ZephyrAB User Manual

ZephyrAB 0.1.0 (preview) · September 2026

Table of contents

1. About this manual

This manual is for people who have a mailbox on a ZephyrAB server. It covers the web client (webmail), the calendar, and how to connect ordinary mail apps on your phone or computer. You do not need any technical background to use it.

ZephyrAB 0.1.0 (preview) · September 2026

A few things to know before you start:

- ZephyrAB is run by an operator — the person or team who set up your server. Some features described here can be switched off by the operator. Where that is the case, this manual says "if your server has this enabled". If a panel or button described here is missing, your server most likely does not offer that feature.
- Your address in this manual is written as `ada@example.com` and your server as `mail.example.com`. Substitute your own.

- If you run the server, read the Admin Manual at `/manual-admin.html`. If you write software against the server, read the API Manual at `/manual-api.html`.

2. Create your account

You need an **invite code**. ZephyrAB servers do not have open registration: an administrator creates a code and gives it to you. If you do not have one, ask your administrator.

On the sign-in page, choose **Create an account**. The form asks for:

Field	What to enter
Invite code	The code your administrator gave you.
Choose your address	Just the name — the part before the @. The invite decides the domain.
Display name	Optional. The name shown on mail you send.
Recovery address	Optional, strongly advised. A different mailbox you can read.
Password and **Confirm password**	At least 12 characters.

Choosing your address

Type only the part before the @. If your invite is for `example.com` and you type `ada`, your address becomes `ada@example.com`. The rules, exactly as the form states them: letters, digits, dot, dash or underscore; 1–64 characters; must start and end with a letter or digit. Two dots in a row are not allowed. If you type an @ sign, the form stops you and explains.

The password rule

There is exactly one rule, and the form says so in as many words:

> At least 12 characters — and that is the ONLY rule. Uppercase, digits and symbols are welcome but not required; length is what makes a password strong, so a few random words work well.

As you type, a live counter shows your length against the minimum and whether the two password fields match.

The recovery address, and why it matters more than it looks

A recovery address is a *different* mailbox you can read — for example, an account you hold somewhere else. It is the only way to reset a forgotten password.

Here is the hard truth, stated up front because it cannot be fixed later: **without a confirmed recovery address, a forgotten password is permanent.** Nobody can get you

back in — not you, not the operator. The server never stores your password, only a mathematical fingerprint (a hash) of it, and a hash cannot be turned back into the password. If you forget it and have no confirmed recovery address, the account's mail is out of reach until an administrator sets a brand-new password for you — and even they cannot read the old one or any mail you encrypted.

Because the recovery address is that important, the server checks it is real before accepting it:

1. It checks the domain actually runs a mail service — it looks up the domain's mail server records and briefly connects to make sure something answers. A web-only domain, or a typo, is refused on the spot with a reason (for example: "that domain does not publish a mail server (no MX record), so a confirmation message could never arrive").
2. It then mails a **confirmation link** to that address. The link works once and expires 30 minutes after it was sent. Until you open it, the address is stored but **cannot** reset your password. You can see whether it is confirmed at any time under **Settings** (see section 14).

A refused recovery address does not cost you your invite — fix the address and submit again.

Common signup errors and what they mean

Message	What it means
"that invite code is not valid"	The code is unknown, expired, or already used up. All three read the same on purpose. Ask your administrator for a fresh one.
"that address is not available"	Someone already has it, or the name is reserved (names like `postmaster` belong to the server). Both read the same on purpose. Pick another name. Your invite is given back.
"password must be at least 12 characters"	Make it longer. Length is the only requirement.
"Address: type just the name part, before the @ …"	You typed a full address. Enter only the part before the @.
An error naming the recovery address	The domain you gave cannot receive mail, or could not be checked right now. The wording tells you which: "try again" means a temporary problem; "please use an address you can receive mail at" means the domain has no mail service.

When the account is created you are signed straight in. If a recovery address was given, open the confirmation link in that other mailbox within 30 minutes.

3. Sign in

Go to the webmail page your operator gave you (usually `https://mail.example.com/mail`). Enter your **Email address** and **Password**, then press **Sign in**.

If two-factor authentication is on for your account, a third field appears: **Code from your authenticator app**. Type the six-digit code from your phone. If you lost your phone, type one of your recovery codes instead (see section 14).

If your organisation signs you in (single sign-on)

Some organisations connect this mailbox to the account you already sign in with everywhere else — a company or government login. If yours does, three things follow, and none of them is a fault:

- **You may have no separate mailbox password at all**, and that is the point. The whole reason for connecting the two is that this server stops being another place a password of yours is kept. If you were never given a mailbox password, you were not forgotten.
- **You sign in through your organisation's system, in the app or portal they gave you.** The webmail page here asks for an address and a password and has no "sign in with…" button — so if you have no mailbox password, this page is not your way in. Ask whoever set up your account which app to use.
- **Your organisation's own security rules apply, and this server does not add a second set.** If they ask you for a code or a security key, that happens at their sign-in. This server does not then ask for its own second factor as well — you would have no way to answer it, and being asked twice for the same thing protects nobody.

If your organisation's sign-in is down, so is your way in — there is nothing to fall back to unless somebody set one up for you in advance. That is worth asking about before you need it.

The recovery warning

If your account has no working way to reset its password, a dialog appears right after sign-in: **"Your password cannot be reset"**. It appears in two situations, with different wording:

- You have never set a recovery address at all.
- You set one, but never opened the confirmation link — so it cannot be used yet.

Press **Set one up now** to go straight to the setting. Press **Not now** (or Escape) to dismiss it; it then stays quiet for 7 days on this browser before asking again. Fixing it takes a minute and is worth doing — see section 2 for why.

Language and text direction

A language picker sits in the top corner of the page, outside every panel, so you can switch language before signing in. The interface supports right-to-left languages: choosing one flips the whole layout, not just the text. Your language choice is remembered on this browser.

Reloading signs you out — on purpose

The sign-in card says it plainly:

> Your password is kept in memory for this tab only — never in browser storage, and never in a cookie. Reloading signs you out.

This is a deliberate safety choice, not a bug. If the password were saved in the browser, any malicious script that ever ran on the page could read it. Instead it lives only in the tab's memory, which vanishes when the tab reloads or closes. Behind the scenes the page exchanges your password for a temporary session credential that lasts up to 12 hours, so your actual password is sent only once per sign-in.

Forgot your password?

Press **Forgot your password?** on the sign-in card, enter your address, and press **Send reset link**. Whatever you type, the answer is the same:

> If that address has a verified recovery address on file, a reset link is on its way. It expires in 30 minutes.

