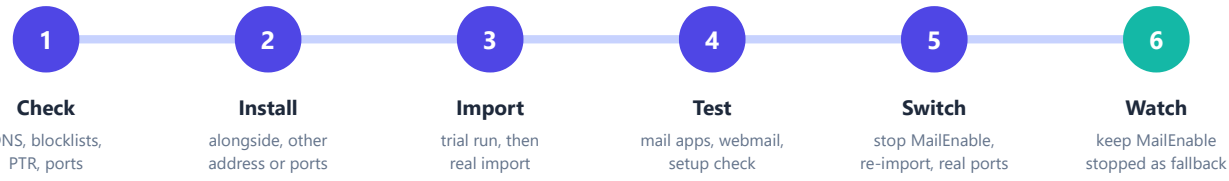


Figure 19.2 — The six steps from the old server to MailKeep.

1. **Check** the server: reverse DNS, blocklists, outgoing port 25, disk space.
2. **Install alongside** the old server so nothing changes for users yet: either on a second IP address with the normal ports (each server bound to its own address, figure 4.4), or on spare ports such as 2525, 1143 and 1993.
3. **Import**: a trial run, then the real import.
4. **Test** with real mail apps and webmail, and fix everything the Setup check flags. Get the real certificate.

5. **Switch** on a quiet evening: stop the old server, run the import once more (only new mail is copied), move MailKeep to the real ports or address, and start it. If the MX records already point at the server's name, they don't change.
6. **Watch** the Overview and Live log for a few days. Keep the old server installed but stopped, so you can switch back.

> ! **Rolling back**
> Switching back is just stopping MailKeep and starting the old server, but mail that arrived in between stays in MailKeep. Keep the window short, and decide early.

CHAPTER 20

For users: webmail, mail apps and phones

Everything the people who use the mail need: webmail with its calendar and tasks, setting up mail apps and phones, out-of-office, passkeys and two-factor sign-in, and shared mailboxes.

Webmail

Webmail is at **https://mail.example.com/webmail/**. Sign in with your full e-mail address and password, and the 6-digit code if two-factor sign-in is on, or press Sign in with a passkey if you've added one. Forgot your password? sends a reset link to the backup address you set under ⚙ Settings → Profile. The link always points at your own mail server's address; a reset e-mail with a link to any other site isn't from MailKeep. On your own domain's address, such as `mail.yourcompany.com`, the name before the @ is enough: the domain is shown greyed after the box. If your company has its own look, the sign-in page and the top bar show its name, colour and logo.

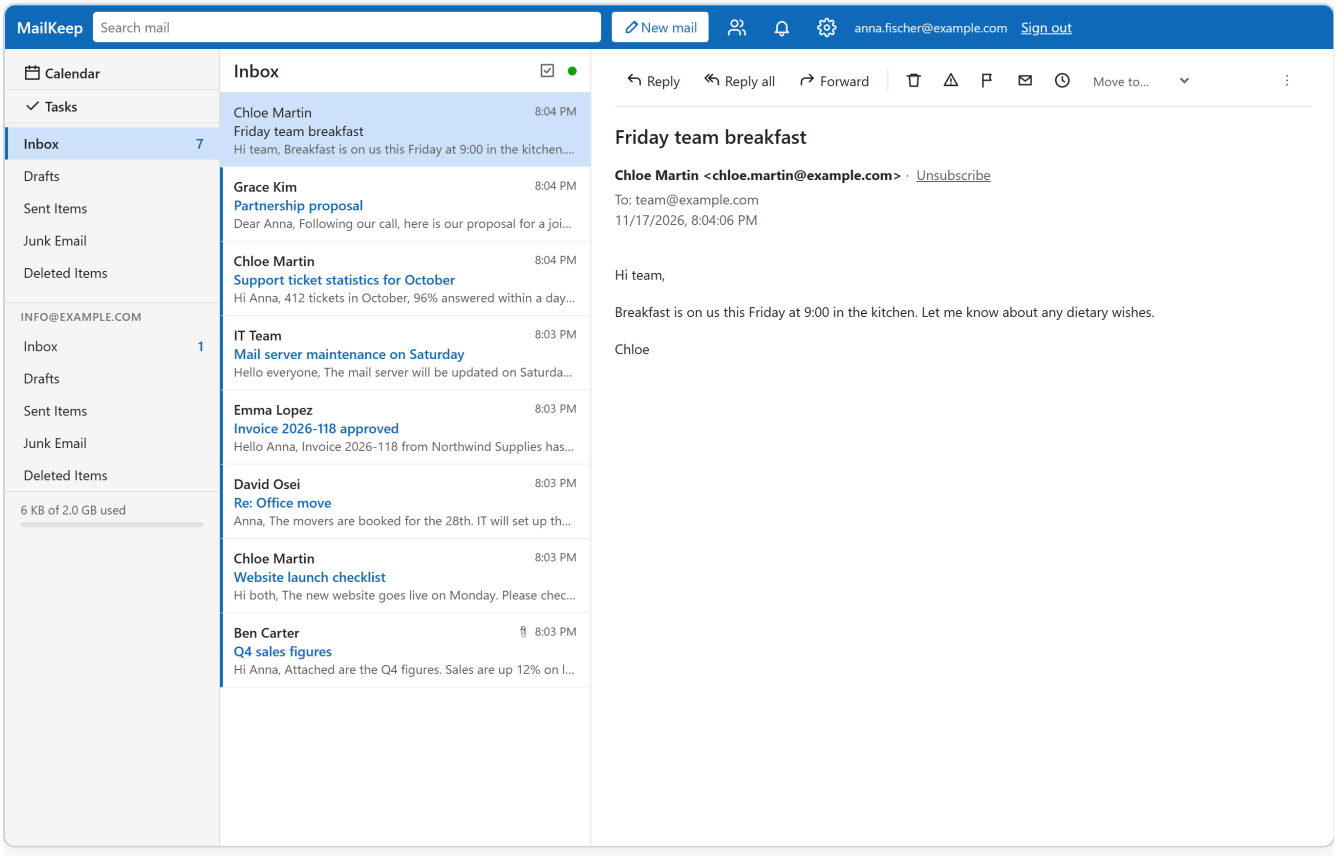


Figure 20.1 — Webmail: folders, the message list and the reading pane.

- **Folders** on the left with unread counts; the **message list** in the middle with previews; the **reading pane** on the right.
- Buttons for the open message: Reply, Reply all, Forward (keeps attachments), then icons for **Delete** (to Deleted Items; from there, permanently), **Junk** / **Not junk** (teaches your spam filter), **Flag**, **Mark unread**, **Snooze** (the message leaves the Inbox and comes back at the time you choose) and Move to.... Less common actions (print, show the original, **Report phishing**...) are under ⋯.

- **Conversations**: replies are grouped with the message they answer, so a whole exchange reads top to bottom. Turn it off under ⚙ Settings → Writing → Reading.
- **Attachments** open in a preview (pictures, PDFs, text) without downloading; Download is in the preview.
- **Select several** with the tick-box button above the list, then delete, move, flag or mark them together.
- **Search** at the top looks through sender, subject and text.
- New mail appears by itself (the green dot shows the live connection).
- HTML mail is shown safely: no scripts, and no remote images or tracking pixels, though pictures inside the message still show.
- Mail from **outside your organization** shows a banner. If it uses a colleague's name, a red *Be careful* warning appears instead (a common fraud trick); saving the sender in your contacts stops it.
- Newsletters get an Unsubscribe button. A sender who asked for a **read receipt** gets a Send receipt button, and you can ask for one when you write.

Writing

- **Undo send**: for a few seconds after pressing Send, an Undo button takes the message back (the delay is set under ⚙ Settings → Writing).
- **Send later**: the clock next to Send picks a time; the message waits on the server, even if your computer is off.
- **Templates**: save a message you write often with Save as a template… and insert it from the compose window. **Signatures** are set in Settings → Writing.
- **Big files**: attachments too big for e-mail are uploaded and sent as a download link instead.
- Addresses are suggested as you type, from your contacts and the **company directory**.

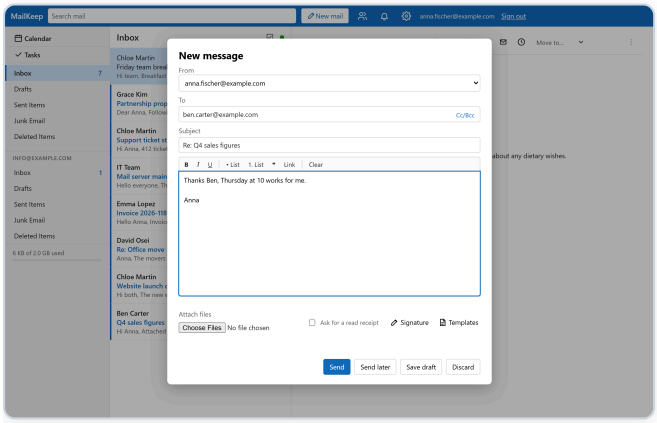


Figure 20.2 — Writing a message: To, Cc, Bcc, subject, text and attachments.

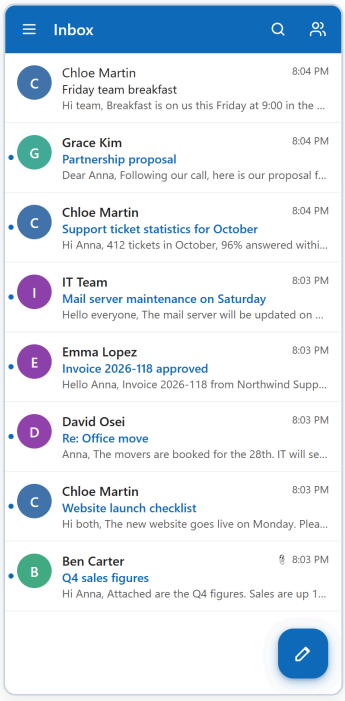


Figure 20.3 — On a phone, one pane at a time.

Webmail as an app

Webmail can be installed like an app, with its own window and icon:

- **On a PC** (Edge or Chrome): open webmail and choose ⋯ → **Apps** → **Install MailKeep Mail**, or click the install icon at the right of the address bar. It then has its own window, a taskbar and Start menu entry.
- **On Android** (Chrome): ⋮ → **Add to Home screen** → **Install**.
- **On an iPhone or iPad** (Safari): the share button, then **Add to Home Screen**. On an iPhone, new-mail notifications (below) only work when webmail is opened from this Home Screen icon (iOS 16.4 or later).

Signing in works as on the web page. To remove it, uninstall it like any app (on a PC, ⋯ → **Uninstall** in its window).

New-mail notifications

Click the 🔔 button at the top and allow notifications. New mail then pops up on your desktop or phone even when the webmail page is closed. Each browser is turned on separately, and ⚙ **Settings** → **Notifications** lists them with a test button.

