groupios Mare Cloud

Onboarding-Leitfaden

step3IT GmbH

Table of contents

1. Von Kauf bis produktivem Betrieb 3
1.1 Was ist die groupios Mare Cloud? 3
1.2 Was Sie uns bereitstellen müssen 3
1.3 Erster Login & Orientierung 3
1.4 Ihre Konfigurationsaufgaben 4
1.5 Externe Konfiguration: DNS 4
1.6 Externe Konfiguration: Mailserver 5
1.7 Support & nächste Schritte 5
2. Gateway Konfiguration 6
2.1 Domains 6
2.2 Next-Hop 9
2.3 Konfiguration 12
2.4 Black/Whitelists 17
3. Mailserver 19
3.1 Mailserver Konfiguration 19
3.2 Exchange Online 20
3.3 mailcow 26

1. Von Kauf bis produktivem Betrieb

Dieser Leitfaden begleitet Sie Schritt für Schritt vom Vertragsabschluss bis zum laufenden Betrieb Ihrer groupios Mare Cloud. Er ist bewusst kompakt gehalten und zeigt Ihnen, was Sie selbst tun müssen – und was wir für Sie erledigen.

1.1 Was ist die groupios Mare Cloud?

Die groupios Mare Cloud ist ein Managed Service für professionelle E-Mail-Sicherheit. Nach Vertragsabschluss richten wir Ihren Mandanten für Sie ein – Sie müssen lediglich einige wenige Angaben bereitstellen und anschließend Ihre eigene Umgebung konfigurieren.

1.1.1 Ihr Onboarding-Ablauf auf einen Blick

1. Ihre Daten bereitstellen
2. Wir richten Ihren Mandanten ein (und melden uns bei Ihnen)
3. Erster Login & Orientierung im Interface
4. Gateway-Einstellungen konfigurieren
5. DNS-Einträge setzen
6. Mailserver / Exchange anbinden
7. Betrieb & Monitoring

1.2 Was Sie uns bereitstellen müssen

Bevor wir Ihren Mandanten anlegen können, benötigen wir folgende Informationen von Ihnen:

1.2.1 Pflichtangaben

- Domain(s) (zwingend erforderlich) – z. B. ihrunternehmen.de (es können auch mehrere Domains angegeben werden)
- Unternehmensname und Kontaktperson
- Adresse (Straße, PLZ, Ort)
- Telefonnummer und E-Mail-Adresse

1.2.2 Was danach passiert

Nach Eingang Ihrer Daten wird Ihr Mandant angelegt. Sie erhalten anschließend eine Rückmeldung mit Ihren Zugangsdaten. Bitte rechnen Sie mit einer Bearbeitungszeit von [X Werktagen].

1.3 Erster Login & Orientierung

1.3.1 Zugang zum Interface

Login-URL: https://manage.groupios-mare.cloud/

Ihre Zugangsdaten erhalten Sie per E-Mail nach der Einrichtung durch uns. Sie erhalten einen Zugang, mit dem Sie auch administrativ tätig sein können. Wir behalten uns ebenfalls das Recht vor, administrativ tätig zu sein.

1.3.2 Orientierung im Interface

Nach dem Login sehen Sie das Dashboard mit folgenden Hauptbereichen:

- Dashboard - Systemstatus und Überblick
- System
  - Domains - Domain-Verwaltung
  - Users - Benutzer-Verwaltung
  - User Federation - Anbindung externer Benutzer-Verwaltung
  - Roles - Zugriffsrechte-Verwaltung
- Mailserver - Gateway-UI
  - Mail-Logs - Protokoll aller verarbeiteten Nachrichten
  - Domains - Gateway-Konfiguration der Domainen (Whitelist, Blacklist, Scoring)

1.4 Ihre Konfigurationsaufgaben

1.4.1 Gateway-Einstellungen

Folgende Einstellungen können Sie selbst im Interface vornehmen (weitere Konfigurationsmöglichkeiten werden ergänzt):

- Next-Hop - Zielserver für die Zustellung
- Whitelist - Absender oder Domänen, die immer durchgelassen werden
- Blacklist - Absender oder Domänen, die grundsätzlich blockiert werden
- Anhänge - Regeln für Dateianhänge
- Checks & Scoring – Gewichtung von Spam- und Malware-Prüfungen

> **Wichtiger Hinweis: Globale Einstellungen**
>
> Bestimmte Einstellungen gelten aktuell global für alle Domains und können nicht domainspezifisch angepasst werden. Bitte wenden Sie sich für individuelle Anpassungen an unseren Support.

1.4.2 Monitoring: Mail-Logs prüfen

Im Bereich Mail-Logs sehen Sie alle eingehenden und ausgehenden Nachrichten.

Bei Verdacht auf fälschlicherweise blockierte Mails: Support kontaktieren oder Absender auf Whitelist setzen.

1.5 Externe Konfiguration: DNS

Damit E-Mails korrekt über die groupios Mare Cloud geroutet werden, müssen folgende DNS-Einträge bei Ihrem Domain-Registrar oder DNS-Provider gesetzt werden:

- MX-Einträge:
  - `smtp.groupios-mare.cloud`
  - `worker01.groupios-mare.cloud`
- SPF-Eintrag (TXT): `v=spf1 redirect=smtp.groupios-mare.cloud`
- DKIM-Eintrag (TXT): DKIM Schlüssel werden individuell erstellt für jede Domain erstellt
- DMARC-Eintrag (TXT) – optional, aber empfohlen:

```
v=DMARC1; p=reject; rua=mailto:<Reporting Postfach>; ruf=mailto:<Reporting Postfach>; adkim=s; aspf=s;
```

Hinweis

Wir empfehlen auch einen SPF-Eintrag für die Wildcard Subdomain zu setzen: `v=spf1 -all`. Dies verhindert das ein Angreifer zum Beispiel von sales.example.com senden kann.

Hinweis

DNS-Änderungen benötigen je nach Provider bis zu 24–48 Stunden zur vollständigen Propagierung.

1.6 Externe Konfiguration: Mailserver

Welche Konfiguration Sie für Ihren Mailserver setzen entnehmen Sie den folgenden Dokumentationen:

- Exchange Online
- mailcow

1.7 Support & nächste Schritte

1.7.1 Wo bekomme ich Hilfe?

- Support-E-Mail: support@groupios.com

1.7.2 Was tun, wenn etwas nicht funktioniert?

- Mails kommen nicht an: DNS-Einträge prüfen, Support kontaktieren.
- Mails werden fälschlicherweise geblockt: Absender in Whitelist aufnehmen.
- Login funktioniert nicht: Support kontaktieren mit Ihrer Domain-Angabe.

1.7.3 Weiterführende Ressourcen

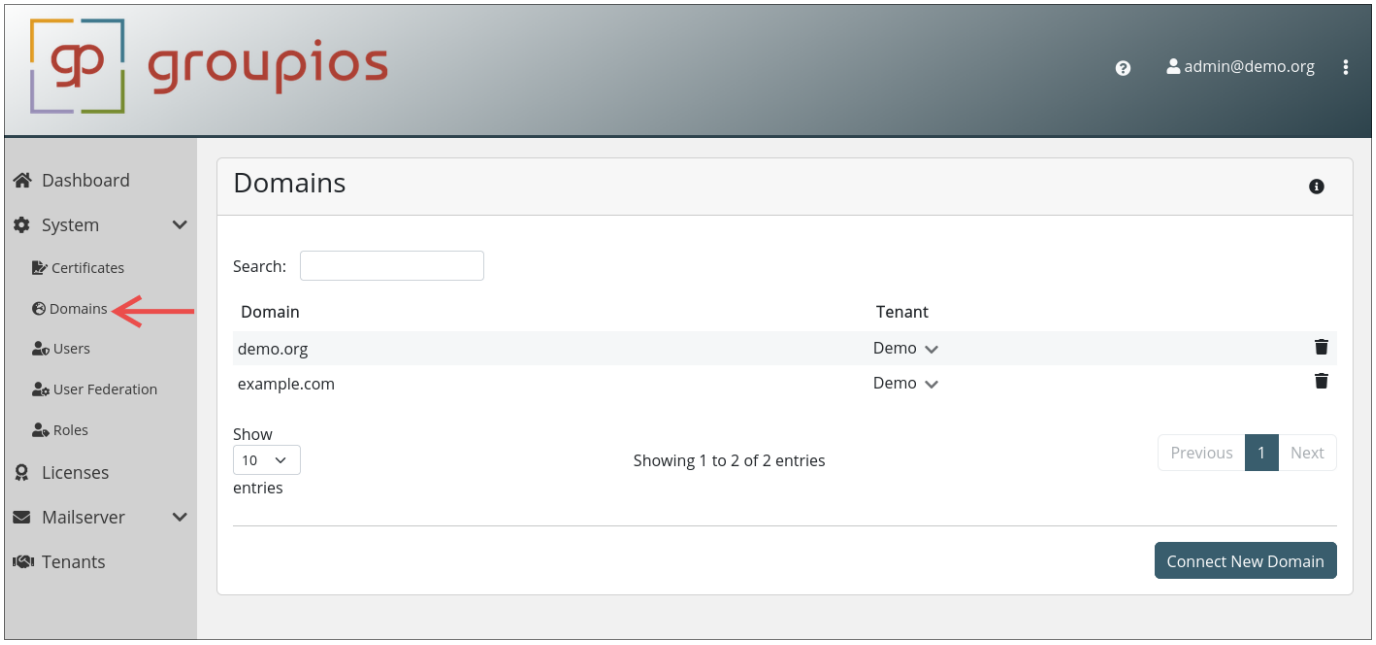
- Vollständiges Handbuch: manual.groupios-mare.cloud

Willkommen in der groupios Mare Cloud – wir freuen uns, Sie als Kunden zu begrüßen!

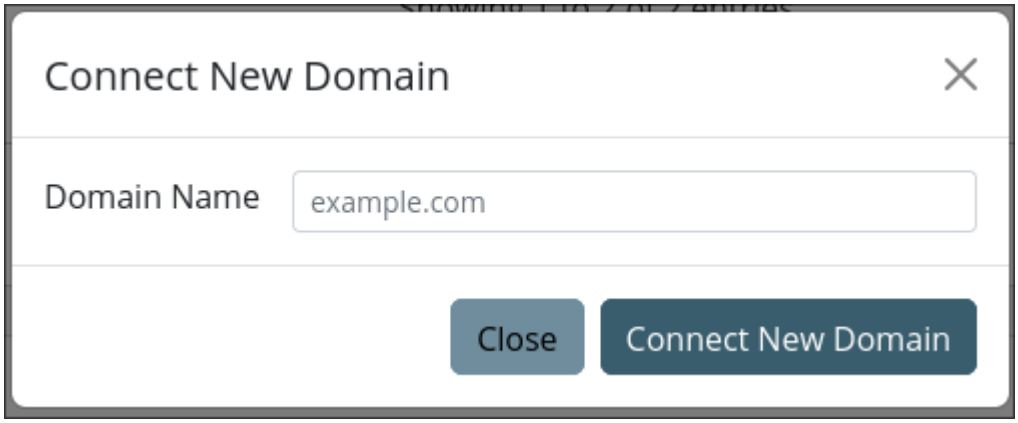
2. Gateway Konfiguration

2.1 Domains

Damit die groupios Mare Cloud E-Mails verarbeiten kann, die an Ihre Domains gerichtet sind, müssen diese Domains der groupios Mare Cloud bekannt sein. Standardmäßig werden die E-Mails an den Postfachspeicher der groupios Mare Cloud gesendet, um das Verhalten zu ändern muss entsprechend der Next-Hop umkonfiguriert werden.