The page cannot tell you more than that, on purpose — a page that said "no such account" would let strangers test which addresses exist. If your recovery address is confirmed, the link arrives there; opening it shows **Choose a new password**. The link works once and expires 30 minutes after it was sent. If you never confirmed a recovery address, no link can arrive — see section 20 for what to do then.

4. Read your mail

After sign-in you see three panes: your folders on one side, the message list in the middle, and the reading pane. On a phone, the panes stack and you move between them.

Folders

Every account gets these folders automatically: **Inbox, Archive, Drafts, Junk, Sent, Trash**. You do not create them and cannot delete them — your mail apps rely on them. Any folders you make yourself (section 9) appear alongside. A number next to a folder shows how many unread messages it holds.

Reading

Click a message to open it. Unread messages show in bold with a dot; opening one marks it read. To reverse that, open it and press **Mark unread**. To clear a whole folder's unread state at once, press **Mark all read** in the bar above the list.

Flag marks a message as needing your attention; the button then reads **Unflag** and takes the mark off again. The flag lives on the server rather than in this browser, so it is the same mark your other mail apps call a flag or a star — set it here and it shows there, and the other way round. Nothing on the server acts on a flag; it is a note to yourself.

If a message is part of a longer exchange, a **Conversation** section appears under it listing the other messages in the same thread — click any of them to jump there.

Moving through a long folder

The list shows **40 messages at a time**. Above it, a counter reads something like "1–40 of 137", and the ← and → buttons beside it move a page back and forward; they grey out at the two ends. The counter is the whole folder, so it also answers "how much is in here?" without opening anything.

Paging is not the same as searching. If you are looking for one message, the search box (section 8) covers the entire account in one go and is almost always quicker than walking pages.

Refresh

Refresh in the header reloads the current folder and the folder list. You should rarely need it — new mail appears on its own (see the push badge below) — but it is the thing to press if you have just made a change in another mail app, or on another device, and want to see it here immediately.

Formatted messages, and switching to plain text

Messages that were sent as HTML are shown formatted — headings, bold, links, tables, colours. Above the message you get a switch:

> **Formatted | Plain text**

Formatted is the default when the sender provided HTML. **Plain text** shows the plain version instead, and is worth a click whenever a message looks odd or you simply want it out of the way. If the sender provided *only* HTML, the plain-text view is made by stripping the formatting out, and a banner says so.

A message's formatting cannot reach the rest of the page. It is shown inside a sealed box that has no ability to run code, no access to your mailbox, and no access to the page around it. Whatever the sender wrote, it can only draw inside that box.

Very large bodies are cut off with a banner ("Body truncated by the server at 300 KB").

Pictures from the internet are blocked until you ask

Most formatted mail pulls its pictures from the sender's website rather than including them. Loading one tells the sender you opened the message, and roughly when. So they are blocked, and you get a line saying so:

> Images from the internet are blocked. Loading them tells the sender you opened this message. **Show images**

Click **Show images** and that message loads them. The choice is for **that message only** — open the next one and pictures are blocked again. There is no setting to turn them on for everything, on purpose: "I trust this sender" is a decision about one message from one sender, not about all mail forever.

Pictures the sender *attached* to the message are different — they are already on the server, they tell the sender nothing, and they are shown straight away.

Attachments on received mail

Files attached to a message appear as labelled chips under it, each with its name and size. Click one to download it. Downloads are always saved as files rather than opened in the page.

Storage

If your account has a storage limit, **Settings** shows a **Storage** panel: "Using 3.2 MB of 2 GB (0%)", with a bar. If no panel appears, your account has no hard limit.

Keyboard

With the list focused: `j` and `k` move down and up through messages, `c` opens a new message, `u` returns to the list on a phone layout. All lists and buttons can be reached with Tab and Enter.

The push badge

A small badge in the header reads either `live` or `poll`. `live` means the server tells the page the moment mail arrives; `poll` means the page checks on a timer instead. Both keep the list current — `poll` is just a little slower. Which one you get depends on your browser; it is nothing you need to act on.

5. Write and send

Press **Compose** in the header. The form has **To**, **Cc**, **Subject** and **Message**. Separate several recipients with commas.

The webmail composer has no Bcc field yet. If you need Bcc, use a connected mail app (section 17) — the server supports it; this client just does not offer the field. A blind copy

stays blind: the server removes the Bcc line before the message goes anywhere, so no recipient sees who else was on it.

- **Reply** answers the sender.
- **Reply all** answers the sender and everyone on the To and Cc lines.
- **Forward** passes the message on — and a forward carries the original's attachments, its HTML version and its inline images, so the recipient sees what you saw. Your own note is added as plain text above it.

Press **Send**. When it succeeds you briefly see "Sent" and the panel closes. A copy of every message you send is filed into your **Sent** folder automatically.

If Send is refused, the message stays in the composer and the reason is shown next to the button — nothing is half-sent. Two refusals worth knowing about are covered in the next two sections: an attachment still uploading, and a link password pasted into the message.

Addresses you send from

The webmail always sends from your primary address. If your administrator has given your account extra addresses (aliases), mail sent *to* any of them lands in this same mailbox. Connected mail apps can also send *from* an alias — the server allows sending only from addresses your account actually owns, so nobody can put your name on mail from another account, and you cannot accidentally send as someone else.

6. Attach files

In the composer, the **Attachments** box is where files join the message. Under **Files to attach**, choose one or more files.

Files upload when you choose them, not when you press Send. The hint under the field says why: "Files are uploaded as soon as you choose them, so this server can accept or refuse them before you send." A refused file is named immediately, while you are still looking at the form — instead of surfacing later as a mysterious "your message could not be sent".

What a refusal looks like, by example:

- Too big for one upload: "*report.zip* is over this server's limit for one upload, which is 40 MB. Send it as a link instead."
- The files together are too much for one message: "Those files come to more than one message can carry on this server, which is 100 MB. Attach fewer, or send one as a link."
- Too many files: "This server allows at most *N* attachments in one message."
- An empty file: "*notes.txt* is empty, so there is nothing to attach."

The exact limits belong to your server; the message always names the one that applied.

Each attached file appears in a list with its size and a **Remove** button. Remove takes it out of *this message*; the copy already uploaded to the server expires on its own, so there is nothing else to clean up.

If you press **Send** while an upload is still running, the send is refused: "Still uploading. Wait for it to finish, or the file will not be in the message." That protects you from sending a message whose attachment silently never made it in.

