Vade for Google Workspace - Administrator Guide

Last modified: February 5, 2024

Table of Contents

1. Overview..... 3

1.1. Overview..... 3

1.2. Architecture Diagram..... 4

1.3. Frequently Asked Questions..... 5

1.4. Support..... 7

2. Dashboard..... 8

3. Logs..... 11

3.1. Email logs..... 11

3.1.1. Filtering use cases..... 18

3.1.2. Filtering log fields..... 19

3.2. Remediate and report emails..... 21

3.3. Remediation logs..... 23

3.4. URL logs - Time-of-Click..... 24

3.4.1. Time-of-Click log storage..... 27

4. Reports..... 29

4.1. Threat Report..... 29

4.2. Low priority Report..... 31

4.3. Auto-remediation Report..... 32

5. Toolbox..... 33

5.1. Time-of-Click URL decoding..... 33

6. Settings..... 35

6.1. General..... 35

6.2. URL protection..... 36

6.3. Email protection..... 37

6.3.1. Anti-Malware..... 37

6.3.2. Anti-Phishing..... 39

6.3.3. Anti-Spear Phishing..... 40

6.3.4. Anti-Spam..... 42

6.3.5. Classification.....44

7. RBAC.....45

7.1. Add mapping..... 46

1. Overview

1.1. Overview

What is Vade for Google Workspace?

Vade for Google Workspace 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 Google Workspace messaging solution and increases its security thanks to Artificial Intelligence.

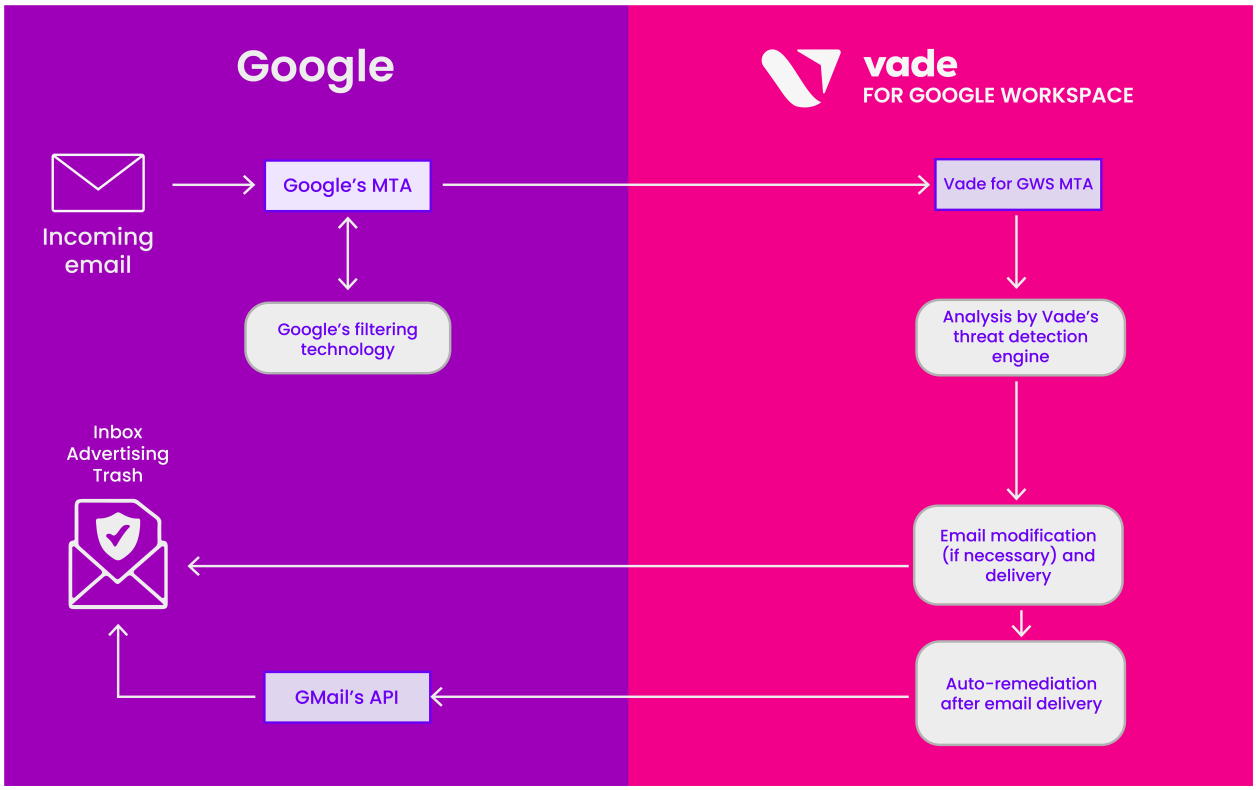
You can enable Vade for Google Workspace with small architecture changes, implemented directly in your workspace's settings (no MX record changes). The administration UI was designed to provide simple configuration and full reports and analysis information about blocked attacks. Your users won't have to change the way they access their emails or use a new interface.

