S/MIME Gateway for Postfix · Version 1.5.8

Secure email – simply explained

Guide for users

Who is this guide for?

For everyone who protects their emails with the S/MIME Gateway. You do not need any computer knowledge. Read calmly, step by step – you cannot break anything.

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 · User guide

Contents

1 What is this about?

2 What you need

3 Signing in

4 Choosing your own password

5 Securing your sign-in with a code NEW

6 The start page

7 Looking at your mailbox

8 Getting a digital ID (certificate)

9 Settings – what the switches mean

10 Switching something off for a single email

11 Your contacts' IDs

12 The reminder email

13 Signing out and language

14 When something does not work

15 Small glossary

Copyright and license

1 What is this about?

A normal email is like a **postcard**: anyone who gets hold of it on the way can read it. And nobody can say for sure whether it really comes from you.

The S/MIME Gateway is a program on your company's mail server. It turns your emails into “secure letters” – automatically. You write your emails as always in your usual email program. The gateway does the rest in the background.

✍️

Signing

The recipient sees: this email really comes from you and was not changed on the way.

✉️

Sealing (“encrypting”)

Like a sealed envelope: only the right recipient can read the email.

🪪

ID (“certificate”)

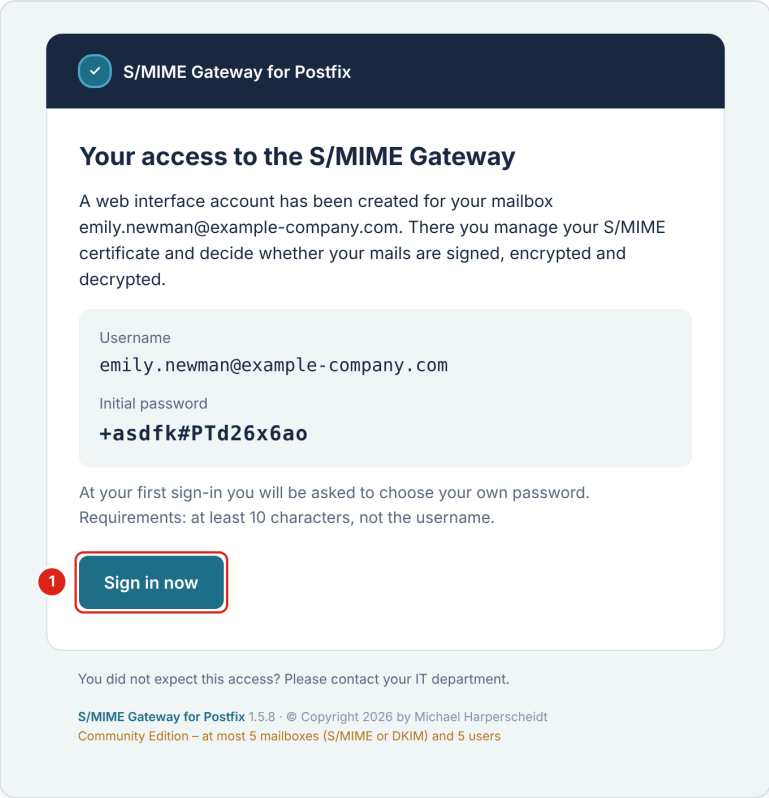
For this to work, your mailbox needs a digital ID. Chapter 8 explains how to get one.

Good to know

You rarely need the gateway's web page: for the first setup, to check that everything is fine, and when your ID has to be renewed after one or two years. In everyday work you hardly notice the gateway.

2 What you need

Your administrator (the person who looks after the gateway in your company) sends you an email with your credentials. It looks roughly like this:



The email with your credentials. Username and first password are in the grey box.

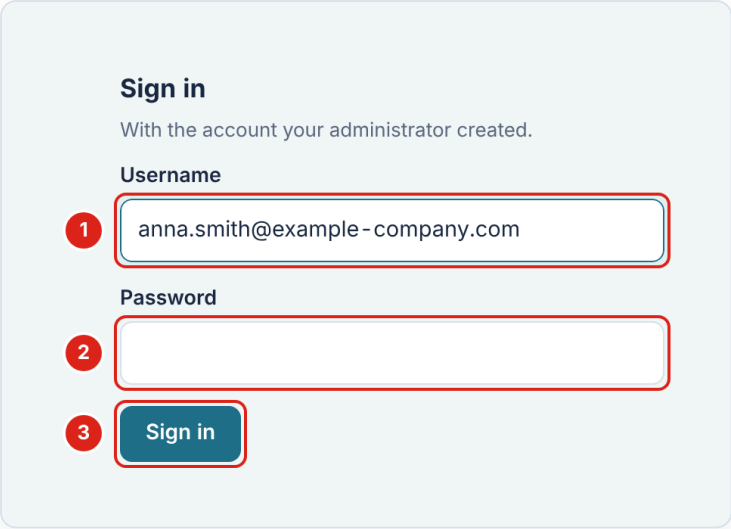
It contains three things:

- the address of the web page – open it with the blue button **“Sign in now”**,
- your **username** – usually your email address,
- a first **password** – you change it when you sign in for the first time (chapter 4).

> **Please note**
>
> Never give your password to anyone – not even on the phone. Your administrator will never ask you for it.

3 Signing in

Click **“Sign in now”** in the email. Your web browser (for example Edge, Firefox, Chrome or Safari) opens the sign-in page.



The sign-in page

1. Click into the **Username** field and type your username (usually your email address).
2. Click into the **Password** field and type your password. Instead of letters you only see dots – that is how it should be.
3. Click the blue button **“Sign in”**.