Attaching a file vs. sharing it as a link

These are two different things, and the composer offers both:

- An **attachment** travels inside the message. The recipient keeps it forever, but receiving servers set limits — many refuse anything much over 25 MB, whatever your own server allows.
- A **link** (next section) uploads the file to your account's storage and puts a download URL in the message text. There is no attachment at all; the recipient downloads the file from your server, and the link expires.

For anything large, the link is usually the answer that actually arrives.

7. Share large files as links

The composer's second box is **Share a large file as a link**. Its own explainer is worth repeating, because the distinction is the whole feature:

> This does not attach a file to the message — use Attachments above for that. The file is uploaded to your account and a download link to it is inserted into the message body. Anyone holding the link can download the file until it expires.

Choose a file under **File to share**, optionally open **Link options**, then press **Create link and insert**. The link and a short description are inserted into your message text, where you can move or reword them like any other text. **Remove file** clears the chosen file.

Link options

All three are optional. The hint says: "Leave blank to use this server's own setting. A value it does not allow is refused outright, not quietly reduced."

Option	Meaning
Expires after (days)	How long the link works. If you leave it blank, the server's own setting applies (30 days unless your operator changed it).
Maximum downloads	After this many downloads the link stops working. Blank means the server's setting; on most servers that is unlimited.
Password	The recipient must type this to download.

At least 8 characters.

The server reports what it actually applied

After the link is created, a short list titled **"What the server actually applied"** appears: the real expiry date, the real download limit, and whether a password is required. This can differ from what you asked for — servers set their own bounds, and if a value you asked for is outside them, the request is refused with the reason rather than silently adjusted. If anything differs, the box says so plainly: "The server did not apply everything you asked for. What it did apply is listed above, and that is what the message now says." Read it before you send; it is what your recipient will experience.

The link password never travels with the link

The warning next to the password field is a rule, not advice:

> The password is never put in this message — not in the body, not in the subject, not in a header. Give it to the recipient another way, by phone or another app. A password that travels with its link protects nothing.

The client enforces it: if the password appears anywhere in your subject or body — because you pasted it under the link, say — **the send is refused**, with the message "Not sent: the link password is in the message. Take it out — a password that travels with its link protects nothing." This is on purpose. A link and its password in the same email protect against exactly nothing: anyone who has the message has both.

If you choose a file and forget to create the link

Pressing Send with a chosen-but-unlinked file stops you once: "You chose a file but no link was created for it, so nothing from that file is in this message. Create the link, remove the file, or press Send again to send the message without it." Pressing Send a second time sends the message without the file.

What the recipient sees

The recipient gets an ordinary message with a download URL in the text (plus the file's name, size, the expiry, and — if you set one — a line saying a password is needed and arrives separately). Opening the link downloads the file directly; if a password is set, a small page asks for it first. A wrong password is told it is wrong; the link is not damaged by wrong guesses. The download is always delivered as a file to save, never rendered in the browser — that is a safety property of the download site.

Once the link expires, is used up, or is withdrawn, the recipient sees a "gone" page. All three cases look identical from the outside, deliberately. When someone tries an expired link, the server lets you — the sender — know once by mail, so a late request does not go unnoticed.

There is currently no way to create a share link outside the composer, and the webmail has no button to withdraw one; if a link must die early, ask your operator, who can revoke it

immediately (revocation takes effect on the very next request). The account API also offers self-service revocation — see the API Manual.

8. Find a message

The search field above the message list reads **"Search this account…"**. Type and press Enter. A search covers your whole account, not just the open folder; the **×** button clears it and returns to the folder view.

Search matches words, not fragments

The search engine works on *words* and their close forms:

- `invoice` finds messages containing "invoice", "invoices" or "invoicing" — related word forms count as the same word.
- `reunion` finds "réunion" — accents do not get in the way.
- Searching works for Chinese and Japanese text too.
- `nvoice` finds **nothing**. A fragment from the middle of a word is not a word, and the index has no entry for it. If a search comes back empty, try the whole word.

Several words together mean **those words, next to each other, in that order**. Searching `quarterly report` finds messages that say "quarterly report"; it does not find a message that merely contains "quarterly" in one paragraph and "report" in another.

Searching by sender or subject

The webmail's one search box looks at the whole message. Mail apps and the API can also search specifically by sender, recipient or subject — those searches match exactly the text you type, anywhere in the field, so `ada@` matches every message from that address.

Encrypted mailboxes cannot search message text

If you have turned on mailbox encryption (section 15), searching *inside message bodies* stops working — searching means reading, and the server can no longer read your mail. Searches by subject, sender and recipient still work, because message headers stay readable. A body search on an encrypted mailbox is refused with a clear answer rather than quietly returning nothing.

9. Organize with folders

Create, rename, delete

At the bottom of the folder pane sit three buttons: **New folder**, **Rename** and **Delete**. Rename and Delete act on the folder you currently have selected.

- **New folder** asks for a name and confirms: "It will appear in your folder list on every device." Folders live on the server, so every connected app sees them.
- **Rename** moves the messages with the folder: "The messages in it move with it, and any device that has this folder open will see it change name."
- **Delete** is the one to read carefully. Deleting an empty folder costs nothing ("It is empty, so nothing goes with it."). Deleting a folder that holds mail **deletes that mail** — this is not a move to Trash — and the confirmation says exactly how much: "It is NOT empty. Messages it holds: 12. Deleting the folder deletes them for good — this is not a move to Trash." If your server keeps recently-deleted copies, those messages can still be put back for the recovery window (section 10). A folder with folders inside it is refused: delete or move the children first.

The standard folders (Inbox, Archive, Drafts, Junk, Sent, Trash) cannot be renamed or deleted: "Inbox is one of the folders your mail apps rely on, so it cannot be renamed or deleted here."

The webmail creates folders at the top level only. Folders-inside-folders made in another mail app are displayed here, indented, but cannot be created here — use a connected app for that.

Move messages

With a message open, the **Move to…** selector in the reader files it into any folder. **Archive** and **Delete** are shortcuts for the two commonest moves.

Select several at once

Each row in the message list has a checkbox, and **Select all** at the top selects the whole page. With a selection made, the bar shows "Selected: 4" and switches to bulk actions: a **Move to…** folder picker, **Mark read**, and **Delete**. Bulk delete follows the same rule as single delete: it moves to Trash, except in Trash and Junk where it becomes **Delete for good** (section 10). If some of a bulk action fails, the result is honest: "3 of 4 done. The first refusal was: …".

Plus-addressing: infinite variations on your address

Your address accepts a suffix after a plus sign: mail to `ada+shopping@example.com` is delivered to `ada@example.com`. You can invent these on the spot — give `ada+newsletter@example.com` to a mailing list and `ada+shop@example.com` to a shop — nothing needs to be set up first.

