USER AND SETUP MANUAL

lua Panel

Domains, mailboxes, service groups and access for your company

In this guide you will learn to:

- Sign in, turn on two-step verification and choose language and theme
- Add your domain and set up DKIM, DMARC and Autodiscover
- Create and edit mailboxes, aliases and app passwords
- Use service groups: working hours, access location (IP), webmail only and phones
- Follow logs and statistics and track messages
- Give other people access with users and teams
- Migrate email from another provider and open support tickets
- Use the panel on your phone and solve common problems

Version: November 2026 · English · painel.lua.email

Contents

1. First sign-in . . . 3
2. The home screen . . . 9
3. Adding the domain . . . 12
4. DNS: DKIM, DMARC and Autodiscover . . . 17
5. Creating mailboxes . . . 27
6. Editing a mailbox . . . 38
7. Aliases . . . 57
8. Domain health . . . 63
9. Service groups: schedule, session, directory and email . . . 70
10. Colabora, directories and sharing . . . 91
11. Per-account routing (lua Bridge) . . . 96
12. Logs, statistics and tracking . . . 105
13. Diagnostic tools . . . 111
14. Users, teams and roles . . . 116
15. Other features . . . 129
16. Migrate email from another provider . . . 138
17. Support tickets . . . 142
18. Language, theme, and using it on your phone . . . 146
19. Common problems . . . 150
Still need help? . . . 151

1. First sign-in

When the company subscribes, Lua creates the administrator's user in the panel. The login is the **primary email** given at signup, and the first password is temporary.

1. Open painel.lua.email and sign in with the primary email and the temporary password you received.
2. The panel asks for a personal password before anything else. It must have at least 8 characters, with an uppercase letter, a lowercase letter, a number and a special character.
3. Click **Set password and continue**. From then on, the temporary password no longer works.

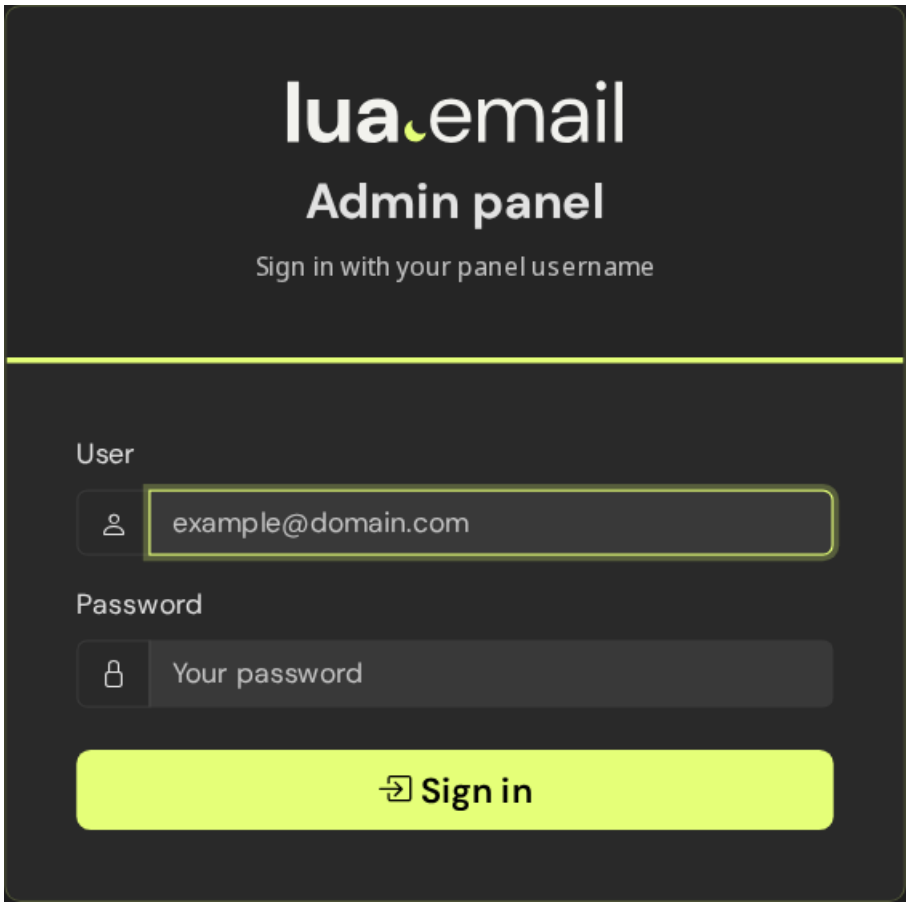


Figure 1: Panel sign-in. Fictional data.

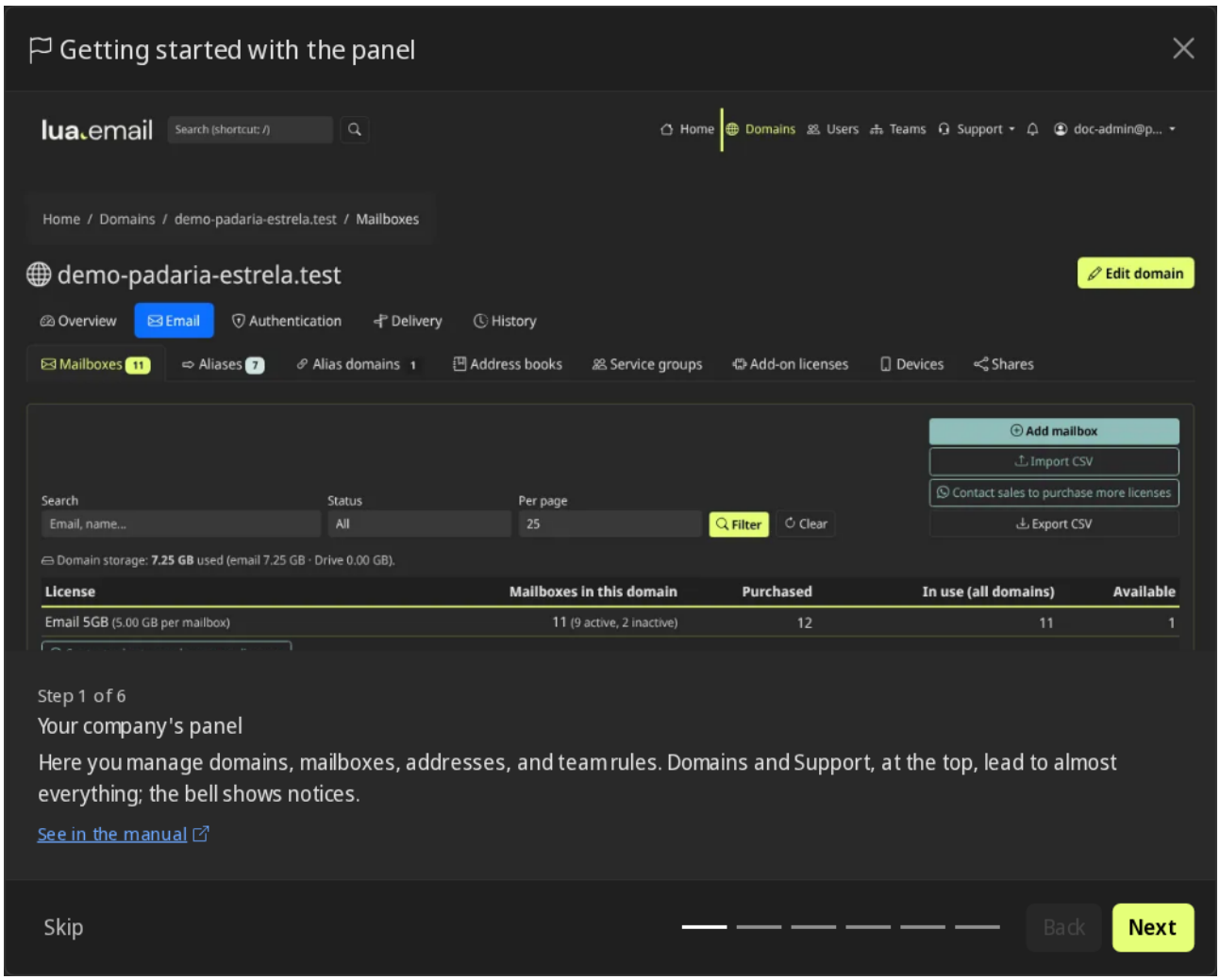


Figure 2: On first sign-in, the panel asks for a personal password.

The primary email and the alternate email

The primary email is your login and also the address that receives panel notices: domain activated, TXT deadline running out, new user created, another administrator's password changed, API token generated. These notices appear on the **bell** at the top and arrive by email.

If your primary email is a mailbox on the same domain you are about to set up, also add an **alternate email** under **your name (top right) → My profile**. When it is filled in, notices go there. That way you keep receiving notices even while the domain is not yet receiving email, or if your mailbox is blocked.

My profile brings everything together on one page, with five tabs: **Data**, **Password**, **Security**, **Preferences** and **API token**. To change the alternate email, the panel asks for your **current password** (a field on the Data tab): that address receives the security alerts and the two-step verification code, and the password stops someone with your open session from redirecting them. Name and phone do not ask for the password.

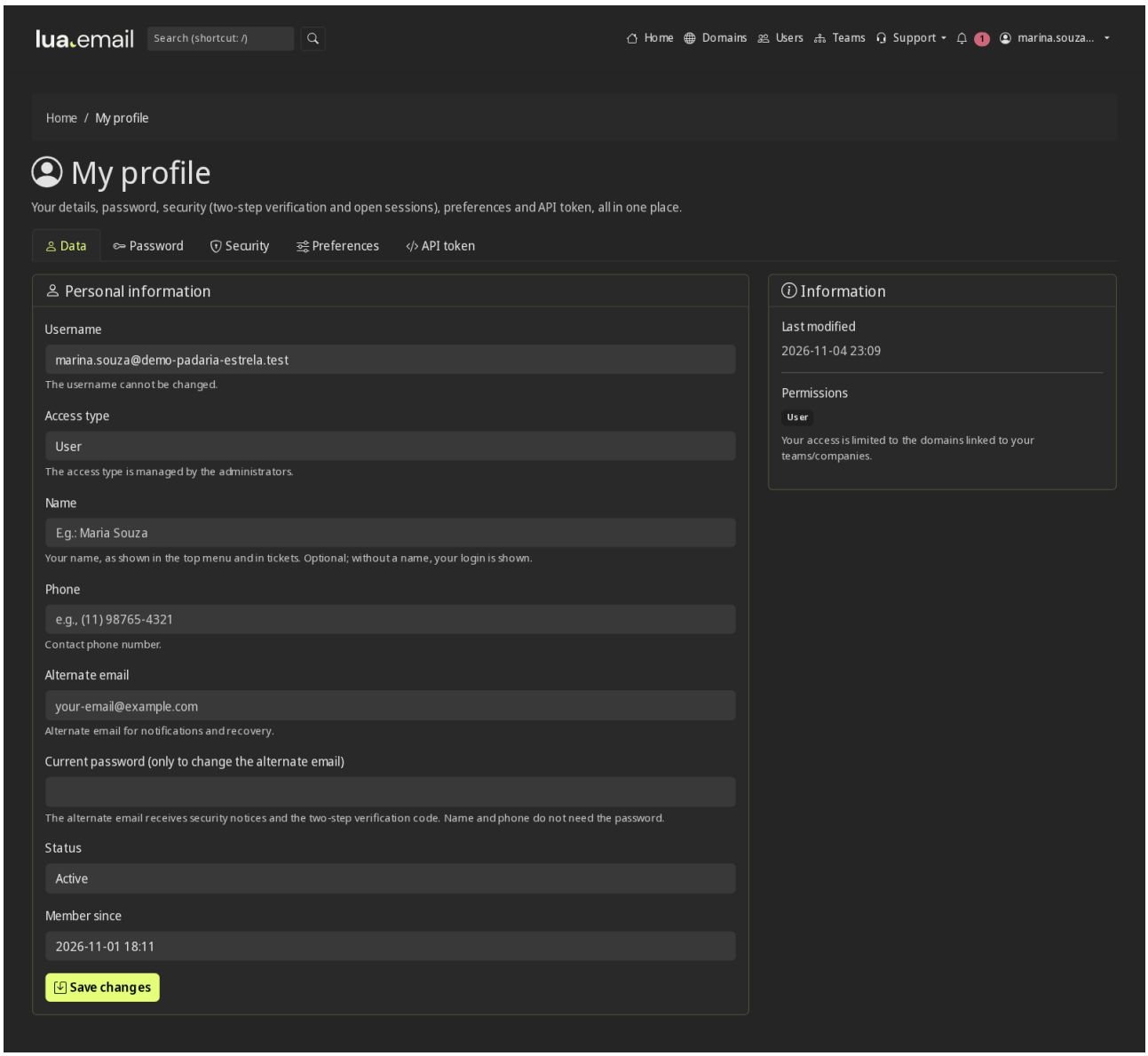


Figure 3: My profile, Data tab: the alternate email only changes with the current password.

- **Language and theme:** the **Preferences** tab of My profile sets the language (Portuguese or English) and the theme (dark or light). See chapter 18.
- **Change your password:** My profile → Password tab (asks for the current password).
- **Active sessions:** on the Security tab of My profile, it shows where you are signed in and lets you end a session left open on another computer. The list is paginated, with 25 sessions per page, and **End other sessions** applies to all of them, not just the ones on the open page.
- **API token:** on the API token tab (it only appears for people who can generate one), to connect another system to the panel. Whoever has the token reaches the API with the same access you have, so generate it only when you need it and choose an expiry. The token appears **only once**, when it is generated: copy it and keep it. If you lose it, generate another (the previous one stops working). **Requesting a domain through the API** depends on a permission that our team turns on for your user: the token requests the domain at POST `/api/v1/domains`, it stays pending until the TXT is validated, and the progress is available at GET `/api/v1/domain-requests/{id}`. Internal or reserved names, such as `.local` and `.test`, are refused.
- **Signing out:** click your name in the top right corner, then **Sign out**.

Two-step verification

With two-step verification, the panel asks for a code in addition to your password every time you sign in. Anyone who finds out your password cannot get in without the code. Turn it on at **your name → My profile → Security tab → Two-step verification → Enable**.

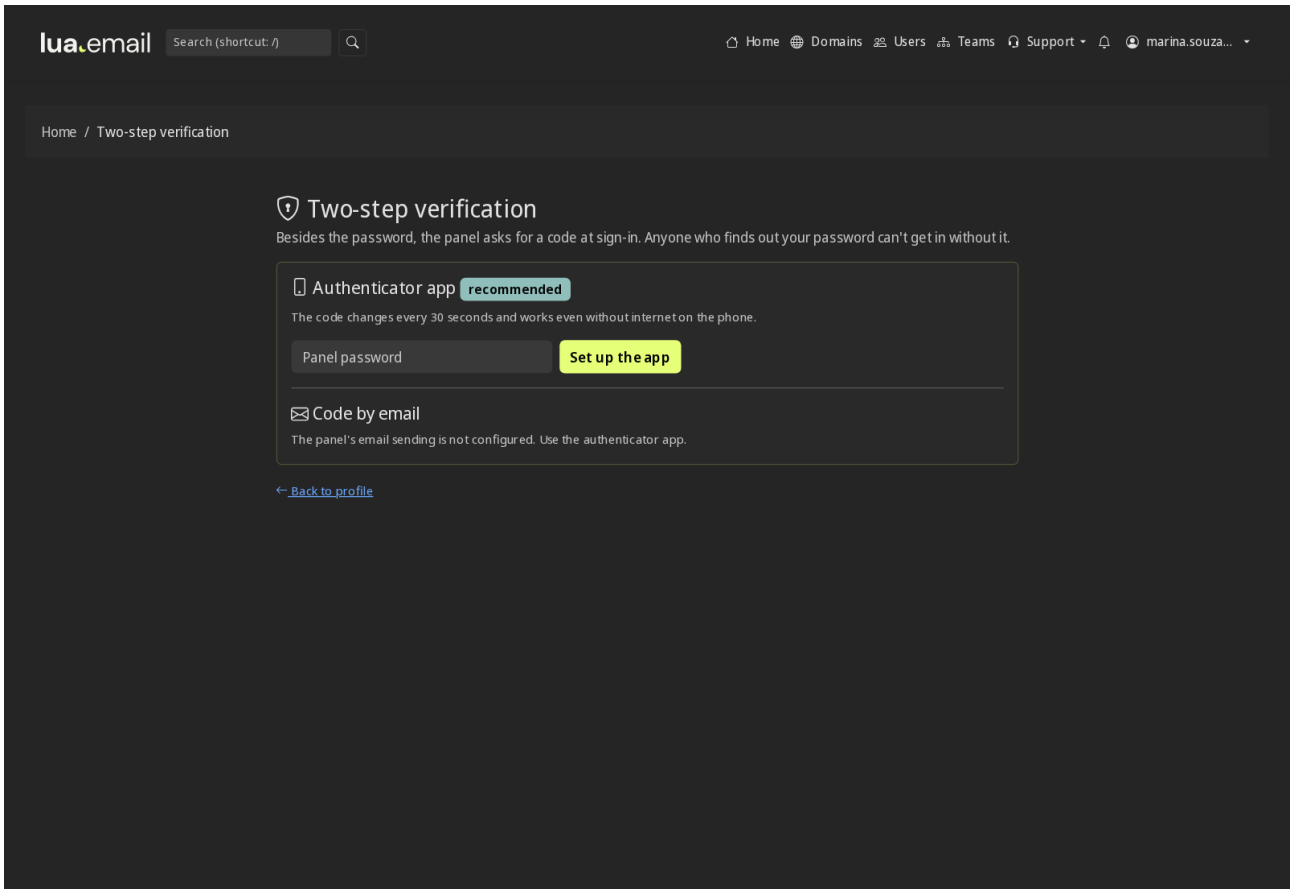


Figure 4: Choosing between the authenticator app and the code by email.

With the authenticator app (recommended). Use Google Authenticator, Microsoft Authenticator, Authy, 1Password, Bitwarden or another app that shows 6-digit codes. The code changes every 30 seconds and works even when the phone has no internet.

1. Type your panel password and click **Set up the app**.
2. In the phone app, add an account and scan the **QR code** on the screen. With no camera, type the key shown next to it.
3. Type the 6-digit code shown in the app and click **Enable**.

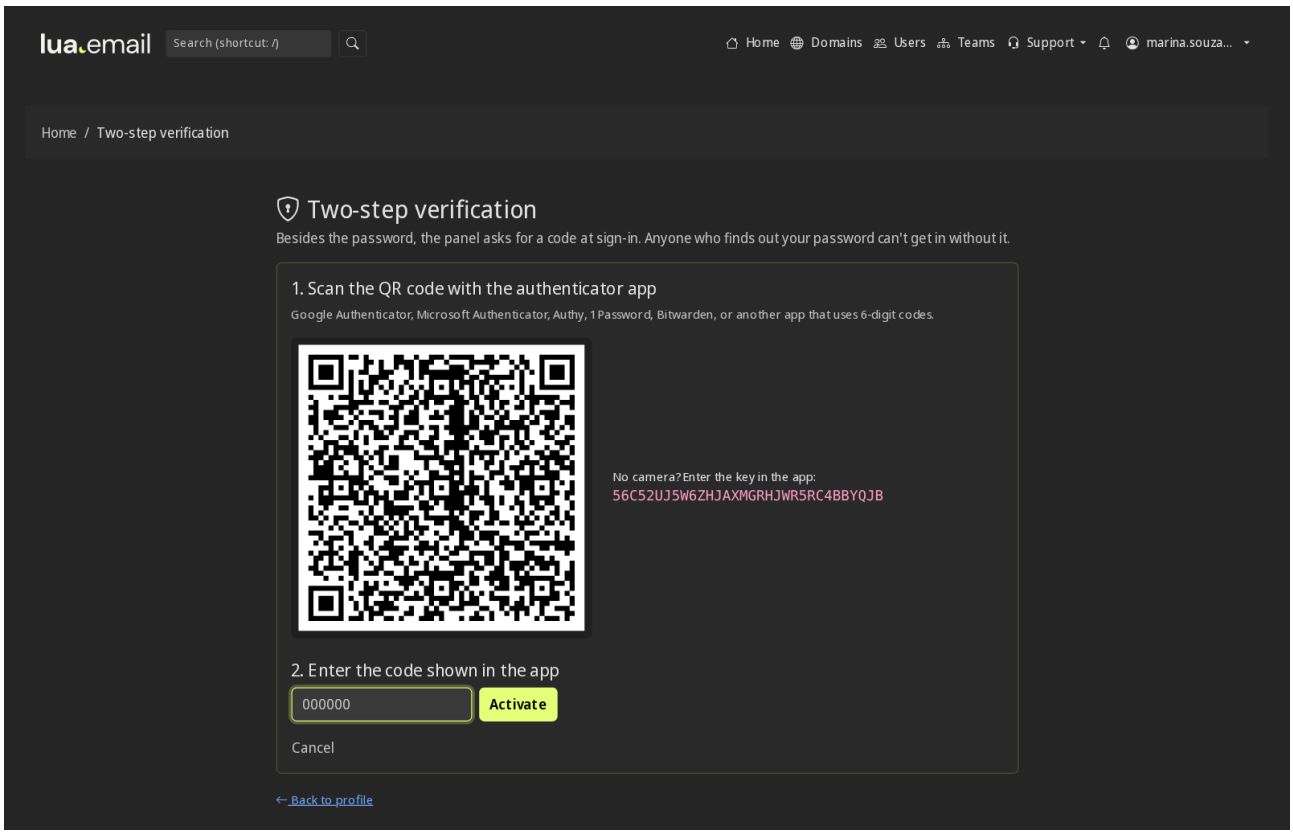


Figure 5: Scan the QR code with the app and type the code to enable. Fictional key.

With a code by email. At each sign-in, a 6-digit code arrives at the email you chose and is valid for 10 minutes. Choose the email (your login or the alternate email from My profile), type your password, click **Send code**, and enter the code you received. Prefer an email outside the company: if the code arrives in a mailbox on your own domain, whoever administers the domain can read it too. Lua superadministrators always use the app.

Keep the recovery codes. When you enable it, the panel shows 10 codes. Each is good for one sign-in, in place of the app or email code, for when you lose your phone or access to your email. They appear only at that moment: copy, print or write them down and keep them somewhere safe. When you enable it, the other sessions open with your account are ended.

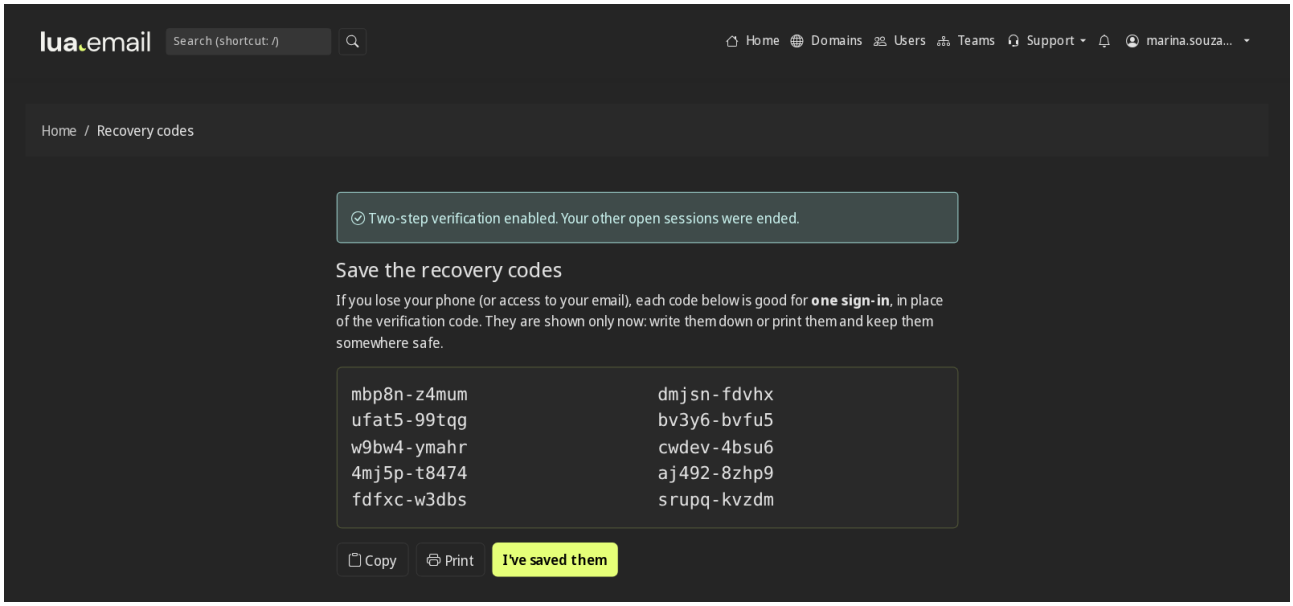


Figure 6: The recovery codes appear only once. Fictional codes.

Day to day. After the password, the panel asks for the code. Type the app code (or the one that arrived by email; if it did not arrive, use **Send another code**). If you lost your phone, type a recovery code in the same field. After five wrong codes, the panel goes back to the password.

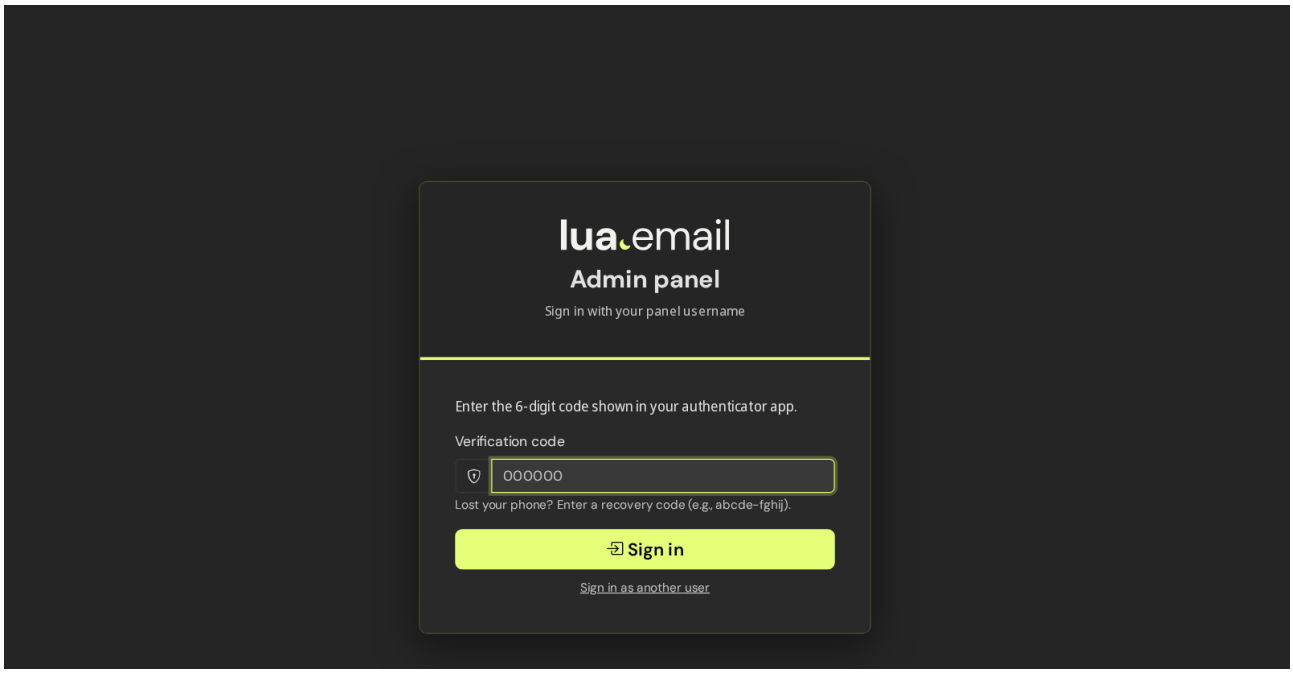


Figure 7: After the password, the code.

- **Switching phones or methods, or generating new recovery codes:** in My profile → Security tab → Two-step verification, enter your password and a code and choose **Change method**, **Generate new recovery codes** or **Disable**.
- **Lost your phone and the recovery codes:** ask an administrator at your company to reset your two-step verification (chapter 14), or contact support.
- If your company makes verification mandatory, the panel asks you to set it up right after you sign in, before any other screen.

2. The home screen

After you sign in, **Home** shows what needs your attention first and, right below it, the shortcuts and your company's numbers:

- **Getting started:** the setup checklist (domain, TXT, DNS and first mailbox), until it is complete. You can hide it.
- **Tickets that need you:** tickets with a new reply from our team and those waiting for a reply from you, with how long ago and a link to open them. With nothing pending, the card says all is good.
- **DNS of your domains:** says whether everything is fine or how many domains need a fix. The **See domains with problems** button opens the domain list already filtered (see chapter 8).
- **Licenses by type:** how many mailboxes of each plan the company has purchased, how many are in use and how many are still free. Resources purchased separately (video meetings and recovery of deleted messages) appear in the same list, as add-on licenses. When no free license is left, the card warns you and offers the next step: **Buy more**, for customers who subscribed on the website, or **Ask support for more licenses**, which opens a ticket already filled in with the subject, type, quantity and domain.
- **Shortcuts:** create a mailbox, change a mailbox password, set up email on a phone, your account and password, and the manual. They appear according to your access level: people who only view see fewer shortcuts.
- **Top senders in the last 24 hours:** the accounts on your domains that sent the most, and how many messages each one sent.
- **At a glance:** how many domains and mailboxes the company has and how many mailboxes are inactive.

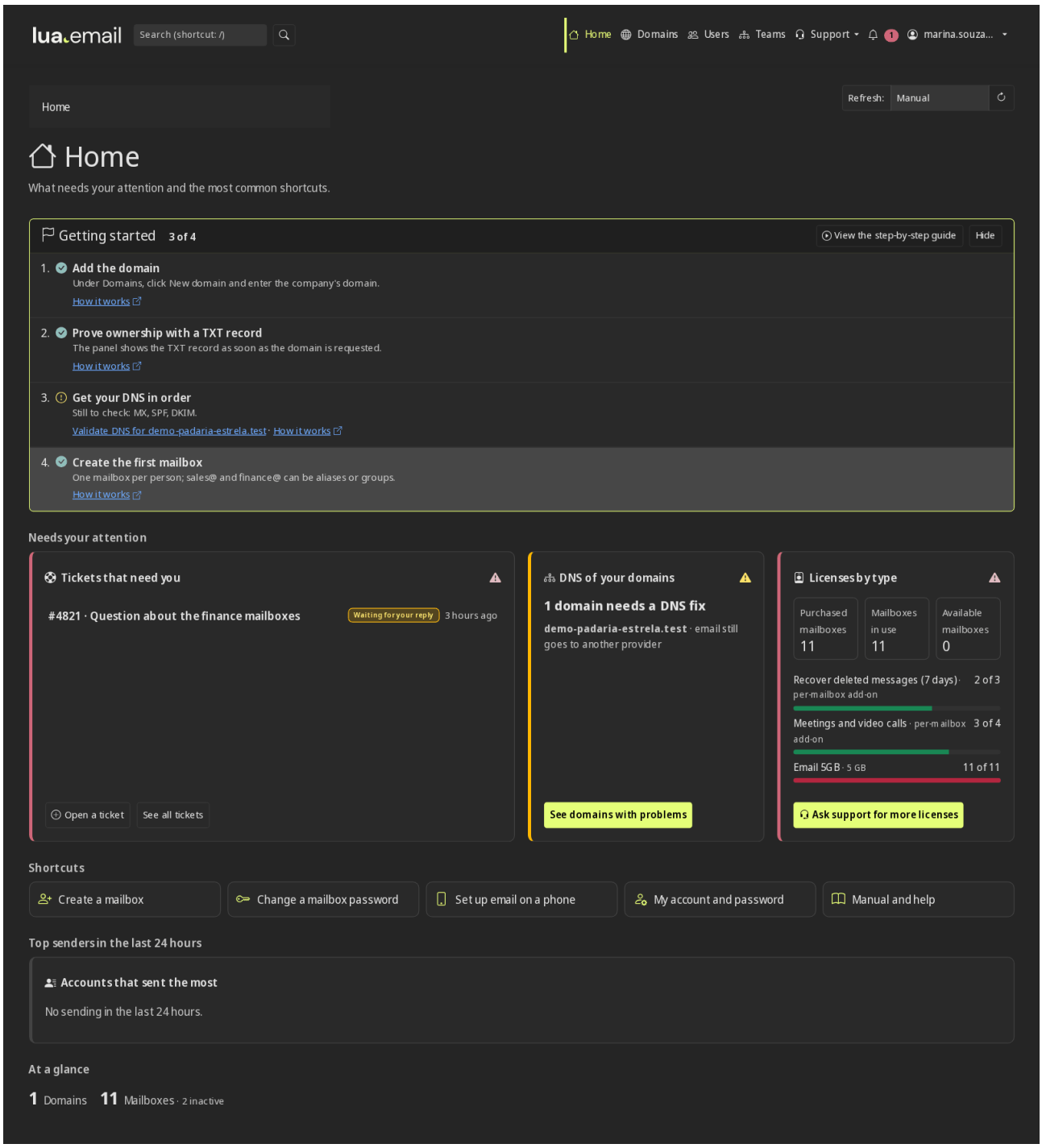


Figure 8: Home for the example company: what needs you first, then the shortcuts.

Refresh. At the top of Home, and also on the statistics and log screens (see chapter 12), the **Refresh** control sets whether the page refreshes automatically: **Manual**, or every **1**, **5** or **10** minutes. The button next to it, **Refresh now**, fetches the data right away. Automatic refresh pauses while the browser tab is hidden, and your choice is saved in the browser for each screen.

At the top are the **Domains** menu, the **Support** menu (tickets, documentation, email migration, tools and tracing), the notification bell and the search. Search finds mailboxes, aliases, domains, service groups, panel users and tickets by address, name or title: type two letters and pick from the list. To reach it without the mouse, press **/** on any screen (the shortcut does nothing while you are typing in a field). Each person only sees what is within their reach: a company administrator cannot find another customer's domain, mailbox, user or ticket, neither in the list that appears as you type nor on the results page.

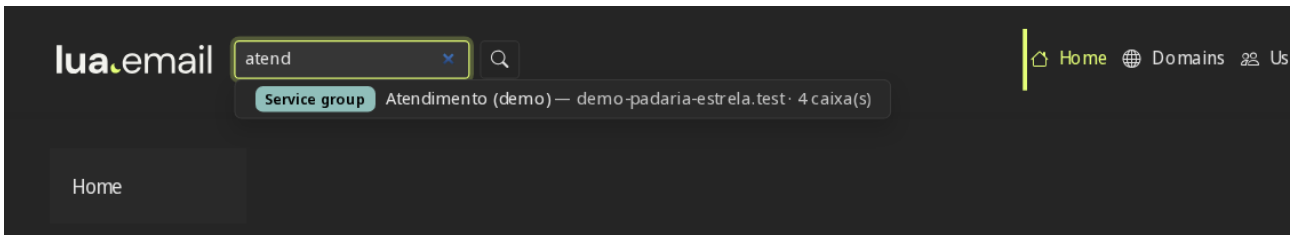


Figure 9: The top search also finds service groups and says how many mailboxes each has.

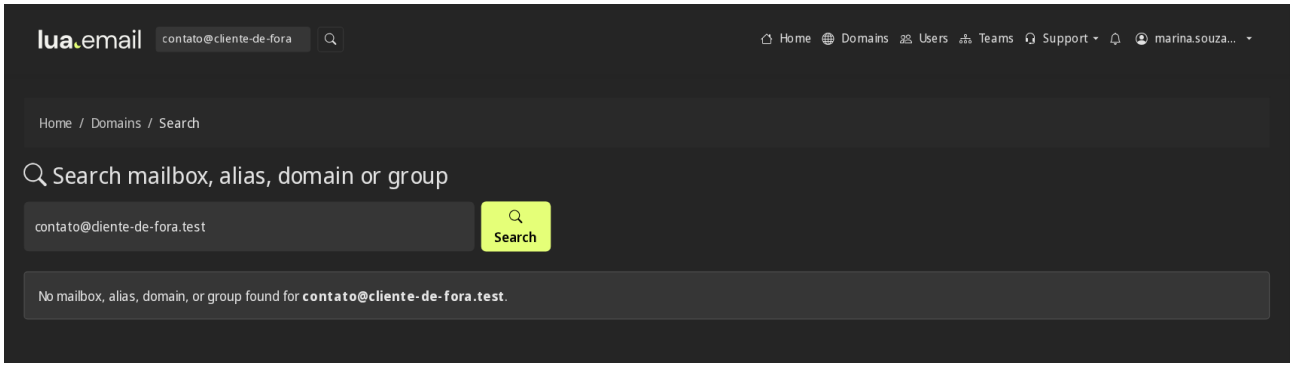


Figure 10: Searchers only find what is within their reach: another customer's address comes back with no results (real screen, fictional data).

Where you are. The path at the top of each screen (Home, Domains, the domain, the current screen) always starts at **Home**; click any level to go back to it. When you open a mailbox or alias from the list and then go back, the list keeps the filter, the search and the page you were on.

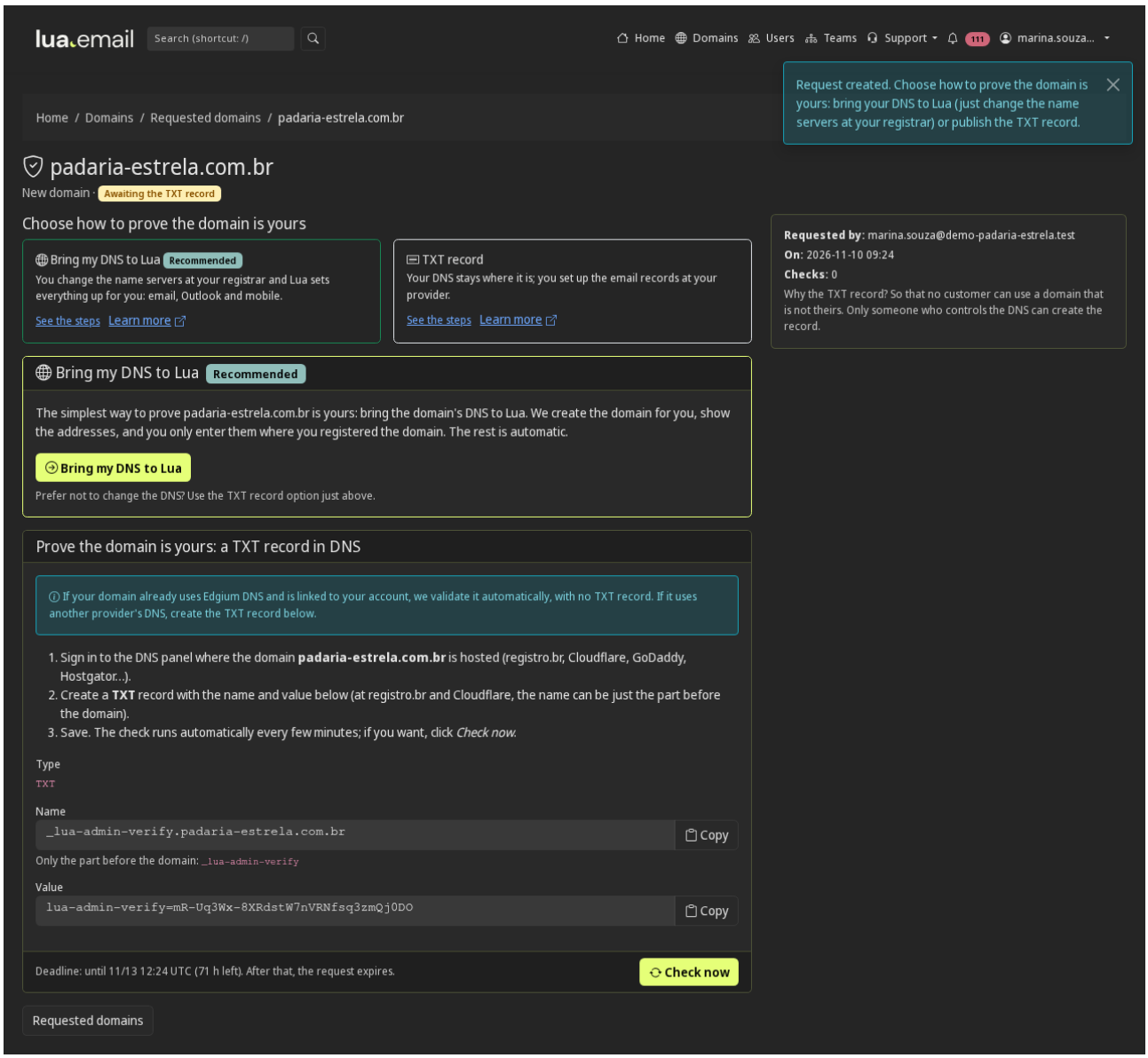
Notices and confirmations. The panel no longer uses the browser's confirmation box. Everything that asks "are you sure?" (disabling an alias, removing an entry, removing a mailbox) opens a panel window, with the action button and **Cancel**; in the more serious cases, such as removing a mailbox, it only enables the button after you type the address. Success and error notices appear as a box in the corner of the screen; the success one disappears on its own, the error one stays until you close it.

3. Adding the domain

A domain only becomes your company's after you prove that you control its DNS. The panel offers two paths: publish a TXT record in the DNS where the domain is, or bring the DNS to Edgium by changing the name servers at the registrar.

First time? The onboarding tutorial takes the domain from the request to the first mailbox, on both paths, with a video.

The two paths, side by side. The request screen shows **Bring my DNS to Lua**, marked as recommended, and **TXT record**, each with the **See the steps** and **Learn more** links. The Bring my DNS to Lua path is for those who are already registered Edgium customers: you only change the name servers at the registrar. The panel detects the change, activates the domain and sets up by itself the SPF (merged with the one you already had), the DKIM, the DMARC (Lua's recommended default), Autodiscover and, if the domain has an active mailbox, the MX. If you validate with the TXT record and change the name servers to Edgium later, the result is the same. The MX is not changed automatically when the domain does not have an active mailbox yet, when an email migration is in progress or when the domain's **External MX** option was set manually: the bell notice says that only the MX is missing, which you change under **Fix problems**, in Domain health. A domain with Lua Shield never has its MX changed. See the comparison and the step-by-step for both paths in domain onboarding and in Bring my DNS to Lua.



The domain request: bring your DNS (recommended) or publish the TXT record.

1. Under **Domains**, click **New domain**, type the domain (for example, `exemplo-engenharia.test`) and, if you like, a description. As you type, the panel tells you whether the domain is new to the platform.
2. Click **Continue**. The next screen shows the TXT record: the **name** (`_lua-admin-verify.yourdomain`) and the **value**, each with a Copy button.
3. In the domain's DNS panel (registro.br, Cloudflare, your hosting provider), create a **TXT** record with that name and value. In many panels, the name is only the part before the domain: `_lua-admin-verify`.
4. Go back to the panel and click **Check now**. If the TXT record has not shown up yet, the screen says so and keeps checking on its own every few minutes.
5. When the TXT record appears, the domain becomes active right away and the bell notifies you. The verification TXT record can now be removed from DNS.

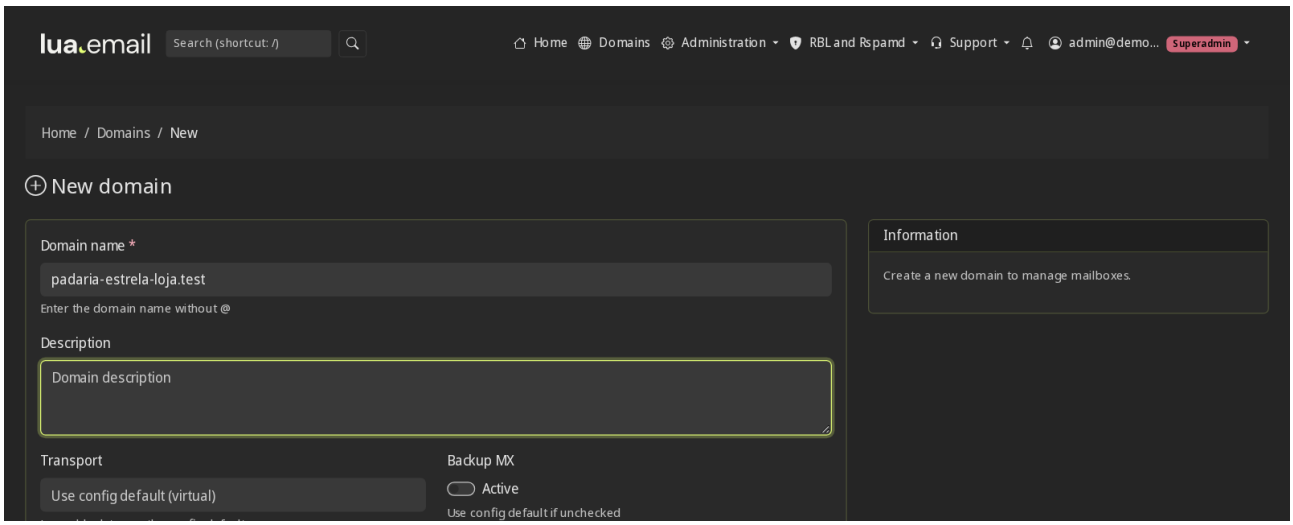


Figure 11: Add domain: the panel gives feedback as you type.

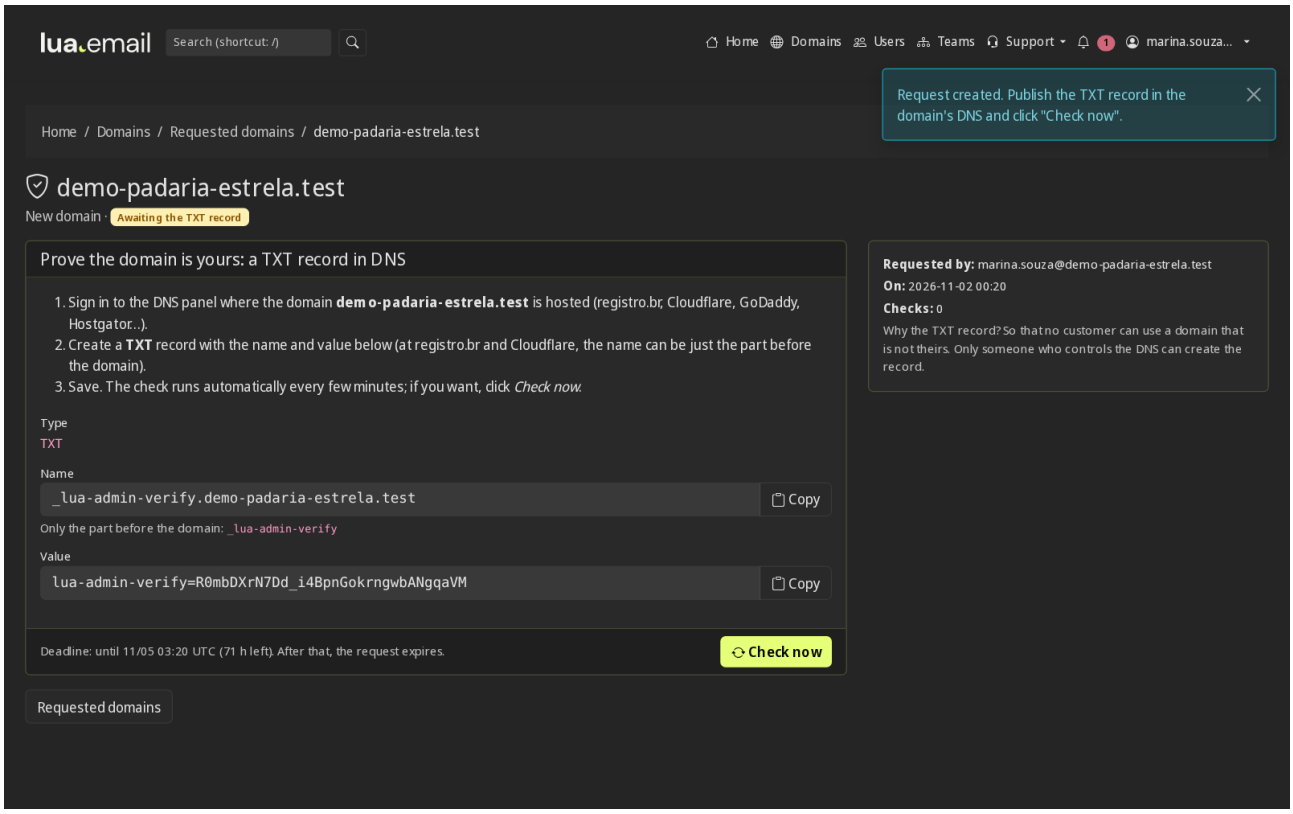


Figure 12: The TXT record that proves domain ownership.

The request is valid for **72 hours**. After that it expires and you need to request it again. Requests in progress are in **Domains → Requested domains**.

A domain that is already at Lua under another account

If the domain is already on the platform under another customer, the request becomes a **transfer**. The TXT record alone is not enough: the Lua team checks and approves it (or declines it, with the reason, which shows up for you on the request screen).

When to use the TXT request: when bringing the company's domain to Lua for the first time; when adding the domain of a branch or a new brand (afterwards, define who administers it with a team); and to take over a domain that was with another customer of the platform, in which case the request becomes a transfer and goes through Lua's check. The 72-hour window gives you time to publish the record without rushing: if you miss it,

simply request again.

With the domain active, its page is organized into tab groups: **Overview**, **Email** (mailboxes, aliases, alias domains, address books, service groups, devices and shares), **Authentication** (DKIM, DMARC and Validate DNS), **Delivery** (routing, access lists and training the filter) and **History** (statistics, logs and tracing).

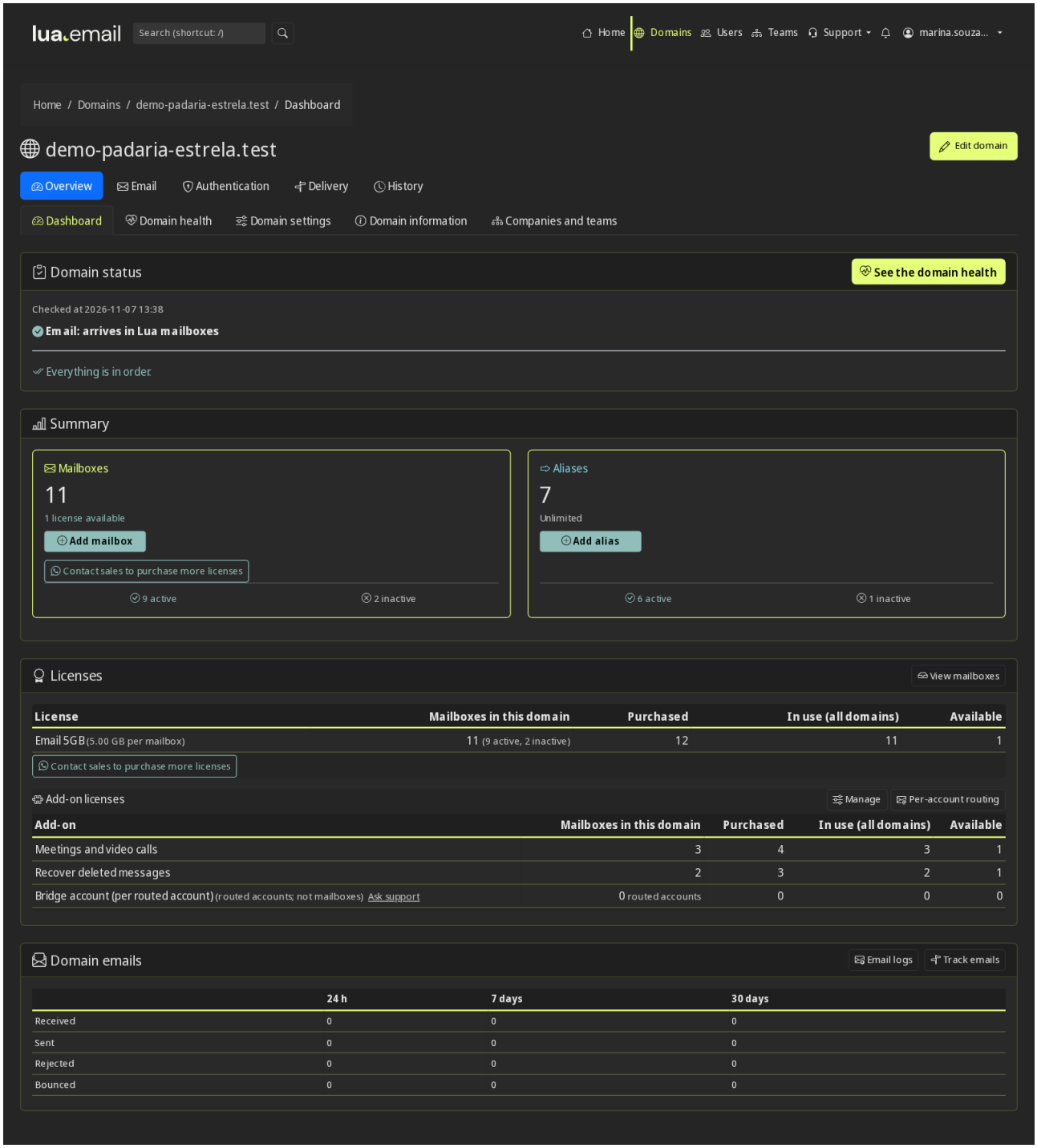


Figure 13: Domain overview.

Just changing the logo: the domain administrator changes the logo that shows after sign-in, in webmail and Colabora, under **Domains → the domain → Configure domain**, at no cost. See the step by step for the company logo.

Your brand on the webmail and Colabora: for the webmail and Colabora to open at your company's address (such as `webmail.yourcompany.com`), with its logo and colors, test the logo in the brand simulator and upload the.zip in the panel, under **Domain settings → Webmail with your brand** (step by step in chapter 15). The

simulator already builds the two addresses; the final DNS values appear in the panel. It is per domain and has no cost for now.

4. DNS: DKIM, DMARC and Autodiscover

For the domain to receive and send well, the DNS needs MX, SPF, DKIM, DMARC and Autodiscover and, for phones and email programs to find the server on their own, the two addresses `autodiscover.yourdomain` and `autoconfig.yourdomain` (Automatic email setup). The panel generates the values and checks whether they are published. The complete list of records, with examples, is in the DNS chapter of the webmail manual.

Who publishes the records depends on where the domain's DNS is hosted:

	DNS at Lua (at Edgium)	DNS at another provider
Email records	Automatic: DKIM, DMARC (Lua's default), SPF (adding Lua to what you already have), Autodiscover, the two A records of the automatic email setup (`autodiscover.yourdomain` and `autoconfig.yourdomain`) and, when the domain has an active mailbox, the MX. They go in as soon as the DNS becomes active at Edgium, through Bring my DNS to Lua or through the TXT with the name server change, and also through **Fix problems**.	The panel shows each record ready to copy, including the two A records `autodiscover.yourdomain` and `autoconfig.yourdomain`, with the value shown in the panel. You publish them at the provider where the DNS is.
DKIM signing	Turns on by itself when the check sees the right record.	Turns on by itself when the check sees the right record, after you publish it.
What you do	Approve the Fix problems preview, when it asks.	Copy the records, publish them and click **Check now** in Domain health.

DKIM

DKIM is the signature that proves the email really came from your domain. **Every new domain is created with its DKIM key already in place** (selector `luadkim`, 2048-bit key), with nothing for you to do. What is left is publishing the record in DNS:

1. On the domain page, open **Authentication → DKIM** (or **Domain health**). The panel shows the record ready to use: type TXT, name `luadkim._domainkey.yourdomain` and the value that starts with `v=DKIM1`. Use **Copy name** and **Copy value**.
2. Publish the record in the domain's DNS. Some DNS providers (Cloudflare, Registro.br and others) accept at most 255 characters per part of the value: when the value is longer than that, the panel also shows the value **split into parts, in quotes**, with the **Copy in parts** button. Splitting is normal and does not change the record.
3. Done. When the panel detects the record published with the right key, **signing turns on by itself** and you get a notice. With DNS at Lua, the record is already published for you.

A domain that already existed and has no key yet: open **Authentication → DKIM** and click **Set up DKIM** (or use the button the DKIM badge in Domain health points to). The panel creates the key and shows the record; from then on it is the same path: you publish it and signing turns on by itself. A domain that already had a key keeps it, with the selector it already used.

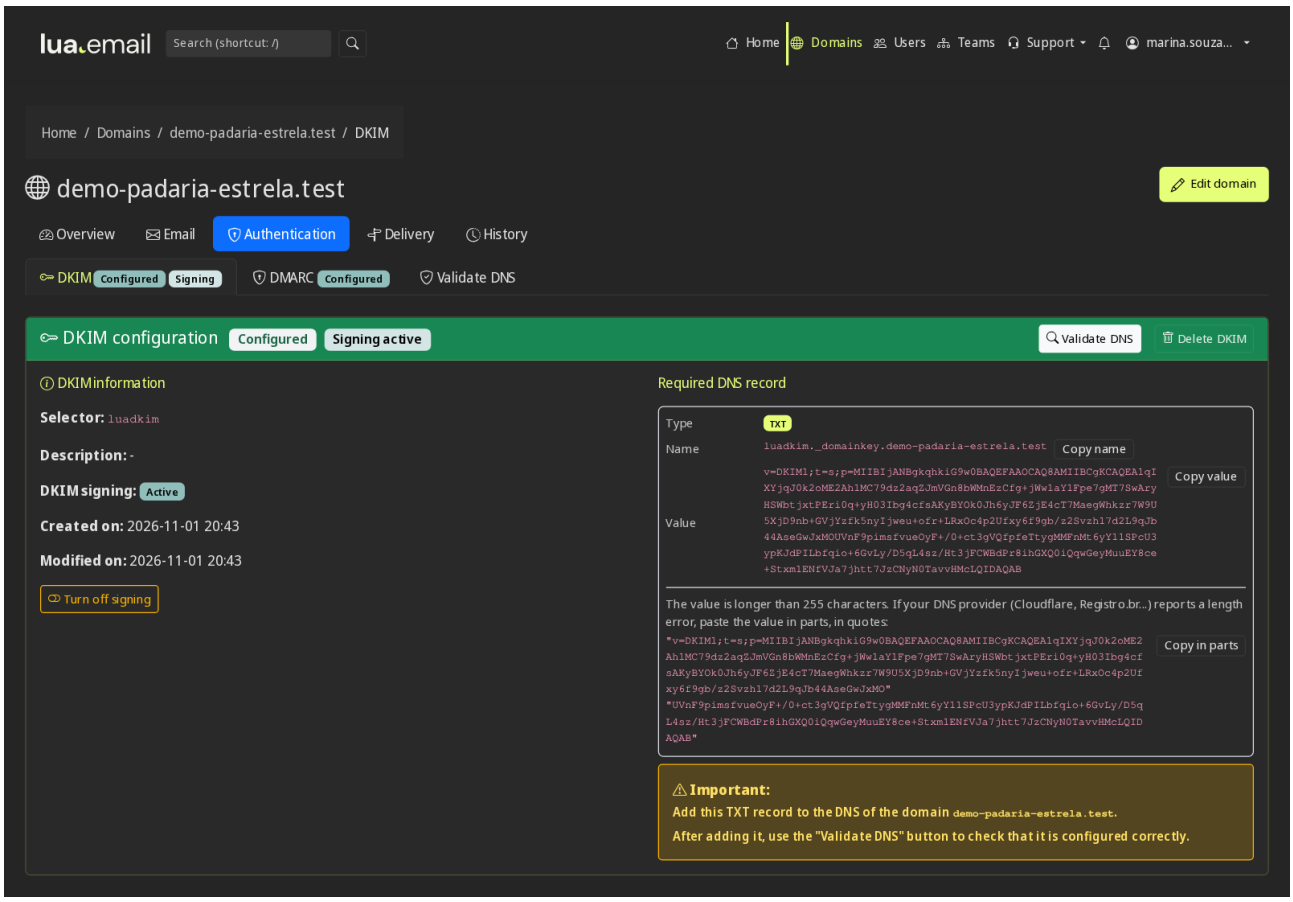


Figure 14: DKIM created: the record, ready to copy.

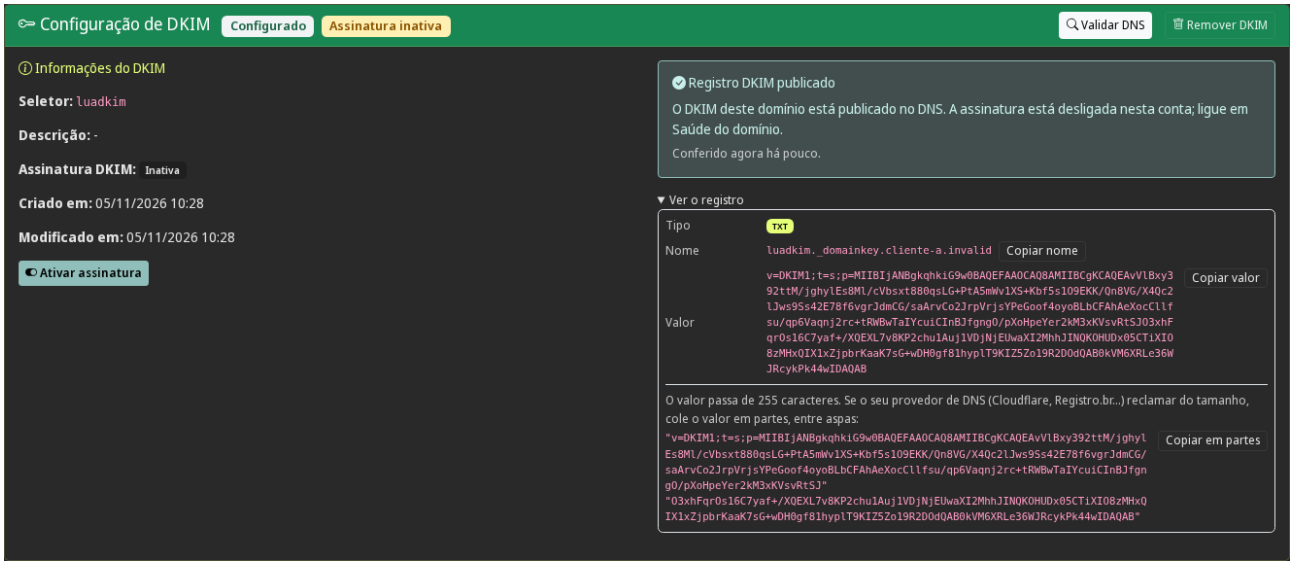


Figure 14 (continued): the DKIM tab when the record is already published in DNS with the right key (screenshot in Portuguese).

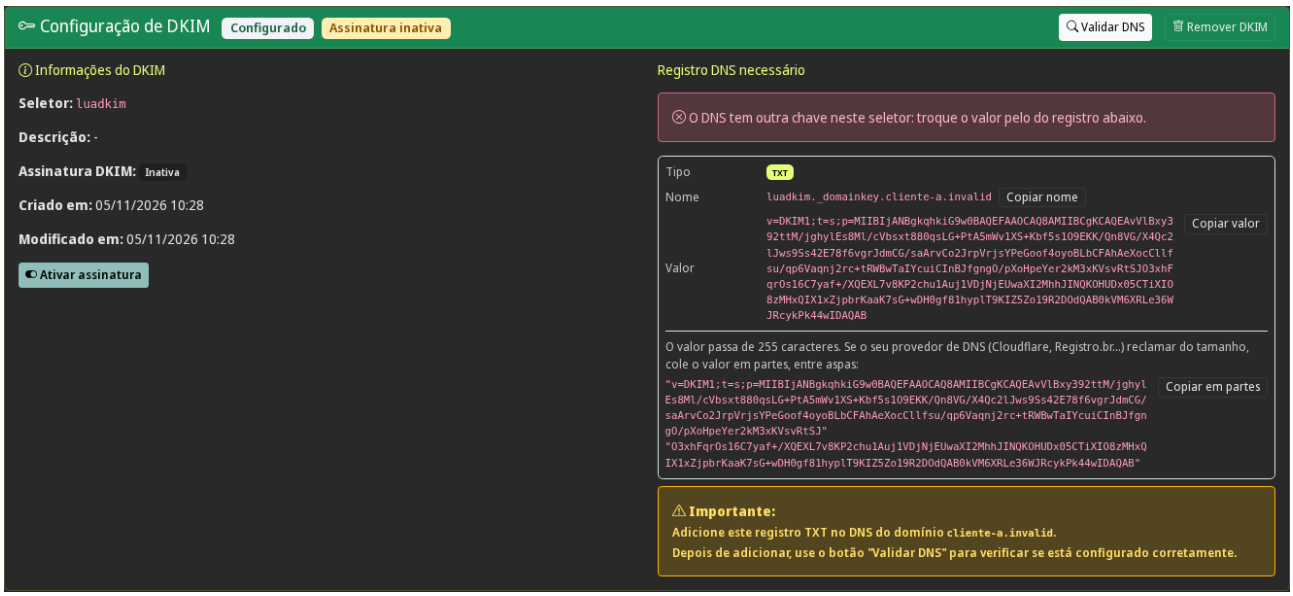


Figure 14 (continued): DNS has a different key on the selector; replace the value with the record shown (screenshot in Portuguese).

DMARC

DMARC tells other providers what to do with email that pretends to be from your domain, and asks for reports about it. Lua's default record, published at `_dmarc.yourdomain` (type TXT), is:

```
v=DMARC1; p=quarantine; adkim=r; aspf=r; pct=100; rua=mailto:reportdmarc@lua.email
```

- `v=DMARC1`: says this TXT is a DMARC record.
- `p=quarantine`: what to do with a message that fails the check. *Quarantine* means sending it to the recipient's spam folder, instead of delivering it normally or rejecting it.
- `adkim=r` and `aspf=r`: the DKIM and SPF check is *relaxed*: it also passes when the signing or sending domain is a subdomain of yours. It is the most common mode and the one with the fewest false alarms.
- `pct=100`: the policy applies to 100% of messages.
- `rua=mailto:reportdmarc@lua.email`: where the aggregate reports go. This address is created together with the domain.

The panel builds this record for you: it appears ready to copy under **Authentication → DMARC** (the DMARC badge in Domain health takes you there). With DNS hosted by Lua you copy nothing: it goes in by itself in Bring my DNS and in **Fix problems**.

Who decides, depending on where DNS is. With DNS on Edgium, when the panel sets up email (when you bring your DNS, in the automatic setup and in the **Apply** button), Lua's default replaces any existing DMARC. With DNS at another provider, the panel changes nothing: if your record is weaker than the default (for example, it only monitors, with p=none), the Domain health badge turns yellow ("DMARC only monitors") and the DMARC tab only **suggests** the recommended record, and the decision to change it is yours. Under **Authentication → DMARC → Edit configuration** you can also adjust the policy, the percentage and the reports. If other systems send email through the domain, first check that the SPF and DKIM of all of them are correct.

The **Authentication → DMARC** tab shows the real state of the record in DNS, right below the generated record:

- **Green, "All good: the DMARC record is published in DNS and protecting the domain."** Published with `quarantine` or `reject`.
- **Yellow, only monitors.** Published with p=none: the notice explains that the domain is not protected yet.
- **Yellow "Important: add this record".** There is no record in DNS: publish the one the tab shows.



Figure 14 (continued): DMARC tab with the record published and protecting the domain.

If the domain came from another provider and already has a DMARC record published in DNS, validation shows the **Import from DNS** button: the panel starts using the record that already exists, with the same policy, instead of starting from scratch.

Validate DNS

In **Authentication → Validate DNS**, the panel now queries public DNS and shows, for each record, whether it is correct. When something is missing, the record appears ready to copy. Use **Test again** after changing DNS: the change can take from a few minutes to a few hours to take effect.

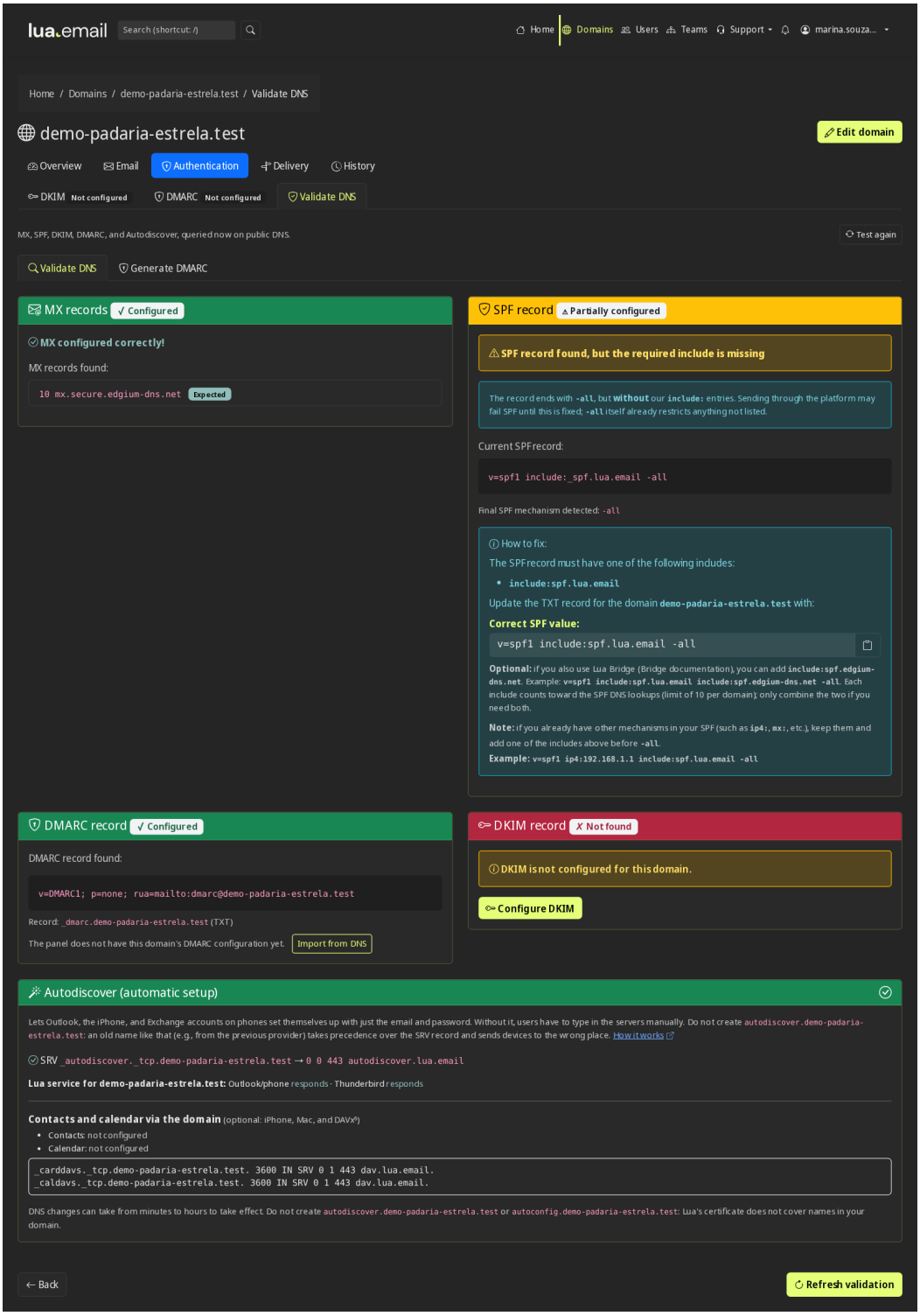


Figure 15: Validate DNS: each record shows its status and, if something is missing, the correct value.

Autodiscover: Outlook and phones set themselves up

Do not forget to create this record. Autodiscover is what lets the Exchange account (ActiveSync) on iPhone and Android, and Outlook, set themselves up. **Without it**, the phone cannot find the server and asks for the details by hand (`sync.lua.email`), classic Outlook on Windows cannot find the account, and support gets the "I can't set it up" request. Email itself works; only the automatic setup fails. Until the record exists, the person types the server: `sync.lua.email` on the phone's Exchange account and `mail.lua.email` in Outlook over IMAP (webmail manual).

The record is a single SRV per domain, with type SRV, name `_autodiscover._tcp.yourdomain`, priority 0, weight 0, port 443 and target `autodiscover.lua.email`. The panel shows the exact record and explains the fields your DNS panel usually asks for: service `_autodiscover`, protocol `_tcp`, priority 0, weight 0, port 443 and target `autodiscover.lua.email`.