Webmail settings

⚙ **Settings** has a list of sections on the left:

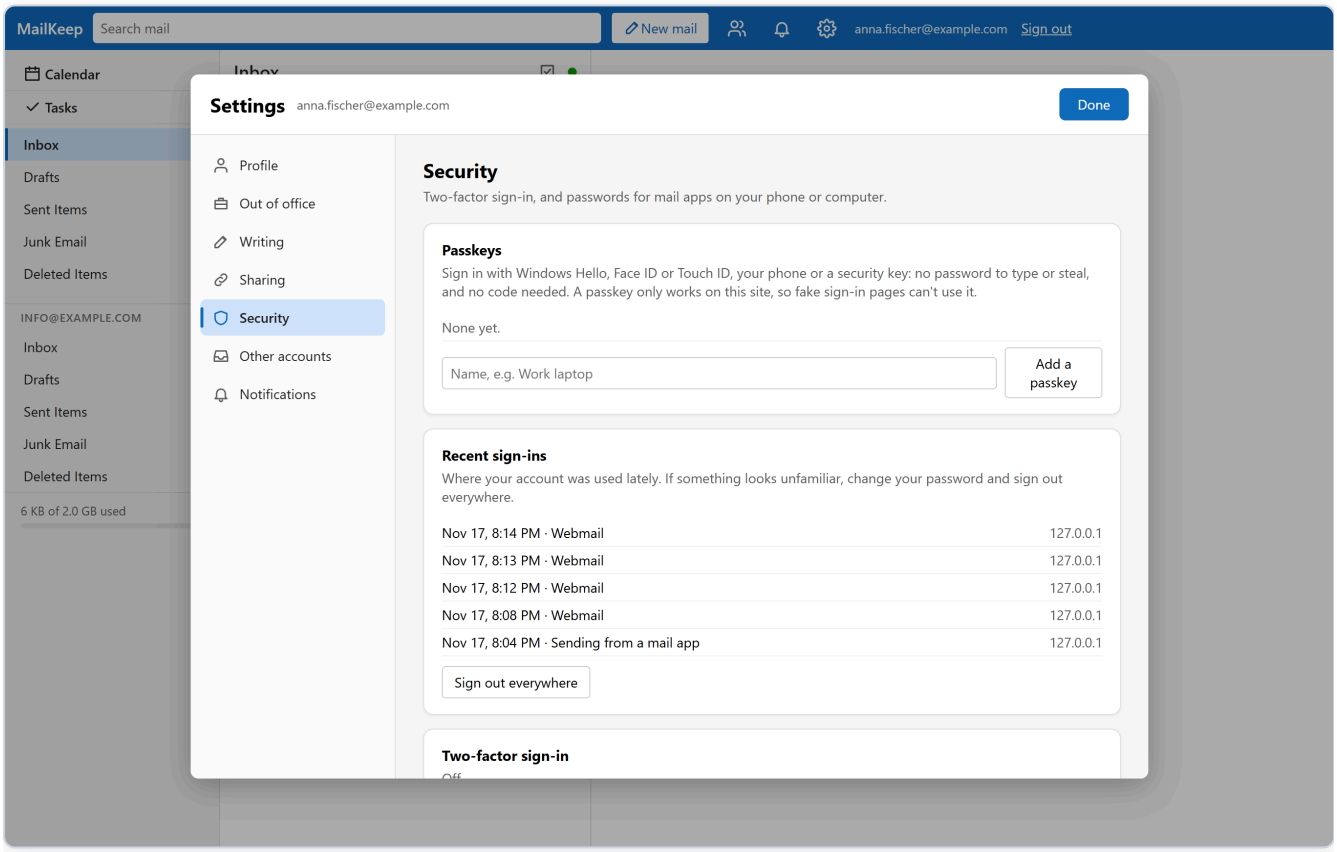


Figure 20.4 — ⚙ Settings in webmail, on the Security section.

Section	What you can do
Profile	Your name; change your password (your other sessions are signed out); a **backup address** for resetting a forgotten password.

Section	What you can do
Out of office	**Automatic reply**: turn on, write the subject and message, choose how often the same person gets it (once every 7 days by default); it never answers mailing lists, robots or Bcc copies. **Forwarding** to another address, keeping a copy here or not.
Writing	Signatures, templates, the undo-send delay, conversations on or off, **Newsletters**: whether newsletters and marketing mail go to a Newsletters folder instead of the Inbox (move a message back to the Inbox and that sender stays there; move one into Newsletters and its sender goes there from then on), and **auto-archive**: read mail older than 3, 6, 12 or 24 months moves from the Inbox to Archive (flagged and unread mail stays), which keeps the Inbox and your phone quick.
Sharing	Folders you've shared by link, and big files you've sent as download links, with when they expire.
Security	**Passkeys**; **recent sign-ins** (when, from where, through which service) with Sign out everywhere; two-factor sign-in; app passwords for mail apps.
Other accounts	Collect mail from another address (POP3) into this mailbox.
Notifications	Which browsers get new-mail notifications; send a test.

The calendar

Click Calendar at the top of the folder list. It shows a month or a list, with your calendars and those shared with you.

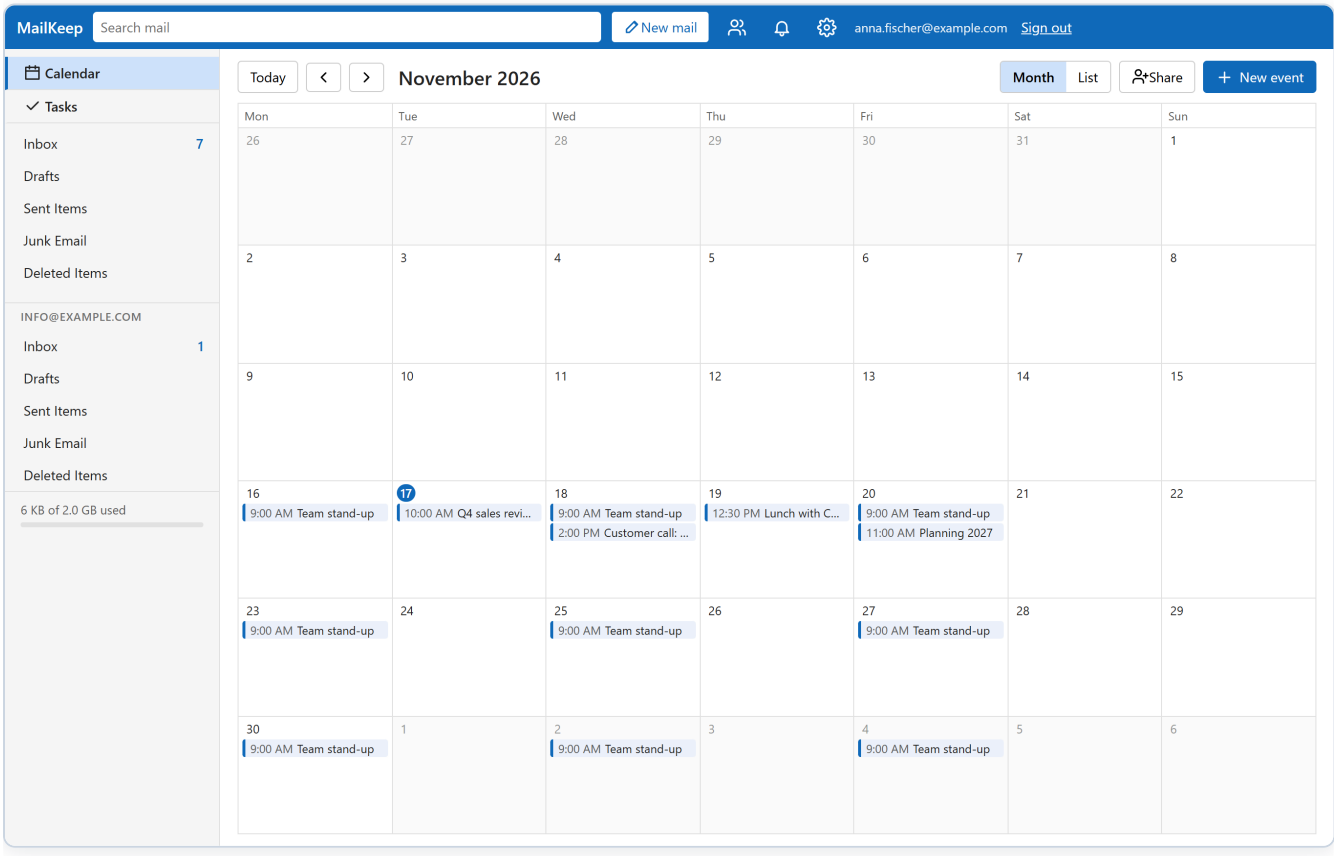


Figure 20.5 — The calendar.

- New event: a title, the time (or all day), where, notes, and whether it **repeats**.
- **Meetings**: under Invite people, add colleagues or outside addresses. Everyone on this server shows whether they're **free or busy** at that time. Invitations go out by e-mail, so Outlook, Gmail, Apple Mail and phones understand them; answers (Accept, Maybe, Decline) update your event by themselves.
- **Meeting rooms**: pick a Meeting room. A room is a mailbox that answers by itself: accepted when free, declined when already booked. (An administrator creates a mailbox for the room, then on the Users page chooses ⋯ → Name, title and phone… and sets *This mailbox is* to *A meeting room*.)
- An invitation you receive shows Accept, Maybe and Decline right in the message.
- Share: let colleagues see, or also change, one of your calendars (a team calendar, or an assistant keeping someone's diary). Shared calendars appear next to theirs, in webmail and on phones.

Tasks

Tasks is a simple to-do list with due dates. Tick a task when it's done. Tasks sync with phones over CalDAV (Apple Reminders, and Android apps through DAVx[5]).

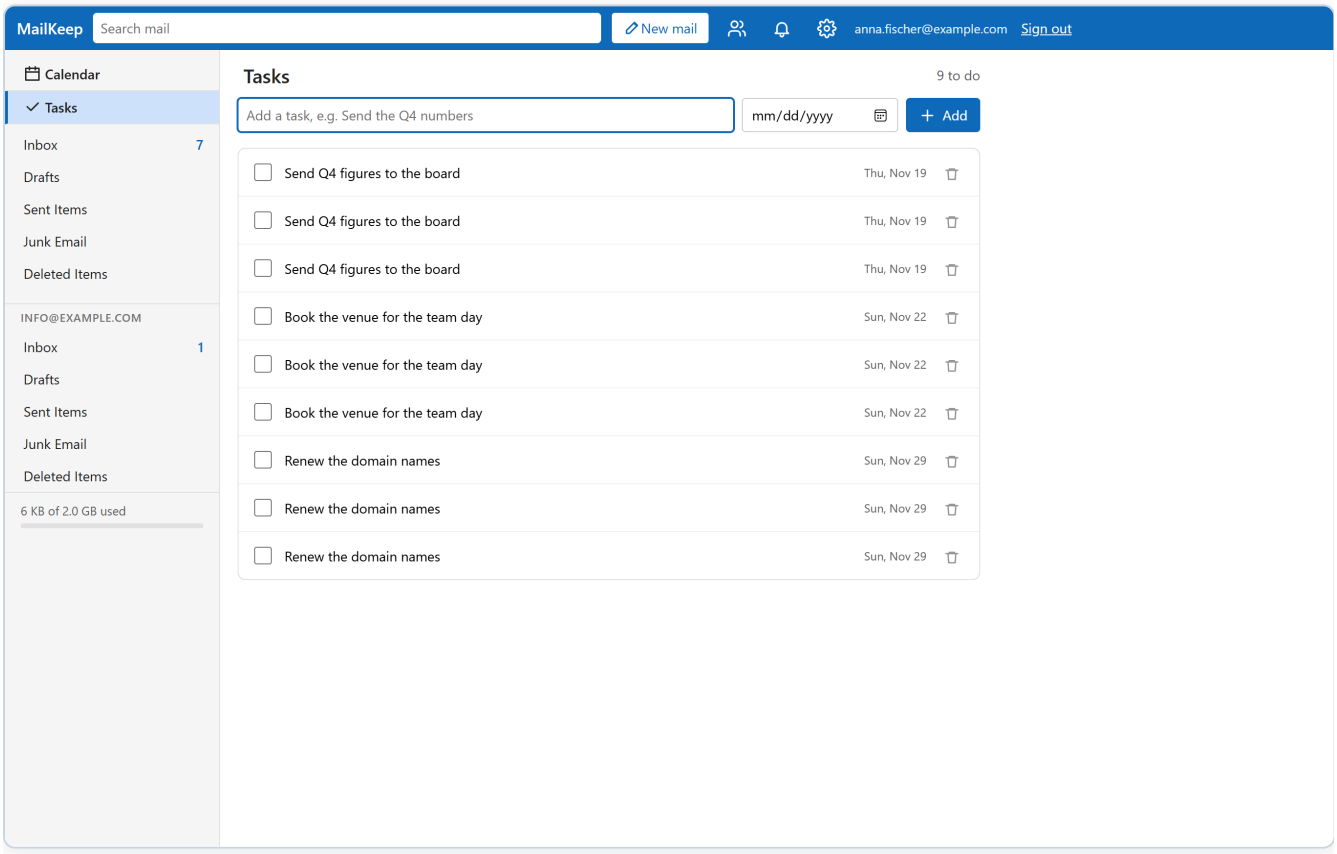


Figure 20.6 — Tasks.

