O365 FAQs

- How to Whitelist by IP Address in Office 365 and by Domain in Microsoft Defender for Office 365 Portal - OLD

How to Whitelist by IP Address in Office 365 and by Domain in Microsoft Defender for Office 365 Portal - OLD

Why Whitelist in Office 365?

Whitelisting ensures the CyTech phishing simulation (PS) functions without issue and prevents PS emails from being automatically moved to the spam folder or notifying users about potential phishing emails. The Connection Filter Policy and Spam Filtering both required to be whitelisted.

Whitelist Connection Filter Policy

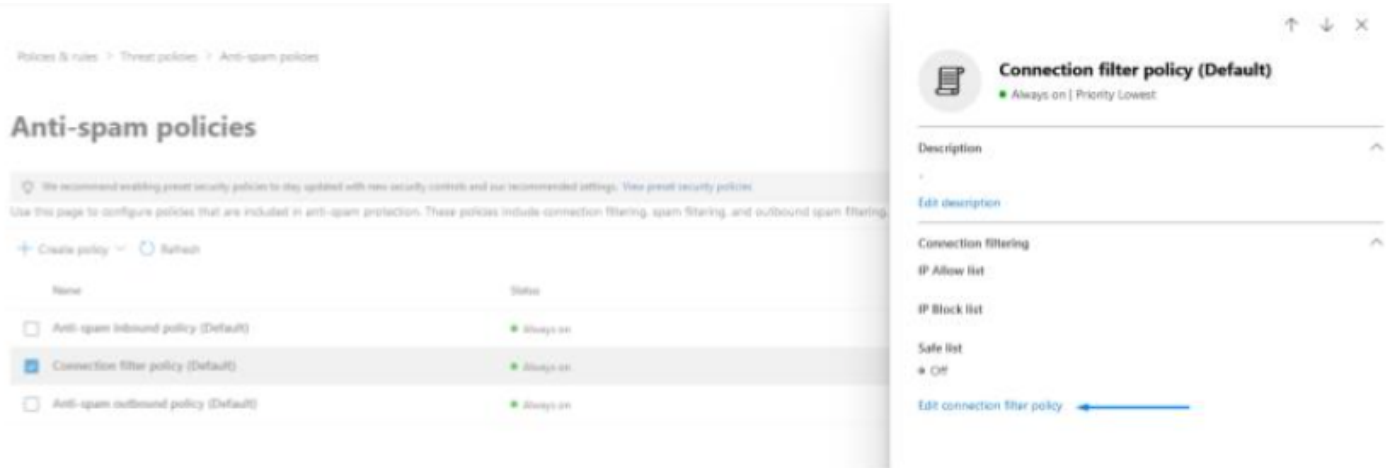
The Office 365 Exchange Connection Filter identifies good or bad source email servers by their IP addresses. The actions below will allow all emails from CyTech IP addresses to be received.

