vade
FOR M365

Vade for M365

Administrator Guide

Last modified: July 8, 2022

Version 2.48

VADE USA, INCORPORATED – 100 Pine Street, Suite 1250 – San Francisco CA 94111

Contents

Chapter
1

Overview

What is Vade for M365?

Vade for M365 protects your users and your company from highly sophisticated phishing, spear phishing and malware attacks, from the very first email.

Our filtering solution is based on machine learning models which perform real-time behavioral analysis to check the whole email, URLs and attachments.

Vade integrates seamlessly with your Microsoft 365 messaging solution and increases its security thanks to Artificial Intelligence.

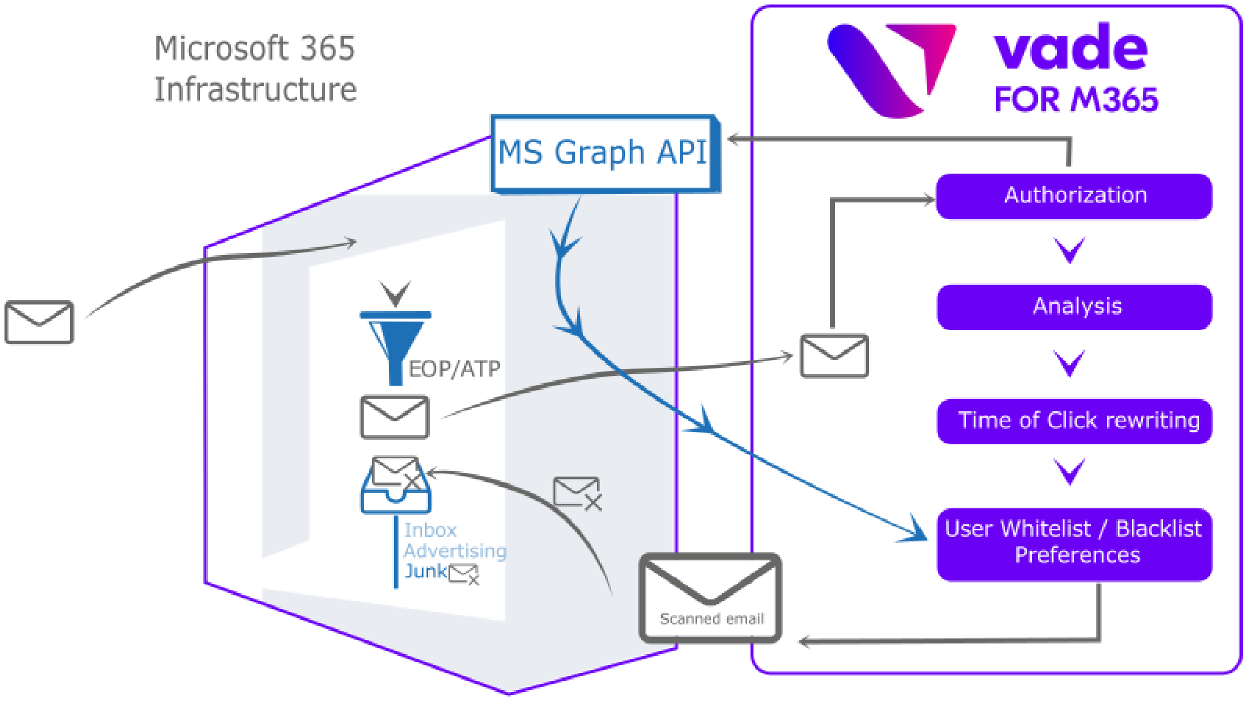
You can enable Vade for M365 in just a few clicks without any architecture change (no MX record changes). The administration UI was designed to provide simple configuration and full reports and analysis information about blocked attacks. Your users won't have to change the way they access their emails or use a new interface.

Supported browsers

The Vade for M365 admin console has been tested and is fully functional with the last version of the following browsers:

- Google Chrome
- Firefox
- Edge
- Safari

Architecture Diagram



How it works

1. When you receive a new message, Microsoft 365 scans it with EOP/ATP protection.
2. A copy of the email is then sent to Vade for M365 through the Microsoft 365 journal rules.
3. Vade for M365 performs the analysis on the copy of the message.
4. Vade for M365 connects to Microsoft 365 using MS Graph API, to retrieve the user preferences, etc.
5. Vade for M365 then moves the message to the proper subfolder, or deletes it using MS Graph API.

Activation process

Follow the steps below to set up Vade for M365.

Before you begin

You must contact your Vade Sales representative to subscribe to a valid license plan.

Procedure

1. Retrieve the Tenant ID on page 5
2. Activate your license on page 6
3. Confirm permissions on page 6
4. Create a journal rule
   - Create a journal rule via the Exchange admin center on page 6
   - Create a journal rule with command lines using Powershell on page 7

Retrieve the Tenant ID

Procedure

1. Log in to the Microsoft Azure Portal with your admin credentials.
2. Select ***Azure Active Directory*** under ***Azure services***.

Results
You will find the *Tenant ID* in the ***Overview***.

What to do next
Your Vade Sales representative will create your client account and order a license for you.

Activate your license

Procedure

1. Check your emails for an activation email sent by Vade.
2. Click ***Activate your license*** in your activation email.
   A window opens.
3. Check ***I accept*** to read and accept the Terms of service.

   Note: You can check the information about your license by clicking ***My license***.

4. Click ***Activate my license***.

Results
Your license is active.

Confirm permissions

Procedure

1. Log into the Vade admin console using a Microsoft 365Global Admin account.
   - For Europe: https://m365.eu.vadesecure.com/

     Note: Germany: https://m365.de.vadesecure.com/

   - For the US: https://m365.us.vadesecure.com/
   - For Asia: https://m365.asia.vadesecure.com/
2. Click ***Accept*** to accept the basic permissions required by Vade.
3. Click ***Continue***.
4. Click ***Accept*** to confirm all permissions in the pop-in window for the Vade platform to work properly.
   After confirming the permissions, you can log in to the console with a Global Admin account or an Exchange Admin account.

Create a journal rule via the Exchange admin center

Procedure

1. Go to the Exchange admin center.
2. Click ***compliance management*** in the left menu.
3. Click ***journal rules***.
4. Select an email address to ***send undeliverable journal reports to*** in case emails were not journalized.

   Warning: Microsoft 365 disables journaling on the address used to receive the reports so Vade for M365 cannot protect it. Consequently, we recommend using a dedicated address or an internal mailing list **outside the protected domain**.

   We provide dedicated email addresses for this exact purpose, add one to your contact list:

   a. Go to ***recipients*** > ***contacts*** > **+** > ***Mail contact*** in the left menu of your Exchange admin center.
   b. Type in `Vade - support journaling` in ***Display name***.

c. Type in `vs.support.journaling` in ***Alias***.

d. Copy one of the following Vade addresses and paste it in ***External email address*** according to your location:

  - For Europe:
    - Servers based in France: `undeliverable@bounce.eu.vadesecure.com`
    - Servers based in Germany: `undeliverable@bounce.de.vadesecure.com`
  - For the United States: `undeliverable@bounce.us.vadesecure.com`
  - For Asia: `undeliverable@bounce.asia.vadesecure.com`

e. Click ***Save***.

5. Add a journal rule to send a copy of the email traffic to Vade for M365:

   a) Click the **+** icon.
   The ***new journal rule*** window opens.

   b) Copy and paste your dedicated address under ***Send journal reports to***.

   - For Europe: `journal@m365.eu.vadesecure.com`

     Dedicated address for Germany: `journal@m365.de.vadesecure.com`
   - For the US: `journal@m365.us.vadesecure.com`
   - For Asia: `journal@m365.asia.vadesecure.com`

   c) Type the name of the rule.

   d) Select ***[Apply to all messages]*** or ***A specific user or group...*** under ***If the message is sent to or received from*** depending on your needs.

   e) Select `All messages` under ***Journal the following messages...***.

   f) Click ***Save***.

Results

You can now see your newly created journal rule in the list of rules. Make sure it is checked.

Related information

Create a journal rule with command lines using Powershell on page 7

Create a journal rule with command lines using Powershell

This section shows how to create a journal rule with Powershell.

1. Open a Powershell window.
2. Enter the following command to import the ExchangeOnlineManagement module:

```
Import-Module ExchangeOnlineManagement
```

3. Enter the following command to log in to Exchange Online:

```
Connect-ExchangeOnline -UserPrincipalName adminmail@domain.com
```

4. Enter the following command to send undeliverable journal reports to the address provided by Vade:

```
Set-TransportConfig -JournalingReportNdrTo
undeliverable@bounce.eu.vadesecure.com
```

Note:

- For Europe:

    - Servers in France: `undeliverable@bounce.eu.vadesecure.com`
    - Servers in Germany: `undeliverable@bounce.de.vadesecure.com`
  - For the United States: `undeliverable@bounce.us.vadesecure.com`
  - For Asia: `undeliverable@bounce.asia.vadesecure.com`

5. Enter the following command to create and activate your journal rule:

```
New-JournalRule -Name "Vade Journaling" -JournalEmailAddress
journal@m365.eu.vadesecure.com -Scope Global -Enabled $True
```

Frequently Asked Questions

Are Microsoft 365 EOP & ATP protections still available?

Yes, the Vade for M365 filtering comes on top of integrated EOP and ATP layers. The journal rules are triggered after the message has been scanned by the Microsoft 365 EOP and ATP filters.

How well does the Vade solution integrate with Microsoft?

In order to strengthen the Vade filtering engine, the integration of the Microsoft Exchange API now makes it possible to take advantage of spam and phishing reports sent from the Microsoft interface.

When a user reports a spam or a phishing attempt to Microsoft, the Vade filter also takes this feedback into account to improve its filtering engine and better protect them.

How to report an email to Microsoft while improving Vade filter?

As our filter improves each time you report an email through Outlook, do not hesitate to do so every time you receive an illegitimate message.

Report an email from Outlook Web:

1. Click the email to report.
2. Click ⋯.
3. Click ***Report message***.
4. Click ***Junk***, ***Phishing*** or ***Not Junk***.
5. Click ***Report*** in the pop-in window.

Report an email from the Outlook client:

1. Download the Report Message add-in on Microsoft AppSource.
2. Install the add-in.
3. Click the email to report.
4. Click ⋯.
5. Click ***Report message***.
6. Click ***Junk***, ***Phishing*** or ***Not Junk***.
7. Click ***Report*** in the pop-in window.

Do I need Exchange Online Protection (EOP) as well as the Vade solution to work effectively?

Exchange Online Protection is included within all Microsoft cloud email services such as Exchange Online and Microsoft 365, so no extra license is required. Vade can work as a standalone or as layered protection on top of EOP.

Will I stop receiving newsletters if the solution moves them?

You will still receive this type of email, depending on the settings in the Vade for M365 admin console. The filtered newsletters will be moved to the ***Newsletters*** subfolder in Outlook/OWA. If you do not need this feature, you can turn it off by selecting ***No action*** and you will receive newsletters in their main folder.

Will I see banners in the Outlook Desktop Client as well?

Yes, the experience in the Desktop Client is the same as in the Outlook Web App and across devices.

Does Vade keep a copy of all emails?

No, Vade deletes the copy after the analysis.

Do I need to update my MX record?

No, the MX record still points to Microsoft 365, and remains unchanged. The Vade for M365 is natively integrated to the Microsoft 365 platform through Microsoft API. As such, the only required step is to activate the solution so that the filter is allowed to scan your Tenant's emails. See Activation process on page 5.

Does the filter override my preferences?

The short answer is No! Vade for M365 is natively integrated to the Microsoft 365 platform. As such, the *Allowed* and *Block* lists you created are respected by the filter. There is only one exception to this: The user received a message which matches one of their *whitelist* entries, and which was identified as a `malware` by the filter. In this specific case only, the message will be deleted, moved to the corresponding folder, etc. according to your settings, even though your rule enforced a delivery in the *Inbox*.

⚠ **Important:** For administrator-level lists, Vade recommends using Exchange ***mail flow rules*** instead.

Does the filter override the inbox rules?

No, the inbox rules (e.g. *Move messages from ... to folder ...*) will always take precedence. Vade for M365 will only move messages that were meant to be delivered in the *Inbox*.

Where do I create whitelists in the product?

You can create whitelists on Microsoft 365. You may not create whitelists on the Vade for M365 platform itself.

⚠ **Important:** For administrator-level lists, Vade recommends using Exchange ***mail flow rules*** instead.

How come I get so many spear phishing notifications?

The spear phishing protection provided by the product notifies you about suspicious and potential risks. These risks, as described in the *Administration Guide*, include spoofing, calls to action, etc. As such, the solution will consider suspicious scenarios such as:

- A domain user sending an email from their Gmail account: The user is legitimate, but the email is coming from an external domain.
- Domain emails are sent from the outside (using external SMTP relays), with no matching SPF records.
- Etc.

Tip: In any case, these scenarios **are** suspicious, as they represent a potential breach in the email security you are setting up for your domain.

What happens in the case I have blacklisted an address which a user has whitelisted?

Filtering rules created on Microsoft 365 always take precedence over the filter decisions, or inbox rules created by the user.

Is the Vade filtering applied to all messages?

The Vade filtering is applied to all the emails in your users' mailbox, except when they are whitelisted, to ensure their protection. However, if a malware is detected, the filtering ignores user rules. For low priority emails, the Vade filtering system applies only on inbox and junk folder.

How to use admin whitelists?

Create mail flow rules to make sure Vade for M365 takes into account your Microsoft 365 whitelist.

About this task

The whitelist you created on Microsoft 365 might not always be shared with our solution: Vade for M365 recommends creating ***Mail Flow rules*** directly in the Microsoft 365 configuration to make sure we do not filter desired emails.

In order to create ***Mail Flow rules***, follow these steps:

Procedure

1. Log in to the Microsoft 365 admin center.
2. Go to ***Mail flow*** > ***Rules*** > **+** > ***Bypass spam filtering...***.
   The ***new rule*** window opens.
3. Create a new mail flow rule:
   a) Enter a name for the rule.
   b) Select ***The sender...*** in the ***Apply this rule if..*** drop-down menu.
      - Select ***domain is*** to whitelist a domain, or
      - Select ***Adress matches any of these text patterns*** to whitelist one or more sender email addresses.

   c) Enter the domain name or the address you want to whitelist in the new pop-in window.
   d) Click **+** > ***OK***

   Any email from the domain or the sender you have entered is now whitelisted by Microsoft filters (EOP and ATP).

   Tip: You may even add a condition which matches the recipient of the message to be even more restrictive.

4. Add the following actions in the ***new rule*** window for Vade to stop filtering the emails specified earlier:
   a) Click ***add action***.
   b) Select ***Modify the message properties...*** > ***set a message header*** in the drop-down menu.
   c) Click the first ***Enter text...*** link in the text on the right.
   The ***message header*** pop-in window is displayed.
   d) Enter the following value: `X-VADE-0365`.
   e) Click ***OK***
   f) Click the second ***Enter text...*** link.
   The ***header value*** pop-in window is displayed.
   g) Enter the name of the client.
   h) Click ***OK***.
5. Uncheck the ***Audit this rule with severity level*** box.
6. Click ***Save***.

Results

The new rule is now on display in your ***Rules***.

Tip: Make sure the new rule is checked in the ***Rules*** list.

How to manage reports?

Vade for M365 allows you to schedule reports, update report scheduling and cancel them as well.

How to schedule reports?

You can configure the *Threat Report* and the *Low Priority Report* to receive them automatically by email, as PDF files and on a regular basis.

1. Click ***Reports*** on the left panel of the Vade for M365 admin console.
2. Click ***Threats*** or ***Low Priority***.
3. Click ***Schedule report*** in the top right corner.
4. Enter a comma-separated list of email addresses to send the report to in the ***To*** field of the pop-in window.
5. Select how often you want to receive reports (daily, weekly, monthly) in the ***Frequency*** field.
6. Check ***Threats*** and/or ***Low Priority*** to receive Threat and/or Low Priority reports.
7. Click ***Save***.

Depending on the frequency the user chooses, they will receive the reports from the alias ***Vade for M365*** at different times for different time frames.

Frequency	Day	Time (time zone of the profile)	Time frame
Daily	Every day	7 am	Previous day from 12:00 am to 11:59:59 pm
Weekly	Mondays	7 am	Previous week from Monday 12:00 am to Sunday 11:59:59 pm
Monthly	First day of the month	7 am	Previous month from the first day 12:00 am to the last day 11:59:59 pm

How to edit my report?

In order to edit your report, you must:

1. Click ***Reports*** on the left panel.
2. Click ***Threats*** or ***Low Priority***.
3. Click ***Schedule report*** in the top right corner.
4. Edit the fields you want to update in the pop-in window.
5. Click ***Update*** at the bottom of the pop-in window.

How to cancel my report?

In order to cancel your report, you must:

1. Click ***Reports*** on the left panel.
2. Click ***Threats*** or ***Low Priority***.
3. Click ***Schedule report*** in the top right corner.
4. Click ***Remove scheduling*** at the bottom of the pop-in window.

Related information

Threat Report on page 32

Low priority Report on page 33

How to revoke the rights of Vade for M365?

If you do not want to be protected by Vade for M365 anymore, you need to follow a few step process to revoke its rights.

Procedure

1. Delete the journal rule.
   a) Log in to the Microsoft Admin Center.
   b) Click the ***left menu*** > ***Show all*** > ***Exchange*** > ***Classic Exchange admin center*** > ***compliance management*** > ***journal rules***.
   c) Check the box next to the journal rule.
   d) Click the bin icon.
   The journal rule is deleted.
2. Remove the application.
   a) Log in to the Azure Portal
   b) Go to ***left menu*** > ***Azure Active Directory*** > ***Enterprise applications***.
   The application list is displayed.
   c) Click ***Vade for M365*** in the table.
   The ***Vade for M365*** window opens.
   d) Click ***Properties*** under ***Manage*** in the middle menu.
   e) Click the ***Delete*** button to delete the application and revoke rights.
   The application is removed.

   Vade for M365 cannot access or process your emails anymore.

How to grant my partner access to my admin console?

With just a click, you can grant your partner access to your Vade for M365 admin console.

Before you begin

Your partner needs to request access from the Partner Portal and follow these steps:

Procedure

1. Log in to the Partner Portal.
2. Click the ***Clients & Licenses*** tab.
3. Click the ***Request access*** of a specific client.

Results

Access pending is now displayed after refreshing the page. You or your administrative contact will receive an email inviting you to log in to your admin console.

ⓘ **Note:** After logging in to your Vade for M365 admin console, go to ***Settings*** > ***Global*** and enable the ***Grant partner access to my admin console*** toggle. The partner will receive an email confirming their access to your console and have a direct access to the admin console via an ***Access*** button.

How to revoke access to the admin console?

You might change your mind and want to revoke the access to your admin console from your partner.

Before you begin

You need an admin account to revoke the access.

Procedure

1. Log in to the Vade for M365 admin console.
2. Click ***Settings*** > ***Global*** in the left menu.
3. Disable the ***Grant partner access to my admin console*** toggle in the ***Partner access*** section.

Results

The toggle turns gray. Your partner will be informed by email that they no longer have access to the admin console.

How to retrieve emails?

As an administrator, you can download emails as .eml files, even deleted ones.

Before you begin

You need a Global Admin account to perform this task.

Procedure

1. Log in to the Microsoft 365 Security & Compliance Center.
2. Add a new eDiscovery Administrator:
   a) Click ***Permissions*** in the left menu.
   b) Check the ***eDiscovery Manager*** box.
   The ***eDiscovery Manager*** pop-in window opens.
   c) Click ***Edit*** next to ***eDiscovery Administrator***.
   The ***Editing Choose eDiscovery Administrator*** window opens.
   d) Click ***Choose eDiscovery Administrator***.
   e) Click ***Add***.
   f) Check the box of the administrator in the list.
   g) Click ***Add*** > ***Done*** > ***Save*** > ***Close***.

   You are now a member of the eDiscovery Manager group. You must log off and log back in to benefit from your new rights.
3. Click ***Search*** > ***Content search*** in the left menu.
   The ***Content search*** window opens.
4. Run a new search query.
   a) Click ***+ New search***.
   b) Enter a name and a description.
   c) Click ***Next***.
   d) Turn on all ***Specific locations*** in the status column.
   e) Click ***Next***.
   f) ***Add conditions*** and ***Keywords*** of the emails you wish to retrieve.
   g) Click ***Next*** > ***Submit***.

   Your search is added to the list.
5. Check the box of your search in the list of search.
   A window of your search opens.
6. Click ***Action*** > ***Export results*** > ***Export***.
   A new export is created in the Export table.

7. Click *Export*.
8. Check the box of your results in the Export table.
9. Click *Download results*.

How to export email logs?

Export your email logs as a .csv file thanks to the **Export to CSV** feature.

Before you begin

Go to *Logs* > *Emails* in the Vade for M365 admin console.

Procedure

1. Apply any search criteria.
   You can now click the *Export to CSV* button if less than 1,000 logs are available.
2. Click the *Export to CSV* button.

Results

Your browser downloads your filtered log list as a .csv file.

Note: The log file contains the following information, separated by semi-colon:

Date and time
The date and time of the email.

Sender
The sender of the email (MAILFROM).

Sender Header
The header of the sender (FROM).

To
The recipient of the email (RCPT TO).

Subject
The subject of the email.

URL
The URLs contained in the email, separated by a space.

Attachments
The attachments contained in the email, separated by a space.

Status
The status of the email.

Action
The actions applied to the email.

Destination
The destination folder of the email if one of the actions was *MOVED*.

Remediation
The remediation status of the email, if any (*manual* or *auto*).

Support

Vade provides technical support by phone or email for Vade for M365.

Vade support can be joined 7/7, and 24/24, via:

Email:

support@vadesecure.com

Phone:

- France: +33 3 59 61 66 51
- Germany: +49 32 221097669
- Switzerland: +41 31 528 17 38
- USA: +1-360-359-7770
- Japan: +81-3-4577-7747

Note: Support is available in English and French.

Chapter 2

Dashboard

Dashboard

The dashboard provides a global insight of the last detected threats filtered by the platform.

The dashboard provides figures and charts representing the number of threats by type over time and a detail of the last threats identified.

The dashboard can be configured to provide details over a 1-day, 7-day (default) or 30-day periods.

On this page, you can:

- click 🛡 ***Protection mode enabled*** to open the Settings page.
- click ***View reports*** to open the Threat report page.
- click ***View logs*** or any threat name or figures to open the Email logs page.

Threats detected

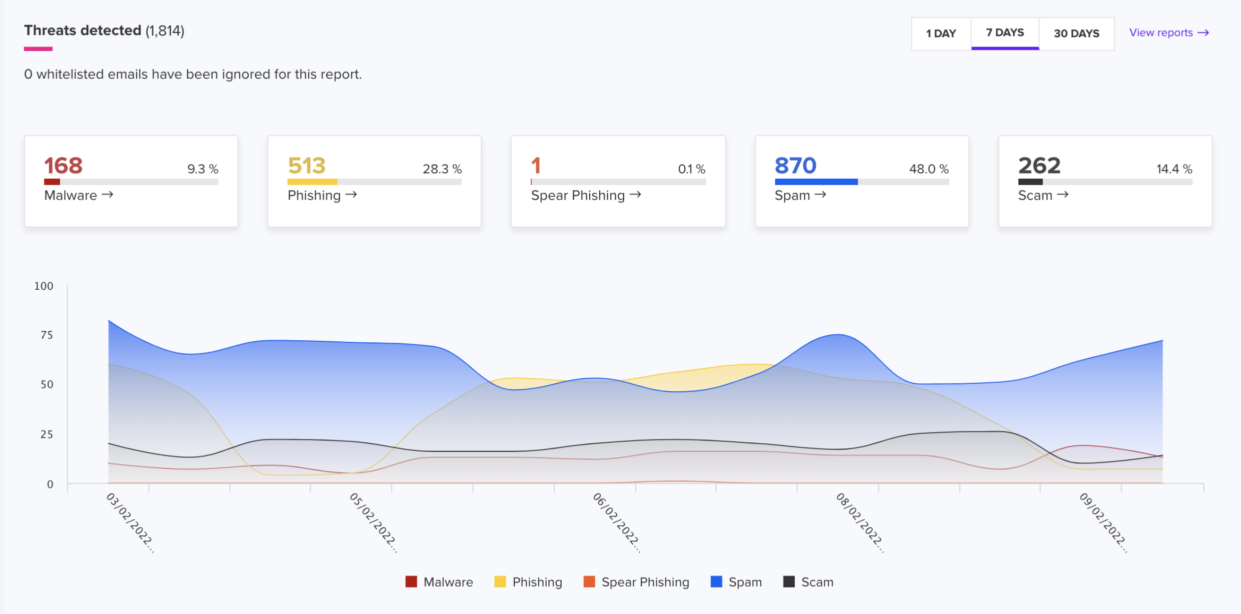
This section offers an overview of the threats detected by Vade for M365 during the period of time you selected in the top right-hand corner.

Note: Whitelisted emails are not taken into account in this analysis.

Above each category of threat (malware, phishing, spear phishing, spam and scam), you can see how many of them were detected during the selected period of time and their share in percentage among all threats.

You can also check the chart below to get a visual representation of the threats our solution has detected.

Tip: Click a threat to display the email log page filtered on this specific threat.



Threats detected (1,814)

1 DAY | 7 DAYS | 30 DAYS | View reports →

0 whitelisted emails have been ignored for this report.

168	9.3 %	Malware →
513	28.3 %	Phishing →
1	0.1 %	Spear Phishing →
870	48.0 %	Spam →
262	14.4 %	Scam →

Last targeted attacks

This section displays details of the last threats our solution has detected.

Date & time

The date and time the message was originally processed.

From

The email address of the sender.

To

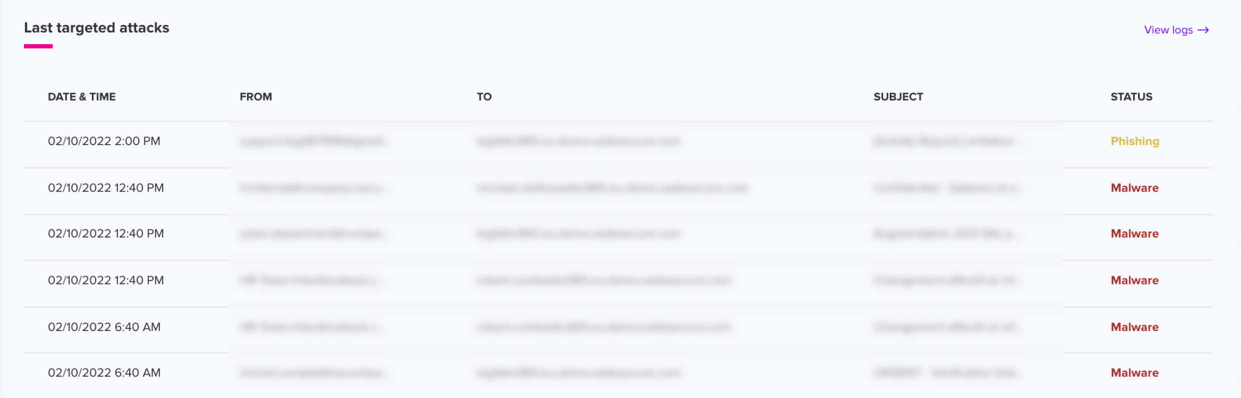
The email address of the recipient.

Subject

The subject of the message.

Status

The filtering status for the message : phishing, malware or spear phishing.



Last targeted attacks

View logs →

DATE & TIME	FROM	TO	SUBJECT	STATUS
02/10/2022 2:00 PM	[illegible]	[illegible]	[illegible]	Phishing
02/10/2022 12:40 PM	[illegible]	[illegible]	[illegible]	Malware
02/10/2022 12:40 PM	[illegible]	[illegible]	[illegible]	Malware
02/10/2022 12:40 PM	[illegible]	[illegible]	[illegible]	Malware
02/10/2022 6:40 AM	[illegible]	[illegible]	[illegible]	Malware
02/10/2022 6:40 AM	[illegible]	[illegible]	[illegible]	Malware

Related information

Settings - Global on page 40

Email logs on page 18

Threat Report on page 32

Logs

Email logs

This page displays filtering logs in real time, allows you to search for specific log entries and to remediate and report emails.

Log search

You can search for specific log entries by providing search criteria in the search bar, and a specific period.

Notice: If you do not use any filter, the search string will match the following fields: ***FROM***, ***SUBJECT***, ***TO*** and ***CAMPAIGN ID***.

Period field

This field allows you to limit the search to a given period of time. Available default ranges are `1 hour`, `4 hours`, `1 day` and `7 days`. You may also specify a custom range by providing a start and end date as well as an exact time of day by clicking on the ***Custom*** button.

[Filters]

The search field allows you to search for a sender, a recipient, a subject, an action, a status, emails with attachments and emails with URLs.

You can apply one or several filters after clicking on the ***Filters*** button.

Note: Select ***CONTAINS*** for ***FROM***, ***SUBJECT*** or ***TO*** if you want to display emails matching partially what you are looking for, or ***IS*** if you want to display emails matching perfectly what you are looking for.

FROM

Type in an email address or part of an email address to display all the emails sent from the matching addresses.

TO

Type in an email address or part of an email address to display all the emails sent to the matching addresses.

SUBJECT

Type in the whole subject or part of a subject to display all emails matching those words.

CAMPAIGN ID

Type in a campaign ID to display all emails impacted by specific remediation campaigns.

STATUS

Threat

Emails identified as

- Malware
- Phishing
- Spear phishing

- Spam (high spam, medium spam, low spam)
- Scam

Legitimate

Emails identified as

- Low priority (newsletters, social, purchase, travel)
- Whitelists

Note: Select one of the subcategories to display only a certain type of threat.

ACTION

Moved

Emails Vade for M365 moved.

Banner

Emails detected as spear phishing with a Vade for M365 warning banner.

Deleted

Emails Vade for M365 deleted.

Attach. removed

Emails Vade for M365 removed malicious attachments from.

No action

Emails Vade for M365 did not handle.

REMEDIATED

Auto

Auto-remediated emails.

Manual

Manually remediated emails.

Not remediated

Emails not remediated.

MANUAL REPORTS

Reported as legitimate

Emails that have been reported as legitimate.

Reported as malicious

Emails that have been reported as malicious.

Not reported

Emails that have not been reported.

URL

ALL

Emails, with or without URLs.

WITH

Emails with at least one URL.

WITHOUT

Emails without any URLs.

ATTACHMENTS

ALL

Emails, with or without attachments.

WITH

Emails with at least one attachment.

WITHOUT

Emails without any attachments.

CURRENT EVENTS

Displays all emails including news keywords, defined by Vade, in their subject and/or body (such as *Black Friday*, *elections*, etc.). These words will be updated regularly to keep up with current events.

Note: If the email is identified as ***Legitimate*** or *graymail*, the word must appear at least twice in the email to be filtered by ***Current Events***. It must only appear once if the email is identified as ***Threat***.

Real-time logs

In order to view the real-time processing logs of the filtering solution, enable the ***Real-time log mode*** by clicking the switch button.

This will display the processing logs of all incoming emails processed by the platform.

Note: When the ***Real-time log mode*** is enabled, the ***Export to CSV*** and ***Remediate*** button are not available.

Search results

The logs matching the search criteria will be displayed in a table providing:

Date & Time

The date and time the email was originally processed.

From

The email address of the sender.

To

The email address of the recipient.

Subject

The subject of the email.

Status

The filtering status for the email, which corresponds to one of the status that can be configured under the Settings page for spam, phishing, etc. The list of potential status is:

Legitimate

The Vade filter identified the email as legitimate.

Phishing

The Vade filter identified the email as a phishing attempt.

Malware

The Vade filter identified a malware contained in the email.

Spear phishing

The Vade filter identified the email as a spear phishing attempt (because of partial or complete spoofing, etc.).

Low spam

The Vade filter identified the spam as an emailing campaign sent through professional routing platforms (ESP). These market players follow the rules of use for email advertising, by providing unsubscribe links, list cleaning, etc.

Medium spam

The Vade filter identified the spam as an emailing campaing not sent through a professional routing platform. The heuristic rules that catch these emails are predictive and generic.

High spam

The Vade filter identified the email as a spam not complying to emailing rules and presenting poorly organized content, non-compliant with CAN-SPAM, missing unsubscription links, etc.

Scam

The Vade filter identified the email as a scam.

Newsletters

The Vade filter identified the email as a newsletter.

Social

The Vade filter identified the email as a social network notification.

Purchase

The Vade filter identified the email as a purchase confirmation, billing and invoices information, etc.

Travel

The Vade filter identified the email as a travel plan confirmation.

Whitelists

The email matched one of the ***whitelists*** configured by the user or administrator on Microsoft 365. The action performed corresponds to the action defined for whitelisted emails on Microsoft 365.

Blacklists

The email matched one of the ***blacklists*** configured by the user or administrator on Microsoft 365. The action performed corresponds to the action defined for blacklisted emails on Microsoft 365.

Remediation

The remediation status:

- Remediated, or
- Not remediated (empty field)

The exposure of the user:

- Email opened, or
- Email unopened

Note: Only available after a remediation if the email has not been deleted by the user.

Action

The action taken on the message depending on the action configured for the message status. Potential actions are:

Moved

The email was moved from the inbox to another folder.

Deleted

The email was deleted.

Banner

A warning banner was added to the email.

No action

No action was performed on the email.

Note: Click the ⋯ ***dot icon*** > ***Details*** next to a specific email and check the ***No action*** section to know why no action was performed.

Attach. removed

Malicious attachments were removed from the email.

Failed

This action may occur when trying to perform actions on emails sent to a distribution list, for which the recipient no longer exists on Microsoft 365 (but was removed from the distribution list). This prevents Vade for M365 from taking any action on the email.

Attachments/URLs

If the email contains an attachment, this column displays the 📎 attachment icon. If it contains a URL, the column displays the 🔗 URL icon.

Details

Clicking the ··· ***dot icon*** > ***Details*** opens a new tab:

An overview of the details at the top of the page displays the status of the email, the last action applied to it, the delivery date and time, the sender, the recipient and the subject.

Description

The Message ID, the Sender Header, the Sender IP and the size of the email.

History

All actions applied, automatically or manually, to the email, including date and time. A ***Remediate*** button is also available if you want to manually remediate an email.

Attachments

The name and size of each attachment.

Click the ⤓ icon to download the attachment.

Click the 🔍 icon to access analyze the attachment further:

⚠ **Important:** We can only analyze PDF, Microsoft Word, Excel and PowerPoint files under 15 Mb.

- ***Attachment source:*** Information about the email of the attachment and the parent of the attachment.
- ***Properties:*** First-level analysis of the document.
- ***Features:*** Main attributes of the file.
- ***Embedded links:*** URL or mailto links found in the attachment.
- ***Code Analysis:*** Details of the code detected in the attachment.
- ***Embedded files:*** Details of the different files detected in the attachment.

URL

URLs included in the email.

ⓘ **Note:** The first tab closes when you open more than 3 tabs.

Log search reset

Delete the content of the search bar and press Enter, or click the ***X*** button.

Export to CSV

Select a filter and click the ***Export to CSV*** button to export a .csv file of the list on display.

Remediate

Select a filter and click the ***Remediate*** button to remediate and report emails.

Related tasks

How to export emails logs? on page 14

Related information

How to search more accurately with a dedicated syntax in the search bar? on page 23

How to remediate emails? on page 25

Filtering use cases

Let's say you don't use any filter and search for the word `phishing`, you will find it in email addresses (be it the sender or the recipient), in subjects, in email bodies and even as a verdict.

Now, you want to search for all the emails you received from `Tom Watson`. You will have to use the filter `from`:

```
from:"tom.watson@test.com"
```

Note: Make sure you use quotation marks if you want a perfect match in your search results.

If you want to search for all the emails `Tom Watson` sent to `Emma Tomson`. You will have to use `from` and `to` filters:

```
from:"tom.watson@test.com" AND to:"emma.tomson@test.com"
```

You may not trust Tom and want to display all emails he sent that are considered as spams by Vade for M365, then you need to use:

```
from:"tom.watson@test.com" AND status:"SPAM"
```

You may be wondering which of Tom's emails our solution deleted. You can just check it out with:

```
from:"tom.watson@test.com" AND action:"DELETE"
```

You only want to see Tom's emails with URLS and attachments. To do that, just type:

```
from:"tom.watson@test.com" AND hasattachment:"YES" AND hasurl:"YES"
```

Finally, you want to ignore emails with a subject containing "dear":

```
from:"john.doe@example.com" AND hasattachment:"YES" AND hasurl:"YES" AND NOT
subject:dear
```

For more information, explore "How to benefit from the powerful search bar?" above the search bar and the Lexicon right to the search bar.

Filtering log fields

As every mail processing platform, we have a duty to keep the filtering logs for a given period of time (depending on local regulations and laws).

The logs stored by the platform include the following information:

[Filter specific information]

Most of the information logged contain details about the filter analysis itself, such as the current filter version, the date of the analysis, unique analysis IDs, filter verdicts and spamcause, etc.).

SMTP headers & envelope

Some of the original SMTP headers & envelope information contained in the message are returned:

Message ID

The Unique ID of the message (generated by the mail platform itself, such as Microsoft 365).

helo

The contents of the HELO command that occurred during the transaction.

mail from

The contents of the MAIL FROM command that occurred during the transaction, typically containing the email address of the sender.

From header

The email address declared in the From: header of the message, which may differ from the address used in the SMTP MAIL FROM command.

rcpt to

The contents of the RCPT TO command that occurred during the transaction, typically containing the email address of the recipient.

To header

The email address declared in the To: header of the message, which may differ from the address used in the SMTP RCPT TO command.

Subject

The contents of the Subject header of the message.

Source IP

The originating IP the message was sent from. In addition, the metadata returned may contain information about the IP range this source IP belongs to (/24 usually).

Domain

The domain part of the sender's address.

Received

An array containing the list of Received headers found in the message headers, which trace the route the message has taken from the sender to the recipient.

Authentication results

Contains the following information about various Auth results, if present:

- SPF check result for sender's IP and domain
- DKIM results
- DMARC results

URL related information

A boolean indicating if URLs were found in the message, and if present, a list of URLs found in the message.

Attachment-related information

The metadata may contain information about the attachment, if present:

Content-Type

The Content-type declared for the message.

Number of attachments

If present, the number of attachments found in the message, otherwise 0.

Attachment names

If present, an array containing the list of the attachment names.

Mime Version

The mime version declared for the message part.

[Microsoft 365 specific headers]

As part of the Microsoft 365 processing, the metadata returned may contain information provided by Microsoft 365 through their native API:

malware

A boolean indicating if the message matched as containing a malware.

blacklisted

A boolean indicating if the message matched a Microsoft 365 user blacklist.

whitelisted

A boolean indicating if the message matched a Microsoft 365 user whitelist.

folder

The folder the message was moved to.

action

The action taken on the message by Microsoft 365.

Verdict information

Verdict information returned by Microsoft 365, based on their EOP analysis of the message: obcl, opcl, oscl, score.

Remediate and report emails

Remediate lets Vade for M365 protect your users **before** the attack (**predictive technology**), **during** the attack (data gathered from more than 1 billion mailboxes to live-remediate any attack) and **after** the attack. In order to respond after an email attack, Vade for M365 allows you to move users' emails from their delivery folder to any other folder or even delete them.

How to remediate a single email?

1. Go to the Email logs page.
2. Search the email you want to remediate.
3. Click the ∘∘∘ icon for the corresponding email.
4. Click ***Remediate*** in the drop-down menu.
5. Click ***Next*** in the pop-in window.
6. Check the ***Remediate*** box.
7. Choose a folder to move the email into.

   Note: You can also report the email as legitimate or malicious by checking the corresponding box.

8. Click ***Confirm***.

   The pop-in window displays the information of the selected email, and the available actions.

How to remediate multiple emails?

1. Go to the Email logs page.
2. Click ***Filters***.
3. Select a filter.
4. Click the ***Remediate*** button in the top right corner of the list.
5. Select the emails to remediate and to report in the popin window.

   Note: The emails are all selected by default.

6. Click ***Next***.
7. Check the ***Remediate*** box.
8. Choose a folder to move the emails into.

   Note: You can also report the emails as legitimate or malicious by checking the corresponding box.

9. Click ***Confirm***.

Tip: The console displays up to 100 emails by default, but you can select as many as 500 emails in the pop-in window.

Pop-in window actions

After clicking the ***Remediate*** button, a pop-in window allows you to take action:

- ***Remediate*** the emails you selected, and select the folder to move the emails to.

- ***Report as legitimate***.
- ***Report as malicious***.

You can check the ***Report as legitimate*** or ***Report as malicious*** box to help our teams improve the accuracy of the solution.

You can also ***Edit*** the emails you selected, ***Close the pop-in window*** or simply ***Confirm*** at the bottom of the page.

Related concepts

Remediation logs on page 26

Related information

Event logs on page 29

Tracking

It is mandatory to keep track of remediation actions in logs, i.e. who moved the emails, when, and which one(s).

Several ways are available for you to track emails.

Remediation logs

Any remediation and auto-remediation are recorded and displayed in the remediation logs. These logs can be filtered by status, action and remediation type to analyze all actions applied to the emails of the users.

Event Logs

This page displays all actions taken by users like remediations, setting updates, etc.

1. Click the ***Filters*** button and select ***Remediate*** to display all remediated emails.
2. You can check who used the ***Remediate*** action and the date of the action in the event list.
3. Click the ⋯ ***icon*** > ***View logs*** to see how many emails were remediated for that event, and what folder they were moved to.

Note: In case of remediation of an email in another pending remediation, the description shows: ***[NUMBER OF MESSAGES] messages skipped due to pending remediation***.

Remediation logs

This page displays remediated campaigns by type of remediation and auto-remediation.

Any remediation is recorded and displayed in the remediation logs. You can filter them to analyze all actions taken on the emails of your users.

Type
The type of remediation: auto-remediation or manual remediation.

Date
The date of the remediation.

Campaign ID
The ID of the campaign.

Affected users
Percentage of users that opened the email before remediation.

Remediated
The number of remediated or auto-remediated emails.

Updated status

The last status of a campaign.

Action

The action performed on the campaign.

Details

The ***View logs*** buttons redirects the user to the logs of the selected campaign.

URL logs - Time-of-Click

This page displays logs related to URLs scanned by **Time-of-Click**, and allows you to search for specific log entries, and view logs in real time.

Log search

You can search for specific log entries by providing search criteria in the ***search bar***, and a specific period.

ⓘ **Notice**: If you do not use any filter, the search string will match the following fields: ***FROM***, ***TO*** and ***URL***.

Period field

This field allows you to limit the search to a given period of time. Available default ranges are `1 hour`, `4 hours`, `1 day` and `7 days`. You may also specify a custom range by providing a start and end date as well as an exact time of day by clicking on the ***Custom*** button.

[Filters]

The search field allows you to search for a sender, a recipient and URLs.

You can apply one or several filters after clicking on the ***Filters*** button.

ⓘ **Note**: Select ***CONTAINS*** for ***FROM*** or ***TO*** if you want to display emails matching partially what you are looking for, or ***IS*** if you want to display emails with URLs matching perfectly what you are looking for.

FROM

Type in an email address or part of an email address to display all the emails sent from the matching addresses.

TO

Type in an email address or part of an email address to display all the emails sent to the matching addresses.

URL

Type in a URL or part of a URL to display all emails containing a specific link.

STATUS

Clean

Displays all emails identified as legitimate.

Phishing

Displays all emails identified as phishing.

Timeout

Displays all emails that could not be analyzed due to a timeout.

Error

Displays all emails that could not be analyzed due to an internal error.

ACTION

Visited

Displays all URLs a user has visited.

Blocked

Displays all malicious URLs blocked by Vade.

Warning - Visited

Displays all URLs a user has visited after the warning.

Warning - Not visited

Displays all URLs a user has not visited after the warning.

Real-time logs

In order to view the real-time processing logs of the Time-of-Click protection, enable the ***Real-time log mode*** by clicking the switch button.

This will display the processing logs of all URLs scanned by the *Time-of-Click* protection.

Search results

The logs matching the search criteria will display in a table providing:

Date & Time

The date and time the message was originally processed.

From

The email address of the sender.

To

The email address of the recipient.

URL

The URL analyzed.

Status

The Filtering status for the URL, which corresponds to one of the status given by the *Time-of-Click* protection if the protection is enabled under the Anti-Phishing Settings page.

Typically, this will display `Clean`, `Phishing`, `Timeout`, `Error`.

Action

The action taken on the URL of the message: `Visited`, `Blocked`, `Warning - Visit` or `Warning - Did not visit`.

Time-of-Click log storage

As every mail processing platform, we have the need to keep the filtering logs for a given period of time (depending on local regulations and laws).

The logs stored by the platform include the following information:

Internal information

All the entries below (prefixed with _) are internal only, and contain information about the log entry itself:

- _index
- _type
- _id
- _version
- _score
- _source

id

The analysis ID that relates to the log entry.

clientType

One of Vade product names, e.g. "Microsoft" or "Cloud", etc.

clientID

The unique ID of the client, which relates to the Tenant ID in the context of Microsoft 365.

creationDate

The date on which the log entry was created.

from

The sender's email address, as present in the `From:` header of the message.

to

The recipient's email address, as present in the `To:` header of the message.

Note: This is required in order to send a notification alert to the IT administrator in case one of the domain users clicked on a phishing link.

url

In the context of a *Time-of-Click* analysis log entry, this contains the URL that was analyzed.

iipResult

In the context of a *Time-of-Click* analysis log entry, this contains the Vade IsItPhishing result (e.g. "phishing" or "clean").

action

The action the user performed on the link after the analysis of the page.

Event logs

The event logs track the activity performed on the filtering solution by administrators or users.

Any connection, configuration change, remediation, auto-remediation etc. will be recorded and displayed in the event logs.

Log search

You can search for specific event logs by providing search criteria in the search bar, and a specific period.

Notice: If you do not use any filter, the search string will match any field (user, event, etc.).

Period field

This field allows you to limit the search to a given period of time. Available default ranges are `1 hour`, `4 hours`, `1 day` and `7 days`. You may also specify a custom range by providing a start and end date as well as an exact time of day by clicking on the ***Custom*** button.

[Search field]

The search field allows you to search for a user or an event.

You can apply one or several filters after clicking on the ***Filters*** button:

USER

Type in the name of a user or part of the name of a user to display all actions they have taken.

Note: Select ***CONTAINS*** if you want to display users matching partially what you are looking for, or ***IS*** if you want to display users matching perfectly what you are looking for.

EVENTS

Connection

All connection events.

Auto-Remediate campaign sent
: A training campaign is sent automatically via Auto-Remediate.

Admin campaign sent
: The administrator manually sends a training campaign.

Time-of-Click campaign sent
: A training campaign is sent automatically via Time-of-Click.

The license is activated
: A user activates a license.

The license is deactivated
: A user deactivates a license.

Settings update
: A user updates settings.

Delegate permissions
: A user grants Vade access to their Microsoft account.

Partner access update
: A user activates or deactivates the Partner Access feature.

Auto-Remediate
: The Auto-Remediate feature was used.

Remediate
: The Remediate feature was used.

Intelligence Community disabled
: The administrator disables Vade Threat Coach Intelligence Community.

Intelligence Community enabled
: The administrator enables Vade Threat Coach Intelligence Community.

Automatic report sent
: A report is sent automatically.

Schedule stats report create
: A user schedules a stats report.

Schedule stats report update
: A user updates a scheduled stats report (report type, recipients, etc.).

Schedule stats report delete
: A user deletes a scheduled stats report.

Attachment downloaded
: A user downloaded an attachment via Vade for M365.

Email downloaded
: A user downloaded an email via Vade for M365.

Real-time logs

In order to view the new events in real time, enable the ***Real-time logs mode*** by clicking the switch button.

Search results

The logs matching the search criteria will be displayed in a table providing:

Date & Time
: The date and time of the event.

User
: The user behind the event.

Events

The type of event.

Log details

Click the ⋯ icon to display a pop-in window with information such as the time, the date and the user involved.

Note: In the case of remediation, you will find the Campaign ID and the ***View logs*** in order to display the involved emails.

Chapter
4

Reports

Threat Report

The Threat Report provides a detailed summary of the threats identified by type (malware, spear phishing, etc.) and can be used to investigate on a specific type of threat.

The dropdown menu in the top left corner allows you to choose between ***All domains*** or a specific domain you want the data of.

The ***Period*** field in the top right corner allows you to limit the search to a given period of time. Available default ranges are `1 hour`, `4 hours`, `1 day` and `7 days`. You may also specify a custom range by providing a start and end date as well as an exact time of day by clicking on the ***Custom*** button.

The different bar charts show how many emails were identified as threats during the period of time set in the ***Period*** field. The percentage indicates the part of a specific threat compared to the total number of threats received. Click any of them to display the filtered email logs.

ⓘ Notice: If you want to use the special ***Current Events*** filter, go to ***Logs*** > ***Emails***, apply the ***Current Events*** filter and go back to ***Reports*** > ***Threats*** to have your reports filtered.

Threats

The Threats charts provide visual representations of the identified threats distribution. You can click each threat label to get more details for a specific threats.

Time-of-Click

The Time-of-Click charts provide insights regarding the phishing and URL protection. It lists the number of phishing links detected, the number of times the users visited the phishing sites, etc.

Phishing

This chart shows the part of phishing attempts identified either by the filter or by Time-of-Click.

Spam

This chart shows the part of spams identified as high spams, medium spams or low spams.

Spear Phishing

This chart shows the part of the different kinds of spear phishing attempts.

Top attachments

This list provides insights about the attachment names that have been identified the most frequently by the platform in messages that were identified as threats.

Top extensions

This list provides the attachment extensions that have been seen the most frequently in messages that were identified as threats.

Top sender domains

Provides the list of domains which are sending the largest number of emails identified as threats to your domains.

Top sender addresses

Provides the list of senders who are sending the largest number of emails identified as threats to your domains.

Top recipient addresses

Provides the list of your domain's recipients who receive most emails identified as threats.

Top phishing URL domains

Provides the top domains of URLs identified as phishing by the *Time-of-Click*.

ⓘ **Note:** The time chart shows detected threats according to the email reception date with the up-to-date verdict displayed.

Related information

How to manage reports? on page 11

Low priority Report

This report provides a detailed view of each message type, and the possibility to investigate each type individually.

The report provides figures and charts representing the number of messages by type (newsletters, social notifications, etc.) over time and the possibility to detail each type.

The dropdown menu in the top left corner allows you to choose between ***All domains*** or a specific domain you want the data of.

The ***Period*** field in the top right corner allows you to limit the search to a given period of time. Available default ranges are `1 hour`, `4 hours`, `1 day` and `7 days`. You may also specify a custom range by providing a start and end date as well as an exact time of day by clicking on the ***Custom*** button.

The different bar charts show how many emails were identified as low priority messages during the period of time set in the ***Period*** field. The percentage indicates the part of a specific low priority email compared to the total number received. Click any of them to display the filtered email logs.

Low priority emails

Provides details regarding the classification that was performed over the messages, by category: `Newsletters`, `Social`, `Purchase` and `Travel`.

Top sender domains

Provides the list of the top sender domains for low priority emails.

Top sender addresses

Provides the list of the top sender email addresses for low priority emails.

Top recipient addresses

Provides the list of email addresses which receive most of the messages for low priority emails.

Related information

How to manage reports? on page 11

Auto-remediation Report

This report provides information about auto-remediated messages.

The dropdown menu in the top left corner allows you to choose between ***All domains*** or a specific domain you want the data of.

The ***Period*** field in the top right corner allows you to limit the search to a given period of time. Available default ranges are `1 hour`, `4 hours`, `1 day` and `7 days`. You may also specify a custom range by providing a start and end date as well as an exact time of day by clicking on the ***Custom*** button.

The different bar charts show how many emails were identified as threats during the period of time set in the ***Period*** field. The percentage indicates the part of a specific threat compared to the total number of threats received. Click any of them to display the filtered email logs.

Auto-remediation status evolution

This chart shows the number of auto-remediated emails in the set period.

Added value Report

This report shows Vade for M365 added value in comparison to the protection of Microsoft 365 only.

Available in the ***Reports*** menu, this page shows all the threats detected by Vade, in addition to the ones detected by Microsoft.

The ***Period*** field in the top right corner allows you to limit the search to a given period of time. Available default ranges are `1 hour`, `4 hours`, `1 day` and `7 days`. You may also specify a custom range by providing a start and end date as well as an exact time of day by clicking on the ***Custom*** button.

Additional threats detected by Vade

Each colored square represents a threat. The number indicates how many emails Vade for M365 has identified after the Microsoft analysis and the curve shows the evolution of the detection.

Chapter

5

Vade Threat Coach

Vade Threat Coach

Vade Threat Coach is a training feature that allows adminitrators to improve the behavior of their users towards phishing emails.

Vade Threat Coach is a platform with various exercises aiming to train users and improve their behavior regarding their emails. This platform is accessible via campaigns you triggered manually or automatically.

Launch campaign

The ***Launch campaign*** feature allows to manually send training campaigns to different groups of users using the name of a brand for the exercises. The users receive an email inviting them to take the course.

Note: The groups of users are the ones set in your Microsoft account and the top 10 recipient addresses.

Overview

7 days and ***30 days*** buttons allow to display the figures of the last 7 or 30 days.

The bar charts show different interesting numbers:

Campaigns
Total number of campaigns sent

Trainings
Total number of trainings received (admin campaigns, warning pages, ...)

Started
Total number of trainings started

Completed
Total number of trainings successfully completed

Failed
Total number of trainings with at least 1 mistake

Recent Campaigns

The Recent Campaigns logs allow you to see the last campaigns that has been sent thanks to Vade for M365. They display the following information:

Note: You can export the details of recent campaigns as a .csv file by clicking the ***Export to CSV*** button.

Date & Time
Date and time the campaign was sent.

Brand

Brand used for the campaign.

Type

Type of campaign (admin, Auto-Remediate, Time-of-Click).

Trainings

Total number of trainings received during this specific campaign.

Started

Total number of trainings started.

Completed

Total number of trainings successfully completed.

Failed

Total number of trainings with at least 1 mistake.

Details

Clicking the ⚬⚬⚬ dot icon displays a new window with information about a specific campaign:

Report tab

- Date & Time: date and time the campaign was sent.
- Brand: brand used for the campaign.
- Type: type of the campaign.
- Sent: number of users who received the campaign.
- Started: number of users who clicked the link to the training.
- Completed: number of users who successfully completed the training.

A button is also displayed to send the campaign once again to users who have not clicked the link to the training.

Details tab

This tab shows the different metrics of a campaign for a specific user.

Note: You can export the details of a specific campaign as a .csv file by clicking the ***Export to CSV*** button.

Sensitive users

The Sensitive users section displays the users who have had the least satisfying results after 1 or several campaigns, from most sensitive to less sensitive. As these users are more likely to be victims of phishing attacks, it is necessary to keep a close eye on their online behavior.

Note: You can export the details of sensitive users as a .csv file by clicking the ***Export to CSV*** button.

User

Email address of the user

Campaigns

Total number of campaign received

Failures

Total number of failed trainings

Last failure

Date and time of the last failed training

Details

Clicking the ⚬⚬⚬ dot icon displays a new window with information about the user such as:

- Date & Time: date and time of the campaign received.
- Brand: brand used for the campaign.
- Type: type of the campaign.
- Started: did the user clicked the link to the training?

- Completed: did the user successfully completed the training?
- Results: the results of the user.

Chapter
6

Toolbox

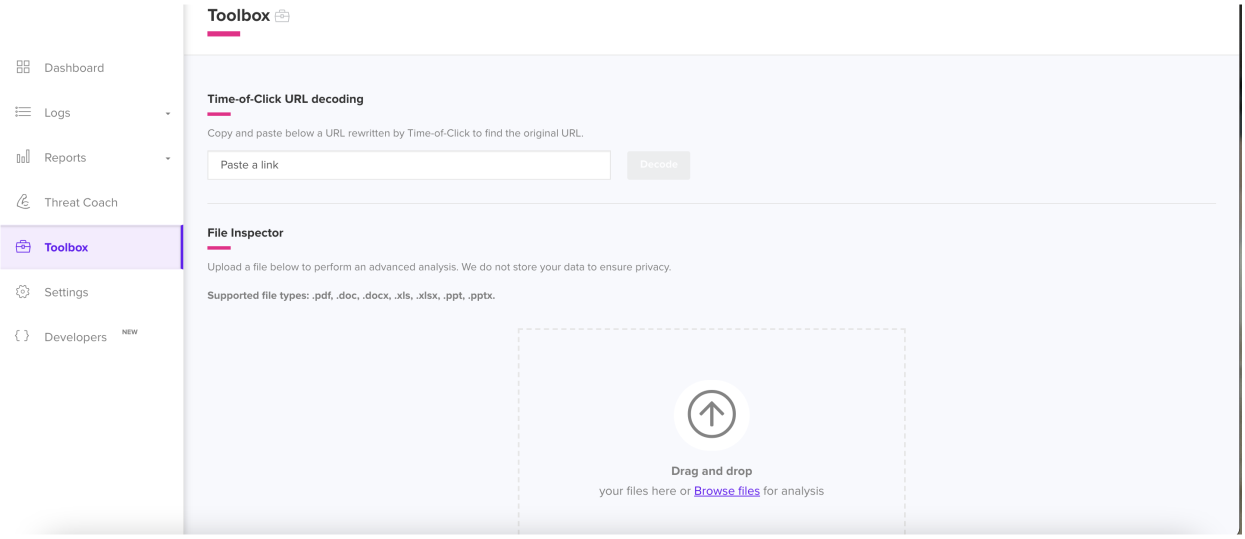
Time-of-Click URL decoding

This toolbox helps you decrypt URLs rewritten by the Time-of-Click feature.

If you activated the Time-of-Click feature, the URLs in your emails are automatically rewritten for them to be analyzed by Vade for M365. Sometimes, you might want to know what the original URL was before being rewritten. To do so, you can navigate to the ***Toolbox*** in the Vade for M365 admin console.

1. Log in to the Vade for M365 admin console.
2. Click ***Toolbox*** in the left menu.
3. Enter the URL you want to decrypt in the field.
4. Click ***Decrypt***.

The decrypted URL is displayed under the field. You can copy it using the ***Copy*** button on the right.



Time-of-Click URL decoding

Copy and paste below a URL rewritten by Time-of-Click to find the original URL.

Paste a link

File Inspector

Upload a file below to perform an advanced analysis. We do not store your data to ensure privacy.

Supported file types: .pdf, .doc, .docx, .xls, .xlsx, .ppt, .pptx.

Drag and drop
your files here or Browse files for analysis

Important:

You can only decrypt rewritten URLs in a specific format. They should start as follows:

- `<host>/v2?...`,
- `<host>/v3?...`, or
- `<host>/v4?...`.

Trying to decrypt older URL formats will trigger a `"We can't decrypt this URL"` warning.

Make sure the URL you are trying to decrypt are safe before accessing any website!

Related information

URL logs - Time-of-Click on page 27
Settings - Anti-Phishing on page 44

File Inspector

This feature allows you to analyze files for better threat analysis.

Some files, especially received via email, may seem suspicious to you. With File Inspector, you can get a deep analysis to perform a detailed investigation.

1. Log in to the Vade for M365 admin console.
2. Click ***Toolbox*** in the left menu.
3. Select the file you want to analyze under File Inspector.

You will find the following information about the file:

- ***Properties:*** First-level analysis.
- ***Features:*** Main attributes.
- ***Embedded links:*** URL or mailto links found in the file.
- ***Code Analysis:*** Details of the code detected in the file.
- ***Embedded files:*** Details of the different files included in the file.

Note: We do not store information retrieved in the ***Toolbox***.

Chapter 7

Settings

Global

Here you can choose your protection mode and manage your partner's access to your administration console.

Global settings

Protection

Click ***Protection*** to enable active filtering of Vade for M365.

Tip: Once enabled, ***Protection mode enabled*** will be displayed on the Dashboard on page 16 page.

Monitoring

Click ***Monitoring*** if you simply want the Vade for M365 to log detections (and not block anything) to monitor the solution.

Partner access

Activate ***Partner access*** to grant your partner access to your admin console

User group restriction

The user group restriction is only intended to be enabled by Vade employees. This feature restricts the actions of Vade for M365 to a limited number of users inside a specific tenant.

Tip: The logs only show the data of the users inside the user group. The other email adresses associated with the tenant are not protected: you cannot see them in the admin interface, logs, graphs, etc.

To enable the user group restriction, you must:

- Allow the client to use the feature from the Partner Portal,
- Enable the feature in the Vade for M365 administration console.

Related tasks

Allow user group restriction on the Partner Portal on page 41
Enable user group restriction in Vade for M365 on page 41
Disable user group restriction on page 41

Related information

Verify the user group status on page 42

Allow user group restriction on the Partner Portal

You must explicitly allow your clients to use the user group restrictions from the Partner Portal.

About this task

Allowing access to the user group restriction feature from the Partner Portal displays an additional button in Vade for M365 admin console for the client to enable it.

Procedure

1. Click ***Clients & Licenses*** on the Partner Portal.
2. Click the ***Details*** icon in front of the client name in the list.
3. Click ***Edit*** in front of the license in the ***Licenses*** tab.
4. Click ***Allow user group restriction***.
5. Click ***Edit a license*** after the icon turns green.
6. Click ***Access*** on the right after the window closes.

Results

The Vade for M365 admin console opens in a new tab after you click ***Access***.

ⓘ Note: You can also allow the feature when you add a license from the ***Add a license*** window.

Enable user group restriction in Vade for M365

You must enable the user Group feature in the Vade for M365 admin console after Vade has enabled it on the Partner Portal.

About this task

The client is able to see and enable the feature for a specific group of users in their admin console.

Tip: The user group must be named **Vade_Secure_user_group_restriction** on the Microsoft platform for the Vade for M365 admin console to find it automatically.

Procedure

1. Click ***Settings*** > ***User group restriction*** in the left menu.

   Tip: If the user group is appropriately set up, the administration console automatically detects it. If it does not, select your group in the drop-down menu.

2. Click ***Apply*** to enable the feature.

Results

The user group restriction is now enabled, and will restrict the actions taken by the Vade for M365 to the list of users selected.

Disable user group restriction

You must disable restrictions in the Vade for M365 admin console first, and then on the Partner Portal.

Procedure

1. Click ***Settings*** in the Vade for M365 admin console.
   a) Click ***Enable user group restriction*** in the ***Global*** tab.
   b) Click ***Apply*** to confirm.

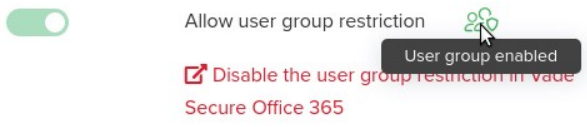
2. Click *Clients* on the Partner Portal.
   a) Click ***Details*** next to the client of your choice.
   b) Click ***Edit*** next to the license.
   c) Click ***Allow user group restriction*** to make it unavailable on the user side.
   d) Click ***Edit a license*** to confirm.

Results
The user group restriction is now disabled and configured filtering actions will now be performed for all users.

Verify the user group status

You can check the status of the user group (**Clients** > **Licenses** > **Details** > **Edit**) at any time from the Partner Portal.

Enabled



Allow user group restriction

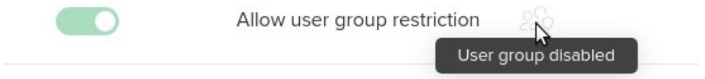
User group enabled

Disable the user group restriction in Vade Secure Office 365

The user group is active and is protected by Vade for M365.

Note: Check Disable user group restriction on page 41 if you want to disable the user group restriction.

Disabled

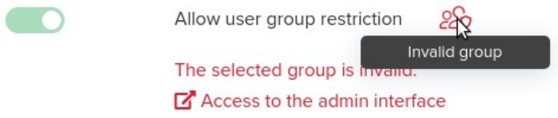


Allow user group restriction

User group disabled

The user group restriction is inactive, and all users are protected by Vade for M365. The client may not have enabled the feature in their admin console.

Invalid



Allow user group restriction

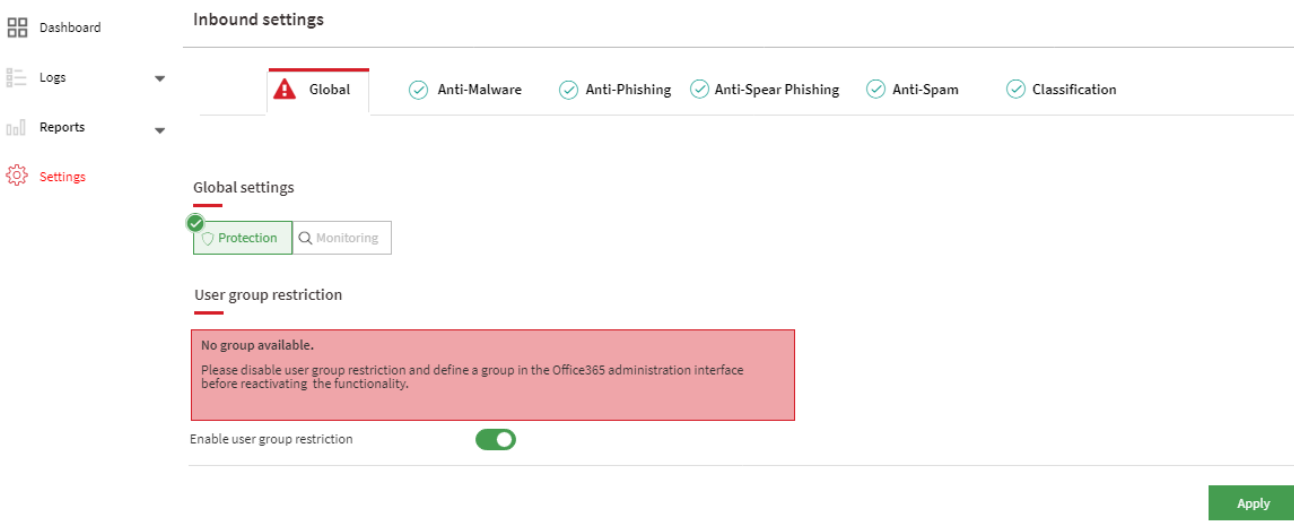
Invalid group

The selected group is invalid.

Access to the admin interface

Warning: The user group is inactive, the users are not protected by Vade for M365 and their messages are not logged.

The admin console displays an error banner in the ***Global*** settings:



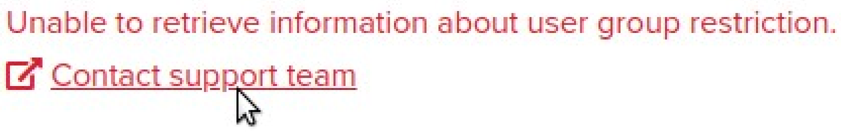
No group available.

Please disable user group restriction and define a group in the Office365 administration interface before reactivating the functionality.

Enable user group restriction

The client may have deleted the user group in their Vade for M365 admin console and may need to define a new one.

Error



Unable to retrieve information about user group restriction.

Contact support team

The user group is not active, and all users are protected by Vade for M365. An error may have occurred between the Partner Portal and the admin console.

Incident Response

Here you can manage the filtering of different types of emails.

Anti-Malware

This tab allows you to configure the actions to take upon detecting malware in attachments.

Manage actions by status

Status

Select the action to take upon detecting malware contained in message attachments. The recommended action is to ***Delete*** the message.

Action

The action the platform should take upon detecting a message containing a malware. Options are:

No action

The platform will not perform any action on the message. It will be delivered as-is in the user's mailbox.

Delete

The platform will delete the message: It will not be available in the user's mailbox or any other mailbox folder.

Move

The platform will move the message to the folder declared in the ***Folder*** field.

Remove attachments

The platform will remove malicious attachments found in the message, and move it to the folder declared in the ***Folder*** field.

Note: In case some of the attachments were removed, a banner will be added to the message.

Folder

The name of the inbox folder to move the message to.

Auto-Remediate

Activated by default, this feature learns over time and can fix automatically email verdicts received over the last seven days.

Important: Auto-Remediate is disabled in Monitoring mode and not applicable in the following cases:

- From legit to graymail (Newsletter, Social, Purchase...) and the other way around.
- On whitelisted email addresses (unless a malware is detected).
- In Monitoring mode.
- If the license is expired or suspended.
- If the email has already been moved by a user rule to another folder.
- If the email has already been remediated manually.

Customize the warning banner

Banner

Color

Choose the color theme to use for the banner.

Banner

Click a doted area to edit the text or to add the logo of your company.

Anti-Phishing

This tab allows you to configure the detection and actions to take upon detecting phishing attempts.

Manage actions by status

Allows you to choose which action to take upon detecting a phishing attempt.

Status

Select the action to take upon detecting a phishing attempt. The recommended action is to ***Move*** the message.

Action

The action the platform should take upon detecting a message of this type. Options are:

No action

The platform will not perform any action on the message. It will be delivered as-is in the user's inbox or folder.

Delete

The platform will delete the message: It will not be available in the user's mailbox or any other mailbox folder.

Move

The platform will move the message to the folder declared in the ***Folder*** field.

Folder

The name of the inbox folder to move the message to.

Auto-Remediate

Activated by default, this feature learns over time and can fix automatically email verdicts received over the last seven days.

⚠ **Important:** Auto-Remediate is disabled in Monitoring mode and not applicable in the following cases:

- From legit to graymail (Newsletter, Social, Purchase...) and the other way around.
- On whitelisted email addresses (unless a malware is detected).
- In Monitoring mode.
- If the license is expired or suspended.
- If the email has already been moved by a user rule to another folder.
- If the email has already been remediated manually.

Time-of-Click

Allows you to enable the *Time-of-Click* protection, which provides real-time protection against phishing URLs.

If this feature is enabled, the URLs contained in the emails received will be rewritten to point to a proxy, which will scan each target URL before redirecting the user to the original URL, or display a warning if a phishing site is discovered.

ⓘ **Note:** This feature does not apply to whitelisted messages, unless detected as malware.

Display the link 'Proceed to webpage with caution'

Displays a link on the warning page in order to allow users to access the page. This feature is enabled by default, you may disable it at any time.

Receive an alert for each detected phishing

Allows you to configure an administrator email address which will receive an alert for each phishing URL received by their users. You can specify the email address in the field below.

Address(es) receiving the alerts

Type in the email address(es) (comma-separated list) who will receive the phishing alert notifications.

Customization of the pending and warning pages

Allows you to customize the pages that are displayed while the proxy scans the target page and when the warning is displayed. You may customize both the header and footer parts of the pages.

ⓘ **Note:** These fields accept HTML code with inline formatting.

Anti-Spear Phishing

The Anti-Spear Phishing tab allows you to configure the action to take upon detecting the various types of targeted attacks.

Identity Spoofing

Vade Anti-Spear Phishing engine combines the analysis of an AI-based natural language processing and end-users' communication habits to flag email address, alias or domain impersonation attempts. You may customize a different action for each threat type.

Initial contact

The email does not contain any malicious content other than an incentive to reply (“Are you available?”). The main goal is to invite the recipient to answer so that the sending malicious address is recognized as a legitimate address.

CEO fraud

The email, supposedly sent by the CEO or senior management, requests an urgent money transfer, usually to an unknown bank account.

Tax fraud

This is a kind of phishing attempt involving the impersonation of Executives or HR members designed to steal social security numbers or tax identification numbers. Collected data are generally used for identity theft schemes.

Lawyer fraud

This involves an impersonation of lawyers or law firms. The main goal is to make sure victims will not raise awareness. Confidentiality restrictions are implied.

Gift card fraud

The email, supposedly coming from an Executive impersonation, requests a money transfer to set up gift cards for employees. Confidentiality and discretion are usually implied.

Manage actions by status

Allows you to choose which action to take upon detecting a spear phishing attempt.

Action

The action the platform should take upon detecting a targeted attack. Options are:

No action

The platform will not perform any action on the message. It will be delivered as-is in the user's mailbox.

Move

The platform will move the message to the folder declared in the ***Folder*** field.

Banner (Recommended)

The platform will prepend an alert banner to the top of the message body, to warn the user of the potential targeted attack. You may customize the banner using the fields below.

Folder

The name of the inbox folder to move the message to.

Customize the warning banner

Color

Choose the color theme to use for the banner.

Banner

Click a doted area to edit the text or to add the logo of your company.

Anti-Spam

This tab allows you to configure the actions to take upon detecting various spam types.

Status

The spam level returned by the filter.

High spam

High-volume spams that do not respect emailing campaigns best practices.

Recommended action is to `Delete` these messages.

Medium spam

Spams that respect best practices but that have been reported by users due to volumes or content.

Low spam

Spams that respect emailing campaigns best practices.

Scam

Potentially risky scam messages. Recommended action is to `Delete` these messages.

Action

The action the platform should take upon detecting a message of this type. Options are:

No action

The platform will not perform any action on the message. It will be delivered as-is in the user's inbox or folder.

Delete

The platform will delete the message: It will not be available in the user's mailbox or any other mailbox folder.

Move

The platform will move the message to the folder declared in the ***Folder*** field.

Folder

The name of the inbox folder to move the message to.

Auto-Remediate

Activated by default, this feature learns over time and can fix automatically email verdicts received over the last seven days.

⚠ **Important**: Auto-Remediate is disabled in Monitoring mode and not applicable in the following cases:

- From legit to graymail (Newsletter, Social, Purchase...) and the other way around.
- On whitelisted email addresses (unless a malware is detected).
- In Monitoring mode.
- If the license is expired or suspended.
- If the email has already been moved by a user rule to another folder.
- If the email has already been remediated manually.

Classification

This tab allows you to configure the actions to take for the various low-priority email types.

Status

The type of message detected by the filter.

Newsletters

Newsletter messages.

Social

Social media messages.

Purchase

Order/confirmation, invoices, etc.

Travel

Travel booking, reservation, confirmation, etc.

Action

The action the platform should take upon detecting a message of this type. Options are:

No action

The platform will not perform any action on the message. It will be delivered as-is in the user's inbox or folder.

Delete

The platform will delete the message: It will not be available in the user's mailbox or any other mailbox folder.

Move

The platform will move the message to the folder declared in the ***Folder*** field.

Folder

The name of the inbox folder to move the message to.

Vade Threat Coach

Vade Threat Coach is a quick training aiming to raise awareness among your users.

Vade Threat Coach

Automatically start a training on phishing based on users' behavior

Whenever a user clicks a link in a suspicious email, Vade Threat Coach displays a training link in the warning page. Moreover, if Auto-Remediate moves an email identified as a phishing attempt, the user will automatically receive an email for the training. Enable the toggle and click ***Apply*** at the bottom of the page to activate Vade Threat Coach.

⚠ **Important:** The Auto-Remediate feature must be activated first. One automatic training session maximum is offered in a 7-day period.

Help Vade enhance its threat detection technology

Users can help Vade solutions get better for an enhanced protection and more accuracy during the Vade Threat Coach training sessions with real life phishing emails. Enable the toggle, accept the disclaimer and click ***Apply*** at the bottom of the page to be part of the Vade Intelligence Community and start sharing **anonymously** your malicious emails with Vade.

ⓘ **Note:** You will receive an email whenever you enable or disable the feature. A partner cannot enable or disable this feature, even if they have access to the admin console.

Admin test

Click ***Launch a test*** to receive a campaign email like any user would if you launched a campaign automatically.

ⓘ **Note:** The brand used in the exercises is Microsoft by default. The test is sent to the email address you used to log in to the console.

Customize the training email

You can update the logo in the campaign emails.

RBAC

With RBAC, map Azure AD roles to Vade for M365 roles for customized user permissions.

RBAC, or Role-Based Access Control, helps you define users' rights on your administration console by mapping Microsoft Azure AD roles to Vade for M365 roles.

Vade for M365 roles and permissions

Click ***Show*** in a role box to display the following information:

Permissions

List of user permissions for the Vade for M365 role.

Search role

Type in any Azure AD role in the search bar.

Add mapping

Click the ***Add mapping*** button to map Azure AD roles to Vade for M365 roles.

Azure AD role

List of Azure AD roles mapped to Vade for M365 roles.

> **Note**: You can edit ✏ or delete 🗑 associations.

List of mappings

All Azure AD roles mapped to Vade for M365 roles you can edit ✏ or delete 🗑.

Search role

Type in any Azure AD role in the search bar.

Add mapping

Click the ***Add mapping*** button to map Azure AD roles to Vade for M365 roles.

Add mapping

You can associate Azure AD roles to Vade for M365 roles to define users' rights.

Procedure

1. Go to ***Settings*** > ***RBAC***.
2. Click the ***Add mapping*** button.
3. Search the Azure AD role to map to a Vade for M365 role.
4. Click ***Next***.
5. Select a Vade for M365 role.
6. Click ***Next***.
7. Click ***Associate***.

> **Note**: You can edit ✏ or delete 🗑 mappings from the list of mappings.

Chapter

8

Developers

Vade for M365 API

This tab shows how to use the Vade for M365 API for deep threats analysis.

The Vade for M365 API is a RESTful API that allows you to search for email logs, auto-remediation logs and manual remediation logs. You can also integrate our API into your SIEM for better threat investigation and threat intelligence.

Note: This feature is only available in English.

Use case #1: Retrieving URLs and attachments from a specific sender

As a user based in Europe, you want data about the URLs and attachments sent by zzz@yyy.com:

1. Retrieve your TOKEN by following the instructions in the ***Get started*** tab.
2. Enter this request in your terminal:

```
curl -X POST
"https://m365.eu.vadesecure.com/api/v1/tenants/{tenant_id}/logs/emails/search"
 \
-H "authorization: Bearer <YOUR_TOKEN>" \
-H "accept: application/json" \
-H "Content-Type: application/json" \
-d '{
    "fields": [
        "urls",
        "attachments"
    ],
    "query": {
        "eq": {
            "from": "zzz@yyy.v"
        }
    }
}'
```

3. The terminal returns URLs and attachment data sent by zzz@yyy.com.

Note: You will find information about the different fields and parameters in the API tab.

Use case #2: Retrieving all email logs

As a user based in Asia, you want to regularly retrieve all email logs and integrate them into your SIEM to know in real time what is happening on your tenant.

1. Enter this request in your terminal:

```
curl -X POST
"https://m365.asia.vadesecure.com/api/v1/tenants/{tenant_id}/logs/emails/search"
```

```
 \
-H "authorization: Bearer <YOUR_TOKEN>" \
-H "accept: application/json" \
-H "Content-Type: application/json" \
-d '{
    "sort": [
         "date",
         "id"
     ],
    "query": {
         "range": {
              "date": {
               "gte": "` date --date='5 minutes ago' --rfc-3339 `"}
        }
    }
}'
```

2. Integrate the logs into your SIEM.
3. Export logs into your SIEM every 5 minutes.