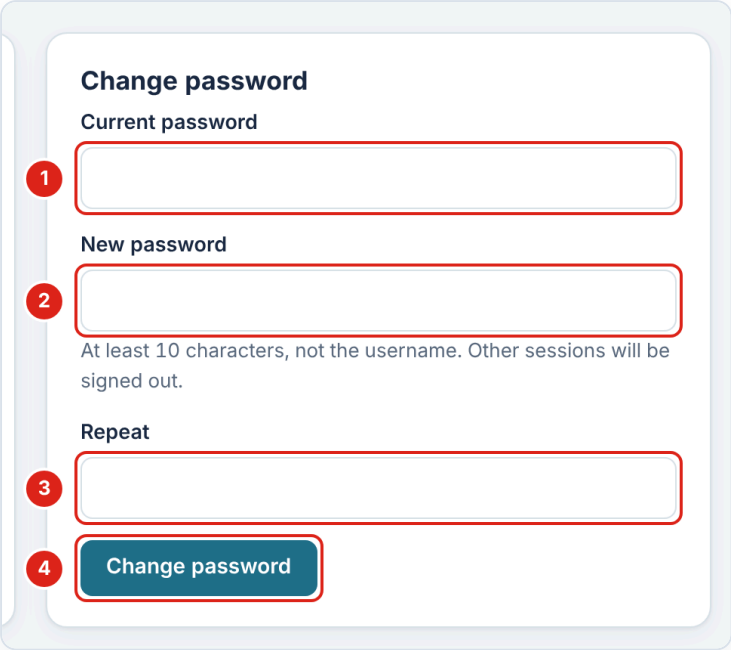
If your administrator has switched on two-factor sign-in, the gateway then asks for a code as well. Chapter 5 explains how.

> **Tip**
> Save the page as a bookmark (favourite). Then you will find it faster next time.

> **It does not work?**
> Pay attention to upper and lower case in the password. After several wrong attempts, signing in is blocked for a few minutes – wait a moment and try again.

4 Choosing your own password

When you sign in for the first time, the gateway asks you to set your own password. You do this on the page **“My account”**. You can also get there at any time later via the menu on the left.



You change your password on the “My account” page

1. Type your previous password under **Current password** (the first time: the one from the email).
2. Type your new password under **New password**. Below it you see what it must contain (for example at least 10 characters).
3. Type it once more under **Repeat** – this avoids typing errors.
4. Click **“Change password”**.

Signing in with your email password?

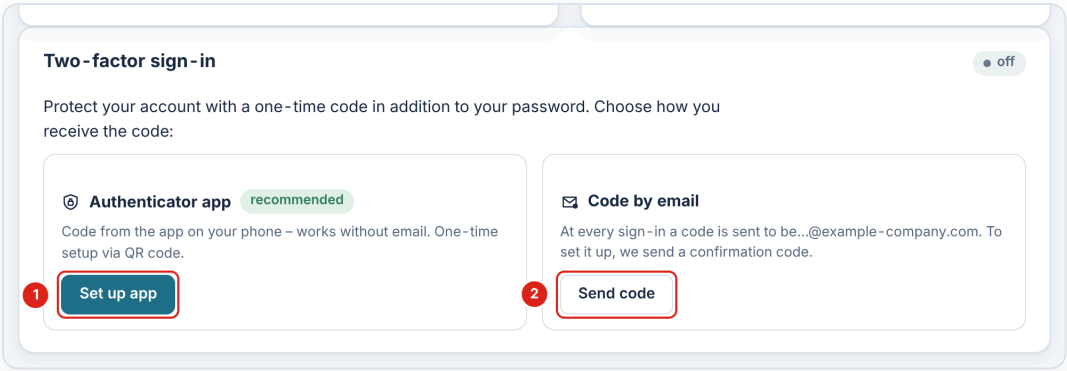
If your administrator has set up sign-in via the mail server, you sign in with the password of your email mailbox. Then there is nothing to change here.

How to find a good password

Take a short sentence that is easy to remember, for example `My-dog-is-called-Bello-2026!` – long is better than complicated.

5 Securing your sign-in with a code NEW in 1.5.5

A password can be lost or guessed. With a **one-time code** your access stays safe anyway: after the password you enter a six-digit code that only you receive. This section only exists if your administrator has switched on two-factor sign-in. You find it at the bottom of **“My account”**.



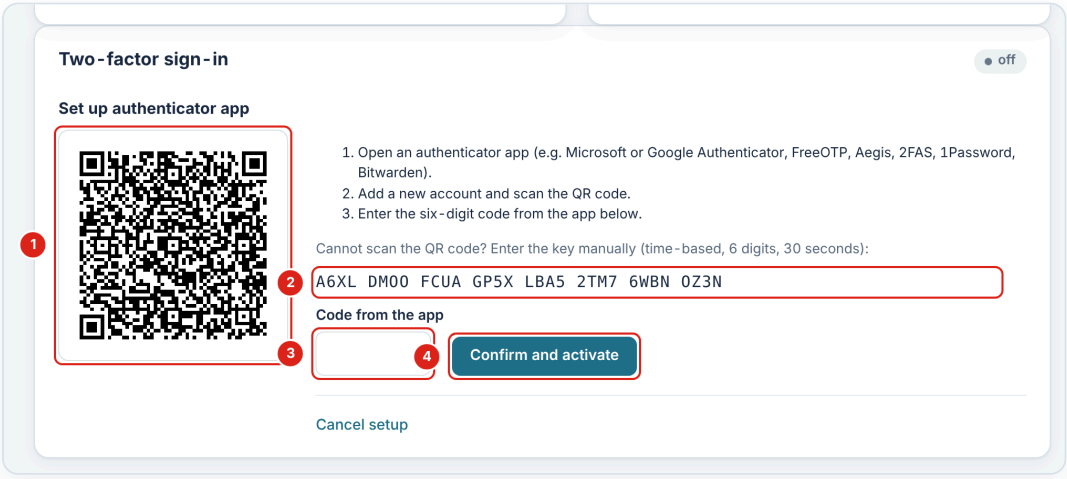
Choose how you receive the code

1. **“Set up app”** – the code comes from an app on your phone. This is the safest option and works without email. **Recommended.**
2. **“Send code”** – the code comes by email every time. To set it up, the gateway sends you a confirmation code that you enter there.

