noSpamProxy® SERVER

Version 14

Integrating NoSpamProxy

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

Net at Work
Building IT-Excellence.

Legal information

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

THIS DOCUMENT WAS LAST EDITED ON MARCH 31, 2023.

Content

Introduction

Since version 10, NoSpamProxy® can be fully integrated into Microsoft Office 365. This manual describes the configuration steps both for NoSpamProxy and Office 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**.

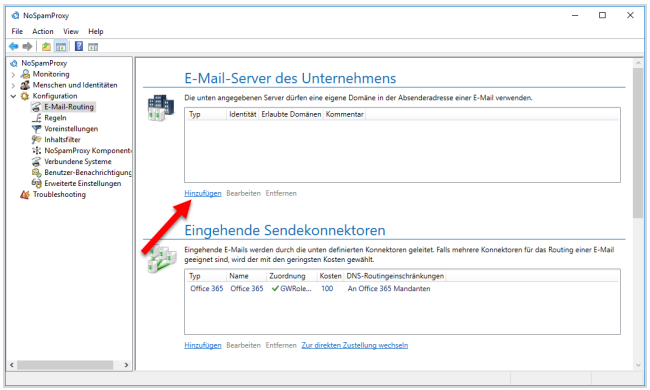
Enabling Office 365 as a relay host

In this step, you configure Office 365 in the NoSpamProxy®configuration as a relay host, enabling Office 365 to send emails to external communication partners through NoSpamProxy.

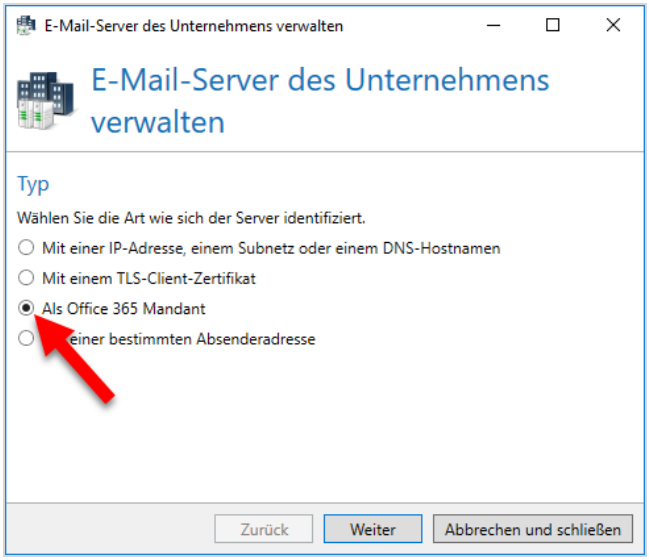
Without this configuration, NoSpamProxy will evaluate and reject emails as relay abuse attempts.

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

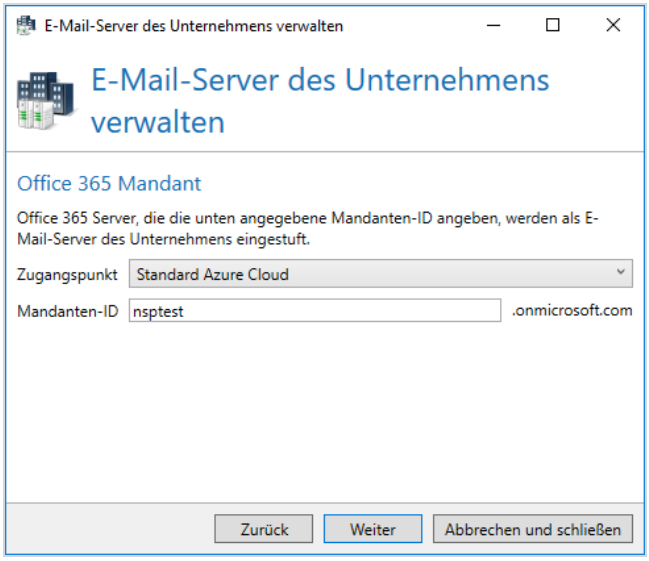
1. In the NoSpamProxy Command Center, go to **Configuration > Email Routing** and click **Add**.



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



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**.



6. Under **Assigned company** domains, select the domains that you have stored in Office 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**.