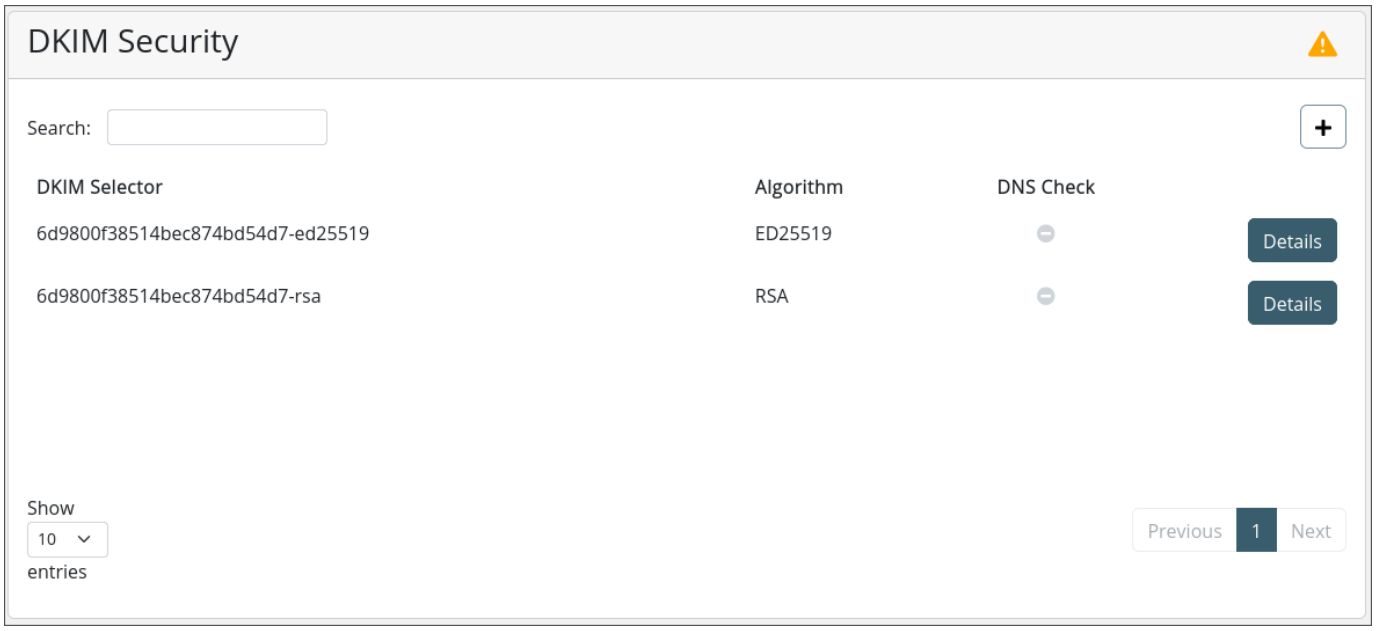
2.1.1 Eine neue Domain verbinden



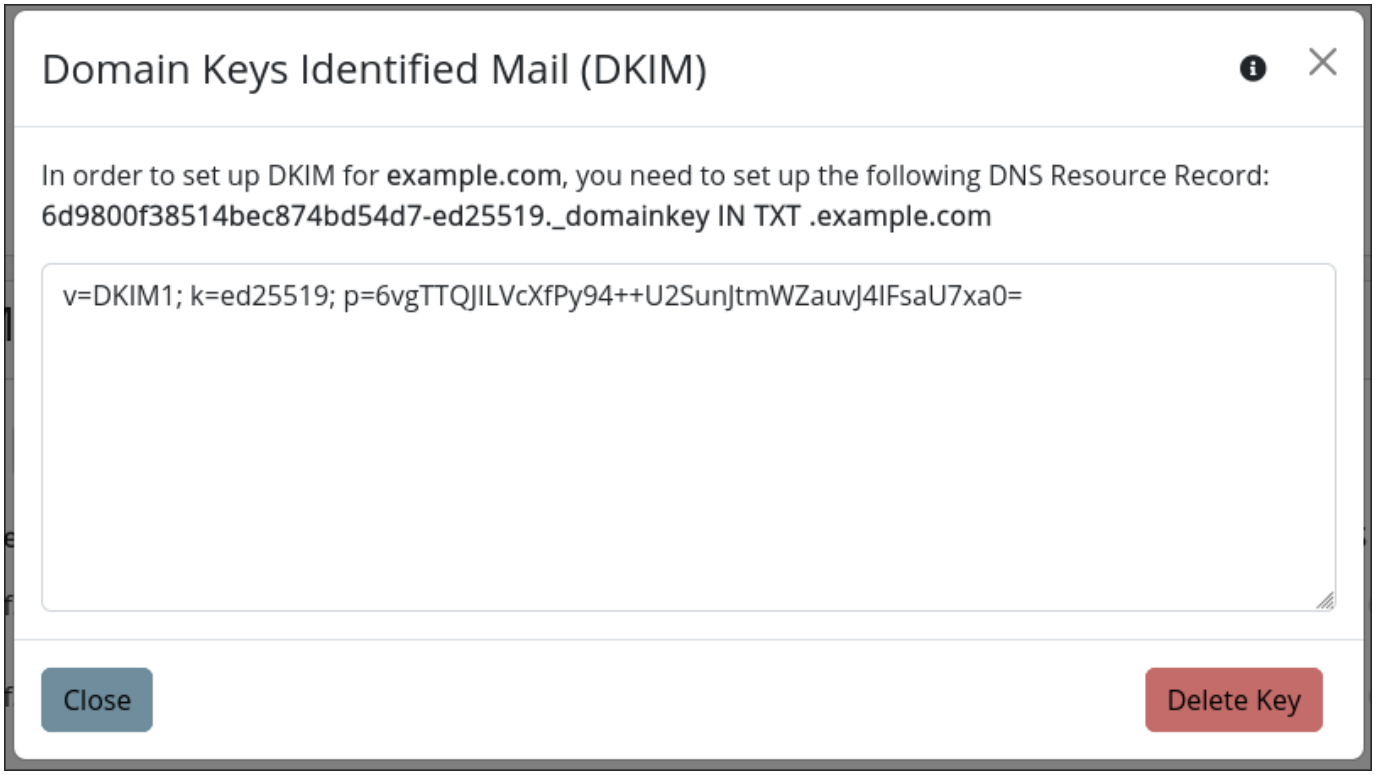
Klicken Sie auf "Connect New Domain". Geben Sie den Domainnamen in das dafür vorgesehene Eingabefeld ein.

2.1.2 DKIM Keys

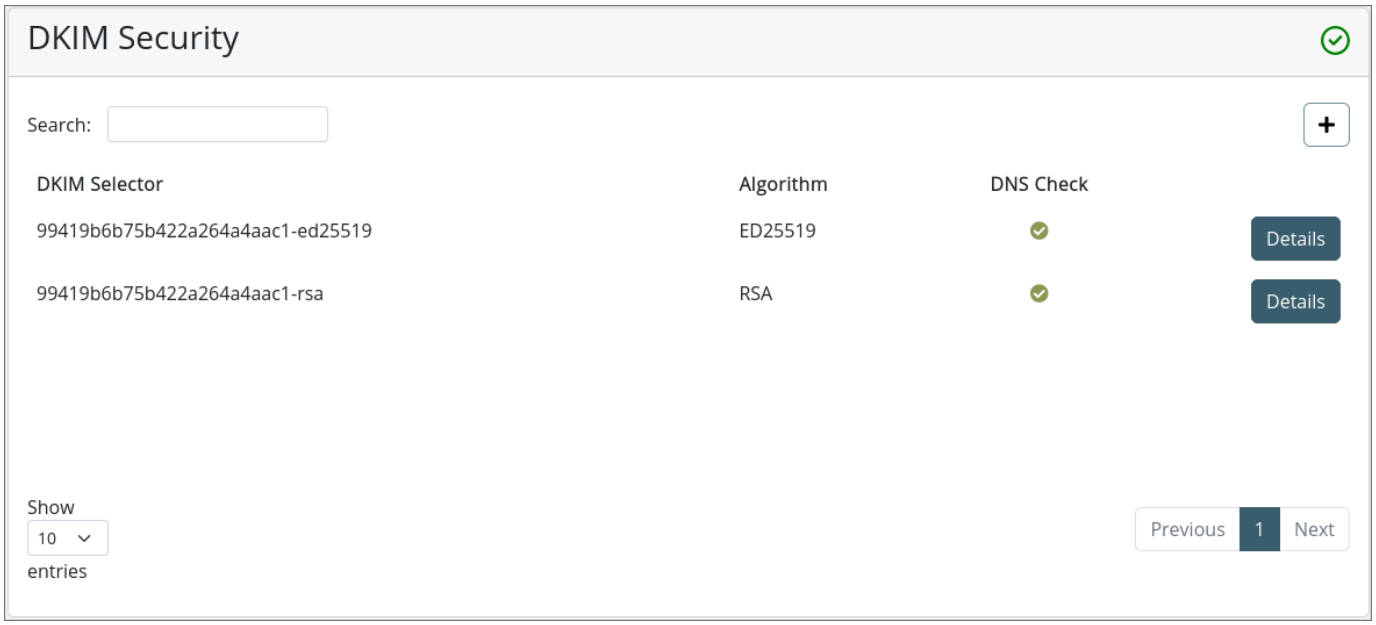
Für jede angelegte Domaine wird automatisch ein DKIM Schlüsselpar erstellt.



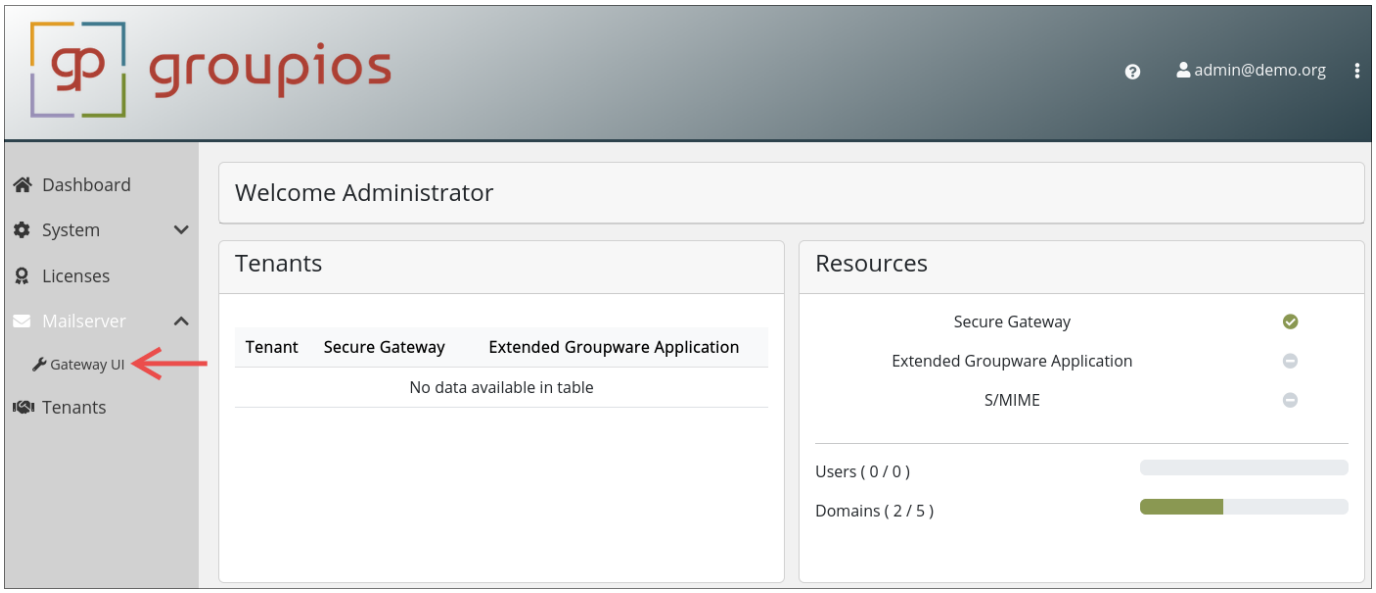
Mit Klick auf "Details" lassen sich jeweils der DKIM DNS Identifier und DKIM Public Key in die Zwischenablage kopieren.



