S/MIME Gateway for Postfix · Version 1.5.7

Das S/MIME Gateway einrichten und betreuen

Anleitung für Administratorinnen und Administratoren

Für wen ist diese Anleitung?

Für die Person, die das Gateway in der Firma betreut. Sie brauchen keine Vorkenntnisse über Verschlüsselung. Für die erste Installation auf dem Server (Kapitel 19) hilft Ihnen am besten Ihr IT-Dienstleister – alles andere erledigen Sie bequem im Internet-Programm.

So lesen Sie die Bilder: 1 Rote Kreise mit Zahlen zeigen, **wo** Sie klicken oder etwas eintragen. Die Zahl im Bild gehört zum gleichen Schritt im Text.

Die Bilder zeigen eine erfundene Beispiel-Firma („Beispiel-Firma GmbH“). Bei Ihnen stehen dort Ihre eigenen Namen und Adressen.

© 2026 Michael Harperscheidt. Alle Rechte vorbehalten. · S/MIME Gateway for Postfix 1.5.7 · Anleitung für Administratoren

Inhalt

1	Was macht das Gateway – und was ist Ihre Aufgabe?	
2	Anmelden	
3	Die Übersicht und das Menü	
4	Die ersten Schritte – Ihre Checkliste	
5	Mailserver eintragen	
6	Konten für Ihre Kollegen anlegen	
7	Postfächer und Aliase anlegen	NEU
8	Postfächer und Aliase löschen	NEU
9	Eigene Zertifizierungsstelle und Ausweise	
10	S/MIME-Einstellungen	
11	Erinnerungen und Info-Mails	
12	DKIM – der Echtheits-Stempel für Ihre Domain	
13	Mail-DNS – SPF, DMARC, MTA-STS und Co. prüfen	NEU
14	Statistik und täglicher Bericht	
15	Alias-Adressen	
16	Zwei-Faktor-Anmeldung (MFA)	NEU
17	Die Lizenz	
18	Wenn die Lizenz nicht mehr reicht	
19	Installieren und aktualisieren	
20	Wenn etwas nicht klappt	
21	Kleines Wörterbuch	
	Copyright und Lizenz	

1 Was macht das Gateway – und was ist Ihre Aufgabe?

Das Gateway sitzt auf dem Mail-Server Ihrer Firma, wie eine Poststelle. Jede E-Mail läuft hindurch.



Ausgehende E-Mails

werden digital unterschrieben und – wenn der Empfänger bekannt ist – verschlossen.



Eingehende E-Mails

werden auf Wunsch geöffnet (entschlüsselt). Ausweise der Absender werden gesammelt.



DKIM

Jede E-Mail Ihrer Domain bekommt einen Echtheits-Stempel. Das schützt vor dem Spam-Ordner.

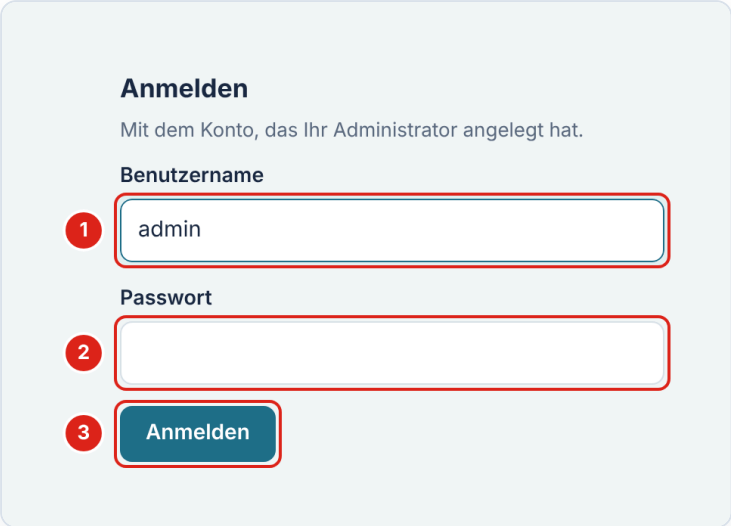
Ihre Kollegen merken davon fast nichts: Sie schreiben weiter in ihrem gewohnten E-Mail-Programm. Ihre Aufgaben als Administrator sind:

- das Gateway einmal einrichten (Kapitel 4),
- Konten und Postfächer anlegen, Ausweise ausstellen – und nicht mehr benötigte Postfächer löschen (Kapitel 6 bis Kapitel 9),
- ab und zu auf die Übersicht, die Info-Mails und den täglichen Bericht schauen (Kapitel 3, Kapitel 11 und Kapitel 14),
- sich um die Lizenz kümmern (Kapitel 17 und Kapitel 18).

> **Zwei Arten von Personen**
>
> **Administratoren** sehen und ändern alles. **Benutzer** sehen nur ihre eigenen Postfächer. Für Benutzer gibt es eine eigene, einfache Anleitung – geben Sie sie Ihren Kollegen.

2 Anmelden

Öffnen Sie die Adresse des Gateways in Ihrem Internet-Programm (zum Beispiel `https://mail.beispiel-firma.de/smime`).



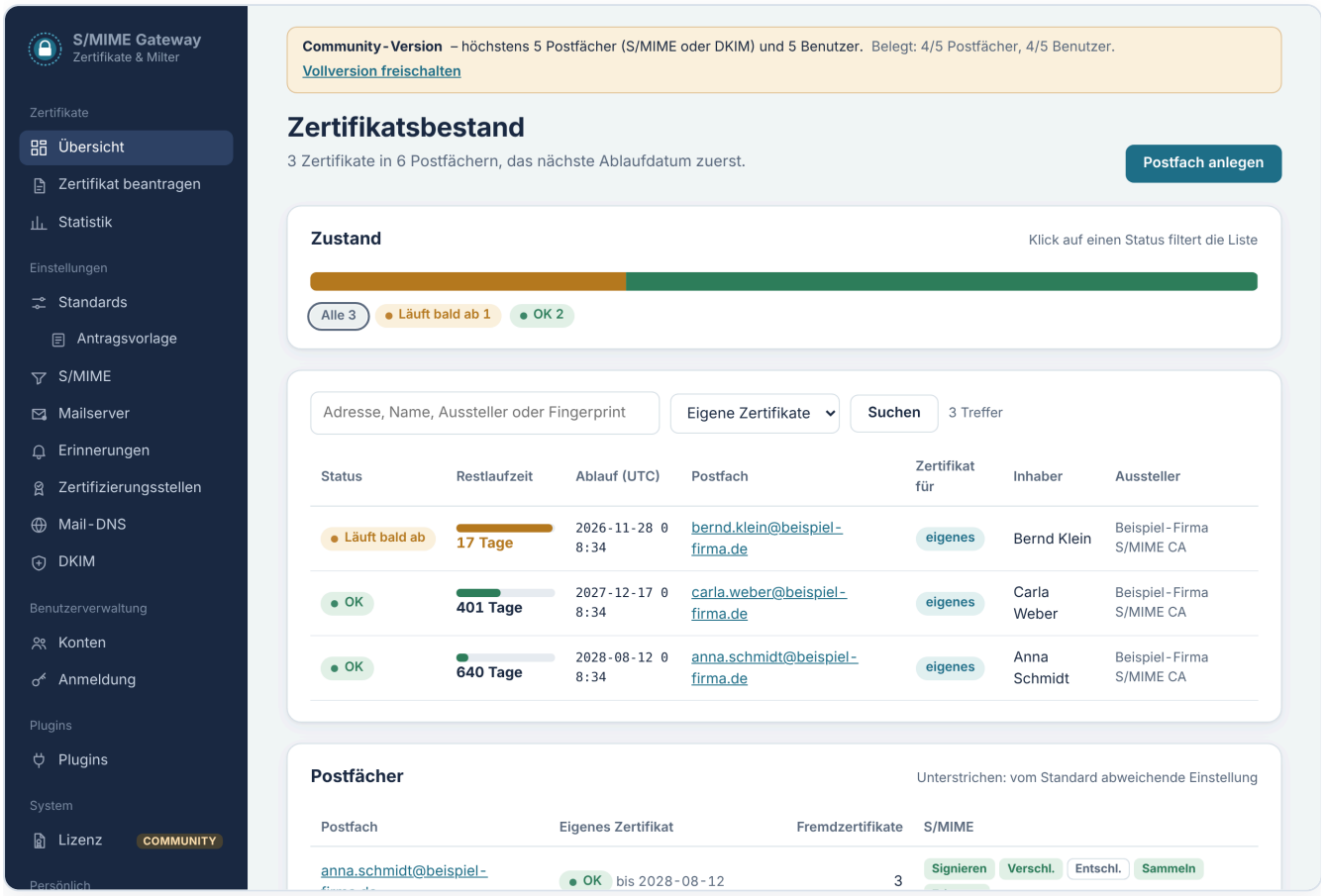
Anmelden als Administrator

1. Benutzername eintragen, zum Beispiel **admin**.
2. Passwort eintragen.
3. Auf **„Anmelden“** klicken.

Der Notfallzugang

In der Konfigurationsdatei auf dem Server gibt es einen Notfallzugang (Einstellung `admin_user` und `admin_password_hash`). Er funktioniert immer – auch wenn Sie sich sonst ausgesperrt haben. Bewahren Sie dieses Passwort sicher auf, zum Beispiel in einem versiegelten Umschlag im Tresor.

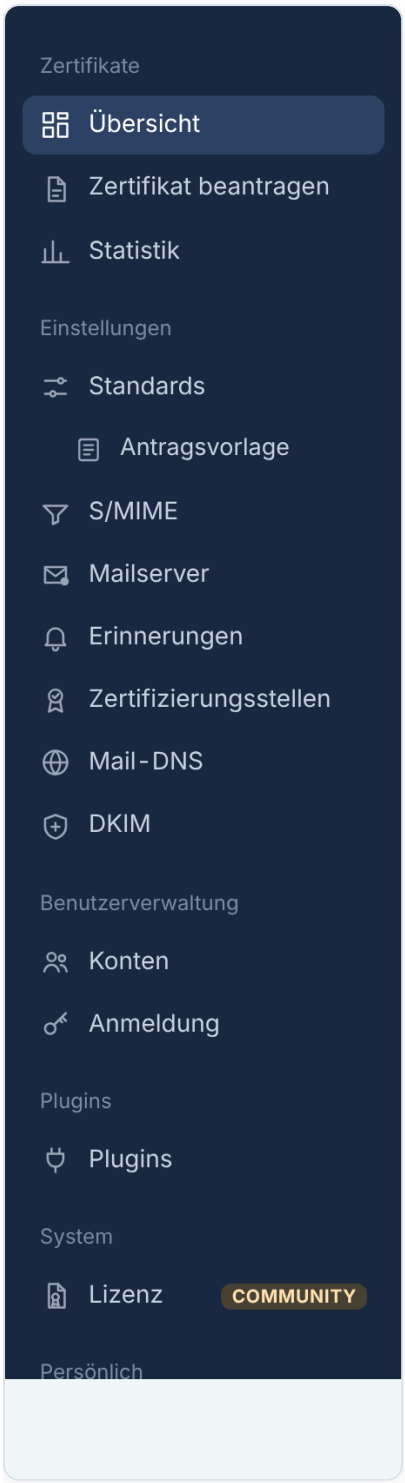
3 Die Übersicht und das Menü



Die Übersicht nach dem Anmelden

Die Übersicht zeigt alle Ausweise aller Postfächer. Die farbigen Zeichen bedeuten: ● **OK** alles gut, ● **Läuft bald ab** bald erneuern, ● **Abgelaufen** sofort handeln. Ein Klick auf eine Farbe zeigt nur diese Einträge.

Weiter unten steht die Liste **Postfächer**. Aliase stehen direkt unter ihrem Postfach und sind eingerückt (↳) NEU in 1.5.5 – so sehen Sie auf einen Blick, welche Adressen zusammengehören. Das gilt für alle Listen mit Postfächern, auch für die Konten, die Statistik, die Lizenzseite und den täglichen Bericht. Oben steht der gelbe Streifen „Community-Version“: Sie nutzen die kostenlose Ausgabe (mehr in Kapitel 17).