Setting up a mail app

Most mail apps set themselves up from just your e-mail address and password.

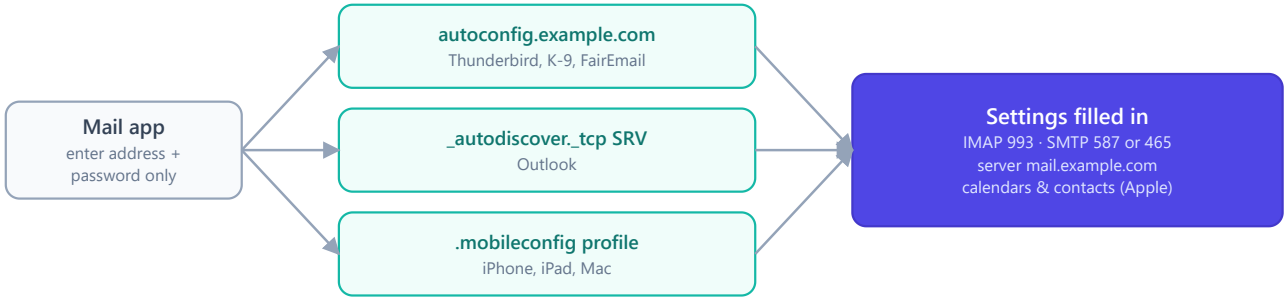


Figure 20.7 — How mail apps find the right settings.

If an app asks for the settings, use these (with your server's name):

	Server	Port	Security
Incoming (IMAP) — recommended	mail.example.com	993	SSL/TLS
Incoming (IMAP)	mail.example.com	143	STARTTLS
Incoming (POP3)	mail.example.com	995 / 110	SSL/TLS / STARTTLS
Outgoing (SMTP)	mail.example.com	587	STARTTLS
Outgoing (SMTP)	mail.example.com	465	SSL/TLS

User name: your **full e-mail address**. Password: your password, or an app password if two-factor sign-in is on. Outgoing server requires sign-in: yes, same as incoming.

> *i* **IMAP or POP3?**
> Use IMAP. Your mail stays on the server, so every device sees the same folders, read state and flags, and new mail arrives instantly. POP3 downloads mail to one device.

iPhone, iPad and Mac

Open **https://mail.example.com/apple/mailserver.mobileconfig** in Safari and install the profile (Settings → Profile Downloaded). It sets up mail, calendars and contacts in one go.

Android

In Gmail, Outlook, K-9 or FairEmail, add an account with your e-mail address and password; choose IMAP if asked. For calendars and contacts, install DAVx[5] and sign in with `https://mail.example.com/`.

Outlook and Thunderbird

Add the account with your e-mail address; both find the settings by themselves (Outlook through autodiscover, Thunderbird through autoconfig). Thunderbird also syncs calendars and address books: add a *network calendar* or *CardDAV address book* with `https://mail.example.com/`.

Calendars and contacts

Calendars and address books sync with CalDAV and CardDAV. Point any calendar or contacts app at `https://mail.example.com/` and sign in with your e-mail address and password; it finds your calendars and address books by itself. You can have several of each, with names and colours, and changes sync to every device.

Everyone also gets a read-only **Company directory** address book with every colleague's name, job title and phone, kept up to date by the server, so nobody has to add colleagues by hand.

Mail rules

Server-side rules run on every message as it arrives, even when all your devices are off. Mail apps that support **ManageSieve** (port 4190) — Thunderbird with a Sieve add-on, Roundcube, and others — can edit them. A rule that files invoices into a folder:

```
require ["fileinto", "mailbox"];
if header :contains "subject" "invoice" { fileinto :create "Accounts"; }
```

A broken rule or a missing folder never loses mail; the message goes to the Inbox instead.

Shared mailboxes

If you've been given access to a shared mailbox such as `info@example.com`, everyone with access sees the same messages: if you read or flag one, the others see that too — and if you delete one, it's gone for everyone.

In webmail, the shared mailbox appears below your own folders, under its address. Open its folders as usual. You only get the buttons your access allows: with read-only access there is no Delete, Flag or Move. Shared folders refresh every minute (your own Inbox updates instantly).

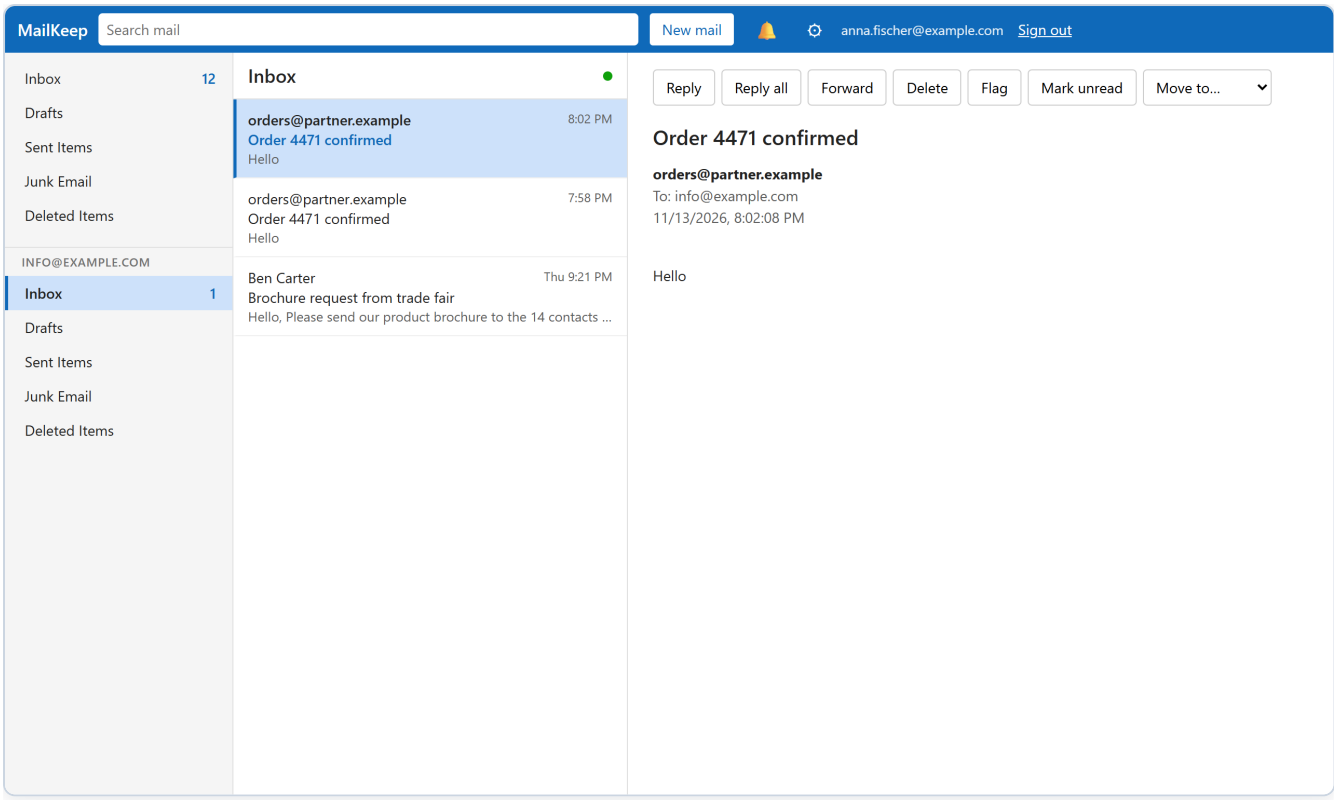


Figure 20.8 — Anna's webmail: her own folders, then the shared info@example.com.

Sending as the shared address. If you were given "send as", a **From** list appears when you write a message. Replying to a message in the shared mailbox picks its address for you, so the customer gets an answer from info@, not from you. The sent message is kept in your own Sent folder.

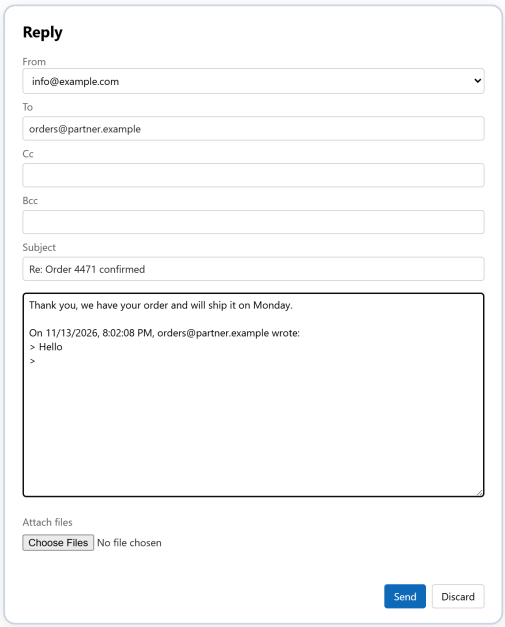


Figure 20.9 — Replying from info@example.com.

In a mail app, it appears under **Shared** → **info@example.com**. *Shared* and the mailbox's address are headings; open the folders under them. With "send as" access, choose the shared address as From in your mail app.

CHAPTER 21

Settings reference

Every setting in mailserver.toml, where to find it in the admin console, its default and what it does.

Settings live in `mailserver.toml`, which `mailserver init` creates with every value at its default. Change them under **Settings** in the admin console or in the file, then restart (**Settings → Restart server**, or restart the service). Settings marked *file only* are edited in the file. Saving in the console checks the values and keeps the last five versions of the file as `.bak`.