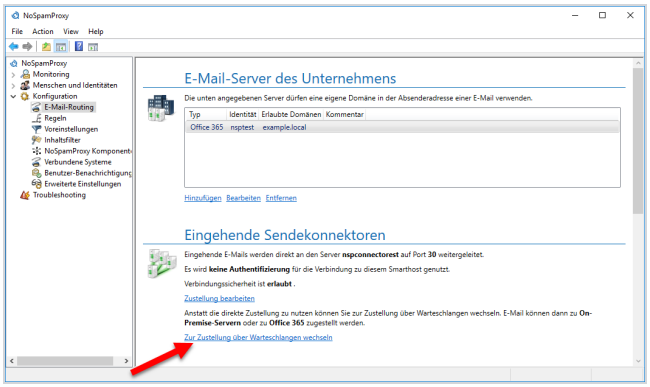
The email server is now created.

Setting up forwarding to Office 365

> **NOTE:** To set up forwarding to Office 365, a TLS certificate issued by a root certification authority trusted by Microsoft is required. 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® to forward all inbound emails to Office 365. To do this, you must edit the corresponding send connectors.

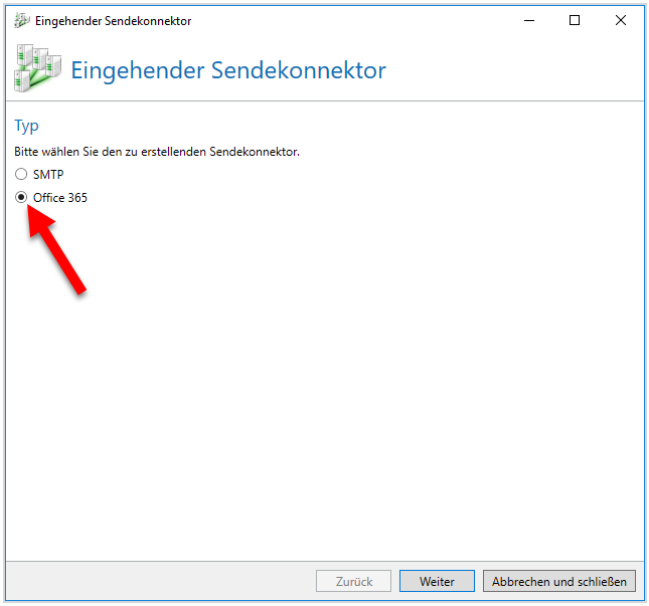
1. Go to **Configuration > Email routing**.
2. Under **Inbound send connectors**, click **Switch to queued delivery**.



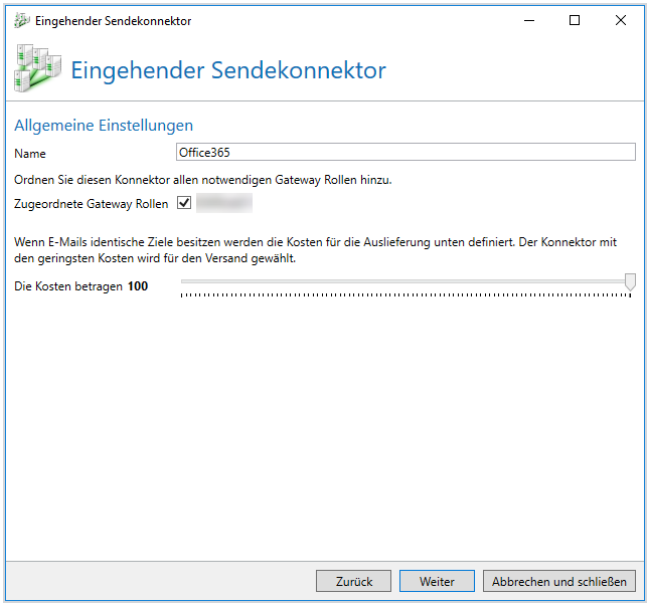
3. In the **Change Delivery** dialog, select **Replace delivery**.

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

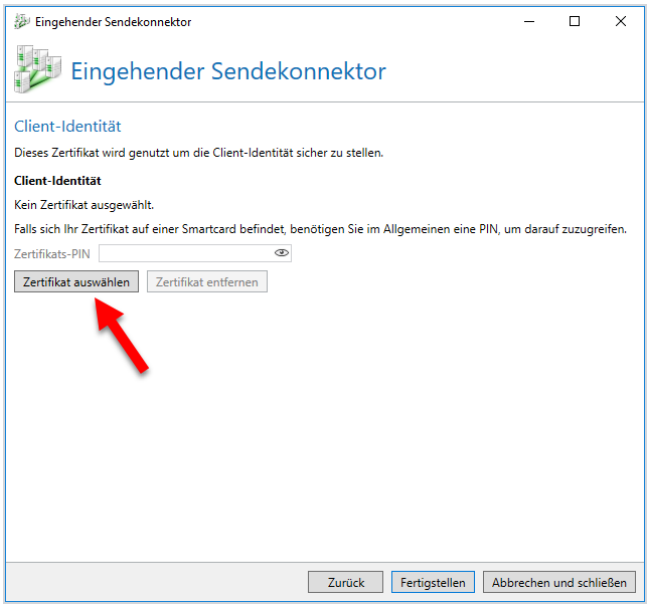
4. In the dialog box that appears, select **Office 365** and click **Next**.



