BULLPHISH ID

Microsoft Office 365 Whitelisting Guide

Microsoft 365 Defender Third PartyPhishing
Simulation Configuration

Section	Details	Date of Change
Section B Step 11-14 Point 2:	Steps added for the routing setup Added a	November 16th, 2021
Sending Domains	new SMTPserver “34.237.252.20” to improve email deliverability. Added a new SMTP server to Fix	November 29th, 2021
Section 3	email delivery issues for errorcode "451 4.7.50 Server is Busy" in Exchange Online Exporting Sending Domains links updatedOld URL “*.secureawareness.net	January 27th, 2022
Section 2, Step 5	/*” replaced with “*.cloudsurveillance.net	January 28th, 2022
Section 2, Simulation URLsto allow	~~/*“~~	~~February 10th, 2022~~

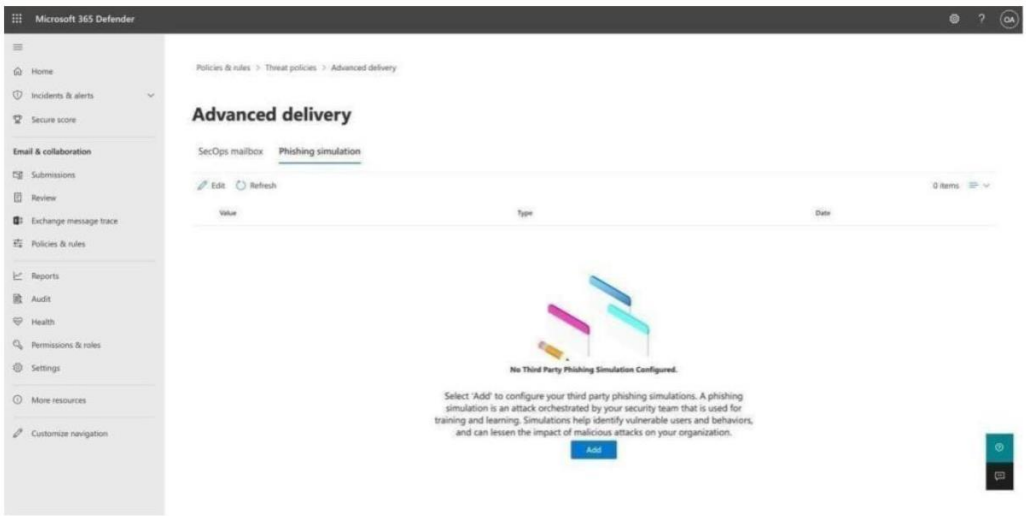
Objective: This guide will help you configure the delivery of third-party phishing simulationsto Microsoft 365 Defender.

1. In the Microsoft 365 Defender portal, go to **Email & Collaboration** > **Policies & Rules** > **Threat policies** page > **Rules**section > **Advanced delivery**. Or follow the **link**.

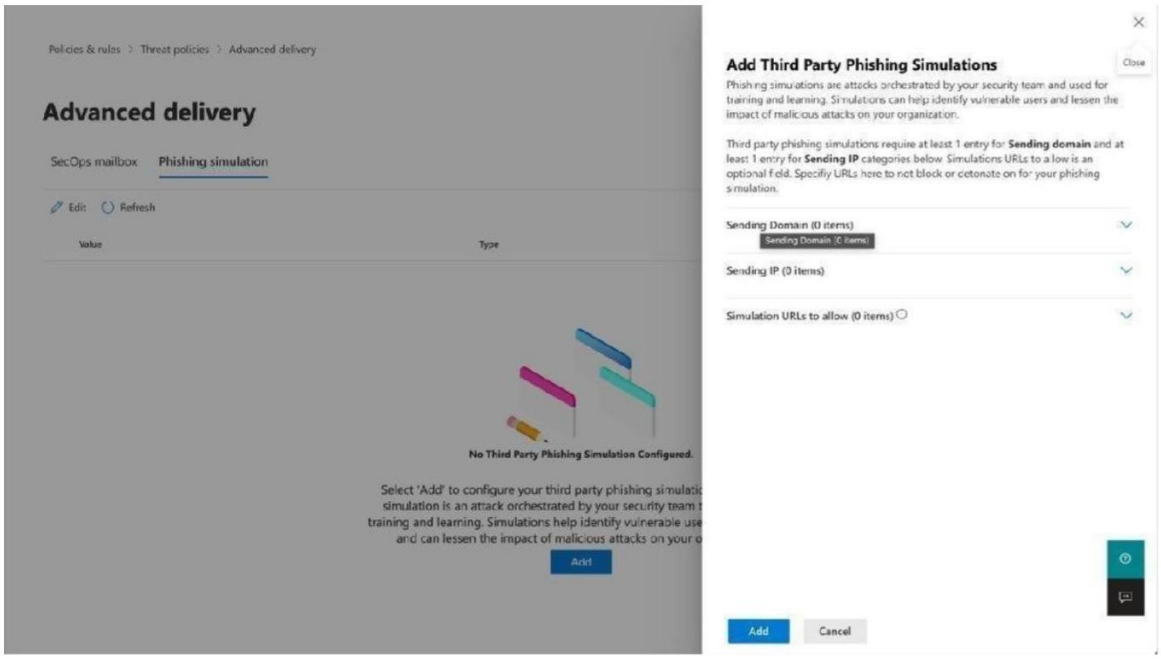
2. On the **Advanced delivery** page, select the **Phishing simulation** tab,and then do one of the following steps:

   Click **Edit**.

   If there are no configured phishing simulations, click **Add**



3. On the **Edit third-party phishing simulation** flyout that opens, configure the following settings:



- **Sending domain**:
  Pre-requisite: Please click on the following **link** to download the up-to- date list of sending domains. If you would like to manually download thefile, access Bullphish ID website under section **Guides & FAQ / Sending Domains.**

  Expand 'Sending Domain' setting and enter the sending domains available in the downloaded list from previous point by clicking in thebox, entering a value, and then pressing Enter or selecting the valuethat's displayed below the box. Repeat this step as many times as necessary.

- **Sending IP**: Expand this setting and enter IPv4 addresses below by clicking in the box, entering a value, and then pressing Enter or selecting the value that's displayed below the box. Repeat this step asmany times as necessary. You can add up to 10 entries. Values to be added are:
  - 168.245.13.192 (SendGrid IP - Needed for sending of notification emails)
  - 34.237.252.20 (New SMTP Server IP- Where we send Phishing &Training Emails from)
  - 54.211.230.155 (NAT gateway IP - IP address of background processes who initiate sending Phishing & Training Emails)
  - 18.223.13.154 (Fallback - Secondary IP)
  - 3.18.16.105 (Fallback - Secondary IP)
  - 3.18.67.92 (Fallback - Secondary IP)
  - 3.17.244.221 (Fallback - Secondary IP)

- 3.18.32.205 (Fallback - Secondary IP

Simulation URLs to allow: Expand this setting and enter the following URLs by clicking in the box, entering a value, and then pressing Enter or selecting the valuethat's displayed below the box.

service-noreply.info/* bpidtr.com/*
.bpidtr.com/ *.cloudsurveillance.net/*

To remove an existing value, click remove  next to the value.

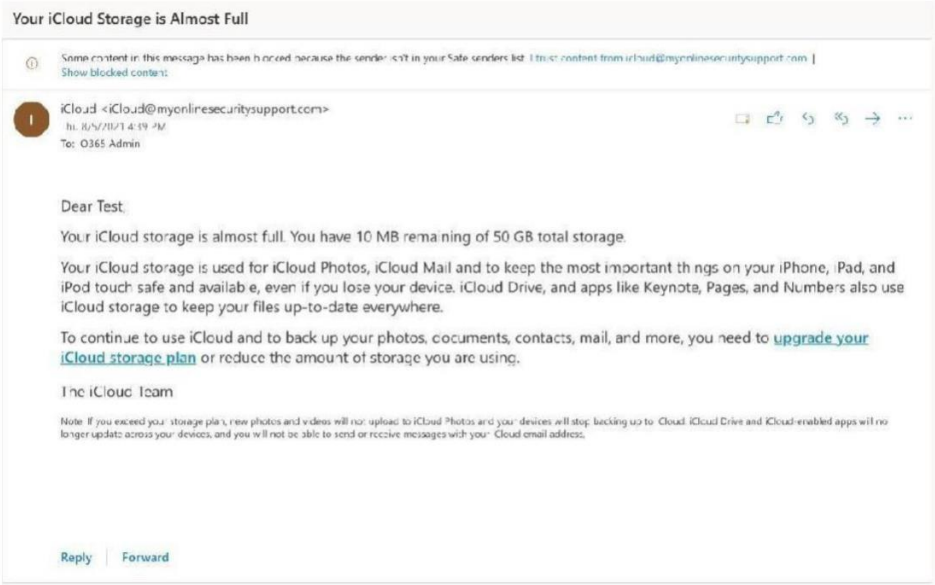
***Note:** You must specify at least one **Sending domain** and at least one **Sending IP** to configure a third-party phishing simulation in Advanced Delivery. You may optionally include **Simulation URLs to allow** to ensure URLs present in simulation messages are not blocked. You may specify up to 10 entries for each field. There must be a match on at least one **Sending domain** and one **Sending IP** but no association between values is maintained.*