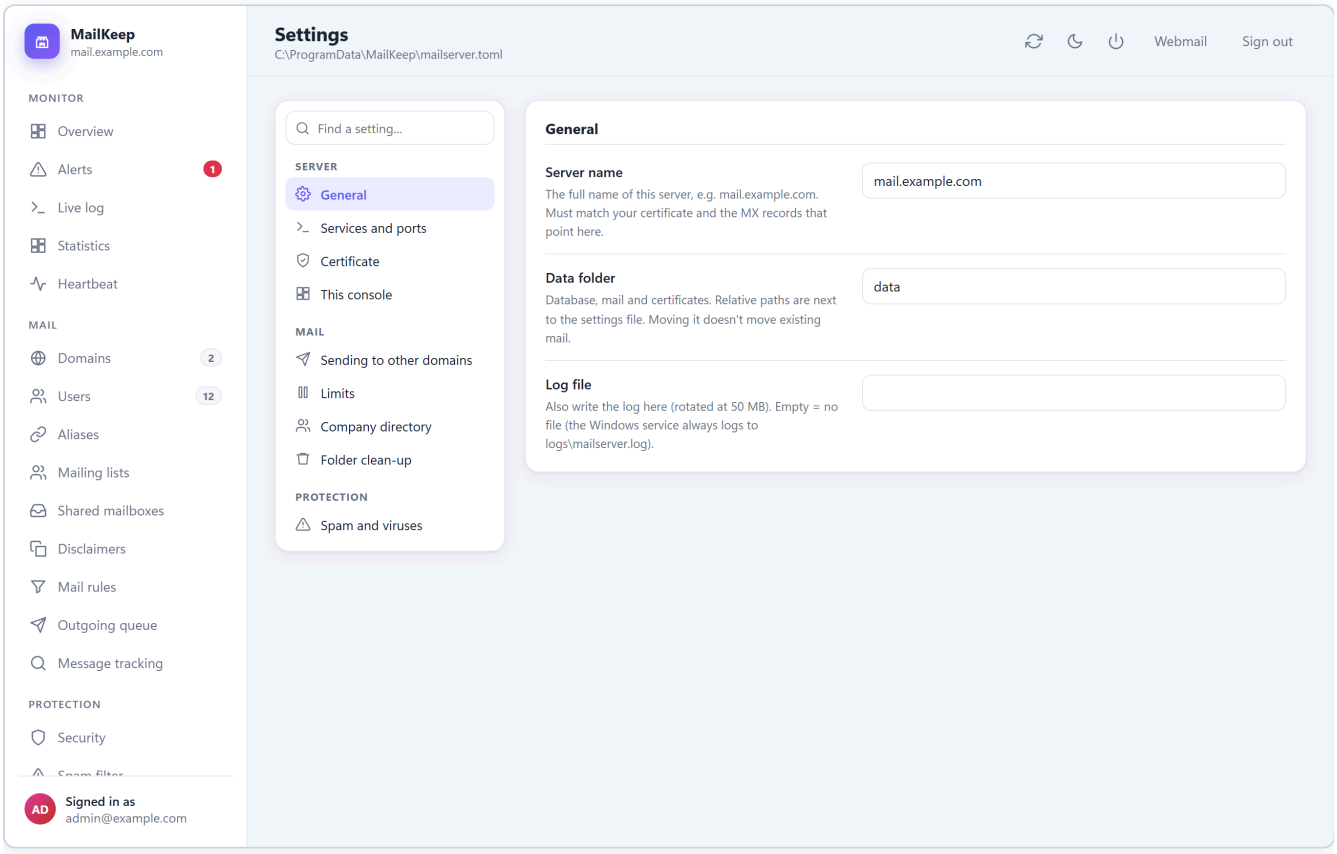


Figure 21.1 — The Settings page, with a button for each section at the top.

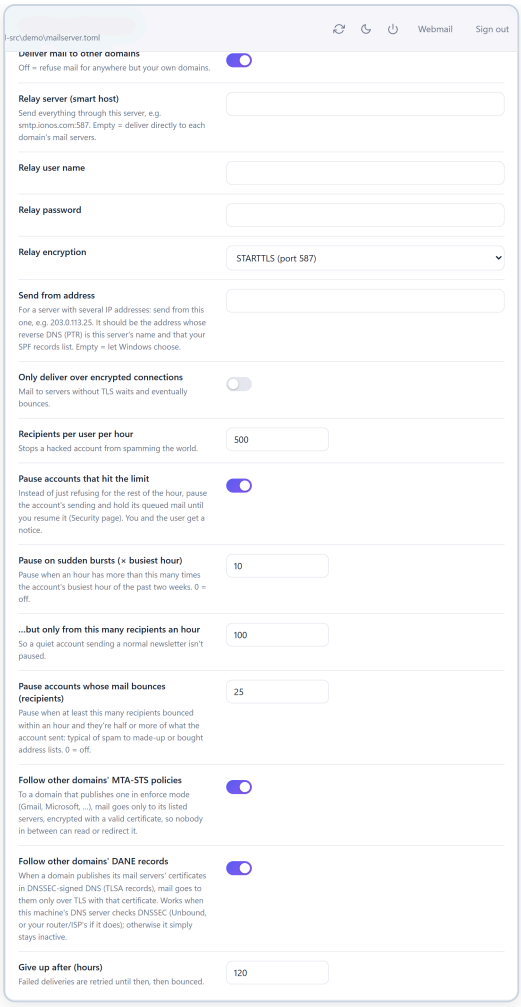


Figure 21.2 — A section of the Settings page: Sending to other domains.

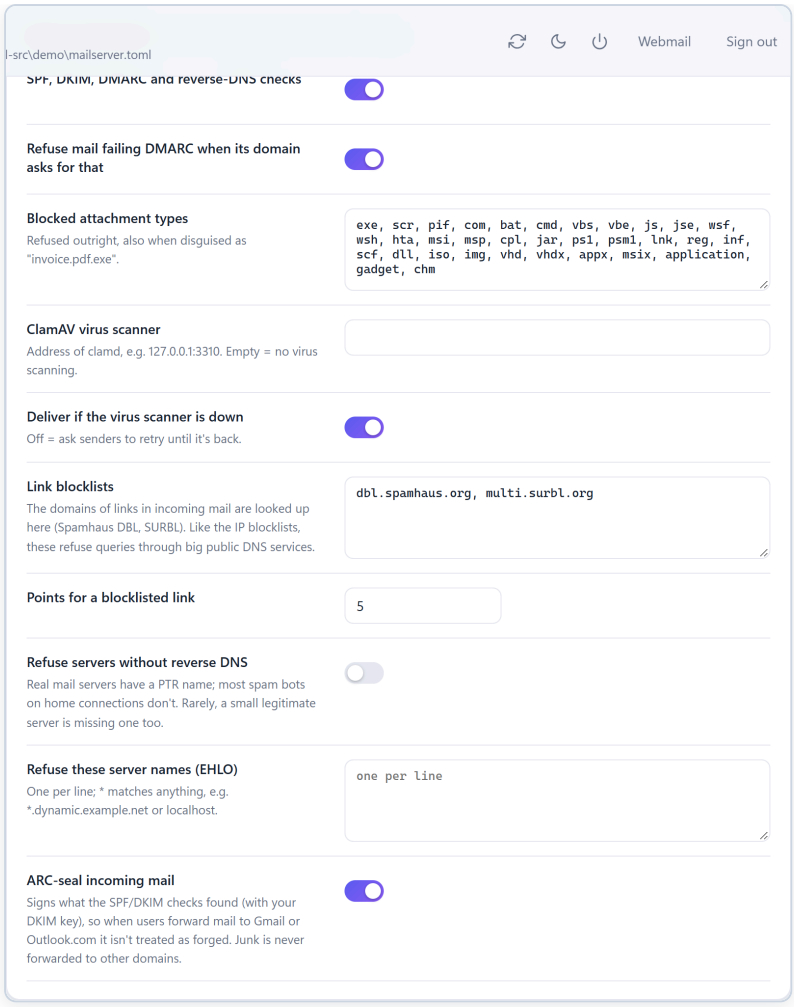


Figure 21.3 — Spam and viruses.

General

The top of the file: the server's name and where it keeps its data.

Setting	In the console	Default	What it does
`hostname`	Server name	mail.example.com	Name this server uses in greetings and Received headers (e.g. mail.example.com).
`data_dir`	Data folder	data	Folder for the database, message files and generated certificates.
`log_file`	Log file	—	Also write the log to this file (rotated at 50 MB, 5 kept). The Windows service always logs to a file: this one, or logs\mailserver.log next to the settings.

[listeners] — services and ports

Address and port for each service, e.g. "0.0.0.0:25" (all addresses) or "108.181.187.170:25" (one address). Leave one empty to turn that service off.

Setting	In the console	Default	What it does
`smtp`	SMTP (mail from other servers)	0.0.0.0:25	Inbound mail from other servers (MX), STARTTLS available.
`submission`	Submission	0.0.0.0:587	Mail submission from clients, STARTTLS, AUTH required.
`submissions`	Submission over TLS	0.0.0.0:465	Mail submission over implicit TLS.
`pop3`	POP3	0.0.0.0:110	
`pop3s`	POP3 over TLS	0.0.0.0:995	
`imap`	IMAP	0.0.0.0:143	
`imaps`	IMAP over TLS	0.0.0.0:993	
`managesieve`	ManageSieve	0.0.0.0:4190	ManageSieve (RFC 5804): mail apps edit server-side rules here.
`http`	Web (HTTP)	0.0.0.0:80	Web: auto-setup for mail apps; on plain HTTP, sign-ins only from this machine.
`https`	Web (HTTPS)	0.0.0.0:443	Web over TLS: calendars and contacts (CalDAV/CardDAV), auto-setup.

[limits]

Sizes and connection limits that protect the server.

Setting	In the console	Default	What it does
`max_message_bytes`	Largest message (MB)	50 MB	
`max_recipients`	Recipients per message	100	
`idle_timeout_secs`	Disconnect idle clients after (seconds)	300	Seconds a client may stay silent before being disconnected.
`max_bad_commands`	file only	10	Unknown or out-of-order commands allowed before disconnecting.
`max_connections`	Connections in total	2000	
`max_connections_per_ip`	Connections per IP	20	
`tracking_days`	file only	30	Keep the message-tracking log (what happened to each message) this many days.
`big_file_mb`	Biggest file sent as a link from webmail (MB)	1024	Webmail: attachments too big for e-mail are uploaded and sent as a download link. Largest such file (MB).
`big_file_days`	Those download links work for (days)	14	…and how long the link works (days).

Setting	In the console	Default	What it does
`fetch_accounts`	Other accounts each user may collect mail from (POP3)	5	Webmail: other accounts (POP3) each user may collect mail from. 0 = off.
`fetch_allow_local`	...also from servers on this network	off	...and may they collect from servers on this machine's own network (an old mail server in the office)? Off: only servers on the internet.

[security] — sign-in security

Bans, lockouts, country rules and web front ends. In the console: the Security page's Settings.

Setting	In the console	Default	What it does
`require_tls_for_auth`	Passwords only over encrypted connections	on	Refuse passwords over unencrypted connections (loopback is exempt).
`max_auth_failures`	Failed sign-ins before an IP is banned	5	Failed logins from one IP within `failure_window_secs` before it is banned.
`failure_window_secs`	file only	600	
`ban_secs`	Ban length (seconds)	3600	
`allowlist`	Never ban these IPs	(empty)	IPs that are never banned or throttled.
`trusted_proxies`	Web front ends (e.g. IIS)	(empty)	Web front ends (e.g. IIS with Application Request Routing) that pass requests on to this server, e.g. ["127.0.0.1"]. From these addresses only, the visitor's address is taken from X-Forwarded-For and HTTPS from X-Forwarded-Proto, so sign-in limits, bans and "local network only" apply to the real visitor.
`max_user_failures`	Failures (any IPs) before an account is locked	20	Failed logins for one account (from any IPs) within an hour before that account is locked for new locations. Places it signed in from before keep working.
`user_lock_secs`	Account lock length (seconds)	1800	
`attack_ips`	Alert when this many addresses try one mailbox (10 min)	5	Alert when this many different addresses try one real mailbox within 10 minutes (an attack spread over many addresses; 0 = off). Only alerts: bans and locks stay as they are.