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**.

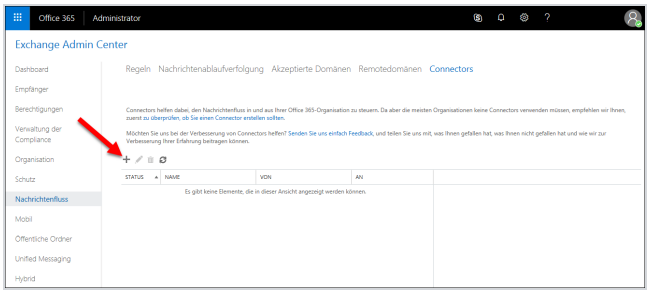
The configuration for NoSpamProxy is now complete.

Configuring Office 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 on to your Office 365 client at **https://outlook.office365.com/ecp**.

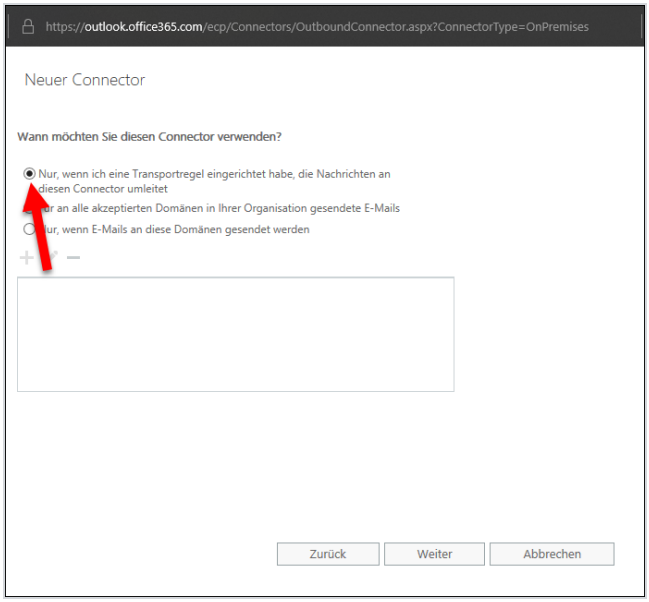
> **NOTE:** Use a user with administrative rights to log on.

1. In the Exchange Admin Center, go to **Mail flow > Connectors**; then click the **plus sign**. The wizard for creating a new connector opens.

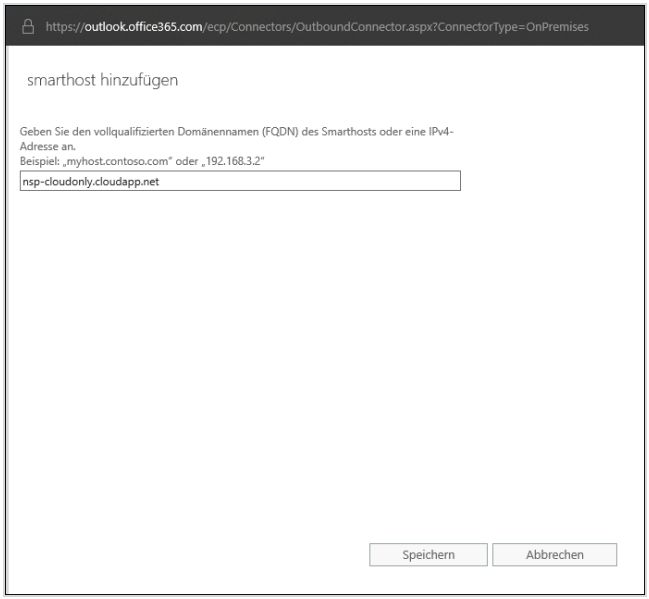


2. On the first page, in the field **From**, select **Office 365**; in the field **To**, select **Partner Organization**.
3. Click **Next**. This setting sends outgoing e-mail from the Office 365 client to NoSpamProxy.
4. On the following page, enter any name for the connector.
5. Enter a description if required and click **Next**.
6. On the following page, select the option **Only when I have a transport rule set up that redirects messages to this connector**.

