S/MIME Gateway for Postfix · Version 1.5.8

Setting up and running the S/MIME Gateway

Guide for administrators

Who is this guide for?

For the person who looks after the gateway in your company. You do not need any prior knowledge of encryption. For the first installation on the server (chapter 19) your IT service provider is the best help – everything else is done comfortably in your web browser.

How to read the pictures: 1 Red circles with numbers show **where** to click or type. The number in the picture belongs to the step with the same number in the text.

The pictures show a made-up example company (“Example Company Ltd”). On your screen you will see your own names and addresses.

© 2026 Michael Harperscheidt. All rights reserved. · S/MIME Gateway for Postfix 1.5.8 · Administrator guide

Contents

1 What does the gateway do – and what is your job?

2 Signing in

3 The overview and the menu

4 First steps – your checklist

5 Setting up the mail server

6 Creating accounts for your colleagues

7 Creating mailboxes and aliases NEW

8 Deleting mailboxes and aliases NEW

9 Your own certificate authority and IDs

10 S/MIME settings

11 Reminders and info mails

12 DKIM – the authenticity stamp for your domain

13 Mail DNS – checking SPF, DMARC, MTA-STS and co. NEW

14 Statistics and daily report

15 Alias addresses

16 Two-factor sign-in (MFA) NEW

17 The license

18 When the license is no longer enough

19 Installing and updating

20 When something does not work

21 Small glossary

Copyright and license

1 What does the gateway do – and what is your job?

The gateway sits on your company's mail server, like a mail room. Every email passes through it.



Outgoing emails

are digitally signed and – if the recipient is known – sealed (encrypted).



Incoming emails

are opened (decrypted) on request. The senders' IDs are collected.



DKIM

Every email of your domain gets an authenticity stamp. This keeps it out of the spam folder.

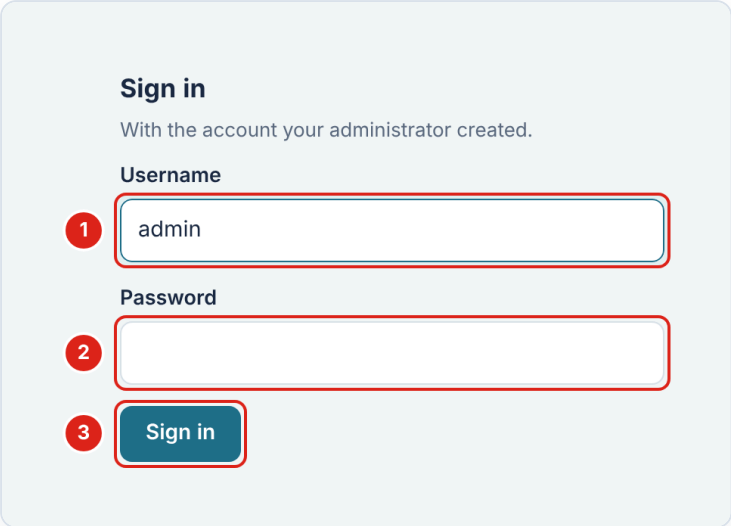
Your colleagues hardly notice anything: they keep writing in their usual email program. Your tasks as an administrator are:

- set up the gateway once (chapter 4),
- create accounts and mailboxes, issue IDs – and delete mailboxes that are no longer needed (chapter 6 to chapter 9),
- now and then look at the overview, the info mails and the daily report (chapter 3, chapter 11 and chapter 14),
- take care of the license (chapter 17 and chapter 18).

> **Two kinds of people**
>
> **Administrators** see and change everything. **Users** only see their own mailboxes. There is a separate, simple guide for users – give it to your colleagues.

2 Signing in

Open the gateway's address in your web browser (for example `https://mail.example-company.com/smime`).

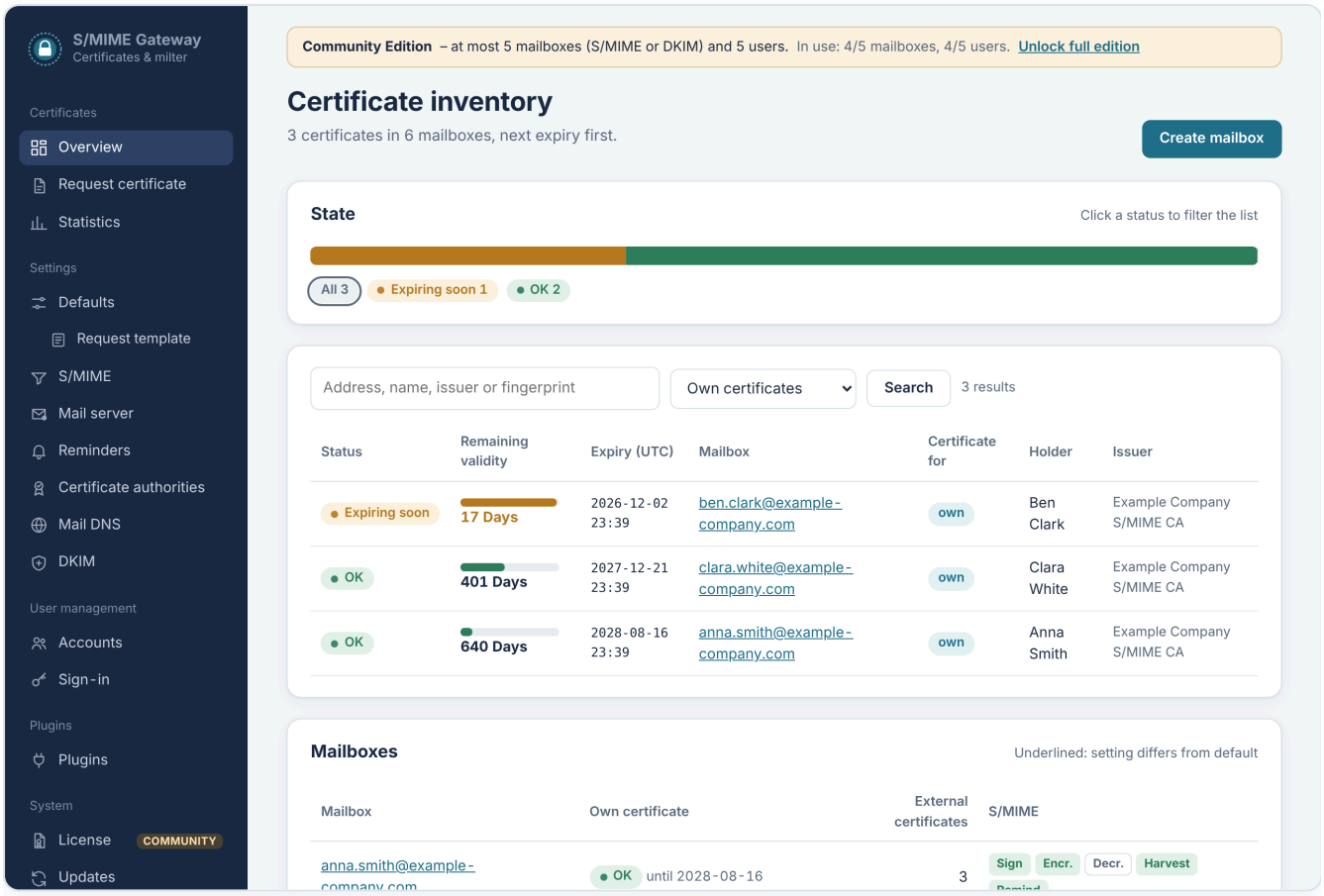


Signing in as administrator

1. Enter the username, for example **admin**.
2. Enter the password.
3. Click **“Sign in”**.

> **The emergency access**
>
> The configuration file on the server contains an emergency access (settings `admin_user` and `admin_password_hash`). It always works – even if you have otherwise locked yourself out. Keep this password safe, for example in a sealed envelope in the safe.

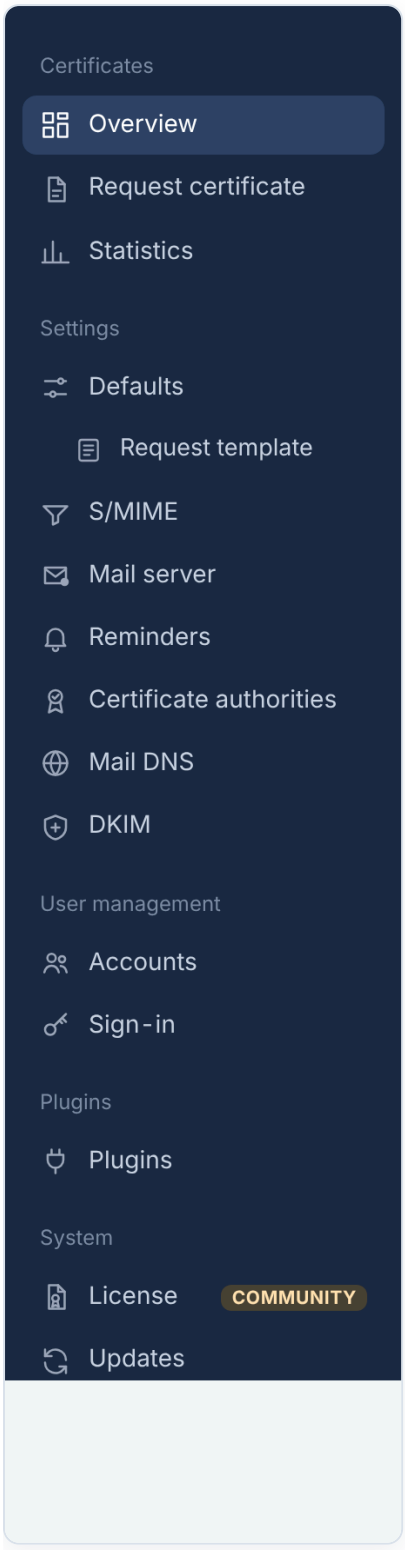
3 The overview and the menu



The overview after signing in

The overview shows all IDs of all mailboxes. The coloured marks mean: ● **OK** all good, ● **Expiring soon** renew soon, ● **Expired** act now. Clicking a colour shows only those entries.

Further down is the list of **Mailboxes**. Aliases are listed directly below their mailbox and indented (↳) NEW in 1.5.5 – so you can see at a glance which addresses belong together. This applies to every list of mailboxes, including the accounts, the statistics, the license page and the daily report. At the top is the yellow “Community Edition” bar: you are using the free edition (more in chapter 17).



The menu on the left

Menu item	What for?
Overview	all IDs and mailboxes at a glance, create a new mailbox
Request certificate	request an ID for a mailbox
Statistics	numbers and charts, daily report
Defaults	basic settings for all mailboxes
S/MIME	rules for signing and sealing
Mail server	sender for the gateway's emails
Reminders	mails before IDs expire, info mails about mailboxes
Certificate authorities	your own “ID office”
DKIM	authenticity stamp for your domain
MFA settings	two-factor sign-in (only with the MFA plugin active)
Accounts	who may sign in, alias addresses
License	edition, limits, license file

4 First steps – your checklist

After the installation, go through these points once, in this order. Tick off what is done:

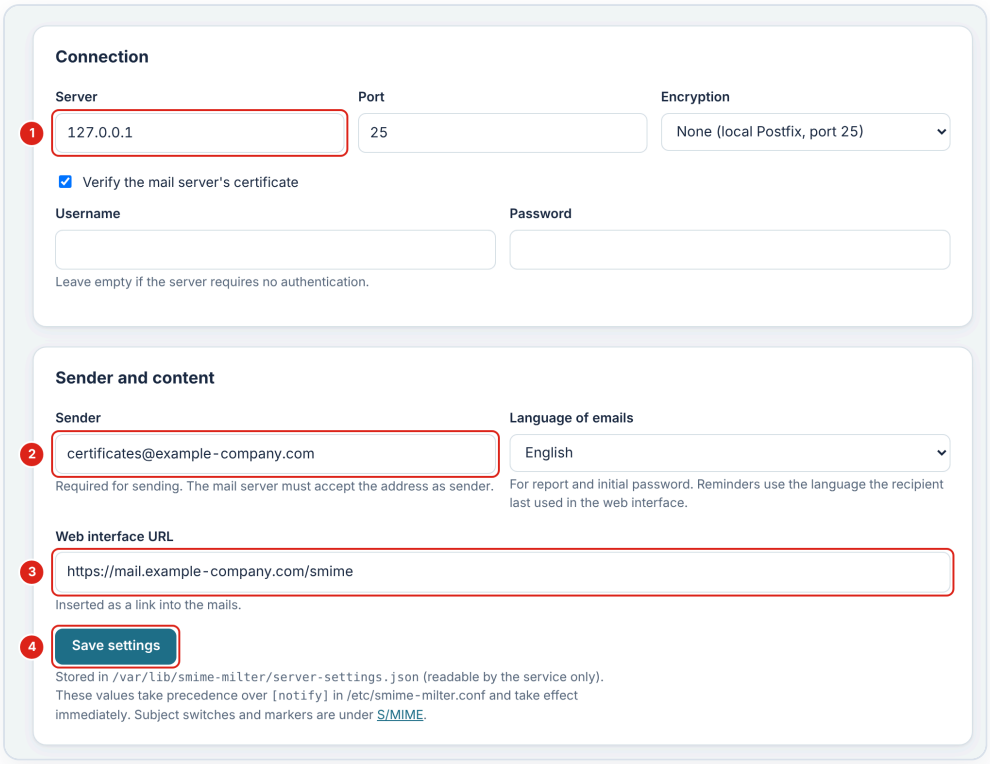
✓	What	Where	Chapter
☐	Enter sender address and web address, send a test mail	Mail server	5
☐	Enter your email domain(s)	S/MIME	10
☐	Create your own certificate authority	Certificate authorities	9
☐	Create accounts for colleagues	Accounts	6
☐	Create further mailboxes and aliases (for example `info@`)	Overview	7
☐	Switch on reminders, check the recipients of the info mails	Reminders	11
☐	Generate DKIM keys and add them to DNS	DKIM	12
☐	Switch on the daily report	Statistics	14
☐	Recommended: switch on two-factor sign-in	Plugins › MFA	16
☐	More than 5 mailboxes: request a license	License	17

Do not be afraid of mistakes

All settings can be changed again at any time. After every save a green message appears at the top. Only deleting a mailbox (chapter 8) is final – that is why the gateway asks twice.