Whitelist the Connection Filter Policy

1. Go to the https://security.microsoft.com/antispam.

2. Click on "Connection filter policy".

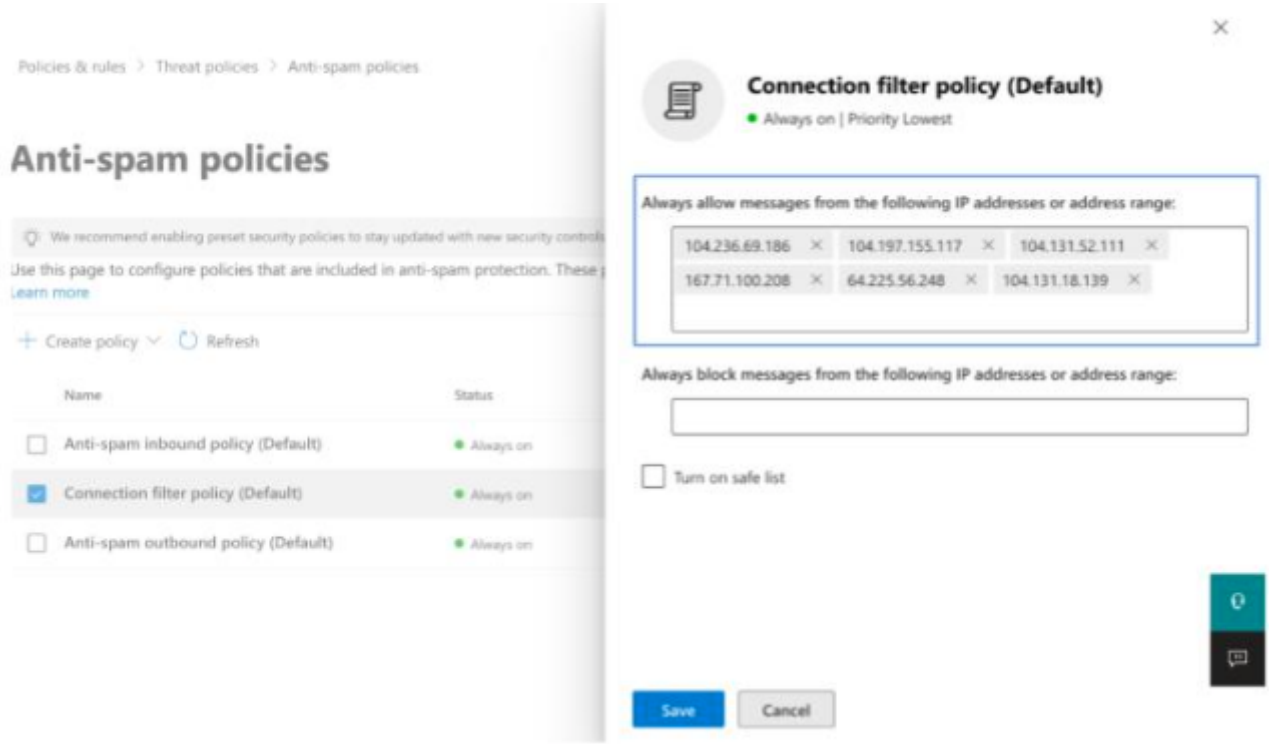
3. Then click on "Edit connection filter policy".



4. Add the IPs to the "Always allow messages from the following IP addresses or address range" input, one by one:

Allow IP: 35.153.237.243

5. Click on the "**Save**" button (refer to the screenshot below which depicts how the fields are populated with multiple IPs, the relevant list of IP addresses is always represented in the abovementioned list).