7. Click **Next**.

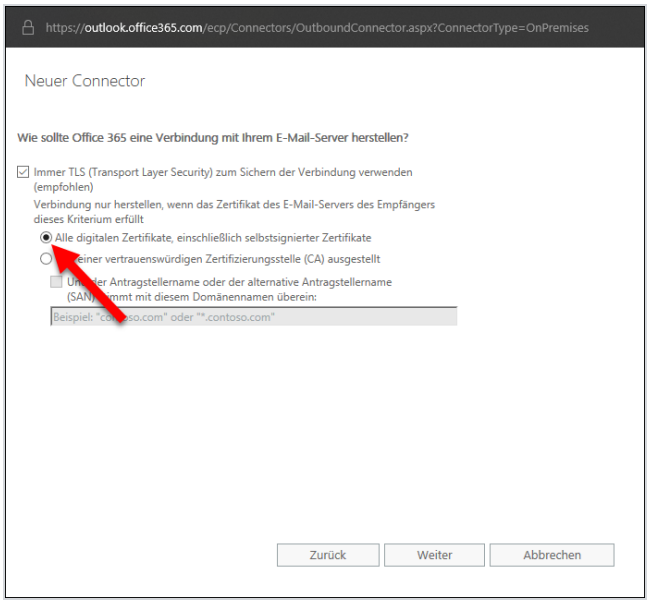


8. Specify the name or IP address of the server (smart host) where the Gateway Role is installed, then click **Save**.

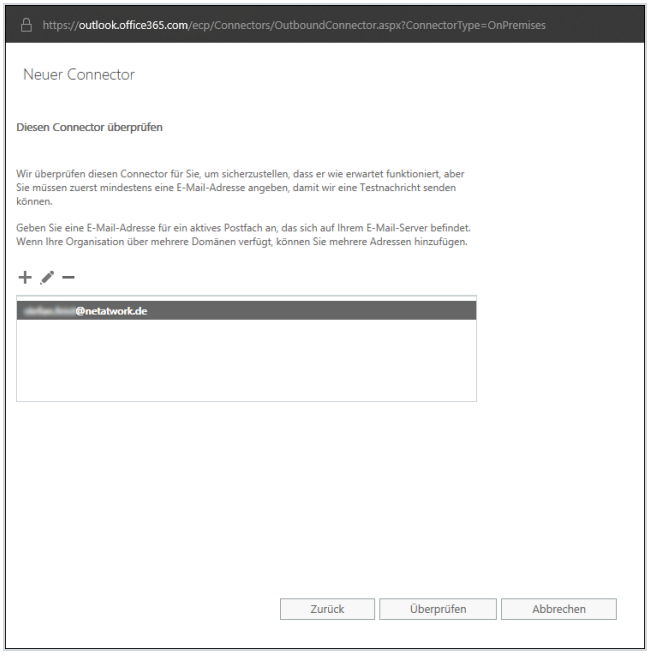


9. In the following dialog box, enable the option **Always use Transport Layer Security (TLS) to secure the connection (recommended)**. In the dialog box

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



10. Check the summary of your information for accuracy and click **Next**.
11. In the following dialog, enter one or more e-mail addresses that you want to use to verify this connector.



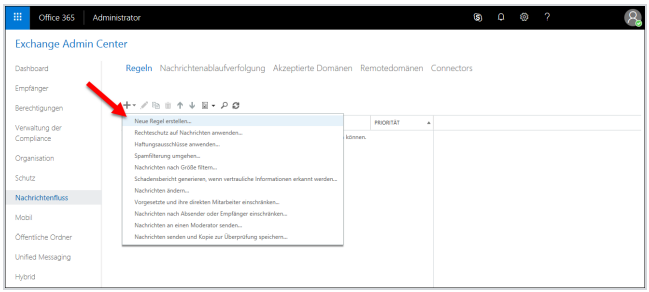
12. Click **Validate**.

> **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.