> **Is the code by email required?**
>
> Then the top right says “Code by email (required)”. You do not need to set anything up – the code arrives automatically at every sign-in. If you prefer the app, you can still set it up.

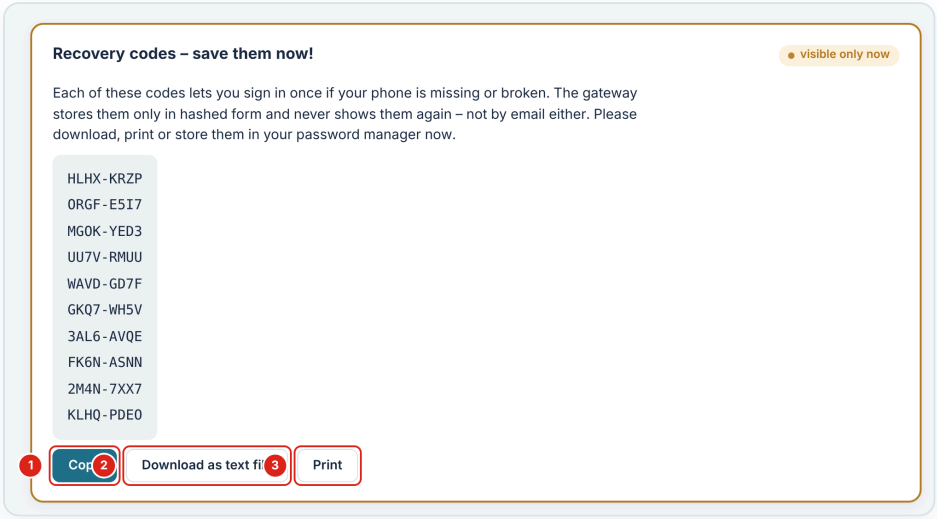
Setting up the authenticator app

Install an authenticator app on your phone, for example **Microsoft Authenticator**, **Google Authenticator**, **FreeOTP** or **Aegis**. Many password managers can do this too.



Scan the QR code with the app

1. Open the app, tap “Add account” (or “+”) and point the camera at the **QR code**.
2. If scanning does not work, type the **key** below it instead (type: time-based).
3. The app now shows a six-digit code that changes every 30 seconds. Type it into **Code from the app**.
4. Click **“Confirm and activate”**.

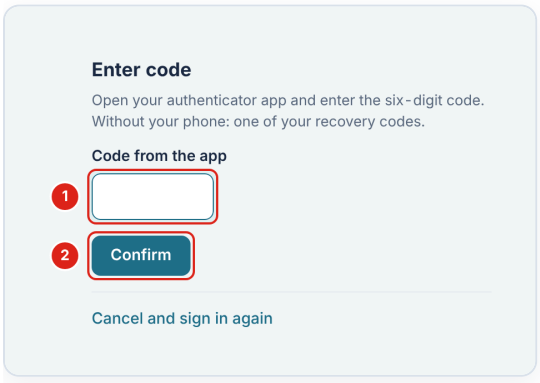


The recovery codes – shown only once!

Keep the recovery codes safe

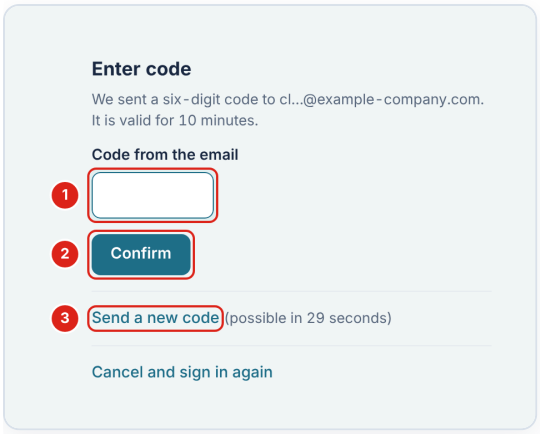
Right afterwards, the gateway shows ten **recovery codes** at the very top of the page. Each lets you sign in **once** if your phone is missing or broken. They are **not sent by email** and are never shown again. Save them right away: (1) **“Copy”** and paste them into your password manager, (2) **“Download as text file”** or (3) **“Print”**. Missed them? Under “My account” › “New recovery codes” you create new ones with a code from the app – the old ones become invalid.

How you sign in now



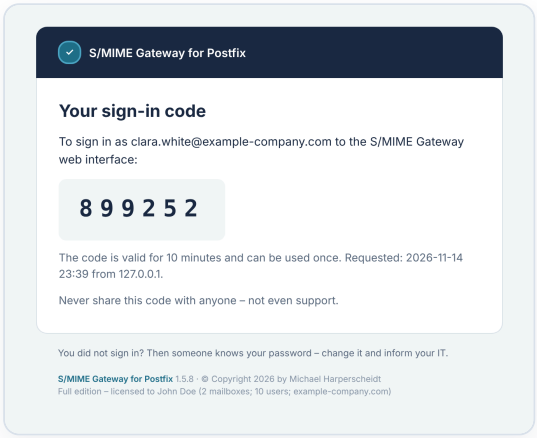
Second step with the app

1. After username and password, the page **Enter code** appears. Type the current code from your app (or a recovery code).
2. Click **“Confirm”**.



Second step with a code by email

1. With a code by email: open the email “Your sign-in code” and type the code.
2. Click **“Confirm”**.
3. No email? After half a minute you can click **“Send a new code”**. The code is valid for only a few minutes (usually 10) and only once.