Das Menü links

Menüpunkt	Wofür?
Übersicht	alle Ausweise und Postfächer auf einen Blick, neues Postfach anlegen
Zertifikat beantragen	einen Ausweis für ein Postfach beantragen
Statistik	Zahlen und Grafiken, täglicher Bericht
Standards	Grundeinstellungen für alle Postfächer
S/MIME	Regeln für das Unterschreiben und Verschließen
Mailserver	Absender für E-Mails des Gateways
Erinnerungen	Mails vor Ablauf der Ausweise, Info-Mails zu Postfächern
Zertifizierungsstellen	die eigene „Ausweisbehörde“
DKIM	Echtheits-Stempel für Ihre Domain
MFA-Einstellungen	Zwei-Faktor-Anmeldung (nur bei aktivem Plugin MFA)
Konten	wer sich anmelden darf, Alias-Adressen
Lizenz	Ausgabe, Grenzen, Lizenzdatei

4 Die ersten Schritte – Ihre Checkliste

Nach der Installation gehen Sie diese Punkte einmal der Reihe nach durch. Haken Sie ab, was erledigt ist:

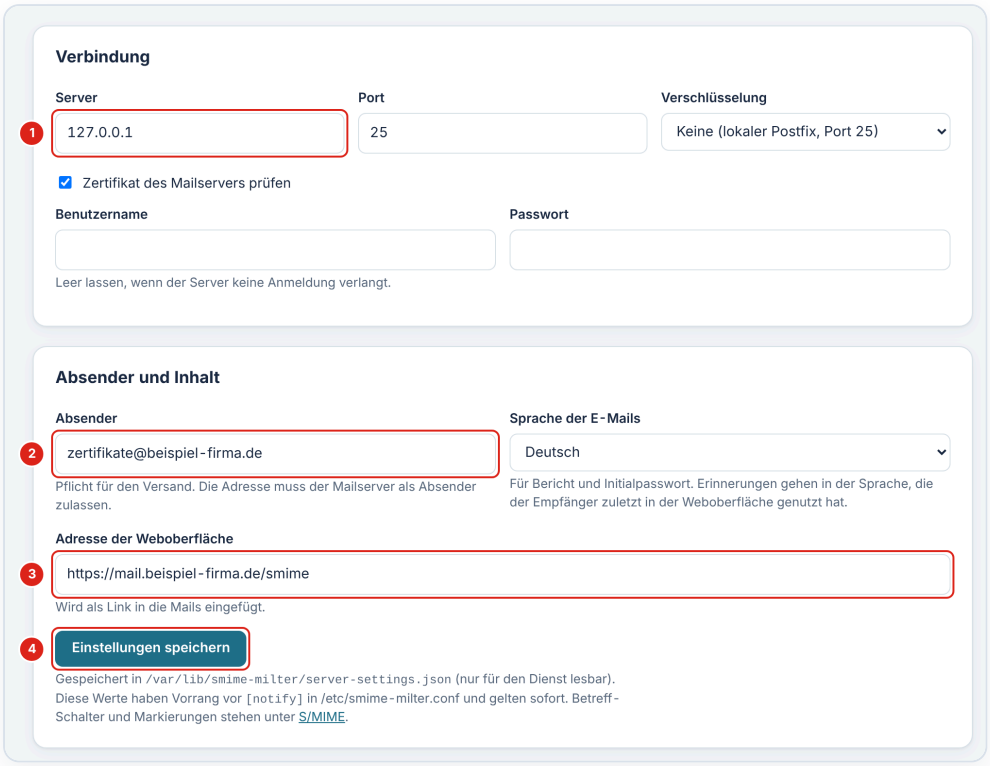
✓	Was	Wo	Kapitel
☐	Absender-Adresse und Webadresse eintragen, Testmail schicken	Mailserver	5
☐	Ihre E-Mail-Domain(s) eintragen	S/MIME	10
☐	Eigene Zertifizierungsstelle anlegen	Zertifizierungsstellen	9
☐	Konten für Kollegen anlegen	Konten	6
☐	Weitere Postfächer und Aliase anlegen (zum Beispiel `info@`)	Übersicht	7
☐	Erinnerungen einschalten, Empfänger der Info-Mails prüfen	Erinnerungen	11
☐	DKIM-Schlüssel erzeugen und im DNS eintragen	DKIM	12
☐	Täglichen Bericht einschalten	Statistik	14
☐	Empfohlen: Zwei-Faktor-Anmeldung einschalten	Plugins › MFA	16
☐	Bei mehr als 5 Postfächern: Lizenz anfragen	Lizenz	17

Keine Angst vor Fehlern

Alle Einstellungen lassen sich jederzeit wieder ändern. Nach jedem Speichern erscheint oben ein grüner Hinweis. Nur das Löschen eines Postfachs (Kapitel 8) ist endgültig – dafür fragt das Gateway zweimal nach.

5 Mailserver eintragen

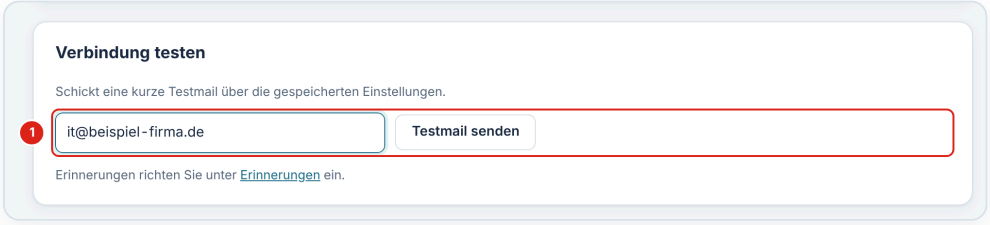
Damit das Gateway E-Mails verschicken kann (Zugangsdaten, Erinnerungen, Info-Mails, Berichte), braucht es einen Absender. Klicken Sie im Menü auf **„Mailserver“**.



Die Seite „Mailserver“

1. **Server**: der Mail-Server, über den verschickt wird. Läuft das Gateway auf dem Mail-Server selbst, bleibt hier `127.0.0.1` stehen.
2. **Absender**: die Adresse, von der die E-Mails kommen, zum Beispiel `zertifikate@beispiel-firma.de`.
3. **Adresse der Weboberfläche**: die Adresse, unter der Ihre Kollegen das Gateway öffnen. Sie steht später als Knopf in den E-Mails.
4. Klicken Sie auf **„Einstellungen speichern“**.

Eine Testmail schicken

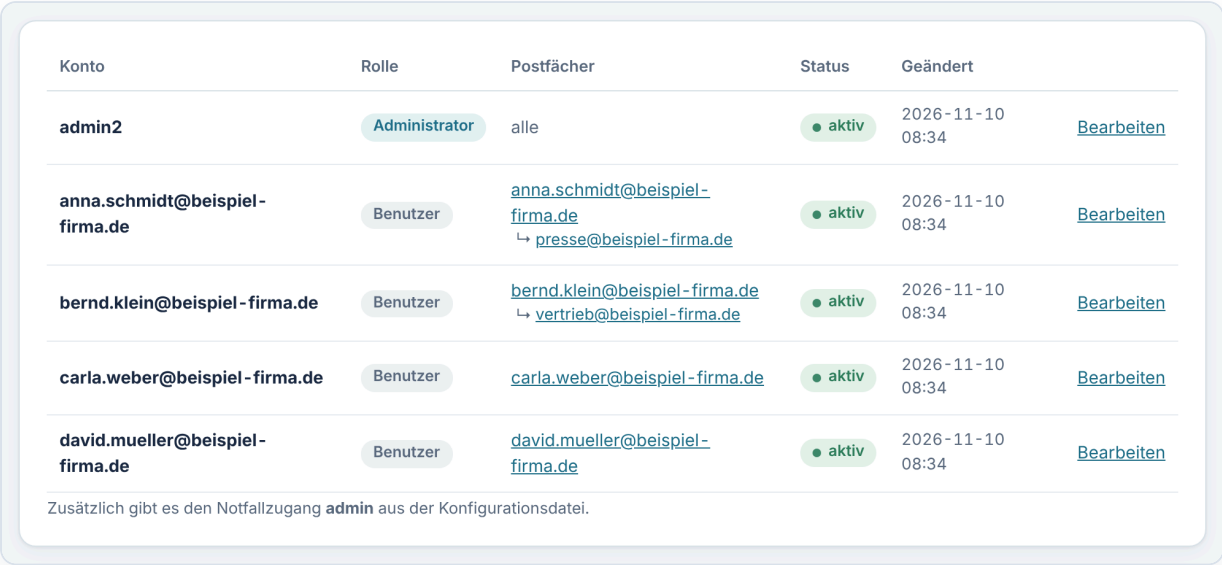


Eine Testmail schicken

1. Tragen Sie Ihre eigene Adresse ein und klicken Sie auf **„Testmail senden“**. Kommt die E-Mail an, ist alles richtig.

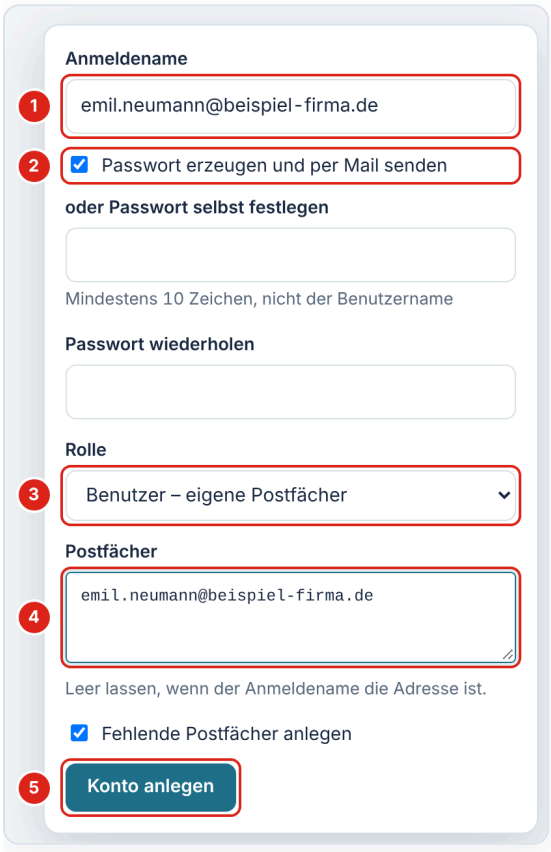
6 Konten für Ihre Kollegen anlegen

Klicken Sie im Menü auf **„Konten“**. Sie sehen alle Personen, die sich anmelden dürfen.



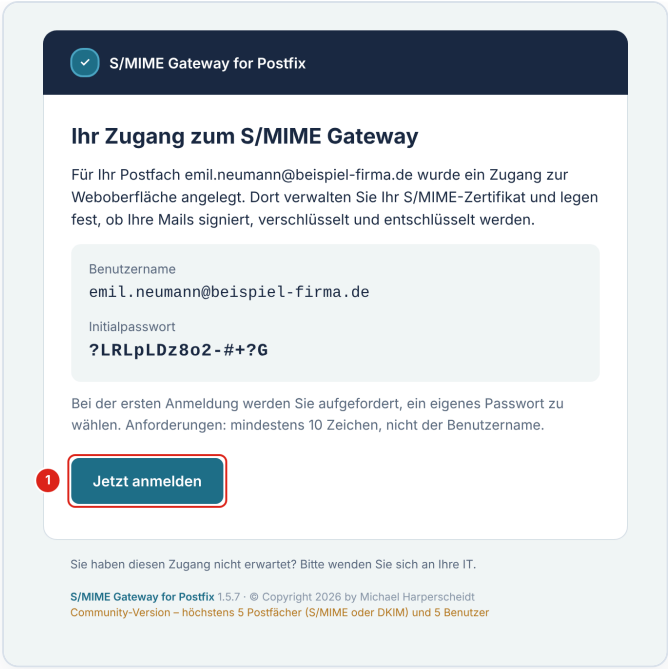
Die Liste der Konten

Klicken Sie oben rechts auf **„Konto anlegen“**. Es öffnet sich ein kleines Fenster:



Ein neues Konto anlegen

1. **Anmeldename**: am besten die E-Mail-Adresse des Kollegen, zum Beispiel *emil.neumann@beispiel-firma.de*.
2. Lassen Sie **„Passwort erzeugen und per Mail senden“** angehakt. Dann bekommt der Kollege eine E-Mail mit seinem ersten Passwort – Sie müssen sich keines ausdenken.
3. **Rolle**: „Benutzer – eigene Postfächer“ für normale Kollegen. „Administrator – alles“ nur für Personen, die alles verwalten sollen.
4. **Postfächer**: welche E-Mail-Adressen der Kollege verwalten darf. Leer lassen, wenn der Anmeldename schon die Adresse ist.
5. Auf **„Konto anlegen“** klicken. Fertig – der Kollege bekommt sofort seine E-Mail.



So sieht die E-Mail aus, die Ihr Kollege bekommt

Passwort vergessen?

Klicken Sie in der Liste beim Konto auf **„Bearbeiten“**. Dort können Sie ein neues Passwort per E-Mail schicken, das Konto sperren oder die Rolle ändern.

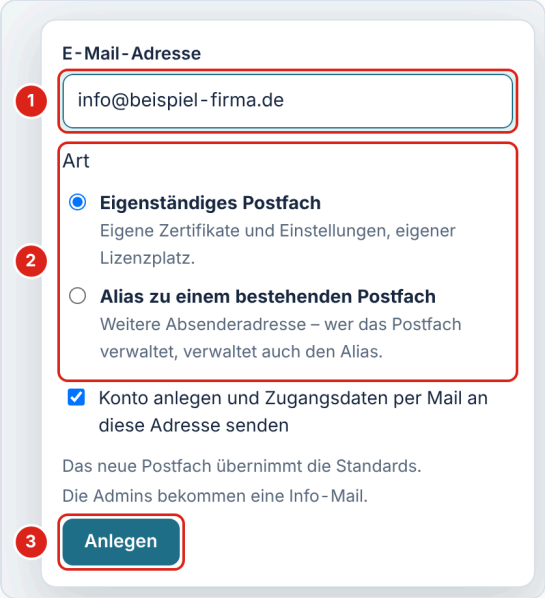
Grenze der kostenlosen Ausgabe

In der Community-Version dürfen sich höchstens **5 Benutzer** anmelden. Ein Administrator-Konto (das älteste) und der Notfallzugang zählen nicht mit. Weitere Administrator-Konten zählen mit.

7 Postfächer und Aliase anlegen NEU in 1.5.3

Ein **Postfach** ist eine E-Mail-Adresse mit eigenen Ausweisen und Einstellungen. Ein **Alias** ist eine weitere Absenderadresse, die zu einem Postfach gehört – zum Beispiel `info@beispiel-firma.de`, die Anna mitbetreut. Wer das Postfach verwaltet, verwaltet auch den Alias.

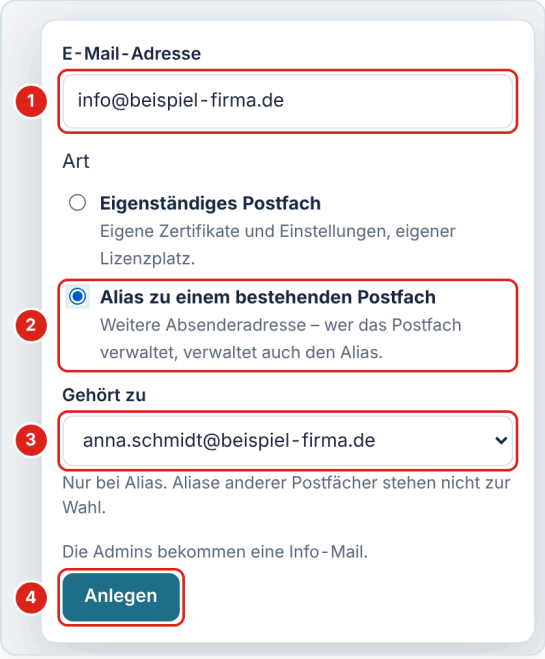
Klicken Sie in der **„Übersicht“** oben rechts auf **„Postfach anlegen“**. Das Gateway fragt Sie jetzt, was die Adresse werden soll:



Ein eigenständiges Postfach anlegen

Eigenständiges Postfach

1. Die **E-Mail-Adresse** eintragen.
2. Bei **Art** „Eigenständiges Postfach“ wählen. Das Postfach bekommt eigene Ausweise, eigene Einstellungen und belegt einen eigenen Lizenzplatz. Mit dem Haken darunter legen Sie gleich ein Konto an und schicken die Zugangsdaten an diese Adresse.
3. Auf **„Anlegen“** klicken.



