



Version 15

## Integration von NoSpamProxy

- in Office 365
- in Microsoft Azure
- als On-Premises-Lösung

## 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 © 2023 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 11. DEZEMBER 2024 ÜBERARBEITET.**

# Inhalt

Einleitung .....	1
Microsoft 365 als Relayhost freigeben .....	2
Weiterleitung an Microsoft 365 einrichten .....	5
Microsoft 365 konfigurieren .....	9
Die Transportregel erstellen .....	12
Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online .....	14
Schritt 1: Anlegen eines eingehenden Connectors für die Domain * .....	14
Schritt 2: Anlegen einer Transportregel zur Abschaltung des Spamfilters .....	19
Notwendige Konfigurationen für den Betrieb in Microsoft Azure .....	22
<b>Hilfe und Unterstützung .....</b>	<b>27</b>

# Einleitung

Seit Version 10 ist NoSpamProxy® vollständig in Microsoft 365 integrierbar. Dieses Handbuch beschreibt die Konfigurationsschritte sowohl für NoSpamProxy und Microsoft 365 als auch für die eingesetzte Serverumgebung.

Die beschriebene Konfiguration gilt dabei ebenso für den Einsatz von NoSpamProxy als On-Premises-Lösung und in Microsoft Azure.



**HINWEIS:** Die spezifischen Konfigurationsschritte für den Einsatz in Microsoft Azure werden unter [Notwendige Konfigurationen für den Betrieb in Microsoft Azure](#) beschrieben.

# Microsoft 365 als Relayhost freigeben

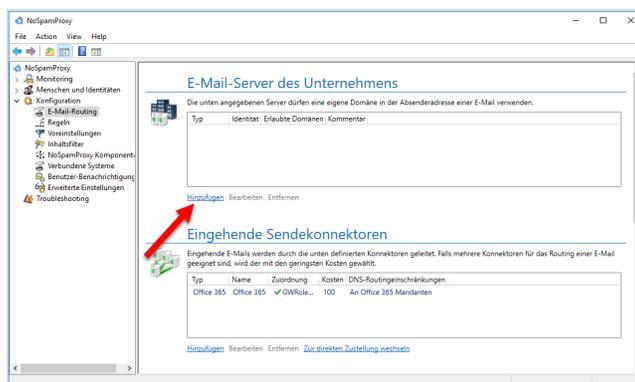
In diesem Schritt lassen Sie Microsoft 365 in der NoSpamProxy®-Konfiguration als Relayhost zu, damit E-Mails aus Microsoft 365 heraus durch NoSpamProxy an externe Kommunikationspartner verschickt werden können.

Ohne diese Konfiguration wird NoSpamProxy E-Mails als Relay-Missbrauchsversuch bewerten und abweisen.



**HINWEIS:** Stellen Sie sicher, dass Sie mindestens eine Unternehmensdomäne eingerichtet haben, bevor Sie mit der Konfiguration beginnen.

1. Wechseln Sie im NoSpamProxy Command Center zu **Konfiguration > E-Mail-Routing** und klicken Sie **Hinzufügen**.



2. Wählen Sie den Typ **Als Office 365 Mandant** und klicken Sie danach **Weiter**.

The screenshot shows a window titled 'E-Mail-Server des Unternehmens verwalten'. The main heading is 'E-Mail-Server des Unternehmens verwalten'. Under the heading 'Typ', there is a sub-heading 'Wählen Sie die Art wie sich der Server identifiziert.' followed by four radio button options: 'Mit einer IP-Adresse, einem Subnetz oder einem DNS-Hostnamen', 'Mit einem TLS-Client-Zertifikat', 'Als Office 365 Mandant' (which is selected and has a red arrow pointing to it), and 'Mit einer bestimmten Absenderadresse'. At the bottom of the window are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

3. Treffen Sie unter **Zugangspunkt** die für Ihre Organisationsumgebung passende Auswahl.
4. Geben Sie ihre Mandanten-ID ein. Achten Sie darauf, dass Sie den Namen der ID eingeben (nicht die ID in hexadezimaler Schreibweise).
5. Klicken Sie **Weiter**.

The screenshot shows the same window as the previous step, but now on the 'Office 365 Mandant' step. The sub-heading is 'Office 365 Mandant' with the text 'Office 365 Server, die die unten angegebene Mandanten-ID angeben, werden als E-Mail-Server des Unternehmens eingestuft.' Below this, there is a dropdown menu for 'Zugangspunkt' set to 'Standard Azure Cloud' and a text input field for 'Mandanten-ID' containing 'nspstest' followed by '.onmicrosoft.com'. At the bottom are the same three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

6. Wählen Sie unter **Zugeordnete Unternehmensdomänen** die Domänen aus, die Sie in Microsoft 365 hinterlegt haben und die in der Absenderadresse für ausgehende E-Mails vorkommen werden.



**HINWEIS:** Wenn Sie hier nicht alle Domänen vorfinden, müssen Sie die fehlenden Domänen unter **Identitäten > Unternehmensdomänen > Unternehmensdomänen** hinzufügen. Dies ist auch zu einem späteren Zeitpunkt möglich.