Allow IP: 35.153.237.243

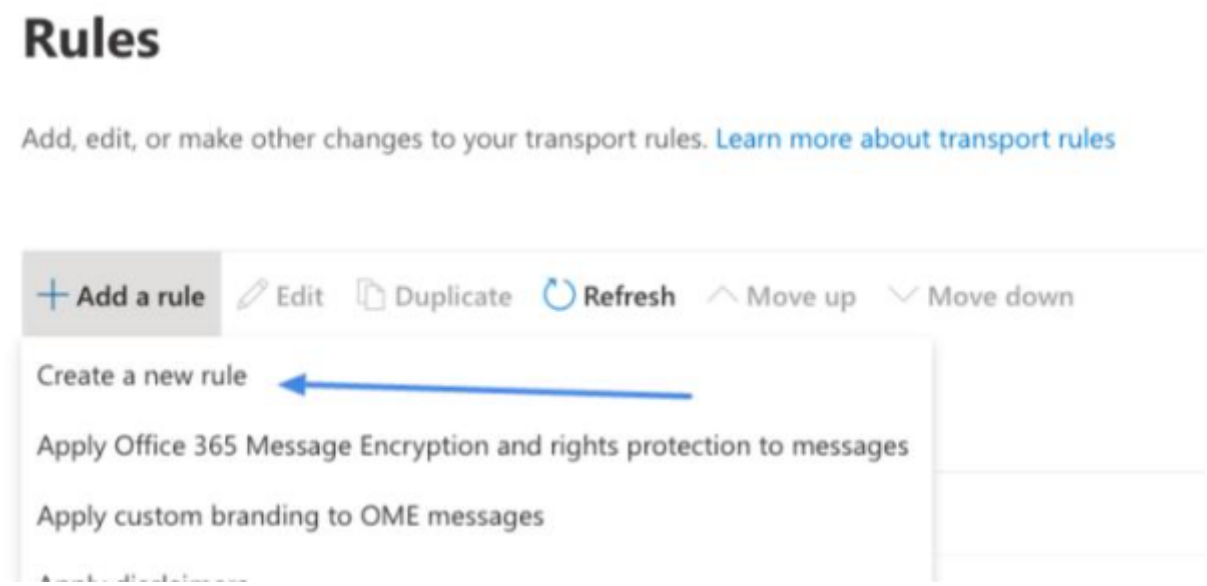
Whitelist Spam Filtering

All mail systems have spam filtering. As the CyTech PS emails are "phishing: by definition, the Microsoft spam filter must be whitelisted. The steps below outline how to disable all spam checks for CyTech PS emails, so you won't experience issues with 100% clicked and 100% opened emails, even if the users don't click on them.

Steps to Whitelist the Spam Filtering

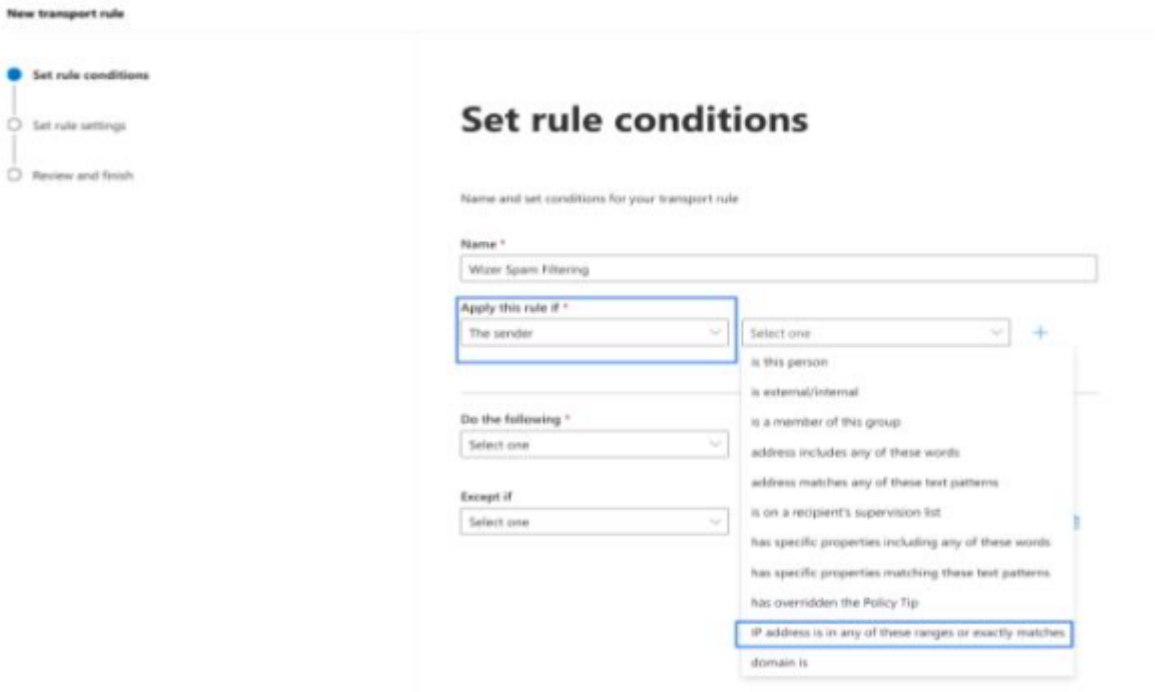
1. Go to the https://admin.exchange.microsoft.com/#/transportrules.