Eine Adresse als Alias anlegen

Alias zu einem bestehenden Postfach

1. Die **E-Mail-Adresse** des Alias eintragen, zum Beispiel `info@beispiel-firma.de`.
2. „Alias zu einem bestehenden Postfach“ wählen.
3. Bei **Gehört zu** das Postfach auswählen, zu dem der Alias gehört. In der Liste stehen nur echte Postfächer – ein Alias kann nicht zu einem anderen Alias gehören.
4. Auf **„Anlegen“** klicken.

Was das Gateway dabei prüft

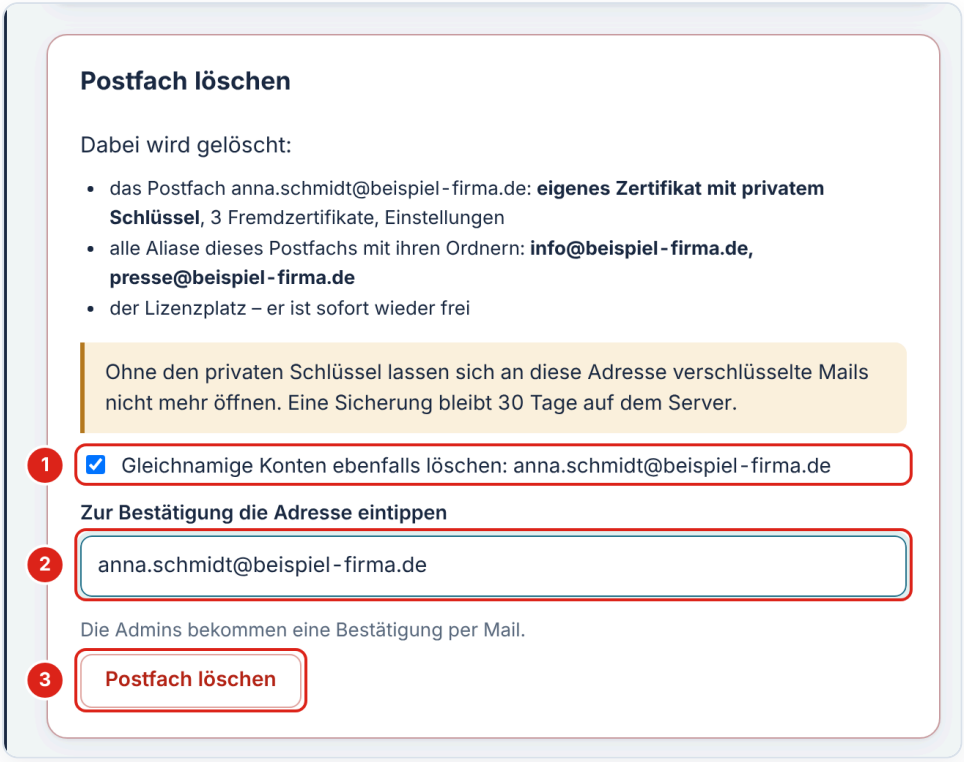
Die Adresse muss zu Ihren Domains gehören. Hat die Adresse selbst schon Aliase oder ist sie bereits Alias eines anderen Postfachs, lehnt das Gateway ab und sagt warum. Hat die Adresse schon einen eigenen Ausweis oder ein eigenes Konto, bekommen Sie einen Hinweis – beides bleibt erhalten.

Sie bekommen eine Info-Mail

Bei **jedem** neuen Postfach und Alias schickt das Gateway Ihnen eine kurze Info-Mail – auch dann, wenn es eine Adresse im laufenden Betrieb von selbst lernt (zum Beispiel, weil eine unterschriebene E-Mail an eine neue Adresse ankommt). So wissen Sie immer, was dazugekommen ist. Mehr in Kapitel 11.

8 Postfächer und Aliase löschen NEU in 1.5.3

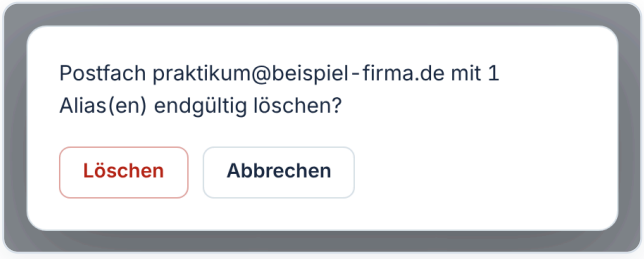
Ein Postfach wird nicht mehr gebraucht, zum Beispiel weil eine Kollegin die Firma verlassen hat? Dann löschen Sie es. Öffnen Sie dazu das Postfach (Klick auf die Adresse in der Übersicht) und gehen Sie ganz nach unten zum roten Kasten **„Postfach löschen“**. Bei einem Alias heißt er **„Alias löschen“**.



Unten auf der Seite des Postfachs

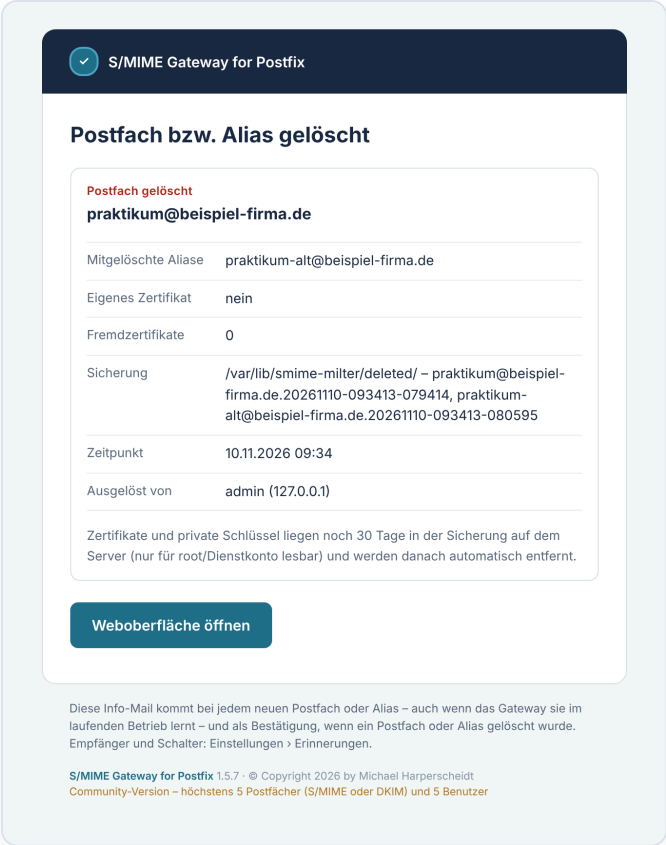
Oben im Kasten steht, was alles gelöscht wird: der Ausweis mit dem geheimen Schlüssel, die gesammelten Ausweise der Gesprächspartner, die Einstellungen – und **alle Aliase** des Postfachs. Steht das Postfach in anderen Konten, wird es dort nur entfernt; die Konten bleiben.

1. **Gleichnamige Konten ebenfalls löschen**: Gibt es ein Konto mit genau dieser Adresse als Anmeldename, wird es mitgelöscht. Ihr eigenes Konto und das letzte Administrator-Konto werden nie gelöscht.
2. Tippen Sie zur Sicherheit die **Adresse** genau ab.
3. Klicken Sie auf **„Postfach löschen“** und bestätigen Sie die Rückfrage mit **„Löschen“**.



Die Rückfrage vor dem Löschen

Danach ist der Lizenzplatz sofort wieder frei, und Sie bekommen eine **Bestätigung per E-Mail**:



Die Bestätigung: was gelöscht wurde, wann und von wem

Eine Sicherung für 30 Tage

Ohne den geheimen Schlüssel lassen sich alte, verschlossene E-Mails an diese Adresse nicht mehr öffnen. Deshalb legt das Gateway den Ordner des Postfachs noch **30 Tage** in eine Sicherung auf dem Server (`/var/lib/smime-milter/deleted/` , nur für das Dienstkonto lesbar). Danach wird sie automatisch entfernt. Brauchen Sie in dieser Zeit etwas zurück, hilft Ihr IT-Dienstleister.

Nur den Alias lösen, nicht löschen

Unter **„Konten“** › **„Alias-Adressen“** gibt es bei jedem Alias auch **„Löschen“**. Das löst nur die Zuordnung; der Ordner und die Ausweise der Adresse bleiben erhalten. Auch dafür bekommen Sie eine Bestätigung.

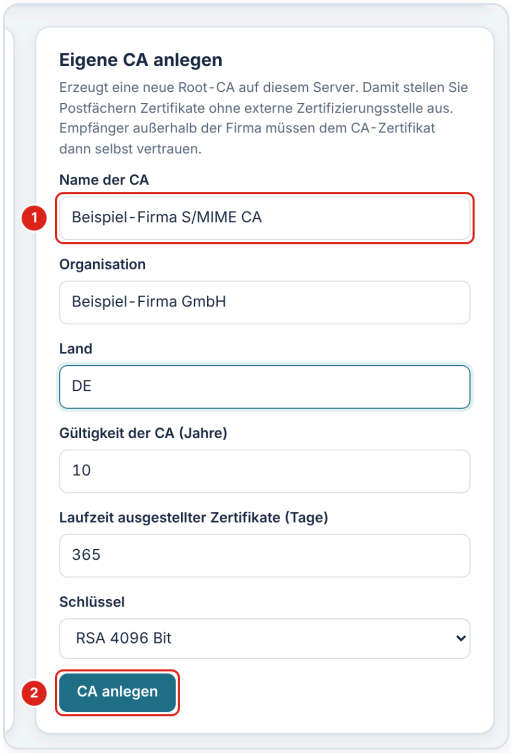
Kommt das Postfach wieder?

Kommt später wieder eine unterschriebene E-Mail an die gelöschte Adresse, legt das Gateway sie neu (leer) an – und schickt Ihnen eine Info-Mail. Sperren Sie unbekannte Adressen deshalb am besten schon im Mail-Server.

9 Eigene Zertifizierungsstelle und Ausweise

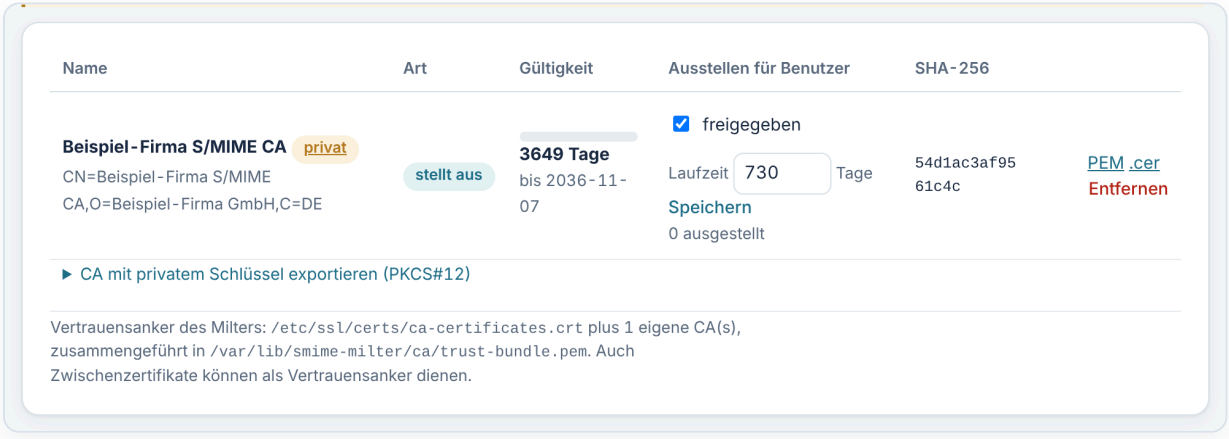
Eine **Zertifizierungsstelle (CA)** ist wie eine Ausweisbehörde. Mit einer eigenen CA stellt das Gateway Ihren Kollegen die Ausweise selbst aus – sofort und kostenlos. (Alternativ können Sie Ausweise bei einem öffentlichen Anbieter kaufen; die werden von fremden Firmen ohne Zusatzschritt anerkannt.)

Klicken Sie im Menü auf **„Zertifizierungsstellen“**.



Eine eigene CA anlegen

1. Tragen Sie bei **Name der CA** einen Namen ein, zum Beispiel *Beispiel-Firma S/MIME CA*, und füllen Sie **Organisation** und **Land** aus. Die übrigen Felder können so bleiben.
2. Klicken Sie auf **„CA anlegen“**.



Die fertige CA in der Liste. „Freigegeben“ bedeutet: Auch Benutzer dürfen sich damit selbst Ausweise ausstellen.