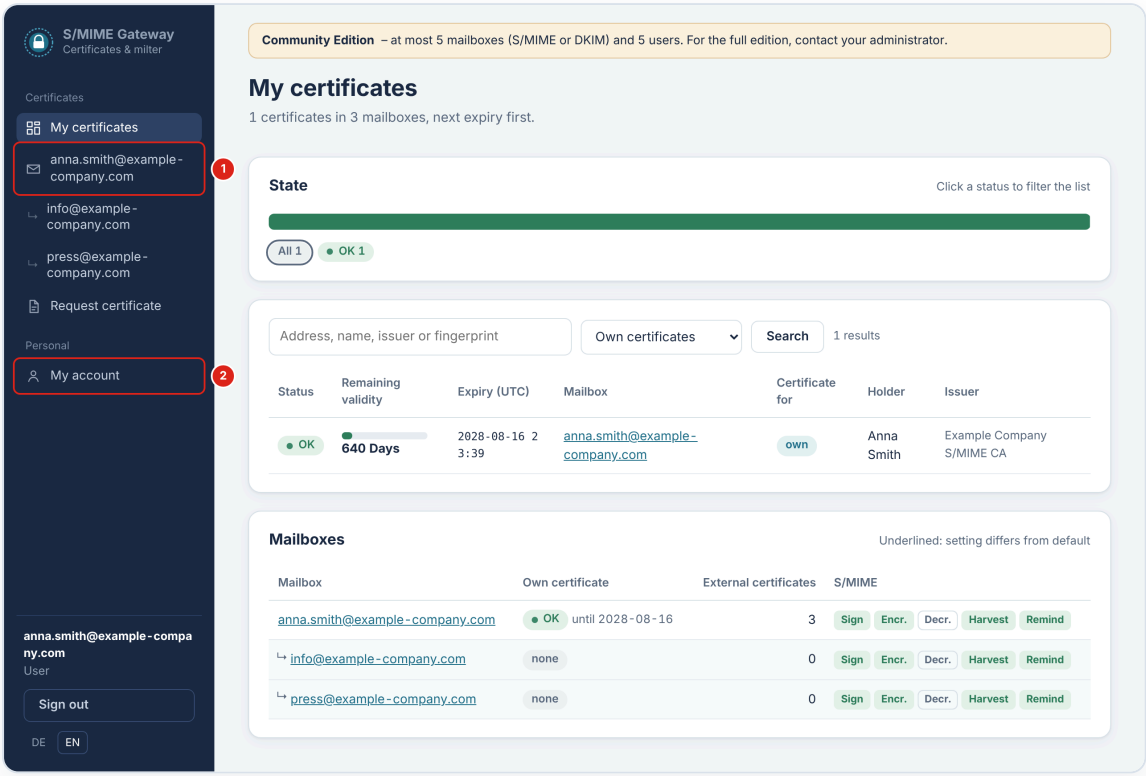
This is what the email with the code looks like

Never share it

Never share codes with anyone – not even on the phone with someone claiming to be “support”. If you receive a code without having signed in, someone knows your password: change it immediately and tell your administrator.

6 The start page

After signing in you see the start page **“My certificates”**. The menu is always on the left.



The start page. The menu on the left, the overview in the middle.

1. Here are your **mailboxes** (your email addresses). Clicking one opens the mailbox page. If your administrator has assigned further addresses to you – for example `press@` or `info@` – they are listed here, too.
2. **“My account”** – this is where you change your password.

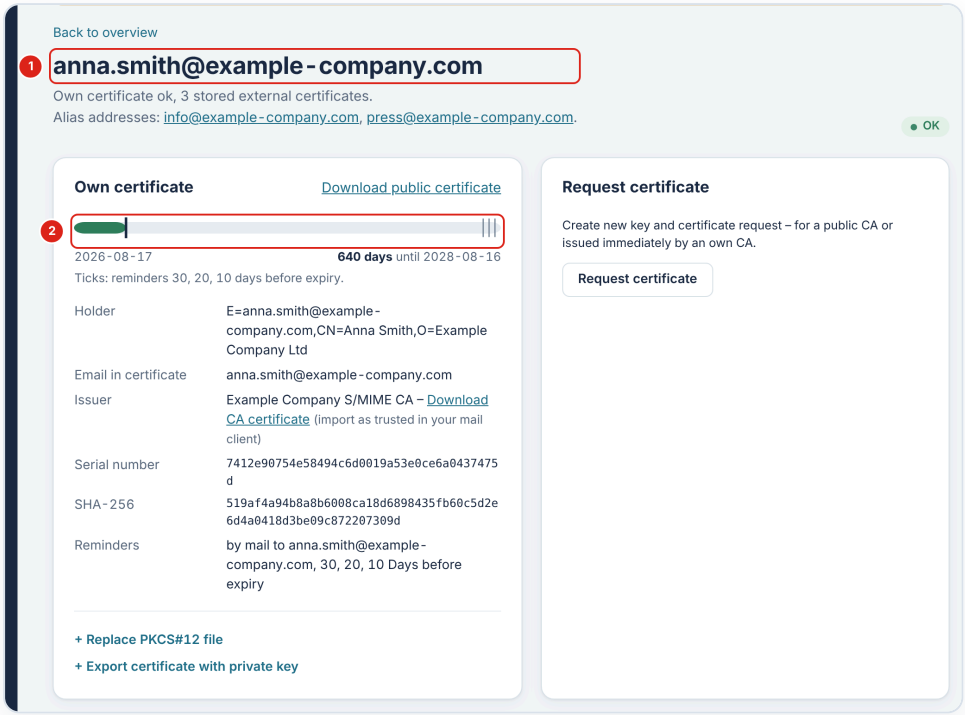
At the very top you sometimes see a yellow bar saying “Community Edition”. That only concerns your administrator and means: the free edition of the program is limited to a few mailboxes. You do not need to do anything.

In the middle is a list of your IDs with a coloured mark:

Mark	Meaning	What you do
● **OK**	Everything is fine.	Nothing.
● **Expiring soon / Critical**	Your ID expires in the next few weeks.	Request a new one soon (chapter 8).
● **Expired**	The ID is no longer valid. Your emails are no longer signed.	Request a new one right away or ask your administrator.

7 Looking at your mailbox

Click your email address in the menu on the left. You then see everything about your mailbox.



