M365 Quarantine Issues Troubleshooting

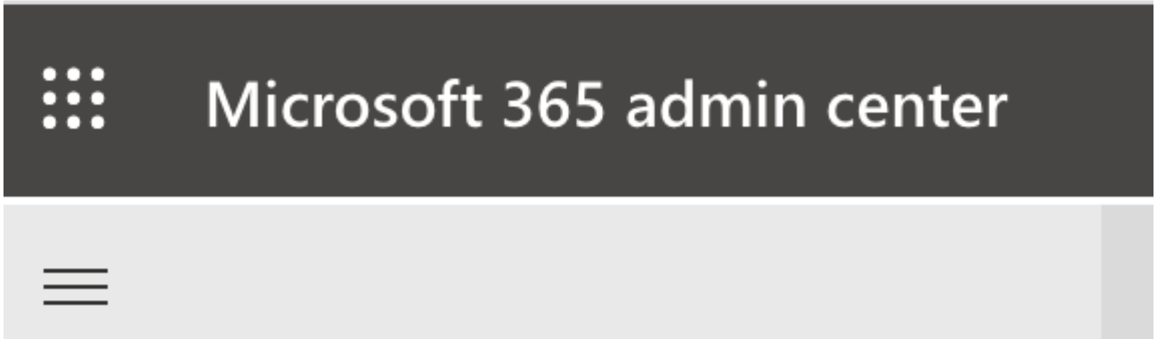
We have received two reports of Microsoft M365 suddenly moving conversations to Quarantine as of July 19th, 2022. There have been no changes on the ExchangeDefender side that can explain this and we have not been able to reproduce the issue when ExchangeDefender is deployed correctly with the proper DNS records and IP allow policies.

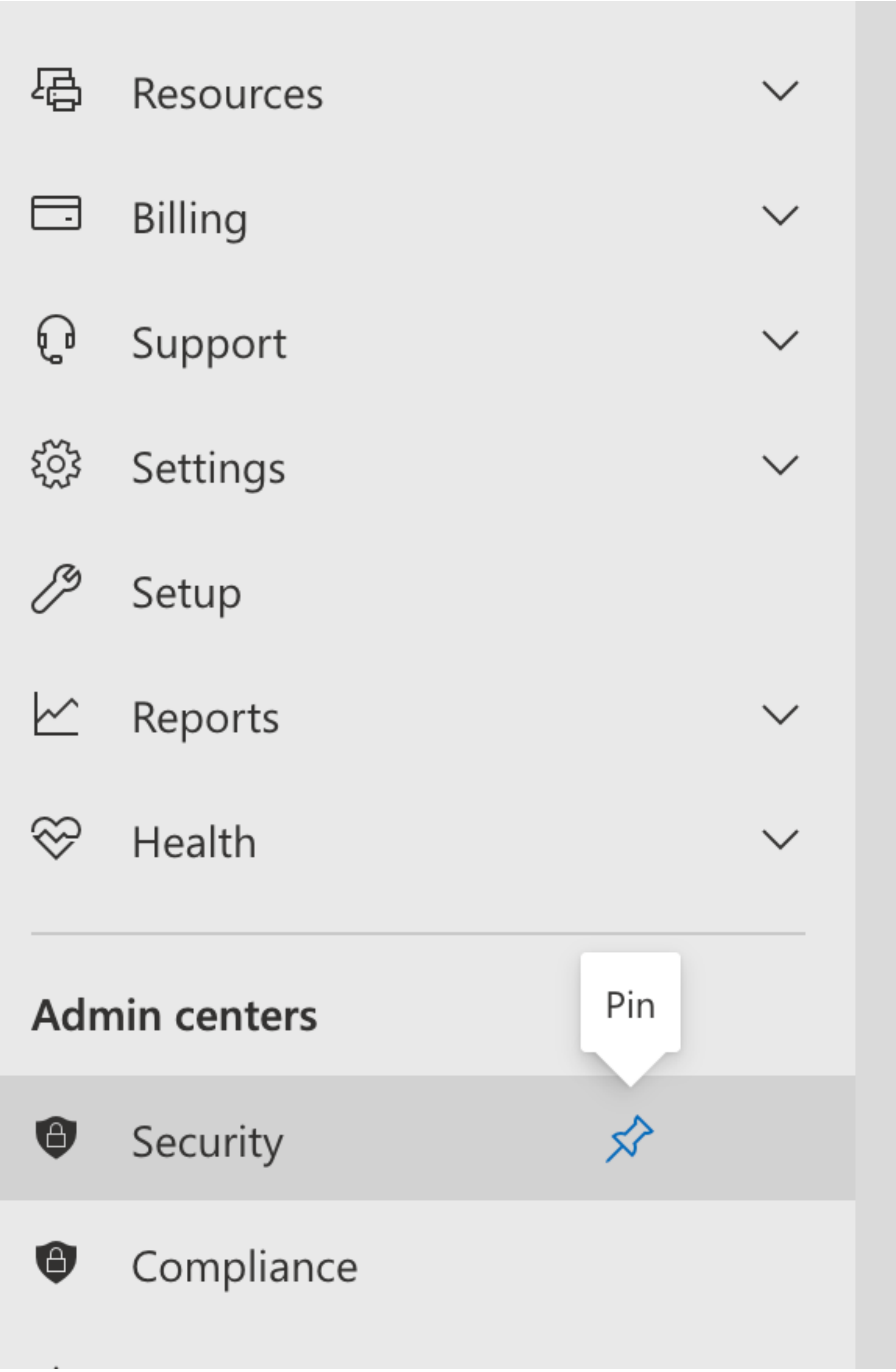
If you are having problems, here are three things you should do:

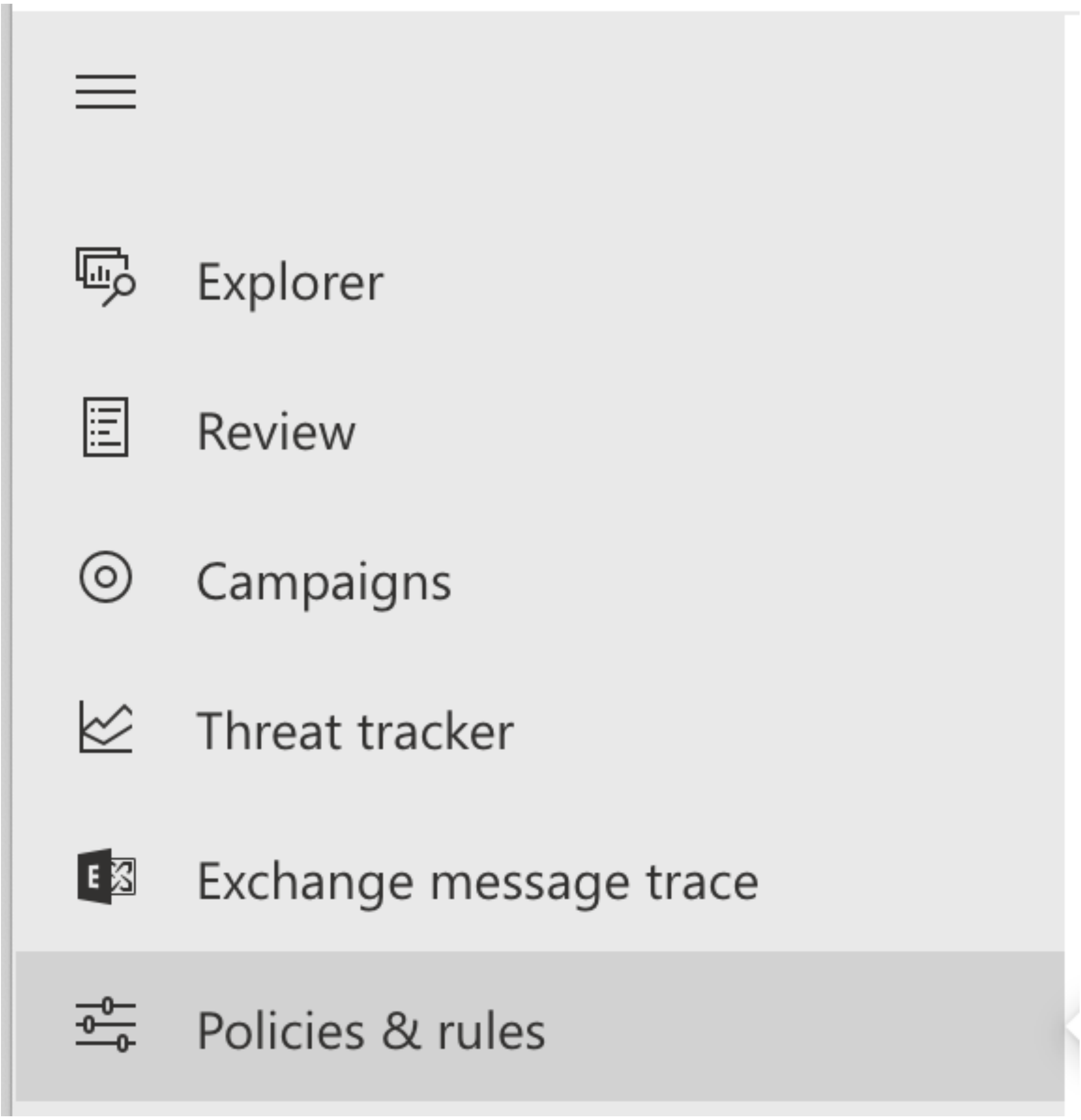
1. Confirm that you've rolled out ExchangeDefender properly and setup all the security policies to allow us to relay to your Inbox: https://exchangedefender.com/docs/configure-outbound-smart-host-office-365
2. Contact Microsoft with samples of messages that are in the Quarantine and ask them to explain how/why they were classified as such when they were relayed through a trusted gateway that is on the IP whitelist.
3. Turn off all threat features off. This issue started after Microsoft M365 had a security compromise and our suspicion is that clients that did not have our IP ranges in M365 are now seeing their messages flagged as phishing. Please make sure you follow the document from Step #1 and try this:

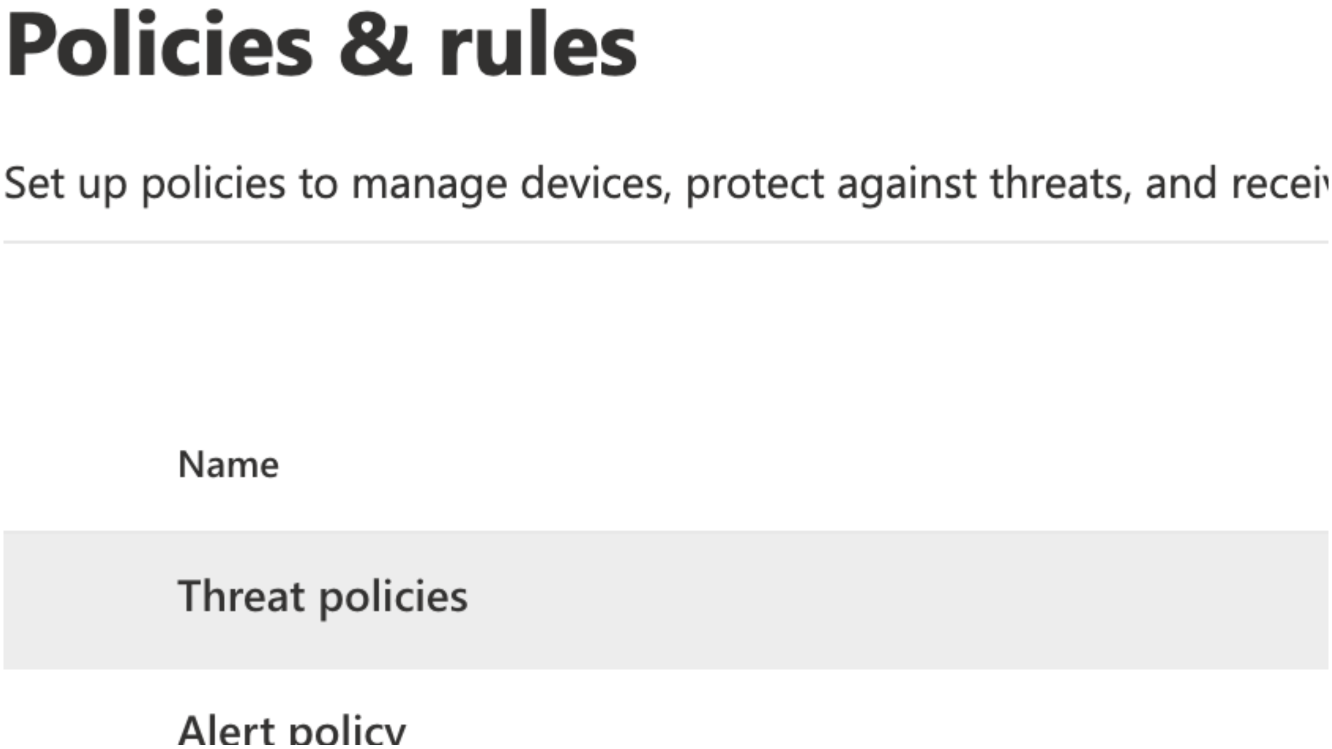
Manage Anti-Phishing Rules

1. Log into your 365 admin center
2. Navigate to **Security**
3. Navigate to **Policies and Rules**
4. Select **Threat Policies**
5. Select **Anti-phishing**
6. Edit the active policy
7. Select **Edit Protection Settings**
8. Disable **Enable spoof protection**




Resources
Billing
Support
Settings
Setup
Reports
Health
Admin centers
Pin
Security
Compliance