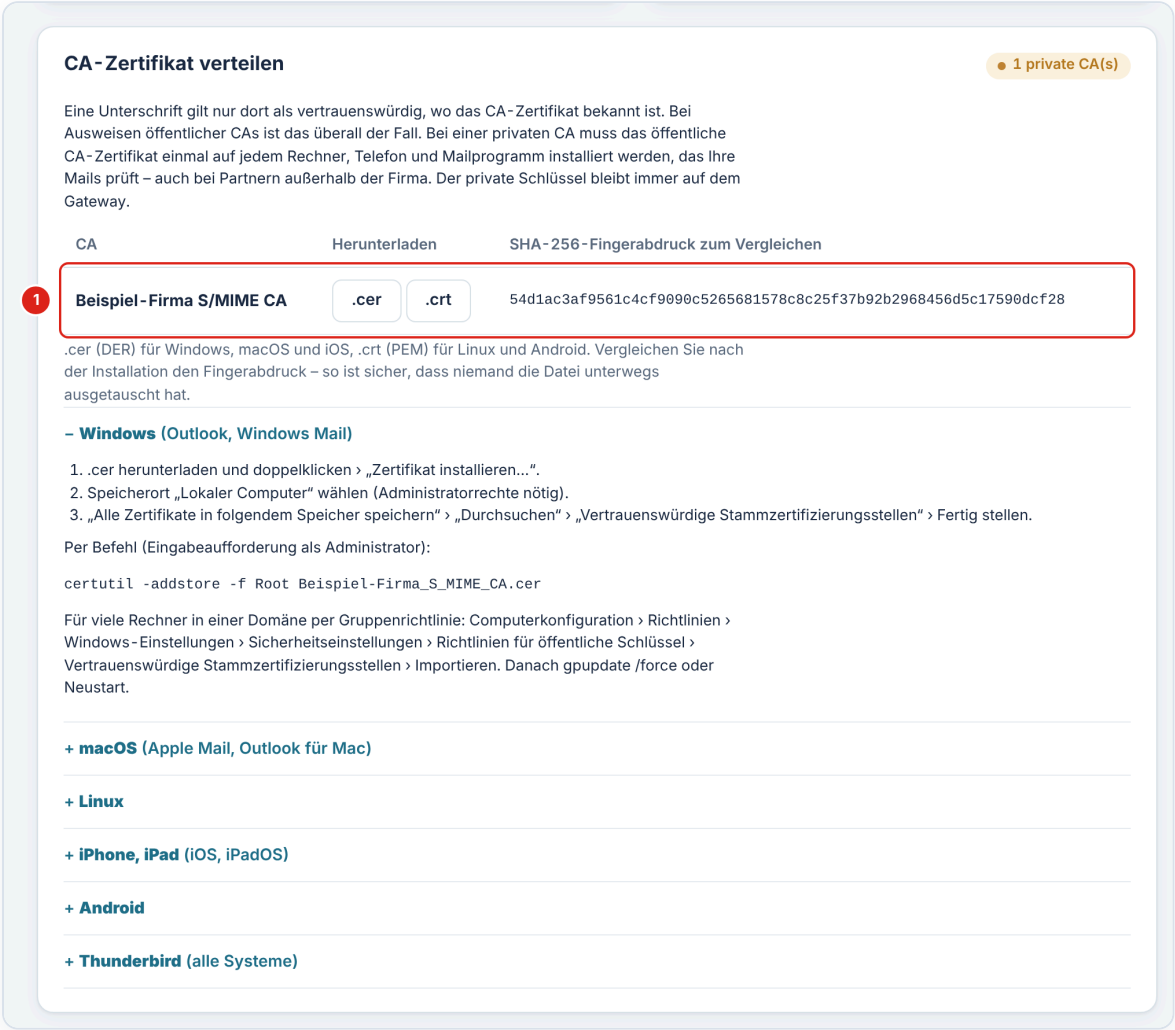
Einem Kollegen einen Ausweis geben

Öffnen Sie das Postfach (über die Übersicht oder **„Zertifikat beantragen“** im Menü) und gehen Sie genau so vor wie in der Anleitung für Benutzer, Kapitel 8: Name eintragen, bei „Ausstellen durch“

die eigene CA wählen, **„Antrag erzeugen“**.

Das CA-Zertifikat verteilen NEU in 1.5.6

Ihre eigene CA ist eine **private CA**: Kein Rechner und kein Telefon kennt sie von Haus aus. Bis das CA-Zertifikat dort installiert ist, zeigen Outlook, Apple Mail, Thunderbird und Co. die Unterschriften Ihrer Kollegen als „nicht vertrauenswürdig“ an. Das Gateway kennzeichnet private CAs in der Liste mit **privat** und erinnert Sie oben auf der Seite daran, bis Sie es erledigt haben.



Der Abschnitt „CA-Zertifikat verteilen“ mit Anleitung je System

1. Laden Sie das CA-Zertifikat herunter: **.cer** für Windows, macOS, iPhone und iPad, **.crt** für Linux und Android. Es enthält keinen geheimen Schlüssel und darf frei weitergegeben werden.

Darunter steht für jedes System eine Schritt-für-Schritt-Anleitung zum Aufklappen – für Windows auch mit dem Befehl `certutil` und dem Weg über eine Gruppenrichtlinie, für macOS mit `security add-trusted-cert`, für Linux je Distribution, für iPhone/iPad (Profil installieren und unter „Zertifikatsvertrauenseinstellungen“ einschalten), Android und Thunderbird (eigener Speicher). Firmen-Telefone verteilen Sie am bequemsten über eine Geräteverwaltung (MDM).

Auch für Ihre Gesprächspartner

Fremde Firmen müssen das CA-Zertifikat ebenfalls einmal installieren, sonst sehen auch sie „nicht vertrauenswürdig“. Schicken Sie ihnen die .cer-Datei und den SHA-256-Fingerabdruck auf einem zweiten Weg (zum Beispiel am Telefon), damit sie die Datei prüfen können. Den Link „CA-Zertifikat herunterladen“ finden Sie auch auf jeder Postfach-Seite.

Die CA im System des Servers hinterlegen (z. B. für grommunio Web) NEU in 1.5.5

grommunio Web prüft Unterschriften selbst – gegen den Vertrauensspeicher des Servers, nicht gegen den des Gateways. Kennt der Server Ihre CA nicht, zeigt grommunio bei jeder unterschriebenen E-Mail: „Die ausstellende Zertifizierungsstelle ist nicht im S/MIME-Vertrauensspeicher des Servers enthalten“.



Der Kasten „System-Vertrauensspeicher“ auf der Seite „Zertifizierungsstellen“

1. Klicken Sie auf **„Ins System übernehmen“** und bestätigen Sie. Das Gateway legt jede eigene CA als `own-smime-ca-….crt` in `/usr/local/share/ca-certificates/` ab (dazu alle zusammen in `own-smime-cas.pem`) und führt `update-ca-certificates` aus. Ist das Plugin „grommunio admin auth“ aktiv, startet es außerdem php-fpm neu, damit grommunio Web die CA sofort kennt. Danach steht oben „übernommen“.

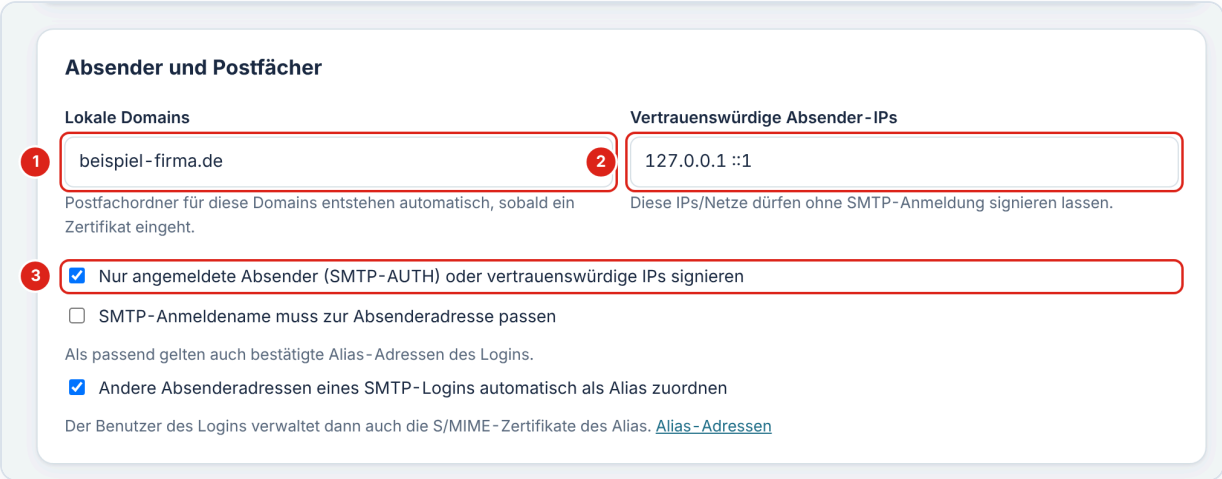
Das erledigt ein kleiner Hilfsdienst mit root-Rechten (`smime-ca-sync`), den `install.sh` und `update.sh` einrichten. Die Weboberfläche selbst hat bewusst keine root-Rechte. Antwortet der Hilfsdienst nicht, klappt der Kasten „Hinweis für den Administrator“ auf. Dort stehen die Befehle, die Ihr IT-Dienstleister einmal als root ausführt. Nach dem Anlegen oder Löschen einer CA zeigt der Kasten „nicht übernommen“ – dann einfach erneut auf den Knopf klicken.

Gut zu wissen

Im System-Vertrauensspeicher vertraut der ganze Server Ihrer CA – auch für verschlüsselte Webseiten (TLS). Schützen Sie deshalb den Server und die CA gut, und legen Sie nur CAs an, die Sie wirklich brauchen.

10 S/MIME-Einstellungen

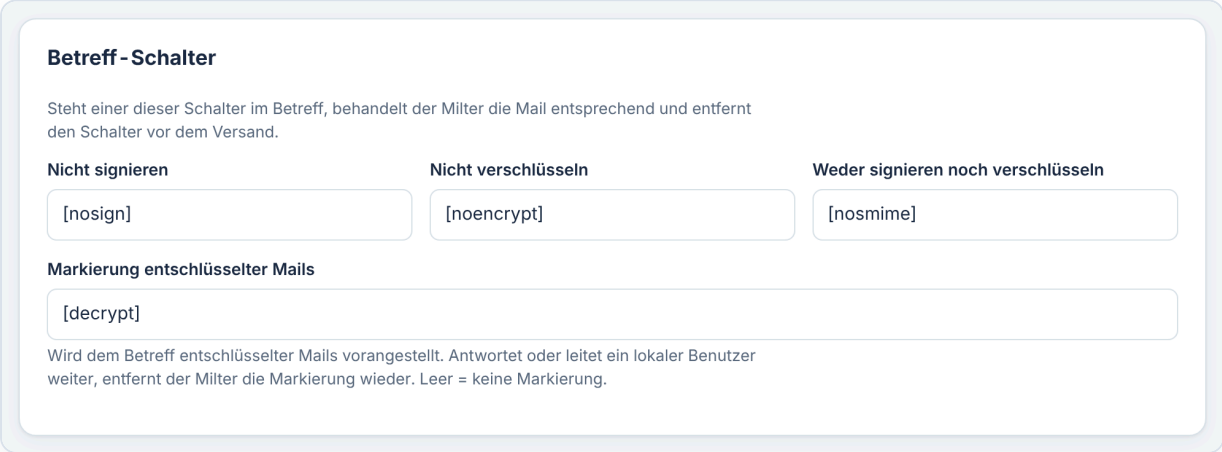
Klicken Sie im Menü auf **„S/MIME“**. Das Wichtigste steht im Kasten **„Absender und Postfächer“**:



Domains und erlaubte Absender

1. **Lokale Domains**: der Teil Ihrer E-Mail-Adressen hinter dem @, zum Beispiel `beispiel-firma.de`. Mehrere durch Leerzeichen trennen.
2. **Vertrauenswürdige Absender-IPs**: Geräte, die ohne Anmeldung E-Mails einliefern dürfen (zum Beispiel der Mail-Server selbst: `127.0.0.1`). Im Zweifel nicht ändern.
3. **Nur angemeldete Absender …**: sollte angehakt bleiben. Dann kann niemand von außen E-Mails in Ihrem Namen unterschreiben lassen.

Die „Zauberwörter“ im Betreff



Betreff-Schalter

Oben auf der Seite legen Sie die **Betreff-Schalter** fest – die Wörter, mit denen Kollegen eine einzelne E-Mail ohne Unterschrift oder unverschlossen schicken (`[nosign]`, `[noencrypt]`, `[nosmime]`). Die Grundeinstellungen für alle Postfächer finden Sie unter **„Standards“**.

11 Erinnerungen und Info-Mails

Ausweise gelten nur eine bestimmte Zeit. Damit keiner vergessen wird, schickt das Gateway rechtzeitig Erinnerungen. Klicken Sie im Menü auf **„Erinnerungen“**.

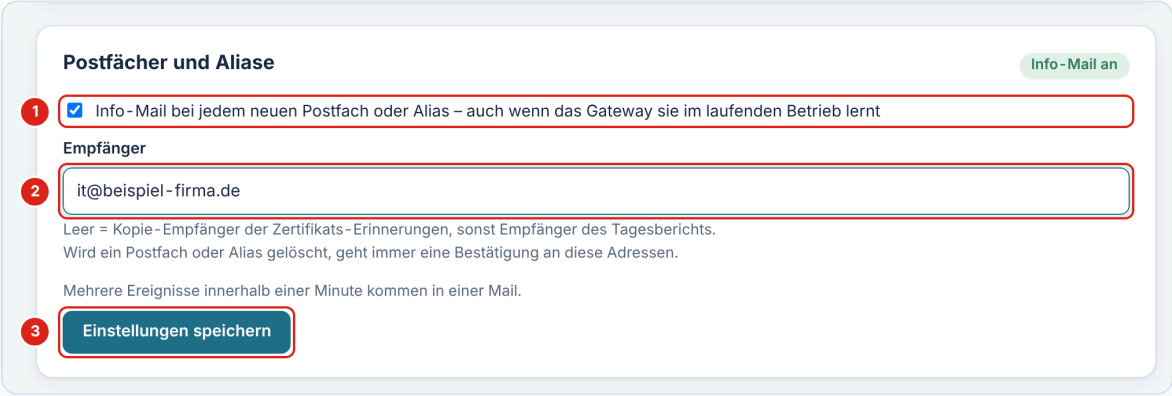


Erinnerungen einschalten

1. Haken bei **„Erinnerungen vor Zertifikatsablauf verschicken“** setzen.
2. **Tage vor Ablauf**: zum Beispiel `30 20 10` – dann kommt 30, 20 und 10 Tage vorher je eine E-Mail.
3. **„Einstellungen speichern“**. Unter „Kopie an“ können Sie sich selbst eine Kopie jeder Erinnerung schicken lassen.

