Microsoft 365 Whitelisting

Microsoft's new secure by default feature may affect current whitelisting rules that your organization has in place. Due to this change, you can use Microsoft's new **Advanced Delivery Policies** feature to whitelist.

To create, modify, or remove settings in an advanced delivery policy, **you need to be a member** of these role groups:

- Security Administrator role group in the Microsoft Security & Compliance Center
- Organization Management role group in Microsoft Exchange Online

Avoid Spam Issues related to Office365

How are Phishing Simulations mails whitelisted in O365? - Microsoft has made fundamental changes to mail flow and filtering in mid-2021. Any exceptions in mail flow rules are no longer mandatory, various security default settings are made that cannot be bypassed. For example, mails classified as 'High Confidence Phish' will no longer be allowed to pass through via an Exchange Online Rule.

In this context, Microsoft has also created the possibility to store an extra configuration for phishing campaigns, so that the exceptions only have to be defined at a central point.

In the Exchange Online Protection Policies there is the Advanced Delivery section and there Phishing Simulation.

The domain names and senders of phishing simulations can be stored there.

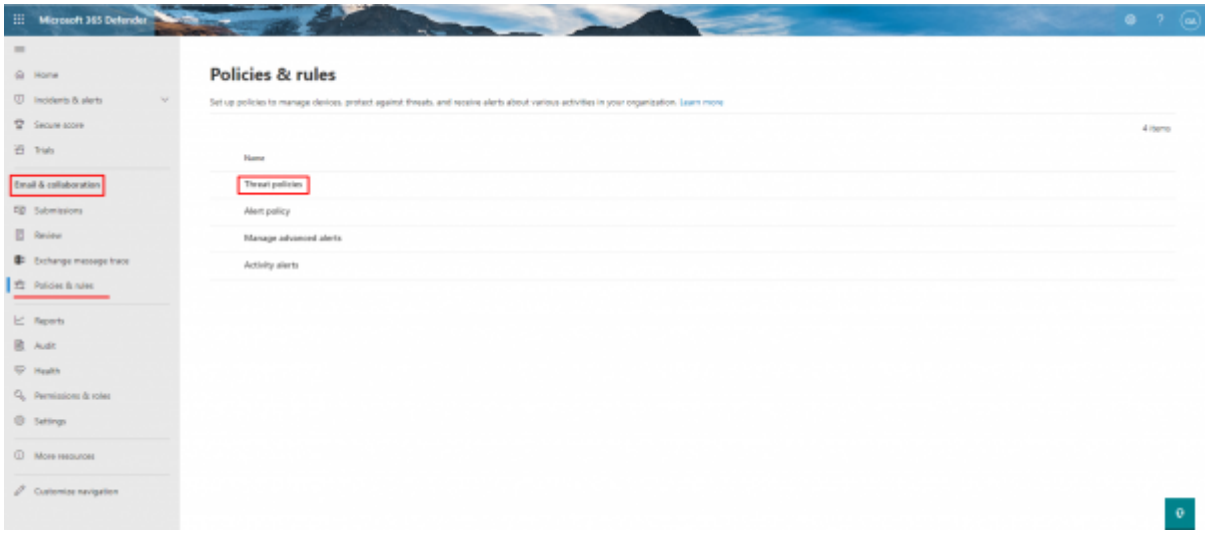
Details about the new behavior and the Advanced Delivery / Phishing Simulation can be found here:
https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/mastering-configuration-in-defender-for-office-365-part-two/ba-p/2307134
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-advanced-delivery?view=o365-worldwide

Navigate to the configuration via the security.microsoft.com website, alternatively directly via this link: https://security.microsoft.com/advanceddelivery?viewid=PhishingSimulation

