noSpam proxy® CLOUD

Quick Start Guide

Deutsch/German

Rechtliche Hinweise

Alle Rechte vorbehalten. Dieses Dokument und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der Net at Work GmbH, Paderborn, Bundesrepublik Deutschland. Änderungen vorbehalten. Die in diesem Dokument enthaltenen Informationen begründen keine Gewährleistungs- und Haftungsübernahme seitens der Net at Work GmbH. Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der Net at Work GmbH zulässig.

Copyright © 2026 Net at Work GmbH

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Deutschland

Microsoft®, Windows®, Microsoft Exchange®, SQL Server®, SQL Server Express®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft .NET Framework®, Microsoft Report Viewer®, Microsoft Office®, Microsoft 365®, Office 365®, Microsoft Outlook®, Microsoft Visual Studio® und Azure® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® und 32Guards® sind eingetragene Handelsmarken der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern beziehungsweise Inhabern.

DIESES DOKUMENT WURDE ZULETZT AM 17. MÄRZ 2026 ÜBERARBEITET.

Inhalt

Einleitung 1

Konfiguration 2

NoSpamProxy konfigurieren 2

Wie finde ich den notwendigen Wert für die Kopzeile? 54

Regeln 59

Wichtige Hinweise 89

Branding 90

Administration 92

Identitäten 96

Partner 96

Ihre Zertifikate 103

Verwaltete Zertifikate anfordern 105

Überprüfte Domänen für die verwalteten Zertifikate hinzufügen 108

E-Mails filtern 110

Details zu einer E-Mail anzeigen 111

Angehaltene E-Mails 118

Gesperrte Anhänge 120

Status-Typen 121

Reporting 124

Large Files 126

Vorlagen erstellen 128

Eine Vorlage hinzufügen 128

Optionen in der Werkzeugleiste (HTML-Ansicht) 129

Standardvorlagen hinzufügen 131

Regeln hinzufügen 131

Reihenfolge der Regeln ändern 133

Lizenzverwaltung 135

Support 140

Einleitung

Über NoSpamProxy Cloud

NoSpamProxy Cloud ist eine hochverfügbare Plattform für E-Mail-Kommunikation. Neueste technische Entwicklungen und leichte Bedienbarkeit ermöglichen es Ihnen, mit NoSpamProxy Cloud zuverlässig ungewollte E-Mails abzuwehren und Ihr Unternehmen zuverlässig vor Angriffen zu schützen.

Jeder einzelne Stack von NoSpamProxy Cloud ist für maximale Verfügbarkeit konzipiert und erstreckt sich über zwei Availibility Zones.

NoSpamProxy Cloud wird auf Servern in Deutschland betrieben.

Voraussetzungen

- Ein Microsoft-Konto zur Anmeldung bei NoSpamProxy Cloud
- Eine oder mehrere Unternehmensdomänen (keine Freemailer)
- Zugriff auf DNS-Einstellungen der Unternehmensdomänen
- Vollständige Auflistung der gültigen E-Mail-Adressen: E-Mails an ungültige Adressen werden abgewiesen!
- Vorliegende E-Mail-Routing-Informationen: Wohin sollen eingehende E-Mails weitergeleitet werden? Welche Server dürfen E-Mails einliefern?
- TLS-basierte Verbindungsverschlüsselung

Konfiguration

NoSpamProxy konfigurieren

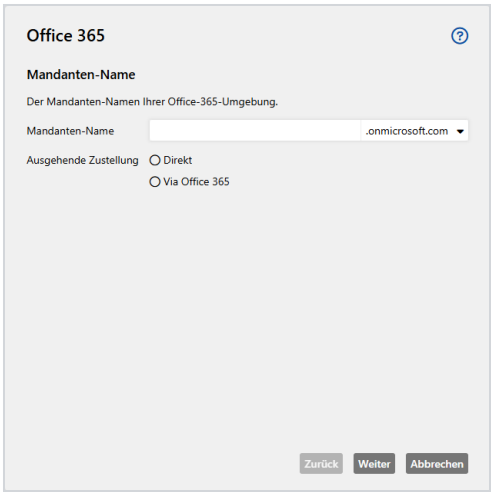
Office 365 einbinden

Falls Sie ein Office-365-Abonnement besitzen, verbinden Sie NoSpamProxy Cloud hier mit Ihrem Office-365-Mandanten.

> **TIP:** Durch das Hinzufügen von Office 365 wird das erforderliche E-Mail-Routing in NoSpamProxy Cloud sowie optional der automatische Benutzerimport bereits eingerichtet. Beachten Sie die unterschiedlichen Zustellungsmethoden: Falls Sie NoSpamProxy Encryption als Standalone-Modul nutzen, wählen Sie **Via Office 365**.

1. Gehen Sie zu **Konfiguration > Office 365**.
2. Klicken Sie **Hinzufügen**.

3. Geben Sie den Mandantennamen Ihrer Office-365-Umgebung an.



4. Wählen Sie eine der folgenden Zustellmethoden:
   - **Direkt|** Wählen Sie diese Option, wenn Sie NoSpamProxy Protection nutzen.
   - **Via Office 365|** Wählen Sie diese Option , wenn Sie ausschließlich NoSpamProxy Encryption als Standalone-Modul nutzen.
5. Spezifizieren Sie die Domänen, für die der Office-365-Konnektor gültig ist und klicken Sie **Weiter**.
6. (Optional) Aktivieren Sie den automatischen Benutzerimport für Ihren Office-365-Mandanten.

> **HINWEIS:** Sie müssen eine mandantenweite Administratoreinwilligung erteilen, um den automatischen Benutzerimport einzurichten. Folgen Sie dazu den Anweisungen im Dialog.

7. Klicken Sie **Beenden**.

Domänen konfigurieren

Domänen hinzufügen

Geben Sie als Erstes die Domänen an, die durch NoSpamProxy Cloud verwaltet werden sollen.

1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Klicken Sie **Hinzufügen**.

3. Geben Sie eine Unternehmensdomäne ein, die durch NoSpamProxyCloud

verwaltet werden soll. Wiederholen Sie diesen Schritt bei Bedarf.

4. Klicken Sie **Hinzufügen** und dann **Speichern**.

DNS-Konfiguration einrichten

Bevor Sie Domänen mit NoSpamProxyCloud verwenden können, müssen sie nachweisen, dass Sie diese Domänen besitzen. Außerdem müssen Sie für die Sicherstellung der E-Mail-Sicherheit verschiedene DNS-Einstellungen vornehmen.

1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Klicken Sie die Domäne, für die Sie die DNS-Konfiguration einrichten wollen und klicken Sie **Zeige DNS-Konfiguration**.
3. Kopieren Sie den unter **TXT** angezeigten Wert in die Zwischenablage und erstellen Sie für diesen Wert einen DNS-Eintrag für Ihre Domäne.

   > **HINWEIS:** Sie können diesen DNS-Eintrag nach erfolgreicher Verifizierung wieder löschen.

4. Hängen Sie den unter **Sender Policy Framework (SPF)** angezeigten Ausdruck an Ihren bestehenden SPF-Eintrag an.
5. Richten Sie die vier **CNAME-Einträge** (und damit die DKIM-Schlüssel für Ihre Domäne) **permanent** bei Ihrem Provider ein.

> **HINWEIS:** Beachten Sie die TTL (Time to Live) der zuvor angepassten CNAME-Einträge und stellen Sie sicher, dass diese übernommen wurden, bevor Sie den MX-Eintrag einrichten.

6. Richten Sie den angezeigten **MX-Eintrag permanent** bei Ihrem Provider ein
7. Klicken Sie **Schließen**.

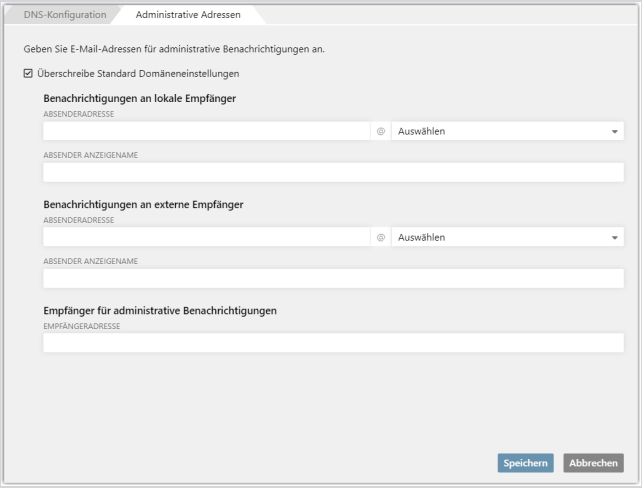
> **HINWEIS:** Falls Sie das Standalone-Modul NoSpamProxy Encryption (ohne NoSpamProxy Protection) nutzen, ist das Setzen der MX- und SPF-Einträge nicht erforderlich.

> **HINWEIS:** Nutzern von Microsoft 365 wird nach dem Einrichten der MX-Einträge eventuell eine Fehlermeldung angezeigt, da die Einträge nicht mehr den standardmäßig erwarteten Werten entsprechen. Sie können diese Fehlermeldung ignorieren.

Administrative Adressen einrichten

NoSpamProxy Cloud benötigt für zu sendenden E-Mail-Benachrichtigungen gültige Absenderadressen sowie eine Adresse, an die administrative Benachrichtigungen gesendet werden. Hinterlegen Sie hier die entsprechenden Adressen.

1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Klicken Sie die Domäne, für die Sie die administrativen Adressen einrichten wollen und klicken Sie **Bearbeiten**.
3. Wechseln Sie zur Registerkarte **Administrative Adressen**.



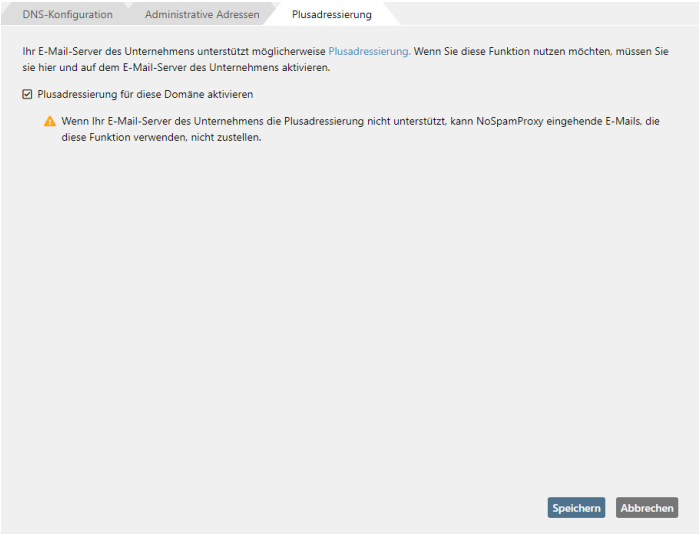
4. Geben Sie Absenderadressen für Benachrichtigungen an lokale und externe Empfänger sowie eine Empfängeradresse an.
5. Klicken Sie **Speichern**.

> **TIP:** Wenn Sie für die jeweilige Domäne die Standard-Domäneneinstellungen für administrative Adressen nutzen wollen, entfernen Sie das Häkchen bei **Überschreibe Standard-Domäneneinstellungen**.

> **HINWEIS:** Falls Sie eine Benachrichtigungsadresse für lokale Empfänger verwenden wollen, der ein Exchange-Konto zugeordnet ist, müssen Sie in Exchange die entsprechende "SendAs"-Berechtigung für diese Adresse setzen.

Plusadressierung einrichten

Plusadressierung (auch bekannt als Unteradressierung) ist eine Methode, um dynamische, verwerfbare E-Mail-Adressen für Postfächer zu unterstützen. Falls aktiviert, ordnet NoSpamProxy beispielsweise der E-Mail-Adresse **max.mustermann+newsletter@example.com** den Unternehmensbenutzer mit der E-Mail-Adresse **max.mustermann@example.com** zu.



WARNING: Wenn Ihr E-Mail-Server des Unternehmens die Plusadressierung nicht unterstützt, kann NoSpamProxy eingehende E-Mails, die diese Funktion verwenden, nicht zustellen.

Plusadressen (auch Unteradressen genannt) werden im Rahmen der Lizenzierung **nicht** gezählt, sofern die Plusadressierung für die jeweilige Domäne aktiviert ist. Dies gilt sowohl für die Lizenzierung der Module als auch für die Lizenzierung von Diensten. Es werden nur die zu Grunde liegenden E-Mail-Adressen der Benutzer gezählt, für die Plusadressen vorliegen.

HINWEIS: Wenn Sie diese Funktion nutzen möchten, müssen Sie sie hier **und** auf dem E-Mail-Server des Unternehmens aktivieren (also beispielsweise Ihrem Exchange-Server).

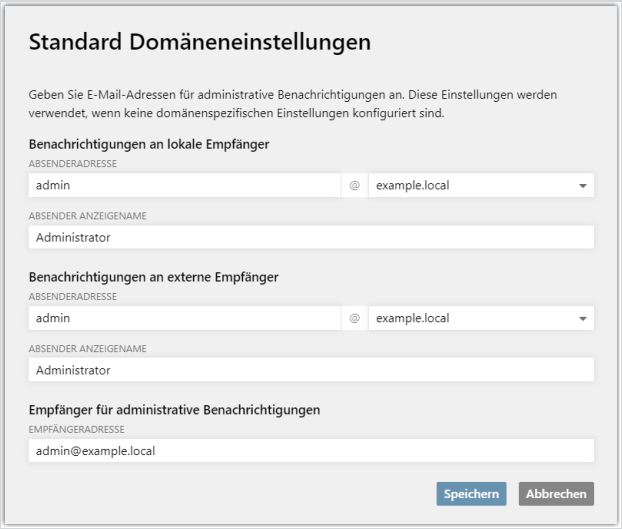
1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Doppelklicken Sie die Domäne, die Sie bearbeiten wollen oder markieren Sie sie und klicken Sie **Bearbeiten**.
3. Wechseln Sie zur Registerkarte **Plusadressierung**.
4. Setzen Sie das Häkchen bei **Plusadressierung für diese Domäne aktivieren**.
5. Klicken Sie **Speichern und schließen**.

> **TIP:** Weitere Informationen finden Sie in der **Microsoft-Dokumentation**.

Standard-Domäneneinstellungen vornehmen

Hinterlegen Sie hier administrative Adressen, die für das Senden von E-Mail-Benachrichtigungen sowie das Empfangen von administrativen Benachrichtigungen genutzt werden, wenn keine spezifischen Einstellungen für die Domäne konfiguriert sind.

1. Gehen Sie zu **Identitäten > Unternehmensdomänen**.
2. Klicken Sie unter **Standard-Domäneneinstellungen** auf **Bearbeiten**.



3. Geben Sie Absenderadressen für Benachrichtigungen an lokale und externe Empfänger sowie eine Empfängeradresse an.
4. Klicken Sie **Speichern**.

Nachdem Sie Ihre Domänen konfiguriert haben und diese Domänen erfolgreich validiert wurden, müssen Sie alle Benutzer hinzufügen, die durch NoSpamProxyCloud verwalten werden sollen. Siehe **Benutzer hinzufügen**.

Benutzer hinzufügen

Automatischer Benutzerimport über Ihren Office-365-Mandanten

Falls Sie Office 365 bereits eingebunden haben, können Sie den automatischen Benutzerimport jederzeit aktivieren und deaktivieren. Gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Office 365**.
2. Klicken Sie neben Ihrem Office-365-Mandanten auf ✎, um diesen zu bearbeiten.
3. Wechseln Sie zur Registerkarte **Benutzerimport**.
4. Aktivieren oder deaktivieren Sie den automatischen Benutzerimport.

   > **HINWEIS:** Sie müssen eine mandantenweite Administratoreinwilligung erteilen, um den automatischen Benutzerimport einzurichten. Folgen Sie dazu den Anweisungen im Dialog.

5. Klicken Sie **Speichern**.

Automatischer Benutzerimport via Azure Active Directory

1. Gehen Sie zu **Identitäten > Automatischer Benutzerimport**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie einen Namen für den Benutzerimport ein und konfigurieren Sie den Status des Benutzerimports.
4. Geben Sie den Namen Ihres Azure-Mandanten an.

   > **HINWEIS:** Sie müssen eine mandantenweite Administratoreinwilligung erteilen, um den automatischen Benutzerimport einzurichten. Folgen Sie dazu den Anweisungen im Dialog.

5. (Optional) Klicken Sie **Hinzufügen**, um eine in Ihrem Azure Active Directory hinterlegte Gruppe hinzuzufügen und konfigurieren Sie diese, um den jeweiligen Benutzern unterschiedliche Funktionen zuzuweisen:

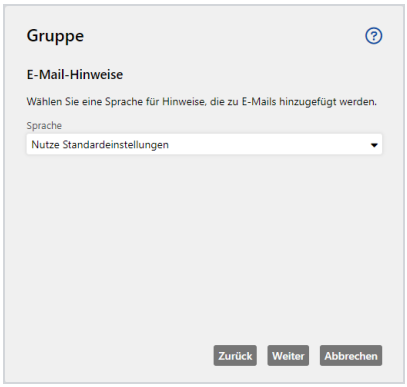
- **Allgemein|** Wählen Sie die Gruppe aus, die Sie hinzufügen wollen.

- **Inhaltsfilterung|** Wird für eingehende und ausgehende E-Mails auf enthaltene Anhänge angewendet. Siehe **Wichtige Hinweise**.

- **CxO Fraud Detection|** Verwendet die Namen aller Gruppenmitglieder, um Phishing-Angriffe zu erkennen. Siehe **Automatischer Benutzerimport**

via Azure Active Directory

- **Sprache|** Wählen Sie eine Sprache für E-Mail-Hinweise und -Benachrichtigungen, die zu E-Mails hinzugefügt werden.



- **Zertifikatsanforderung|** Fordert für Mitglieder dieser Gruppe automatisch S/MIME-Zertifikate an.

6. Klicken Sie **Beenden**.

> **TIP:** Klicken Sie **Jetzt ausführen**, um den Benutzerimport manuell auszulösen.

> **HINWEIS:** NoSpamProxy unterstützt keine öffentlichen Ordner, da diese seitens Azure Active Directory ebenfalls nicht mehr unterstützt werden.

Hinweise

- Damit für alle Benutzer verwaltete Zertifikate angefordert werden können, müssen Sie eine ausreichende Anzahl an Benutzern lizenziert haben. Sollte

beispielsweise die hinzugefügte Gruppe mehr Benutzer enthalten als Lizenzen zur Verfügung stehen, so werden keine verwalteten Zertifikate angefordert. Der Administrator erhält in diesem Fall eine Benachrichtigungs-E-Mail.

- Damit verwaltete Zertifikate für Benutzer angefordert werden können, muss das Benutzerattribut **E-Mail-Adresse** für diese Benutzer hinterlegt sein.

Die **CxO-Betrugserkennung** dient der Erkennung und Abwehr von Phishing-Angriffen, welche die Identität von besonders exponierten Entscheidungsträgern in Unternehmen missbrauchen. Sie vergleicht den Absendernamen aus 'Header-From' und 'MAIL FROM' in eingehenden E-Mails mit den Namen von Unternehmensbenutzern.

Gefälschte E-Mails, die im Namen von Vorgesetzten oder Mitarbeitern an Sie gesendet werden, werden so abgefangen.

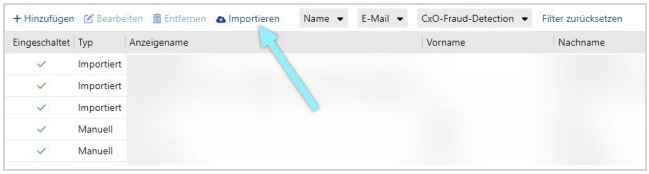
Bei der Überprüfung werden unterschiedliche Varianten des Absendernamens in den Vergleich einbezogen. Hier einige Beispiele:

- Erika Mustermann
- Mustermann Erika
- ErikaMustermann
- MustermannErika

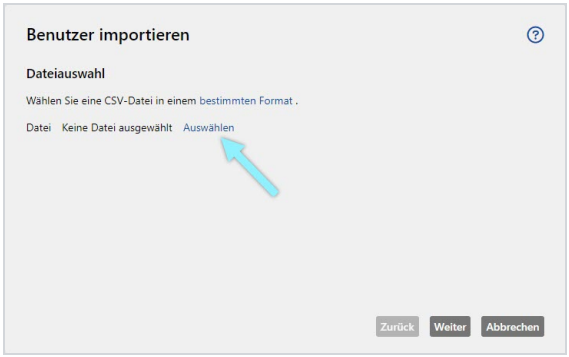
Alle Unternehmensbenutzer, die Sie für die CxO-Betrugserkennung verwenden wollen, müssen Sie dafür einzeln oder bequem per Active-Directory-Gruppen aktivieren.

Benutzer importieren

1. Gehen Sie zu **Identitäten > Unternehmensbenutzer**.
2. Klicken Sie **Importieren**.



3. Klicken Sie im folgenden Dialog **Auswählen**, um eine CSV-Datei von Ihrem Computer auszuwählen und klicken Sie **Weiter**.



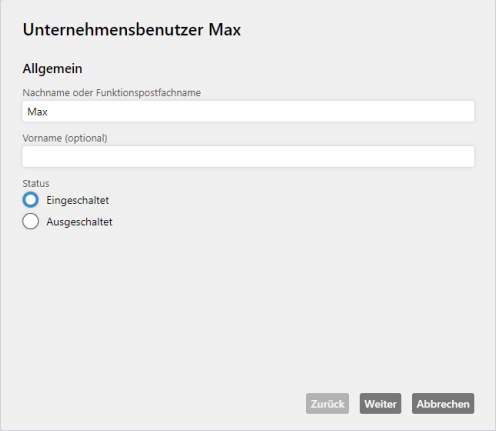
4. Prüfen Sie die angezeigten CSV-Daten auf Gültigkeit und klicken Sie **Beenden**.

```
Surname (required);Primary email address (required);Additional email addresses;CxO fraud detection;Given name
NoSpamProxyTestUser;test@nospamproxy.test;test@nospamproxy.de, test2@nospamproxy.de;true;Test
```

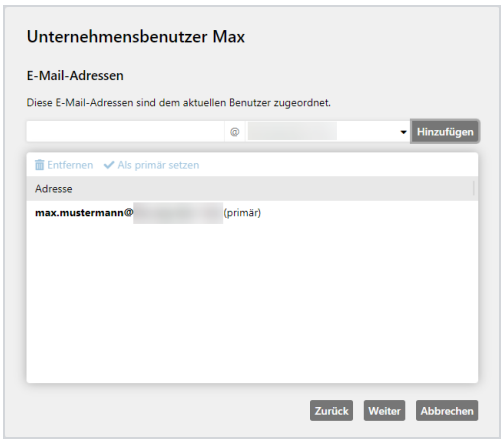
HINWEIS: Die CSV-Datei muss unter Verwendung der UTF-8-Kodierung gespeichert worden sein.

Benutzer manuell hinzufügen

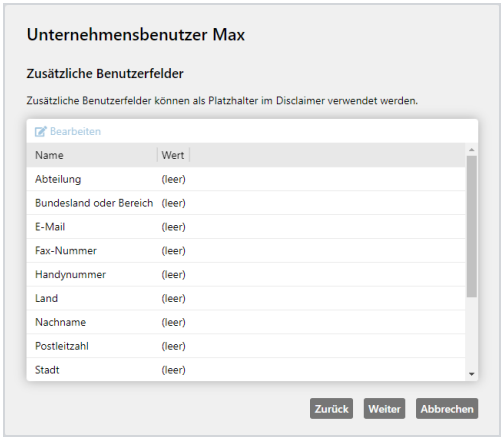
1. Gehen Sie zu **Identitäten > Unternehmensbenutzer**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie unter **Allgemein** den Nachnamen oder Funktionspostfachnamen, optional den Vornamen des Benutzerssowie den Aktivitätsstatus an.