Two things make this useful:

- You can see at a glance who leaked or sold your address, because the suffix tells you who you gave it to.
- You can sort with filters: a Sieve filter (section 19) can test the suffix and file `+newsletter` mail straight into a folder.

The suffix works when receiving from anywhere, including other mail systems, and in every mail app, because it is handled by the server. Your operator can switch plus-addressing off; on most servers it is on.

10. Delete and recover

Delete means "move to Trash" — almost everywhere

The **Delete** button on a message, and the bulk **Delete**, move the message to Trash. That is recoverable: open Trash and move it back.

The exception is Trash and Junk themselves. A message that is already in Trash or Junk gets a **Delete for good** button instead, in warning colours, and the confirmation says what "for good" means *on this server*. There are three possible answers, and the dialog always states the one that applies:

- "Deleted mail can be put back from Settings for 7 days after that." — your server keeps a recovery copy for a while (the number is the server's own setting, not a fixed promise).
- "This deployment keeps no copy, so it cannot be undone." — gone means gone.
- "Whether a copy is kept could not be read, so treat this as permanent." — the page could not find out, and refuses to guess reassuringly.

Empty Trash, Empty Junk

Inside Trash the list bar offers **Empty Trash** (inside Junk, **Empty Junk**). The confirmation counts first: "Messages in Trash: 138. Every one of them will be removed from the server." — so someone who has not opened Trash in a year finds out here, not afterwards. Very large folders may take more than one pass; the page tells you: "Removed: 500. Still there: 121 — do it again to continue."

Recently deleted — putting a message back

If your server keeps recovery copies, **Settings** has a **Recently deleted** panel:

> A message you delete for good can be put back for 7 days. Ordinary deletions go to Trash and your mail app puts those back itself.

Each entry names the folder it was deleted from and when, with a **Put back** button. Put back returns the message to the folder it came from.

The panel shows the most recent deletions rather than every one. If there are more than fit, it says so underneath — "Only the most recent are listed." — so a message you deleted a few days ago may not be on screen even though it is still inside the recovery window. If you cannot see what you are looking for, ask your operator before the window runs out.

Two more details worth knowing:

- **The folder is recreated if needed.** If you deleted a whole folder and want one message from it back, putting it back re-creates the folder and files the message into it — your filing survives.
- **A restored message arrives as new.** It gets a new position in the folder, so mail apps see it as a fresh arrival; and it stands alone rather than rejoining its old conversation immediately.

The recovery window is the server's, and the panel states the real number. This also covers deletions made from mail apps — an app that "compacts" or expunges a folder produces the same recovery records. Nothing is recoverable from before the feature was switched on, and once the window passes, recovery needs an operator and a backup.

11. Deal with spam

Report spam, Not spam

With a message open, press **Report spam**. The message moves to Junk, and — just as important — the report **trains the server's filter**: you have shown it one more example of what spam looks like for your organisation. If a good message ends up in Junk, open it there and press **Not spam**: it moves back to your Inbox and the filter learns from that too. Correcting a mistake actually does double work — it takes back the wrong label *and* records the right one.

Moving messages **into or out of Junk in any mail app does the same thing** — the training is triggered by the move, whichever app makes it. (Deleting a message out of Junk to Trash trains nothing: throwing something away is not the same as saying it was wanted.)

Why a new server's filter may do nothing yet

The filter learns only from what people mark. Until it has seen enough examples of **both** spam **and** normal mail — dozens of each — it refuses to act at all, because a filter trained on a handful of examples is not a weak filter, it is a confidently wrong one. So on a new server, reporting spam is an investment: nothing visible happens at first, and then one day it starts catching things. Your operator may also run the filter in a learning-only mode for a while, where it observes and files nothing.

Where filtered mail goes

When the filter does act, suspected spam is **filed into Junk — never refused, never deleted**. A wrong guess costs you a trip to the Junk folder, not a lost message. The same is true of mail quarantined for failing sender-authentication checks. The practical habit that follows: **glance through Junk now and then**, especially in the first weeks, and press **Not spam** on anything that does not belong there.

12. Calendar

Press **Calendar** in the header to switch views; the same button (now reading **Mail**) switches back.

The agenda

The calendar is an agenda — a list of your events grouped by day — rather than a month grid. The arrows move a month back and forward, **Today** returns to now, and your calendars are listed on the side; click one to view it.

Create, edit, delete events

Press **New event**. The form takes a **Title**, **Starts**, **Ends** and a **Location**; **Save** stores it. Click any event to edit it; **Delete** removes it. If someone else changed the event while you had it open, saving is refused with "Someone else changed this event. Reopen it to see their version." — reopen and redo your edit, so nobody's change is silently lost.

How times work

Times you pick are your local times, and the event is stored as an exact universal moment (UTC) — so it lands at the right instant for everyone, everywhere.

Events that arrive from other people can carry their own time zone rules. When the browser cannot resolve one of those zones, the event is shown at its **written** time and labelled: "shown as written — this event names a time zone we do not resolve in the browser". A labelled honest time beats a confidently wrong one.

Invitations

When someone invites you to a meeting:

- The invitation **lands in your Inbox** as a message, like any other mail.
- It also **appears in your calendar** automatically, marked as needing your answer. Nothing is ever accepted on your behalf — an invitation cannot create a commitment by itself.

To answer, open the event in a **calendar app connected to your account** (iPhone or Mac Calendar, Thunderbird, DAVx5 — see section 17) and press Accept, Maybe or Decline there. Your answer is mailed back to the organiser automatically, and if the organiser is on a compatible system they see your tick appear. The webmail's calendar shows the invitation but has no answer buttons yet.

When **you** invite others: create the event with invitees in a connected calendar app. The server mails each invitee a standard invitation:

- **Gmail and Outlook users** see it as a native invitation card with Yes / No / Maybe buttons in their own interface, and their answer flows back into your event.

- **Apple users (iPhone, iPad, Mac)** are a special case, and it is Apple's behaviour, not this server's: Apple Mail does not show Accept buttons on *emailed* invitations. Apple devices show the invitation interface only for calendar **accounts**. So an Apple user receives the invitation properly the moment their calendar account is connected to a compatible server (including this one); an .ics file in Apple Mail alone will only offer "Add to Calendar".

One practical warning that applies to every provider: an invitation that lands in the recipient's spam folder never shows answer buttons anywhere. If someone says they got your invitation "as just an email", ask them to check spam first.

Email reminders

If your server has calendar alarms enabled, an event with an email reminder on it (set from a connected calendar app) produces a reminder message to your own mailbox at the right moment, once — even when no calendar app is open anywhere. Most calendar apps also fire their own on-device alerts regardless; the email reminder is the belt-and-braces copy for the events you must not miss.

