

Avanan Deployment Guide

Contents



Moving to Inline
Protection



Customizing
Policies

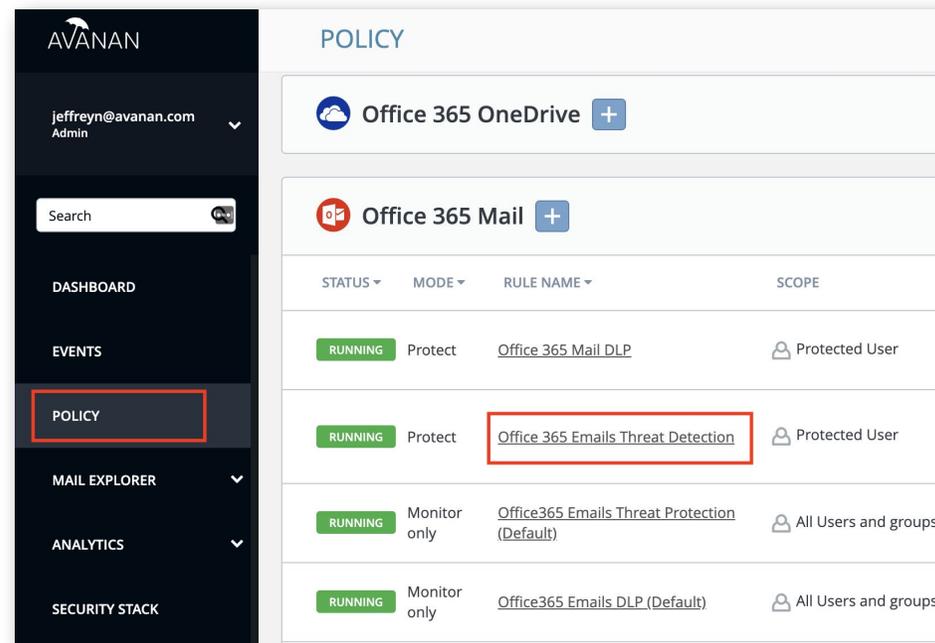


Responding to
Incidents

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).

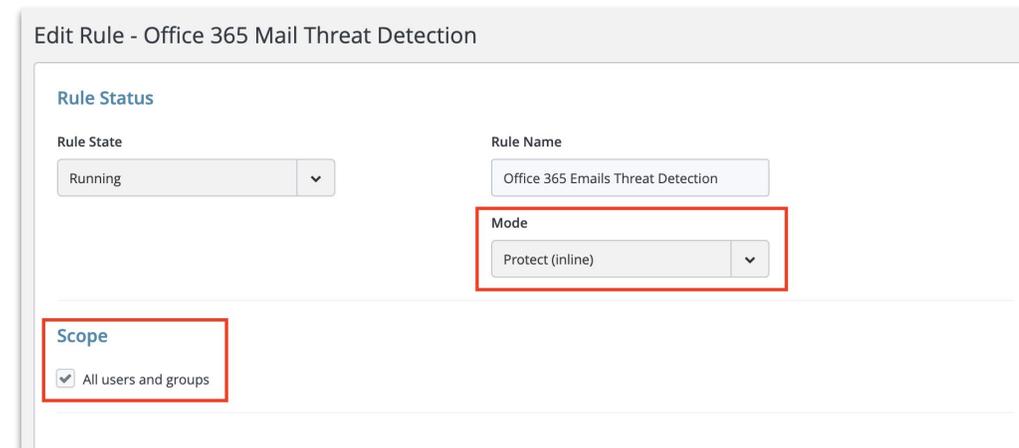


The screenshot shows the Avanan web interface. On the left is a dark sidebar with navigation options: DASHBOARD, EVENTS, POLICY (highlighted with a red box), MAIL EXPLORER, ANALYTICS, and SECURITY STACK. The main content area is titled 'POLICY' and shows configuration for 'Office 365 Mail'. Below this, there is a table of active policies.

STATUS	MODE	RULE NAME	SCOPE
RUNNING	Protect	Office_365 Mail DLP	Protected User
RUNNING	Protect	Office 365 Emails Threat Detection	Protected User
RUNNING	Monitor only	Office365 Emails Threat Protection (Default)	All Users and groups
RUNNING	Monitor only	Office365 Emails DLP (Default)	All Users and groups

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.