When you're finished, do one of the following steps:
First time: Click **Add**, and then click **Close**.**Edit existing**: Click **Save** and then click **Close**.

The third-party phishing simulation entries that you configured are displayed onthe **Phishing simulation** tab. To make changes, click  **Edit** on the tab.

Prevent Outlook from blocking content in your emails and displaying a Safe Senders warning

Emails from domains that are not on the Outlook Safe Senders list may have a warning displayed on them, as well as some of the email content includingimages blocked.



To prevent the ‘Some content in this message has been blocked because thesender isn't in your Safe sender’s list' message from showing up, you will need to add BullPhish ID Sending domains to the Outlook Safe Sender lists ofeach of your end-users:

1. Open PowerShell.
2. Execute the following command if the ExchangeOnlineManagement module is not installed:

   ```
   Install-Module ExchangeOnlineManagement
   ```

3. Execute the following command to import the module:

   ```
   Import-Module ExchangeOnlineManagement
   ```

4. Connect to Exchange Online https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps

   ```
   Connect-ExchangeOnline -UserPrincipalName <UPN>
   ```

   Note: *<UPN> is your account in user principal name format (for example, navin@contoso.com).*

5. Execute the following script to add BullPhish ID Sending domains to the Outlook Safe Sender lists of each of your end-users. You will needto do this for each BullPhish ID Sending domain. The list of sending domains is available at the BullPhish website under section **Guides & FAQ / Sending Domains** or by **link**.

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All |
foreach {Set-MailboxJunkEmailConfiguration $_.Name -TrustedSendersAndDomains
@{Add="<domain>"}}
```

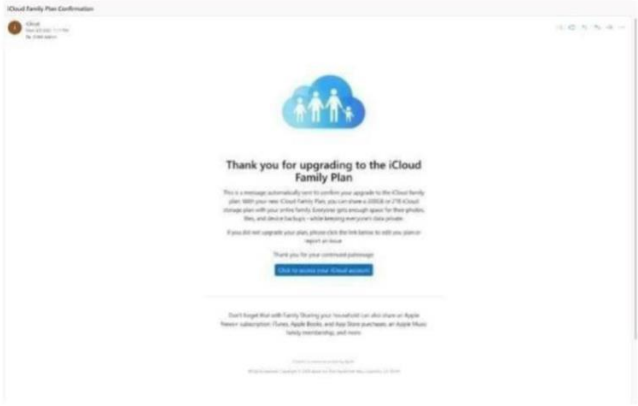
Note: *<domain> is BullPhish ID sending domain (for example, myonlinesecuritysupport.com).*

Example of the command for myonlinesecuritysupport.com domain:

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All |
foreach {Set-MailboxJunkEmailConfiguration $_.Name -TrustedSendersAndDomains
@{Add="myonlinesecuritysupport.com"}}
```

Important: You will need to run this script every time you add new users toensure all users have BullPhish ID Sending domains added to their Safe Senders list.

Enjoy the result:



6. Add command to add multiple domains:

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All
| foreach {Set-MailboxJunkEmailConfiguration $_.Name -TrustedSendersAndDomains
@{Add="<domain1>","<domain2>"...}}
```

Note: If user runs script 1 by mistake - listed in script domains will be added to Trusted Domains list. Emails from added domains will be passing spam filters. Or in case of wrong syntax script will throw error and nothing happened toTrusted Domains list.

Note: Domain names must be separated by comma, each domain must be double quoted. An example with 3 domains is below:

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All
| foreach {Set-MailboxJunkEmailConfiguration $_.Name -TrustedSendersAndDomains
@{Add="myonlinesecuritysupport.com","myonlinesecurity.com","bptr.net"}}
```

7. Add command to remove single domain:

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All
| foreach {Set-MailboxJunkEmailConfiguration $_.Name -
TrustedSendersAndDomains @{Remove="<domain1>"}}
```

Note: Domain name must be double quoted as below:

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All
| foreach {Set-MailboxJunkEmailConfiguration $_.Name -TrustedSendersAndDomains
@{Remove="myonlinesecuritysupport.com"}}
```

Note: If user runs this script by mistake, then listed in script domain will be removedfrom Trusted Domains list. Emails from removed domain will be filtered by spam filter.Or in case of wrong syntax script will throw error and nothing happened to Trusted Domains list.