Info-Mails zu Postfächern und Aliasen NEU in 1.5.3

Weiter unten auf derselben Seite steht der Kasten **„Postfächer und Aliase“**. Hier legen Sie fest, wer die Info-Mails bekommt:

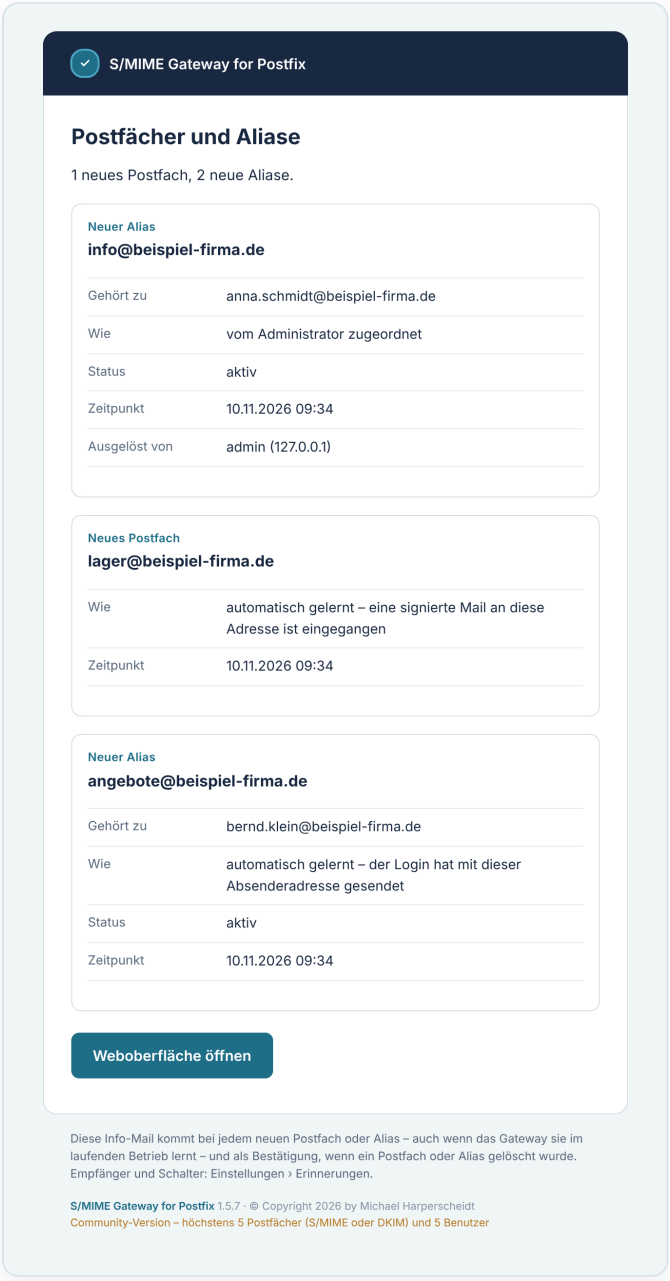


Empfänger der Info-Mails

1. Haken bei **„Info-Mail bei jedem neuen Postfach oder Alias“** setzen (ist von Anfang an gesetzt).

2. **Empfänger**: eine oder mehrere Adressen, durch Komma getrennt. Leer = die Adressen unter „Kopie an“ (oben), sonst die Empfänger des täglichen Berichts.
3. **„Einstellungen speichern“**.

Eine Info-Mail kommt, wenn ein Postfach oder Alias **neu** ist – egal, ob Sie es angelegt haben, ob es beim Zuordnen zu einem Konto entstanden ist oder ob das Gateway es im laufenden Betrieb gelernt hat. Was innerhalb einer Minute passiert, kommt gesammelt in **einer** E-Mail:



Eine Info-Mail mit drei neuen Adressen

Wird ein Postfach oder Alias **gelöscht**, kommt immer eine Bestätigung an dieselben Adressen – auch wenn der Haken oben aus ist (Kapitel 8).

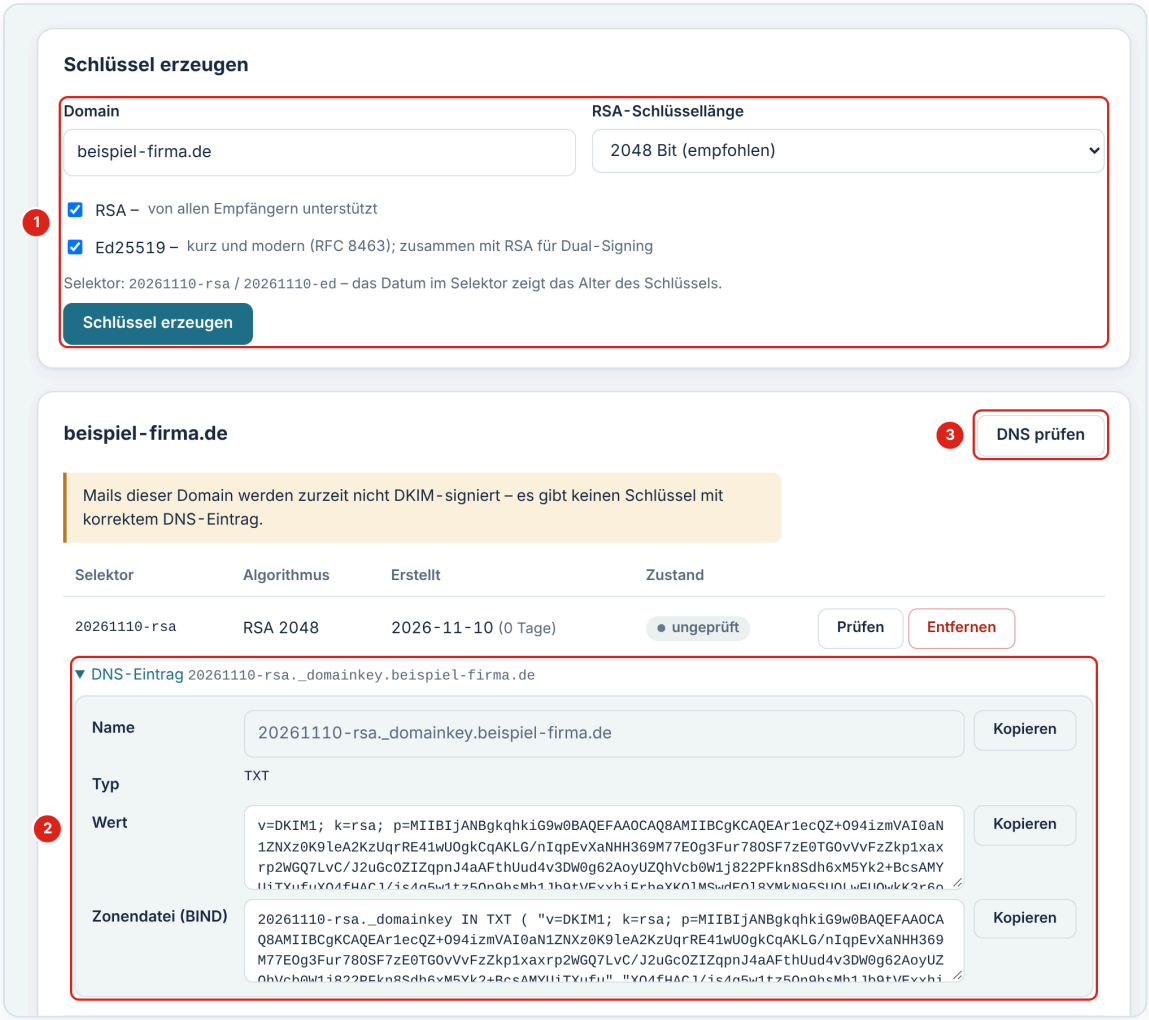
Ein gelernter Alias wartet auf Sie?

Ist unter **„S/MIME“** „SMTP-Anmeldename muss zur Absenderadresse passen“ eingeschaltet, warten neu gelernte Aliase auf Ihre Bestätigung. Das steht dann in der Info-Mail, mit einem Knopf direkt zur Liste (Kapitel 15).

12 DKIM – der Echtheits-Stempel für Ihre Domain

DKIM ist ein unsichtbarer Stempel auf jeder E-Mail Ihrer Firma. Empfänger-Server prüfen ihn und wissen dann: Diese E-Mail kommt wirklich von *beispiel-firma.de*. Ihre E-Mails landen dadurch seltener im Spam-Ordner.

DKIM ist ein **Plugin** (Zusatzbaustein). Schalten Sie es unter **„Plugins“** ein; danach erscheint im Menü **„DKIM“**.



Die DKIM-Seite: Schlüssel erzeugen und DNS-Eintrag

1. Domain eintragen und auf **„Schlüssel erzeugen“** klicken. Lassen Sie RSA und Ed25519 angehakt.

2. Unter **„DNS-Eintrag“** stehen Name und Wert. Diese müssen im **DNS** Ihrer Domain eingetragen werden – das ist das „Telefonbuch des Internets“, das Ihr Domain-Anbieter verwaltet. Mit **„Kopieren“** übernehmen Sie die Werte, ohne zu tippen. Wenn Sie das nicht selbst können: Schicken Sie die Werte Ihrem Domain-Anbieter oder IT-Dienstleister.

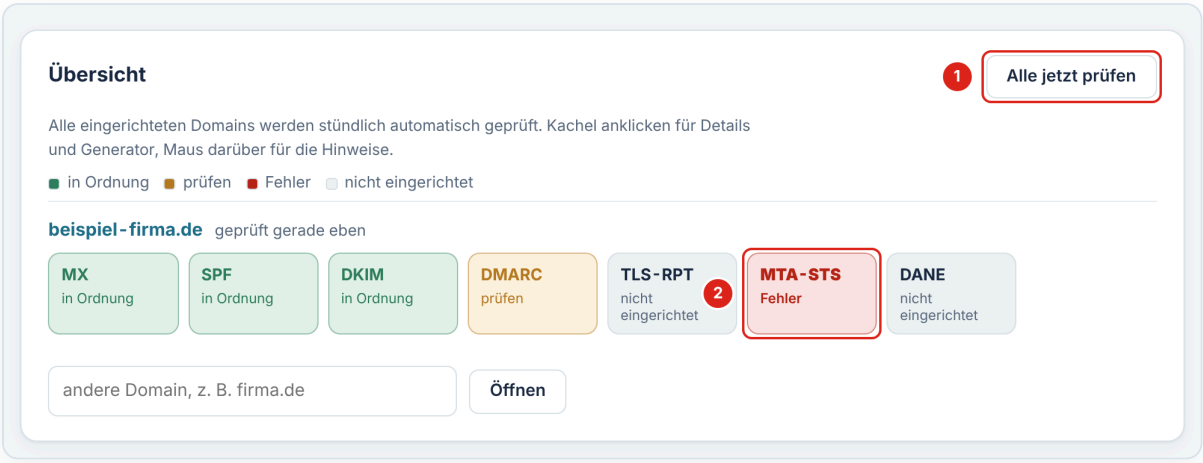
3. Nach dem Eintragen (das kann ein paar Stunden dauern) klicken Sie auf **„DNS prüfen“**. Steht beim Schlüssel ein grünes Zeichen, stempelt das Gateway ab sofort jede E-Mail. Das Gateway prüft außerdem jede Stunde von selbst.

Gut zu wissen

Solange der DNS-Eintrag fehlt, steht ein gelber Hinweis „Mails dieser Domain werden zurzeit nicht DKIM-signiert“. Das ist kein Fehler, sondern nur eine Erinnerung.

13 Mail-DNS – SPF, DMARC, MTA-STS und Co. prüfen NEU in 1.5.7

Ob Ihre E-Mails beim Empfänger ankommen und als echt gelten, hängt an ein paar Einträgen im **DNS** Ihrer Domain. Unter **„Einstellungen › Mail-DNS“** prüft das Gateway alle auf einmal und zeigt, was fehlt – mit Erklärung und, wo möglich, dem fertigen Eintrag zum Kopieren.



Die Übersicht: je Domain eine Reihe Kacheln

Das Gateway prüft alle eingerichteten Domains (Ihre lokalen Domains, Domains mit DKIM-Schlüssel und Domains, für die Sie einen Eintrag erzeugt haben) **jede Stunde von selbst**. Das Ergebnis steht oben als kleine Kacheln, eine Reihe je Domain: **grün** = in Ordnung, **gelb** = bitte prüfen, **rot** = Fehler, **grau** = nicht eingerichtet (gestrichelt: noch nicht geprüft).

1. **„Alle jetzt prüfen“** startet die Prüfung sofort, ohne auf die nächste Stunde zu warten (läuft im Hintergrund – Seite nach etwa einer Minute neu laden).
2. Fahren Sie mit der Maus über eine Kachel, erscheinen die wichtigsten Hinweise. Ein Klick öffnet die Domain direkt beim passenden Abschnitt mit Erklärung und Generator.