7. Klicken Sie **Weiter**.
8. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie dann **Fertigstellen**.

Der E-Mail-Server ist nun angelegt.

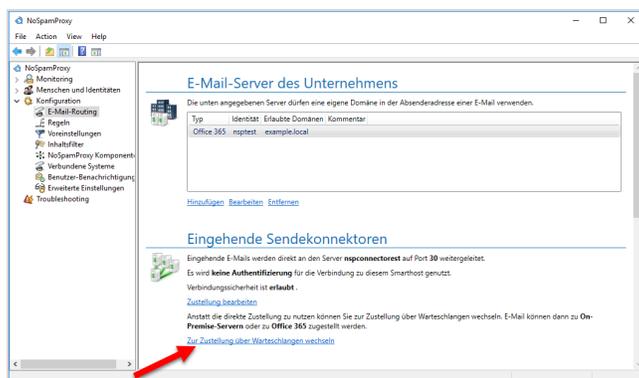
# Weiterleitung an Microsoft 365 einrichten



**HINWEIS:** Für die Einrichtung der Weiterleitung an Microsoft 365 ist ein TLS-Zertifikat erforderlich, das von einer von Microsoft vertrauten Stammzertifizierungsstelle ausgestellt wurde. Eine aktuelle Liste der vertrauten Stellen finden Sie unter <https://docs.microsoft.com/en-us/security/trusted-root/participants-list>.

In diesem Schritt konfigurieren Sie NoSpamProxy® so, dass alle eingehenden E-Mails an Microsoft 365 weitergeleitet werden. Dazu müssen Sie die entsprechenden Sendekonnektoren bearbeiten.

1. Wechseln Sie zu **Konfiguration > E-Mail-Routing**.
2. Klicken Sie unter **Eingehende Sendekonnektoren** auf **Zur Zustellung über Warteschlangen wechseln**.

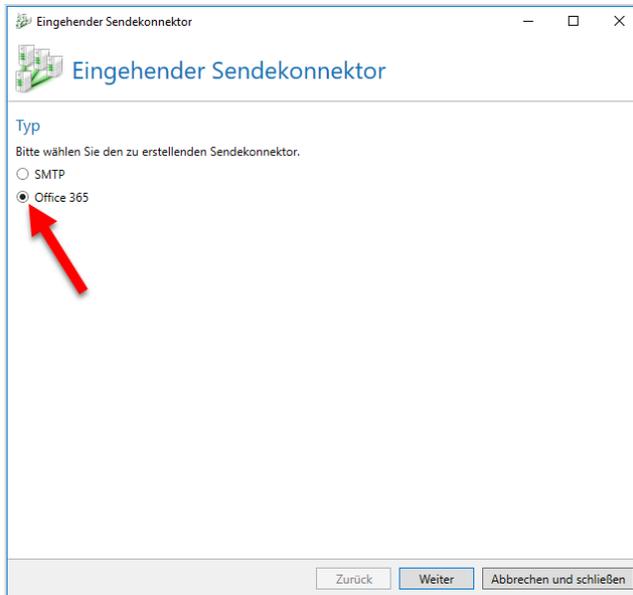


3. Wählen Sie im Dialog **Zustellung ändern** die Option **Zustellung ersetzen**.



**HINWEIS:** Ab Version 13 entfällt dieser Schritt, da die direkte Zustellung ab dieser Version nicht mehr unterstützt wird.

4. Wählen Sie im dann folgenden Dialog **Office 365** und klicken Sie **Weiter**.



5. Geben Sie einen beliebigen Namen für den eingehenden Sendekonnektor ein und wählen Sie danach die Gatewayrolle(n) aus, die E-Mails an Office 365 verarbeiten sollen.

## 6. Klicken Sie **Weiter**.

The screenshot shows the 'Eingehender Sendekonnektor' configuration window. The title bar reads 'Eingehender Sendekonnektor'. Below the title bar, there is a header with a server icon and the text 'Eingehender Sendekonnektor'. The main content area is titled 'Allgemeine Einstellungen'. It contains a 'Name' field with the value 'Office365'. Below this, there is a checkbox labeled 'Zugeordnete Gateway Rollen' which is checked. A note states: 'Wenn E-Mails identische Ziele besitzen werden die Kosten für die Auslieferung unten definiert. Der Konnektor mit den geringsten Kosten wird für den Versand gewählt.' Below the note, there is a field 'Die Kosten betragen 100' with a slider control. At the bottom of the window, there are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

## 7. Klicken Sie **Zertifikat auswählen**, um ein Zertifikat für die Client-Identität anzugeben, mit dem sich NoSpamProxy beim Office-365-Server authentifizieren kann.