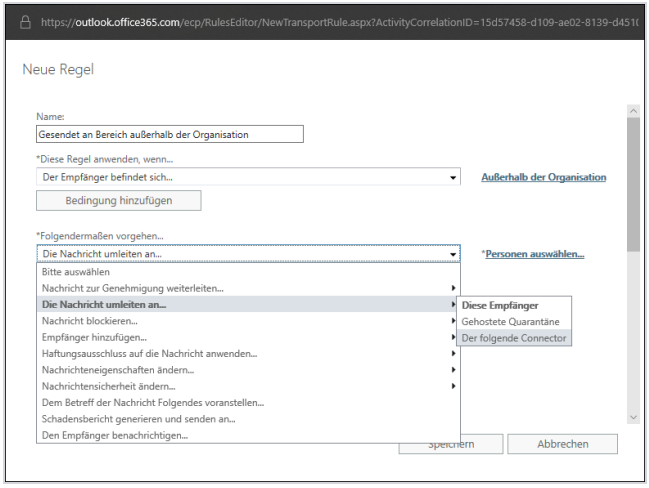
13. Click **Save** to close the dialog.

Creating the transport rule

1. From the Office 365 management interface, go to **Mail Flow > Rules**.
2. Click the **plus sign**.



3. Select Create a new rule. The wizard for creating a new transport rule opens.



4. Enter any name for the rule.
5. Under **Apply this rule if**, set the following options:
    - **The recipient is located** and
    - **Outside the organization**.
6. Under **Do the following**, select **Use the following connector**.

7. Then specify the previously created connector and click **OK**.

> **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.

8. Click **Save**.

Operating NoSpamProxy in Office 365 with Exchange Online

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

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:

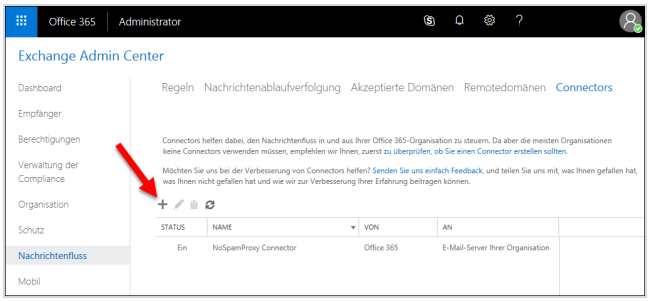
```
New-InboundConnector

-Name "AcceptOnlyEMailsFromThisServer<NoSpamProxy>"

-ConnectorType Partner

-SenderDomains *

-RestrictDomainsToCertificate $true

-TlsSenderCertificateName <TheCertificatePreviouslyCreatedAndSelected>

-AssociatedAcceptedDomains

<AllDomainsListedUnderCorporateDomainsAndUsedInTheOffice365Tenant>
```

WARNING: To ensure spam protection by NoSpamProxy®, you must route all inbound email traffic through NoSpamProxy and address Office 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.

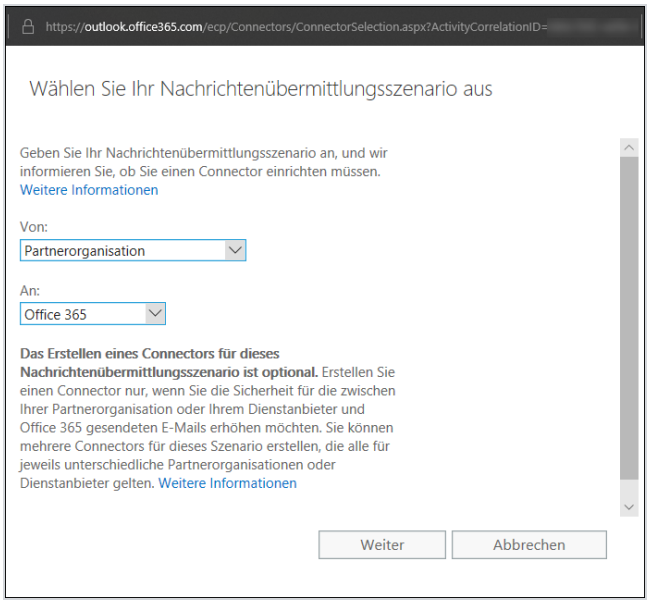
TIP: Instead of the IP address, you can also store the certificate of the supplying gateway.