5 Setting up the mail server

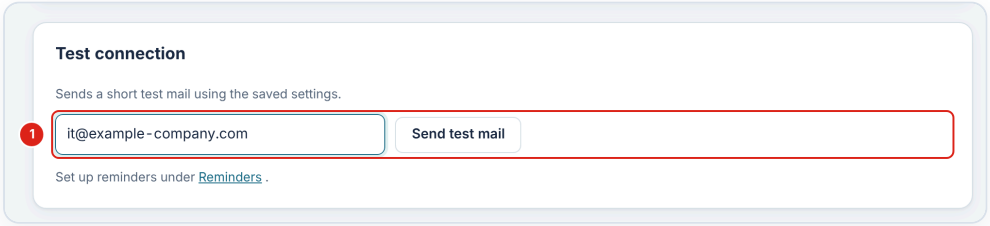
So that the gateway can send emails (credentials, reminders, info mails, reports), it needs a sender. Click **“Mail server”** in the menu.



The “Mail server” page

1. **Server**: the mail server used for sending. If the gateway runs on the mail server itself, leave `127.0.0.1`.
2. **Sender**: the address the emails come from, for example `certificates@example-company.com`.
3. **Web interface address**: the address at which your colleagues open the gateway. It appears as a button in the emails.
4. Click **“Save settings”**.

Sending a test mail

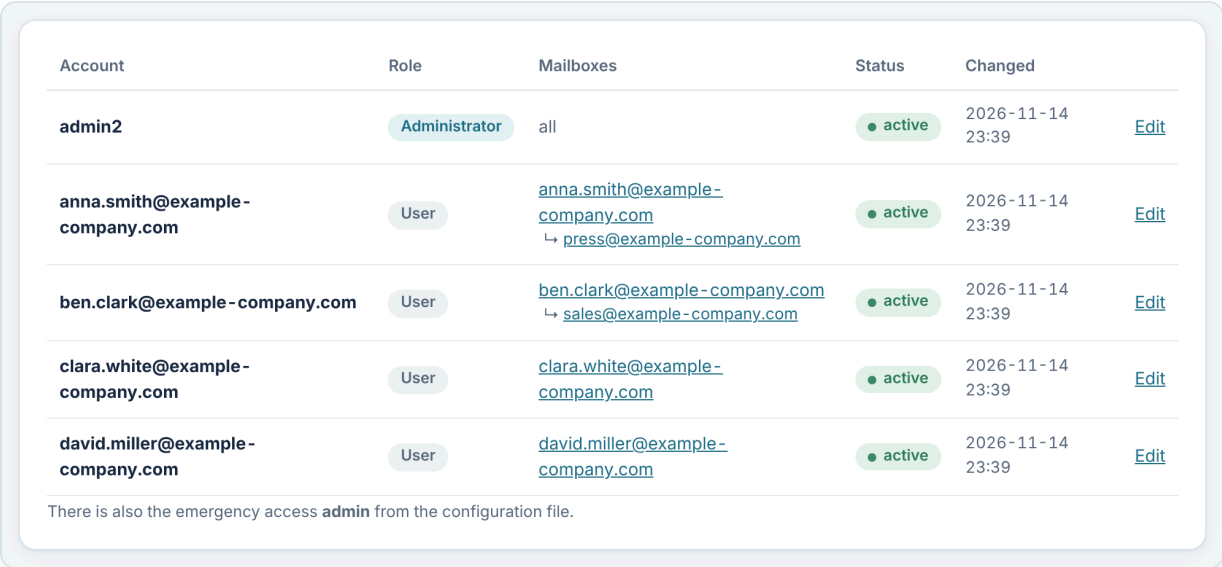


Sending a test mail

1. Enter your own address and click **“Send test mail”**. If the email arrives, everything is right.

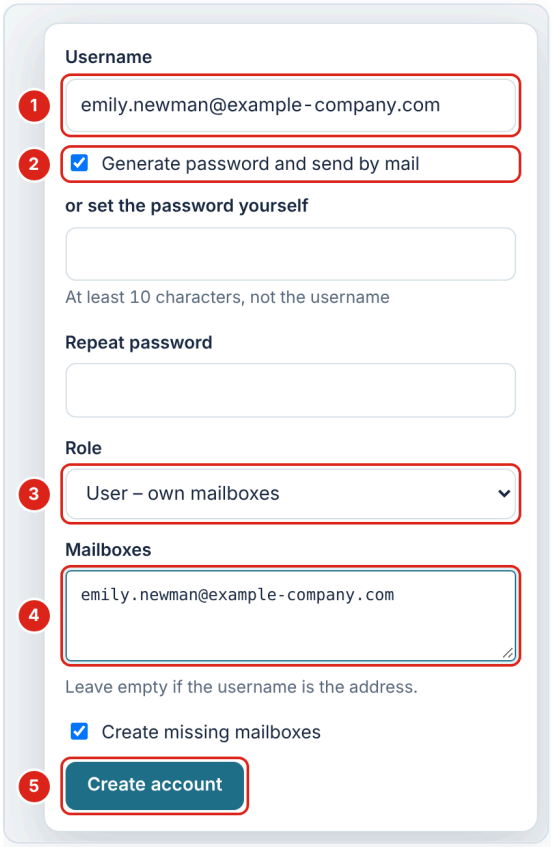
6 Creating accounts for your colleagues

Click **“Accounts”** in the menu. You see everyone who may sign in.



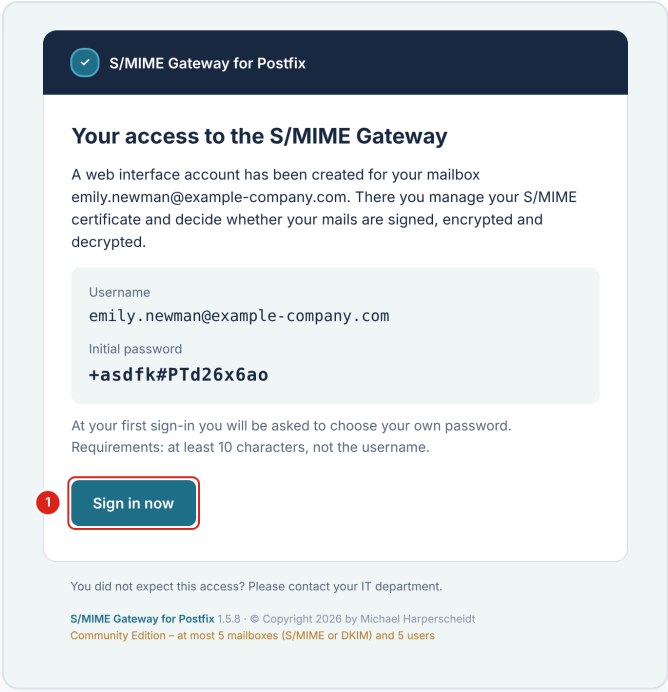
The list of accounts

Click **“Create account”** at the top right. A small window opens:



Creating a new account

1. **Username**: ideally your colleague's email address, for example *emily.newman@example-company.com*.
2. Leave **“Generate password and send by mail”** ticked. Your colleague then receives an email with their first password – you do not have to make one up.
3. **Role**: “User – own mailboxes” for normal colleagues. “Administrator – everything” only for people who should manage everything.
4. **Mailboxes**: which email addresses your colleague may manage. Leave empty if the username already is the address.
5. Click **“Create account”**. Done – your colleague gets the email right away.



The email your colleague receives

Forgotten password?

Click **“Edit”** next to the account in the list. There you can send a new password by email, lock the account or change the role.

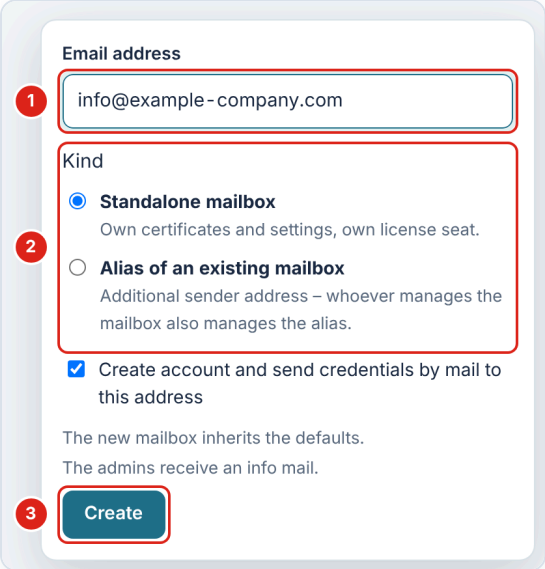
Limit of the free edition

In the Community Edition at most **5 users** may sign in. One administrator account (the oldest) and the emergency access do not count. Further administrator accounts do count.

7 Creating mailboxes and aliases NEW in 1.5.3

A **mailbox** is an email address with its own IDs and settings. An **alias** is an additional sender address that belongs to a mailbox – for example `info@example-company.com`, which Anna looks after as well. Whoever manages the mailbox also manages the alias.

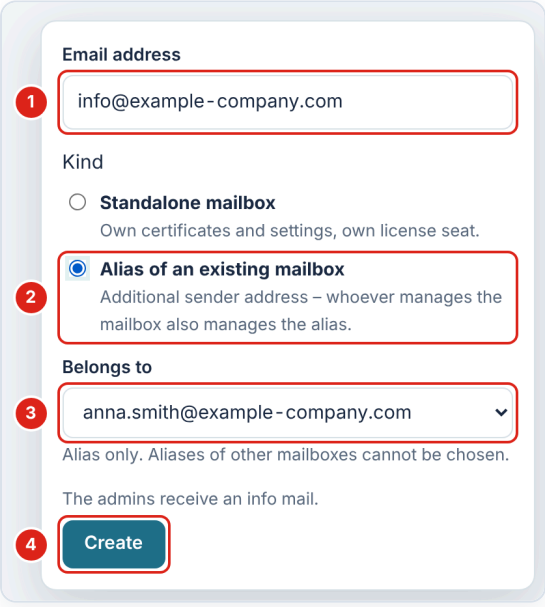
In the **“Overview”**, click **“Create mailbox”** at the top right. The gateway now asks what the address should become:



Creating a standalone mailbox

Standalone mailbox

1. Enter the **email address**.
2. Under **Kind** choose “Standalone mailbox”. The mailbox gets its own IDs, its own settings and takes its own license seat. With the tick box below you also create an account and send the credentials to this address.
3. Click **“Create”**.



Creating an address as an alias

Alias of an existing mailbox

1. Enter the alias' **email address**, for example `info@example-company.com`.
2. Choose “Alias of an existing mailbox”.
3. Under **Belongs to** select the mailbox the alias belongs to. The list only shows real mailboxes – an alias cannot belong to another alias.
4. Click **“Create”**.

What the gateway checks

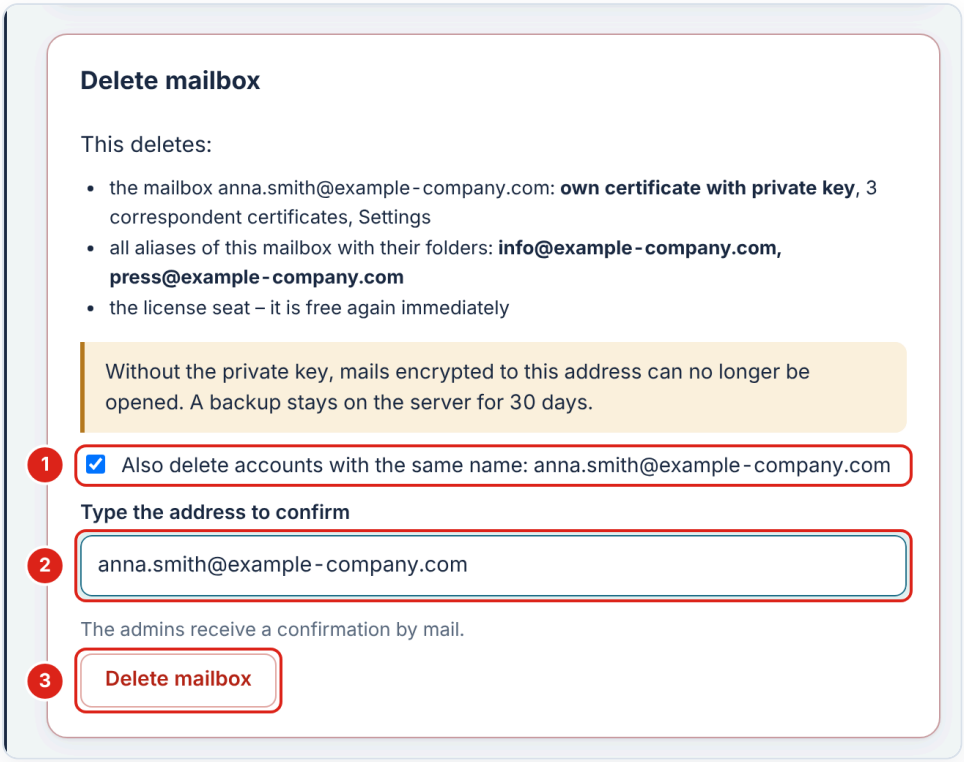
The address must belong to your domains. If the address already has aliases of its own or already is an alias of another mailbox, the gateway refuses and tells you why. If the address already has its own ID or its own account, you get a note – both are kept.