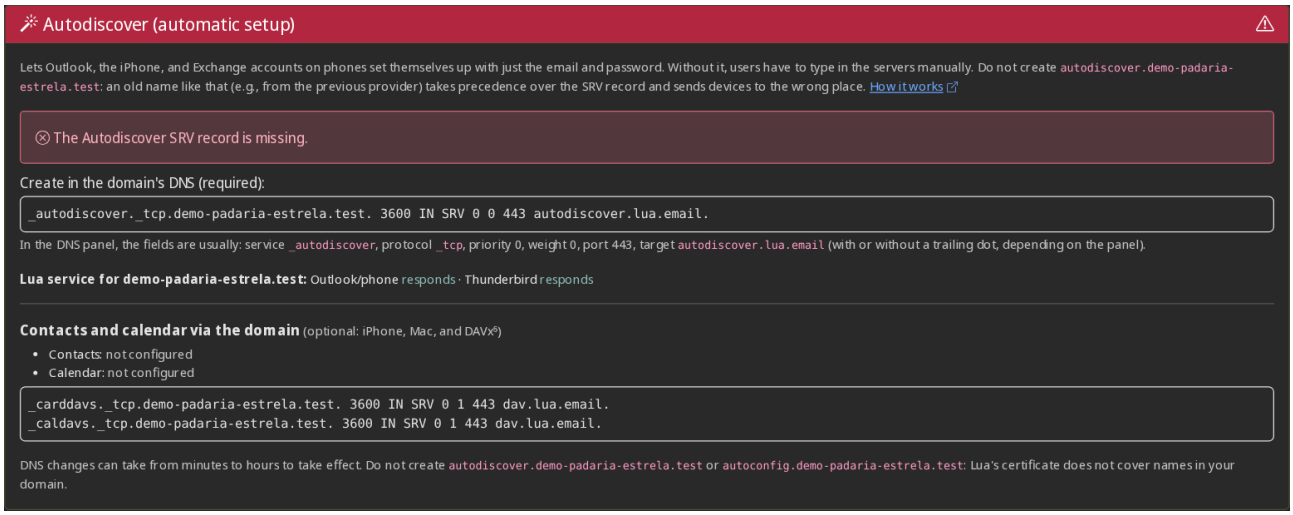


Figure 16: Autodiscover is missing: the panel shows what to create.

How to know it worked: in **Validate DNS**, the **Autodiscover (automatic setup)** box gets a green header and shows the SRV found. Red means the record is missing or points elsewhere. After creating it, wait a few minutes and use **Test again**. Outside the panel: `dig +short SRV _autodiscover._tcp.yourdomain` should answer `0 0 443 autodiscover.lua.email.`. If the domain's DNS is on Cloudflare, the SRV has no orange cloud (it is always "DNS only") and the target goes without the trailing dot.

The `autodiscover.yourdomain` and `autoconfig.yourdomain` addresses have a block of their own, the Automatic email setup, just below. If the domain already has these names pointing to the previous provider (Microsoft 365 or Google Workspace, for example), the panel warns you and only replaces them after you confirm.

Automatic email setup: autodiscover and autoconfig

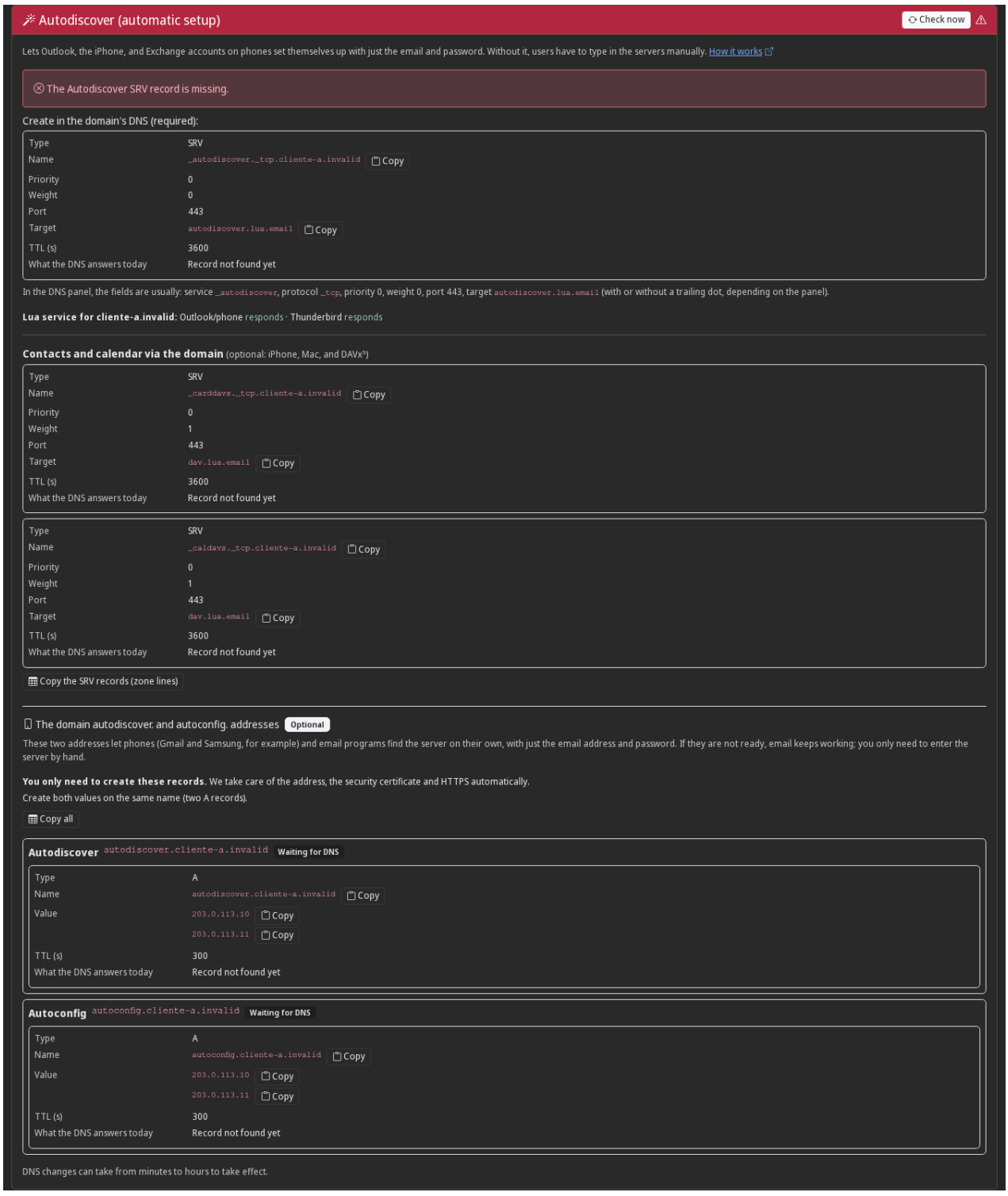
Phones (Android with an Exchange account, Gmail or Samsung) and email programs find the server on their own, with just the email address and password, when the domain has the `autodiscover.yourdomain` and `autoconfig.yourdomain` addresses. Everything is in one place: in the **Validate DNS** tab, in the **Autodiscover (automatic setup)** card, in this order: the explanation and the `_autodiscover._tcp` SRV record; **Contacts and calendar** (`_carddavs` and `_caldavs` SRV); and the `autodiscover.` and `autoconfig.` addresses, in the **Automatic email setup** block, marked **Optional**. All records (SRV and A) appear in cards, with their fields and the **Copy** button. **Check now** is in the card header.

Where the domain's DNS is	What happens
At Edgium	The panel writes the two A records to the zone and continues on its own. You do not have to do anything.
At another provider	The setup turns on by itself and the **Validate DNS** tab already shows the records. You create just the two A records (`autodiscover.yourdomain` and `autoconfig.yourdomain`), with the value exactly as it appears on the screen, each field with **Copy**. There is one card per name, with the **two values** (two A records on the same name). The address, the certificate and HTTPS are automatic.

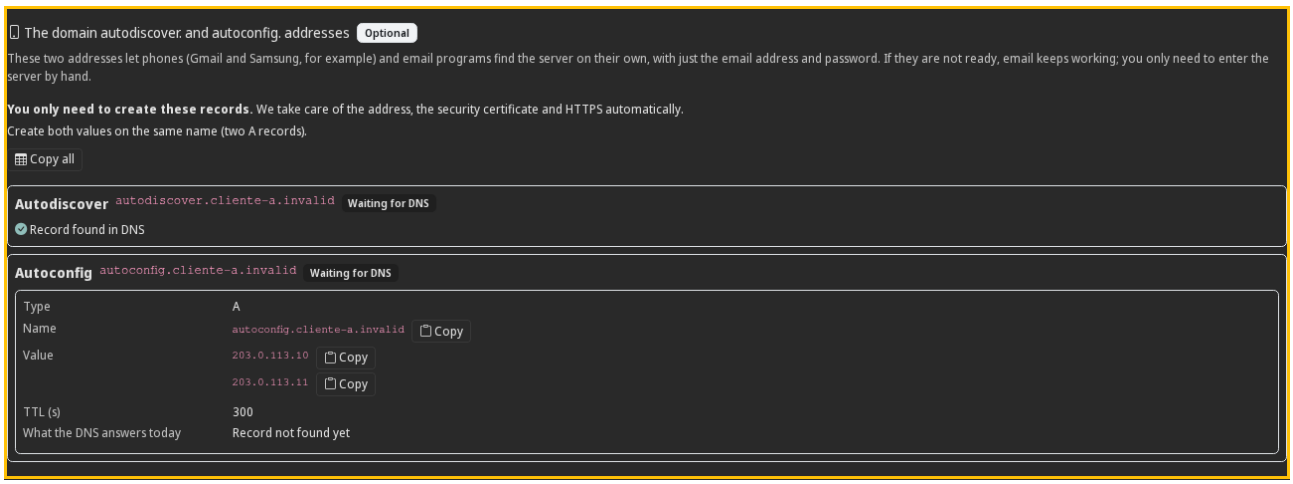
When it turns on by itself: with active DNS and a domain that has an active mailbox, no email migration in progress and outside Shield (the same conditions as the automatic MX). The first time, the screen may show **Preparing the records**, for about a minute. **Fix problems** also turns it on, and its window warns that the two addresses will be activated. **The Activate button** only exists when the domain has no active mailbox or has a migration in progress; the screen explains why, and a domain administrator clicks **Activate** when ready.

Nothing is created until the name answers for Edgium. The panel checks the public DNS (every hour, for 30 days; **Check now** reopens the period) and only then continues. When the DNS of a name already points to Lua, the record disappears from the list and **Record found in DNS** appears, and **Copy all** copies only what is missing. If the DNS stops pointing along the way, the block goes back to **Waiting for DNS**. If your DNS is at Cloudflare, leave the two A records as "DNS only" (gray cloud), so the name answers with the value shown in the panel.

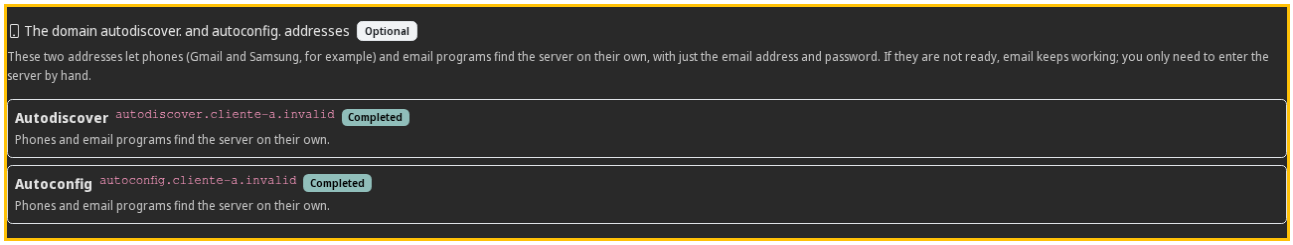
State	What it means
Waiting for DNS	The name does not answer for Edgium yet. With DNS at another provider, create the records in the card and use **Check now**. In the **What the DNS answers today** column you see **Pointing to Lua**, **Record not found yet**, **Not checked yet** or the place the record points to today.
Activating	We are setting up the address and the security certificate. It is automatic and usually takes a few minutes.
Completed	Phones and email programs find the server on their own.
Needs confirmation	The address already points somewhere else (an old email service, for example) and nothing was changed. A domain administrator confirms in a window (**Replace the current address?**, **Use the Lua address** button) for the panel to replace it. With DNS at another provider, you are the one who changes the record, and the panel warns that phones and programs using the old address will start using Lua.
Address already in use	This address is already used by another setup of yours. Nothing is changed, and the screen shows the **Open a ticket** button so our team can check.
Has a problem	We could not finish. The message is simple and the **Open a ticket** button already carries the domain and what happened. If the DNS still did not point after the deadline, the message says so and suggests **Check now** after you create the records.



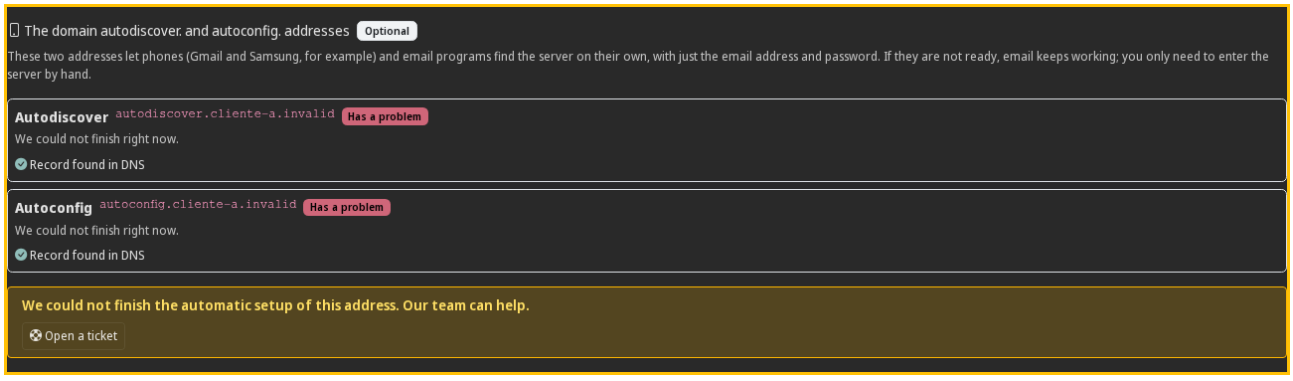
The Autodiscover (automatic setup) card in the Validate DNS tab: the SRV, Contacts and calendar and, last, the autodiscover. and autoconfig. addresses, with the value shown in the panel.



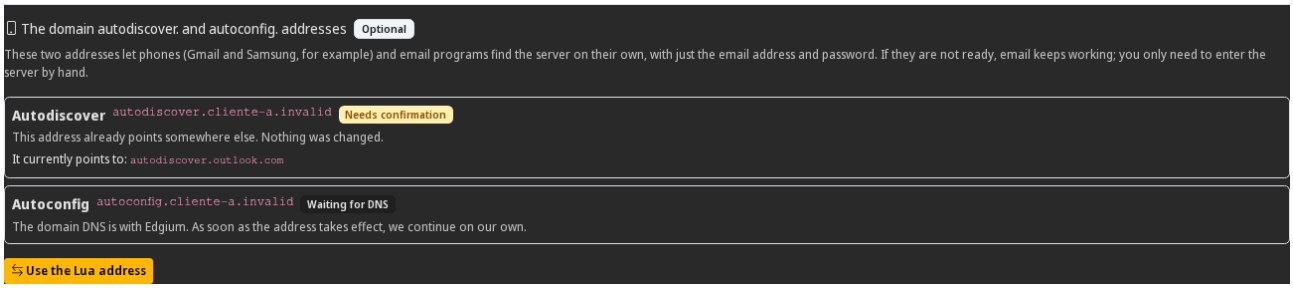
When the DNS of a name already points, the record disappears from the list and Record found in DNS appears.



Completed: phones and email programs find the server on their own.

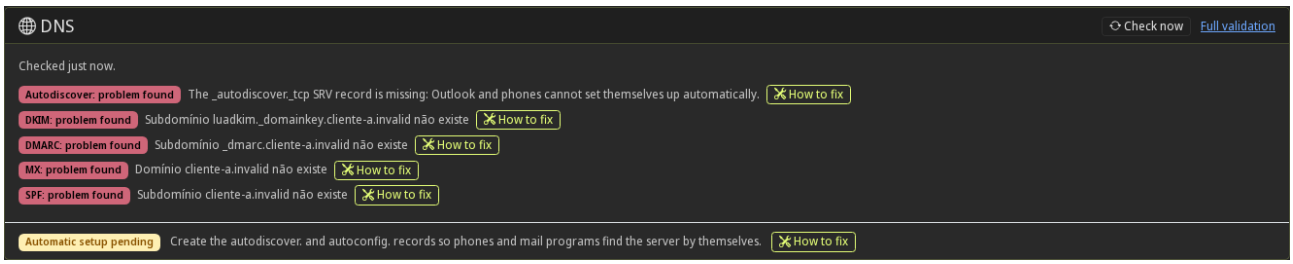


If there is an error, the panel shows a simple message and the Open a ticket button.



A record that already points somewhere else: the panel warns you and only replaces it after you confirm in a window.

In **Domain health** there is no large block: just one line in the DNS alert list, **Automatic setup pending** (yellow), **Automatic setup in progress** or **Automatic setup with a problem** (red), with **How to fix** (or **View progress**), which leads to the card in the Validate DNS tab. The line disappears when the setup is **Completed**. Because it is optional, it does not turn on the warning triangle in Domain health.



In Domain health there is just one alert line, with How to fix, which leads to the card in the Validate DNS tab.

Whoever can only read (helpdesk and read-only) sees the state but cannot act. **If it is not ready**, email keeps working; just enter the server by hand (`sync.lua.email` in the phone's Exchange account).

5. Creating mailboxes

Each mailbox uses one license from the plan you subscribed to. The license sets the mailbox size, so there is no quota field to fill in.

1. On the domain page, open **Email → Mailboxes** and click **Add mailbox**.
2. Type the part before the @ (the panel shows the full address), the person's full name and the password. The **Generate** button creates a strong password and **Copy** puts it on the clipboard, with the notice "Copied."
3. Choose the **license**. The list shows how many seats are left in each plan. If no license is available, the panel warns: "Without a license, the mailbox is created but only works after you assign a license to it." (see Mailboxes without a license).
4. Click **Create mailbox**. With a license, the mailbox can receive email and sign in to webmail right away. Without one, the panel says: "Mailbox created. It starts working when you assign a license."

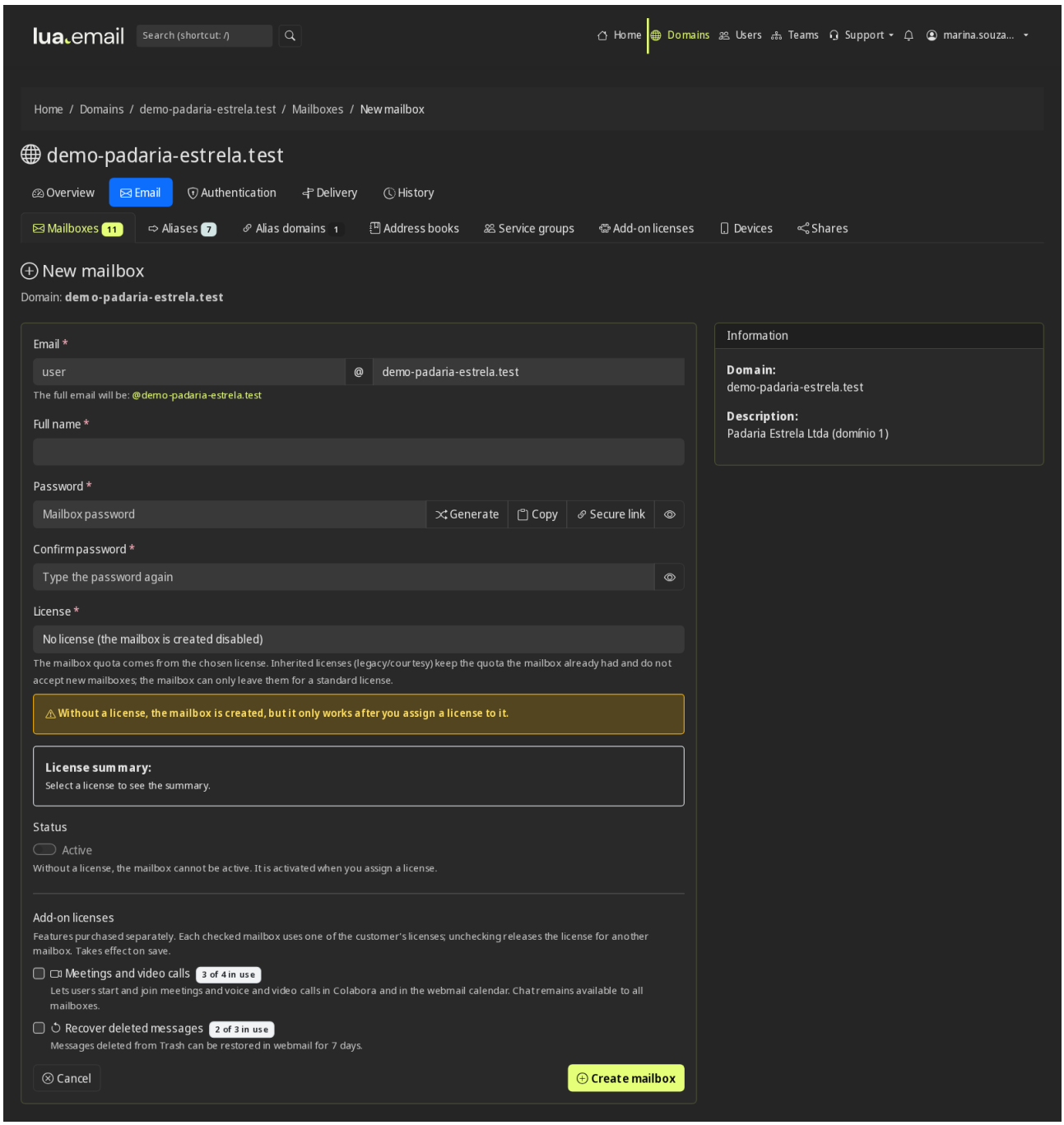


Figure 17: New mailbox: the chosen license sets the size.

The mailbox list shows, for each one, the name, the license, the status and the used space, email and drive combined. Above the table is the domain's license summary. The buttons on each row open the mailbox, edit it, **change the password** (the key), disable it or remove it. The key appears for the administrator and the domain's helpdesk, and only on active mailboxes; read-only users do not see it.

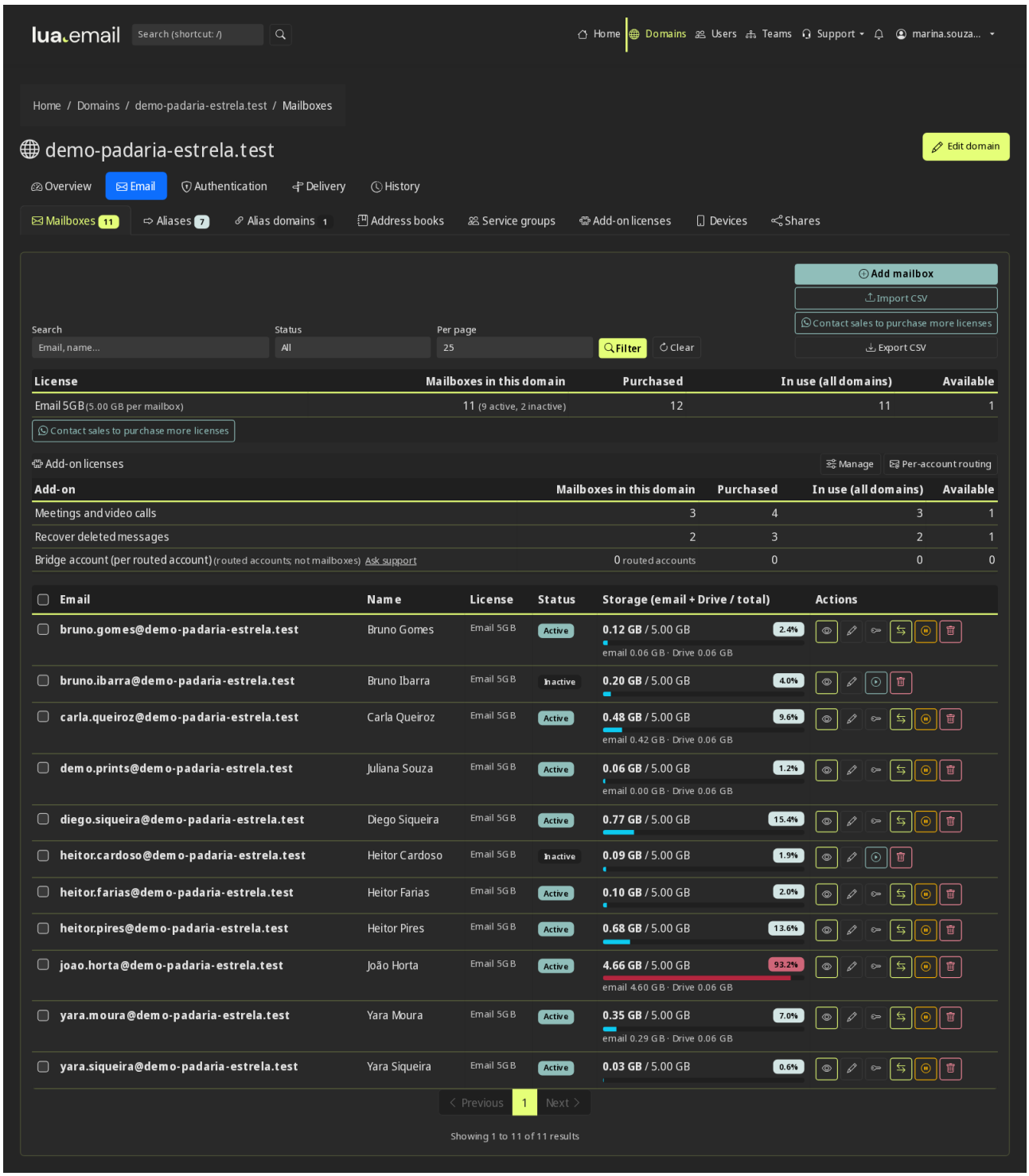


Figure 18: The domain's mailboxes, with each one's space.

Creating many mailboxes at once

In **Import CSV**, upload a file with the columns `email`, `name` and `password` (separated by commas or semicolons). With an empty password, the panel generates a strong one and shows it at the end, only once. Before creating, a preview lists what will be done and marks the rows with problems (an address that already exists, a license with no seat): those are left out. Aliases can be imported this way too.

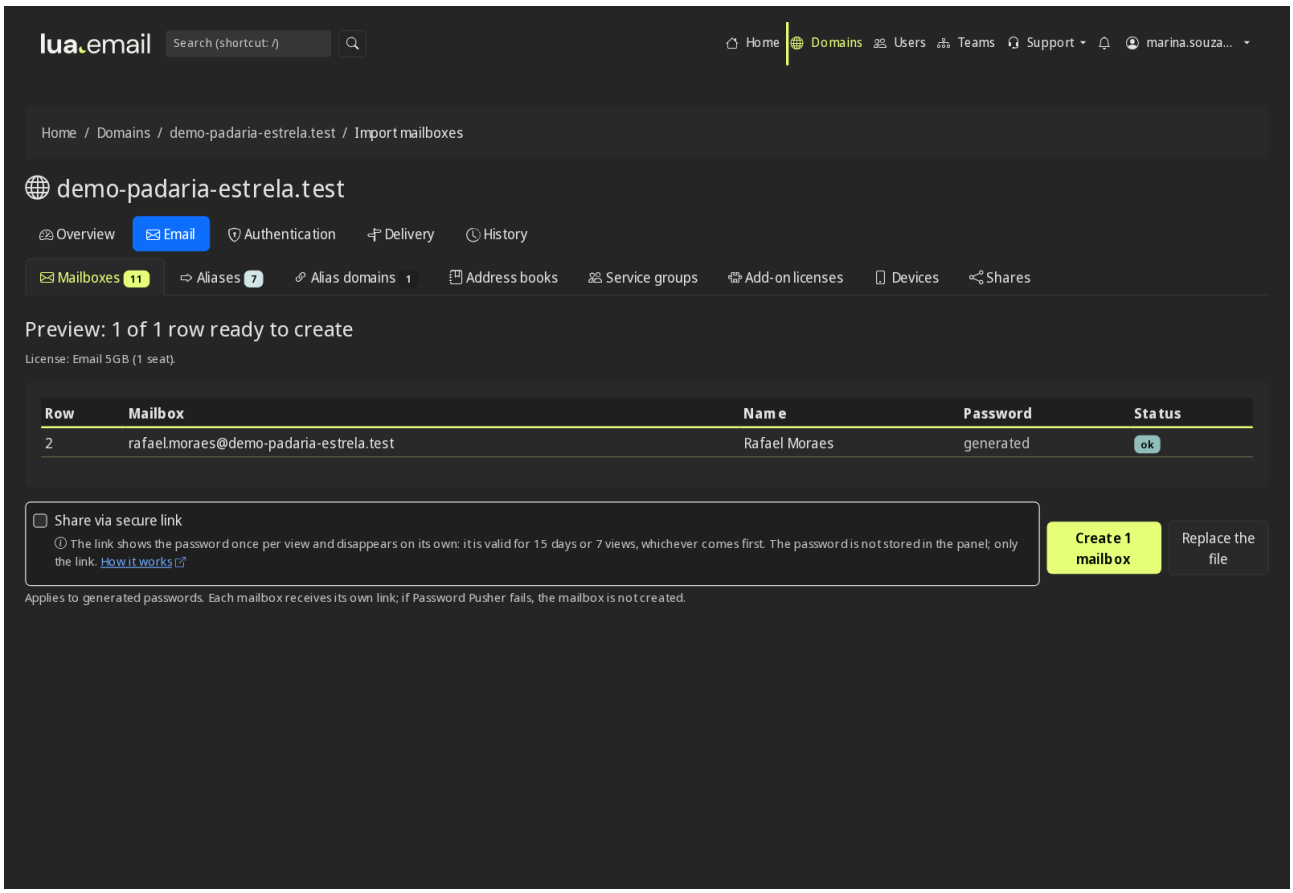


Figure 19: Import preview: nothing is created before you confirm.

The **Export CSV** button downloads the domain's mailbox list, useful for checking licenses and space in a spreadsheet.

Swapping the license between two mailboxes

When one mailbox needs more space and another one on the same domain uses less than its license offers, the two can **swap licenses**: the one with the 1 GB license gets the 5 GB one and the other keeps the 1 GB one. No license is bought or released, and each mailbox's quota changes along with the license. The swap is done by the **domain administrator**; view-only users and the helpdesk do not see the button.

1. In the **Mailboxes** list, click the **Swap license with another mailbox** button (the two arrows) on the mailbox's row. The same **Swap license with another mailbox** button is also on the mailbox page.
2. Pick the other mailbox in the search. The list shows only active mailboxes of the same domain with a different license.
3. Check the **Today → After the swap** table: license, quota, usage (email + Drive = total) and how full each mailbox is, calculated with today's usage, and the **What changes** list.
4. With the **Within the quota** (green) or **Quota nearly full** (yellow) badge, click **Swap**. Both mailboxes use the new license right away.

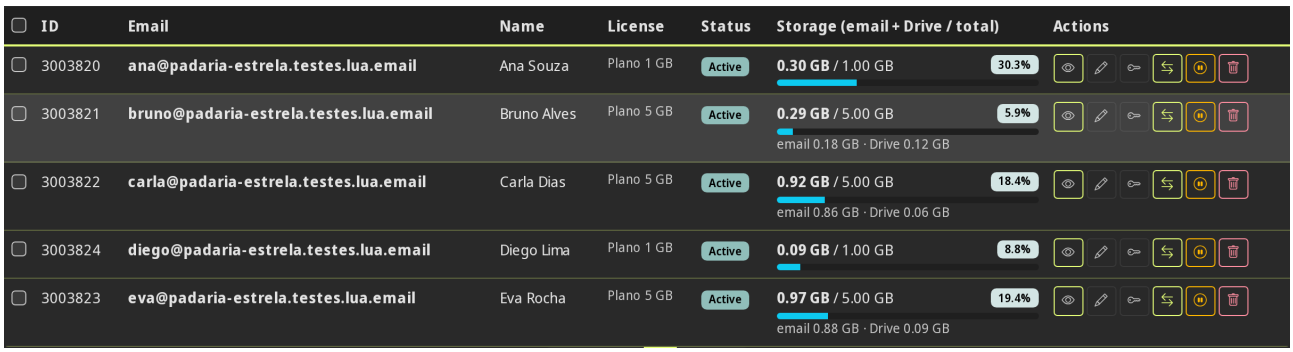


Figure 19 (continued): the Swap license button on every row of the mailbox list (real screen, fictional data).

The rules. Mailboxes of the same domain only, both active, each with a different mailbox license. Usage counts email plus Drive, and the mailbox moving to the smaller license needs room in the new quota:

- up to 90% of the new quota: "Within the quota" badge (green);
- from 90% to 95%: the swap is allowed, with the yellow "Quota nearly full" badge;
- above 95%: the swap is blocked. The panel says why and how much to delete: "delete messages or files until usage is below X";
- above 100% of the new quota: the swap is blocked too.

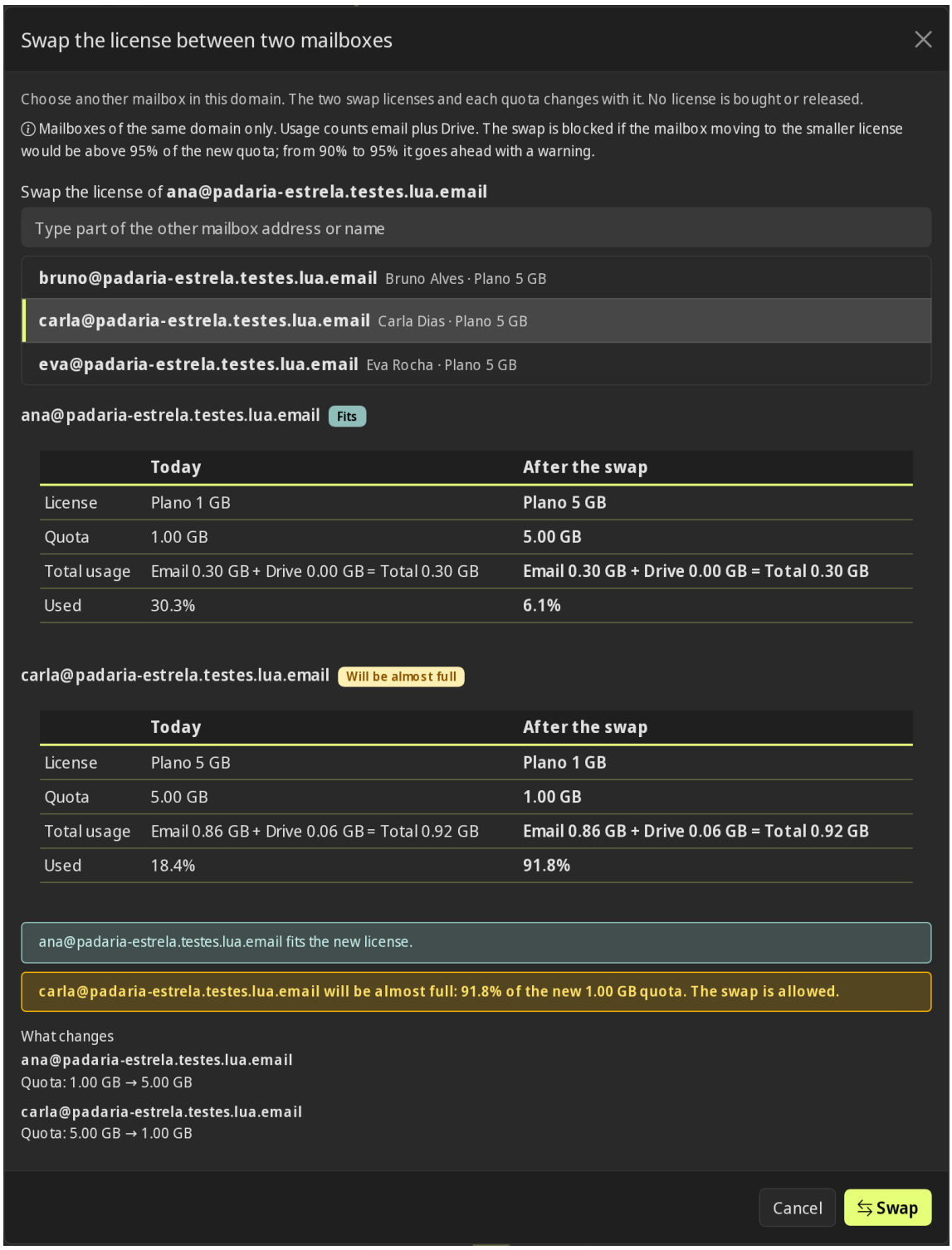


Figure 19 (continued): from 90% to 95% the swap is allowed, with a yellow warning (real screen, fictional data).

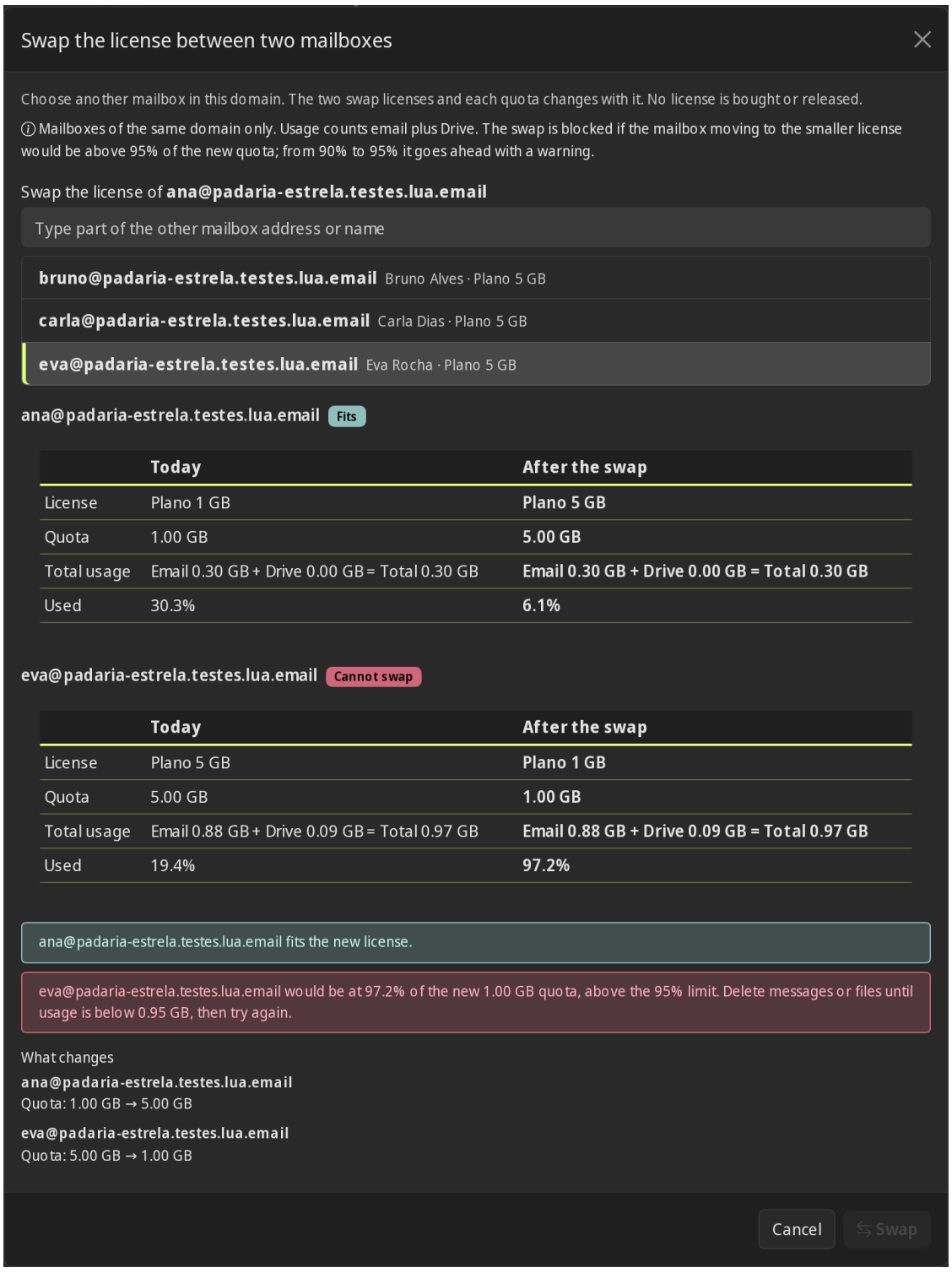


Figure 19 (continued): above 95% the Swap button is disabled and the panel explains what to delete (real screen, fictional data).

The panel checks everything again at the moment of the swap, with that moment's usage. If one of the mailboxes fills up after you open the window, the swap is refused with the reason and nothing changes. If you click twice, the second attempt only says the swap was already done. Each swap is recorded in the panel history, with who did it, when, the licenses before and after and each mailbox's usage.

After the swap, the mail server and Colabora use the new quota on their own. The mail server keeps the quota for up to 1 hour, so the new limit of the mailbox that gained space can take that long to apply.

Mailboxes without a license

You can create a mailbox even when no license is available. It is created with the **No license** status and is completely deactivated: it neither sends nor receives email and cannot sign in to the webmail, email programs or the phone. The mailbox is always activated by the domain administrator, by assigning a license to it: first you buy the license, then you assign it to the mailbox.

1. In **Add mailbox**, fill in the details as usual. When no license is available, the panel warns: "Without a license, the mailbox is created but only works after you assign a license to it." On the mailbox list, the notice reads: "You have no licenses available. New mailboxes only work after you buy and assign a license."
2. Click **Create mailbox**. The panel confirms: "Mailbox created. It starts working when you assign a license."
3. On the **Mailboxes** list, the mailbox shows the **No license** badge, no space (a dash in place of the quota) and the **Assign license** button next to it. The panel explains: "This mailbox does not have a license yet, so it does not send or receive email. Assign a license to it." The same button is on the mailbox page.
4. To get licenses, use the **Purchase licenses** button (on other panel screens, the button is called **Purchase more licenses**). It opens the ordering portal, where you choose the mailboxes and pay by PIX or boleto. The step by step for buying is in Subscribe to more mailboxes and add-ons, in the billing portal manual. If you buy through our team, the button is **Contact us to sign up for more licenses**: it opens a pre-filled support ticket, and our team places the order with you.
5. After payment, the new license shows up as available in the panel. **The mailbox stays with No license**: payment does not activate it.
6. With a license available, click **Assign license** and choose one of the free licenses. Each option shows the **total quota (email + Drive)** and how many seats are left.
7. Click **Assign and activate**. The license, the quota and the activation happen together, right away, and the panel confirms with "License assigned: the mailbox was activated".

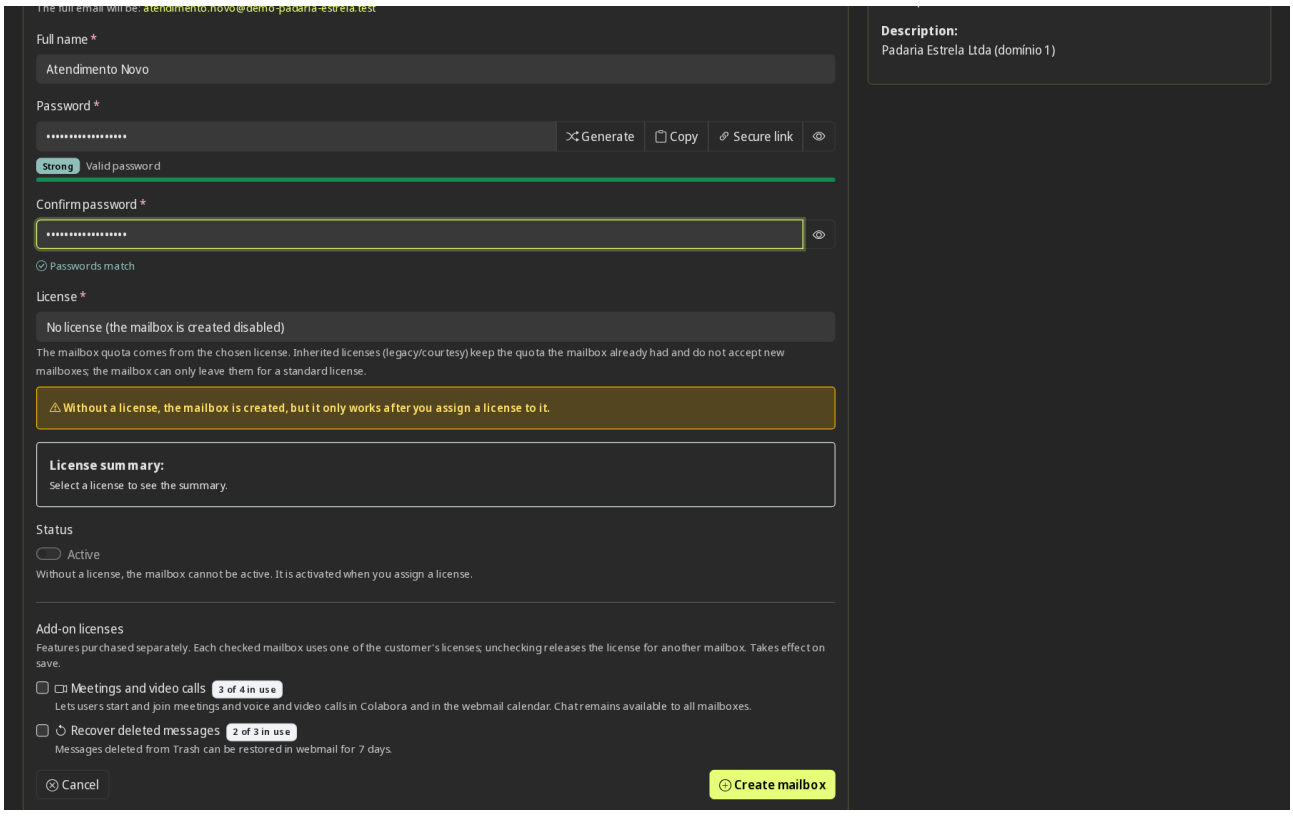


Figure 19 (continued): when you create a mailbox with no license available, the panel warns that it only works after a license is assigned (real screen, sample data).

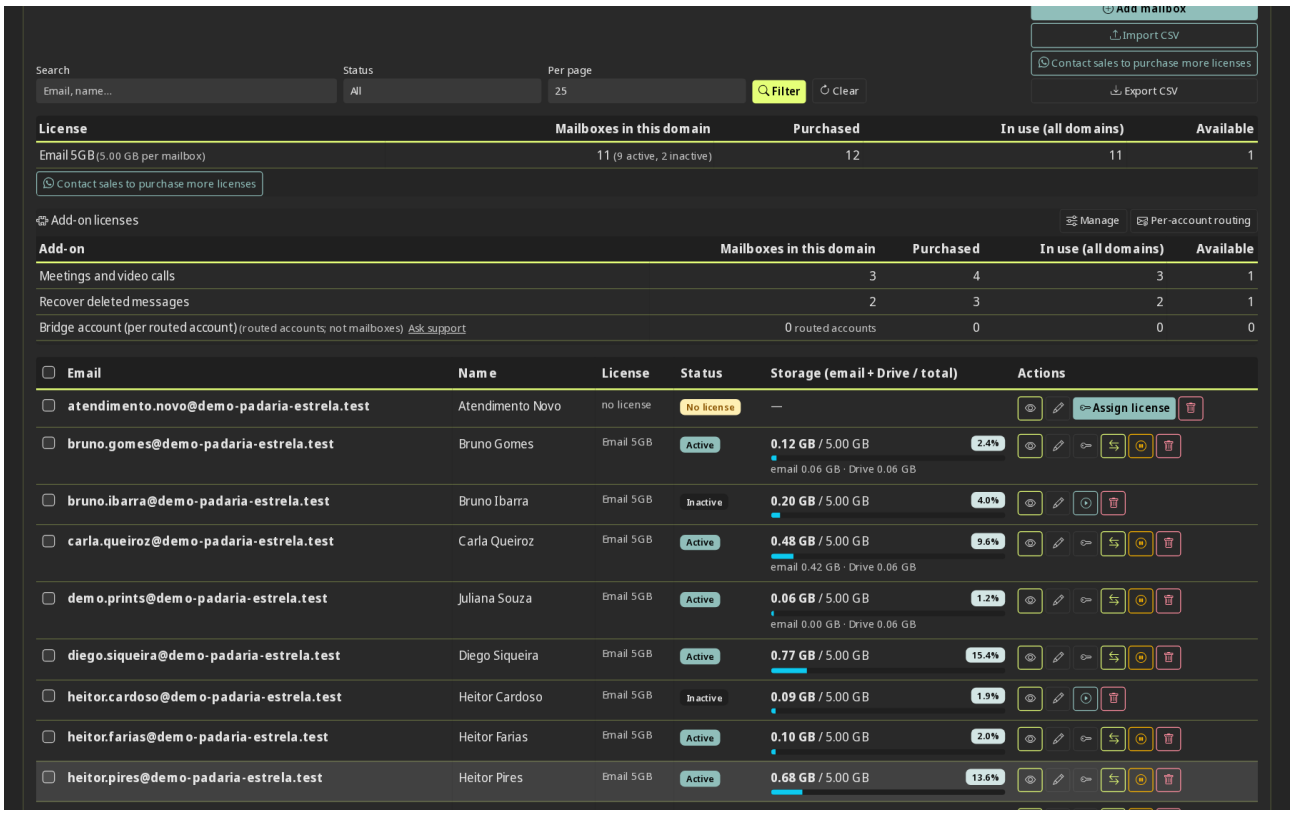


Figure 19 (continued): the mailbox without a license in the list, with the Assign license button (real screen, fictional data).

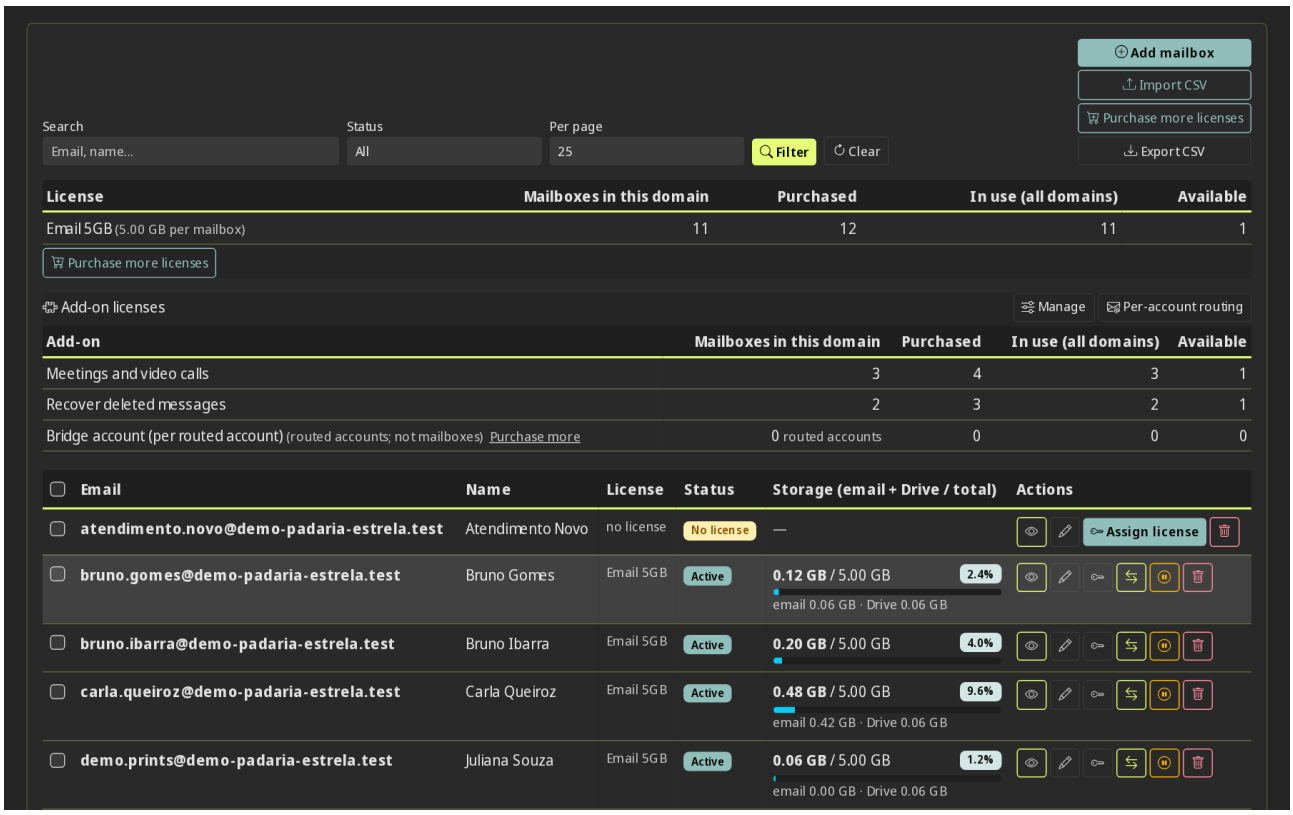


Figure 19 (continued): after you buy and pay, the license shows up as free in the summary (Available), and the mailbox stays with No license until you assign the license to it (real screen, fictional data).

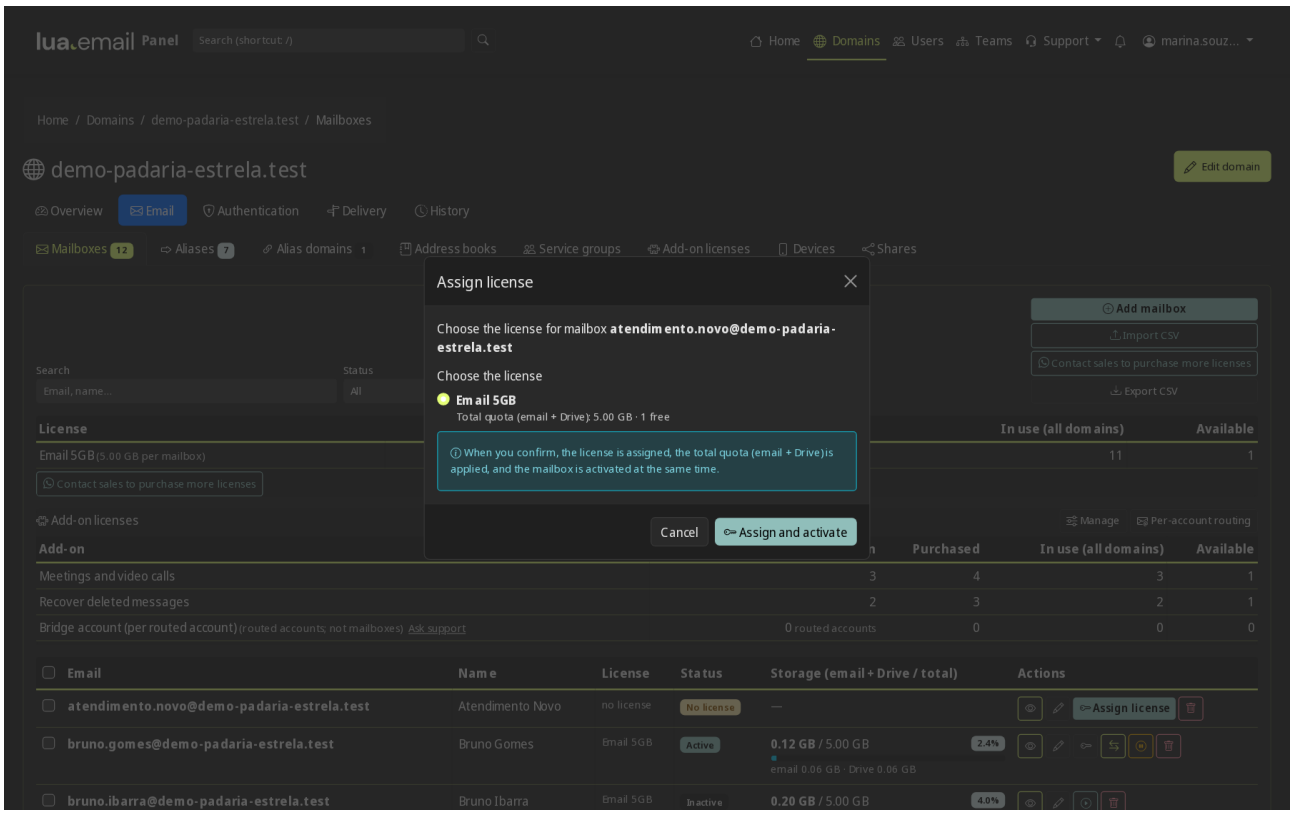


Figure 19 (continued): when assigning, the window shows the total quota (email + Drive) of each free license (real screen, fictional data).

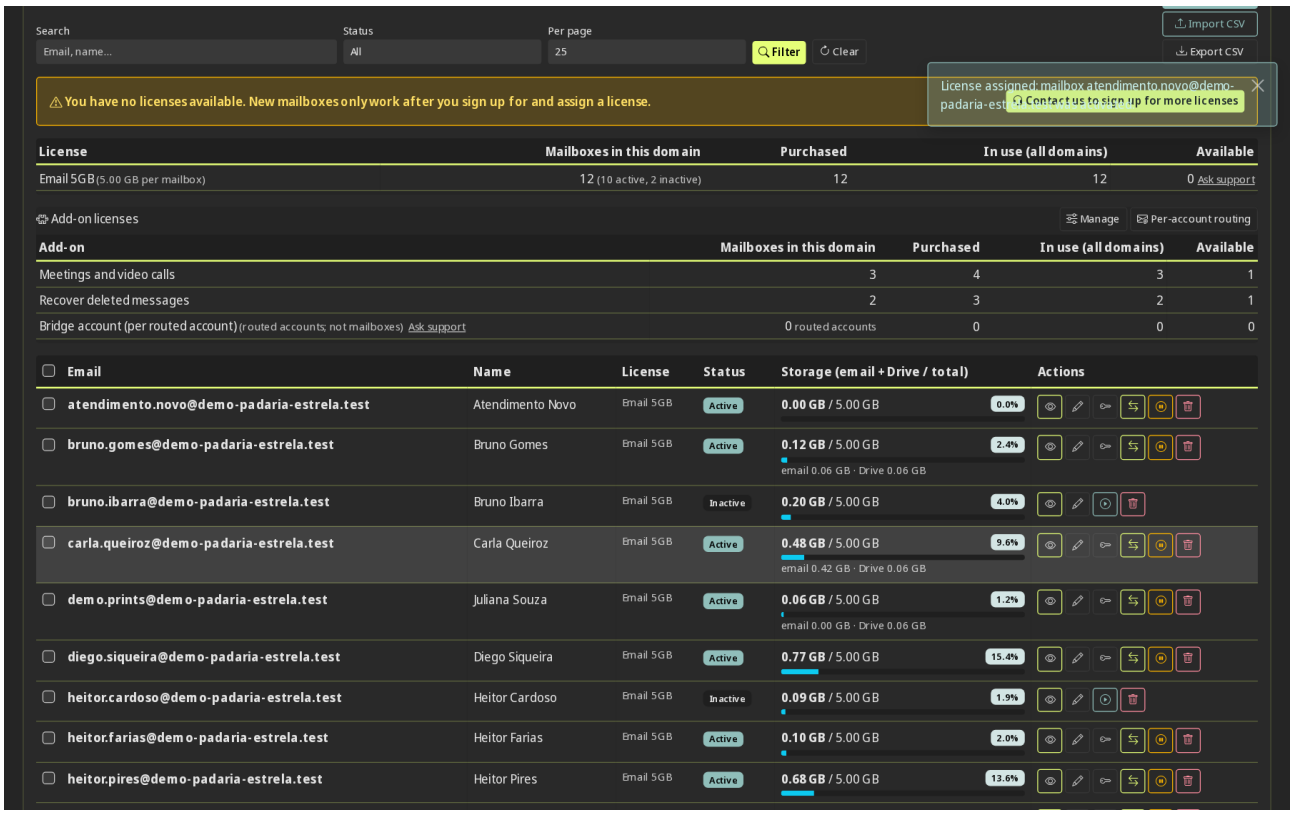


Figure 19 (continued): after assigning, the mailbox is active and takes one seat of the license (real screen, fictional data).

The rules.

- **A mailbox without a license is created disabled** and stays disabled until it receives a license. It does not send or receive email and cannot sign in to webmail, programs or the phone.

- **Only assigning a license activates the mailbox.** A mailbox without a license has no Activate button, and CSV import, the API and every other path also refuse to activate it. The way is always **Assign license**.
- **The quota is the total.** The limit that comes from the license covers email and Drive together, and the mailbox starts using it as soon as it is activated.
- **A mailbox with a license cannot be left without one.** You can switch its license to another one, or swap with another mailbox, but you cannot remove the license.
- The domain administrator assigns the license. Support and read-only profiles only see the mailbox and the badge.

6. Editing a mailbox

Click the mailbox address to see everything about it: status, used space (email and drive separately), how many messages it received, sent and had rejected in 24 hours, 7 and 30 days, connected devices, shares and the access history.

Finding a mailbox in the list. The search field in the **Mailboxes**, **Aliases** and **Per-account routing** lists, and the field that adds mailboxes to a service group, show suggestions as you type (from 2 letters). Use the arrows and Enter, or click the result; **Esc** closes the list. If no suggestion fits, Enter filters the list by the text you typed.

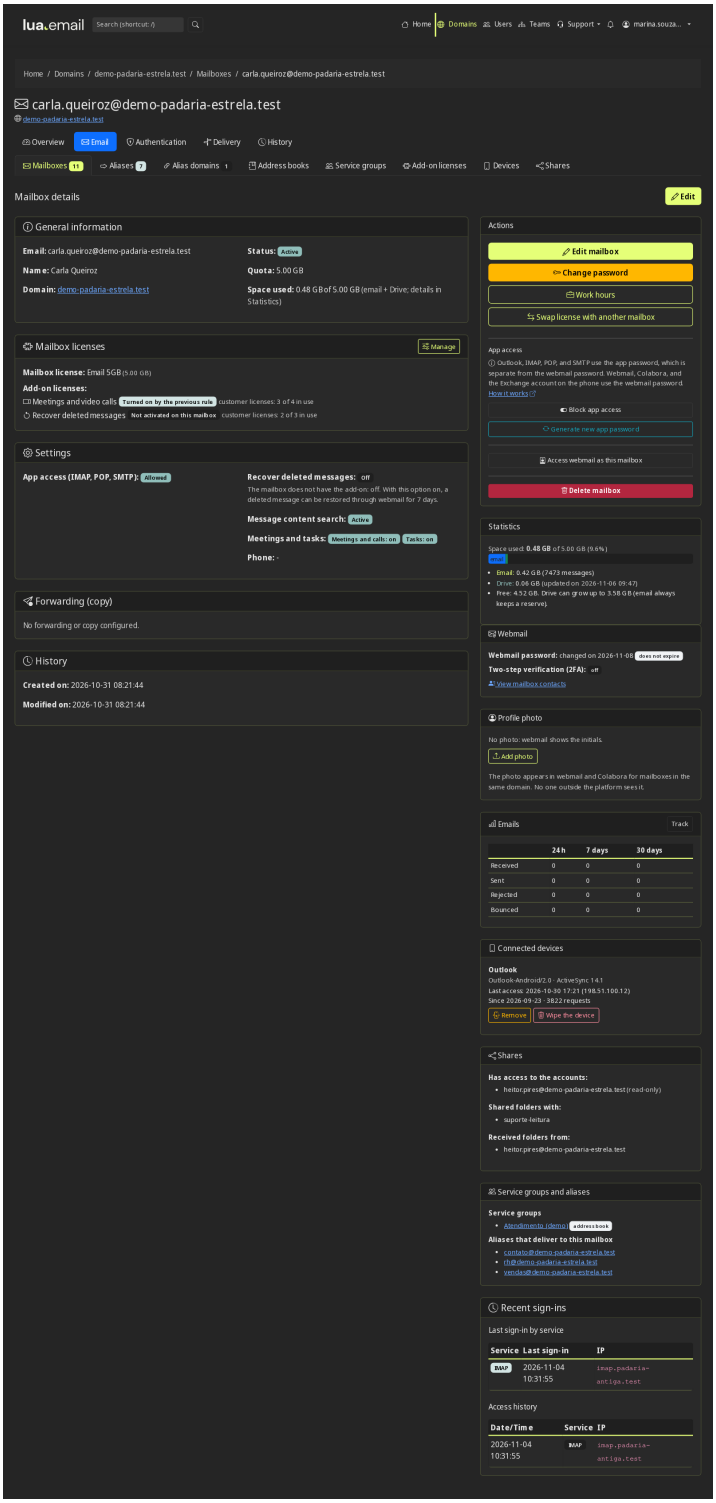


Figure 20: The mailbox page.

On the same page, the **Service groups and aliases** box shows which service groups the mailbox is in and which aliases deliver to it, with a link to each. The **out for now** tag appears when the mailbox is in a group but is disabled: it stays in the group and comes back on its own when it is re-enabled.

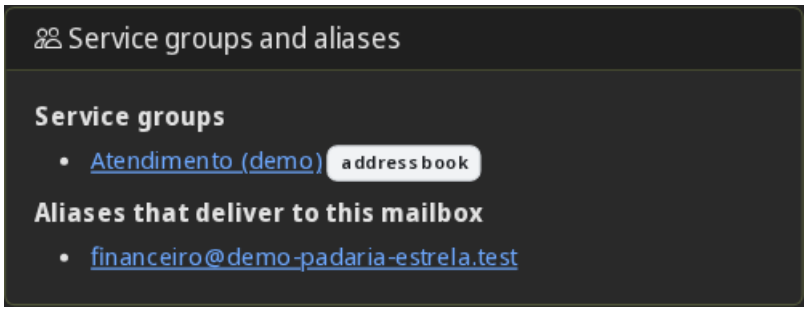


Figure 21: A mailbox's groups and aliases, with links.

In **Edit mailbox** you change:

- **Full name** and phone.
- **License:** this is where you change the mailbox's plan (see below).
- **Only senders from the same domain:** the mailbox only receives from people in the domain. Messages from outside are rejected. Good for internal-use mailboxes.
- **Tasks:** turns the tasks panel on or off, when the mailbox's license includes the feature.
- **Add-on licenses:** video meetings and calls, and recovery of deleted messages, one checkbox for each feature (see below).
- **Forwarding (copy):** addresses that receive a copy of everything that arrives at the mailbox. There can be several internal ones and at most one external one.
- **Status:** disabling blocks access and delivery, but the mailbox still takes up the license.

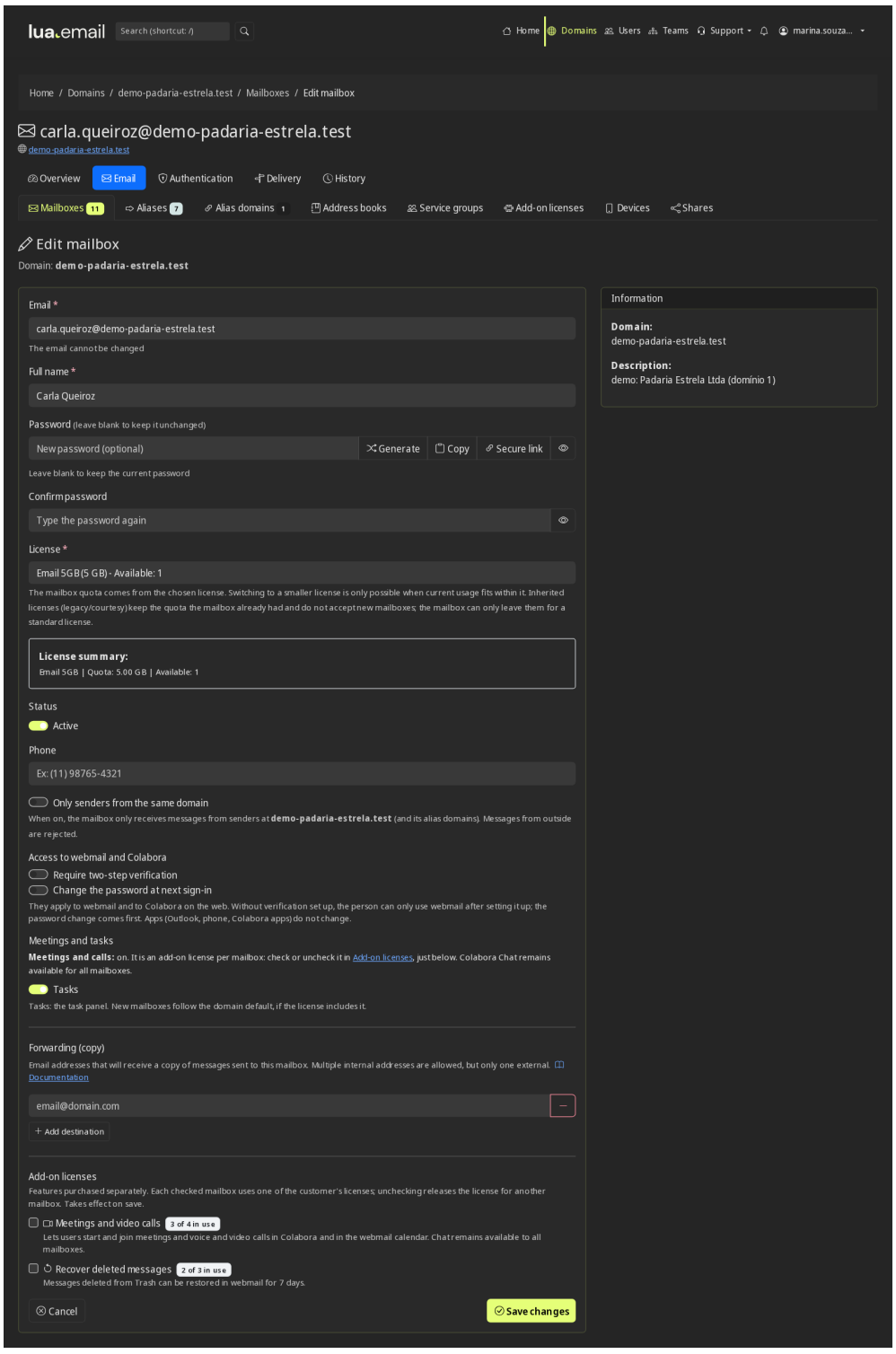


Figure 22: Editing the mailbox.

Changing a mailbox's plan (license)

Choose the new license in the **License** field and save. The mailbox size changes right away. For a smaller plan, current usage (email plus drive) needs room in the new quota. The new license needs a free seat: if a plan's seats have run out, talk to sales to subscribe to more.

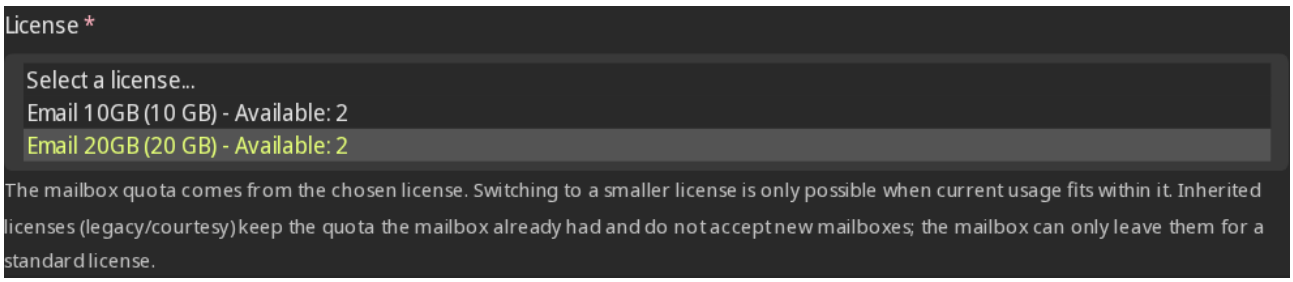


Figure 23: Changing license: the list shows each plan's seats.

Changing the mailbox password

Scam alert: lua.email never asks for your password or your two-step verification code. If someone asks, it is a scam: do not share it and contact support.

Use **Change password** when the person forgets the password. This is the webmail password. You get there in two ways: the key on the mailbox row in the list, or the **Change password** button on the mailbox page. Both open the same window, in two steps, without leaving the screen you are on.

