



Version 14

## Integration von NoSpamProxy Encryption

- 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 27. NOVEMBER 2023 ÜBERARBEITET.**

# Inhalt

Einleitung .....	1
Microsoft 365 als Relayhost freigeben .....	2
Weiterleitung an Microsoft 365 einrichten .....	5
Microsoft 365 konfigurieren .....	9
Die Transportregeln erstellen .....	16
Notwendige Konfigurationen für den Betrieb in Microsoft Azure .....	20
<b>Hilfe und Unterstützung .....</b>	<b>26</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

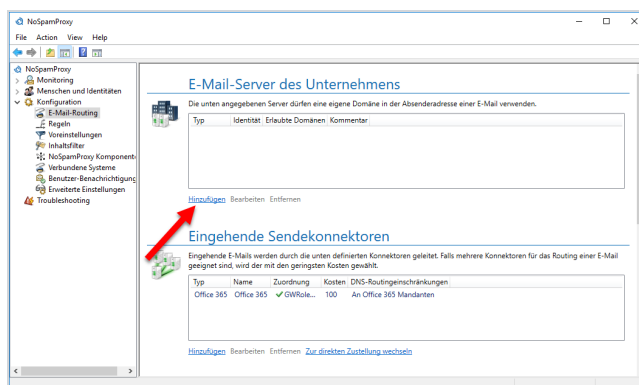
In diesem Schritt lassen Sie Microsoft 365 in der NoSpamProxy®-Konfiguration als Relayhost zu, damit E-Mails aus Microsoft 365 heraus durch NoSpamProxy an externe Kommunikationspartner verschickt werden können.

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

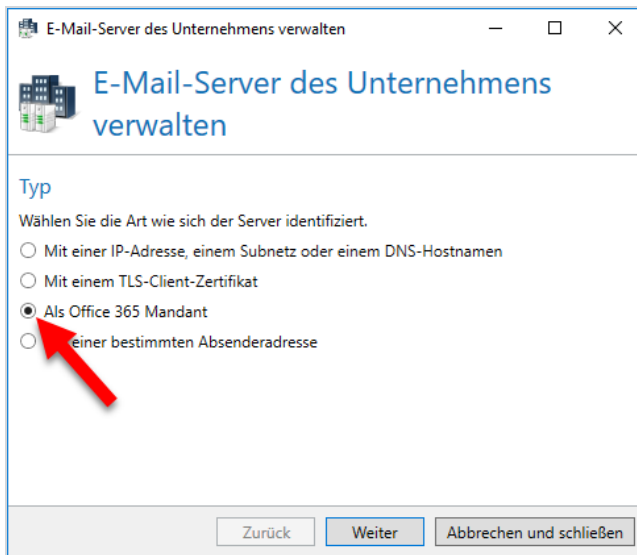


**HINWEIS:** Stellen Sie sicher, dass Sie mindestens eine Unternehmensdomäne eingerichtet haben, bevor Sie mit der Konfiguration beginnen.