13. Auto-reply and forwarding

Open **Settings** and find **Auto-reply and forwarding**. A status line reports what is in force right now — "No auto-reply and no forwarding.", "Rules are active on this mailbox.", or a warning covered below.

Vacation message

Tick **Send an automatic reply while I am away**, then fill in:

Field	Notes
Reply subject	Optional. Left empty, the reply uses "Re:" plus the sender's own subject.
Reply message	The text people receive. Required.
Answer the same person at most once every … days	Default 7. Someone who mails you ten times gets one reply per window, not ten.

Press **Save rules**. The form's own footnote states the built-in behaviour:

> Mailing lists, bounces and other automatic mail are never answered, and a copy of the original always stays in your Inbox.

That first part matters: replies never go to newsletters, list traffic, delivery failure notices or other machines — that is what keeps auto-replies from starting mail storms. So do not be surprised when a test from a mailing list draws no reply. There is no start or end date on the form; you switch it on when you leave and off when you return.

Forwarding

Forward a copy to takes one address, or several separated by commas — up to 5. **Also keep a copy in my Inbox** is ticked by default; untick it and the form warns in red: "With this off, forwarded mail is not stored here at all." That is a real choice — with keep off, this mailbox stops accumulating your mail entirely.

The custom-filter warning

Both of these are stored as your account's mail filter (a Sieve script — section 19). If a filter *not written by this form* is already running on your mailbox — one you or an administrator wrote by hand — the panel warns in red:

> This mailbox has a filter that was not written here. Saving would replace it. Your existing filter is shown below.

Show the filter that is running displays it. Saving the simple form over a hand-written filter replaces it, and there is no undo — so the form makes you confirm before it will. If you rely on a hand-written filter, change it with the tool that made it instead.

14. Account security

Everything in this section lives in **Settings**.

If your organisation signs you in: being asked to sign in again

On an account connected to your organisation's sign-in (section 3), some of the changes described in this section will send you back there before they go through. You will see a message telling you to sign in again and retry — not "wrong password", and nothing has gone wrong.

The changes that do this are the ones that hand out or take away access: changing a password, setting a recovery address, creating an app password, and turning two-factor on or off. Where you have a password of your own, the form asks you to retype it before one of these — that is the same check, in the form it takes when there is a password to retype. Signing in again is what stands in for it when there is not.

The reason is worth a sentence, because it is the whole point of the check: it is not enough for the server to know a sign-in *happened at some point*. Someone who walked past your unlocked screen is signed in too. Asking your organisation to confirm it is you **right now** is what stops a borrowed session from being enough to mint a credential that outlives it. If you find yourself sent back more than feels reasonable, that is the size of the window your operator chose — tell them; it is one setting.

Retrying the same thing without signing in again will not work, so do not keep pressing the button.

Two panels do not work this way, and if you have no mailbox password you cannot use them at all: mailbox encryption (section 15) and the writing assistant's settings (section 16). Those forms ask for your current password and have no "sign in again" alternative, so on an account that was never given a mailbox password there is nothing you can type that they will accept — the answer you get is "the current password is not correct", which is true but unhelpful, because there is no correct one. Viewing those settings works normally; only changing them is blocked. This is a gap in the software rather than a rule about who may do what. If you need either of them changed, ask whoever set up your account.

Change password

Under **Change password**, enter your **Current password**, the **New password** (at least 12 characters — still the only rule) and **Confirm new password**, then press **Change password**.

Changing your password has deliberate side effects, and they are the point:

- **Every app password is cancelled at once.** The panel says so: "Changing your own password cancels every app password at once, so you would need to set your apps up again. That is deliberate: if you change your password because something went wrong, everything should stop."
- Every signed-in webmail session ends, and any password-reset link already in a mailbox stops working.
- Two-factor authentication is **not** removed — a password reset that also removed the second factor would be a way around it.

Recovery address

The **Recovery address** panel shows one of three states, and the middle one is the trap:

State shown	Meaning
"No recovery address. If you forget your password it cannot be reset — not even by the operator…"	You have none. Set one.
"ada@somewhere-else.com — awaiting confirmation. It CANNOT reset your password yet. …"	You set one but never opened the confirmation link. **Waiting is not protection.** Open the link; if it never arrived, that mailbox may be unreachable — set a different one.
"ada@somewhere-else.com — confirmed. This mailbox can reset your password."	You are covered.

To set or change it, enter your **Current password** and the address, then **Save recovery address**. The server checks the address's domain can receive mail (the same check as at signup), then mails the confirmation link there: "Saved. Open the confirmation link we just mailed there — it cannot be used to reset your password until you do."

Two-factor authentication

Two-factor authentication (2FA) adds a six-digit code from an authenticator app on your phone to your sign-in. The panel's own summary is exact: "An extra code from an app on your phone, asked for when you sign in here. Mail apps cannot be asked for a code, so once this is on they need an app password instead."

Turning it on:

1. Enter your password and press **Turn on two-factor authentication**.
2. Add the account to your authenticator app (any standard one works — Aegis, Google Authenticator, 1Password and so on) using the code the page shows.
3. **Recovery codes — save these now.** Ten codes appear, once, and never again. Each works exactly once, and they are the only way in if you lose your phone. Store them somewhere safe that is not this account.
4. Type the code your app currently shows and press **Finish turning it on**.

Until step 4, nothing has changed — a half-finished enrolment protects nothing, and the panel says so plainly ("Started but not finished — nothing is protecting your account yet.") rather than pretending you are covered.

Once it is on:

- Webmail sign-in asks for a code after your password. If a code is refused, check your phone's clock is set automatically — authenticator codes are time-based.
- Your account password **stops working in mail apps entirely** — not as an oversight, but because a mail app that skipped the second factor would make the second factor decoration. Every connected app needs an **app password** instead (below).
- Each code works once. If you sign in twice within the same half-minute, wait for the next code.

Turning it off needs both your password and a current code. **Lost your phone?** Sign in with a recovery code (type it where the app code goes). Lost the recovery codes too? Only an operator can remove the second factor for you, and they will want to be sure it is really you.

App passwords

An app password is a separate, randomly generated password for **one** app or device. The panel's summary: "A separate password for one app or device, which you can take back without changing your own password. Give each device its own, so losing one costs you that device and nothing else."

To create one: give it a label under **What is it for?** ("Ada's iPhone"), tick what it may reach under **What may it reach?** — **Mail**, **Calendar and contacts**, or both — enter your own password, and press **Create app password**.