1. **Save.** Type the new password and the confirmation (the **Generate** button creates a strong one and **Copy** puts it on the clipboard). The password must have at least 8 characters, with an uppercase letter, a lowercase letter, a number and a special character. The option **Ask the person to change the password at the next webmail sign-in** comes checked. If you want to send the password by link, check **Share by secure link after saving** and choose the expiry, the views and, if you like, a secret phrase. Click **Change password**.
2. **Get the link.** Only after the password is saved does the window move to the second step. If you checked the link option, it appears with the **Copy** button and the text ready to send. Without the link, the window closes and the panel says the password was changed.

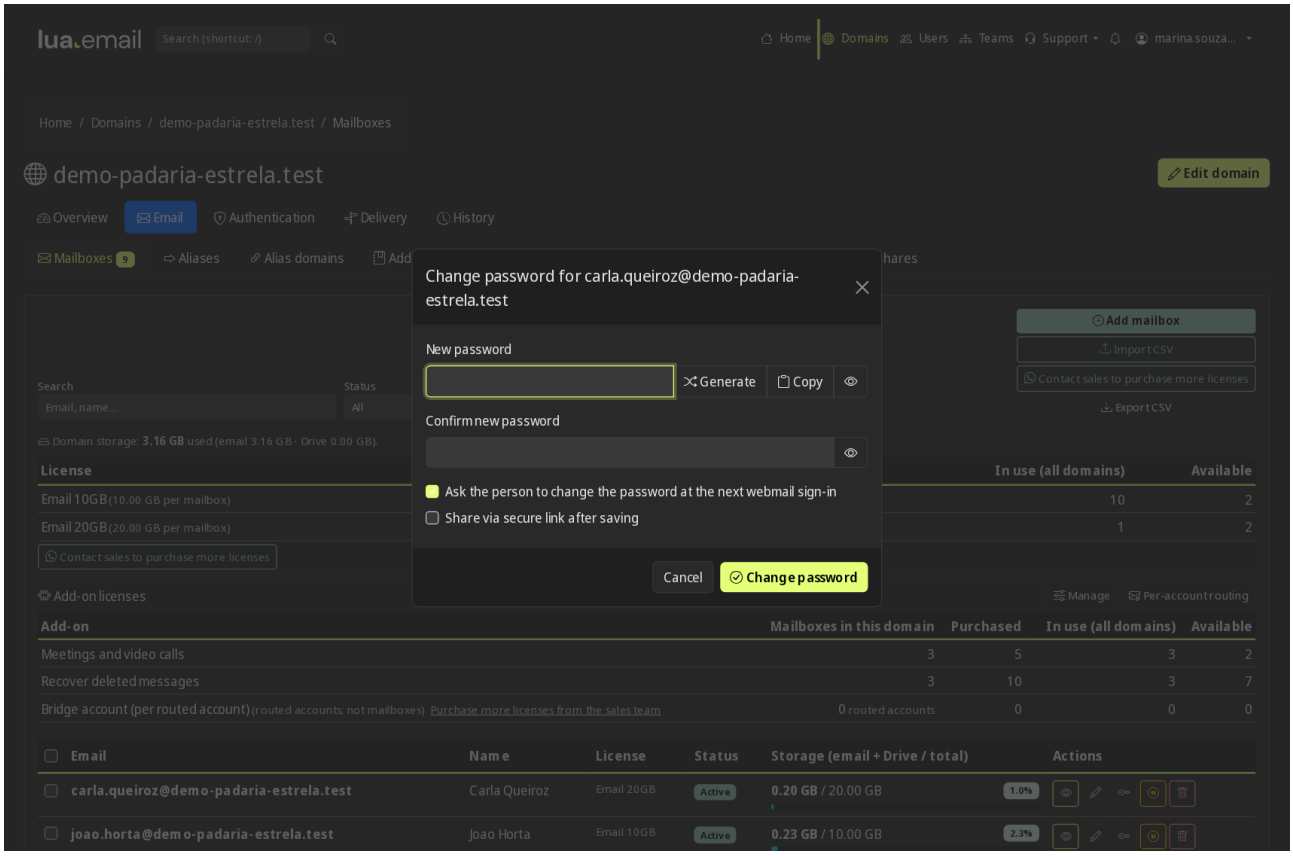


Figure 24: Change password: the first step, without leaving the mailbox list (real screen, fictional data).

The link is only created after the password is saved: that way it never opens a password that is not yet valid. If the secure link service does not respond right then, the password is still saved. The window says the password was changed, that the link was not sent and that nothing was created, and offers **Try creating the link again**. If you close without having copied the link, the panel warns you once; the link does not appear again after it is closed.

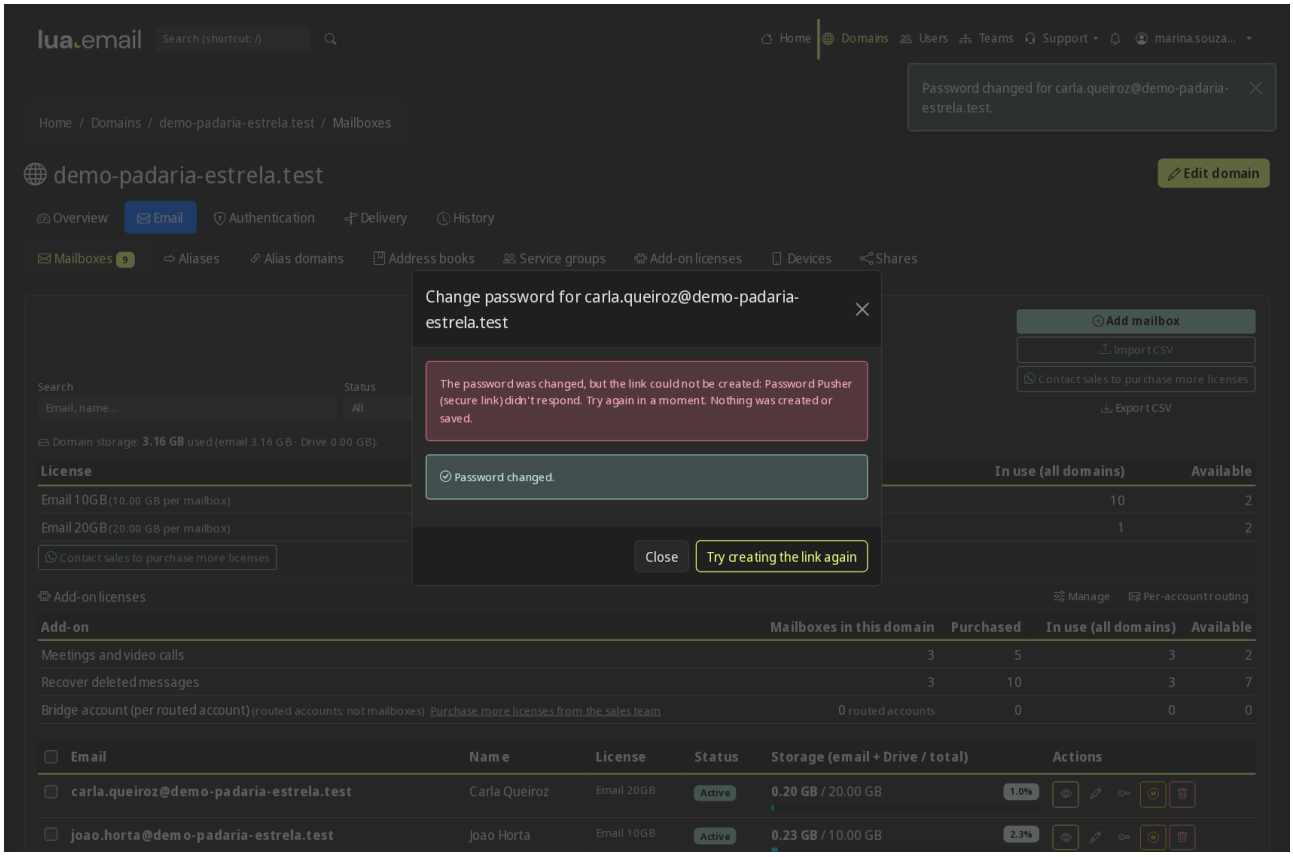


Figure 25: If the secure link service is down, the password stays changed and you can try the link again (real screen, fictional data).

App password (Outlook, phone, IMAP, POP and SMTP)

Email apps use their own password, separate from the webmail password. If someone finds out the Outlook password, they cannot get into webmail, and vice versa.

1. On the mailbox page, under **App access**, click **Generate new app password** and confirm.
2. The password appears only once. Write it down or give it to the person right away: afterwards it cannot be shown again, only another one generated.
3. Generating a new password invalidates the previous one: apps configured with it ask for the new password.

If the mailbox is in a webmail-only group, the mailbox page shows the controls disabled with the group's name.

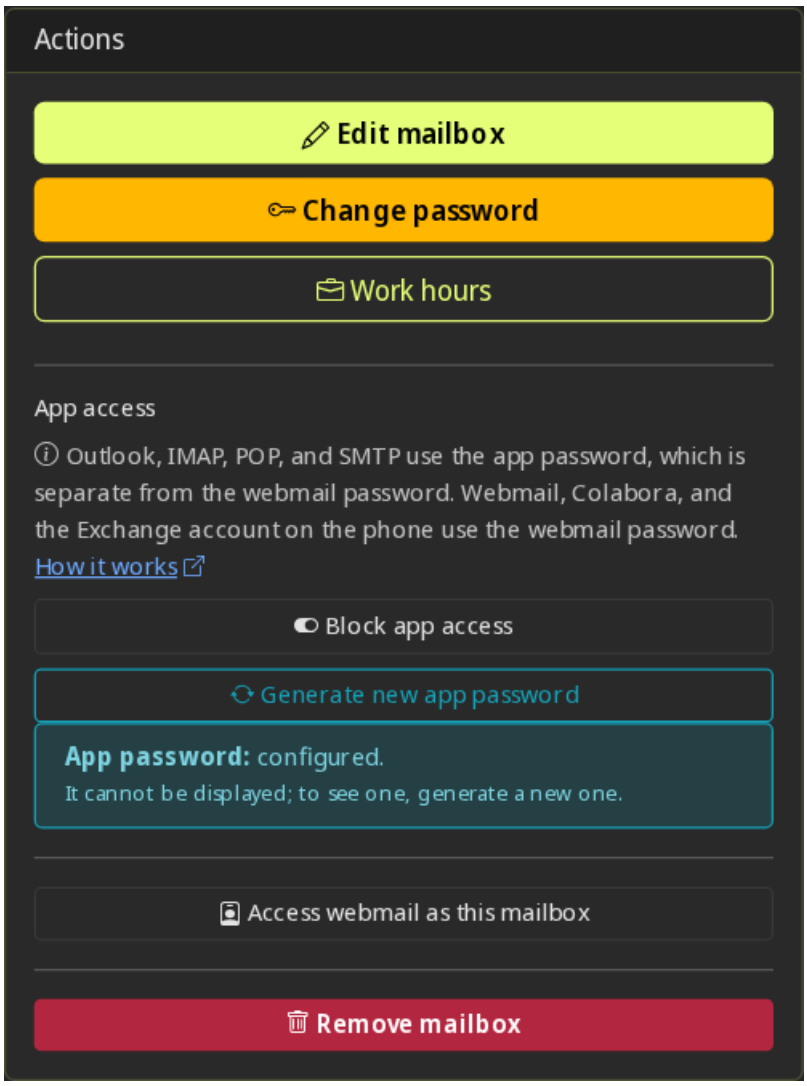


Figure 26: Generating the app password.

Sending the password by secure link

Next to every password the panel shows (the mailbox password when creating or resetting, the app password and a panel user's password), the **Share by secure link** button opens a single window to create a lua.email Password Pusher link, at pwpush.lua.email. On the mailbox password change, the link is part of the window itself (see above). On the other screens, if the password has not been saved yet, the window tells you to save before sending the link.

- The link is valid for **15 days or 7 views**, whichever comes first. You can lower that and require a secret phrase.
- In the window you choose the expiry (1, 3, 7 or 15 days), the views (1, 3, 5 or 7) and, if you like, the **secret phrase**, which the person types when opening the link. Send the phrase through another channel, not in the same message.
- The panel shows the link with the **Copy** button and a text ready to send to the person. **The link does not appear again after you close the window**: if you did not copy it, create another.
- The password does not go in the email or in WhatsApp: whoever receives it opens the link, clicks to view and can delete the link right away. After it expires, the content is deleted.
- The panel log records who generated the link and for which account, never the password.

The same service works for other sensitive data, outside the panel. See what else the secure link is for.

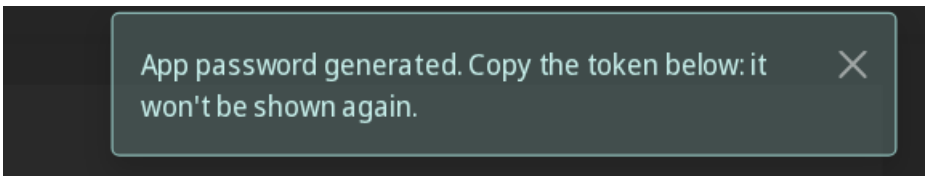


Figure 27: The password appears only once, with the notice "Write down the password below: it will not be shown again." Sample password.

Block app access stops the mailbox from being used in apps and phones (IMAP, POP and SMTP), keeping webmail. To turn it back on, use **Allow app access**.

Add-on licenses per mailbox

Two features are subscribed separately and turned on mailbox by mailbox. Colabora Chat remains available to all mailboxes; what needs a license is what comes beyond it:

Add-on license	What the mailbox gets
Video meetings and calls	Start and join voice and video meetings and calls in Colabora and in the webmail calendar (the "Online meeting"). The price is R$ 3.00 per mailbox, per month.
Recover deleted messages	Restore messages deleted from Trash through webmail, for 7 days.

Two-step verification required. With the requirement on, on the mailbox or the group, the person cannot turn off verification or remove the last method in webmail. To switch methods, they add the new one and remove the old one.

Only with Colabora on. Add-on licenses only appear in domains where Colabora is on. Without it, the domain's **Add-on licenses** tab, the add-ons block in **New mailbox** and **Edit mailbox**, the **Manage** button on the mailbox card and the summaries on Home and Mailboxes disappear; the plan license stays. Turning Colabora off does not delete anything: whatever was active reappears when it is turned back on, and the license keeps counting as in use in the meantime. Without Colabora, meetings stop; recovery of deleted messages keeps working for those who already have the license.

Where to see them. The license summary on **Home** and on **Mailboxes** shows, for each add-on license, how many were subscribed, how many are in use and how many are left. On a mailbox page, the **Mailbox licenses** card says which is the plan license and which add-ons are active, with the **Manage** button.

License	Quota	Purchased	Allocated	Available
Recuperar mensagens apagadas (7 dias)	per-mailbox add-on	10	3	7
Reuniões e chamadas de vídeo	per-mailbox add-on	5	3	2
Email 10GB	10 GB	12	10	2
Email 20GB	20 GB	3	1	2

Figure 28: Add-on licenses appear in the license table, with what was subscribed and what is in use (real screen, fictional data).



Figure 29: The Mailbox licenses card on the mailbox page (real screen, fictional data).

How to turn them on and off, one mailbox at a time. In **New mailbox** and in **Edit mailbox**, the **Add-on licenses** block has a checkbox for each feature and the counter **x of y in use**, which adds up all the company's domains.

Check it and save, and the mailbox starts using a license. Uncheck it and save, and the license is freed for another mailbox. On a new mailbox, the feature is turned on right after the mailbox is created.

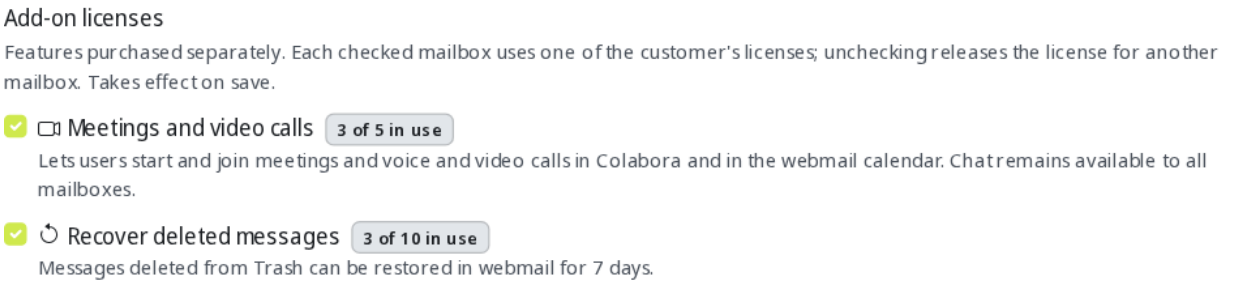


Figure 30: Edit mailbox: one checkbox per feature, with the usage counter (real screen, fictional data).

On many mailboxes at once. In **Email → Add-on licenses** there is a table with all the domain's mailboxes and a column for each feature. Use the search, the **Show** filter and the header checkbox to **select all** mailboxes on the page. Nothing changes until you click **Review and save**: the panel lists each activation or deactivation and the total that will be used, and only saves after **Confirm and save**.

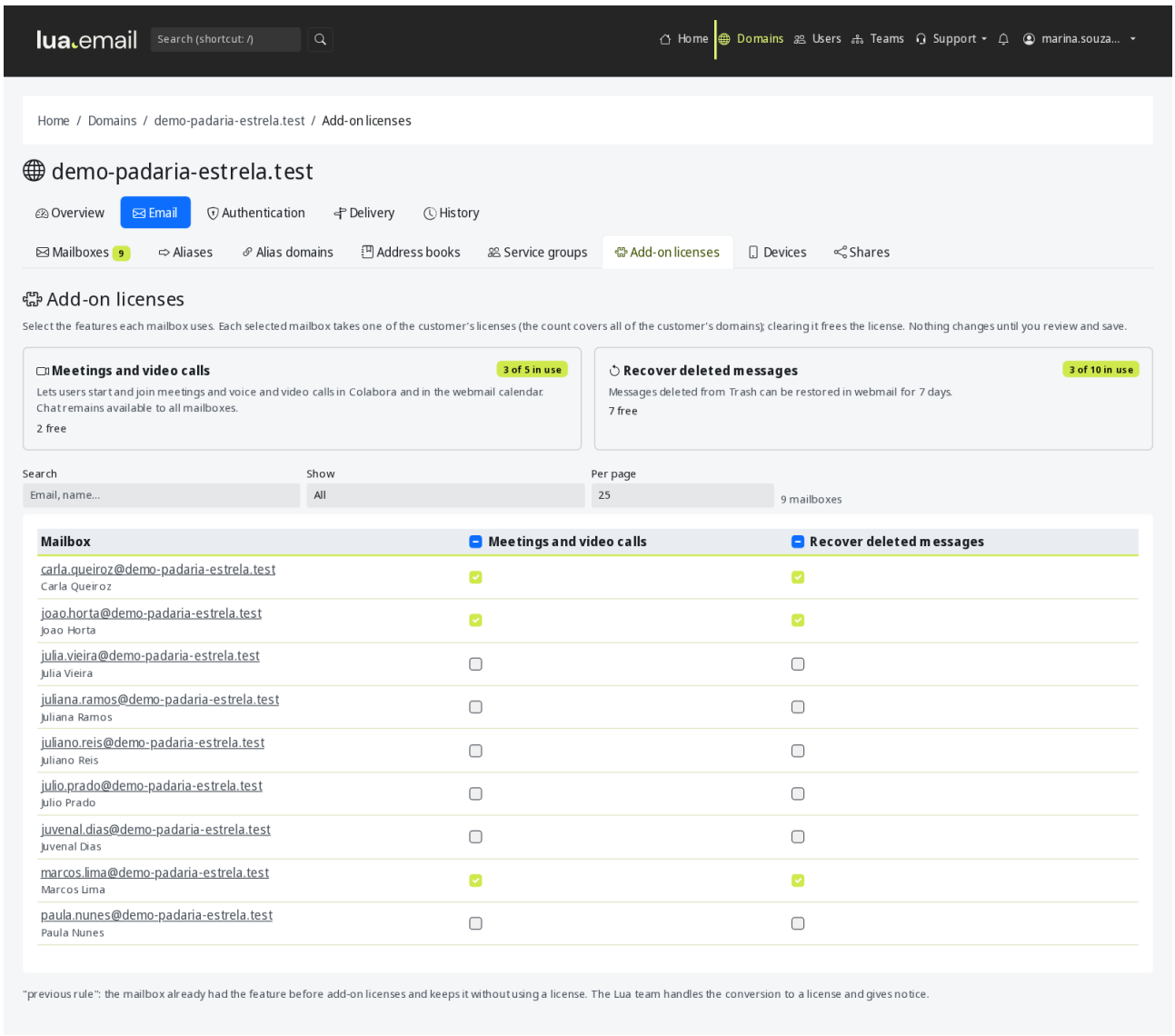


Figure 31: Domain tab: selected mailboxes carry the "will activate" label until you save (real screen, fictional data).

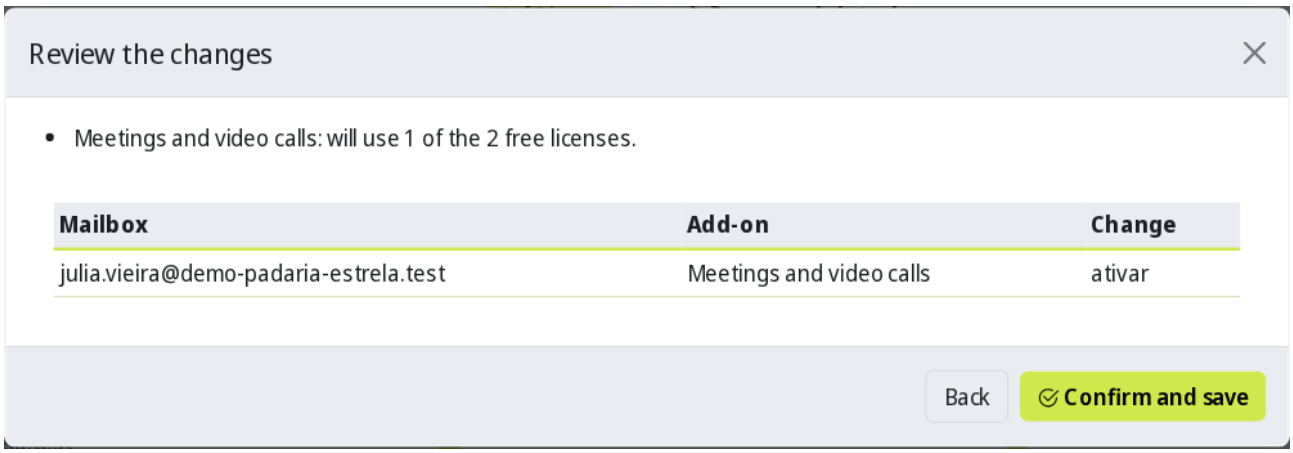


Figure 32: The review shows what will change before saving (real screen, fictional data).

Rules that apply to both ways:

- **With no license left, the checkbox is disabled.** The screen shows "No license left" and the link to subscribe to more. If someone else uses the last license between opening the screen and Save, the rest of the form is saved and the panel says the add-on was not activated.
- **A removed mailbox frees the license** right away. If you cancel the removal, the add-on does not come back on its own: activate it again, if a license is available.
- **A disabled mailbox still holds the license** until you take the add-on off (the domain tab allows it) or remove the mailbox. The feature has no effect while it is disabled.
- **A mailbox with a legacy or complimentary license does not get add-ons.** First change the mailbox's license to a current plan (see above); the screen gives the reason.
- **"On under the previous rule":** those who already had meetings or recovery before add-on licenses keep the feature without taking up a license. When you activate the license, the mailbox starts using one from the contract.
- **Who can change it:** the domain administrator and the Lua team. Read-only and support users see the checkboxes but cannot change them.

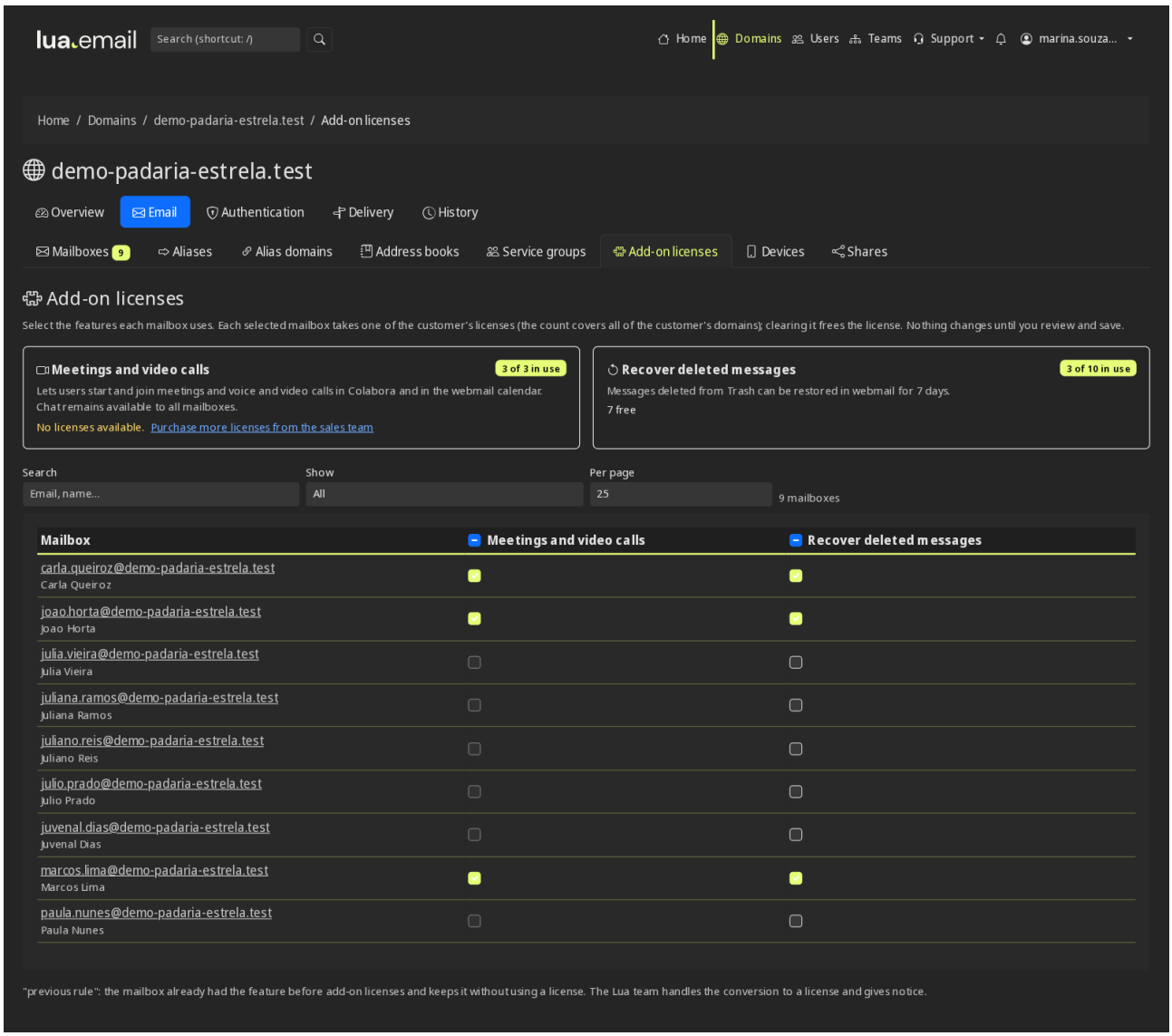


Figure 33: No license left: the checkbox is disabled and the panel shows how to subscribe to more (real screen, fictional data).

Requiring two-step verification and a password change

You can require that the person, before using webmail and Colabora on the web, **sets up two-step verification** and/or **changes the password**. With both options, the person only gets through after complying; the password change comes before setting up verification. Through the service group, you can also make the group's mailboxes **receive email only from the same domain**.

Where	Option	Effect
Create or edit the mailbox, **Access to webmail and Colabora** block	Require two-step verification	Anyone who has not yet set up the authenticator app or email can only use webmail after setting it up.
Create or edit the mailbox	Change the password at the first (or next) sign-in	Until it is changed, only the new password screen opens. Once changed, the flag clears on its own.
Change password on the mailbox	Ask the person to change the password at the next webmail sign-in	It comes **checked**: the password you set is temporary and the person picks their own.

Service group, **Access security** tab (also on the **Default** group, which applies to all of the domain's mailboxes)	Require two-step verification	Applies to all the group's mailboxes. When you edit the mailbox, the option is **locked**, with the group's name.
Service group, Access security tab	Change the password at the next sign-in	When turned on, all the group's mailboxes change the password at their next sign-in; whoever already changed it, changed it. A mailbox that joins the group later changes it too. **Require the change again for everyone** asks again, including from those who already changed it.
Service group, Access security tab	Only senders from the same domain	The group's mailboxes only receive email from people in the domain; anything from outside is rejected on arrival. When you edit the mailbox, the option is **locked**.

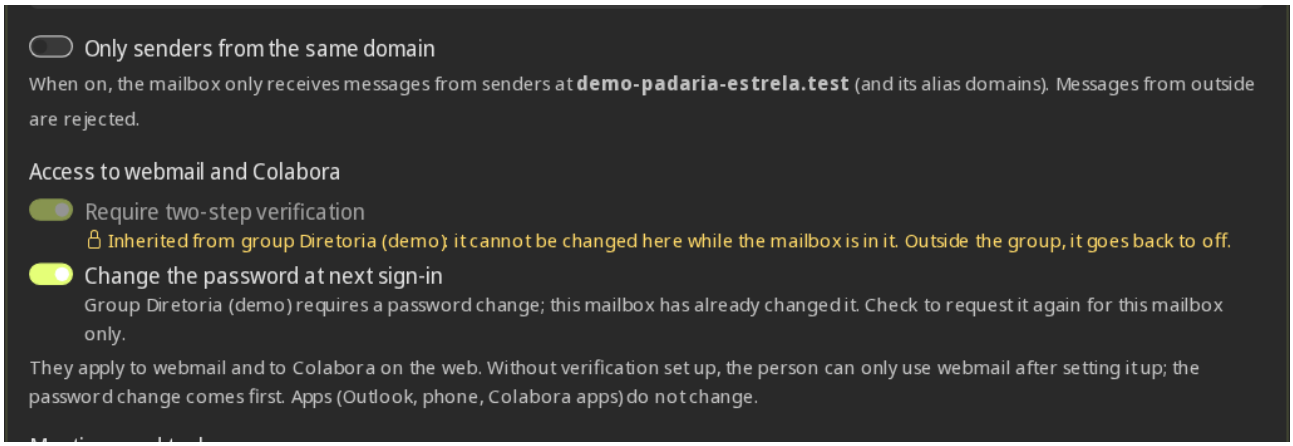


Figure 34: When editing the mailbox, whatever comes from the group is locked and says which group; changing the password remains free.

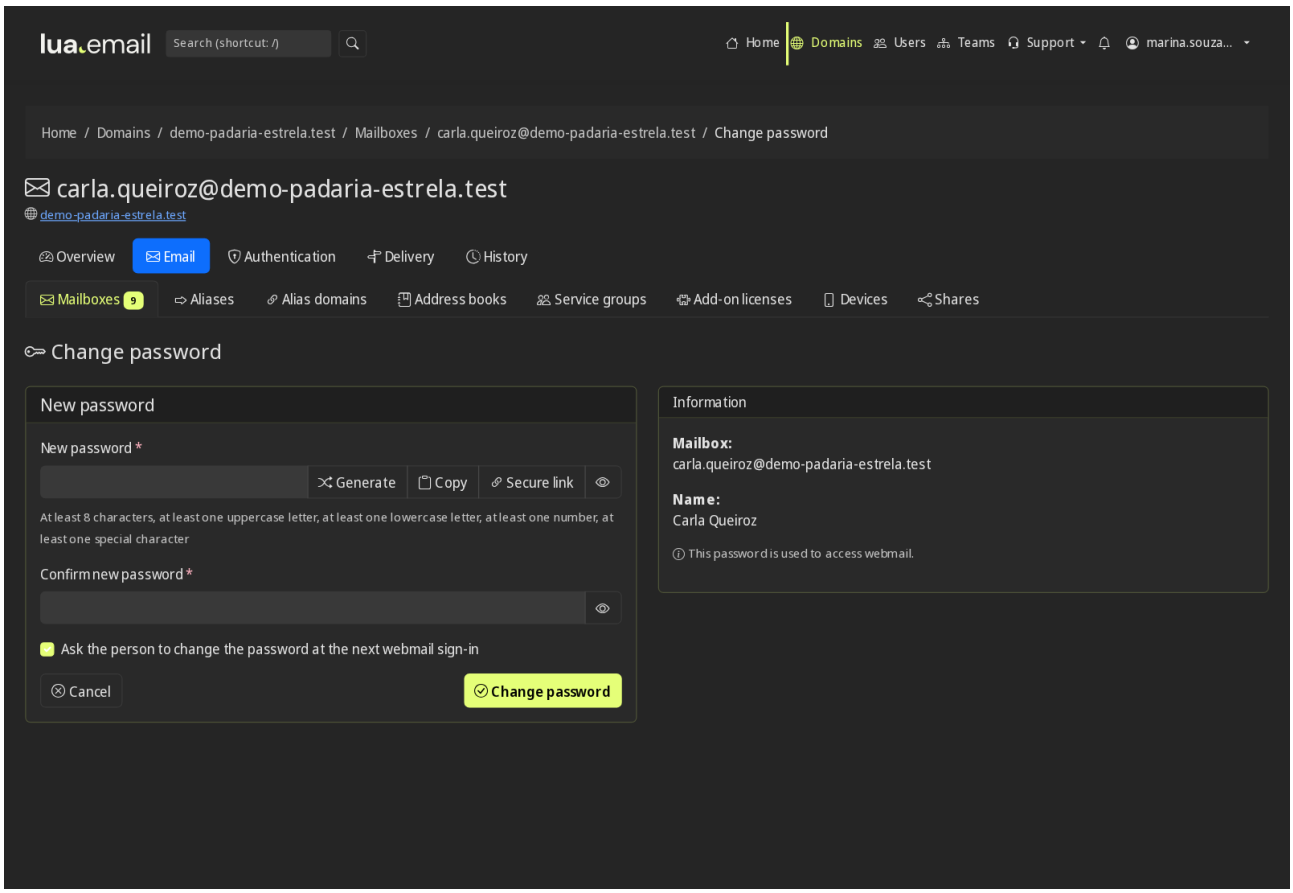


Figure 35: Changing a mailbox's password: the option to ask for the change comes checked.

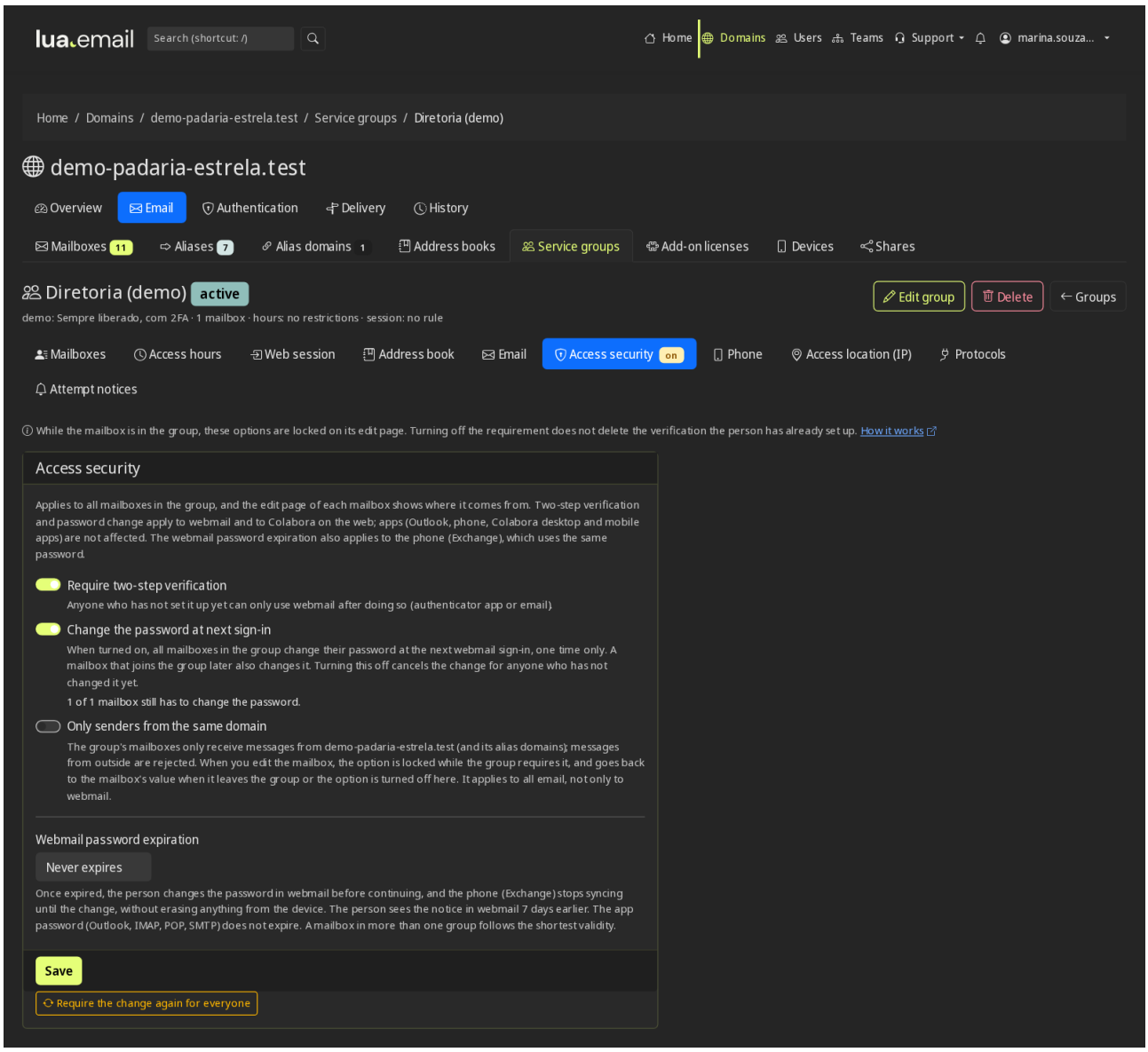


Figure 36: Access security in the group: it applies to all of its mailboxes.

- **Apps do not change:** Outlook, phone, IMAP, POP, SMTP, ActiveSync, contacts and calendar over DAV, and the Colabora apps on computer and phone stay as they are. The requirements apply to people who sign in through the browser.
- **The Default group** (all the domain's mailboxes, including ones created later) has the Web session and Access security tabs, through the **Session and security** button on the group list. A disabled group does not count.
- **Inherited from the group:** two-step verification and "same domain only" are locked on the mailbox edit while it is in the group. When the mailbox leaves the group, or the option is turned off in the group, what the mailbox itself had comes back. The mailbox view shows, next to each group, what it requires.
- **Change requested by the group:** if the mailbox leaves the group before changing the password, the change requested by the group goes away; the one requested on the mailbox itself remains.
- **Turning off the requirement** does not delete the verification the person already set up. To remove it, they turn it off in webmail.

When to use it:

- **New mailbox:** you create it with a temporary password and turn on *change the password at first sign-in*. The password that went through a message or paper stops working at the first sign-in.

- **Sensitive departments:** finance, management and HR in a group with *Require two-step verification*. If the password leaks, it alone does not open the mailbox.
- **A team that only talks to the company** (production, shop floor, interns): a group with *Only senders from the same domain*. Scams and spam from outside never even arrive.
- **After an incident involving several people**: in the group, *Require the change again for everyone* asks everyone for a new password at once.
- **After a scare** (suspected exposed password, fake support scam): change the password and ask for a change at the next sign-in. If the person lost the authenticator phone, see Resetting two-step verification.

Webmail password expiry

On the service group's **Access security** tab (also on the **Default** group, which applies to the whole domain), the **Webmail password expiration** field sets how often the person must change the password: **never** (the default), **30, 60, 90, 180 or 360 days**. As with the other requirements, the group's rule applies to all its mailboxes and, with no rule in the group, the domain default applies. If the mailbox is in more than one group, the shortest expiry applies.

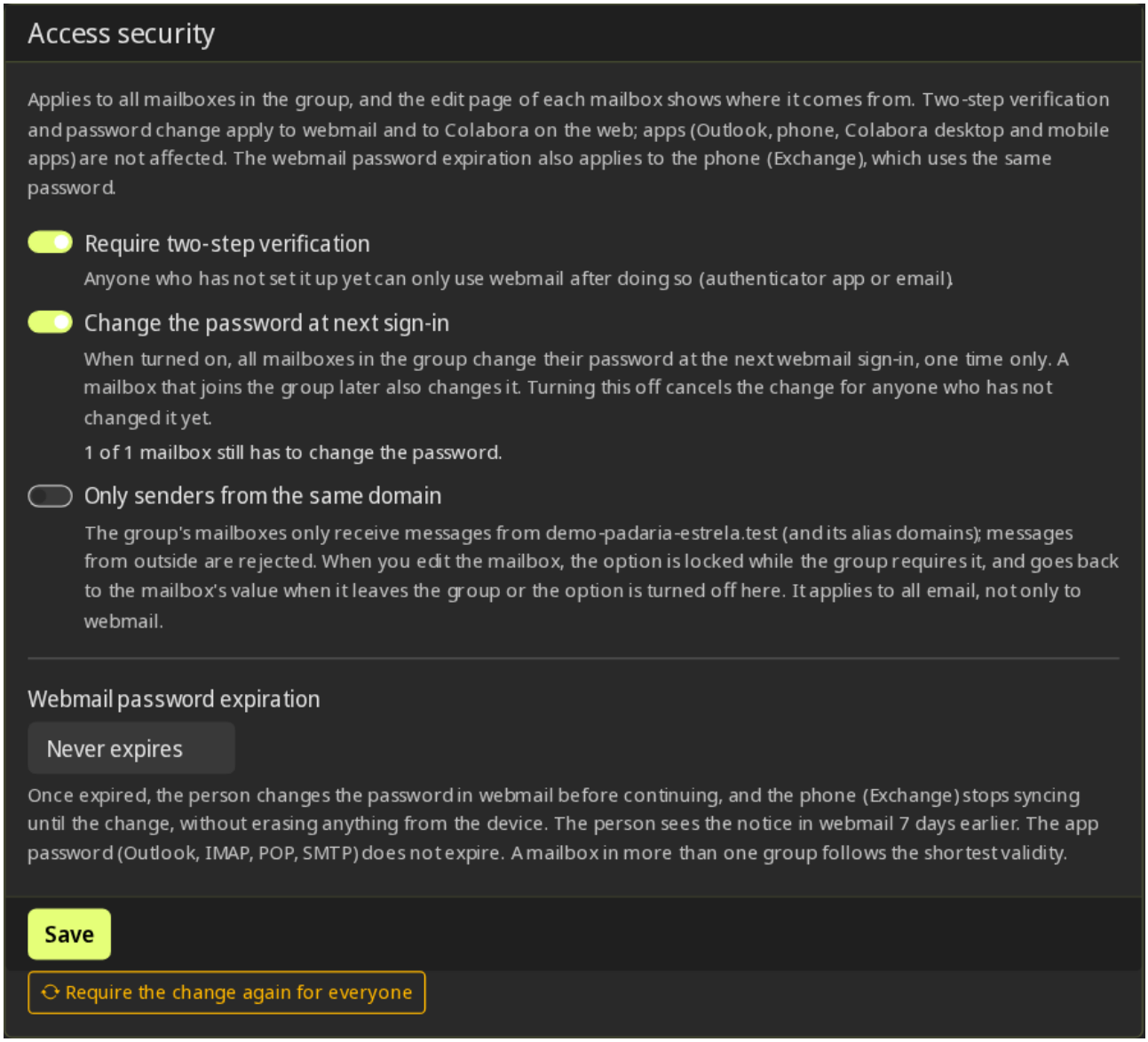


Figure 37: Password expiry in the service group (real screen, fictional data).

- **When it expires:** expiry counts from the last password change, made in the panel, in webmail or through the reset link. When you turn expiry on, or change it, no one expires before **7 days**: those already past the deadline get this grace period, with a notice in webmail. The same applies to a mailbox that joins the group later.
- **Expired password:** on webmail and Colabora on the web, only the password change screen opens until the person sets the new one. The **phone with an Exchange account** stops syncing until the change, without deleting anything from the device; after the change, the person types the new password on the phone and syncing resumes.
- **App passwords do not expire:** Outlook, IMAP, POP and SMTP keep using the same app password.
- **Notice to the person:** in the 7 days before expiry, one notification per day ("Your webmail password expires in N days") appears in webmail and Colabora. We do not send an email with a link for this notice, on purpose: the person changes the password by signing in to webmail as usual (see the webmail manual).
- **Notice to the administrator:** the panel bell warns, once per domain and per expiry date, that passwords are about to expire.

On each mailbox page, the **Webmail** box shows "Webmail password: changed on..., expires on..." with the status (up to date, expires in N days, expired or does not expire) and which group sets the rule.

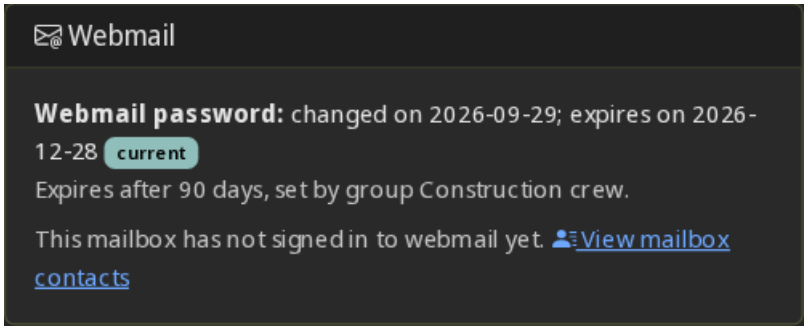


Figure 38: The date of the last change and of the expiry, on the mailbox page (real screen, fictional data).

The **Password expiration** report is on the button of the same name on the service group list. It separates mailboxes that **need attention**, the **expired** ones and **all** those with an expiry, with the date of the last change and the expiry date, and the **Download spreadsheet (CSV)** button.

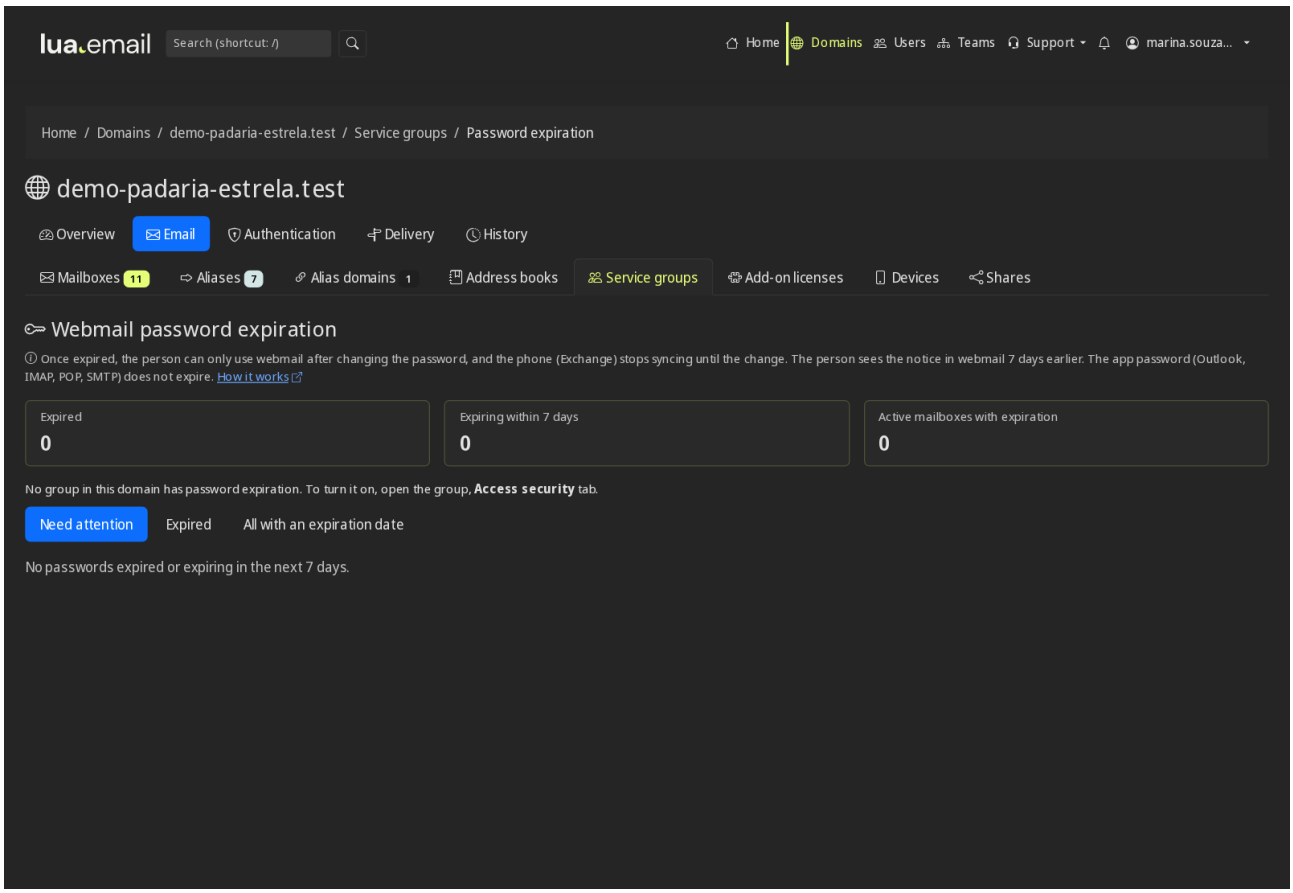


Figure 39: The report of expired and soon-to-expire passwords, with a spreadsheet to download (real screen, fictional data).

Space usage

Each mailbox's space is shared between email and the Colabora drive files. In **Statistics**, on the mailbox page, you see how much each uses, the free space and how far the drive can still grow: a portion is always reserved so email can keep arriving. Near the limit, the person gets an email warning with the usage broken down.

Accessing webmail as the mailbox (support)

When someone at the company asks for help ("a message disappeared", "the folder does not show up", "the filter does not work"), the domain manager can open webmail **as the person's mailbox** and see exactly what they see, without asking for or changing their password.

Who can: company administrators (Administrator role), only on mailboxes in the domains they administer. Helpdesk and read-only users do not see the button. Lua support uses the same path, with the same log.

1. On the mailbox page, click **Access webmail as this mailbox**.
2. Write the **reason** (for example, "Ticket 4821: can't find yesterday's messages").
3. Choose the mode, **Read-only** or **With changes** (table below).
4. Click **Open webmail**. Webmail opens in a new tab, with a banner at the top showing the mode, the mailbox, who signed in and until what time the access is valid. When you finish, click **End** on the banner.

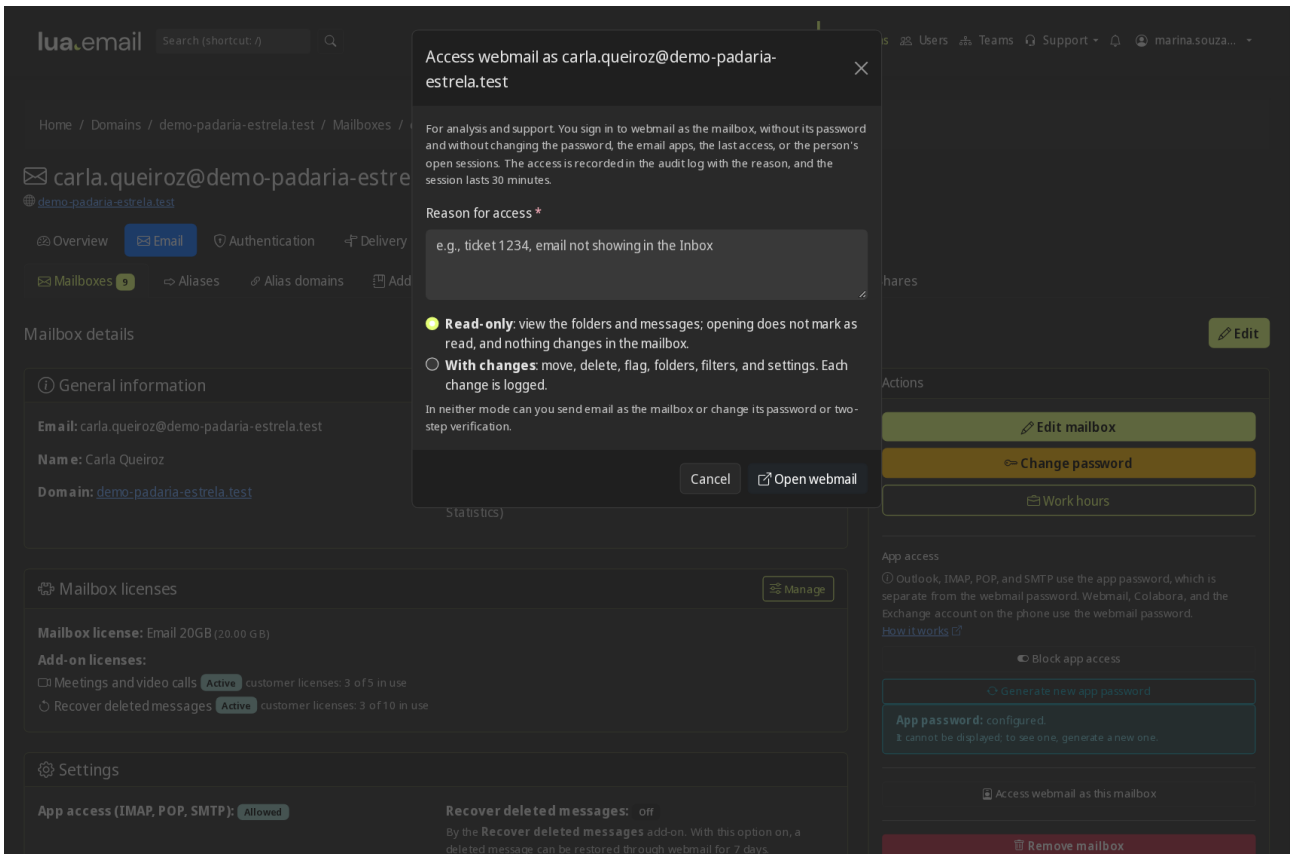


Figure 40: Reason and mode for accessing webmail as the mailbox. Fictional data.

	Read-only	With changes
See folders, messages, attachments, contacts, calendar and filters	Yes	Yes
Does opening a message mark it as read?	No	No (marking as read on purpose, yes)
Move, delete, flag, create or rename folders	No	Yes
Adjust filters and mailbox settings	No	Yes
Every change is logged	There are no changes	Yes

What is never possible, in any mode:

- writing or sending email as the person;
- changing their password or touching their two-step verification;
- giving someone else access to the mailbox: sharing the account or folders, forwarding or redirecting messages, creating a calendar connection or public link;
- seeing or taking the person's encryption keys.

These actions would remain in effect after the support session ended, or would make the person look like the author of something they did not do. That is why they are outside support access.

Why the reason is required. A mailbox holds conversations, contracts and personal data. Entering it means accessing another person's information, and the data protection law (LGPD) asks that this kind of access have a clear purpose. The reason records **why** the access happened:

- the person and the company know the entry was to solve a problem, and not out of curiosity;
- whoever did the access can show, afterwards, that they were handling a request;
- including the ticket number links the access to the support case.

How it works, and why.

- **Without the person's password:** the password is neither changed nor shown. Their phone, Outlook and webmail keep working during and after the support session.
- **Single-use entry:** the button generates an entry that is valid for 1 minute and only once. It cannot be used again or passed on to someone else.
- **The permission is checked again at entry:** if the administrator lost access to the domain in the meantime, webmail does not open.
- **30-minute limit and a banner at the top:** the access is not left open and forgotten, and it is clear to whoever is on the screen that the session is a support one (orange: read-only; red: with changes).
- **Nothing changes for the person:** opening does not mark as read, their last sign-in stays the same and their open sessions stay valid. They do not lose work or see "signs" of access that was not theirs.
- **Everything logged:** in **History → System logs**, the access appears as **Accessed webmail as the mailbox (support)**, with who did it, when, the mailbox, the mode and the reason. In the with-changes mode, each change is also logged.

> **Tip:** tell the person beforehand whenever possible, use **Read-only** when just looking is enough, and click **End** as soon as you finish.

When to use it, and when not to:

- **Use it** to see what the person sees: "a message disappeared", the folder does not show up, the filter sent everything to trash, the signature came out wrong. With *Read-only* you investigate without touching anything; with *With changes* you fix the filter or the folder on the spot, and the log shows what changed.
- **Do not use it** for "I forgot my password": there is Change password for that, and the helpdesk user does it without opening anyone's mailbox.
- **Do not use it** to read the mailbox of someone who left the company or to investigate a person: the access exists to handle a request, and the reason is logged. If the company needs access to a departed person's mailbox, agree with the person responsible for the matter (legal, HR) and use mailbox sharing before removing it.

Removing a mailbox

In **Delete mailbox**, confirm by typing the address. The mailbox becomes inactive right away and the license is freed. Within a few minutes, the messages go to a quarantine area and the account is removed for good, along with the contacts, calendar and webmail settings. Before that, we keep a copy of the account data: if the removal was a mistake, contact support to restore the mailbox.

If the mailbox address was already redirecting to someone else (an alias), that redirect stays and emails keep reaching them. For the address to stop existing, also delete the alias in Aliases.

When someone leaves the company, which path?

- **You may need the content later:** turn off **Active** when editing the mailbox. It stops signing in and working, but nothing is deleted, and you can re-enable it.
- **A colleague will keep handling the same address** (for example, `sales@` that belonged to the person who left): remove the mailbox and create an alias with the same address pointing to the colleague, or a service group with a group email.
- **Gone for good:** use **Delete mailbox**. The license is freed and the account is removed completely within a few minutes; the saved copy lets you recover it if it was a mistake.

7. Aliases

An alias is an address that has no mailbox of its own and delivers to other mailboxes: `comercial@` for two people, `contato@` for the front desk.

1. Under **Email → Aliases**, click **New alias**. A window opens without leaving the page: the address and the destinations are in view and the rest is under **More options**. If you prefer the full screen, with the status of each destination, use **Open full page**. If something is wrong, the error appears inside the window and what you typed stays; when you create the alias, the list returns with the filter that was applied.
2. In **From**, type the part before the `@`. You can also paste the full address in the same domain: the panel removes the `@` and the domain by itself. An address in another domain is refused, with the message "The alias must belong to the domain X. Type only the name before the @.". In **Name** (under **More options**), enter something to recognize the alias in the list, such as "Equipe comercial".
3. In **To (participants)**, one address per line. If you paste a list separated by commas, semicolons or spaces, the panel organizes it automatically, counts the addresses and shows the status of each one: **Mailbox**, **Alias**, **Outside the domain**, **Mailbox disabled**, **No license** or **Does not exist**.
4. If you like, check **Only senders from the same domain** (internal list) or fill in **Allowed senders** (only those addresses or domains can write to the alias).
5. Click **Create**.

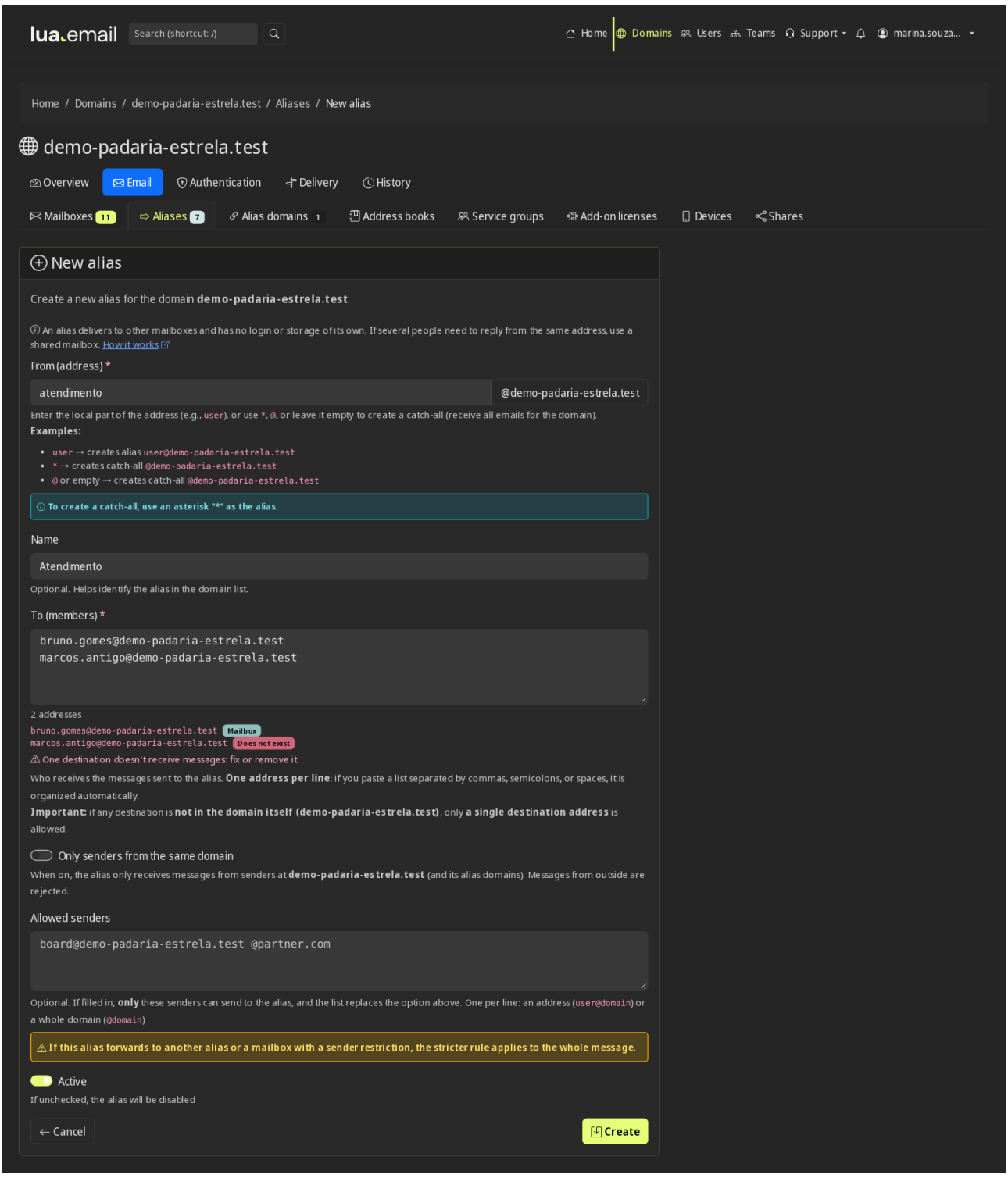


Figure 41: New alias on the full screen: the destination that does not exist appears flagged.

- Aliases that deliver to a mailbox can also be used as a sender by the person who owns that mailbox, in the webmail, under **Settings → Identities**, up to 5 aliases per person (see the webmail manual). For an alias to appear for someone, add that person's mailbox to its destinations.
- If one of the destinations is at another provider (outside the domain), it must be the alias's only destination.
- When a message passes through more than one alias or mailbox with a sender restriction, the most restrictive rule applies.
- To create a **catch-all**, which receives any address in the domain that does not exist, use * in the From field. Use it with care: it also receives spam sent to made-up addresses.

- Addresses that start with `grp-` are reserved. The alias also cannot have the name of a service group in the domain, regardless of case or accents: an alias `comercial@` and a group "Comercial" would look the same in Colabora search.

Editing an alias

Click **Edit** on the alias row. The address does not change (for another address, create a new alias), but the name, destinations, sender restrictions and status do. The status of each destination appears again while you edit.

In the list, each alias has a badge that says who can write to it:

- **open**: any sender, including people outside the company;
- **internal**: only senders from your own domain;
- **restricted senders**: only the authorized addresses or domains. You can see who they are when you edit the alias: the list does not appear on the badge.

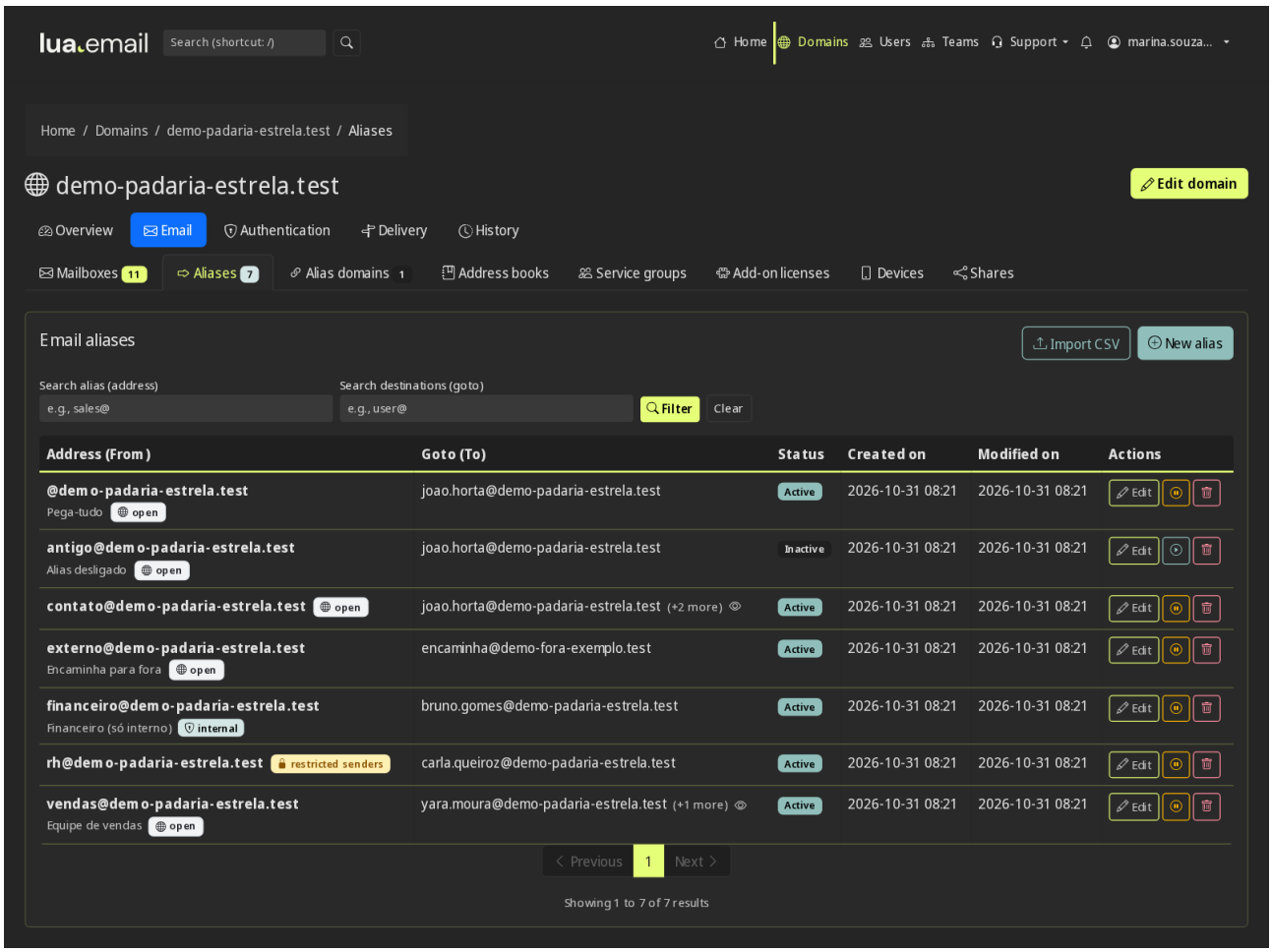


Figure 42: The alias list. The badge says who can write to each one: anyone (open), only the domain itself (internal) or only authorized senders.

An alias that is a group's email address

The alias marked **Service group email** is maintained by the group (see Group email): its destinations are the group's mailboxes and change on their own when someone joins, leaves, is deactivated or is reactivated. That is why it can't be edited, paused or removed from the list. The **Manage in group** button takes you to the Group email tab, where the address and the allowed senders are set.

Alias with a destination that does not receive

An alias can end up pointing to a mailbox that was deactivated or to an address that no longer exists (someone who left the company, for example). Messages to that destination come back with "user does not exist", and the sender gets the bounce. The panel shows the problem in three places:

- in the alias list, with the **destination(s) with a problem** warning;
- in the alias edit screen, with the **Does not exist** or **Mailbox deactivated** label next to the destination;
- in Domain health, with the **Fix** button.

To resolve it, remove the destination from the alias or replace it with the address of whoever took over the role.

Alias

If one of the destinations of the alias is a mailbox without a license, messages sent to the alias are returned with an error until the mailbox receives a license. The panel shows this in three places:

- in the list of aliases, the destination appears with the **No license** tag and the explanation "This mailbox has no license. Messages sent to this alias are returned with an error until the mailbox receives a license.";
- at the top of the **Aliases** tab, a notice counts how many aliases are in this situation. The **Show only these** button filters the list to show only them, and **Show all aliases** returns to the full list;
- in the alias form, next to the destination, the **Assign a license to the mailbox** link. It appears only to people who administer the domain.

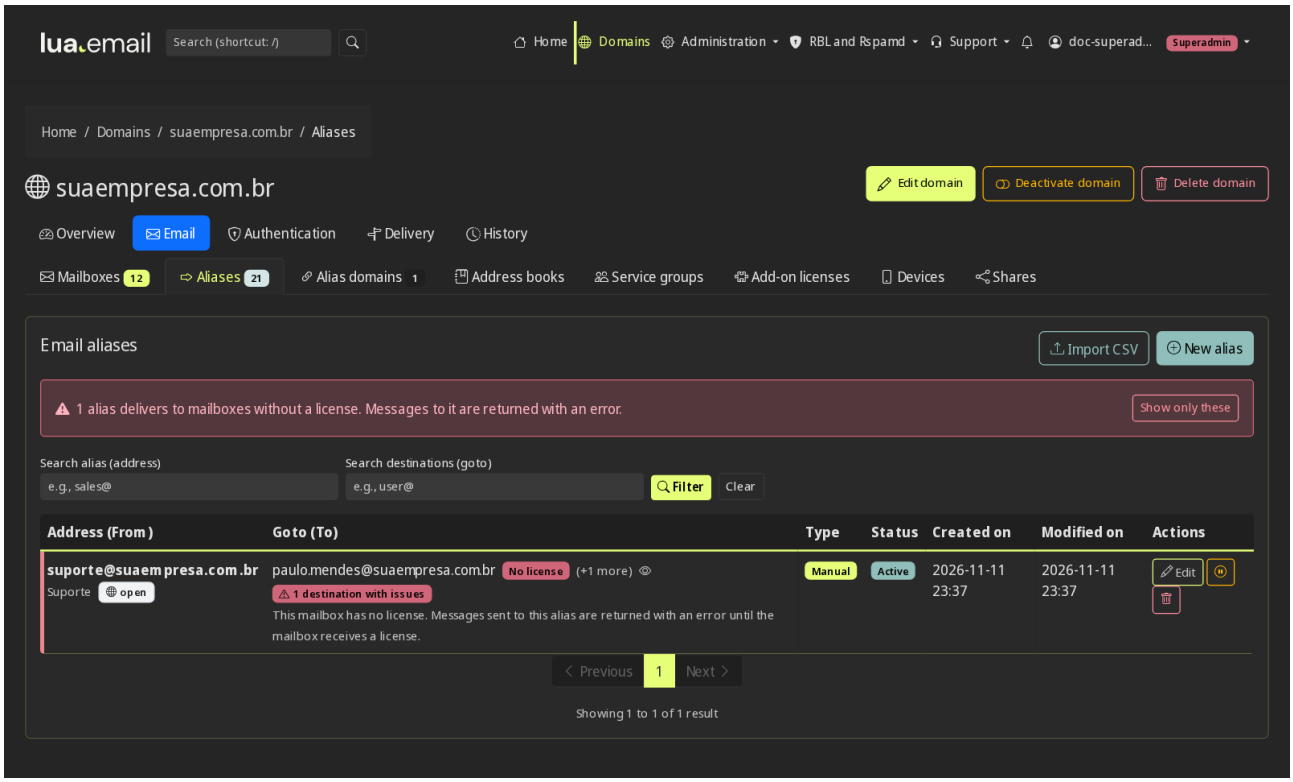


Figure 43: The notice at the top of the Aliases tab and the destination marked as No license.

