Installation guide

Install Email Meter Enterprise on your Microsoft 365 domain

Before starting

Email Meter Enterprise needs to be installed on your domain.

This means installation needs to be performed by an administrator — or by a user with enough permissions to do this in the Microsoft 365 admin center.

Step 1

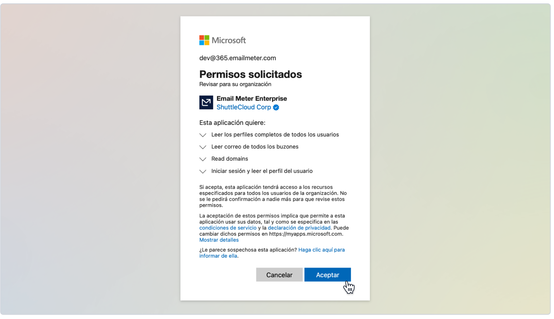
Install Email Meter on your Microsoft 365 domain

Click the following link to go to the Email Meter Enterprise application on the Google Workspace Marketplace.

Email Meter Enterprise application →

You'll be redirected to a Microsoft 365 login page.

Sign in using a global admin account (or a user with a license and privileged administrator role) and accept the permissions on the consent screen.



You'll be automatically redirected to an Email Meter page that confirms the installation.

That's it! Email Meter Enterprise is now installed on your domain.

Limiting access to specific mailboxes

You can restict Email Meter's access to specific mailboxes by using mail-enabled security groups and an ApplicationAccessPolicy.

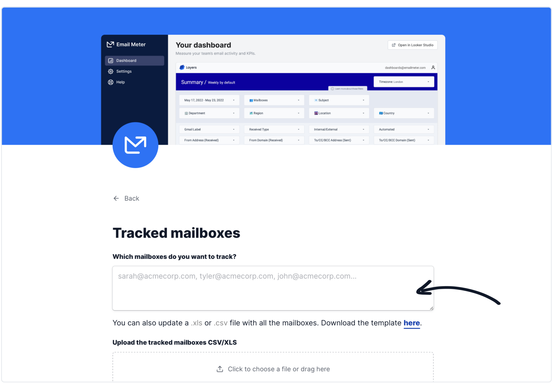
To do it, you can follow this guide or Microsoft's official documentation here.

Step 2

Fill out the onboarding form

Once the application is installed, you'll need to fill out the onboarding form.

Email Meter onboarding form →



In the onboarding form, you will be asked to provide information such as the mailboxes that need to be tracked, the users that need access to see email statistics, the level of access they should have, business hours, timezone and other relevant settings.

Our team will be automatically notified and will start building your custom email statistics dashboard.

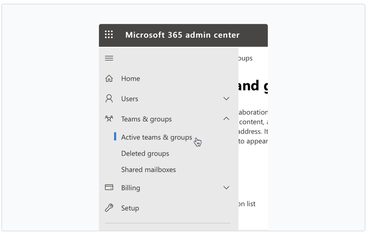
© 2023 Email Meter

Limiting permissions to specific mailboxes

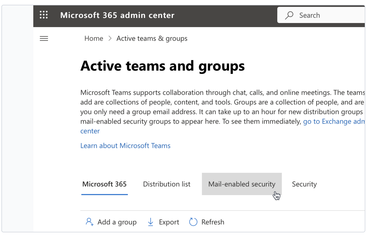
Step 1

Create a Mail-enabled security group

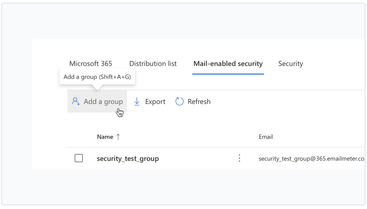
Log into your Microsoft 365 admin portal and click on Groups → Active.



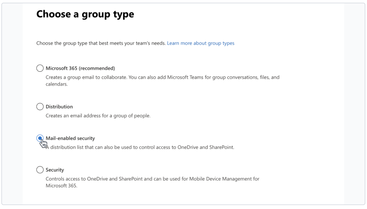
Choose **Mail-enabled security** on the secondary navigation menu.



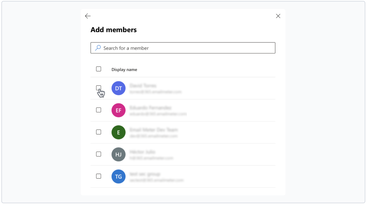
Click on **Add a group** to create a new group.



On the following screen, select **Mail-enabled security group**. Then, select the name, owners and members that you desire.



Once created, you can click into the just created Mail-enabled security group and click on "Members" to choose the members that you want to add to the security group. **Those will be the only mailboxes that Email Meter will be able to get data from.**



Step 2

Create an ApplicationAccessPolicy

Now you'll need to create an ApplicationAccessPolicy to limit Email Meter access to the specific mailboxes you've added to the Mail-enabled security group.

Read more about this on Microsoft's documentation →

Connect to Exchange Online PowerShell

For detailed instructions, please read:

Microsoft's documentation on connecting to Exchange Online PowerShell.

Create an ApplicationAccessPolicy

In PowerShell, run the following command, replacing the arguments for **PolicyScopeGroupId**, and **Description**.

```
New-ApplicationAccessPolicy -AppId
e7e4dbfc-046f-4074-9b3b-2ae8f144f59b -PolicyScopeGroupId
securitygroup@yourcompany.com -AccessRight RestrictAccess -
Description "Restrict this app to members of the Mail-
enabled security group."
```

Test the newly created application access policy

Once this is done, you'll be able to easily test that the policy is restricting access to the members in the Security Group by running a PowerShell command.

Just replace the argument for **Identity**, and run the following command:

```
Test-ApplicationAccessPolicy -Identity
exampleuser@yourcompany.com -AppId
e7e4dbfc-046f-4074-9b3b-2ae8f144f59b
```

Before starting

Changes to application access policies can take longer than 1 hour to take effect in Microsoft Graph REST API calls, even when `Test-ApplicationAccessPolicy` shows positive results.

© 2023 Email Meter

What Microsoft Graph permissions does Email Meter request?

In order to ingest email to generate email statistics, Email Meter connects using the Microsoft Graph API.

This page lists the permissions that Email Meter requires and provides information on what each permission is used for.

Permission	Display String	Description	Used for
Mail.Read	Read mail in all mailboxes	Allows the app to read mail in all mailboxes without a signed-in user.	Reading email headers in user's mailboxes to generate email statistics.
User.Read.All	Read all users' full profiles	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization.	Getting the full name and profile picture of users.
Domain.ReadAll	Read-only	Allows the app to read the domain list.	Setting the default domains that are considered as internal on the email metric calculations. This can be manually customized later.

Although Mail.Read gives the app permission to read the body of our emails, none of Email Meter's systems read, process or store the body or attachments of emails. The only information that we analyze are the email headers which contain data such as: `from`, `to`, `subject` and `date`. Please get in touch if you want more details about this.

© 2023 Email Meter