2. Click on the plus sign → "Create a new rule".

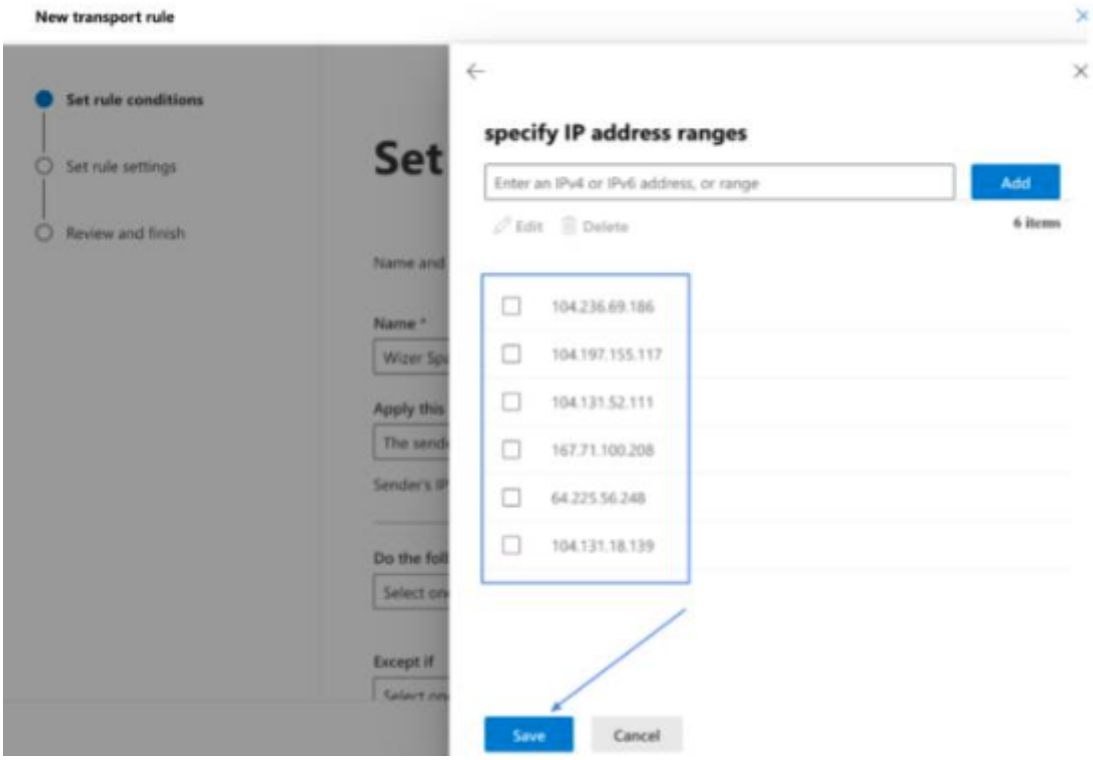


3. Give the rule a name, such as "CyTech Spam Filtering".

4. Click on "Apply this rule if → The sender → IP address is in any of these ranges or exactly matches".



5. Specify the IP addresses in the field IP: **35.153.237.243.** Please do not forget to click on **"Save".**



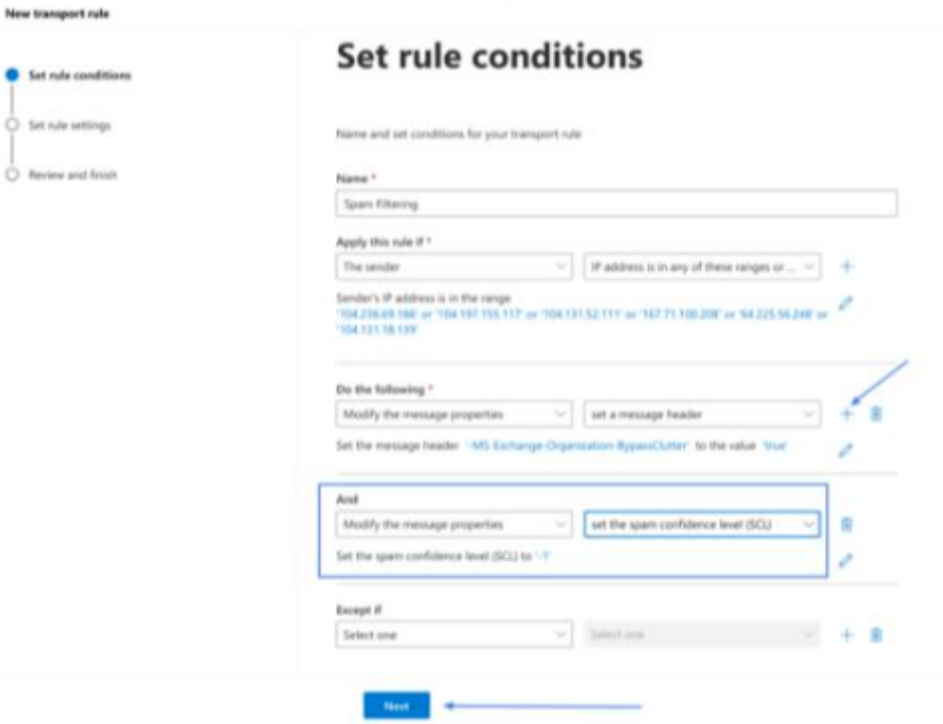
6. Click on "Do the following → Modify the message properties → Set a Message Header".