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

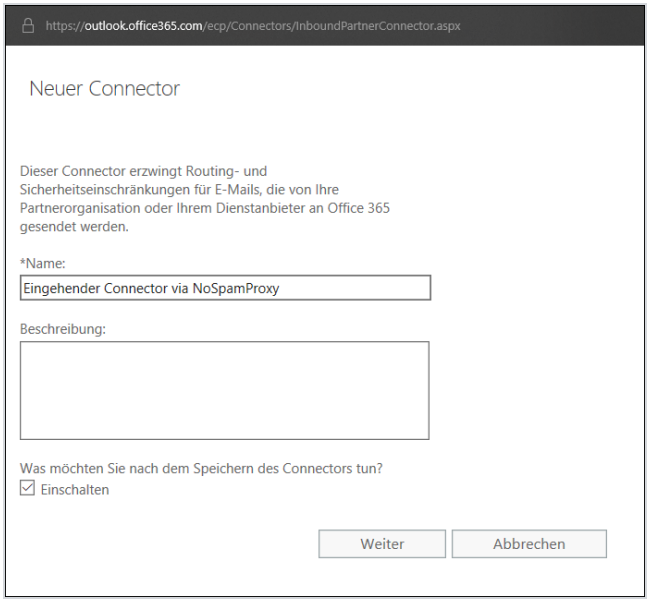
1. Go to **Mail flow > Connectors** and click the **plus**sign.



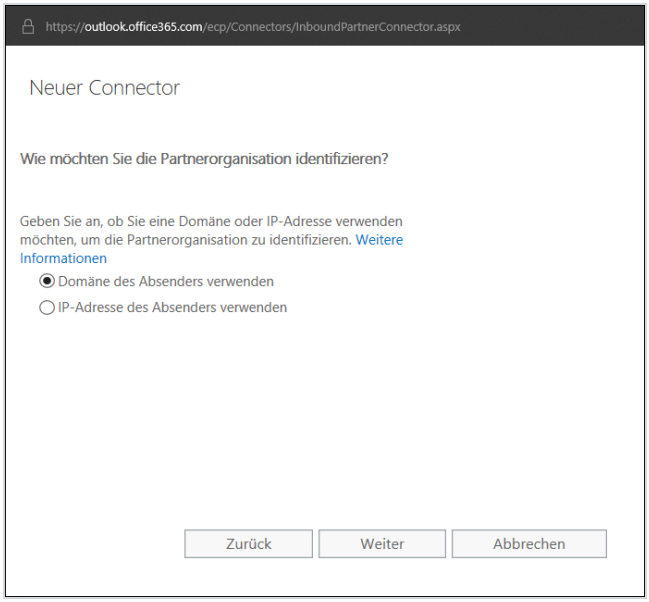
2. In the dialog box, select **Partner organization** and **Office 365**, and then click **Next**.



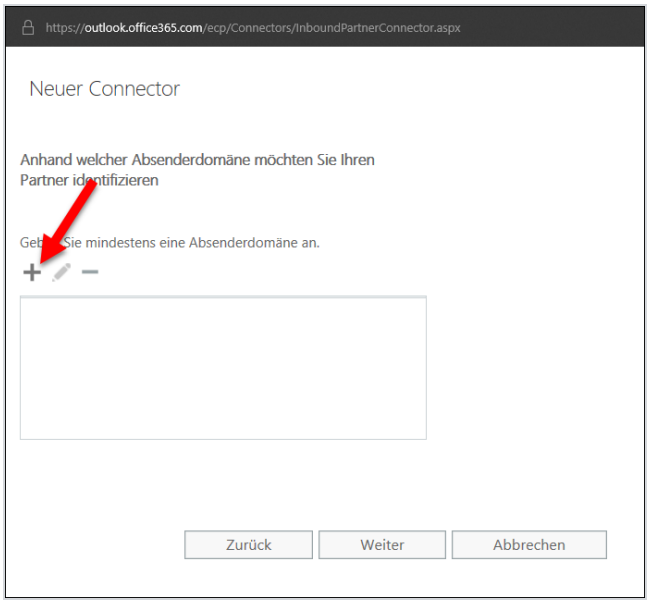
3. In the **New Connector** dialog, enter a name for the connector and add a description if required. Leave the check mark next to **Switch on**. Then click **Next**.