Setting	In the console	Default	What it does
`spray_accounts`	Alert when one network tries this many accounts (15 min)	10	Alert when one network (IPv4 /24, IPv6 /48) tries this many different accounts within 15 minutes (password spraying; 0 = off).
`ban_unknown_accounts`	Ban guessing at accounts that don't exist	on	Ban an IP straight away when it tries to sign in with a name that can't exist here (no @domain, or a domain this server doesn't host), and on the second try for a mailbox that doesn't exist on a hosted domain. IPs that have signed in successfully before, and the allowlist, are exempt (a typo there counts as an ordinary failure).
`geoip_db`	Country database (.mmdb)	—	Country database (.mmdb from MaxMind GeoLite2 or DB-IP Lite) for the options below.
`blocked_countries`	Blocked countries	(empty)	Drop connections from these countries (ISO codes like "RU"). Mail servers on port 25 are only blocked if `block_countries_smtp` is on.
`block_countries_smtp`	Also block them for incoming mail (port 25)	off	
`login_countries`	Allow sign-ins only from	(empty)	If not empty, sign-ins are only allowed from these countries.
`security_alerts`	E-mail users about new locations and lockouts	on	E-mail users when they sign in from a country they haven't used before, when their account gets locked, or when someone knows their password but is stopped by two-factor.
`password_rules`	Refuse weak passwords	on	Refuse weak new passwords (too short, very common, containing the name or domain).
`min_password_length`	Shortest password allowed	—	Shortest new password allowed (8–64).
`min_admin_password_length`	…for administrators	—	Shortest new password for administrators (8–64; never below `min_password_length`).
`password_reset`	Let users reset a forgotten password	on	Let users reset a forgotten password through a confirmed backup e-mail address.

[tls] — certificates

Let's Encrypt or your own certificate files.

Setting	In the console	Default	What it does
`cert`	Or: your own certificate file	—	PEM certificate chain. If both paths are empty a self-signed one is generated.
`key`	Its private key file	—	
`acme`	Free certificate from Let's Encrypt	off	Get (and renew) a free certificate from Let's Encrypt for `hostname` plus `acme_names`. Port 80 must be reachable from the internet for the check.
`acme_email`	E-mail for expiry warnings	—	Where Let's Encrypt sends expiry warnings (optional).
`acme_names`	Extra names on the certificate	(empty)	Extra names on the certificate, e.g. autoconfig.example.com.
`acme_staging`	Test mode	off	Use Let's Encrypt's test service (untrusted certificates, generous limits).
`acme_domain_names`	Per-domain names	(empty)	For every hosted domain, also get that domain's own certificate for these names (e.g. ["mail", "webmail", "autodiscover"] → mail.<domain>, ...; "@" = the domain itself). Only names whose DNS points at this server are included.

[outbound] — sending to other domains

Delivery, relays, the send-from address and hacked-account protection. Per-domain relays are [outbound.sender_relays."domain"] with relay, user, password and security.

Setting	In the console	Default	What it does
`enabled`	Deliver mail to other domains	on	Turn off to refuse all mail for remote domains.
`relay`	Relay server (smart host)	—	Send everything through this server ("smart host") instead of looking up MX records, e.g. "smtp.sendgrid.net:587". Useful when your ISP blocks port 25.
`relay_user`	Relay user name	—	
`relay_password`	Relay password	—	
`relay_security`	Relay encryption	starttls	"starttls" (default), "tls" (implicit, port 465) or "none".
`mx_port`	file only	25	Port used when delivering straight to a domain's MX servers.

Setting	In the console	Default	What it does
`source_ip`	Send from address	—	Send from this address of the machine, e.g. "203.0.113.25", when it has several. It should be the one whose reverse DNS (PTR) matches `hostname` and that your SPF records list. Empty = let the system choose. Servers with only an address of the other kind (IPv6 vs IPv4) are skipped, so mail never leaves from an unlisted address.
`routes`	file only	(none)	Per-domain overrides: domain → "host:port". Sent there instead of the MX.
`sender_relays`	file only	(none)	Relays by sender domain: mail from these domains goes through that domain's own relay (e.g. the IONOS mailbox the domain is hosted with) instead of `relay`.
`require_tls`	Only deliver over encrypted connections	off	Refuse to deliver over unencrypted connections.
`max_queue_hours`	Give up after (hours)	120	Give up and bounce after this many hours of failed attempts.
`concurrency`	file only	20	Deliveries running at the same time.
`max_recipients_per_hour`	Recipients per user per hour	500	Recipients one user may send to per hour (stops a hacked account spamming).
`pause_on_limit`	Pause accounts that hit the limit	on	Going over the hourly limit pauses the account's sending (and holds its queued mail) until an admin resumes it, instead of just refusing for the rest of the hour.
`burst_factor`	Pause on sudden bursts (× busiest hour)	10	Also pause when an hour has at least `burst_min` recipients and more than `burst_factor` times the account's busiest hour of the past two weeks. 0 = off.
`burst_min`	…but only from this many recipients an hour	100	
`bounce_pause_min`	Pause accounts whose mail bounces (recipients)	25	Also pause when at least this many of an account's recipients bounced in the last hour and they're half or more of what it sent (spam to made-up or bought address lists bounces a lot). 0 = off.
`mta_sts`	Follow other domains' MTA-STS policies	on	Follow other domains' MTA-STS policies (RFC 8461): to a domain that publishes one in "enforce" mode, mail goes only to its listed servers, over TLS with a valid certificate.
`dane`	Follow other domains' DANE records	on	Follow other domains' DANE (TLSA) records: when a mail server's certificate is published in DNSSEC-signed DNS, deliver only over TLS with that certificate. Needs a DNS server that checks DNSSEC; with one that doesn't, it stays inactive.

Setting	In the console	Default	What it does
`connect_timeout_secs`	file only	30	
`command_timeout_secs`	file only	300	

[spam] — spam and viruses

Filtering of mail arriving from the internet, and the quarantine. In the console: the main switches on the Spam filter page, the quarantine on the Quarantine page, the rest under Settings → Spam and viruses.

Setting	In the console	Default	What it does
`enabled`	Filter mail from the internet	on	
`junk_score`	Junk score	5.0	Score at which mail goes to the recipient's Junk folder.
`reject_score`	Refuse score	15.0	Score at which mail is refused outright.
`check_authentication`	SPF, DKIM, DMARC and reverse-DNS checks	on	SPF, DKIM, DMARC and reverse-DNS checks.
`honor_dmarc_reject`	Refuse mail failing DMARC when its domain asks for that	on	Refuse mail that fails DMARC when the sender's domain asks for p=reject.
`dnsbl`	Blocklists	3 entries	DNS blocklists to look the connecting IP up in.
`dnsbl_reject`	Refuse blocklisted senders outright	off	Refuse listed IPs instead of just adding to the score.
`greylisting`	Greylisting	off	Ask unknown senders to retry later (most spam bots never do).
`greylist_delay_secs`	file only	300	
`blocked_extensions`	Blocked attachment types	33 entries	Attachments refused outright (also catches "invoice.pdf.exe").
`clamav`	ClamAV virus scanner	—	clamd address for virus scanning, e.g. "127.0.0.1:3310". Empty = off.

Setting	In the console	Default	What it does
`clamav_fail_open`	Deliver if the virus scanner is down	on	If clamd is down: true = deliver anyway, false = ask the sender to retry.
`bayes`	Learning filter	on	Per-user learning filter, trained by moving mail into and out of Junk.
`bayes_min_trained`	file only	20	Messages of each kind a user must have trained before the filter votes.
`check_local_connections`	file only	off	Also run DNS-based checks for loopback and private-network clients.
`quarantine`	Quarantine instead of refusing	off	Keep mail that would be refused (spam score, viruses, blocked attachments) in the quarantine, where admins can release it, instead of refusing it.
`quarantine_days`	Keep quarantined mail for (days)	30	Quarantined mail is deleted after this many days.
`quarantine_digest`	Daily held-mail summary for users	on	Once a day, tell each user what was held for them, with a link to deliver it.
`quarantine_digest_hour`	Send the summary at (hour)	8	Hour (0-23, local time) the daily digest goes out.
`arc_seal`	ARC-seal incoming mail	on	Add an ARC seal (RFC 8617) to mail from the internet, signed with a DKIM key of yours: when a user forwards it (to Gmail, say), the receiver can still trust the SPF/DKIM results seen here. Needs a DKIM key on one of your domains.
`external_warning`	Warn about mail from outside	on	Mark mail from outside the organization (webmail shows a banner; a sender using a colleague's name gets a strong warning).
`scan_outgoing`	Check outgoing mail for spam	on	Check mail our users send to other domains with the content rules; refuse what scores as spam (a hacked account) and alert the administrators.

Setting	In the console	Default	What it does
`newsletters`	Newsletters folder	on	Put bulk mail from companies (newsletters, marketing, notifications from mailing services) in a "Newsletters" folder instead of the Inbox. Each user can turn it off.
`external_subject_tag`	Tag the subject of outside mail		Also put this in front of the subject of outside mail, e.g. "[EXTERNAL]", for Outlook and phones. Empty = don't change subjects.
`uri_blocklists`	Link blocklists	dbl.spamhaus.org, multi.surbl.org	Link blocklists: the domains of links in a message are looked up here (Spamhaus DBL, SURBL). Catches spam from new senders that only its links give away.
`uri_points`	Points for a blocklisted link	5.0	Points for a link on one of them.
`require_rdns`	Refuse servers without reverse DNS	off	Refuse mail from servers whose address has no reverse DNS (PTR) name.
`blocked_helo`	Refuse these server names (EHLO)	(empty)	Refuse servers that introduce themselves (EHLO) with these names. `*` matches anything, e.g. `*.dynamic.example.net`, `localhost`.

[admin] — console, backups, alerts and heartbeat

In the console: Settings → This console, and the Settings of the Backups, Alerts, Blocklists and Heartbeat pages.

Setting	In the console	Default	What it does
`allow_remote`	Allow the console from the internet	off	Allow the admin console from the internet, not just this machine and the local network. Admins should then have two-factor turned on.
`allowed_ips`	Admin console only from	—	If not empty, the console (and its API) only answers these addresses or ranges, e.g. ["203.0.113.7", "198.51.100.0/24"]. This machine is always allowed, so a mistake can be fixed on the server itself.
`require_2fa`	Administrators must use two-factor sign-in	—	Administrators must have two-factor sign-in or a passkey to use the console.

