



Version 15

Integrating NoSpamProxy Encryption

- 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	9
Creating the transport rules	14
Necessary configurations for the operation in Microsoft Azure	18
Help and support	23

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

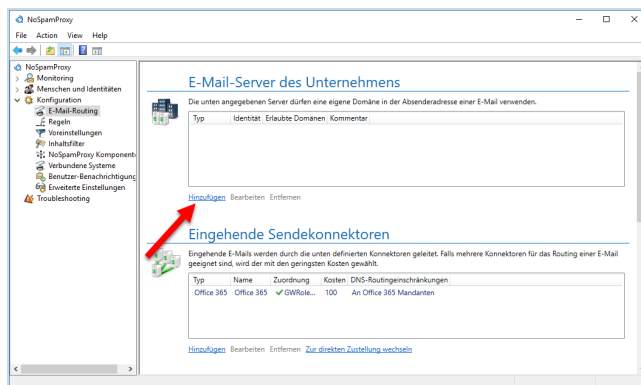
In this step, you allow Microsoft 365 to be used as a relay host in the NoSpamProxy® configuration so that emails can be sent from Microsoft 365 to external communication partners through NoSpamProxy.

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

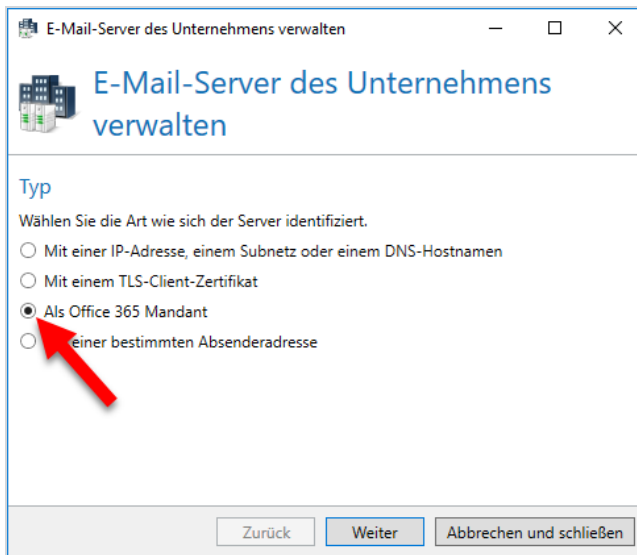


NOTE: Make sure that you have set up at least one corporate domain before you start the configuration.

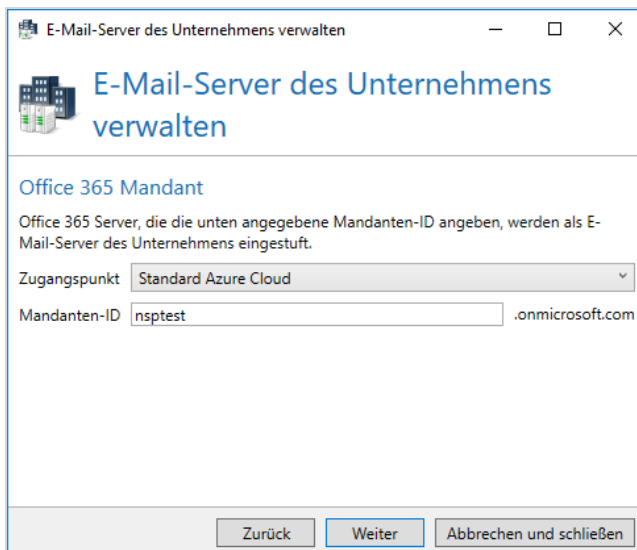
1. In the NoSpamProxy Command Center, go to **Configuration > Email Routing** and click **Add**.



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



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. 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**.

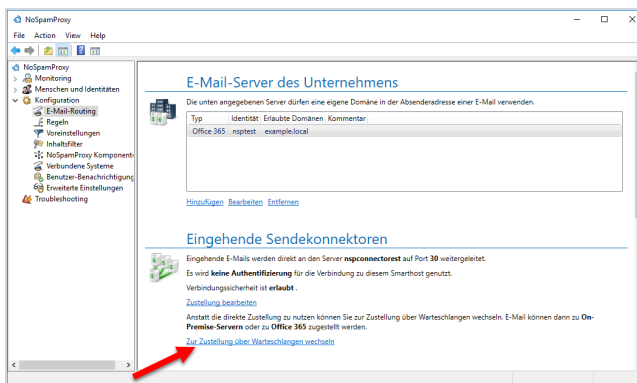
The email server has been created.

