Avanan Deployment Guide

AVANAN

Contents

Moving to Inline Protection

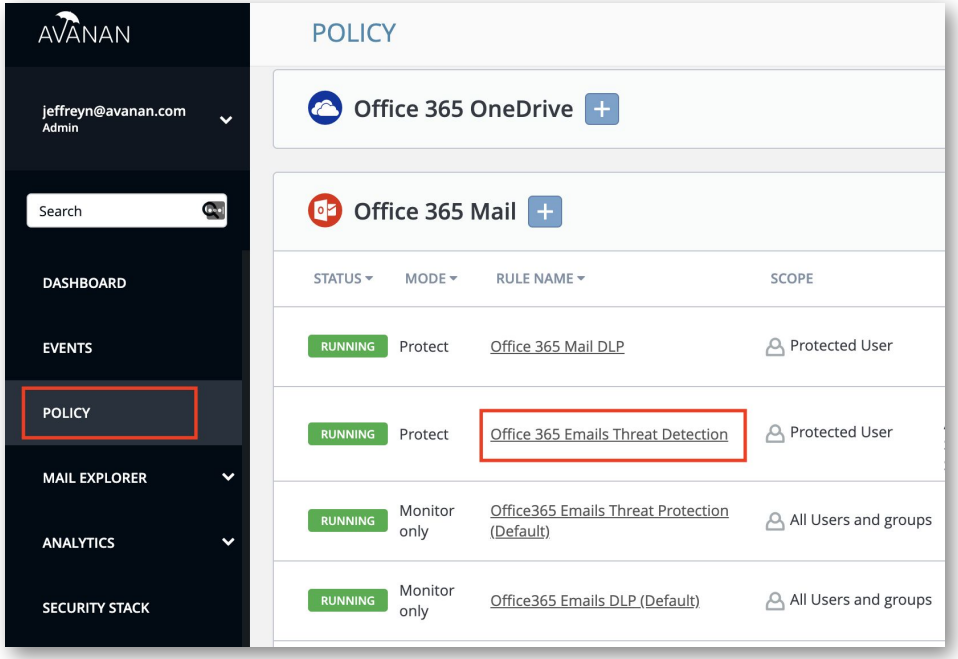
Customizing Policies

Responding to Incidents

Moving to Inline Protection

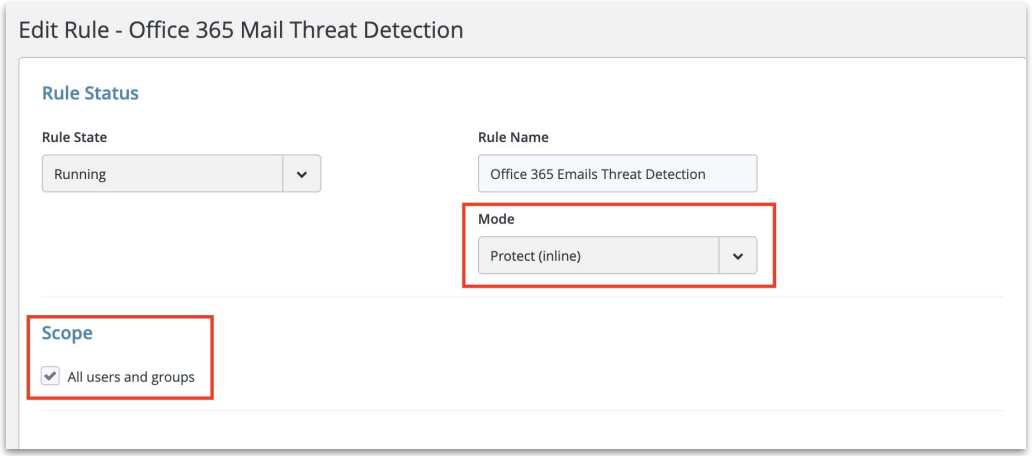
To deploy SmartPhish with best practices, move your users to Inline Protection.

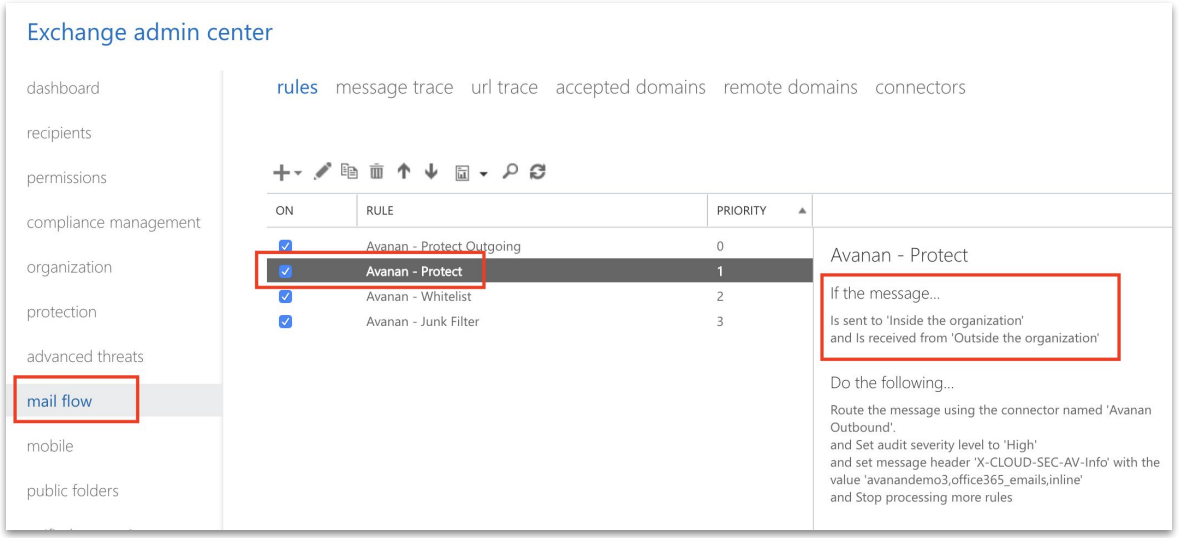
- Avanan will scan emails before they arrive in the users' inboxes.
- Admins can specify workflows for different types of detections (malware, phishing, suspicious phishing, and spam).



Moving to Inline Protection

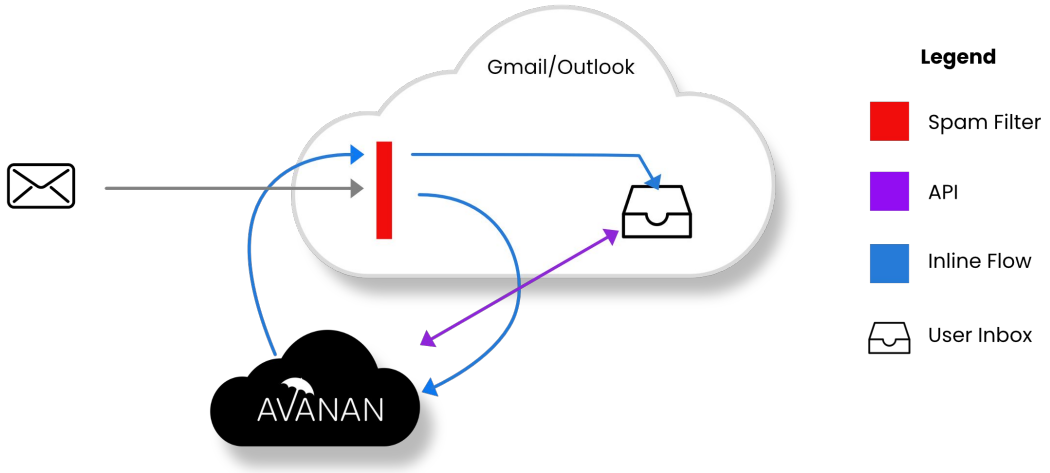
- Select “Protect (Inline)” and select the scope of users you wish to protect. By default, all users and groups will be protected.
- Alternatively, you may also choose to protect only specific users or members of a security group.
- Avanan will leverage its service user to make the appropriate changes in Exchange. This takes a few moments.
- In the Exchange Admin Center, the scope of protected users will be reflected in the “Avanan - Protect” mail flow rule.





Moving to Inline Protection

Email Security Protect Inline:
API & Mailflow



- Email sent to users protected inline will be processed twice.
- The first time, the emails are sent to Avanan for scanning by SmartPhish (and your sandboxing tool, if applicable). This is done by the “Avanan - Protect” mail flow rule.
- Emails that are not quarantined will be sent back and processed by the “Avanan - Whitelist” or “Avanan - Junk Filter” mail flow rules based on the original SCL as determined by Office 365.
- Please refer to this guide to stop inline protection.

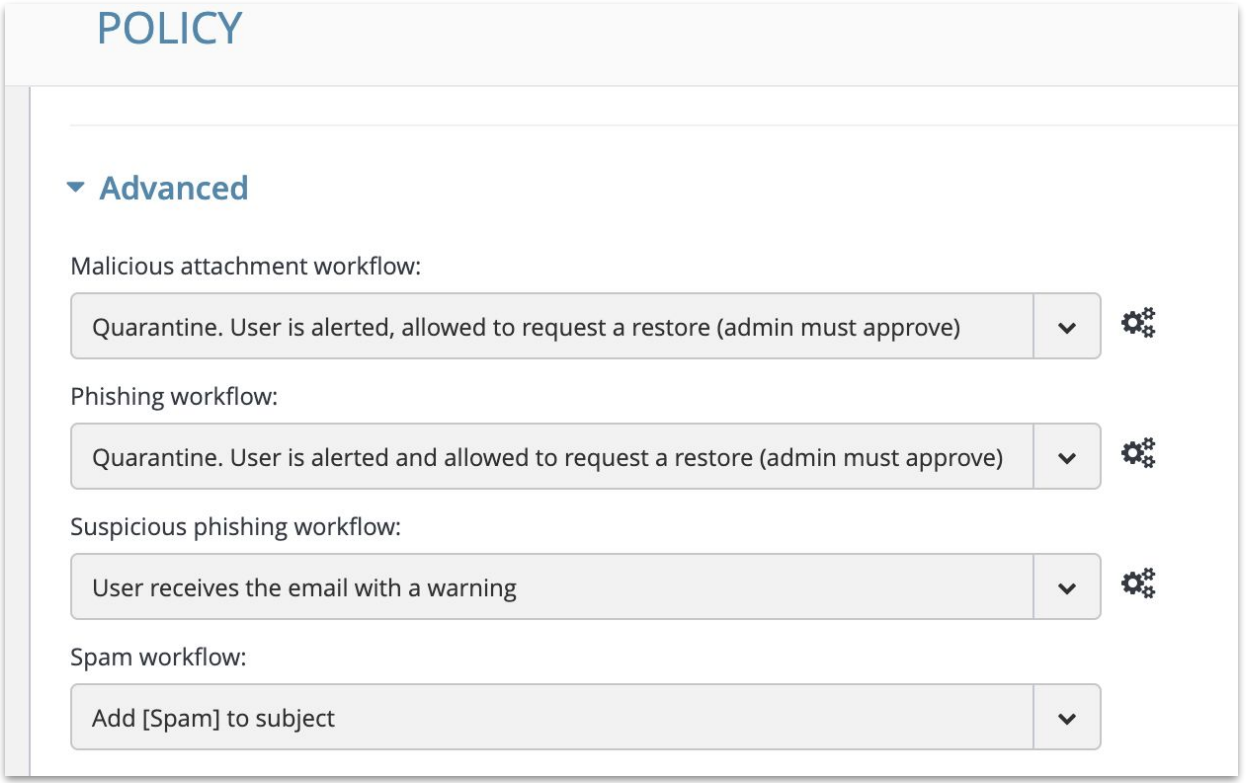
Customizing Policies

When you move users to inline protection, you can customize the remediation workflows for each type of detection:

- Malicious (a sandboxing tool identified malware in an attachment, if applicable)
- Phishing (SmartPhish is confident)
- Suspicious Phishing (SmartPhish is not sure)
- Spam

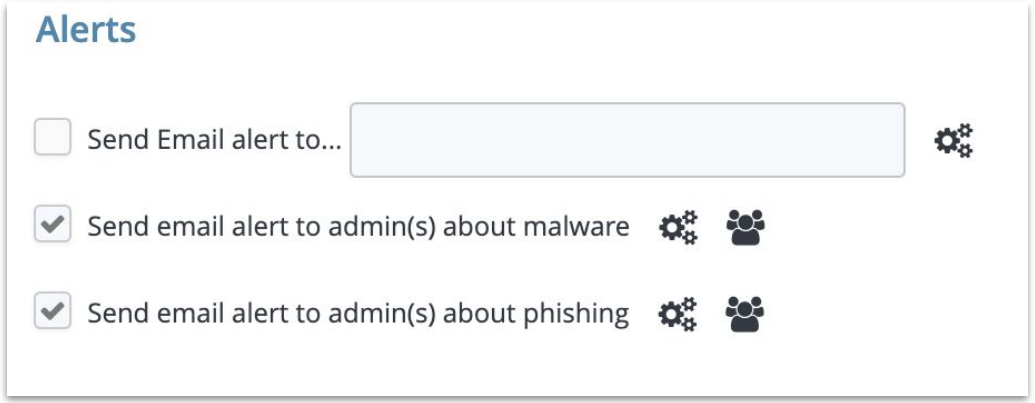
Alerts and warnings can be customized by clicking on the gear icon.

In order to select a workflow quarantine emails, you will need to set up a quarantine mailbox by adding a user in Office 365. We suggest a user called “Avanan Quarantine” for reference. The user must be licensed (at least E1).

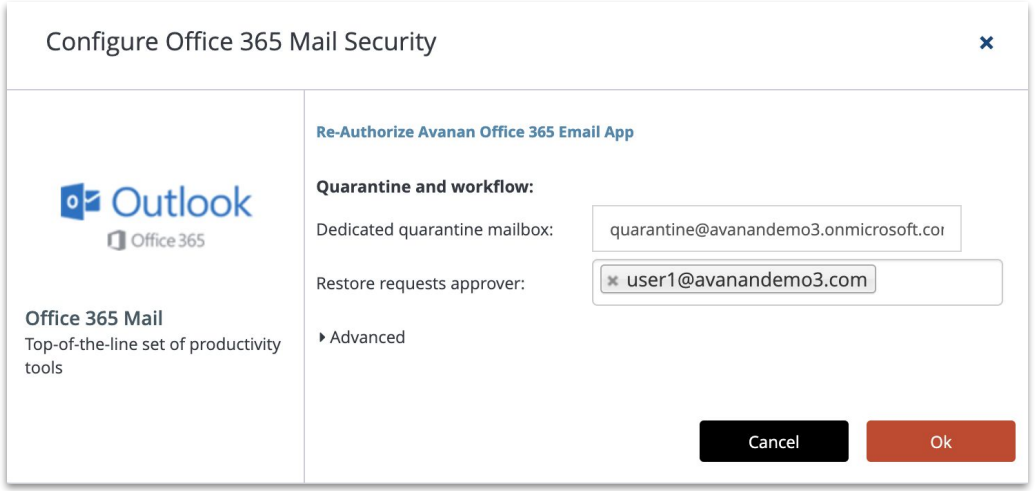


Customizing Policies

- We recommend sending alerts for phishing and malware detections to admins.
- If you would like to set up a distribution list to receive alerts and restore requests, ensure to add the distribution list in **Configuration → User Management**
- Additionally, you can always change the quarantine mailbox and who receives restore requests in **Configuration → Cloud App Store → Configure Outlook**



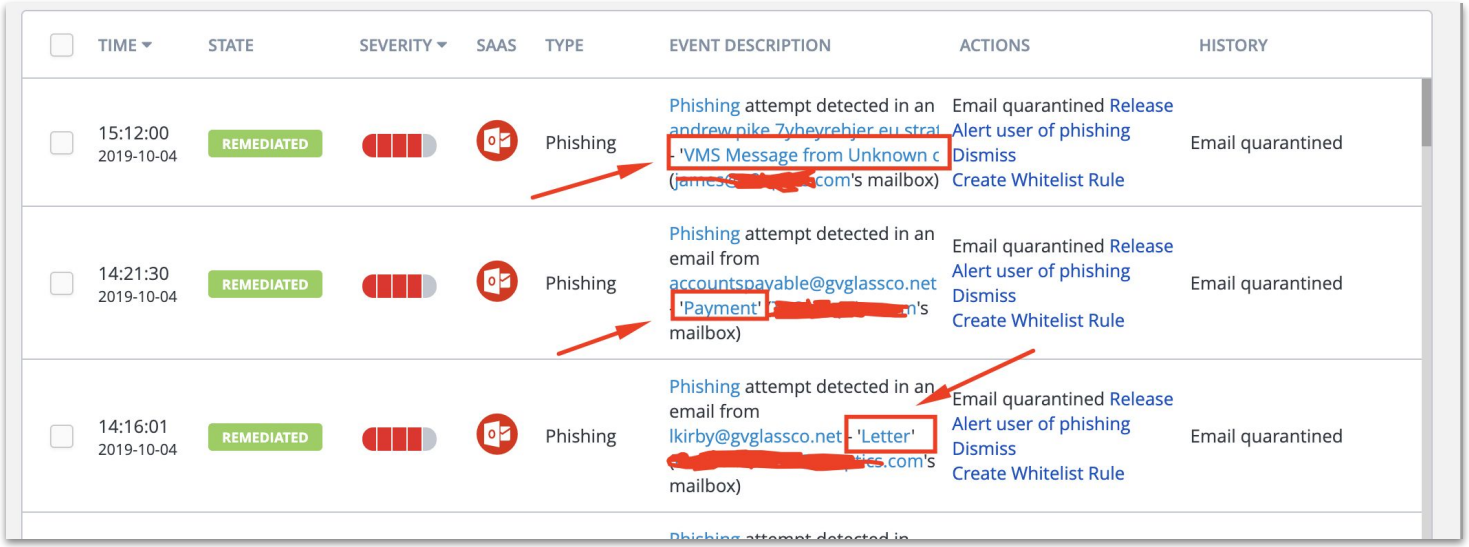
Configuration → Cloud App Store → Configure Outlook

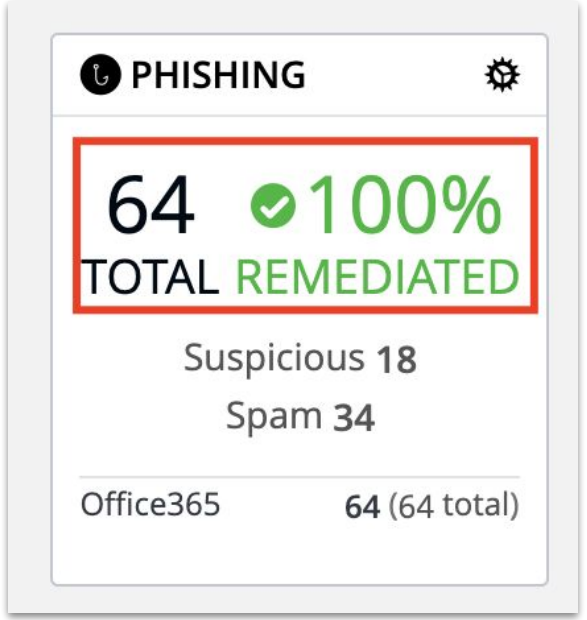


Responding to Incidents

When deploying Avanan for the first time, you will want to review catches for accuracy.

- Click on the phishing card to open up a filtered event view of phishing events.
- Then, browse through the events identified as phishing. Click on the subject of any email to view the email profile.

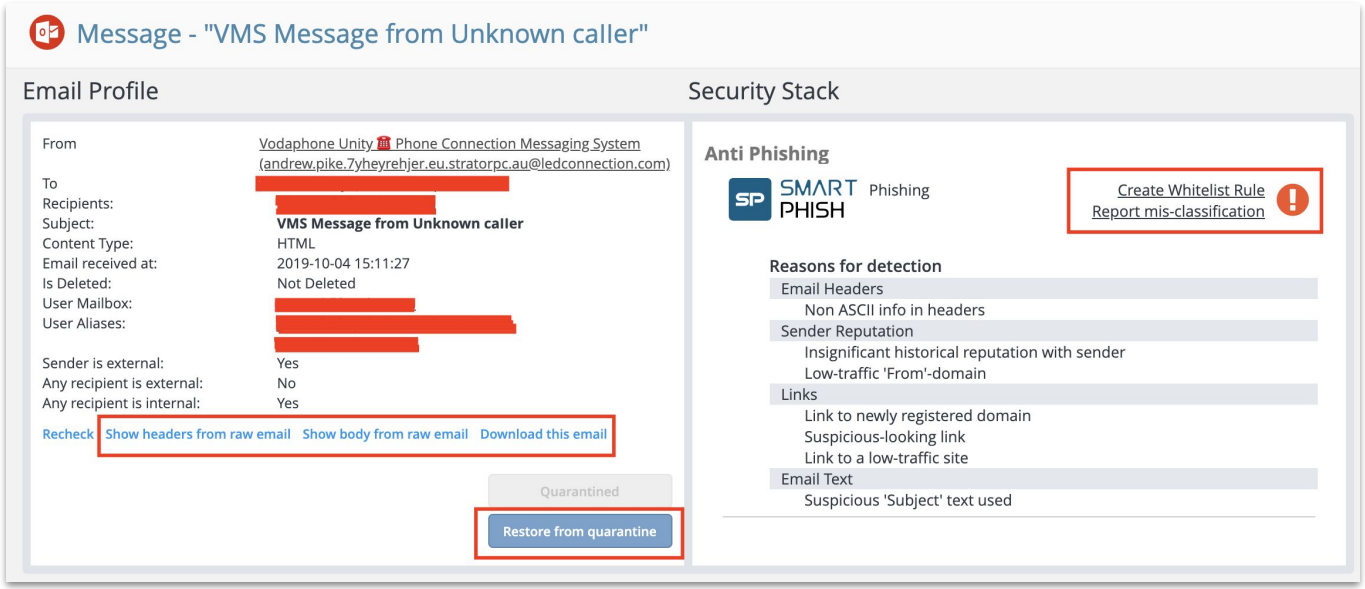




Responding to Incidents

The email profile page will display metadata and several options for investigation and mitigation. You can:

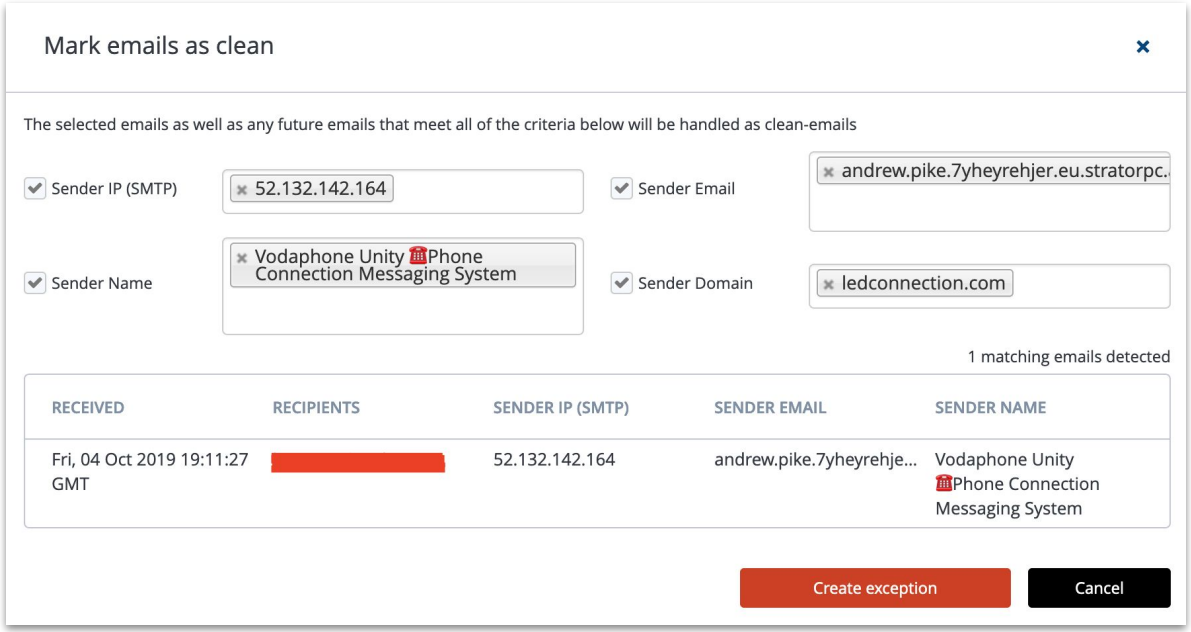
- View headers of the email
- View the body of the email (if the Avanan administrator has granted “View Private Data” rights)
- Download the email (if the Avanan administrator has granted “View Private Data” rights)
- View SmartPhish’s reasons for detection
- Create a Whitelist Rule
- Report a misclassification
  - This creates a training event for our machine learning)



Responding to Incidents

You can whitelist:

- Sender IP address
- Sender email
- Sender name
- Sender domain
- Any combination of the above. The more items that are checked, the more specific the whitelist is. The fewer items that are checked, the more broad the whitelist is.



When you create an exception, all emails will be marked as clean, and if applicable, will be released from quarantine. No future emails matching the conditions will be scanned by SmartPhish.

- Admins can manage your whitelist in Configuration → Antiphishing Whitelist