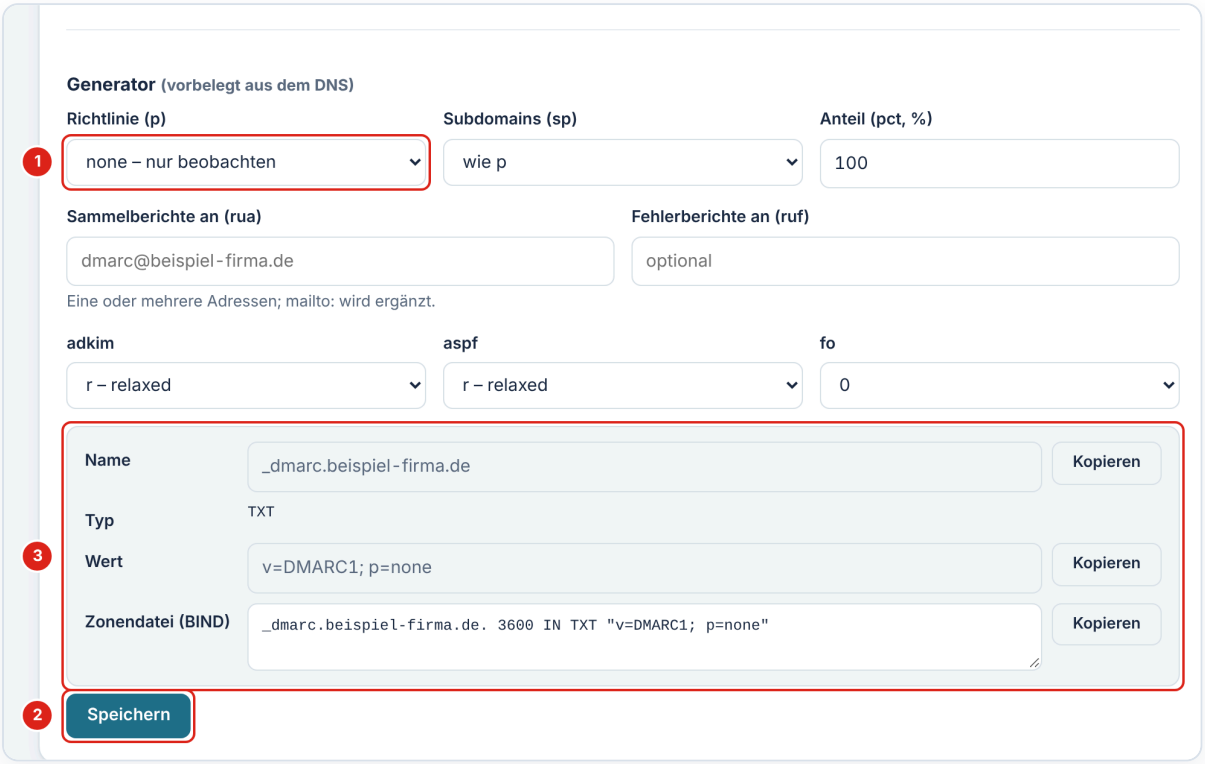
Unter der Übersicht sind die Abschnitte der gewählten Domain zugeklappt, damit die Seite übersichtlich bleibt. Unter **„Einstellungen der Prüfung“** lässt sich die stündliche Prüfung abschalten.

Verfahren	Wofür?
SPF	Liste der Server, die für Ihre Domain senden dürfen.
DKIM	Der Stempel aus Kapitel 12. Ist das Plugin aktiv, prüft die Seite genau dessen Schlüssel.
DMARC	Was mit gefälschten Mails passiert (beobachten, Spam-Ordner, ablehnen) und wohin Berichte gehen.
TLS-RPT	Tägliche Berichte anderer Mailserver, ob die verschlüsselte Zustellung zu Ihnen geklappt hat.
MTA-STS	Verlangt von anderen Mailservern, nur verschlüsselt und mit gültigem Zertifikat an Sie zu senden (Richtlinie per HTTPS).

DANE	Dasselbe Ziel über DNSSEC: Das Zertifikat Ihres Mailservers steht als TLSA-Eintrag im DNS.

Einen Eintrag erzeugen

Jeder Abschnitt beginnt mit **„Was bewirkt …?“** – dort ist jede Einstellung erklärt. Darunter stehen die Prüfergebnisse und der **Generator**. Er ist mit dem vorhandenen Eintrag vorbelegt.



Der DMARC-Generator

1. Einstellungen wählen, z. B. bei DMARC die Richtlinie und die Adresse für Berichte.
2. **„Speichern“**.
3. Name, Typ und Wert des Eintrags stehen darunter – mit **„Kopieren“** übernehmen Sie sie für Ihren Domain-Anbieter. Die Zeile „Zonendatei“ ist für Administratoren eines eigenen DNS-Servers.

Nach dem Eintragen beim Domain-Anbieter zeigt die nächste stündliche Prüfung das Ergebnis – oder sofort mit **„Jetzt prüfen“**.

Ganz oben gibt es alle erzeugten Einträge zusammen als Datei (**„Alle erzeugten Einträge als Zonendatei“**). Für DKIM gibt es hier keinen Generator – den Schlüssel erzeugt das Plugin DKIM.

MTA-STS über das Gateway veröffentlichen

MTA-STS braucht eine kleine Datei unter `https://mta-sts.<Ihre-Domain>/.well-known/mta-sts.txt`. Das Gateway kann sie selbst ausliefern: Haken bei **„Richtlinie über das Gateway veröffentlichen“** setzen und speichern. Die Seite zeigt dann die nötigen DNS-Einträge, die Richtlinie, eine kleine HTML-Infoseite und fertige

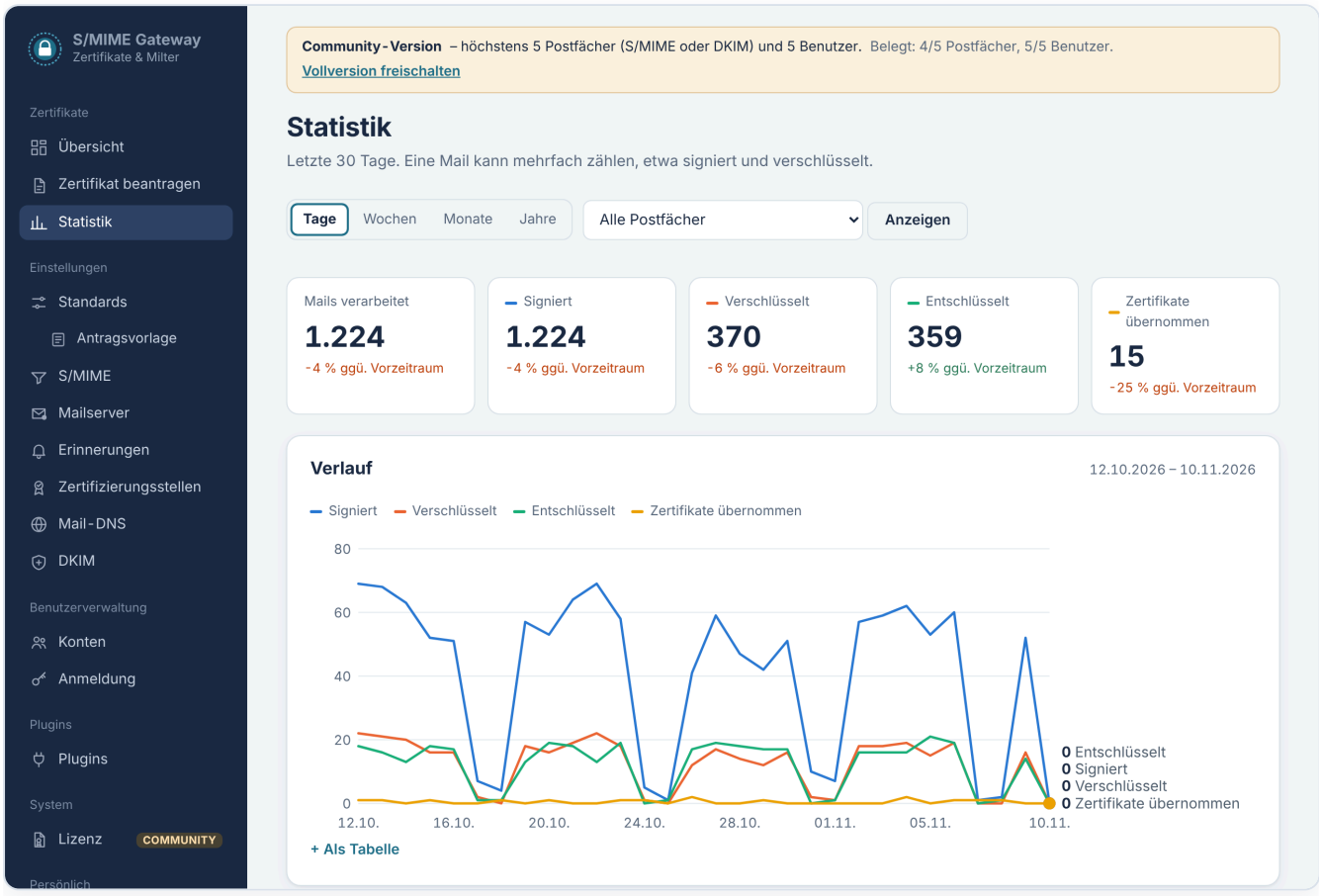
nginx-Vorlagen – für einen eigenen Webserver-Eintrag und für grommunio. nginx gibt nur diese Datei nach außen, nicht die Weboberfläche.

Erst testen, dann erzwingen

Beginnen Sie MTA-STS mit **testing** und richten Sie vorher TLS-RPT ein. Kommen einige Wochen keine Fehlerberichte, stellen Sie auf **enforce**. Bei DANE gilt: TLSA-Einträge nur eintragen, wenn Ihre Domain per DNSSEC signiert ist, und vor jedem Zertifikats- oder Schlüsselwechsel den neuen Eintrag zusätzlich veröffentlichen.

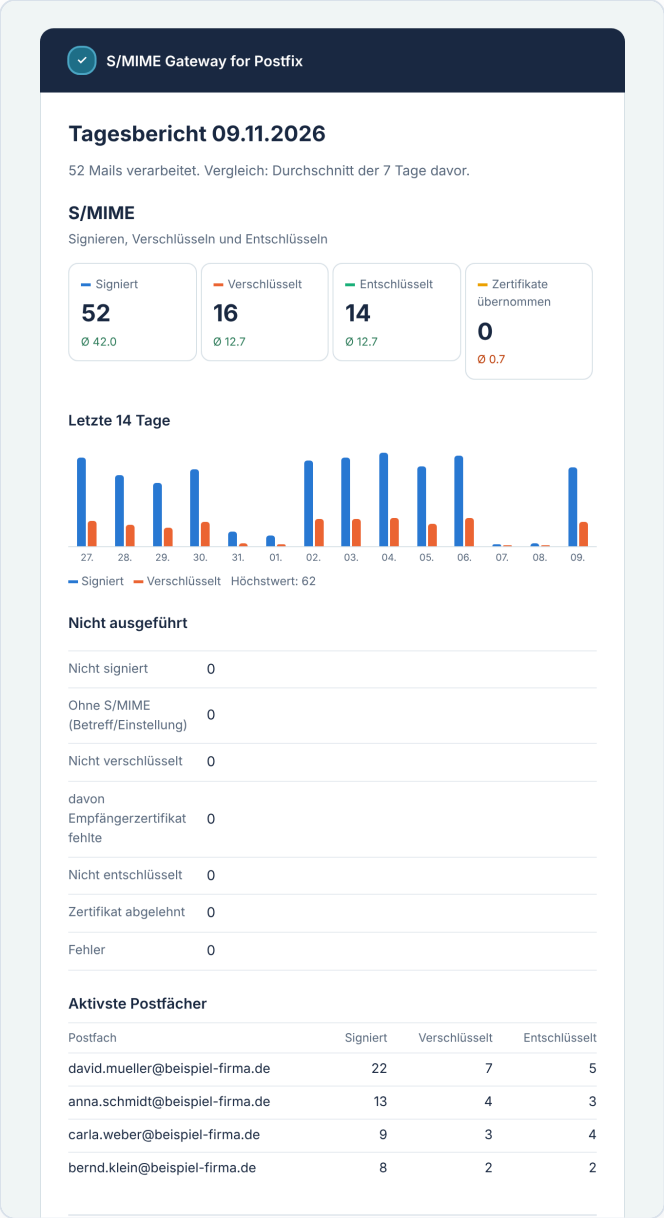
14 Statistik und täglicher Bericht

Unter **„Statistik“** sehen Sie, wie viele E-Mails unterschrieben, verschlossen und geöffnet wurden – als Zahlen und Grafik.



Die Statistik der letzten 30 Tage

Ganz unten auf der Seite schalten Sie den **täglichen Bericht** ein: Haken bei **„Jeden Tag einen Bericht über den Vortag per Mail senden“** setzen, Ihre Adresse eintragen, Uhrzeit wählen, speichern. Dann bekommen Sie jeden Morgen eine E-Mail wie diese:



Der tägliche Bericht (Ausschnitt). Weiter unten folgen DKIM, Mailverkehr je Postfach und Ausweise, die bald ablaufen.

Worauf Sie achten sollten

Der Abschnitt „Zertifikate mit Handlungsbedarf“ am Ende des Berichts. Steht dort ein Postfach, sollte es bald einen neuen Ausweis bekommen.

15 Alias-Adressen

Manche Kollegen verschicken E-Mails auch unter einer anderen Adresse, zum Beispiel Anna als *presse@beispiel-firma.de*. Das Gateway merkt das von selbst und ordnet die Adresse Annas Konto zu – Sie bekommen dazu eine Info-Mail. Anna kann dann auch für presse@ einen Ausweis beantragen. Selbst anlegen können Sie Aliase beim **„Postfach anlegen“** (Kapitel 7).



Die Alias-Adressen auf der Seite „Konten“

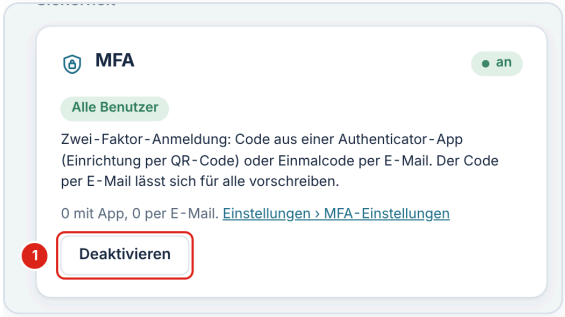
Die Liste ist nach Postfach gruppiert: Über jeder Gruppe steht das Postfach (bzw. der SMTP-Login), darunter eingerückt seine Aliase.