The screenshot shows the 'Eingehender Sendekonnektor' configuration window, now on the 'Client-Identität' tab. The title bar reads 'Eingehender Sendekonnektor'. Below the title bar, there is a header with a server icon and the text 'Eingehender Sendekonnektor'. The main content area is titled 'Client-Identität'. It contains the text: 'Dieses Zertifikat wird genutzt um die Client-Identität sicher zu stellen.' Below this, there is a section titled 'Client-Identität' with the text: 'Kein Zertifikat ausgewählt.' and 'Falls sich Ihr Zertifikat auf einer Smartcard befindet, benötigen Sie im Allgemeinen eine PIN, um darauf zuzugreifen.' Below this, there is a 'Zertifikats-PIN' field with a toggle icon. At the bottom of the main content area, there are two buttons: 'Zertifikat auswählen' and 'Zertifikat entfernen'. A red arrow points to the 'Zertifikat auswählen' button. At the bottom of the window, there are three buttons: 'Zurück', 'Fertigstellen', and 'Abbrechen und schließen'.

8. Wählen Sie im dann folgenden Dialog das TLS-Zertifikat aus, das Sie zuvor bei einer von Microsoft vertrauten Stammzertifizierungsstelle beantragt haben und klicken Sie danach **Auswählen und schließen**.
9. Klicken Sie **Auswählen und schließen**.
10. Klicken Sie im folgenden Dialogfenster **Fertigstellen**.
11. Öffnen Sie unter **Empfangskonnektoren** den genutzten Empfangskonnektor und wechseln Sie zur Registerkarte **Verbindungssicherheit**.
12. Wählen Sie entweder das von NoSpamProxy mitgelieferte oder das zuvor beantragte Zertifikat aus.
13. Klicken Sie **Auswählen und schließen** und dann **Speichern und schließen**.

Die Konfiguration für NoSpamProxy ist nun abgeschlossen.

# Microsoft 365 konfigurieren

In diesem Schritt konfigurieren Sie den Office-365-Mandanten so, dass ausgehende E-Mails nicht direkt an den Empfängerserver, sondern zunächst an NoSpamProxy® zugestellt werden. Melden Sie sich dazu in an Ihrem Exchange Admin Center unter <https://admin.exchange.microsoft.com/> an.



**HINWEIS:** Verwenden Sie für die Anmeldung einen Benutzer, der über Administrationsrechte verfügt.

1. Wechseln Sie im Exchange Admin Center zu **E-Mail-Fluss > Connectors**; klicken Sie danach **Connector hinzufügen**.
2. Wählen Sie auf der ersten Seite unter **Verbindung von** die Option **Office 365** aus; wählen Sie unter **Verbindung mit** die Option **Partnerorganisation** aus.

**Connector hinzufügen**

- Neuer Connector
- Name
- Verwendung des Connectors
- Routing
- Sicherheitseinschränkungen
- Überprüfungs-E-Mail
- Connector überprüfen

### Neuer Connector

Geben Sie Ihr E-Mail-Flussszenario an. Wir teilen Ihnen dann mit, ob Sie einen Connector einrichten müssen.

**Verbindung von**

- Office 365
- E-Mail-Server Ihrer Organisation
- Partnerorganisation

**Verbindung mit**

- E-Mail-Server Ihrer Organisation
- Partnerorganisation

3. Klicken Sie **Weiter**.
4. Geben Sie auf der folgenden Seite einen beliebigen Namen für den Connector und bei Bedarf eine Beschreibung ein und klicken Sie **Weiter**.
5. Wählen Sie auf der dann folgenden Seite die Option **Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Konnektor**

umleitet und klicken Sie **Weiter**.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Verwendung des Connectors' step selected. The left sidebar lists steps: Neuer Connector, Name, Verwendung des Connectors (selected), Routing, Sicherheitseinschränkungen, Überprüfungs-E-Mail, and Connector überprüfen. The main content area is titled 'Verwendung des Connectors' and contains the text: 'Geben Sie an, wann Sie diesen Connector verwenden möchten.' Below this are two radio button options: 'Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Connector umleitet' (selected) and 'Nur, wenn E-Mails an diese Domänen gesendet werden'.

6. Wählen Sie die Option **E-Mail über die diese Smarthosts weiterleiten** geben Sie den Namen oder die IP-Adresse des Servers (Smarthost) an, auf dem die Gatewayrolle installiert ist und klicken Sie **Speichern**.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Routing' step selected. The left sidebar lists steps: Neuer Connector, Name, Verwendung des Connectors, Routing (selected), Sicherheitseinschränkungen, Überprüfungs-E-Mail, and Connector überprüfen. The main content area is titled 'Routing' and contains the text: 'Wie möchten Sie E-Mails weiterleiten?' Below this is a paragraph: 'Geben Sie einen oder mehrere Smarthosts an, an die Office 365 E-Mail-Nachrichten übermittelt. Ein Smarthost ist ein alternativer Server und kann mithilfe eines vollqualifizierten Domainnamens (FQDN) oder einer IP-Adresse identifiziert werden.' There are two radio button options: 'MX-Eintrag verwenden, der der Domäne des Partners zugeordnet ist' and 'E-Mail über die diese Smarthosts weiterleiten' (selected). Below the second option is a text input field with the example text 'Beispiel: myhost.contoso.com oder 192.168.3.2' and a blue '+' button.



**HINWEIS:** Beachten Sie beim Eintragen des Hostnamens, dass Microsoft 365 bei der Auflösung die MX-Einträge vor den A-Einträgen betrachtet. Sollte für den eingetragenen Hostnamen neben einem A-Eintrag auch ein MX-Eintrag existieren, wird der Konnektor auf diesen zurückgreifen.