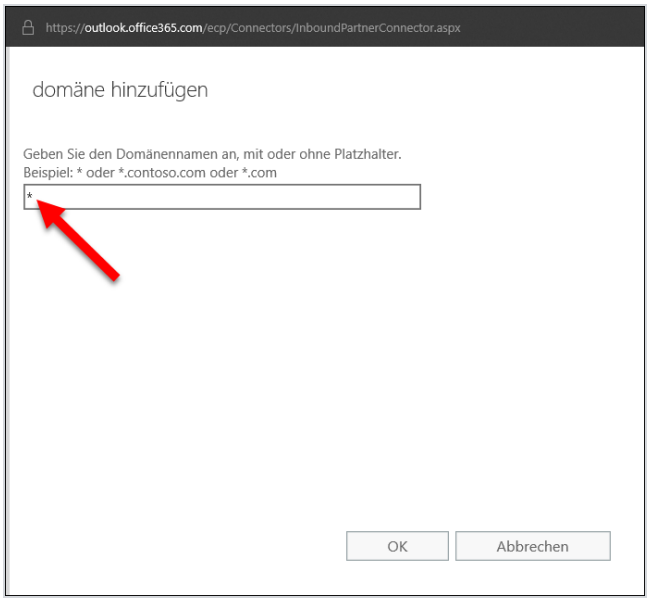
4. In the following dialog box, select **Use the sender's domain** and click **Next**.



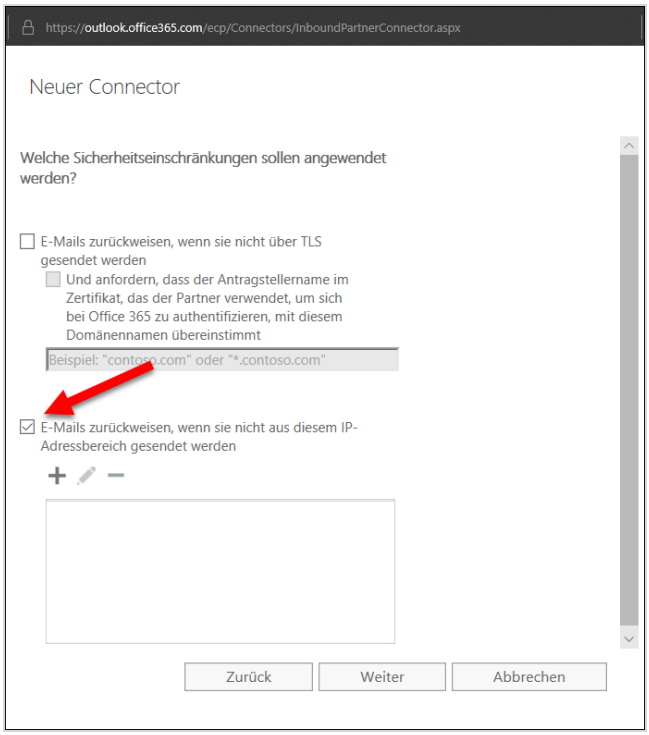
5. Click the **plus**sign in the following dialog box.



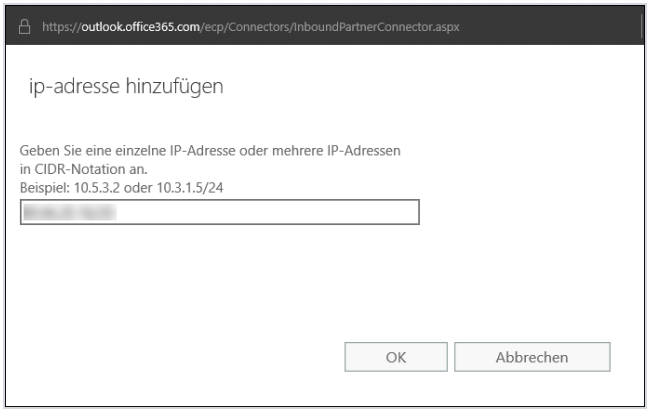
6. Enter an asterisk ("*") as the domain name. Then click **OK** and on the following page **Next**.



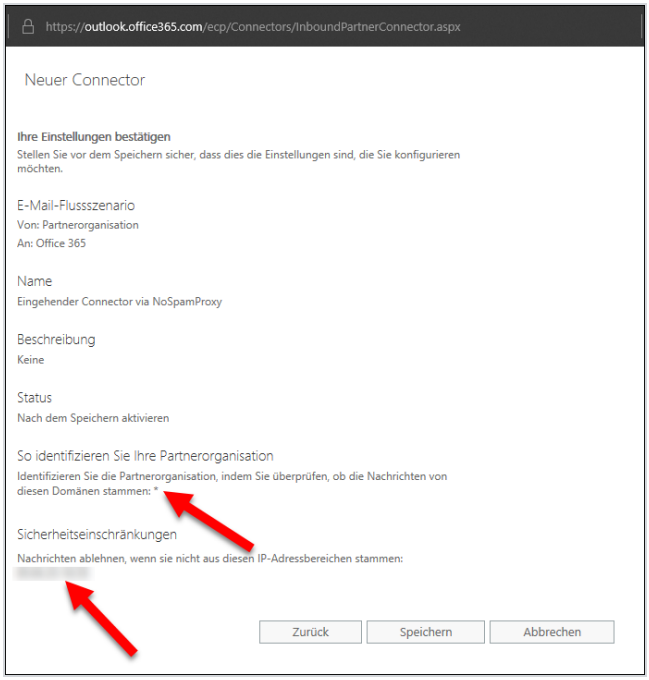
7. On the following page, tick the check box Reject **email messages if they aren't sent from within this IP address**. Click **Next**.