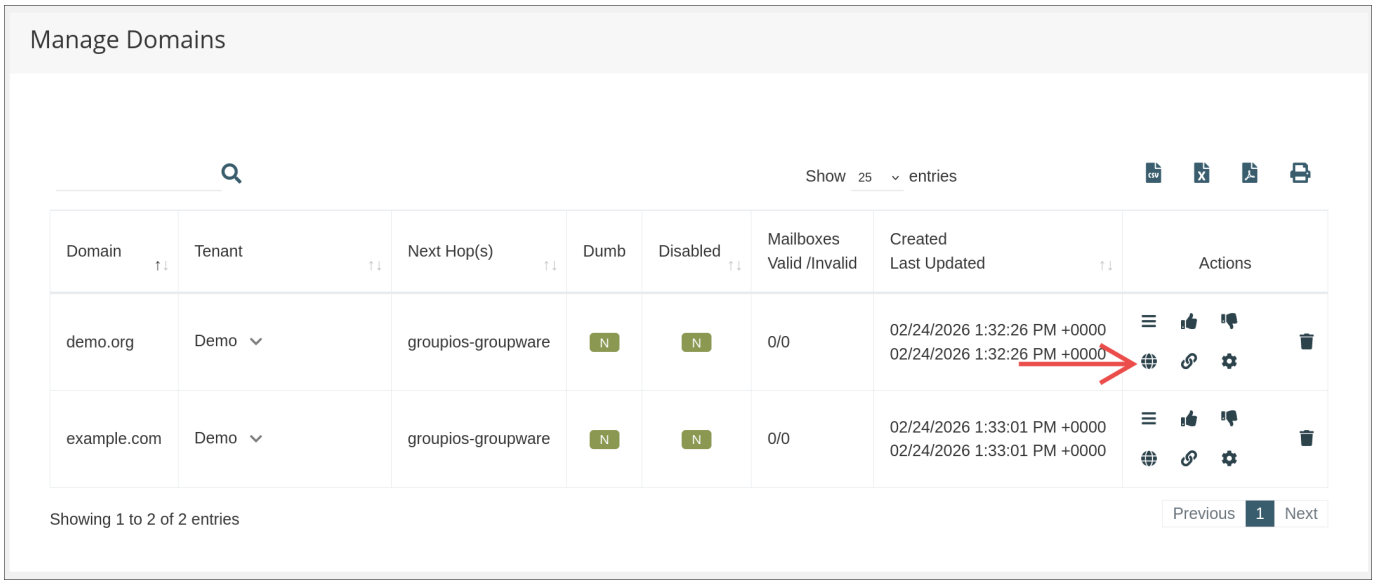
Nachdem der DKIM DNS Eintrag erfolgreich angelegt wurde, wird ein DNS Check überprüfen ob die Einstellungen korrekt angelegt wurden:



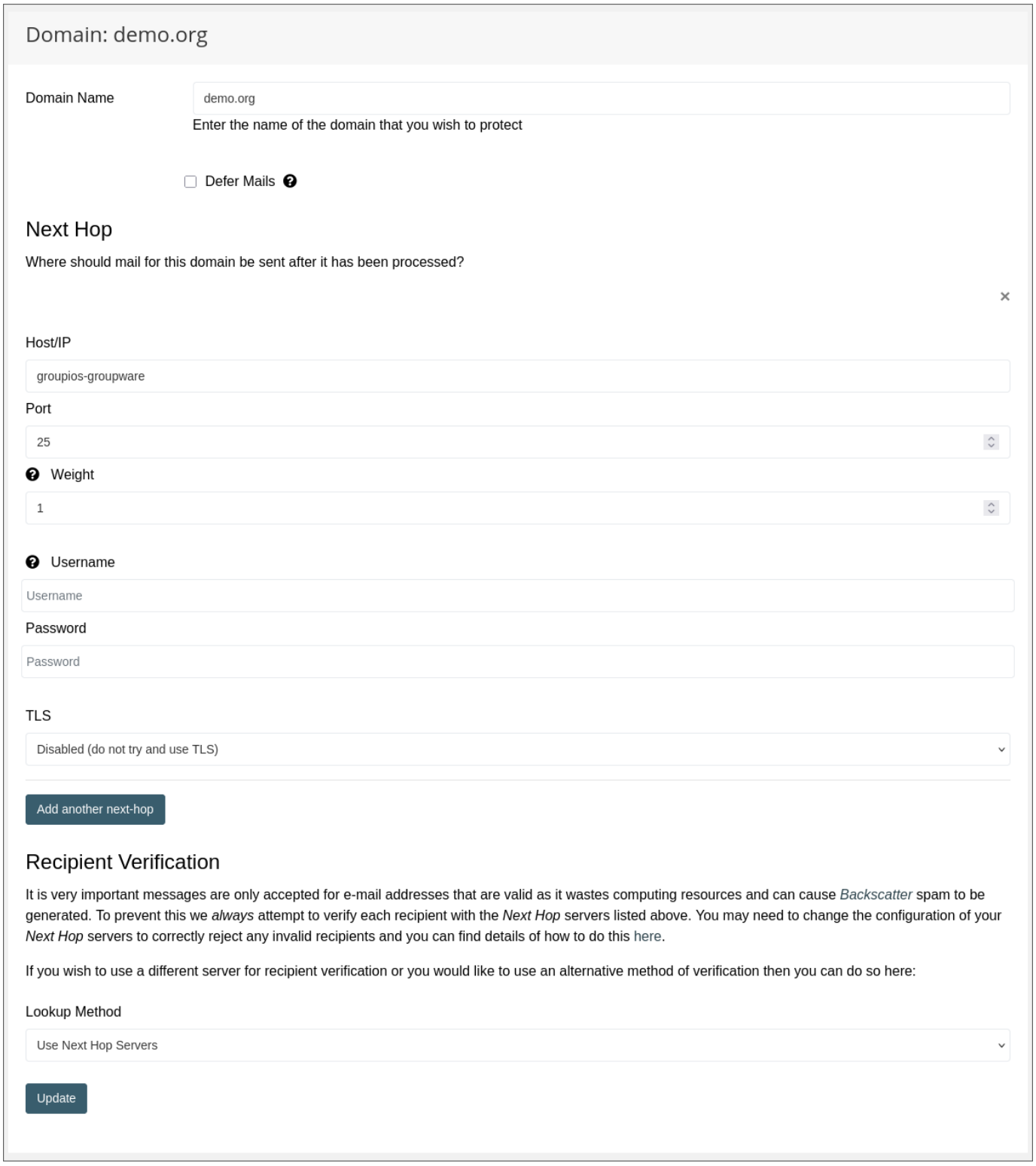
2.2 Next-Hop



Im Gateway Interface können für die Domainen Next-Hop(s) eingestellt werden.



E-Mails, die an die ausgewählte Domain gesendet werden, werden an die hier angegebenen Host(s) zugestellt. Sie können beliebig viele Hops hinzufügen, indem Sie auf „Add another next-hop“ klicken. Antwortet der erste Next-Hop-Server nicht, wird automatisch der nächste versucht, bis zum letzten Eintrag. Ist auch dieser nicht erreichbar, wird die Nachricht in die Warteschlange gestellt und später erneut zugestellt.



2.2.1 Empfänger Verifizierung

Das groupios Mare Gateway versucht stets, jeden Empfänger zu verifizieren. Es ist äußerst wichtig, dass Nachrichten nur an E-Mail-Adressen akzeptiert werden, die auf dem Backend-Mailserver gültig sind. Andernfalls werden Rechenressourcen verschwendet und Backscatter-Spam kann entstehen.

Dazu führt das Gateway eine Dummy-SMTP-Transaktion durch, indem es sich mit den angegebenen Hosts verbindet und den tatsächlichen Empfänger zusammen mit einem Dummy-Empfänger sendet. So wird getestet, ob der Host ungültige Empfänger ablehnen kann (oder über eine Catch-All-Adresse verfügt).

Akzeptiert ein Host ungültige Empfänger, wird ein Cache-Eintrag erstellt. Die Empfängerverifizierung wird erst fortgesetzt, wenn dieser Cache-Eintrag nach 24 Stunden abläuft. Anschließend wird der Host erneut getestet und gegebenenfalls ein neuer Cache-Eintrag erstellt.

Da die Empfängerverifizierung häufig durchgeführt wird, kommt ein Verbindungspool zum Einsatz. So können mehrere Empfänger über dieselbe Verbindung verifiziert werden, ohne dass eine erneute Verbindung erforderlich ist. Standardmäßig bleibt die Pool-Verbindung 5 Minuten lang geöffnet, und es sind maximal 10 Verbindungen gleichzeitig zulässig.

Sobald ein Empfänger verifiziert wurde, wird das Ergebnis für eine Stunde zwischengespeichert. Ungültige Empfänger werden für fünf Minuten zwischengespeichert. Der Cache-Eintrag wird jedoch nur verwendet, wenn keine Verbindung aus dem Verbindungspool verfügbar ist.

Dies dient dazu, eine möglichst genaue Antwort zu liefern und den Verbindungspool zu schonen.

Standardmäßig werden die Empfänger mit den Next-Hop-Servern überprüft. Über das Dropdown-Menü „Abfragemethode“ können Sie „SMTP“ auswählen und einen oder mehrere andere SMTP-Server für die Empfängerverifizierung konfigurieren. Sie können mehrere Hosts angeben, indem Sie diese durch Komma, Leerzeichen oder Semikolon trennen.

2.3 Konfiguration

Nach dem Erstellen einer Domain können Sie domänenspezifische Konfigurationseinstellungen festlegen, indem Sie auf das Zahnrad-Symbol neben einem Eintrag in der Domainliste klicken:

Folgende Einstellungen können gesetzt werden:

- **Core** – Grundeinstellungen des Mailfilters/Gateways (globale Limits und Basisverhalten).
- **Pre-DATA Checks** – Prüfungen vor dem vollständigen Annehmen der Nachricht (frühes Blocken, spart Bandbreite/Ressourcen).
- **Anti-Virus** – Viren- und Malwareprüfung von E-Mails und Anhängen (Erkennen und ggf. Blockieren schädlicher Inhalte).
- **Post-DATA Checks** – Prüfungen nach Annahme des Nachrichteninhalts (z. B. Spam-Scoring, Content-Analyse, weitere Richtlinien).
- **Anhänge** – Regeln zur Behandlung von Dateianhängen und Archiven (Dateitypen, Namen, Größen, Verschachtelung).
- **Alerts** – Einstellungen für automatische Warnmeldungen bei sicherheitsrelevanten oder technischen Ereignissen.
- **Reports** – Konfiguration geplanter Berichte/Statistiken (Zeitplan, Empfänger, Zeitzone).
- **Ausnahmen** – Regeln, um bestimmte Absender/Empfänger/Domains/Inhalte von Prüfungen oder Aktionen auszunehmen.

2.3.1 Core

Maximum Message Size

Dies legt die global maximal zulässige Nachrichtengröße fest. Überschreitet eine Nachricht diese Größe, wird sie mit `Message too big!` abgewiesen.