7. Aktivieren Sie im folgenden Dialogfenster die Option **Immer TLS zum Sichern der Verbindung verwenden**. Im darunterliegenden Dialogfenster wählen Sie den Punkt **Alle digitalen Zertifikate, einschließlich selbstsignierter**

## Zertifikate aus und klicken **Weiter**.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Sicherheitseinschränkungen' step selected in the left-hand navigation pane. The main content area is titled 'Sicherheitseinschränkungen' and contains the following text: 'Wie sollte Office 365 eine Verbindung mit dem E-Mail-Server Ihrer Partnerorganisation herstellen?' Below this, there are three radio button options: 'Immer TLS (Transport Layer Security) zum Sichern der Verbindung verwenden (empfohlen)' (checked), 'Verbindung nur herstellen, wenn das Zertifikat des E-Mail-Servers des Empfängers dieses Kriterium erfüllt', and 'Alle digitalen Zertifikate, einschließlich selbstsignierter Zertifikate'. There is also an option 'Von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt' with a sub-option 'Fügen Sie den Betreffnamen oder alternativen Betreffnamen (SAN) hinzu, der diesem Domänennamen entspricht.' and a text input field with the example 'Beispiel: "contoso.com" oder "\*"contoso.com"'. A 'Weiter' button is not visible in this step.

8. Kontrollieren Sie die Zusammenfassung Ihrer Angaben auf Richtigkeit und klicken Sie **Weiter**.

9. Geben Sie im folgenden Dialog eine oder mehrere E-Mail-Adressen ein, die Sie für die Überprüfung dieses Konnektors verwenden möchten.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Überprüfungs-E-Mail' step selected in the left-hand navigation pane. The main content area is titled 'Überprüfungs-E-Mail' and contains the text: 'Geben Sie eine E-Mail-Adresse für ein abtestes Postfach an, das sich in Ihrer Partnerdomäne befindet. Wenn Ihre Partnerorganisation über mehrere Domänen verfügt, können Sie mehrere Adressen hinzufügen.' Below this is a text input field with the example 'Beispiel: benutzer@contoso.com' and a blue '+' button. An 'Überprüfen' button is located below the input field.

10. Klicken Sie **Überprüfen**.

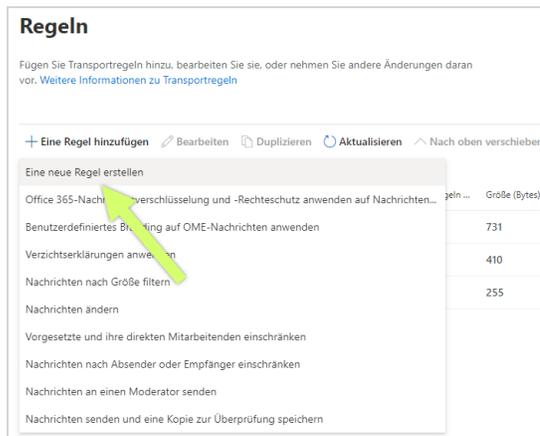


**HINWEIS:** Es werden nun eine oder mehrere Test-Nachrichten gesendet. Nach Abschluss der Prüfung erhalten Sie ein Überprüfungsergebnis. Die Test-Nachricht schlägt in der Regel fehl; dies können Sie zunächst ignorieren.

11. Klicken Sie **Speichern**, um den Dialog zu schließen.

# Die Transportregel erstellen

1. Wechseln Sie im Exchange Admin Center zu **E-Mail-Fluss > Regeln**; klicken Sie danach **Eine Regel hinzufügen**.
2. Wählen Sie die Option **Eine neue Regel erstellen**.



3. Geben Sie einen beliebigen Namen für die Regel ein.
4. Stellen Sie unter **Diese Regel anwenden wenn** die folgenden Optionen ein:
  - **Der Empfänger**
  - **ist extern/intern**
  - **Außerhalb der Organisation**
5. Stellen Sie unter **Gehen Sie wie folgt vor** die folgenden Optionen ein:
  - **Nachricht umleiten an**
  - **Der folgende Connector**
6. Geben Sie danach den vorher erstellten Konnektor an und klicken Sie **Speichern** und dann **Weiter**.



**HINWEIS:** Falls Sie an dieser Stelle nur **Personen** auswählen können, klicken Sie im unteren Abschnitt **Weitere Optionen**. Dort können Sie unter **Die Nachricht umleiten an** die Option **Folgenden Connector verwenden** auswählen. Anschließend können Sie den zuvor erstellten Konnektor verwenden.

7. Klicken Sie **Speichern**.

1. Stellen Sie unter **Gehen Sie wie folgt vor** die folgenden Optionen ein:

- **Nachricht umleiten an**
- **Der folgende Connector**

# Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online

Wenn Sie NoSpamProxy® in Microsoft 365 in Verbindung mit Exchange Online nutzen, müssen Sie in Ihrem Tenant zusätzliche Einstellungen vornehmen, die die Spamabwehr sicherstellen.