You receive an info mail

For **every** new mailbox and alias the gateway sends you a short info mail – even when it learns an address by itself during normal operation (for example because a signed email to a new address arrives). So you always know what has been added. More in chapter 11.

8 Deleting mailboxes and aliases NEW in 1.5.3

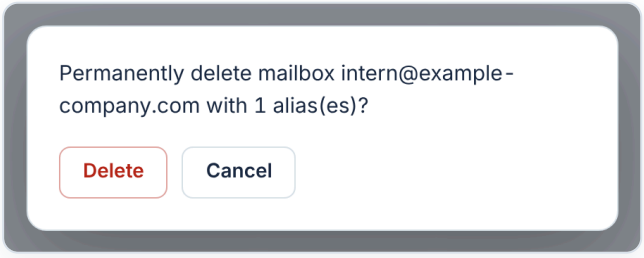
A mailbox is no longer needed, for example because a colleague has left the company? Then delete it. Open the mailbox (click its address in the overview) and scroll all the way down to the red box **“Delete mailbox”**. For an alias it is called **“Delete alias”**.



At the bottom of the mailbox page

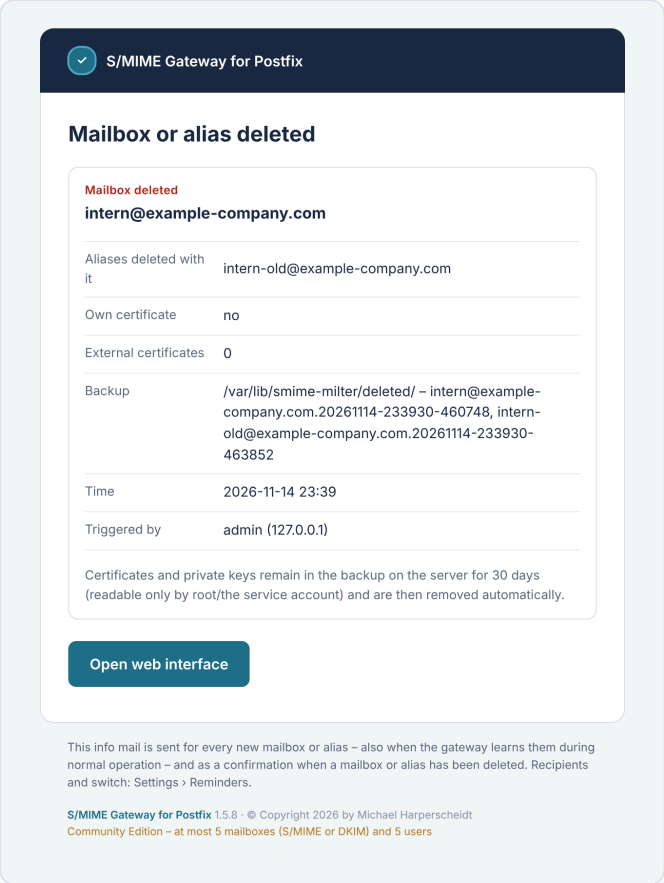
The top of the box lists everything that will be deleted: the ID with its secret key, the collected IDs of contacts, the settings – and **all aliases** of the mailbox. If the mailbox is listed in other accounts, it is only removed there; those accounts stay.

1. **Also delete accounts with the same name**: if there is an account with exactly this address as username, it is deleted too. Your own account and the last administrator account are never deleted.
2. For safety, type the **address** exactly.
3. Click **“Delete mailbox”** and confirm the question with **“Delete”**.



The question before deleting

Afterwards the license seat is free again immediately, and you receive a **confirmation by email**:



The confirmation: what was deleted, when and by whom

A backup for 30 days

Without the secret key, old sealed emails to this address can no longer be opened. That is why the gateway keeps the mailbox folder in a backup on the server for another **30 days** (`/var/lib/smime-milter/deleted/`, readable only by the service account). After that it is removed automatically. If you need something back during that time, ask your IT service provider.

Only detach an alias, do not delete it

Under **“Accounts”** › **“Alias addresses”** every alias also has **“Delete”**. That only removes the assignment; the folder and IDs of the address are kept. You receive a confirmation for this as well.

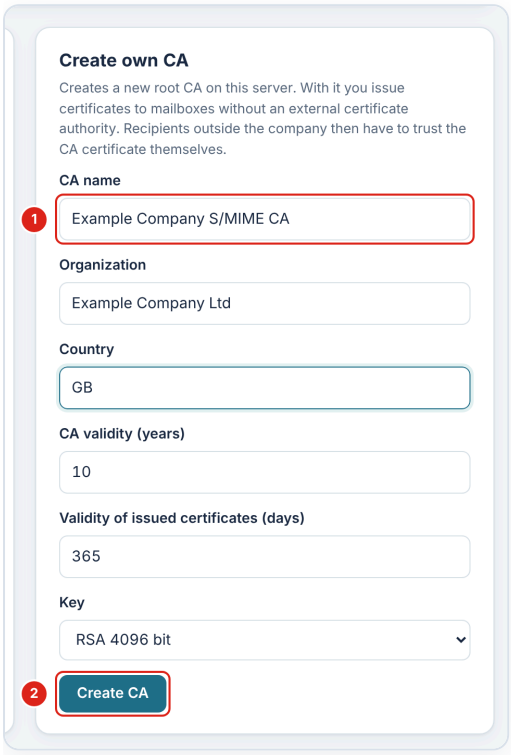
Will the mailbox come back?

If a signed email to the deleted address arrives later, the gateway creates it again (empty) – and sends you an info mail. So it is best to reject unknown addresses in the mail server.

9 Your own certificate authority and IDs

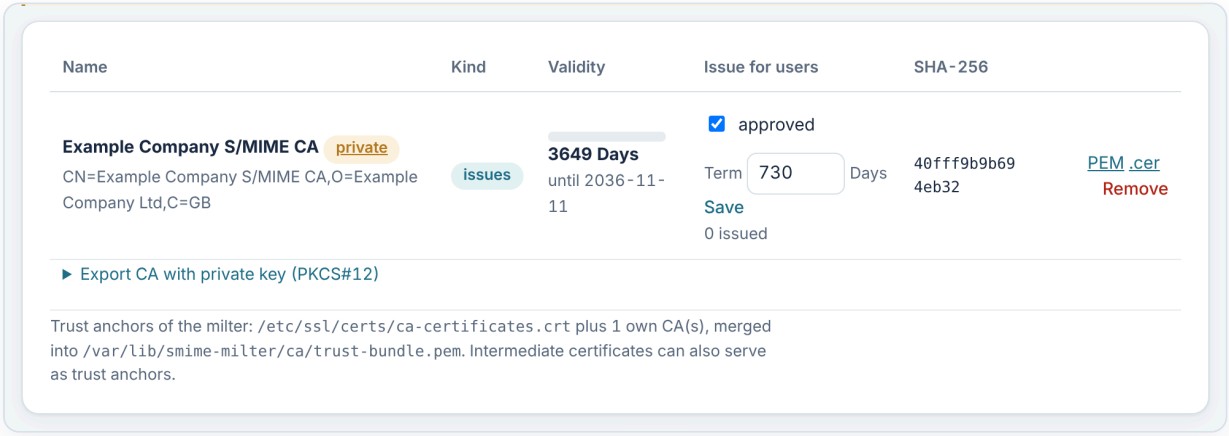
A **certificate authority (CA)** is like an ID office. With your own CA the gateway issues IDs to your colleagues itself – immediately and free of charge. (Alternatively you can buy IDs from a public provider; other companies recognise those without any extra step.)

Click **“Certificate authorities”** in the menu.



Creating your own CA

1. Enter a name under **CA name**, for example *Example Company S/MIME CA*, and fill in **Organization** and **Country**. The other fields can stay as they are.
2. Click **“Create CA”**.



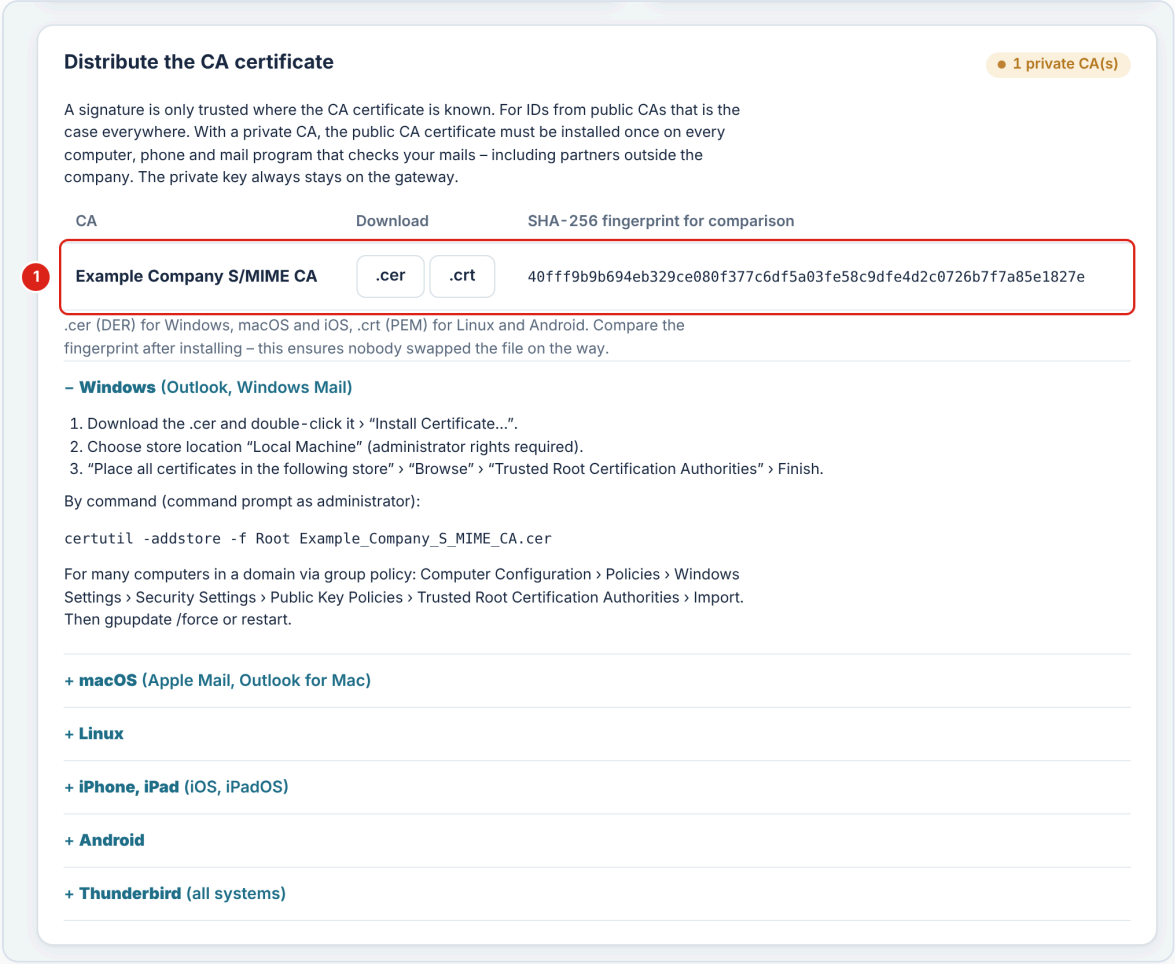
The new CA in the list. “approved” means: users may issue IDs to themselves with it, too.

Giving a colleague an ID

Open the mailbox (from the overview or via **“Request certificate”** in the menu) and proceed exactly as in the user guide, chapter 8: enter the name, choose your own CA under “Issue by”, **“Create request”**.

Distributing the CA certificate NEW in 1.5.6

Your own CA is a **private CA**: no computer or phone knows it out of the box. Until the CA certificate is installed there, Outlook, Apple Mail, Thunderbird and others show your colleagues' signatures as “not trusted”. The gateway marks private CAs as **private** in the list and reminds you at the top of the page until you have done it.



The “Distribute the CA certificate” section with instructions per system

1. Download the CA certificate: **.cer** for Windows, macOS, iPhone and iPad, **.crt** for Linux and Android. It contains no secret key and may be shared freely.

