Vade Secure for Office 365

Version 2.19

Administrator Guide

Last modified: November 22, 2019

Contents

Chapter 1

Overview

What is Vade Secure for Office 365?

Vade Secure for Office 365 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 Secure integrates seemlessly in your Office 365 messaging solution and increases its security thanks to Artificial Intelligence.

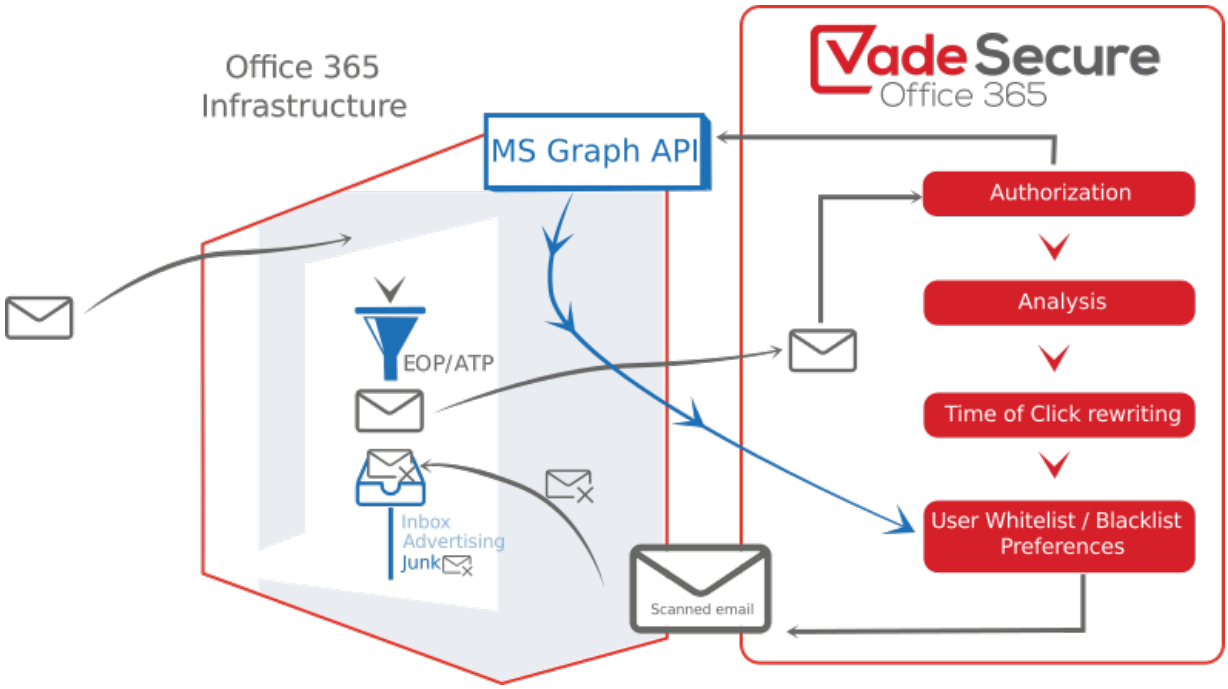
Vade Secure for Office 365 can be enabled in just a few clicks and requires no architecture changes (no MX record changes). The administration UI was designed to provide simple configuration and full reports and analysis information about blocked attacks. Your users won't have to change the way they access their emails or use a new interface.

Supported browsers

The Vade Secure for Office 365 admin console has been tested and is fully functional with the following browsers:

- Google Chrome (45 or later)
- Firefox (28 or later)
- Edge (15 or later)
- Safari (11 or later)
- Internet Explorer (11 or later)

Architecture Diagram



How it works

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

Activation process

Follow the steps below to set up Vade Secure for Office 365.

Before you begin

Warning: You must first contact your Vade Secure Sales representative to subscribe to a valid license plan prior to following the activation process.

Procedure

1. *Retrieve the Tenant ID* on page 6
2. *Create a new customer on the Partner Portal* on page 6
3. *Add a license to the profile of a customer* on page 6
4. *Activate your license* on page 6
5. *Confirm the permissions using an Office 365 Global Admin account* on page 7
6. *Create a journal rule* on page 7

Retrieve the Tenant ID

Procedure

1. Log in to the *Microsoft Azure Portal* with your admin credentials.
2. Type in `Azure Active Directory` in the search bar.
3. Click on **Azure Active Directory** under **Services**.
4. Click on **Properties** in the left menu.

Results

You will find the *Tenant ID* under **Directory ID**.

Create a new customer on the Partner Portal

Procedure

1. Access the Portal at *https://partner.vadesecure.com*.
2. Click the **Customers** tab.
3. Click **Add a Customer** button.
4. Fill in the required fields.
5. Click the **Add a Customer** button.