Passt eine Zuordnung nicht, klicken Sie auf **„Sperren“** – dann wird die Adresse nicht wieder automatisch zugeordnet. **„Löschen“** löst nur die Zuordnung. Mit **„Alias zuordnen“** ordnen Sie eine Adresse selbst zu. Adressen, die sich selbst anmelden oder schon einen eigenen Ausweis haben, werden nie automatisch zugeordnet. Einen Alias samt Ordner löschen Sie auf seiner Postfach-Seite (Kapitel 8).

16 Zwei-Faktor-Anmeldung (MFA) NEU in 1.5.5

Mit der **Zwei-Faktor-Anmeldung** genügt ein gestohlenes Passwort nicht mehr. Nach dem Passwort fragt das Gateway nach einem sechsstelligen Einmalcode – entweder aus einer **Authenticator-App** auf dem Telefon oder aus einer **E-Mail**.

Das Plugin einschalten

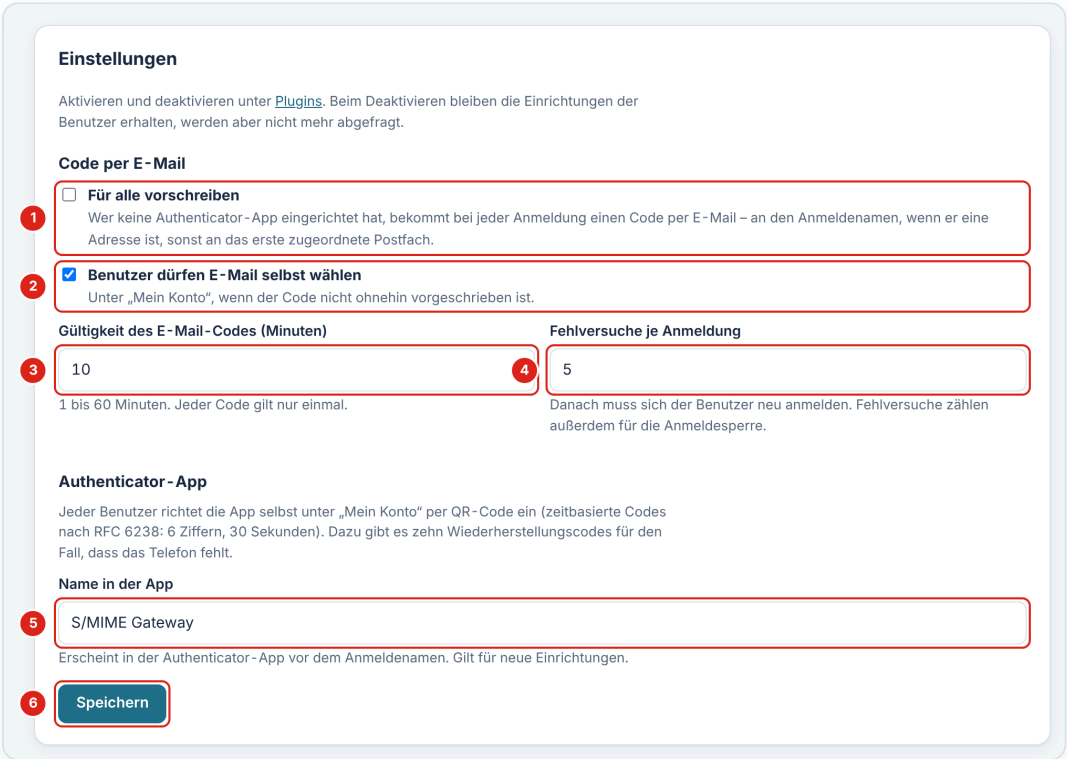


Das Plugin „MFA“ unter Plugins

1 Klicken Sie im Menü auf **„Plugins“** und beim Plugin **MFA** (Gruppe „Sicherheit“) auf **„Aktivieren“**.

Erst dann erscheinen der Menüpunkt **„MFA-Einstellungen“** unter „Einstellungen“ und bei allen Benutzern unter **„Mein Konto“** der Abschnitt „Zwei-Faktor-Anmeldung“. Schalten Sie das Plugin wieder aus, bleiben die Einrichtungen erhalten, werden aber nicht mehr abgefragt.

Die MFA-Einstellungen



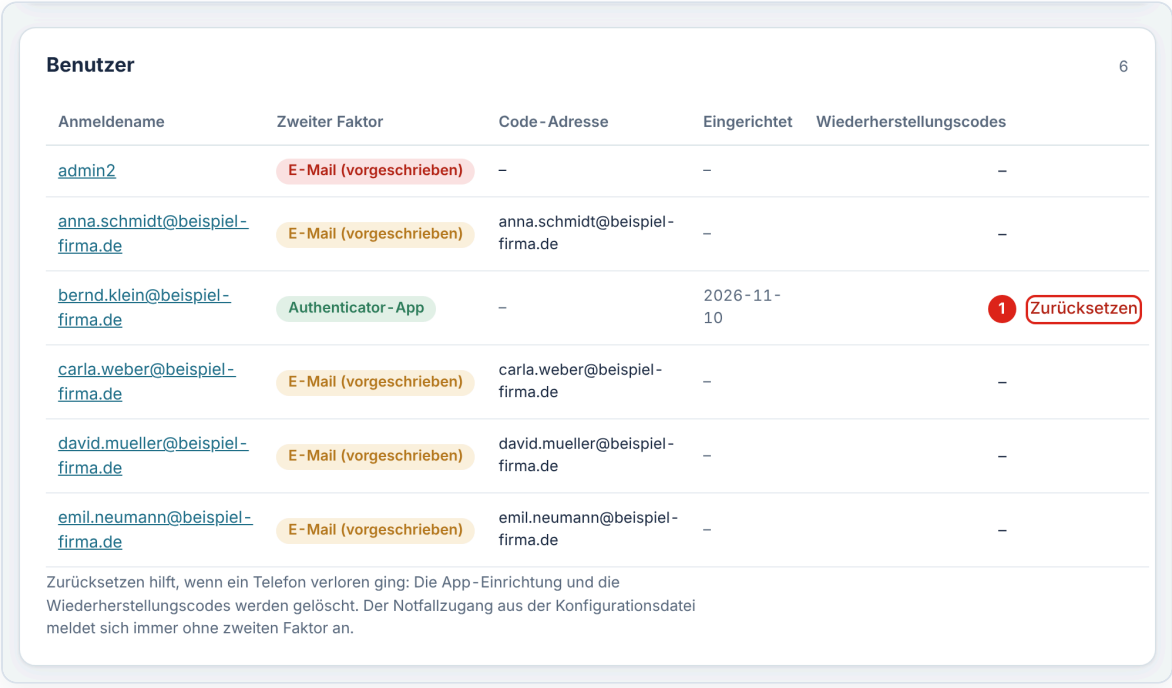
Die Seite „MFA-Einstellungen“

1 **Für alle vorschreiben**: Wer keine Authenticator-App eingerichtet hat, bekommt bei jeder Anmeldung einen Code per E-Mail. Er geht an den Anmeldenamen, wenn dieser eine E-Mail-Adresse ist, sonst an das erste zugeordnete Postfach.

2. **Benutzer dürfen E-Mail selbst wählen**: Ist der Code nicht vorgeschrieben, kann jeder unter „Mein Konto“ selbst entscheiden, ob er ihn per E-Mail bekommt.
3. **Gültigkeit des E-Mail-Codes**: 1 bis 60 Minuten (Standard: 10). Jeder Code gilt nur einmal.
4. **Fehlversuche je Anmeldung**: Danach muss sich der Benutzer neu anmelden. Falsche Codes zählen außerdem für die normale Anmeldesperre.
5. **Name in der App**: So heißt der Eintrag in der Authenticator-App, zum Beispiel „S/MIME Gateway“.
6. Auf **„Speichern“** klicken. Das gilt ab der nächsten Anmeldung.

> **Zuerst den Mailserver einrichten**
>
> Codes per E-Mail funktionieren nur, wenn unter **„Mailserver“** ein Absender eingetragen ist (Kapitel 5). Konten ohne E-Mail-Adresse (zum Beispiel ein Konto „admin“) können keinen Code per E-Mail bekommen. Sie melden sich bis dahin nur mit Passwort an und werden gebeten, eine Authenticator-App einzurichten. Die Seite zeigt solche Konten oben in einem gelben Kasten.

Wer nutzt was? – Zurücksetzen



Die Liste „Benutzer“ auf der Seite „MFA-Einstellungen“

Die Liste zeigt jedes Konto mit seinem zweiten Faktor: **Authenticator-App**, **E-Mail**, **E-Mail (vorgeschrieben)** oder **nur Passwort**.

1. Hat jemand sein Telefon verloren, klicken Sie bei ihm auf **„Zurücksetzen“**. Die App-Einrichtung und die Wiederherstellungscodes werden gelöscht. Danach meldet er sich mit Passwort an (und Code per E-Mail, falls vorgeschrieben) und richtet die App neu ein.

> **So melden sich Ihre Kollegen an**
>
> Die Benutzer-Anleitung erklärt Schritt für Schritt, wie man die App einrichtet und den Code eingibt. Sie selbst richten Ihre App genauso unter **„Mein Konto“** ein. Der **Notfallzugang** aus der Konfigurationsdatei (Kapitel 2) fragt nie nach einem Code – damit Sie sich nicht aussperren können. Bewahren Sie sein Passwort deshalb besonders gut auf.

17 Die Lizenz

Das Gateway gibt es in zwei Ausgaben:

	Community-Version (kostenlos)	Vollversion (mit Lizenzdatei)
Postfächer	höchstens 5	so viele, wie die Lizenz erlaubt
Benutzer	höchstens 5 (ein Administrator zählt nicht)	so viele, wie die Lizenz erlaubt
Mail-Domains	alle	die in der Lizenz genannten
Funktionen	alle	alle

Als **Postfach** zählt jede Adresse, die einen eigenen Ausweis hat oder deren E-Mails in den letzten 30 Tagen den DKIM-Stempel bekommen haben. Eine Adresse mit beidem zählt nur einmal. Löschen Sie ein Postfach, ist sein Platz sofort wieder frei.

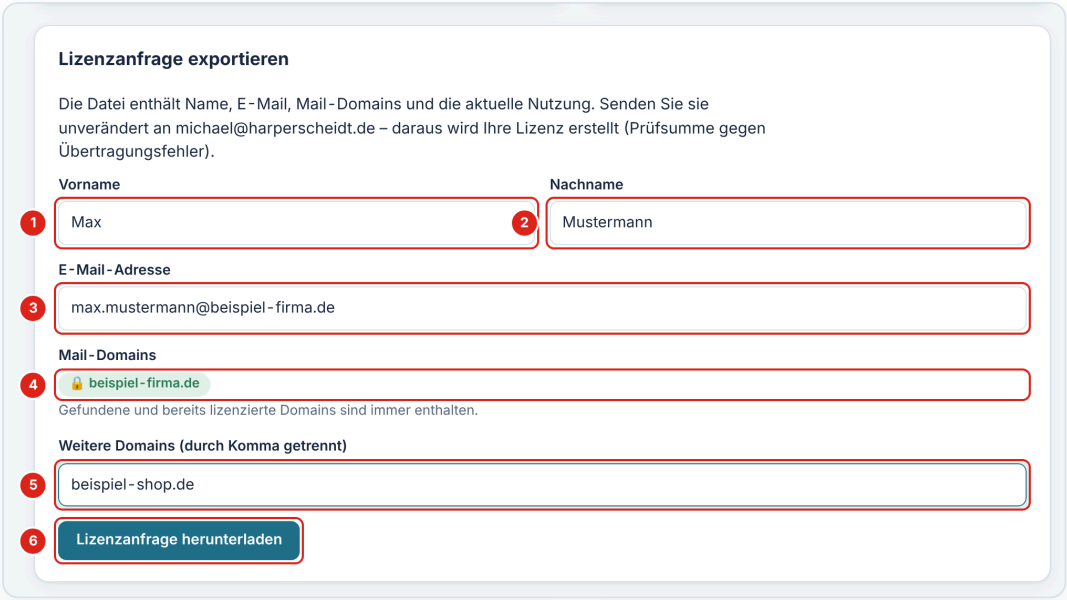
Klicken Sie im Menü unter „System“ auf **„Lizenz“**:



Der Kasten „Status“ auf der Lizenzseite

1. **Zum Versenden verwendete Domains**: Hier sehen Sie, welche Ihrer Domains schon E-Mails über das Gateway verschickt haben und wie viele Postfächer dazugehören. „gezählt“ sind die Postfächer, die für die Lizenz zählen – zusammen ergibt das die Zahl unter „Nutzung“. „gesehen“ sind alle Adressen, die überhaupt schon etwas verschickt haben, auch ohne Ausweis und ohne DKIM-Stempel. Diese zählen nicht. Mit „Alle Absender mit Begründung anzeigen“ sehen Sie bei jeder Adresse, ob und warum sie zählt.
2. Mit **„Lizenzanfrage exportieren“** springen Sie zum Formular für die Anfrage.

Eine Lizenz anfragen



Die Lizenzanfrage ausfüllen

1. **Vorname** eintragen.
2. **Nachname** eintragen.
3. **E-Mail-Adresse**, an die die Lizenz geschickt werden soll.
4. Die Domains mit Schloss 🔒 hat das Gateway gefunden – sie sind immer dabei und lassen sich nicht entfernen.
5. Weitere Domains, die Sie künftig nutzen möchten, tragen Sie hier ein – durch Komma getrennt.
6. Klicken Sie auf **„Lizenzanfrage herunterladen“**. Ihr Internet-Programm speichert eine Datei, zum Beispiel `lic-Mustermann-20261108-DyFO.req`.

Schicken Sie diese Datei unverändert per E-Mail an **michael@harperscheidt.de** und schreiben Sie dazu, wie viele Postfächer und Benutzer Sie brauchen. Mehr Informationen: **https://harperscheidt.de**.

> **Haben Sie schon eine Lizenz?**
>
> Dann sind Name und E-Mail bereits ausgefüllt. Die Anfrage enthält Ihre bisherige Lizenz – so kann eine Erweiterung oder eine neue Domain passend ausgestellt werden.

Die Lizenzdatei einspielen

Sie bekommen eine Datei mit der Endung `.lic` zurück.