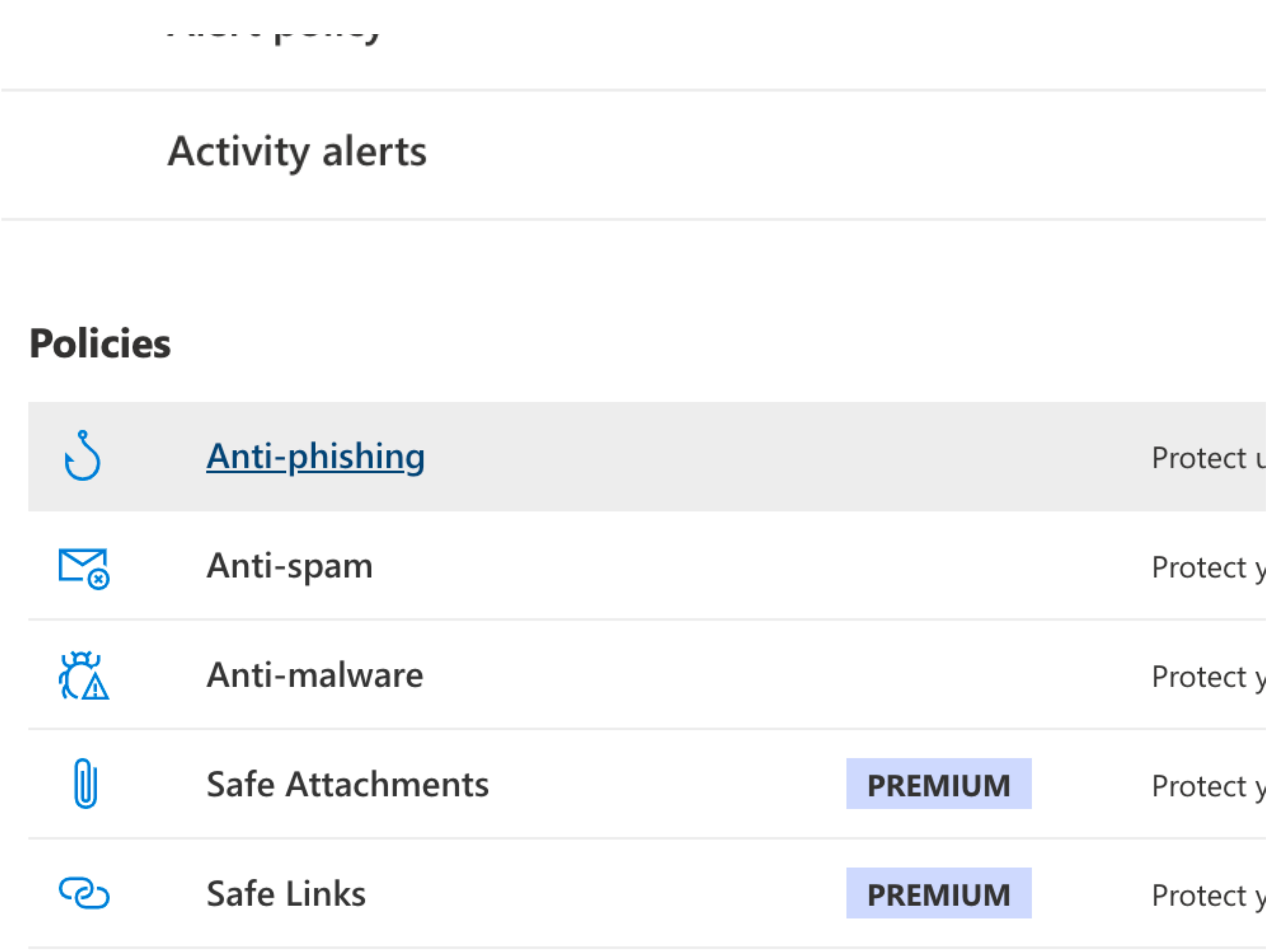




Policies & rules

Set up policies to manage devices, protect against threats, and recei

Name
Threat policies
Alert policy

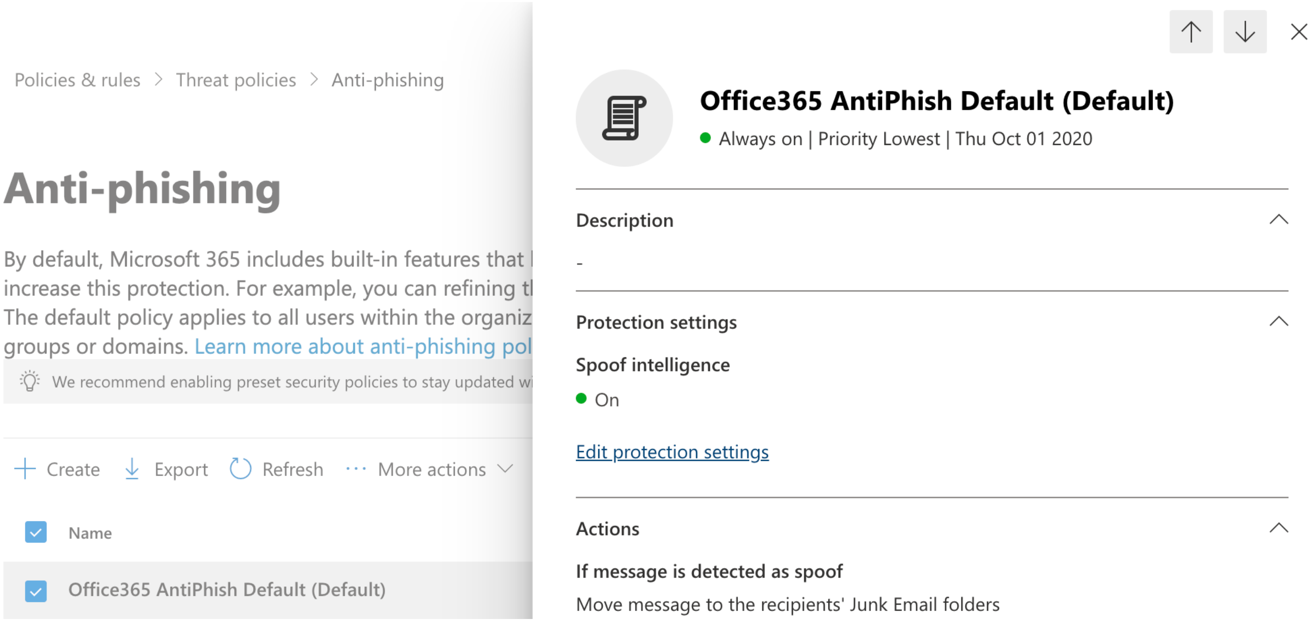


Alert policy

Activity alerts

Policies

Anti-phishing		Protect u
Anti-spam		Protect y
Anti-malware		Protect y
Safe Attachments	PREMIUM	Protect y
Safe Links	PREMIUM	Protect y



Policies & rules > Threat policies > Anti-phishing

Anti-phishing

By default, Microsoft 365 includes built-in features that |
increase this protection. For example, you can refining tl
The default policy applies to all users within the organiz
groups or domains. Learn more about anti-phishing pol

We recommend enabling preset security policies to stay updated w

☑	Name
☑	Office365 AntiPhish Default (Default)

Office365 AntiPhish Default (Default)