## I Schritt 1: Anlegen eines eingehenden Connectors für die Domain \*

Um die Zustellung von unerwünschten E-Mails aus dem Internet zu unterbinden, legen Sie einen eingehenden Connector an. Dieser Connector erlaubt für die Domain \* nur E-Mails von bestimmten IP-Adressen - Ihrem eigenen E-Mail-Server oder NoSpamProxy. Hierfür wird ein entsprechender Partner Connector benötigt.

Um den Partner Connector in PowerShell anzulegen, geben Sie Folgendes ein:

```
New-InboundConnector  
  
-Name "NurE-MailsVonDiesemServerAkzeptieren<NoSpamProxy>"  
  
-ConnectorType Partner  
  
-SenderDomains *
```

```
-RestrictDomainsToCertificate $true
```

```
-TlsSenderCertificateName <DasZuvorErstellteUndAusgewählteZertifikat>
```

```
-AssociatedAcceptedDomains
```

```
<AlleDomänenDieInNoSpamProxyUnterEigeneDomänenStehenUndImOffice365TenantVerwendetWerden>
```



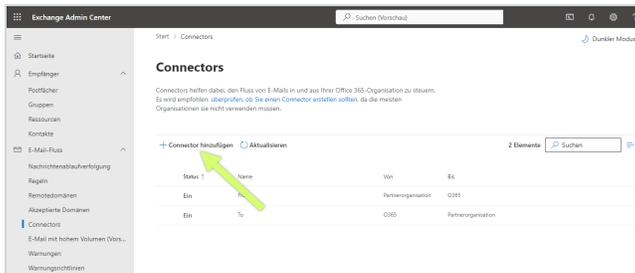
**WARNING:** Um den Spam-Schutz durch NoSpamProxy® sicherzustellen, müssen Sie sämtlichen eingehenden E-Mail-Verkehr über NoSpamProxy leiten und Microsoft 365 ausschließlich durch NoSpamProxy unter Verwendung eines dedizierten Konnektors ansprechen. Ansonsten ist es möglich, dass sich die Anti-Spam-Funktionalitäten von NoSpamProxy und Exchange Online Protection (EOP) gegenseitig behindern. Wir empfehlen Ihnen dringend, diese Einstellung vorzunehmen, da die Sicherheit und Stabilität Ihrer Konfiguration sonst nicht gewährleistet ist.



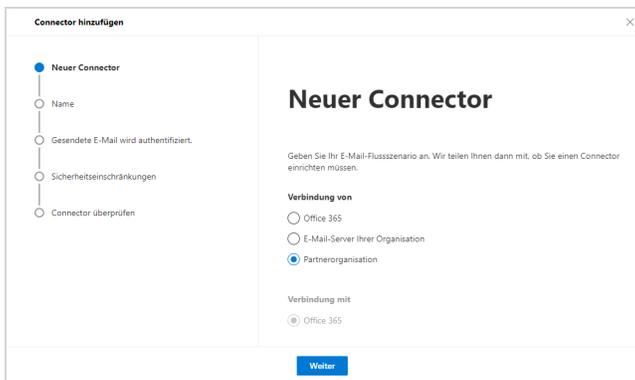
**TIP:** Sie können an Stelle der IP-Adresse auch das Zertifikat des einliefernden Gateways hinterlegen.

Um den Partner Connector über das Exchange Control Panel anzulegen, gehen Sie folgendermaßen vor:

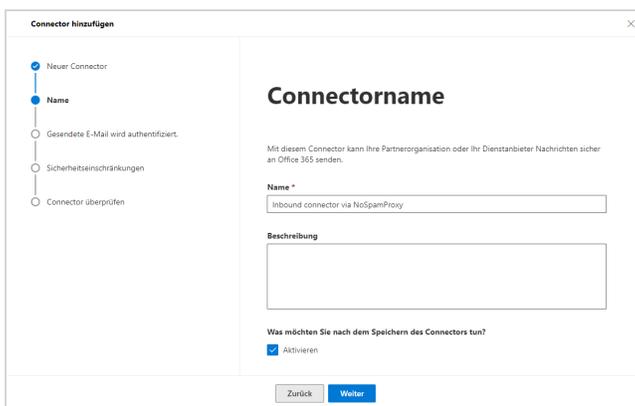
1. Gehen Sie zu **E-Mail-Fluss > Connectors** und klicken Sie **Connector hinzufügen**.



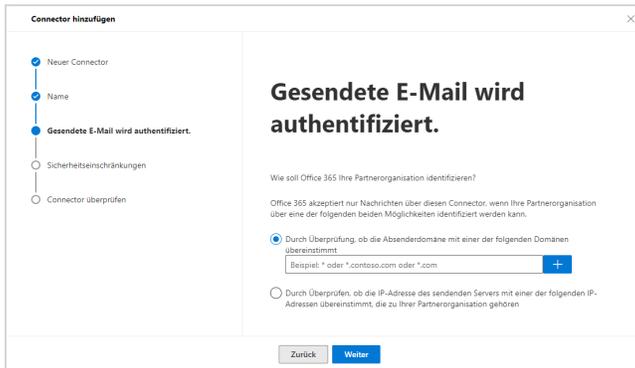
2. Wählen Sie im Dialogfenster die Optionen **Partnerorganisation** und **Office 365** aus und klicken Sie danach **Weiter**.