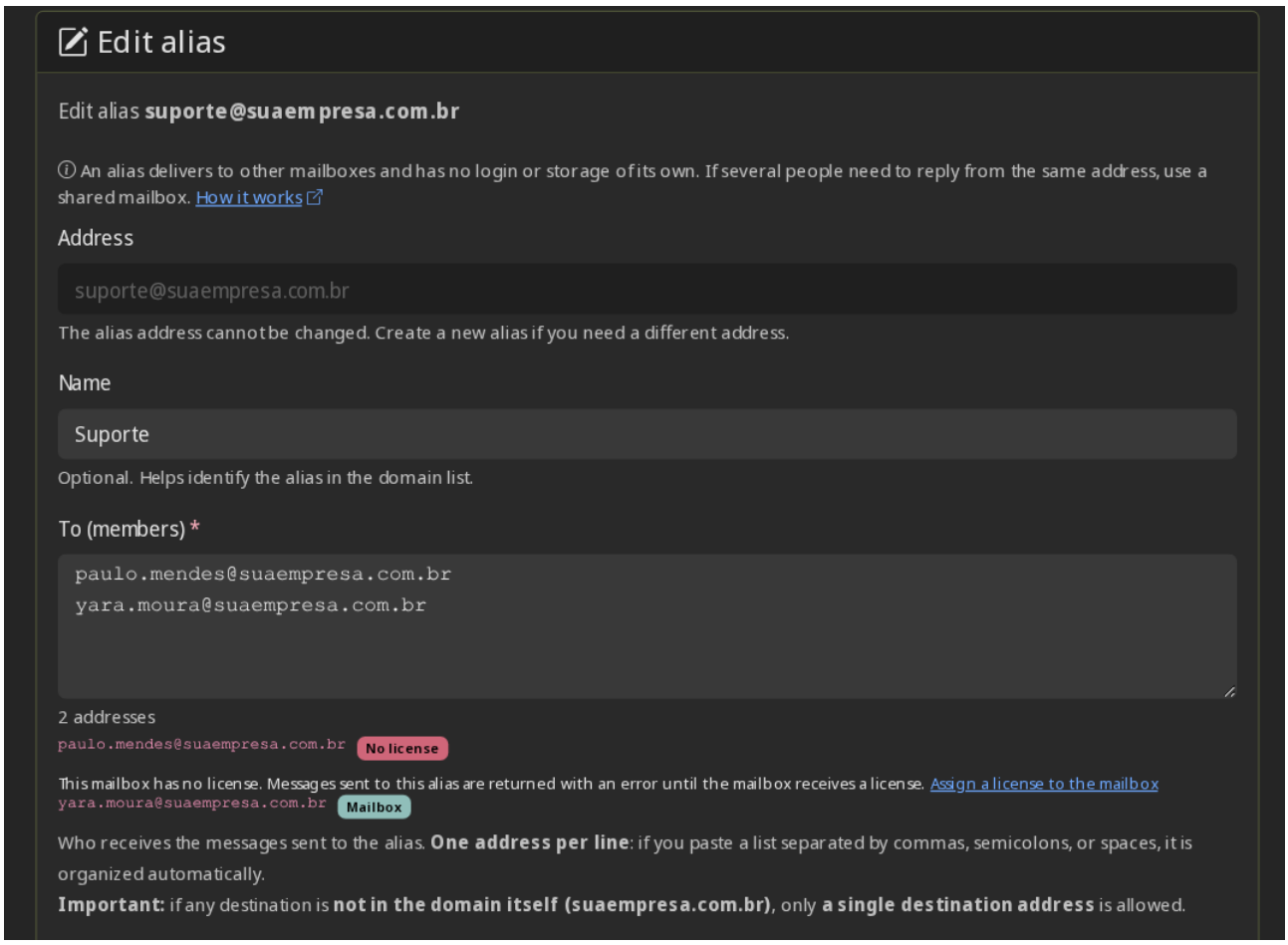


Figure 44: In the alias form, the Assign a license to the mailbox link goes straight to the license.

Default domain addresses

`abuse@` (abuse and spam reports) and `reportdmarc@` (DMARC reports) are created along with the domain and show the "domain default" tag. You can change where they go (**Edit destination**), but you can't pause or remove them.

Alias domain

An alias domain makes `jane@otherdomain` arrive at `jane@yourdomain`, for all mailboxes. It is useful when the company has both the `.com` and the `.com.br` version of its name. In **Email → Alias domains → New**, enter the domain. If it is not on Lua yet, the panel asks for the same verification TXT record as in chapter 3, and the alias is added automatically once the TXT record appears.

If the alias domain is already registered on Lua, it must belong to the same customer as the main domain. A domain that belongs to another company can't become an alias of yours.

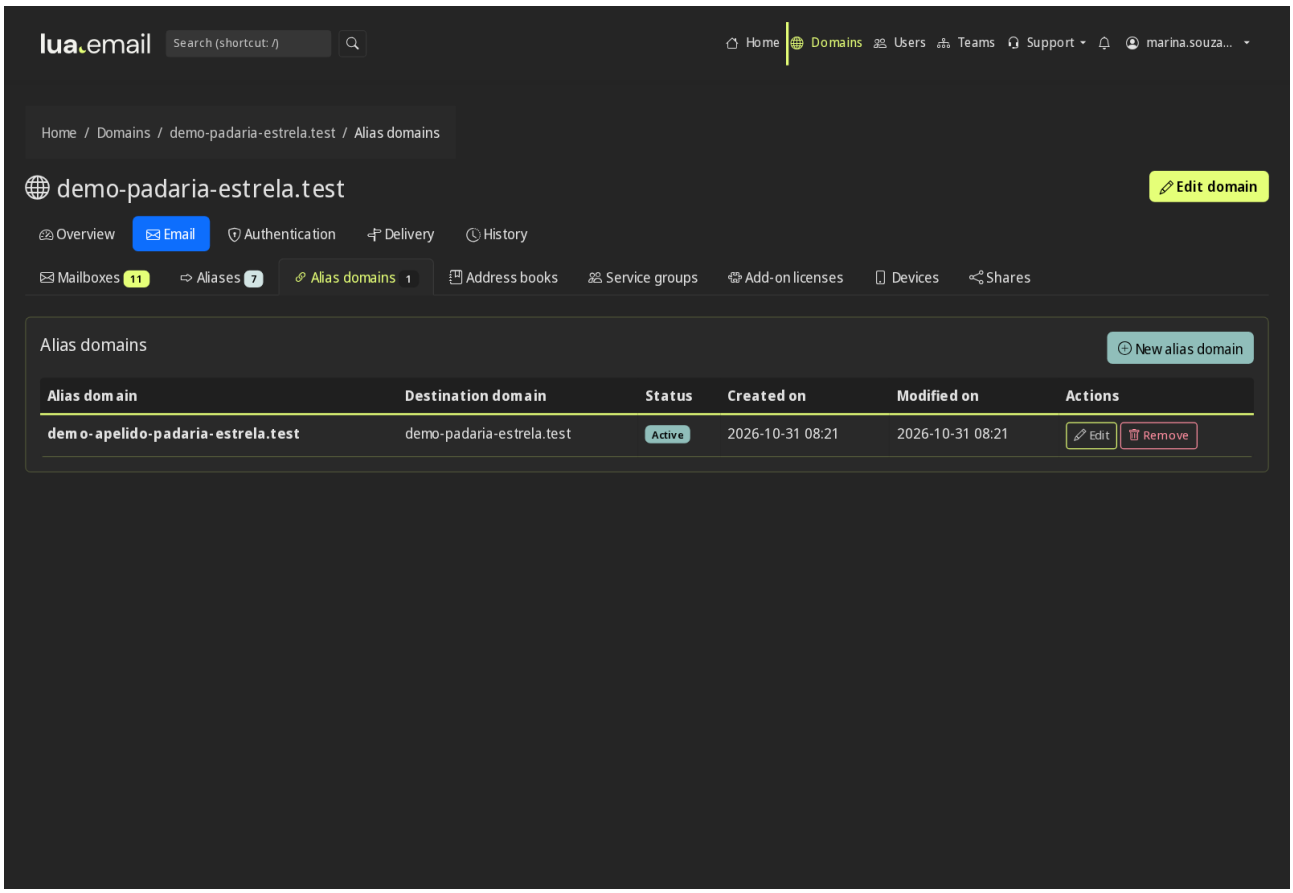


Figure 45: Alias domains: a new domain also proves ownership with a TXT record.

8. Domain health

In **Overview → Domain health**, the panel gathers what deserves attention:

- **Aliases with a destination that doesn't receive**, with the Fix button.
- **Mailboxes at 90% of their space or more.**
- **Active mailboxes with no access** for 30, 60, 90 or 180 days (no sign-in through webmail, IMAP or POP). An idle mailbox takes up a license: it is worth checking whether it is still in use.
- **DNS:** one badge for each item (Autodiscover, DKIM, DMARC, MX and SPF), with the **Check now** button, the **How to fix** link on each item, the name servers and, on Edgium DNS, **Fix problems**.
- **Automatic email setup:** one line in the DNS alert list (**Automatic setup pending**, **in progress** or **with a problem**), with **How to fix**, which leads to the card in the Validate DNS tab. It disappears when it is **Completed**. See Automatic email setup.

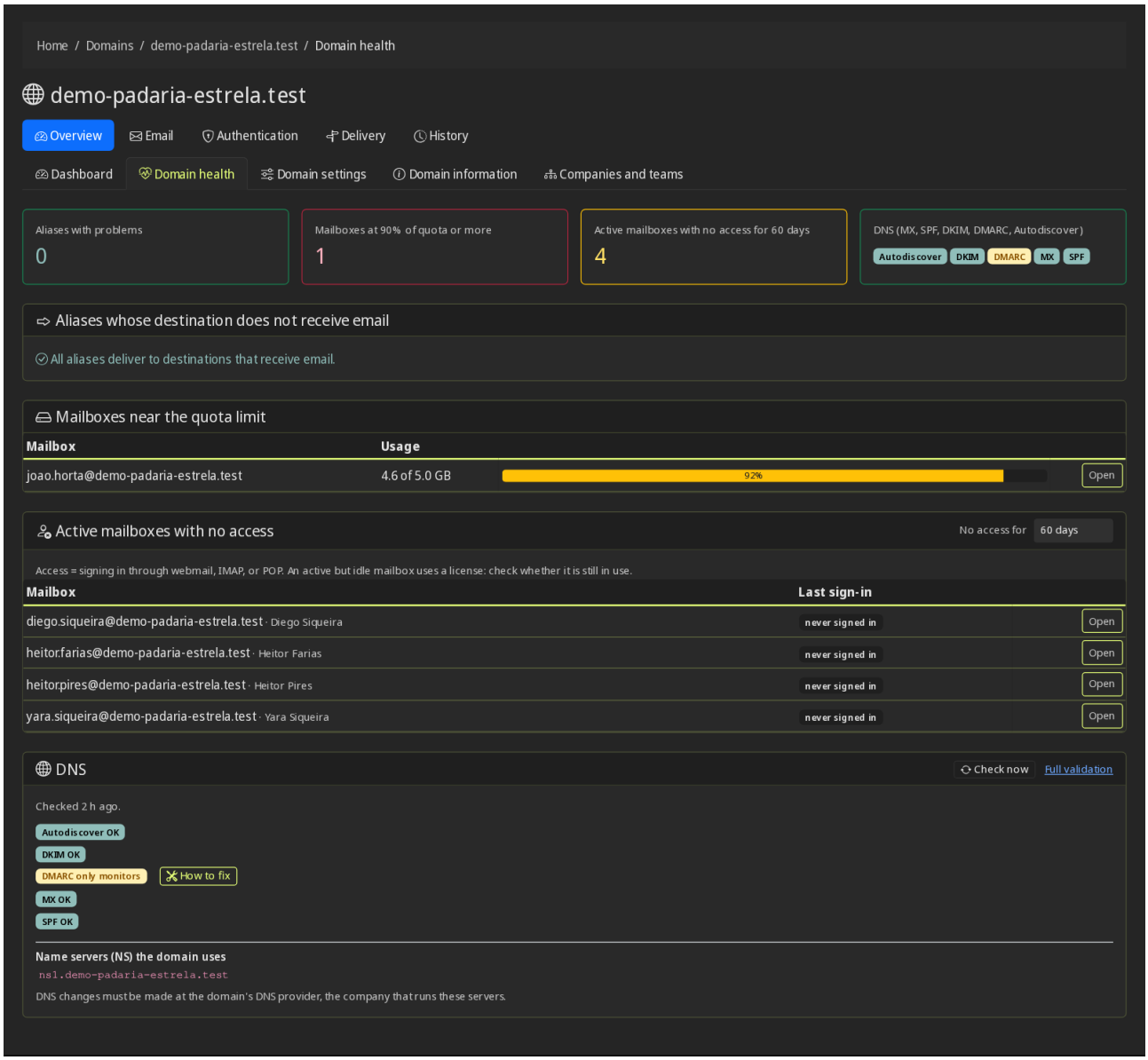


Figure 46: Domain health, with the DNS section showing when it was last checked, the Check now button and the domain's name servers.

In the domain's **Overview**, the panel only **shows** the status (email, DNS and records). All DNS actions live in the domain health page: the **View domain health** button in the Overview takes you straight there.

DNS in Domain health: last result and Check now

Opening the health page does not run a new DNS lookup: the **DNS** card shows the **last saved result**, with the time of the check (**Checked 2 h ago**) or **Not checked yet** if the domain has never been checked. The panel checks domains in the background. To see how your DNS is right now, click **Check now**: the panel looks up MX, SPF, DKIM, DMARC and Autodiscover and refreshes the health page itself, without sending you to another screen. Each record with a problem has a **How to fix** button. To avoid overloading DNS, a domain can only be checked again after 5 minutes; until then, the panel shows the last result and tells you how many minutes to wait. For a more detailed check, use the **Full validation** link.

DKIM and DMARC in Domain health

Domain health no longer has one card for DKIM and another for DMARC. Both appear as **badges** in the **DNS** block, along with Autodiscover, MX and SPF:

- **Green badge (ok):** the record is published and correct.
- **Red badge (problem):** the badge is a **link to the tab that fixes it**: DKIM goes to **Authentication → DKIM** and DMARC to **Authentication → DMARC**, where the record is ready to copy. **How to fix** stays next to it.
- **Yellow badge "DMARC only monitors":** DMARC is published with p=none. It works, but it only observes and does not protect the domain; that is why the badge does not say "DMARC ok". With DNS at another provider, your record is not replaced: the DMARC tab shows the recommended one for you to decide. With DNS on Edgium, Lua's default replaces it when the panel sets up email.

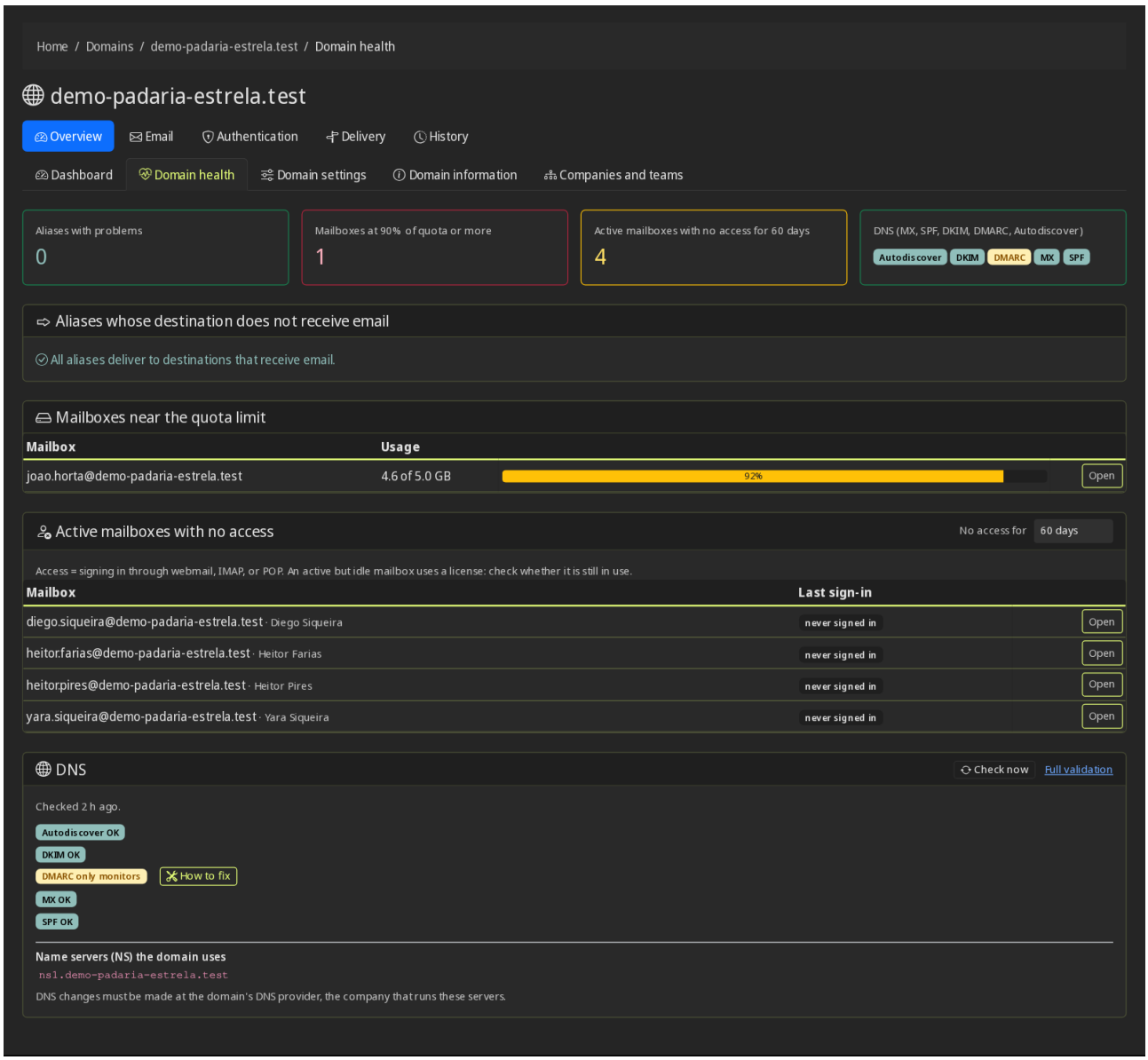


Figure 46 (continued): the badges in the DNS block. DMARC with p=none appears in yellow, as "only monitors".

When signing turns on and off

- **It turns on by itself** when DNS publishes the record with the panel's right key.
- **It turns off by itself** only after **several checks in a row** that do not find the record. A momentary DNS failure turns nothing off. When it turns off, **the key is kept** and you get a notice; publish the record again and signing comes back by itself.
- **You can turn it off and on again.** The **Turn off signing** (or **Turn on signing**) button is on the **Authentication → DKIM** tab, no longer in Domain health. It asks for confirmation (without signing, delivery of your emails may get worse) and keeps the key. Once you turn it off, signing **does not turn on by itself**: use **Turn on signing** when you want. But **you cannot turn it on without the record published** with the right key: the button stays disabled and explains what is missing.
- Only the **superadmin** and the **domain administrator** can turn signing on or off; support (helpdesk) and read-only users just see the state.

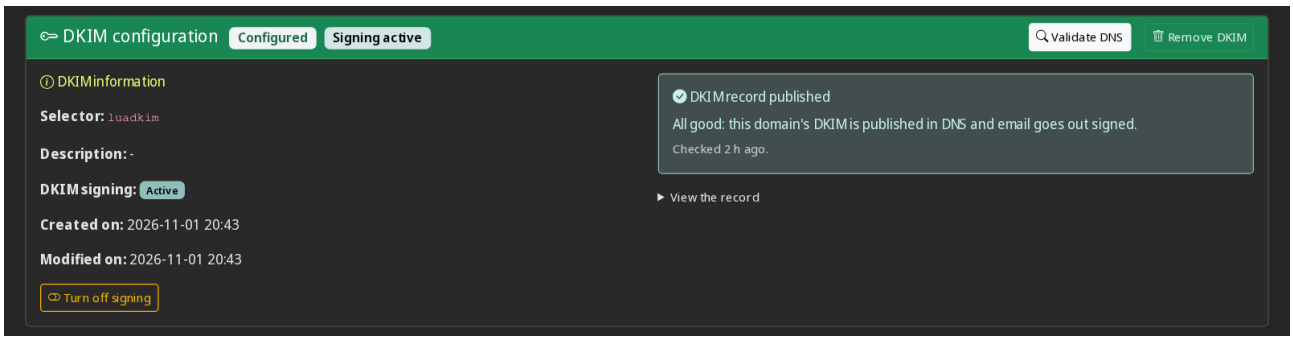


Figure 46 (continued): on the DKIM tab, signing active with the record published and the Turn off signing button.

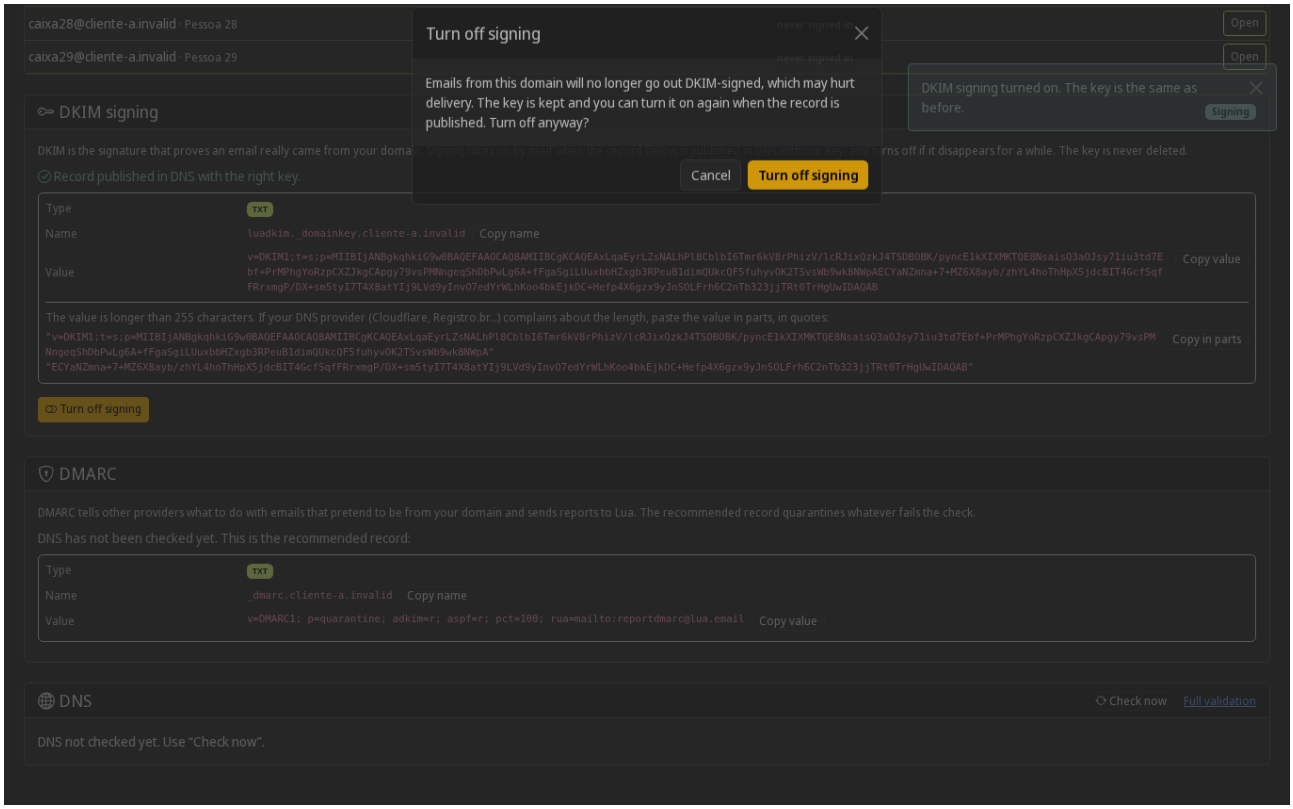


Figure 46 (continued): when you turn signing off (on the DKIM tab), the panel asks for confirmation and keeps the key.

Where to make DNS changes

Right below the records, the health page shows the **name servers (NS) the domain uses**. They tell you where the domain's DNS is hosted, and that is where any change has to be made. The panel says so in one sentence, for example: *"DNS changes must be made at the domain's DNS provider: provider name"*. If the DNS is at Edgium, the text says the changes are made in the Edgium panel.

DNS at Edgium: open the panel and fix problems

When the domain's DNS is hosted at Edgium, the section shows two buttons:

- **Open the Edgium panel**, to edit the DNS there.
- **Fix problems**, which fixes the email records for you, but only after showing what will change and getting your approval.

When you click **Fix problems**, a window opens with the **record-by-record preview**: the **current** value, the **new** one and the **action** (create, merge, replace or keep). Nothing is saved until you approve, and you can edit a record's value before then. There is only one button, **Apply**, which applies everything, the MX included.

- **Your SPF is kept.** The SPF you already have is not erased: the panel only adds Lua's authorization, so Lua can also send email on behalf of your domain.
- **SPF ending in `~all`.** The window warns you: your SPF was kept as it is and only gained Lua's authorization; because it ends in `~all` (soft fail), mail sent on behalf of your domain by servers outside the list may still be accepted, usually flagged as suspicious. If every service that sends email for your domain (website, system, store, marketing) is already in the SPF, `-all` (hard fail) asks receivers to reject the rest and protects better against spoofing. For that, there is the **Change ~all to -all** option, which is only worth it under that condition: if a service is missing from the list, its messages may be rejected. The change is optional and comes unchecked.
- **DMARC.** Lua's default record (`quarantine` policy, with the reports received by Lua) goes into the preview. If the domain already has a different DMARC, Lua's default replaces it; if it is the same, it is kept. The value you edit in the preview is the one that applies.
- **Changing the MX.** The MX decides where the domain's email arrives. When the preview includes the MX change, the window itself shows the notice **Email will start arriving at Lua** and asks for your confirmation: first, confirm that the mailboxes already exist and that SPF and DKIM are live, check the confirmation box and click **Apply and switch the MX**. It is the same click, with no other button. A domain with Lua Shield (antispam only) never has its MX changed.
- **Undo.** The window has an **Undo the last change** button, which puts the records back as they were. Emails that arrived between the change and the undo stay where they arrived.

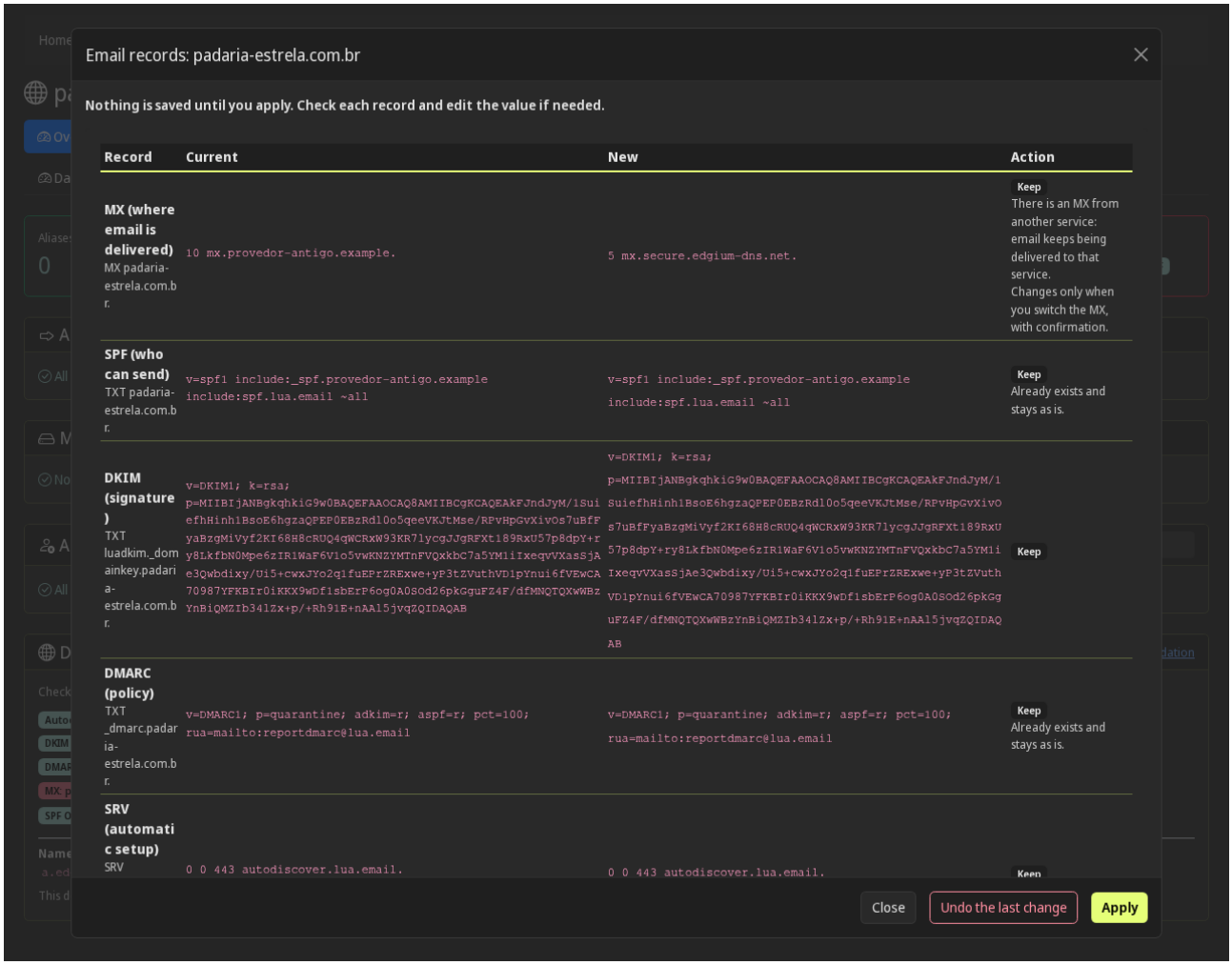
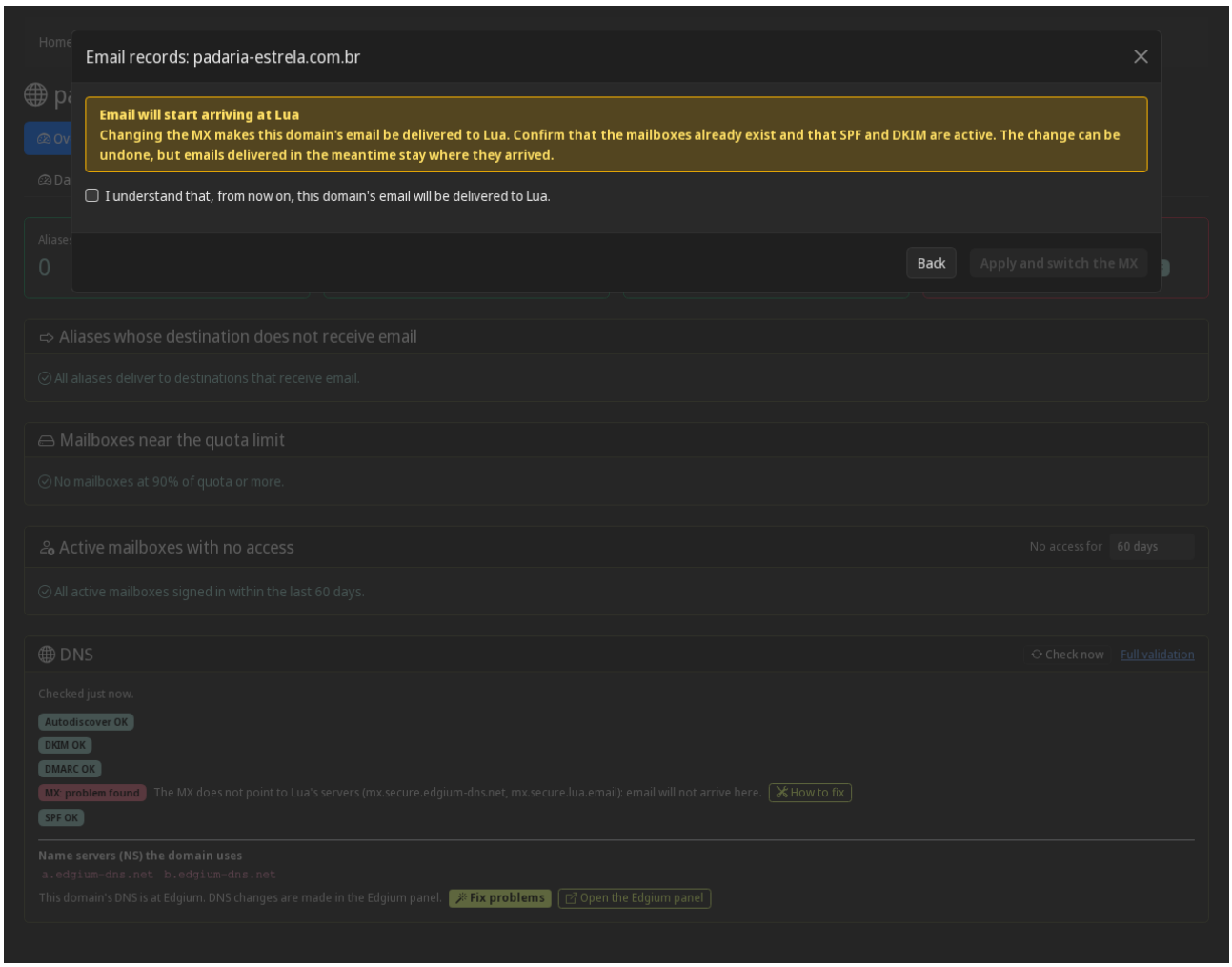


Figure 46 (continued): the Email records window, with the record-by-record preview and the Apply button.



The notice before the MX is changed, in the Email records window.

Only the **domain administrator** can apply fixes. People with a helpdesk or read-only role see the DNS status and the name servers, but not the buttons that change records. If the domain's DNS is not at Edgium, the window shows the records that need to exist and you set them up at the provider where the DNS is hosted today.

I adjusted DNS and the warning is still there

The DNS warning (the **Your domains' DNS** card on Home, the triangle in the domain list and Domain health) shows the **result of the last saved check**. The panel does not query DNS every time you open the screen.

- **After adjusting, check.** In Domain health, click **Check now** (one check every 5 minutes per domain). With DNS on Edgium, the result appears as soon as the record is applied, without waiting for DNS propagation. The next time the screen loads, the domain no longer shows the warning. If you do not click, the automatic check goes through all domains within 24 hours.
- **DNS keeps answers for a while.** DNS servers remember an answer for the time set in the record (the TTL). If the record did not exist yet, the "does not exist" answer is also kept, for the time set at the domain's provider, usually 5 to 30 minutes, sometimes more. So right after creating or changing a record, the check may still show the old value: wait a few minutes and check again.
- **Changing the name servers (NS)** at the registrar can take longer: hours, and up to 48 hours at some registrars.

For support: if the customer says they adjusted DNS and the warning is still there, ask them to click **Check now**. If it still reports a problem, wait a few minutes and check again. If it persists after that, open **Full validation** and compare the published value with the expected one.

The DNS alert in the domain list

In **Domains**, a **warning triangle** next to the name means the domain's DNS needs attention: email still goes to another provider, the name servers have not been changed yet, the DNS is blocked or the email records are incomplete. Hover over the triangle to see the reason and when the DNS was checked. Click it to open the **domain health** page, right at the DNS section. The triangle is **red** only when the problem affects email delivery (the MX does not point to Lua or the SPF has a problem) and **yellow** for the rest (DKIM, DMARC, Autodiscover, name servers or incomplete records). To see only the domains with an alert, choose the **DNS problem** filter, or click **View domains with problems** on the Home page.

The list does not query DNS when it opens either: it uses the last saved result. So a new problem shows up in the list when the domain is checked again, and the alert goes away after you fix the DNS and check once more. Deactivated domains and those that only use the spam filter (lua Shield) are left out.

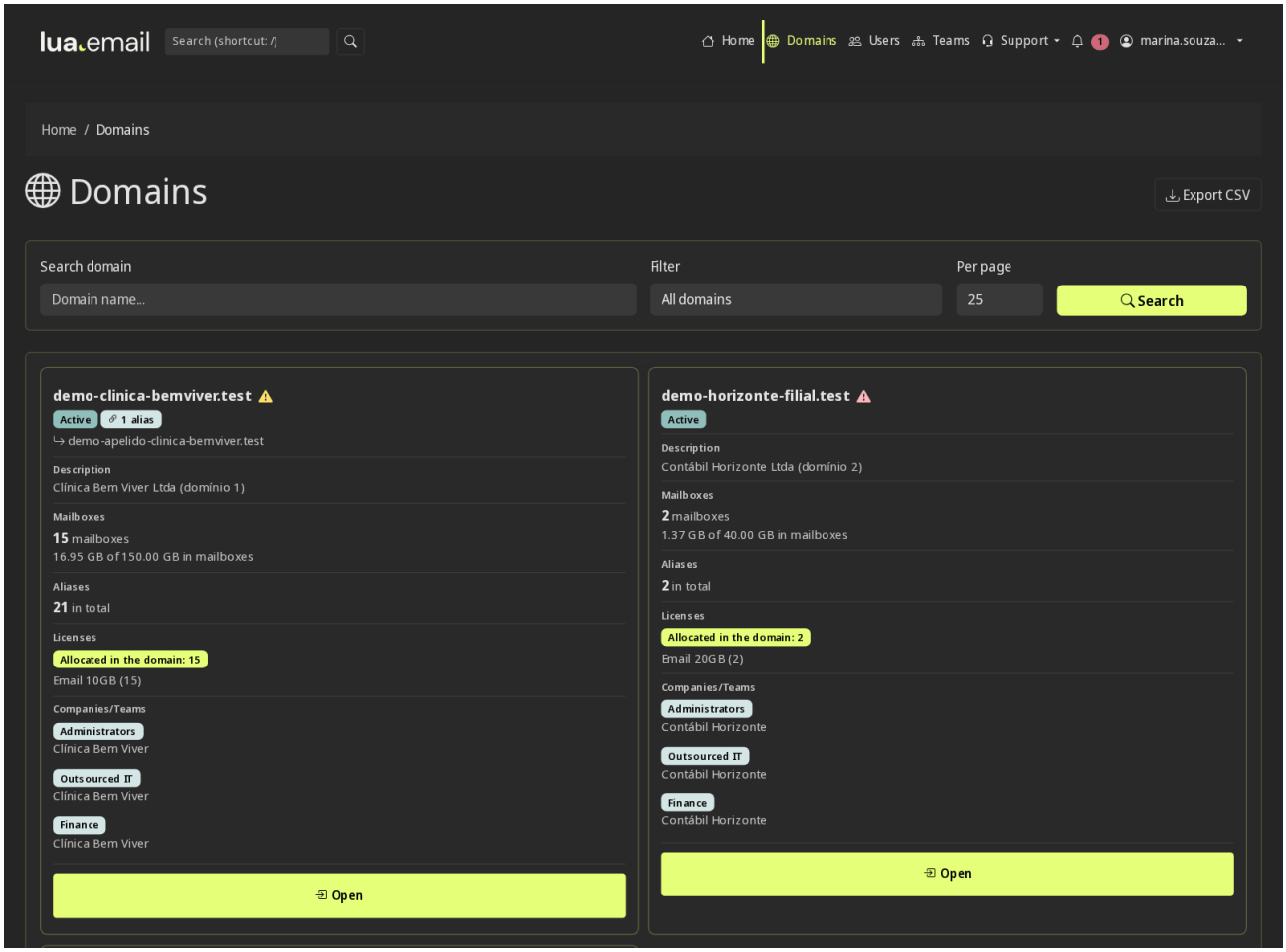


Figure 47: The triangle next to the domain leads to Domain health: red when it affects email delivery, yellow in the other cases.

9. Service groups: schedule, session, directory and email

A **service group** brings together mailboxes of the company, such as the field team or sales, for a few purposes: the hours when access is blocked, the browser session length, which IPs the mailboxes can sign in from, whether they can use email apps or only webmail, an address directory that also becomes a group in Colabora, and an email address that delivers to everyone in the group.

In addition, the **Mobile** tab sets the security requirements for phones with an Exchange account.

Every domain has the **Default** group, with all mailboxes and no rules. The rules live in the groups you create. A mailbox in more than one group follows the most restrictive rule.

Creating a group

1. In **Email → Service groups**, click **New group** and give it a name (for example, "Field team"). The name can't be the same as the address of a mailbox or alias in the domain: a group called "Sales" in a domain that already has `sales@` is rejected.
2. In the **Mailboxes** tab, type part of the name or address, choose the mailboxes from the list and click **Add**.
3. In the **Access hours** tab, turn on **Restrict access hours** and mark the blocked days and hours. The **Use "outside business hours"** button fills it in for you: Monday to Friday from 6 PM to 7 AM, and all day Saturday and Sunday.
4. If the group should also be locked out on holidays, turn on **Block the whole day on the domain's holidays**.
5. In the **Web session** tab, decide whether people can use "stay signed in" and after how many hours the session ends.
6. If you want, publish the group in the **Directory** tab and give it an address in the **Email** tab (both explained below).

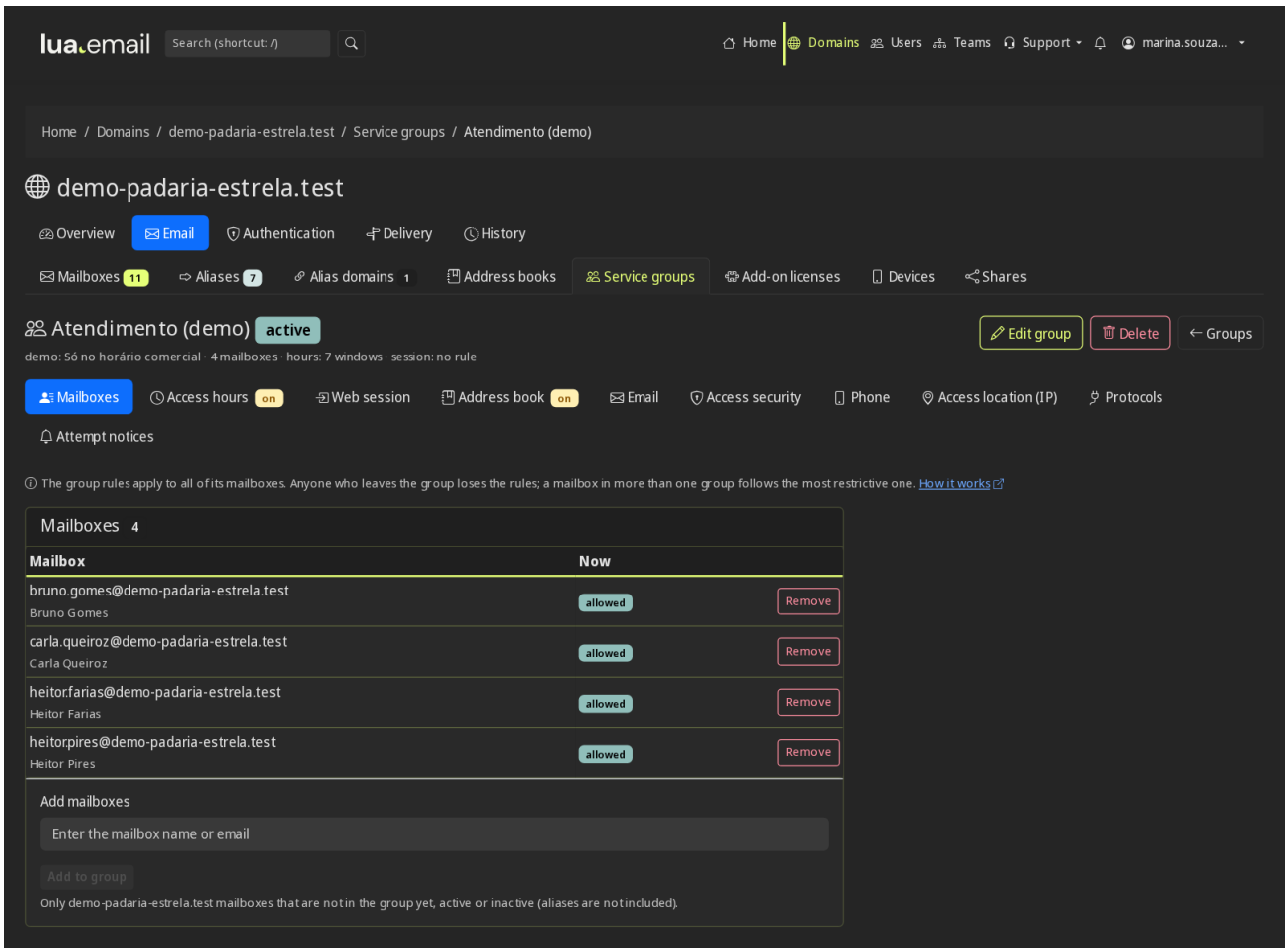


Figure 48: The group's mailboxes.

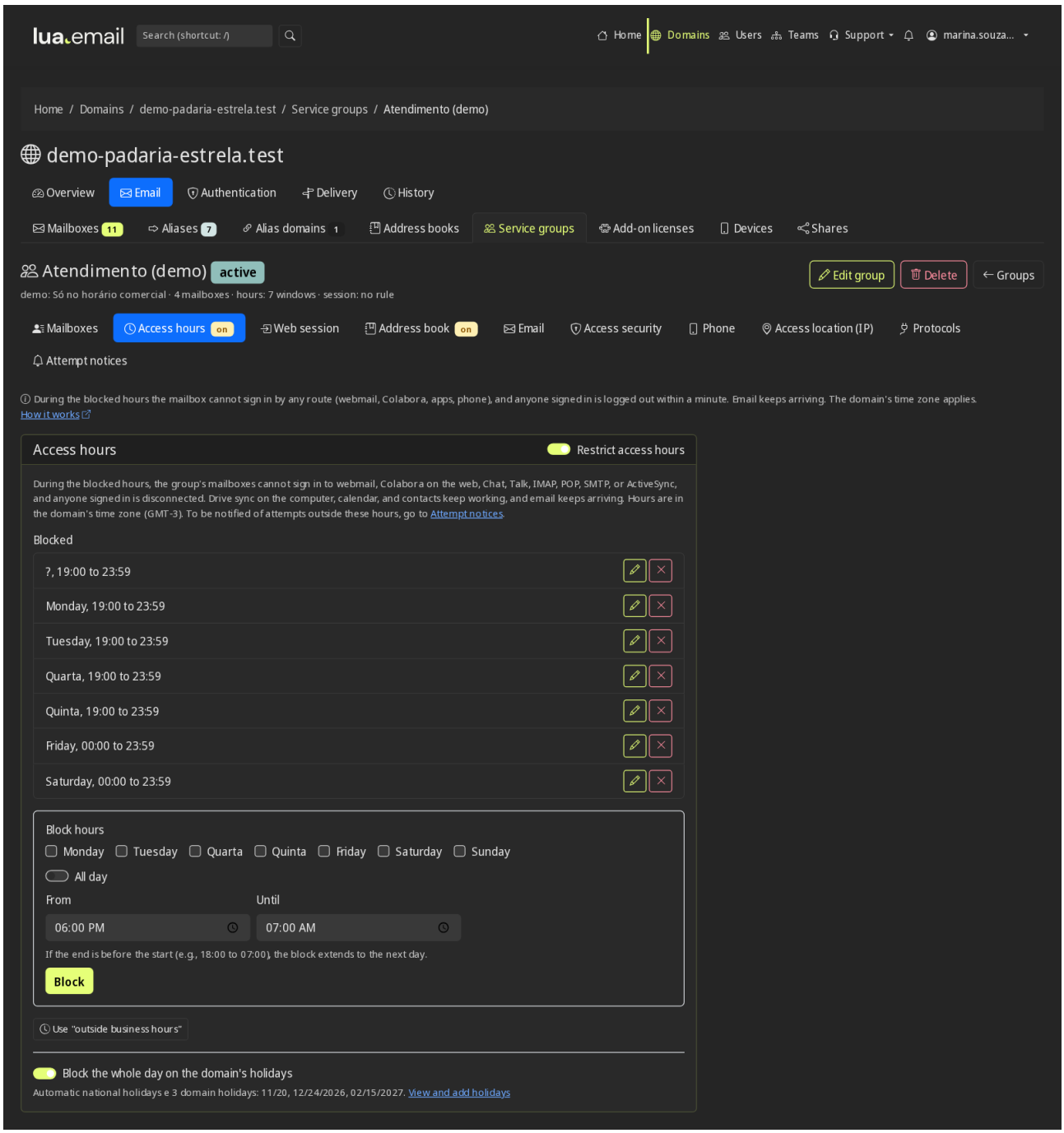


Figure 49: Block outside business hours, including holidays.

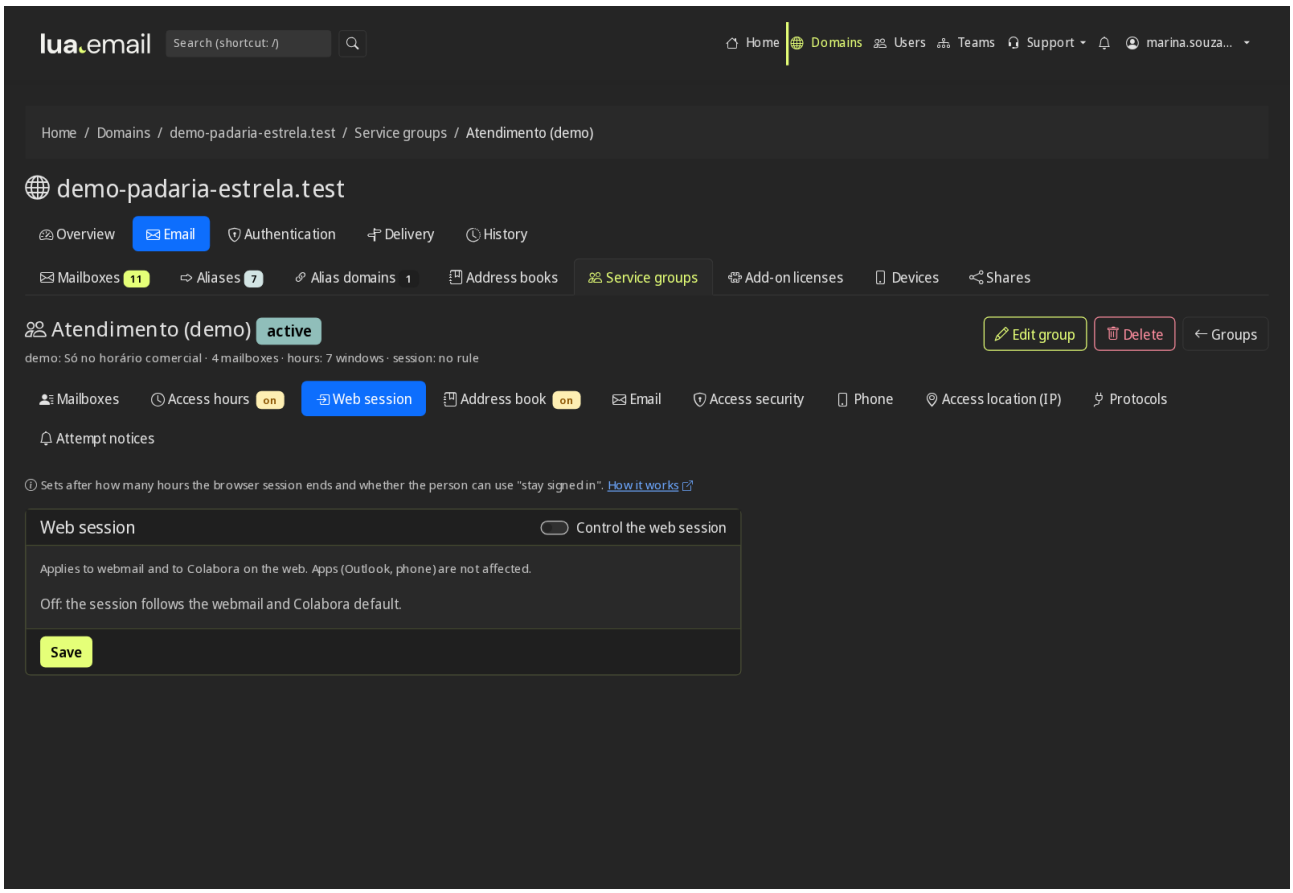


Figure 50: The Web session tab: turn the option on to set how many hours the session lasts and whether "keep me signed in" is allowed.

The hours apply in the **domain's time zone**, which is set in **Overview → Domain settings**. The holidays and working hours are on that same screen.

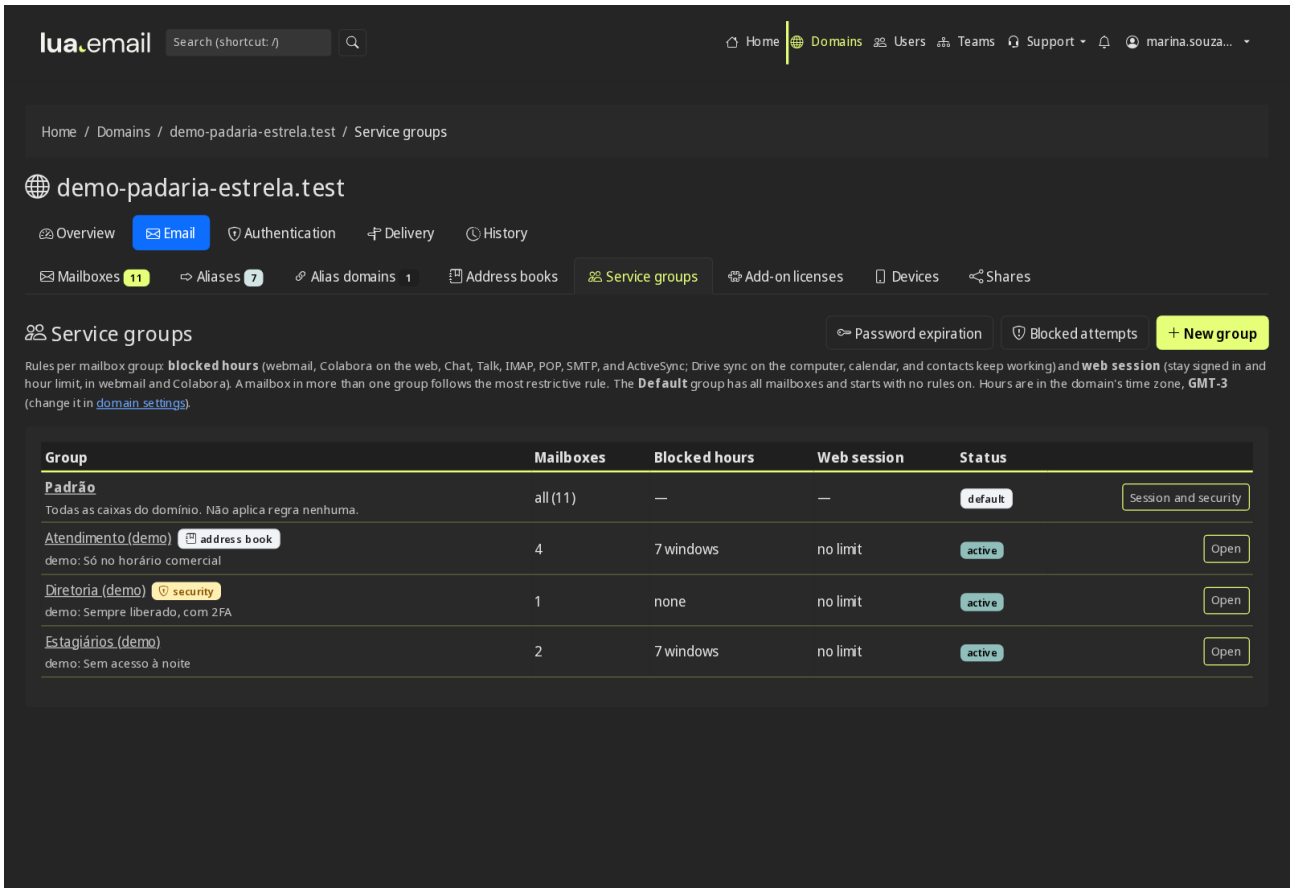


Figure 51: The group list shows a summary of each rule.

What happens in each service

During blocked hours, the rule applies to every way of getting into the mailbox. Anyone already signed in is signed out within a minute. Email **keeps arriving** as usual: the person finds everything in the mailbox when access reopens.

Service	What the person sees during blocked hours
Webmail	Goes back to the sign-in screen with the message "Access outside the hours allowed by your company."
Colabora on the web (Drive, Chat, Talk)	"Session ended" page, with the same reason.
Email app (IMAP or POP)	The app can't connect and shows the message "Access outside the hours allowed by your company."
Sending from the app (SMTP)	Sending is rejected with error `554 5.7.1` and the same reason. The app does not ask for the password again.
Phone with an Exchange account (ActiveSync)	Stops syncing until access reopens.
Desktop Drive, calendar and contacts	Keep working.
Email delivery	No change: messages arrive as usual.

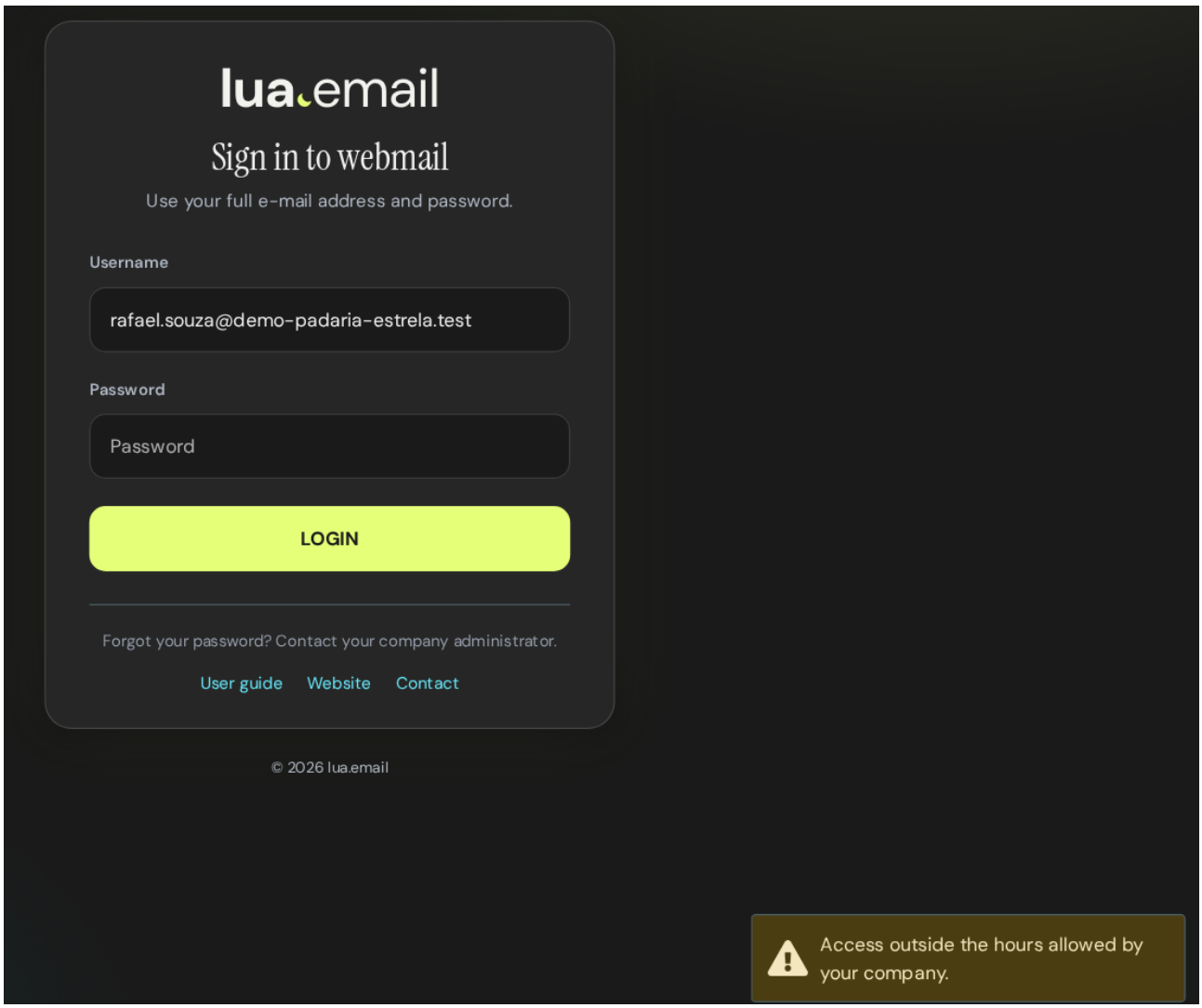


Figure 52: Webmail during blocked hours.

The **web session** applies only to webmail and to Colabora in the browser. Once the hour limit since sign-in has passed, the person signs in again. With "stay signed in" not allowed, the session ends when the browser is closed. Apps and phones are not affected by this part.

For the whole domain: the web session can also be set in the **Default** group, and it applies to all mailboxes, including those created later. If the mailbox is also in another group with a session rule, the most restrictive one applies: the lowest hour limit and, if any group doesn't allow it, no "stay signed in".

When you give someone access outside their hours (by removing the mailbox from the group or changing the schedule), the change takes effect within a minute. If the person complains about being blocked, first check whether they are in any group: the mailbox page shows it. A wrong password is a different matter and appears as "wrong password" in tracking.

Access location: only from IPs the company knows

In the **Access location (IP)** tab, you list the addresses the group's mailboxes can sign in from, such as headquarters, a branch office or the company VPN. With at least one address on the list, anyone trying to sign in from elsewhere is blocked, even with the right password. With no addresses, nothing changes.

1. Open the group and the **Access location (IP)** tab.
2. In **Add address**, enter the IP. For a whole network, also enter the **mask**, for example 28. Without a mask, it applies only to that one address.

3 Write a **description** (Headquarters, Joinville branch, VPN) and click **Add**.

4 To apply it to the whole domain, do the same in the **Default** group.

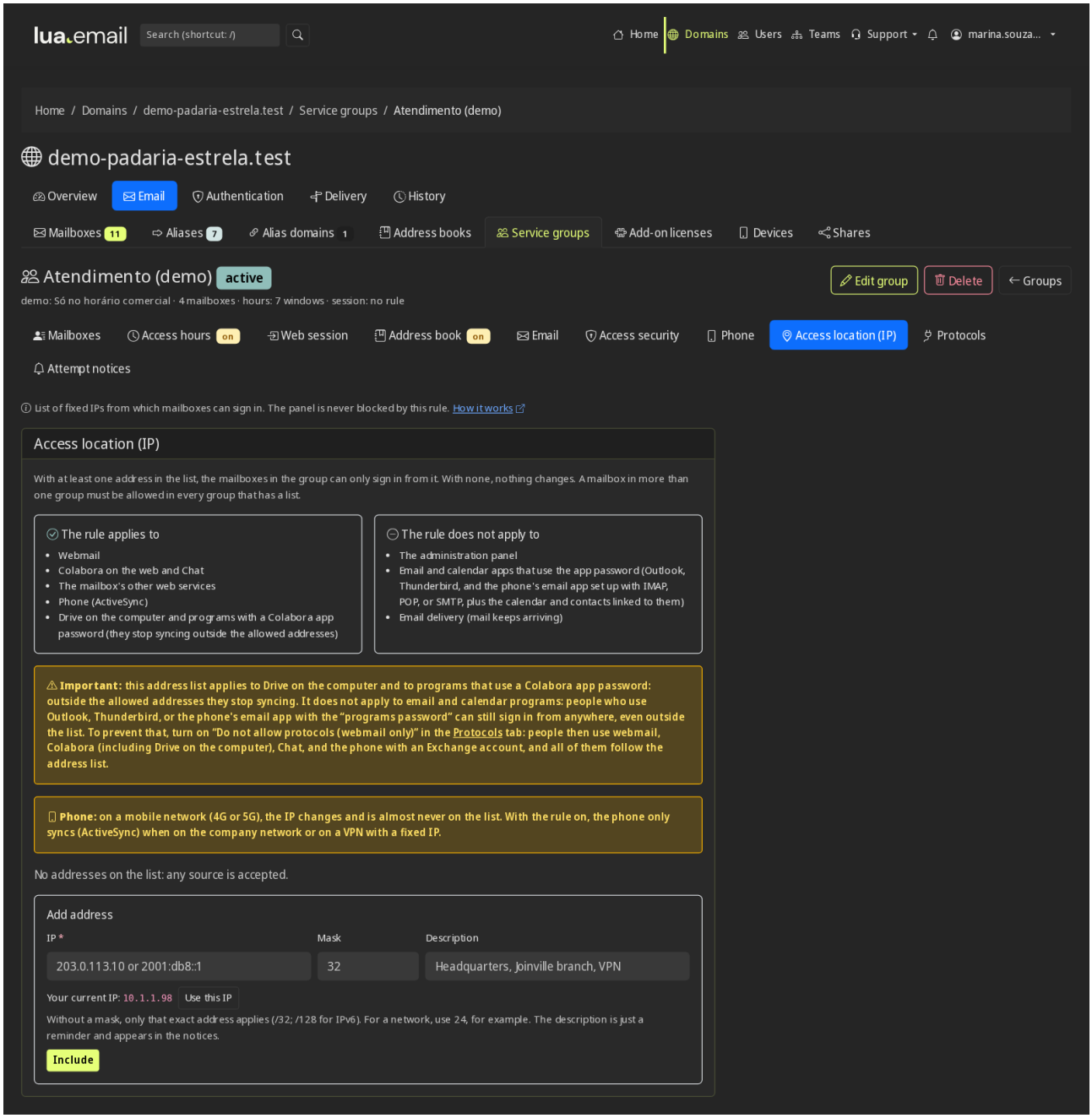


Figure 53: The group's IP list, with what the rule covers and what it doesn't (real screen, fictional data).

Service	Does the IP rule apply?
Webmail	Sim.
Colabora on the web and Chat, including the Chat app on the phone	Sim.
Phone with an Exchange account (ActiveSync)	Sim.

Colabora calendar, contacts and files in apps (CalDAV, CardDAV and WebDAV), with the account password	Sim.
Outlook, Thunderbird and the phone email app (IMAP, POP and SMTP with the app password) and calendar and contacts with the token (`dav.lua.email`)	No. To block these, use webmail only.
Desktop Drive and other Colabora apps with an app password	Yes. Outside the allowed IPs, they stop syncing.
The management panel itself	Never: the administrator is not locked out.
Email delivery	No change: messages keep arriving.

The tab itself shows this notice in an **Important** box, with the path to the **Do not allow protocols (webmail only)** option. If webmail only is already on for the group, the notice says the apps are turned off. See also the notice about the IP list.

- **Mask:** `/32` (or `/128` in IPv6) is a single address. `/24` covers 256 addresses. A very wide mask, such as `/8`, asks for confirmation before saving.
- **Duplicate or invalid:** the panel rejects it and gives the reason. The description is only a reminder and appears in the alerts.
- **More than one group:** if the mailbox is in groups that have a list, it must be allowed in all of them (the most restrictive applies).
- **Your current IP:** the screen shows the address you are connecting from and the **Use this IP** button. When you add the first address, the panel confirms how many mailboxes will only be able to sign in from there, and it also asks for confirmation before you remove an address.
- **What the person sees:** "Access not allowed from this location. Contact your company's administrator." The message only appears with the right password; anyone who gets the password wrong sees the normal password error.
- **When the change takes effect:** in webmail and Colabora, the rule is checked every minute, so a change can take up to 60 seconds, and anyone signed in from another location is signed out within that time.

Watch out for phones. On the mobile network (4G and 5G) the IP changes and is almost never on the list. With the rule on, a phone with an Exchange account only syncs on the company network or over a VPN with a fixed IP. Let the team know before turning it on.

Use the company's public IP. The rule checks the address the person uses to reach lua.email, not the one on the internal network: addresses such as `192.168.x.x` and `10.x.x.x` don't work. The company's internet connection needs a fixed IP, otherwise the list stops working when the provider changes the address. If you publish webmail or Colabora through your own proxy, using the company's address, the proxy must pass along the real IP of whoever is connecting, otherwise everyone appears with the proxy's IP; talk to support before turning the rule on.

What to combine with the rule. The list controls where people sign in from, and it does not replace two-step verification or webmail only. To keep email on the company network only, turn on both rules in the same group: the list covers webmail, Colabora and phones, and webmail only covers the apps.

Webmail only: no email apps

In the **Protocols** tab, the **Don't allow protocols (webmail only)** option stops the group's mailboxes from using the app password. In practice: no Outlook, Thunderbird or similar apps over IMAP, POP or SMTP, and no calendar and contacts in apps through the token address. The mailboxes keep using webmail, Colabora, Chat and the phone's Exchange account, which sign in with the webmail password, and keep receiving email normally.

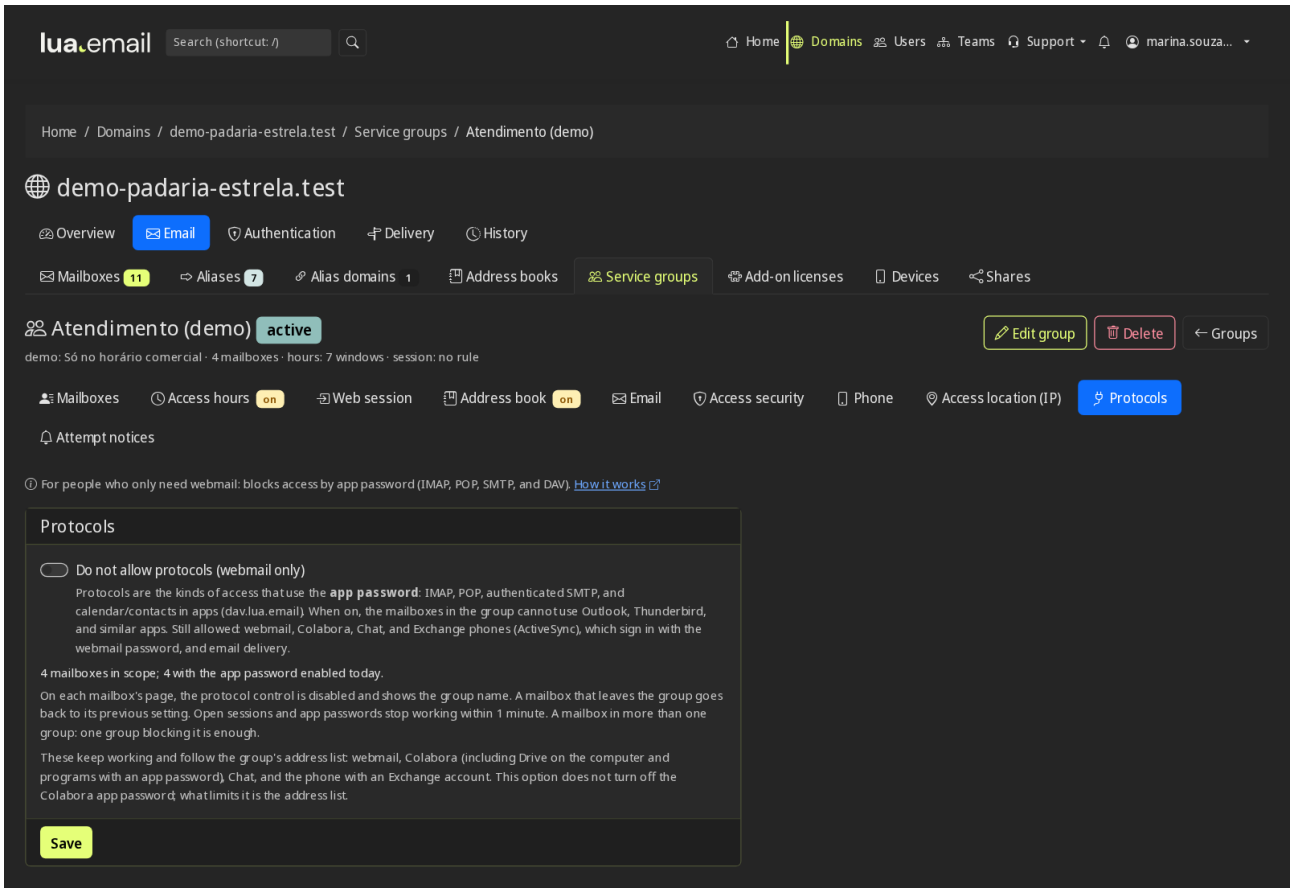


Figure 54: The "Webmail only" option (real screen, fictional data).

On the page of each mailbox in the group, the protocols control and the button to generate an app password are disabled, showing the group's name. It is not just the screen: the server also refuses to allow access by apps.