● Always on | Priority Lowest | Thu Oct 01 2020

Description

-

Protection settings

Spoof intelligence

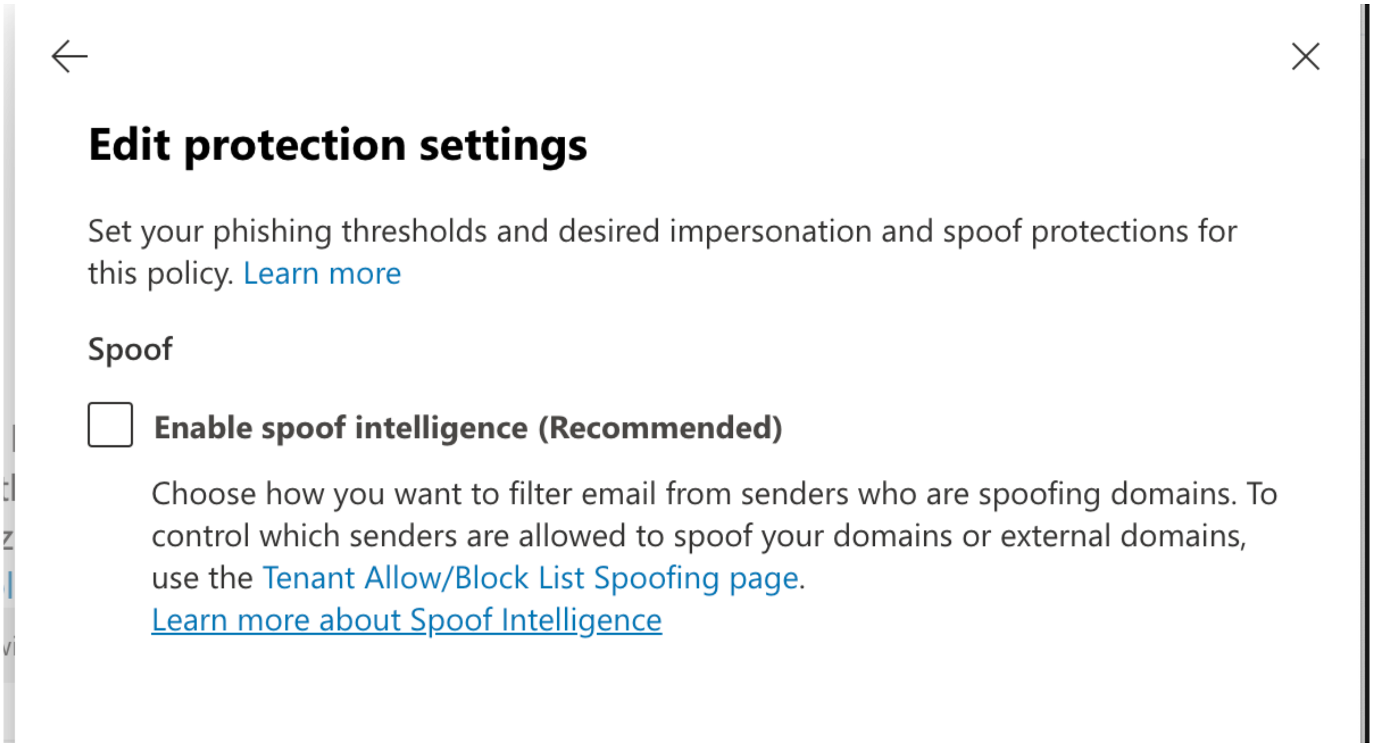
● On

Edit protection settings

Actions

If message is detected as spoof

Move message to the recipients' Junk Email folders



Edit protection settings

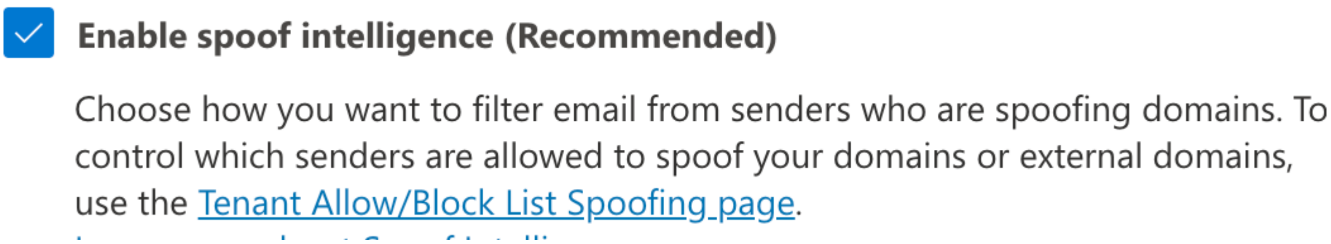
Set your phishing thresholds and desired impersonation and spoof protections for this policy. Learn more

Spoof

☐ Enable spoof intelligence (Recommended)