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

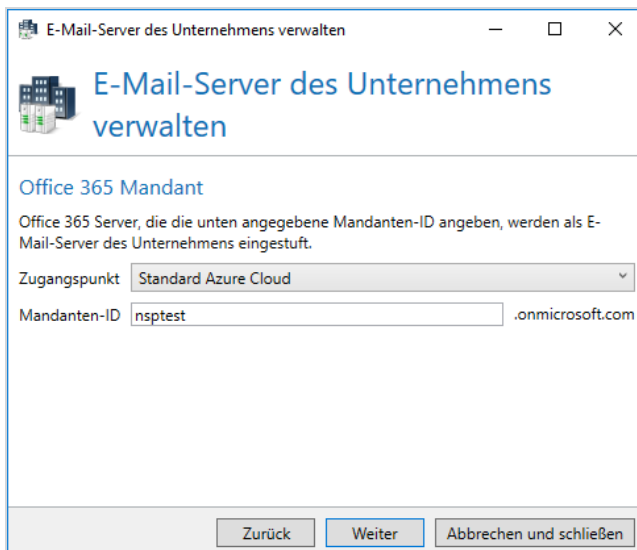


2. Wählen Sie den Typ **Als Office 365 Mandant** und klicken Sie danach **Weiter**.



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 one, but now on the 'Office 365 Mandant' step. The sub-heading is 'Office 365 Mandant' and the text below it says 'Office 365 Server, die die unten angegebene Mandanten-ID angeben, werden als E-Mail-Server des Unternehmens eingestuft.' There are two input fields: 'Zugangspunkt' with a dropdown menu showing 'Standard Azure Cloud' and 'Mandanten-ID' with a text box containing 'nsptest' and a '.onmicrosoft.com' suffix. 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**.

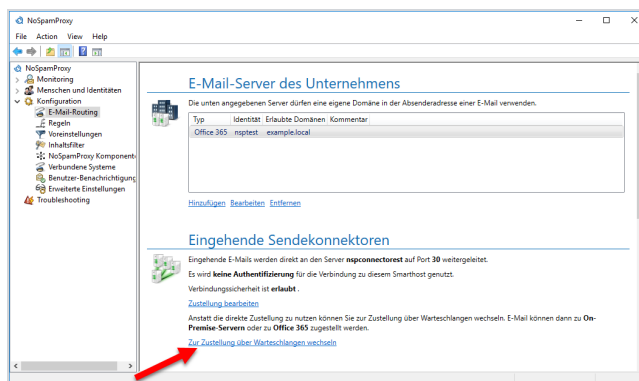
Der E-Mail-Server ist nun angelegt.

# Weiterleitung an Microsoft 365 einrichten

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

## Den eingehenden Sendekonnektor anlegen

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



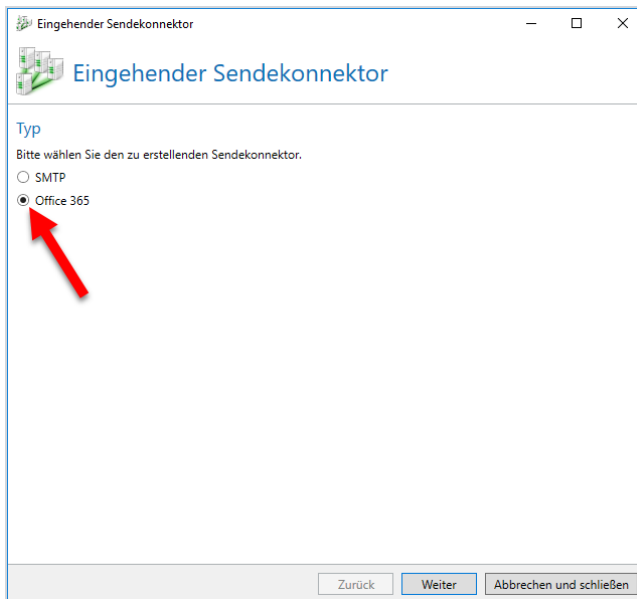
3. Wählen Sie im Dialog **Zustellung ändern** die Option **Zustellung ersetzen**.



**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** und dann **Fertigstellen**.

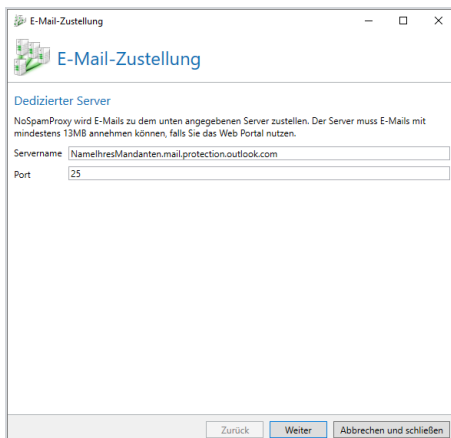
## ■ Den ausgehenden Sendekonnektor anlegen

1. Gehen Sie zu **Konfiguration > E-Mail-Routing**.
2. Klicken Sie unter **Ausgehende Sendekonnectoren** auf **Hinzufügen**, wählen Sie **SMTP** und klicken Sie **Weiter**.
3. Geben Sie einen beliebigen Namen für den ausgehenden Sendekonnektor ein, wählen Sie danach die Gatewayrolle(n) aus, die ausgehende E-Mails

verarbeiten sollen und bestimmen Sie die Kosten.