Supported browsers

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

- Google Chrome
- Firefox
- Edge
- Safari

1.2. Architecture Diagram



How it works

1. When you receive a new email, Google scans it with their own filtering solution.
2. The email itself is then redirected to Vade for Google Workspace's MTA to be analyzed.
3. Vade for Google Workspace performs the analysis on the email.
4. Vade for Google Workspace connects to Google's API to retrieve the user's preferences, etc.
5. Vade for Google Workspace then moves the email to the proper label, or deletes it using Vade's MTA.

1.3. Frequently Asked Questions

Is Google Workspace's phishing and malware protection still available?

Yes, the Vade for Google Workspace filtering comes on top of Google Workspace's protection.

How well does the Vade solution integrate with Google Workspace?

Vade for Google Workspace receives the email before it arrives in the users mailbox. The email is modified according to the admin's preferences with Vade's MTA, and is sent back to Google Workspace.

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 Google Workspace admin console. By default, Vade will use Google's labels "**Social**", "**Updates**", "**Forum**" and "**Promotions**" to move newsletters and graymail detected by Vade's filter. These labels are natively available in Gmail mailboxes. If you wish to change the way Vade for Google Workspace acts on newsletters and graymail, you can turn it off by selecting "No action" in **Settings > Email Protection**.

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 Google Workspace, and remains unchanged.

Does the filter override my preferences?

No, Google Workspace applies your preferences before Vade receives the emails to filter. As such, the allowlists, denylists, approved senders lists and labels you created are respected by the filter.

Does the filter override the inbox rules?

No, the inbox rules (e.g. *Move emails from … to label …*) will always take precedence. Vade for Google Workspace will only move emails that were meant to be delivered in the Inbox.

Where do I create allowlists in the product?

You can create allowlists on Vade for Google Workspace. To do so, navigate to **Settings > Email Protection**. Google's API does not provide Vade with the means to get the Allowlists set up in the Admin console.

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.

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 denylisted an address which a user has allowlisted?

Filtering rules created on Google Workspace always take precedence over the filter decisions, or inbox rules created by the user. However, if your filtering rules are set up on Vade for Google Workspace, these rules will take precedence over the inbox rules created by the user.

Is the Vade filtering applied to all email?

The Vade filtering is applied to all the emails in your users' inbox.

1.4. Support

Vade provides technical support by phone or email for Vade for Google Workspace.

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

Support is available in English and French.