Setting	In the console	Default	What it does
`backup_dir`	Backup folder	—	Where "Back up now" and `mailserver backup` put backups (default: data_dir/../backups).
`metrics_token`	Metrics token	—	If set, /metrics also accepts "Authorization: Bearer <token>" from anywhere (otherwise only from this machine and the local network).
`backup_hour`	Back up every day at (hour)	—	Back up every day at this hour (0–23, local time). Not set = no scheduled backups.
`backup_keep`	Backups to keep	7	Every backup (scheduled, "Back up now", before an update) keeps this many of the newest and deletes older ones.
`alerts`	E-mail admins about problems	on	E-mail administrators about failed backups, stuck mail, expiring certificates and paused accounts.
`alert_email`	Also e-mail alerts to	—	Also send alerts to this outside address (so you hear even if this server's mail is down).
`alert_webhook`	Push alerts to your phone	—	And to a phone: an ntfy topic URL (https://ntfy.sh/your-topic) or a Discord, Slack or Teams incoming-webhook URL.
`daily_summary`	Daily summary e-mail	on	E-mail administrators a summary of the last 24 hours every day: what needs attention, mail in and out, sign-ins and attacks, disk, certificate and backups.
`summary_hour`	Send the summary at (hour, 0–23)	7	The hour (0–23, local time) the daily summary goes out.
`disk_min_free_gb`	Low-disk alert below (GB)	2.0	Alert when the mail disk has less than this much free (GB), or under 5%.
`monitor_blocklists`	Blocklists to watch this server on	8 entries	Blocklists this server's own addresses are watched on (Blocklists page).
`blocklist_check_hours`	Check them every (hours)	3	…checked every this many hours.
`heartbeat_urls`	file only	(empty)	Optional: outside monitoring services to call every few minutes (Healthchecks.io, Better Stack, Cronitor…). When the calls stop, they alert you that this server is down.
`heartbeat_minutes`	file only	5	…every this many minutes (1–60).

[archive] — journaling

A copy of every message for compliance and legal holds. In the console: the Archive page's Settings.

Setting	In the console	Default	What it does
`journal`	Keep a copy of all mail	off	Keep a copy of all mail sent and received.
`journal_domains`	Only for these domains	(empty)	Only for these domains (empty = all hosted domains).
`journal_to`	Also send each copy to	—	Also send every copy, wrapped in a journal report, to this address (e.g. an outside archiving service).
`retention_days`	Delete archived mail after (days)	0	Delete archived mail after this many days (0 = keep forever). Mail of accounts on legal hold is never deleted.

[retention] — folder clean-up

Automatic deletion of old mail in chosen folders.

Setting	In the console	Default	What it does
`junk_days`	Empty Junk after (days)	0	Delete mail in Junk after this many days (0 = keep).
`trash_days`	Empty Trash after (days)	0	Delete mail in Trash after this many days (0 = keep).
`folders`	file only	(none)	More folders by name, e.g. { "Newsletters" = 90 }.

[reports] — DMARC/TLS reports and MTA-STS

Reading and sending reports, and your MTA-STS policy. In the console: the Reports page's Settings.

Setting	In the console	Default	What it does
`read_incoming`	Read DMARC and TLS reports that arrive	on	Read DMARC and TLS reports that arrive for your domains (rua=mailto:...) and show them on the Reports page: who sends mail as your domains, and whether it passes.
`send_dmarc`	Send DMARC reports	on	Once a day, send DMARC aggregate reports to the domains whose mail came in and that ask for them (what big providers do).
`send_tls`	Send TLS reports	on	Once a day, send TLS reports (RFC 8460) to domains we delivered to that ask for them.
`org_name`	Name on the reports	—	Name on the reports we send. Empty = your main domain.
`keep_days`	Keep received reports for (days)	180	Keep received reports this many days.
`mta_sts_mode`	Your MTA-STS policy	testing	MTA-STS policy served at https://mta-sts.<domain>/.well-known/mta-sts.txt: "testing" (report problems, deliver anyway), "enforce" (senders must use TLS with a valid certificate) or "off".

Setting	In the console	Default	What it does
`mta_sts_mx`	Other mail servers in the policy	(empty)	Extra mail server names for the policy, besides this server's name (e.g. a backup MX).
`mta_sts_max_age`	file only	604800	How long senders may keep the policy (seconds). Policies must allow at least a day.

[offsite] — off-site backup copies

A copy of every backup on another disk, a network share or S3-compatible storage. In the console: the Backups page's Settings.

Setting	In the console	Default	What it does
`target`	Copy each backup to		"" (off), "folder" or "s3".
`folder`	Folder	—	For "folder": another disk or a network share, e.g. E:\MailBackups or \\nas\backups.
`s3_endpoint`	Storage address		For "s3": the storage address, e.g. https://s3.us-west-004.backblazeb2.com.
`s3_region`	Region		Region, e.g. us-west-004 (us-east-1 if empty).
`s3_bucket`	Bucket		Bucket name. Empty when the address already names it (https://bucket.s3.amazonaws.com).
`s3_prefix`	Folder in the bucket	mailkeep	Folder inside the bucket.
`s3_access_key`	Access key (key ID)		
`s3_secret_key`	Secret key	—	
`passphrase`	Encryption passphrase	—	Encrypts the copies uploaded to S3. Keep it somewhere safe besides this server: without it the copies can't be opened.
`keep`	Copies to keep there	14	Off-site copies to keep (older ones are deleted there).

[directory] — company directory

Which colleagues people see in the company directory.

Setting	In the console	Default	What it does
`scope`	Colleagues people see	domain	"domain" (people see their own domain's mailboxes), "server" (every domain) or "off".

An example settings file

```
hostname = "mail.example.com"
data_dir = "data"
log_file = "logs/mailserver.log"

[tls]
acme = true
acme_email = "it@example.com"

[outbound]
source_ip = "203.0.113.25"

[spam]
clamav = "127.0.0.1:3310"
quarantine = true

[security]
allowlist = ["198.51.100.10"]

[admin]
backup_hour = 3
alert_email = "it-alerts@gmail.com"
alert_webhook = "https://ntfy.sh/example-mail-alerts"

[retention]
junk_days = 30
trash_days = 30
```

CHAPTER 22

Command-line reference

Every mailserver command and its options.

Every command accepts `-c, --config <file>` (default `mailserver.toml` in the current folder) and `-h, --help`. Most commands work while the server is running; `restore` needs it stopped. Commands that change accounts or settings are written to the audit log as *cli*.

mailserver setup

`mailserver setup`

Install, upgrade or remove MailKeep with a wizard in its own window (Windows). Double-clicking mailserver.exe does the same

```
mailserver setup [OPTIONS]
```

`--uninstall`	Remove MailKeep (what Settings → Apps → Uninstall runs)
`--test <TEST>`	Try the wizard without changing the system: files go under this folder, and the service, firewall and Apps entry are only listed
`--no-browser`	Don't open the setup window (print the address instead)

mailserver init

`mailserver init`

Write a default settings file

```
mailserver init [OPTIONS]
```

mailserver serve

`mailserver serve`

Run the server

```
mailserver serve [OPTIONS]
```

mailserver service

Run as a Windows service (install/uninstall need an administrator PowerShell)

`mailserver service install`

Register the service: starts at boot, restarts if it fails, uses this --config

```
mailserver service install [OPTIONS]
```

`mailserver service uninstall`

Stop and remove the service (settings and mail are kept)

```
mailserver service uninstall [OPTIONS]
```

`mailserver service start`

```
mailserver service start [OPTIONS]
```

`mailserver service stop`

```
mailserver service stop [OPTIONS]
```

`mailserver service status`

```
mailserver service status [OPTIONS]
```

---

mailserver release-key

Release signing: only files signed with your release key can be installed from the admin console's Update page

`mailserver release-key new`

Make a new release key (once). Prints the public half for assets/release-key.pub

```
mailserver release-key new [OPTIONS] <FILE>
```

`<FILE>`

`mailserver release-key sign`

Sign a built mailserver.exe for the admin console's Update page

```
mailserver release-key sign [OPTIONS] --key <KEY> --out <OUT> <EXE>
```

`<EXE>`

`--key <KEY>`

`--out <OUT>`

---

mailserver domain

Manage hosted domains

`mailserver domain add`

```
mailserver domain add [OPTIONS] <NAME>
```

`<NAME>`

`mailserver domain remove`

```
mailserver domain remove [OPTIONS] <NAME>
```

`<NAME>`

`mailserver domain list`

```
mailserver domain list [OPTIONS]
```

---

mailserver user

Manage mailbox users

`mailserver user import`

Add many users from a CSV file: address, password, size limit (like 500 or 2 GB). An empty password gets a random one, printed at the end

```
mailserver user import [OPTIONS] <FILE>
```

`<FILE>`	
`--update`	Also change the password and limit of users that already exist
`--dry-run`	Only show what would happen

`mailserver user add`

Add a user. Without --password, the password is read from standard input

```
mailserver user add [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--password <PASSWORD>`	
`--quota-mb <QUOTA_MB>`	Mailbox size limit in megabytes (0 = unlimited) [default: 0]

`mailserver user passwd`

```
mailserver user passwd [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--password <PASSWORD>`	

`mailserver user quota`

```
mailserver user quota [OPTIONS] <ADDRESS> <QUOTA_MB>
```

`<ADDRESS>`	
`<QUOTA_MB>`	

`mailserver user disable`

```
mailserver user disable [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	

`mailserver user enable`

```
mailserver user enable [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	

`mailserver user remove`

```
mailserver user remove [OPTIONS] <ADDRESS>
```

`<ADDRESS>`

`mailserver user list`

```
mailserver user list [OPTIONS]
```

`mailserver user 2fa`

Two-factor authentication (authenticator app codes)

```
mailserver user 2fa [OPTIONS] <COMMAND>
```

`mailserver user 2fa enable`

Start setup: shows a QR code to scan with an authenticator app

```
mailserver user 2fa enable [OPTIONS] <ADDRESS>
```

`<ADDRESS>`

`mailserver user 2fa confirm`

Finish setup with the 6-digit code the app shows

```
mailserver user 2fa confirm [OPTIONS] <ADDRESS> <CODE>
```

`<ADDRESS>`

`<CODE>`

`mailserver user 2fa disable`

```
mailserver user 2fa disable [OPTIONS] <ADDRESS>
```

`<ADDRESS>`

`mailserver user app-password`

Separate passwords for mail apps (needed once two-factor is on)

```
mailserver user app-password [OPTIONS] <COMMAND>
```

`mailserver user app-password add`

Create one (shown once), e.g. `user app-password add bob@example.com "iPhone Mail"`

```
mailserver user app-password add [OPTIONS] <ADDRESS> <NAME>
```

`<ADDRESS>`

`<NAME>`

`mailserver user app-password list`

```
mailserver user app-password list [OPTIONS] <ADDRESS>
```

`<ADDRESS>`

---

mailserver user app-password revoke

```
mailserver user app-password revoke [OPTIONS] <ADDRESS> <NAME>
```

<ADDRESS>

<NAME>

---

mailserver user vacation

Out-of-office auto-reply

```
mailserver user vacation [OPTIONS] <ADDRESS>
```

<ADDRESS>

--message <MESSAGE>	Reply text (use \n for new lines)
--subject <SUBJECT>	[default: "Out of office"]
--days <DAYS>	Reply to the same person at most once per this many days [default: 7]
--off	Turn the auto-reply off

---

mailserver user forward

Forward incoming mail to another address

```
mailserver user forward [OPTIONS] <ADDRESS> [TO]
```

<ADDRESS>

[TO]

--no-copy	Don't keep a copy in this mailbox
--off	

---

mailserver alias

Manage aliases (use @example.com for a catch-all)

mailserver alias add

```
mailserver alias add [OPTIONS] <SOURCE> <TARGET>
```

<SOURCE>

<TARGET>

---

mailserver alias remove

```
mailserver alias remove [OPTIONS] <SOURCE>
```

<SOURCE>

---

mailserver alias list

```
mailserver alias list [OPTIONS]
```

---

mailserver list

Mailing lists: one address that reaches every member

`mailserver list add`

Create a list, e.g. `list add team@example.com --name "Our team"`

```
mailserver list add [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--name <NAME>`	[default: ""]

`mailserver list remove`

Delete a list and its member list