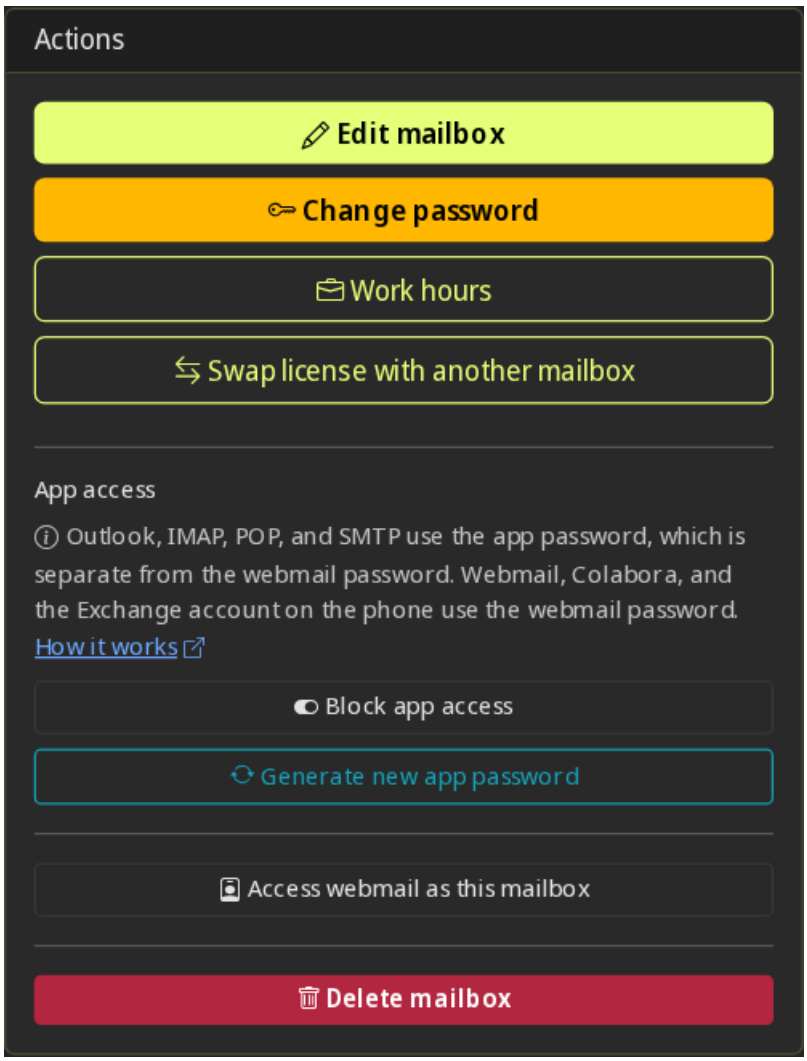


Figure 55: On the mailbox, app access can be blocked; when the group blocks it, the notice says which group is in charge (real screen, fictional data).

- **Leaving the group:** the mailbox goes back to what it had before. Anyone who used Outlook can use it again, with the same app password.
- **Already connected:** connections opened by apps drop within a minute.
- **What stays the same:** the Drive on your computer uses a Colabora app password and does not go through this rule, and the phone's Exchange account keeps syncing. To limit the phone and the Drive on your computer, use the IP list.
- **More than one group:** it takes just one group blocking for the mailbox to be left without protocols. In the Default group, it applies to the whole domain, including new mailboxes.

Alerts for blocked attempts

When someone is blocked for an **unallowed location** or **outside hours**, the panel can alert the administrators. Choose in the **Attempt alerts** tab, separately for each case: **Don't alert** (default), **Panel notifications only** or **By email and in panel notifications**. In the email you can include the person themselves and one extra address, such as the company's security contact.

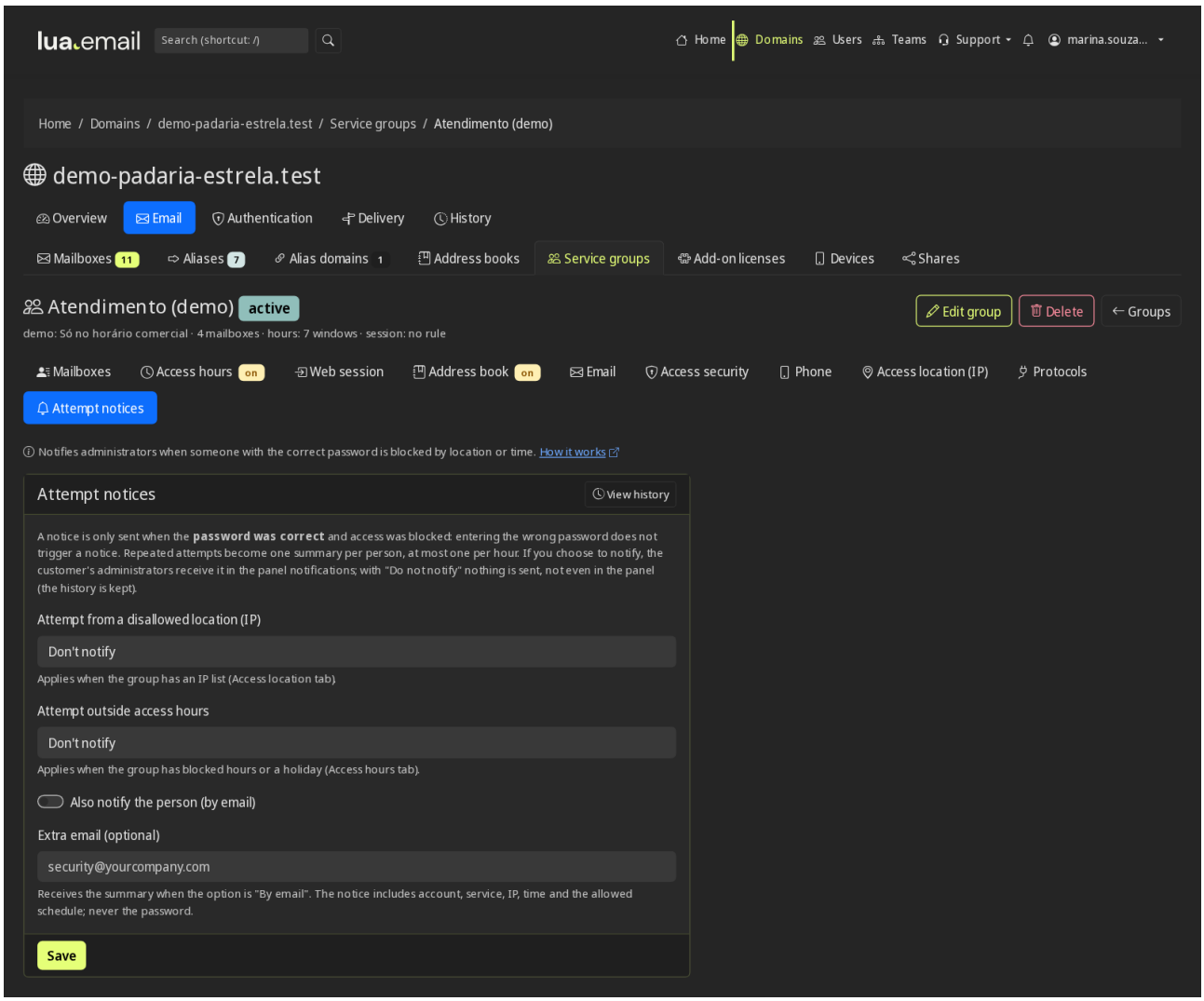


Figure 56: Alerts by email or in the panel only, for IP and for hours (real screen, fictional data).

- **Only with the right password.** The alert is only sent when the password was correct and access was blocked. A wrong password does not generate an alert, and no one can use this feature to send email to third parties.
- **No flood.** Repeated attempts become one summary per person, at most one per hour, with the account, the service, the IP, the time and the first and last attempts.
- **Who receives it.** The customer's administrators see it in the panel bell. By email, it goes to the administrators, to the person themselves (if selected) and to the extra address, which must belong to a company domain or to a panel user.
- **Where the alerts come from.** Webmail, Colabora, Chat and phones with an Exchange account. The block outside hours on IMAP, POP and SMTP still applies, but it does not generate an alert or appear in the history.

The history is in **Service groups → Blocked attempts**, with filters by type, service and mailbox. It keeps 90 days.

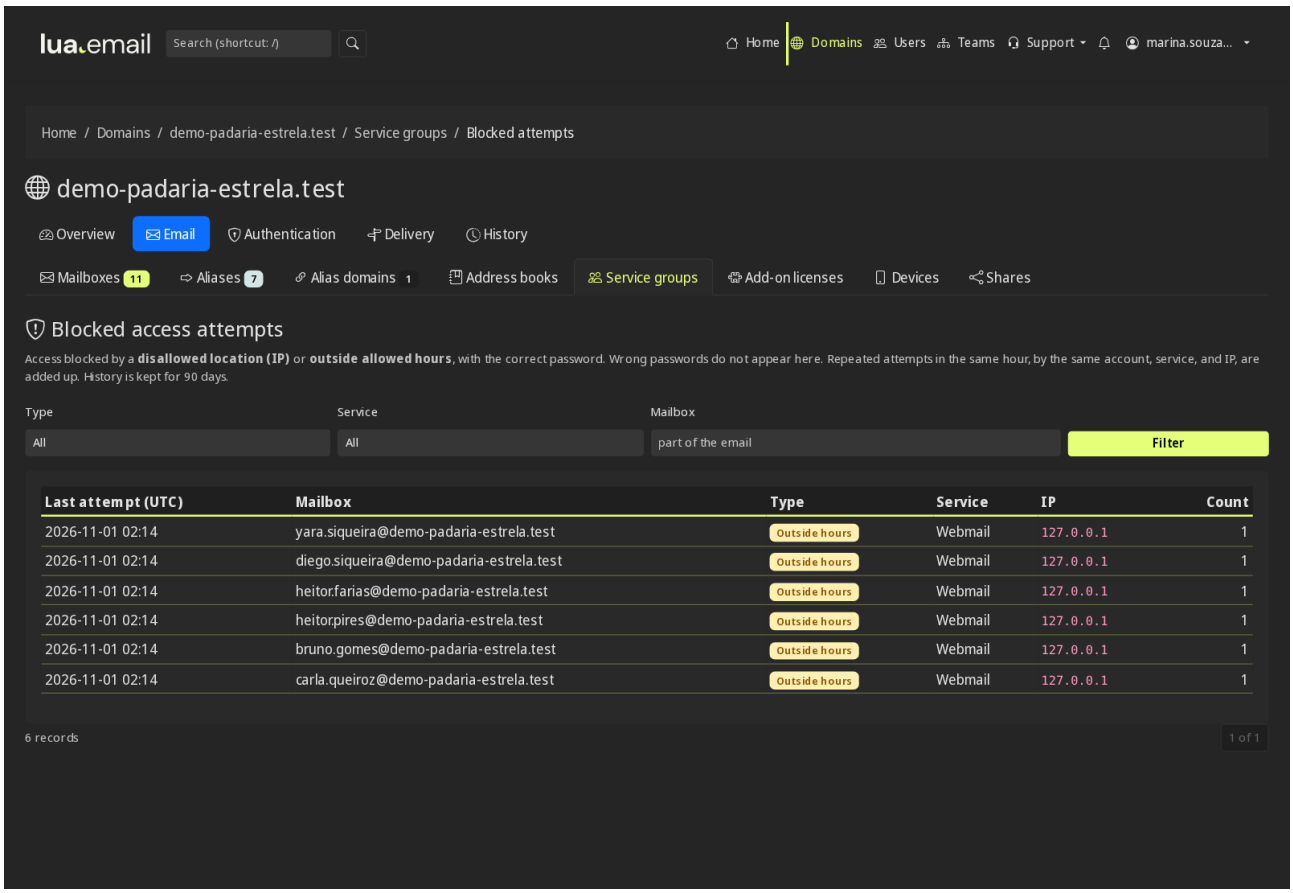


Figure 57: The history of blocked attempts (real screen, fictional data).

Holidays in the calendar and working hours

In **Overview → Domain settings** there is a single holiday registry for the domain. The same registry serves the groups' access hours (the option to block on holidays) and the mailboxes' **calendar**. National holidays and the Holidays calendar come **turned on in all domains**; if your company doesn't want them, turn them off here.

- **Automatic national holidays:** they are added by themselves every year, including the ones with moving dates (Carnival, Good Friday, Corpus Christi), with no registration needed. **Include optional holidays** adds the days many companies also take off.
- **Domain holidays:** register the ones for your city and state, the company's anniversary, a break or a bridge day. **Register holiday** opens a window: enter a name and date; for a period, also fill in "until" (up to 31 days); check **Repeats every year** when it applies. A date that is already an automatic national holiday is rejected, and the warning appears inside the window, without losing what you typed. When you add it, the list updates right away. To remove a registered one, use **Remove**.
- **Show holidays in the calendar:** when on, all mailboxes in the domain get a read-only **Holidays** calendar, in webmail, in Colabora, on phones and in calendar apps. It appears within a few minutes. Holidays don't take up anyone's calendar and don't change availability: not every company stops on holidays.

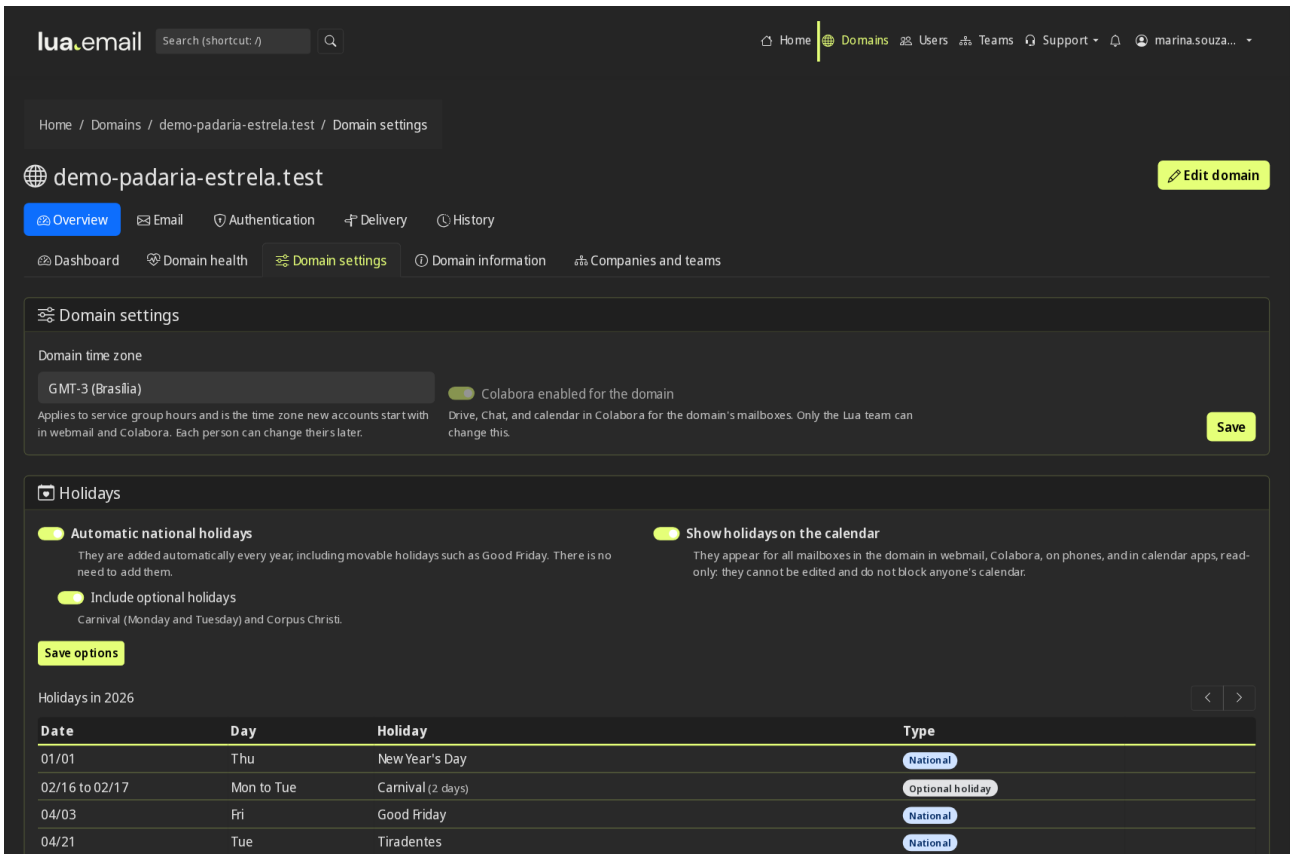


Figure 58: Domain holidays: automatic national ones, optional holidays and your company's own. The "Holiday added." message appears in the corner after registering (real screen, fictional data).

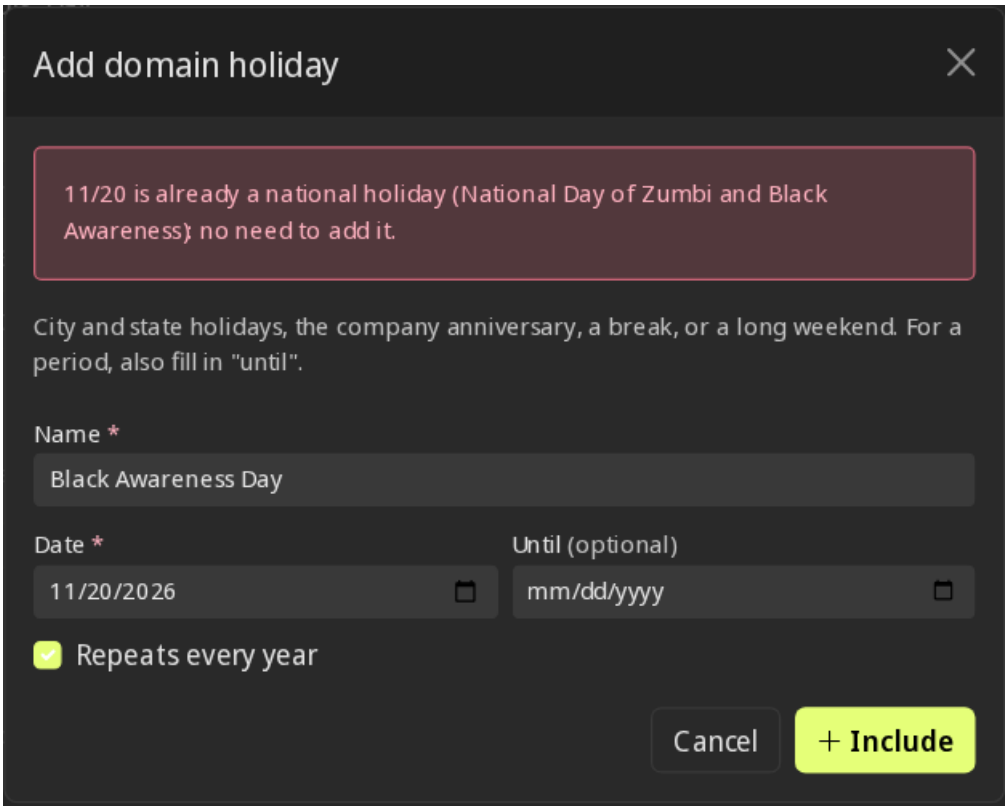


Figure 59: Register holiday: a date that is already a national holiday is rejected, with the warning inside the window (real screen, fictional data).

Working hours. Right below, set the domain's default working hours: one period per day (for example, Monday to Friday, 8 AM to 6 PM) and an optional break, the same for all selected days, such as lunch. Outside those

hours, anyone trying to schedule a meeting with the person sees "Outside working hours" in the availability view, and their calendar shows those hours dimmed. With no hours set, the person shows as free all day, as before.

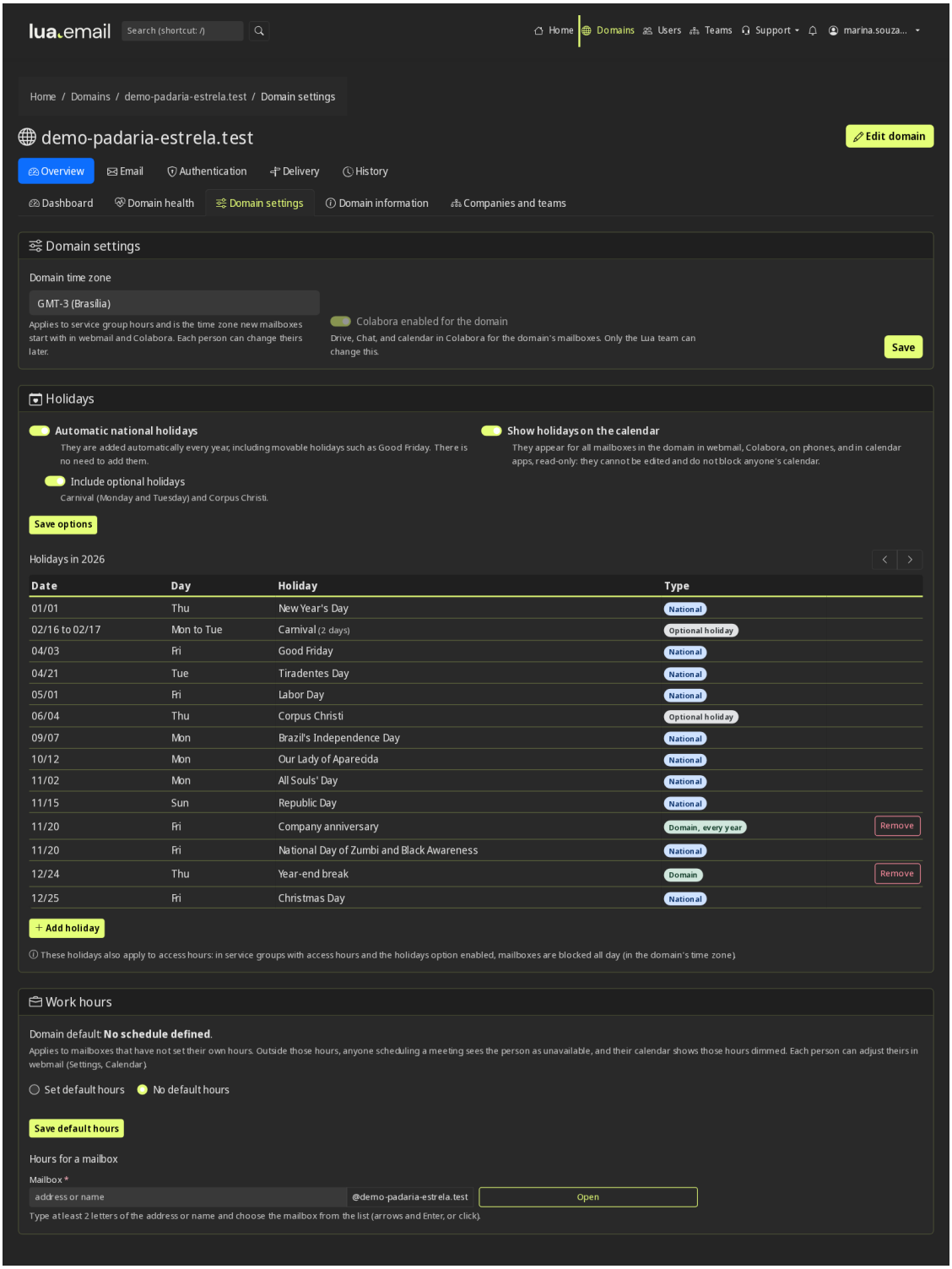


Figure 60: The domain's default working hours and the mailboxes with their own hours (real screen, fictional data).

The **Mailbox hours** field searches as you type: from 2 letters of the address or name, it shows up to 10 mailboxes in the domain, each with the **own hours** or **follows the default** tag. Choose with the arrow keys and Enter, or with a click, and the mailbox's hours open. With a single result, Enter opens the mailbox right away.



Figure 61: The mailbox search shows suggestions as you type (real screen, fictional data).

Each mailbox can have its own: in the actions box on the mailbox page, click **Working hours** (or use the **Mailbox hours** field on the settings screen itself). A window opens where you choose **follow the default** or **own hours** and click **Save**; **Back** closes it without changing anything. The **Mailboxes with their own hours** list summarizes who differs from the default. Each person can also adjust their own in Settings, Calendar, in webmail. Only the domain administrator and the Lua team can change the holidays and the default.

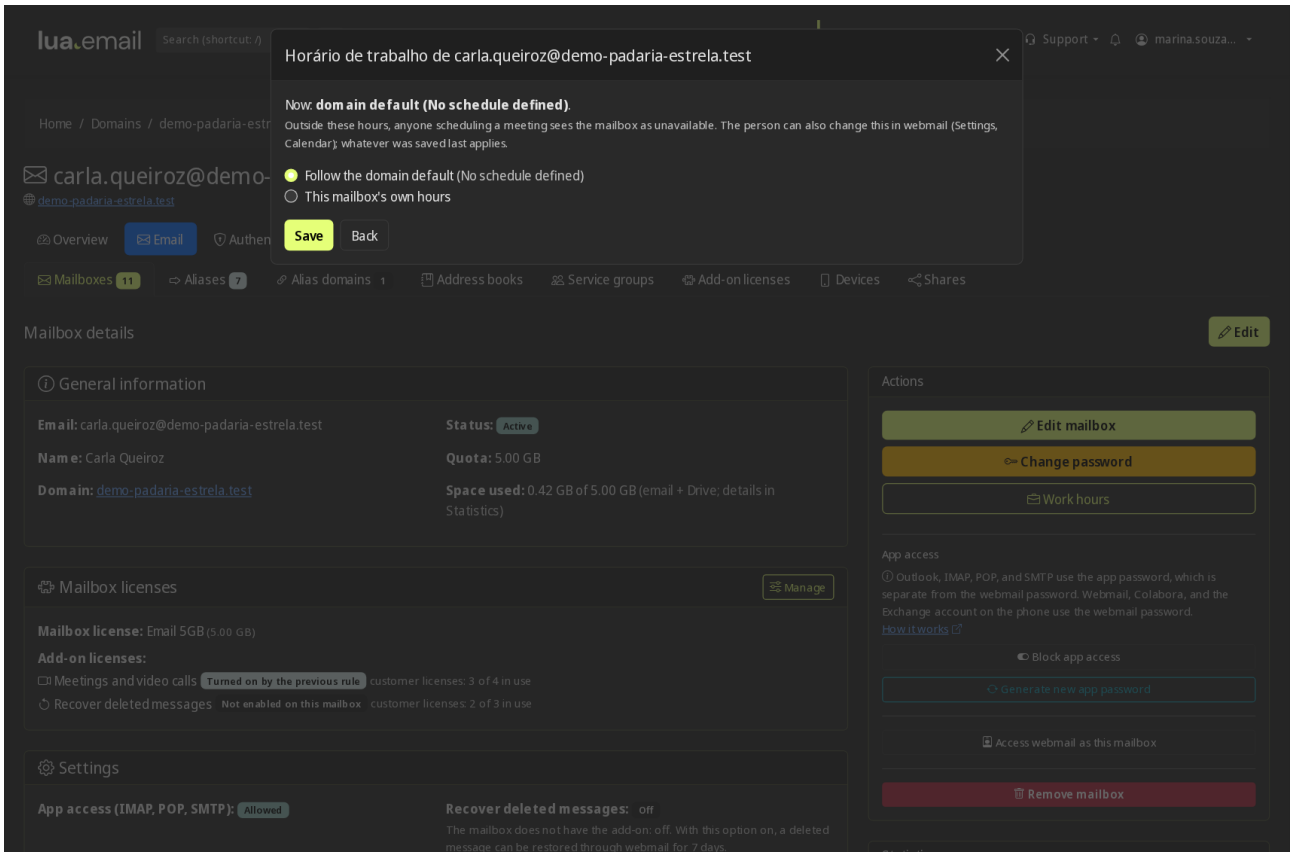


Figure 62: A mailbox's hours open in a window, on top of the mailbox page (real screen, fictional data).

Phone: screen lock and wipe after wrong passcodes

In the **Mobile** tab of the group (including the **Default** group, which applies to the whole domain) you set what a phone with an Exchange account must require. The rule applies only to people using the Exchange account. Apps over IMAP, POP and SMTP are not affected.

Option on screen	What the device will require
Level 1: screen lock required	Any screen lock.
Level 2: PIN of 4 or more, no sequences	PIN of 4 digits or more, with no repeated digits or sequences (or a password).

Level 3: letters and numbers, 6 or more	On iPhone, a password with letters and numbers, 6 characters or more. On Android, a password of 6 or more, or a PIN of 8 or more: Android does not require letters.
Wipe after N wrong passcodes (4 to 16)	The device wipes itself after N wrong passcodes on the lock screen.
Password expiration (1 to 730 days), password history (1 to 50), minimum special characters (1 to 4), time until the screen locks (1 to 60 minutes) and block the camera	Each one has the **applies to: iPhone only** badge. Other devices ignore these rules. Expiration, history and special characters require a screen lock to be on.

Four badges appear next to the options: *applies to: iPhone*, *Android and Outlook* (level 1), *applies to: iPhone and Android* (levels 2 and 3; in Outlook it only requires the lock), each device's badge on "wipe after wrong passcodes", and *applies to: iPhone only*. The screen only shows what at least one device can meet. According to the manufacturers, current Android does not let the email app require password expiration, a blocked camera, a memory card or encryption, which is why those options are not here.

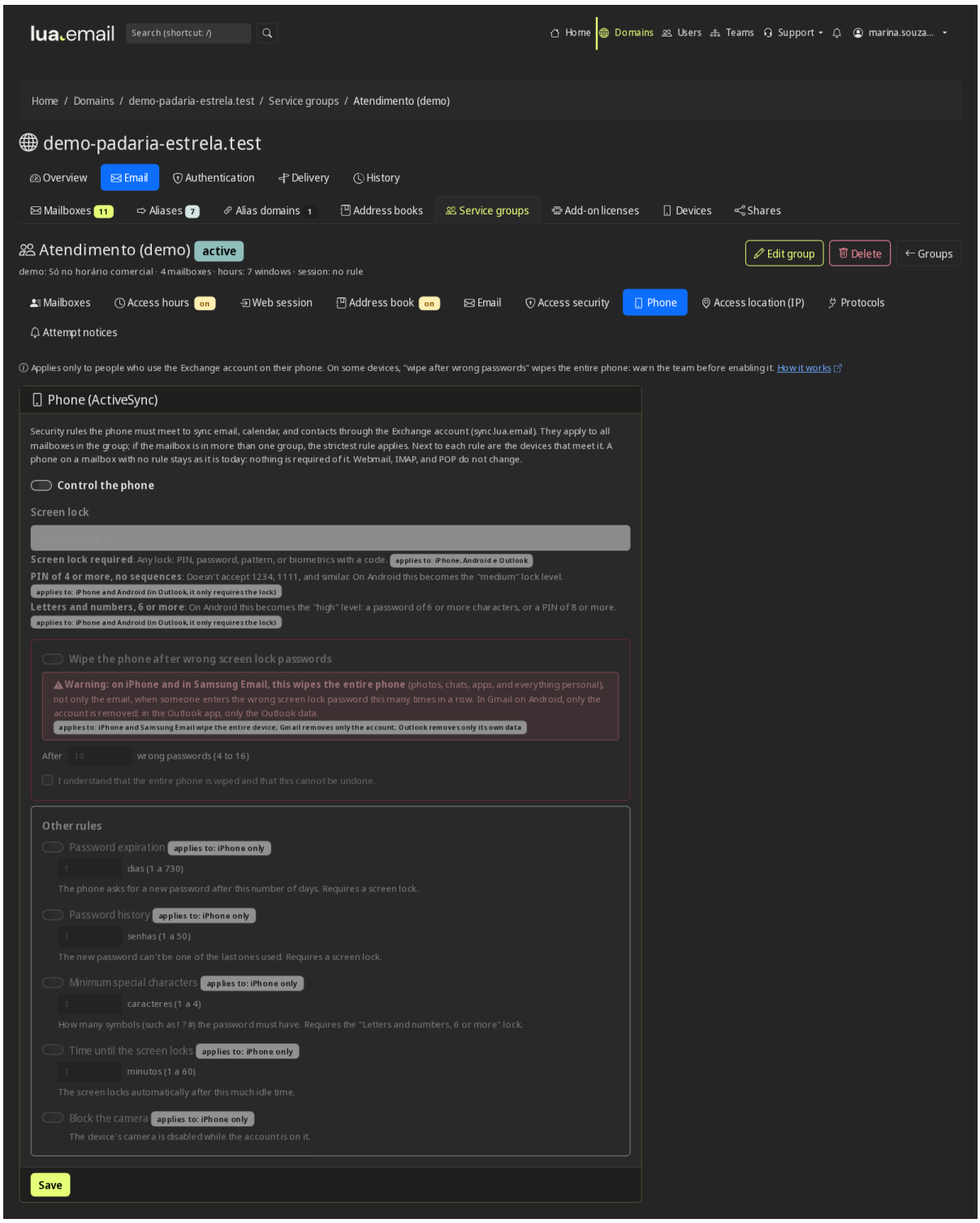


Figure 63: The group's Phone tab, with the rules that apply to the device.

Be careful with "wipe after wrong passcodes". On some devices the entire phone is wiped, including the person's photos and apps. The screen shows this warning and only lets you save after you confirm you understand. Prefer a high number (for example, 10) and let the team know before turning it on.

What happens in each app:

Device and app	Screen lock (levels 1 to 3)	Wipe after N wrong passcodes
iPhone, Mail	Requires the passcode, at the requested level.	Wipes the **entire iPhone**.

Samsung, Samsung Email	Requires the lock, according to the Android levels.	Wipes the **entire device**.
Android, Google's email app	Requires the lock, according to the Android levels.	Removes **only the account** from the app.
Outlook for iPhone and Android	Requires the lock (the length only applies on Android).	Wipes **only the Outlook data**.

When there is more than one group. The mailbox's groups and the Default group all count, and the most restrictive applies: the highest lock level and the lowest number of attempts. The mailbox screen shows the policy that applies to it. A mailbox with no rules stays as it always was, with nothing required of the device.

On the device. On the next sync (within about a minute), the phone shows the policy and asks to accept it. Anyone who accepted appears with "Policy accepted" in the device list. If you remove the rule, the device drops the requirements.

According to the manufacturers: the table comes from what each app supports through the protocol and from Apple, Google and Microsoft documentation. We have not checked it on a real device yet. Before turning it on for the whole domain, test it with an iPhone and an Android of your own.

Step by step: require a passcode on employees' phones

For domain administrators. It takes about five minutes. Before you start, decide whether the rule applies to **everyone** (Default group) or just one team (a service group of yours).

1. Open the domain and go to **Email → Service groups**.
2. Click the group: **Default** for the whole domain, or the team's group.
3. Open the **Mobile** tab and turn on **Control the phone**. Without this switch, the options are grayed out.
4. Under **Screen lock**, choose the level: **1** (any lock), **2** (PIN of 4 or more, no sequences) or **3** (letters and numbers, 6 or more). If in doubt, start with 2.
5. If you like, turn on **Wipe the phone after wrong passwords**. Read the red warning: on iPhone and Samsung Email the **entire device** is wiped, in Google's email app only the account, and in Outlook only its own data. Choose a high number (we suggest 10) and check **I understand that the entire phone is wiped**. Without that checkbox, the screen won't let you save.
6. If you want, turn on password expiration, history, special characters, time until the screen locks or camera blocking under **Other rules**. All of them apply only to iPhone, as the badge says.
7. Click **Save**.
8. Check it on a mailbox in the group: on the mailbox page, the **Connected devices** box shows the **Phone policy** that applies to it and which group it comes from.
9. Let the team know beforehand: on the next sync (within about a minute), the phone shows the security policy and asks to accept it. Anyone with no screen lock is prompted to create one. Anyone who accepted appears with the date under **Policy accepted** in the domain's **Devices** tab.

- **To undo it:** turn off **Control the phone** and save. The device drops the requirements on the next sync.
- **More than one group:** the most restrictive applies, counting Default too. The mailbox page shows the result.
- **Who isn't affected:** apps over IMAP, POP and SMTP, and webmail.

Address book and group in Colabora

Turn on **Publish as domain directory** in the group's **Directory** tab. Two things happen:

- the group's mailboxes become an **address directory** in the webmail of all mailboxes in the domain, read-only;
- the group is created in Colabora with the same name. Group members can find the group by name and share with it, all at once, folders, documents, whiteboards, task boards and calendars, and add the whole group to a Chat conversation. The step by step is in the Colabora manual.

Only people in the group see the group and share with it. No one from another company can find the group. Anyone who joins the group starts seeing what has already been shared with it, and anyone who leaves stops seeing it, within 1 minute. In Chat conversations, whoever joins the group joins the conversation, and whoever leaves is removed.

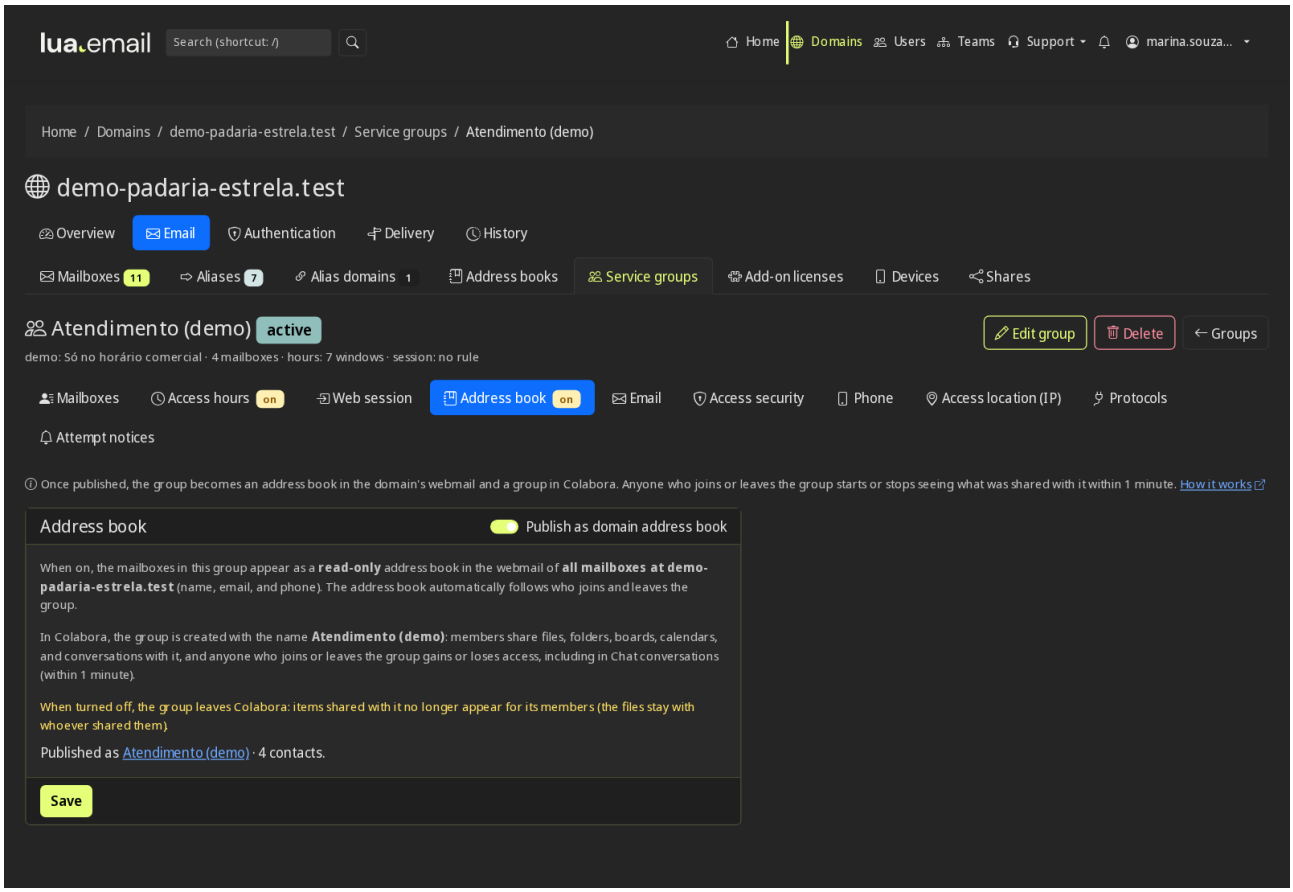


Figure 64: Publishing the group: directory in webmail and group in Colabora.

Turning off publishing removes the directory and the group from Colabora. What had been shared with the group stops appearing for the members, but the files stay with whoever shared them.

Group email

In the **Email** tab, the group gets an address that delivers to all of its mailboxes, such as `obra@` for the field team. It is an alias that the group maintains itself: no one has to remember to add newcomers or remove people who left.

1. Type the part before the @ and click **Turn on email**. The address can't belong to an existing mailbox or alias or start with `grp-`.
2. Check under **Delivers to** the mailboxes that receive it now. Only the group's **active** mailboxes receive it.

3 Under **Who can send**, the email starts out accepting only senders from the domain, which avoids spam to the whole group at once. You can open it to any sender or limit it to a list of addresses and domains (for example, a supplier).

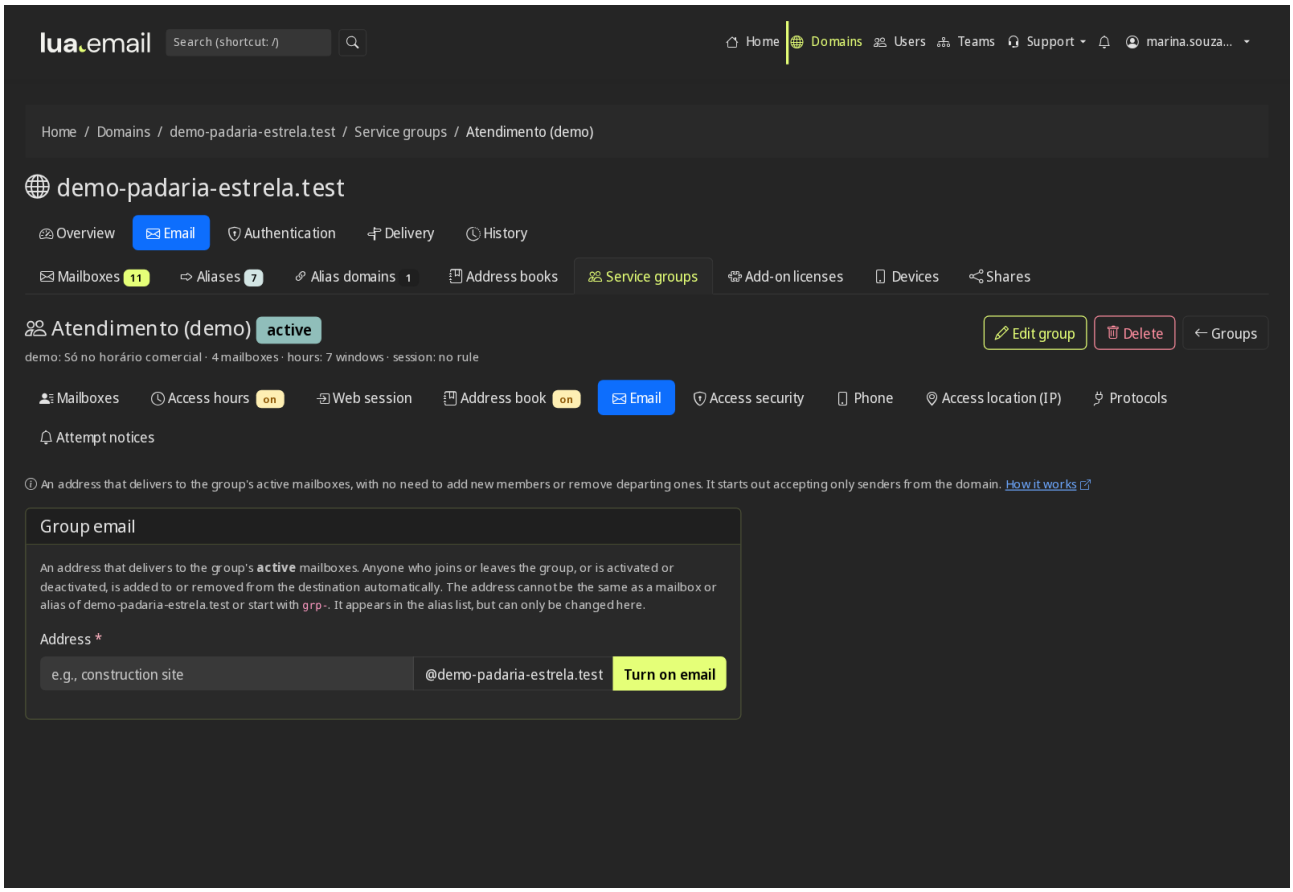


Figure 65: The group's email: delivery to active mailboxes, only from senders in the domain.

To change the address, type the new one and click **Change address**. **Turn off email** deletes the alias, and so does deleting the group. In the alias list, it appears as group email and can only be changed here. If the group is left with no active mailbox, the address stops receiving until someone comes back.

When a mailbox is deactivated or reactivated

Deactivating a mailbox does not remove it from the group: it just stops counting while it is deactivated. That way, when you reactivate it, everything comes back on its own, with no need to add it again.

What happens to the mailbox	Group in Colabora, directory and group email
Deactivated (or in the removal queue)	Leaves all three. It stays listed in the group, with the "out for now" tag on the mailbox page.
Reactivated	Returns to all three.
Removed from the group	Leaves all three.
Permanently removed	Leaves the group and all three.

In the panel and in email the change takes effect immediately; in Colabora, within 1 minute, including in Chat conversations. Every night the panel checks the groups and fixes any difference.

When to use it and use cases

A service group handles what the **mailboxes** can do and how the team appears to others. Who can **administer the panel** is a team matter: they are different things, and the two work together.

Situation	How to set it up
Contractors and shift workers who should only have access during work hours	A group with their mailboxes and the **access hours** set to Monday to Friday, business hours. Outside them, webmail, the email app and the phone can't sign in, and email keeps arriving to be read the next day. Use the domain's holidays so you don't need an exception for each date.
Front desk, reception or a shared computer	A group with a short **web session** and no "stay signed in": the person is signed out of webmail and Colabora when they close the browser or after the defined hours.
Field team, sales, projects that work together	A group with the **directory** turned on. The team appears as an address list and becomes a group in Colabora, to share a folder, a board, a Kanban or a conversation with everyone at once, without picking people one by one. Whoever joins or leaves the group changes access within a minute.
Team address (`sales@`, `obra@`)	The **group email** delivers to all of its active mailboxes. Keep it internal only (receives just from inside the domain) for addresses such as `hr@`, or open, or limited to a list of senders.
Finance and executives with more protection	A group with **Access security**: mandatory two-step verification for all of its mailboxes.
A team that only needs webmail	A group with **Protocols** blocked: webmail only. No one sets up Outlook or an email app with the app password.
Access only from the company (headquarters, branches and VPN)	A group, or Default, with the fixed IP list. Turn on the alerts to know about attempts from outside, and remember phones.

When not to use it: for a rule that applies to the whole domain, such as web session or access security, use the Default group; you don't need a group with everyone in it. For an exception for a single person, a one-mailbox group works, but first check that the most restrictive rule among their groups isn't getting in the way.

10. Colabora, directories and sharing

Drive and Colabora

lua Colabora (Drive, documents, Chat and meetings) is turned on for the entire domain by the Lua team, according to the contract. In **Domain settings** you can see whether it is on. Once it is on:

- each person signs in to Colabora with the same email and password as webmail, with no separate registration;
- the plan's space is shared between email and Drive files, and the panel shows the two separately on each mailbox;
- **meetings and video calls** are an add-on license, activated mailbox by mailbox (Chat remains available to all), and **Tasks** are turned on per mailbox, in **Edit mailbox**, when the license includes the feature;
- sharing files and folders is done by each person themselves, in Drive. The step by step is in the Colabora manual.

Domain address directories

In **Email → Directories** you create contact lists that appear in the webmail of **all mailboxes in the domain**, read-only: suppliers, key customers, useful phone numbers. Open a directory to add, edit, hide or delete contacts (name, email and phone).

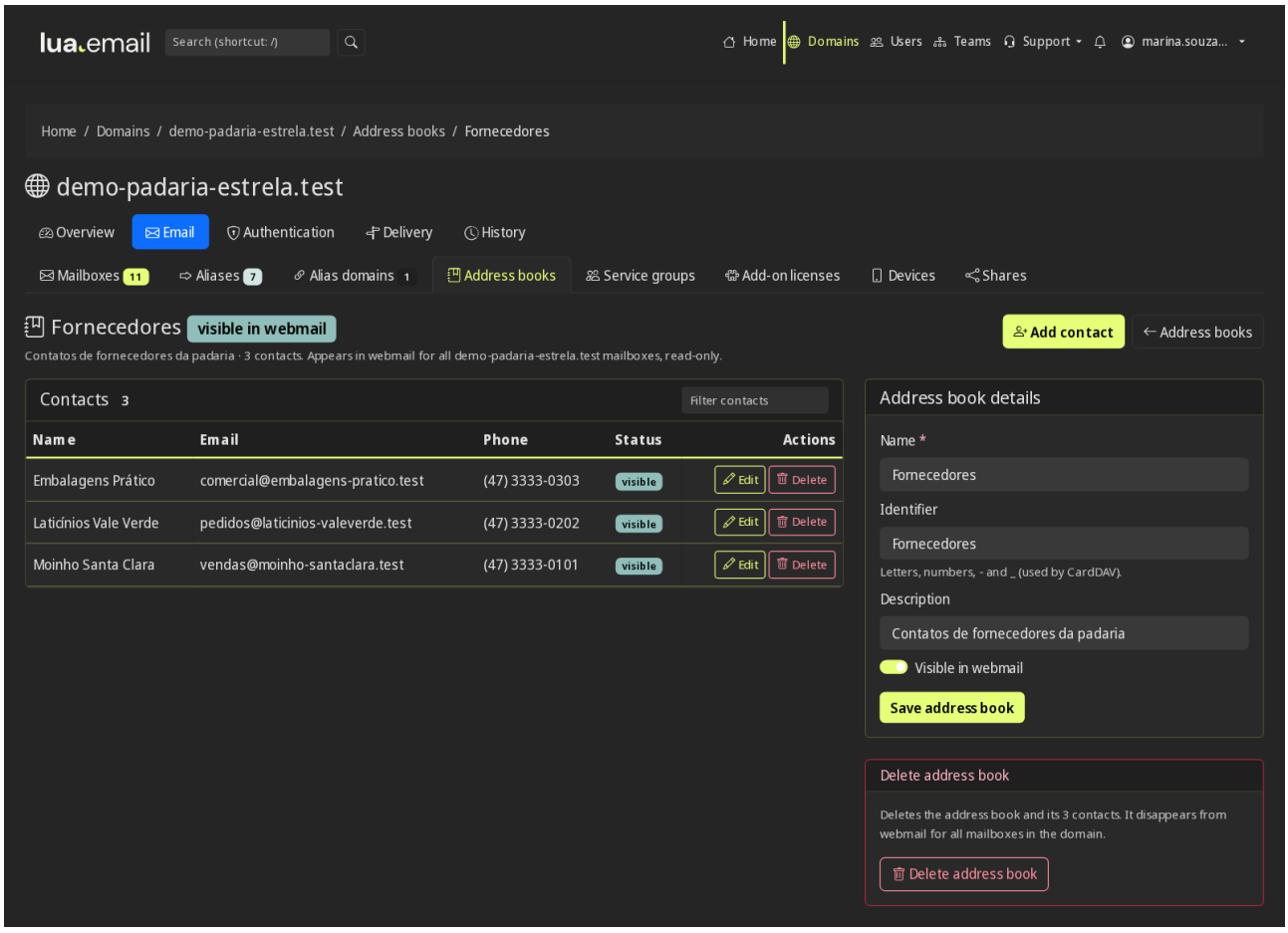


Figure 66: A domain directory with suppliers.

A directory published by a service group appears in the list with the group's link and is **read-only** here: the contacts are the group's mailboxes, and the name, the contacts and the publishing are changed through the group. The **Manage in service group** button takes you there.

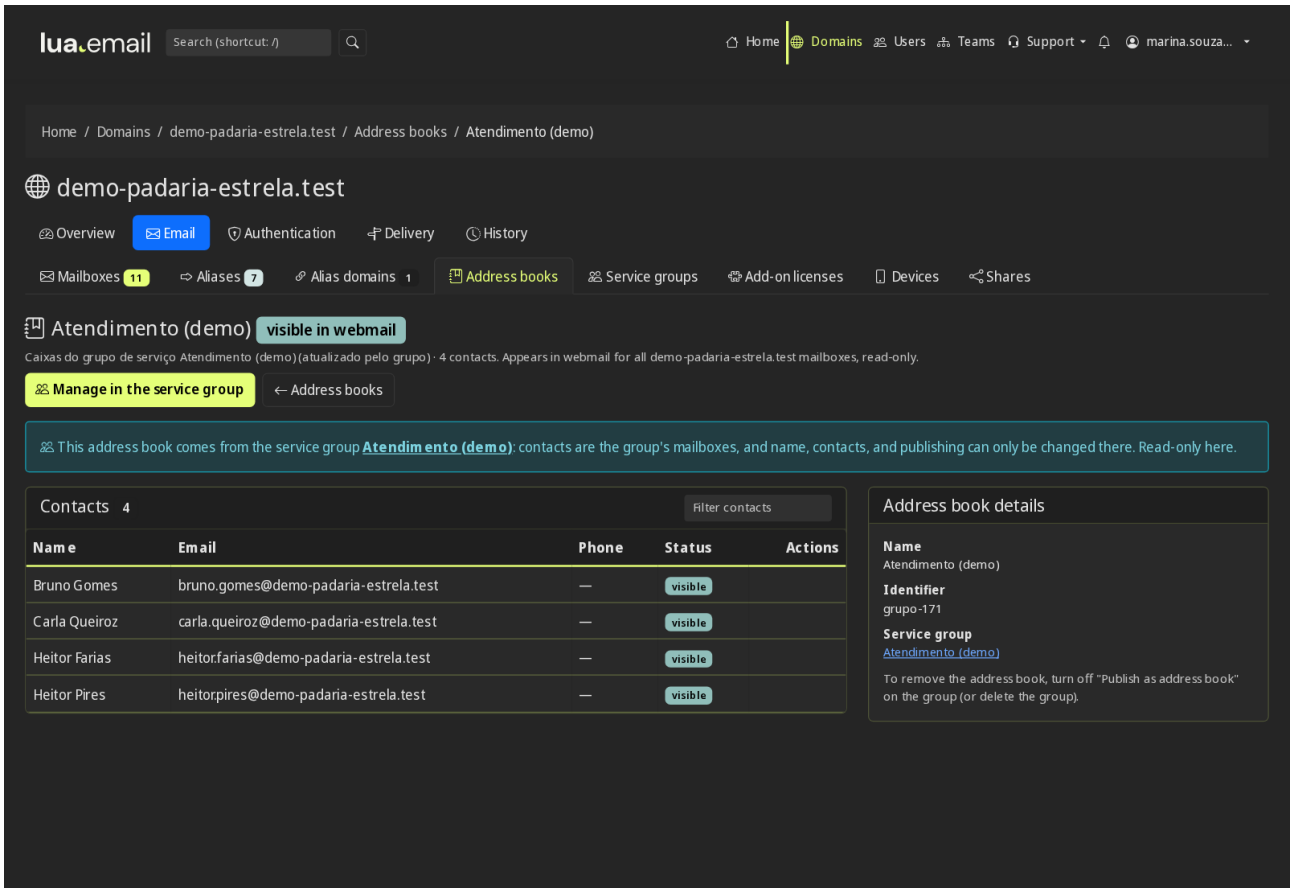


Figure 67: A group's directory: read-only, with the group's link.

Sharing

In **Email → Sharing** you see what the mailboxes share through webmail: the whole account (with the access type, such as "read only" or "full access") and shared folders. It is view-only: the person themselves creates and removes shares, in webmail. This helps answer questions like "who can read the reception mailbox?".

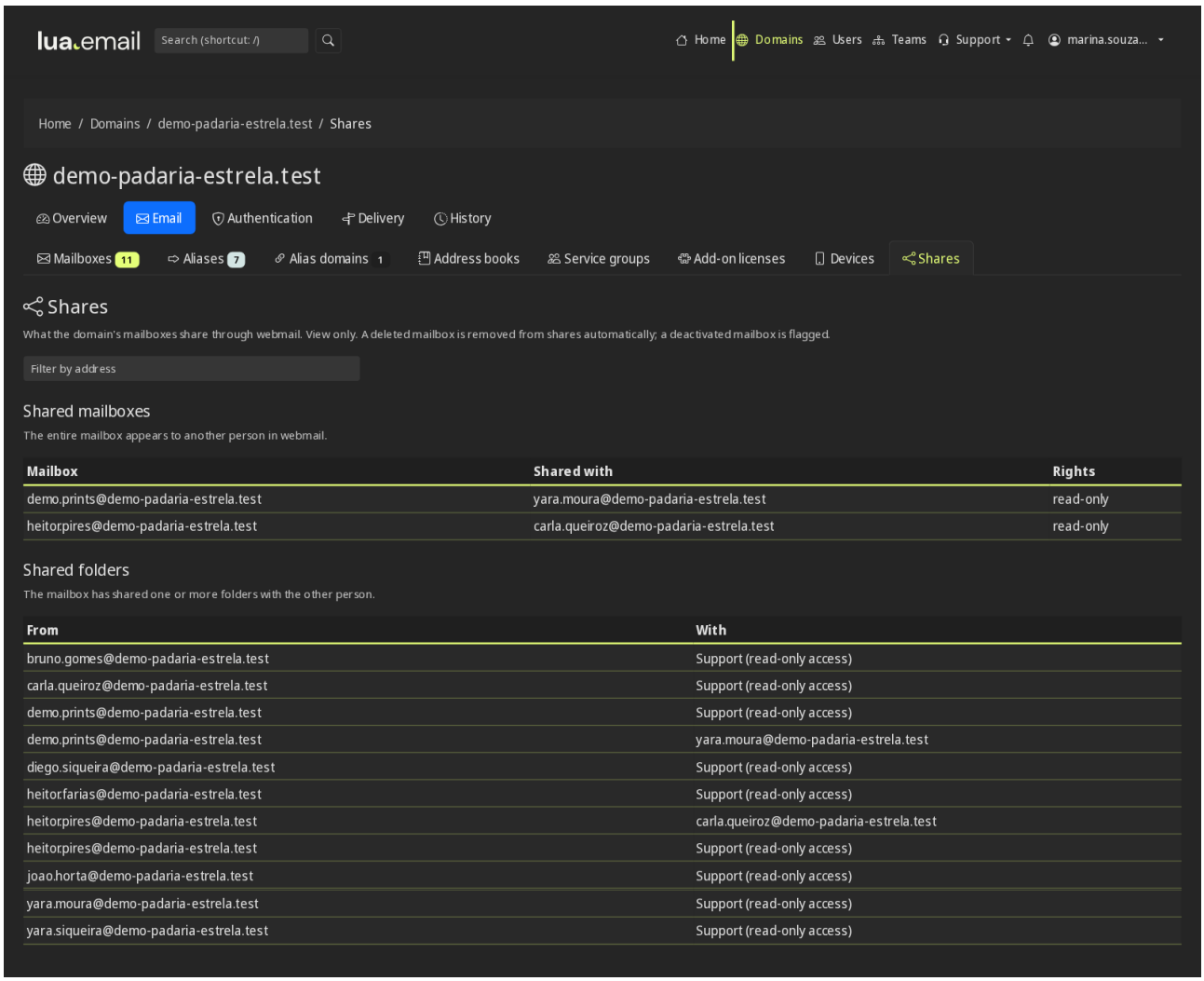


Figure 68: Shares made through webmail.

Devices: remove, wipe and the 30-day cleanup

The **Devices** tab lists the phones and apps that sync through the Exchange account (ActiveSync), with each one's account, first and last access and request history. The same actions appear in the **Connected devices** box on the mailbox page. What each device syncs is in the table in the webmail manual.

Action	What it does	When to use
Remove	Deletes only the device's sync state on the server. The phone is **not** wiped. If it comes back with the right password, it syncs everything again.	An old device the person no longer uses, or a stuck sync.
Wipe the device	Tells the phone to wipe itself. On iPhone and Samsung Email, it wipes the entire device. In Google's email app, it removes only the account. In Outlook, it wipes only the app's data.	A lost or stolen phone.

- **Wipe the device is off by default.** It is a feature available on request: when it is enabled for your domain, the button appears. While it is off, the button doesn't even show on screen, and only **Remove** is available. Remove works without it.
- **Confirmation:** you write the reason (5 to 500 characters) and type the mailbox's full email address.

- **Record:** each request stores who made it, from which IP, when, the reason and the result, and it is kept in the panel's audit log.
- **Who can:** the domain administrator. Support or read-only users see the list and the requests, but can't make or cancel them.
- **Cancel:** while the request is "pending". Once it is "sent" there is no going back. The states are pending, sent, done, failed and canceled.
- **Change the password only afterward.** The device receives the command after signing in with the password. If you change the mailbox password before the request reaches "done", the device can't sign in and doesn't receive the command.

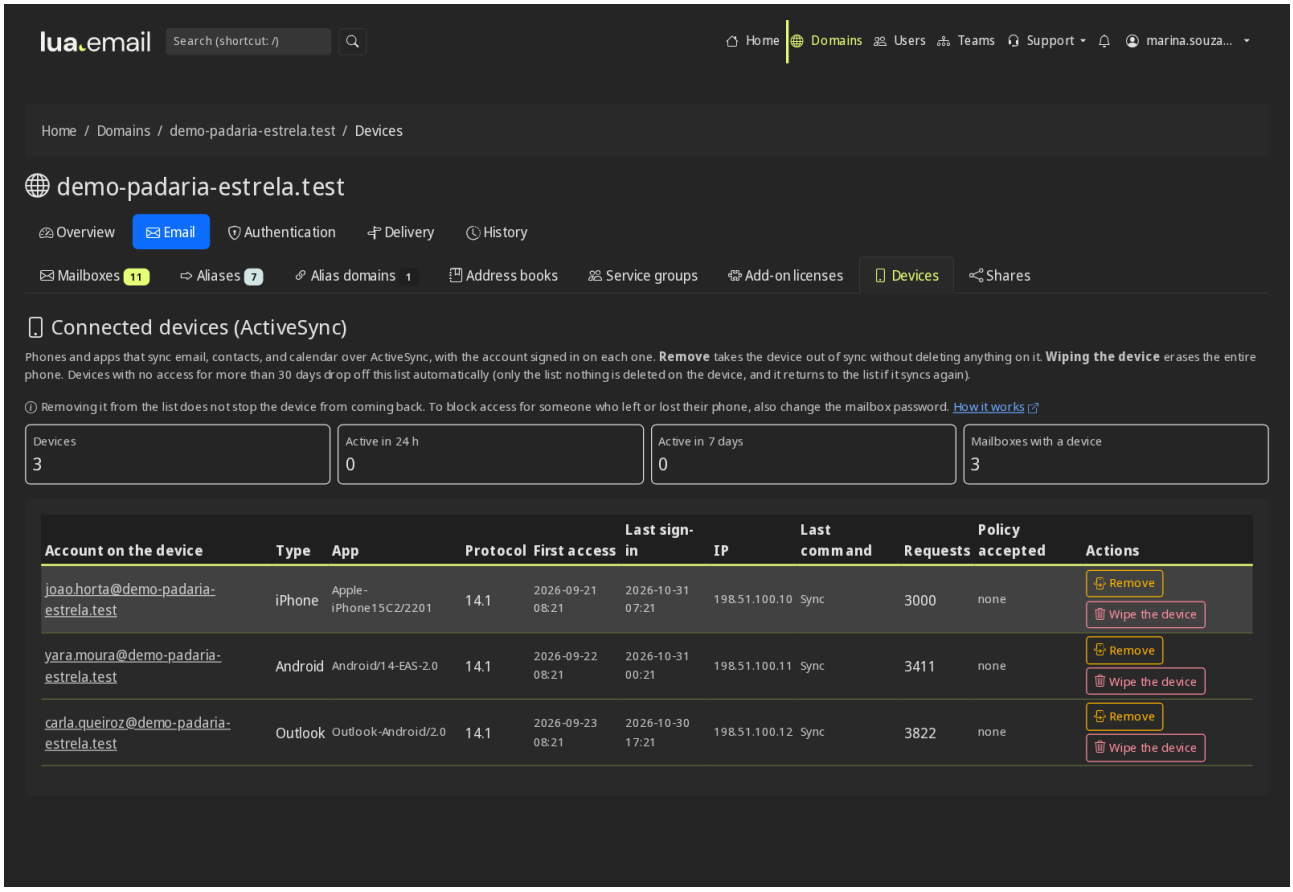


Figure 69: The domain's devices, with the Remove button on each one (test devices and IPs).

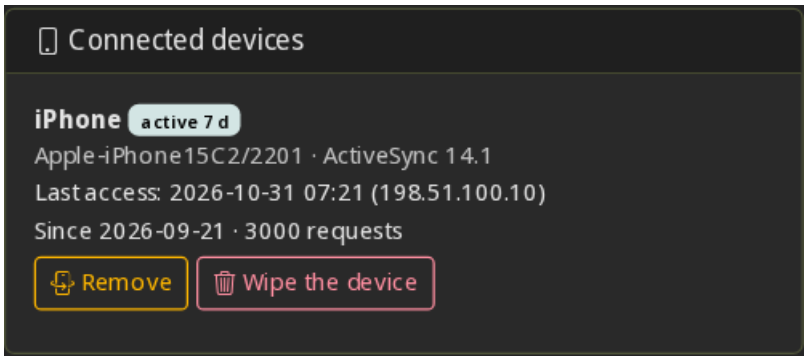


Figure 70: The same card on the mailbox page.

Automatic 30-day cleanup: devices with no access for more than 30 days drop off the list by themselves, once a day. The cleanup only touches the list: it doesn't wipe any phone. If the device syncs again, it returns to the list.

Step by step: remove a lost device, or one from someone who left (and change the password)

For domain administrators. The order matters: what really cuts off access is the **password**. **Remove** only clears the device from the sync list and, on its own, doesn't stop it from coming back.

1. Open the domain and go to **Email → Devices**. Find the person's account and the device by **Type**, **App** and **Last access**. The same list is on the mailbox page, in the **Connected devices** box.
2. **If the Wipe the device button appears on your screen** (the feature was enabled for your domain) and the phone was stolen or lost: click **Wipe the device**, write the reason (5 to 500 characters) and type the mailbox's full email address. Remember that on iPhone and Samsung Email this wipes the entire device, personal data included. Wait for the request to become **done**: the device only receives the command when it connects, and it only gets in if the password is still the old one. **Without the button, skip this step.**
3. **Change the mailbox password.** On the mailbox page, click Change password. The phone's Exchange account uses the webmail password, so the device stops syncing. If the person also used the mailbox over IMAP or POP on the device, generate a new app password.
4. Go back to the list and click **Remove** on the device's row. Write the reason and type the mailbox's email address to confirm. The request appears as **pending** and becomes **done** in about a minute.
5. Check it: the device leaves the list, and the request appears under **Requests (remove and wipe)**, with who made it, when and the result. It is also kept in the panel's audit log.

- **Someone left the company and the mailbox stays with someone else:** change the password and remove all of the mailbox's old devices. Whoever takes over the mailbox sets up the phone again.
- **Picked the wrong device?** While the request is **pending**, click **Cancel**. Once it goes out, there is no going back. Remove doesn't delete anything on the phone: whoever signs in again with the right password syncs everything.
- **With the wipe feature off**, changing the password and removing the device is the complete path: the phone keeps the data it already downloaded, but receives nothing new.

11. Per-account routing (lua Bridge)

With lua Bridge, some of the domain's accounts stay on lua.email and some stay on Google, Microsoft or another provider. Per-account routing says where each address outside lua.email goes, and you register, adjust and remove those accounts yourself in the panel.

The **Delivery → Per-account routing** tab exists in every domain, whether regular or spam-filter only. Each routed account uses a **Bridge Account**, the Bridge license, which is billed per routed account. The **New routing** button is enabled when the company has the license and still has a slot. The license belongs to the company: it applies to all of its domains, regular and spam-filter only, and the accounts from all of them count together.

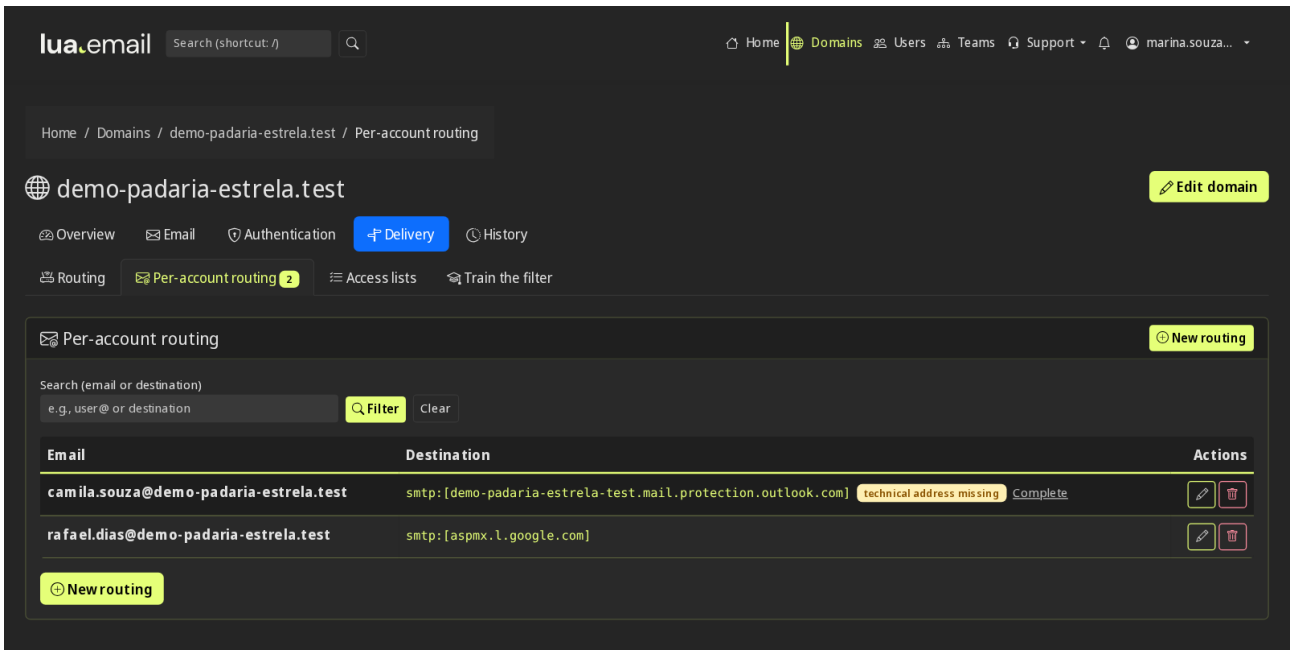


Figure 71: The domain's accounts on other providers, with the New routing button and each account's actions (real screen, fictional data).

Add a routed account, step by step

Click **New routing**. The wizard has five steps, on the same screen, and works the same on a computer and on a phone:

1. **Account address.** Type the part before the @, for example `rafael.dias`. The domain is the one on the screen.
2. **Where their mailbox is.** Choose Microsoft 365, Google Workspace or cPanel and other providers. Your choice fills in the next step with a suggestion.
3. **Inbound destination.** This is the provider's server that receives the account's email. For Microsoft 365 the panel suggests the domain with hyphens in place of dots, `yourcompany-com-br.mail.protection.outlook.com`; for Google, `aspmx.l.google.com`. You can change it. The message address doesn't change: people who write to `rafael.dias@yourcompany.com` keep writing to that address. Leave the port blank for 25; the panel accepts 25, 587 and 2525. The **i** icon next to the field explains it.
4. **Technical address.** This is the account's address inside the provider, for example `rafael.dias@yourcompany.onmicrosoft.com` on Microsoft 365. It lets people on lua.email send to this account: without it, a message from a lua.email mailbox to the account lands here and fails. The panel suggests the address using the tenant you already used in this domain (the tenant name may differ from the inbound host, so check it), and the wizard creates the alias for you.

5 **Review and confirm.** The summary shows the account, the provider, where the email is delivered and the alias. Click **Create routed account**.