The secret is shown **exactly once**: "Copy this now — it is not shown again." That is not a policy that could be relaxed — the server keeps only a fingerprint of it, so no screen can ever display it again. Type it into the app in place of your password.

Things to know:

- **App passwords do not work on the webmail sign-in form — on purpose.** The webmail is where the second factor is asked for; a credential that walked past it would defeat it. If an app password gets a "wrong password" answer in a browser, that is the design working.
- A credential used at the wrong door is told so: an app password scoped to Mail, typed into a calendar app, gets a "wrong scope" style refusal rather than "wrong password" — so you check the scope, not a password that was never wrong.
- The list shows when each one was **last used**. "never used" is the answer that tells you one is safe to revoke.
- **Revoke** one when you retire, sell or lose a device: "That app password no longer works. Any device using it will stop." Revoking needs no password — cutting off access is always allowed.
- You can hold up to 24. If you are anywhere near that, some of them are forgotten devices; prune.

Even without 2FA, app passwords are worth using for every device: one lost phone then costs you one revocation, not a password change everywhere.

What locks an account, and how to get back in

Five wrong password attempts lock the account for **15 minutes**. The refusal looks exactly like a wrong password — deliberately, so the sign-in form cannot be used to probe which accounts exist. If you are sure of your password and it suddenly stops working, the likeliest causes are the lockout (wait 15 minutes) or a mail app somewhere retrying an old password every minute (fix or remove that account — it will keep re-arming the lockout).

A successful password reset clears the lockout immediately: reset via your recovery link, or ask an administrator to set a new password. See also section 20.

15. Mailbox encryption

This feature is opt-in, and most people should leave it off unless they know they need it. It exists for mailboxes whose contents must be unreadable even to the server that stores them. If your server offers it, Settings shows an **Encrypt my mail at rest** panel; if there is no such panel, your server does not.

What turning it on does

From the moment it is on, every incoming message is encrypted **to your public key** before it is stored. The server keeps no readable copy and never holds your private key — so the

server, its operator, its backups and anyone who ever stole its disks cannot read your stored mail. Only someone holding your private key can.

The three consequences, stated before the switch

The panel states these before you can turn it on, because every one is irreversible in the direction that hurts:

> Before you turn this on: we cannot recover your mail if you lose your private key — there is no operator override, because an override would be a copy of your key. Searching message text stops working on this mailbox, because searching means reading; searching by subject, sender and recipient still works. And mail that arrives when you have no usable key is refused rather than stored unencrypted.

To spell the third one out: if encryption is required and your key becomes unusable (you removed it, or your certificate expired), the server does **not** quietly fall back to storing mail readable. It refuses the mail, and the sender is told their message did not arrive. That is the safe failure — but it means mail to you bounces until you add a key. If that state ever occurs, the panel shows a red alarm: "Mail to this address is being REFUSED right now: encryption is required and there is no usable key. Add a key to start receiving mail again."

Keys

Under **Add a public key or certificate**, paste an armoured OpenPGP **public** key, or a PEM S/MIME certificate — whichever format your mail app can decrypt. One format at a time; adding the other kind retires the current one. A private key is refused whichever you paste, whatever its header claims — the whole design rests on the server never holding one. Every change on this panel — adding or removing keys, turning encryption on or off — asks for your **Current password**, so a moment at your unlocked screen cannot alter it.

You cannot turn encryption on with no usable key: that would refuse all your mail from the first second. And while it is on, do not remove your last key, for the same reason.

Turning it **off** stops encrypting *new* mail. Mail already stored encrypted stays encrypted — the server cannot decrypt it for you, ever. If your domain administrator requires encryption for your domain, the panel says so and you cannot turn it off here.

Reading an encrypted mailbox

The webmail cannot decrypt. It never holds your private key (that is the point), so encrypted messages are not readable in the browser. To read an encrypted mailbox you need a mail app that can decrypt with your private key — for OpenPGP, Thunderbird's built-in encryption is the common choice; for S/MIME, most desktop mail apps can, once your certificate and key are installed on the device. Set up and test that app *before* turning encryption on.

Mail you receive is filed, forwarded and recovered exactly as before — filters, folders and Recently deleted all work on encrypted mail — but anything that requires reading the

message text (body search, the spam filter's content analysis, the writing assistant's server modes) cannot apply to it.

16. The writing assistant

If your server runs an assistant — or if you bring your own — the composer gains a **Writing assistant** box. The settings panel's first line is the contract:

> Drafts replies for you. Nothing is ever sent on your behalf — a suggestion goes into a box where you can read it, edit it or throw it away.

Using it

In the composer: type what you want under **What should it say?** ("decline politely, and ask about next month"), then press **Draft**, **Reply to this message**, or **Rewrite my text**. The result appears in a read-only **Suggestion** box with three buttons: **Use this** copies it into your message, **Try again** asks for another, **Discard** throws it away. The assistant never sends anything — **you** press Send, after reading. That reading step is a real safety boundary, not politeness: replies are drafted from a stranger's message, and a stranger's message can try to talk an assistant into something ("reply confirming the new bank details…"). The human reading the draft is what stops that.

Who runs the model — the privacy choice

In Settings, **Who runs the model** offers up to four modes, and the note under the selector states exactly where your text goes in each:

Mode	Where your text goes
This server's assistant	"The text you ask about is sent to this server, which asks its own model."
My own model, called by this server	"…sent to this server, which then asks your model using the key you store here."
My own model, called by this browser	"The text goes straight from this browser to your model. The server never sees it, and never holds your key."
No assistant	"No text is sent anywhere. The assistant does not appear when you write a message."

For your own model you supply an **Endpoint** (an OpenAI-compatible base URL; it must be `https://`) and a **Model** name, plus an **API key** where the model needs one. Saving any change here asks for your account password, "because this decides where your drafts are sent."

Bring-your-own, browser-called: checkable, not a promise

The third mode is the private one, and its privacy is a matter of construction rather than trust: the request goes from your browser directly to your model's address. The mail server is never in the path, refuses to relay for this mode, and never stores the key. Anyone can verify it with their browser's network tools — that is what "checkable, not a promise" means.

The price of that design: **your API key is stored in this browser only** ("Kept in this browser only, so you do not have to paste it again. It is never sent to the server…"). Anything stored in a browser profile can be read by whoever uses that profile. **Do not configure a browser-called model on a shared or public computer** — use a private machine, or choose a different mode.

If your mailbox is encrypted at rest (section 15), the two server-side modes additionally ask you to tick a confirmation each time, because sending text to the server makes readable to it something it otherwise could not read. That is a per-use decision, deliberately — not a setting you agree to once and forget.