8. Add command to remove multiple domains:

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All
| foreach {Set-MailboxJunkEmailConfiguration $_.Name -TrustedSendersAndDomains
@{Remove="<domain1>","<domain2>"...}}
```

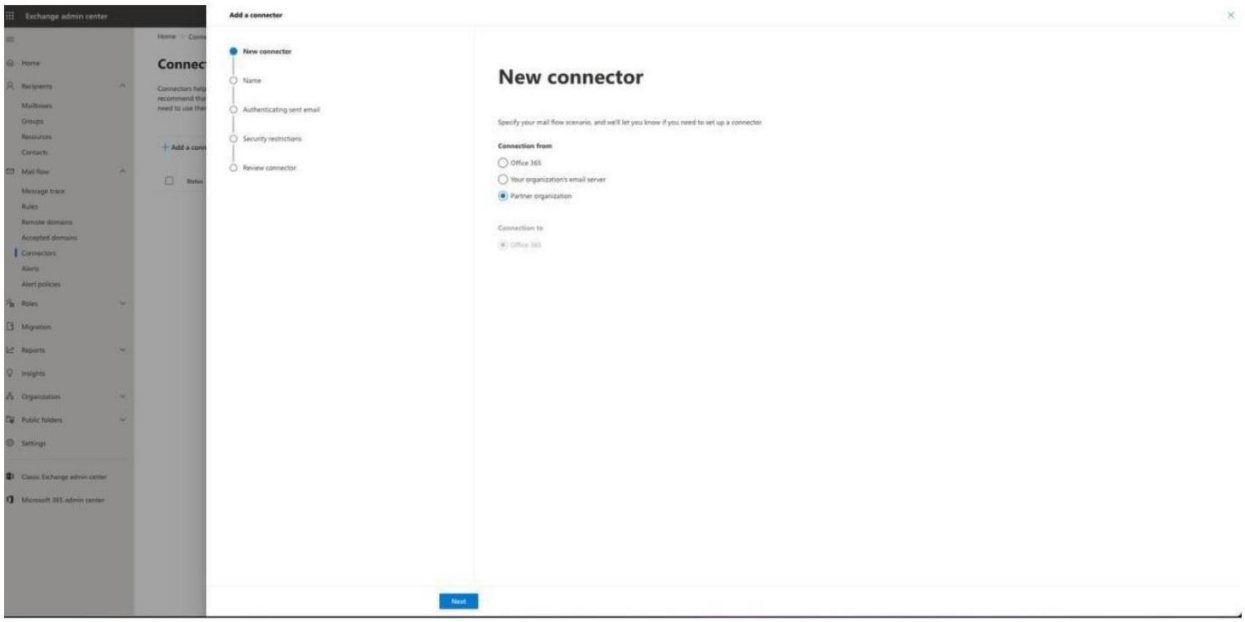
Note: Domain names must be separated by comma, each domain must be double quoted. An example with 3 domains is below:

```
$All = Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize Unlimited; $All
| foreach {Set-MailboxJunkEmailConfiguration $_.Name -TrustedSendersAndDomains
@{Remove="myonlinesecuritysupport.com","myonlinesecurity.com","bptr.net"}}
```

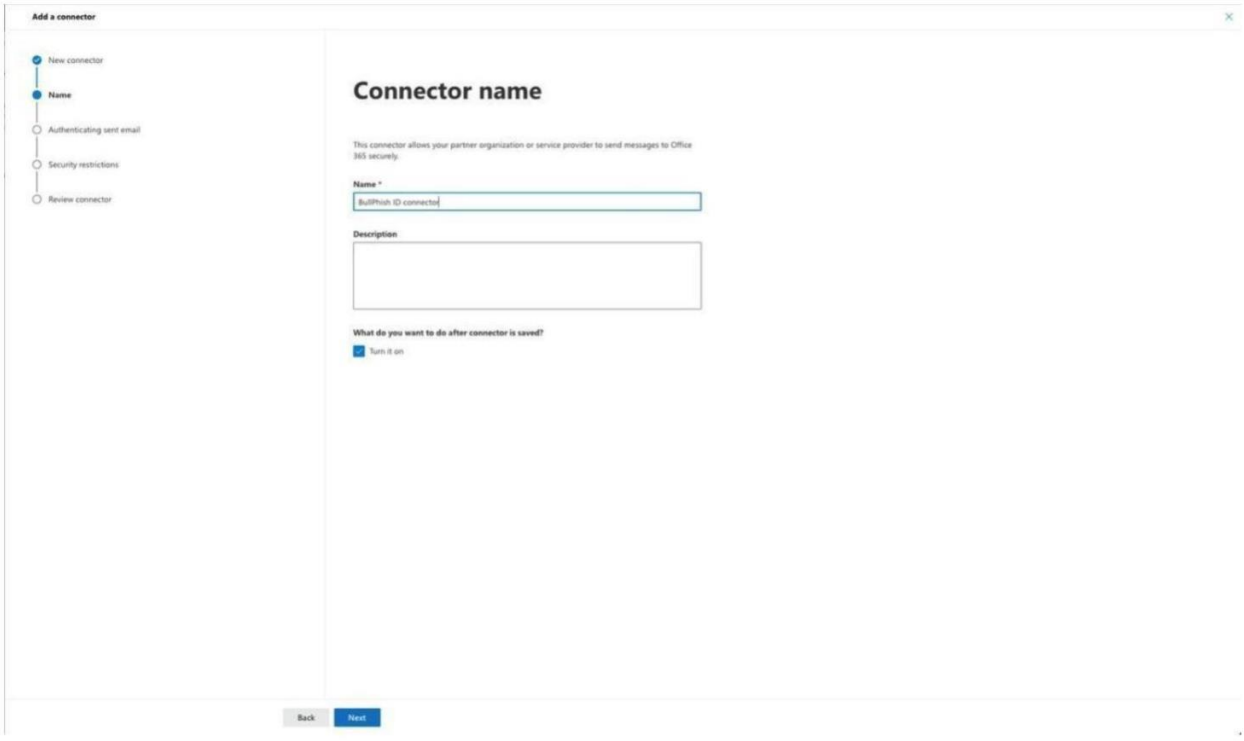
Note: If user runs this script by mistake, then listed in script domains will be removed from Trusted Domains list. Emails from removed domains will be filtered by spam filter. Or in case of wrong syntax script will throw error and nothing happened to Trusted Domains list.

Fix email delivery issues for error code "451 4.7.50Server is Busy" with the new SMTP server in Exchange Online