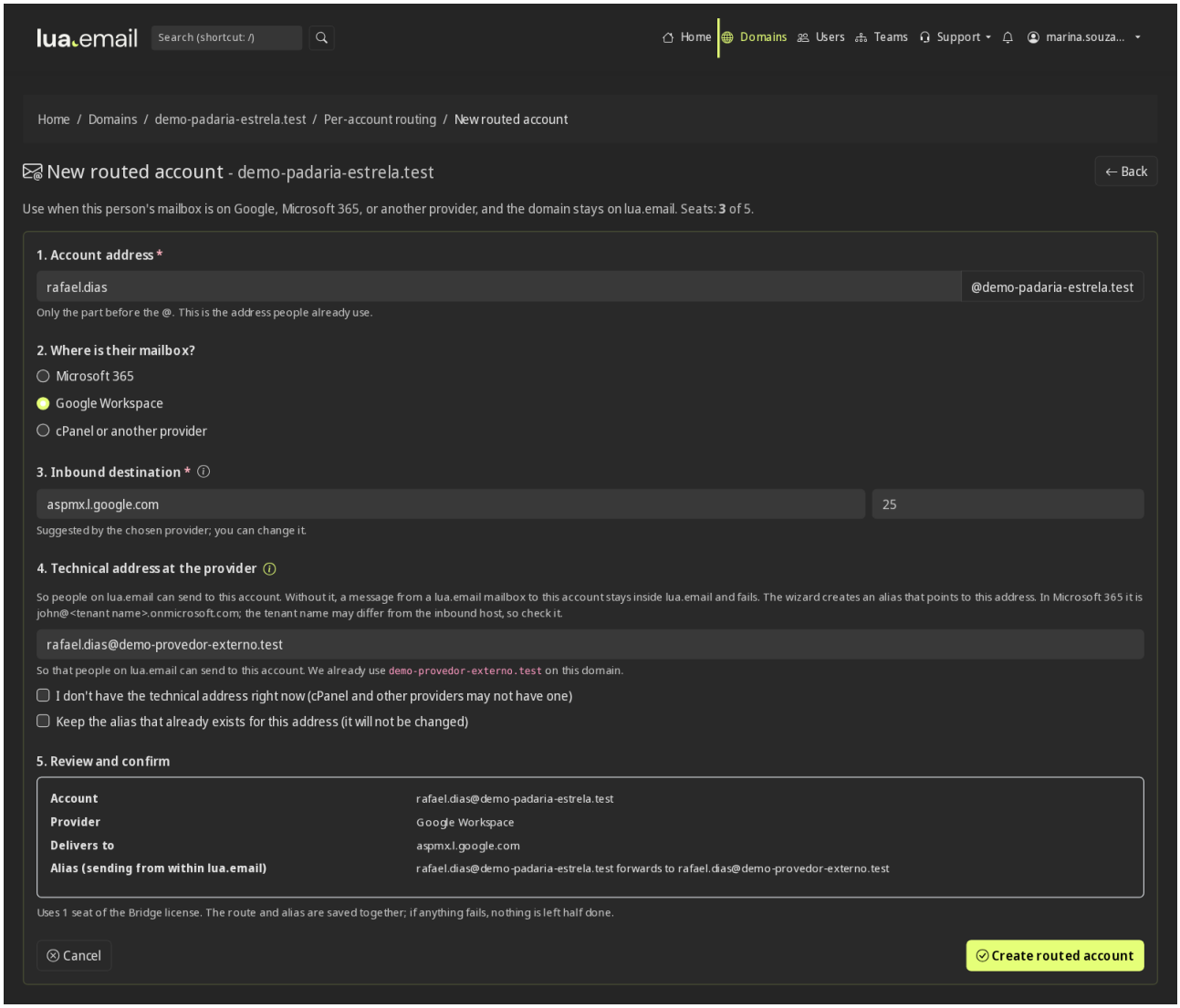


Figure 72: The routed account wizard, with the technical address explanation open (real screen, fictional data).

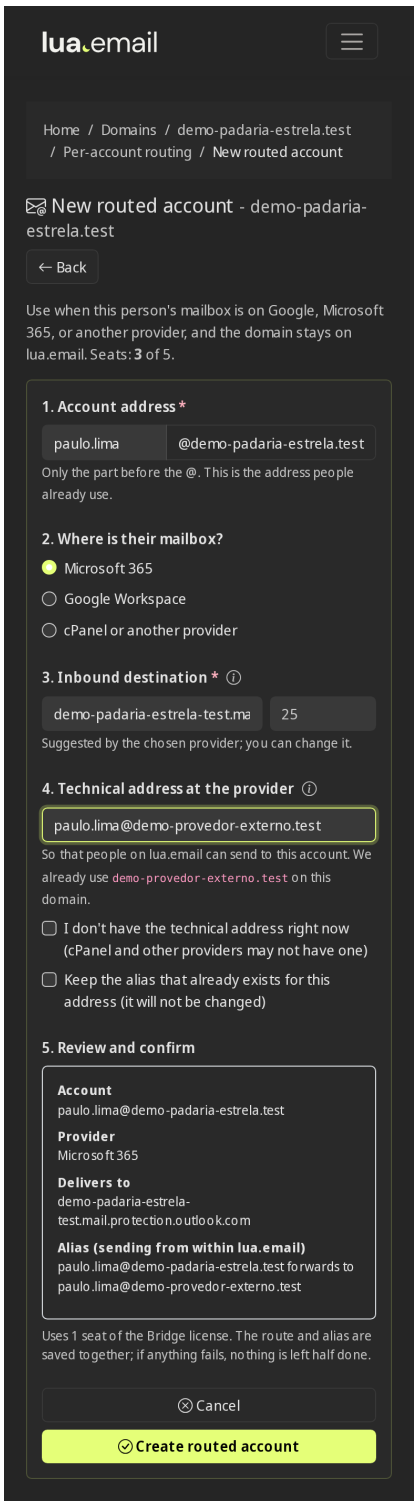


Figure 73: On a phone the steps stack one below the other, with no sideways scrolling (real screen, fictional data).

Route and alias go together. The panel saves the route and the alias in a single operation: if something fails midway (for example, the last slot was taken by someone else at the same time), the alias it had created is undone and nothing is left half done. If you click the button twice, only one account is created.

What the panel doesn't do: it doesn't overwrite an alias that already exists. If there is already an alias for the address, the panel shows what it does and creates nothing; if that alias already leads to the right technical address, check **Keep the existing alias** and the route is created without touching it. It also doesn't route an address that is already a lua.email mailbox (its email would stop arriving): remove the mailbox first, if that is the case.

Without the technical address

On cPanel and some providers there is no technical address to enter. Check **I don't have the technical address now**: the account is created with the route only. The panel's warning states the consequence, and it is real: email arriving from outside goes to the account, but people on lua.email can't send to it. The account is marked **technical address missing** in the list, with a **Complete** link that opens the edit screen so you can enter the address later. Accounts that already existed, created before the wizard and without an alias, get the same warning; the panel doesn't change anything on its own.

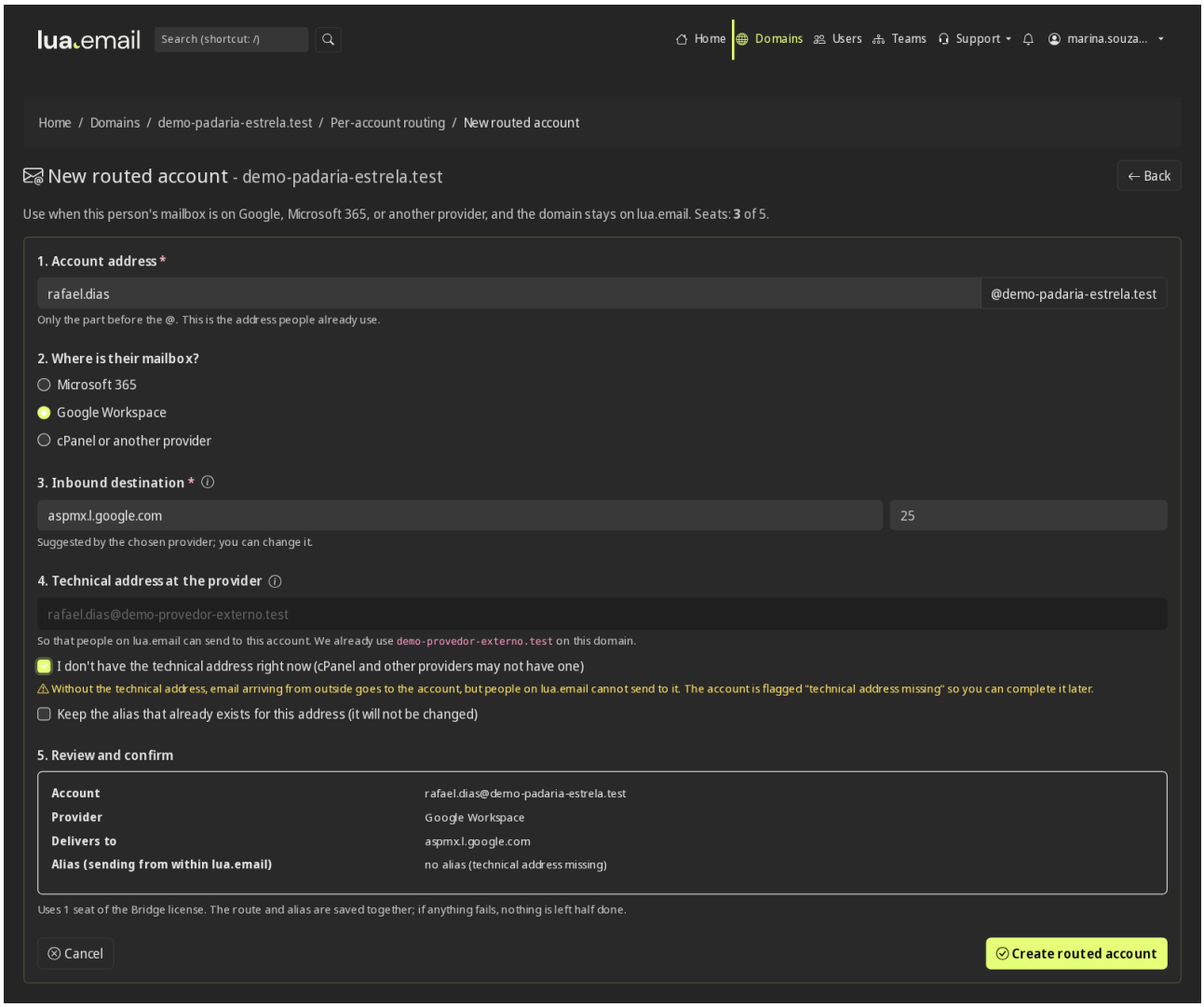


Figure 74: Without the technical address, the panel warns what stops working (real screen, fictional data).

Edit and remove

In the list, the pencil opens the edit screen: you change the host, the port and the technical address, and the panel updates the route and the alias it created. If the account's alias is yours (created by hand or already there), the panel shows the address and doesn't touch it. The trash can removes the routed account after a confirmation; it returns the license slot and also removes the alias the wizard created. Aliases you created are never removed by this screen.

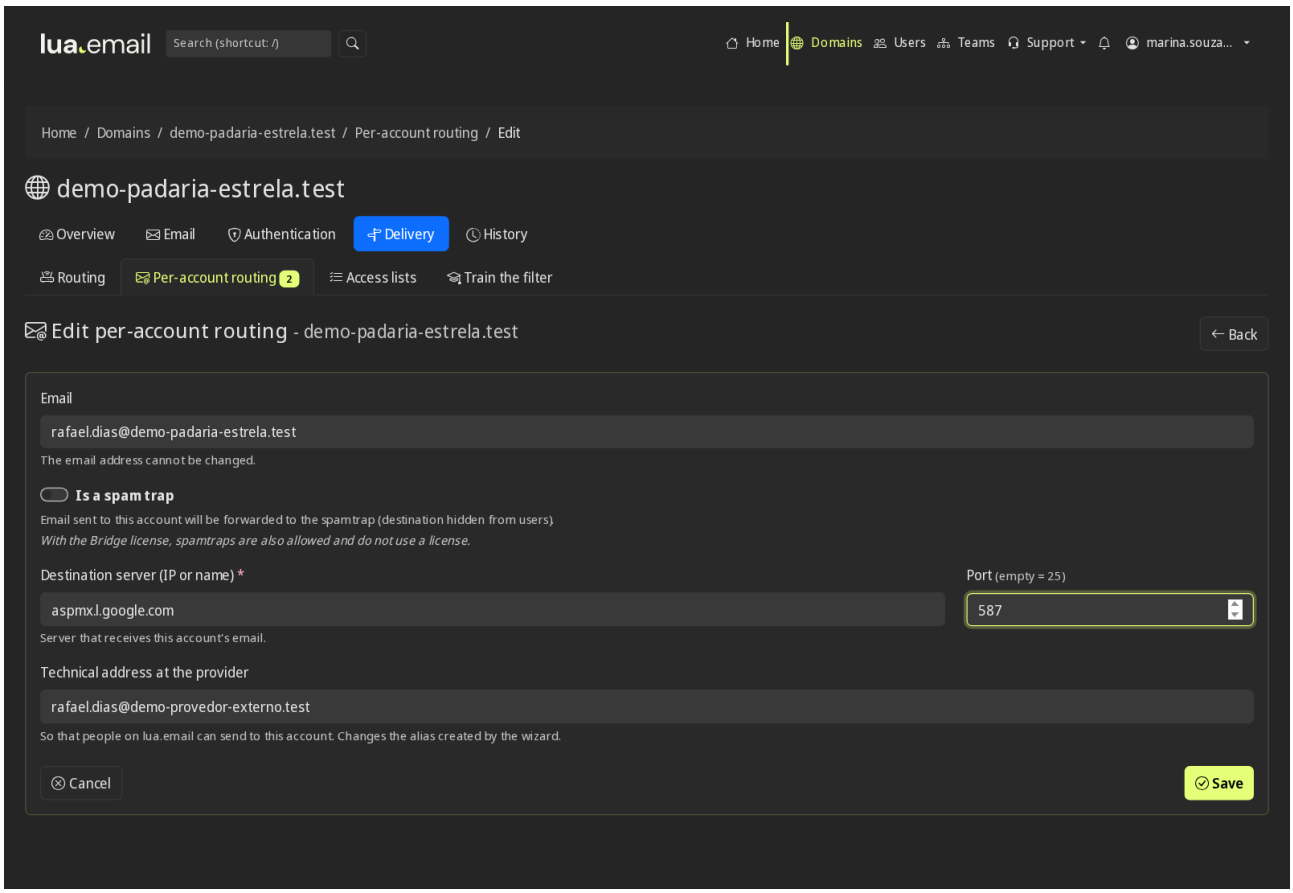


Figure 75: Edit: host, port and technical address (the panel updates the route and the alias) (real screen, fictional data).

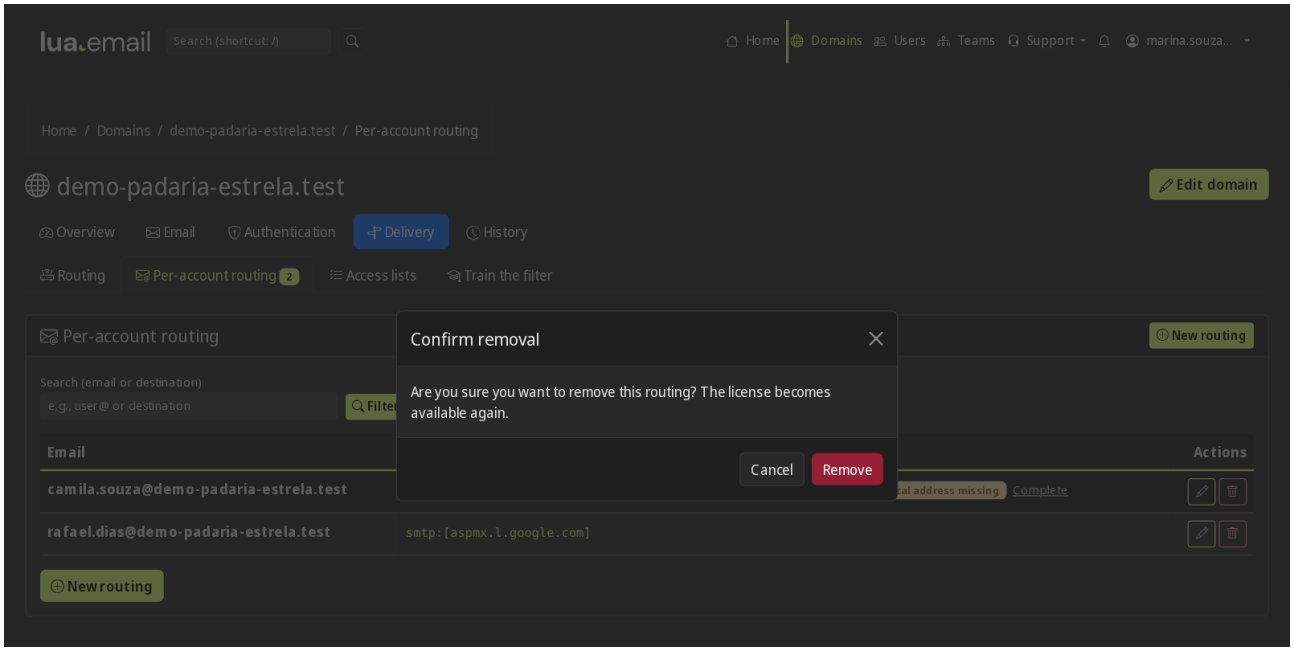


Figure 76: Remove: the license becomes available again (real screen, fictional data).

When the license runs out or doesn't exist

With the license but no free slot, the **New routing** button is disabled, and the message says **All routing licenses are in use**, with how many were purchased and how many are in use. Without the license, the message is **To use per-account routing, you need to buy the license**. In both cases the message includes the **Get more licenses** shortcut, the same one used elsewhere in the panel: it takes you to the subscription portal or, depending on the company's registration, to sales on WhatsApp. The license is purchased on the website or at checkout. Accounts that are already routed keep working and can be edited and removed; the rule only applies to adding new accounts. Read-only or helpdesk users see the list, without the add button and without the shortcut.

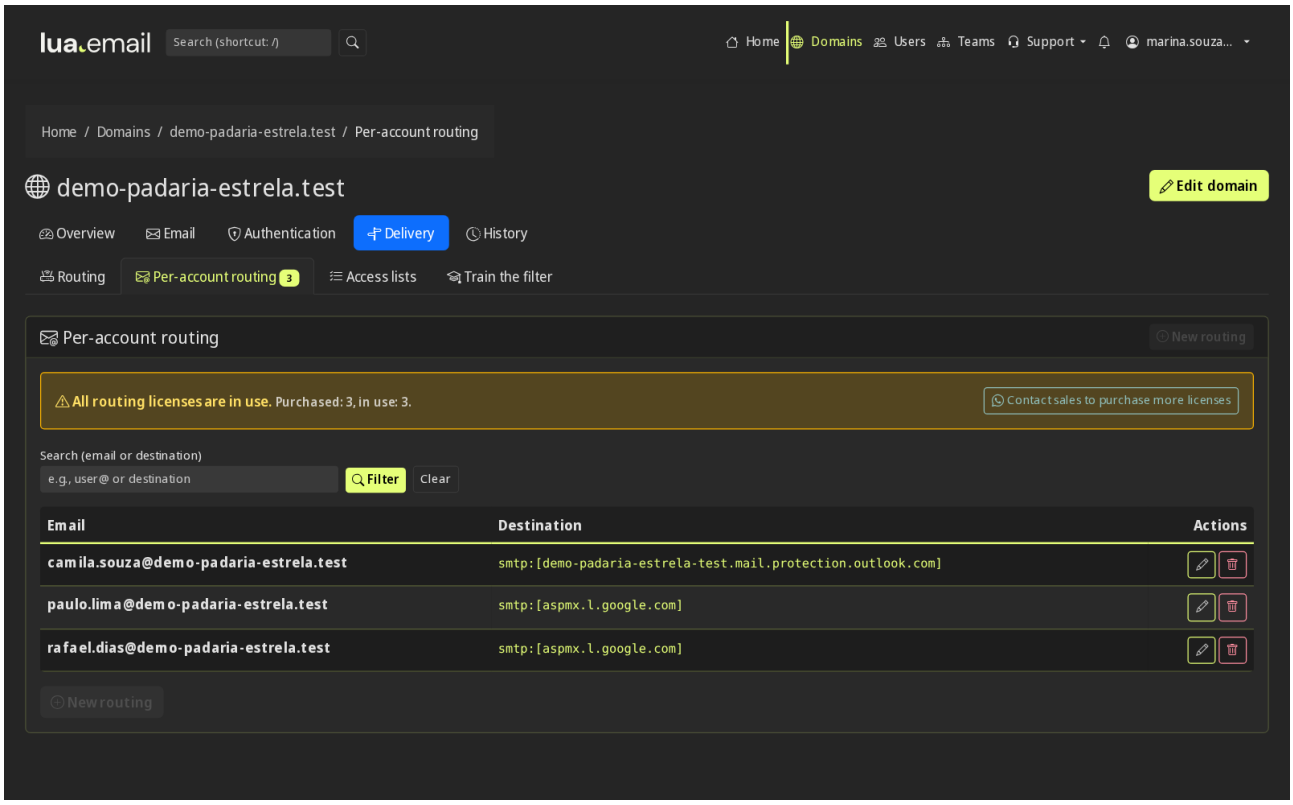


Figure 77: No free slot: disabled button, message and shortcut to subscribe (real screen, fictional data).

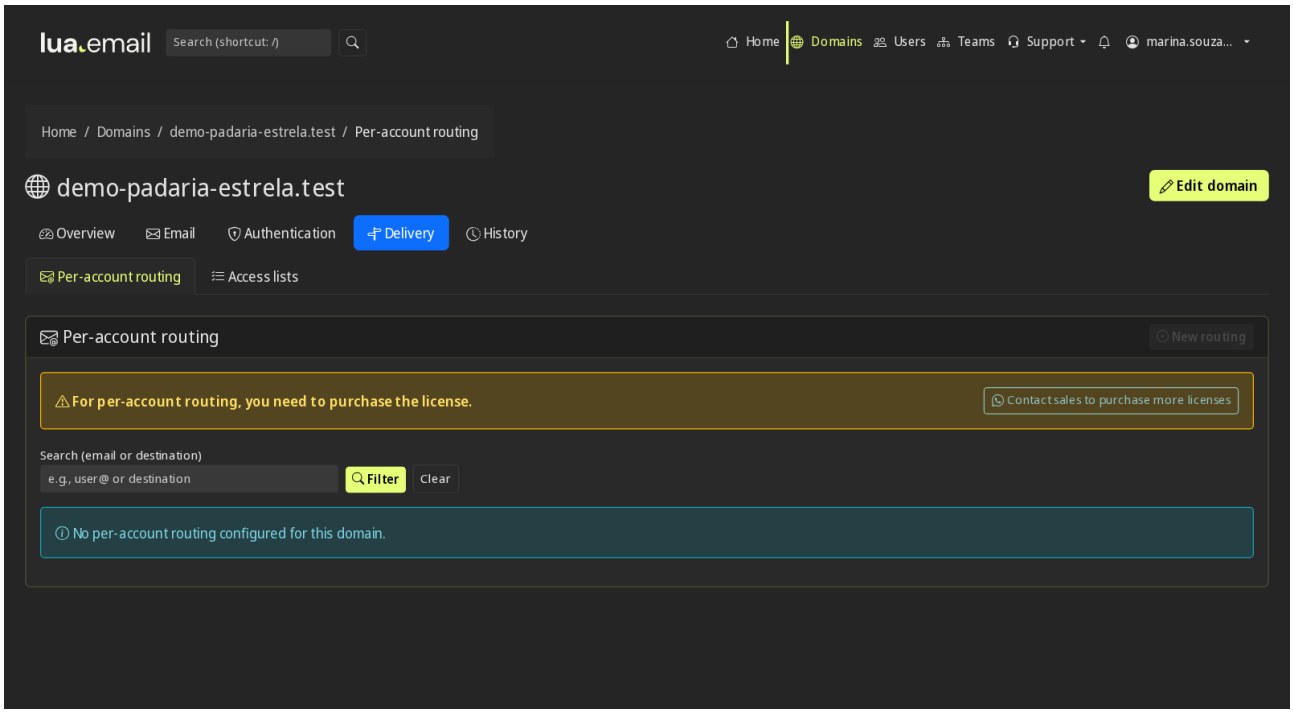


Figure 78: Without the license: the message and the shortcut to subscribe (real screen, fictional data).

In a spam-filter-only domain

The license applies equally to domains that only have spam filtering (antispam). The difference is that these domains have no mailboxes on lua.email, so the wizard skips the technical address: there is no one here to send. Spam trap accounts (**Add as spamtrap**) remain free on these domains, don't use a license, and don't need Bridge.

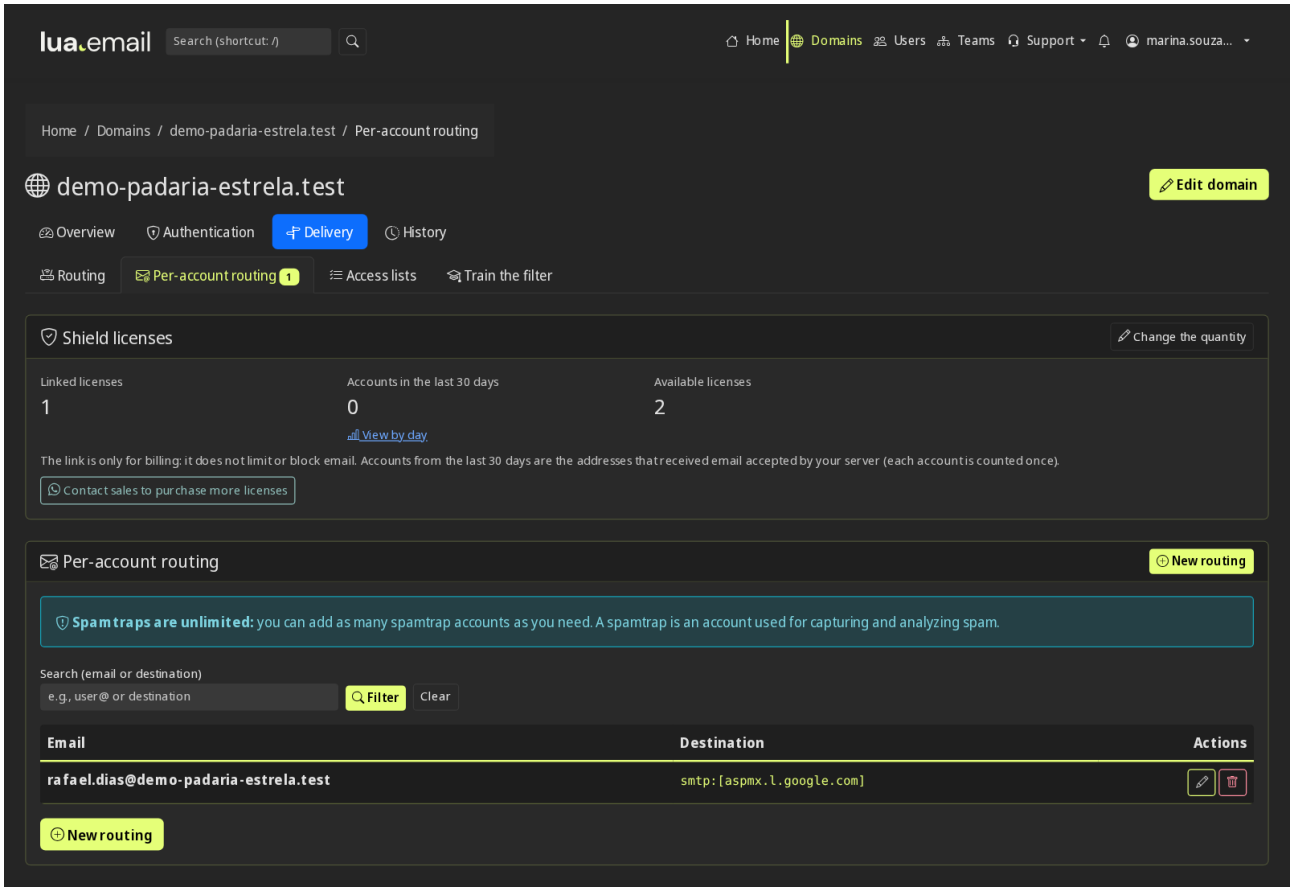


Figure 79: Spam-filter-only domain: the same license and the same list (real screen, fictional data).

What the panel accepts as a destination

The destination must be an **outside** server, maintained by the account's provider: a name that resolves to a public address, or a public IP address, and a mail port (25, 587 or 2525). The panel rejects internal network addresses, `localhost`, reserved addresses, lua.email's own servers, names that don't exist and ports for other services, and gives the reason on screen. The same applies to the account address (only letters, numbers, dots, hyphens and underscores) and to the technical address (it must be from another domain, outside lua.email).

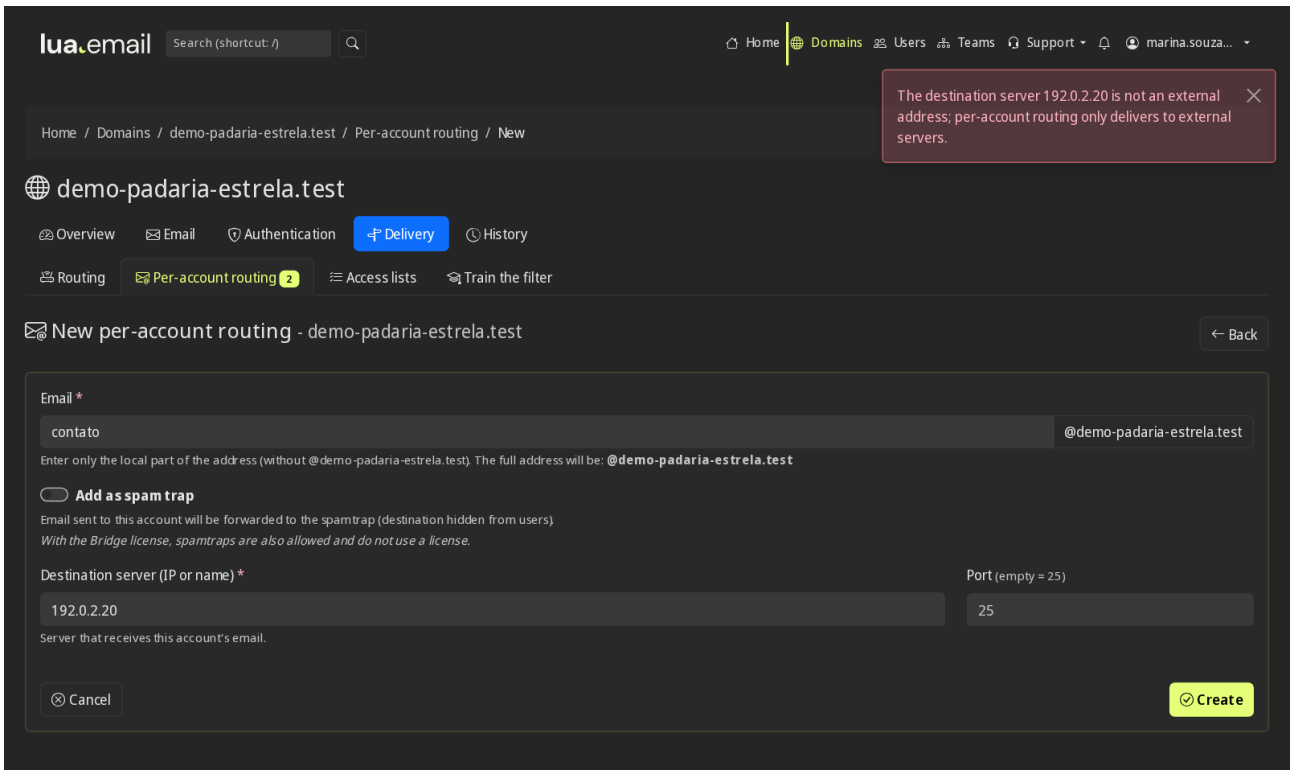


Figure 80: The panel explains why it rejected the destination (real screen, fictional data).

Routing for the whole domain. If your company has a routing license, the domain's routing screen shows only the destination server: server, port and type. The same rule as above applies, an outside server and port 25, 587 or 2525. The other routing settings are handled by our team.

Where to see usage

The domain's **Home** and the **Email → Mailboxes** tab have the **Additional licenses** block. It includes the **Bridge Account (per routed account)** line, with the domain's routed accounts, the ones purchased, the ones in use (across all of the company's domains) and the ones remaining. It is not added to the mailbox licenses. Without a contract, the line shows zero and the link to subscribe. For older accounts, from before the license, the legacy license appears, which keeps what already exists and doesn't open new slots.



Figure 81: The Bridge Account in the domain's license summary (real screen, fictional data).

How it works

Every message that arrives for the domain goes through the Lua antispam. If the recipient has routing, it continues to the registered provider; if not, it is delivered to the lua.email mailbox. Anyone with neither a mailbox nor routing gets the "user does not exist" rejection. The setup on each provider's side (connectors, relay, SPF) is in the lua Bridge documentation, and each provider's technical address is in its chapter 4.

The account must exist at the registered provider. If it doesn't exist there, the provider returns the message to Lua, which sends it again, and the message comes back with "loop detected". Don't check **Add as spamtrap** on accounts that belong to people: that option turns the address into a spam trap, and messages sent to it reach no

one.

12. Logs, statistics and tracking

The domain's **History** group and the **Support → Track email** menu answer everyday questions: "the customer says they sent it and it didn't arrive", "why did my message bounce", "who deleted this email". You only see messages from your own domains. The history keeps 180 days.

Statistics

Shows the period's receiving (total, delivered, marked as spam and rejected) in a chart, the accounts that sent the most and the sends per hour. Choose 24 hours, 7, 15 or 30 days. The **Refresh** control, on the right, sets whether the page refreshes automatically (**Manual**, or every **1**, **5** or **10** minutes) and the **Refresh now** button fetches the data right away. It also appears on the email logs and tracking, and applies only to the screen you are on.

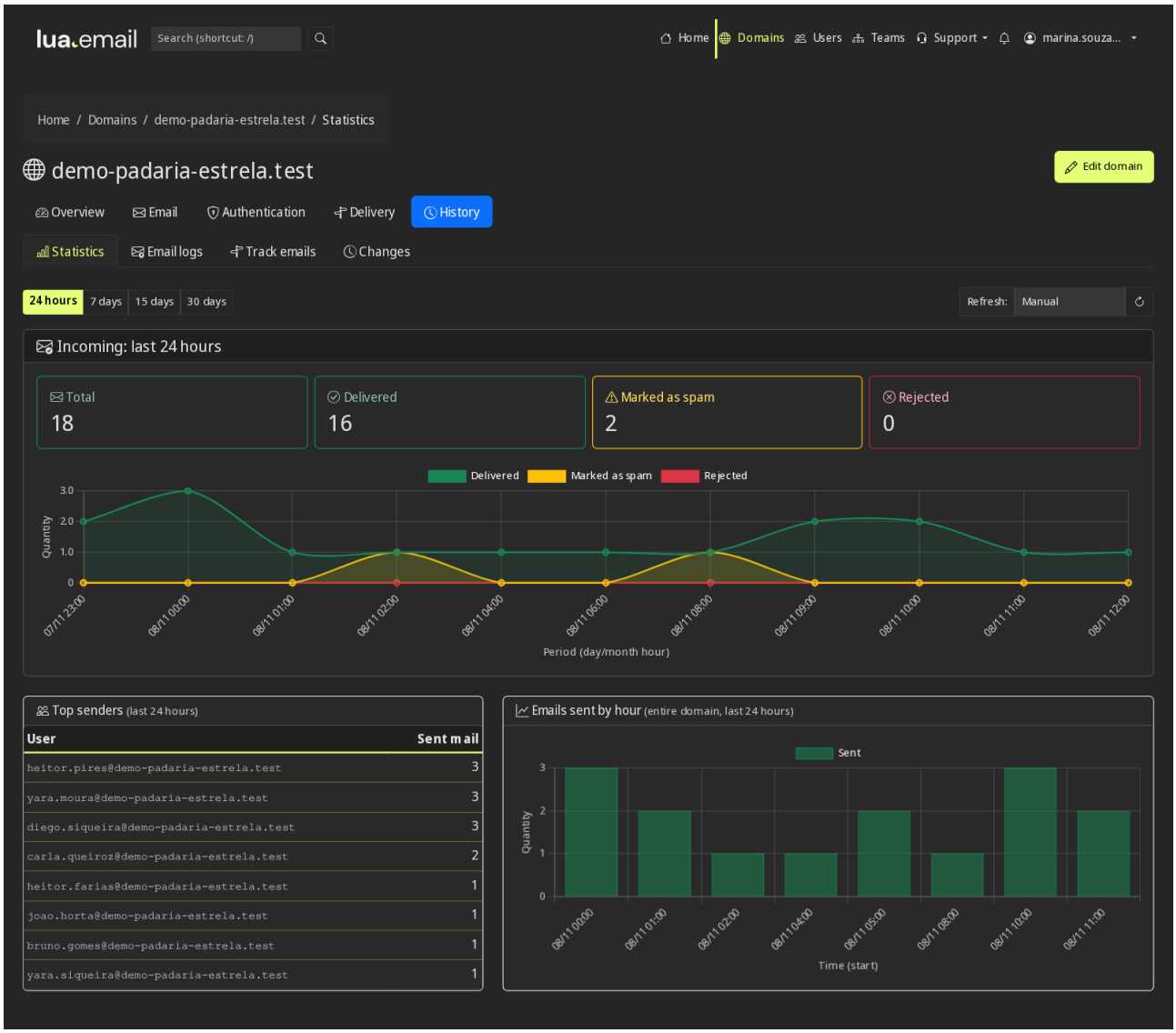


Figure 82: The domain's statistics.



Figure 83: The Refresh control: Manual, 1, 5 or 10 minutes, and the Refresh now button.

Email logs

The domain's incoming and outgoing mail in the same table, with an arrow showing inbound or outbound. For each message: date, sender, recipient, what the filter did (delivered, marked as spam, rejected, greylisted), size, subject and the DKIM, SPF and DMARC results. Filter by period, type, source, destination, subject or action. Without dates, the search shows the last 24 hours. In **Log type**, choose all, received only or sent only. Rejected messages are hidden by default: check **Include rejected messages** to see them.

In a domain that uses only the Lua antispam (lua Shield or receiving through another server), sending goes out through the company's server: the list shows only what arrived, and the type filter doesn't appear.

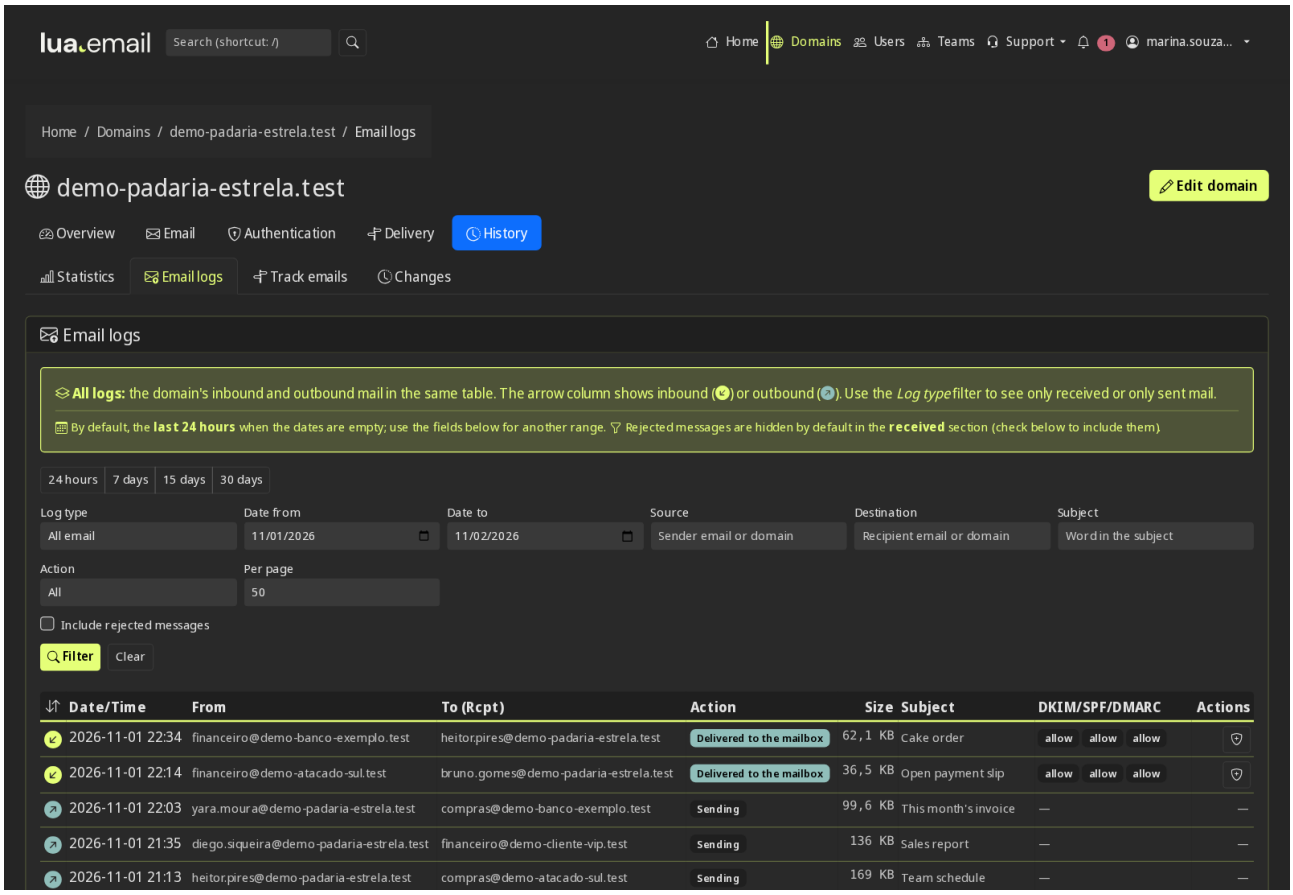


Figure 84: The domain's email logs.

Track a message

In **Support → Track email** (or the **Track** button on the mailbox page), each row is a message to one recipient, from newest to oldest. The search opens with the last hour: change the period to 24 hours, 7 or 30 days, or choose dates. Filter by address (either side), sender, recipient or Message-ID.

The **What happened** column says how the message ended: delivered to the mailbox, delivered to the destination server, rejected (with the reason), bounced or still trying to deliver. For rejections and errors, **view log** shows the server's response so you can copy it. The **In the mailbox** column shows which folder the message was delivered to and what happened afterward.

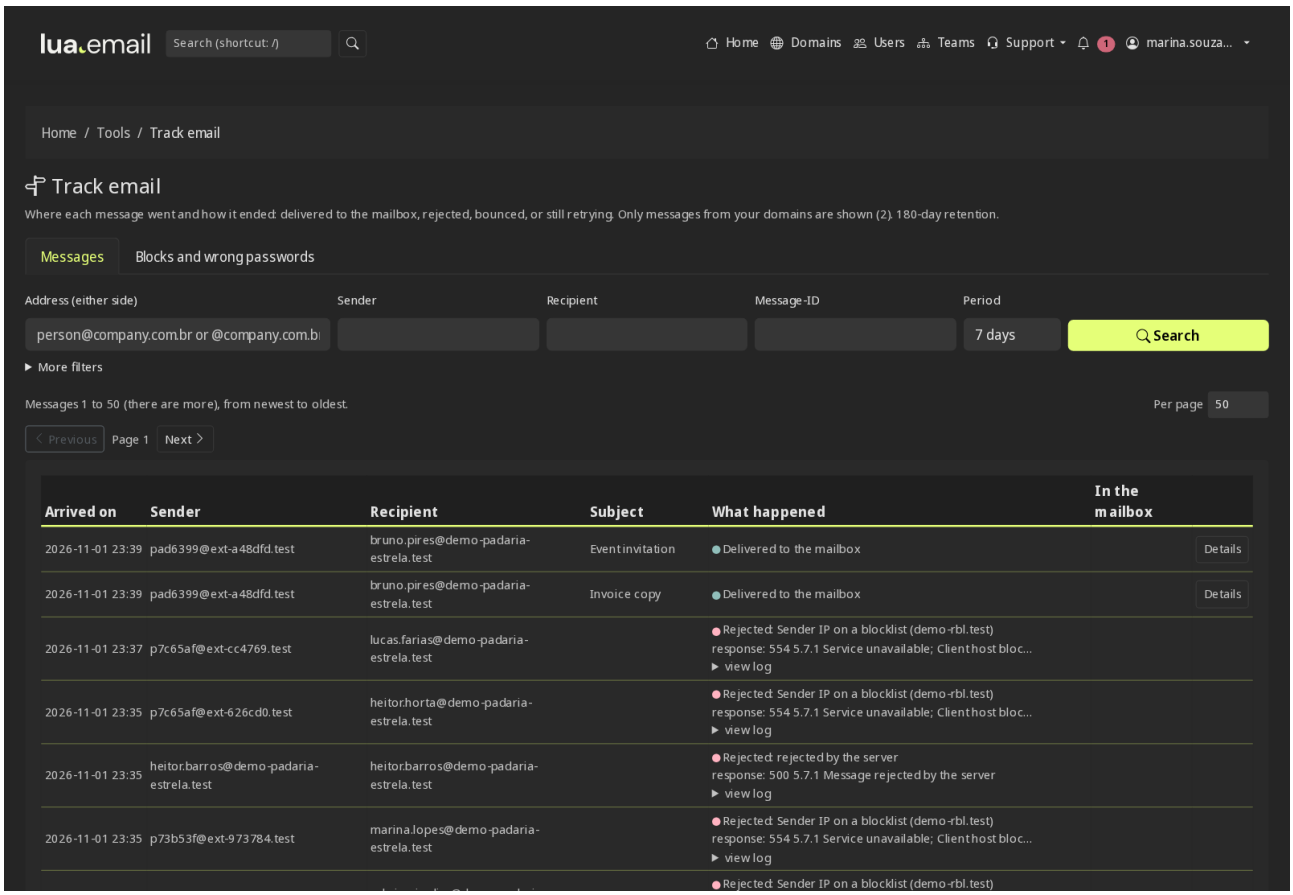


Figure 85: Tracking shows how each message ended.

Click **Details** to open the side panel with each step: when it arrived, who sent it, where it was delivered and what the person did with it in the mailbox (moved to another folder, marked as deleted, permanently deleted, answered by a rule).

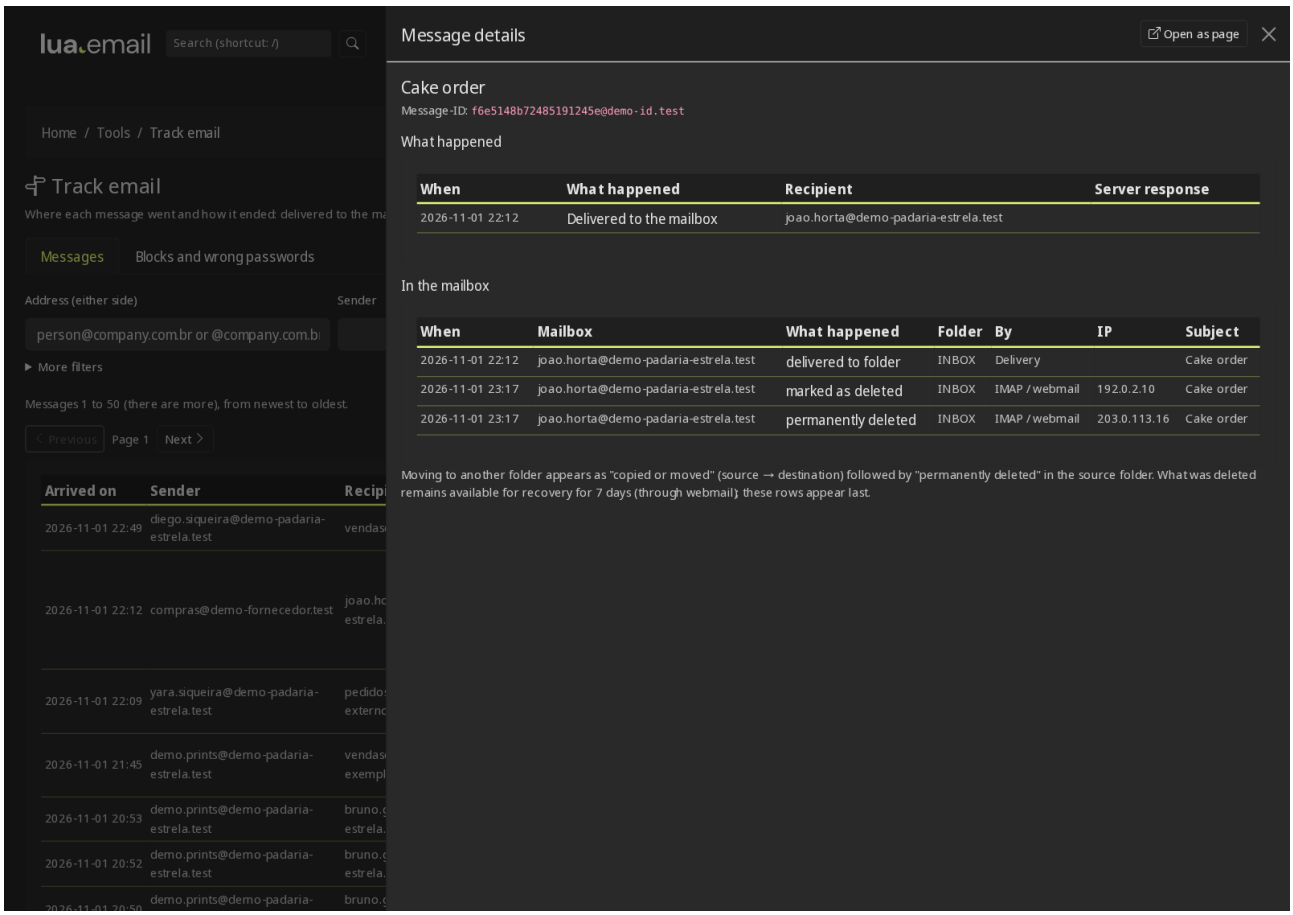


Figure 86: Details: the message was delivered and later deleted by the person.

Blocks and wrong passwords

The second tab of tracking has three parts:

- **Rejections:** each message rejected on arrival, with the reason in plain language: the destination mailbox doesn't exist, the mailbox only receives from its own domain, the sender failed SPF or DMARC, IP on a blocklist, mailbox full, message too large.
- **By reason:** how many rejections for each reason in the period. Click a reason to see its rejections.
- **Failed logins:** account, reason (wrong password, nonexistent account, lockout after attempts), source IP, how many times, and the first and last attempt. Many attempts from an unfamiliar IP on one account are a sign that someone is trying to guess the password.

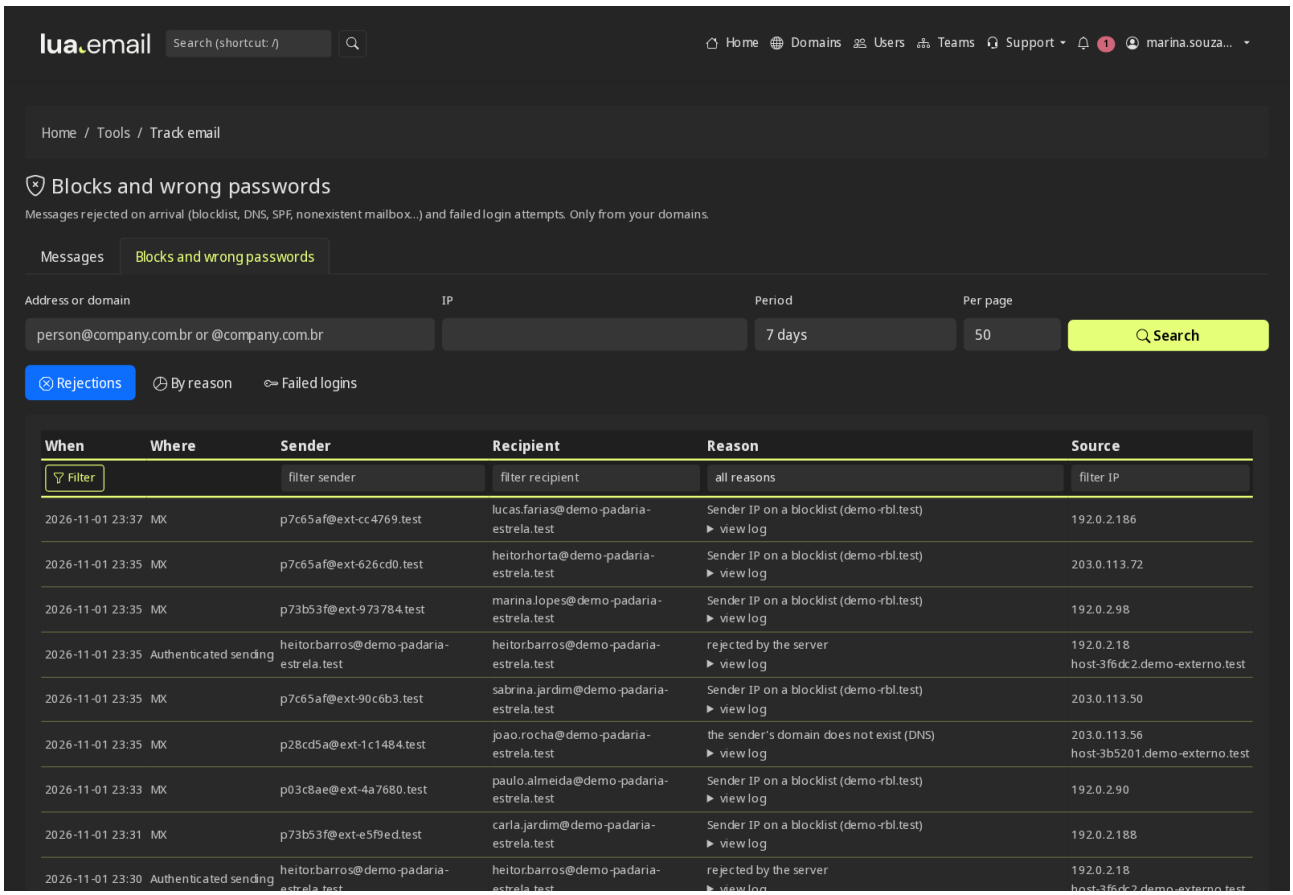


Figure 87: Rejections on arrival, with the reason for each one.

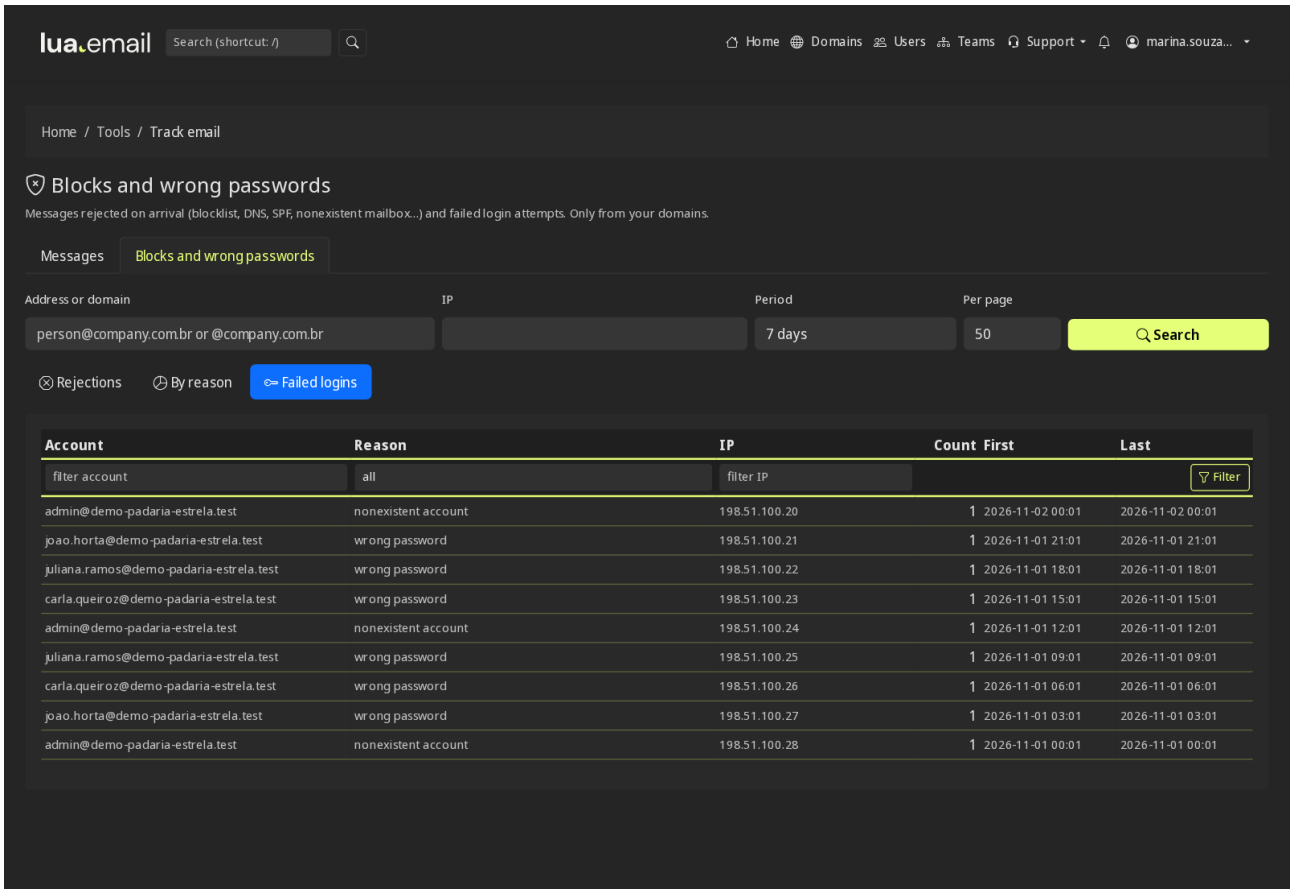


Figure 88: Failed logins.

System logs

In **History → System logs** is everything done in the domain through the panel: who did it, when, what and on which account. Filter by type (mailboxes, aliases, domain and DNS, service groups), action, who did it, affected account and period. Use it to answer "who changed this mailbox's password?" or "when did this alias change?".

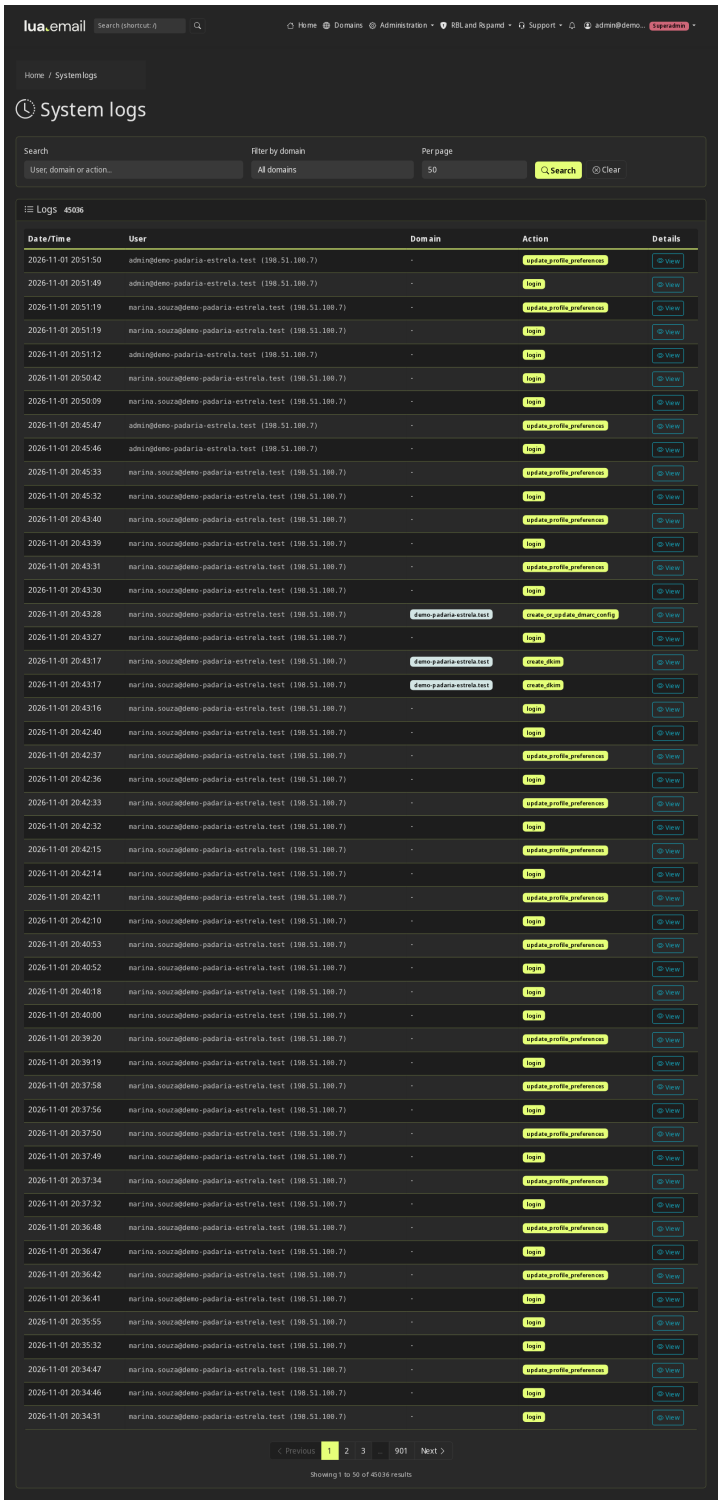


Figure 89: System logs: what was done in the panel and by whom.

13. Diagnostic tools

In **Support → Tools** there are four tests that work for any domain, including that of a customer or supplier who says they don't receive your messages.

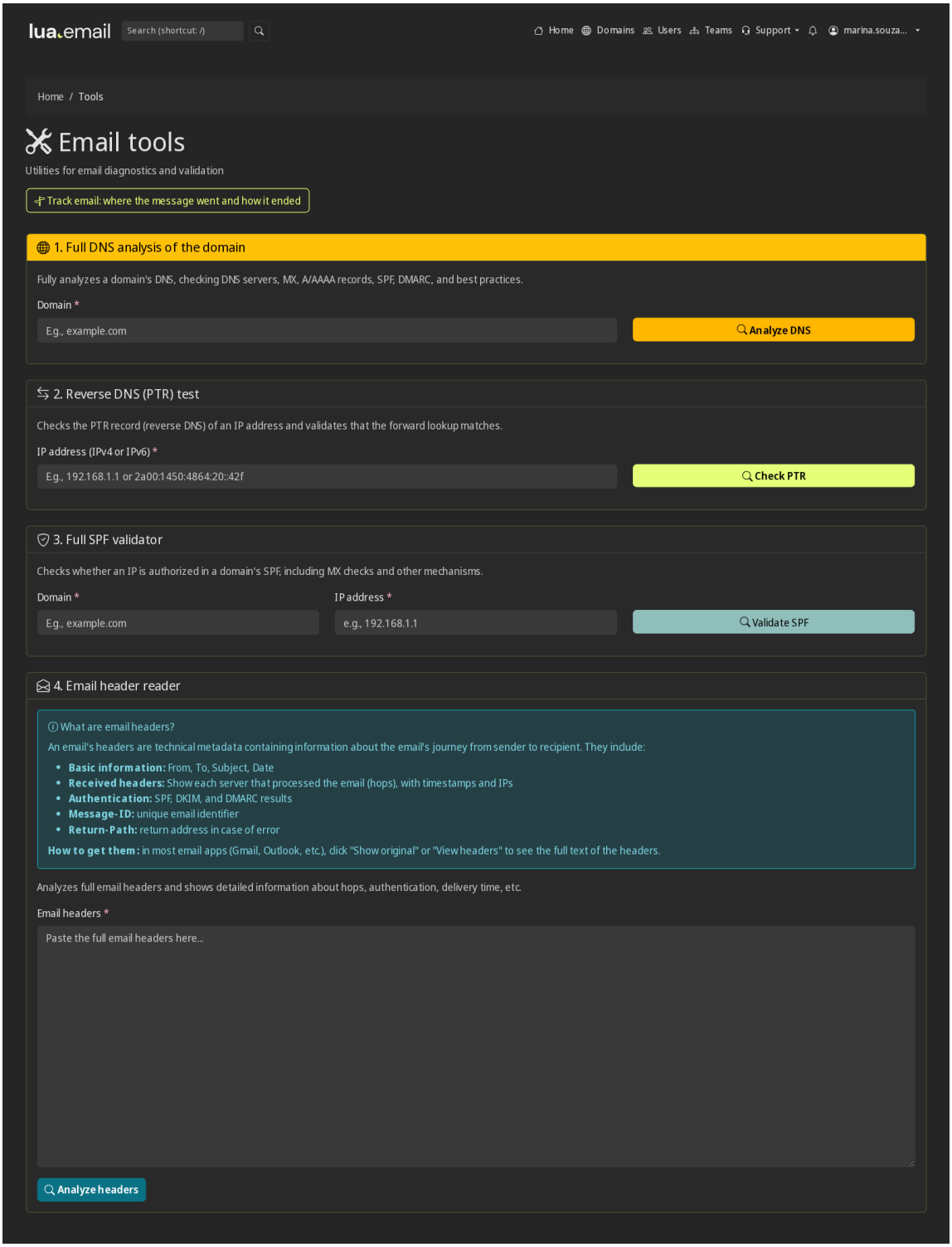


Figure 90: The diagnostic tools.

Tool	What it answers	Where to see the result

Full DNS analysis	The domain's DNS servers, MX, root and www records, SPF and DMARC, with a best-practices score and recommendations.	Below the form, on the same screen. For your own domain, the check that counts is Validate DNS, which also checks DKIM and Autodiscover.
Reverse DNS (PTR)	Whether an IP has a reverse name and whether the name points back to the same IP. Useful when a third-party server can't deliver.	On the same screen, with the PTR found and the validation.
SPF validator	Whether an IP is authorized to send for the domain, showing each SPF mechanism (include, ip4, all).	On the same screen: "IP allowed? YES or NO" and the list of mechanisms.
Header reader	Paste a message's full header ("show original") and see the sender, subject, SPF, DKIM and DMARC results and the path between servers, with the time of each hop.	On the same screen. To find out what happened to a message inside Lua, use tracking.

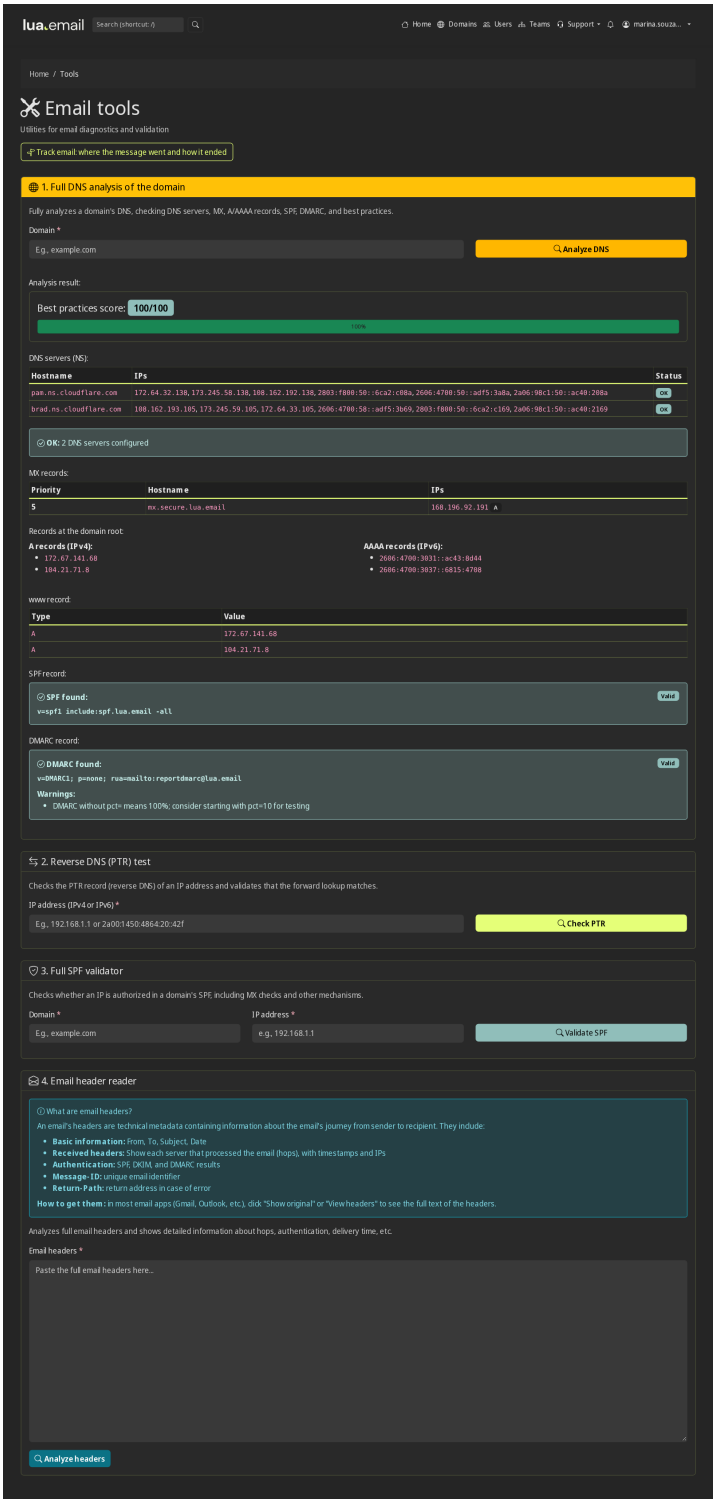


Figure 91: Full DNS analysis of a domain.

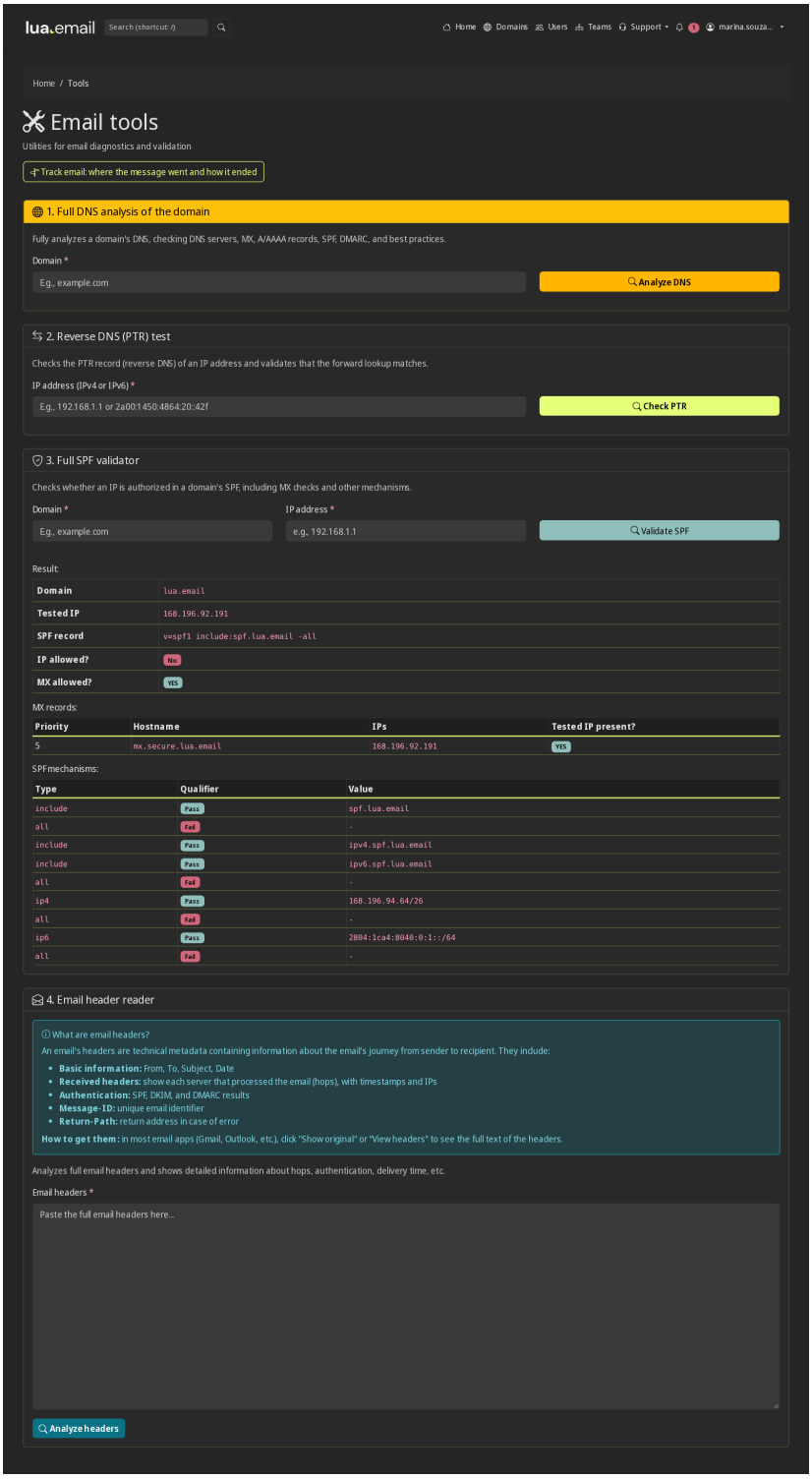


Figure 92: SPF validator: this IP is not authorized to send for the domain.