17. Use another mail app

You can read this mailbox in Apple Mail, Thunderbird, Outlook, K-9 Mail and anything else that speaks IMAP, and sync the calendar and contacts to apps that speak CalDAV and CardDAV.

Your server's exact settings live in Settings → "Use another mail app." That panel is filled in by the server itself with the names and ports this deployment actually listens on — trust it over any manual, including this one. What follows is the general shape plus per-app notes.

The general shape

Setting	Typical value
Incoming mail (IMAP)	your mail server, port **993**, SSL/TLS
Incoming mail (POP3)	port **995**, SSL/TLS — only if your server offers POP3
Outgoing mail (SMTP)	port **465**, SSL/TLS — or port **587**, STARTTLS; both work
Username	your **full** email address
Password	your mailbox password — or an **app password**, required once two-factor is on
Calendar (CalDAV), Contacts (CardDAV)	many apps find these from just your address; the panel shows the server name for apps that ask

Prefer IMAP over POP3: IMAP keeps mail on the server so every device sees the same mailbox; POP3 downloads, and mail read on one device stays unread on the others.

One rule with no exceptions, from the panel itself: "Every one of these is encrypted — there is no unencrypted way in, by design. If an app offers 'no encryption' or asks you to accept a certificate warning, something is wrong; stop and tell the operator."

App by app

Thunderbird (computer): works, including calendar and contacts. Add the account with just your address and password — Thunderbird finds the settings itself ("Configuration found at email provider"). For calendar and contacts, Thunderbird can pick up the calendar at setup; contacts may need the CalDAV/CardDAV address entered once from the settings panel.

Apple Mail (Mac): works, but **enter the server name by hand** — automatic setup from just your address does not work for mail on Apple's clients (they do not consult the discovery records this server publishes; that is Apple's lookup behaviour, not a fault in your account). Choose "Other Mail Account", and when the automatic attempt fails, type your server's name into both the incoming and outgoing server fields, with your full address as the username. It then connects first time.

iPhone / iPad: mail as above (enter the server name if asked). **Calendar and contacts set themselves up from just your address**: Settings → add a CalDAV account and a CardDAV account, enter your address and password, done — the server is found automatically, and this path is well proven, including answering meeting invitations.

K-9 Mail (Android): works; **automatic setup works** from just your address and password. For calendar and contacts on Android, install DAVx5 and give it the same address — it also discovers everything automatically.

Outlook (computer): mail works **over IMAP**, but Outlook will not find the settings on its own — choose IMAP and type them in from the panel. **Outlook's calendar and contacts cannot connect at all**: Outlook only syncs those over Exchange, which ZephyrAB does not provide, and it does not speak CalDAV/CardDAV. Use a different app for calendar and contacts.

Outlook mobile and Windows Mail: cannot connect at all. Both require Exchange/ActiveSync, which ZephyrAB does not provide. On a phone, use any IMAP mail app (K-9, Thunderbird for Android, Apple Mail on iOS) instead.

macOS Contacts app: does not work correctly. Reading is fine, but edits made in it create duplicates and lose fields — a long-standing bug in Apple's macOS Contacts CardDAV client that affects many servers, not just this one (iOS Contacts is fine). Use another CardDAV client on the Mac, such as Thunderbird's address book.

Plus-addressing (section 9) works from every app with no setup, because the server does it.

If two-factor is on

Mail apps cannot ask you for a code, so once two-factor authentication is on, your account password stops working in them by design. Create one **app password per app** (section 14) and use that as the app's password. If an app suddenly starts failing after you enabled two-factor, this is why.

If your organisation signs you in

An app that supports your organisation's sign-in can use it here for mail: this server accepts it for IMAP, POP3, sending, and the JMAP protocol some newer apps use. In practice that means the app shows your organisation's sign-in page instead of asking for a password, and you never type a mailbox password at all.

Apps that cannot do that need an app password (section 14) — and that includes every calendar and contacts app, because calendar and contacts sync here does not accept organisation sign-in at all. So a typical setup on a connected account is: mail through your organisation's sign-in where the app supports it, and an app password for everything else.

If you have no mailbox password of your own, you cannot create an app password from the webmail sign-in page, because you cannot get into it. Ask whoever set up your account to issue one for you.

18. Shared mailboxes

An administrator can grant you access to another mailbox — a team inbox, or a colleague's mail while they are away.

When that happens, **mail apps** connected over IMAP show the shared mailbox under a folder called "**Other Users**" — for example `Other Users/support@example.com` is that account's Inbox, and `Other Users/support@example.com/Sent` its Sent folder. What you can do there depends on the rights you were granted: you may be able only to read, or also to flag, file and delete. An app may open a shared mailbox read-only when your rights do not allow changes.

The webmail does not show shared mailboxes. It lists only your own folders. To work in a shared mailbox, use a connected mail app.

Mail in a shared mailbox counts against its owner's storage, not yours.

19. Filters (advanced)

Every account's incoming mail runs through a filter script in the **Sieve** language — a small, safe language made for mail filtering. You may never need to know this: the Auto-reply and forwarding form (section 13) writes the script for you.

Power users can write their own. A hand-written script can file messages into folders by sender, list, or plus-address suffix, set flags, forward selectively, and more. You manage scripts with a **ManageSieve**-capable client (several desktop mail clients have one built in or as an extension); your operator can tell you the connection details, which use your normal credentials (or an app password).

This server advertises the following Sieve capabilities, which is the list a script's `require` line may name: `fileinto`, `vacation`, `envelope`, `imap4flags`, `date`, `body`, `relational`, `subaddress`, `variables`, `include`, and the comparators `comparator-i;octet`, `comparator-i;ascii-casemap`, `comparator-i;ascii-numeric`.

Two safety properties worth knowing:

- **A broken filter never loses mail.** If your script fails to run — or fails to parse after an upload from an older tool — the message is simply kept in your Inbox, unfiltered. The failure mode is "my rule did not run", never "my mail vanished".
- **The simple rules form and your script are the same thing.** Saving the form *replaces* the account's script. If a hand-written script is in place, the form warns you and refuses to overwrite it without an explicit confirmation (section 13). Keep hand-written filtering in your Sieve tool, and do not mix the two.

Scripts are validated when you upload them — a script that does not parse is refused at upload with the reason, including a couple of deliberate strictnesses: a forwarding address or folder name containing control characters is refused outright, because it could not be acted on safely.

20. Fix common problems

"Wrong address or password" — but the password is right

Two likely causes. **Lockout:** five wrong attempts lock the account for 15 minutes, and the lockout answers exactly like a wrong password. Wait 15 minutes and try once, carefully. **A forgotten device:** a mail app somewhere still retrying an old password will re-arm the lockout every few minutes forever; find it and fix or remove the account. A password reset (below) also clears the lockout immediately.