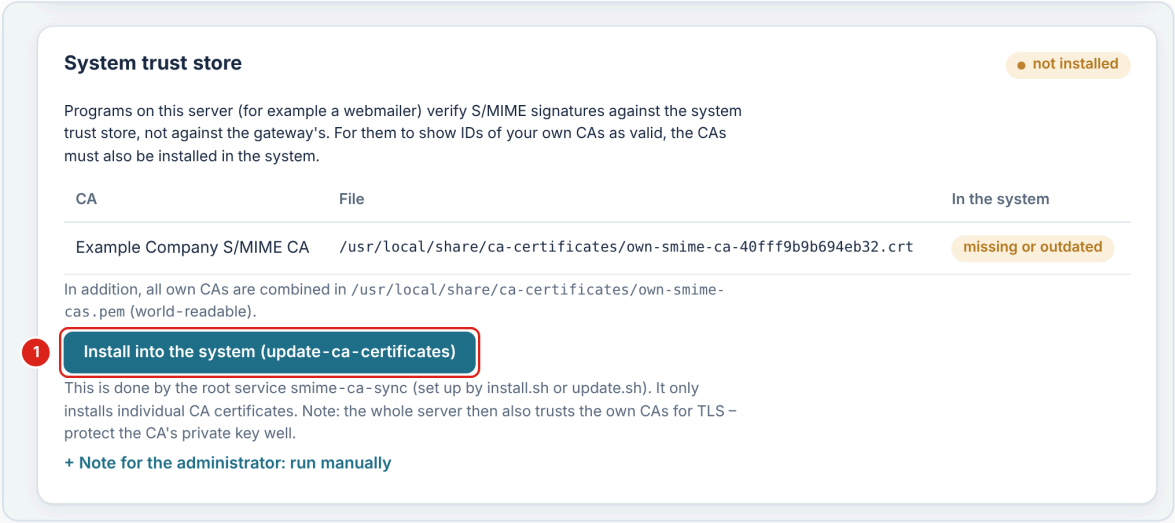
Below it there are step-by-step instructions for each system to expand – for Windows including the `certutil` command and the group policy route, for macOS with `security add-trusted-cert`, for Linux per distribution, for iPhone/iPad (install the profile and enable it under “Certificate Trust Settings”), Android and Thunderbird (own store). Company phones are easiest to supply via device management (MDM).

For your contacts too

Other companies also need to install the CA certificate once, otherwise they also see “not trusted”. Send them the .cer file and the SHA-256 fingerprint via a second channel (for example by phone) so they can check the file. You also find the link “Download CA certificate” on every mailbox page.

Installing the CA in the server's system (e.g. for grommunio Web) NEW in 1.5.5

grommunio Web verifies signatures itself – against the server's trust store, not against the gateway's. If the server does not know your CA, grommunio shows for every signed email: “The issuing certificate authority is not in the server's S/MIME trust store”.



The “System trust store” box on the “Certificate authorities” page

1. Click **“Install into the system”** and confirm. The gateway places each own CA as `own-smime-ca-….crt` in `/usr/local/share/ca-certificates/` (plus all of them together in `own-smime-cas.pem`) and runs `update-ca-certificates`. If the “grommunio admin auth” plugin is active, it also restarts php-fpm so that grommunio Web knows the CA immediately. Afterwards the box shows “installed”.

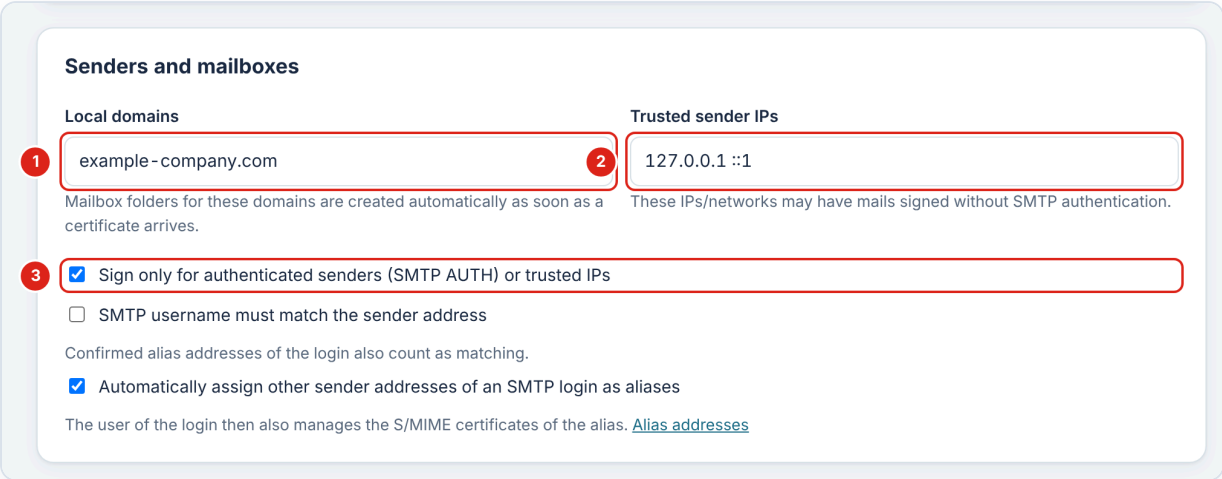
This is done by a small helper service with root privileges (`smime-ca-sync`), set up by `install.sh` and `update.sh`. The web interface itself deliberately has no root privileges. If the helper does not respond, the box “Note for the administrator” opens. It lists the commands your IT service provider runs once as root. After creating or deleting a CA the box shows “not installed” – just click the button again.

Good to know

In the system trust store, the whole server trusts your CA – including for encrypted websites (TLS). So protect the server and the CA well, and only create CAs you really need.

10 S/MIME settings

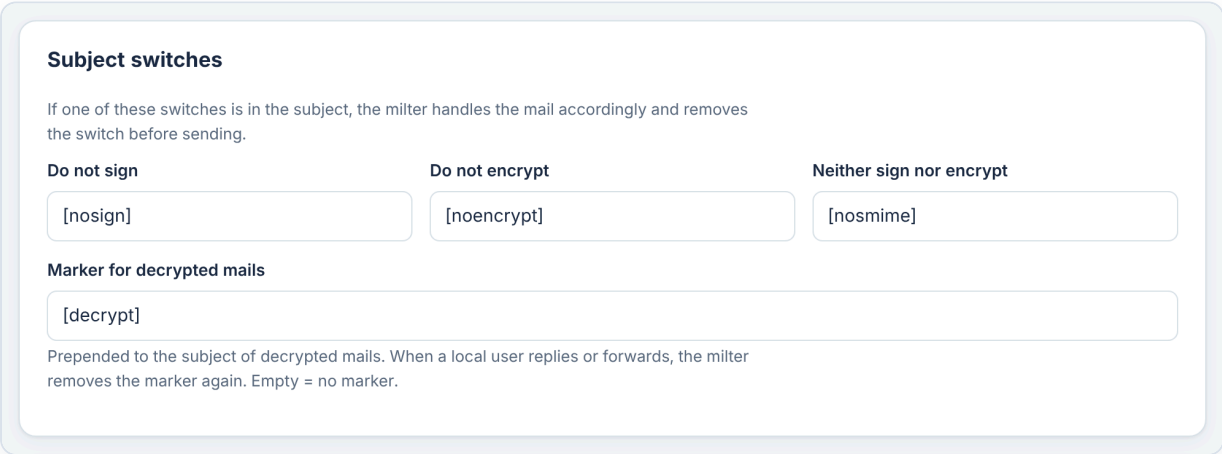
Click **“S/MIME”** in the menu. The most important part is the box **“Senders and mailboxes”**:



Domains and allowed senders

1. **Local domains**: the part of your email addresses after the @, for example `example-company.com`. Separate several with spaces.
2. **Trusted sender IPs**: devices that may hand in emails without signing in (for example the mail server itself: `127.0.0.1`). If in doubt, do not change.
3. **Sign only for authenticated senders …**: should stay ticked. Then nobody from outside can have emails signed in your name.

The “magic words” in the subject

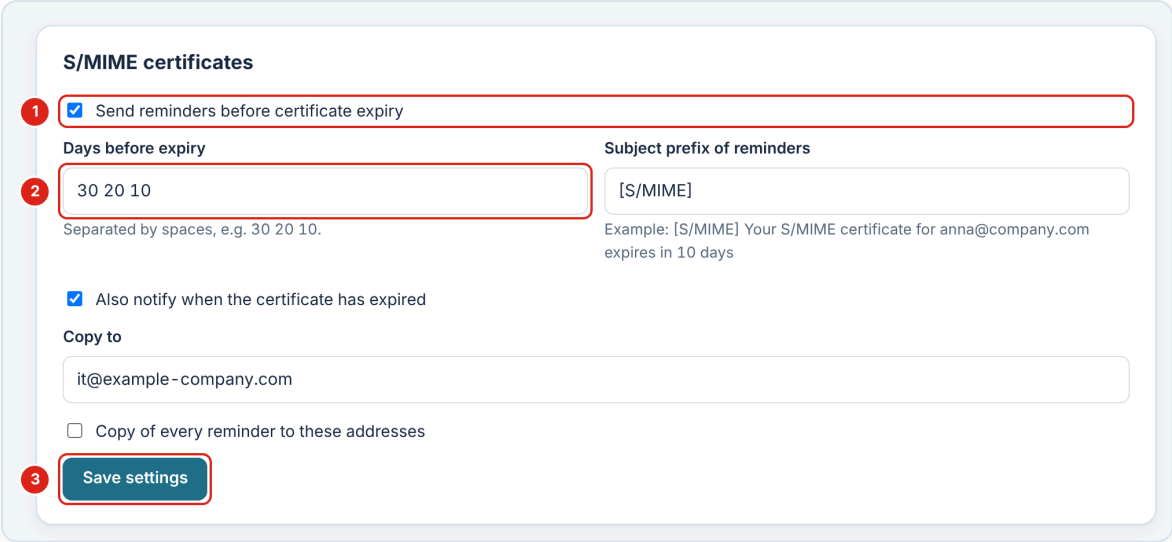


Subject switches

At the top of the page you set the **subject switches** – the words colleagues use to send a single email without signature or unsealed (`[nosign]` , `[noencrypt]` , `[nosmime]`). The basic settings for all mailboxes are under **“Defaults”**.

11 Reminders and info mails

IDs are only valid for a certain time. So that none is forgotten, the gateway sends reminders in good time. Click **“Reminders”** in the menu.

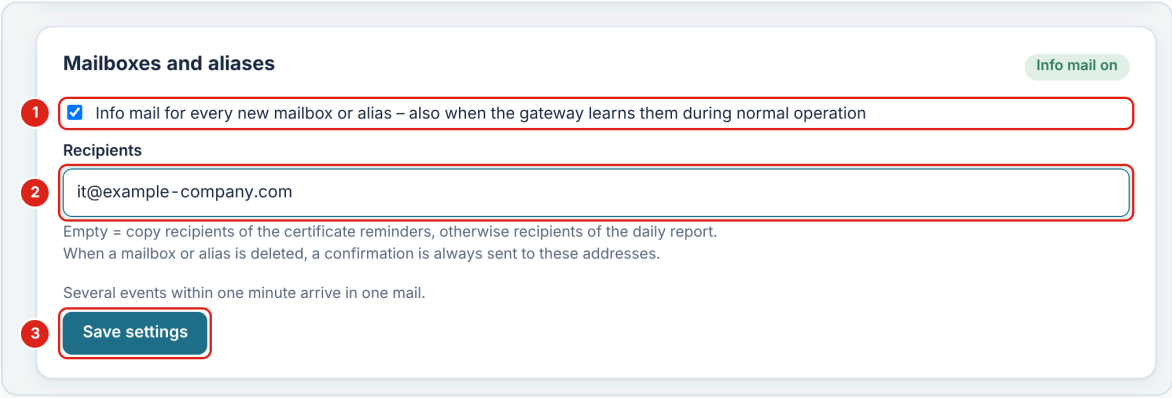


Switching on reminders

1. Tick **“Send reminders before certificate expiry”**.
2. **Days before expiry**: for example `30 20 10` – then one email comes 30, 20 and 10 days before.
3. **“Save settings”**. Under “Copy to” you can have a copy of every reminder sent to yourself.

Info mails about mailboxes and aliases NEW in 1.5.3

Further down on the same page is the box **“Mailboxes and aliases”**. Here you decide who receives the info mails:



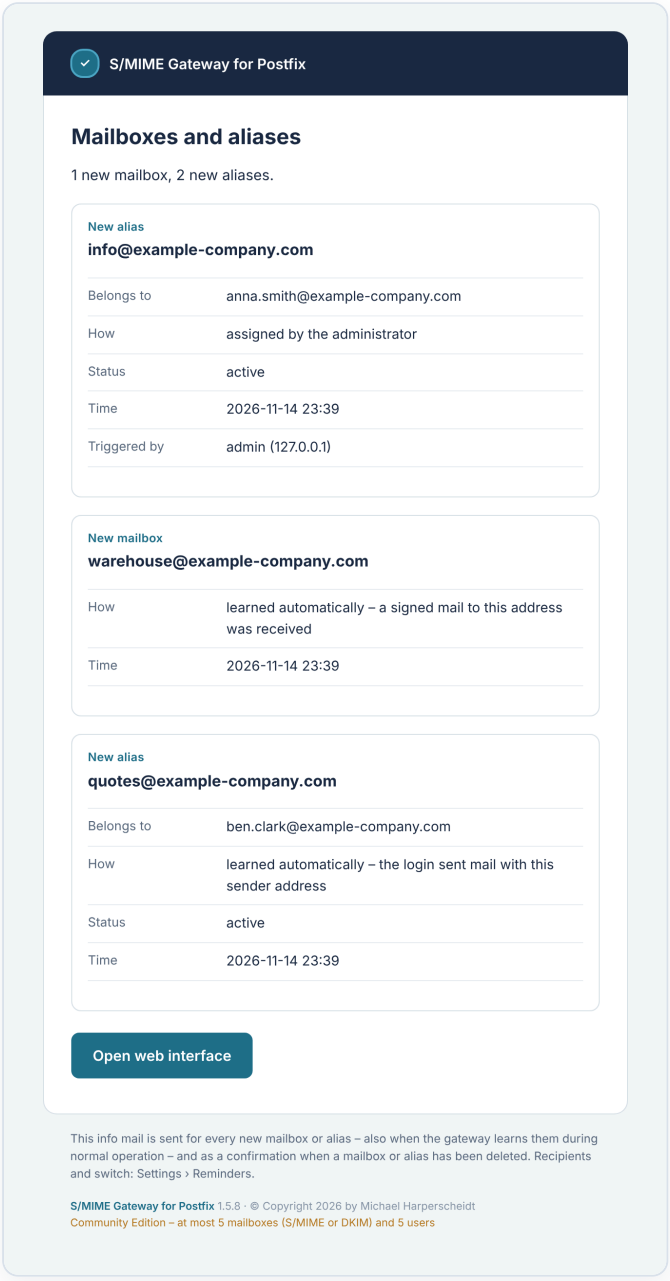
Recipients of the info mails

1. Tick **“Info mail for every new mailbox or alias”** (ticked from the start).

2. **Recipients**: one or more addresses, separated by commas. Empty = the addresses under “Copy to” (above), otherwise the recipients of the daily report.