Spam Tag

Diese Option ermöglicht es, ein benutzerdefiniertes Tag festzulegen, das beim Markieren von möglichem Spam an die Betreffzeile angehängt wird. Der Standardwert ist: `[SPAM]`

2.3.2 Pre-DATA Checks

Pre-DATA-Prüfungen werden ausgeführt, bevor der eigentliche Nachrichteninhalt (Message Body) verarbeitet wird. Das Zurückweisen von Nachrichten in dieser Phase ist sehr wichtig, da dadurch erhebliche Rechenressourcen eingespart werden. Alle Pre-DATA-Zurückweisungen werden grundsätzlich so lange zurückgestellt, bis jeder Empfänger der Nachricht erfasst wurde, damit Black- oder Whitelisting für jeden Empfänger angewendet werden kann.

Bounce Messages

Bounce-Nachrichten bzw. Zustellbenachrichtigungen (Message Delivery Notifications, MDNs) werden gesendet, wenn eine Nachricht von einem SMTP-Server angenommen wurde, die anschließende Zustellung durch diesen Server an das Ziel jedoch fehlschlägt (z. B. weil der Empfänger ungültig ist). Sie sind für das Funktionieren von E Mail wichtig und informieren den Absender bei fehlgeschlagener Zustellung, damit er weiß, dass die gesendete Nachricht nicht angekommen ist und nicht einfach „im Nirwana“ verschwunden ist. Allerdings können sie auch zum Problem werden, wenn jemand Ihren Domainnamen fälscht (Spoofing) und damit Spam an schlecht konzipierte Systeme sendet; dann kann es passieren, dass Ihre Benutzer mit einer Flut von Bounce-Nachrichten für E Mails überhäuft werden, die sie gar nicht gesendet haben.

SINGLE RECIPIENT ONLY

Bounce-Nachrichten zurückweisen, die mehr als einen Empfänger haben.

ENABLE BACKSCATTERER DNSBL LIST

Prüft die IP-Adresse der einliefernden Verbindung gegen die spezielle DNSBL **ips.backscatterer.org**, die Hosts auflistet, die Backscatter an Trap-Adressen erzeugen. Diese Liste wird nur für Nachrichten mit leerem Return-Path (Null Return-Path) abgefragt und nicht für normale Nachrichten.

REJECT ALL

Alle Bounce-Nachrichten zurückweisen. Nicht empfohlen, außer unter außergewöhnlichen Umständen.

Greylisting

Greylisting verzögert absichtlich Nachrichten von unbekannten Servern für kurze Zeit, um nachzuweisen, dass der Server die Nachricht später korrekt erneut zustellt (dies ist ein erforderliches Verhalten eines Mailservers). Diese Verzögerung verbessert außerdem die Wirksamkeit von DNS-Blacklists erheblich, da zwischen der Erkennung von Spam und der Aufnahme der IP oder Domain in eine Blacklist naturgemäß eine zeitliche Verzögerung liegt.

2.3.3 Anti-Virus

Anti-Virus-Prüfungen werden anders behandelt als Spam-Prüfungen. Whitelisting über ACLs gilt für diese Prüfungen nicht, um jede Möglichkeit auszuschließen, dass ein Virus durchgelassen wird.

Reject Broken Executable

Beschädigte Windows-PE- oder Linux-ELF-Programme zurückweisen.

Reject Encrypted archives

Verschlüsselte ZIP- oder RAR-Archive zurückweisen.

Enable PUA signatures

Potentiell unerwünschte Anwendungen (PUA) zurückweisen.

Reject OLE2 Macros

Nachricht zurückweisen, wenn ein Anhang ein OLE2-Makro enthält, z. B. ein Microsoft-Office-Dokument.

Enable Google Safebrowsing signatures

Nachricht zurückweisen, wenn eine URL gefunden wird, die auf der Google Safe Browsing Liste steht.

Enable Phishing signatures

Nachricht zurückweisen, wenn eine Phishing-Signatur erkannt wird.

Exclude List

Viren, die dieser Liste entsprechen (ein Eintrag pro Zeile), nicht zurückweisen. Stattdessen wird ein Header **X-Haraka-Virus:** eingefügt und für das Scoring verwendet. Kommentare werden mit **#** eingeleitet, Treffer sind **nicht groß-/kleinschreibungssensitiv**. Muster werden entweder über **Wildcards** (z. B. `*` und `?`) oder per **Regex** angegeben, indem das Muster in `//` eingeschlossen wird. Um einen Treffer zu **negieren** (z. B. „zurückweisen, wenn es passt“), wird dem Muster ein **!** vorangestellt. Negative Treffer werden immer zuerst geprüft.

2.3.4 Post-DATA Checks

Prüfungen, die erst nach dem vollständigen Empfang der E-Mail (inkl. Body und Anhänge) ausgeführt werden. Sie ermöglichen inhaltsbasierte Analysen wie Spam-Scoring, Viren-/Signatur- und Anhangprüfungen sowie Richtlinienentscheidungen (z. B. markieren, in Quarantäne verschieben oder ablehnen).

Watermarking

Watermarking nimmt eine kleine Änderung an ein- und ausgehenden Nachrichten vor, sodass das System beim Empfang einer eingehenden Nachricht erkennen kann, dass es sich um eine Antwort handelt. Dadurch können ungültige Bounce-Nachrichten abgewiesen werden und Antworten können die Spam-Prüfungen umgehen. Das reduziert die Gesamtlast des Systems und verhindert False-Positives. Am besten funktioniert es, wenn alle ausgehenden E-Mails für eingehende Domains diese Watermarks enthalten.

REJECT BOUNCES WITHOUT WATERMARK

Bounce-Nachrichten zurückweisen, die keinen gültigen Watermark im Nachrichteninhalt enthalten. Dies sollte nur aktiviert werden, wenn der gesamte ausgehende Traffic der Domain mit Watermarks versehen ist.

Rspamd

Ein leistungsfähiger Spamfilter, der E-Mails per Regelwerk und Scoring analysiert (Header, Inhalt, URLs, Anhänge usw.) und je nach Score Nachrichten markiert, in Quarantäne verschiebt oder ablehnt.

TAG SCORE

Rspamd-Score, ab dem die Nachricht im Betreff gekennzeichnet wird und ein Header **X-Spam-Flag: YES** hinzugefügt wird.

QUARANTINE SCORE

Rspamd-Score, ab dem die Nachricht in Quarantäne verschoben wird.

REJECT SCORE

Rspamd-Score, ab dem die Nachricht zurückgewiesen wird.

RELAY REJECT SCORE

Rspamd-Score, ab dem eine Nachricht von einem Relay zurückgewiesen wird.

Verschiedenes/Experimentell

REJECT UNREPLYABLE MESSAGES

Stellt sicher, dass eine Nachricht einen **Reply-To**-, **From**- oder **Sender**-Header enthält, dessen Domainname zu einem gültigen **MX-Record** auflöst, und weist die Nachricht andernfalls zurück. **Strict** bevorzugt es, nur einen der Header in der angegebenen Reihenfolge zu prüfen.

PREVENT SPOOFING OF LOCAL DOMAINS

Weist E-Mails zurück, die einen **Reply-To**-Header mit einer Domain angeben, die nicht der Domain im **From**-Header entspricht.

MARK FROM HEADER

Verbessert die Sichtbarkeit der Nachrichtenherkunft für Benutzer und liefert explizite Warnhinweise zu möglichen Phishing-, Virus- oder Spam-Bedrohungen. Dabei wird der Anzeigename im „From"-Header angepasst. Füge **„[INSECURE]"** hinzu, wenn die Nachricht über einen unverschlüsselten Kanal empfangen wurde. Füge **„[UNVERIFIED]"** hinzu, wenn der Host, der die Nachricht zustellt, nicht der Domain zugeordnet/authentifiziert werden kann. Wenn der Envelope-From nicht mit dem From-Header übereinstimmt: Umschreiben zu **„** `<envelope-from> on behalf of <from>` **"**. Umschreiben zu **„** `<display name> via <list> <from>` **"**, wenn die Nachricht über eine Mailingliste empfangen wurde.

2.3.5 Attachements

Anhangfilterung ist eine erste Verteidigungslinie gegen Viren/Malware, da viele Schadprogramme bereits blockiert werden können, indem bestimmte Dateiendungen verhindert werden.

- `*` = beliebige Zeichenfolge
- `?` = genau ein Zeichen.

> **Notiz**
>
> Groß-/Kleinschreibung wird nicht berücksichtigt.

Filename Rules

Liste der abzulehnenden Dateinamen, ein Eintrag pro Zeile. Platzhalter:

Archive Filename Rules

Liste der abzulehnenden Dateinamen (wenn sie in Archiven gefunden werden).

Maximum Archive Depth

Maximale Verschachtelungstiefe von Archiven innerhalb von Archiven. Alles, was diesen Wert überschreitet, wird abgelehnt. Ein Wert von 0 (Null) lehnt alle verschachtelten Archive ab.

MIME-Type Rules

Liste der abzulehnenden MIME-Typen, ein Eintrag pro Zeile. Die MIME-Typen jedes Nachrichtenteils und jedes Anhangs werden geprüft.

2.3.6 Warnmeldungen

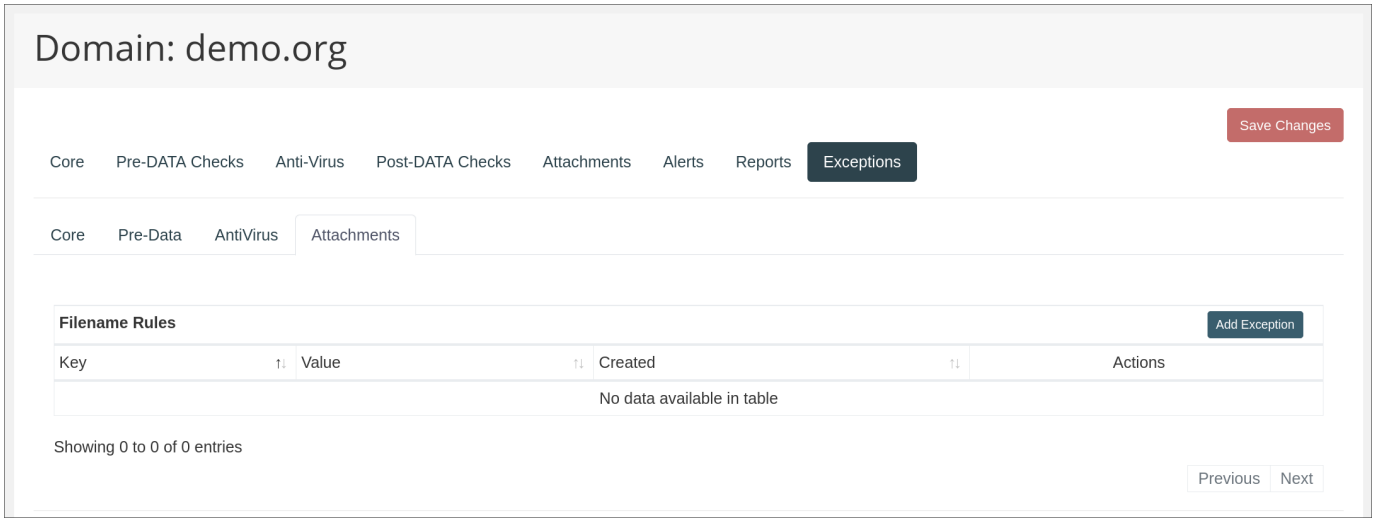
Warnmeldungen werden gesendet, wenn ein vertrauenswürdiger Host (z. B. ein Relay oder ein SMTP-AUTH-Client) etwas Unerwartetes tut, z. B. die konfigurierten Rate-Limits überschreitet oder eine Nachricht sendet, die abgelehnt wird.