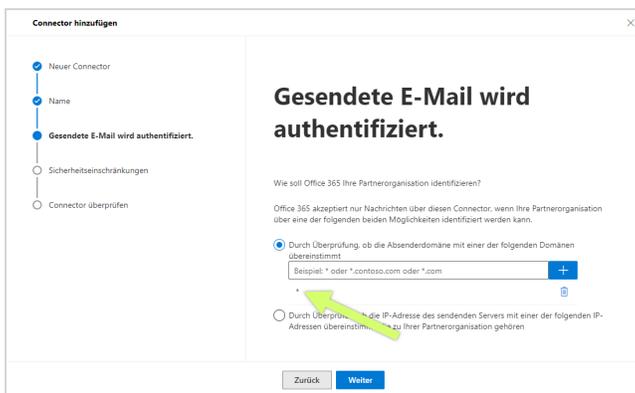
3. Geben Sie im Dialog **Neuer Connector** einen Namen für den Connector ein und fügen Sie bei Bedarf eine Beschreibung hinzu. Lassen Sie das Häkchen neben **Aktivieren** gesetzt. Klicken Sie dann **Weiter**.



4. Wählen Sie im folgenden Dialogfenster die Option **Durch Überprüfung, ob die Absenderdomäne [...]**.



5. Geben Sie als Domainnamen ein Sternchen ("\*") ein und klicken Sie danach das **Plus-Zeichen**



6. Setzen Sie auf der folgenden Seite das Häkchen bei **E-Mails zurückweisen, wenn Sie nicht aus diesem Adressbereich gesendet werden**, geben Sie die **IP-Adresse des Servers** an, auf dem die Gatewayrolle installiert ist und

klicken Sie das Plus-Zeichen.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Sicherheitseinschränkungen' step selected in the left-hand navigation pane. The main content area is titled 'Sicherheitseinschränkungen' and contains the following text: 'Welche Sicherheitseinschränkungen sollen angewendet werden?'. There are two checkboxes: the first is unchecked and labeled 'E-Mails zurückweisen, wenn sie nicht über TLS gesendet werden', with a sub-note 'Und anfordern, dass der Anfragstellername im Zertifikat, das der Partner verwendet, um sich bei Office 365 zu authentifizieren, mit diesem Domänennamen übereinstimmt' and an example input field 'Beispiel: "contoso.com" oder "\*"contoso.com";'. The second checkbox is checked and labeled 'E-Mails zurückweisen, wenn sie nicht aus diesem IP-Adressbereich gesendet werden', with an example input field 'Beispiel: 10.5.3.2 oder 10.3.1.5/24' and a plus sign button to the right. A green arrow points to this plus sign button. At the bottom, there are 'Zurück' and 'Weiter' buttons.

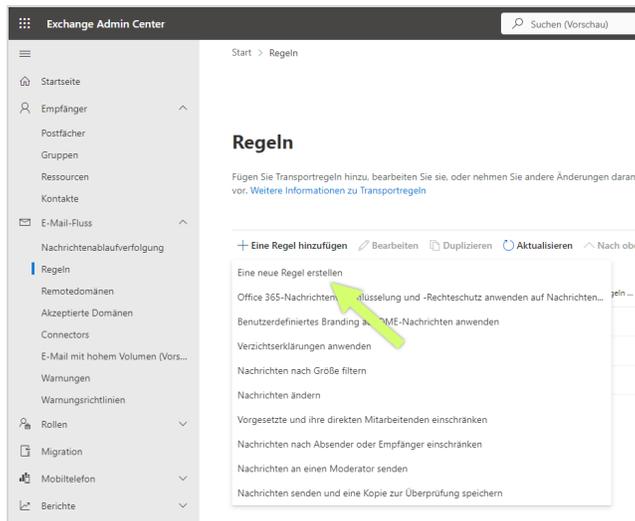
7. Überprüfen Sie die Angaben in der Zusammenfassung auf Richtigkeit und klicken Sie OK.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Connector überprüfen' step selected in the left-hand navigation pane. The main content area is titled 'Connector überprüfen' and contains the following information: 'E-Mail-Flusszenario' (Von: Partnerorganisation, An: Office 365), 'Name' (Inbound connector via NoSpamProxy), and 'Status' (Nach dem Speichern aktivieren, with a 'Namen bearbeiten' link). Below this is a section 'So identifizieren Sie Ihre Partnerorganisation' with the instruction 'Identifizieren Sie die Partnerorganisation, indem Sie überprüfen, ob die Nachrichten von diesen Domänen stammen.' and a link 'Identität von ... ändern E-Mails bearbeiten'. At the bottom, there is a section 'Sicherheitseinschränkungen' with the instruction 'Nachrichten ablehnen, wenn sie nicht aus diesen IP-Adressbereichen stammen:' and a link 'Einschränkungen bearbeiten'. A green arrow points to the 'Connector erstellen' button at the bottom right. At the bottom left, there are 'Zurück' and 'Connector erstellen' buttons.