Your mailbox page

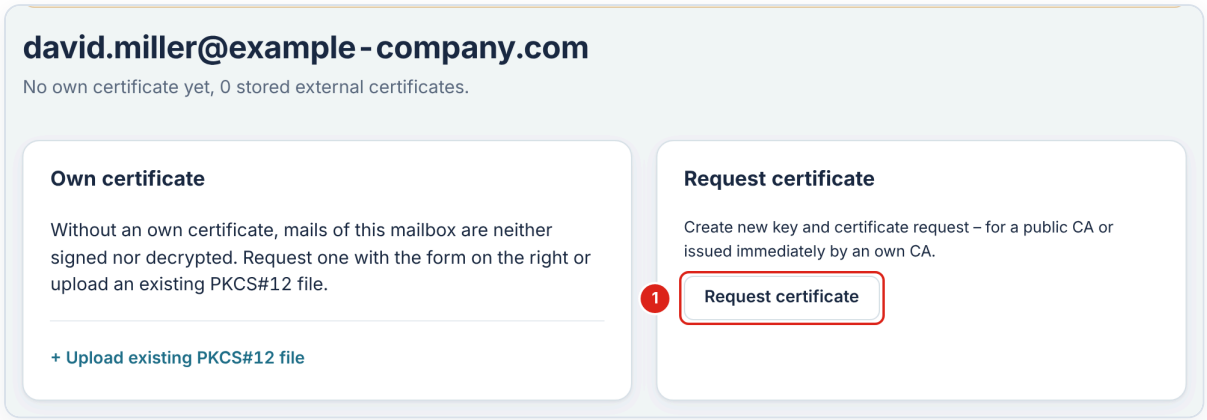
1. At the very top is the mailbox's **email address**. To the right, the coloured mark (green = all good). Below it are your alias addresses, if there are any.

2. The box **“Own certificate”** shows your ID: the bar shows how much longer it is valid. Next to it you see until when – for example “640 days until 2028-08-10”.

> **Good to know**
>
> The small lines at the end of the bar show when you will receive a reminder by email – for example 30, 20 and 10 days before it expires.

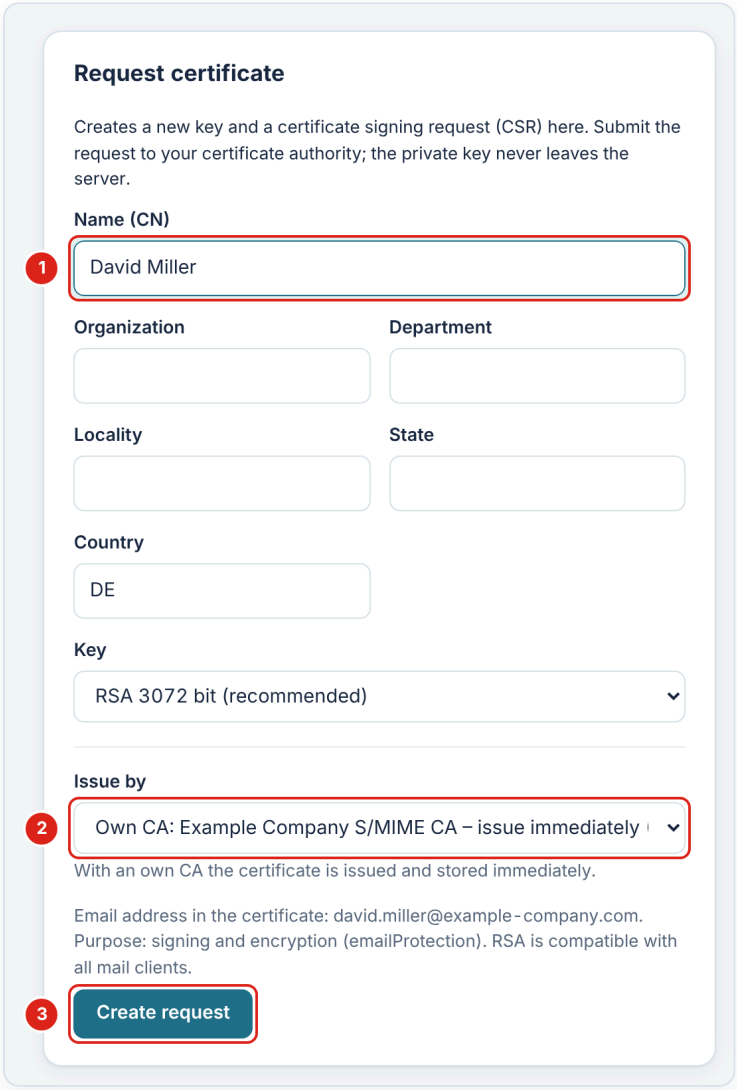
8 Getting a digital ID (certificate)

If your mailbox does not have an ID yet, the box **“Own certificate”** says: “Without an own certificate, mails of this mailbox are neither signed nor decrypted.” This is how you get one:



No ID yet

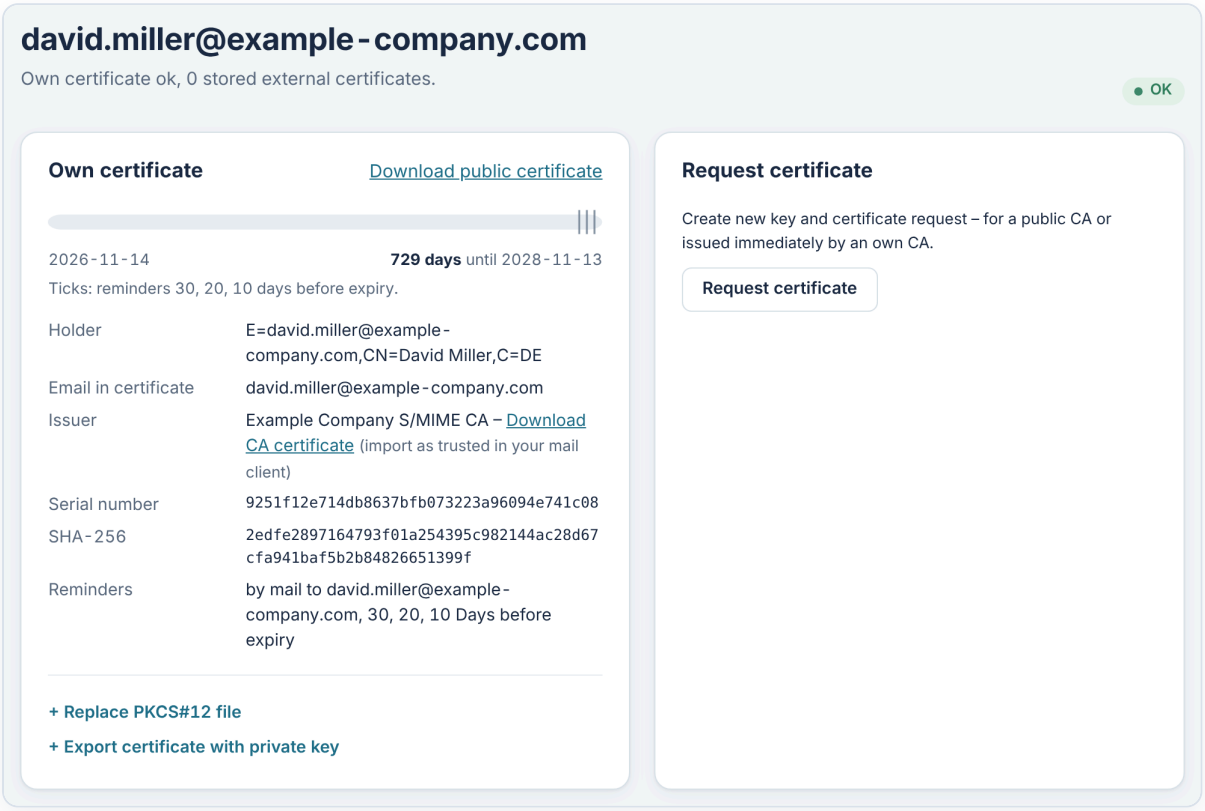
1 Click the button **“Request certificate”** on the right.



The request. Most fields may stay empty.

1. Type your first and last name under **Name (CN)**, for example *David Miller*. The other fields (organization, locality …) may stay empty – or your administrator has already filled them in.
2. Under **Issue by** choose the line that starts with “Own CA: …” and ends with “issue immediately”. If there is no such line, ask your administrator.
3. Click **“Create request”**. Done!

A few seconds later your ID is there. Your mailbox page now shows a green **OK** at the top right:

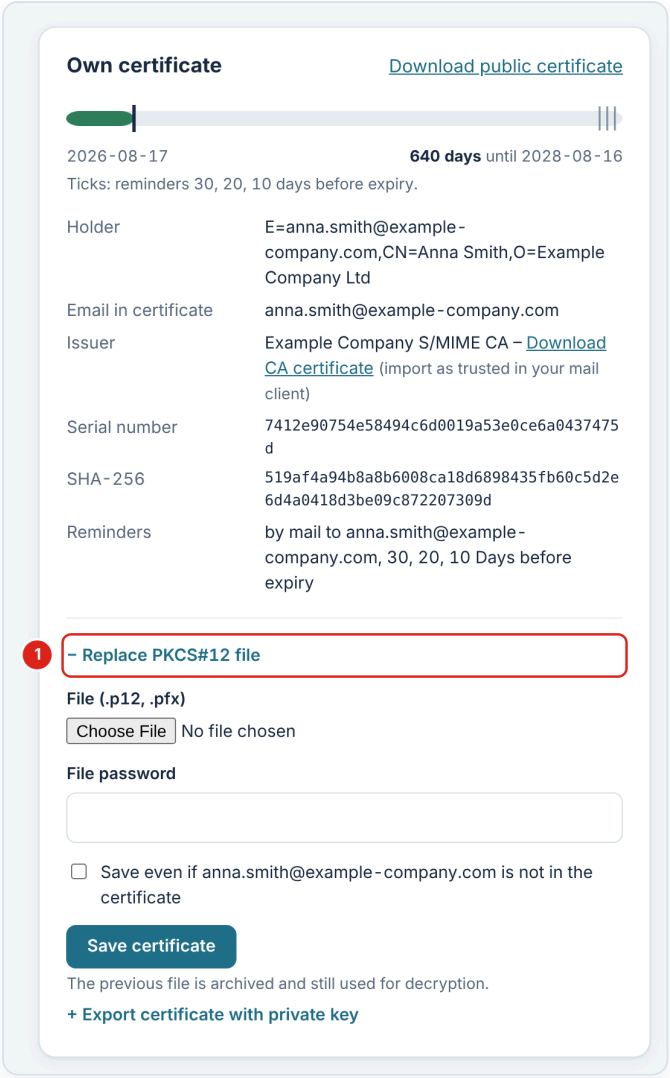


Done: the ID is there and valid for two years.

> **From now on everything runs by itself**
>
> Every email you send is signed automatically. If the gateway also knows the recipient's ID, it is sealed as well.

Did your IT department give you an ID file?