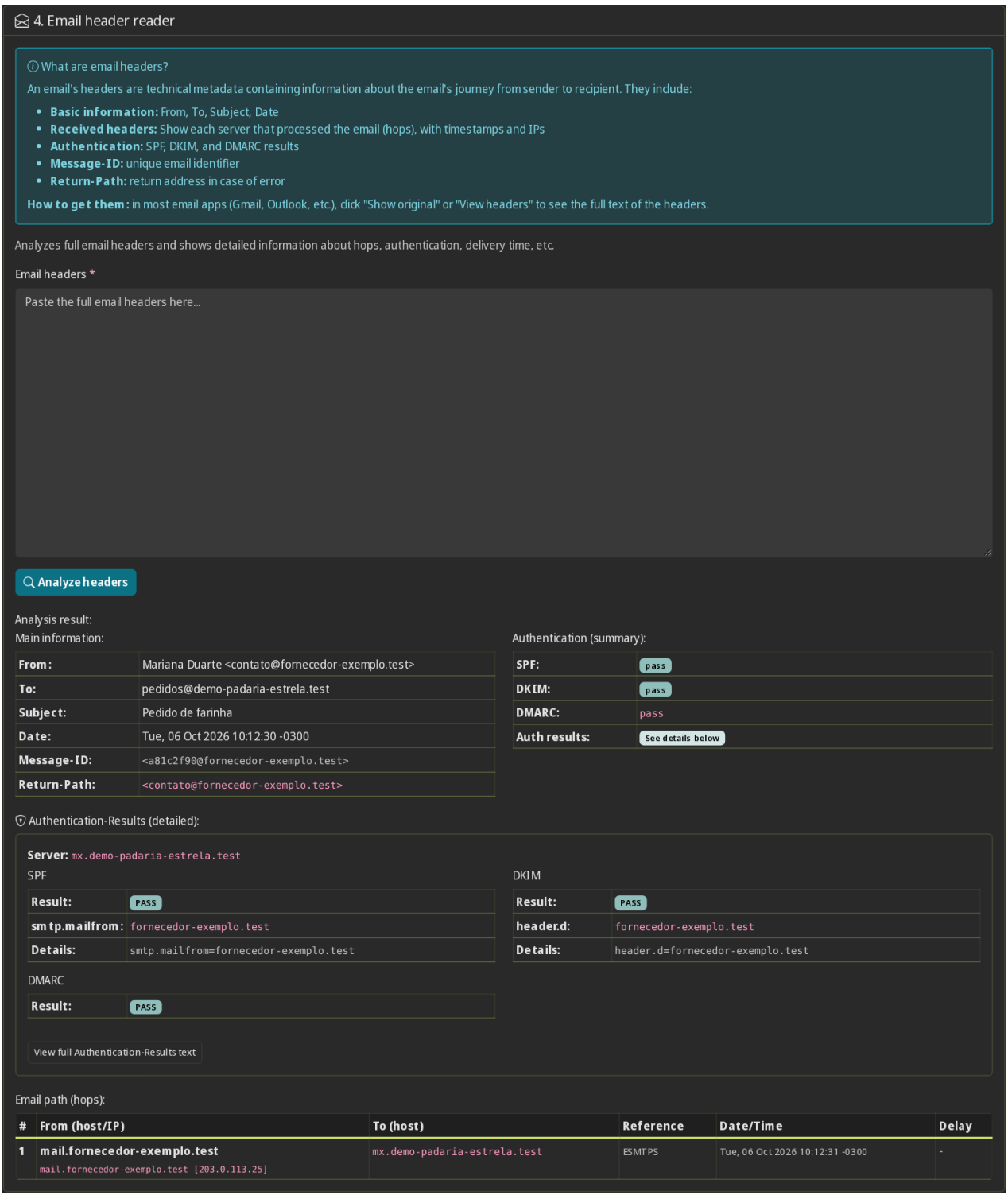


Figure 93: Header reader with a fictional message.

14. Users, teams and roles

More people can administer the company's email, each with their own login. The role defines what each one can do, and the access teams define which domains and at what level.

Role	Sees	Can change
Administrator	The team's domains	Everything this manual shows: domains, mailboxes, aliases, groups, routing, panel users.
Helpdesk	The team's domains	Only mailbox passwords and support tickets. Ideal for whoever handles "I forgot my password".
Read-only	The team's domains	Nothing. It works for auditing, for finance to check licenses or for a consultant.

All three roles can still look after their own account: change their own password, see their sessions and mark notifications as read.

Add a user

1. Open **Users** (address `painel.lua.email/teams/users`) and click **New user**.
2. Enter the person's email (it is the login), the password and the confirmation. The **Generate** button creates a strong password.
3. Choose the **Role**: Administrator, Helpdesk or Read-only.
4. Fill in the phone and, if you want, the alternate email, and click **Save**. The new user joins the same team as you and sees the same domains.

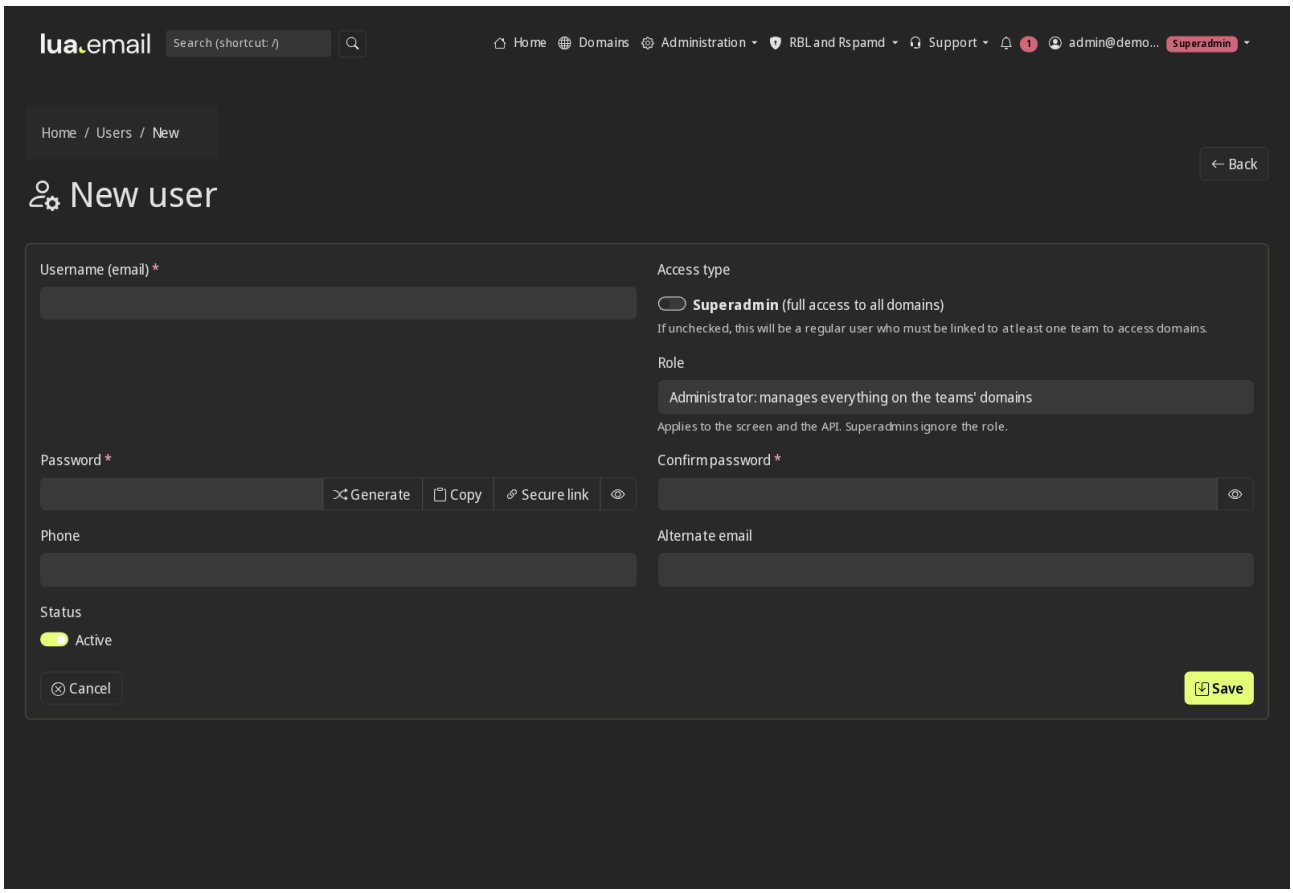


Figure 94: New user with the helpdesk role.

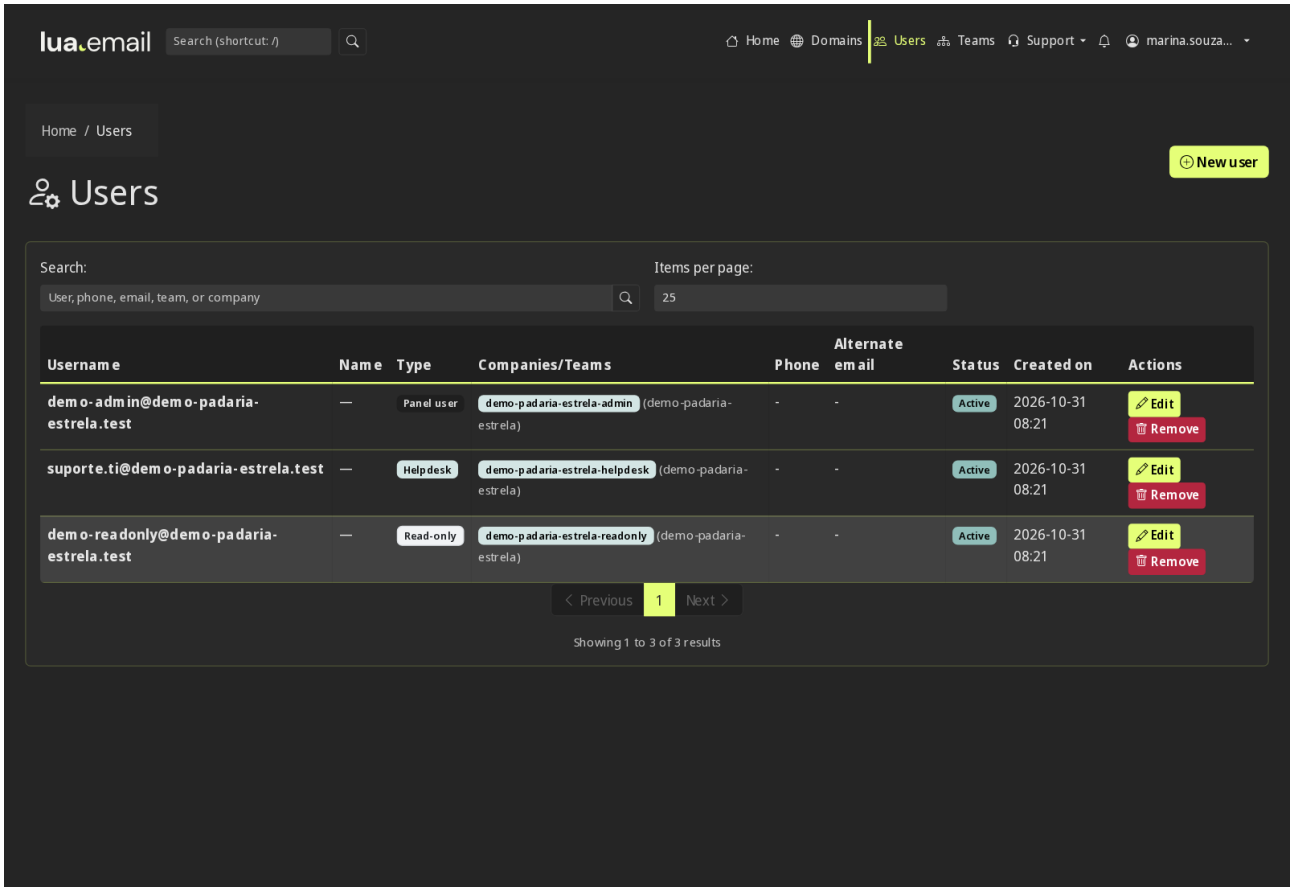


Figure 95: The panel's users and each one's role.

When someone creates a user, generates an API token or changes another administrator's password, the company's administrators get a notice in the bell and by email. If you don't recognize the action, contact support.

Anyone who signs in with a restricted role sees a notice at the top of every screen. Buttons the role doesn't allow appear disabled, and the panel rejects the change even if someone tries another way.

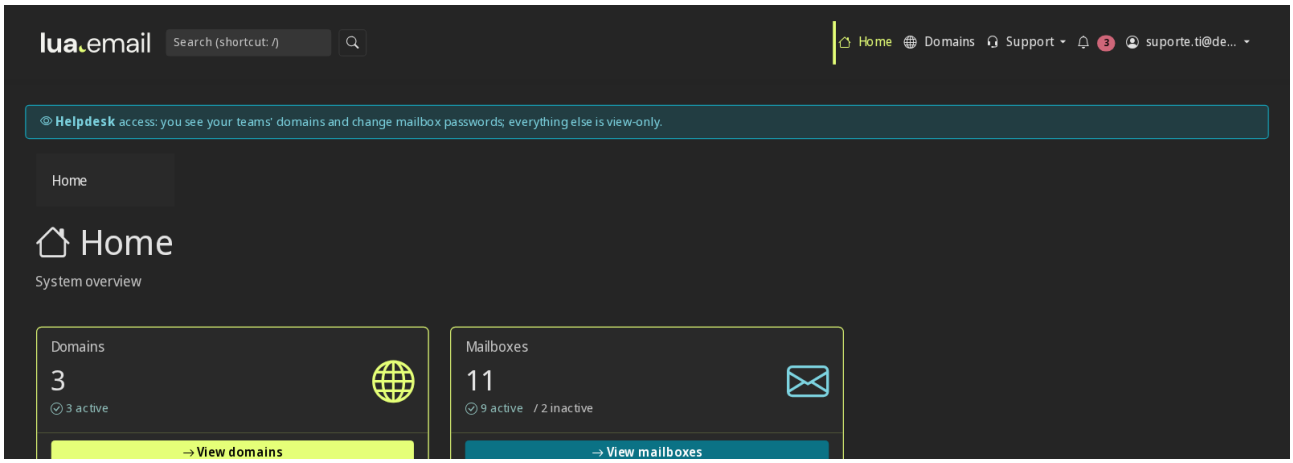


Figure 96: The notice the helpdesk user sees at the top.

To remove access for someone who left the company, use **Remove** in the user list, or turn off **Active** in the edit screen to suspend without deleting.

Reset a user's two-step verification

If someone lost their phone and their recovery codes, open **Users**, click **Edit** on that person, and under **Two-step verification** click **Reset**. At the next sign-in, the password is enough; the person can turn it on again in My profile (if it is mandatory, the panel asks them to set it up right after signing in).



Figure 97: The verification status and the Reset button, in the user's edit screen.

Only administrators can reset it, and only for the users they administer. Nobody resets their own verification here: for that, use My profile, with your password and a code. The person and the company's administrators receive a notice.

Access teams: who sees which domain, and at what level

A **team** brings people together and gives them a **level** (administrator, helpdesk or read-only) over a set of the company's domains. Instead of adjusting the role person by person, you build the team once and add whoever needs it. The **Teams** menu sits next to **Users**, for whoever administers the company.

How it works:

- **Team level:** applies to everyone on the team, in the team's domains. Administrator manages everything; helpdesk views and only changes mailbox passwords; read-only just views.
- **Team domains:** either **all of the company's domains, including ones added later**, or only the ones you select. With "all", a new company domain already applies to the team, with nothing for you to remember to adjust.
- **More than one team:** someone on two teams gets, in each domain, the **highest** level between them. The same person can be an administrator of one domain and a read-only user of another.
- **Older teams:** teams created before this option have no level. In them, each person keeps the role they have in their own record, as at the start of this chapter. They appear in the list with the **View** button (view-only).

Team level	Sees	Can change
Administrator	The team's domains	Everything this manual shows in those domains. Also administers teams and users, within its own level.
Helpdesk	The team's domains	Only mailbox passwords.
Read-only	The team's domains	Nada.

Why use teams: when people change (an intern joins, the IT firm leaves), you change one place only. Access follows the role, not the person. And it is easy to answer, in an audit, who can do what in each domain: just open the team list.

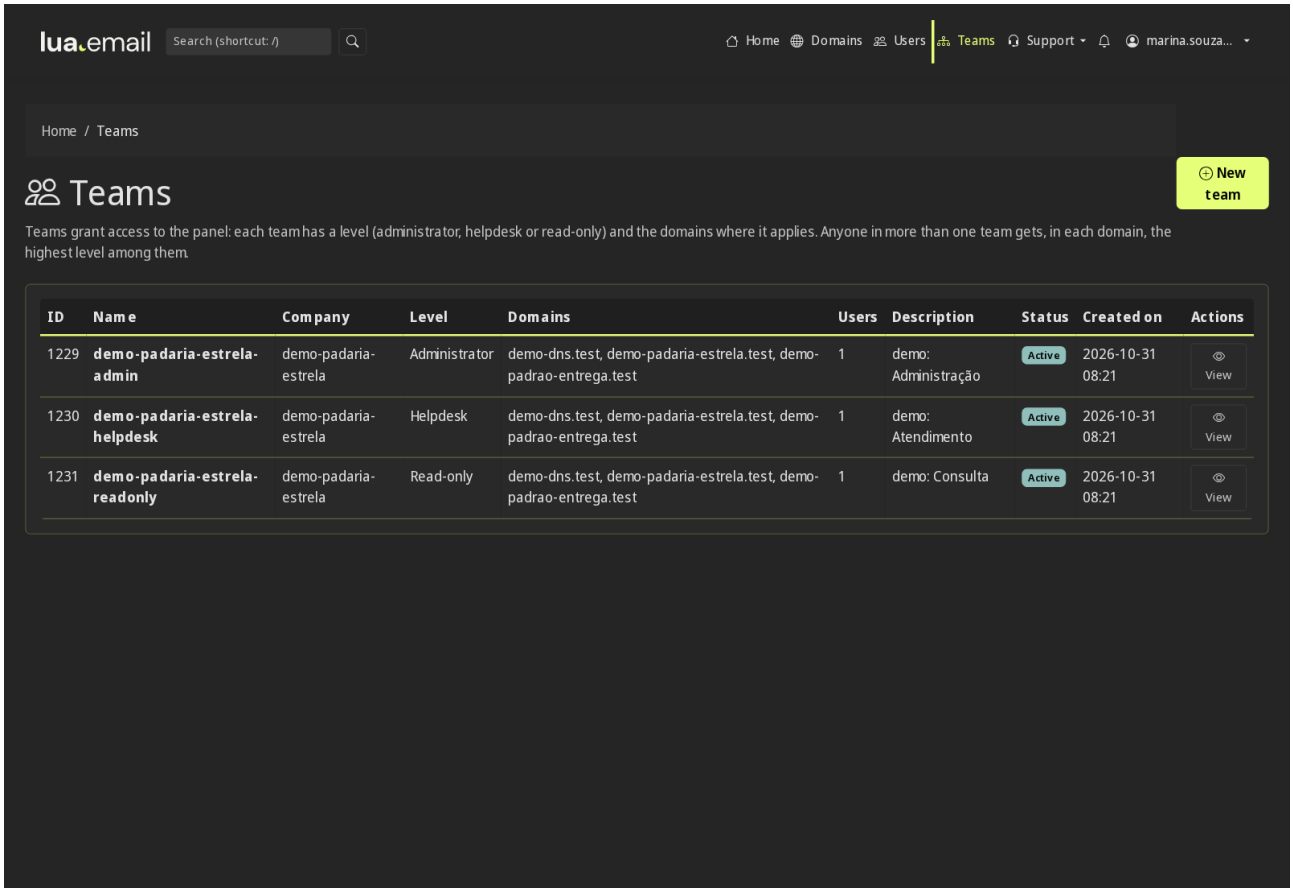


Figure 98: The company's team list, one per access level.

Create a team

1. Open **Teams** and click **New team**.
2. Give it a **name** (for example, "Outsourced IT"). The name is unique in the panel: if it already exists, the screen asks for another one, without saying whose it is.
3. Check the **Company** and, if you want, write a description to remember what the team is for.
4. Choose the **Access level**. You can grant up to your own level, never more.
5. Under **Domains**, check **All of the company's domains** or **Only the domains selected below** and move the domains to the **Managed** list (double-click or with the arrows). The list only shows the company's domains where your level reaches the chosen level.
6. Click **Create team**. The next screen is the edit page, where you add people.

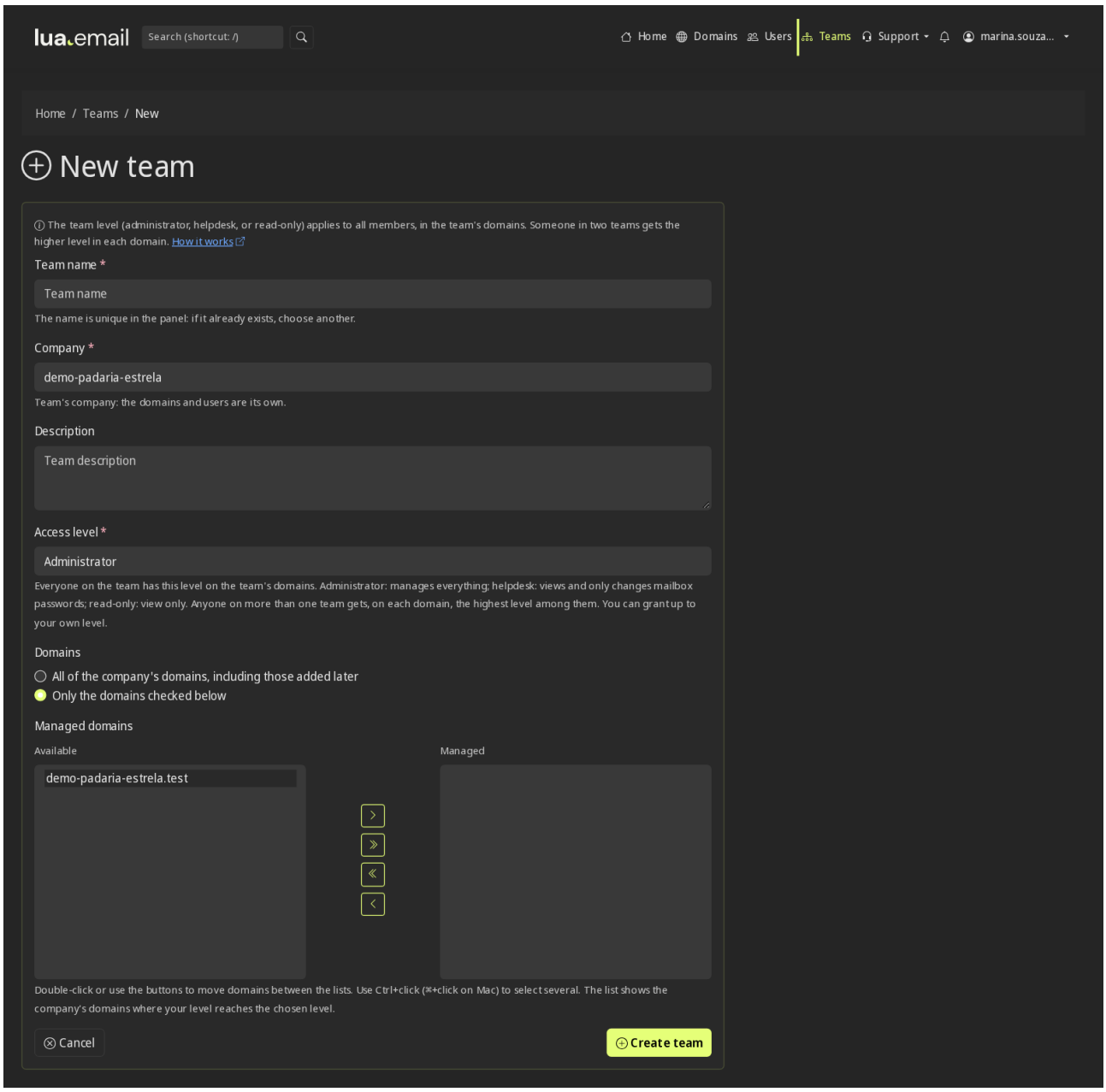


Figure 99: New team: the level and the domains define what each person on the team can do.

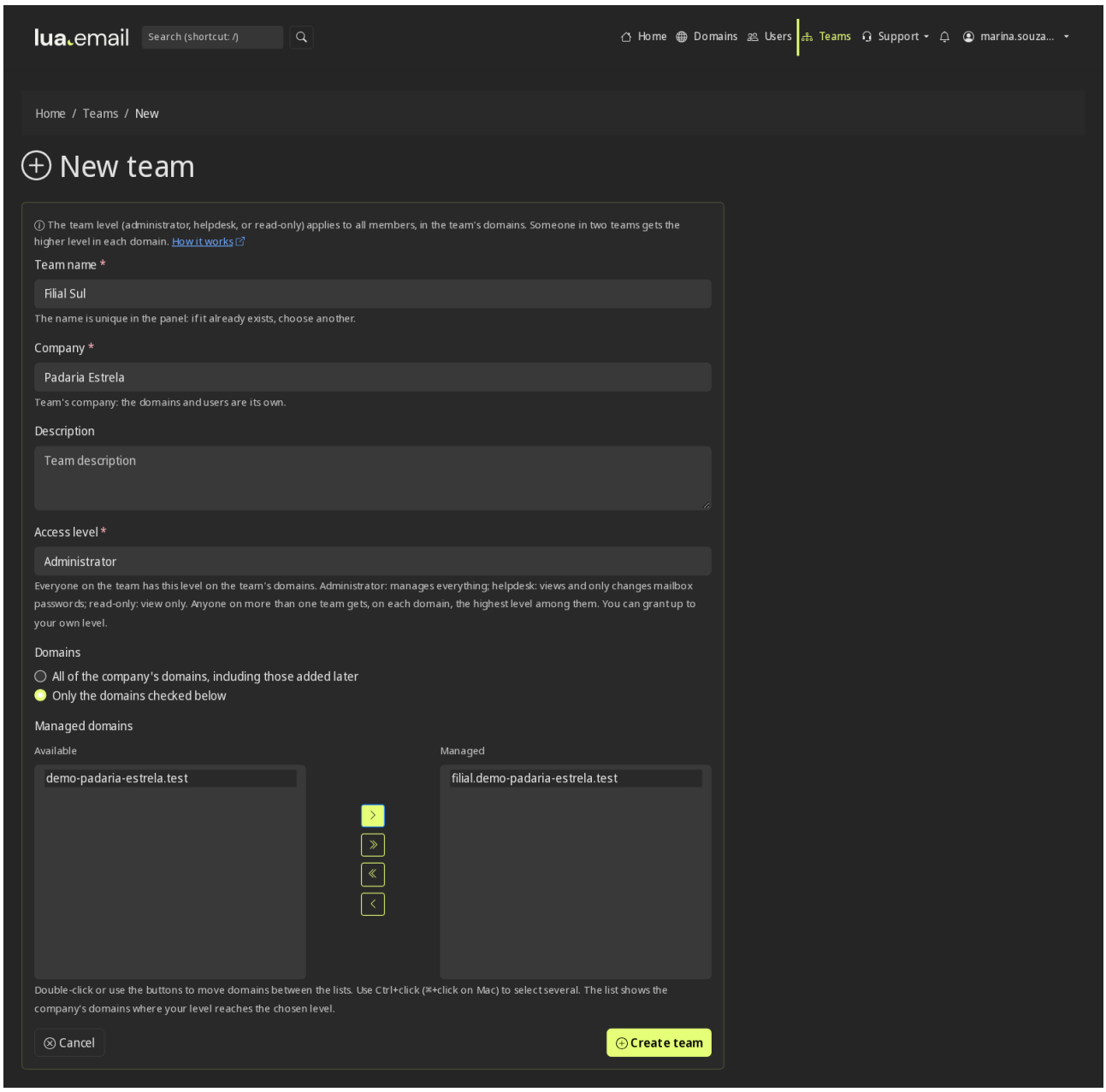


Figure 100: Administrator team for a single domain: the selected domain moves to the Managed list.

Add people to the team

On the team edit page, the **Team users** section shows who is already on it, with **Remove** on each row. To add someone:

- **Someone who already has a login:** type their email under **Add user** (from 2 characters) and click the result. The search only shows people who are already on some team in your company.
- **Someone who doesn't have a login yet:** click **Create user in this team**. The form is the same as **New user**, with a notice that the person joins the team at the team's level (the Role field only applies to teams without a level). It can be someone outside the company, such as the technician at the IT firm: their email is their login.

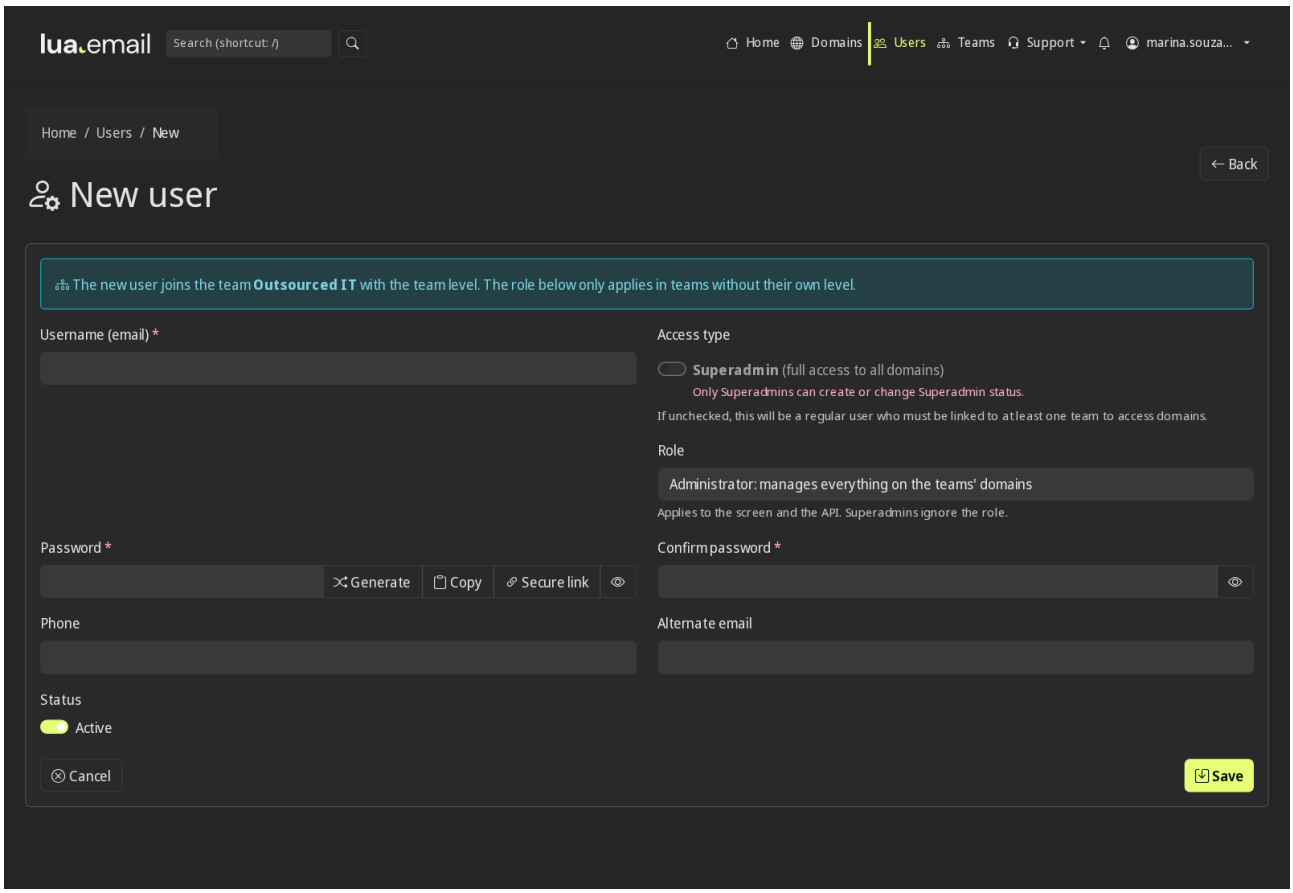


Figure 101: New user created inside the team: the notice at the top explains that the team's level applies.

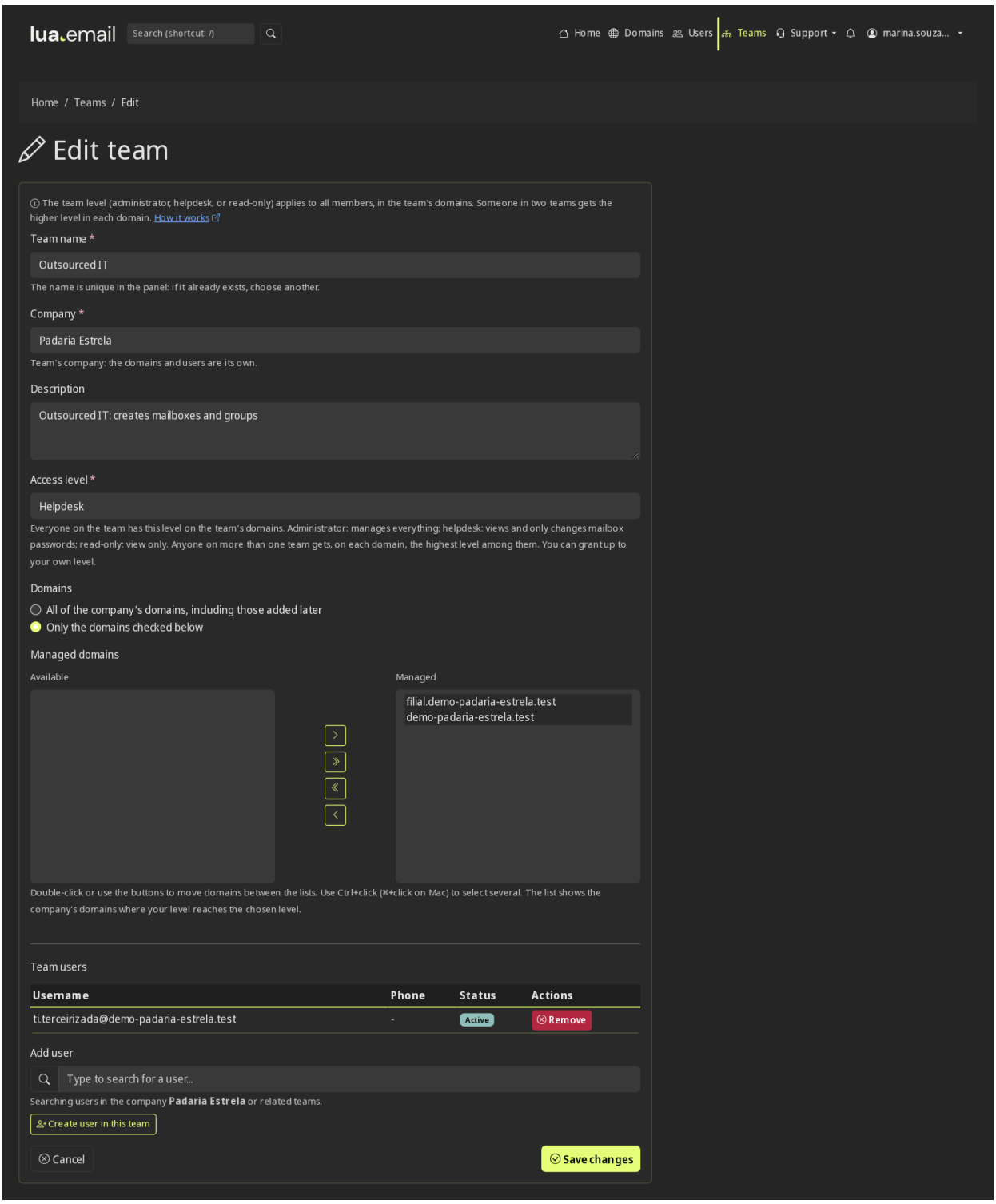


Figure 102: Team edit screen: level, domains and the people who belong to it.

In the **Users** list, the **Companies/Teams** column shows which team each person is on.

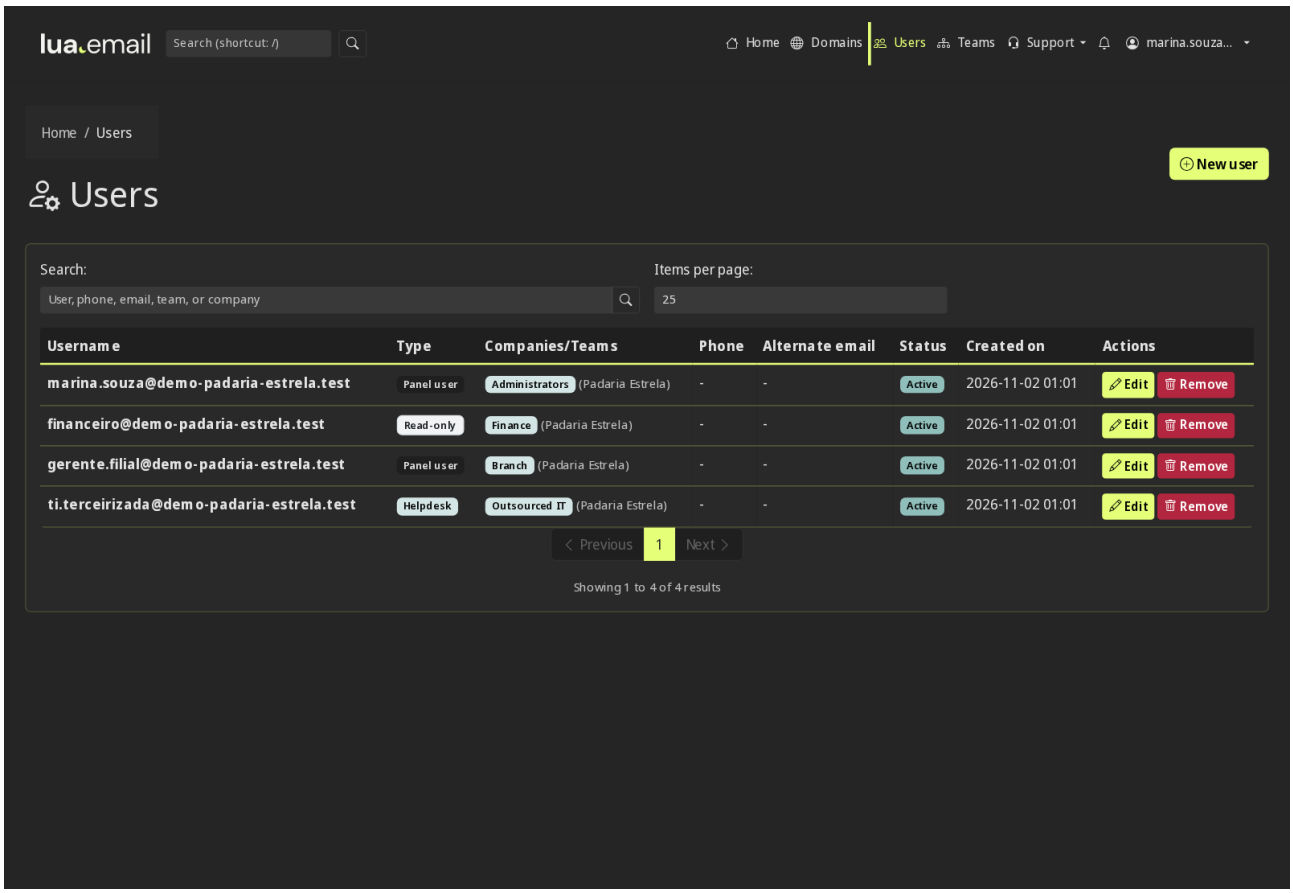


Figure 103: The panel's users and each one's team.

What the person sees when signing in

Each person sees only the domains their team reaches, and the notice at the top says which level applies. Buttons the level does not allow appear disabled, and the panel refuses the change even if someone tries another way. Anyone with different levels on different domains sees a notice that, on a screen that mixes domains, the most restrictive level applies. Read-only users see the notice "Read-only access: you can view but not change." Helpdesk team members see "Helpdesk access: view your teams' domains and change mailbox passwords; the other items are view-only." Items that only our team can change carry the notice "Only the Lua team can change this."

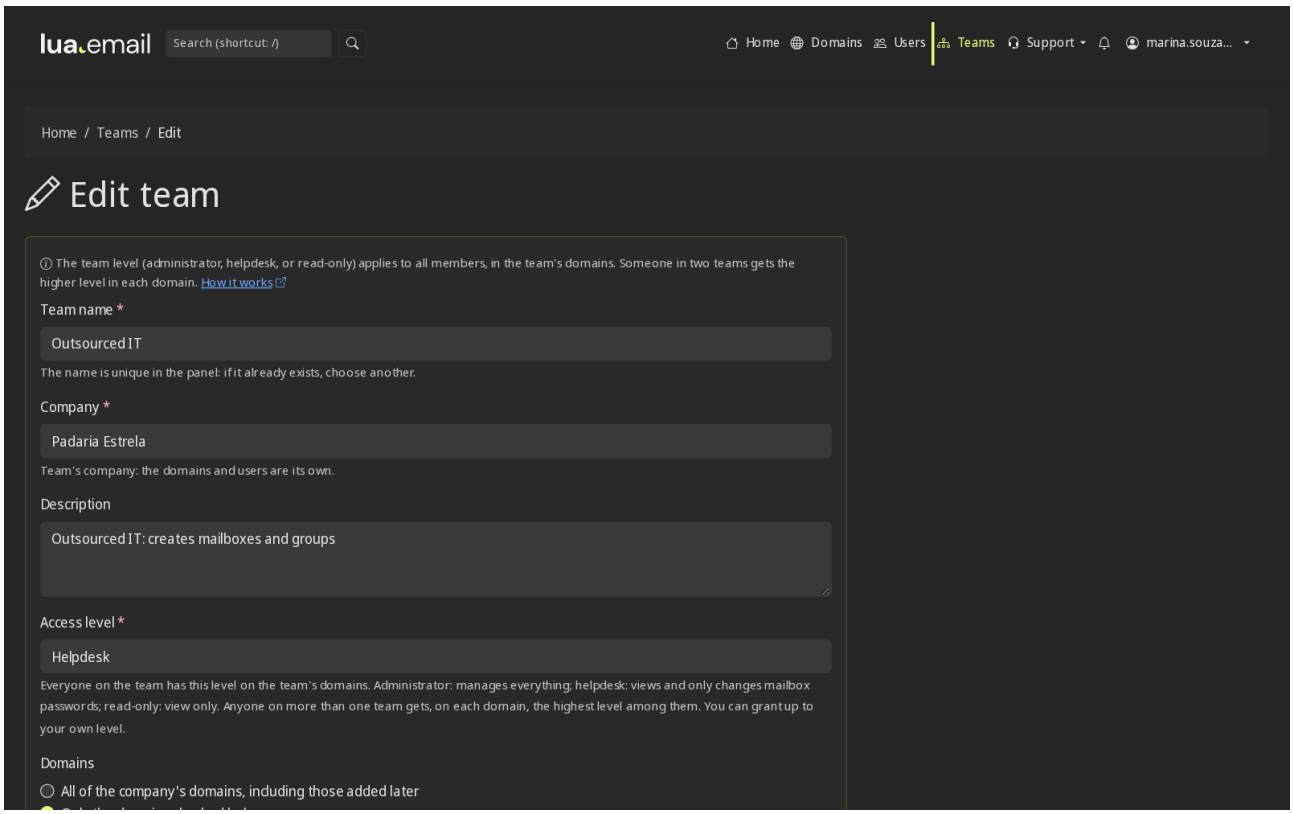


Figure 104: Someone on a helpdesk team: notice at the top and only the team's domains.

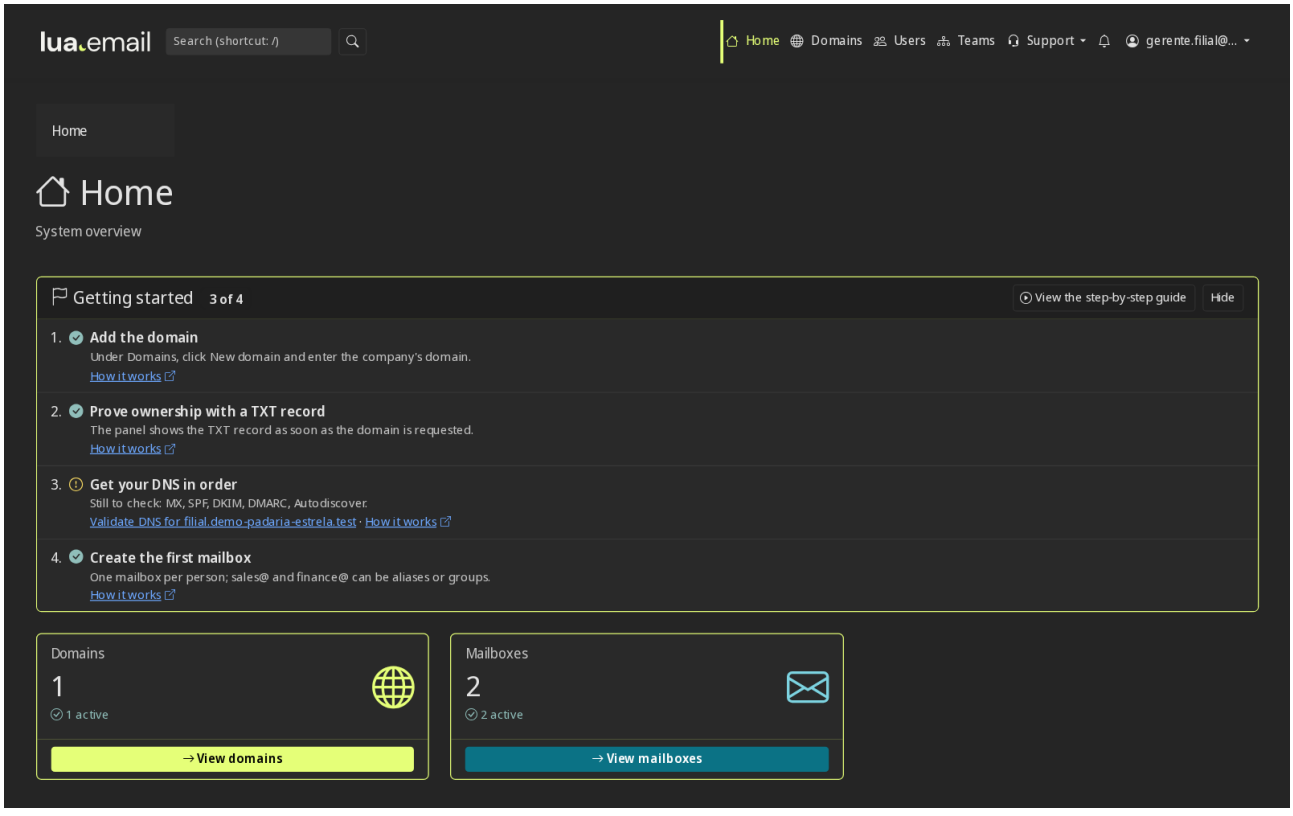


Figure 105: Someone who administers only the branch's domain sees one domain and two mailboxes.

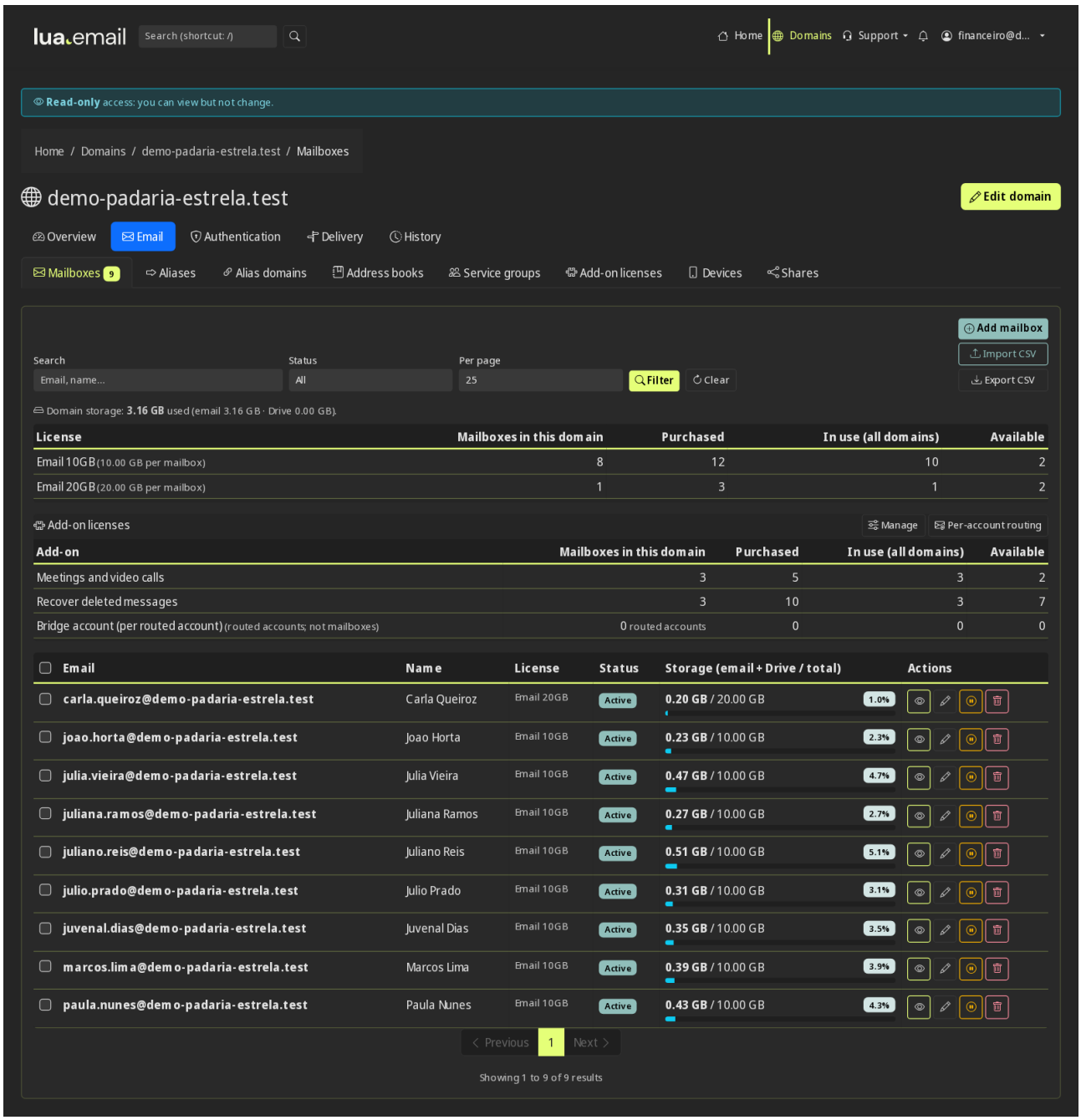


Figure 106: Read-only: finance sees the mailboxes and licenses, without changing anything.

What the team's administrator can and can't do

- **Only your own company:** you see and change the teams of the companies you administer. Another company's team doesn't show up, not even by its address.
- **You can't give more than you have:** the team's level is, at most, your own level in each of its domains. "All domains" only appears if you cover all of the company's domains. No one becomes a superadministrator through a team.
- **You can't lock yourself out:** the panel refuses to remove the team, leave it, lower the level, take away domains or change your own role if that would make you lose your administrator level in the company.
- **View-only:** older teams (without a level) and teams that give more access than you have appear with **View**, without editing.

- **Only people from the company:** you add to the team people who are already on a team in the same company, or create the person there. Who manages whom also follows the level: a single-domain administrator just doesn't manage the administrator of the whole company, and helpdesk doesn't manage administrators.
- **Everything is in the history:** creating, editing and removing a team, and adding or removing people, appear in **History → System logs** of each of the team's domains.

Removing a team takes away from its members the access the team gave. Anyone with access through another team, or through the role in their record, keeps that other access.

When to use it and use cases

Use a team whenever the **same access** applies to **more than one person** or changes over time. Real examples of combinations:

Situation	Team	Why this setup
Outsourced IT team serving the whole company	Helpdesk, all of the company's domains	They solve "I forgot my password" in any domain, including ones the company opens later, and they don't touch DNS, aliases or mailboxes. When the contract ends, you remove the team and the access goes away.
Finance checks mailboxes and licenses	Read-only, all domains	They see how many mailboxes and licenses are in use and the cost, with no risk of deleting or editing something by mistake.
Branch with its own domain and a manager who handles everything there	Administrator, only the branch's domain	The manager creates the branch's mailboxes, aliases and groups. The headquarters domains don't appear for them.
Support intern learning the panel	Read-only, only the selected domains	Follows day-to-day support without being able to change anything. When they are hired full-time, just switch teams or raise the team's level.
Executives who want to see what is happening, without operating	Read-only, all domains	They see statistics, logs and message tracking with their own login, without receiving anyone's password.
Partner serving more than one company	One team in each company, at whatever level each one wants	A team always belongs to a single company, so each company creates its own team and the partner's login in it. Each company decides and revokes its own access.

Two levels at once: the headquarters IT analyst is an administrator at headquarters ("Headquarters" team) and read-only at the branch ("Branch, read-only" team). Since the highest level applies in each domain, she administers headquarters and only views the branch, without needing two logins.

When not to use it

- **To give access to a folder or a mailbox:** teams give access to the **panel**. Whoever reads another person's mailbox uses sharing in webmail; whoever needs access hours, a directory or a team email uses a service group.
- **For one person, one time:** if it's just one person and it will always be that way, a user with a role is enough. A team pays off when there are more people, more than one domain, or when you want to revoke everything at once.
- **To solve a one-off ticket in a mailbox:** use support access to webmail, which has a time limit, a reason and a record.

15. Other features

Access lists (allow and block senders)

In **Delivery → Access lists**:

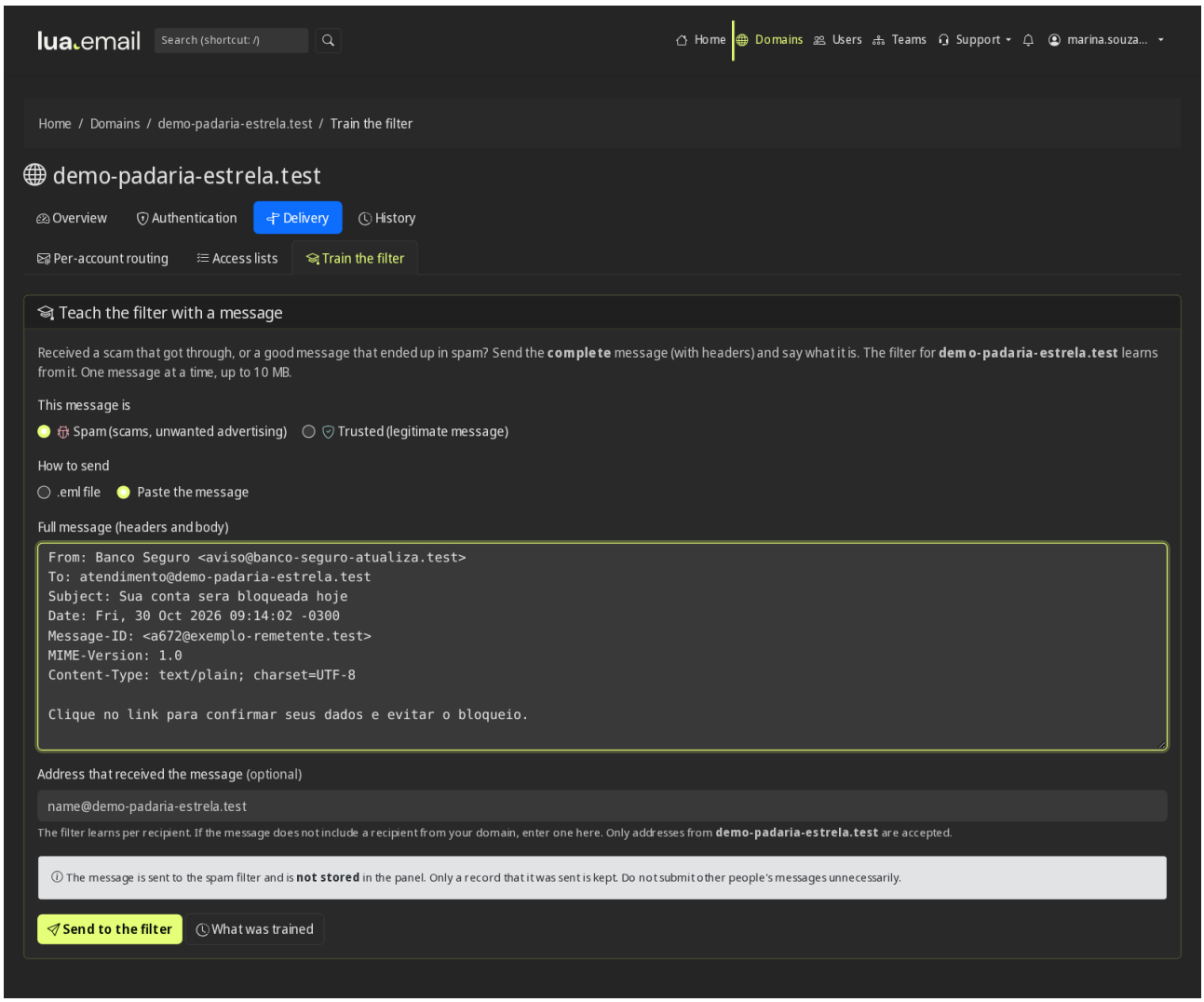
- **Whitelist:** senders that always get through the spam filters. Use `*@supplier.com.br` for a whole domain. Only allow senders you know: whatever is on the list gets through even if it looks like spam.
- **Blacklist:** senders that are always rejected, for example someone who keeps sending advertising.

Each entry has two fields. **To** is the recipient: just the user (`sales`) or the full email address; with * or blank, it applies to all mailboxes in the domain. **From** is the sender: an email address, a whole domain (`*@supplier.com.br`) or * for everyone. For example, To `sales` and From `customer@supplier.com.br` allows only that customer, and only to sales@.

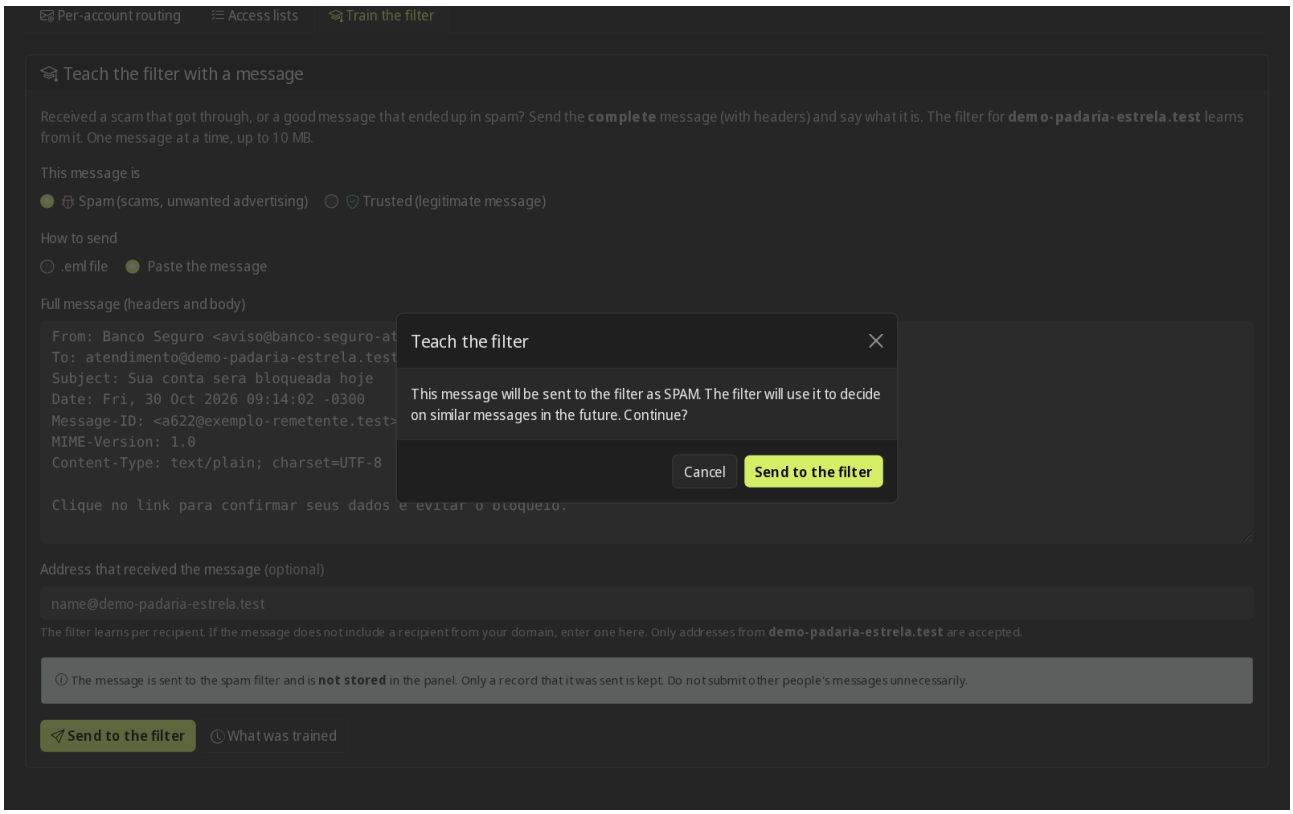
If a legitimate message went to spam, prefer to teach the filter (in webmail, by moving it out of the Spam folder, or in Delivery → Train the filter) before allowing the sender.

Train the spam filter

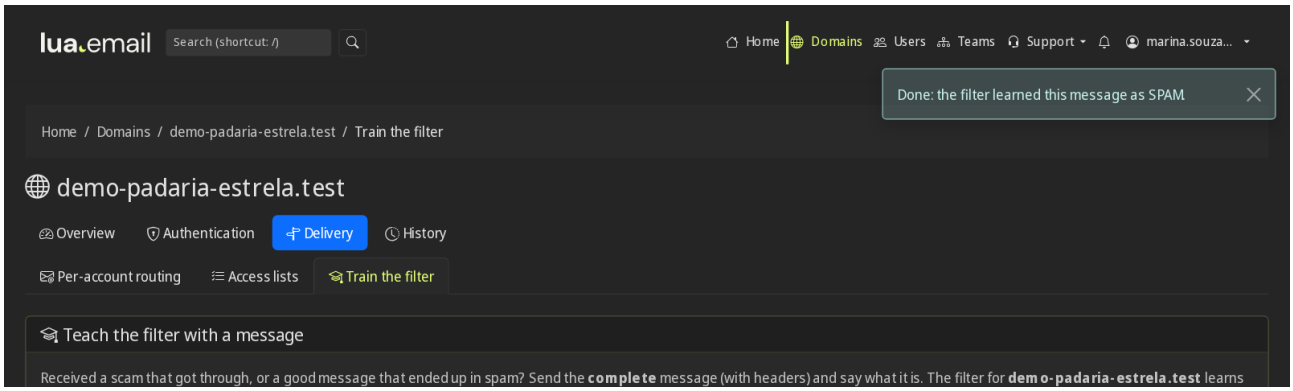
With the **Shield** or **Bridge** license, in **Delivery → Train the filter** you teach the domain's filter with a message that got through as spam or was marked for no reason. Choose **SPAM** or **TRUSTED**, upload the `.eml` file or paste the full message, with the headers, and confirm.



Delivery → Train the filter: the type, the message, and the address that received it (real screen, fictional data).



The confirmation before sending (real screen, fictional data).



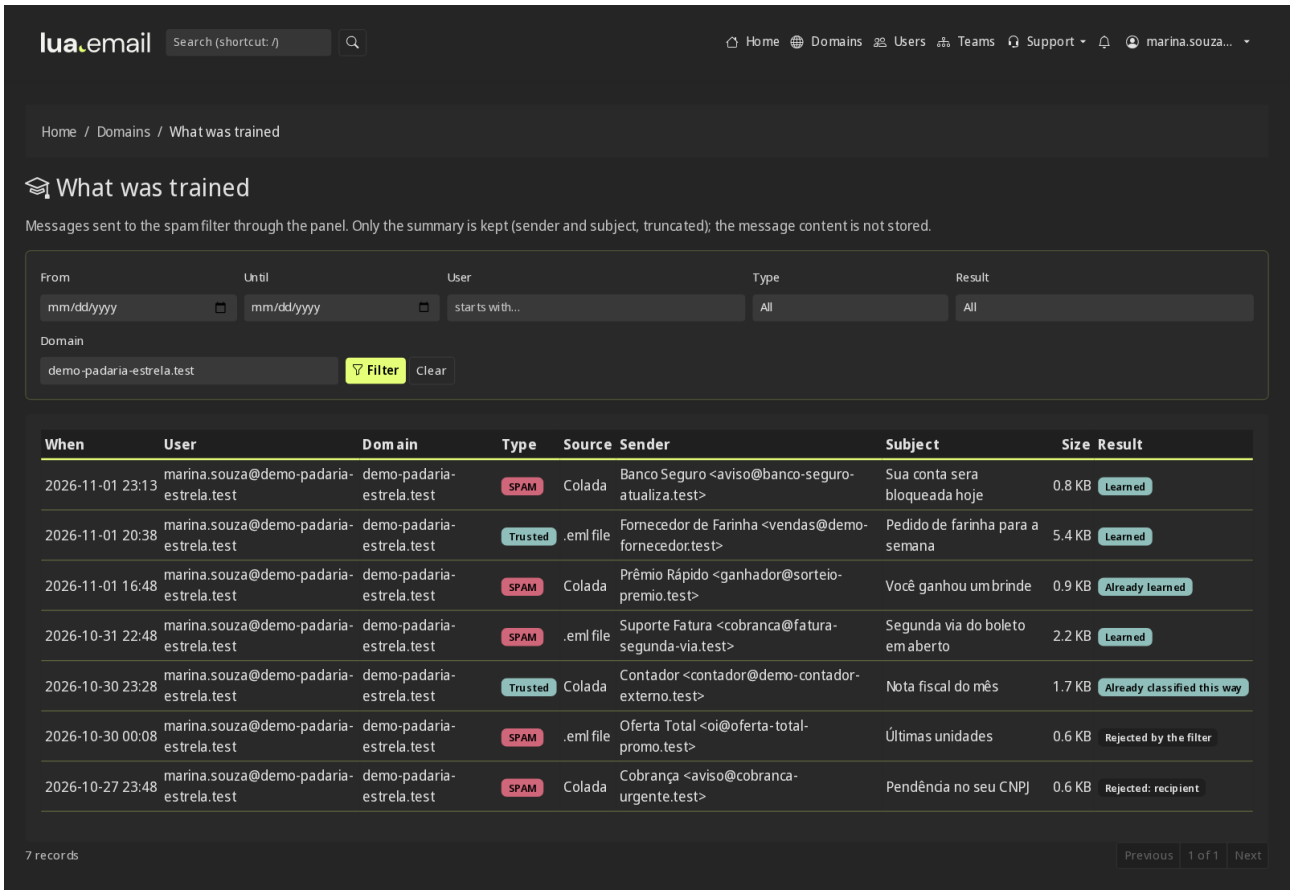
The result: the message appears at the top of the page (real screen, fictional data).

- The filter learns by **destination address**, not for the whole domain: the message teaches the mailbox that received it. Only addresses in the domain are accepted; if the message doesn't include one, enter the mailbox in the optional field.
- One message at a time, up to 10 MB, with a limit of submissions per hour. Read-only and Helpdesk profiles see the screen without the form.
- "All good: the filter had already learned this" is a success. "Couldn't train right now. Try again later" means the filter is unavailable for the moment.

The step by step, including how to get the.eml in each app, is in the Shield documentation and in the Bridge one.

What was trained

The **What was trained** button shows each submission, with date, who sent it, type, sender, subject and result, and filters by date, user, type, result and domain. The message content is never stored.



What was trained: the domain's submissions and the result of each one (real screen, fictional data).

Webmail with your brand (whitelabel)

With the whitelabel, your company's webmail and Colabora open with your logo, your name and your colors, at `webmail.yourcompany.com` and `colabora.yourcompany.com`. It is per domain and, for now, **has no cost**. The domain administrator does everything alone in the panel; the Lua team does not need to be involved.

Who can do what: the **domain administrator** creates, uploads the.zip, checks and turns off. The Helpdesk and Read-only roles can only view the screen. **Deleting the brand** and using an address outside the standard (other than `webmail.<your domain>` and `colabora.<your domain>`) remain with the Lua team: open a ticket if you need it.

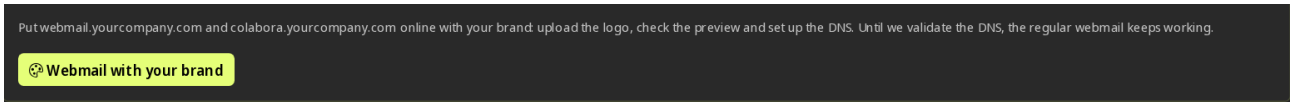
In short, there are five steps: **1)** generate the.zip in the simulator; **2)** upload the.zip in the panel; **3)** see the preview; **4)** confirm and apply, and the panel **turns on** the `webmail.yourcompany.com` and `colabora.yourcompany.com` addresses by itself; **5)** set up the DNS, if it is at another provider, and follow along until it is ready. Until the DNS is set up and validated, webmail and Colabora with your brand **do not open**: keep using the regular webmail.

1. Generate the brand.zip in the simulator

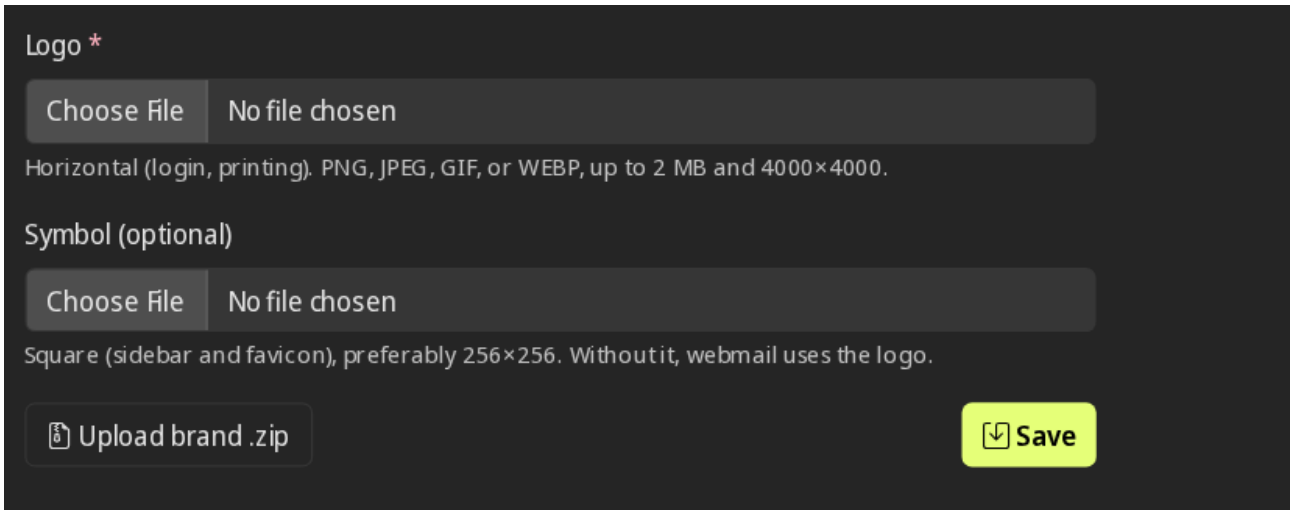
In the brand simulator you choose the logo, see how it looks and download the ready.zip with the logo, the symbol, the colors and the addresses. Nothing leaves your computer until you upload the file to the panel. If you prefer, you can also fill in the fields by hand on the screen itself and click **Save**.

2. Upload the.zip in the panel

Open the domain and, in the domain settings, click **Webmail with your brand**. At the bottom of the form, click **Upload brand.zip**.

