

vade
FOR M365

Vade for M365

Activation Guide

Last modified: May 16, 2022

Version 2.46

Chapter 1: Overview.....3

 Support.....3

 Architecture Diagram.....3

 Frequently Asked Questions.....4

 How to grant access to the admin console?.....6

Chapter 2: Set up process.....7

 Activation process.....7

 Retrieve the Tenant ID.....7

 Create a new client on the Partner Portal.....7

 Add a license to the profile of a client.....8

 Activate your license.....8

 Confirm the permissions using a Microsoft 365 Global Admin account.....8

 Create a journal rule.....8

About permissions.....10

Overview

Support

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

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

Email:

support@vadesecure.com

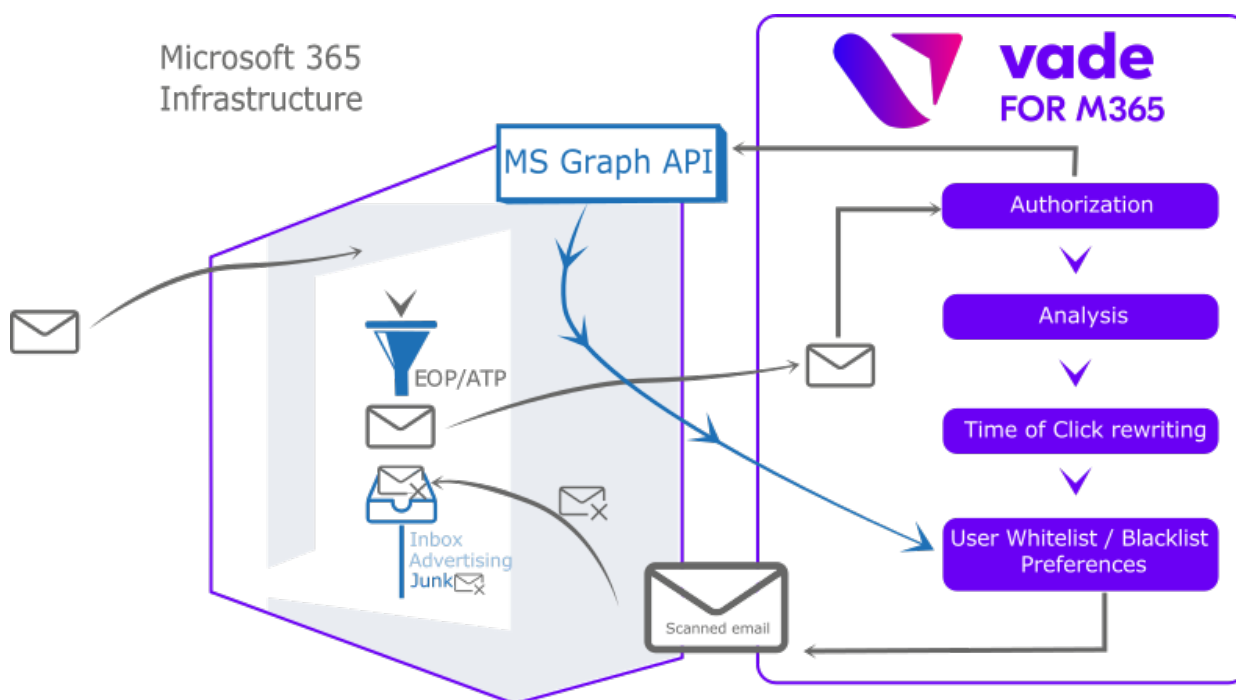
Phone:

- 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



Note: Support is available in English and French.

Architecture Diagram



How it works

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

Frequently Asked Questions

Are Microsoft 365 EOP & ATP protections still available?

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

How well does the Vade solution integrate with Microsoft?

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

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

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

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

Report an email from Outlook Web:

1. Open an email.
2. Click **Junk**.
3. Click **Junk** or **Phishing**.

Report an email from the Outlook client:

1. Download the [Report Message add-in on Microsoft AppSource](#).
2. Install the add-in.
3. Open an email in the Outlook client.
4. Click the new **Report message** button.
5. Click **Junk** or **Phishing**.

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

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

Will I stop receiving newsletters if the solution moves them?

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

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

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

Does Vade keep a copy of all emails?

No, Vade deletes the copy after the analysis.

Do I need to update my MX record?

No, the MX record still points to Microsoft 365, and remains unchanged. The Vade for M365 is natively integrated to the Microsoft 365 platform through Microsoft API. As such, the only required step is to activate the solution so that the filter is allowed to scan your Tenant's emails. See [Activation process](#) on page 7.

Does the filter override my preferences?

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



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

Does the filter override the inbox rules?

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

Where do I create whitelists in the product?

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



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

How come I get so many spear phishing notifications?

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

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



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

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

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

Is the Vade filtering applied to all messages?

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

How to grant access to the admin console?