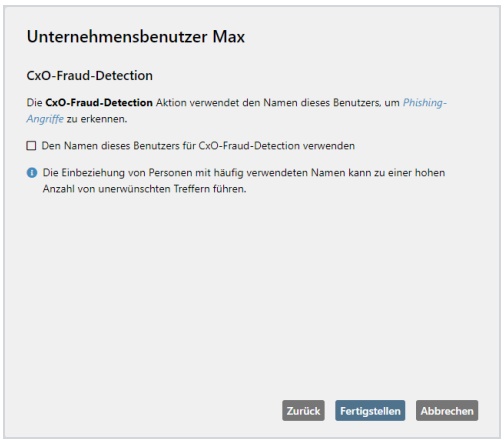
4. Wählen Sie eine oder mehrere E-Mail-Adressen für den Benutzer und klicken Sie **Weiter**.



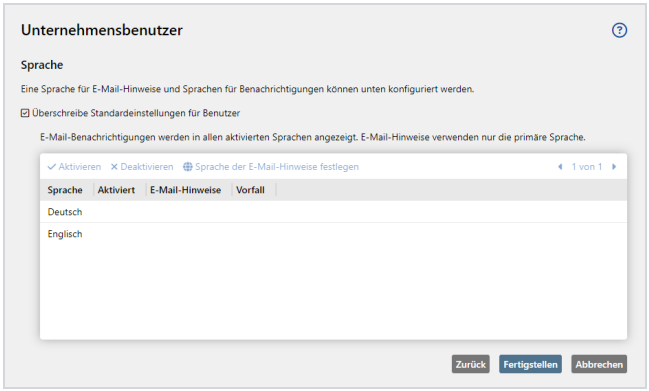
5. (Optional) Fügen Sie Werte für die Zusätzlichen Benutzerfelder hinzu. Diese Werte ersetzen dann die entsprechenden Platzhalter in Disclaimer-Vorlagen.



6. Bestimmen Sie, ob Sie den Namen des Benutzers in die CxO-Betrugserkennung einbeziehen wollen.



7. Wählen Sie eine Sprache für E-Mail-Hinweise und -Benachrichtigungen, die zu E-Mails hinzugefügt werden.



8. Klicken Sie **Fertigstellen**.

Über die CxO-Betrugserkennung

Die CxO-Betrugserkennung dient der Erkennung von Phishing-Angriffen. Sie vergleicht den Absendernamen von eingehenden E-Mails mit den Namen von Unternehmensbenutzern. Gefälschte E-Mails, die im Namen von Vorgesetzten oder Mitarbeitern an Sie gesendet werden, werden so abgefangen.

Bei der Überprüfung werden unterschiedliche Varianten des Absendernamens in den Vergleich einbezogen:

- Erika Mustermann
- Mustermann Erika
- ErikaMustermann
- MustermannErika

Die CxO-Betrugserkennung trennt Namen beziehungsweise löst sie auf, wenn sie durch die folgenden Trennzeichen verbunden sind:

- Punkte (.)
- Kommata (,)
- Semikolons (;)
- Doppelpunkte (:)
- Bindestriche (-)
- Unterstriche (_)
- Anführungszeichen (")

- Apostrophe (')
- Akzente (´)
- Gravis (`)
- Leerzeichen ( ).

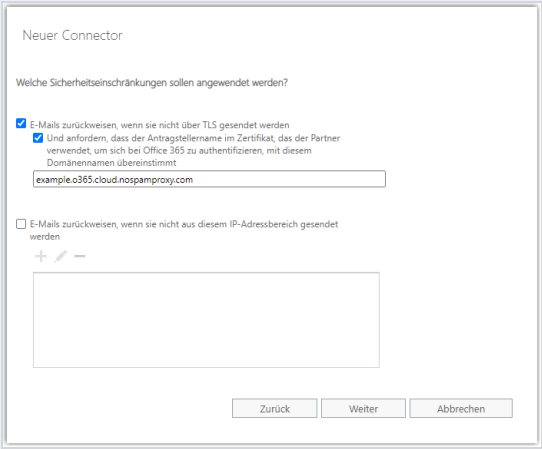
Nachrichtenfluss konfigurieren

Einrichtung per PowerShell

1. Gehen Sie zu **Konfiguration > Office 365**.
2. Markieren Sie Ihren Office-365-Mandanten.
3. Klicken Sie **Zeige Exchange-Konfiguration**.
4. Klicken Sie **Konfigurationskommandos in die Zwischenablage kopieren**.
5. Klicken Sie **Schließen**.
6. Führen Sie das Skript in Ihrer Exchange Online PowerShell aus.
7. Wählen Sie nach dem Ausführen des Skripts die gewünschte Variante des E-Mail-Routings:
    - Wählen Sie **Direct**, falls Sie NoSpamProxy Protection nutzen.
    - Wählen Sie **Parallel**, falls Sie NoSpamProxy Encryption als Standalone-Modul nutzen.

Dieses PowerShell-Skript erstellt – abhängig von der gewählten Zustellmethode – einen eingehenden Partner-Konnektor, der standardmäßig mit einer Wildcard versehen ist und **für alle eingehenden E-Mails greift**. Außerdem werden Transport-Regeln erstellt, welche ausgehende E-Mails **uneingeschränkt** zu NoSpamProxy Cloud routen.

HINWEIS: Einige E-Mail-Server haben den alten MX-Eintrag noch bis zu 24 Stunden im Cache. Deshalb empfehlen wir, die Einschränkung auf den Antragstellernamen in Ihrem **Exchange Admin Center** unter **Nachrichtenfluss > Connectors** zunächst wieder zu deaktivieren und nach frühestens 24 Stunden aktiv zu schalten. Ansonsten ist es möglich, dass E-Mails von Exchange abgelehnt werden.



Manuelle Einrichtung

> **HINWEIS:** Wenn Sie ausgehende E-Mails nicht über Port 25 weiterleiten können, ist es auch möglich, Port 587 zu verwenden. Beachten Sie, dass an Port 587 STARTTLS erforderlich ist.

NoSpamProxy Cloud

Mandantenspezifische TLS- und Domänennamen anzeigen

Um die für Ihren Mandanten erforderlichen TLS- und Domänennamen anzuzeigen, gehen Sie folgendermaßen vor:

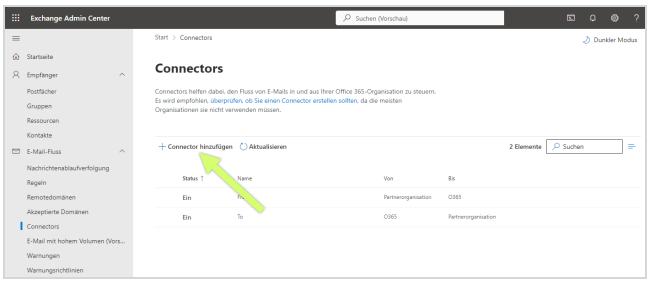
1. Gehen Sie zu **Konfiguration > Office 365**.
2. Markieren Sie Ihren Office-365-Mandanten.
3. Klicken Sie **Zeige Exchange-Konfiguration**.

Die relevanten Informationen werden angezeigt.

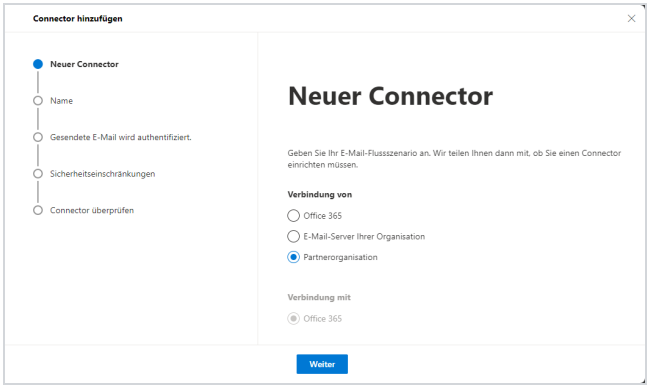
Einen eingehenden Konnektor anlegen

1. Öffnen Sie Ihr Exchange Admin Center unter **https://admin.exchange.microsoft.com/**.

2. Gehen Sie zu **E-Mail-Fluss > Connectors** und klicken Sie **Connector hinzufügen**.

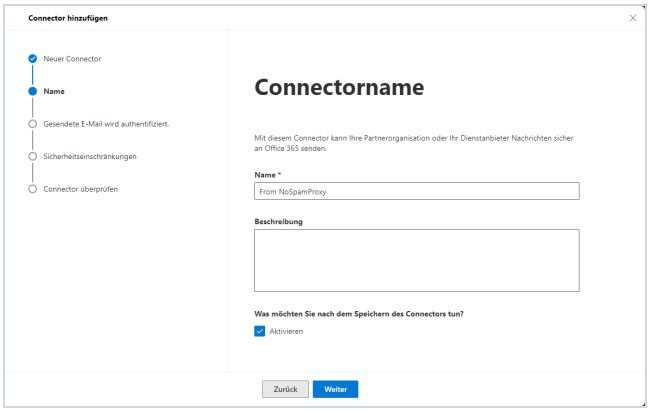


3. Wählen Sie unter **Verbindung von** die Option **Partnerorganisation**, wählen Sie unter **Verbindung mit** die Option **Office 365** und klicken Sie **Weiter**.

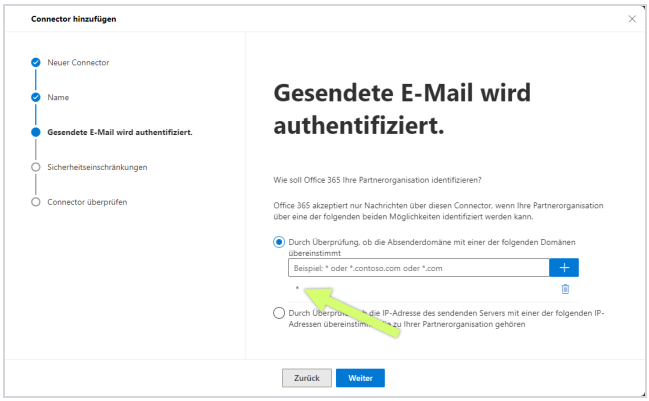


4. Geben Sie **From NoSpamProxy** als Namen für den Konnektor ein, fügen Sie optional eine Beschreibung hinzu, setzen Sie das Häkchen neben

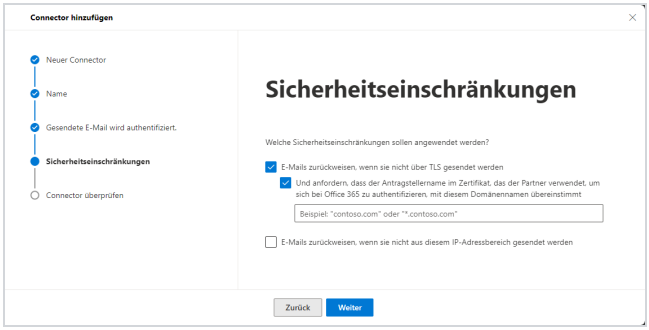
Aktivieren und klicken Sie **Weiter**.



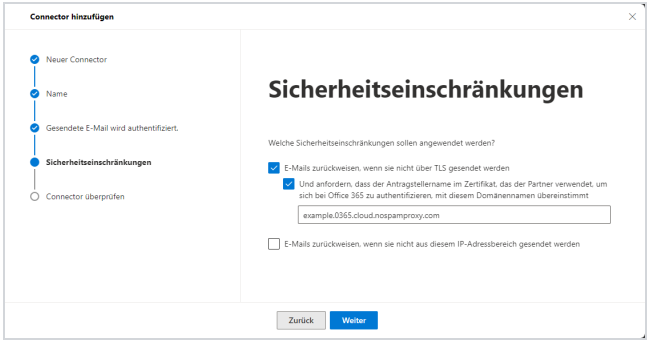
5. Wählen Sie die Option **Durch Überprüfung, ob die Absenderdomäne [...]**, geben Sie ***** als Absenderdomäne ein, klicken Sie das **Plus-Zeichen** und dann **Weiter**.



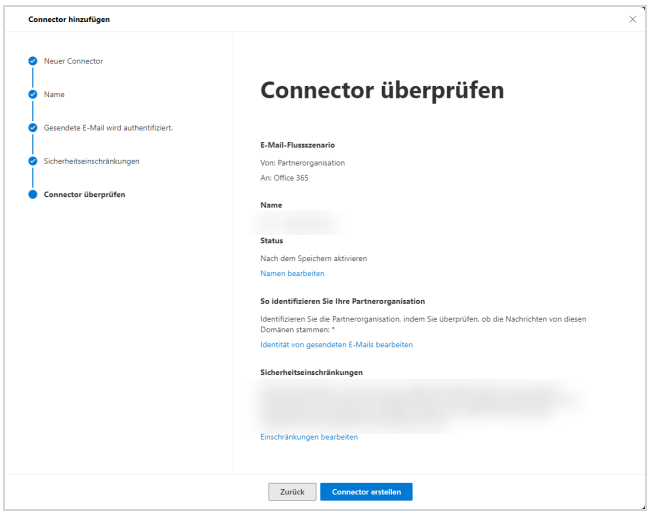
6. Setzen Sie die Häkchen neben **E-Mails zurückweisen, wenn [...]** sowie **Und anfordern, dass [...]**.



7. Geben Sie den TLS-Antragsteller für den eingehenden Exchange-Sendekonnektor an und klicken Sie **Weiter**.



8. Überprüfen Sie die von Ihnen vorgenommen Einstellungen und klicken Sie **Connector erstellen**.

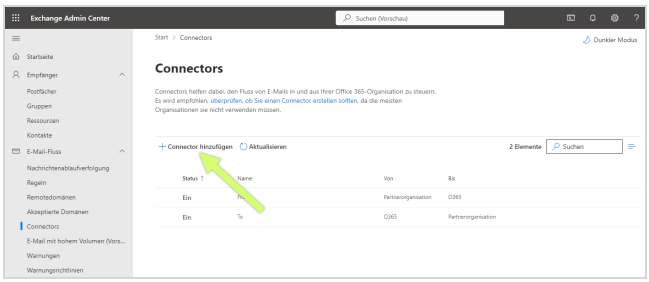


> **HINWEIS:** Einige E-Mail-Server haben den alten MX-Eintrag noch bis zu 24 Stunden im Cache. Deshalb empfehlen wir, die Einschränkung auf den Antragstellernamen erst 24 Stunden nach der Umstellung des MX-Eintrag aktiv zu schalten. Ansonsten ist es möglich, dass E-Mails von Exchange Online mit 5.7.51 abgelehnt werden.

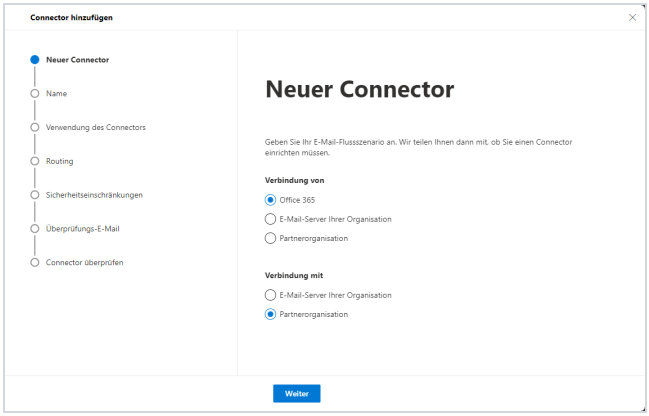
Einen ausgehenden Sendekonnektor anlegen

1. Öffnen Sie Ihr Exchange Admin Center unter https://admin.exchange.microsoft.com/.

2. Gehen Sie zu **E-Mail-Fluss > Connectors** und klicken Sie **Connector hinzufügen**.

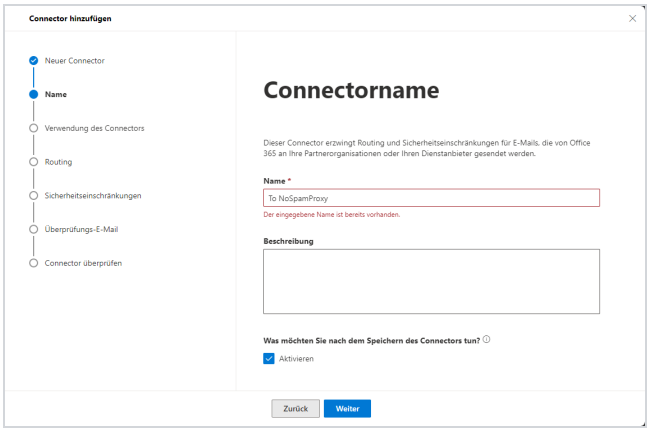


3. Wählen Sie unter **Verbindung von** die Option **Office 365**, wählen Sie unter **Verbindung mit** die Option **Partnerorganisation** und klicken Sie **Weiter**.

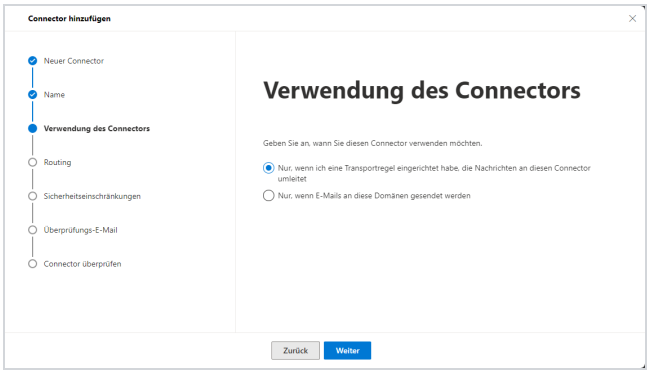


4. Geben Sie **To NoSpamProxy** als Namen für den Konnektor ein, fügen Sie optional eine Beschreibung hinzu, setzen Sie das Häkchen neben

Einschalten und klicken Sie **Weiter**.

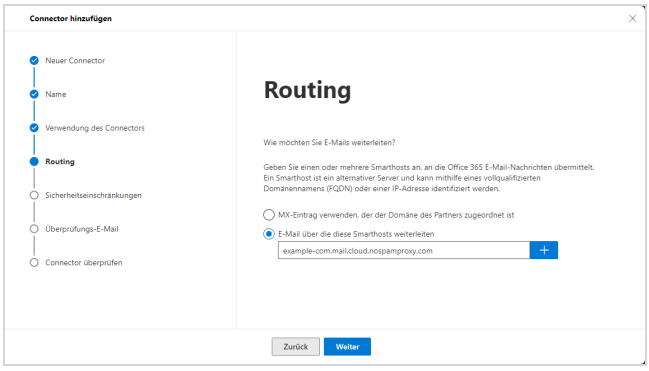


5. Wählen Sie die Option **Nur, wenn ich eine Transportregel eingerichtet habe, [...]** und klicken Sie **Weiter**.

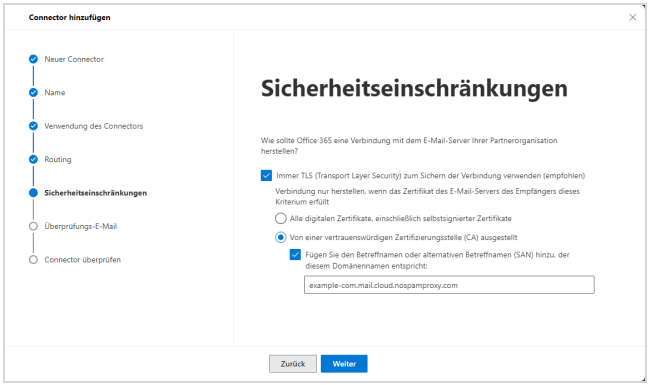


6. Wählen Sie die Option **E-Mail über diese Smarthosts weiterleiten**, geben Sie die entsprechenden Smarthosts auf dem ausgehenden Exchange-

Sendekonnektor an und klicken Sie das **Plus-Zeichen**.



7. Klicken Sie **Speichern** und dann **Weiter**.
8. Setzen Sie das Häkchen neben **Immer TLS (Transport Layer Security) zum Sichern [...]** und wählen Sie die Option **Von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt**.
9. Setzen Sie das Häkchen neben **Fügen Sie den Betreffnamen oder alternativen Betreffnamen (SAN) hinzu [...]** und geben Sie den TLS-Antragsteller für den ausgehenden Exchange-Sendekonnektor an.

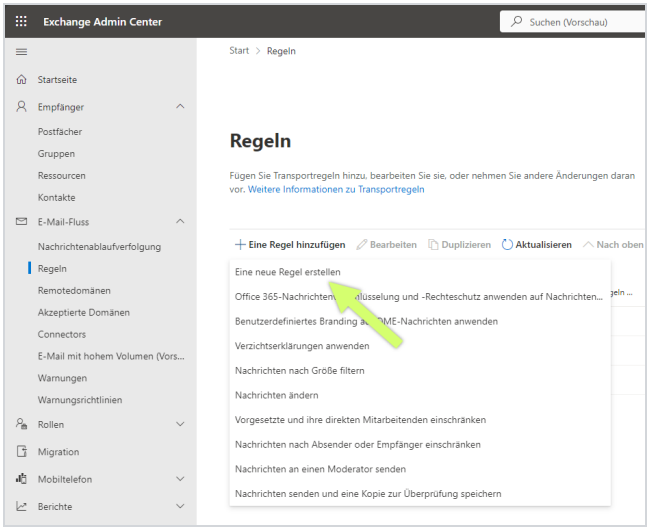


10. Klicken Sie **Weiter**.

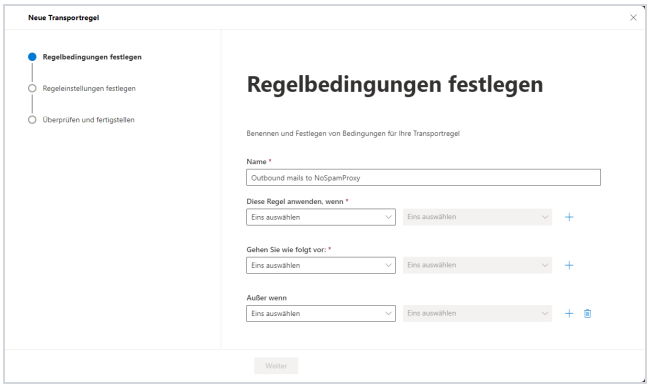
11. Geben Sie im folgenden Dialog eine oder mehrere E-Mail-Adressen ein, klicken Sie das **Plus-Zeichen**, dann **Überprüfen** und folgen Sie den Anweisungen im Dialog.

Eine Transportregel erstellen

1. Öffnen Sie Ihr Exchange Admin Center unter **https://admin.exchange.microsoft.com/**.
2. Gehen Sie zu **E-Mail-Fluss > Regeln**.
3. Klicken Sie **Eine Regel hinzufügen** und dann **Eine neue Regel erstellen**.

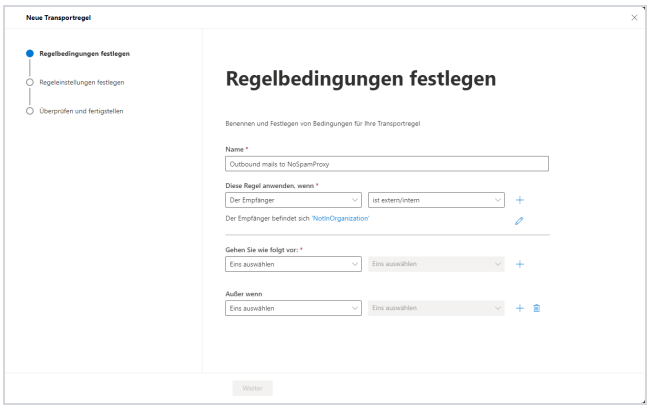


4. Geben Sie der Regel den Namen **Outbound mails to NoSpamProxy**.

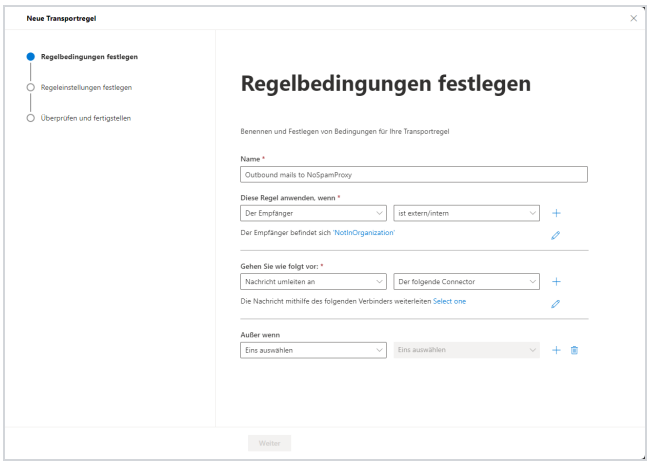


5. Stellen Sie unter **Diese Regel anwenden, wenn** die folgenden Optionen ein:

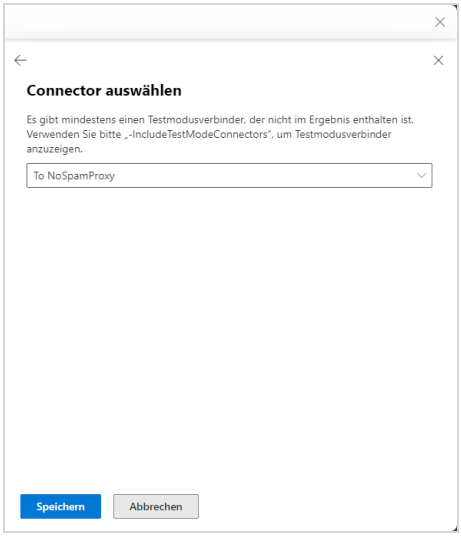
   - **Der Empfänger**
   - **ist extern/intern**
   - **Outside the organization**



6. Stellen Sie unter **Gehen Sie wie folgt vor** die Option **Nachricht umleiten an** und dann **Der folgende Connector** ein.