```
mailserver list remove [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	

`mailserver list list`

All lists

```
mailserver list list [OPTIONS]
```

`mailserver list set`

Change a list's settings

```
mailserver list set [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--name <NAME>`	
`--description <DESCRIPTION>`	
`--post <POST>`	members, anyone or moderators (announcement list)
`--subscribe <SUBSCRIBE>`	closed or open (anyone may join, after confirming by e-mail)
`--reply-to <REPLY_TO>`	Where replies go: list or sender
`--prefix <PREFIX>`	Put in front of every subject, e.g. "[team]" ("" = none)
`--footer <FOOTER>`	Added under every message ("" = none)
`--moderation <MODERATION>`	Posts from people who may not post: refuse, hold (for a moderator) or all (hold every post)
`--archive <ARCHIVE>`	Web archive of past posts: members, public or off

`mailserver list digest`

Send a member one digest a day instead of every message (on/off)

```
mailserver list digest [OPTIONS] <LIST> <MEMBER> <ON>
```

`<LIST>`	
`<MEMBER>`	
`<ON>`	

`mailserver list held`

Posts waiting for a moderator

```
mailserver list held [OPTIONS] <LIST>
```

`<LIST>`

`mailserver list approve`

Approve a held post (sends it to the list)

```
mailserver list approve [OPTIONS] <ID>
```

`<ID>`

`mailserver list reject`

Reject a held post (deletes it)

```
mailserver list reject [OPTIONS] <ID>
```

`<ID>`

`mailserver list members`

Show a list's members

```
mailserver list members [OPTIONS] <ADDRESS>
```

`<ADDRESS>`

`mailserver list subscribe`

Add members (any number of addresses)

```
mailserver list subscribe [OPTIONS] <LIST> [MEMBERS]...
```

`<LIST>`

`[MEMBERS]...`

`--moderator`	Make them moderators (they get the list-owner mail and may post to announcement lists)

`mailserver list unsubscribe`

Remove members

```
mailserver list unsubscribe [OPTIONS] <LIST> [MEMBERS]...
```

`<LIST>`

`[MEMBERS]...`

---

mailserver shared

Shared mailboxes (info@, support@) and who may open other people's folders in their mail app

`mailserver shared add`

Create a shared mailbox (nobody signs in to it; give people access instead)

```
mailserver shared add [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--name <NAME>`	[default: ""]

`mailserver shared mark`

Turn an existing mailbox into a shared one (it keeps its mail)

```
mailserver shared mark [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--name <NAME>`	[default: ""]

`mailserver shared list`

Shared mailboxes and who has access

```
mailserver shared list [OPTIONS]
```

`mailserver shared grant`

Let someone into a mailbox: they see it in their mail app under Shared/<mailbox>/

```
mailserver shared grant [OPTIONS] <MAILBOX> <USER>
```

`<MAILBOX>`	The mailbox being opened up
`<USER>`	Who gets access
`--level <LEVEL>`	read, write or full [default: write]
`--folder <FOLDER>`	Only this folder (and its subfolders) instead of all of them [default: ""]
`--send-as`	May also send mail as the mailbox's address

`mailserver shared revoke`

Take someone's access away

```
mailserver shared revoke [OPTIONS] <MAILBOX> <USER>
```

`<MAILBOX>`	
`<USER>`	
`--folder <FOLDER>`	[default: ""]

`mailserver queue`

Outbound mail waiting to be delivered

`mailserver queue list`

```
mailserver queue list [OPTIONS]
```

`mailserver queue retry`

Retry everything now (picked up by the running server within 30 seconds)

```
mailserver queue retry [OPTIONS]
```

`mailserver queue delete`

Drop a message from the queue without delivering or bouncing it

```
mailserver queue delete [OPTIONS] <ID>
```

`<ID>`

---

mailserver dkim

DKIM signing keys for your domains

`mailserver dkim generate`

Create a signing key and print the DNS record to publish

```
mailserver dkim generate [OPTIONS] <DOMAIN>
```

`<DOMAIN>`

`--selector <SELECTOR>`	[default: mail]
`--bits <BITS>`	[default: 2048]

`mailserver dkim show`

Print the DNS record for an existing key

```
mailserver dkim show [OPTIONS] <DOMAIN>
```

`<DOMAIN>`

`mailserver dkim remove`

```
mailserver dkim remove [OPTIONS] <DOMAIN>
```

`<DOMAIN>`

---

mailserver dns

`mailserver dns`

Show the DNS records a domain needs (MX, SPF, DMARC, DKIM)

```
mailserver dns [OPTIONS] <DOMAIN>
```

`<DOMAIN>`

---

mailserver checkup

`mailserver checkup`

Check DNS, reverse DNS, blocklists, certificate and ports for every domain

```
mailserver checkup [OPTIONS]
```

mailserver check-mx

`mailserver check-mx`

Look up a domain's mail servers and test whether this machine can reach them

```
mailserver check-mx [OPTIONS] <DOMAIN>
```

`<DOMAIN>`

mailserver check-relay

`mailserver check-relay`

Sign in to the outgoing relay (or a sender domain's relay) without sending anything

```
mailserver check-relay [OPTIONS]
```

`--domain <DOMAIN>`	Test this sender domain's relay instead of the general one

mailserver spam

Spam filter: allow/block lists, training stats, test a message

`mailserver spam allow`

Always deliver mail from this address or domain to the inbox

```
mailserver spam allow [OPTIONS] <PATTERN>
```

`<PATTERN>`

`--user <USER>`	Only for this user (default: everyone)

`mailserver spam block`

Always send mail from this address or domain to Junk

```
mailserver spam block [OPTIONS] <PATTERN>
```

`<PATTERN>`

`--user <USER>`

mailserver spam remove

Remove an allow/block entry

```
mailserver spam remove [OPTIONS] <PATTERN>
```

`<PATTERN>`	
`--user <USER>`	

---

mailserver spam list

Show allow/block lists

```
mailserver spam list [OPTIONS]
```

---

mailserver spam stats

How much each user's learning filter has been trained

```
mailserver spam stats [OPTIONS]
```

---

mailserver spam check

Run a saved message (.eml) through the filter, including live DNS checks

```
mailserver spam check [OPTIONS] <FILE>
```

`<FILE>`	
`--ip <IP>`	The IP the message came from [default: 192.0.2.1]
`--from <FROM>`	Envelope sender (MAIL FROM). Defaults to the From header
`--helo <HELO>`	[default: unknown]
`--user <USER>`	Apply this user's lists and learning filter too

---

mailserver admin

Who may use the web admin console (/admin/)

mailserver admin add

Let this account use the admin console. With --domain, only for those domains (their users, aliases, lists, shared mailboxes, disclaimers and relays)

```
mailserver admin add [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--domain <DOMAINS>`	Manage only this domain (repeat for more). Without it: everything

---

mailserver admin remove

```
mailserver admin remove [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	

---

mailserver admin list

```
mailserver admin list [OPTIONS]
```

---

mailserver backup

`mailserver backup`

Back up the database, all mail, the certificate and settings (safe while running)

```
mailserver backup [OPTIONS]
```

`--to <TO>`	Folder to put the backup in (default: [admin] backup_dir, or data_dir/../backups)

mailserver restore

`mailserver restore`

Restore a backup folder. Stop the server first

```
mailserver restore [OPTIONS] <FROM>
```

`<FROM>`

mailserver offsite

Off-site backup copies ([offsite] in the settings): list them, bring one back

`mailserver offsite list`

List the copies at the off-site target, newest first

```
mailserver offsite list [OPTIONS]
```

`mailserver offsite test`

Try the off-site settings: write and remove a small file there

```
mailserver offsite test [OPTIONS]
```

`mailserver offsite get`

Bring one copy back as a backup folder for `mailserver restore`

```
mailserver offsite get [OPTIONS] <NAME>
```

`<NAME>`

`--into <INTO>`	Where to put it (default: the current folder) [default: .]

`mailserver offsite unpack`

Unpack a downloaded .mkbk file (e.g. on a new machine whose settings are lost). The passphrase is asked for if not in the settings or MAILKEEP_BACKUP_PASSPHRASE

```
mailserver offsite unpack [OPTIONS] <FILE>
```

`<FILE>`

`--into <INTO>`	[default: .]

mailserver import-mailenable

`mailserver import-mailenable`

Move in from MailEnable: domains, mailboxes with their passwords, addresses, DKIM keys, folders and mail. Safe to run again (only new mail is added)

```
mailserver import-mailenable [OPTIONS] <FROM>
```

`<FROM>`	MailEnable's folder (the one holding Config and Postoffices)
`--dry-run`	Only show what would be imported
`--only <ONLY>`	Only this domain / post office

mailserver import-imap

`mailserver import-imap`

Copy a mailbox from another server over IMAP (folders, flags, dates). Safe to run again: only new mail is copied. With --csv, many mailboxes at once

```
mailserver import-imap [OPTIONS] --host <HOST>
```

`--host <HOST>`	The other server, e.g. imap.oldhost.com
`--port <PORT>`	
`--security <SECURITY>`	tls (port 993), starttls (143) or none [default: tls]
`--insecure`	Accept the other server's certificate even if it isn't trusted (self-signed)
`--user <USER>`	Sign-in name on the other server
`--password <PASSWORD>`	Its password (asked for if left out)
`--to <TO>`	The mailbox here to copy into
`--csv <CSV>`	A file with one mailbox per line: remote user,remote password,local address
`--dry-run`	Only sign in and show the folders

mailserver archive

The archive (journaled mail and legal holds)

`mailserver archive search`

Find archived mail

```
mailserver archive search [OPTIONS] [TEXT]
```

`[TEXT]`	Words in sender, recipients, subject or Message-ID [default: ""]
`--address <ADDRESS>`	Only mail to or from this address
`--since <SINCE>`	From this day (YYYY-MM-DD)
`--until <UNTIL>`	Up to this day (YYYY-MM-DD)
`--export <EXPORT>`	Write the matches to this mbox file instead of listing them

`mailserver archive hold`

Put a mailbox on legal hold: nothing of its mail can be destroyed

```
mailserver archive hold [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	
`--reason <REASON>`	[default: ""]

`mailserver archive release`

Lift a legal hold

```
mailserver archive release [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	

`mailserver archive holds`

Mailboxes on legal hold

```
mailserver archive holds [OPTIONS]
```

---

mailserver sieve

Server-side mail rules (Sieve scripts)

`mailserver sieve put`

Upload a rules script from a file

```
mailserver sieve put [OPTIONS] <ADDRESS> <NAME> <FILE>
```

`<ADDRESS>`	
`<NAME>`	
`<FILE>`	
`--activate`	Make it the script that runs

`mailserver sieve list`

```
mailserver sieve list [OPTIONS] <ADDRESS>
```

`<ADDRESS>`	

`mailserver sieve show`

```
mailserver sieve show [OPTIONS] <ADDRESS> <NAME>
```

`<ADDRESS>`	
`<NAME>`	

`mailserver sieve activate`

Make this the script that runs (only one runs at a time)

```
mailserver sieve activate [OPTIONS] <ADDRESS> <NAME>
```

`<ADDRESS>`

`<NAME>`

`mailserver sieve deactivate`

Turn rules off for this user

```
mailserver sieve deactivate [OPTIONS] <ADDRESS>
```

`<ADDRESS>`

`mailserver sieve delete`

```
mailserver sieve delete [OPTIONS] <ADDRESS> <NAME>
```

`<ADDRESS>`

`<NAME>`

`mailserver sieve check`

Check a script file for mistakes without uploading