2.3.7 Berichte

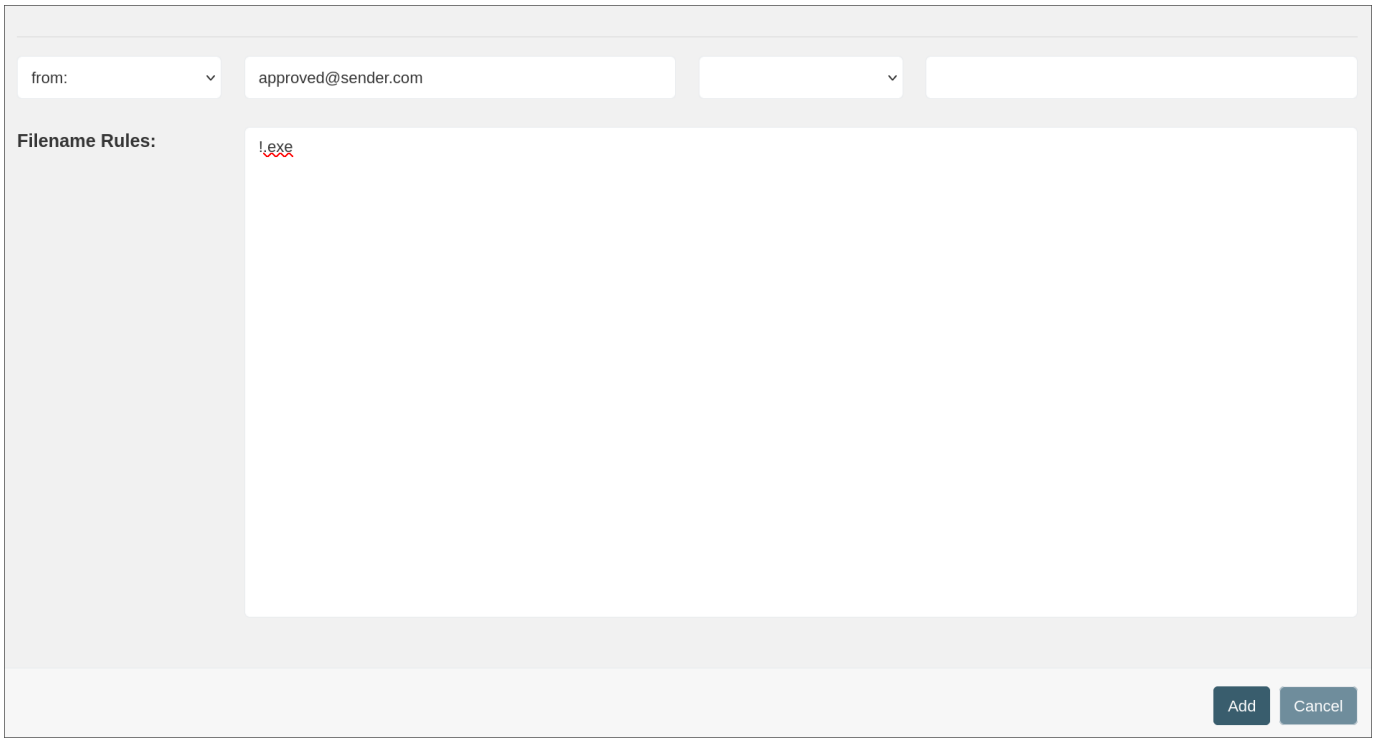
Berichte werden an jede E Mail-Adresse gesendet, für die es Nachrichten gibt, die aus irgendeinem Grund nicht angenommen wurden (z. B. zurückgestellt/deferred, in Quarantäne verschoben oder abgelehnt). Der Bericht zeigt, wie effektiv der Filter für jede Adresse ist, und ermöglicht das Anzeigen oder Freigeben von Quarantäne-Nachrichten.

2.3.8 Ausnahmen

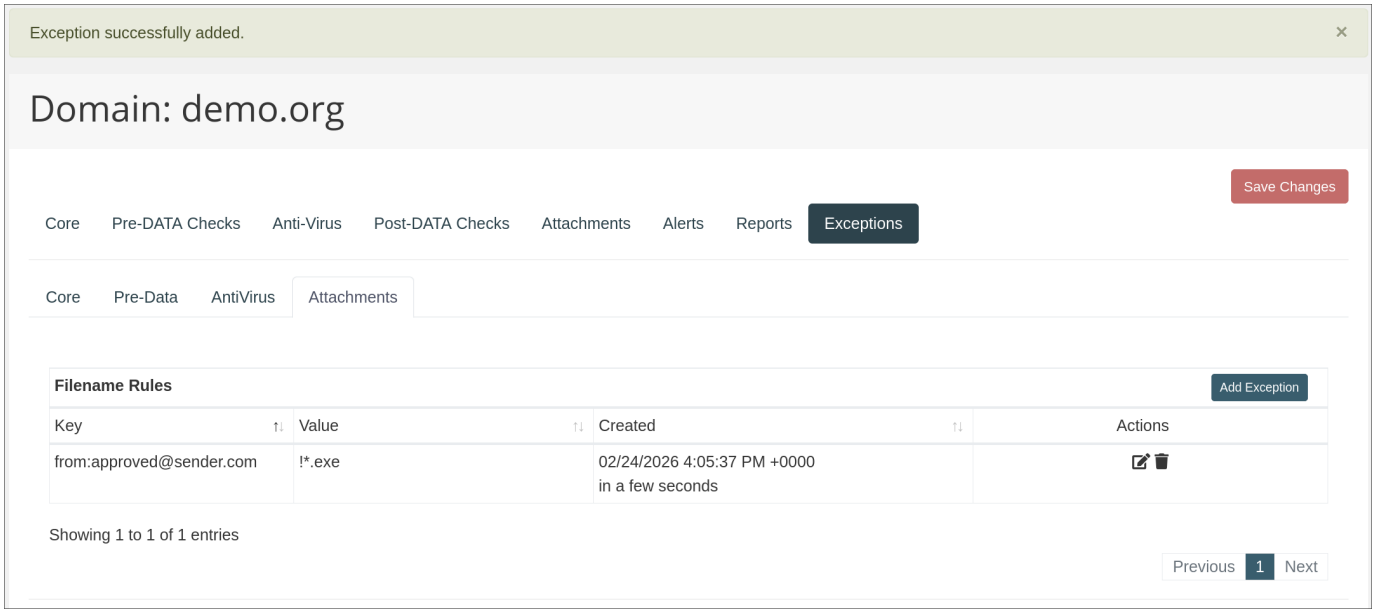
Es ist möglich Ausnahmeregeln für eine Domain festzulegen, indem Sie die Schaltfläche „Add Exception" im Abschnitt „Exception" der Konfigurationsansicht verwenden:



Es öffnet sich ein Modalfenster, in dem Sie eine Regel festlegen können, die angewendet werden soll (hier erlauben wir „approved@sender.com", uns „.exe"-Dateien zu senden):



Die resultierende Ausnahme kann in der Listenansicht bearbeitet und gelöscht werden:



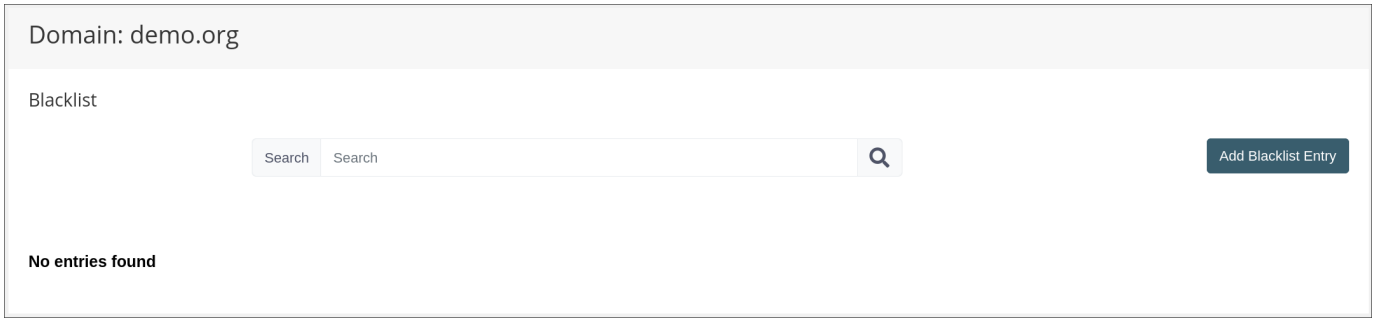
Notiz

Wenn Sie eine Regel für Dateinamen oder Archivdateinamen hinzufügen, achten Sie darauf, jede Dateinamenregel in eine separate Zeile zu setzen. Bei Ausnahmen sollten die Werte mit einem Ausrufezeichen „!“ versehen werden (dies wird jedoch beim Speichern der Regel automatisch korrigiert).

2.4 Black/Whitelists

Black- und Whitelists ermöglichen gezielte Ausnahmen von den Standardregeln: Über **Whitelists** können vertrauenswürdige Absender, Empfänger, Domains oder IPs ausdrücklich zugelassen bzw. von bestimmten Prüfungen ausgenommen werden. **Blacklists** blockieren unerwünschte Absender, Domains oder IPs zuverlässig. So lassen sich Fehlalarme reduzieren und bekannte Spam- oder Angriffquellen schnell sperren.

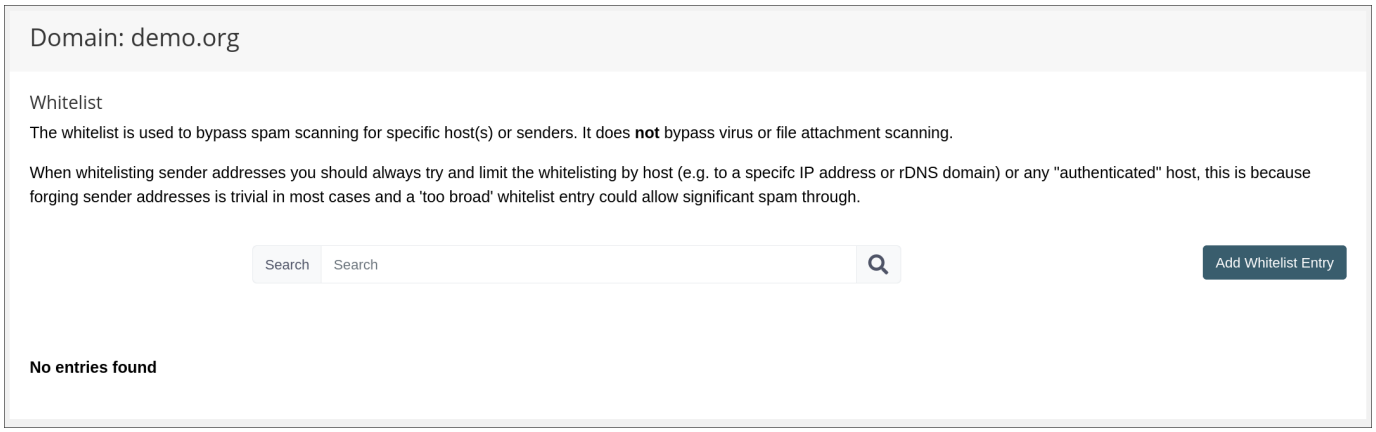
2.4.1 Blacklist

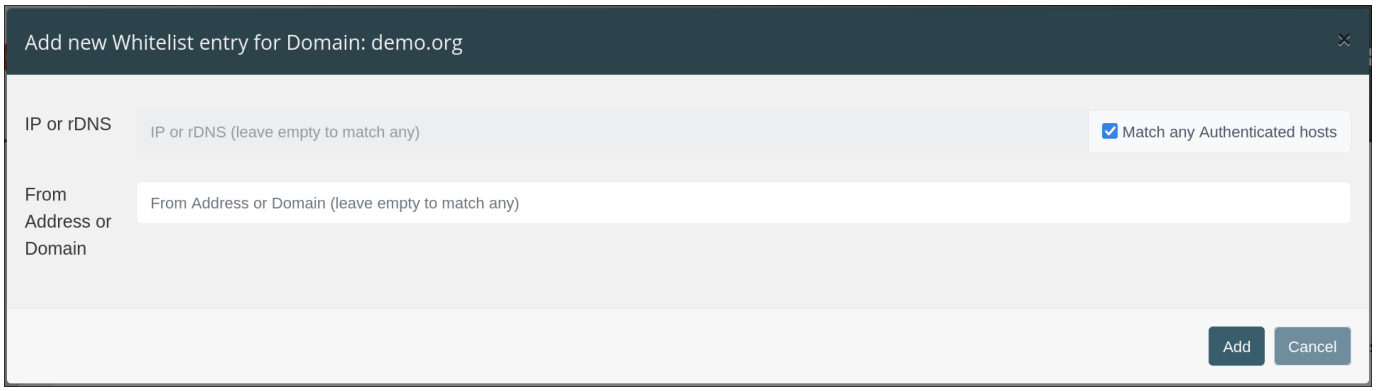


2.4.2 Whitelist

Die Whitelist wird verwendet, um die Spam-Prüfung für bestimmte Hosts oder Absender zu umgehen. Sie umgeht jedoch nicht die Virenprüfung oder die Prüfung von Dateianhängen.

