Allowlisting - Use M365 Defender to allow a Phishing Simulation

To ensure GrintOps can effectively simulate phishing campaigns, you will need to allowlist our emails. **We highly recommend this method for allowlisting as it's been explicitly created by Microsoft for the purpose of conducting phishing simulations.**

Note: If you find that website links are being re-written and lead to a "suspicious website" page after allowlisting, your organisation may need to add additional attachment and URL exemptions.

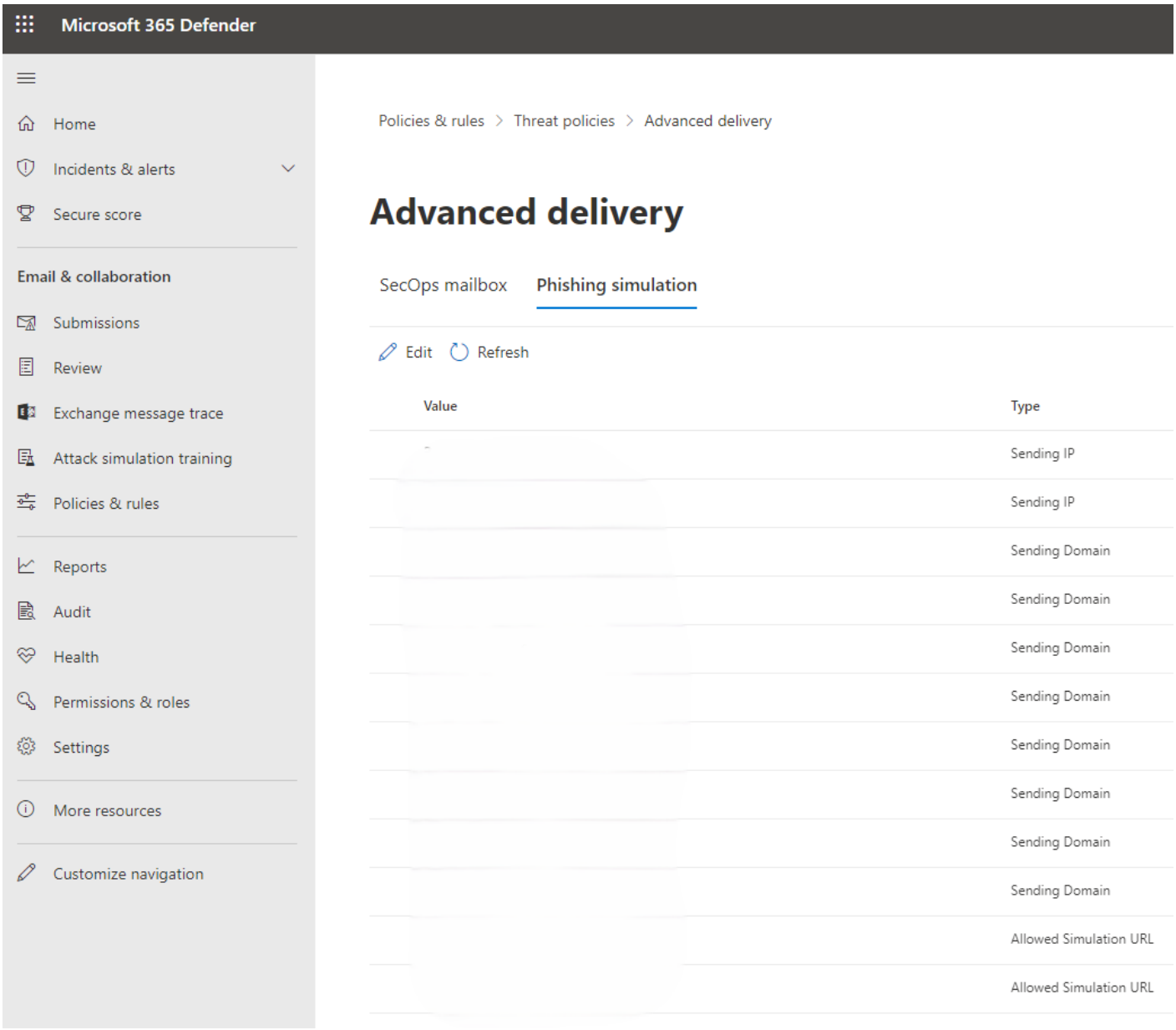
To enable these exemptions please see our support article: **Allowlisting - Bypass Safe Link/Attachment Processing of M365 Advanced Threat Protection (ATP)**