2. 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

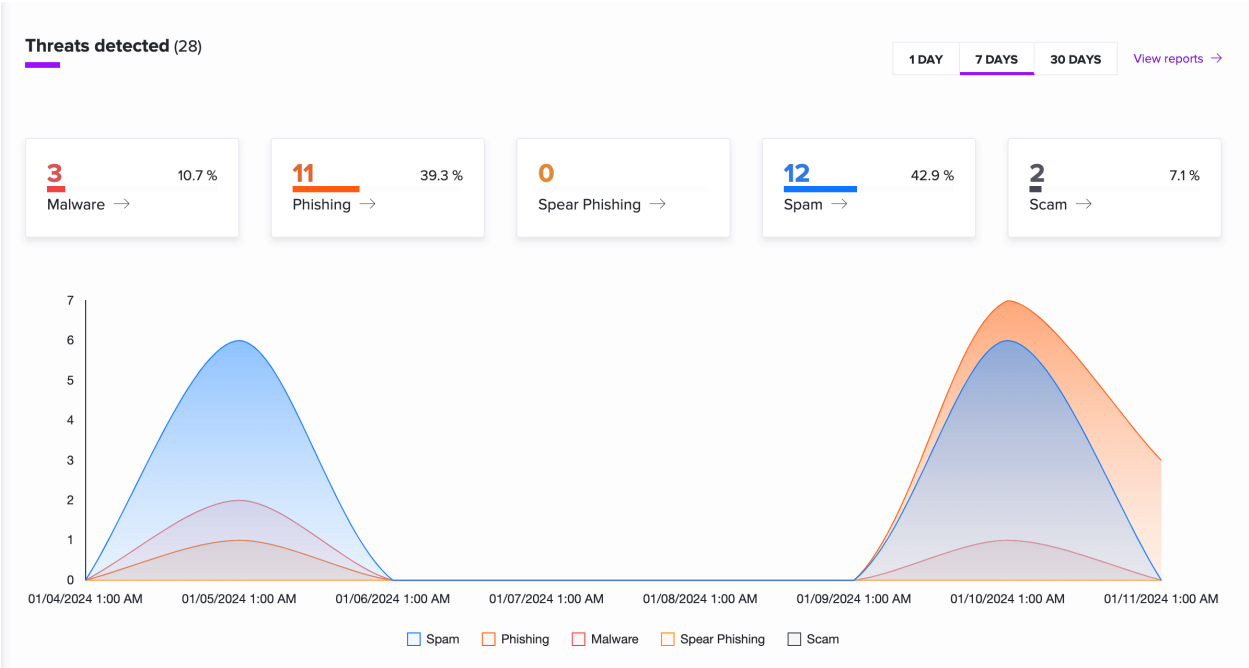
This section offers an overview of the threats detected by Vade for Google Workspace during the period of time you selected in the top right-hand corner.

	Allowlisted 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.

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



Last targeted attacks

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

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 phishing, malware or spear phishing.

Related information

Settings - Global

Email logs

Threat Report

3. Logs

3.1. 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.

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

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.

REMEDIATION ID

Type in a remediation 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

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

ACTION

Moved

Emails Vade for Google Workspace moved.

Banner

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

Deleted

Emails Vade for Google Workspace deleted.

Attach. removed

Emails Vade for Google Workspace removed malicious attachments from.

No action

Emails Vade for Google Workspace 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.

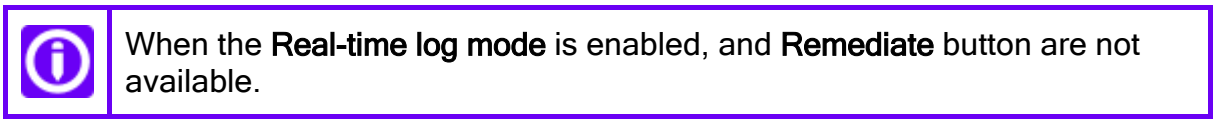
WITHOUT

Emails without any attachments.

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.



Search results

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 campaign 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.

Remediation

The remediation status:
- Remediated, or
- Not remediated (empty field)

The exposure of the user:
- Email opened, or
- Email unopened

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

Action

Actions are taken on the email depending on the Vade for Google Workspace settings. Actions can be successful or fail. Potential actions are:

Moved

The email was moved from the inbox to another folder.

Deleted

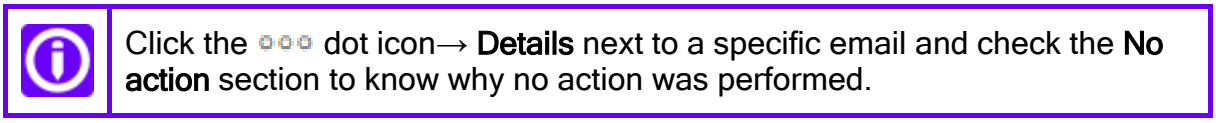
The email was deleted.

Banner

A warning banner was added to the email.

No action

No action was performed on the email.



Attach. removed

Malicious attachments were removed from 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

Click the ooo **dot icon→ Details** to open a new tab with all the details of the email log.