3. **“Save settings”**.

An info mail arrives when a mailbox or alias is **new** – no matter whether you created it, whether it was created when assigning it to an account, or whether the gateway learned it during normal operation. Everything that happens within one minute is collected in **one** email:



An info mail with three new addresses

When a mailbox or alias is **deleted**, a confirmation always goes to the same addresses – even if the tick box above is off (chapter 8).

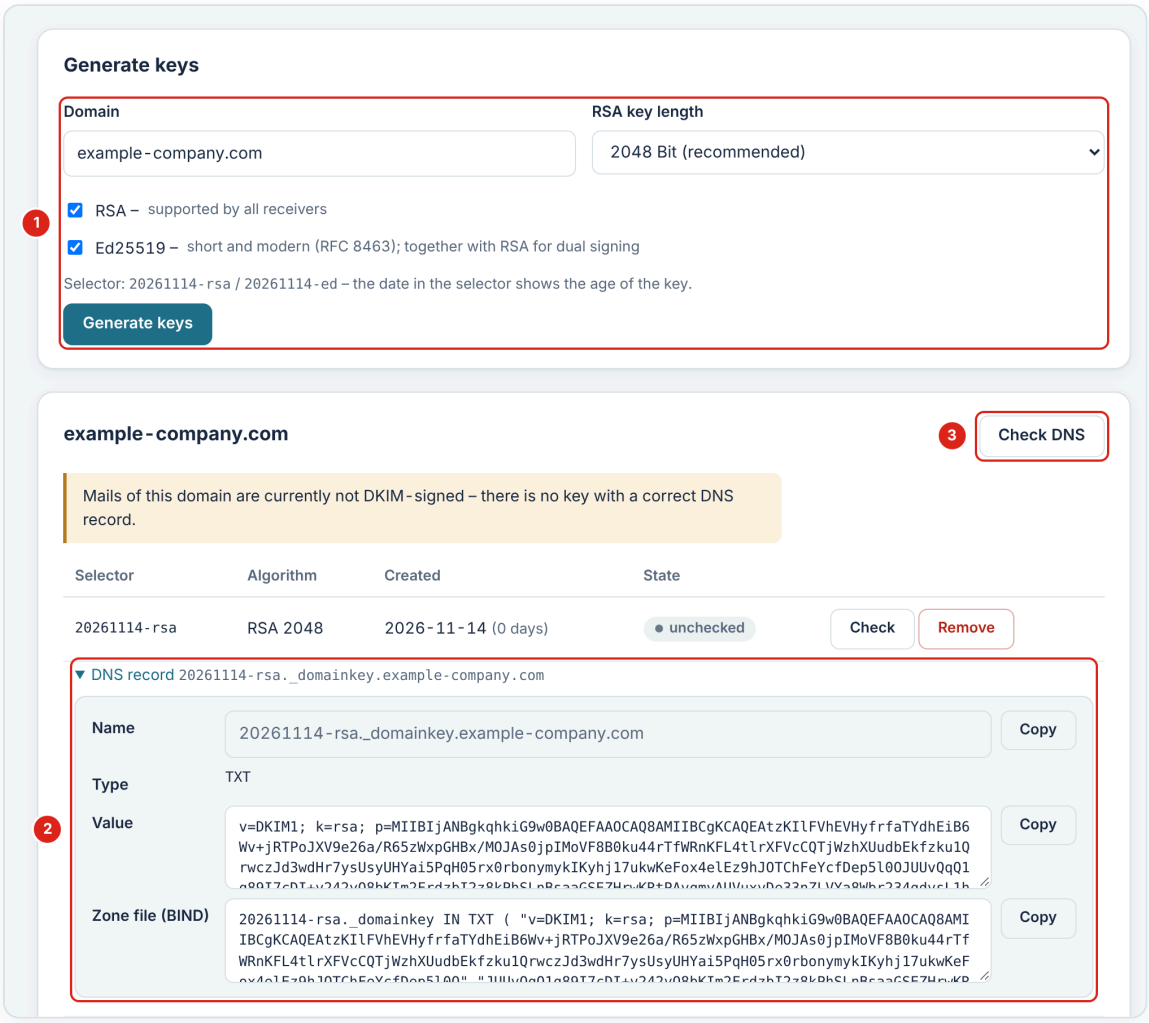
Is a learned alias waiting for you?

If “SMTP username must match the sender address” is switched on under **“S/MIME”**, newly learned aliases wait for your confirmation. The info mail then says so, with a button straight to the list (chapter 15).

12 DKIM – the authenticity stamp for your domain

DKIM is an invisible stamp on every email of your company. Receiving servers check it and then know: this email really comes from *example-company.com*. As a result, your emails end up in the spam folder less often.

DKIM is a **plugin** (add-on). Switch it on under **“Plugins”**; then **“DKIM”** appears in the menu.



The DKIM page: generating keys and the DNS record

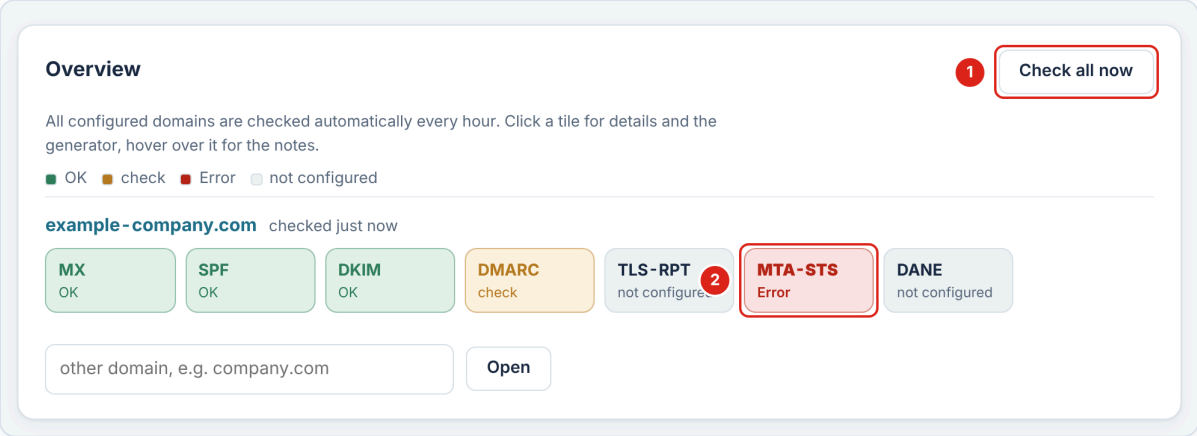
1. Enter the domain and click **“Generate keys”**. Leave RSA and Ed25519 ticked.
2. Under **“DNS record”** you see name and value. These must be entered in your domain's **DNS** – the “phone book of the internet”, managed by your domain provider. **“Copy”** takes over the values without typing. If you cannot do this yourself, send the values to your domain provider or IT service provider.
3. After entering them (this can take a few hours), click **“Check DNS”**. Once the key shows a green mark, the gateway stamps every email from then on. The gateway also checks by itself every hour.

Good to know

As long as the DNS record is missing, a yellow note says “Mails of this domain are currently not DKIM-signed”. That is not an error, just a reminder.

13 Mail DNS – checking SPF, DMARC, MTA-STS and co. NEW in 1.5.7

Whether your emails arrive and are considered genuine depends on a few records in the **DNS** of your domain. Under **“Settings › Mail DNS”** the gateway checks them all at once and shows what is missing – with an explanation and, where possible, the finished record to copy.



The overview: one row of tiles per domain

The gateway checks all configured domains (your local domains, domains with a DKIM key and domains you created a record for) **by itself every hour**. The result is shown at the top as small tiles, one row per domain: **green** = OK, **yellow** = please check, **red** = error, **grey** = not set up (dashed: not checked yet).

1. **“Check all now”** starts the check immediately instead of waiting for the next hour (runs in the background – reload the page after about a minute).
2. Hover over a tile to see the most important notes. A click opens the domain directly at the matching section with explanation and generator.

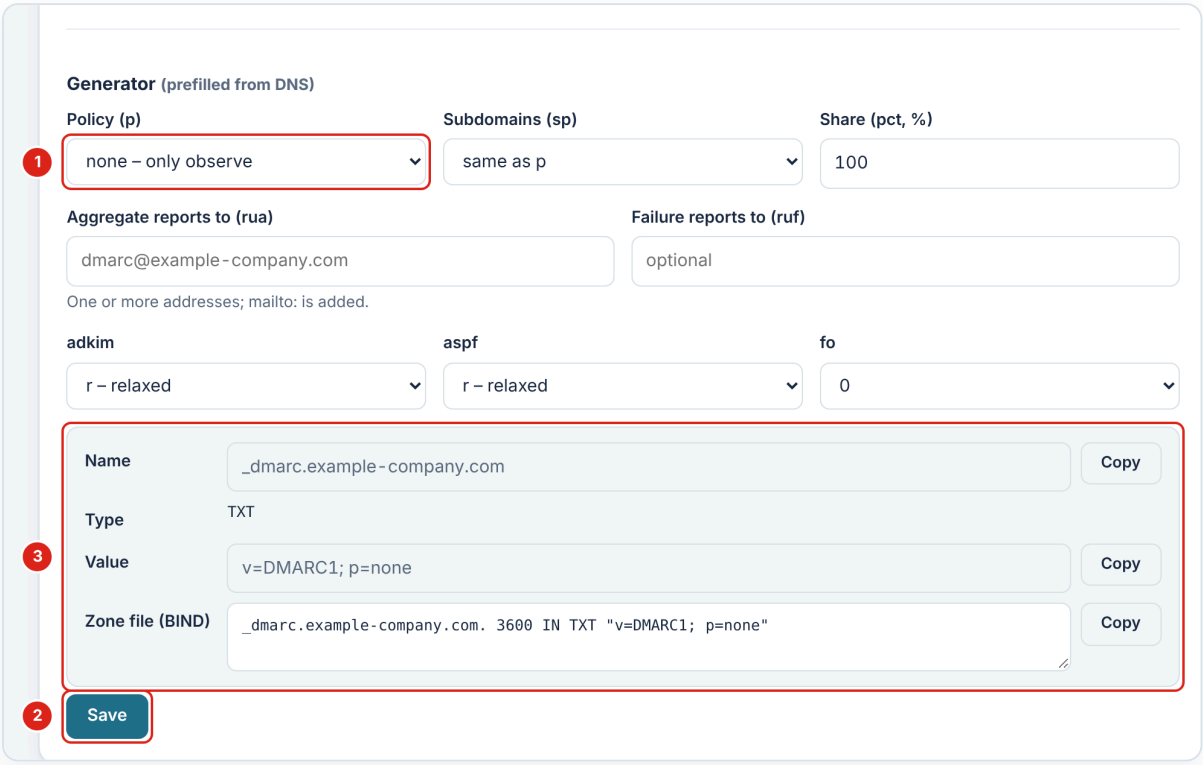
Below the overview, the sections of the selected domain are collapsed so the page stays clear. The hourly check can be turned off under **“Check settings”**.

Mechanism	What for?
SPF	List of the servers allowed to send for your domain.
DKIM	The stamp from chapter 12. If the plugin is active, the page checks exactly its keys.
DMARC	What happens to forged mails (observe, spam folder, reject) and where reports go.
TLS-RPT	Daily reports from other mail servers on whether encrypted delivery to you worked.
MTA-STS	Requires other mail servers to send to you only encrypted and with a valid certificate (policy via HTTPS).

DANE	The same goal via DNSSEC: your mail server's certificate is published as a TLSA record in DNS.

Creating a record

Each section starts with **“What does … do?”** – every setting is explained there. Below are the check results and the **generator**. It is prefilled with the existing record.



The DMARC generator

1. Choose the settings, e.g. for DMARC the policy and the address for reports.
2. **“Save”**.
3. Name, type and value of the record are shown below – use **“Copy”** to pass them to your domain provider. The “zone file” line is for administrators of their own DNS server.

After the record has been added at your domain provider, the next hourly check shows the result – or right away with **“Check now”**.

At the top, all generated records are available together as a file (**“All generated records as zone file”**). There is no generator for DKIM here – the DKIM plugin creates the key.