You might want to help your partner assist you more easily. To do that, you can grant them access to your Vade for M365 admin console.

Procedure

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

Results

The partner will receive an email confirming their access to your admin console.

Set up process

Activation process

Follow the steps below to set up Vade for M365.

Before you begin



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

Procedure

1. Retrieve the [Tenant ID](#) on page 7
2. Create a new client on the [Partner Portal](#) on page 7
3. Add a license to the profile of a client on page 8
4. Activate your license on page 8
5. Confirm the permissions using a [Microsoft 365 Global Admin account](#) on page 8
6. Create a journal rule on page 8

Retrieve the Tenant ID

Procedure

1. Log in to the [Microsoft Azure Portal](#) with your admin credentials.
2. Click [Azure Active Directory](#) under [Azure services](#) in the left menu.

Results

You will find the *Tenant ID* in the [Overview](#).

Create a new client on the Partner Portal

Procedure

1. Access the Portal at <https://partner.vadesecure.com>.
2. Click the [Clients](#) tab.
3. Click the [Add a client](#) button.
4. Fill in the required fields.
5. Click the [Add a client](#) button.

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

Add a license to the profile of a client

Procedure

1. Log in to the Partner Portal.
2. Click the **Clients** tab in the left menu.
3. Click the **Details** button of a specific client.
4. Click 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) Fill in the number of users associated with the Tenant ID.
 - f) Click the *I understand that I am ordering licenses and that I must settle this order with my distributor* checkbox.
5. Click the **Order a license** button.

Results

The license state is **Pending validation** until the end user activates it via the activation email. The state is then **Active**.

Activate your license


Procedure

1. Check your emails for an activation email sent by Vade.
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 a Microsoft 365 Global Admin account

Procedure

1. Log into the Vade admin console.
 - For Europe: <https://m365.eu.vadesecure.com/>
 -  **Note:** Germany: <https://m365.de.vadesecure.com/>
 - For the US: <https://m365.us.vadesecure.com/>
 - For Asia: <https://m365.asia.vadesecure.com/>
2. Click **Accept** to accept the basic permissions required by the Vade 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 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 the **Exchange admin center**.
2. Click **Classic Exchange admin center** in the left menu to open the classic interface.



Note: It is impossible to create journal rules in the new interface of the Exchange admin center.

3. Click **compliance management** in the left menu.
4. Click **journal rules**.
5. Click **Send undeliverable journal reports to...** to add the email address which will receive the undeliverable journal reports in case emails were not journalized.



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

We provide dedicated email addresses for this exact purpose. Make sure to add the one you need to your contact list:

- a. Go to **recipients > contacts > + > Mail contact**.
- b. Type in Vade - support journaling in **Display name**.
- c. Type in vs.support.journaling in **Alias**.
- d. Type in one of the Vade addresses in **External email address** according to your location:
 - For Europe:
 - Servers based in France: undeliverable@bounce.eu.vadesecure.com
 - Servers based in Germany: undeliverable@bounce.de.vadesecure.com
 - For the United States: undeliverable@bounce.us.vadesecure.com
 - For Asia: undeliverable@bounce.asia.vadesecure.com
- e. Click **Save**.

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

- a) Click the **+** icon.
The **new journal rule** window opens.
- b) Type your dedicated address under **Send journal reports to**.
 - For Europe: journal@m365.eu.vadesecure.com
 - Dedicated address for Germany: journal@m365.de.vadesecure.com
 - For the US: journal@m365.us.vadesecure.com
 - For Asia: journal@m365.asia.vadesecure.com
- c) Type the name of the rule.
- d) Select **[Apply to all messages]** or **A specific user or group...** under **If the message is sent to or received from** depending on your needs.
- e) Select **All** messages under **Journal the following messages...**
- f) Click **Save**.

Results

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

About permissions

Learn more about the permissions you have to grant when you first log in to the admin console.



Tip:

- DELEGATED: Application can act on behalf of a signed-in user.
- APPLICATION: Application can act on its own without a signed-in user.

Read all users' full profiles

Allows the app to read user profiles. (APPLICATION)

Read all usage reports

Allows the app to read all service usage reports. (DELEGATED + APPLICATION)



Note: Services that provide usage reports include Microsoft 365 and Azure Active Directory.

Read directory data

Allows the app to read data in your organization's directory, such as users, groups and apps. (DELEGATED + APPLICATION)

Read and write access to user mail

Allows the app to create, read, update, and delete emails in user mailboxes. Does not include permission to send emails. (DELEGATED)

Sign in and read user profile

Allows users to sign in to the app, and allows the app to read the profile and basic company information of signed-in users. (DELEGATED)

Read and write mail in all mailboxes

Allows the app to create, read, update, and delete mail in all mailboxes. Does not include permission to send emails. (APPLICATION)

Read all groups

Allows the app to read group properties and memberships, and read the calendar and conversations for all groups. (APPLICATION)