Edit Rule - Office 365 Mail Threat Detection

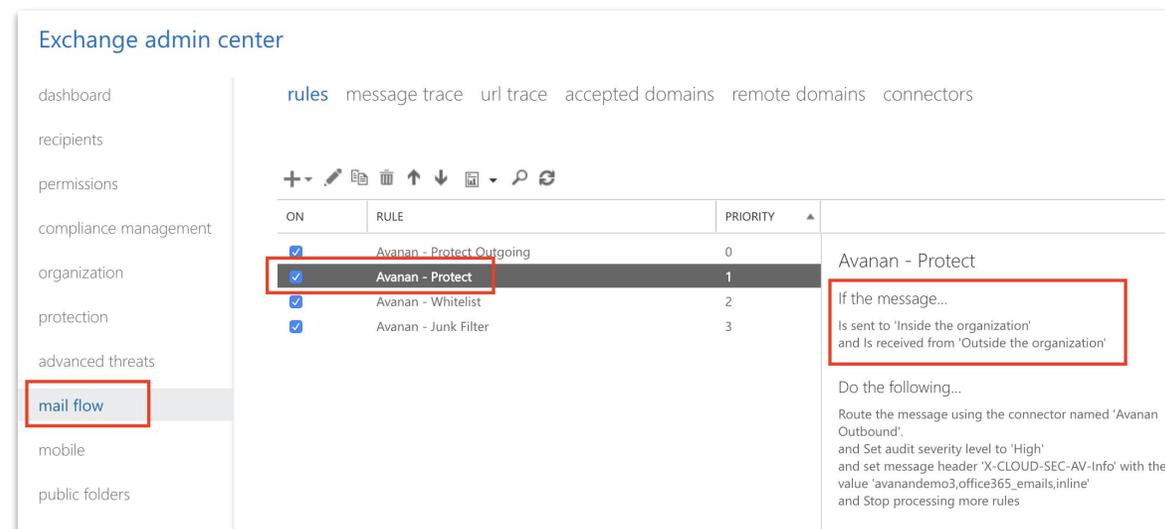
Rule Status

Rule State: Running

Rule Name: Office 365 Emails Threat Detection

Mode: Protect (inline)

Scope: All users and groups



Exchange admin center

rules message trace url trace accepted domains remote domains connectors

ON	RULE	PRIORITY
<input checked="" type="checkbox"/>	Avanan - Protect Outgoing	0
<input checked="" type="checkbox"/>	Avanan - Protect	1
<input checked="" type="checkbox"/>	Avanan - Whitelist	2
<input checked="" type="checkbox"/>	Avanan - Junk Filter	3

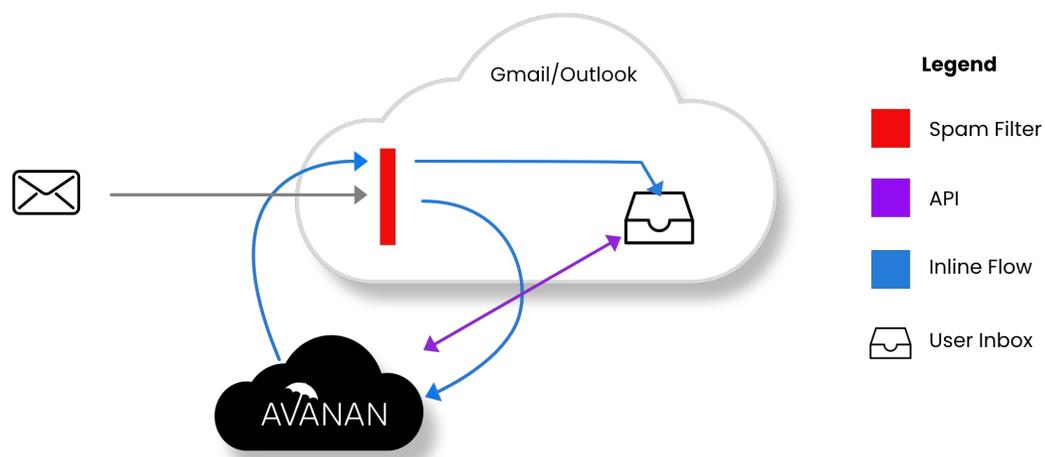
Avanan - Protect

If the message...
Is sent to 'Inside the organization'
and Is received from 'Outside the organization'

Do the following...
Route the message using the connector named 'Avanan Outbound'.
and Set audit severity level to 'High'
and set message header 'X-CLOUD-SEC-AV-Info' with the value 'avanandemo3.office365_emails,inline'
and Stop processing more rules

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).

POLICY

▼ **Advanced**

Malicious attachment workflow:

Quarantine. User is alerted, allowed to request a restore (admin must approve) ▼ ⚙

Phishing workflow:

Quarantine. User is alerted and allowed to request a restore (admin must approve) ▼ ⚙

Suspicious phishing workflow:

User receives the email with a warning ▼ ⚙

Spam workflow:

Add [Spam] to subject ▼

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**

Alerts

Send Email alert to... 

Send email alert to admin(s) about malware  

Send email alert to admin(s) about phishing  

Configuration → Cloud App Store → Configure Outlook

Configure Office 365 Mail Security
✕



Office 365 Mail
Top-of-the-line set of productivity tools

Re-authorize Avanan Office 365 Email App

Quarantine and workflow:

Dedicated quarantine mailbox:

Restore requests approver:

▶ Advanced

Cancel
Ok

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.