Publishing MTA-STS via the gateway

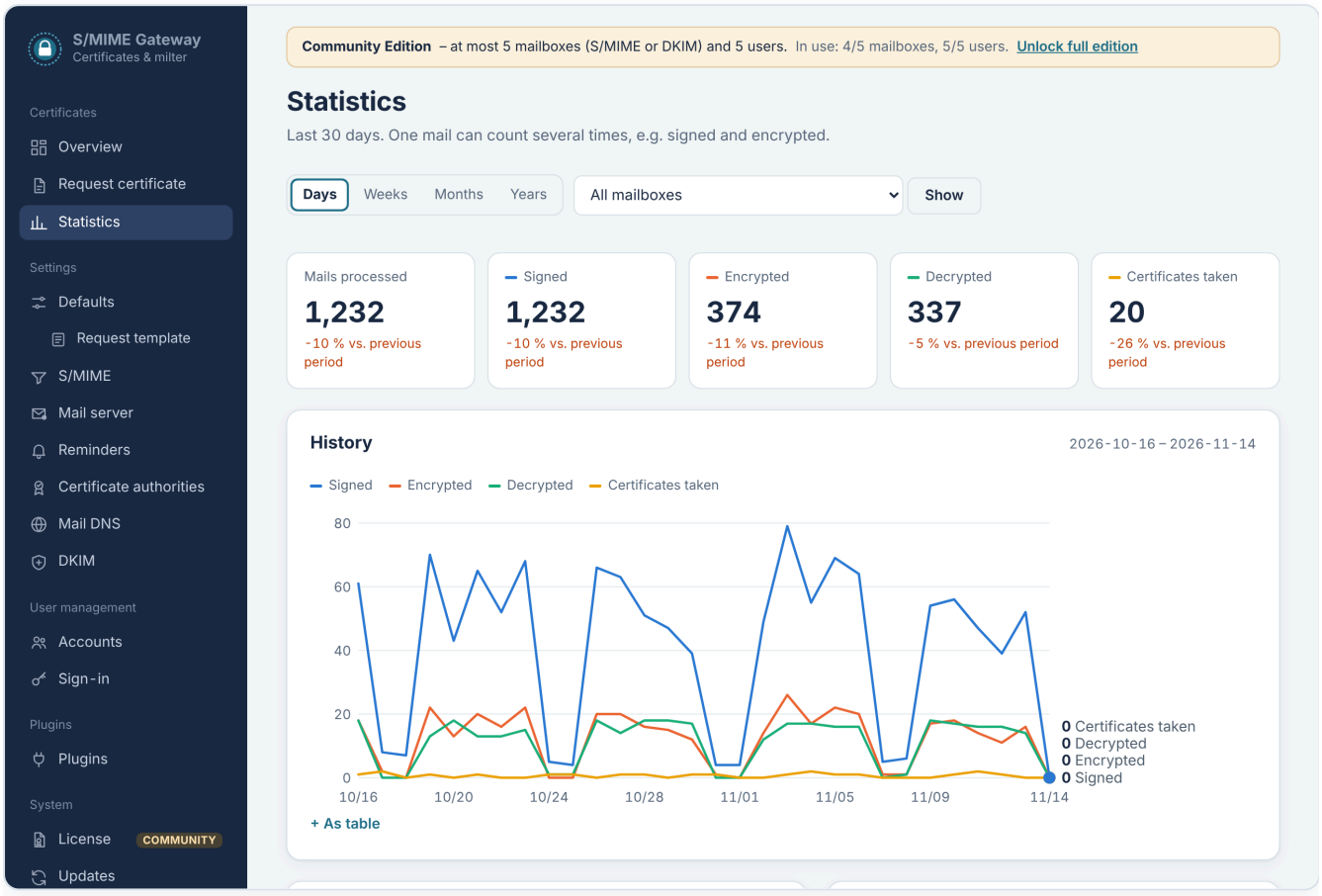
MTA-STS needs a small file at `https://mta-sts.<your-domain>/.well-known/mta-sts.txt`. The gateway can serve it itself: tick **“Publish the policy via the gateway”** and save. The page then shows the required DNS records, the policy, a small HTML info page and ready-made **nginx**

templates – for a separate web server entry and for grommunio. nginx only exposes this file, not the web interface.

> **Test first, then enforce**
>
> Start MTA-STS with **testing** and set up TLS-RPT beforehand. If no failure reports arrive for a few weeks, switch to **enforce**. For DANE: only publish TLSA records if your domain is DNSSEC-signed, and before every certificate or key change publish the new record in addition.

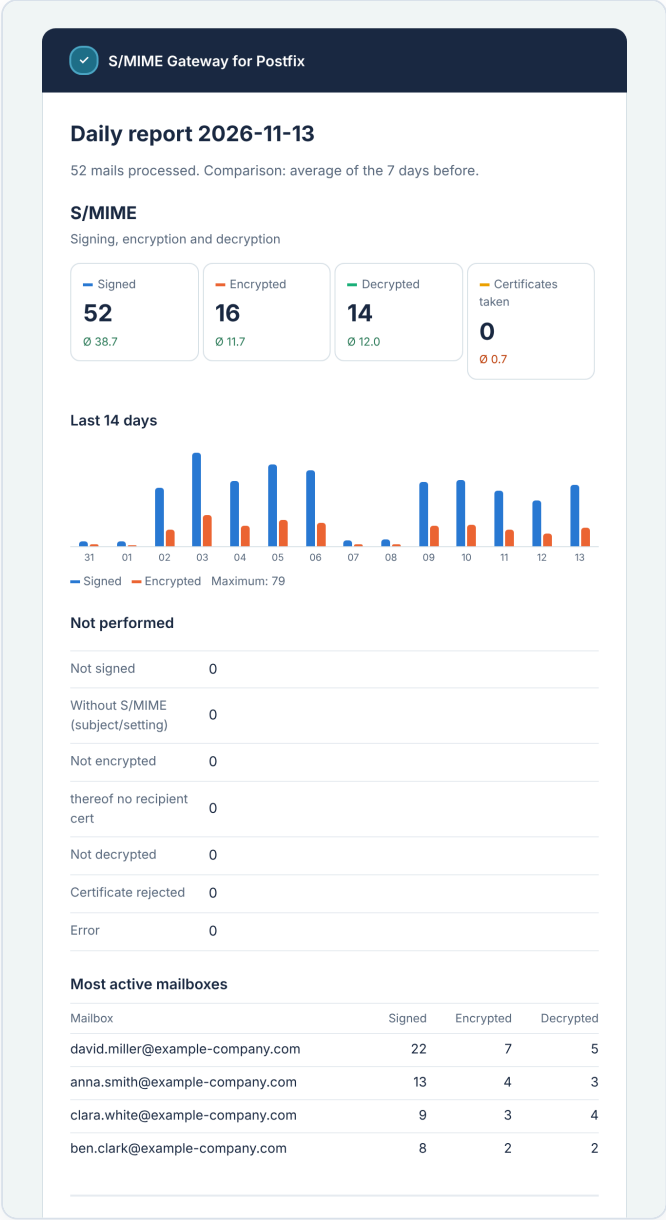
14 Statistics and daily report

Under **“Statistics”** you see how many emails were signed, sealed and opened – as numbers and a chart.



The statistics for the last 30 days

At the very bottom of the page you switch on the **daily report**: tick **“Send a report on the previous day by mail every day”**, enter your address, choose a time, save. Then you receive an email like this every morning:



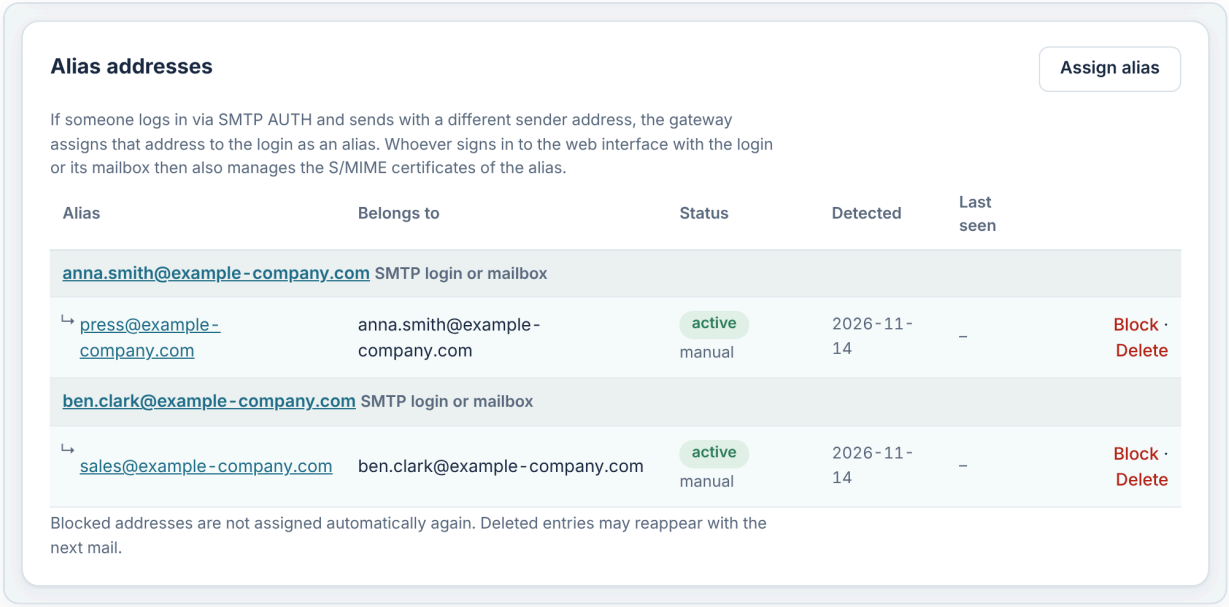
The daily report (excerpt). Further down follow DKIM, mail traffic per mailbox and IDs that expire soon.

What to look out for

The section “Certificates needing action” at the end of the report. If a mailbox is listed there, it should get a new ID soon.

15 Alias addresses

Some colleagues also send emails under another address, for example Anna as *press@example-company.com*. The gateway notices this by itself and assigns the address to Anna's account – you receive an info mail about it. Anna can then also request an ID for press@. You can create aliases yourself with **“Create mailbox”** (chapter 7).



The alias addresses on the “Accounts” page

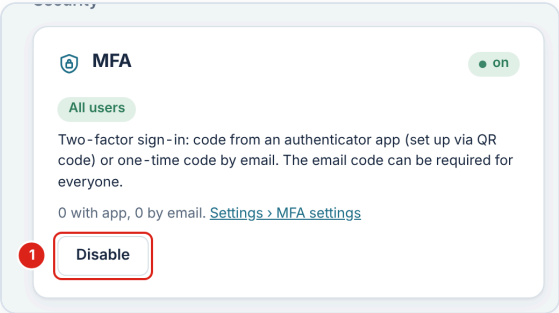
The list is grouped by mailbox: each group starts with the mailbox (or SMTP login), followed by its aliases, indented.

If an assignment is wrong, click **“Block”** – then the address is not assigned automatically again. **“Delete”** only removes the assignment. With **“Assign alias”** you assign an address yourself. Addresses that sign in themselves or already have their own ID are never assigned automatically. To delete an alias including its folder, use its mailbox page (chapter 8).

16 Two-factor sign-in (MFA) NEW in 1.5.5

With **two-factor sign-in**, a stolen password is no longer enough. After the password, the gateway asks for a six-digit one-time code – either from an **authenticator app** on the phone or from an **email**.

Switching on the plugin

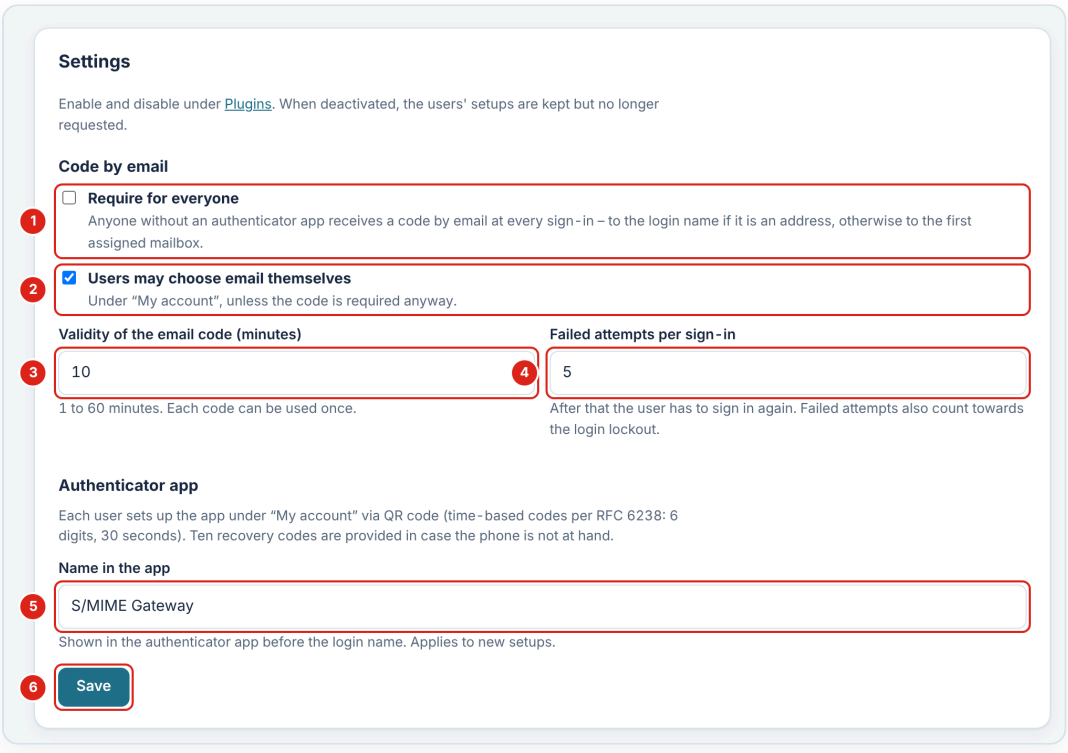


The “MFA” plugin under Plugins

1 Click **“Plugins”** in the menu and, for the **MFA** plugin (group “Security”), click **“Activate”**.

Only then does the menu item **“MFA settings”** appear under “Settings”, and every user gets the section “Two-factor sign-in” under **“My account”**. If you switch the plugin off again, the setups are kept but no longer requested.