I was told to sign in again while changing a setting

On an account connected to your organisation's sign-in, a handful of settings changes need a *recent* confirmation that it is really you — see section 14. Go back to your organisation's sign-in, authenticate again, and retry the change. Retrying without doing that cannot work, however many times you press the button, so do not treat it as a stuck page.

Forgot the password

Use **Forgot your password?** on the sign-in page. A reset link goes to your **confirmed** recovery address; it works once and expires in 30 minutes. If you never confirmed a

recovery address, no link can arrive — ask your administrator to set a **new** password for you. They cannot look up or recover the old one; nobody can. (This is also the moment to set and confirm a recovery address, so it does not happen twice.)

My mail to Gmail (or Yahoo) landed in spam

Almost certainly not your fault and not a misconfiguration. Big providers score senders by **reputation** — the history of the sending server and domain — and a new or low-volume server starts with none, so its mail is treated cautiously even when every technical check passes. It improves with time and normal sending. Meanwhile: ask your recipient to find the message in spam and mark it "Not spam", or to add your address to their contacts — both teach their provider directly.

A message I sent came back refused: "not accepting messages"

A refusal like `550 5.2.1 … not accepting messages` means the recipient's mailbox exists but is currently refusing mail. On a ZephyrAB server the usual cause is section 15 in reverse: the recipient's mailbox requires encryption and has no usable key right now, so the server refuses rather than storing their mail readable. Nothing you can fix from your end — contact the recipient another way; once they add a key, mail flows again.

My attachment was refused

Read the wording — it names the cause. Over the size limit: send the file as a link instead (section 7), which exists for exactly this. Refused by the malware scanner: the file matched a virus signature; the message names the detection, and no part of the file went anywhere. If the scanner itself is unavailable, the server refuses to share what it could not scan — try again later.

Search finds nothing, but I know the message exists

Search matches **words**, not fragments (section 8). `nvoice` finds nothing; `invoice` finds it. Several words must appear together, in order — search for a phrase the message actually contains, or for a single distinctive word. And if your mailbox is encrypted at rest, message text is not searchable at all — search by subject or sender instead.

A calendar invite shows no Accept button in Apple Mail

That is Apple's behaviour with emailed invitations, on every mail server. Connect the **calendar account** instead (iPhone/Mac: add a CalDAV account with your address — section 17), and invitations appear in the Calendar app itself, with the proper Accept / Maybe / Decline. Also check the invitation did not land in spam: an invitation delivered to spam never gets answer buttons anywhere.

I reloaded the page and was signed out

By design — your password is never stored in the browser (section 3). Sign in again.

My app password does not work on the webmail

By design — app passwords work only in mail, calendar and contacts apps, never on the interactive sign-in (section 14). Use your account password (and code) there.

The message body looks plain / images are missing

Check the switch above the message first. If it reads **Plain text**, click **Formatted**. If there is no switch at all, the sender did not send a formatted version — there is nothing to show.

Missing pictures are usually the block on pictures loaded from the internet: look for "Images from the internet are blocked" and click **Show images** (section 4). If you clicked it and they are still missing, the sender's website is not serving them; that is at their end, not yours.

Formatting is deliberately limited — the sender's own stylesheets are dropped, so a heavily designed newsletter looks plainer here than in some apps. The content is intact.

My auto-reply did not answer a test message

Three usual reasons: the same sender is only answered once per window (default: once every 7 days); automatic mail — mailing lists, notifications, bounces — is never answered; and a reply goes out only for mail that actually arrives from outside while the rule is on.

I deleted a folder by mistake

If your server keeps recovery copies, the folder's messages are in **Settings → Recently deleted** for the recovery window, and putting one back re-creates the folder (section 10). Otherwise, contact your operator quickly — restoring from backup is possible for a while but needs a human.

21. Glossary

Term	Meaning
Alias	An extra address that delivers into your mailbox. Set up by an administrator.
App password	A separate, randomly generated password for one app or device, revocable on its own. Cannot be used on the webmail sign-in.
CalDAV / CardDAV	The standard protocols calendar and contacts apps use to sync with a server.
Flag	A mark you put on a message to say it needs your attention. Stored on the server, so every app you use sees it — other apps may call it a star.
Hash	A one-way mathematical fingerprint. The

	server stores a hash of your password, never the password — which is why nobody can read a password back, ever.
IMAP	The standard protocol mail apps use to read mail that stays on the server. Every device sees the same mailbox.
Invite code	A single-purpose code from your administrator that lets you create an account. It decides your domain and quota.
JMAP	The modern mail protocol the webmail itself uses. You never need to configure it.
ManageSieve	The protocol for uploading and managing Sieve filter scripts from a client.
MX record	The public directory entry that says which server receives a domain's mail. Its absence is how the recovery-address check knows a domain cannot receive mail.
OpenPGP	A widely used end-to-end encryption standard. Mailbox encryption can encrypt your stored mail to an OpenPGP public key; you decrypt with the private key in a capable mail app.
Plus-addressing	Address variants like `ada+shop@example.com` that deliver to `ada@example.com`. Useful for sorting and for spotting who shared your address.
POP3	An older protocol that downloads mail to one device. Supported, but IMAP is almost always the better choice.
Quota	Your storage limit on the server, shown in Settings when one is set.
Recovery address	A different mailbox, confirmed by link, that can receive a password-reset link. Without one, a forgotten password is permanent.
Sieve	The standard filtering language your incoming-mail rules are written in. The rules form writes it for you; power users write it directly.
S/MIME	A certificate-based encryption standard, the corporate cousin of OpenPGP. Mailbox encryption accepts an S/MIME certificate as an alternative to an OpenPGP key.

Single sign-on (SSO)	Signing in with your organisation's own login instead of a password kept here. Where it is set up, mail apps that support it use it; calendar and contacts apps and the webmail sign-in page do not, and need an app password.
SMTP	The protocol that carries mail between servers, and from your app to the server (called "submission", on ports 465 or 587).
SSL/TLS / STARTTLS	Two ways a connection is encrypted: SSL/TLS from the first byte, STARTTLS upgrading right after hello. Both are safe; "no encryption" is not offered.
Thread / conversation	Messages grouped because they are replies to one another. The reader shows the rest of a conversation under the open message.
TOTP	Time-based one-time passwords — the six-digit codes an authenticator app shows, used for two-factor authentication.
Two-factor authentication (2FA)	Requiring both your password and a current code at sign-in, so a stolen password alone is not enough.