Beim Whitelisting von Absenderadressen sollten Sie die Freistellung nach Möglichkeit immer über den Host einschränken (z. B. auf eine bestimmte IP-Adresse oder rDNS-Domain) oder auf „authentifizierte“ Hosts begrenzen. Der Grund ist, dass Absenderadressen in den meisten Fällen leicht gefälscht werden können und ein zu weit gefasster Whitelist-Eintrag erheblichen Spam durchlassen könnte.





3. Mailserver

3.1 Mailserver Konfiguration

Alle Domains, für die groupios Mare Cloud Gateway für eingehende E Mails konfiguriert ist, sollten sicherstellen, dass ihre Mailserver so eingerichtet sind, dass:

- **Alle Spam-Prüfungen deaktiviert sind**, um unnötige I/O durch doppelte Prüfungen zu vermeiden, Backscatter zu verhindern (wenn diese Spam-Prüfungen bei der Zustellung durch groupios Mare Cloud Gateway eine SMTP-Ablehnung zurückgeben, wird groupios Mare Cloud Gateway gezwungen, eine Bounce-Nachricht an den Absender zu erzeugen) und Support-Probleme zu vermeiden, die durch ungenaue Spam-Prüfungen auf dem Mailbox-Host entstehen können.
- **Alle Rate-Limits und Drosselungen deaktiviert sind**, da dies sonst zu Zustellfehlern oder Verzögerungen führen kann.
- **Alle SMTP-Proxy-Funktionen der Firewall bzw. Protokoll-„Helper“ deaktiviert sind**, z. B. Cisco ESMTP/SMTP Inspection, Cisco PIX Fixup Protocol SMTP (Mailguard), Watchguard SMTP Proxy, Endian Mail Proxy usw.
- So konfiguriert sind, dass **ungültige Empfänger bereits auf SMTP-Ebene abgewiesen werden**. Das ist sehr wichtig, um Backscatter zu verhindern und unnötige I/O im groupios Mare Cloud Gateway zu vermeiden.

Wenn Ihr Mailserver in der Lage ist, Spam-Ergebnisse von einem externen System zu übernehmen oder systemweite Regeln besitzt, um Nachrichten in einen „Spam“- bzw. „Junk“-Ordner zuzustellen, sollten Sie dies anhand des Headers `X-Spam-Flag: YES` konfigurieren.

3.2 Exchange Online

Für eine Domain, die durch groupios Mare Cloud Gateway geschützt wird, sollten die folgenden Einstellungen im **Microsoft 365 Exchange Admin Center** konfiguriert werden. Diese Regeln stellen sicher, dass Microsoft 365 von groupios Mare Cloud Gateway als Spam klassifizierte Nachrichten entsprechend behandelt und in den **„Junk"-Ordner** des Benutzers zustellt, und dass Microsoft 365 keine zusätzliche Filterung durchführt.

Zusätzlich sollte jeweils ein Inbound-Connector und ein Outbound-Connector angelegt werden

- Erstellen Sie einen Inbound-Connector, um E-Mail von den groupios Mare Cloud Gateway-Gateways **anzunehmen**.
- Erstellen Sie den Outbound-Connector, um alle ausgehenden E-Mails über die groupios Mare Cloud Gateway-Gateways **zu senden** (optional. Nur erforderlich, wenn ausgehende E-Mail über groupios Mare Cloud-Server geroutet werden soll).

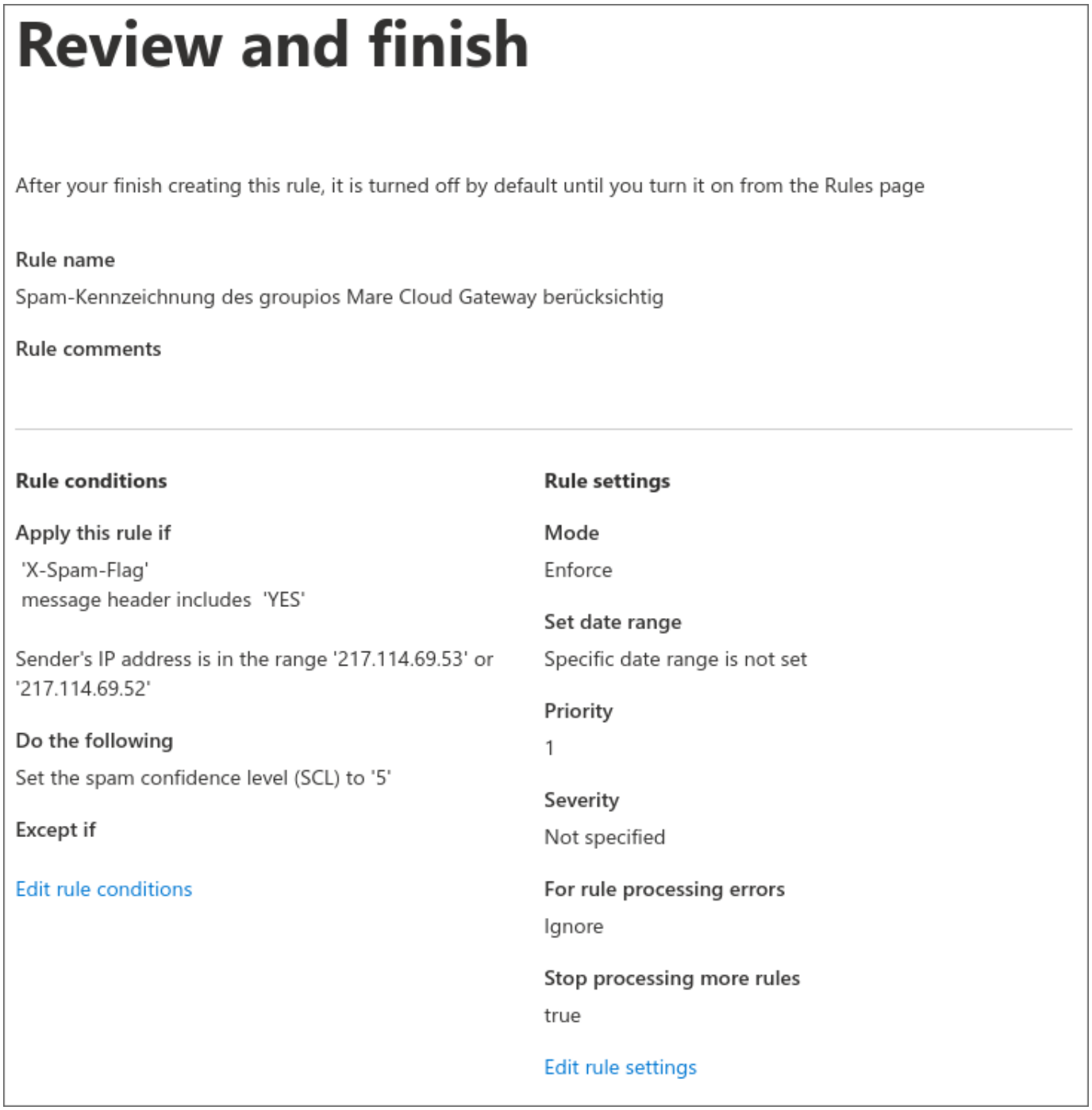
3.2.1 Mail Flow Regeln

Erstellen Sie anschließend die Mailflow-Regel, um E-Mails von den groupios Mare Cloud Gateway-Gateways korrekt zu verarbeiten:

Spam-Kennzeichnung des groupios Mare Cloud Gateway berücksichtigen

1. Gehen Sie zu **„mail flow" -> „rules"**, klicken Sie auf das **„+"**-Symbol und wählen Sie die Option **„Create a new rule"** (Spamfilterung umgehen) und geben Sie die folgenden Einstellungen ein:
2. **Name:** Spam-Kennzeichnung des groupios Mare Cloud Gateway berücksichtigen
3. **Apply this rule if:** A message header…. Includes any of these words.
4. Klicken Sie auf **„Enter Text…"** und geben Sie als Header-Namen **„X-Spam-Flag"** an.
5. Klicken Sie auf **„Enter words…"**, fügen Sie **„YES"** hinzu und klicken Sie auf **„+"**, um es hinzuzufügen. Klicken Sie anschließend auf **„OK"**.
6. Klicken Sie auf **„Add Condition"** und wählen Sie **„The sender… IP address is in any of these ranges or exactly matches"**. Fügen Sie dann die IP-Adressen des groupios Mare Cloud Gateway hinzu. Klicken Sie nach Abschluss auf **„OK"**.
   - `217.114.69.53`
   - `217.114.69.52`
7. Stellen Sie unter **„Do the following…"** sicher, dass **„Modify the message properties"** auf **„set the spam confidence level (SCL) to…"** gesetzt ist. Klicken Sie dann auf den Link **„Set the spam confidence level (SCL) to"** und wählen Sie im Dropdown den SCL-Wert **„5"** aus. Klicken Sie auf **„OK"**.
8. Scrollen Sie nach unten und aktivieren Sie **„Stop processing more rules"**.
9. Klicken Sie auf **„Save"**.