Setting up forwarding to Microsoft 365

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

Creating the inbound send connector

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

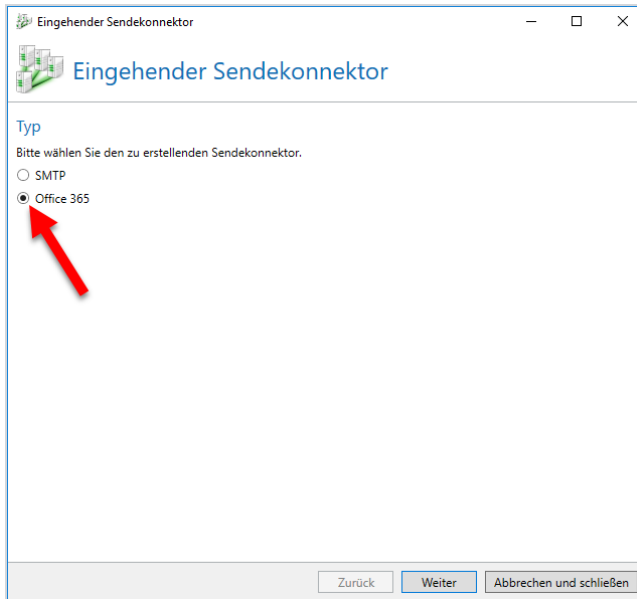


3. In the **Change delivery** dialog, select **Replace delivery**.



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**.

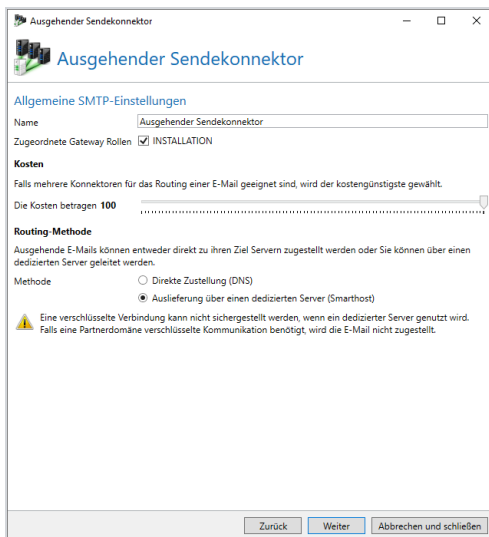


5. Type any name for the inbound send connector, and then select the Gateway Role(s) that you want to process emails to Office 365.
6. Click **Next** and then **Finish**.

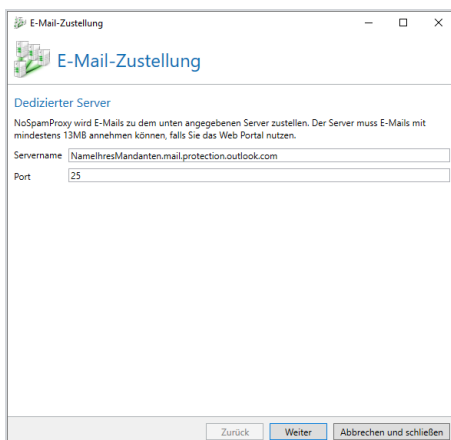
■ Creating the outbound send connector

1. Go to **Configuration > Email routing**.
2. Under **Outbound send connectors** click **Add**, select **SMTP** and click **Next**.

3. Enter any name for the outbound send connector, then select the Gateway Role(s) to process outbound emails and determine the cost.



4. Under **Routing method** select **Delivery via a dedicated server (smarthost)** and click **Next**.
5. Under **Delivery** click on **Add** and enter the appropriate name as the server name using the pattern **NameYourClient.mail.protection.outlook.com**



6. Select the option **Do not use authentication** and click **Next**.

7. Determine the connection security, select a certificate if necessary and click **Finish** and then **Next**.
8. Leave the setting under **DNS routing restrictions** as they are.
9. Click **Finish**.

The configuration for NoSpamProxy is now complete.

Configuring Microsoft 365

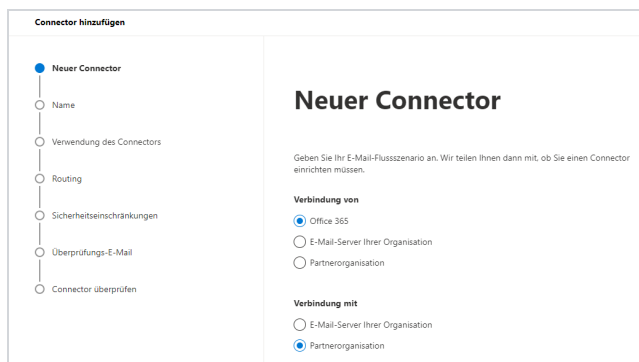
Creating a connector for outbound emails

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.



Connector hinzufügen

Neuer Connector

Name

Verwendung des Connectors

Routing

Sicherheitseinschränkungen

Überprüfungs-E-Mail

Connector überprüfen

Neuer Connector

Geben Sie Ihr E-Mail-Flusszenario 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. 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**.

Connector hinzufügen

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

Verwendung des Connectors

Geben Sie an, wann Sie diesen Connector verwenden möchten.

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

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**.

Connector hinzufügen

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

Routing

Wie möchten Sie E-Mails weiterleiten?

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.

MX-Eintrag verwenden, der der Domäne des Partners zugeordnet ist

E-Mail über die diese Smarthosts weiterleiten

Beispiel: myhost.contoso.com oder 192.168.3.2



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 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 'Fügen Sie den Betreffnamen oder alternativen Betreffnamen (SAN) hinzu, der diesem Domänennamen entspricht:' and an example: 'Beispiel: "contoso.com" oder "*.contoso.com"'. The 'Überprüfungs-E-Mail' step in the navigation pane is currently unselected.