```
mailserver sieve check [OPTIONS] <FILE>
```

`<FILE>`

---

mailserver audit

`mailserver audit`

Security log: sign-ins, failures, lockouts, bans and admin changes

```
mailserver audit [OPTIONS]
```

`--user <USER>`	Only this account
`--limit <LIMIT>`	[default: 50]

CHAPTER 23

Troubleshooting and FAQ

Common problems, how to find the cause, and how to fix them.

Where to look first

1. **Overview → Server health**: is every service green?
2. **Live log**: errors appear as they happen. Reproduce the problem and watch.
3. **Setup check**: DNS, reverse DNS, certificate and port problems, each with a fix.
4. **Security → Audit log**: sign-in failures, bans and lockouts for the user.
5. **Outgoing queue**: the last error for mail that hasn't been delivered.
6. **Message tracking**: every step of a particular message, and why it was refused or bounced.

Receiving mail

Problem	Likely cause and fix
No mail arrives from outside	Check the MX record points at the server name, the server name's A record at the server, and that port 25 is open in the firewall and forwarded by the router. `mailserver check-mx yourdomain.com` from another network shows whether it's reachable.
Mail for one address is refused ("no such user")	The mailbox or alias doesn't exist, or the account is disabled. Check Users and Aliases.
Wanted mail lands in Junk	Look at its `X-Spam-Status` header to see which rules fired. Move it out of Junk (this trains the filter), or add the sender to the allow list.
A message never arrived	Search Message tracking for the sender's address: it shows whether the message was refused at the door (unknown address, blocklist, DMARC reject) and why, greylisted, held in the quarantine, or delivered (to which folder). Nothing at all means it never reached this server: ask the sender for their bounce message.
"Mailbox full"	The mailbox reached its limit. Raise it under Users → ⋯ → Change quota, or ask the user to empty Trash, or to turn on auto-archive.
Setup check: "MX … not this server" while mail does arrive	The domain's MX uses its own name (such as `mail.customer.com`) that points to this server's address. Mail works; check with `nslookup mail.customer.com` that the address is this server's. Note that an MX lookup must be done on the **domain** (`customer.com`), not on the mail server's name.
Setup check: "MTA-STS … the policy can't be fetched"	The `_mta-sts` TXT record is published but `https://mta-sts.<domain>/.well-known/mta-sts.txt` doesn't answer. Point `mta-sts.<domain>` at this server, add `mta-sts` to the per-domain certificate names, make sure MailKeep answers on port 443 (chapter 4), or remove the TXT record.

Sending mail

Problem	Likely cause and fix
An alert says mail to Gmail, Yahoo or another provider "isn't authenticated"	Its DKIM signature was missing or failing and SPF didn't pass. The alert lists the Setup check results: publish the DKIM record exactly as shown (Domains page → DNS records) and make sure SPF includes this server. It clears itself once mail is accepted again.
Mail to Gmail or Outlook bounces or lands in spam	Run the Setup check: reverse DNS must match the server name, and SPF, DKIM and DMARC must be published. Check the server's address isn't on a blocklist. On a server with several addresses, set the send-from address.
Mail stays in the queue: "connect timed out"	Your provider blocks outgoing port 25. Check with `mailserver check-mx gmail.com`, and use a relay (chapter 12).
"You are not allowed to send as …"	The From address isn't the user's own address, one of their aliases, or a shared mailbox they have "send as" on.
A user can't send at all; Users shows "sending paused"	The account went over its limit or sent a sudden burst, possibly because it's been hacked. Change the password, then resume under Security.
"This message looks like spam, so it wasn't sent"	The outgoing spam check refused it, and the administrators got an alert. If the user didn't write it, the account is probably hacked: change the password and check Security for recent sign-ins. If it's a genuine message, rephrase it or turn off *Check outgoing mail for spam*.
The queue has items tagged *bounce* to strange domains (often .shop, .top and the like)	Items with an empty sender are sent by the server itself. A subject starting *Report Domain:* is a daily DMARC or TLS report to a domain that asked for one; spam domains often do, and their servers rarely answer. They're harmless: delete them, or turn off *Send DMARC reports* on the Reports page. Real bounces to spam senders are no longer sent (chapter 12).
A sender says their mail to a full mailbox was refused	Mailboxes over their quota refuse new mail with *552 mailbox full*, so the sender's own server tells them. Raise the quota (Users → ⋯ → Quota) or ask the user to clear out mail.
A relay refuses the sender	Relays such as IONOS only accept senders of their own contract. Use a mailbox of the same domain as the relay user. `mailserver check-relay` tests it.

Signing in

Problem	Likely cause and fix
Mail app: "authentication failed" after two-factor was turned on	Mail apps need an app password (webmail → Settings → App passwords), or the password followed by the current 6-digit code.
Nobody from one office can sign in	The office's address may be banned after repeated failures, for example one phone with an old password, or a new device trying a mistyped address twice before anyone there had signed in. Unban it under Security, and add it to *Never ban these IPs*.
"Use https:// to sign in"	Passwords are only accepted over encrypted connections. Use https, or the TLS ports. Behind IIS, IIS must send `X-Forwarded-Proto: https`.

Problem	Likely cause and fix
The admin console says "only available from the local network"	Use it from the server or the local network, or turn on *Allow the console from the internet* (with two-factor sign-in).
The admin console says "isn't available from your address"	Your address isn't on *Admin console only from*. Sign in on the server itself (Remote Desktop, `http://localhost/admin/`) and add your new address or range.
The console says administrators need two-factor sign-in or a passkey	*Administrators must use two-factor sign-in* is on. Open webmail, go to **⚙ Settings → Security**, turn on two-factor or add a passkey, then sign in to the console again.
"The password must be at least N characters"	The server's minimum (higher for administrators). Choose a longer one; a few unrelated words work well.
A user's account is locked	Too many failed sign-ins. Devices they used before still work; it unlocks by itself after 30 minutes, or use Security → Unlock.
Webmail says "This is the sign-in page for … Sign in at … instead"	The page was opened on another domain's address. Use the link, or sign in on your own domain's address or the server's own name (chapter 6).
The audit log shows failed sign-ins to an account that doesn't exist, from changing addresses	Someone is working through a list of addresses, often through a VPN. Nothing to do: there's no mailbox to get into, and each address is banned after its second guess at a mailbox that doesn't exist (straight away for a domain that isn't hosted here). Addresses that have signed in before are exempt, so a user's typo doesn't lock them out.
Hundreds of failed sign-ins, but nobody's password was tried	Look at the kinds (Security page card, daily summary): *refused by the country rule* and *no such account* never test a real password. Only *wrong password* and *stopped by two-factor* do; the second means the password is known, so change it.
The Network row in the IP panel says "unavailable"	The registry didn't answer, or an antivirus on the server re-signs HTTPS so the answer can't be trusted. Nothing else depends on it; it is asked again the next time you open the panel.
An alert says many addresses tried one mailbox	Nothing is broken: the addresses are banned as they go and the user keeps working from known places. Make sure the password is strong and two-factor sign-in is on, and turn off services the user doesn't need.
An address can't connect at all, not even to webmail	It's on **Security → Blocked IP addresses**, or in a blocked range. Unblock it there.

The server

Problem	Likely cause and fix
The server won't start: "Only one usage of each socket address"	Another program, or an older MailKeep still shutting down, holds a port. Wait for it to stop, or move the port in the settings. `netstat -ano | findstr :25` shows who holds port 25.
Browsers and mail apps warn about the certificate	The server is using its self-signed certificate. Turn on Let's Encrypt (port 80 must reach the server from the internet), or set your own certificate files.

Problem	Likely cause and fix
Let's Encrypt fails	Port 80 isn't reachable from the internet, or the server name doesn't point at this server. Use Test mode while fixing it, to stay within Let's Encrypt's limits.
Settings changes have no effect	Most settings need a restart: the banner under the top bar (on every page, however far you scroll) offers *Restart now*, or use the power button in the top bar, which shows an orange dot while a restart is waiting.
The backup folder fills up with old backups	*Backups to keep* on the Backups page sets how many stay; older ones are deleted after every backup. To remove one now, press *Delete* on its row.
Ports 80 and 443 stay taken after moving IIS to one address	HTTP.sys still listens on every address. Run `netsh http add iplisten ipaddress=<IIS address>` and restart the machine (chapter 4). If `net stop http` hangs, a reboot is the clean way.
"The virus scanner isn't answering", or the test says it didn't answer	Check `Get-Service clamd, freshclam`: both should be Running and Automatic; `net start clamd` starts it. After a reboot clamd needs a minute or so to load its signatures; the alert resolves itself once it answers.
ClamAV: "The specified executable is not a valid application for this OS platform"	The ARM64 version of ClamAV was installed on an x64 server. Uninstall it and install the **x64** .msi.
The off-site copy card stays "off" after setting up Backblaze	*Copy each backup to* is still *Nowhere*, or the server wasn't restarted after saving. Set it to S3-compatible storage, save, restart, then Back up now; the message should end with "copying it off-site now".
Shared folders don't show in a mail app	Refresh the folder list, or choose "show all folders" / subscriptions. In webmail, reload the page after access was given.
The Update page refuses the file	"Isn't a signed MailKeep release": use the `MailKeep-Setup-….exe` built and signed for you, not a renamed copy. "The signature doesn't match": the file was changed after signing, or signed with a different release key. Either way, the installer still works.

Frequently asked questions

Does MailKeep support Exchange ActiveSync?

No. ActiveSync is a Microsoft protocol covered by Microsoft patents and licensing. Phones use IMAP with push for mail, and CalDAV/CardDAV for calendars and contacts: iPhones support both built in (install the setup profile, chapter 20), and on Android the DAVx[5] app adds calendars and contacts. Classic Outlook syncs calendars with a CalDAV add-on.

How many users can it handle?

Thousands of mailboxes on ordinary hardware. The limits are disk space and, for very busy servers, disk speed.

Can I run it next to my old mail server?

Yes: on a second IP address with the normal ports, or on spare ports (chapter 19).

Where are my users' messages?

One `.eml` file per message under `data/mail/`, indexed in `data/mailserver.db`. Always back up and restore with `mailserver backup` / `restore` rather than copying files by hand.

Is my mail encrypted?

Every connection offers encryption, and passwords are only accepted over encrypted connections. Mail to other servers is encrypted whenever they support it, which nearly all do; *Only deliver over encrypted connections* makes it mandatory.

Glossary

MX record	DNS record saying which server receives a domain's mail.
PTR / reverse DNS	The name an IP address resolves to. Must match the server name.
SPF	DNS record listing which servers may send a domain's mail.
DKIM	A signature on each message proving it came from the domain unchanged.
DMARC	A domain's policy for mail that fails SPF and DKIM, plus where to send reports.
IMAP / POP3	Protocols for reading mail: IMAP keeps it on the server, POP3 downloads it.
SMTP / submission	The protocol for sending mail; submission (587/465) is the signed-in kind for mail apps.
STARTTLS / TLS	Encryption: STARTTLS upgrades a plain connection, TLS is encrypted from the start.
Relay / smart host	Another mail server that sends your mail on for you.
Sieve	The standard language for server-side mail rules.
CalDAV / CardDAV	Standards for syncing calendars and contacts.
JMAP	A modern protocol for mail apps, using the web.
ACL	Access control list: who may do what with a mailbox's folders.
Journaling	Keeping a copy of every message for compliance.
Legal hold	Preserving all of a mailbox's mail so nothing can be destroyed.