4. Wählen Sie unter **Routing-Methode** die Option **Auslieferung über einen dedizierten Server (Smarthost)** und klicken Sie **Weiter**.
5. Klicken Sie unter **Zustellung** auf **Hinzufügen** und geben Sie als Servernamen den entsprechenden Namen nach dem Muster **NamelhresMandanten.mail.protection.outlook.com** an.



6. Wählen Sie die Option **Keine Authentifizierung verwenden** und klicken Sie **Weiter**.

7. Bestimmen Sie die Verbindungssicherheit, wählen Sie gegebenenfalls ein Zertifikat und klicken Sie **Fertigstellen** und dann **Weiter**.
8. Belassen Sie die Einstellung unter **DNS-Routingeinschränkungen**.
9. Klicken Sie **Fertigstellen**.

Die Konfiguration für NoSpamProxy ist nun abgeschlossen.

# Microsoft 365 konfigurieren

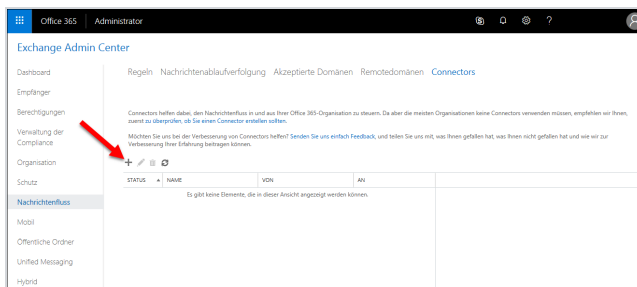
## ■ Einen Konnektor für ausgehende E-Mails anlegen

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 Office-365-Mandanten unter <https://outlook.office365.com/ecp> an.



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

1. Wechseln Sie im Exchange Admin Center zu **Nachrichtenfluss > Connectors**; klicken Sie danach das **Plus-Zeichen**. Der Assistent zum Anlegen eines neuen Connectors öffnet sich.



2. Wählen Sie auf der ersten Seite im Feld **Von** die Option **Office 365** aus; wählen Sie im Feld **An** die Option **Partnerorganisation** aus.
3. Klicken Sie **Weiter**. Mit dieser Einstellung werden ausgehende E-Mails vom Office-365-Mandanten an NoSpamProxy gesendet.

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

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

Neuer Connector

Wann möchten Sie diesen Connector verwenden?

Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Connector umleitet

Nur an alle akzeptierten Domänen in Ihrer Organisation gesendete E-Mails

Nur, wenn E-Mails an diese Domänen gesendet werden

+ -

Zurück Weiter Abbrechen

8. Geben Sie den Namen oder die IP-Adresse des Servers (Smarthost) an, auf dem die Gatewayrolle installiert ist und klicken Sie danach **Speichern**.

https://outlook.office365.com/ocp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

smarthost hinzufügen

Geben Sie den vollqualifizierten Domännennamen (FQDN) des Smarthosts oder eine IPv4-Adresse an.  
Beispiel: „myhost.contoso.com“ oder „192.168.3.2“

Speichern Abbrechen



**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.

9. 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.

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

Neuer Connector

Wie sollte Office 365 eine Verbindung mit Ihrem E-Mail-Server herstellen?

Immer TLS (Transport Layer Security) zum Sichern der Verbindung verwenden (empfohlen)  
Verbindung nur herstellen, wenn das Zertifikat des E-Mail-Servers des Empfängers dieses Kriterium erfüllt

Alle digitalen Zertifikate, einschließlich selbstsignierter Zertifikate

Nur Zertifikate einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt

Nur Zertifikate einer Antragstellername oder der alternative Antragstellername (SAN), die mit diesem Domännennamen überein:  
Beispiel: ".contoso.com" oder "\*.contoso.com"

Zurück Weiter Abbrechen

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

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

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

Neuer Connector

Diesen Connector überprüfen

Wir überprüfen diesen Connector für Sie, um sicherzustellen, dass er wie erwartet funktioniert, aber Sie müssen zuerst mindestens eine E-Mail-Adresse angeben, damit wir eine Testnachricht senden können.