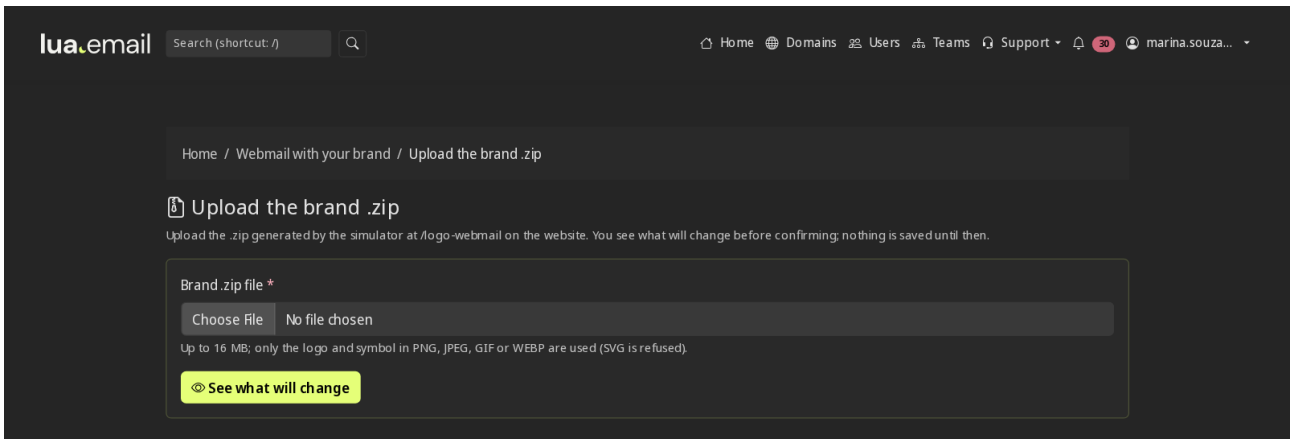


In Domain settings, the Webmail with your brand button (real screen, fictional data).



The Upload brand.zip button is at the end of the form (real screen, fictional data).

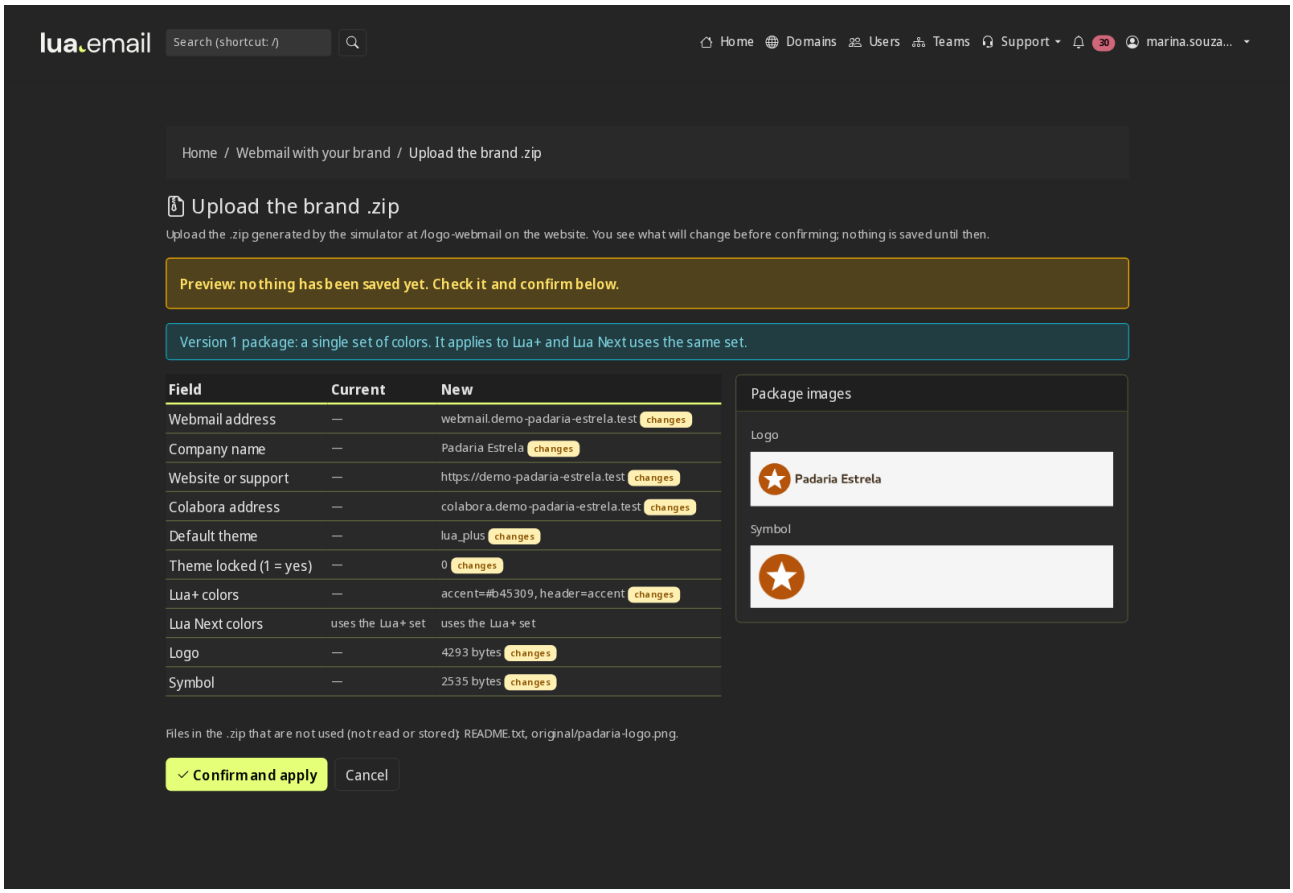
Choose the file and click **See what will change**. The limit is 16 MB; only the logo and the symbol (PNG, JPEG, GIF or WEBP, up to 2 MB and 4000 × 4000 pixels each) are used, and SVG is refused for security. The webmail address inside the.zip must be your domain's; if it belongs to another, the panel refuses it and explains why.



Upload the brand.zip (real screen, fictional data).

3. Check the preview

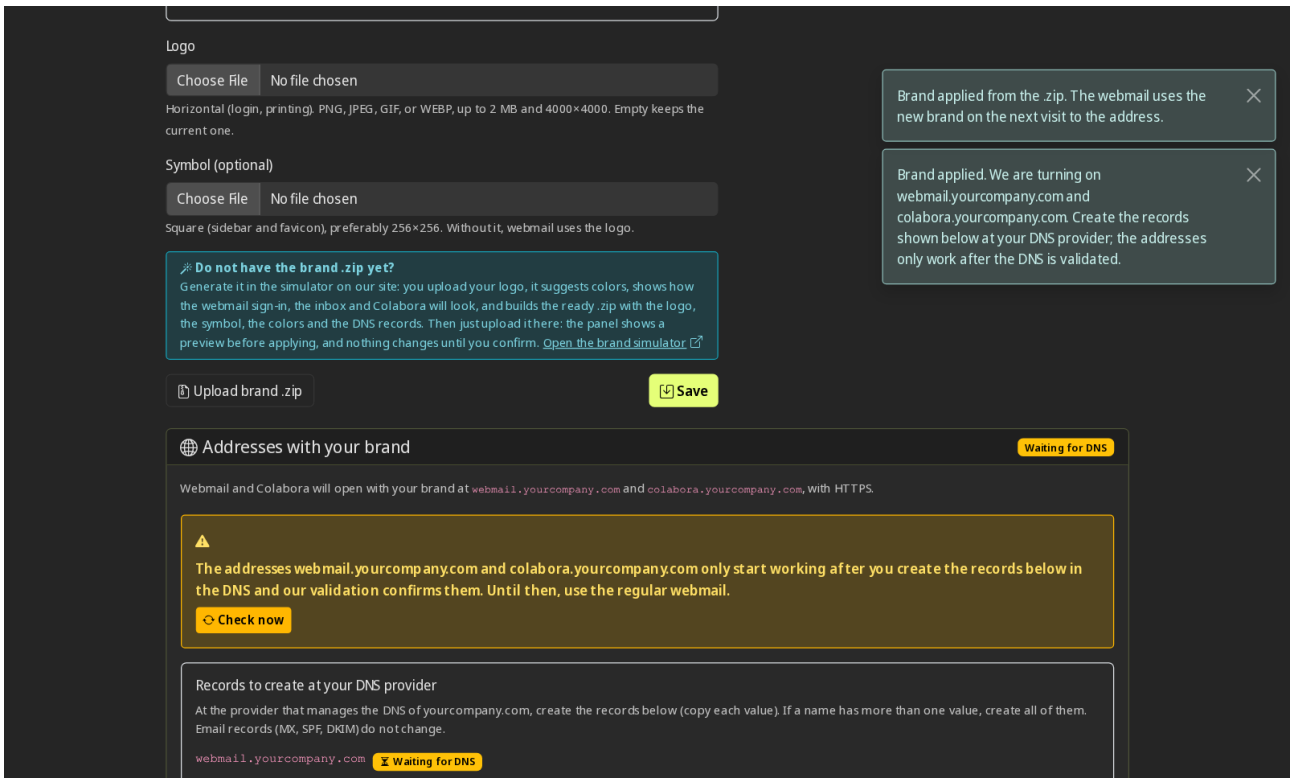
The panel shows what will change, field by field, and the images in the package. **Nothing is saved yet.**



The preview: what changes and the package images, before saving (real screen, fictional data).

4. Confirm and apply

If it looks right, click **Confirm and apply**; if not, **Cancel**. On confirming, the brand is saved and the panel **turns on** both addresses by itself, `webmail.<domain>` and `colabora.<domain>`. There is no *Turn on* button anymore: the screen already shows the progress. If the addresses cannot be turned on at that moment, the brand stays saved and the **Try turning on again** button appears.

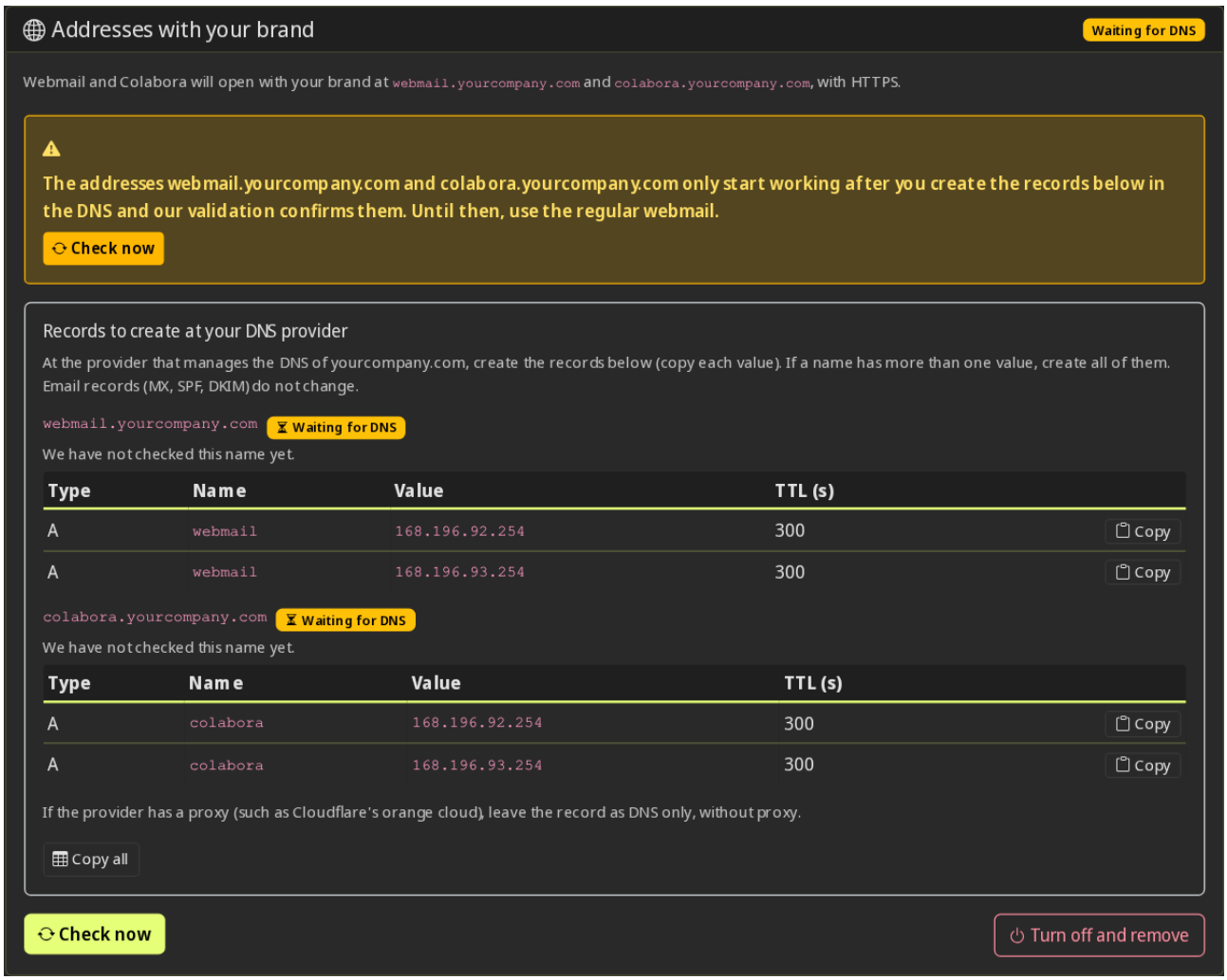


After confirming: the addresses are already being turned on (real screen, fictional data).

5. Set up the DNS and follow along until it is ready

The webmail.<domain> and colabora.<domain> addresses only start working once the DNS is set up and our validation confirms it. Until then, use the regular webmail.

With the DNS at Edgium, everything is automatic and you just follow along. With the DNS at **another provider**, the screen shows, for each name (`webmail.<domain>` and `colabora.<domain>`), the **A** records, one for each Edgium CDN IP (today there are two IPs, so two A records for each name), with name, value, **a TTL of 300 seconds** and a **Copy** button on each row, plus **Copy all**. The yellow notice at the top reminds you that the addresses only work after the DNS is validated. The screen also shows what the public DNS answers right now and the state of each name: *waiting for DNS*, *pointing* or *ready*. We use A records (not CNAME) and the values are the ones on the screen: never copy IPs from anywhere else.



The records to create at your DNS provider, the notice and the state of each name (real screen, fictional data).

Domain with DNS on Edgium

It is automatic: we create the records and validate them. The screen says we are creating the records and validating, and that it takes a few minutes. You just follow along and see which records they are (read-only). There is nothing else to do.

Domain with DNS at another provider

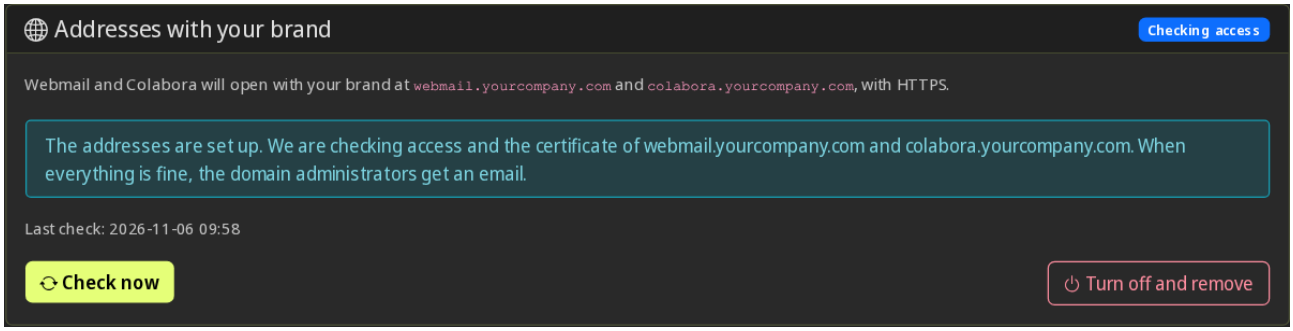
At the provider where the domain's DNS is managed, create the A records the screen shows, for `webmail` and for `colabora`. Do not delete the email records (MX, SPF, DKIM, DMARC). In each record:

- **Type:** A.
- **Name:** just `webmail` or `colabora`. Providers that add the domain on their own do not want the full name (`webmail.yourcompany.com` would become `webmail.yourcompany.com.yourcompany.com`). When the provider asks for the full name, use the full name.
- **Value:** the CDN IP shown on the screen (<CDN IP shown on the screen>). If the screen lists more than one IP, create one A record for each.
- **TTL:** 300 seconds, or the lowest value the provider accepts.
- **Registro.br:** in *Domain panel → DNS → Edit zone* (or *Configure DNS zone*), click *New record*. It only applies if the domain uses the Registro.br DNS servers.
- **Cloudflare:** in *DNS → Records → Add record*. Set *Proxy status* to **DNS only** (gray cloud). With the orange cloud on, validation and the certificate do not work.

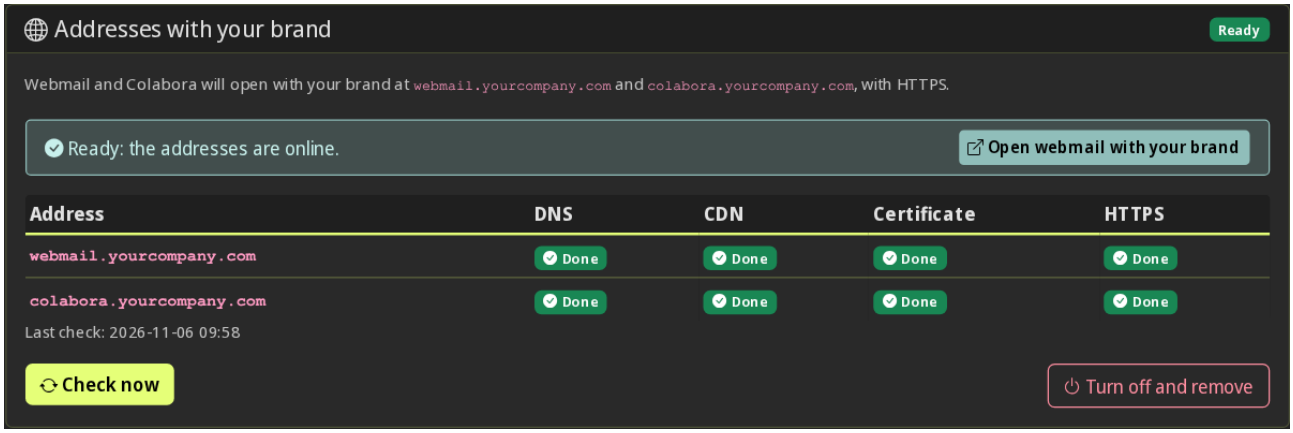
- **GoDaddy:** in *My Products* → *DNS* → *Manage* → *Add New Record*. In the *Name* field, just `webmail` or `colabora`.
- **cPanel:** in *Zone Editor* (*Zone Editor*) → *Manage* → *Add Record*. cPanel completes the domain on its own if you type only the name; check how it looks in the list.
- Another provider: look for *DNS*, *zone* or *records* and follow the same rule for type, name, value and TTL.

How long it takes and how to know it worked

- **Time:** usually a few minutes; it can take a few hours, because of propagation at your provider.
- **Checking:** the panel checks on its own every hour. If you have already created the records, click **Check now**. After 30 days without pointing, it stops checking on its own, and **Check now** starts the checking again.
- **The steps:** for each address, the screen shows four steps: **DNS** (the name points to the CDN), **CDN** (the address is active), **Certificate** (issued automatically) and **HTTPS** (the address answers securely).
- **Checking access:** when the four steps finish, the panel runs a **final HTTPS access test** on both addresses: it checks that they open, that the certificate is valid and that your brand shows on the page. While the test runs, the state is **Checking access**. If it does not pass within 24 hours, the screen shows a clear notice and the **Try again** button.
- **It worked when:** both addresses pass the test and the state becomes **Ready: the addresses are online**. Then the **Open webmail with your brand** button takes you to the address.
- **Notice email:** when it is ready, the domain administrators get an email, *Your branded webmail is online*, with the two addresses. It is a single notice.
- **HTTPS certificate:** it is automatic once the DNS points. You do not need to do anything.



The final HTTPS test: the state stays at Checking access (real screen, fictional data).



Ready: both addresses passed the test, with the four steps done (real screen, fictional data).

Common errors

- **Cloudflare orange proxy on:** leave the record as *DNS only* (gray cloud).

- **CNAME or root domain name:** we do not use CNAME. The names are the `webmail` and `colabora` subdomains, not the root domain (`yourcompany.com`).
- **Old record on the same name:** an old A record or CNAME on `webmail` or `colabora` conflicts with the new one. Delete the old one and keep only the A records from the screen.
- **Forgetting `colabora`:** both names must be ready for the notice to change to "Ready".
- **Typos:** check the name and the IP, character by character. Use the **Copy** button on the screen instead of typing.

While the DNS is not ready, nothing changes for your team: use the regular webmail.

Other statuses and turning off

- If *Needs attention* appears, use **Try again**; if it continues, open a ticket. If the automatic turn-on fails when you confirm the brand, use **Try turning on again**.
- **Turn off and remove** asks for confirmation, removes what was created for the webmail and Colabora and makes those addresses stop opening. The brand stays saved.

To change the logo or the colors later, upload a new.zip the same way. The difference from the company logo per domain is that this is the full brand, on your company's own addresses.

Email migration

In **Support → Email migration** you bring the emails from another provider into your Lua mailboxes, with the migration GB you bought and the preview of what will be copied. The step by step is in chapter 16 and in the full tutorial.

Notifications

The bell at the top shows the panel's notices: domain activated, TXT pending, transfer request, user created. **See all** opens the full list, with an unread filter.

Quota alert. Every day at 8 AM, a mailbox that has passed the usage percentages set by the platform receives an email saying how much it has used, adding email and Drive together. The notice repeats every day while the mailbox stays above the limit. To stop it for a domain, turn off **Quota notifications** in the domain's edit screen.

16. Migrate email from another provider

You bring the emails from the accounts at another provider into your Lua mailboxes yourself, through the admin panel. The copy signs in to each old account over IMAP, brings the folders and messages and **deletes nothing** at the old provider. Before migrating, you buy the migration GB yourself, in GB, at the lua.email checkout, without talking to anyone: R$ 2.00 per GB migrated from the source, paid once, no monthly fee. They become a balance in the admin panel, and the copy respects that balance. If you prefer that our team handles the switch, it is billed by the hour: see how we migrate.

In 4 steps: (1) estimate how much the mailboxes add up to at the old provider; the panel preview measures it for free; (2) buy the migration GB yourself at the lua.email checkout; (3) upload the spreadsheet, check the balance and confirm; (4) follow the copy live. Ran short? Buy more migration GB and use **Copy the accounts that were left out**: the migration picks up where it stopped.

Complete tutorial: the step by step, with the video, where each piece of spreadsheet data comes from, how to create the app password and what to do for each error is in Migrate email with the panel. This chapter is the summary.

Download the migration video from the panel

The migration done by the customer's administrator, from the migration GB to the finished copy. Fictional data.

Before you start

Buy the migration GB at the checkout (see Migration GB), create the destination mailboxes (see Create email mailboxes) and gather, for each old account, the address, the password (or app password), the IMAP server and the port (almost always 993 with SSL). The copy does not change the destination mailbox's app password or app access: Outlook and phones keep working during and after the migration. The destination mailbox needs an active license and room for everything coming from the old account. Servers of the most common providers: access details.

Microsoft 365 and Outlook.com: migration done by our team

Microsoft 365 (formerly Office 365), Outlook.com, Hotmail and Live accounts use a different type of authentication that the admin panel tool does not support yet. That is why we migrate these accounts with our own team: contact us to schedule the date and plan the steps. For Google and other providers with 2-step verification, use an **app password**. See the full table.

The accounts spreadsheet (CSV)

One row per old account, with six columns: `source_email`, `source_password`, `source_imap_host`, `source_imap_port`, `source_ssl` and `dest_username`. Download the template and see how to build it in Excel and Google Sheets.

Preview: balance, what will be copied and what stays out

In **Support → Email migration → New migration**, give it a name, upload the spreadsheet and click **Preview**. The panel signs in to each old account and shows whether the login worked, the messages and the size, and checks them against the **migration GB you bought**. It shows what is available, which accounts **will be copied** and which **are left out**, with how much is missing and the way to subscribe to more. Each account gets the **Within the balance** or **Exceeds the balance** badge; when no account goes over the balance, the preview says "All measured accounts are within the balance", and an account without enough room in the destination mailbox gets the warning "They will not be copied because the destination mailbox is out of space". Accounts go in spreadsheet order until the migration GB run out. Confirm with **Confirm and create the migration** (only accounts within the balance go into the queue); the preview is valid for 1 hour.

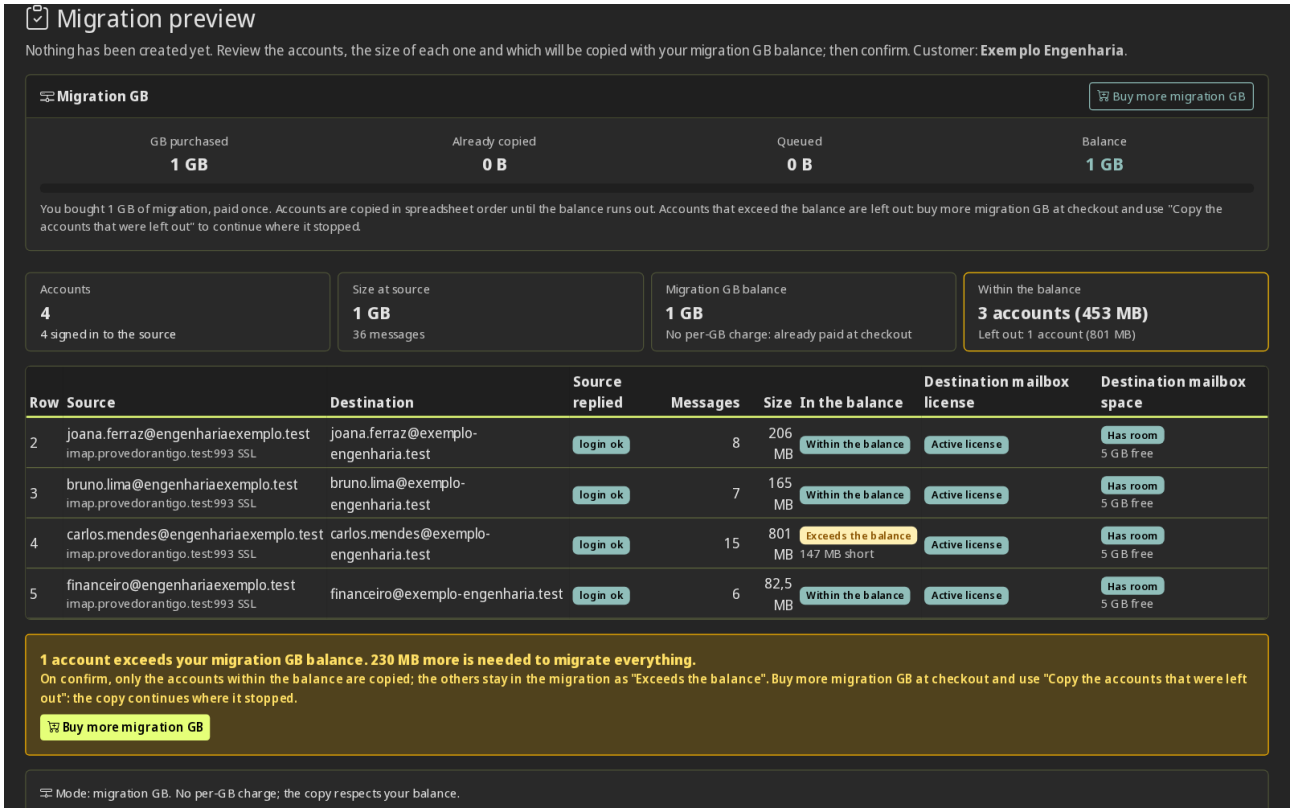


Figure 107: The preview, before confirming: the migration GB, what will be copied and what is left out (fictional data).

Following the copy

The task page refreshes by itself. The **What is happening now** panel shows, in real time, the copy events, the message and data bars per account, the current folder, the speed and the time left.

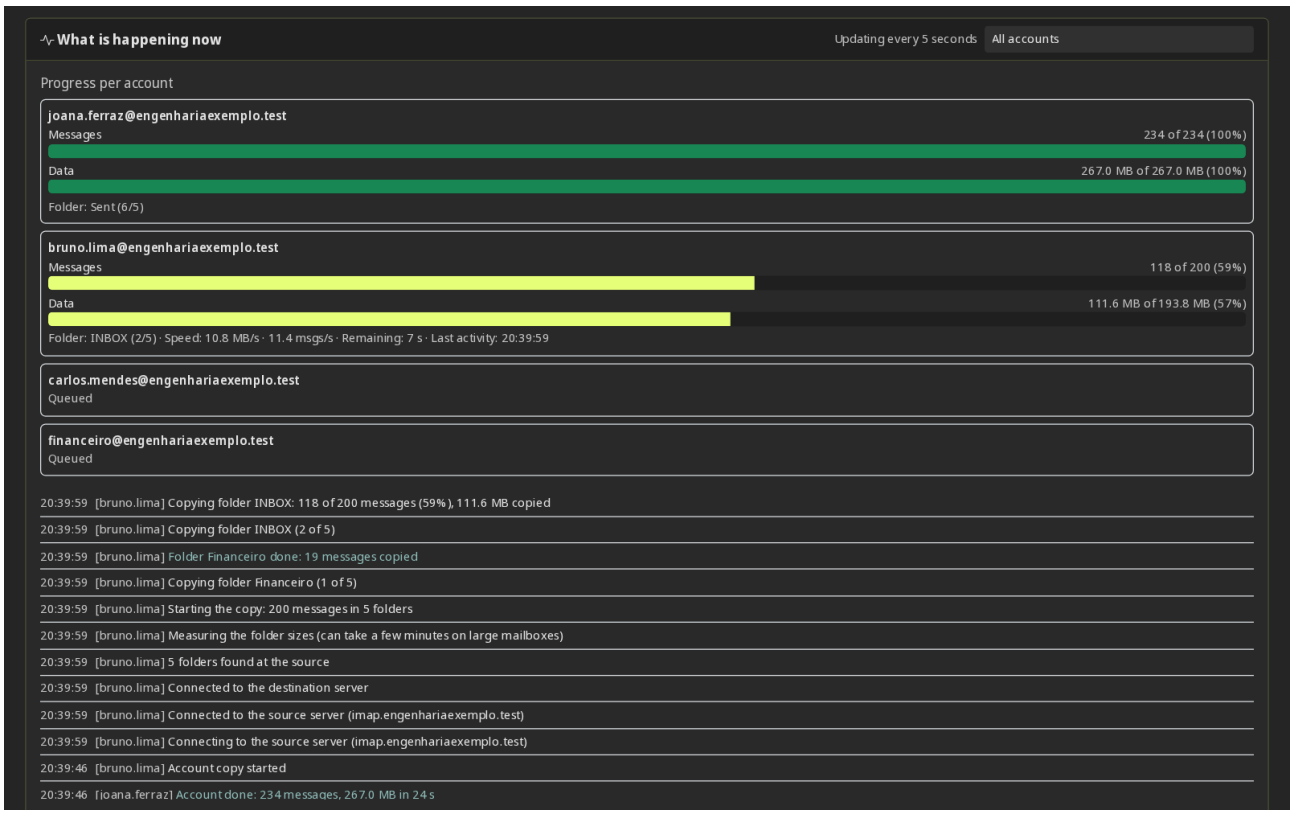


Figure 108: During the copy, the page updates by itself, account by account (sample data).

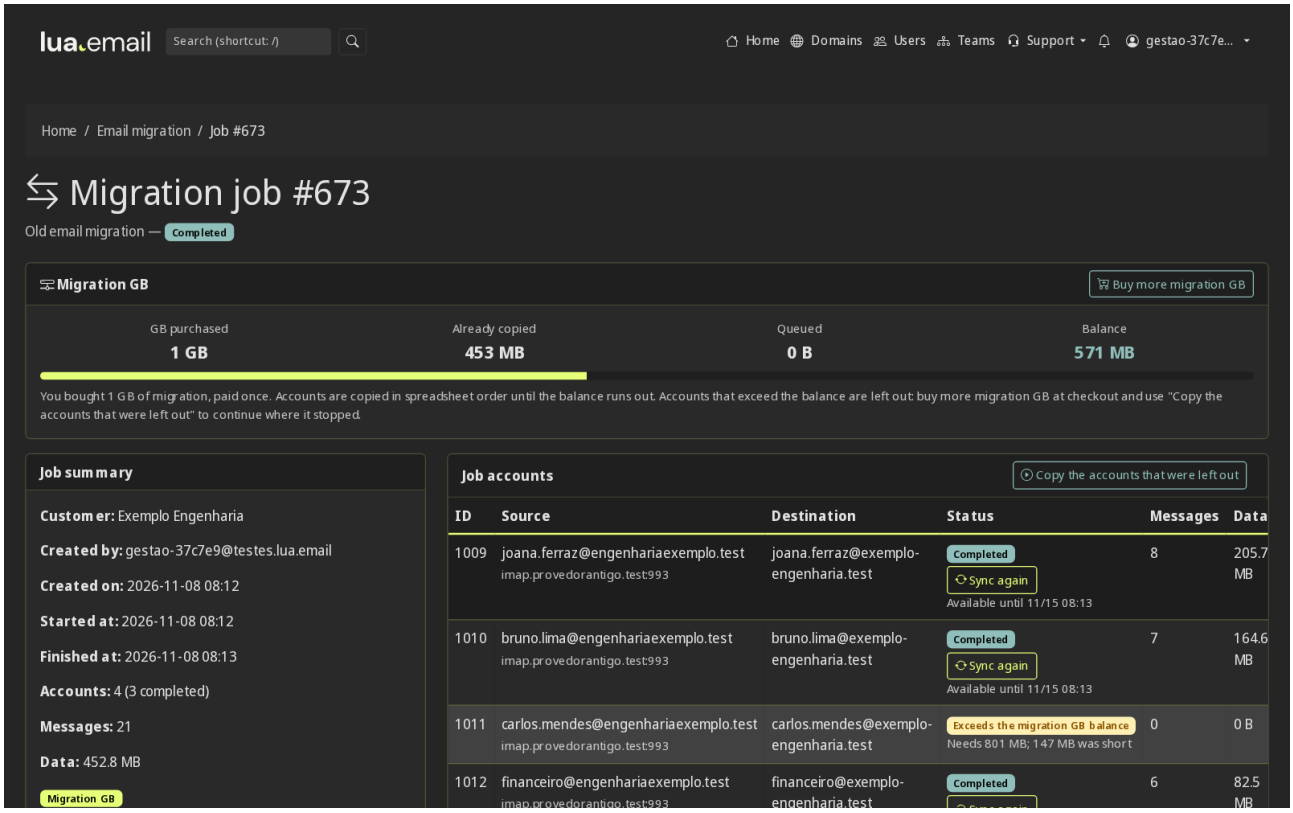


Figure 109: Migration finished: the balance went down, and the account that exceeded the balance waits for more migration GB (fictional data).

When an account fails

The reason appears on the account's row, such as "The source refused the login" (check the password or use the app password) or "Could not connect to the source server" (check address and port). After fixing it, click **Retry the failed accounts**: the copy continues where it stopped. The table of errors and fixes is in the tutorial.

On DNS switch day, sync again

Do the first copy ahead of time. On the day the domain moves to Lua, open the task and click **Sync again** on each finished account: only what arrived at the old provider after the last copy comes over now. What comes in is taken from the migration GB balance. The button stays available for 7 days after the first complete copy; after that, the screen explains and you just create a new task. Details in On MX switch day.

Migration GB: buy, balance and buy more

The migration GB are bought **before** migrating, at the lua.email checkout: R$ 2.00 per GB migrated from the source, **paid once**, no monthly fee and no renewal. They become a balance in the admin panel. Buying again **adds** to the balance.

- **Where to see the balance:** in the **Migration GB** box on the migration screen and, on **Home**, in the **Email migration** card, with the GB purchased, the GB already used, the balance and the link to the tool.
- **What uses the balance:** copying the accounts and **Sync again**. The balance belongs to the whole customer and does not renew on its own.
- **Short?** The accounts left out stay on record in the task, with nothing deleted. Buy more migration GB and click **Copy the accounts that were left out**: they go back into the queue and use the new balance. The old provider's password is kept for 7 days.

When to use it and use cases

- **Changing provider without losing history:** create the mailboxes, copy everything before the switch, change the MX and sync again on switch day.
- **Migration in stages:** start with one or two mailboxes, check the result and only then bring the rest.
- **The mailbox of someone who left the company:** copy the old account into the mailbox of whoever took over the work.
- **Merging accounts into one mailbox:** one row per old account, all with the same destination.
- **When to ask the Lua team:** Microsoft 365 and Outlook.com accounts, or volumes where you prefer our team to handle it.

Contacts and calendar do not come with the copy: import them as a file in webmail (see how).

17. Support tickets

Need help from the Lua team? Open a ticket right from the panel, under **Support → Tickets**. You describe the problem, attach a screenshot and follow the conversation on the same screen. The examples below are from a fictional company, Padaria Estrela Ltda.

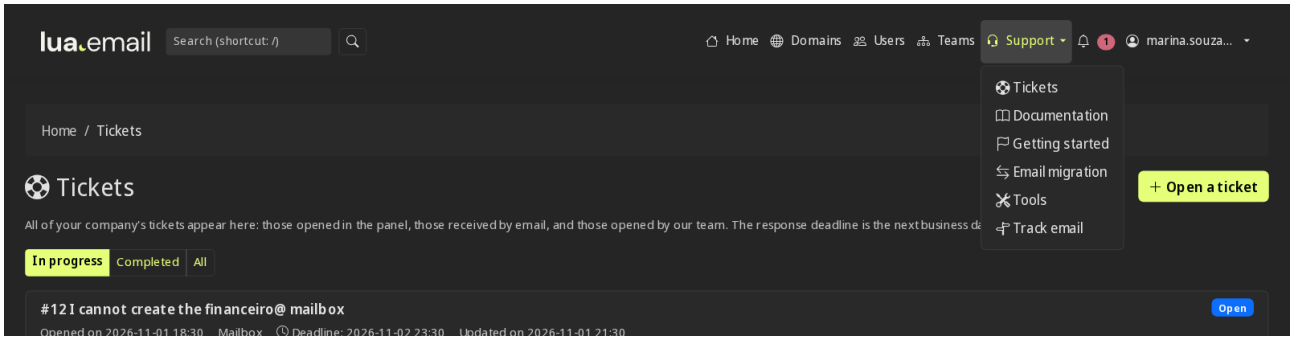


Figure 110: Support → Tickets is the first item in the menu. Real screen, sample data.

The ticket list

The list shows all of the company's tickets: the ones you opened in the panel, the ones that came in by email and the ones our team opened for you. Each row shows the number, the title, when it was opened, the assignee (once there is one) and the last update.

- **Filters:** *In progress* (the default), *Closed* and *All*. When there are many tickets, the **Older** button opens the next page.
- **Status:** the badge on the right of each ticket says, for example, *Open* or *Closed by customer*. Tickets that came in by email or that the team opened also show where they came from.

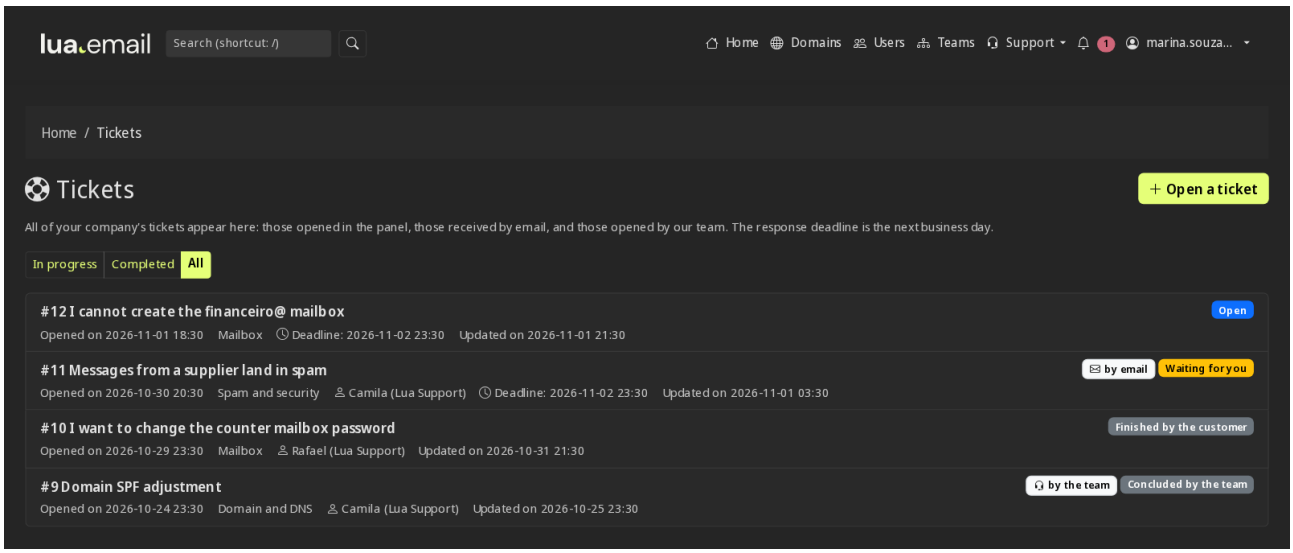


Figure 111: The list with the All filter: open tickets, tickets waiting for you and finished tickets, with the origin (panel, email or team). Real screen, sample data.

Opening a ticket

Click **Open a ticket** at the top of the list and fill in:

1. **Title:** a sentence that sums up the problem, for example "I can't create the account financeiro@".
2. **Category:** choose from the list (mailbox, sending and receiving, spam and security, domain and DNS, webmail and mobile, Colabora, migration, billing or other). The list comes from Lua's ticket system and may

change.

3 **What is happening?** tell us what happened, since when and what appears on the screen. The text box accepts basic formatting: the toolbar buttons (or the text `**bold**` and `*italic*`) mark highlights, lines starting with `-` or `1.` become lists and `http` addresses become links.

4 **Attachments:** click **Attach file**. You can attach up to 5 files per message, in these formats: image (PNG, JPG, GIF, WEBP), video (MP4, MOV, WEBM), PDF, TXT, DOC and DOCX. Each file can be up to 25 MB, and video up to 100 MB. Each one appears in the list with a "ready" notice when it finishes uploading, and you can take it out with **remove**.

5 Click **Open a ticket**. The panel shows the ticket number.

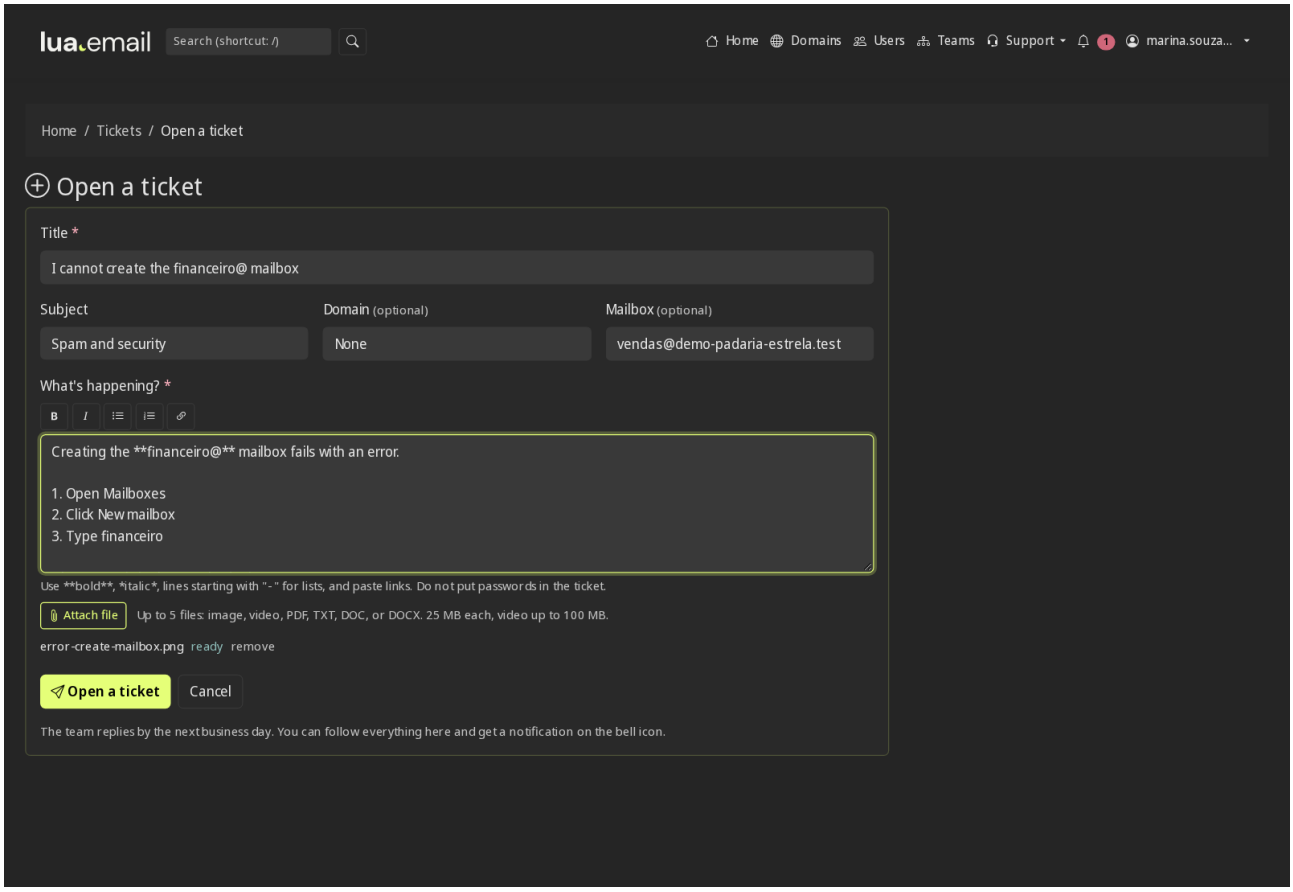


Figure 112: The opening form, with title, category, description and an attached screenshot. Real screen, sample data.

Careful: do not put passwords in the ticket. If the team needs to get into a mailbox, it uses webmail support access, which has a reason, an expiry and a log.

Following, replying and attaching

Click the ticket in the list to open the conversation. At the top are the title, the status, who opened it and when, the assignee (or "Waiting for an assignee"). Below come the ticket description and the messages, from oldest to newest. The description also appears on tickets that came in by email or that the team opened. Team replies appear with the support icon; yours appear with your username. Only public messages are part of the conversation.

To reply, write in the **Reply** field, attach files if you need to (the same rules as the opening form) and click **Send**. Images appear as thumbnails and open larger; videos play on the screen itself; PDF, TXT, DOC and DOCX appear as a download button.

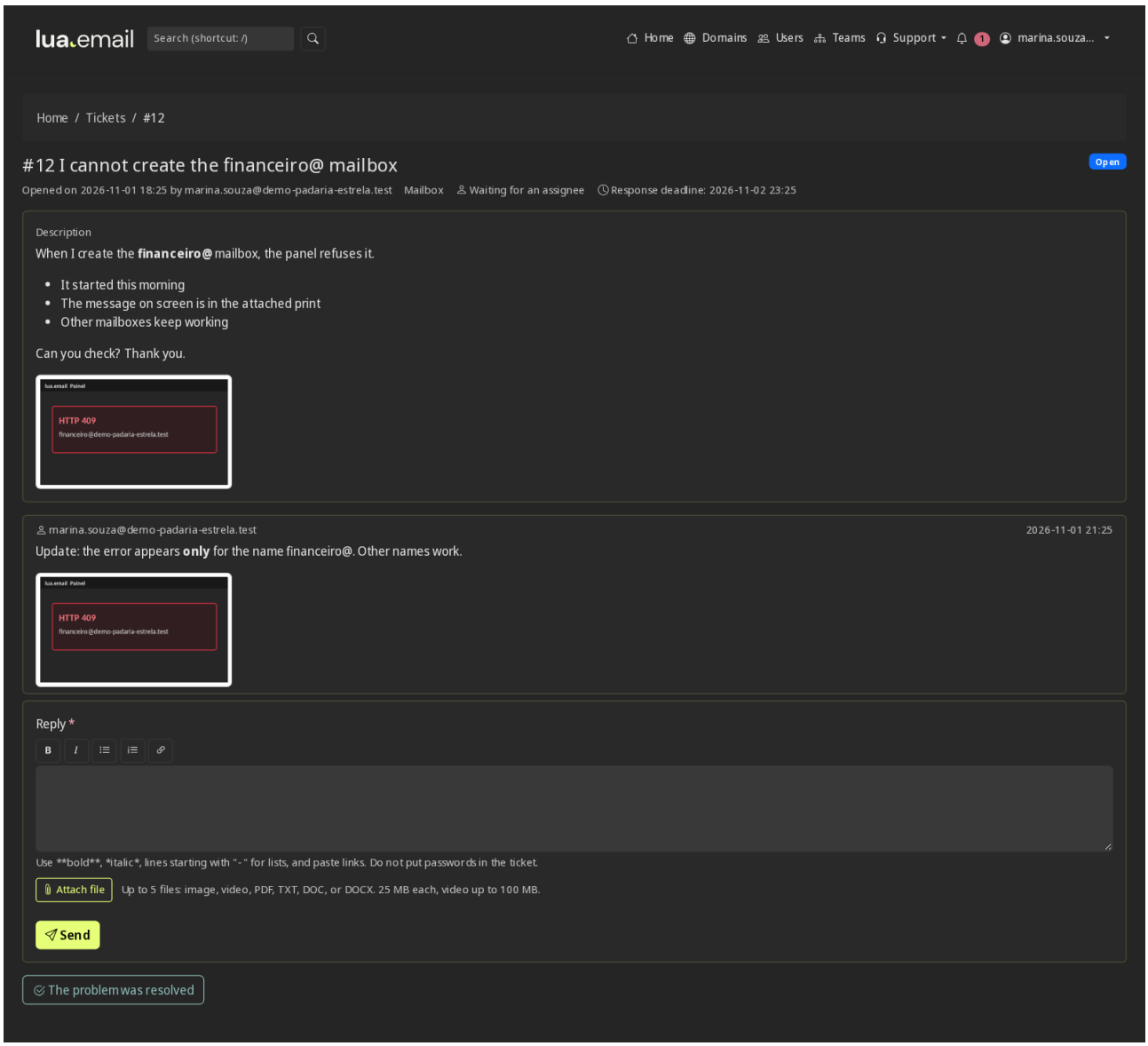


Figure 113: The open ticket: description, a reply with an attachment and the reply field. Real screen, sample data.

Closing, reopening and rating

Did you solve the problem yourself, or has the team already helped? Click **The problem was resolved**. The panel shows the field "Tell us what solved the problem (optional)", up to 500 characters. After **Close the ticket**, it moves to *Closed by the customer*.

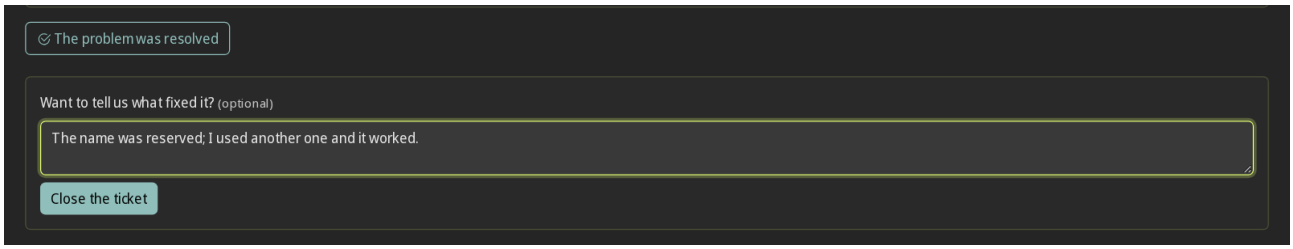


Figure 114: Closing the ticket, with the optional reason. Real screen, sample data.

On a closed ticket, the panel shows a green notice with who closed it and when.

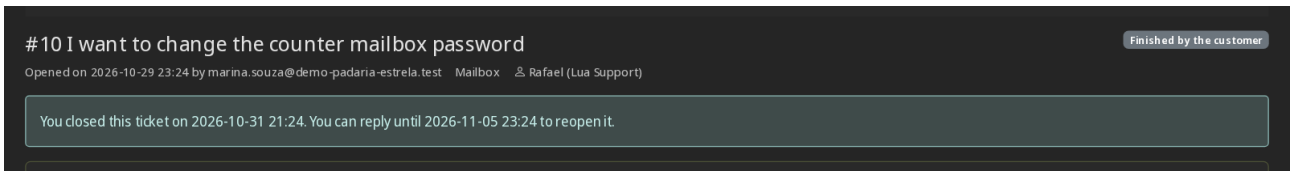


Figure 115: The notice on a closed ticket, with the deadline to reopen. Real screen, sample data.

- **Within the window:** did the problem come back? Reply in the **Reply and reopen** field, or click **Reopen**, explain why the problem was not solved (required field) and confirm with **Reopen the ticket**.
- **After the window:** the ticket can no longer be reopened. The button becomes **Open related ticket**: it opens the form already linked to the previous one, and the team sees the history.
- **Rating:** when the team is the one that completes the ticket, the panel shows the question "How was the service?", with a rating from 1 to 5 and an optional comment. After you send it, the screen shows your rating.

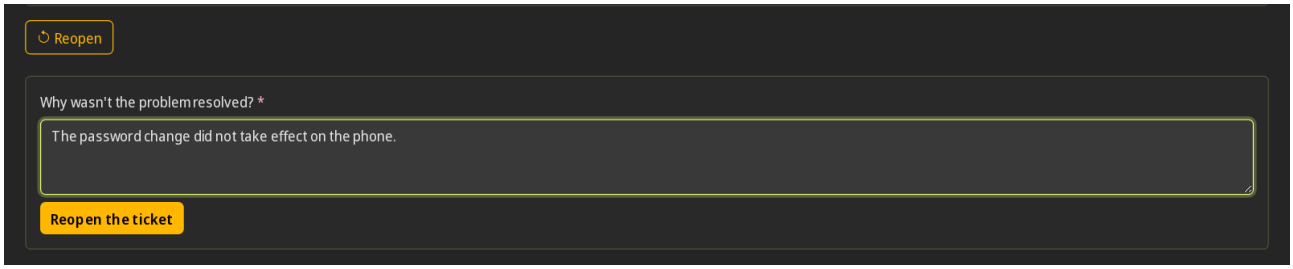


Figure 116: Reopening a ticket within the window, explaining the reason. Real screen, sample data.

Who can do what, and how you are notified

Who	What they do in Tickets
Administrator and Helpdesk	Open, reply to, attach files to, close, reopen and rate the company's tickets.
Read-only	Sees the list and the tickets, without the open button or the reply fields.
Anyone who manages more than one company	Picks the company at the top of the screen before viewing or opening tickets.

Each person only sees the tickets of the company they have access to. One company's tickets never appear for another. If your company is a Lua reseller and only follows the status of its customers' tickets, the screen shows the title, status, assignee and dates, and the ticket details stay with the reseller.

Notifications: when the team replies to, completes or changes the status of a ticket opened in the panel, the notification arrives in the **bell** at the top, for the person who opened it and for the other people in the company. Tickets that came in by email or that the team opened appear in the list as soon as you open the tickets screen.

18. Language, theme, and using it on your phone

Since version 1.3.29, each person chooses the language and theme of the panel. The choice applies only to your account, follows you in any browser, and changes nothing for the other users in the company. Anyone who doesn't choose keeps the panel in Brazilian Portuguese and the dark theme.

Choosing the language and theme

There are two ways, and both save the same preference.

1. Click your name in the top right corner and open **My profile**.
2. On the **Preferences** tab, choose the **Interface language** and the **Theme**.
3. Click **Save preferences**. The page reloads already in the language and theme you chose.

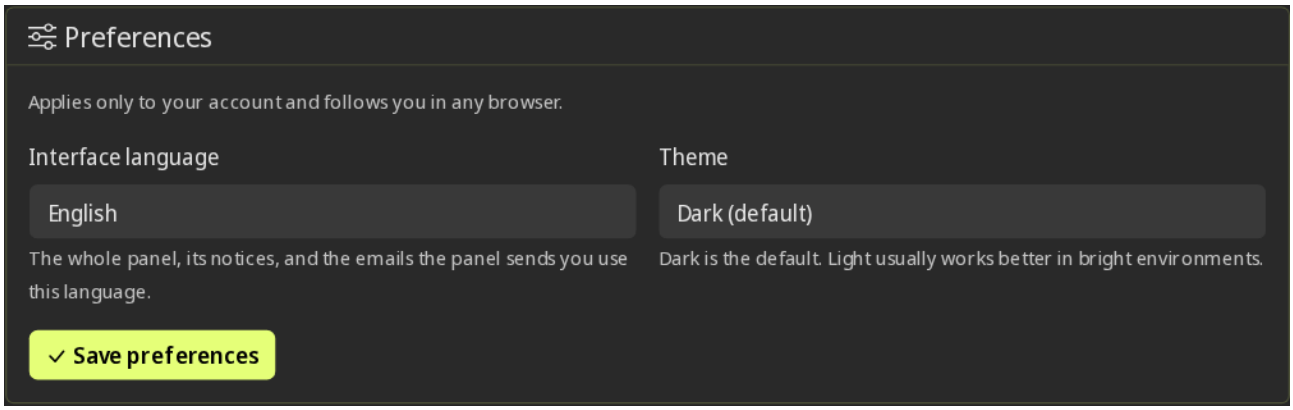


Figure 117: In My profile, the Preferences tab stores your account's language and theme (real screen, fictional data).

To switch without opening your profile, use the shortcut in the user menu: under **Interface language**, click **Português (Brasil)** or **English**, and under **Theme**, click **Dark** or **Light**. You return to the page you came from.

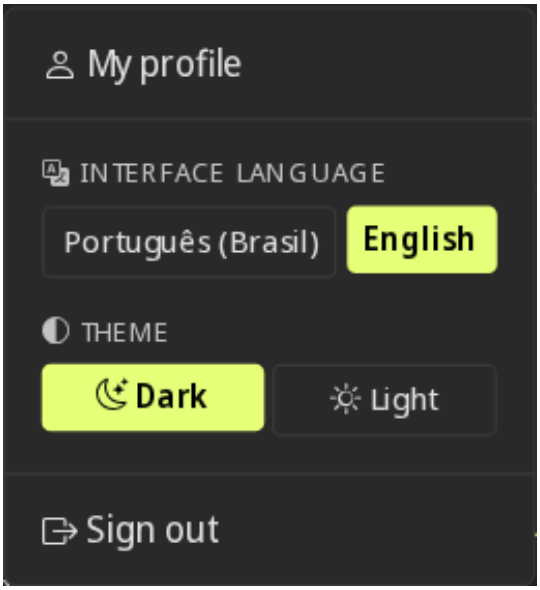


Figure 118: The language and theme shortcut in the user menu (real screen, fictional data).

Field	Options	What changes

Interface language	Português (Brasil), the default, or English.	The whole panel, the notices, and the emails the panel sends you. If a translation is missing, the text appears in Portuguese.
Theme	Dark (default) or Light.	The colors of the screens, modals, and charts. Light is usually better in bright environments.

The light theme has the same content and the same buttons as the dark one. The logo is white, so the header stays dark in both themes. The sign-in page opens in the language and theme of the last visit in that browser.

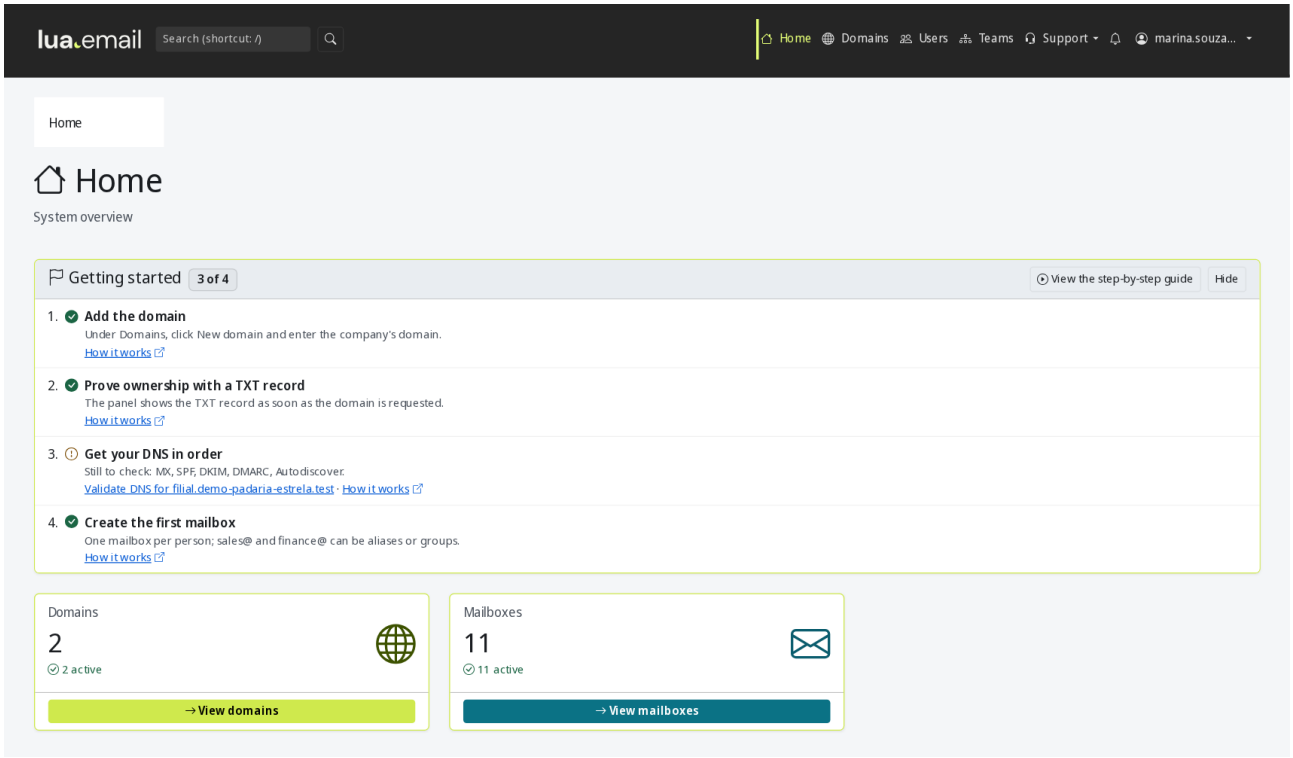


Figure 119: The Home page in the light theme. The header stays dark in both themes (real screen, fictional data).

> **Tip:** the screenshots in this manual use the dark theme, the default. If you use the light one, the screens have the same layout and the same names.

Using the panel on your phone

The panel works on small screens. Below 768 px wide:

- **Domain tabs:** sit in a row that scrolls sideways. The faded edge tells you there are more tabs, and the active tab is scrolled into view when the page opens.
- **Tables:** users, companies, teams, sessions, logs, migrations, domain licenses, alias domains, and the superadministrator screens turn into **cards**. Each card shows the same fields as the row, plus the actions (Edit, Remove, and the rest).
- **Menu:** the three-line button at the top opens the menu, with the language and theme shortcut.

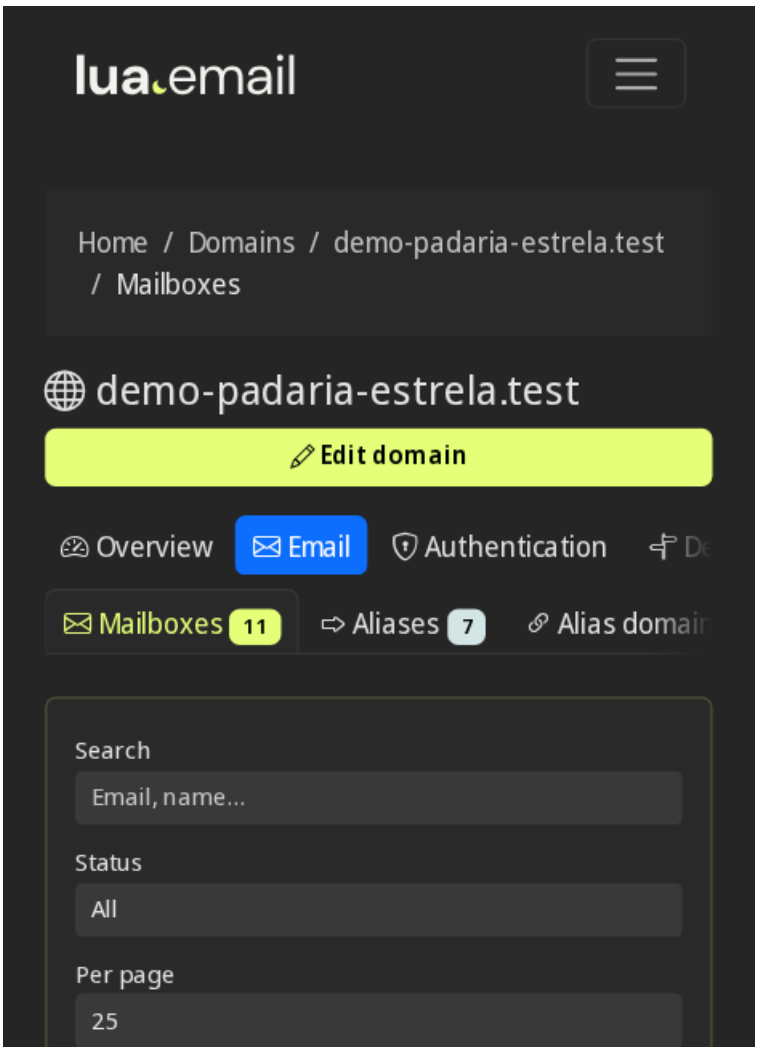


Figure 120: On a phone, the domain tabs scroll sideways and the active tab stays in view (real screen, 375 px wide, fictional data).

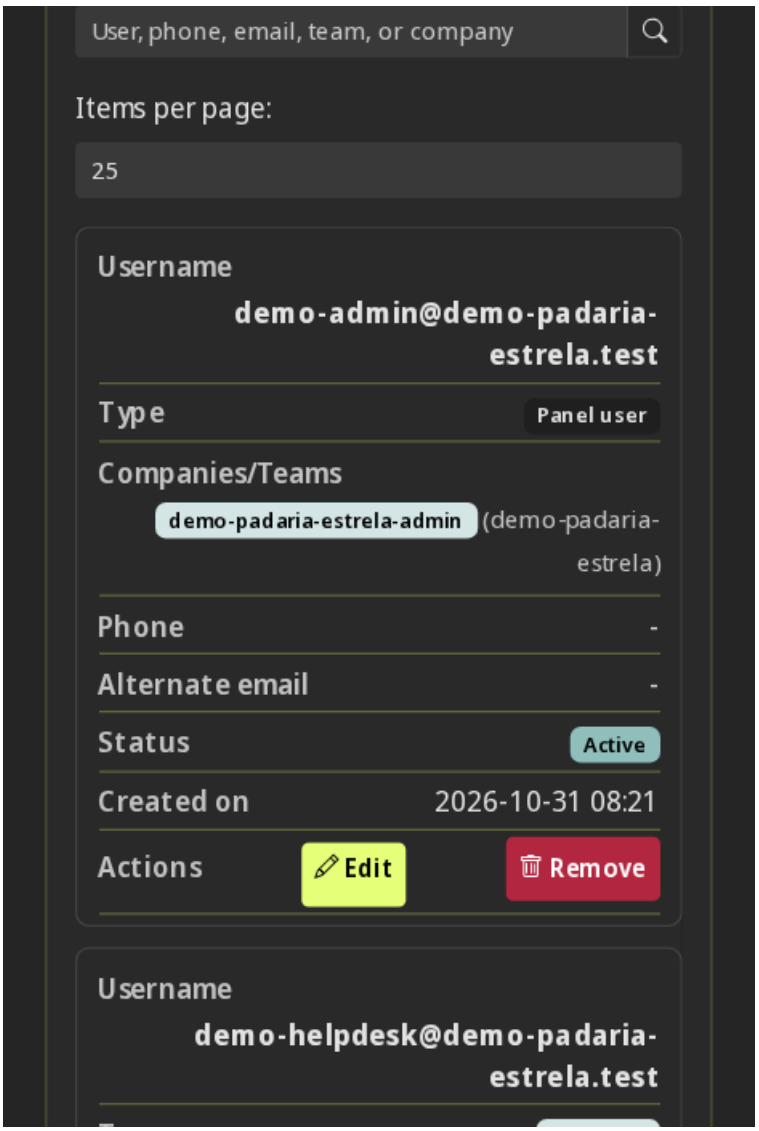


Figure 121: On a phone, wide tables turn into cards, each with its own actions (real screen, 375 px wide, fictional data).

The notice about the IP list

On the **Access location (IP)** and **Protocols** tabs of a service group, the panel shows a notice to avoid a false sense of security:

- **Access location (IP):** the **Important** notice says the address list does not apply to email and calendar apps. Anyone who uses Outlook, Thunderbird, or the phone's email app with the app password can still sign in from anywhere, even outside the list. To prevent that, the notice points to the **Protocols** tab and the **Do not allow protocols (webmail only)** option.
- **When webmail only is already on:** the notice says the email and calendar apps are turned off for the group, so nobody can get around the list through them.
- **What the list also covers:** the Colabora app password (the Drive sync on your computer) follows the list: outside the allowed IPs, the Drive on your computer and apps that use an app password stop syncing. Outlook, Thunderbird and the phone email app stay outside the list and are turned off with webmail only. `dav.lua.email` also stays outside the list.
- **Protocols tab:** the same explanation appears there, with what keeps working and follows the group's list: webmail, Colabora, Chat, and the phone with an Exchange account.

The step-by-step for the IP list and webmail only is in chapter 9.

19. Common problems

"The TXT record has not appeared in the domain's DNS yet"

Check that the record name is right. In many DNS panels the name is just `_lua-admin-verify`, without the domain at the end; with the domain, some panels create `_lua-admin-verify.yourdomain.yourdomain`. Copy the entire value, with no spaces. After saving, wait a few minutes: the check continues on its own.

The mailbox shows "No license" or there are no licenses available

When every license in the plan is already in use, the panel warns: "You have no licenses available. New mailboxes only work after you purchase and assign a license." The new mailbox is created with the **No license** status and stays deactivated: it neither sends nor receives email. To fix this, buy licenses with the **Purchase licenses** or **Purchase more licenses** button (if you buy through our team, with the **Contact us to sign up for more licenses** button). The step by step for buying is in Subscribe to more mailboxes and add-ons. After payment, click **Assign license** on the mailbox, choose the license and click **Assign and activate** (see Mailboxes without a license). Buying the license does not activate the mailbox. You can also free up a license by removing a mailbox that is no longer used (the Domain health page shows idle mailboxes). The same applies to add-on licenses: with no license left, the mailbox brand option stays disabled with the link to buy.

Someone writing to an alias gets "user does not exist"

One of the alias destinations no longer exists or is disabled. See chapter 7.

The panel rejects the address or the group name

Mailboxes, aliases and service groups cannot have names that can be confused with each other. The panel rejects:

- a mailbox or alias that starts with `grp-` (reserved prefix);
- a mailbox or alias with a group's email address or the name of a domain group, regardless of case or accents ("Área" blocks `area@`);
- a group whose name matches the address of a mailbox or alias;
- a group email with the address of a mailbox or alias that already exists.

Choose another name or rename the existing one. The panel's message tells you what it conflicts with.

"They sent me an email and it didn't arrive"

Ask for the sender's address and the approximate time, and search the tracking by sender. If the message shows as delivered, look in the mailbox (including Spam and filter folders). If it shows as rejected, the reason is on the row. If it does not appear, it never reached Lua: the problem is on the sender's side, and the tools help show what is missing in their DNS.

The person can't sign in

Check Failed logins to see whether "wrong password" appears (change the password on the mailbox page) and check whether the mailbox is in a group with access hours. In Outlook and on the phone, remember that the password is the app password, not the webmail one.

Still need help?

Contact support. A person on Lua support answers, based in Brazil, in Portuguese.

Talk to support: WhatsApp (47) 99276-7511 **Write to us**: suporte@lua.email **Other ways to get help**: Support page

To speed things up, send the domain, the mailbox or alias involved, what you were doing and, if you can, a screenshot of the panel screen.