The MFA settings



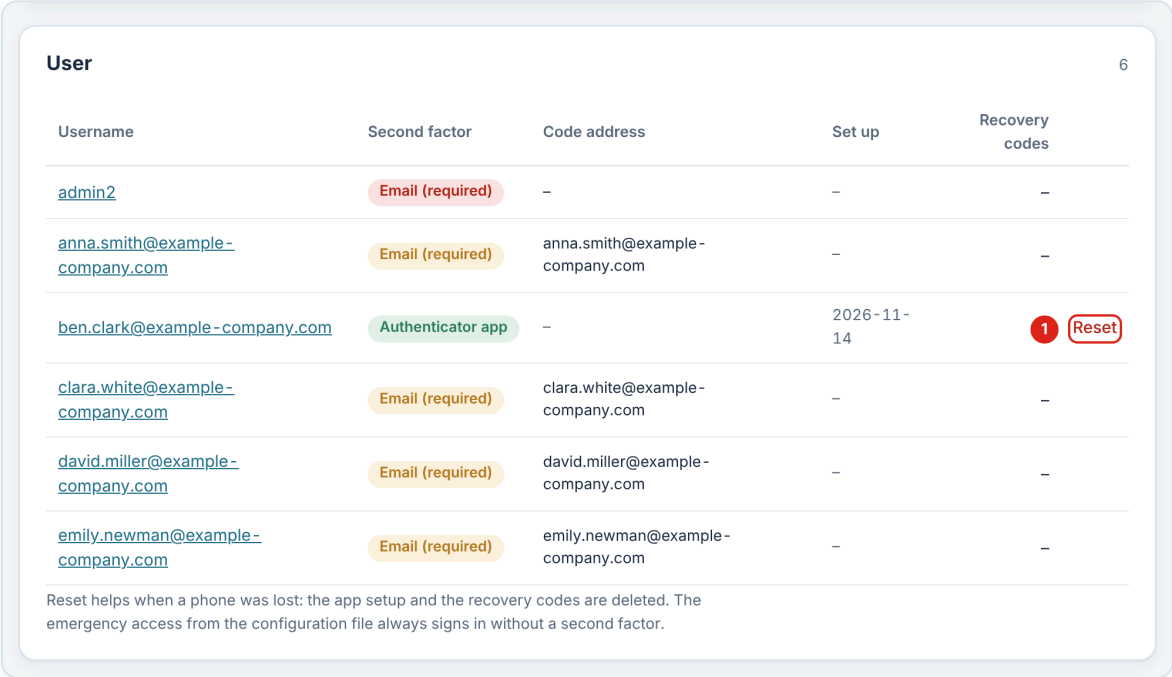
The “MFA settings” page

1 **Require for everyone**: anyone without an authenticator app receives a code by email at every sign-in. It goes to the login name if that is an email address, otherwise to the first assigned mailbox.

2. **Users may choose email themselves**: if the code is not required, everyone can decide under “My account” whether to receive it by email.
3. **Validity of the email code**: 1 to 60 minutes (default: 10). Each code works only once.
4. **Failed attempts per sign-in**: after that the user has to sign in again. Wrong codes also count towards the normal login lockout.
5. **Name in the app**: the name of the entry in the authenticator app, for example “S/MIME Gateway”.
6. Click **“Save”**. This applies from the next sign-in.

> **Set up the mail server first**
>
> Codes by email only work if a sender is configured under **“Mail server”** (chapter 5). Accounts without an email address (for example an account “admin”) cannot receive a code by email. Until then they sign in with the password only and are asked to set up an authenticator app. The page lists such accounts at the top in a yellow box.

Who uses what? – Reset



The “Users” list on the “MFA settings” page

The list shows every account with its second factor: **Authenticator app**, **Email**, **Email (required)** or **password only**.

1. If someone has lost their phone, click **“Reset”** for them. The app setup and the recovery codes are deleted. They then sign in with the password (plus a code by email if required) and set up the app again.

How your colleagues sign in

The user guide explains step by step how to set up the app and enter the code. You set up your own app the same way under **“My account”**. The **emergency access** from the configuration file (chapter 2) never asks for a code – so you cannot lock yourself out. Keep its password especially safe.

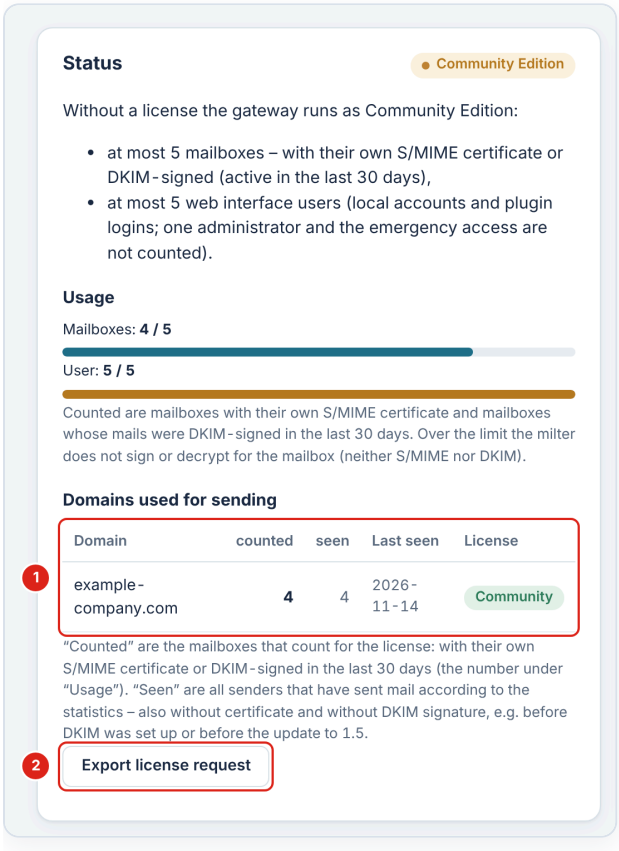
17 The license

The gateway comes in two editions:

	Community Edition (free)	Full version (with license file)
Mailboxes	at most 5	as many as the license allows
Users	at most 5 (one administrator does not count)	as many as the license allows
Mail domains	all	those named in the license
Features	all	all

Every address that has its own ID, or whose emails received the DKIM stamp in the last 30 days, counts as a **mailbox**. An address with both counts only once. When you delete a mailbox, its seat is free again immediately.

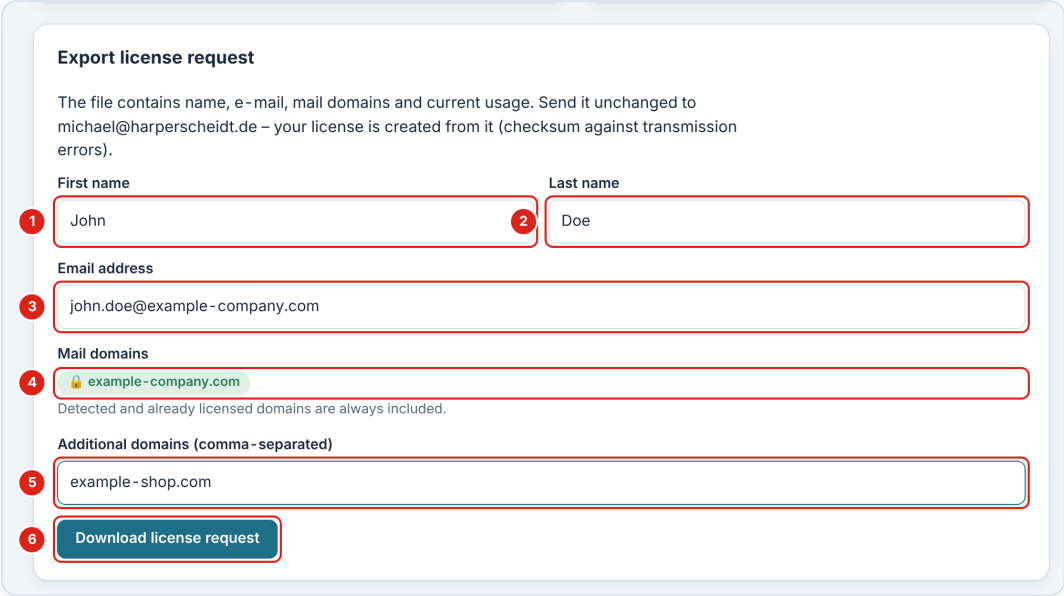
Click **“License”** under “System” in the menu:



The “Status” box on the license page

1. **Domains used for sending**: here you see which of your domains have already sent emails through the gateway and how many mailboxes belong to them. “counted” are the mailboxes that count for the license – together they make up the number under “Usage”. “seen” are all addresses that have sent anything at all, even without ID and without DKIM stamp. Those do not count. “Show all senders with reason” shows for every address whether and why it counts.
2. **“Export license request”** takes you to the request form.

Requesting a license



Filling in the license request

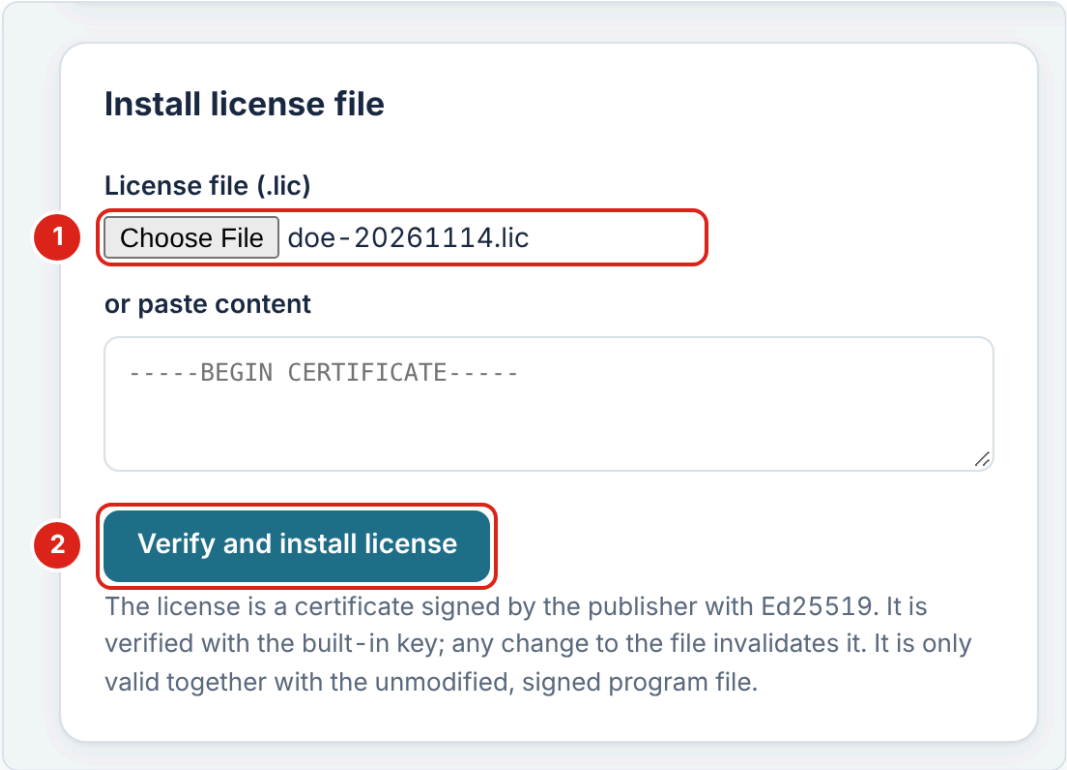
1. Enter the **first name**.
2. Enter the **last name**.
3. The **email address** the license should be sent to.
4. The domains with a lock 🔒 were found by the gateway – they are always included and cannot be removed.
5. Enter further domains you want to use in future here – separated by commas.
6. Click **“Download license request”**. Your browser saves a file, for example `lic-Doe-20261108-DyFO.req`.

Send this file unchanged by email to **michael@harperscheidt.de** and say how many mailboxes and users you need. More information: **https://harperscheidt.de**.

> **Do you already have a license?**
>
> Then name and email are already filled in. The request contains your current license – so an extension or a new domain can be issued to match.

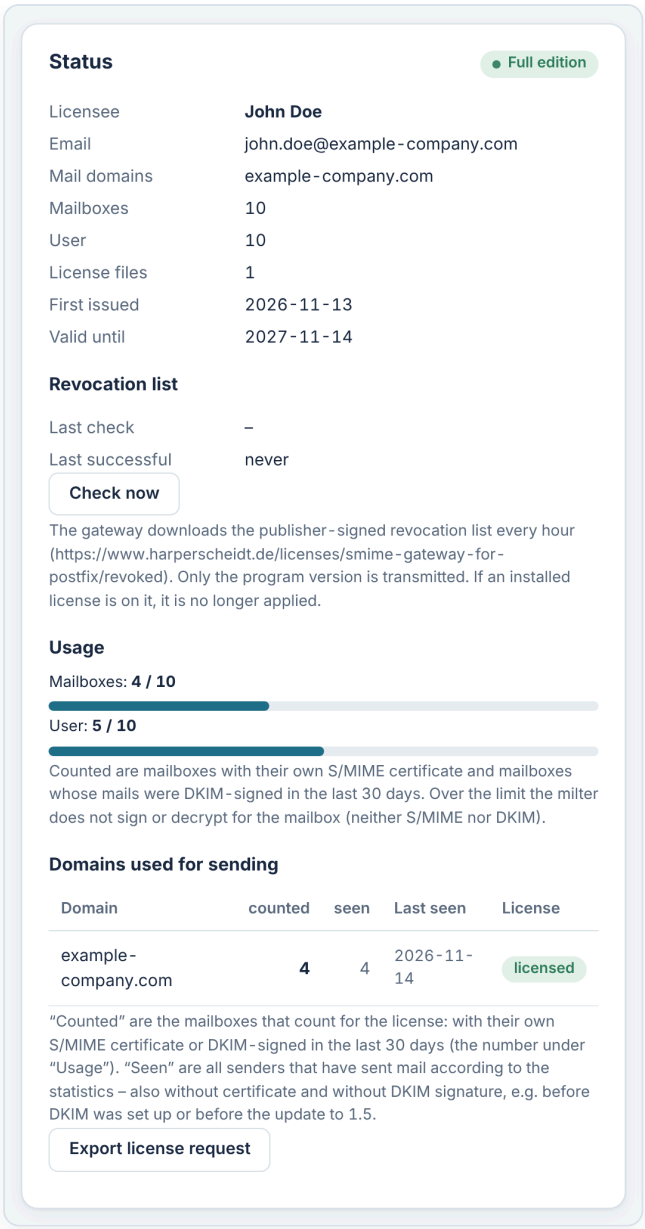
Installing the license file

You receive a file ending in `.lic`.