Geben Sie eine E-Mail-Adresse für ein aktives Postfach an, das sich auf Ihrem E-Mail-Server befindet. Wenn Ihre Organisation über mehrere Domänen verfügt, können Sie mehrere Adressen hinzufügen.

+ ✎ -

@nctatwork.de

Zurück Überprüfen Abbrechen

12. 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.

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

## **|** Einen Konnektor für eingehende E-Mails anlegen

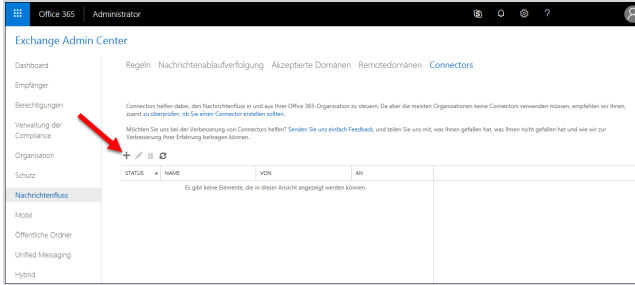
In diesem Schritt konfigurieren Sie den Office-365-Mandanten so, dass eingehende E-Mails nicht direkt an den Empfängerserver, sondern zunächst an NoSpamProxy® zugestellt werden. Melden Sie sich dazu in an Ihrem Office-365-Mandanten unter <https://outlook.office365.com/ecp> an.



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

1. Wechseln Sie im Exchange Admin Center zu **Nachrichtenfluss > Connectors**; klicken Sie danach das **Plus-Zeichen**. Der Assistent zum Anlegen eines neuen Connectors öffnet sich.





2. Wählen Sie auf der ersten Seite im Feld **Von** die Option **E-Mail-Server Ihrer Organisation** aus; wählen Sie im Feld **An** die Option **Office 365** aus.
3. Klicken Sie **Weiter**.
4. Geben Sie auf der dann folgenden Seite einen beliebigen Namen für den Konnektor ein.



**HINWEIS:** Entfernen Sie unbedingt das Häkchen neben **Interne Exchange-Email-Header beibehalten (empfohlen)**.

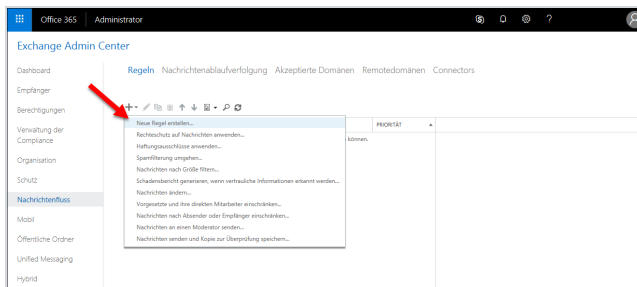
5. Geben Sie bei Bedarf eine Beschreibung ein und klicken Sie **Weiter**.

6. Wählen Sie auf der dann folgenden Seite die Option **Durch Überprüfen, ob die IP-Adresse [...]**, klicken Sie das **Plus-Zeichen** und geben Sie die IP-Adresse des NoSpamProxy-Servers an.
7. Klicken Sie **OK, Weiter** und dann **Speichern**.