7. Geben Sie den zuvor erstellten Konnektor **To NoSpamProxy** an und klicken Sie **OK**.

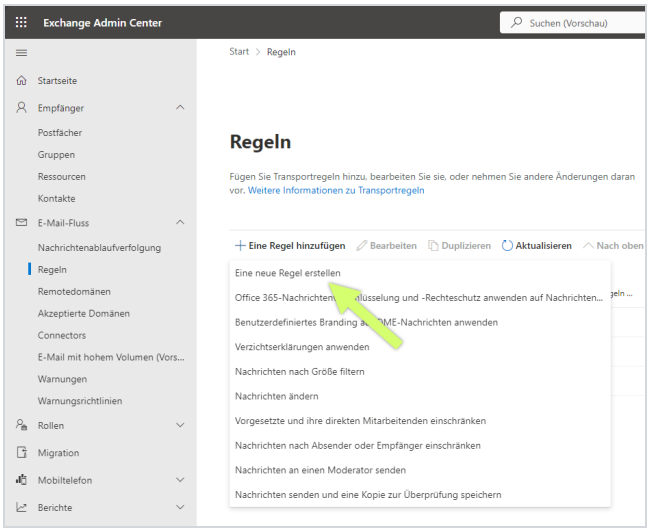


8. Klicken Sie **Weiter**.

9. Lassen Sie die Einstellungen für Ihre Transportregel unverändert und klicken Sie **Weiter**.
10. Überprüfen Sie die von Ihnen vorgenommenen Einstellungen und klicken Sie **Fertigstellen**.

Spamfilterung durch Office 365 unterbinden

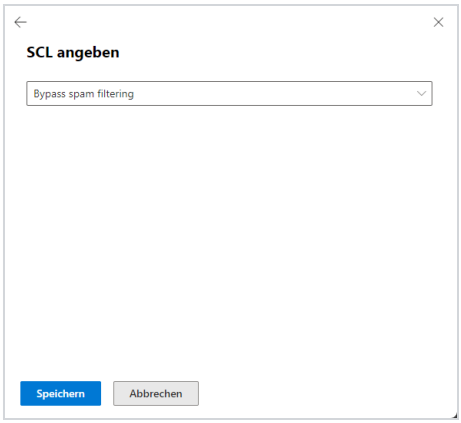
1. Öffnen Sie Ihr Exchange Admin Center unter **https://admin.exchange.microsoft.com/**.
2. Gehen Sie zu **E-Mail-Fluss > Regeln**.
3. Klicken Sie **Eine Regel hinzufügen** und dann **Eine neue Regel erstellen**.



4. Geben Sie der Regel den Namen **Disable spam filtering for inbound emails**.
5. Stellen Sie unter **Diese Regel anwenden, wenn** die folgenden Optionen ein:

- **Der Absender**
- **ist extern/intern**
- **Outside the organization**

6. Wählen Sie unter **Gehen Sie wie folgt vor** die folgenden Optionen:
   - Nachrichteneigenschaften ändern
   - SCL-Bewertung (Spam Confidence Level) festlegen
7. Wählen Sie im folgenden Dialog unter **SCL angeben** die Option **Bypass spam filtering**.



8. Klicken Sie **Speichern** und dann **Weiter**.
9. Lassen Sie die Einstellungen für Ihre Transportregel unverändert und klicken Sie **Weiter** und dann **Fertigstellen**.

NoSpamProxy Cloud Encryption (ohne NoSpamProxy Protection)

Mandantenspezifische TLS- und Domänennamen anzeigen

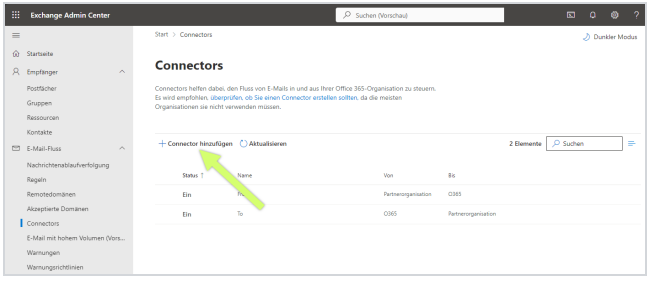
Um die für Ihren Mandanten erforderlichen TLS- und Domänennamen anzuzeigen, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Office 365**.
2. Markieren Sie Ihren Office-365-Mandanten.
3. Klicken Sie **Zeige Exchange-Konfiguration**.

Die relevanten Informationen werden angezeigt.

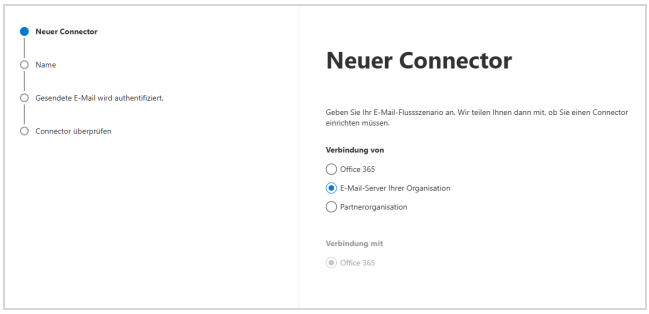
Einen eingehenden Konnektor anlegen

1. Öffnen Sie Ihr Exchange Admin Center unter https://admin.exchange.microsoft.com/.
2. Gehen Sie zu **E-Mail-Fluss > Connectors** und klicken Sie **Connector hinzufügen**.

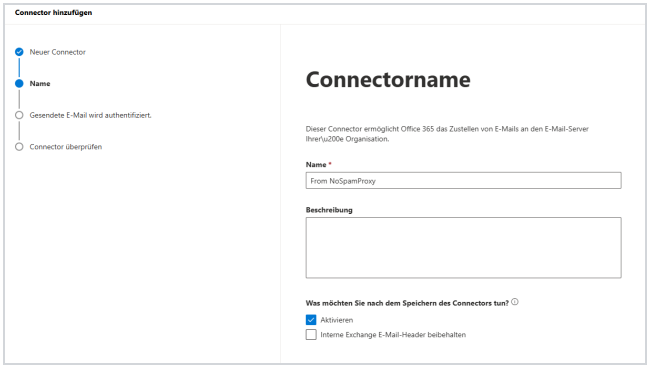


3. Wählen Sie unter **Verbindung von** die Option **E-Mail-Server Ihrer Organisation**, wählen Sie unter **Verbindung mit** die Option **Office 365** und

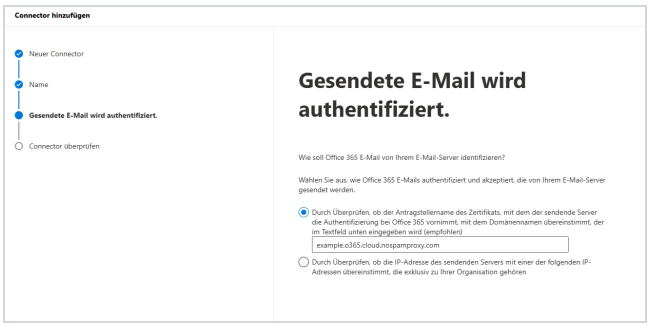
klicken Sie **Weiter**.



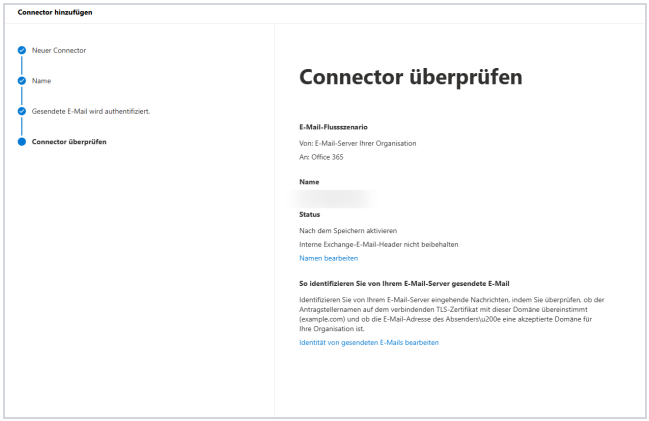
4. Geben Sie **From NoSpamProxy** als Namen für den Konnektor ein, fügen Sie optional eine Beschreibung hinzu, setzen Sie das Häkchen neben **Aktivieren** und klicken Sie **Weiter**.



5. Geben Sie den TLS-Antragsteller für den eingehenden Exchange-Sendekonnektor an und klicken Sie **Weiter**.



6. Überprüfen Sie die von Ihnen vorgenommen Einstellungen und klicken Sie **Connector erstellen**.



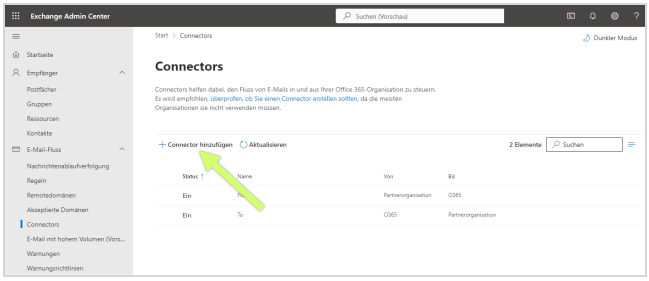
7. Öffnen Sie **https://security.microsoft.com/**.
8. Gehen Sie zu **E-Mail & Zusammenarbeit > Richtlinien und Regeln > Bedrohungsrichtlinien > Erweiterte Filterung (für Connectors)**.
9. Klicken Sie den Konnektor **From NoSpamProxy (without Protection)**.

10. Wählen Sie die folgenden Optionen:
    - **Automatisch erkennen und die letzte IP-Adresse überspringen**
    - **Auf die gesamte Organisation anwenden**
11. Klicken Sie **Speichern**.

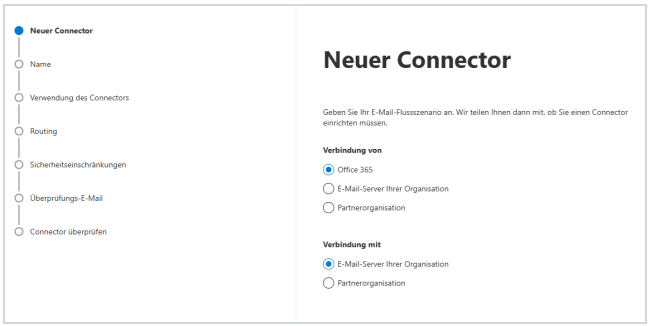
> **HINWEIS:** Einige E-Mail-Server haben den alten MX-Eintrag noch bis zu 24 Stunden im Cache. Deshalb empfehlen wir, die Einschränkung auf den Antragstellernamen erst 24 Stunden nach der Umstellung des MX-Eintrag aktiv zu schalten. Ansonsten ist es möglich, dass E-Mails von Exchange Online mit 5.7.51 abgelehnt werden.

Einen ausgehenden Sendekonnektor anlegen

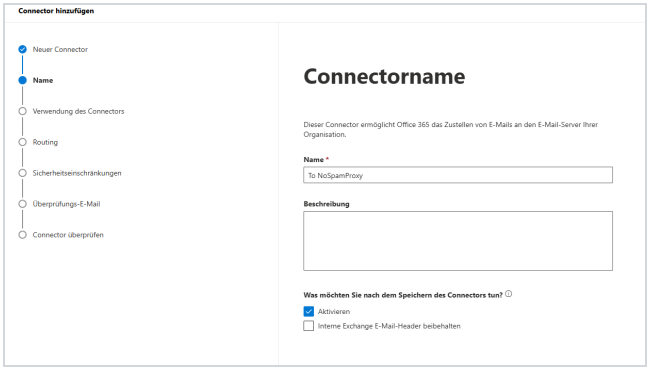
1. Öffnen Sie Ihr Exchange Admin Center unter https://admin.exchange.microsoft.com/.
2. Gehen Sie zu **E-Mail-Fluss > Connectors** und klicken Sie **Connector hinzufügen**.



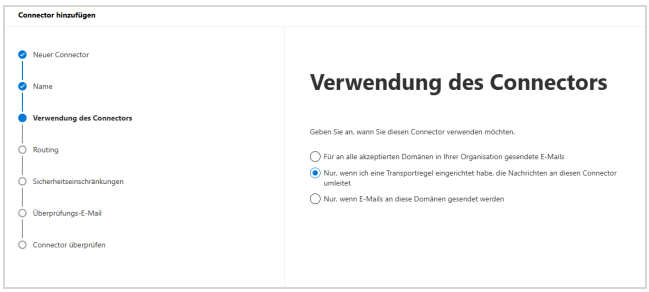
3. Wählen Sie unter **Verbindung von** die Option **Office 365**, wählen Sie unter **Verbindung mit** die Option **E-Mail-Server Ihrer Organisation** und klicken Sie **Weiter**.



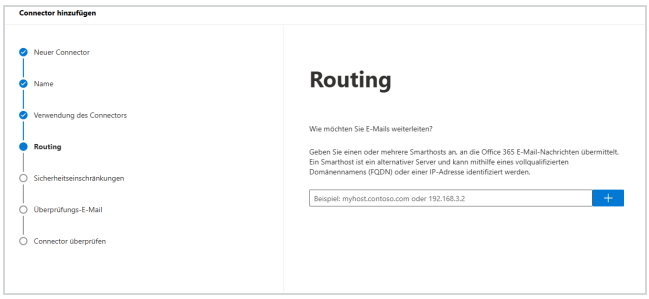
4. Geben Sie **To NoSpamProxy** als Namen für den Konnektor ein, fügen Sie optional eine Beschreibung hinzu, setzen Sie das Häkchen neben **Einschalten** und klicken Sie **Weiter**.



5. Wählen Sie die Option **Nur, wenn ich eine Transportregel eingerichtet habe, [...]** und klicken Sie **Weiter**.

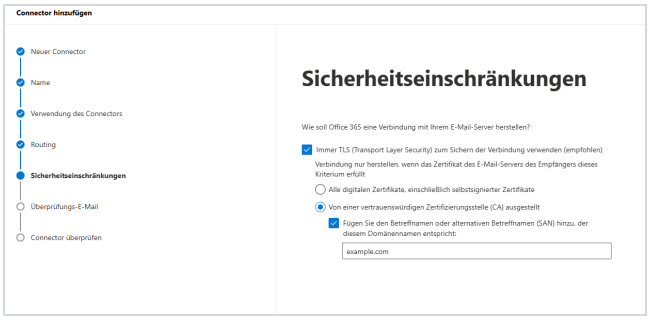


6. Geben Sie einen oder mehrere Smarthosts an, an die Office 365 E-Mail-Nachrichten übermittelt.



7. Klicken Sie **Weiter**.
8. Setzen Sie das Häkchen neben **Immer TLS (Transport Layer Security) zum Sichern [...]** und wählen Sie die Option **Von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt**.
9. Setzen Sie das Häkchen neben **Fügen Sie den Betreffnamen oder alternativen Betreffnamen (SAN) hinzu [...]** und geben Sie den TLS-

Antragsteller für den ausgehenden Exchange-Sendekonnektor an.

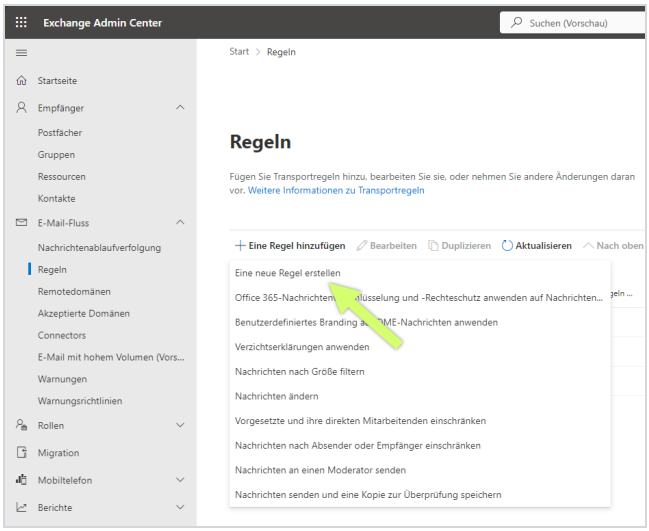


10. Klicken Sie **Weiter**.
11. Geben Sie im folgenden Dialog eine oder mehrere E-Mail-Adressen ein, klicken Sie das **Plus-Zeichen**, dann **Überprüfen** und folgen Sie den Anweisungen im Dialog.

Transportregel erstellen: Eingehende E-Mails durch den obenstehenden Konnektor leiten

1. Öffnen Sie Ihr Exchange Admin Center unter **https://admin.exchange.microsoft.com/**.
2. Gehen Sie zu **E-Mail-Fluss > Regeln**.

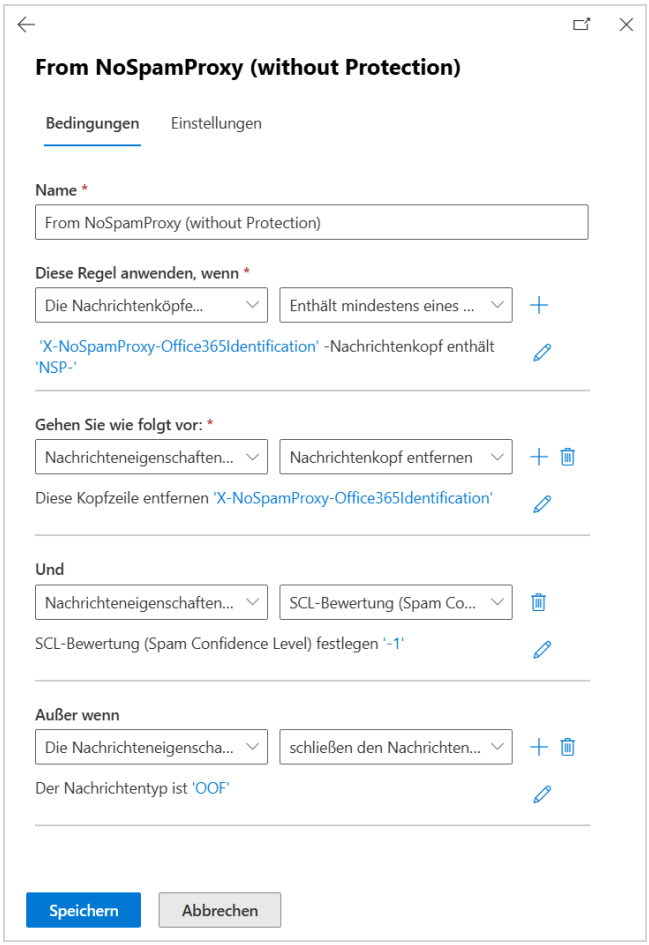
3. Klicken Sie **Eine Regel hinzufügen** und dann **Eine neue Regel erstellen**.



4. Geben Sie der Regel den Namen **From NoSpamProxy (without Protection)**.
5. Stellen Sie unter **Diese Regel anwenden, wenn** die folgenden Optionen ein:
    - **Die Nachrichtenköpfe…**
    - **Enthält mindestens eines dieser Wörter**
6. Klicken Sie **Enter text** und geben Sie den Wert **X-NoSpamProxy-Office365Identification** an.
7. Klicken Sie **Enter words** und geben Sie den **notwendigen Wert für die Kopfzeile** an. Siehe **Wie finde ich den notwendigen Wert für die Kopzeile?**

8. Stellen Sie unter **Gehen Sie wie folgt vor** die Optionen **Nachrichteneigenschaften ändern** und **Nachrichtenkopf entfernen** ein und geben Sie den Wert **X-NoSpamProxy-Office365Identification** an.
9. Klicken Sie das **Plus-Zeichen**.
10. Stellen Sie unter **Gehen Sie wie folgt vor** die Optionen **Nachrichteneigenschaften ändern** und **SCL-Bewertung (Spam Confidence Level) festlegen** ein und wählen Sie im folgenden Dialog unter **SCL angeben** die Option **Bypass spam filtering**.
11. Stellen Sie unter **Außer wenn** die Optionen **Die Nachrichteneigenschaften** und **schließen den Nachrichtentyp ein** ein und geben Sie den Wert **Automatic reply an**. Der Dialog sollte jetzt so

aussehen:

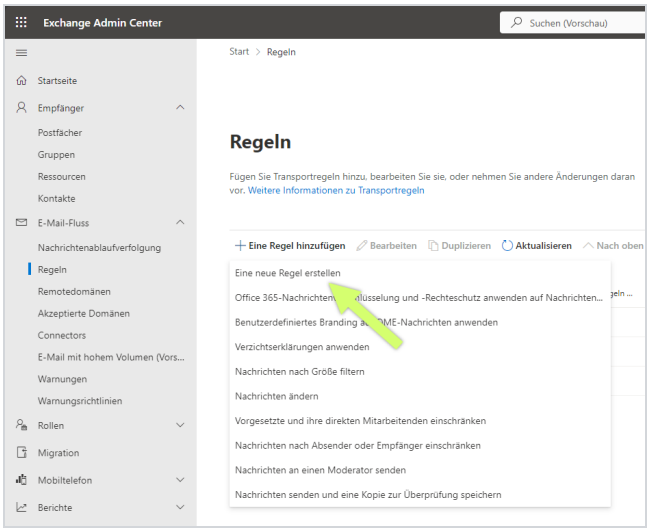


12. Klicken Sie **Weiter** und setzen Sie das Häkchen bei **Verarbeiten weiterer Regeln beenden**.
13. Lassen Sie die übrigen Einstellungen für diese Transportregel unverändert und klicken Sie **Weiter**.

14. Überprüfen Sie die von Ihnen vorgenommenen Einstellungen und klicken Sie **Fertigstellen**.

Transportregel erstellen: Ausgehende E-Mails an NoSpamProxy leiten

1. Öffnen Sie Ihr Exchange Admin Center unter https://admin.exchange.microsoft.com/.
2. Gehen Sie zu **E-Mail-Fluss > Regeln**.
3. Klicken Sie **Eine Regel hinzufügen** und dann **Eine neue Regel erstellen**.