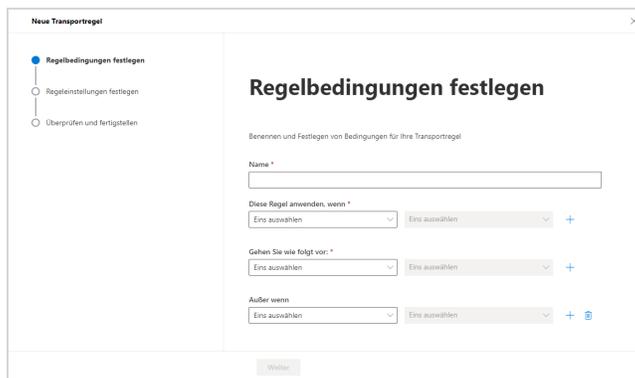
Der neue Connector erscheint jetzt unter **E-Mail-Fluss > Connectors**.

## Schritt 2: Anlegen einer Transportregel zur Abschaltung des Spamfilters

1. Gehen Sie zu **E-Mail-Fluss > Regeln**.
2. Klicken Sie **Eine Regel hinzufügen** und dann **Eine neue Regel erstellen**.



3. Geben Sie der Regel einen Namen.



4. Wählen Sie unter **Diese Regel anwenden, wenn** die Option **Der Absender** und danach **IP liegt in einem dieser Bereiche** oder **stimmt genau überein**

mit.

Neue Transportregel

Regelbedingungen festlegen

Regelinstellungen festlegen

Überprüfen und fertigstellen

### Regelbedingungen festlegen

Benennen und Festlegen von Bedingungen für Ihre Transportregel

Name \*

Outbound mails to NoSpamProxy

Diese Regel anwenden, wenn \*

Der Absender IP liegt in einem dieser Bereiche oder ... +

Die IP-Adresse des Absenders befindet sich im Bereich [Enter words](#) [✎](#)

Gehen Sie wie folgt vor: \*

Eins auswählen Eins auswählen +

Außer wenn

Eins auswählen Eins auswählen + [✎](#)

[Weiter](#)

5. Geben Sie im Dialog **IP-Adressbereiche angeben** die IP-Adresse des Servers an, auf dem die Gatewayrolle installiert ist, klicken Sie **Hinzufügen** und dann **Speichern**.

Neue Transportregel

Regelbedingungen festlegen

Regelinstellungen festlegen

Überprüfen und fertigstellen

### Regelbedingungen festlegen

Benennen und Festlegen von Bedingungen für Ihre Transportregel

Name \*

Outbound mails to NoSpamProxy

Diese Regel anwenden, wenn \*

Der Absender IP liegt in einem dieser Bereiche oder ... +

Die IP-Adresse des Absenders befindet sich im Bereich [✎](#)

Gehen Sie wie folgt vor: \*

Nachrichteneigenschaften ändern SCL-Bewertung (Spam Confidence Lev...) +

SCL-Bewertung (Spam Confidence Level) festlegen - 1 [✎](#)

Außer wenn

Eins auswählen Eins auswählen + [✎](#)

[Weiter](#)

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**.

Die Regel ist nun eingerichtet. Der Spamschutz für die Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online ist sichergestellt.

# Notwendige Konfigurationen für den Betrieb in Microsoft Azure

## Einbinden des TCP Proxy



**HINWEIS:** Sie müssen über einen gültigen Vertrag über Softwarewartung verfügen, um den TCP Proxy nutzen zu können.

Bei einigen cloudbasierten Systemen - zum Beispiel in Microsoft Azure - kann es vorkommen, dass der Port 25 ausgehend vom Anbieter blockiert wird. Port 25 wird aber zum Versand von E-Mails benötigt, was einen Betrieb von NoSpamProxy auf einem solchen System behindert.

Hierzu bieten wir eine Alternative an, um solche Systeme trotzdem zu nutzen: unseren *TCP Proxy*. Dieses System kann auf unten beschriebene Weise in NoSpamProxy aktiviert werden. Dabei wird jede ausgehende Verbindung an eine routingfähige IPv4-Adresse auf TCP-Ebene durch den TCP Proxy für NoSpamProxy geroutet. Die E-Mails werden dann vom Server aus über Port 443 an den TCP Proxy gesendet und von dort dann über Port 25 weiter zum Empfängersystem geleitet.

1. Stoppen Sie den Dienst der Gatewayrolle über das NoSpamProxy Command Center oder die Windows-Dienste
2. Öffnen Sie als Administrator einen Texteditor auf dem System, auf dem die Gatewayrolle installiert ist.
3. Öffnen Sie die Konfigurationsdatei **Gateway Role.config** aus dem Verzeichnis **C:\ProgramData\Net at Work Mail Gateway\Configuration\**.

- Suchen Sie in der Datei nach `<smtpServicePointConfiguration>` und ändern/fügen Sie den Wert

```
isProxyTunnelEnabled="true"  
proxyTunnelAddress="proxy.nospamproxy.com"
```

als Attribute hinzu. Falls `<smtpServicePointConfiguration` nicht vorhanden ist, suchen Sie nach `<netatwork.nospamproxy.proxyconfiguration` und fügen Sie

```
<smtpServicePointConfiguration isProxyTunnelEnabled="true"  
proxyTunnelAddress="proxy.nospamproxy.com" />
```

direkt unter diesem Wert hinzu.