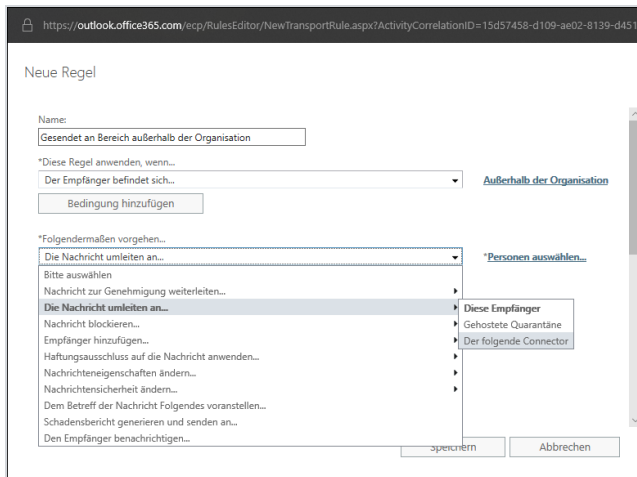
# Die Transportregeln erstellen

## Die ausgehende Transportregel erstellen

1. Gehen Sie in der Office-365-Verwaltungsoberfläche zu **Nachrichtenfluss > Regeln**.
2. Klicken Sie das **Plus-Symbol**.



3. Wählen Sie danach die Option **Neue Regel erstellen**. Der Assistent für die Erstellung einer neuer Transportregel öffnet sich.



4. Geben Sie einen beliebigen Namen für die Regel ein.

5. Stellen Sie unter **Diese Regel anwenden wenn** die folgenden Optionen ein:
  - **Der Empfänger befindet sich** sowie
  - **Außerhalb der Organisation.**
6. Stellen Sie unter **Folgendermaßen vorgehen** die Option **Folgenden Connector verwenden** ein.
7. Geben Sie danach den vorher erstellten Konnektor für ausgehende E-Mails an und klicken Sie **OK**.



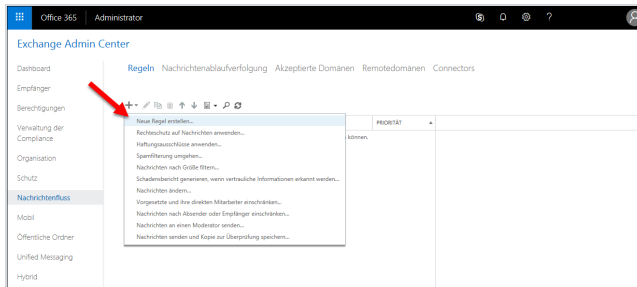
**HINWEIS:** Falls Sie an dieser Stelle nur **Personen** auswählen können, klicken Sie im unteren Abschnitt **Weitere Optionen**. Dort können Sie unter **Die Nachricht umleiten an** die Option **Folgenden Connector verwenden** auswählen. Anschließend können Sie den zuvor erstellten Konnektor verwenden.

8. Klicken Sie **Ausnahme hinzufügen** und dann **Absender** sowie **IP liegt in einem dieser Bereiche oder stimmt genau überein mit**.
9. Fügen Sie die von NoSpamProxy genutzte IP-Adresse hinzu und klicken Sie **OK**.
10. Klicken Sie **Speichern**.

## **|** Die eingehende Transportregel erstellen

1. Gehen Sie in der Office-365-Verwaltungsoberfläche zu **Nachrichtenfluss > Regeln**.

## 2. Klicken Sie das **Plus-Symbol**.



3. Wählen Sie danach die Option **Neue Regel erstellen**. Der Assistent für die Erstellung einer neuer Transportregel öffnet sich.


4. Geben Sie einen beliebigen Namen für die Regel ein.

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

- **Der Empfänger befindet sich** sowie
- **Innerhalb der Organisation.**

6. Stellen Sie unter **Folgendermaßen vorgehen** die Option **Folgenden Connector verwenden** ein.

7. Geben Sie danach den vorher erstellten Connector für eingehende E-Mails an und klicken Sie **Aktion hinzufügen**.

8.  **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 Connector verwenden.

9. Klicken Sie **Ausnahme hinzufügen** und dann **Absender** sowie **IP liegt in einem dieser Bereiche oder stimmt genau überein mit**.

10. Fügen Sie die von NoSpamProxy genutzte IP-Adresse hinzu und klicken Sie **OK**.
11. Klicken Sie **Speichern**.

# 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 routing-fähige 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.

## I 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
```

## I 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.

## I 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.

## NoSpamProxy-Support

---

Unser Support-Team erreichen Sie

- per Telefon unter +49 5251304-636
- per E-Mail unter [support@nospamproxy.de](mailto:support@nospamproxy.de).