Die Regel sollte wie folgt aussehen:

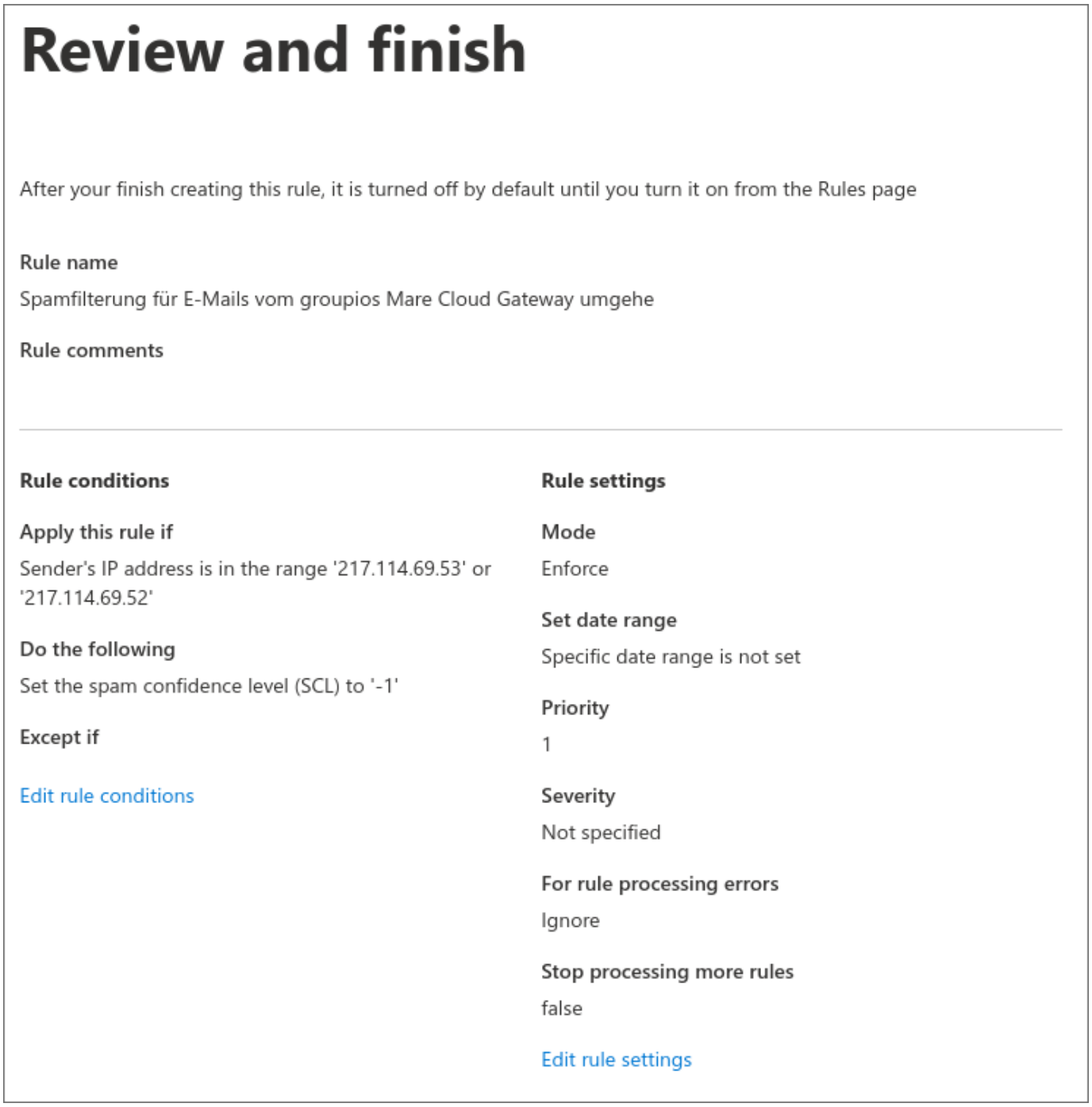


Deaktivieren der Exchange Online Spam Checks

1. Fügen Sie eine weitere Regel hinzu: Klicken Sie auf das **„+“**-Symbol und wählen Sie erneut **„Create a new rule“** und geben Sie die folgenden Einstellungen ein:
2. **Name:** Spamfilterung für E Mails vom groupios Mare Cloud Gateway umgehen
3. **Apply this rule if:** The sender… IP address is in any of these ranges or exactly matches
4. Fügen Sie die IP-Adressen des groupios Mare Cloud Gateway hinzu und klicken Sie auf **„Save“**.
    - `217.114.69.53`
    - `217.114.69.52`

5. Stellen Sie unter **„Do the following…“** sicher, dass **„Modify the message properties“** auf **„set the spam confidence level (SCL) to…“** gesetzt ist. Klicken Sie dann auf den Link **„Set the spam confidence level (SCL) to“** und wählen Sie im Dropdown den SCL-Wert **„Bypass spam filtering“** aus. Klicken Sie auf **„OK“**.
6. Klicken Sie auf **„Save“**.

Die Regel sollte wie folgt aussehen:



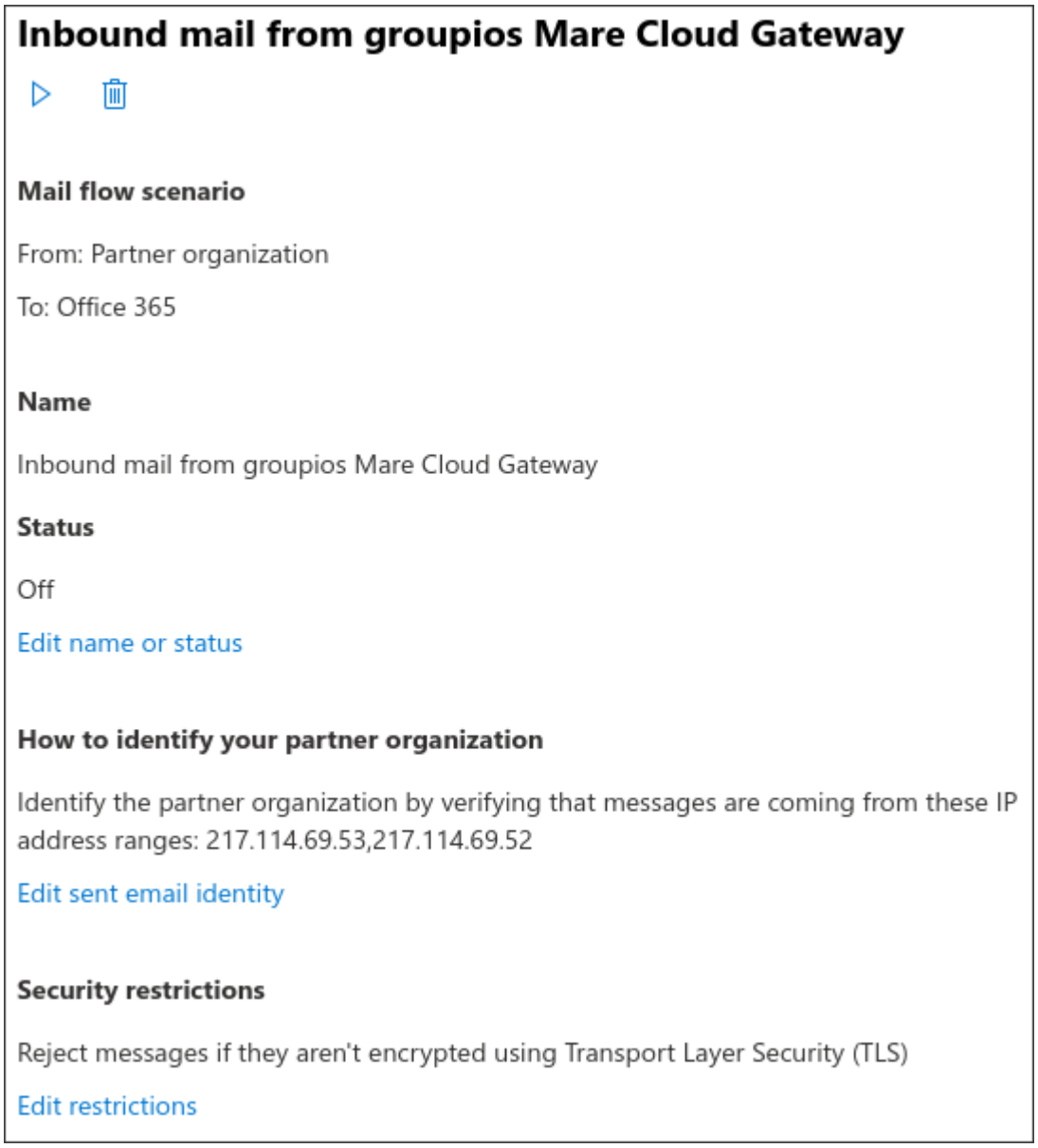
3.2.2 Inbound Connector (E-Mails **von** groupios Mare Cloud Gateway **an** Microsoft 365)

1. Gehen Sie im Microsoft 365 Exchange Admin Center zu **„mail flow“ -> „connectors“** und klicken Sie auf **„+“**, um einen neuen Connector hinzuzufügen.
2. Wählen Sie **From:** „Partner Organization“, **To:** „Microsoft 365“ und klicken Sie auf **„Next“**.

3. Geben Sie als Name z. B. **„Inbound mail from groupios Mare Cloud Gateway“** ein und klicken Sie auf **„Next“**.
4. Wählen Sie die Option, dass eingehende E-Mails anhand der **sendenden IP-Adressen** identifiziert werden (z. B. „By verifying the IP address of the sending server“ / „IP address“), und fügen Sie folgende IPs hinzu:
   - `217.114.69.53`
   - `217.114.69.52`

   Klicken Sie anschließend auf **„Next“**.
5. Überprüfen Sie die Zusammenfassung und klicken Sie auf **„Save“**.

Damit akzeptiert Microsoft 365 eingehende E-Mails, die von den oben genannten IP-Adressen des groupios Mare Cloud Gateway zugestellt werden.



3.2.3 Outbound Connector (E-Mails **von** Microsoft 365 **an** groupios Mare Cloud Gateway)

1. Gehen Sie im Microsoft 365 Exchange Admin Center zu **„mail flow“ -> „connectors“**, klicken Sie auf **„+“**, um einen neuen Connector hinzuzufügen:
2. Wählen Sie **From:** „Microsoft 365“, **To:** „Partner Organization“ und klicken Sie auf **„Next“**.
3. Geben Sie als Name **„Route outbound mail to groupios Mare Cloud Gateway“** ein und klicken Sie auf **„Next“**.

4. Wählen Sie **„Only when email messages are sent to these domains“** und klicken Sie auf **„+“**. Geben Sie als Domainname **„*“** ein und klicken Sie auf **„Ok“**, dann auf **„Next“**.
5. Wählen Sie **„Route email through these smart hosts“** und klicken Sie auf **„+“**. Geben Sie die IP-Adresse oder den Hostnamen der ausgehenden groupios Mare Cloud Gateway-Hosts ein und klicken Sie auf **„Save“**, dann auf **„Next“**.

   Hostnamen:

   - `worker01.groupios-mare.cloud`
   - `smtp.groupios-mare.cloud`
6. Deaktivieren Sie **„Always use Transport Layer Security (TLS) to secure the connection“** und klicken Sie auf **„Next“**. Geben Sie im vorgesehenen Bereich eine externe E-Mail-Adresse ein, um den Connector zu validieren, und klicken Sie auf **„Validate“**.
7. Nach erfolgreicher Validierung klicken Sie auf **„Save“**.

Der hinzugefügte Connector sollte wie in diesem Beispiel aussehen:

Route outbound mail to groupios Mare Cloud Gateway

Mail flow scenario

From: Office 365

To: Partner organization

Name

Route outbound mail to groupios Mare Cloud Gateway

Status

Off

Edit name or status

Use of connector

Use only for email sent to these domains: *

Edit use

Routing

Route email messages through these smart hosts: worker01.groupios-mare.cloud,smtp.groupios-mare.cloud

Edit routing

Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server certificate is issued by a trusted certificate authority (CA).

Edit restrictions

Validation

Last validation result: Validation successful

Last validation time: 2/11/2026, 11:55 AM

Validate this connector

3.3 mailcow

Für eine Domain, die durch groupios Mare Cloud Gateway geschützt wird, sollten die folgenden Einstellungen in der **mailcow Admin-Oberfläche** konfiguriert werden. Diese Konfiguration stellt sicher, dass mailcow von groupios Mare Cloud Gateway bereits gefilterte E-Mails ohne zusätzliche Spam-Prüfung annimmt und dass ausgehende E-Mails über die groupios Mare Cloud Gateway-Server geroutet werden.