- Speichern Sie die Datei ab und schließen Sie den Editor.
- Legen Sie das **Root CA Zertifikat** im Zertifikatsspeicher von Microsoft im Computerkonto unter **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** auf dem Server mit der Gatewayrolle ab.
- Bearbeiten Sie im NoSpamProxy Command Center unter **Konfiguration > NoSpamProxy Komponenten > Gatewayrollen** die entsprechende Gatewayrolle und ändern Sie den Wert für **SMTP Servername** auf den Wert `outboundproxy.nospamproxy.com`.
- Starten Sie den Gatewayrollen-Dienst wieder
- Öffnen Sie die Datei **Gateway Role.config** erneut und prüfen Sie, ob der Wert beim Start erhalten geblieben ist.

## | Anpassen des SPF-Eintrags

- Wenn der TCP-Proxy implementiert ist, tritt dieser als absendendes System auf. Somit muss der TCP-Proxy auch mit in Ihrem SPF-Eintrag aufgenommen werden. Wir empfehlen dringend, folgenden Eintrag in Ihren SPF-Eintrag hinzuzufügen:

```
include:_spf.proxy.nospamproxy.com
```

## | Gegebenenfalls: Anpassen von Microsoft 365

Falls Sie aus Azure heraus E-Mails an eine eigene Microsoft-365-Instanz schicken, bei der ein Konnektor auf die IP-Adressen gebunden ist, aktualisieren Sie bitte die IP-Adressen passend zum Namen `outboundproxy.nospamproxy.com`. Da bei Microsoft 365 die TLS-Zertifikate gegen die HELO-Domain geprüft werden, ist es nur mit deutlich erhöhtem Aufwand möglich, dies entsprechend umzusetzen. Wir empfehlen daher eine Validierung anhand des Namens.

## | Gegebenenfalls: Anpassen der Firewall

- Falls Sie ausgehende Verbindungen gezielt blockieren, sollten Sie die Ausnahme für den TCP Proxy so anpassen, dass Verbindungen zum **IP-Netz 193.37.132.0/24** erlaubt sind.

## Einrichten einer statischen IP-Adresse

Wenn Sie NoSpamProxy oder Teile davon in einer virtuellen Maschine in einer Microsoft-Azure-Umgebung betreiben möchten, benötigen Sie eine IP-Adresse, die auch nach dem Neustart der Maschine erhalten bleibt. Um dies zu erreichen, müssen Sie eine statische IP-Adresse (Reserved IP Address) einrichten. Ansonsten ist es möglich, dass nach dem Neustart der Maschine eine andere IP-Adresse zugewiesen wird.



**HINWEIS:** Diese Einstellung nehmen Sie auf dem virtuellen Computer in Microsoft Azure vor, auf dem NoSpamProxy installiert ist.

1. Öffnen Sie die Webseite [portal.azure.com](https://portal.azure.com).
2. Klicken Sie unter **Home > Virtuelle Computer** auf den virtuellen Computer, auf dem NoSpamProxy installiert ist.
3. Gehen Sie zu **Netzwerk > Netzwerkschnittstelle > IP-Konfigurationen** und wählen Sie die für NoSpamProxy relevante Konfiguration.
4. Aktivieren Sie die Option **Öffentliche IP-Adresse** und klicken sie danach **Neu erstellen**.
5. Geben Sie einen Namen ein und wählen Sie die Option **Statisch** aus.
6. Klicken Sie **OK**.

Die IP-Adresse wird nun unter dem angegebenen Namen angezeigt.



**HINWEIS:** Beachten Sie beim Einrichten einer statischen IP-Adresse die Informationen von der entsprechenden [Seite der Microsoft-Dokumentation](#).

## Anpassen des Reverse-DNS-Eintrags für den NoSpamProxy-Server

1. Öffnen Sie [portal.azure.com](https://portal.azure.com).
2. Gehen Sie zu **Dashboard > Ressourcengruppen > [DieRessourcengruppeZuDerDerVirtuelleComputerGehört] > [IhrVirtuellerComputer] > Eigenschaften**.
3. Geben Sie unter **DNS-Namensbezeichnung** einen Namen für die öffentliche IP-Adresse an.
4. Starten Sie die Azure Shell.
5. Geben Sie den folgenden Befehl ein und ersetzen Sie dabei die vorhandenen Platzhalter:

```
az network public-ip update --resource-group [Ressourcengruppe] --name [NameDerIPAdresse] --reverse-fqdn [VollstaendigerDNSName] --dns-name [DNSName]
```



**HINWEIS:** Beachten Sie auch die Anweisungen auf der entsprechenden [Seite der Microsoft-Azure-Dokumentation](#).

# Hilfe und Unterstützung

---

## Knowledge Base

---

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

## Website

---

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

## 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.

## 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.

## YouTube

---

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

Unser Support-Team erreichen Sie

- per Telefon unter +49 5251304-636
- per E-Mail unter support@nospamproxy.de.