Click **Remediate** to remediate and report the email.

Log search reset

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

Remediate

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

Related information

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

How to remediate emails?

How to export emails logs?

3.1.1. 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"`

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 GWS, 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.

3.1.2. 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 email are returned:

Message ID

The Unique ID of the email (generated by the mail platform itself, such as Gmail).

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 email, 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 email, which may differ from the address used in the SMTP RCPT TO command.

Subject

The contents of the **Subject** header of the email.

Source IP

The originating IP the email 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 email headers, which trace the route the email 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 email, and if present, a list of URLs found in the email.

Attachment-related information

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

Content-Type

The Content-type declared for the email.

Number of attachments

If present, the number of attachments found in the email, 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.

3.2. Remediate and report emails

Remediate lets Vade for Google Workspace 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 Google Workspace allows you to move users' emails from their Inbox to any other label 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.

> ⓘ 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.

> ⓘ The emails are all selected by default.

6. Click **Next**.

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

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

9. Click **Confirm**.

> 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 an action in the drop down menu.

> Selecting Delete will delete the email permanently.

- **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 information

Remediation logs

3.3. 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.

Remediation

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

Date & time

The date of the remediation.

Remediation ID

The ID of the remediation 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. Actions can success or fail.

Details

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

3.4. 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.

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.

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 email 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 email: `Visited`, `Blocked`, `Warning - Visited` or `Warning - Not visited`.

3.4.1. 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. "Google" or "Cloud", etc.

clientID

The unique ID of the client, which relates to the Customer ID in the context of Google Workspace.

creationDate

The date on which the log entry was created.

from

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

to

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

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.

4. Reports

4.1. 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.

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 threat.

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 emails that were identified as threats.

Top extensions

This list provides the attachment extensions that have been seen the most frequently in emails 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*.

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?

4.2. Low priority Report

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

The report provides figures and charts representing the number of emails 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 emails 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 emails, 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 emails for low priority emails.

Related information

How to manage reports?

4.3. Auto-remediation Report

This report provides information about auto-remediated emails.

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.

5. Toolbox

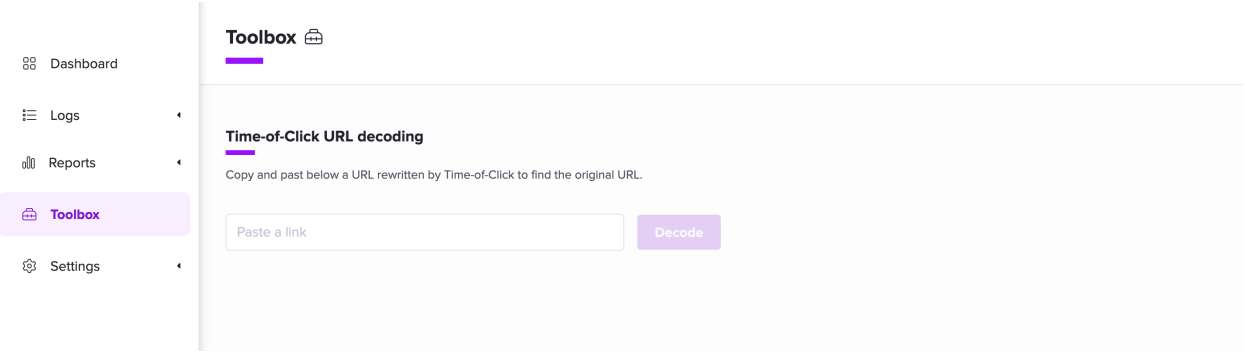
5.1. Time-of-Click URL decoding

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 Google Workspace. 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 Google Workspace admin console.

1. Log in to the Vade for Google Workspace 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.



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

Settings - Anti-Phishing

6. Settings

6.1. General

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 Google Workspace.

> Once enabled, **Protection mode enabled** will be displayed on the Dashboard page.

Monitoring

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

Filter enhancement

Allow Vade to keep a copy of your email flow for up to 7 days to analyze them and further enhance your protection.

6.2. URL protection

On this page you can choose how you defend your organization further by protecting users from malicious URLs.