7. Choose the "Enter text" buttons by the right side of the "Do the following" field and enter these values: "-MS-Exchange-Organization-BypassClutter" and "true".



8. Click on the "+" sign, to add another rule condition.

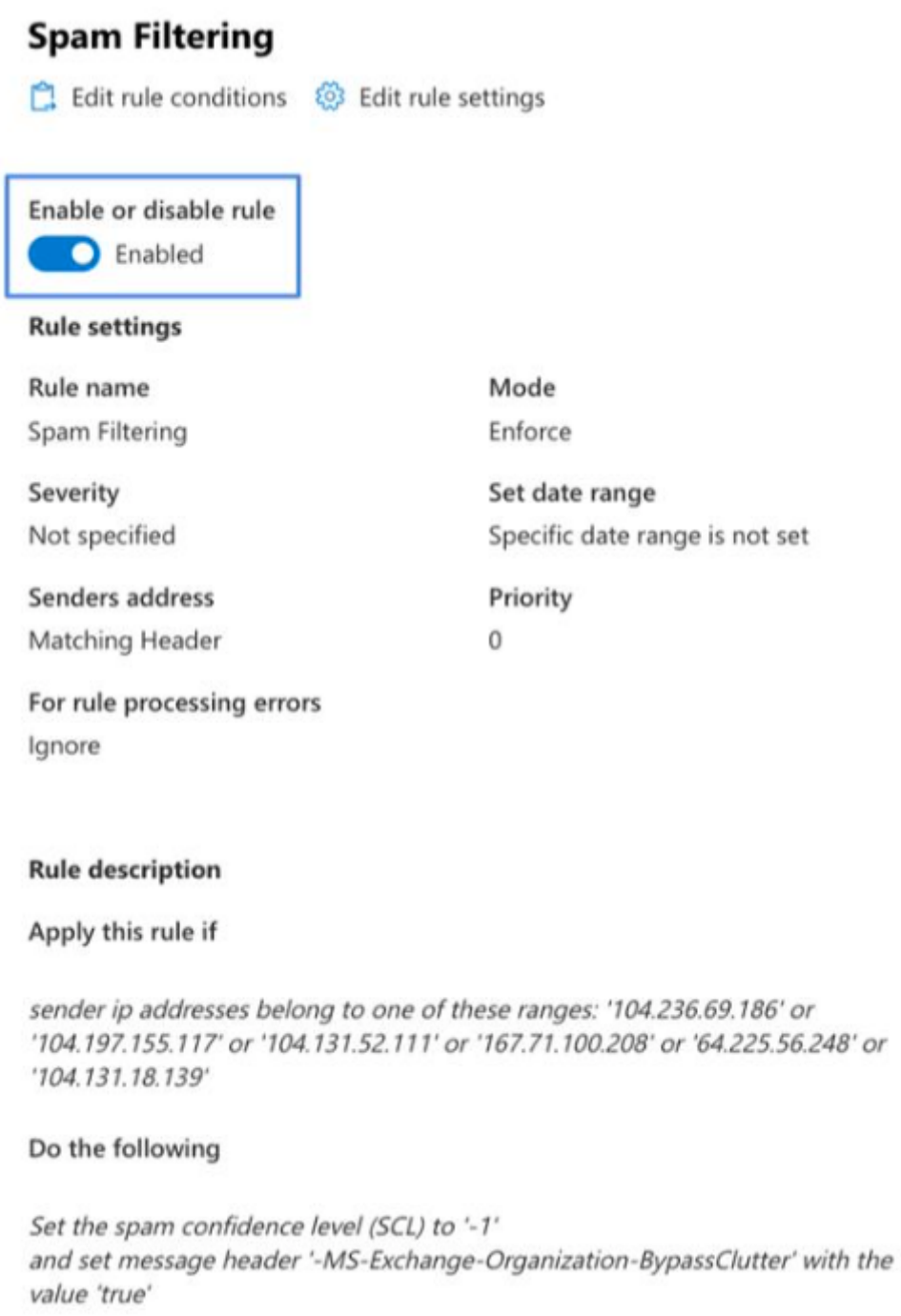
9. Choose "Modify the message properties → Set the spam confidence level (SCL)" to... and select "Bypass Spam Filtering", which will set the value of SCL to -1.