Sometimes you receive the ID as a file (ending `.p12` or `.pfx`) with a password. Then click **“Upload existing PKCS#12 file”** in the box **“Own certificate”** (or “Replace PKCS#12 file” if there already is an ID):

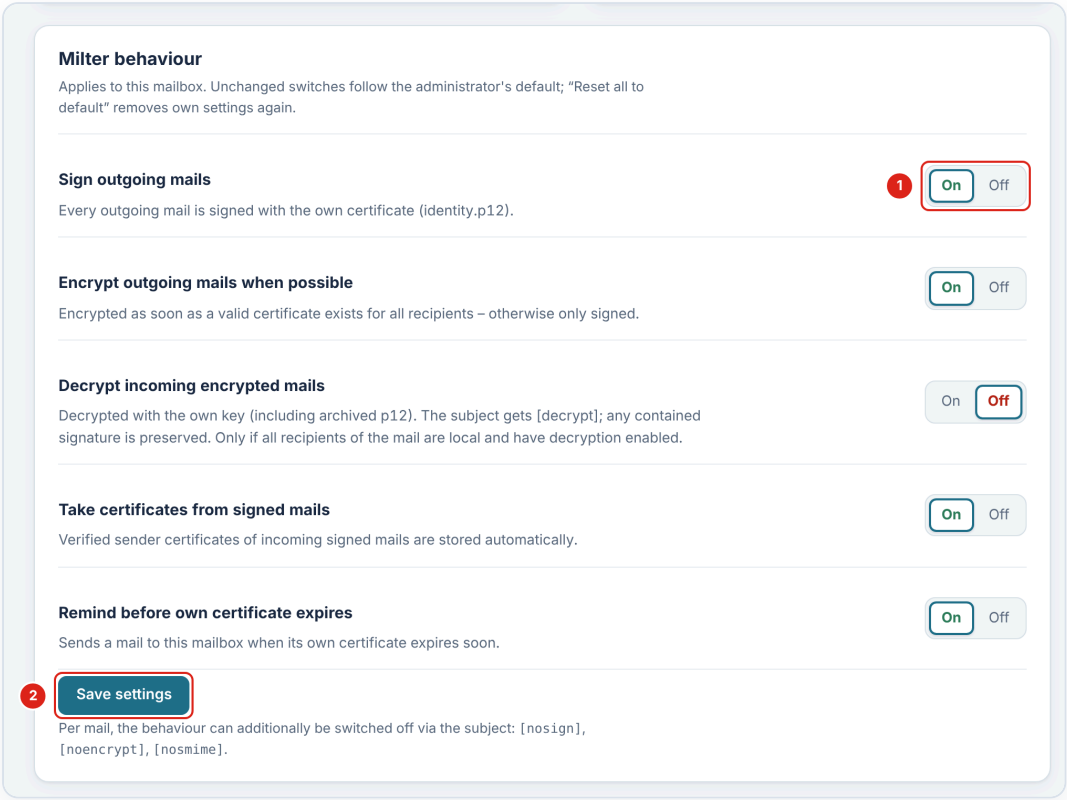


Uploading an ID file

1. Click the link. A small form opens. Choose the file there, type the file's password and click the save button.

9 Settings – what the switches mean

Further down on your mailbox page is the box **“Milter behaviour”**. (“Milter” is just another word for the gateway.) Every line has an **On / Off** switch.



The switches for your mailbox

1. Click **On** or **Off** to flip a switch. The selected value has a frame.
2. Then click **“Save settings”**. Only then does the change apply.

Switch	What it means
Sign outgoing mails	Your emails get your digital signature. Recommended: On.
Encrypt outgoing mails when possible	Emails are sealed if the recipient's ID is known. Otherwise only signed. Recommended: On.
Decrypt incoming encrypted mails	Sealed emails to you are opened before delivery, so you can read them in any program. The subject then contains `[decrypt]`. Ask your administrator whether you need this.
Take certificates from signed mails	The gateway remembers your contacts' IDs automatically. Recommended: On.
Remind before own certificate expires	You receive an email in good time before your ID expires. Recommended: On.

If in doubt: change nothing

Your administrator has preset sensible values. If a switch is grey and cannot be changed, the administrator has fixed it for everyone.

10 Switching something off for a single email

Sometimes you want to send a particular email without signature or unsealed – for example to an old device that cannot handle it. To do this, write a **magic word** into the subject of your email:

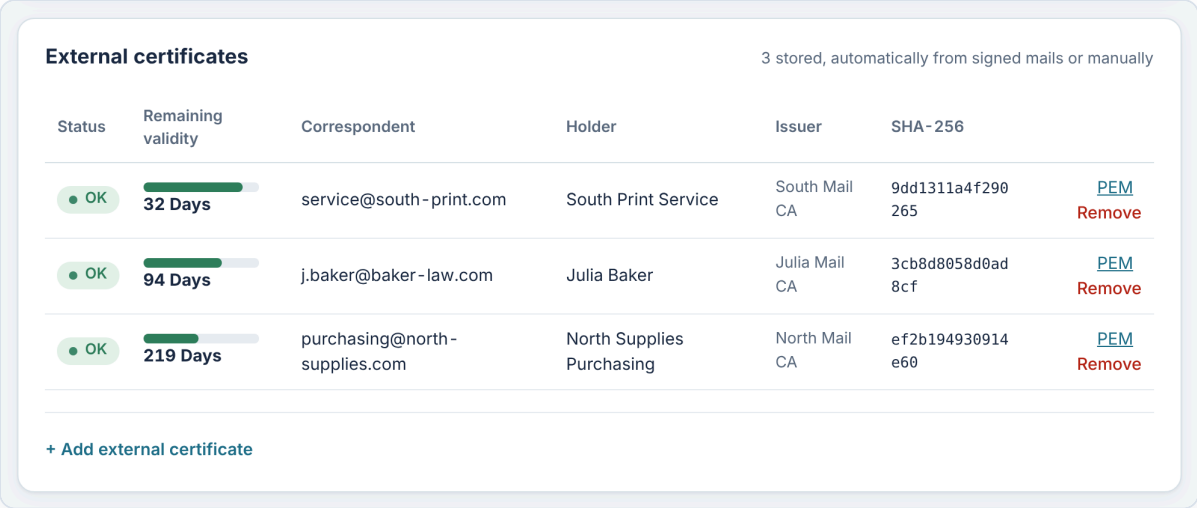
```
Subject: [noencrypt] Offer for Mrs Miller
```

Magic word in the subject	Effect for this one email
`[nosign]`	do not sign
`[noencrypt]`	do not seal (only sign)
`[nosmime]`	neither sign nor seal

The magic word is removed from the subject automatically before sending – the recipient does not see it. Mind the square brackets.