Dazu sollten Weiterleitungs-Hosts und Senderabhängige Transport Maps konfiguriert werden:

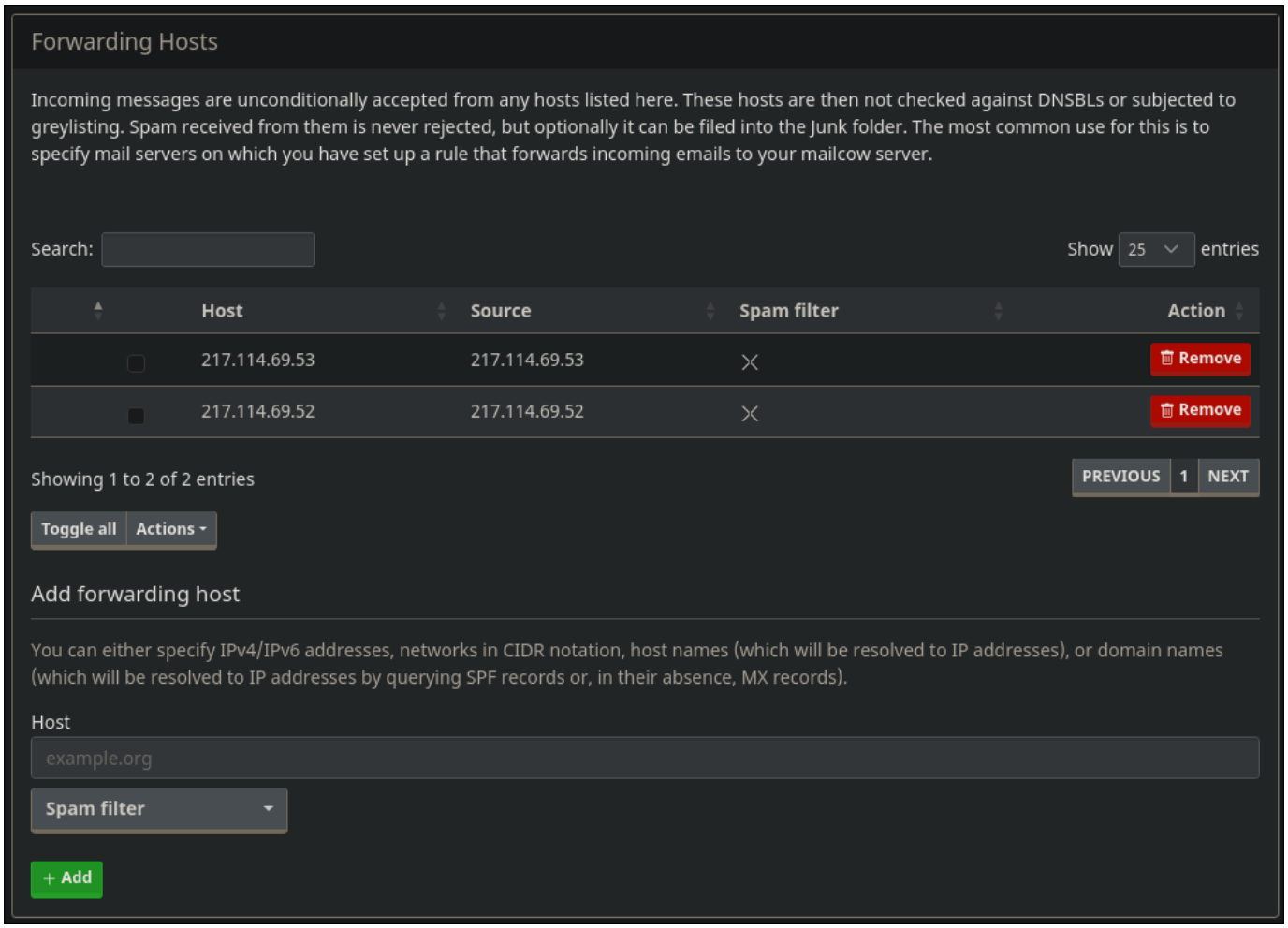
- Erstellen Sie **Weiterleitungs-Hosts**, um die Spam-Filterung für E-Mails von den groupios Mare Cloud Gateway-Servern zu **deaktivieren**.
- Erstellen Sie eine **Senderabhängige Transport Map**, um alle ausgehenden E-Mails über die groupios Mare Cloud Gateway-Server zu **senden** (optional. Nur erforderlich, wenn ausgehende E-Mail über groupios Mare Cloud-Server geroutet werden soll).

3.3.1 Weiterleitungs-Hosts

Durch das Hinzufügen der groupios Mare Cloud Gateway-Server als Weiterleitungs-Hosts wird die Spam-Filterung von mailcow (Rspamd) für E-Mails, die von diesen Servern stammen, deaktiviert. Dies ist notwendig, da die Spam-Filterung bereits durch das groupios Mare Cloud Gateway erfolgt und eine doppelte Prüfung zu unerwünschten Ergebnissen führen kann.

1. Melden Sie sich in der **mailcow Admin-Oberfläche** an und navigieren Sie zu **„System" -> „Konfiguration" -> „Einstellungen" -> „Weiterleitungs-Hosts"** (bzw. **"Weiterleitungs-Hosts"**).
2. Fügen Sie die IP-Adressen der groupios Mare Cloud Gateway-Server als Weiterleitungs-Hosts hinzu:
   - `217.114.69.53`
   - `217.114.69.52`
3. Geben Sie die jeweilige IP-Adresse in das Eingabefeld **„Host"** ein.
4. Wählen Sie als Filter-Typ **„IP"** aus.
5. Aktivieren Sie die Option **„Spam-Filterung inaktiv"**, damit mailcow keine eigene Spam-Bewertung für E-Mails von diesen Hosts vornimmt.
6. Klicken Sie auf **„Hinzufügen"**, um den Weiterleitungs-Host zu speichern.
7. Wiederholen Sie die Schritte 3–6 für die zweite IP-Adresse.

Die Konfiguration sollte wie folgt aussehen:



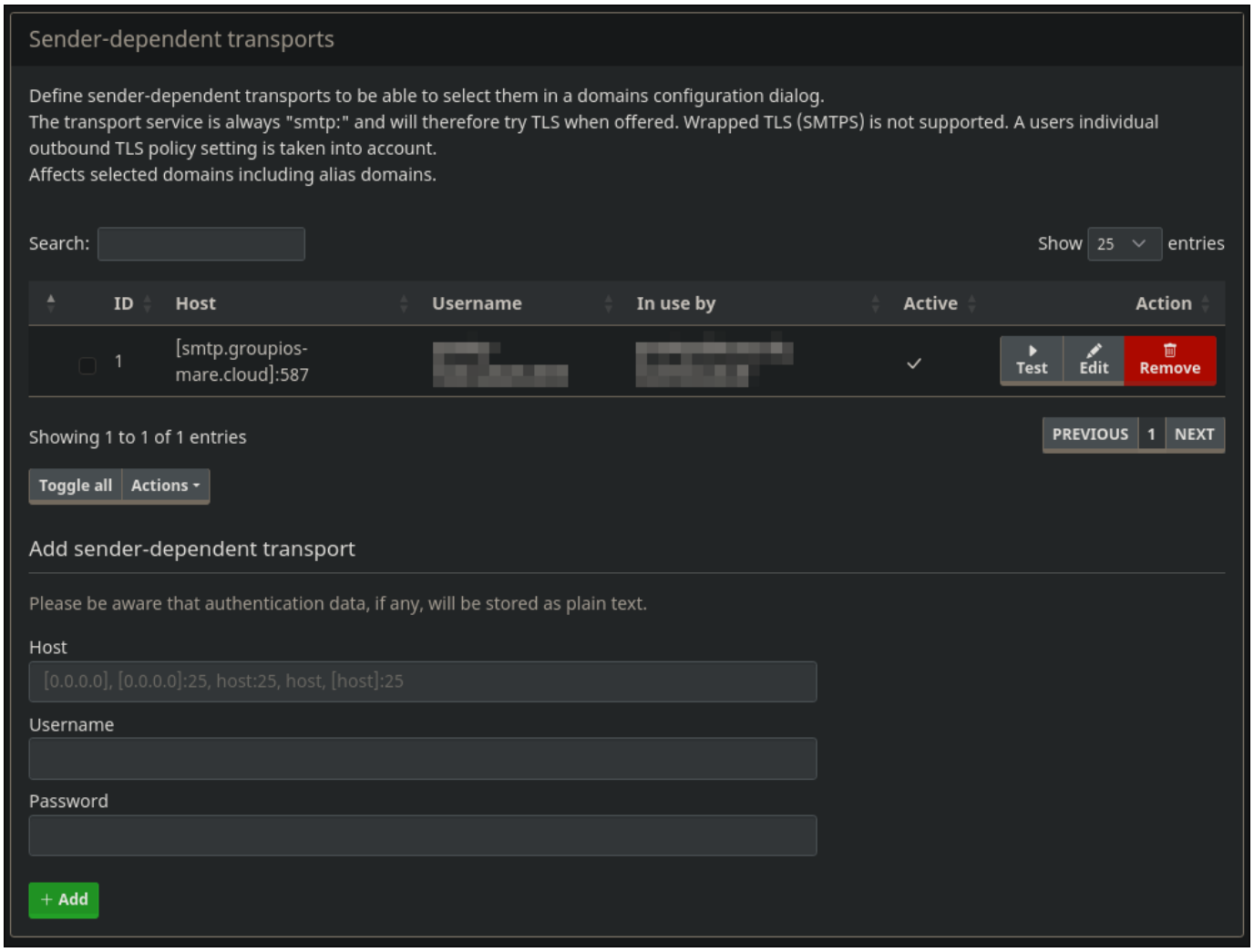
> **Hinweis:** Stellen Sie sicher, dass der MX-Record Ihrer Domain auf die groupios Mare Cloud Gateway-Server zeigt, sodass eingehende E-Mails zuerst vom Gateway gefiltert und anschließend an Ihren mailcow-Server weitergeleitet werden.

3.3.2 Senderabhängige Transport Maps

Durch das Einrichten einer senderabhängigen Transport Map werden alle ausgehenden E-Mails der geschützten Domain über die groupios Mare Cloud Gateway-Server geroutet. Dies ermöglicht eine konsistente Filterung und Signierung ausgehender Nachrichten.

1. Navigieren Sie in der **mailcow Admin-Oberfläche** zu **„System" -> „Konfiguration" -> „Routing" -> „Senderabhängige Transport Maps"**.
2. Geben Sie die folgenden Einstellungen ein:
   - **Ziel (Nexthop):** Geben Sie den Hostnamen des groupios Mare Cloud Gateway-Servers ein:
     - `[smtp.groupios-mare.cloud]:587`
   - **Benutzername:** Wie Ihnen vom groupios Mare Cloud Support mitgeteilt wurde.
   - **Passwort:** Wie Ihnen vom groupios Mare Cloud Support mitgeteilt wurde.
3. Klicken Sie auf **„Hinzufügen"**, um den Transport zu speichern.

Die Transport Map sollte wie folgt aussehen:



1. Navigieren Sie anschließend zu **„E-Mail" -> „Konfiguration" -> „Domains"** und bearbeiten Sie die Domain, für die der ausgehende Transport über das groupios Mare Cloud Gateway erfolgen soll.
2. Wählen Sie im Bereich **„Senderabhängige Transport Maps"** den zuvor erstellten Transport aus dem Dropdown-Menü aus.
3. Klicken Sie auf **„Speichern"**, um die Änderungen zu übernehmen.

Die Domain-Einstellung sollte wie folgt aussehen: