



Version 15

Integrating NoSpamProxy

- into Office 365
- into Microsoft Azure
- as an on-premises solution

Legal information

All rights reserved. This document and the applications described therein are copyrighted products of Net at Work GmbH, Paderborn, Federal Republic of Germany. This document is subject to change without notice. The information contained in this document does not constitute an assumption of warranty or liability on the part of Net at Work GmbH. The partial or complete reproduction is only permitted with the written permission of Net at Work GmbH.

Copyright © 2023 Net at Work GmbH

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

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® and Azure® are registered trademarks of Microsoft Corporation. NoSpamProxy® and 32Guards® are registered trademarks of Net at Work GmbH. All other trademarks used belong to the respective manufacturers or owners.

THIS DOCUMENT WAS LAST EDITED ON DECEMBER 11, 2024.

Content

Introduction	1
Enabling Office 365 as a relay host	2
Setting up forwarding to Microsoft 365	5
Configuring Microsoft 365	8
Creating the transport rule	11
Using NoSpamProxy in Microsoft 365 with Exchange Online	13
Step 1: Creating an inbound connector for the domain *	13
Step 2: Creating a transport rule to deactivate the spam filter	17
Necessary configurations for the operation in Microsoft Azure	20
Help and support	25

Introduction

Since version 10, NoSpamProxy® can be fully integrated into Microsoft Office 365. This manual describes the configuration steps for NoSpamProxy and Microsoft 365 as well as for the server environment used.

The described configuration also applies to the use of NoSpamProxy as an on-premises solution and in Microsoft Azure.



NOTE: The specific configuration steps for use in Microsoft Azure are described below [Necessary configurations for the operation in Microsoft Azure](#).

Enabling Office 365 as a relay host

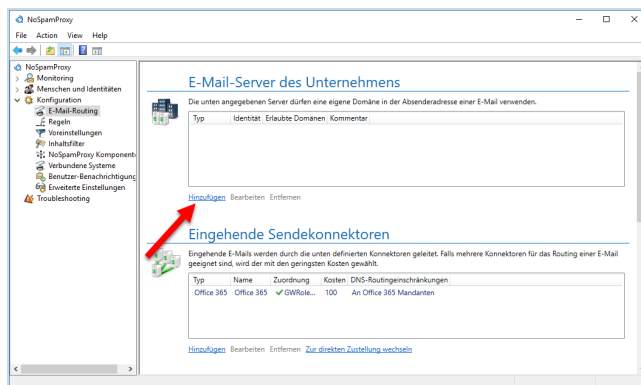
In this step, you allow Microsoft 365 to be used as a relay host in the NoSpamProxy® configuration so that emails can be sent from Microsoft 365 to external communication partners through NoSpamProxy.

Without this configuration, NoSpamProxy will evaluate and reject emails as relay abuse attempts.

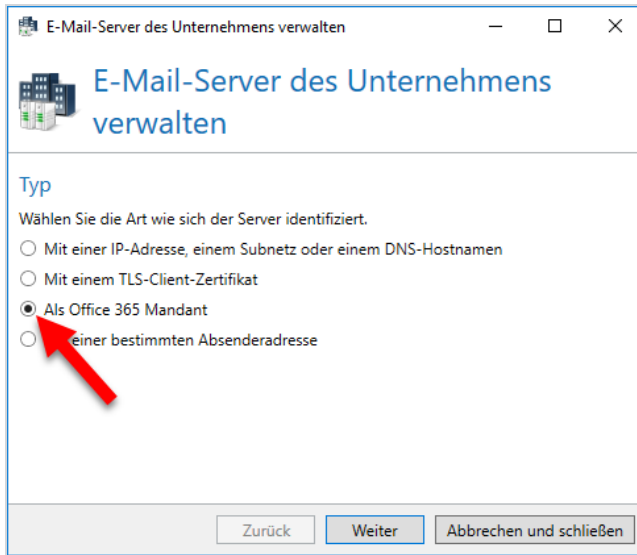


NOTE: Make sure that you have set up at least one corporate domain before you start the configuration.

1. In the NoSpamProxy Command Center, go to **Configuration > Email Routing** and click **Add**.



2. Select the **As Office 365 tenant** type, and then click **Next**.



E-Mail-Server des Unternehmens verwalten

E-Mail-Server des Unternehmens verwalten

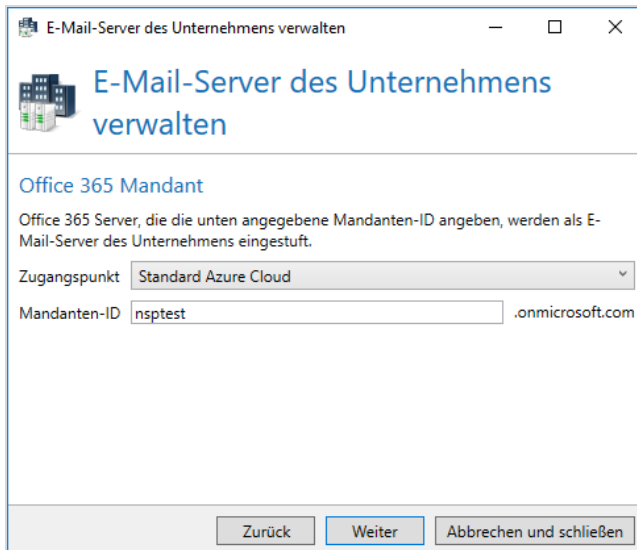
Typ

Wählen Sie die Art wie sich der Server identifiziert.

- Mit einer IP-Adresse, einem Subnetz oder einem DNS-Hostnamen
- Mit einem TLS-Client-Zertifikat
- Als Office 365 Mandant
- Mit einer bestimmten Absenderadresse

Zurück Weiter Abbrechen und schließen

3. Under **Endpoint**, make the appropriate selection for your organisational environment.
4. Enter your tenant ID. Make sure that you enter the name of the ID (not the ID in hexadecimal notation).
5. Click **Next**.



E-Mail-Server des Unternehmens verwalten

E-Mail-Server des Unternehmens verwalten

Office 365 Mandant

Office 365 Server, die die unten angegebene Mandanten-ID angeben, werden als E-Mail-Server des Unternehmens eingestuft.

Zugangspunkt Standard Azure Cloud

Mandanten-ID nsptest .onmicrosoft.com

Zurück Weiter Abbrechen und schließen

6. At **Assigned company domains**, select the domains that you have stored in Microsoft 365 and that will appear in the sender address for outbound emails.



NOTE: If you do not find all domains here, you must add the missing domains under **Identities > Corporate Domains > Corporate Domains**. This is also possible at a later date.

7. Click **Next**.
8. Enter a comment if necessary and then click **Finish**.

The email server has been created.

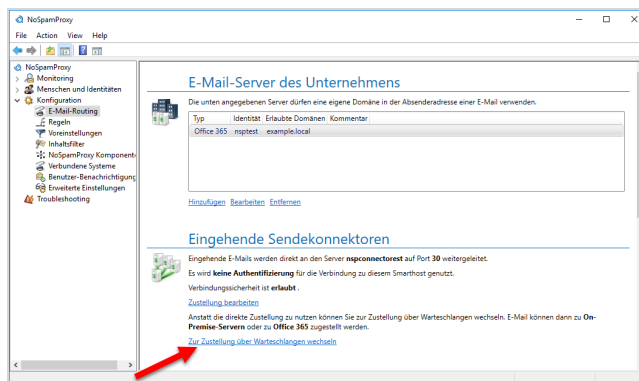
Setting up forwarding to Microsoft 365



NOTE: A TLS certificate issued by a Microsoft trusted root certification authority is required to set up the forwarding to Microsoft 365. You can find an up-to-date list of familiar CAs at <https://docs.microsoft.com/en-us/security/trusted-root/participants-list>.

In this step, you configure NoSpamProxy® so that all inbound emails are forwarded to Microsoft 365. To do this, you must edit the corresponding send connectors.

1. Go to **Configuration > Email routing**.
2. Under **Inbound send connectors**, click **Switch to queued delivery**.

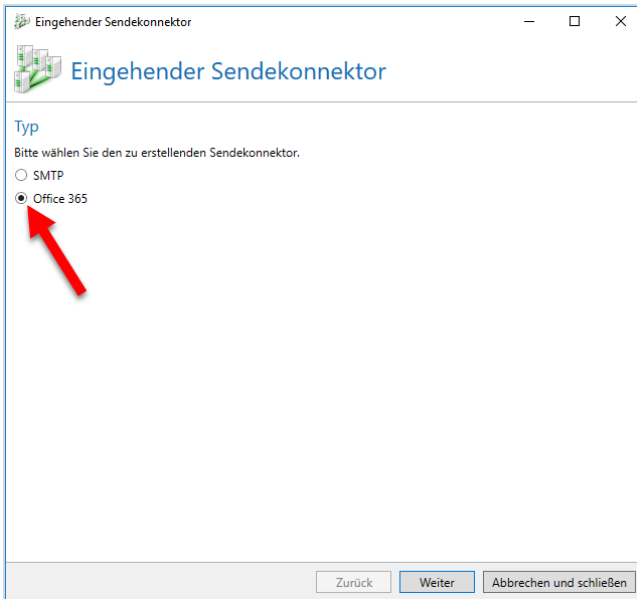


3. In the **Change delivery** dialog, select **Replace delivery**.

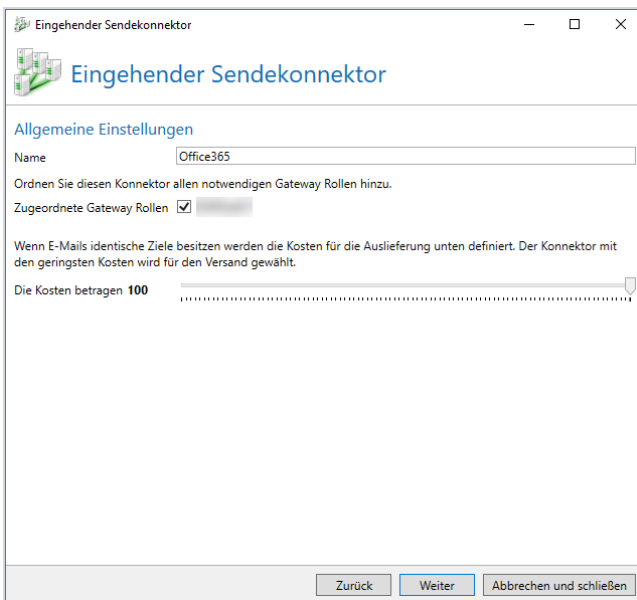


NOTE: From version 13 on, this step is no longer necessary, since direct delivery is no longer supported from this version on.

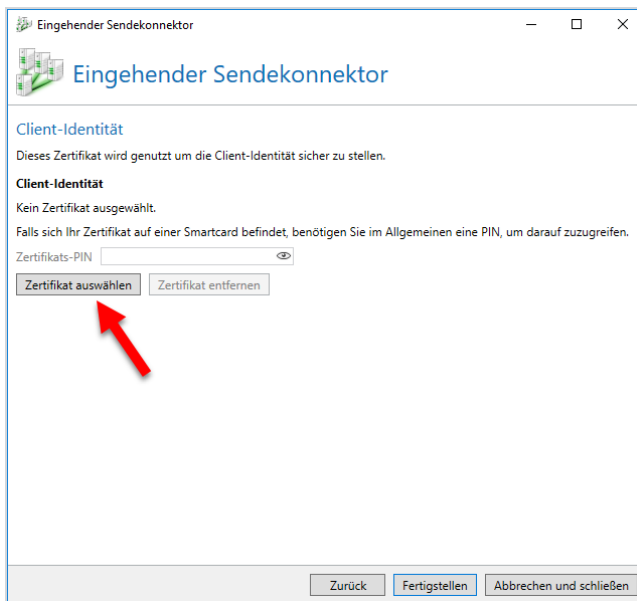
4. In the dialog box that appears, select **Office 365** and click **Next**.



5. Type any name for the inbound send connector, and then select the Gateway Role(s) that you want to process emails to Office 365.
6. Click **Next**.



7. Click **Select certificate** to specify a client identity certificate that NoSpamProxy can use to authenticate to the Office 365 server.



8. In the following dialog box, select the TLS certificate that you have previously applied for from a root CA trusted by Microsoft, and then click **Select and close**.
9. Click **Select and close**.
10. Click **Finish** in the following dialog box.
11. Under **Receive connectors**, open the receive connector in use and switch to the **Connection security** tab.
12. Select either the certificate provided by NoSpamProxy or the certificate you requested previously.
13. Click **Select and close**, then **Save and Close**.

The configuration for NoSpamProxy is now complete.

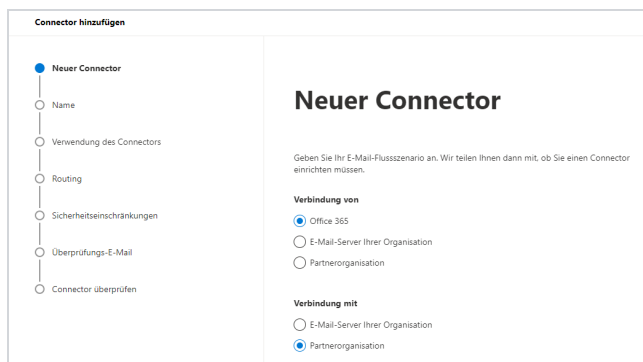
Configuring Microsoft 365

In this step, you configure the Office 365 client not to deliver outbound emails directly to the recipient server, but to NoSpamProxy® first. To do this, log in to your Exchange Admin Centre at <https://admin.exchange.microsoft.com/>.



NOTE: Use a user with administrative rights to log on.

1. In the Exchange Admin Centre, go to **Mail Flow > Connectors**; then click **Add Connector**.
2. On the first page, select **Office 365** in the **From** box; then select **Partner organization** in the **To** box.



3. Click **Next**.
4. On the following page, enter any name for the connector and, if required, a description and click **Next**.

5. On the following page, select the option **Only if I have set up a transport rule that redirects messages to this connector** and click **Next**.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Verwendung des Connectors' step selected. The left sidebar contains a vertical list of steps: 'Neuer Connector', 'Name', 'Verwendung des Connectors', 'Routing', 'Sicherheitsbeschränkungen', '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' (which is selected) and 'Nur, wenn E-Mails an diese Domänen gesendet werden'.

6. Select the option **Forward email via these smart hosts**, enter the name or IP address of the server (smart host) on which the gateway role is installed and click **Save**.

The screenshot shows the 'Connector hinzufügen' dialog box with the 'Routing' step selected. The left sidebar contains a vertical list of steps: 'Neuer Connector', 'Name', 'Verwendung des Connectors', 'Routing', 'Sicherheitsbeschränkungen', 'Überprüfungs-E-Mail', and 'Connector überprüfen'. The main content area is titled 'Routing' and contains the text 'Wie möchten Sie E-Mails weiterleiten?' and '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 Domänennamens (FQDN) oder einer IP-Adresse identifiziert werden.' Below this are two radio button options: 'MX-Eintrag verwenden, der der Domäne des Partners zugeordnet ist' and 'E-Mail über die diese Smarthosts weiterleiten' (which is selected). A text input field contains the example 'myhost.contoso.com oder 192.168.3.2' and a blue '+' button.



NOTE: When entering the host name, note that Microsoft 365 considers the MX records before the A records when resolving. If an MX record exists for the entered host name in addition to an A record, the connector will fall back on the MX record.

7. In the following dialog box, enable the option **Always use Transport Layer Security (TLS) to secure the connection (recommended)**. In the dialog box

below, select **Any digital certificate, including self-signed certificates** and click **Next**.


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 options: 1. 'Immer TLS (Transport Layer Security) zum Sichern der Verbindung verwenden (empfohlen)' with a checked checkbox. 2. 'Verbindung nur herstellen, wenn das Zertifikat des E-Mail-Servers des Empfängers dieses Kriterium erfüllt' with a radio button selected. 3. 'Alle digitalen Zertifikate, einschließlich selbstsignierter Zertifikate' with a radio button selected. Below these options, there is a checkbox for 'Von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt' which is unchecked. Underneath, there is a text input field with the placeholder text 'Beispiel: *.contoso.com' or '*.*.contoso.com'.

8. Check the summary of your information for accuracy and click **Next**.

9. In the following dialog, enter one or more email addresses that you want to use to verify this connector.

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 following text: 'Geben Sie eine E-Mail-Adresse für ein aktives Postfach an, das sich in Ihrer Partnerdomäne befindet. Wenn Ihre Partnerorganisation über mehrere Domänen verfügt, können Sie mehrere Adressen hinzufügen.' Below this text, there is a text input field containing the example email address 'benutzer@contoso.com' and a blue '+' button to the right. Below the input field, there is a 'Überprüfen' button.

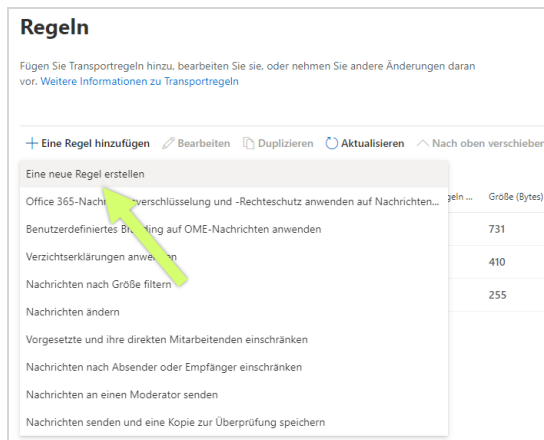
10. Click **Validate**.

 **NOTE:** One or more test messages are now sent. You will receive a check result after the check is completed. The test message usually fails; you can ignore this at first.

11. Click **Save** to close the dialog.

Creating the transport rule

1. In the Exchange Admin Centre, go to **Email flow > Rules**; then click **Add a rule**.
2. Select **Create a new rule**.



3. Enter any name for the rule.
4. Under **Apply this rule if**, set the following options:
 - **The recipient**
 - **is external/internal**
 - **Outside the organization**
5. Set the following options under **Proceed as follows**:
 - **Redirect message to**
 - **The following connector**

6. Enter the previously created connector and click **Save** and then **Next**.



NOTE: If you can only select **persons** at this point, click **More options**. There you can select the option **Use the following connector** under **Redirect the message to**. You can then use the connector you created earlier.

7. Click **Save**.

1. Set the following options under **Proceed as follows**:

- **Redirect message to**
- **The following connector**

Using NoSpamProxy in Microsoft 365 with Exchange Online

If you use NoSpamProxy® in Microsoft 365 in conjunction with Exchange Online, you must make additional settings in your tenant to ensure spam prevention.

I Step 1: Creating an inbound connector for the domain *

To stop the delivery of unwanted emails from the Internet, create an inbound connector. This connector allows for the domain * only emails from specific IP addresses, i.e. your own email server or NoSpamProxy. A corresponding partner connector is required for this.

To create the partner connector in PowerShell, type the following:

```
New-InboundConnector  
  
-Name "AcceptOnlyEMailsFromThisServer<NoSpamProxy>"  
  
-ConnectorType Partner  
  
-SenderDomains *  
  
-RestrictDomainsToCertificate $true  
  
-TlsSenderCertificateName <TheCertificatePreviouslyCreatedAndSelected>  
  
-AssociatedAcceptedDomains  
<AllDomainsListedUnderCorporateDomainsAndUsedInTheOffice365Tenant>
```



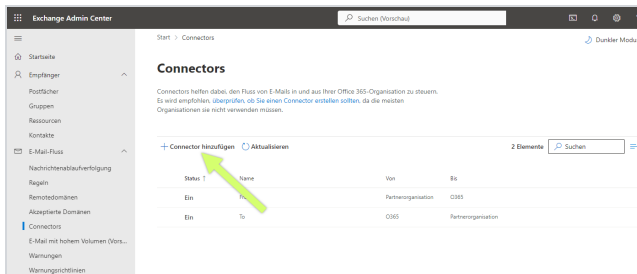

WARNING: To ensure spam protection through NoSpamProxy®, you must route all inbound email traffic through NoSpamProxy and address Microsoft 365 exclusively through NoSpamProxy using a dedicated connector. Otherwise, it is possible that the anti-spam functionalities of NoSpamProxy and Exchange Online Protection (EOP) will interfere with each other. We strongly recommend that you make the following setting, otherwise the security and stability of your configuration cannot be guaranteed.



TIP: Instead of the IP address, you can also store the certificate of the supplying gateway.

To create the partner connector via the Exchange Control Panel, proceed as follows:

1. Go to **Email Flow > Connectors** and click **Add Connector**.



2. In the dialog box, select **Partner organization** and **Office 365**, and then click **Next**.

The screenshot shows the 'Connector hinzufügen' dialog box. On the left, a progress indicator shows five steps: 'Neuer Connector' (selected), 'Name', 'Gesendete E-Mail wird authentifiziert.', 'Sicherheitsbeschränkungen', and 'Connector überprüfen'. The main area is titled 'Neuer Connector' and contains the following text: 'Geben Sie Ihr E-Mail-Flusszenario an. Wir teilen Ihnen dann mit, ob Sie einen Connector einrichten müssen.' Below this, under 'Verbindung von', there are three radio buttons: 'Office 365', 'E-Mail-Server Ihrer Organisation', and 'Partnerorganisation' (selected). Under 'Verbindung mit', there is one radio button: 'Office 365'. A blue 'Weiter' button is at the bottom.

3. In the **New Connector** dialog, enter a name for the connector and add a description if required. Leave the tick next to **Activate**. Then click **Next**.

The screenshot shows the 'Connector hinzufügen' dialog box at the 'Name' step. The progress indicator on the left now has 'Name' selected. The main area is titled 'Connectornamen' and contains the text: 'Mit diesem Connector kann Ihre Partnerorganisation oder Ihr Dienstleister Nachrichten sicher an Office 365 senden.' Below this, there is a 'Name *' field with the text 'Inbound connector via NoSpamProxy'. Under 'Beschreibung', there is a large empty text area. At the bottom, there is a question: 'Was möchten Sie nach dem Speichern des Connectors tun?' with a checked checkbox for 'Aktivieren'. 'Zurück' and 'Weiter' buttons are at the bottom.

4. In the following dialogue window, select the option **By checking whether the sender domain [...]**.

The screenshot shows the 'Connector hinzufügen' dialog box with the following content:

- Progress bar: 1. Neuer Connector, 2. Name, 3. **Gesendete E-Mail wird authentifiziert.**, 4. Sicherheitseinschränkungen, 5. Connector überprüfen
- Section: **Gesendete E-Mail wird authentifiziert.**
- Text: Wie soll Office 365 Ihre Partnerorganisation identifizieren?
- Text: Office 365 akzeptiert nur Nachrichten über diesen Connector, wenn Ihre Partnerorganisation über eine der folgenden beiden Möglichkeiten identifiziert werden kann.
- Option 1 (selected): Durch Überprüfung, ob die Absenderdomäne mit einer der folgenden Domänen übereinstimmt.
Input field: +
- Option 2: Durch Überprüfen, ob die IP-Adresse des sendenden Servers mit einer der folgenden IP-Adressen übereinstimmt, die zu Ihrer Partnerorganisation gehören.
- Buttons: Zurück, Weiter

5. Enter an asterisk ("*") as the domain name and then click on the plus sign

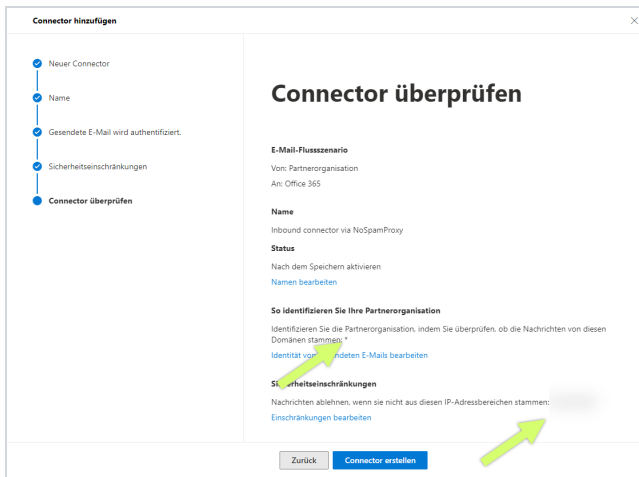
This screenshot is identical to the previous one, but with a green arrow pointing to the asterisk (*) entered in the domain input field.

6. On the following page, tick the **Reject emails if they are not sent from this address range box**, enter the IP address of the server on which the Gateway Role is installed and click the plus sign.

The screenshot shows the 'Connector hinzufügen' dialog box with the following content:

- Progress bar: 1. Neuer Connector, 2. Name, 3. Gesendete E-Mail wird authentifiziert., 4. **Sicherheitseinschränkungen**, 5. Connector überprüfen
- Section: **Sicherheitseinschränkungen**
- Text: Welche Sicherheitseinschränkungen sollen angewendet werden?
- Option 1: E-Mails zurückweisen, wenn sie nicht über TLS gesendet werden
- Option 2: Und anfordern, dass der Antragstellername im Zertifikat, das der Partner verwendet, um sich bei Office 365 zu authentifizieren, mit diesem Domänennamen übereinstimmt.
Input field:
- Option 3 (selected): E-Mails zurückweisen, wenn sie nicht aus diesem IP-Adressbereich gesendet werden
Input field: +
- Buttons: Zurück, Weiter

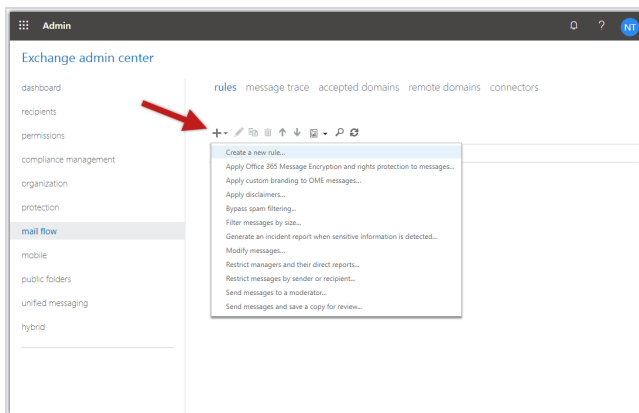
7. Verify that the information in the summary is correct and click **OK**.



The new connector now appears under **Email flow > Connectors**.

Step 2: Creating a transport rule to deactivate the spam filter

1. Go to **Email flow > Rules**.
2. Click **Add a rule** and then **Create a new rule**.



3. Give the rule a name.

Neue Transportregel

Regelbedingungen festlegen

Regelinstellungen festlegen

Überprüfen und fertigstellen

Regelbedingungen festlegen

Benennen und Festlegen von Bedingungen für Ihre Transportregel

Name *

Diese Regel anwenden, wenn *

Gehen Sie wie folgt vor: *

Außer wenn

Weiter

4. Under **Apply this rule**, select if the option **The sender** and then **IP** is in one of these ranges or matches exactly.

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

Außer wenn

Eins auswählen

Weiter

5. In the **Specify IP address ranges** dialogue, enter the IP address of the server on which the gateway role is installed, click **Add** and then **Save**.

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

Weiter

6. Select the following options under **Proceed as follows**:
 - Change message properties
 - Set SCL rating (Spam Confidence Level)
7. In the following dialogue, select the **Bypass spam filtering** option under **Specify SCL**.
8. Click **Save** and then **Next**.
9. Leave the settings for your transport rule unchanged and click **Next** and then **Finish**.

The rule is now set up. Spam protection for the use of NoSpamProxy in Microsoft 365 with Exchange Online is ensured.

Necessary configurations for the operation in Microsoft Azure

Integrating the TCP proxy



NOTE: You must have a valid software maintenance contract to use the TCP Proxy.

It is possible that for cloud-based systems, e.g. Microsoft Azure, port 25 is blocked by the provider. However, port 25 is required for sending emails, and port 25 being blocked prevents NoSpamProxy from operating on such a system.

We offer a solution in the form of our *TCP proxy*. This system can be activated in NoSpamProxy as described below. Each outbound connection is routed to a routable IPv4 address on the TCP level through the TCP proxy for NoSpamProxy. The emails will be sent from the server via port 443 to the TCP proxy and from there via port 25 to the recipient system.