11 Your contacts' IDs

To seal an email, the gateway needs the recipient's ID. It gets it very easily: when someone sends you a **signed** email, the gateway stores their ID automatically. From then on your replies to this person are sealed.

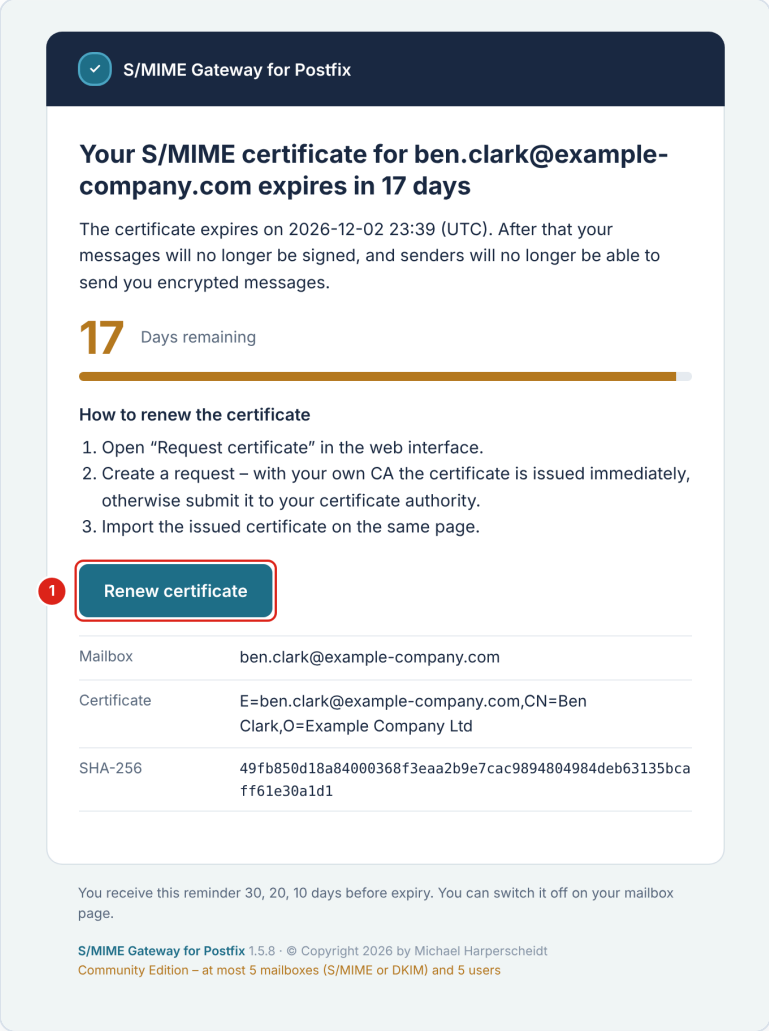


The collected IDs of your contacts (“external certificates”)

> **Tip**
>
> Want to write to someone encrypted right away? Ask them to send you a signed email first. After that it works automatically.

12 The reminder email

An ID is usually valid for one or two years. Shortly before it expires you receive an email like this:



The reminder: your ID expires soon.

1. Click **"Renew certificate"** in the email.
2. Sign in (chapter 3) and request a new ID – exactly as in chapter 8.

The old ID is kept, so you can still read old sealed emails.

13 Signing out and language



Bottom left in the menu

1. Click **“Sign out”** when you are finished – especially on someone else's or a shared computer.
2. Use **DE** and **EN** to switch between German and English.

If you do nothing for a longer time, the gateway signs you out by itself for security reasons. Then simply sign in again.

14 When something does not work

What happens	What you can do
I have forgotten my password.	Ask your administrator for a new one. They will send it to you by email.
My phone with the authenticator app is gone.	Sign in with a recovery code (chapter 5). If you have none left: your administrator can reset the app setup.
The code from the app is not accepted.	Check that the time on your phone is correct (switch on automatic time). Each code works only once – wait for the next one.
The email with the code does not arrive.	Check the spam folder; after half a minute click “Send a new code”.
Signing in is blocked.	Wait a few minutes and try again. If that does not help: ask your administrator.
Note “Community Edition: at most … users can sign in”.	The free edition is full. Your administrator can change that.
My mailbox shows “License limit” in a red box.	Your emails are currently not being signed. Let your administrator know.
A mailbox or address has disappeared from my list.	Your administrator has deleted it or assigned it to another account. Ask them if you still need it.
“Session ended – please sign in again.”	You were inactive for a while, or your account was changed. Simply sign in again.
The recipient says they cannot open my email.	Write `[noencrypt]` in the subject (chapter 10) and send it again.
My mark is red (“Expired”).	Request a new ID (chapter 8).
The subject contains `[decrypt]`.	All fine: the email was sealed and has been opened for you.

> **Your contact person**
>
> Your administrator helps you with all questions. They have the administrator guide.

15 Small glossary

Word	Simply explained
Administrator	The person who set up and looks after the gateway in your company.
Gateway	A program on the mail server that protects your emails automatically.
Mailbox	An email address, for example anna.smith@example-company.com.
Alias	An additional address that belongs to your mailbox, for example press@example-company.com.
Certificate	A digital ID for your mailbox. It is valid for a certain time.
Two-factor sign-in (MFA)	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.
Recovery code	A spare code for emergencies when the phone is missing. Each works once.
Signing	Signing digitally. The recipient sees that the email is genuine.
Encrypting	Putting the email “into a sealed envelope”. Only the recipient can read it.
Decrypting	Opening the envelope again.
External certificate	A contact's ID.
CA (certificate authority)	The “ID office” that issues IDs. Your company can have its own (“Own CA”).
PKCS#12 / .p12	A file containing an ID together with its secret key – always protected by a password.
S/MIME	The name of the worldwide standard for signed and sealed emails.

Copyright and license

© 2026 Michael Harperscheidt. All rights reserved.

This guide (“User 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 (see the administrator guide).

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