10. Click on the "Next" button.

11. Leave the Set Rule settings as is and proceed to the Review and finish window and save the rule.

12. Your final Completed Mail Flow Rule screen should look as below:



Please make sure the rule is Enabled, and priority is set to 0.

Whitelist ATP by Email Header for Mail Filtering

Whitelisting ATP by email header is recommended if you have a mail filter in front of your mail server.

To configure the mail flow rule to bypass ATP link processing by header:

1. Navigate to https://admin.exchange.microsoft.com/#/transportrules

2. Create a new rule & name it "Bypass ATP Links". (this is an example name, as it can be set as desired).

3. In the "Apply this rule if" condition select The message headers and then select "includes any of these words".

4. In the Enter text type the header name X-PHISHTEST.

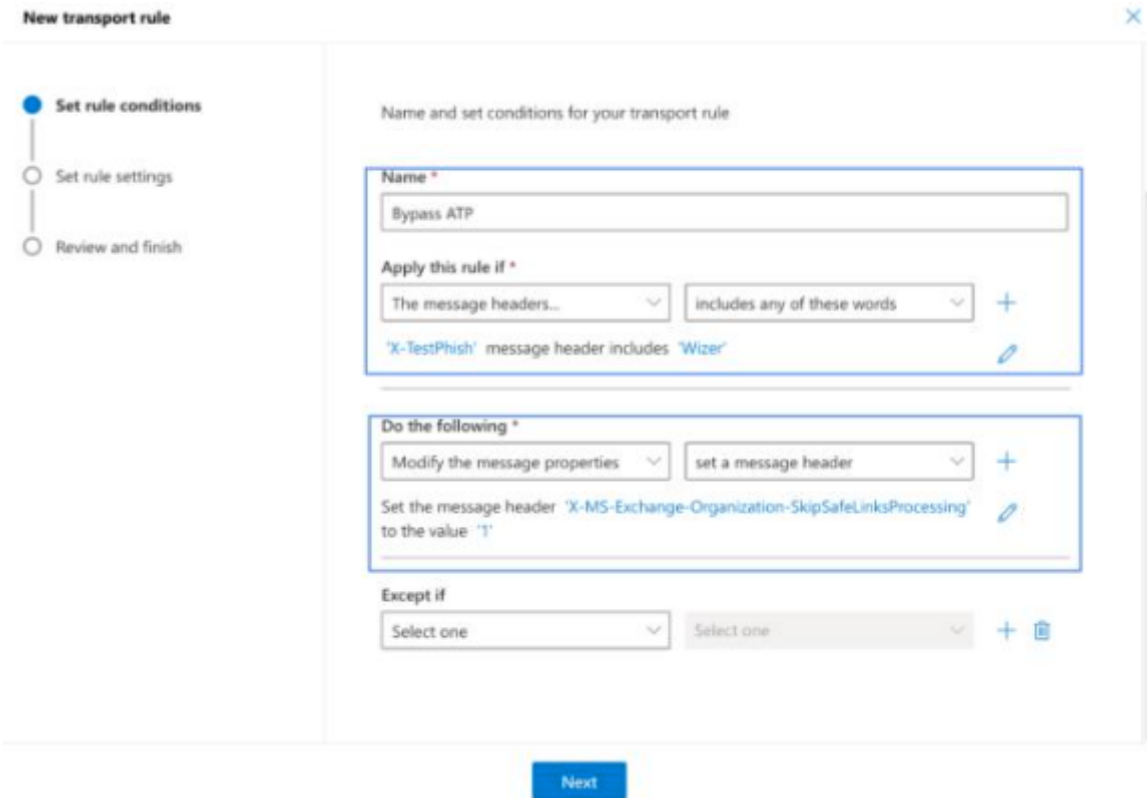
5. In the Enter words type in CYTECH.