1. Stop the Gateway Role via the NoSpamProxy console or the Windows services.
2. Open a text editor using administrative rights on the system where the Gateway Role is installed.
3. Open the configuration file "**Gateway Role.config**" from the directory **C:\ProgramData\Net at Work Mail Gateway\Configuration**.

4. Search the file for `<smtpServicePointConfiguration>` and change/add the value

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

as attributes . If `<smtpServicePointConfiguration` is not present, search for `<netatwork.nospamproxy.proxyconfiguration` and add

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

directly under this value.

5. Save the file and close the editor.
6. Place the **Root CA certificate** in the Microsoft certificate store in the computer account under **Trusted Root Certification Authorities > Certificates** on the server with the Gateway Role.
7. In the NoSpamProxy Command Center under **Configuration > NoSpamProxy components > Gateway Roles** edit the appropriate gateway role and change the value for **SMTP Server Name** to the value `outboundproxy.nospamproxy.com`.
8. Restart the Gateway Role.
9. Open the **Gateway Role.config** file again and check whether the value was retained at startup.

I Adjusting the SPF entry

- If the TCP proxy is implemented, it acts as the sending system. Thus, the TCP proxy must also be included in your SPF record. We strongly recommend adding the following entry to your SPF record:

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

I If applicable: Customising Office 365

If you send emails from Azure to your own Office 365 instance where a connector is bound to the IP addresses, please update the IP addresses to match the name `outboundproxy.nospamproxy.com`. Since with Office 365 the TLS certificates are checked against the HELO domain, it is only possible to implement this accordingly with significantly increased effort. We therefore recommend validation by name.

I If necessary: Adjust the firewall

- If you specifically block outgoing connections, you should adjust the exception for the TCP proxy so that connections to the **IP network 193.37.132.0/24** are allowed.

I Setting up a static IP address

If you want to run NoSpamProxy or parts of it in a virtual machine in a Microsoft Azure environment, you must have an IP address that is retained even after the machine is restarted. To achieve this, you must set up a static IP address (reserved

IP address). Otherwise, it is possible that a different IP address will be assigned after the machine is restarted.



NOTE: You make this setting on the Microsoft Azure virtual machine where NoSpamProxy is installed.

1. Open the web portal.azure.com.
2. Under **Home > Virtual Computers**, click the virtual computer where NoSpamProxy is installed.
3. Go to **Network > Network interface > IP configurations** and select the configuration relevant for NoSpamProxy.
4. Enable the **Public IP address** option and then click **Create new**.
5. Enter a name and select the **Static** option.
6. Click **OK**.

The IP address is now displayed under the specified name.



NOTE: Also note the instructions on the corresponding [page of the Microsoft Azure documentation](#).

| Customizing the Reverse DNS Entry for the NoSpamProxy Server

1. Go to portal.nospamproxy.com.
2. Go to **Dashboard > Resource Groups > [TheResourceGroupTheVirtualComputerBelongsTo] > [YourVirtualComputer] > Properties**.

3. Enter a name for the public IP address under **DNS name label**.
4. Start the Azure Shell.
5. Enter the following command, replacing the placeholders:

```
az network public-ip update --resource-group [ResourceGroup] --name  
[IPAddressName] --reverse-fqdn [FullDNSName] --dns-name [DNSName]
```



NOTE: Also note the instructions on the corresponding [page of the Microsoft Azure documentation](#).

Help and support

Knowledge Base

The [Knowledge Base](#) contains further technical information on various problems.

Website

The [NoSpamProxy website](#) contains manuals, white papers, brochures and other information about NoSpamProxy.

NoSpamProxy Forum

The [NoSpamProxy forum](#) gives you the opportunity to exchange information with other NoSpamProxy users, get tips and tricks and share them with others.

Blog

The [blog](#) offers technical support, tips on new product versions, suggestions for changes to your configuration, warnings about compatibility problems and much more. The latest news from the blog is also displayed on the start page of the NoSpamProxy Command Center.

YouTube

On our [YouTube](#) channel you will find tutorials, how-tos and other product information that will make working with NoSpamProxy easier.

NoSpamProxy Support

You can reach our support team

- by phone at [+49 5251304-636](tel:+495251304636)
- by email at support@nospamproxy.de.