8. In the dialogue **Add IP address**, enter the address of the server on which the gateway role is installed. Click **OK**.



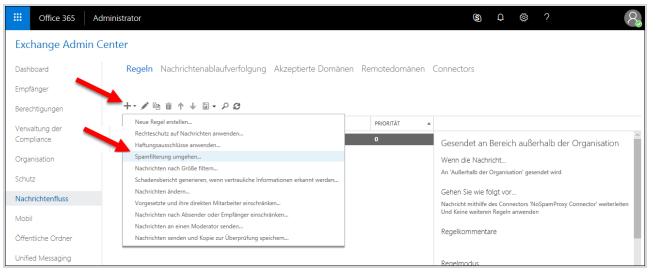
9. Verify that the information in the summary is correct and click **OK**.



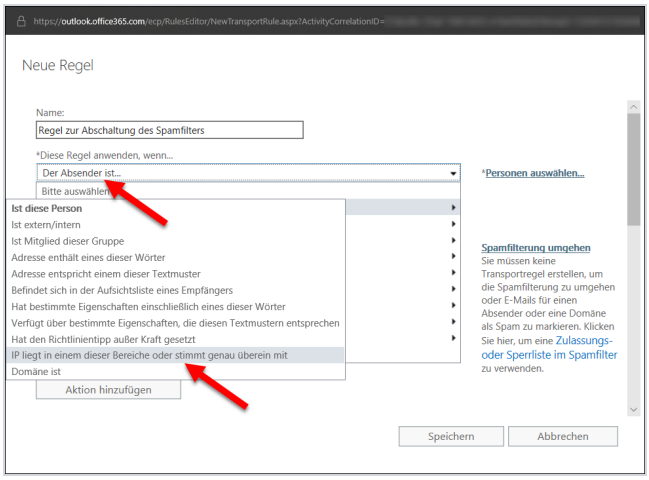
The new connector now appears under **Mail flow > Connectors**.

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

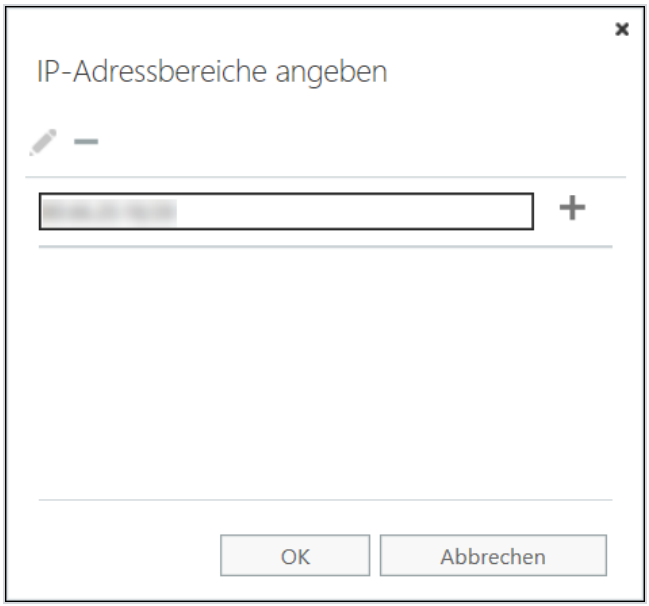
1. Go to **Mail flow > Rules**.
2. Click the **plus**sign .
3. Select **Bypass spam filtering** from the drop-down menu.
4. Give the rule a name.



5. Under **Apply this rule if** select if the option **Sender** and then **IP is in any of these ranges or exactly matches**.



6. In the **Specify IP address ranges** dialog, specify the IP address of the server on which the Gateway Role is installed.



7. Click the **plus** sign and then click **OK**.
8. Click **Save**.

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

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 outgoing 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.

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
```

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.

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.

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 **page 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**
- by email at **support@nospamproxy.de**.