6. In the "Do the following" condition select "Modify the message properties" and "set a message header".

7. Insert below into the "Enter text" fields:

- Click the first *Enter text... link and set the message header to X-MS-Exchange-Organization-SkipSafeLinksProcessing.
- Click the second *Enter text... link and set the value to 1.

Please refer to the below screenshot which illustrates how should the configuration look like:

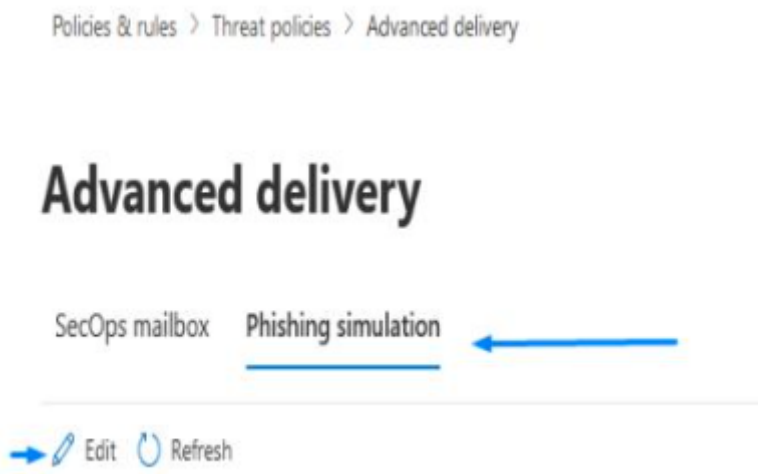


Set the rule settings according to your needs in the next tab, and in the Review and finish tab, press Finish.

Whitelist Using Advanced Delivery Policies in Microsoft Defender for Office 365 1. In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & Collaboration > Policies & Rules > Threat policies > Advanced delivery in the Rules section.

Alternatively, you can use the following link https://security.microsoft.com/advanceddelivery to navigate directly to the Advanced delivery page.

2. In the Advanced delivery menu, navigate to the Phishing simulation tab and press Edit to either add new or configure existing values (refer to the screenshot below).



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

Domain: Expand this setting and enter at least one email address domain 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 as many times as necessary. You can add up to 20 entries.

- a-adobe.com
- accountsgoogle.me
- airbnd.cc
- attlassians.com
- dropboox.site
- eebbey.com
- gitllb.com
- instegram.org
- lastpasss.net
- llinkedln.co
- my1psswords.com
- netpaypal.com
- offficce.com
- onedriives.com
- partnrportalludeemy.com
- slackj.com
- ttrelli.com
- zooms.cc

Edit third party phishing simulations

Phishing simulations are attacks orchestrated by your security team and used for training and learning. Simulations can help identify vulnerable users and lessen the impact of malicious attacks on your organization.

Third-party phishing simulations require at least one Sending domain entry [source domain or DKIM] AND at least one Sending IP entry. Simulations URLs to allow entries are optional, and prevent the simulated phishing URLs from being blocked at time of click.



Sending IP: Expand this setting and enter at least one valid IPv4 address 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 as many times as necessary. You can add up to 10 entries.

Valid values are:

Single IP: For example, 192.168.1.1.

IP range: For example, 192.168.0.1-192.168.0.254.

CIDR IP: For example, 192.168.0.1/25.

Simulation URLs to allow: Expand this setting and optionally enter specific URLs that are part of your phishing simulation campaign that should not be blocked or detonated by clicking in the box, entering a value, and then pressing Enter or selecting the value that's displayed below the box.

For the URL syntax format, see URL syntax for the Tenant Allow/Block List (opens in a new tab). These URLs are wrapped at the time of the click, but they aren't blocked.

When you're finished, you can click Add, and click close afterward if this was a first-time addition, or if you were editing existing values click Save and then click Close.

- https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list-about?view=o365-worldwide#url-syntax-for-the-tenant-allowblock-list