Die Lizenzdatei einspielen

1. Klicken Sie auf **„Datei auswählen“** (bzw. „Choose File“) und wählen Sie die `.lic`-Datei.
2. Klicken Sie auf **„Lizenz prüfen und einspielen“**.



Geschafft: Die Vollversion ist freigeschaltet (Beispiel-Lizenz)

Lizenz erweitern

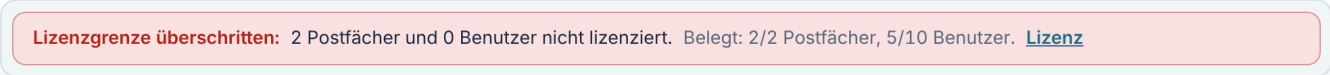
Später eine zweite Lizenz für mehr Postfächer? Einfach ebenso einspielen. Gleicher Name, gleiche E-Mail und gleiche Domains werden **zusammengezählt**. Jede Lizenzdatei zählt nur einmal. Eine Lizenz mit zusätzlichen Domains ersetzt die alte automatisch.

18 Wenn die Lizenz nicht mehr reicht

Nutzt die Firma mehr Postfächer oder Benutzer als erlaubt, gilt eine feste Regel:

- Für Postfächer **über der Grenze** werden E-Mails **weder unterschrieben noch gestempelt** (DKIM) und nicht geöffnet.
- Benutzer über der Grenze können sich nicht anmelden.

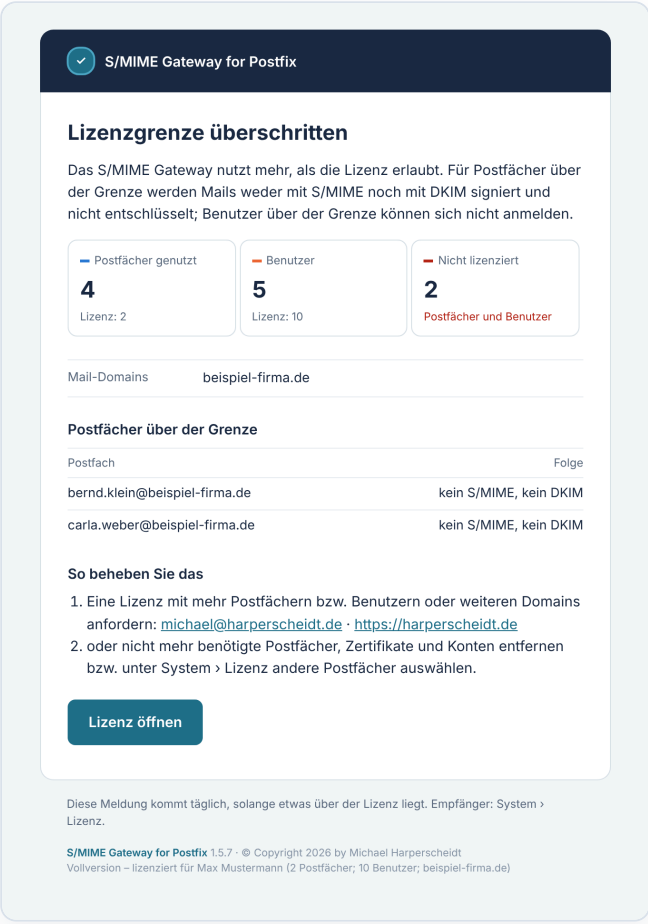
Sie merken das an drei Stellen:



1. Ein roter Streifen oben auf jeder Seite



2. Sofort eine E-Mail, wenn ein neues Postfach über der Grenze eine E-Mail verschickt – einmal pro Postfach

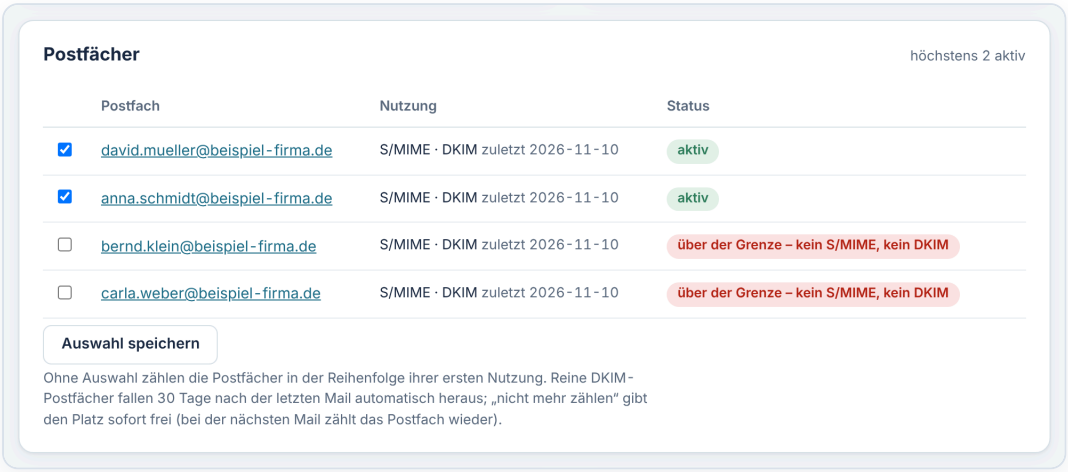


3. Jeden Tag eine Übersicht, solange etwas über der Grenze liegt

Was Sie dann tun

1. **Mehr Lizenz anfragen** (Kapitel 17) – das ist der einfachste Weg.

2 Oder **aufräumen**: Nicht mehr benötigte Postfächer löschen (Kapitel 8) – ihr Platz ist sofort frei. Oder auf der Lizenzseite unter „Postfächer“ mit Haken wählen, welche Postfächer aktiv sein sollen, und auf **„Auswahl speichern“** klicken. Postfächer, die nur gestempelt werden und nicht mehr gebraucht werden, entfernen Sie mit „nicht mehr zählen“.



Die Postfächer auf der Lizenzseite

19 Installieren und aktualisieren

Diese Schritte geschehen auf dem Server selbst, in einem schwarzen Text-Fenster („Terminal“). Wenn Sie das nicht kennen, bitten Sie Ihren IT-Dienstleister – es dauert nur wenige Minuten.

Erstinstallation

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

Das richtet alles ein und legt das Konto **admin** an (Sie werden nach einem Passwort gefragt).

Aktualisieren auf eine neue Version

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

Vorher wird automatisch eine Sicherung gemacht. Klappt etwas nicht, wird die alte Version von selbst zurückgeholt.

> **Wichtig**
>
> Spielen Sie nur Dateien ein, die vom Herausgeber stammen. Das Installationsprogramm prüft die Signatur (`smime_milter.py.sig`) und bricht ab, wenn die Programmdatei verändert wurde. Mit einer veränderten Datei gilt keine Lizenz.

Den Zustand prüfen

```
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
```

Wo die Daten liegen

Ordner / Datei	Inhalt
`/var/lib/smime-milter/senders/`	ein Ordner je Postfach: Ausweis, Schlüssel, Ausweise der Gesprächspartner, Einstellungen
`…/deleted/`	Sicherung gelöschter Postfächer, 30 Tage NEU in 1.5.3
`…/admin-events.json`	noch nicht verschickte Info-Mails NEU in 1.5.3
`…/aliases.json`	Alias-Adressen
`/var/backups/smime-milter/`	Sicherungen von `update.sh`

20 Wenn etwas nicht klappt

Was passiert	Was Sie tun können
Kollegen bekommen keine E-Mail mit Zugangsdaten.	Unter „Mailserver“ eine Testmail schicken (Kapitel 5). Spam-Ordner prüfen lassen.
Ich bekomme keine Info-Mails zu neuen Postfächern.	Unter „Erinnerungen“ › „Postfächer und Aliase“ Haken und Empfänger prüfen (Kapitel 11). Mit „Wartende jetzt senden“ verschicken Sie liegengebliebene Meldungen sofort.
Ich habe mich ausgesperrt.	Mit dem Notfallzugang anmelden (Kapitel 2).
Ein Kollege hat sein Telefon mit der Authenticator-App verloren.	Unter „MFA-Einstellungen“ bei ihm auf „Zurücksetzen“ klicken (Kapitel 16).
Der Code per E-Mail kommt nicht an.	Unter „Mailserver“ eine Testmail schicken (Kapitel 5), Spam-Ordner prüfen. Auf der Anmeldeseite „Neuen Code senden“ anklicken.
Ich habe das falsche Postfach gelöscht.	Innerhalb von 30 Tagen kann Ihr IT-Dienstleister den Ordner aus `/var/lib/smime-milter/deleted/` zurückholen (Kapitel 8).
„… ist bereits als Alias von … eingetragen“ beim Anlegen.	Die Adresse gehört schon zu einem anderen Postfach. Unter „Konten“ › „Alias-Adressen“ zuerst löschen, dann neu anlegen.
„Community-Version: höchstens 5 Benutzer …“ beim Anlegen eines Kontos.	Lizenz anfragen (Kapitel 17) oder ungenutzte Konten sperren.
Roter Streifen „Lizenzgrenze überschritten“.	Kapitel 18.
„Mails dieser Domain werden zurzeit nicht DKIM-signiert“.	DNS-Eintrag fehlt oder ist noch nicht sichtbar (Kapitel 12). Ein paar Stunden warten, dann „DNS prüfen“.
Ein Partner kann verschlossene E-Mails nicht öffnen.	Er braucht einen eigenen Ausweis. Bis dahin: `[noencrypt]` im Betreff.
grommunio Web meldet „Die ausstellende Zertifizierungsstelle ist nicht im S/MIME-Vertrauensspeicher“.	Unter „Zertifizierungsstellen“ auf „Ins System übernehmen“ klicken (Kapitel 9).
Ein Partner sieht „Unterschrift nicht vertrauenswürdig“.	Ihm das CA-Zertifikat schicken (Kapitel 9) oder öffentliche Ausweise verwenden.
Die Lizenz wird nicht angenommen („passt nicht zur vorhandenen“).	Name, E-Mail oder Domains weichen ab. Haken bei „Vorhandene Lizenzen ersetzen“ setzen – oder beim Herausgeber nachfragen.

Auf der Lizenzseite steht „Programmdatei verändert“.	Die Original-Version neu einspielen (Kapitel 19).

> **Hilfe bekommen**
>
> Fragen zur Lizenz: **michael@harperscheidt.de** · **https://harperscheidt.de**. Technische Einzelheiten stehen in der Datei `README.md`.

21 Kleines Wörterbuch

Wort	Einfach erklärt
Gateway / Milter	Das Programm auf dem Mail-Server, durch das jede E-Mail läuft. „Milter“ heißt es in der Fachsprache von Postfix.
Postfix	Ein weit verbreitetes Mail-Server-Programm. Das Gateway arbeitet mit ihm zusammen.
Postfach	Eine E-Mail-Adresse mit eigenen Ausweisen und Einstellungen.
Alias	Eine weitere Adresse, die zu einem Postfach gehört und unter der ein Kollege E-Mails verschickt.
Konto	Ein Zugang zur Webseite des Gateways (Benutzername und Passwort).
MFA / Zwei-Faktor-Anmeldung	Anmelden mit Passwort und zusätzlich einem Einmalcode aus einer App oder E-Mail.
Authenticator-App	Eine App auf dem Telefon, die alle 30 Sekunden einen neuen sechsstelligen Code anzeigt.
Zertifikat	Digitaler Ausweis eines Postfachs.
CA	Zertifizierungsstelle – die „Ausweisbehörde“.
Signieren / Verschlüsseln	Unterschreiben / in einen verschlossenen Umschlag stecken.
DKIM	Unsichtbarer Echtheits-Stempel für alle E-Mails einer Domain.
DNS	Das „Telefonbuch des Internets“. Ihr Domain-Anbieter verwaltet die Einträge.
Domain	Der Teil der E-Mail-Adresse hinter dem @, zum Beispiel beispiel-firma.de.
Info-Mail	Kurze Nachricht an Sie, wenn ein Postfach oder Alias dazukommt oder gelöscht wurde.
Sicherung	Kopie eines gelöschten Postfachs, die noch 30 Tage auf dem Server bleibt.
Lizenzdatei (.lic)	Datei vom Herausgeber, die die Vollversion freischaltet. Fälschungssicher signiert.
Lizenzanfrage (.req)	Datei, die Sie an den Herausgeber schicken, um eine Lizenz zu bekommen.
Community-Version	Die kostenlose Ausgabe: 5 Postfächer, 5 Benutzer.

Copyright und Lizenz

© 2026 Michael Harperscheidt. Alle Rechte vorbehalten.

Diese Anleitung („Anleitung für Administratoren“, Version 1.5.7) gehört zum **S/MIME Gateway for Postfix**. Texte, Aufbau und Bilder sind urheberrechtlich geschützt.

Sie dürfen die Anleitung unverändert zusammen mit der Software weitergeben, sie für den Betrieb des Gateways in Ihrer Organisation ausdrucken und intern verteilen. Jede andere Vervielfältigung, Bearbeitung, Übersetzung oder Veröffentlichung – auch auszugsweise – ist nur mit schriftlicher Zustimmung von Michael Harperscheidt erlaubt.

Software

Die Software S/MIME Gateway for Postfix steht unter der **Business Source License 1.1** (Datei `LICENSE`). Der Einsatz innerhalb der Grenzen der Community-Version ist erlaubt; für mehr Postfächer, Benutzer oder bestimmte Mail-Domains gibt es eine Lizenz (Kapitel 17).

Hinweise

Die Bilder zeigen eine erfundene Beispiel-Firma; Namen und Adressen sind frei erfunden. Ähnlichkeiten mit echten Firmen oder Personen sind zufällig. Genannte Produkt- und Firmennamen (zum Beispiel Postfix, grommunio, Outlook) können Marken ihrer jeweiligen Inhaber sein.

Die Anleitung wurde sorgfältig erstellt. Sie ersetzt keine Beratung für Ihre Umgebung; für Schäden durch fehlerhafte Angaben wird – soweit gesetzlich zulässig – nicht gehaftet.

Kontakt

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