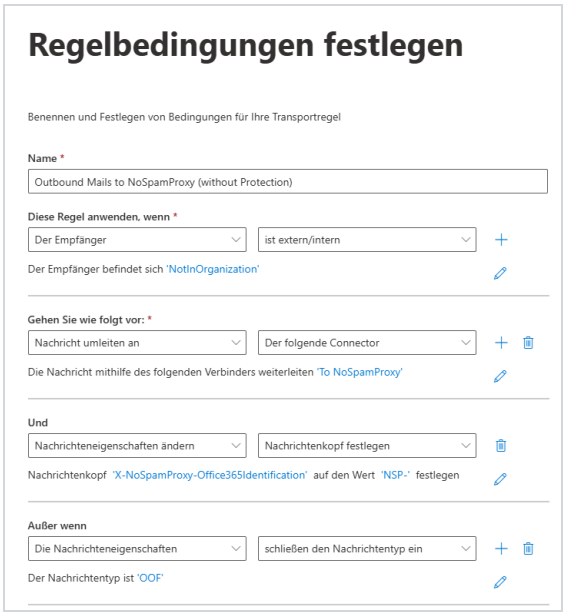


4. Geben Sie der Regel den Namen **Outbound Mails to NoSpamProxy (without Protection)**.
5. Stellen Sie unter **Diese Regel anwenden, wenn** die folgenden Optionen ein:

- **Der Empfänger**
- **ist extern/intern**
- **Outside the organization**

6. Stellen Sie unter **Gehen Sie wie folgt vor** die Optionen **Nachricht umleiten an** und **Der folgende Connector** ein und geben Sie den zuvor erstellten Konnektor **To NoSpamProxy** an.
7. Klicken Sie das **Plus-Zeichen** und stellen Sie ebenso unter **Gehen Sie wie folgt vor** die Optionen **Nachrichteneigenschaften ändern** und **Nachrichtenkopf festlegen** an.
8. Klicken Sie **Enter text** und geben Sie den Wert **X-NoSpamProxy-Office365Identification** an.
9. Klicken Sie **Enter words** und geben Sie den **notwendigen Wert für die Kopfzeile** an. Siehe **Wie finde ich den notwendigen Wert für die Kopzeile?**
10. Stellen Sie unter **Außer wenn** die Optionen **Die Nachrichteneigenschaften** und **schließen den Nachrichtentyp ein** ein und geben Sie den Wert **Automatic reply an**. Der Dialog sollte jetzt so

aussehen:

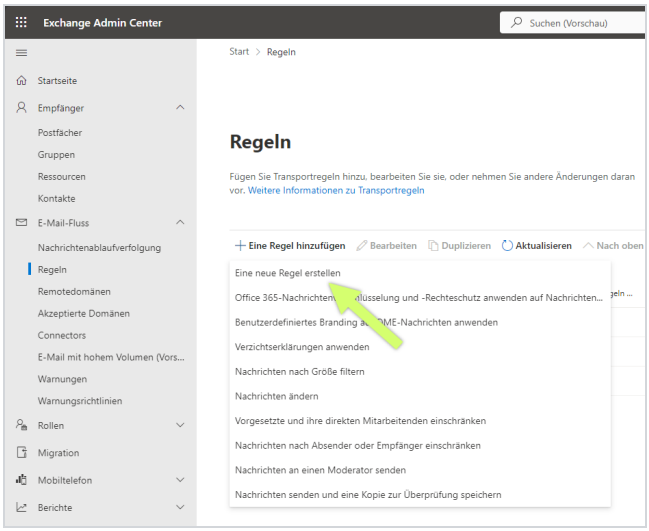


11. Klicken Sie **Weiter** und setzen Sie das Häkchen bei **Verarbeiten weiterer Regeln beenden**.
12. Lassen Sie die übrigen Einstellungen für diese Transportregel unverändert und klicken Sie **Weiter**.
13. Überprüfen Sie die von Ihnen vorgenommenen Einstellungen und klicken Sie **Fertigstellen**.

Transportregel erstellen: Eingehende E-Mails an NoSpamProxy leiten

1. Öffnen Sie Ihr Exchange Admin Center unter https://admin.exchange.microsoft.com/.
2. Gehen Sie zu **E-Mail-Fluss > Regeln**.

3. Klicken Sie **Eine Regel hinzufügen** und dann **Eine neue Regel erstellen**.

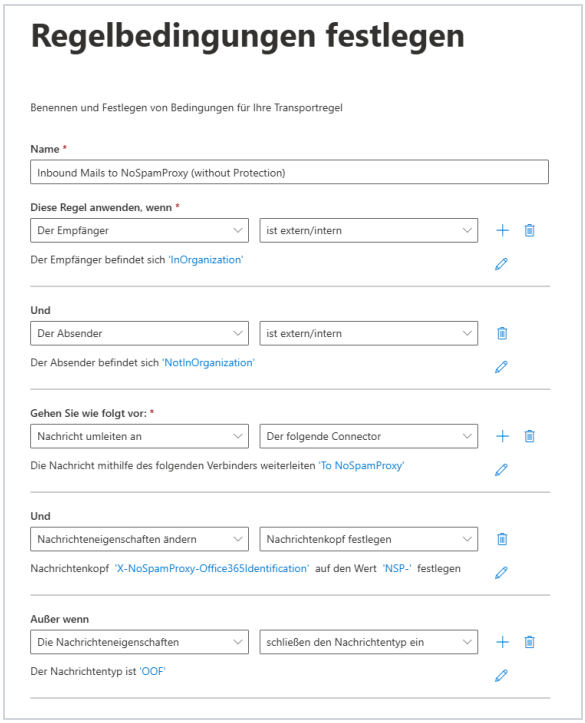


4. Geben Sie der Regel den Namen **Inbound Mails to NoSpamProxy (without Protection)**.
5. Stellen Sie unter **Diese Regel anwenden, wenn** die folgenden Optionen ein:
    - **Der Empfänger**
    - **ist extern/intern**
    - **Inside the organization**
6. Klicken Sie das **Plus-Zeichen** und stellen Sie ebenso unter **Diese Regel anwenden, wenn** die folgenden Optionen ein:
    - **Der Absender**
    - **ist extern/intern**

- **Outside the organization**

7. Stellen Sie unter **Gehen Sie wie folgt vor** die Optionen **Nachricht umleiten an** und **Der folgende Connector** ein und geben Sie den zuvor erstellten Konnektor **To NoSpamProxy** an.
8. Klicken Sie das **Plus-Zeichen** und stellen Sie ebenso unter **Gehen Sie wie folgt vor** die Optionen **Nachrichteneigenschaften ändern** und **Nachrichtenkopf festlegen** an.
9. Klicken Sie **Enter text** und geben Sie den Wert **X-NoSpamProxy-Office365Identification** an.
10. Klicken Sie **Enter words** und geben Sie den **notwendigen Wert für die Kopfzeile** an. Siehe **Wie finde ich den notwendigen Wert für die Kopzeile?**
11. Stellen Sie unter **Außer wenn** die Optionen **Die Nachrichteneigenschaften** und **schließen den Nachrichtentyp ein** ein und geben Sie den Wert **Automatic reply an**. Der Dialog sollte jetzt so

aussehen:



12. Lassen Sie die Einstellungen für diese Transportregel unverändert und klicken Sie **Weiter**.
13. Überprüfen Sie die von Ihnen vorgenommenen Einstellungen und klicken Sie **Fertigstellen**.

Wie finde ich den notwendigen Wert für die Kopzeile?

1. Gehen Sie zu **Konfiguration > Office 365**.
2. Markieren Sie Ihren Office-365-Mandanten.
3. Klicken Sie **Zeige Exchange-Konfiguration**.
4. (Optional) Kopieren Sie den notwendigen Wert für die Kopfzeile in die Zwischenablage.
5. Klicken Sie **Schließen**.

HINWEIS: Beachten Sie Ihre bestehende Exchange-Konfiguration. Diese Anleitung stellt den E-Mail-Verkehr uneingeschränkt um.

Optional: E-Mail-Routing einrichten

TIP: Durch das Hinzufügen von Office 365 wird das erforderliche E-Mail-Routing in NoSpamProxy Cloud sowie optional der automatische Benutzerimport bereits eingerichtet. Falls Sie Office 365 in Cloud einbinden wollen oder bereits eingebunden haben, können Sie dieses Kapitel überspringen. Weitere Informationen finden Sie unter **Konfiguration**.

E-Mail-Server des Unternehmens hinzufügen

> **HINWEIS:** E-Mail-Server des Unternehmens dürfen in der 'MAIL FROM'-Adresse eine Unternehmensdomäne verwenden. Siehe Domänen konfigurieren.

Hinzufügen per SMTP-Authentifizierung (SMTP-Auth)

> **HINWEIS:**
> - Für das Einbinden von Servern mit SMTP-Authentifizierung ist eine TLS-gesicherte Verbindung erforderlich.
> - NoSpamProxy unterstützt die Authentifizierungs-Verfahren **AUTH** und **LOGIN**.

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **Authentifizierter Server**.
4. Notieren Sie den Benutzernamen.
5. Kopieren Sie das angegebene Passwort in die Zwischenablage, notieren Sie es und klicken Sie **Weiter**.
6. Klicken Sie **Fertigstellen**.

7. Konfigurieren Sie den Benutzernamen und das Passwort in den Einstellungen Ihres Drittanbieter-Serverproduktes.

Hinzufügen per SPF-Eintrag

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > E-Mail-Server des Unternehmens**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie **Sender Policy Framework (SPF)**.
4. Beschränken Sie den E-Mail-Server bei Bedarf auf bestimmte Domänen.
5. Klicken Sie **Fertigstellen**.

WARNING:
Domänen und IP-Adressen, die im jeweiligen SPF-Eintrag erscheinen, dürfen Ihre Unternehmensdomänen als Absenderadresse verwenden. Wir empfehlen deshalb Folgendes:

- Fügen Sie nur die unbedingt nötigen Einträge hinzu.
- Nutzen Sie dedizierte Subdomänen. So ist sichergestellt, dass nur diese Subdomänen verwendet werden und die Hauptdomäne dem eigentlichen E-Mail-Server – in der Regel ein Exchange-Server – vorbehalten bleibt. Für eine bessere Kategorisierung ist es hilfreich, die Subdomänen anhand der Funktion zu erstellen, also beispielsweise hr.example.com für die Personalabteilung, marketing.example.com für die Marketingabteilung oder it.example.com für die IT-Abteilung.
- Beschränken Sie die durch SPF geschützte lokale Adresse auf die benötigte Subdomäne oder Domäne.
- Fügen Sie dem SPF-Eintrag immer **-all** hinzu, um alle nicht genannten IP-Adressen vom Senden auszuschließen.

Einbinden eines Office-365-Hosts

Informationen zum Einbinden eines Office-365-Hosts finden Sie unter **Konfiguration**.

Konnektor für ausgehende E-Mails konfigurieren

Um E-Mails über NoSpamProxy Cloud zu versenden, müssen Sie NoSpamProxy Cloud als Smarthost in Ihrem lokalen E-Mail-Server (beispielsweise Microsoft Exchange) hinzufügen.

Sie benötigen dafür

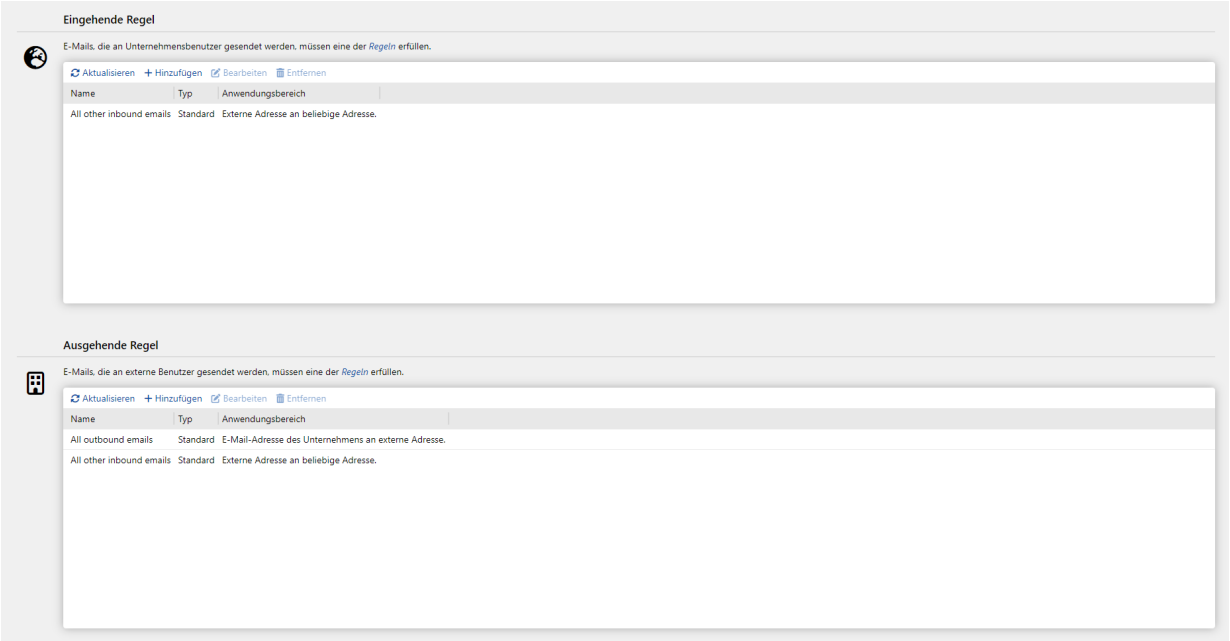
- die unter **Ihr NoSpamProxy-Smarthost** angezeigte Adresse des NoSpamProxy-Smarthost sowie
- den Benutzernamen und das Passwort, die Sie beim Hinzufügen des E-Mail-Servers erhalten haben.

Konnektor für eingehende E-Mails hinzufügen

1. Gehen Sie zu **Konfiguration > E-Mail-Routing > Eingehende E-Mail-Zustellung**
2. Klicken Sie **Hinzufügen**.
3. Geben Sie einen Namen für den Konnektor an, bestimmen Sie dessen Kosten und klicken Sie **Weiter**.
4. Klicken Sie **Hinzufügen** und geben Sie den Servernamen, den Port sowie optional einen Benutzernamen und ein Passwort für Ihr Drittanbieter-Serverprodukt an und klicken Sie **Speichern** und dann **Weiter**.
5. Bestimmen Sie die DNS-Routingbeschränkungen für diesen Konnektor.
6. Klicken Sie **Beenden**.

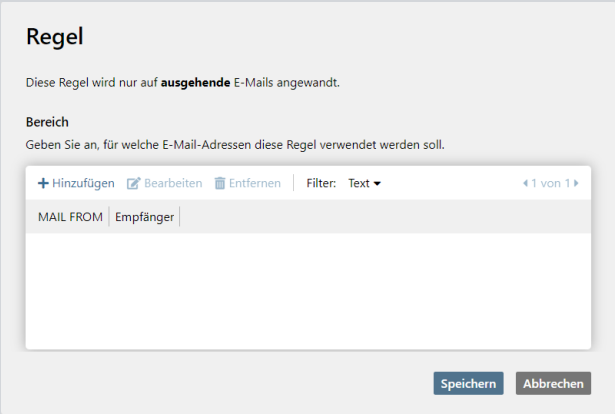
Regeln

Hier finden Sie eine Übersicht über die verfügbaren Regeln. Diese verwalteten Regeln decken bestimmte Anwendungsfälle ab, die durch den Namen und die Beschreibung dokumentiert sind. Diese Regeln werden aktiv, wenn die jeweilige E-Mail im konfigurierten Geltungsbereich liegt. Kommt keine der verwalteten Regeln zur Anwendung, wird die E-Mail auf Basis des Standardregelwerks verarbeitet.

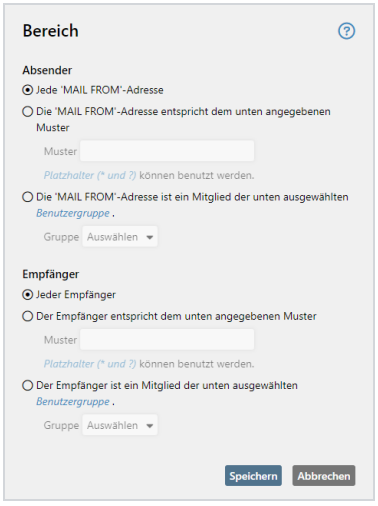


Den Geltungsbereich einer Regel konfigurieren

1. Gehen Sie zu **Konfiguration > Regeln**.
2. Doppelklicken Sie die Regel, die Sie bearbeiten wollen oder markieren Sie diese und klicken Sie **Bearbeiten**.



3. Klicken Sie **Hinzufügen**.
4. Schränken Sie den Geltungsbereich der Regel für Absender (MAIL FROM) und Empfänger wie gewünscht ein.



5. Klicken Sie **Speichern**.

> **EXAMPLE:** Wenn Sie ***benutzer@example.com** eingeben, entspricht dieses Muster allen E-Mail-Adressen, die auf **benutzer@example.com** enden. Wenn Sie ***@example.com** eingeben, stimmen alle Adressen aus der Domäne **example.com** überein. Wenn Sie ***.example.com** eingeben, stimmen alle Unterdomänen von **example.com** überein.

> **HINWEIS:** Damit Sie Gruppen nutzen können, müssen Sie diese vorher einem Benutzerimport hinzufügen. Siehe **Automatischer Benutzerimport via Azure Active Directory**.

Eigenschaften der Regeln

> **HINWEIS:** Bei allen eingehenden und ausgehenden Regeln wird der Malware-Scanner ausgeführt.

> **HINWEIS:** Anders als unsere Standard-Regeln sind die vordefinierten Regeln, in welchen Sie Einträge setzen können, im Bereich auf **Unternehmensdomäne** gefiltert. Das bedeutet, dass wir E-Mails ebenfalls für Benutzer annehmen, die möglicherweise nicht als Unternehmensbenutzer bekannt sind.

Eingehend

Internal communication

Diese eingehende Standard-Regel ermöglicht eine Kommunikation zwischen zwei internen Systemen bei der Nutzung von Unternehmensdomänen. Bei entsprechender Lizenzierung wird sichergestellt, dass wichtige Aktionen wie Entschlüsselung und Signaturprüfung ohne Berücksichtigung von Zertifikatsketten, Aufbringen von eingehenden Disclaimern und Malwareprüfungen durchgeführt wird.

Malware scanning and content filtering/Malware-Prüfung und Inhaltsfilterung

Diese Regel beinhaltet den Malware-Scan und die Inhaltsfilterung von Anhängen, jedoch wird keine Prüfung des Inhalts der E-Mail oder der Reputation des Absenders vorgenommen. Bei entsprechender Lizenzierung werden E-Mails ohne Berücksichtigung der Zertifikatskette entschlüsselt sowie der eingehende Disclaimer aufgetragen.

Malware scanning, no content filtering/Malware-Prüfung, keine Inhaltsfilterung

Diese Regel beinhaltet ausschließlich den Malware-Scan von Anhängen, jedoch wird keine Prüfung des Inhalts der E-Mail oder der Reputation des Absenders vorgenommen. Bei entsprechender Lizenzierung werden E-Mails ohne Berücksichtigung der Zertifikatskette entschlüsselt sowie der eingehende Disclaimer aufgetragen.

> **WARNING:** Diese Regel sollte nur im äußersten Notfall genutzt werden.

All other inbound emails

Diese eingehende Standard-Regel ist immer aktiv und umfasst alle lizenzierten Prüfungen, die den höchsten E-Mail-Schutz bieten.

Soft check

Diese Regel führt eine deutlich reduzierte Spam- und Reputationsprüfung des Absenders durch. Bei entsprechender Lizenzierung wird sichergestellt, dass wichtige Aktionen wie Entschlüsselung und Signaturprüfung ohne Berücksichtigung von Zertifikatsketten und Aufbringen von eingehenden Disclaimern durchgeführt wird. Des Weiteren werden eine Malwareprüfung, Anhangsprüfung sowie eine Blocklistenprüfung vorgenommen. Level of Trust, URL Safeguard, die Core AntiSpam Engine sowie CxO Fraud werden nicht mehr berücksichtigt.

Medium check

Diese Regel führt eine leicht reduzierte Spam- und Reputationsprüfung des Absenders durch und ist auf die Hauptdomäne beschränkt. Bei entsprechender Lizenzierung wird sichergestellt, dass wichtige Aktionen wie Entschlüsselung und Signaturprüfung ohne Berücksichtigung von Zertifikatsketten, Aufbringen von eingehenden Disclaimern sowie Spam- und Malwareprüfung durchgeführt wird. Der URL Safeguard wird nicht mehr aktiv.

Block list/Blockliste

Diese Regel weist eingehende E-Mails ohne Berücksichtigung jeglicher Ausnahmen sofort ab.

Decryption allowlist/Ausnahme für Entschlüsselung

Diese Regel entspricht der Standard-Regel **All other inbound emails**, lässt aber verschlüsselte E-Mails passieren, die NoSpamProxy nicht entschlüsseln kann.

> **HINWEIS:** Öffentliche Schlüssel werden nicht aus digitalen Signaturen eingesammelt.

Ausgehend

> **HINWEIS:** Bei ausgehenden Verbindungen versucht NoSpamProxy Cloud immer, eine TLS-Verbindung aufzubauen.

All outbound emails

Diese ausgehende Standard-Regel ist immer aktiv und umfasst alle lizenzierten Prüfungen und Aktionen, die die höchste E-Mail-Reputation bieten. Vom Client verschlüsselte E-Mails werden abgewiesen; bereits digital signierte E-Mails können nicht zusätzlich mit DKIM signiert werden. Des Weiteren wird - sofern möglich - eine digitale Signatur und/oder Verschlüsselung vorgenommen, und es erfolgt eine Überprüfung des Inhalts.

Plain text email/Klartext-E-Mail

Diese Regel sendet alle E-Mails als Text-E-Mails ohne Signierung und Verschlüsselung. TLS wird weiterhin angewendet, sofern verfügbar.

Forced encryption/Erzwungene Verschlüsselung

Diese Regel erzwingt die Verschlüsselung. Sollte kein Schlüsselmaterial gefunden werden, greift NoSpamProxy Cloud auf PDF Mail (also PDF-Verschlüsselung) zurück. Bei nicht vorhandenem PDF-Passwort wird der Empfänger aufgefordert, ein Passwort zu setzen.

Encryption allowlist/Ausnahme für Verschlüsselung

Diese Regel entspricht der Regel **All outbound emails**, lässt aber bereits vom Client verschlüsselte E-Mails passieren.

Signing only/Ausschließlich signieren

Diese Regel signiert E-Mails, aber verschlüsselt diese niemals mit S/MIME, PGP oder PDF Mail. TLS wird weiterhin angewendet, sofern verfügbar.

No 32Guards/Kein 32Guards

Diese Regel führt keine Prüfung mit 32Guards durch. Sie eignet sich nur für Fälle, in denen ein False Positive von 32Guards vorliegt. Siehe **Melden von False Negatives und False Positives**.

> **HINWEIS:** Sie sollten diese Regel keinesfalls dauerhaft nutzen.

No 32Guards, plain text email/Kein 32Guards, Klartext-E-Mail

Diese Regel sendet alle E-Mails als Text-E-Mails ohne Signierung und Verschlüsselung sowie ohne 32Guards-Prüfung. TLS wird weiterhin angewendet, sofern verfügbar. Sie eignet sich nur für Fälle, in denen ein False Positive von 32Guards vorliegt. Siehe **Melden von False Negatives und False Positives**.

> **HINWEIS:** Sie sollten diese Regel keinesfalls dauerhaft nutzen.

Inhaltsfiltersets zuordnen

Es gibt drei verschiedene Einstellungen für den Inhaltsfilter in NoSpamProxy Cloud, die E-Mail-Anhänge unterschiedlich restriktiv verarbeiten.

Sie können Inhaltsfiltersets

- als Standardeinstellung für Partner,
- für einzelne Partnerdomänen,
- als Standardeinstellung für Unternehmensbenutzer oder
- für einzelne Active-Directory-Gruppen

zuordnen.

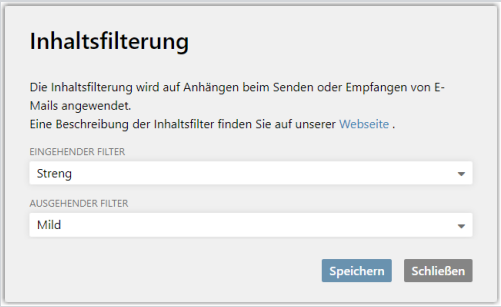
TIP: Wir prüfen bei der Verarbeitung die konfigurierten Inhaltsfilter sowohl auf Seite der Partner als auch auf Seite der Unternehmensbenutzer. Um zu vermeiden, dass ein unerwünschter Inhaltsfilter angewendet wird, empfehlen wir, diese Einstellung zunächst als Standardeinstellung für Partner **oder** Unternehmensbenutzer zu definieren. Dies verbessert zudem die Übersichtlichkeit. In jedem Fall sollten Sie für diese Standardeinstellung den Filter **Strict/Streng** wählen und nur absolut notwendige, granulare Anpassungen für Partnerdomänen oder AD-Gruppen vornehmen.