   Please note that you can also create a Customer profile via the Parner API (see the “Vade Secure Partner API Guide”, “Create a Customer” section).

Add a license to the profile of a customer

Procedure

1. Log in to the Partner Portal.
2. Click on the **Customers** tab in the left menu.
3. Click on the **Details** button of a specific customer.
4. Click on the **Order a license** button.
   a) Select a product
   b) Enter the *Tenant ID*.
   c) Select an environment for the platform.
   d) Select the license validity period.
   e) Click on the **I understand that I am ordering licenses and that I must settle this order with my distributor** checkbox.
5. Click on the **Order a license** button.

Results

The pop-in window closes. The end user will receive an email to activate their license.

Activate your license

Procedure

1. Check your emails for an activation email sent by Vade Secure.
2. Click the **Activate your license** button in your activation email.

You can check the license status (**Pending activation**, **Active**, etc.), renew a subscription or delete a license on the Partner Portal.

Confirm the permissions using an Office 365 Global Admin account

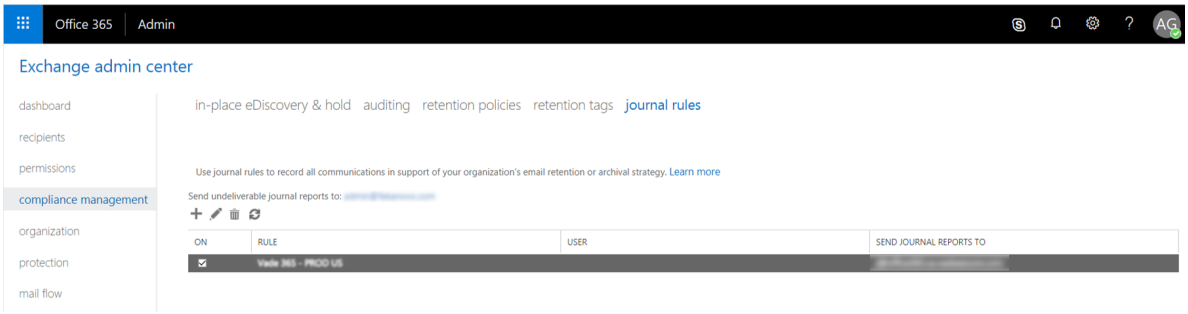
Procedure

1. Log into the Vade Secure admin console
   - For Europe: *https://office365.eu.vadesecure.com/*
   - For the US: *https://office365.us.vadesecure.com/*
   - For Asia: *https://office365.asia.vadesecure.com/*
2. Click **Accept** to accept the basic permissions required by the Vade Secure UI.
3. Click **Continue** to go to the next screen.
4. Click **Accept** to confirm all the permissions in the pop-in window for the Vade Secure 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

Procedure

1. Go to: **Microsoft O365 Admin Center** > **Left Menu** > **Show more** > **Exchange** > **compliance management** > **journal rules**.



2. Configure an email address which will receive the **undeliverable journal reports**, by clicking the link named **Send undeliverable journal reports to...**, as shown above. Microsoft Office 365 requires you to add a notification email address which will receive notifications in case emails sent to a given user were not journalized for various reasons.

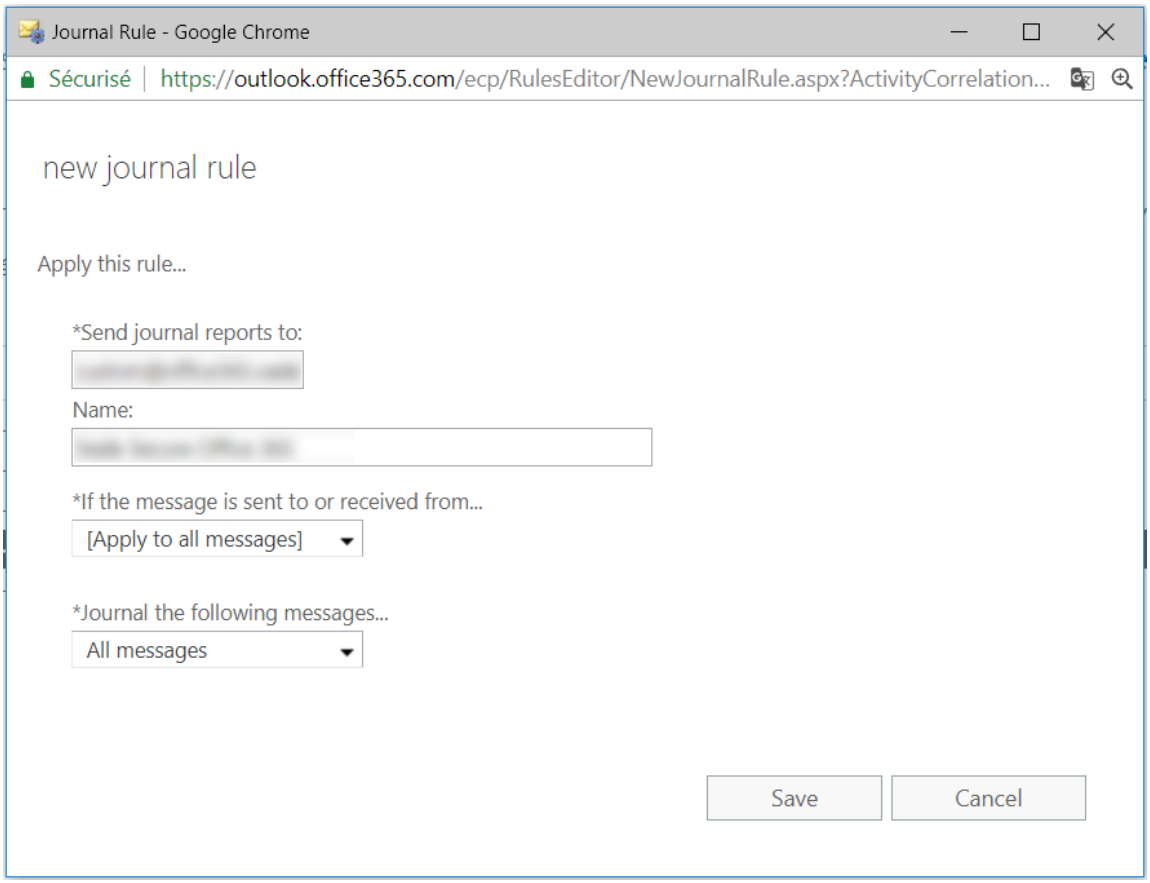
   Warning: Office 365 disables journaling on the address used to receive the **journalisation notification errors**. As such, this address will not be protected. Vade Secure recommends using a dedicated email address or internal mailing list, **outside the protected domain**, for this purpose.

3. Add a journal rule to send a copy of the email traffic to Vade Secure for Office 365.
   a) Send journal reports to the dedicated address.
      - For Europe: `journal-report@office365.eu.vadesecure.com`
      - For the US: `journal-report@office365.us.vadesecure.com`
      - For Asia: `journal-report@office365.asia.vadesecure.com`

   b) Complete the name of the rule.

c) Select **Apply to all messages** (or **user/user group** if you want to restrict the analysis to a person or group of people).

d) Select `all messages` under **Journal the following messages**.



Please note that you can also create a Customer profile via the Parner API (see the "Vade Secure Partner API Guide", "Create a Customer" section).

Frequently Asked Questions

Are Office 365 EOP & ATP protections still available?

Tip: Yes! The Vade Secure for Office 365 filtering comes on top of integrated EOP and ATP layers. The journal rules are triggered after the message has been scanned by the Office 365 EOP and ATP filters.

Does the user need Exchange Online Protection (EOP) as well as the Vade Secure solution to work effectively?

Exchange Online Protection is included within all Microsoft cloud email services such as Exchange Online and Office 365, so no extra license is required. Vade Secure 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 Secure portal. 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 users 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 Secure keep a copy of all emails?

No, Vade Secure deletes the copy after the analysis.

Do I need to update my MX record?

Tip: No! The MX record still point to Office 365, and remains unchanged. The Vade Secure for Office 365 is natively integrated to the Office 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 *#unique_11*.

Does the filter override user preferences?

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

Important: For administrator-level lists, Vade Secure recommends using Exchange **mail flow rules** instead. For more information, please refer to *How to use admin whitelists?* on page 10.

Does the filter override the user inbox rules?

Tip: No! The inbox rules created by the user (e.g. *Move messages from … to folder ...*) will always take precedence. Vade Secure for Office 365 will only move messages that were meant to be delivered in the main *Inbox* of the user.

Where do I create whitelists in the product?

You can create whitelists on Office 365, just like before. Users may not create whitelists on the Vade Secure for Office 365 platform itself.

Important: For administrator-level lists, Vade Secure recommends using Exchange **mail flow rules** instead. For more information, please refer to *How to use admin whitelists?* on page 10.

How come I get so many spear phishing notifications?

The spear phishing protection provided by the product notifies users 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 his 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 the administrator has blacklisted an address which a user has whitelisted?

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

Is the Vade Secure filtering applied to all messages?

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

How to use admin whitelists?

The native integration with MS Office 365 provides the solution with the whitelists that were created by the user, i.e the recipient for the message. However, the whitelists created by an administrator on Office 365 are not always provided to the message context. Vade Secure for Office 365 recommends creating **Mail Flow rules** on Office 365 instead.

About this task

Tip: **Mail flow rules** have been added to Office 365 configuration, and were previously known as *Transport rules*. They allow you to set more complex filtering rules than whitelists or blacklists, and allow you to bypass the spam filtering protection for some messages.

For the example below, let's say you need to whitelist messages issued from a Salesforce platform, which warn sales persons about a deal opportunity for instance.

Procedure

1. Log in to Microsoft Office 365, then click **Admin Center** > **Left menu** > **Admin Centers** > **Exchange**.
2. Create a new mail flow rule:
   a) Click **mail flow** > **rules** in the Exchange Admin center.
   b) Click **+ icon** > **Bypass spam filtering...**.
   The **new rule** window opens.
   c) Enter a name for the rule.
3. 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.

   a) Enter the domain name or the address you want to whitelist in the new pop-in window.
   b) Click the + icon.
   c) 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 with the recipient of the message, e.g. `sales@mycompany.com`, to be even more restrictive.

4. Add the following actions in the **new rule** window for Vade Secure to filter your emails:
   a) Click the **add action** button.
   b) Select **Modify the message properties...**.
   c) Select **set a message header** in the drop-down menu.
   d) Click the first **Enter text...** link in the text on the right.

The **message header** window is displayed.

e) Enter the following value: `X-VADE-O365`.

f) Click the **OK** button.
The **message header** window closes.

g) Click the second **Enter text...** link.

h) Enter the name of the customer.

5. Click **OK**.
6. Uncheck the **Audit rule with severity level** box in the **new rule** window.
7. Click **Save**.

Results

The new rule now appears on your Rules dashboard. Make sure its checkbox is on.

How to schedule reports?

Vade Secure for Office 365 allows you to schedule reports, update report scheduling and cancel them as well.

How to schedule reports?

Users 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.
2. Click **Threat Report** or **Low Priority Report**.
3. Click **Schedule report** in the top right corner.
4. Enter a comma-separated list of email addresses you want 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 **Threat Report** and/or **Low Priority Report** to receive Threat and/or Low Priority reports.
7. Save.

Depending on the frequency the user chooses, they will receive the reports from the alias **Vade Secure for Office 365** 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

For more information about Threat and Low Priority reports, please refer to *Threat Report* on page 34 and *Low Priority Report* on page 35.

How to update report schedule?

In order to update your report schedule, you must:

1. Click **Reports** on the left panel.
2. Click **Threat Report** or **Low Priority Report**.
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 report schedule?

In order to cancel your report schedule, you must:

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

How to remediate emails?

Remediate lets Vade Secure for Office 365 protect your users **before** the attack (*predictive technology*), **during** the attack (data gathered from 600M+ mailboxes to live-remediate any attack) and **after** the attack. In order to you respond after an email attack, Vade Secure for Office 365 allows you to move users' messages from their delivery folder to any other folder or even delete them.

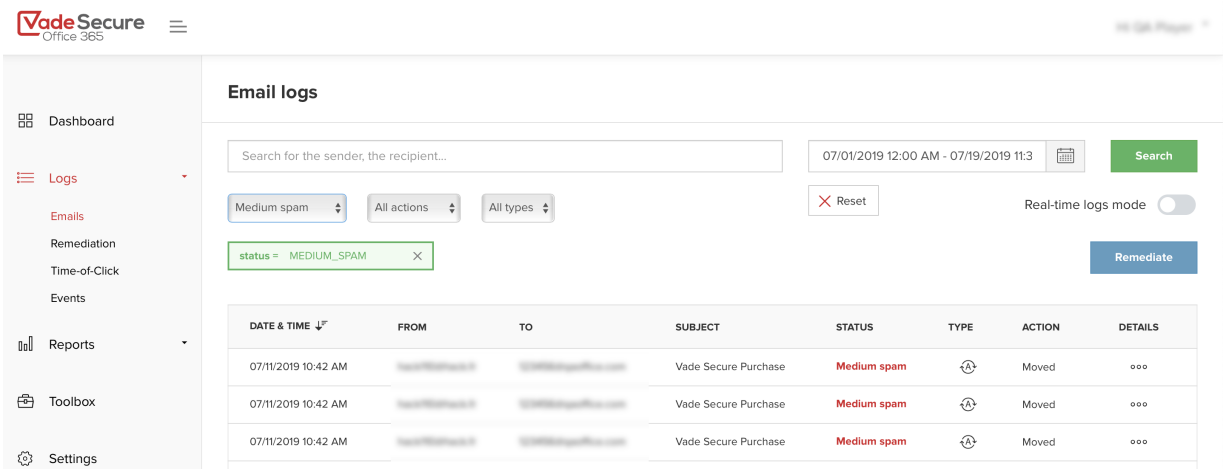
How to display the Remediate button?

In order to display the **Remediate** feature, first apply search criteria in the *Email logs page*. You can then find the **Remediate** button in the top right corner of the list and in the log details.

How to remediate a single email?

1. Access the log details of the email by clicking the ooo icon on the right
2. Click the **Remediate** button in the pop-in window
3. Select an action in the second pop-in window
4. Click **Remediate**

   The second pop-in window displays the subject of the selected email, the available actions and a **Report to Vade Secure** checkbox (see below for more information).



Tip: If you have never remediated this email, the **Remediate** button is next to its original status (**Original detection**). If you have, the **Remediate** button is next to its last status.

How to remediate a category of emails?

1. Click the **Remediate** button in the top right corner of the list
2. Select an action in the pop-in window
3. Click **Remediate**

The pop-in window displays the number of selected emails, the available actions (see below) and a **Report to Vade Secure** checkbox (see below for more information).

Tip: You can apply the **Remediate** action to as much as 100 messages at once. The console always displays the exact number of messages you handle.

Pop-in window actions

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

- Move to Junk Email
- Delete
- Move to Inbox
- Move to [any other folder based on the ones set in the configuration]

You can check the **Report to Vade Secure** box to help our teams improve the accuracy of the solution.

You can also **Cancel** or simply **Remediate** at the bottom of the page.

Confirmation

In order to prevent any unfortunate use of the **Remediate** button, you must first confirm your action.

On computer:

- Click the **Remediate** button
- Hover your mouse over the **Remediate** button until it becomes green in the pop-in window
- Click the **Remediate** button (Remediate) to confirm

On mobile phone:

- Press the **Remediate** button
- Press and hold the **Remediate** button to make it green
- Press the **Remediate** button (Remediate) once again to confirm

Note: The emails you remediate have the status **In Progress**, and then the status **Remediated** when the remediation is complete.

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 thus available for you to check their emails.

Event Logs

Click the **All status** drop-down menu and select **Remediated** to display all remediated emails.

From the log details, you can check who used the **Remediate** action and the date of the action.

The description displays what kind of action a user took: **[NUMBER OF MESSAGES] messages moved to the folder [FOLDER NAME]**.

In case of failure, this description shows: **0 message moved to the folder [FOLDER NAME]. [NUMBER OF MESSAGES] messages failed to remediate**.

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

You can close the window with the **Close** button at the bottom of the window.

How to revoke the rights of Vade Secure for Office 365?

If you do not want to use Vade Secure for Office 365 anymore, you need to follow a few step process to revoke its rights.

Procedure

1. Delete the journal rule.
   a) Go to: **Admin Center** > **Left menu** > **Admin Centers** > **Exchange** > **Compliance management** > **Journal rules**.
   b) Check the box next to the journal rule.
   c) Click the bin icon.
   The journal rule is deleted.
2. Remove the application.
   a) Go to: **Azure Portal** > **Left menu** > **Azure Active Directory** > **Enterprise applications**.
   The application list is displayed.
   b) Select the **Vade Secure for Office 365** application in the table.
   c) Click the **Delete** button to delete the application and revoke rights.
   The application is removed.

Vade Secure for Office 365 cannot access or process your emails anymore.

Support

Vade Secure provides technical support by phone or email for Vade Secure for Office 365.

Vade Secure support can be joined 7/7, and 24/24, through:

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

Chapter 2

Settings

Global Settings

This tab allows you to choose between Protection mode and Monitoring mode.

Protection

Click **Protection** to enable active filtering of Vade Secure for Office 365.

Tip: Once enabled, the **Protection mode enabled** notice will be displayed on the *Dashboard* on page 22 page.

Monitoring

Click **Monitoring** if you simply want the Vade Secure for Office 365 to log detections (and not block anything) to monitor the solution.

Anti-Malware

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

Manage actions by status

Status

Choose 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 **Folders Name** field.

Remove attachments

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

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

Folders Name

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

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.

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 **Folders Name** field.

Folders Name

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

Enable Time-of-Click

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

If 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.

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 his 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.

Custom prefix

You may customize the proxy prefix to redirect to a domain known from the users.

Enable https

Click to enable HTTPS for proxy redirection. If enabled, you need to configure the certificate information in the fields displayed.

Private key

Click the **Add file** button to upload a private key.

Certificate

Click the **Add file** button to upload a certificate.

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.

Check how it looks!

Click this button to display a preview of what the pages look like with the customized HTML excerpts.

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

The message analysis can identify various kinds of spoofing. You may customize a different action for each type.

Exact Sender spoofing

This test detects potential spoofing related to the sender's email address. For instance, for messages sent to `user@domain.com`:

- `"Other User<other.user@domain.com>"`

(where "Other User" is a valid user on your domain) will be detected as an exact spoofing, since the address corresponds to an address that exists on your domain. The information about how the message was conveyed though tell us that the message went through an expected route.

Exact Sender's domain spoofing

This test detects potential spoofing attempts related to the sender's domain. For instance, for messages sent to `user@domain.com`:

- `"Bill Gates <bill.gates@domain.com>"`

will be detected as a domain spoofing attempt, as the domain matches yours, but the user does not exist on your domain.

Alias spoofing

This test detects potential spoofing attempts related to the user alias. For instance, for messages sent to `user@domain.com`:

- `"uSeR <xxx@otherdomain.com>"`
- `"User user@domain.com <xxx@otherdomain.com>"`
- `"user@domain.com <xxx@otherdomain.com>"`

will be detected as alias spoofing.

Close Sender's spoofing

This test detects potential spoofing attempts related to the graphical rendering of the addresses and domains used. For instance, for messages sent to `user@domain.com`:

- `"User <user@doman.com>"`
- `"User <user@d0main.com>"`
- `"User <user@domain.otherdomain.com>"`

will all be detected as spoofing attempts, as they all ressemble your domain's graphical rendering, but characters were replaced.

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.

Banner

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.

Move

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

Folders Name

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

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 options

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

These correspond to high-volume spams that do not respect emailing campaigns best practices. Recommended action is to `Delete` these messages.

Medium spam

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

Low spam

These correspond to spam that respect emailing campaigns best practices.

Scam

These correspond to 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 **Folders Name** field.

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

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
Corresponds to newsletter messages.

Social
Corresponds to social-media messages.

Purchase
Corresponds to purchase order/confirmation, invoices, etc.

Travel
Corresponds to 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 **Folders Name** field.

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

Microsoft Exchange Plug-in

In order to strengthen the Vade Secure filtering engine, the integration of the Microsoft Exchange plug-in 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 Secure filter also takes this feedback into account to improve its filtering engine and better protect them.

Auto-Remediate

Once activated, Auto-Remediate can fix inaccurate email verdicts for an even better protection.

What is Auto-Remediate?

Thanks to an advanced AI, Vade Secure fixes its own diagnosis inacurracies when the email is already in the inbox and notifies the user for the best protection against the most sophisticated new attacks.

The auto-remediation process can fix email verdicts received over the last seven days.

Important: Auto-Remediate is 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.

Related information

How to remediate emails? on page 12

Remediate lets Vade Secure for Office 365 protect your users **before** the attack (*predictive technology*), **during** the attack (data gathered from 600M+ mailboxes to live-remediate any attack) and **after** the attack. In order to you respond after an email attack, Vade Secure for Office 365 allows you to move users' messages from their delivery folder to any other folder or even delete them.

How to activate Auto-Remediate?

About this task

Since the feature is not enabled by default, administrators must first enable it in the Vade Secure for Office 365 admin console.

Procedure

1. Go to **Settings** in the left menu.
2. Click the **Enable Auto-Remediate** switch button.
   The switch button becomes green.
3. Click **Apply**.

Results

The Auto-Remediate feature is enabled and Vade Secure will now improve by fixing its own diagnosis mistakes.

The functionality is disabled if the user returns to Monitoring mode.

Chapter 3

Dashboard

Dashboard

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

The dashboard provides figures and charts representing the number of threats by type (malware, phishing, spam, etc.) overtime 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.

You may view the related log details by clicking each threat name, threat figures or the **View logs** button. This displays the *Email logs* on page 23 window.

Tip: The **Protection mode enabled** notice is displayed in order to remind you at one glance that the active filtering is enabled.

Chapter 4

Logs

Email logs

This page displays filtering logs and allows you to search for specific log entries and view logs in real time.

Real-time logs

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

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

Search logs

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

[Search field]

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.

Notice: If you don't provide a specific field, the search string will match any field (email address, subject, action, etc.).

The following search fields are available:

from

`from="mail@test.com"` displays all emails sent from the address `mail@test.com`.

to

`to="mail@test.com"` displays all emails sent to the address `mail@test.com`.

subject

`subject="hello world"` displays all emails containing `hello world` in their subject.

action

DELETE

`action="DELETE"` displays all emails Vade Secure for Office 365 deleted.

MOVE

`action="MOVE"` displays all emails Vade Secure for Office 365 moved to a subfolder.

CLEAN

`action="CLEAN"` displays all legitimate emails according to Vade Secure for Office 365.

status

MALWARE

`status=MALWARE` displays all emails identified as malware by Vade Secure for Office 365.

SPEAR_PHISHING

`status=SPEAR_PHISHING` displays all emails identified as spear phishing attempts by Vade Secure for Office 365.

SCAM

`status=SCAM` displays all emails identified as scams by Vade Secure for Office 365.

MEDIUM_SPAM

`status=MEDIUM_SPAM` displays all emails identified as medium risk spams by Vade Secure for Office 365.

HIGH_SPAM

`status=HIGH_SPAM` displays all emails identified as high risk spams by Vade Secure for Office 365.

SPAM

`status=SPAM` displays all emails identified as spams (regardless of the risk) by Vade Secure for Office 365.

NEWSLETTER

`status=NEWSLETTER` displays all emails identified as newsletters by Vade Secure for Office 365.

MARKETING

`status=MARKETING` displays all emails identified as marketing emails by Vade Secure for Office 365.

SOCIAL

`status=SOCIAL` displays all emails identified as social emails by Vade Secure for Office 365.

PURCHASE

`status=PURCHASE` displays all emails identified as purchase-related emails by Vade Secure for Office 365.

TRAVEL
`status=TRAVEL` displays all emails identified as travel-related emails by Vade Secure for Office 365.

THREATS
`status=THREATS` displays all emails identified as threats by Vade Secure for Office 365.

LOW_PRIORITY
`status=LOW_PRIORITY` displays all emails identified as low priority emails by Vade Secure for Office 365.

LEGIT
`status=LEGIT` displays all emails identified as legitimate emails by Vade Secure for Office 365.

withattachment

YES
`withattachment="YES"` displays all emails with at least one attachment.

NO
`withattachment="NO"` displays all emails without any attachment.

withurl

YES
`withurl="YES"` displays all emails with at least one URL.

NO
`withurl="NO"` displays all emails without any URLs.

[Date field]
The date field allows you to limit the search to a given period of time. Available 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 by clicking the Calendar icon.

In addition, you may provide a start and end time of day to refine the search results.

[Filters]
In addition, you may filter the logs by resulting Status and Action.

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.

Subject
The subject of the message.

Status

The Filtering status for the message, 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
Vade Secure Filter identified the message as legitimate.

Phishing
Vade Secure Filter identified the message as a phishing attempt.

Malware
Vade Secure Filter identified a malware contained in the message.

Spear phishing
Vade Secure Filter identified the message as a spear phishing attempt (because of partial or complete spoofing, etc.).

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

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

Scam
Vade Secure Filter identified the message as a scam.

Newsletters
Vade Secure Filter identified the message as a newsletter.

Social
Vade Secure Filter identified the message as a social network notification.

Purchase
Vade Secure Filter identified the message as a purchase confirmation, billing and invoices information, etc.

Travel
Vade Secure Filter identified the message as a travel plan confirmation.

Whitelists
The message matched one of the **whitelists** configured by the user or administrator on Office 365. The action performed corresponds to the action defined for whitelisted messages on Office 365.

Blacklists
The message matched one of the **blacklists** configured by the user or administrator on Office 365. The action performed corresponds to the action defined for blacklisted messages on Office 365.

Failed
This action may occur when trying to perform actions on messages sent to a distribution list, for which the recipient no longer exists on Office 365 (but was not removed from the distribution list). This prevents Vade Secure for Office 365 from taking any action on the message.

Type

The type of remediation action that has been applied to the email:

- Manual remediation, or
- Auto-remediation

Action

The action taken on the message (`Moved`, `Deleted`, etc.) depending on the action configured for the message status. Potential actions are:

Moved

The message was moved from the inbox to another folder.

Deleted

The message was deleted.

Banner

A banner was added to the message.

No action

No action was performed on the message.

Whitelists

The message matched one of the **whitelists** configured by the user or administrator on Office 365. The action performed corresponds to the action defined for whitelisted messages on Office 365.

Blacklists

The message matched one of the **blacklists** configured by the user or administrator on Office 365. The action performed corresponds to the action defined for blacklisted messages on Office 365.

Failed

This action may occur when trying to perform actions on messages sent to a distribution list, for which the recipient no longer exists on Office 365 (but was not removed from the distribution list). This prevents Vade Secure for Office 365 from taking any action on the message.

Details

Contains additional information for the message. If the message contained a URL for instance, this column will display the URL icon.

Log details

Clicking the dots icon displays a pop-in window with two tabs:

- **Status & Delivery**: Type of remediation, verdict, action, dates and reasons for the filtering performed per action.
- **Description**: Information about the email, the sender and the content of the email (URLs, attachments,…).

For more information about the filtering logs, please refer to *Filtering log fields* on page 27.

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 Office 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.

[Office 365 specific headers]

As part of the Office 365 processing, the metadata returned may contain information provided by Office 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 an Office 365 user blacklist.

whitelisted

A boolean indicating if the message matched an Office 365 user whitelist.

folder

The folder the message was moved to.

action

The action taken on the message by Office 365.

Verdict information

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

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"
```

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" && 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 Secure for Office 365, then you need to use:

```
from="tom.watson@test.com" && 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" && action="DELETE"
```

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

```
from="tom.watson@test.com" && withattachment="YES" &&
withurl="YES"
```

You are now ready to use log search in our Vade Secure for Office 365 interface!

Time-of-Click Logs

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.

Real-time logs

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

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

Search logs

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

[Search field]

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. To do so, you can use filters such as:

from

`from="mail@test.com"` displays all emails sent from the address `mail@test.com`.

to

`to="mail@test.com"` displays all emails sent to the address `mail@test.com`.

url

`url="testurl.com"` displays a URL users clicked on in their emails.

Please note that if you don't use any filter, the words you are searching for may appear in any field (email address, subject, action, etc.).

[Date field]

The date field allows you to limit the search to a given period of time. Available 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 by clicking the Calendar icon.

In addition, you may provide a start and end time of day to refine the search results.

[Filters]

In addition, you may filter the logs by resulting Status and Action.

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 scanned.

Status
The Filtering status for the URL, which corresponds to one of the status returned 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 message, which can be `Authorized`, `Blocked`, etc. `Authorized` is displayed when the user is redirected automatically, `Warning - Visit` or `Did not visit` when the user had a choice to make.

Log details
Clicking the ◦◦◦ dots icon displays a pop-up window listing the details of the message, including the URL contained in the message that was identified as phishing.

Time-of-Click log fields

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.

messageID
The message ID that relates to the log entry.

clientType
One of Vade Secure product names, e.g. "Office" or "Cloud", etc.

clientID
The unique ID of the client, which relates to the Tenant ID in the context of Office 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 Secure IsItPhishing result (e.g. "phishing" or "clean").

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

filterCategory

creationDate

Events Logs

The Events 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 events logs.

The events logs can be filtered by user and date.

Search logs

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

[Search field]
The search field can take parts of a user ID and can be filtered by status.

[Date field]
The date field allows you to limit the search to a given period of time. Available 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 by clicking the Calendar icon.

In addition, you may provide a start and end time of day to refine the search results.

Remediation logs

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

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.

Chapter 5

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 default view provides a 7-day highlight of all threat types. You may choose a different time period: 1 day, 7 days, 30 days or a custom period.

You can click on a specific threat type (e.g. *malware*) on the pie charts, the summary figures, etc. to view the details of this specific threat. If you click the figures above each threat, the *Email logs* on page 23 are displayed.

Once you click on a specific threat type, the filter information will be displayed on top of the screen, and can be discarded by clicking the X icon.

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.

Top attachments
This list provides insights about the attachment names that have been seen 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 domains sender

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 schedule reports? on page 11
Vade Secure for Office 365 allows you to schedule reports, update report scheduling and cancel them as well.

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.) overtime and the possibility to detail each type.

It can be configured to provide details over a 1 day, 7 day (default) or 30 day periods and filtered by domain.

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 schedule reports? on page 11
Vade Secure for Office 365 allows you to schedule reports, update report scheduling and cancel them as well.

Comparative Report

Comparative Statistics show Vade Secure for Office 365 added value by protecting users with an extra layer of protection.

The feature, available in the **Reports** menu, shows all the threats detected by Vade Secure, in addition to the ones detected by Microsoft.

In the first section, the top line diagram represents all the threats detected by Microsoft and the bottom line represents the threats additionaly detected by Vade Secure.

In the second section, the charts represent the evolution of the threat detection by Microsoft, and the other threats detected **only** by Vade Secure.

Note: By default, the view is set on **7 days**, but users can set a specific time frame (day, week, month, custom period).

Auto-remediation Report

This report provides information about auto-remediated messages.

At the top of the page, hozirontal charts display the amount of updated verdicts per verdict type during the selected period.

The **Auto-remediate status evolution** chart compiles every remediation in the following order:

- Spam
- Phishing
- Malware
- Spam
- Spear Phishing

Chapter 6

Toolbox

URL Decryption tool

If you are using the Anti-Phishing *Time-of-Click* feature, you can use this tool to decrypt URLs which have been rewritten.

In case you want to decrypt a URL which has been rewritten by the *Time-of-Click* feature, navigate to the **Toolbox** main menu.

Important: Please note you will only be able to decrypt rewritten URLs which start with `<host>/v3?...`. Trying to decrypt older URL formats will trigger a `We can't decrypt this URL` warning.

Once the decryption succeeds, the original URL will be displayed.

Index