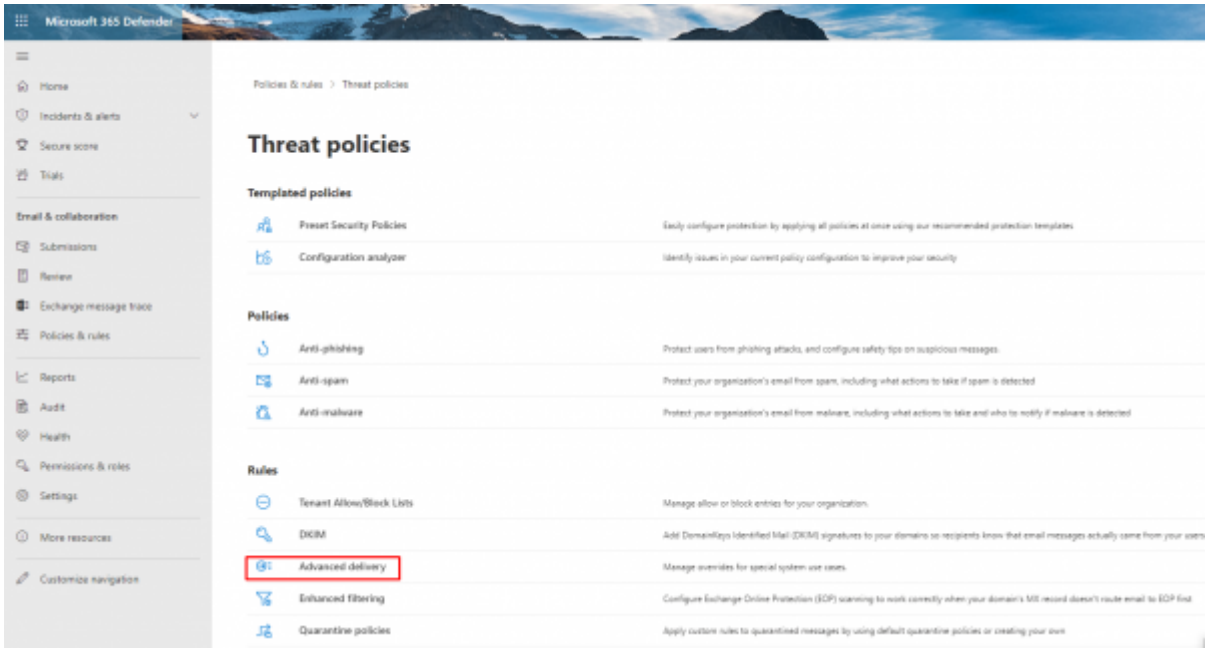
O365. Phishing simulation setup.

Adding sending domain and Sending IP to whitelist

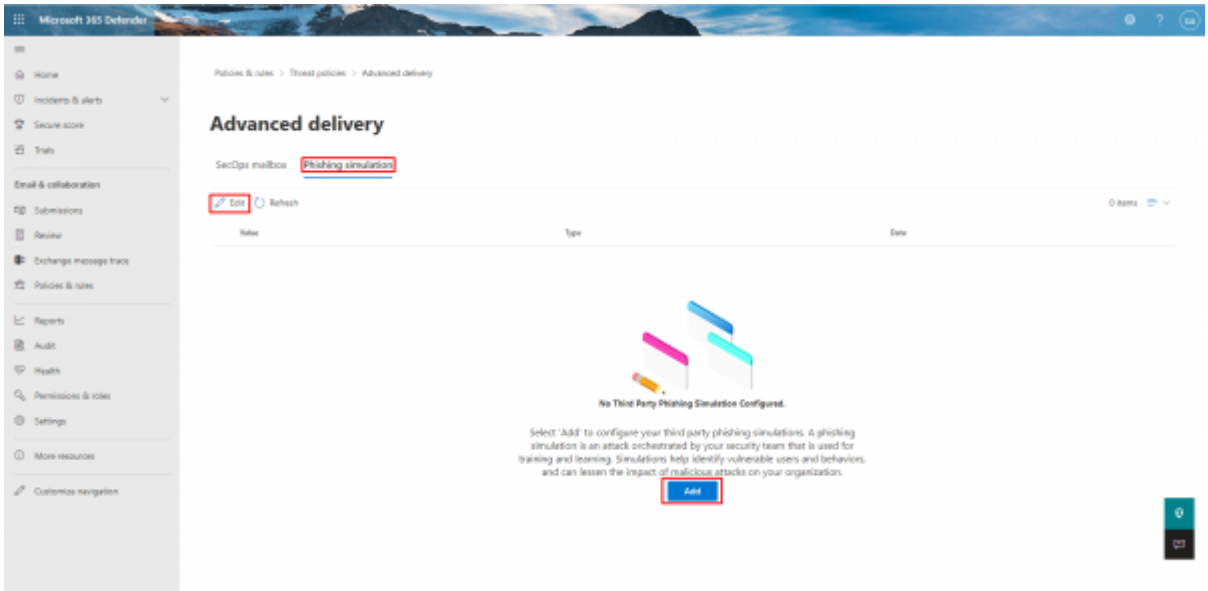
- Open the Microsoft 365 Defender portal at https://security.microsoft.com and sign in with your **Admin** account.
- Under **Email & Collaboration**, navigate to **Policies & Rules** > **Threat policies**



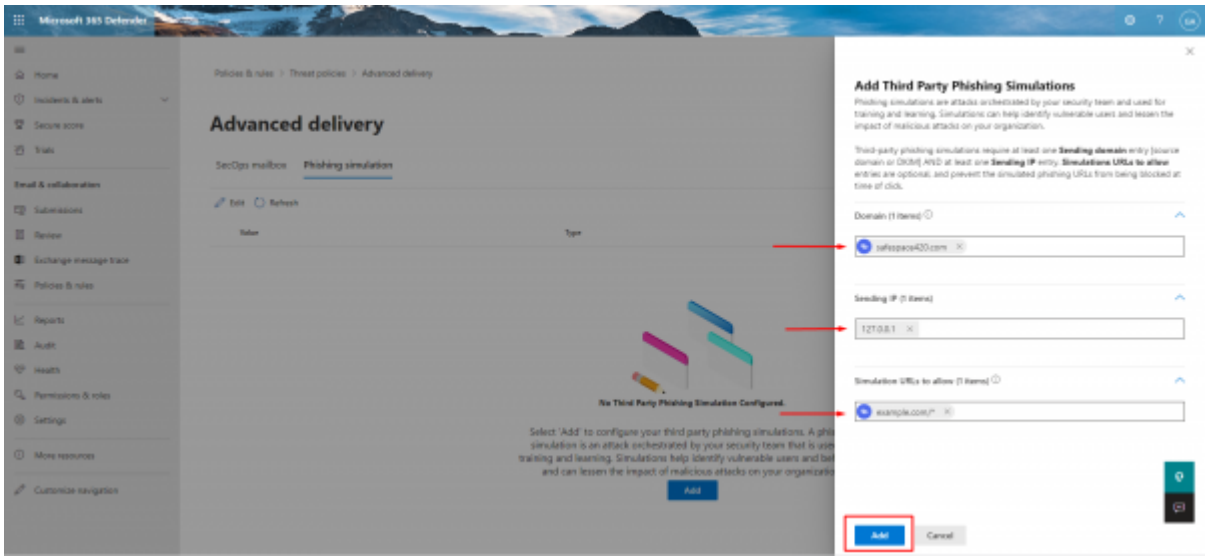
- Choose **Advanced delivery**.



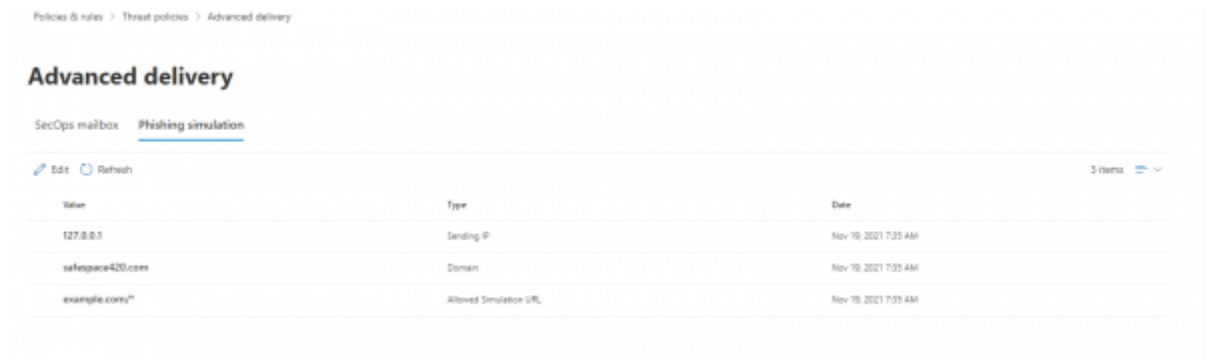
- On the Advanced delivery page, select the **Phishing Simulation tab**. Click the **Edit** icon or If there are no configured phishing simulations, click **Add**.



- In the **Edit third-party phishing** simulation modal, adjust the following settings: at least one **Sending domain** entry [one that you use as Sender email in Lucy] AND at least one **Sending IP**(Lucy instance IP address) entry. Optionally enter **specific URLs** that are part of your phishing simulation campaign that should not be blocked, using the recommended URL syntax format: **example.com/**



- Click **Add**.
- Final result should look like this.



Wait at least 30 minutes for changes to propagate before you start any phishing campaigns! Thank You!

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=o365_whitelisting

Last update: **2021/12/17 11:00**