Choose how you want to filter email from senders who are spoofing domains. To control which senders are allowed to spoof your domains or external domains, use the Tenant Allow/Block List Spoofing page.
Learn more about Spoof Intelligence

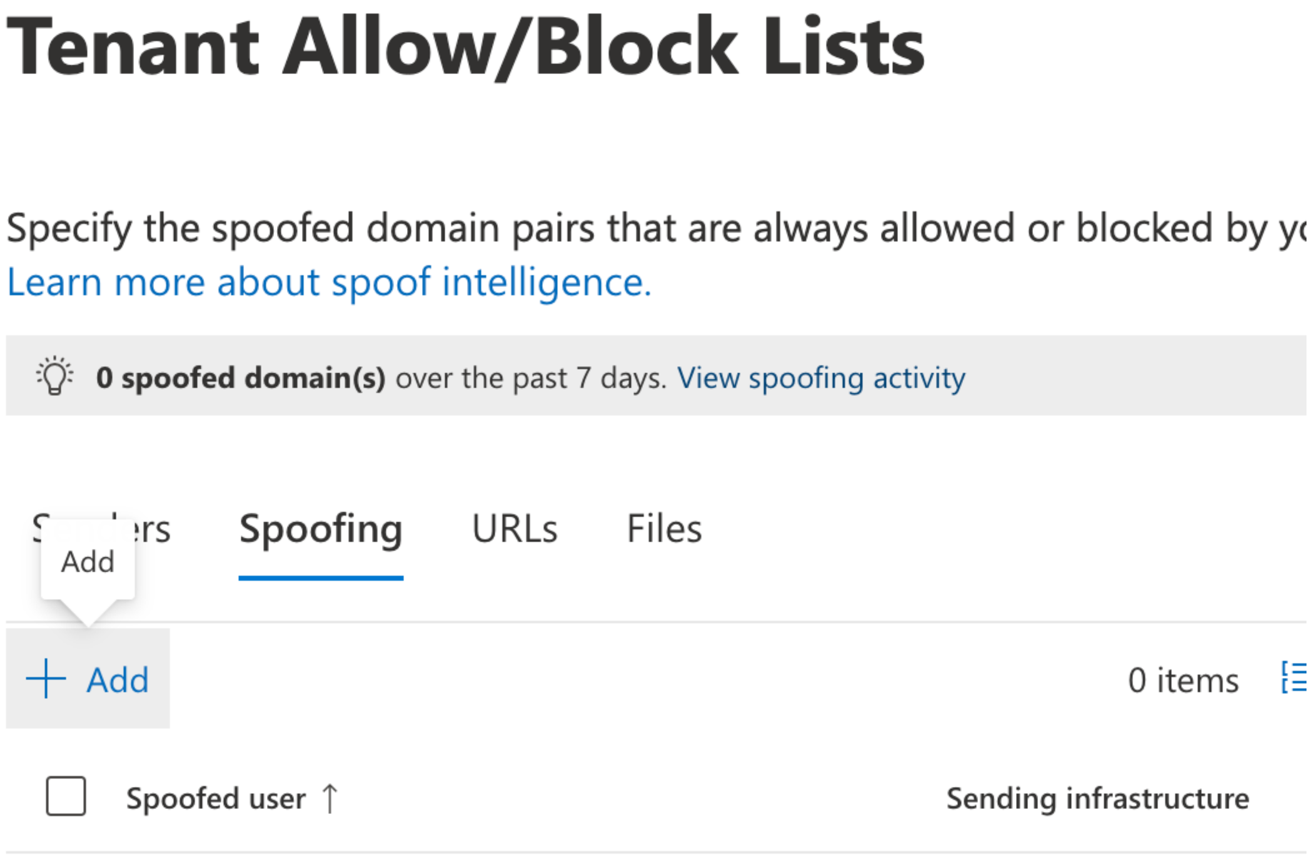
If you do not want to disable spoof intelligence then you will need to add exceptions to our networks under `Tenant Allow/Block List Spoofing`



☑ Enable spoof intelligence (Recommended)

Choose how you want to filter email from senders who are spoofing domains. To control which senders are allowed to spoof your domains or external domains, use the Tenant Allow/Block List Spoofing page.