Installing the license file

1. Click **“Choose File”** and select the `.lic` file.
2. Click **“Verify and install license”**.



Done: the full version is unlocked (example license)

Extending the license

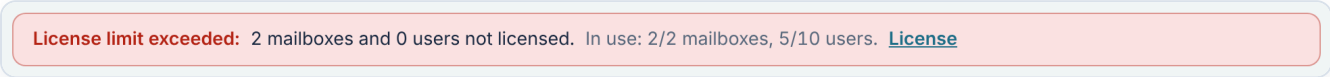
A second license for more mailboxes later? Simply install it the same way. Same name, same email and same domains are **added up**. Every license file counts only once. A license with additional domains automatically replaces the old one.

18 When the license is no longer enough

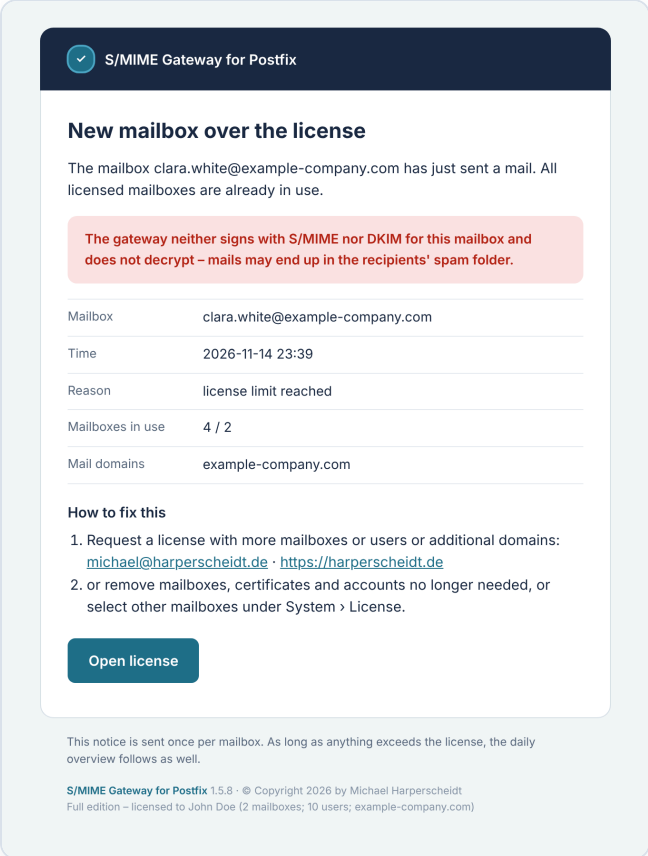
If the company uses more mailboxes or users than allowed, a fixed rule applies:

- For mailboxes **over the limit**, emails are **neither signed nor stamped** (DKIM) and not opened.
- Users over the limit cannot sign in.

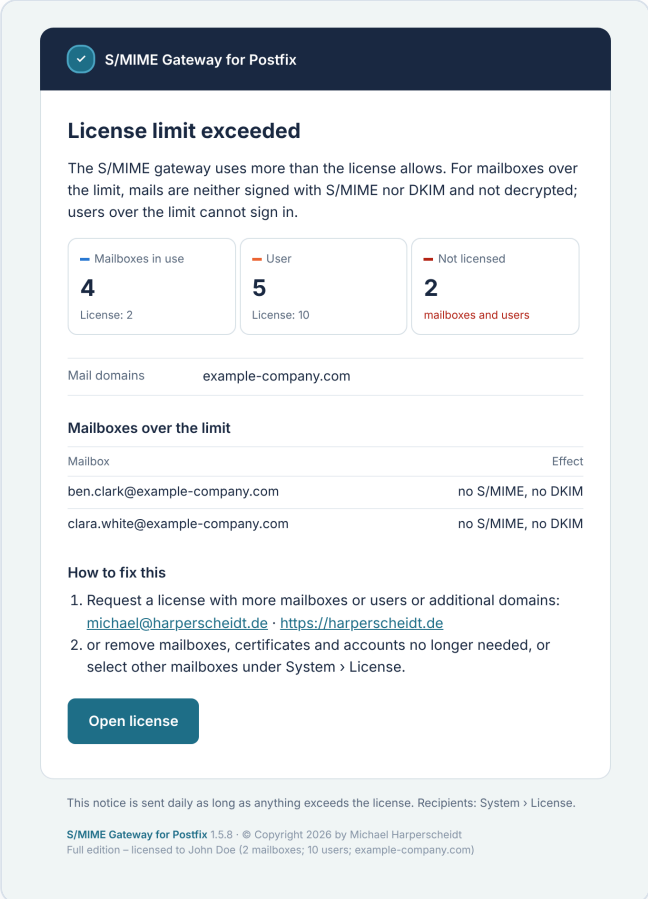
You notice this in three places:



1. A red bar at the top of every page



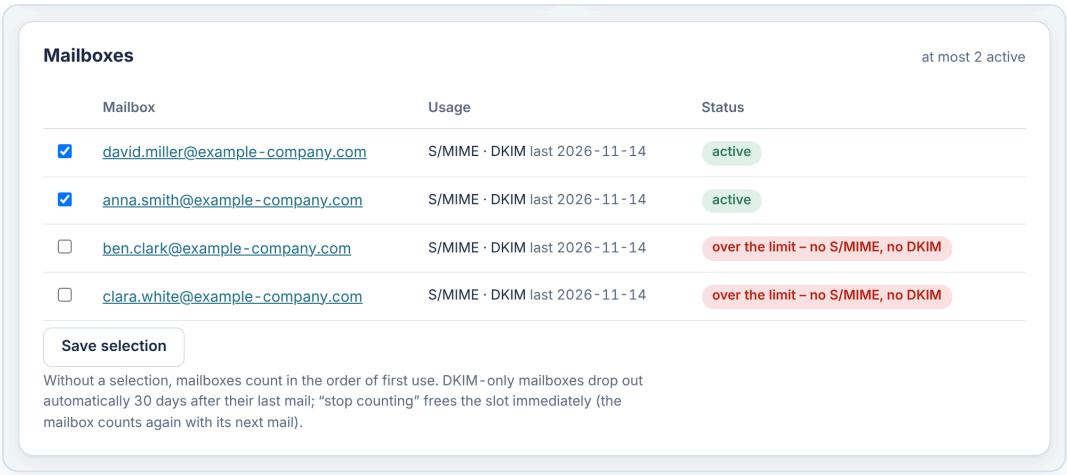
2. An email right away when a new mailbox over the limit sends an email – once per mailbox



3. An overview every day, as long as something is over the limit

What you do then

1. **Request more license** (chapter 17) – that is the easiest way.
2. Or **tidy up**: delete mailboxes that are no longer needed (chapter 8) – their seat is free immediately. Or tick, on the license page under “Mailboxes”, which mailboxes should be active and click **“Save selection”**. Mailboxes that are only stamped and no longer needed are removed with “stop counting”.



The mailboxes on the license page

19 Installing and updating

These steps happen on the server itself, in a black text window (“terminal”). If you are not familiar with it, ask your IT service provider – it only takes a few minutes.

First installation

```
sudo ./install.sh --admin admin --postfix
```

This sets everything up and creates the account **admin** (you are asked for a password).

Updating to a new version

The easiest way is the web interface: when a new version is available, **“System › Updates”** shows the button **“Install update to …”**. Enter your login password to confirm. The gateway downloads the new version from the publisher, verifies its signature, makes a backup and restarts. Afterwards you sign in again. NEW in 1.5.8

Or on the server with the new release archive:

```
sudo ./update.sh
```

A backup is made automatically first. If something goes wrong, the old version is restored by itself.

> **Important**
>
> Only install files that come from the publisher. The installer checks the signature (`smime_milter.py.sig`) and stops if the program file has been changed. With a changed file no license is valid.

Checking the state

```
sudo -u smime-milter /opt/smime-milter/smime_milter.py doctor /etc/smime-milter.conf
sudo -u smime-milter /opt/smime-milter/smime_milter.py license /etc/smime-milter.conf
```

Where the data is stored

Folder / file	Contents
`/var/lib/smime-milter/senders/`	one folder per mailbox: ID, key, contacts' IDs, settings
`…/deleted/`	backup of deleted mailboxes, 30 days NEW in 1.5.3
`…/admin-events.json`	info mails not yet sent NEW in 1.5.3
`…/aliases.json`	alias addresses

`/var/backups/smime-milter/`	backups made by `update.sh` and by the update button

20 When something does not work

What happens	What you can do
Colleagues do not receive an email with their credentials.	Send a test mail under “Mail server” (chapter 5). Have the spam folder checked.
I do not receive info mails about new mailboxes.	Check the tick box and recipients under “Reminders” › “Mailboxes and aliases” (chapter 11). “Send waiting now” sends pending notifications immediately.
I have locked myself out.	Sign in with the emergency access (chapter 2).
A colleague has lost the phone with the authenticator app.	Under “MFA settings”, click “Reset” for them (chapter 16).
The code by email does not arrive.	Send a test mail under “Mail server” (chapter 5), check the spam folder. Click “Send a new code” on the sign-in page.
I deleted the wrong mailbox.	Within 30 days your IT service provider can restore the folder from `/var/lib/smime-milter/deleted/` (chapter 8).
“… is already registered as an alias of …” when creating.	The address already belongs to another mailbox. Delete it first under “Accounts” › “Alias addresses”, then create it again.
“Community Edition: at most 5 users …” when creating an account.	Request a license (chapter 17) or lock unused accounts.
Red bar “License limit exceeded”.	Chapter 18.
“Mails of this domain are currently not DKIM-signed”.	The DNS record is missing or not visible yet (chapter 12). Wait a few hours, then “Check DNS”.
A partner cannot open sealed emails.	They need their own ID. Until then: `[noencrypt]` in the subject.
grommunio Web reports “The issuing certificate authority is not in the S/MIME trust store”.	Click “Install into the system” under “Certificate authorities” (chapter 9).
A partner sees “signature not trusted”.	Send them the CA certificate (chapter 9) or use public IDs.
The license is not accepted (“does not match the existing one”).	Name, email or domains differ. Tick “Replace existing licenses” – or ask the publisher.
The license page says “The program file has been modified”.	Reinstall the original version (chapter 19).

Getting help

Questions about the license: **michael@harperscheidt.de** · **https://harperscheidt.de**.
Technical details are in the file `README.md`.

21 Small glossary

Word	Simply explained
Gateway / milter	The program on the mail server that every email passes through. In Postfix terminology it is called a “milter”.
Postfix	A widely used mail server program. The gateway works together with it.
Mailbox	An email address with its own IDs and settings.
Alias	An additional address that belongs to a mailbox and under which a colleague sends emails.
Account	Access to the gateway's web page (username and password).
MFA / two-factor sign-in	Signing in with the password plus a one-time code from an app or an email.
Authenticator app	An app on the phone that shows a new six-digit code every 30 seconds.
Certificate	Digital ID of a mailbox.
CA	Certificate authority – the “ID office”.
Signing / encrypting	Signing / putting into a sealed envelope.
DKIM	Invisible authenticity stamp for all emails of a domain.
DNS	The “phone book of the internet”. Your domain provider manages the entries.
Domain	The part of the email address after the @, for example example-company.com.
Info mail	Short message to you when a mailbox or alias is added or has been deleted.
Backup	Copy of a deleted mailbox that stays on the server for another 30 days.
License file (.lic)	File from the publisher that unlocks the full version. Signed, so it cannot be forged.
License request (.req)	File you send to the publisher to get a license.
Community Edition	The free edition: 5 mailboxes, 5 users.

Copyright and license

© 2026 Michael Harperscheidt. All rights reserved.

This guide (“Administrator guide”, version 1.5.8) belongs to **S/MIME Gateway for Postfix**. Text, structure and pictures are protected by copyright.

You may pass on this guide unchanged together with the software, print it for operating the gateway in your organisation and distribute it internally. Any other copying, editing, translation or publication – including extracts – requires the written consent of Michael Harperscheidt.

Software

The S/MIME Gateway for Postfix software is licensed under the **Business Source License 1.1** (file `LICENSE`). Use within the limits of the Community Edition is permitted; a license is available for more mailboxes, users or specific mail domains (chapter 17).

Notes

The pictures show a made-up example company; names and addresses are fictitious. Any resemblance to real companies or persons is coincidental. Product and company names mentioned (for example Postfix, grommunio, Outlook) may be trademarks of their respective owners.

This guide was written with care. It does not replace advice for your environment; to the extent permitted by law, no liability is accepted for damage caused by incorrect information.

Contact

Michael Harperscheidt · michael@harperscheidt.de · https://harperscheidt.de