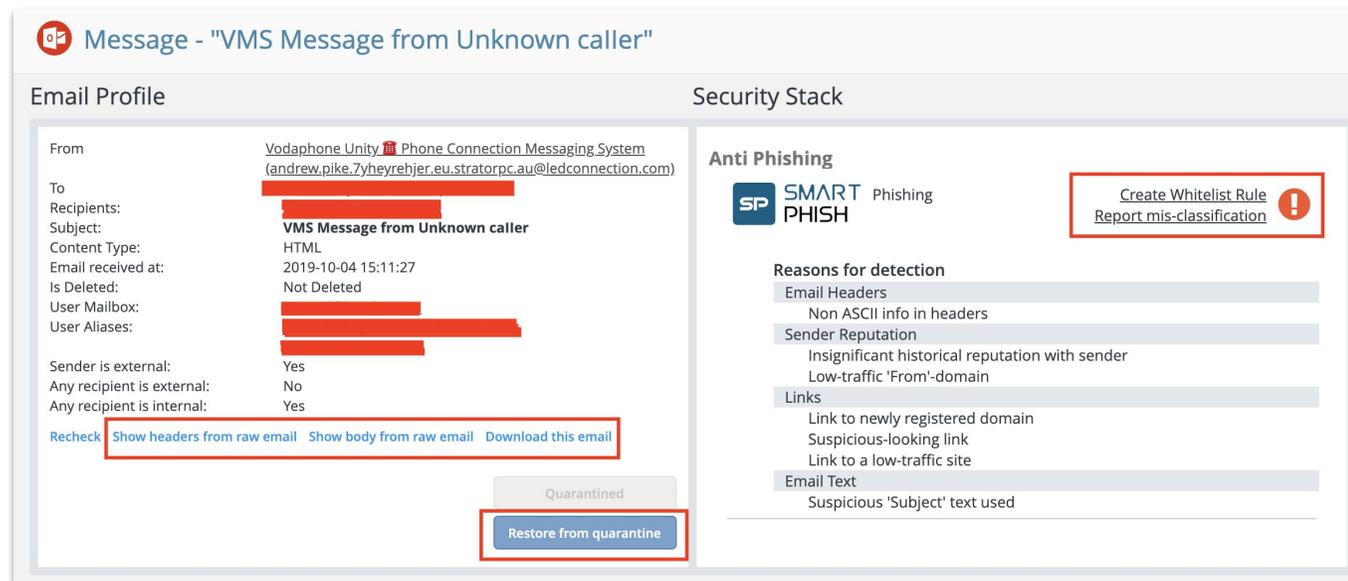


TIME	STATE	SEVERITY	SAAS	TYPE	EVENT DESCRIPTION	ACTIONS	HISTORY
15:12:00 2019-10-04	REMEDIED			Phishing	Phishing attempt detected in an email from andrew.pike.7yheyrehjier.eu.stral (james@...com's mailbox)	Email quarantined Release Alert user of phishing Dismiss Create Whitelist Rule	Email quarantined
14:21:30 2019-10-04	REMEDIED			Phishing	Phishing attempt detected in an email from accounts.payable@gvglassco.net ('Payment' ...'s mailbox)	Email quarantined Release Alert user of phishing Dismiss Create Whitelist Rule	Email quarantined
14:16:01 2019-10-04	REMEDIED			Phishing	Phishing attempt detected in an email from lkirby@gvglassco.net - 'Letter' ...'s mailbox)	Email quarantined Release Alert user of phishing Dismiss Create Whitelist Rule	Email quarantined

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)



Message - "VMS Message from Unknown caller"

Email Profile	Security Stack
<p>From: Vodafone Unity  Phone Connection Messaging System (andrew.pike.Zyheyrehjer.eu.stratorpc.au@ledconnection.com)</p> <p>To: [Redacted]</p> <p>Subject: VMS Message from Unknown caller</p> <p>Content Type: HTML</p> <p>Email received at: 2019-10-04 15:11:27</p> <p>Is Deleted: Not Deleted</p> <p>User Mailbox: [Redacted]</p> <p>User Aliases: [Redacted]</p> <p>Sender is external: Yes</p> <p>Any recipient is external: No</p> <p>Any recipient is internal: Yes</p> <p>Recheck Show headers from raw email Show body from raw email Download this email</p> <p>Quarantined</p> <p>Restore from quarantine</p>	<p>Anti Phishing</p> <p>SP SMART PHISH Phishing</p> <p>Create Whitelist Rule Report mis-classification </p> <p>Reasons for detection</p> <ul style="list-style-type: none"> Email Headers <ul style="list-style-type: none"> Non ASCII info in headers Sender Reputation <ul style="list-style-type: none"> Insignificant historical reputation with sender Low-traffic 'From'-domain Links <ul style="list-style-type: none"> Link to newly registered domain Suspicious-looking link Link to a low-traffic site Email Text <ul style="list-style-type: none"> Suspicious 'Subject' text used

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.

Mark emails as clean

The selected emails as well as any future emails that meet all of the criteria below will be handled as clean-emails

Sender IP (SMTP) Sender Email

Sender Name Sender Domain

1 matching emails detected

RECEIVED	RECIPIENTS	SENDER IP (SMTP)	SENDER EMAIL	SENDER NAME
Fri, 04 Oct 2019 19:11:27 GMT	[REDACTED]	52.132.142.164	andrew.pike.7yheyrehje...	Vodafone Unity Phone Connection Messaging System

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