Tenant Allow/Block Lists

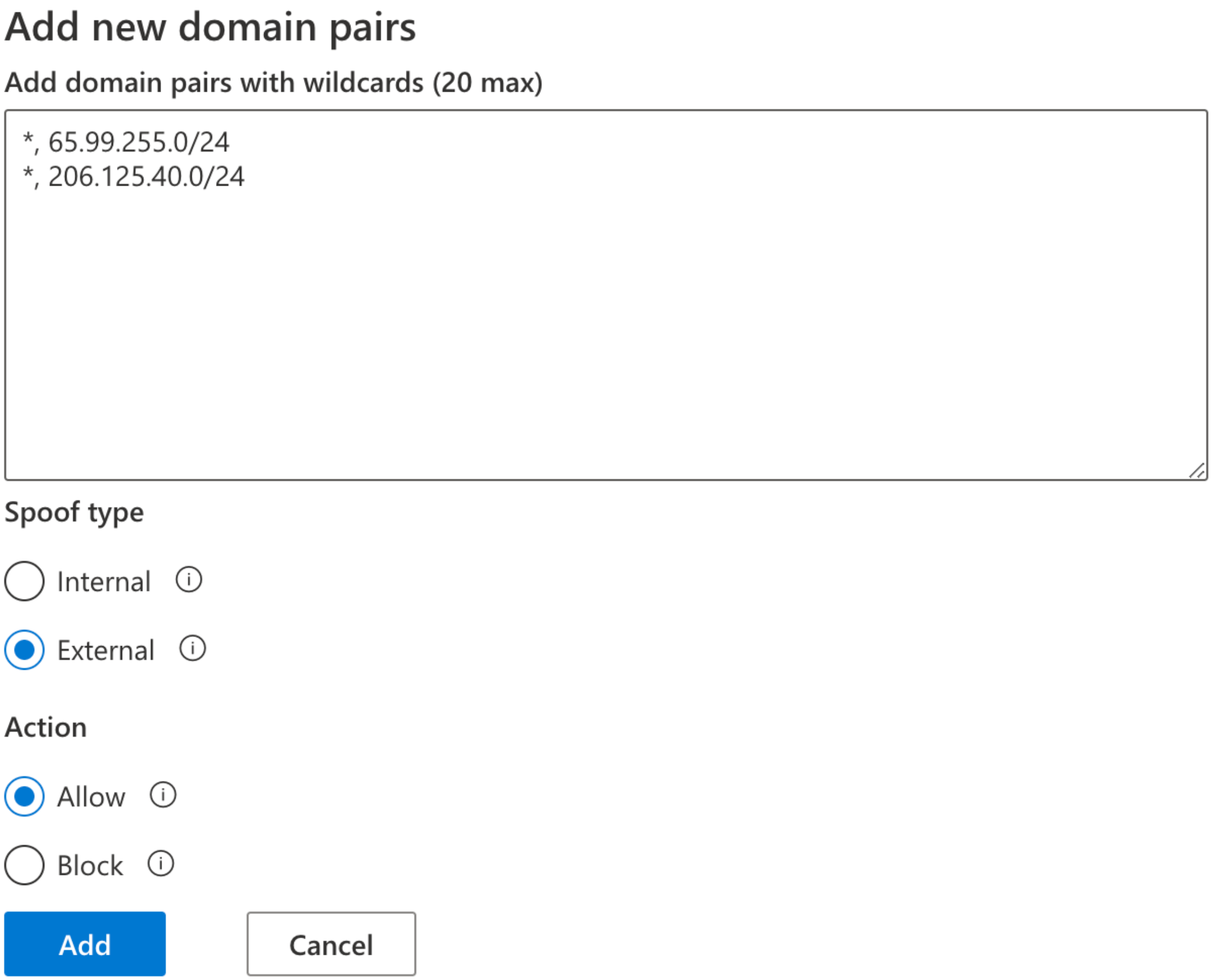


Tenant Allow/Block Lists

Specify the spoofed domain pairs that are always allowed or blocked by y
Learn more about spoof intelligence.

0 spoofed domain(s) over the past 7 days. View spoofing activity

□	Spoofed user ↑	Sending infrastructure



Add new domain pairs

Add domain pairs with wildcards (20 max)

```
*, 65.99.255.0/24
*, 206.125.40.0/24
```

Spoof type

○ Internal

● External

Action

● Allow

○ Block

Below is the content to paste into the domain pair list

```
*, 65.99.255.0/24
*, 206.125.40.0/24
```