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 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 is a text input field containing the example email address 'Beispiel: benutzer@contoso.com' and a blue '+' button to the right. Below the input field is a 'Überprüfen' button. The 'Sicherheitseinschränkungen' step in the navigation pane is currently unselected.

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.

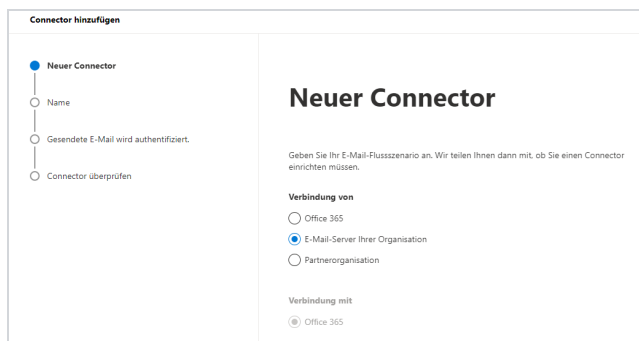
Creating a connector for inbound emails

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, in the **From** field, select **Your organization's email server**; in the **To** field, select **Office 365**



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



NOTE: Be sure to uncheck the box next to **Keep internal Exchange email headers**.

5. On the following page, select the option **By checking whether the IP address [...]**, enter the IP address of the NoSpamProxy server and click the **plus sign**.

Connector hinzufügen

- Neuer Connector
- Name
- Gesendete E-Mail wird authentifiziert.**
- Connector überprüfen

Gesendete E-Mail wird authentifiziert.

Wie soll Office 365 E-Mail von Ihrem E-Mail-Server identifizieren?

Wählen Sie aus, wie Office 365 E-Mails authentifiziert und akzeptiert, die von Ihrem E-Mail-Server gesendet werden.

Durch Überprüfen, ob der Antragstellername des Zertifikats, mit dem der sendende Server die Authentifizierung bei Office 365 vornimmt, mit dem Domänennamen übereinstimmt, der im Textfeld unten eingegeben wird (empfohlen)
Beispiel: "contoso.com" oder "*"contoso.com"

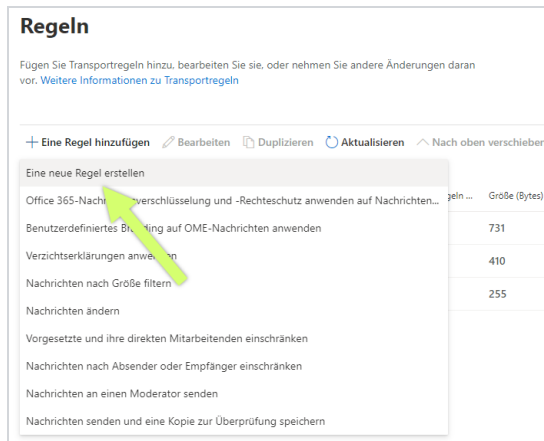
Durch Überprüfen, ob die IP-Adresse des sendenden Servers mit einer der folgenden IP-Adressen übereinstimmt, die exklusiv zu Ihrer Organisation gehören
Beispiel: 10.5.3.2 oder 10.3.1.5/24

6. Click **Next** and then **Save**.

Creating the transport rules

Creating the outbound 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 for outbound emails and click **Save** and then **Next**.



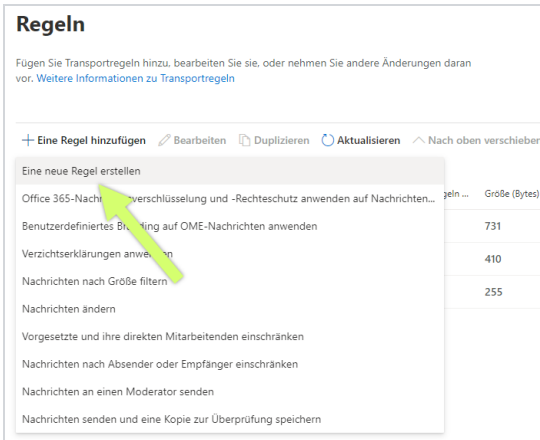
NOTE: If you can only select **persons** at this point, click **More options**. There you can select the option **Use the following connector** under **Redirect the message to**. You can then use the connector you created earlier.

7. Set the following options under **Except if**:
 - **The sender**
 - **IP is in one of these ranges or exactly matches**
8. Add the IP address used by NoSpamProxy and click **Add**, **Save** and then **Next**.
9. Click **Save**.

| Creating the inbound transport rule

1. In the Office 365 administration interface, 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**
- **Inside the organization**

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

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

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

7.



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**. Afterwards you can use the connector you created before.

8. Set the following options under **Except if**:

9. **The sender**

10. **IP is in one of these ranges or exactly matches**

11. Add the IP address used by NoSpamProxy and click **OK**.

12. Click **Save**.

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.