Einstellungen ändern

Um die Einstellungen für den Inhaltsfilter zu ändern, gehen Sie folgendermaßen vor:

1. Führen Sie einen der folgenden beiden Schritte durch:
   - Gehen Sie zu **Identitäten > Unternehmensbenutzer > Inhaltsfilterung**.
   - Gehen Sie zu **Identitäten > Partner > Standardeinstellungen für Partner**.
   - Gehen Sie zu **Identitäten > Partner** und markieren Sie die Partnerdomäne, deren Inhaltsfilterung Sie bearbeiten wollen.
2. Klicken Sie **Bearbeiten**.

3. Wählen Sie die Inhaltsfiltereinstellungen für eingehende und ausgehende E-Mails.



4. Klicken Sie **Speichern**.

> **HINWEIS:** Falls Ihnen hier kein Inhaltsfilter zur Auswahl steht, wurden noch keine Inhaltsfilter für Sie angelegt. Wenden Sie sich in diesem Fall direkt an Ihren Reseller/Managed Service Provider.

Vorkonfigurierte Inhaltsfiltersets

Hier finden Sie eine tabellarische Übersicht der in NoSpamProxy Cloud vorkonfigurierten Inhaltsfiltersets sowie deren jeweilige Einstellungen.

Eingehende E-Mails

Inhaltsfiltereinstellung *Streng*

Dateiname	Dateityp	Aktion trusted	Aktion untrusted	Web Portal E-Mails
Attached file.txt		Erlauben	Erlauben	Erlauben

oledata.mso		Erlauben	Erlauben	Erlauben
sharing_ metadata.xml		Erlauben	Erlauben	Erlauben
winmail.dat		Erlauben	Erlauben	Erlauben
*.asice		Erlauben	Erlauben	Erlauben
*.eml		Erlauben	Erlauben	Erlauben
*.emz		Erlauben	Erlauben	Erlauben
*.heic		Erlauben	Erlauben	Erlauben
*.heif		Erlauben	Erlauben	Erlauben
*.ics		Erlauben	Erlauben	Erlauben
*.vcf		Erlauben	Erlauben	Erlauben
*.wmz		Erlauben	Erlauben	Erlauben
*.js		Erlauben	Abweisen	Erlauben
	Verschlüsselte ZIP-komprimierte Datei	Erlauben	Abweisen	Erlauben
	JPEG	Erlauben	Erlauben	Erlauben
	PNG	Erlauben	Erlauben	Erlauben
	BMP	Erlauben	Erlauben	Erlauben
	EMF	Erlauben	Erlauben	Erlauben
	EMZ	Erlauben	Erlauben	Erlauben
	GIF	Erlauben	Erlauben	Erlauben

	MP3-Audiodateien	Erlauben	Erlauben	Erlauben
	MP4-Audiodateien	Erlauben	Erlauben	Erlauben
	MP4-Videodateien	Erlauben	Erlauben	Erlauben
	OpenDocument spreadsheet (ODS)	Erlauben	Erlauben	Erlauben
	OpenDocument text document (ODT)	Erlauben	Erlauben	Erlauben
	OpenDocument presentation (ODP)	Erlauben	Erlauben	Erlauben
	TIFF	Erlauben	Erlauben	Erlauben
	WMF	Erlauben	Erlauben	Erlauben
	Plain text	Erlauben	Erlauben	Erlauben
	HTML	Erlauben	Erlauben	Erlauben
	ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	7ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	GZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	X.509-Zertifikat (CER, CRT, DER, PEM)	Erlauben	Erlauben	Erlauben
	ZUGFeRD BASIC	Erlauben	Erlauben	Erlauben

	ZUGFeRD BASIC WL	Erlauben	Erlauben	Erlauben
	ZUGFeRD EN 16931	Erlauben	Erlauben	Erlauben
	ZUGFeRD EXTENDED	Erlauben	Erlauben	Erlauben
	ZUGFeRD MINIMUM	Erlauben	Erlauben	Erlauben
	ZUGFeRD XRECHNUNG	Erlauben	Erlauben	Erlauben
	XRechnung	Erlauben	Erlauben	Erlauben
*.pages, *.numbers		Erlauben	Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	AutoCAD Drawing	Erlauben	Abweisen	Abweisen
	AutoCAD Drawing Exchange Format	Erlauben	Abweisen	Abweisen
	AutoCAD Design Web Format	Erlauben	Abweisen	Abweisen
	Word-Dokument (2007-2016, DOCX)	Erlauben	CDR	Erlauben
	Excel-Dokument (2007-2016, XLSX)	Erlauben	CDR	Erlauben

	PDF-Dokument	Erlauben	CDR	Erlauben
	PDF-Dokument mit URLs	Erlauben	CDR	Erlauben
	Powerpoint-Dokument (2007-2016, PPTX)	Erlauben	Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Nicht lesbares PDF-Dokument	Erlauben	CDR	Erlauben
	XML	Erlauben	Abweisen	Erlauben
	Verschlüsselte PDF-Datei	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden
	Unverarbeitbares Archiv	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden
Beliebig		Abweisen	Abweisen	Abweisen

Inhaltsfiltereinstellung *Mittel*

Dateiname	Dateityp	Aktion trusted	Aktion untrusted	Web Portal E-Mails
Attached file.txt		Erlauben	Erlauben	Erlauben
oledata.mso		Erlauben	Erlauben	Erlauben

sharing_ metadata.xml		Erlauben	Erlauben	Erlauben
winmail.dat		Erlauben	Erlauben	Erlauben
*.asice		Erlauben	Erlauben	Erlauben
*.eml		Erlauben	Erlauben	Erlauben
*.emz		Erlauben	Erlauben	Erlauben
*.heic		Erlauben	Erlauben	Erlauben
*.heif		Erlauben	Erlauben	Erlauben
*.ics		Erlauben	Erlauben	Erlauben
*.pages, *.numbers		Erlauben	Erlauben	Erlauben
*.vcf		Erlauben	Erlauben	Erlauben
*.wmz		Erlauben	Erlauben	Erlauben
	JPEG	Erlauben	Erlauben	Erlauben
	PNG	Erlauben	Erlauben	Erlauben
	BMP	Erlauben	Erlauben	Erlauben
	EMF	Erlauben	Erlauben	Erlauben
	Excel-Dokument (2007-2016, XLSX)	Erlauben	Erlauben	Erlauben
	GIF	Erlauben	Erlauben	Erlauben
	MP3-Audiodateien	Erlauben	Erlauben	Erlauben

	MP4-Audiodateien	Erlauben	Erlauben	Erlauben
	MP4-Videodateien	Erlauben	Erlauben	Erlauben
	OpenDocument spreadsheet (ODS)	Erlauben	Erlauben	Erlauben
	OpenDocument text document (ODT)	Erlauben	Erlauben	Erlauben
	OpenDocument presentation (ODP)	Erlauben	Erlauben	Erlauben
	OpenDocument drawing (ODG)	Erlauben	Erlauben	Erlauben
	OpenDocument chart (ODC)	Erlauben	Erlauben	Erlauben
	OpenDocument image (ODI)	Erlauben	Erlauben	Erlauben
	OpenDocument master document (ODM)	Erlauben	Erlauben	Erlauben
	TIFF	Erlauben	Erlauben	Erlauben
	WMF	Erlauben	Erlauben	Erlauben
	Word-Dokument (2007-2016, DOCX)	Erlauben	Erlauben	Erlauben
	Verschlüsseltes PDF-Dokument	Erlauben	Erlauben	Erlauben
	Plain text	Erlauben	Erlauben	Erlauben

	HTML	Erlauben	Erlauben	Erlauben
	ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	7ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	GZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	PowerPoint-Dokument (2007-2016, PPTX)	Erlauben	Erlauben	Erlauben
	Nicht verarbeitbares Archiv	Erlauben	Erlauben	Erlauben
	Verschlüsselte ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	X.509-Zertifikat (CER, CRT, DER, PEM)	Erlauben	Erlauben	Erlauben
	Verschlüsseltes PDF-Dokument	Erlauben	Erlauben	Erlauben
	XML	Erlauben	Erlauben	Erlauben
	ZUGFeRD BASIC	Erlauben	Erlauben	Erlauben
	ZUGFeRD BASIC WL	Erlauben	Erlauben	Erlauben
	ZUGFeRD EN 16931	Erlauben	Erlauben	Erlauben
	ZUGFeRD EXTENDED	Erlauben	Erlauben	Erlauben
	ZUGFeRD MINIMUM	Erlauben	Erlauben	Erlauben
	ZUGFeRD	Erlauben	Erlauben	Erlauben

	XRECHNUNG			
	XRechnung	Erlauben	Erlauben	Erlauben
	AutoCAD Drawing	Erlauben	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden
	AutoCAD Drawing Exchange Format	Erlauben	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden
	AutoCAD Design Web Format	Erlauben	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden
	Word-Dokument (97-2003, DOC)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Word-Dokument mit Makros (97-2003, DOC)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Word-Dokument mit Makros (2007 oder später, DOCM)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2	Erlauben

			Stunden	
	Word-Dokument mit OLE-Objekten (97-2003, DOC)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Word-Dokument mit OLE-Objekten (2007 oder später, DOCX)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Word-Vorlage (2007-2016, DOTX)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Word-Vorlage mit Makros (2007 oder später, DOTM)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Excel-Dokument (97-2003, XLS)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Excel-Dokument mit Makros (97-2003, XLS)	Erlauben	CDR; Quarantäne;	Erlauben

			automatische Freigabe nach 2 Stunden	
	Excel-Dokument mit Makros (2007 oder später, XLSM)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Excel-Dokument mit OLE-Objekten (97-2003, XLS)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Excel-Dokument mit OLE-Objekten (2007 oder später, XLSX)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Excel-Vorlage (2007-2016, XLTX)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Excel-Vorlage mit Makros (2007 oder später, XLTM)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben

	Excel Add-in mit Makros (2007 oder später, XLAM)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	PDF-Dokument	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	PDF-Dokument mit URLs	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Nicht lesbares PDF-Dokument	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	PowerPoint-Präsentation (97-2003, PPT)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	PowerPoint-Vorlage (2007-2016, POTX)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2	Erlauben

			Stunden	
	PowerPoint-Slideshow (2007-2016, PPSX)	Erlauben	CDR; Quarantäne; automatische Freigabe nach 2 Stunden	Erlauben
	Private Zertifikate (PFX, P12)	Erlauben	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden
Beliebig		Abweisen	Abweisen	Abweisen

Inhaltsfiltereinstellung *Mild*

Dateiname	Dateityp	Aktion trusted	Aktion untrusted	Web Portal E-Mails
Attached file.txt		Erlauben	Erlauben	Erlauben
oledata.mso		Erlauben	Erlauben	Erlauben
sharing_ metadata.xml		Erlauben	Erlauben	Erlauben
winmail.dat		Erlauben	Erlauben	Erlauben
*.asice		Erlauben	Erlauben	Erlauben
*.eml		Erlauben	Erlauben	Erlauben
*.emz		Erlauben	Erlauben	Erlauben
*.heic		Erlauben	Erlauben	Erlauben

*.heif		Erlauben	Erlauben	Erlauben
*.ics		Erlauben	Erlauben	Erlauben
*.pages, *.numbers		Erlauben	Erlauben	Erlauben
*.vcf		Erlauben	Erlauben	Erlauben
*.wmz		Erlauben	Erlauben	Erlauben
	JPEG	Erlauben	Erlauben	Erlauben
	PNG	Erlauben	Erlauben	Erlauben
	BMP	Erlauben	Erlauben	Erlauben
	EMF	Erlauben	Erlauben	Erlauben
	EMZ	Erlauben	Erlauben	Erlauben
	GIF	Erlauben	Erlauben	Erlauben
	MP3-Audiodateien	Erlauben	Erlauben	Erlauben
	MP4-Audiodateien	Erlauben	Erlauben	Erlauben
	MP4-Videodateien	Erlauben	Erlauben	Erlauben
	OpenDocument spreadsheet (ODS)	Erlauben	Erlauben	Erlauben
	OpenDocument text document (ODT)	Erlauben	Erlauben	Erlauben
	OpenDocument presentation (ODP)	Erlauben	Erlauben	Erlauben
	OpenDocument	Erlauben	Erlauben	Erlauben

	drawing (ODG)			
	OpenDocument chart (ODC)	Erlauben	Erlauben	Erlauben
	OpenDocument chart template (OTC)	Erlauben	Erlauben	Erlauben
	OpenDocument image (ODI)	Erlauben	Erlauben	Erlauben
	OpenDocument master document (ODM)	Erlauben	Erlauben	Erlauben
	OpenDocument master document template (OTM)	Erlauben	Erlauben	Erlauben
	OpenDocument text template (OTT)	Erlauben	Erlauben	Erlauben
	OpenDocument spreadsheet template (OTS)	Erlauben	Erlauben	Erlauben
	OpenDocument presentation template (OTP)	Erlauben	Erlauben	Erlauben
	OpenDocument drawing template (OTG)	Erlauben	Erlauben	Erlauben
	OpenDocument	Erlauben	Erlauben	Erlauben

	database (ODB)			
	OpenDocument formula (ODF)	Erlauben	Erlauben	Erlauben
	OpenDocument formula template (OTF)	Erlauben	Erlauben	Erlauben
	OpenDocument HTML template (OTH)	Erlauben	Erlauben	Erlauben
	OpenDocument image (ODI)	Erlauben	Erlauben	Erlauben
	TIFF	Erlauben	Erlauben	Erlauben
	WMF	Erlauben	Erlauben	Erlauben
	Plain Text	Erlauben	Erlauben	Erlauben
	HTML	Erlauben	Erlauben	Erlauben
	ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	7ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	GZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	X.509-Zertifikat (CER, CRT, DER, PEM)	Erlauben	Erlauben	Erlauben

	PowerPoint-Dokument (2007-2016, PPTX)	Erlauben	Erlauben	Erlauben
	Unverarbeitbares Archiv	Erlauben	Erlauben	Erlauben
	Verschlüsselte ZIP-komprimierte Datei	Erlauben	Erlauben	Erlauben
	Verschlüsseltes PDF-Dokument	Erlauben	Erlauben	Erlauben
	Verschlüsseltes Excel-Dokument (97-2003, XLS)	Erlauben	Erlauben	Erlauben
	Verschlüsseltes Excel-Dokument (2007-heute, XLSX)	Erlauben	Erlauben	Erlauben
	Verschlüsselte PowerPoint-Präsentation (97-2003, PPT)	Erlauben	Erlauben	Erlauben
	Verschlüsselte PowerPoint-Präsentation (2007-heute, PPTX)	Erlauben	Erlauben	Erlauben
	Verschlüsseltes Word-Dokument (97-2003, DOC)	Erlauben	Erlauben	Erlauben

	Verschlüsseltes Word-Dokument (2007-heute, DOCX)	Erlauben	Erlauben	Erlauben
	Word-Dokument (2007-2016, DOCX)	Erlauben	Erlauben	Erlauben
	Word-Dokument (97-2003, DOC)	Erlauben	Erlauben	Erlauben
	Word-Vorlage (2007-2016, DOTX)	Erlauben	Erlauben	Erlauben
	Excel-Dokument (2007-2016, XLSX)	Erlauben	Erlauben	Erlauben
	Excel-Dokument (97-2003, XLS)	Erlauben	Erlauben	Erlauben
	Excel-Vorlage (2007-2016, XLTX)	Erlauben	Erlauben	Erlauben
	PDF-Dokument	Erlauben	Erlauben	Erlauben
	PDF-Dokument mit URLs	Erlauben	Erlauben	Erlauben
	Nicht lesbares PDF-Dokument	Erlauben	Erlauben	Erlauben
	PowerPoint-Präsentation (2007-2016, PPTX)	Erlauben	Erlauben	Erlauben
	PowerPoint-	Erlauben	Erlauben	Erlauben

	Präsentation (97-2003, PPT)			
	PowerPoint-Präsentation (2007-2016, POTX)	Erlauben	Erlauben	Erlauben
	PowerPoint-Slideshow (2007-2016, PPSX)	Erlauben	Erlauben	Erlauben
	AutoCAD Drawing	Erlauben	Erlauben	Erlauben
	AutoCAD Drawing Exchange Format	Erlauben	Erlauben	Erlauben
	AutoCAD Design Web Format	Erlauben	Erlauben	Erlauben
	XML	Erlauben	Erlauben	Erlauben
	ZUGFeRD BASIC	Erlauben	Erlauben	Erlauben
	ZUGFeRD BASIC WL	Erlauben	Erlauben	Erlauben
	ZUGFeRD EN 16931	Erlauben	Erlauben	Erlauben
	ZUGFeRD EXTENDED	Erlauben	Erlauben	Erlauben
	ZUGFeRD MINIMUM	Erlauben	Erlauben	Erlauben
	ZUGFeRD XRECHNUNG	Erlauben	Erlauben	Erlauben

	XRechnung	Erlauben	Erlauben	Erlauben
	Microsoft shell link (LNK)	Abweisen	Abweisen	Abweisen
	Microsoft shell link (URL)	Abweisen	Abweisen	Abweisen
	RTF	Abweisen	Abweisen	Abweisen
Beliebig		Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden	Quarantäne; automatische Freigabe nach 2 Stunden

Eingehende E-Mails mit Sandboxing

HINWEIS: Die Inhaltsfiltereinstellungen **Mittel - Sandboxing** und **Streng - Sandboxing** sind verfügbar, wenn Sie eine Lizenz für den NoSpamProxy Sandbox Service erworben haben. Der Sandbox Service erhöht die Wahrscheinlichkeit, dass schadhafte Inhalte entdeckt werden.

Wichtige Hinweise

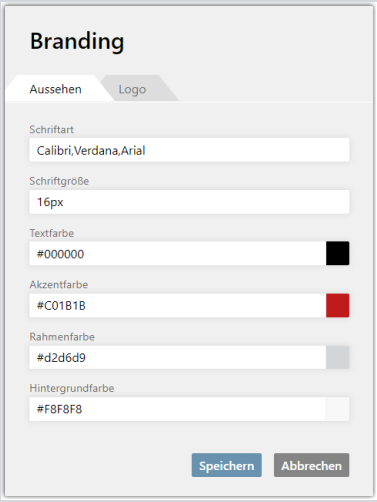
HINWEIS:

- Der Inhaltsfilter **Wildcard** lässt alle eingehenden E-Mails passieren und sollte nur in Ausnahmefällen genutzt werden.
- NoSpamProxy verarbeitet E-Mails, deren Größe 500 MB nicht überschreitet.
- Dateien, die auf dem Web Portal gespeichert werden, werden **nach vier Wochen automatisch gelöscht**. Laden Sie eventuell benötigte Dateien im Zweifelsfall herunter.
- Wir empfehlen Ihnen, für eingehende E-Mails die Einstellung **Streng** zu wählen.
- Befinden sich **nicht erlaubte** Dateitypen in **erlaubten** Archiven wie ZIP, 7ZIP oder GZIP, so wird das gesamte Archiv entsprechend der Konfiguration für den Dateityp behandelt. Enthält eine E-Mail also eine (erlaubte) ZIP-komprimierte Datei, wird sie abgewiesen, falls das ZIP-Archiv beispielsweise eine (nicht erlaubte) ausführbare Datei enthält.

Branding

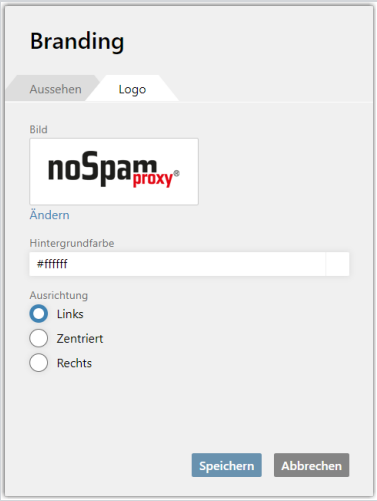
Hier können Sie das Farbschema des Web Portals ändern und es so an die Corporate Identity Ihres Unternehmens anpassen. Außerdem können Sie ein Logo hochladen.

1. Gehen Sie zu **Konfiguration > Branding**.
2. Klicken Sie **Bearbeiten**.
3. Bestimmen Sie unter **Aussehen** die Details zur verwendeten Schrift, die Akzentfarbe, die Rahmenfarbe und die Hintergrundfarbe.



4. Wählen Sie unter **Logo** das Logo, das Sie verwenden wollen sowie die Hintergrundfarbe und die Ausrichtung des Logos.

> **HINWEIS:** Die maximale Größe der Bilddatei ist 100 Kilobyte.



5. Klicken Sie **Speichern**.

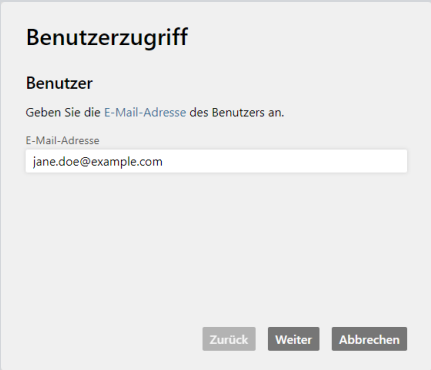
Administration

Als Administrator können Sie bestimmen,

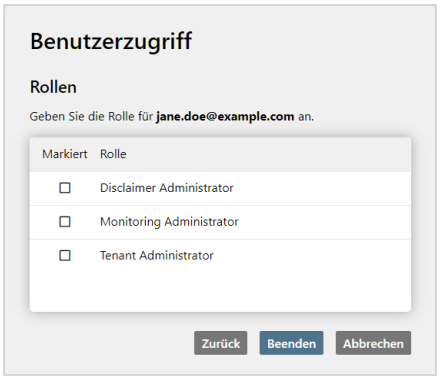
- welche Personen als Benutzer Zugriff auf Ihren Mandanten haben und
- welche Rollen die jeweiligen Benutzer:innen haben.

Benutzer hinzufügen

1. Gehen Sie zu **Administration > Zugriffsverwaltung > Benutzerzugriff**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie die E-Mail-Adresse des Benutzers an.



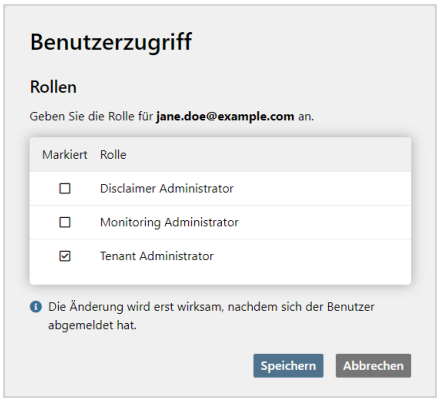
4. Weisen Sie dem/r Benutzer:in eine Rolle zu.



5. Klicken Sie **Speichern**.

Eine andere Rolle zuweisen

1. Gehen Sie zu **Administration > Zugriffsverwaltung > Benutzerzugriff**.
2. Klicken Sie **Bearbeiten**.



3. Wählen Sie die neue Rolle aus dem Drop-Down-Menü aus.
4. Klicken Sie **Speichern**.

> **HINWEIS:** Es muss mindestens ein Tenant Administrator vorhanden sein.

Benutzer löschen

1. Gehen Sie zu **Administration > Zugriffsverwaltung > Benutzerzugriff**.
2. Klicken Sie den **Mülleimer**, der neben dem/r jeweiligen Benutzer:in angezeigt wird.
3. Bestätigen Sie das Löschen, indem Sie **Entfernen** klicken.

Zugriff für Vertriebspartner einrichten

Sie können Ihrem Vertriebspartner Zugriff auf Ihren Mandanten gewähren, damit dieser beispielsweise Wartungsarbeiten durchführen kann.

1. Gehen Sie zu **Administration > Zugriffsverwaltung > Vertriebspartnerzugriff**.
2. Klicken Sie **Bearbeiten**.

3. Wählen Sie **Ordnen Sie die folgende Rolle zu** und wählen Sie die gewünschte

Rolle im Drop-Down-Menü aus.