Remote Browser Isolation (add on)

Enable Vade Remote Browser Isolation (RBI) to protect your devices not only from phishing but from advanced web-based threats including malware, tracking, click-jacking, and more. RBI is the best protection against malicious URLs in emails.

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.

This feature does not apply to allowlisted emails, 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 receiving the alerts

Type in the email address 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.

These fields accept HTML code with inline formatting.

6.3. Email protection

6.3.1. Anti-Malware

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

Manage actions by status

Action

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

No action

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

Hard delete (Recommended)

The platform will delete the email: It will not be available in the user's inbox or under any other mailbox label.

Move

The platform will move the email to the label declared in the **Label** field.

Remove attachments

The platform will remove all attachments found in the email indicated as a Malware by our filtering solution.

In case the attachments were removed, a banner will be added to the email.

Banner

The platform will prepend an alert banner to the top of the email body, to warn the user of the potential targeted attack.

Label

The name of the label to move the email to.

Auto-Remediate

Activated by default, this feature learns over time and can fix automatically email verdicts received over the last 24 hours.

Post-delivery email attacks will be automatically moved to the correct label based on the new verdict.

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 allowlisted 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 label.
- If the email has already been remediated manually.

If Auto-Remediate is activated for Malware and the action chosen is “Remove attachments”, the email will be deleted by Vade for Google Workspace instead. Google’s API doesn’t provide any means to edit post-delivery emails.

Warning banner preview

Banner

A preview version of the banner added at the top of the email body is displayed. This first version is not customizable.

6.3.2. 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 email of this type. Options are:

No action

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

Hard delete

The platform will delete the email: It will not be available in the user's inbox or under any other mailbox label.

Move (Recommended)

The platform will move the email to the label declared in the **Label** field.

Label

The name of the label to move the email to.

Auto-Remediate

Activated by default, this feature learns over time and can fix automatically email verdicts received over the last 24 hours.

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 allowlisted 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 label.
- If the email has already been remediated manually.

6.3.3. Anti-Spear Phishing

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

Impersonation and natural language processing

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.

Banking fraud

Threats relating to banks. The sender pretends to be a financial institution to steal data or money from users.

CEO fraud

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

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.

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.

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.

Payroll fraud

The email is suspicious, it requests to change the bank details of an employee.

Tax scam

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.

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 email. It will be delivered as-is in the user's mailbox.

Move

The platform will move the email to the label declared in the **Label** field.

Banner (Recommended)

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

Label

The name of the label to move the email to.

Customize the warning banner

Banner

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

6.3.4. 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 emails.

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 emails. Recommended action is to Delete these emails.

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 email. It will be delivered as-is in the user's mailbox.

Hard delete

The platform will delete the email permanently.

Move (Recommended)

The platform will move the email under the label declared in the **Label** field. Vade recommends moving low spam to Spam label and moving high spam, medium spam, and scam emails to Trash.

Label

The name of the label to move the email to.

Auto-Remediate

Activated by default, this feature learns over time and can fix automatically email verdicts received over the last 24 hours.

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 allowlisted 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.

6.3.5. Classification

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

Status

The type of email detected by the filter.

> **Newsletters**
>
> Newsletter emails.
>
> **Social**
>
> Social media emails.
>
> **Purchase**
>
> Order/confirmation, invoices, etc.
>
> **Travel**
>
> Travel booking, reservation, confirmation, etc.

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 email. Google Workspace labels will be applied to the emails since Gmail does its own filtering of low-priority email natively.
>
> **Hard delete**
>
> The platform will delete the email permanently.
>
> **Move (Recommended)**
>
> The platform will move the email under the label declared in the **Label** field.

Label

The name of the label to move the email to.

7. RBAC

With RBAC, map Google administrator roles to Vade roles for customized user permissions.

RBAC, or Role-Based Access Control, helps you define users' rights on your administration console by mapping Google administrator roles to Vade roles.

Vade roles and permissions

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

Permissions

List of user permissions for the Vade role.

Search role

Type in any Google role in the search bar.

Add mapping

Click the **Add mapping** button to map Google roles to Vade roles.

Google role

List of Google roles mapped to Vade roles.

7.1. Add mapping

You can associate Google roles to Vade roles to define users' rights.

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