Use the Microsoft 365 Defender portal to configure third-party phishing simulations in the advanced delivery policy

Note: Prefer to use PowerShell? **Use our prepared script**

1. Login to Microsoft 365 Defender at the following link to go straight to the Phishing Simulation allowlisting form:

https://security.microsoft.com/advanceddelivery?viewid=PhishingSimulation



Note: This form can also be accessed by going to https://security.microsoft.com/ and clicking through Email & Collaboration > Policies & Rules > Threat Policies > Advanced Delivery > Phishing Simulation

2. Click Edit icon. **Edit** or 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:

The following are examples of phishing domains that may be used:

office365-webnotif.com
office365-webnotif.site
miro-apps.online
hukum0nline.com
slack-apps.online
github-apps.online

Sending IP:

The following are examples of sending IP addresses that may be used in phishing simulation campaigns or email transmissions:

135.84.80.0/24
136.143.161.0/24
136.143.184.0/24
136.143.188.0/24
165.173.129.0/24
165.173.174.0/23
165.173.180.0/24
165.173.182.0/24

Simulation URLs to allow:

The following are examples of simulation URLs that should be allowed to ensure phishing simulation emails and landing pages function properly:

office365-webnotif.com/*
.office365-webnotif.com/
office365-webnotif.site/*
.office365-webnotif.site/
miro-apps.online/*
.miro-apps.online/
hukum0nline.com/*
.hukum0nline.com/
slack-apps.online/*
.slack-apps.online/
github-apps.online/*
.github-apps.online/

Note: All the above domains and IP addresses are under the sole control of GrintOps. As such we can ensure that no unintended emails will originate from these IPs and domains after allowlisting occurs.

4. When you're finished, click Add/Save and then click Close.

Note: Allowlisting may take up to an hour to take effect.

All done! Allowlisting can be tricky... should you have any difficulties, please don't hesitate to contact us.

Troubleshooting: If you run into issues with emails continuing to go to spam/quarantine folders. You may have Microsoft Advanced Threat Protection (ATP) enabled which may require additional allowlisting. Please see our guide here to **Bypass Safe Link/Attachment Processing of M365 ATP**.

PowerShell Allowlisting Script

Want to automate the deployment of GrintOps allowlisting? Use our prepared PowerShell script below.

Step 1. Ensure Exchange Online V3 For Powershell Is Installed

```
Install-Module -Name ExchangeOnlineManagement -Force
```

Step 2. Connect Exchange Online For Powershell To Your Microsoft 365 Tenant

Note: Please replace the value YOUR-ADMIN-EMAIL with the M365 administrator email that you wish to sign in with.

```
Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline `
```

```
-UserPrincipalName YOUR-ADMIN-EMAIL `
-ShowProgress:$false `
-LoadCmdletHelp # optional: if you want Get-Help for EXO cmdlets
```

Step 3. Create The Phishing Simulation Allowlist Policies And Configurations

Note: If you've white-labelled GrintOps , make sure to replace the grintops.com and learn.grintops.com domains with your white-labelled domains.

```
# 1. Create the override policy
New-PhishSimOverridePolicy -Name PhishSimOverridePolicy

# 2. Confirm it’s there
Get-PhishSimOverridePolicy

# 3. Create the override rule pointing to the allowlisted domains & IPs
New-ExoPhishSimOverrideRule `
-Name PhishSimOverrideRule `
-Policy PhishSimOverridePolicy `
-Domains office365-webnotif.com, office365-webnotif.site, miro-apps.online, hukum0nline.com, slack-apps.online, github-apps.online `
-SenderIpRanges: 135.84.80.0/24 , 136.143.161.0/24 , 136.143.184.0/24 , 136.143.188.0/24 , 165.173.129.0/24 , 165.173.174.0/23 , 165.173.180.0/24, 165.173.182.0/24

# 4. Allowlist the phishing website URLs in Defender’s tenant allow/block list
New-TenantAllowBlockListItems `
-Allow `
-ListType Url `
-ListSubType AdvancedDelivery `
-Entries office365-webnotif.com/*, office365-webnotif.site/*, *.miro-apps.online/*,hukum0nline.com/*,*.slack-apps.online/*,github-apps.online/*`
-NoExpiration

# 5. Verify your rule
Get-ExoPhishSimOverrideRule
```

Revision #27
Created 13 July 2025 14:49:41 by Admin
Updated 29 July 2025 15:11:52 by Admin