4. Klicken Sie **Speichern**.

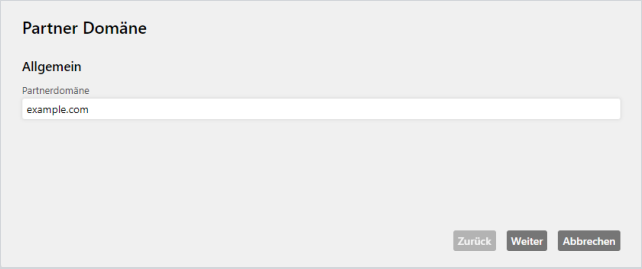
Identitäten

Partner

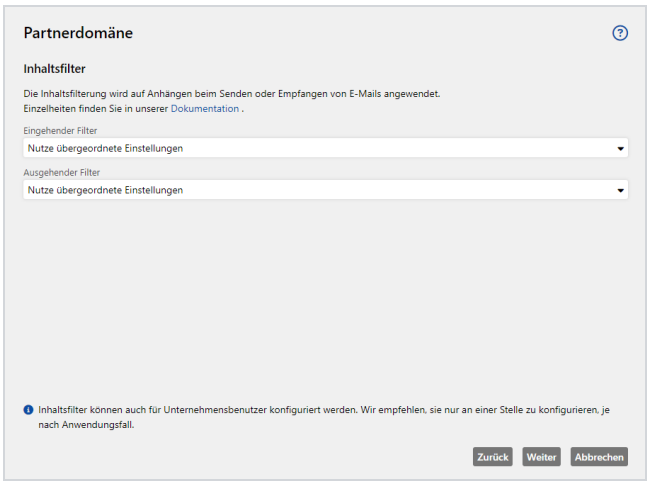
Partner sind Personen außerhalb Ihres Unternehmens, mit denen die Benutzer Ihres Unternehmens E-Mails austauschen.

Partnerdomänen hinzufügen

1. Gehen Sie zu **Identitäten > Partner**.
2. Klicken Sie **Hinzufügen**.
3. Geben Sie den Namen der Partnerdomäne ein.

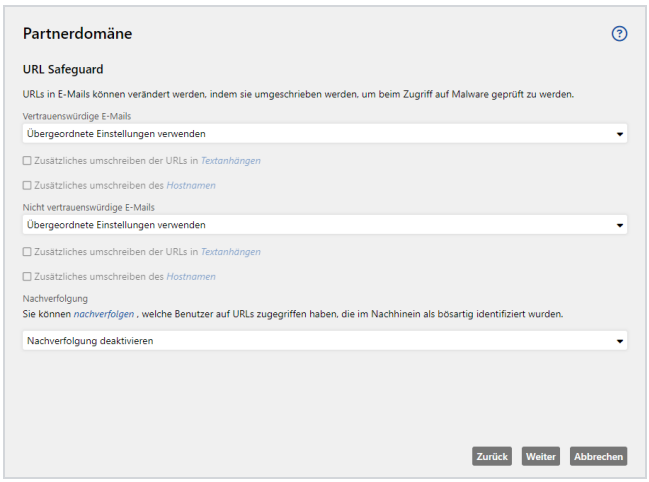


4. Wählen Sie die gewünschten Einstellungen für den **Wichtige Hinweise** für eingehende beziehungsweise ausgehende E-Mails.



HINWEIS: Inhaltsfilter können auch für Unternehmensbenutzer konfiguriert werden. Wir empfehlen, Inhaltsfilter nur an einer Stelle zu konfigurieren.

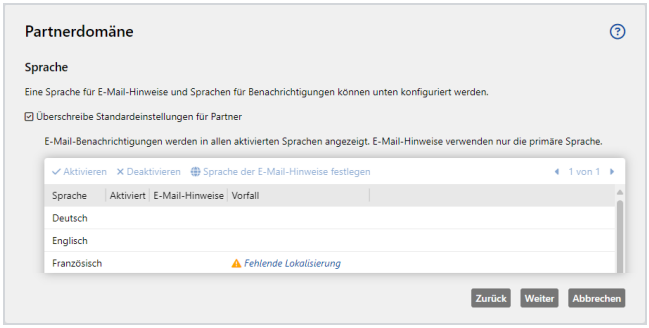
5. Wählen Sie die gewünschten Einstellungen für den URL Safeguard.



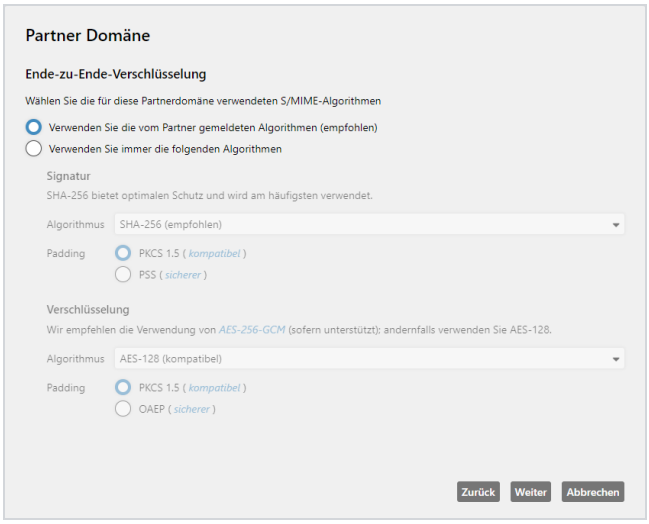
Mit Hilfe der Rückverfolgung können Sie nachvollziehen, welche Benutzer auf

URLs zugegriffen haben, die sich **danach** als bösartig herausgestellt haben. Details finden Sie dann auf der Registerkarte **URL Safeguard** des jeweiligen Message Tracks. Siehe auch URL Tracking.

6. Wählen Sie eine Sprache für E-Mail-Hinweise und -Benachrichtigungen, die zu E-Mails hinzugefügt werden.

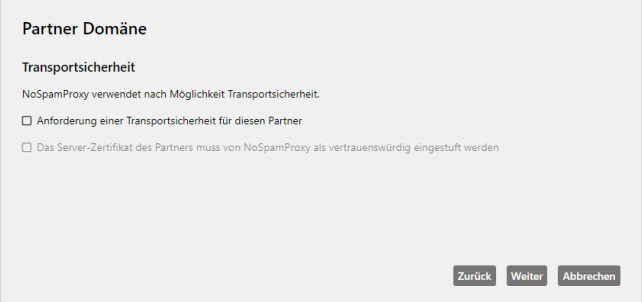


7. Legen Sie die Ende-zu-Ende-Verschlüsselung fest.

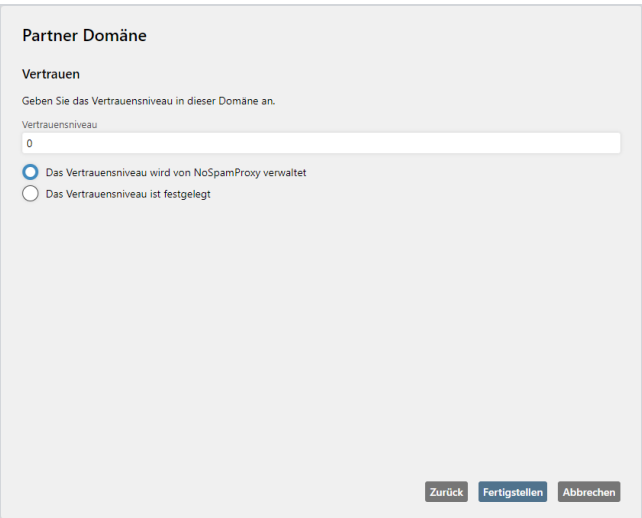


8. Wählen Sie die Transportsicherheit für diese Domäne. Die Transportsicherheit legt fest, ob die Kommunikation zu den Server der Partnerdomäne

verschlüsselt erfolgen muss und welchen Zertifikaten gegebenenfalls vertraut wird.



9. Geben Sie das Vertrauen in diese Domäne an. Das Vertrauen in eine Domäne wird durch an die Domäne gesandte E-Mails stärker und nähert sich ohne weitere E-Mail-Kommunikation mit der Zeit wieder dem Wert 0 an. Sie können das Vertrauen auch auf einen festen Wert einstellen.



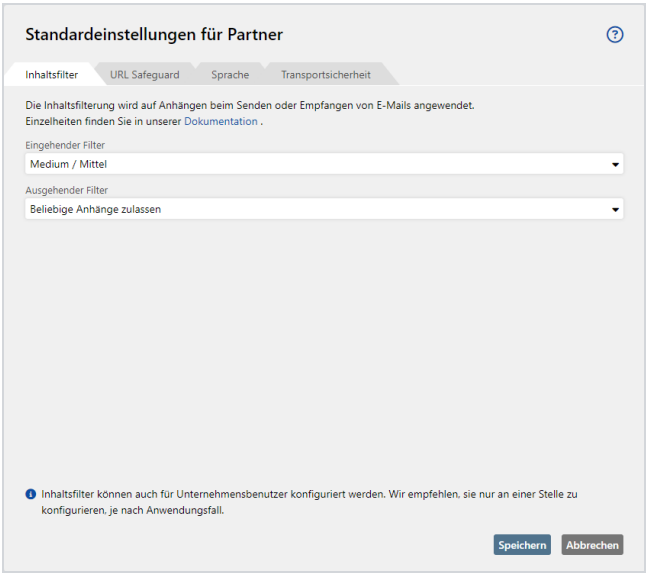
10. Klicken Sie **Fertigstellen**.

Standardeinstellungen für Partner

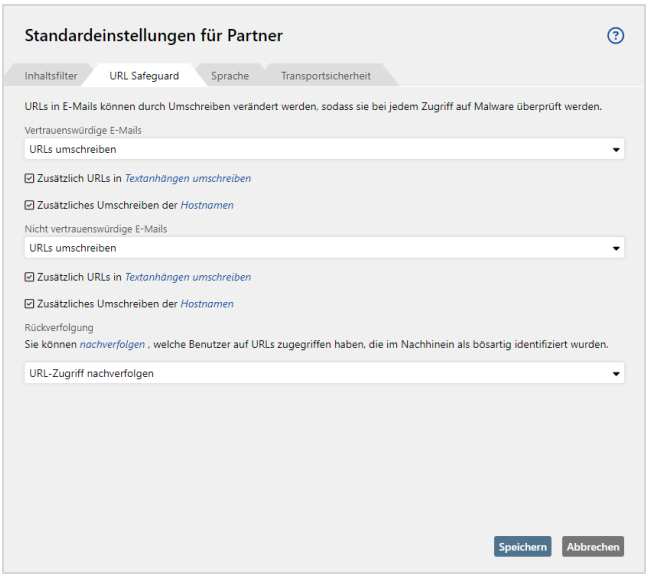
Unter **Identitäten > Partner > Standardeinstellungen für Partner** nehmen Sie übergeordnete Einstellungen vor, die genutzt werden, falls kein Partnereintrag für eine spezifische Domäne vorhanden ist.

- Klicken Sie **Bearbeiten**, um das Dialogfenster **Standardeinstellungen für Partner** zu öffnen.

Inhaltsfilter| Wählen Sie jeweils eine Richtlinie für E-Mail-Anhänge an eingehenden und ausgehenden E-Mails. Siehe **Wichtige Hinweise**.

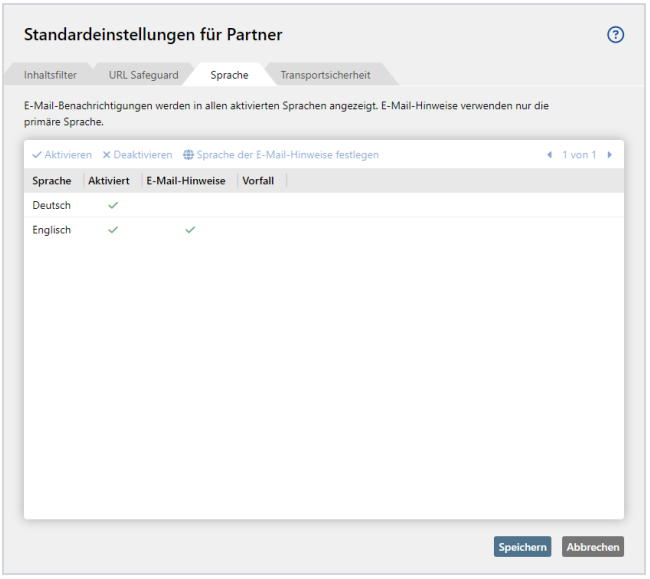


URL Safeguard| Konfigurieren Sie das grundlegende Verhalten des URL Safeguard für vertrauenswürdige und nicht vertrauenswürdige E-Mails. Bestimmen Sie außerdem, ob die Rückverfolgung ein- oder ausgeschaltet sein soll.

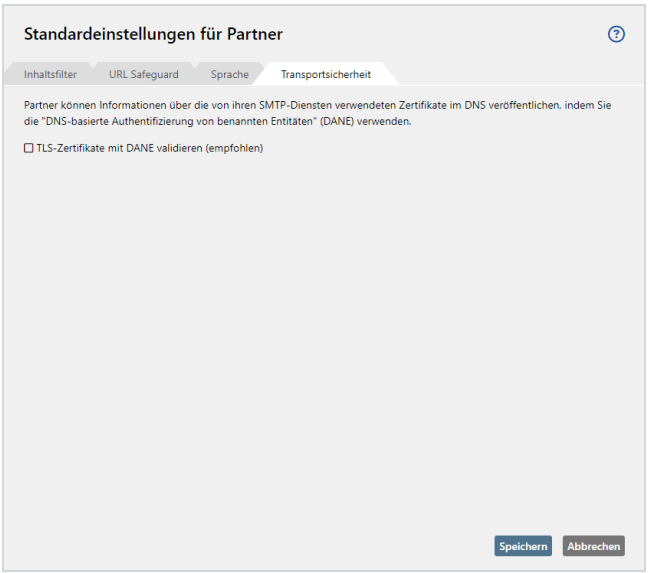


> Mit Hilfe der Rückverfolgung können Sie nachvollziehen, welche Benutzer auf URLs zugegriffen haben, die sich **danach** als bösartig herausgestellt haben.

Sprache| Wählen Sie eine Sprache für E-Mail-Hinweise und -Benachrichtigungen, die zu E-Mails hinzugefügt werden.

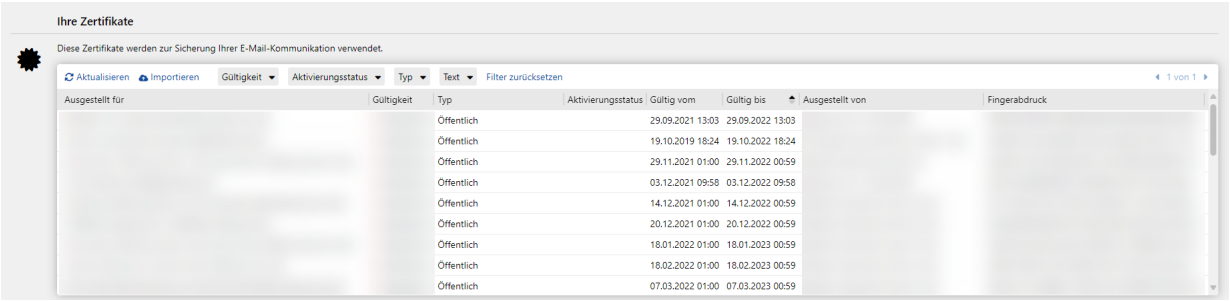


Transportsicherheit| Bestimmen Sie, ob Sie TLS-Zertifikate mit DANE validieren wollen (empfohlen).



> Durch die Benutzung von **DNS-based Authentication of Named Entities** (DANE) werden die TLS-Zertifikate der Transportverschlüsselung überprüft, so dass nur Zertifikate akzeptiert werden, die der Empfänger der E-Mail auch als vertrauenswürdig eingestuft hat.

Ihre Zertifikate



Unter **Identitäten > Zertifikate > Ihre Zertifikate** finden Sie alle Zertifikate, die in NoSpamProxy Cloud für Sie hinterlegt sind.

Zertifikate importieren

HINWEIS:
Sie können bis zu 100 Zertifikate aus einer oder mehreren Dateien auf einmal importieren. Private Schlüssel sind in der Regel passwortgeschützt. Die folgenden Dateiformate werden unterstützt:

- PEM
- CER/DER
- PFX
- P12
- P7B

1. Klicken Sie **Importieren**.
2. Wählen Sie die Zertifikatsdatei aus.

3. Geben Sie bei Bedarf das Passwort ein.
4. Klicken Sie **Importieren**.

Nach Zertifikaten suchen

Um nach bestimmten Zertifikaten zu suchen, stehen Ihnen verschiedene Filter zur Verfügung:

Gültigkeit| Beliebige Gültigkeit, Abgelaufen, Läuft innerhalb eines Monats ab, Läuft innerhalb einer Woche ab, Noch nicht gültig oder Gültig

Aktivierungsstatus| Aktiv, Kein Benutzer zugewiesen oder Lizenz überschritten

Typ| Privat, Öffentlich, Zwischenzertifizierungsstellen oder Stammzertifizierungsstellen

Text| Hier können Sie nach bestimmten Werten in den Feldern ausgestellt für, ausgestellt von, den E-Mail-Adressen oder dem Fingerabdruck suchen.

Verwaltete Zertifikate anfordern

> Diese Funktion ist verfügbar, wenn Sie **Managed Certificates** und **NoSpamProxy Cloud Encryption** lizenziert haben.

Die Anforderung von verwalteten Zertifikaten konfigurieren Sie durch den automatischen Benutzerimport. Siehe **Automatischer Benutzerimport via Azure Active Directory**.

Um verwaltete Zertifikate für bestehende automatische Benutzerimporte zu konfigurieren, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Konfiguration > Automatischer Benutzerimport**.
2. Klicken Sie den Benutzerimport, den Sie konfigurieren wollen.
3. Wechseln Sie zur Registerkarte **Gruppen**.
4. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie **Hinzufügen** und nehmen Sie die Konfiguration wie unter Automatischer Benutzerimport via Azure Active Directory beschrieben vor oder
    - klicken Sie die jeweilige Gruppe, wechseln Sie zur Registerkarte **Zertifikatsanforderung** und setzten Sie das Häkchen bei **Automatisch S/MIME-Zertifikate anfordern und verwalten**.
5. Klicken Sie **Speichern**.

HINWEIS:

- Damit für alle Benutzer verwaltete Zertifikate angefordert werden können, müssen Sie eine ausreichende Anzahl an Benutzern lizenziert haben. Sollte beispielsweise die hinzugefügte Gruppe mehr Benutzer enthalten als Lizenzen zur Verfügung stehen, so werden keine verwalteten Zertifikate angefordert. Der Administrator erhält in diesem Fall eine Benachrichtigungs-E-Mail.
- Damit verwaltete Zertifikate für Benutzer angefordert werden können, muss das Benutzerattribut **E-Mail-Adresse** für diese Benutzer hinterlegt sein.
- Im Azure AD müssen für die E-Mail-Adresse die Attribute **Vorname** und **Nachname** vergeben werden.

Angeforderte verwaltete Zertifikate werden automatisch zu **Open Keys** hochgeladen.

Wann werden verwaltete Zertifikate erneuert?
Verwaltete Zertifikate werden 14 Tage vor Ablauf des vorliegenden Zertifikats erneuert.

Um welche Art Zertifikate handelt es sich bei verwalteten Zertifikaten?

Domain-validierte S/MIME-Zertifikate.

Ich habe eine E-Mail mit Informationen zu einem Zertifikat erhalten. Was muss ich tun?

Werden verwaltete Zertifikate für Unternehmensbenutzer ausgestellt, erhalten diese Unternehmensbenutzer über die Ausstellung sowie bei Ablauf von Zertifikaten eine Benachrichtigung. Sie können diese E-Mail ignorieren, da NoSpamProxy die Zertifikate automatisch ausstellt und importiert.

Überprüfte Domänen für die verwalteten Zertifikate hinzufügen

NoSpamProxy Cloud kann die E-Mail-Zertifikate für Ihre Unternehmensdomänen automatisch verwalten. Damit Sie die verwalteten Zertifikate für Domänen verwenden können, müssen Sie diese Domänen hier hinzufügen.

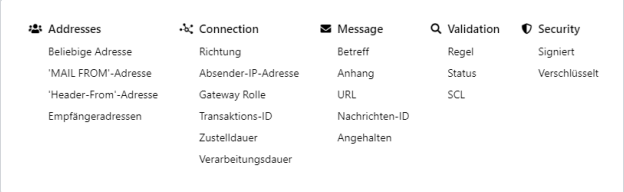
1. Gehen Sie zu **Identitäten > Zertifikate > Überprüfte Domänen für die verwalteten Zertifikate**.
2. Klicken Sie **Hinzufügen**.
3. Wählen Sie die Unternehmensdomäne aus, für die Sie die verwalteten Zertifikate verwenden wollen.
4. Kopieren Sie den angezeigten Verifizierungs-Token in die Zwischenablage.
5. Erstellen Sie einen TXT-Eintrag in der DNS-Zone der zuvor gewählten Domäne.
6. Klicken Sie **Beenden**.

HINWEIS: Die zusätzliche, jährliche Domänenüberprüfung per TXT-Eintrag ist erforderlich, um die automatische Schlüsselanforderung für Domänen zu aktivieren. 30 Tage vor Ablauf der Domänenüberprüfung erhält der Administrator eine Benachrichtigungs-E-Mail mit dem Betreff "Domänenvalidierung für Managed Certificates läuft aus / Domain validation for Managed Certificates will expire".

E-Mails filtern

Bedingungen hinzufügen

1. Klicken Sie **Bedingung hinzufügen** in der linken oberen Ecke der Nachrichtenverfolgung.



2. Wählen und konfigurieren eine oder mehrere Bedingungen.
3. Klicken Sie **Suchen**, um die Abfrage auszuführen.

Um eine Bedingung zu entfernen, klicken Sie **Bedingung entfernen** neben der jeweiligen Bedingung.

Suchen speichern

Um eine von Ihnen konfigurierte Suche nicht jedes Mal neu erstellen zu müssen, können Sie diese speichern. Im Drop-Down-Menü **Gespeicherte Suchen** können Sie diese dann auswählen.

- Klicken Sie nach dem Konfigurieren der Abfrage unter **Gespeicherte Suchen** auf **Aktuelle Suche hinzufügen**, um Sie zu speichern.

Suchen als Standard speichern

Standardsuchen werden bei jedem Öffnen der Nachrichtenverfolgung ausgeführt.

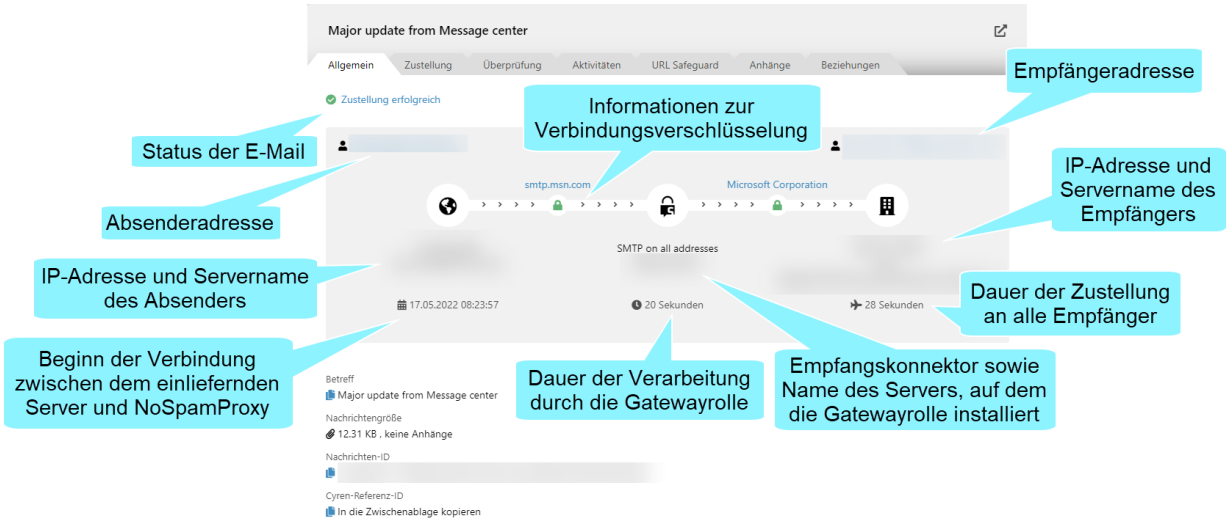
- Markieren Sie im Drop-Down-Menü **Gespeicherte Suchen** die gewünschte Suche mit 💙, um diese als Standardsuche zu speichern.