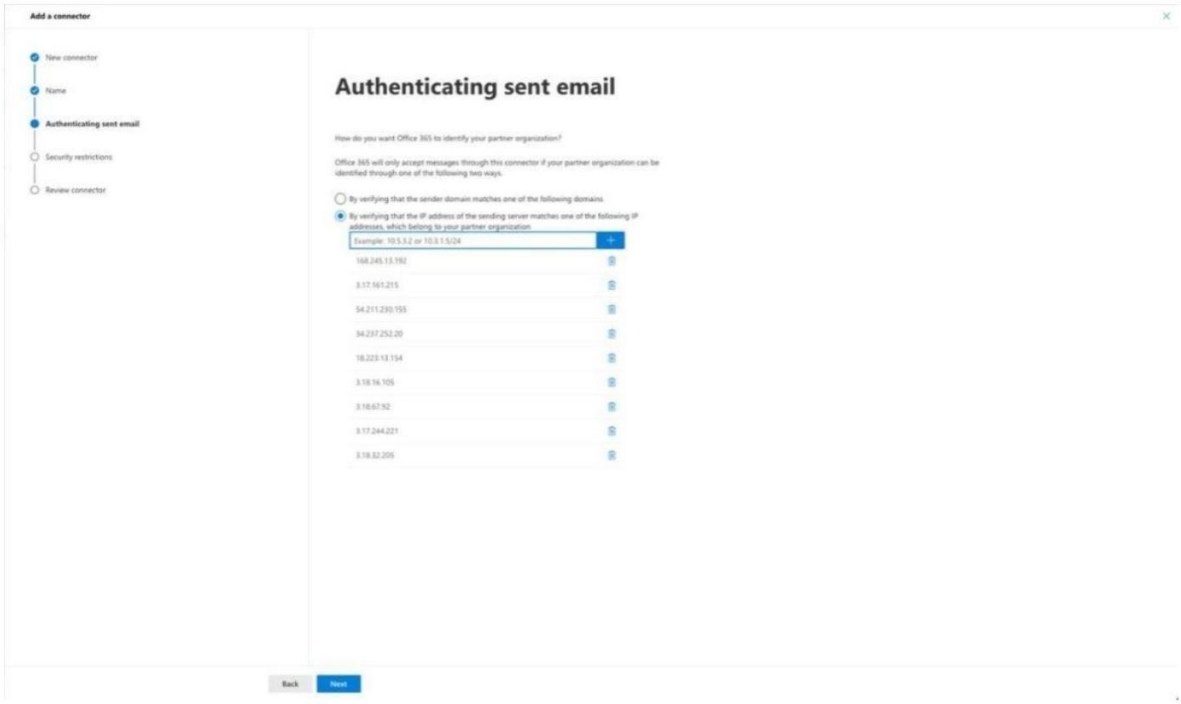
1. Log In to https://admin.exchange.microsoft.com/#/
2. Go to **Mail Flow → Connectors**
3. Click on the **“Add a connector”** button
4. In the window, choose “Connection From“ = “Partner organization“, and click on the“Next“ button



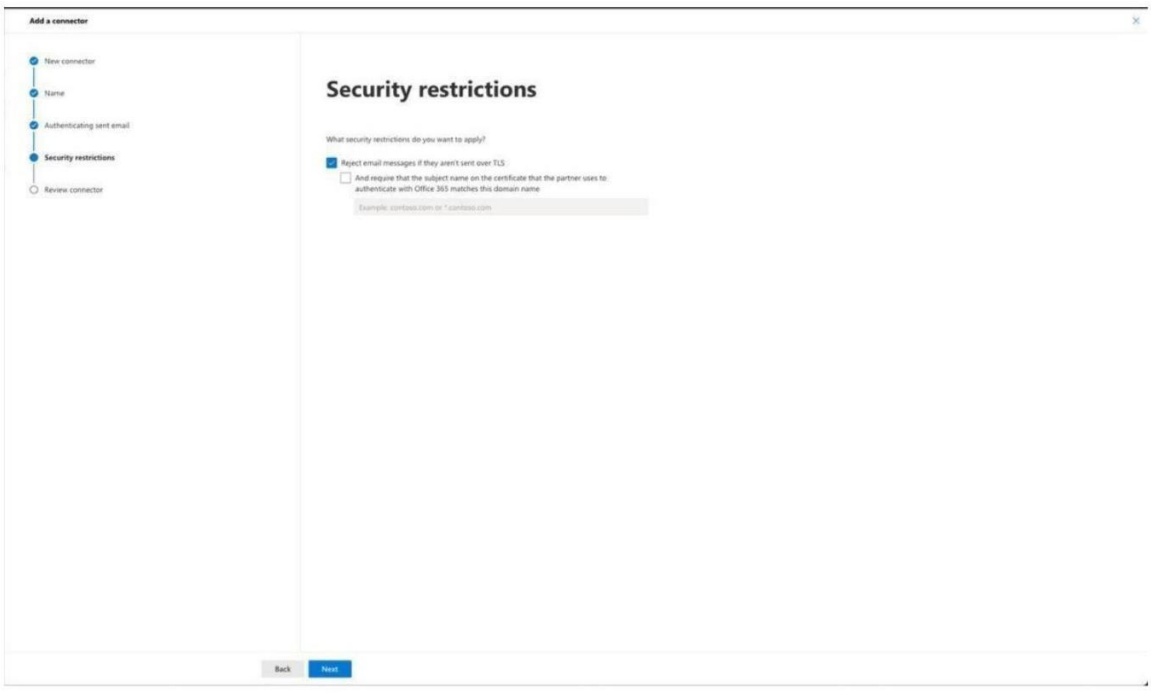
5. Enter the name of the connector. For example: “BullPhish ID” and click on the **“Next”** button



6. Choose “By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization” and add all BullPhish ID IP addresses Then click on the Next button



7. Choose **"Reject email messages if they aren't sent over TLS"**. Click on the “Next” button



8. Click on the “Create connector” button