Details zu einer E-Mail anzeigen

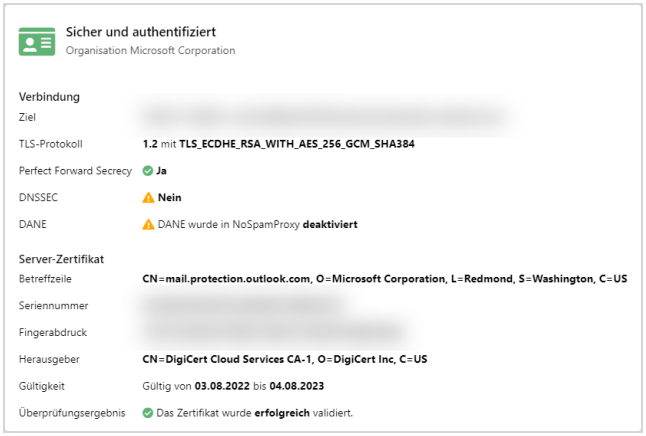
- Klicken Sie die E-Mail, deren Details Sie anzeigen wollen. Die Detailansicht der jeweiligen E-Mail öffnet sich.
- Klicken Sie in der Detailansicht auf der Registerkarte **Allgemein** das Icon ⧉, um die Detailansicht in einem neuen Tab zu öffnen.
- Klicken Sie **Nachrichtenverfolgungsdatensatz herunterladen**, um den Datensatz als json-Datei auf Ihrem Computer zu speichern.

Registerkarte Allgemein

Hier finden Sie allgemeine Informationen zur E-Mail und deren Anhängen sowie zur Verbindung und Übertragung.



- Zur Ermittlung des Servernamens wird auf Basis der IP-Adresse ein Reverse DNS Lookup ausgeführt.
- Durch Klicken auf die Absendeadresse können Sie sowohl die MAIL FROM- als auch die Header-From-Adresse anzeigen lassen (sofern diese unterschiedlich sind).
- Durch Klicken auf die Empfängeradresse können Sie sämtliche Empfänger anzeigen lassen.
- Durch Klicken auf den Namen des TLS-Serverzertifikats können Sie Details zur Verbindungsverschlüsselung einsehen:



Für bestimmte E-Mails kann eine Aktion des Administrators erforderlich sein. Klicken Sie in diesem Fall **Aktion erforderlich**, um weitere Informationen und Optionen anzuzeigen:

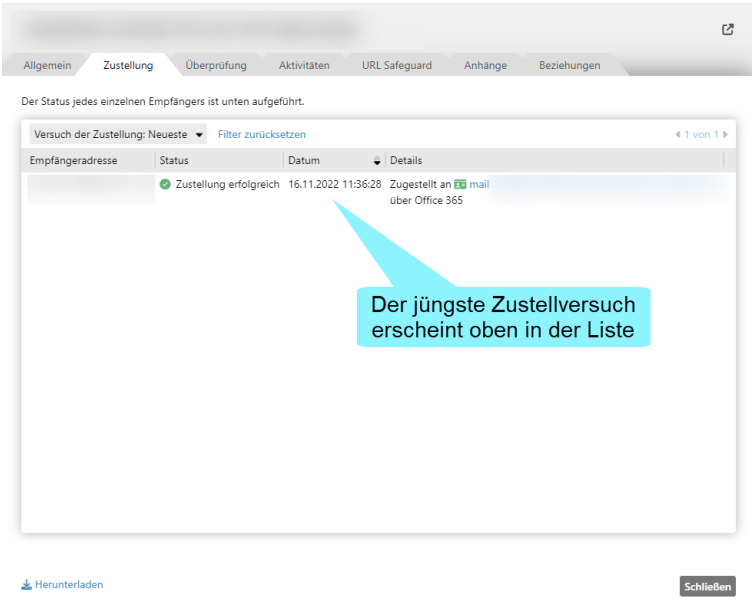
Angehaltene E-Mails| Die E-Mail wurde für mindestens einen Empfänger angehalten. Siehe **Angehaltene E-Mails**.

Gesperrte Anhänge| Mindestens ein Anhang erfordert eine Freigabe durch den Administrator. Siehe **Gesperrte Anhänge**.

> **TIP:** Informationen zu den einzelnen Status-Typen finden Sie unter **Status-Typen**.

Registerkarte Zustellung

Hier finden Sie Informationen zu den einzelnen Zustellversuchen.

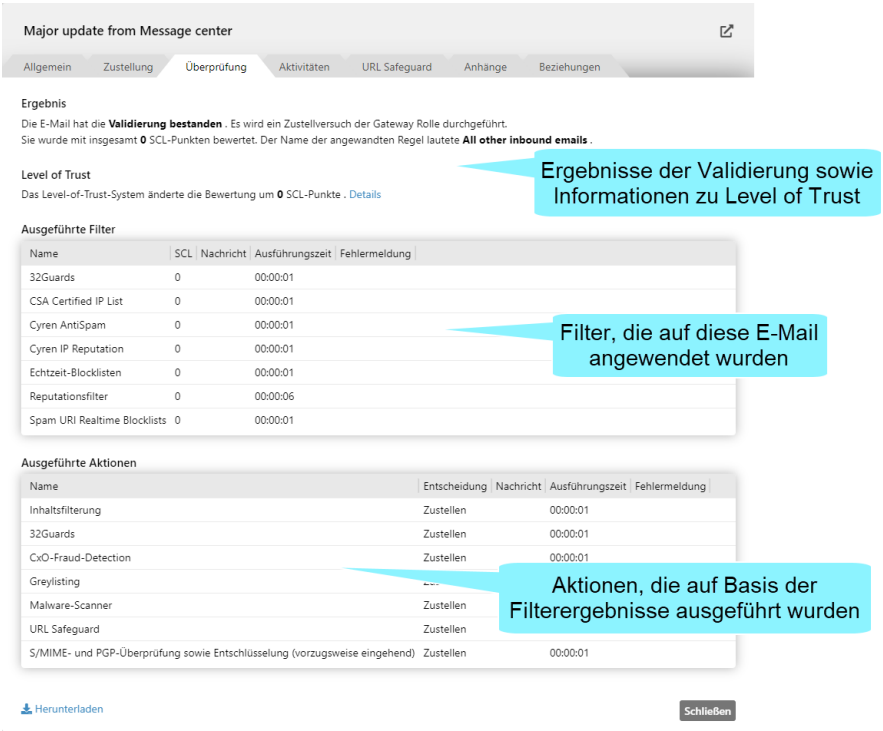


- Sollten initial nicht alle Zustellversuche für die einzelnen Empfänger angezeigt werden, klicken Sie **Alle anzeigen**, um sämtliche Zustellversuche anzuzeigen.

Registerkarte Überprüfung

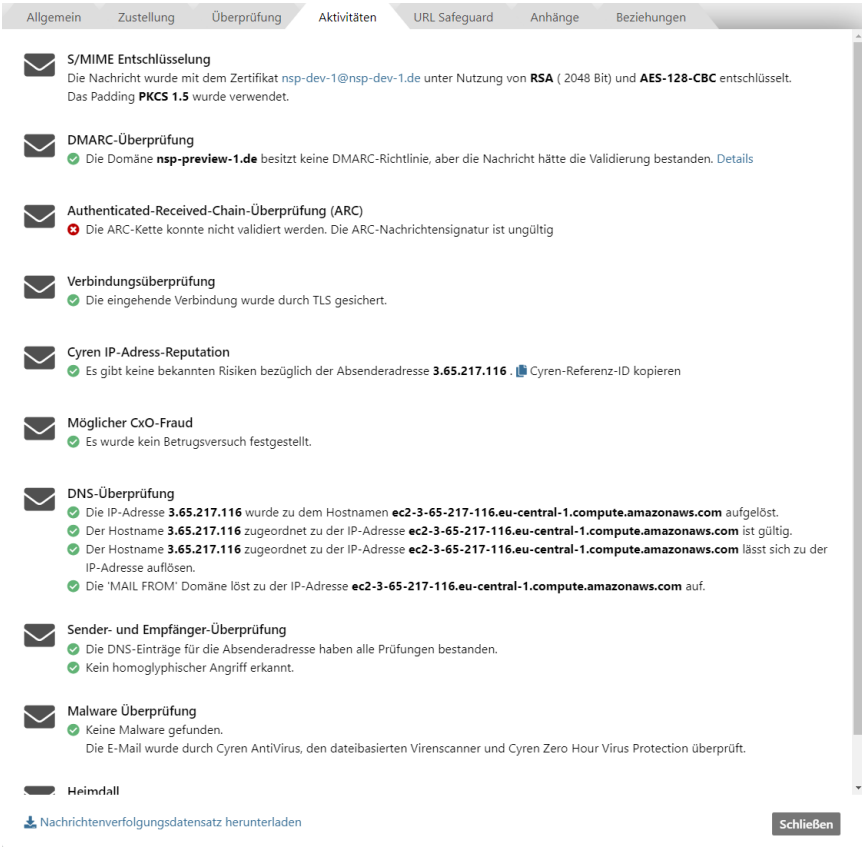
Hier finden Sie Informationen zur Validierung sowie zu angewandten Filtern und ausgeführten Aktionen.

> **HINWEIS:** Einträge in den Listen **Ausgeführte Filter** und **Ausgeführte Aktionen** sind nach **Fehlermeldung (absteigend) > SCL (absteigend) > Name (aufsteigend)** sortiert.

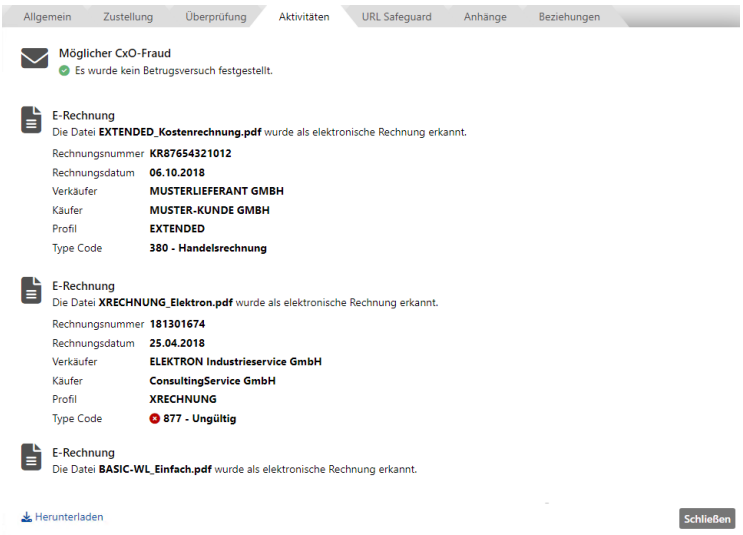


Registerkarte Aktivitäten

Hier finden Sie Informationen darüber, wie die E-Mail auf dem Server verarbeitet wurde. Dies sind beispielsweise Details zur angewandten Verschlüsselung, zur Reputationsprüfung sowie zum Einsatz von Content Disarm and Reconstruction, ARC oder PDF Mail. Außerdem enthält diese Registerkarte Angaben zu den Konsequenzen, die sich aus den Ergebnissen bestimmter Prüfungen ergeben haben.

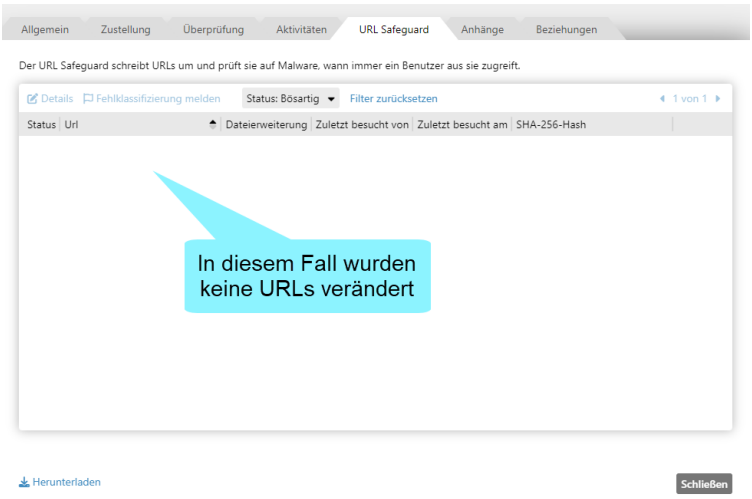


Zudem bietet sie Informationen zu empfangenen oder versendeten E-Rechnungen.



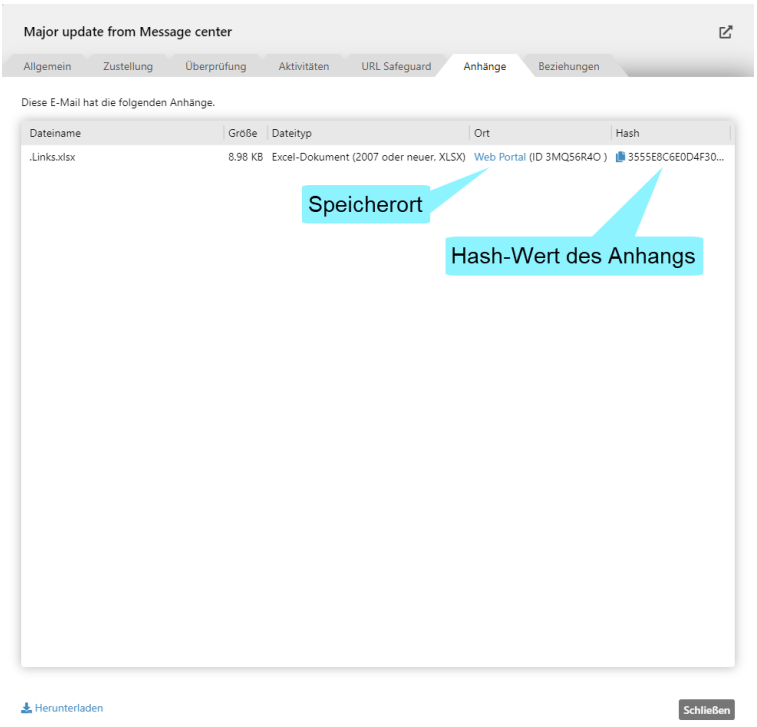
Registerkarte URL Safeguard

Hier finden Sie Informationen zu in der E-Mail oder in den Anhängen enthaltene URLs, die vom URL Safeguard umgeschrieben oder blockiert wurden.



Registerkarte Anhänge

Hier finden Sie Informationen zu in der E-Mail enthaltenen Anhängen.



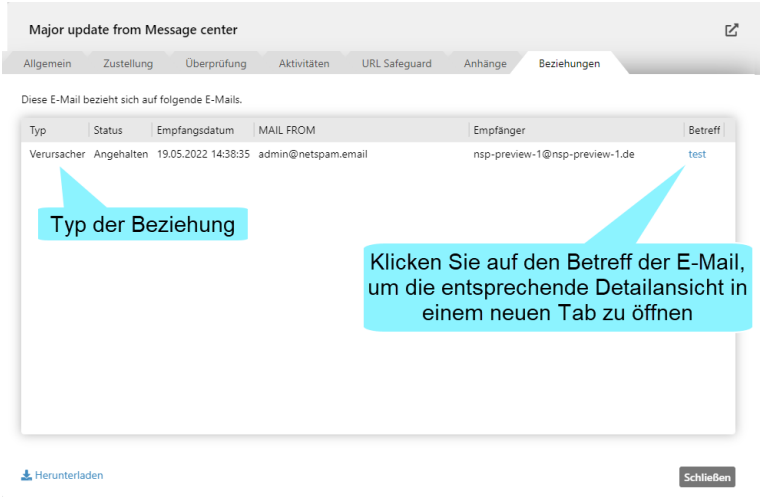
Der Status von Anhängen, die auf dem Webportal gespeichert wurden, wird durch folgende Icons angezeigt:

- |Die Freigabe dieses Anhangs wurde angefordert.
- |Der Malware-Scan für diesen Anhang ist fehlgeschlagen.
- |Für diesen Anhang ist eine automatische Freigabe eingerichtet.
- |Dieser Anhang wurde bereits gelöscht.
- |Dieser Anhang ist gesperrt.

Weitere Informationen zu gesperrten Anhängen finden Sie unter **Gesperrte Anhänge**.

Registerkarte Beziehungen

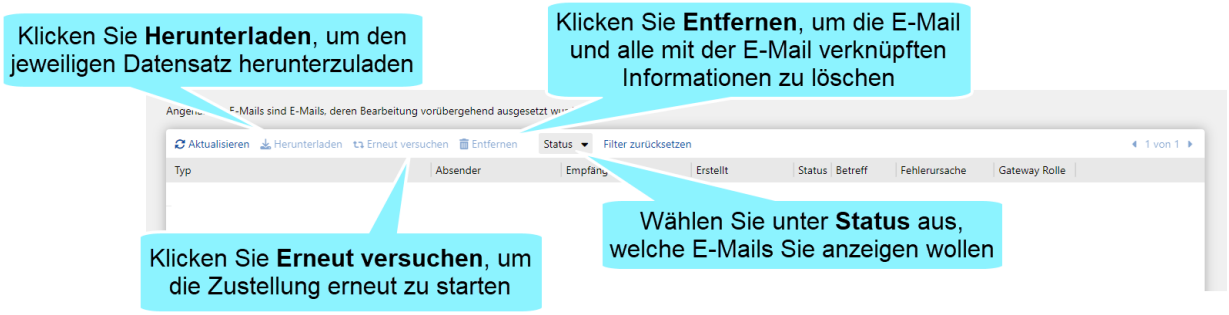
Hier finden Sie Verknüpfungen mit anderen Datensätzen der Nachrichtenverfolgung, die mit diesem Datensatz in Beziehung stehen.



Angehaltene E-Mails

Unter **Monitoring > Angehaltene E-Mails** finden Sie eine Übersicht aller E-Mails, deren Verarbeitung vorübergehend ausgesetzt wurde und die aktuell für mindestens einen Empfänger angehalten sind.

HINWEIS: Standardmäßig werden nur die E-Mails angezeigt, bei denen Ihre Aufmerksamkeit erforderlich ist. Unter **Status** können Sie festlegen, ob Sie stattdessen alle E-Mails anzeigen wollen.



Wann werden E-Mails angehalten?

- Ein erforderlicher kryptographischer Schlüssel liegt aktuell nicht vor.
- Der Inhaltsfilter wird momentan auf diese E-Mail angewendet.
- Eine qualifizierte Signatur konnte nicht aufgebracht oder verifiziert werden.
- Es war nicht möglich, die E-Mail als De-Mail zu senden.
- Die Inhaltsfilterung konnte nicht angewendet werden.

> **HINWEIS:** Die hier angezeigten E-Mails sind **aktuell** angehaltene E-Mails. Um eine Übersicht aller Datensätze anzuzeigen, die in der **Vergangenheit** den Status **Angehalten** hatten, wählen Sie in der Nachrichtenverfolgung die Bedingung **Angehalten** oder **Status = Angehalten** aus.

Gesperrte Anhänge

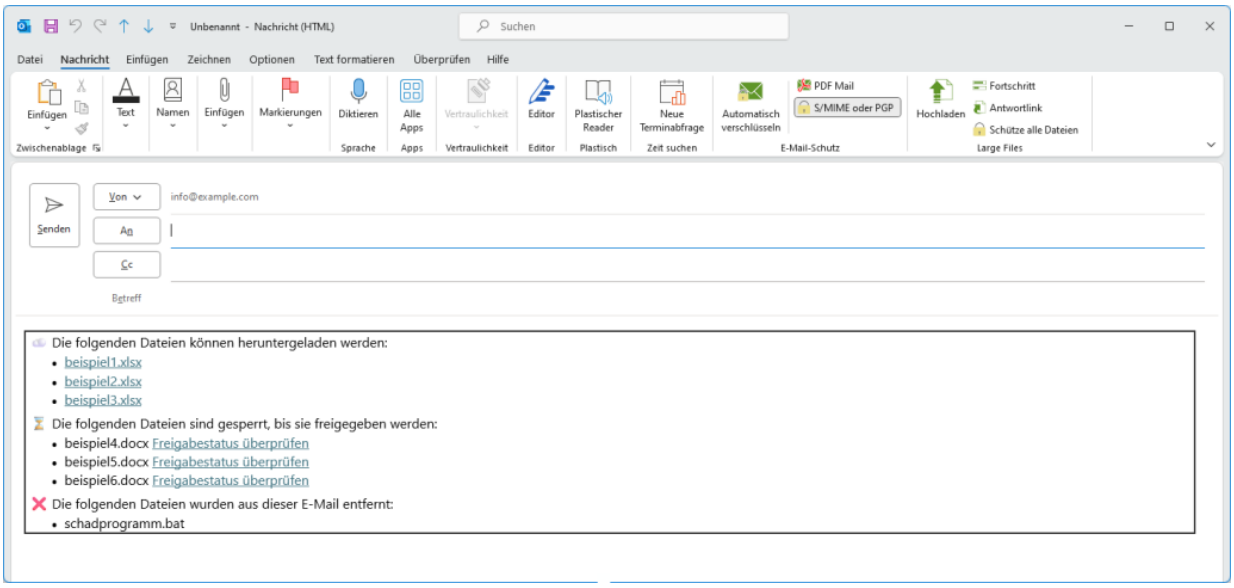
Anhänge, die gesperrt wurden, werden auf dem Web Portal gespeichert. Auf der Registerkarte **Anhänge** in der Detailansicht der jeweiligen E-Mail haben Sie folgenden Optionen:

- Klicken Sie **Anhänge freigeben**, um die jeweiligen Anhänge zu freizugeben.
- Klicken Sie **Anhänge verwerfen**, um die jeweiligen Anhänge zu löschen.

> **TIP:** Um eine Übersicht zu allen E-Mails zu erhalten, die Dateien enthalten, die eine manuelle Freigabe erfordern, fügen Sie in der Nachrichtenverfolgung die Bedingung **Anhang erfordert Freigabe** hinzu.

E-Mail-Hinweise

Links zu Webportal-Dateien werden als Hinweise in den jeweiligen E-Mails hinzugefügt.



Status-Typen

Im Folgenden werden die einzelnen Status-Typen an Hand von Beispielen erklärt.

> **HINWEIS:** Diese Informationen dienen einem grundsätzlichen Verständnis und decken nicht zwingend jeden Fall ab.

- **Erfolgreich|** Die E-Mail konnte erfolgreich an den Empfänger übermittelt werden.
- **Zustellung fehlgeschlagen|** Eine ausgehende E-Mail wurde von dem Empfangssystem abgelehnt. Im Reiter „Zustellung“ können Sie die Rückmeldung des Empfangssystem nachvollziehen.

- **Temporär abgewiesen|** Der einliefernde E-Mail-Server bekommt eine Rückmeldung und wird nach dem konfigurierten Intervall einen weiteren Zustellversuch durchführen.
    - **Greylisting|** Eine eingehende E-Mail hat mindestens 2 SCL-Punkte wegen Verstoß gegen unsere Filter erhalten.
    - **Empfänger entspricht nicht der Regel des ersten Empfängers|** Eine ausgehende E-Mail wird an unterschiedliche Empfänger versendet und nicht für jeden Empfänger liegt ein Zertifikat zum Verschlüsseln vor.
    - **32Guards|** Ein kürzlich neu gesichteter Host wird für einen kurzen Zeitraum temporär abgewiesen, um dessen Reputation zu ermitteln.
    - **Dienst nicht erreichbar|** Der Integrated Malware Scanner ist als einzig ausgewählter Malware-Scanner in der Regel konfiguriert, aber nicht erreichbar.
- **Permanent abgewiesen|** Die E-Mail wurde aufgrund von Verstoß gegen unsere Filter mit mindestens 4 SCL-Punkten bewertet oder durch Aktionen in NoSpamProxy abgewiesen.
- **Zustellung ausstehend|** Die E-Mail befindet sich noch in Zustellung und wird je nach Resultat in Kürze mit einem entsprechenden anderen Status vermerkt. Details finden Sie auf der Registerkarte **Zustellung**.
- **Mehrere Zustellzustände|** Eine E-Mail wurde an mehrere Empfänger versendet und mit unterschiedlichen Ergebnissen vermerkt. Details finden Sie im jeweiligen Eintrag auf der Registerkarte **Zustellung**.
- **Angenommen aber nicht zugestellt|** Die E-Mail wird empfangen, kann aber nicht verarbeitet werden.

- **Ausgehende Inhaltsfilterung|** Der hinterlegte Inhaltsfilter verbietet den Anhang der E-Mail.
- **Verschlüsselung|** Es wird eine Regel mit zwingender Verschlüsselung genutzt; dies war für den Empfänger nicht möglich
- **Der Absender hat eine Verbindung aufgebaut, aber keinen Email Body übermittelt|** In diesem Fall sieht NoSpamProxy nur noch den Email Envelope mit Absender und Empfänger, kann die E-Mail aber nicht verarbeiten. Oftmals wird solch eine Verbindung erzeugt, um eine E-Mail-Adresse einer zuvor ausgehenden E-Mail zu validieren und soll als Anti-Spam-Maßnahme dienen. Das Verfahren ist bekannt als **Callback verification**.
- **De-Mail|** Es wird versucht, eine E-Mail, für die in NoSpamProxy keine Konfiguration vorliegt, an einen De-Mail-Empfänger zuzustellen.

- **Doppelt|** Eine E-Mail wurde doppelt an NoSpamProxy zugestellt. Die Schleife (Email Loop) wird verhindert und die E-Mail wird nicht zugestellt.
  - Eine eingehende E-Mail wird von NoSpamProxy an den hinterlegten E-Mail-Server zugestellt. Diese E-Mail landet jedoch nicht im Postfach des Empfängers, sondern der E-Mail-Server sendet wenige Sekunden nach Empfang der E-Mail diese erneut an NoSpamProxy zurück.
  - Eine eingehende E-Mail wurde doppelt mit der gleichen Nachrichten-ID vom selben oder von unterschiedlichen einliefernden Systemen versendet. Jede E-Mail muss eine eindeutige Mail ID haben.
- **Angehalten|** Es sind weitere Aktionen notwendig, damit die E-Mail erfolgreich zugestellt wird.

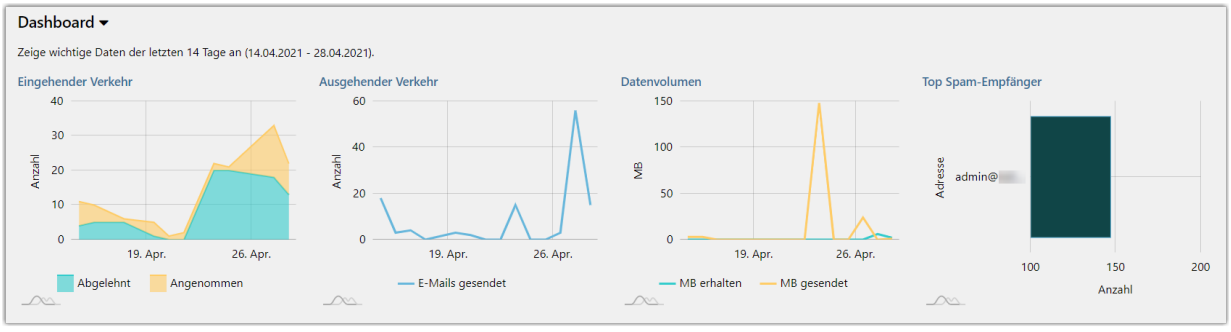
- **Inhaltsfilter|** Die E-Mail wird zur Verarbeitung der angehängten Dateien angehalten und anschließend mit einem zweiten Message Track als erfolgreiche E-Mail zugestellt. Die durchgeführte Aktion lässt sich im Message Track auf der Registerkarte **Aktivitäten** nachvollziehen. Den Nachfolger der angehaltenen E-Mail können Sie im Message Track auf der Registerkarte **Beziehungen** nachvollziehen.
- **PDF-Mail|** Die ausgehende E-Mail wird in ein PDF-Dokument konvertiert und verschlüsselt, da kein S/MIME-Zertifikat für den Empfänger vorliegt. Der Empfänger muss ein Passwort auf dem Webportal vergeben; solange verbleibt die E-Mail in diesem Status. Nach 5 Tagen fehlender Reaktion des Empfängers folgt ein NDR an den Absender.
- **Dienst nicht erreichbar|** Der Integrated Malware Scanner kann Dateien, die zum Webportal hochgeladen werden sollen, nicht erreichen.

Reporting

Mit den Reports in NoSpamProxy haben Sie eine Übersicht des eingehenden und ausgehenden E-Mail-Verkehrs sowie der Top-Spam-Empfänger.

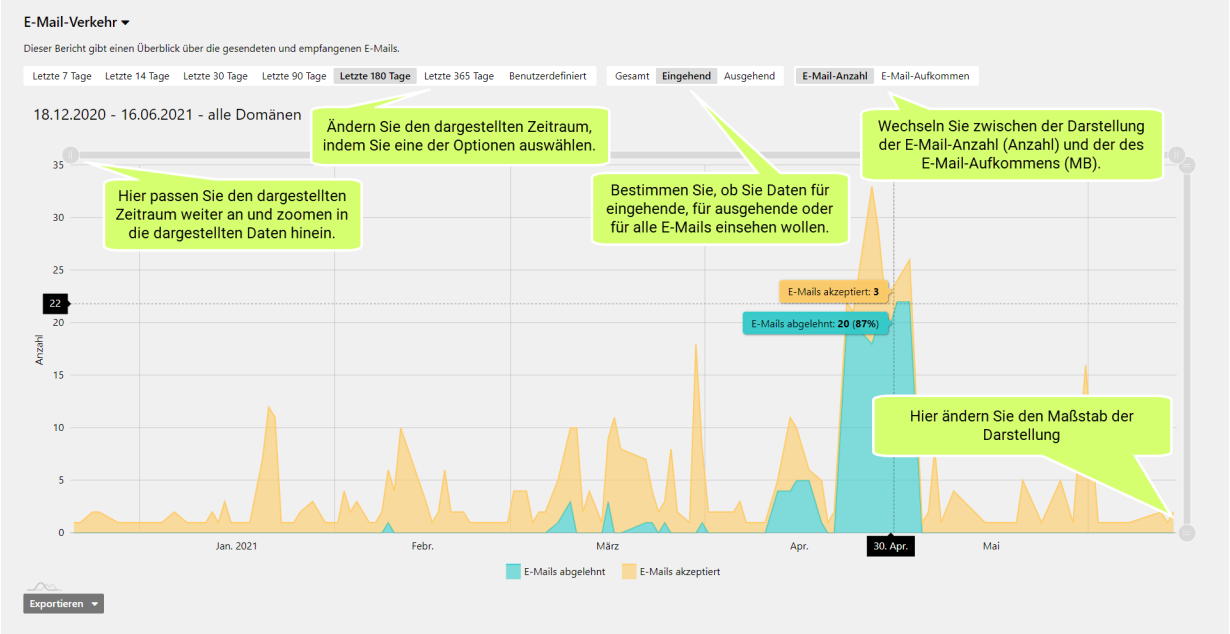
> **TIP:** Sie können in allen Ansichten mit der Maus über einem Datum hovern, um genaue Angaben anzuzeigen.

Dashboard



Das Dashboard zeigt Ihnen vier Schnellübersichten zu

E-Mail-Verkehr



Die Detailansichten zum E-Mail-Verkehr bieten Ihnen detaillierte Übersichten zum gewählten Zeitraum und zur gewählten Richtung des E-Mail-Flusses. Passen Sie die einzelnen Charts an Ihre Bedürfnisse an, indem Sie beispielsweise den dargestellten Zeitraum ändern oder ausschließlich Daten für eingehende E-Mails anzeigen.

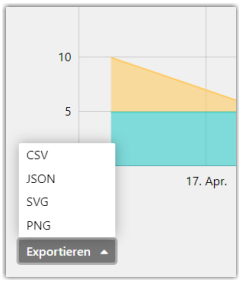
Top-Spam-Empfänger

Diese Ansicht zeigt Ihnen die Empfänger, die im gewählten Zeitraum den meisten Spam erhalten haben.

Charts exportieren

Sie können alle Charts als Dateien in den Formaten CSV, JSON, SVG oder PNG exportieren.

1. Öffnen Sie im gewünschten Chart das Drop-Down-Menü in der linken unteren Ecke.
2. Wählen Sie das Format, in das Sie den Chart exportieren wollen.

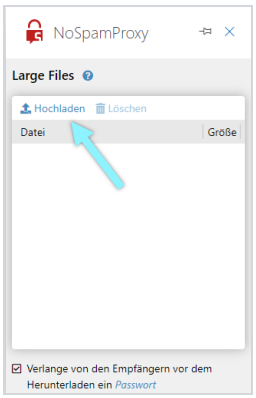


Large Files

1. Stellen Sie sicher, dass Sie mit Ihren Microsoft-365-Anmeldedaten bei Outlook im Web (ehemals Outlook Web App oder Outlook Web Access) angemeldet sind.
2. Klicken Sie **Neue E-Mail**.
3. Klicken Sie **NoSpamProxy** in der Befehlsleiste..

> **HINWEIS:** Falls der Eintrag für **NoSpamProxy** nicht vorhanden ist, kontaktieren Sie Ihre IT-Abteilung.

4. Klicken Sie **Hochladen** und wählen Sie die Dateien aus, die Sie versenden wollen.



5. (Optional) Setzen Sie das Häkchen bei **Verlange von den Empfängern vor dem Herunterladen ein Passwort**.

> **HINWEIS:** Die Empfänger erstellen das jeweilige Passwort beim ersten Herunterladen einer geschützten Datei. Bei jedem weiteren Aufruf des Download-Links ist die Eingabe dieses Passworts erforderlich.

6. Klicken Sie **Senden**, um die E-Mail abzuschicken.

HINWEIS:

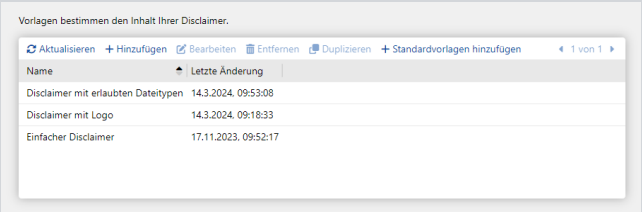
- Large-Files-Dateien werden für 30 Tage in NoSpamProxy Cloud aufbewahrt. Sollten Sie die Dateien über diesen Zeitraum hinaus benötigen, müssen Sie sie herunterladen.
- NoSpamProxy verarbeitet E-Mails, deren Größe 500 MB nicht überschreitet.

Vorlagen erstellen

Vorlagen bestimmen den Inhalt Ihrer Disclaimer.

Eine Vorlage hinzufügen

1. Gehen Sie zu **Disclaimer > Disclaimer-Vorlagen**.
2. Klicken Sie **Hinzufügen**, um eine neue Vorlage hinzuzufügen.



3. Geben Sie unter **Allgemein** einen Namen für die neue Vorlage ein und klicken Sie **Weiter**.
4. Fügen Sie HTML-Inhalt hinzu und klicken Sie Weiter.

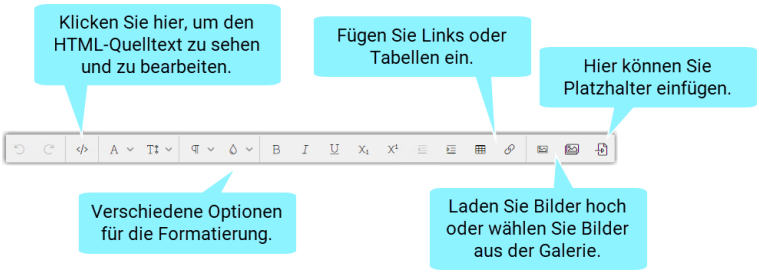
5. Fügen Sie Nur-Text-Inhalt hinzu.
6. Klicken Sie **Beenden**.

In der HTML-Ansicht können Sie die Werkzeugleiste sowie die weiteren Schaltflächen nutzen, um dem Disclaimer Elemente wie Platzhalter oder Grafiken hinzuzufügen. Sie können auch freien Text - wie zum Beispiel eine Grußformel - hinzufügen.

> **HINWEIS:** Die Nur-Text-Ansicht verwenden E-Mail-Clients, wenn die HTML-Anzeige deaktiviert ist. Hier können Sie ausschließlich Platzhalter und freien Text einfügen.

Optionen in der Werkzeugleiste (HTML-Ansicht)

Die Funktionsweise der Werkzeugleiste orientiert sich an vergleichbaren Werkzeugleisten in Office-Produkten.



> **TIP:** Bevor Sie Platzhalter einfügen können, müssen Sie zusätzliche Benutzerfelder erstellen. Siehe Zusätzliche Benutzerfelder hinzufügen, **Schritt 1: Platzhalter für die Verwendung in Disclaimer-Vorlagen vorbereiten**.

Verfügbare Platzhalter

Platzhalter werden durch die in Ihrem Azure Active Directory zugeordneten Werte des jeweiligen Benutzerprofilattributs ersetzt.

Die folgenden Platzhalter sind verfügbar:

Platzhalter	Benutzerprofilattribut im Azure Active Directory
Abteilung	Department
Bundesland	State
E-Mail	Mail
Faxnummer	FaxNumber
Firma	CompanyName
Land	Country
Mobiltelefon	MobilePhone
Nachname	Surname

Platzhalter	Benutzerprofilattribut im Azure Active Directory
Postleitzahl	PostalCode
Stadt	City
Straße	StreetAddress
Telefon	BusinessPhones
Titel	JobTitle
Vorname	GivenName

Standardvorlagen hinzufügen

Standardvorlagen enthalten bereits eine Auswahl häufig benutzter Platzhalter, können aber ebenso wie neu angelegte Vorlagen frei editiert werden.

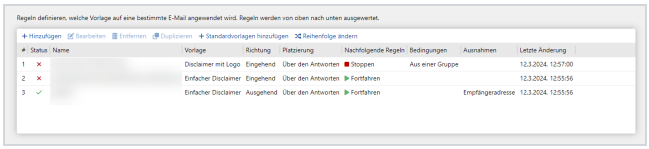
- Klicken Sie **Standardvorlagen hinzufügen**, um diese hinzuzufügen.

Regeln hinzufügen

Regeln bestimmen, wann und wie Disclaimer in Ihre E-Mails eingefügt werden.

1. Gehen Sie zu **Disclaimer > Disclaimer-Regeln**, um die Übersichtsseite der Regeln zu öffnen.

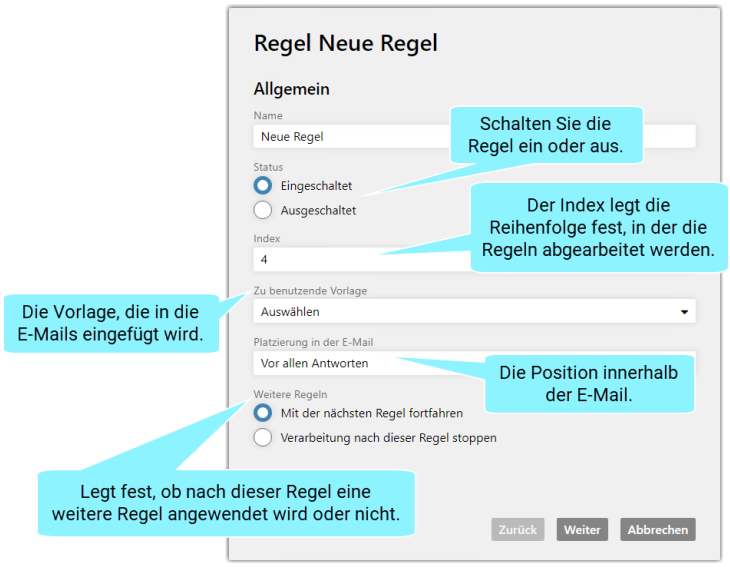
2. Klicken Sie **Hinzufügen**, um eine neue Regeln hinzuzufügen.



3. Konfigurieren Sie die gewünschten Optionen (siehe unten).
4. Klicken Sie **Beenden**, um die vorgenommenen Änderungen zu speichern und zur Übersicht der Regeln zurückzukehren.

Allgemein

Hier nehmen Sie grundlegende Einstellungen für die neue Regel vor.



> **TIP:** Mit einem E-Mail-Disclaimer für eingehende E-Mails können Sie beispielsweise alle E-Mails markieren, die aus dem Internet stammen.

Bedingungen

Eine Regel wird angewendet, wenn **alle** Bedingungen erfüllt sind.

Mit bestimmten Worten (mehrere Optionen)| Die Bedingung ist erfüllt, wenn eines oder mehrere der definierten Worte vorhanden sind.

In einer bestimmten Zeitspanne| Die Bedingung ist in der angegebenen Zeitspanne erfüllt.

Ausnahmen

Eine Regel wird angewendet, wenn **keine** der Ausnahmen zutrifft.

Mit bestimmten Worten (mehrere Optionen)| Die Ausnahme trifft zu, wenn eines oder mehrere der definierten Worte vorhanden sind.

In einer bestimmten Zeitspanne| Die Ausnahme ist in der angegebenen Zeitspanne erfüllt.

Reihenfolge der Regeln ändern

Um die Reihenfolge (den Index) der Regeln zu ändern, gehen Sie folgendermaßen vor:

1. Wählen Sie die Regel aus, deren Index Sie verändern wollen.
2. Klicken Sie **Reihenfolge ändern**.
3. Bewegen Sie die Regel, indem Sie entweder **Nach oben** oder **Nach unten** klicken.
4. Klicken Sie **Speichern**.

Lizenzverwaltung

Übersicht über erworbene und aktive Lizenzen

Gehen Sie zu **Administration > Lizenzierung**, um Details zu den erworbenen und aktiven Lizenzen einzusehen.

Häufig gestellte Fragen

Was ist eine Identität?

Eine Identität ist ein Objekt, das eine oder mehrere E-Mail-Adressen – dies umschließt auch Alias-Adressen – mit einer Unternehmensdomäne beinhaltet und in NoSpamProxy Cloud bekannt ist. Darüber hinaus können persönliche Informationen in diesem Objekt vorhanden sein, also beispielsweise Vor- oder Nachname oder Anschrift. Beispiele für Identitäten sind Postfächer, freigegebene Postfächer (Shared Mailboxes), Kalender, Office-365-Gruppen oder öffentliche Ordner.

Was ist eine Unternehmensdomäne?

Eine Unternehmensdomäne ist eine Domäne, die für das eigene Unternehmen registriert ist.

Was ist eine Domäne?

Eine Domäne ist bei einer E-Mail-Adresse der Teil nach dem @-Zeichen.

Wie kann ich Identitäten hinzufügen?

Identitäten können manuell in NoSpamProxy Cloud erstellt oder über einen Azure-Active-Directory-Import hinzugefügt werden.

Was ist eine aktive Identität?

Aktiv bedeutet, dass die jeweilige Identität E-Mails über NoSpamProxy Cloud empfängt oder versendet.

Was ist eine Teams-Adresse?

Eine Teams-Adresse ist ein Postfach, das auf einen Teams-Kanal weiterleitet. Die Besonderheit hierbei ist, dass eine Teams-Adresse auf die Domäne **@<location>.teams.ms** endet. <location> wird hier durch die Office-365-Mandanten-Region des jeweiligen Kunden ersetzt.

Wann muss ich Teams-Adressen lizenzieren?

Da im Normalfall eine Teams-Adresse auf der Domäne **@<location>.teams.ms** endet, muss diese Adresse nicht lizenziert werden. Die E-Mails werden dadurch nämlich nicht über NoSpamProxy Cloud empfangen oder verarbeitet.

Über Umwege ist es jedoch möglich, eine Unternehmensdomäne zu benutzen. Diese Umwege führen dazu, dass ein neues Postfach erstellt wird und die E-Mails über NoSpamProxy Cloud empfangen werden. In diesem Fall liegt eine aktive Identität vor.

Wie wird gezählt und lizenziert?

- Alle aktiven Identitäten werden gezählt und müssen lizenziert werden.
- Lizenzen für NoSpamProxy Cloud Encryption werden gezählt, sobald eine Identität eine ausgehende E-Mail versendet hat, die verschlüsselt und/oder signiert wurde.
- Alle Werte werden über einen Zeitraum von 90 Tagen gemessen. Eine Ausnahme ist der Wert für die 32Guards Sandbox. Hier wird lediglich ein Zeitraum von 30 Tagen betrachtet.
- Alle Werte werden auf Benutzer aggregiert, sofern dies möglich ist. Wenn die Zuordnung auf Benutzer nicht möglich ist, wird jede E-Mail-Adresse einzeln gezählt. Hierbei werden auch die E-Mail-Adressen gezählt, die unter **E-Mail-Routing/E-Mail-Server des Unternehmens** hinterlegt sind. Dies ist auch dann der Fall, wenn E-Mails von extern unter Benutzung der Unternehmensdomäne gesendet werden.

- Plusadressen (auch Unteradressen genannt) werden im Rahmen der Lizenzierung **nicht** gezählt, sofern die Plusadressierung für die jeweilige Domäne aktiviert ist. Dies gilt sowohl für die Lizenzierung der Module als auch für die Lizenzierung von Diensten. Es werden nur die zu Grunde liegenden E-Mail-Adressen der Benutzer gezählt, für die Plusadressen vorliegen. Zusätzliche Informationen zur Plusadressierung finden Sie in der **Microsoft-Dokumentation**.
- Adressen, die nach dem Sender Rewriting Scheme (SRS) umgeschrieben wurden, werden **nicht** gezählt, weder für die Lizenzierung der Module noch für die Lizenzierung von Diensten. Zusätzliche Informationen zum SRS finden Sie in der **Microsoft-Dokumentation**.

Wie schränke ich die Encryption-Funktion ein (bei abweichender Lizenzierung)?

Sie können die Encryption-Funktion einschränken – beispielsweise, um bei Abweichungen zwischen Encryption- und Protection-Lizenz eine Überschreitung der Encryption-Lizenz zu vermeiden. Gehen Sie dazu folgendermaßen vor:

1. Legen Sie in Entra ID eine Gruppe an, deren Mitglieder unverschlüsselt versenden sollen.

2. Fügen Sie diese Gruppe nach der nächsten Synchronisation unter **Identitäten > Automatischer Benutzerimport** hinzu.

   > **HINWEIS:** Für die Gruppe selbst sind keine besonderen Einstellungen erforderlich.

3. Gehen Sie zu **Konfiguration > Regeln** und fügen Sie die ausgehende Regel **Plain text email / Klartext-E-Mail** hinzu.
4. Hinterlegen Sie in dieser Regel die zuvor angelegte Gruppe als Absender.

E-Mails der Mitglieder dieser Gruppe werden nun weder verschlüsselt noch signiert. Die dieser Regel nachfolgende Standardregel - die für alle übrigen Benutzer außerhalb dieser Gruppe gilt - verschlüsselt und signiert E-Mails weiterhin automatisch (sofern dies möglich ist).

> **HINWEIS:** Falls Sie kein Entra ID nutzen, müssen Sie die Benutzer manuell in der Regel hinterlegen.

Support

Für Supportanfragen wenden Sie sich bitte an Ihren Reseller. Informationen zu den von unserem Support benötigten Informationen finden Sie unter **Wie melde ich ein Problem?**

Alternativ stehen Ihnen die folgenden Möglichkeiten der Unterstützung zur Verfügung:

NoSpamProxy-Dokumentation

Die Dokumentation finden Sie unter **docs.nospamproxy.com**.

NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

YouTube

In unserem **YouTube-Kanal** finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

Blog

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite des NoSpamProxy Command Center angezeigt.