

Application registration and permissions

The Data & More Compliance Solution (DMCS) connects to Microsoft 365 through an app registration in your Entra ID tenant. You can choose between four ways to connect. They differ in what Data & More is allowed to do, from read-only scanning to real-time data loss prevention. This article explains each option and every permission it asks for.

01

Demo
Read-only scan of mail and files. Good for a trial.

02

Production
Full scanning plus policy actions on mail, files and Teams.

03

Production + DLP
Everything in Production plus real-time DLP and Copilot.

04

Add App Registration
You create and control your own app registration.

- **Demo:** read-only scan of mail and files. Good for a trial.
- **Production:** full scanning plus policy actions on mail, files and Teams.
- **Production + DLP:** everything in Production plus real-time DLP and Copilot.
- **Add App Registration:** you create and control your own app registration.

How consent works

In Data & More, go to **Settings → App registration**. The four buttons at the top are the four options: **Demo**, **Production**, **Production + DLP** and **Add App Registration**. The first three use an app registration that Data & More maintains: select the button to get a consent link, and a Microsoft 365 administrator approves the permissions for your whole organisation. If you are not an administrator yourself, the same screen gives you an invitation e-mail to send to one.

All permissions in the first three options are **application permissions**. Data & More acts as a service, not as a signed-in user, so scanning keeps working when people are away and nobody's personal password is involved. You can see and revoke the granted permissions at any time in the Entra admin center under **Enterprise applications**.

Write permissions do not mean automatic deletion. Deletions go through a human approval step in Data & More before anything is removed.

Who needs to approve

- **Global Administrator** or **Privileged Role Administrator**: approves the app permissions (all options).
- **Exchange Administrator** (or Global Administrator): the one-time "Grant Exchange access" step in Production + DLP.
- **Teams Administrator** (or Global Administrator): the one-time "Install Teams bot" step in Production + DLP.

What each option can do

Capability	Demo	Production	Production + DLP	Add App Registration
Scan Outlook mail	Yes	Yes	Yes	You choose
Scan OneDrive and SharePoint files	Yes	Yes	Yes	You choose
Scan Teams channels and chats	No	Yes	Yes	You choose
Recognise known people from Outlook contacts	No	Yes	Yes	You choose

Read your sensitivity labels (Purview)	Yes	Yes	Yes	You choose
Send reports and notifications by e-mail	Yes	Yes	Yes	You choose
Policy actions: move to vault, delete, restore, tag, apply labels	No	Yes	Yes	You choose
Real-time DLP on e-mail, files and Teams	No	No	Yes	You choose
Copilot prompts and responses	No	No	Yes	You choose
Alerts in Teams from the Data & More bot	No	No	Yes	You choose
Who maintains the app registration	Data & More	Data & More	Data & More	You
Access to your data	Read only	Read and write	Read and write	As you grant

You can move to a larger option later. Select the larger option's button in Settings and approve again; the extra permissions are added to the existing app.

Option 1: Demo (read only)

The smallest set. Data & More reads mailboxes and files to show you where personal and sensitive data sits, but it cannot change anything in your tenant. Use it for a trial or a first assessment.

- **Covers:** Outlook, OneDrive and SharePoint files.
- **Changes data:** no, reports only.
- **Approval:** Global Administrator, one click.

Permission	Access	What Data & More uses it for
User.Read.All	Read	Reads the list of users and their basic profile (name, e-mail, department, manager), so it knows whose mailboxes and OneDrives to scan and who owns the data it finds.
Directory.Read.All	Read	Reads groups and group membership, your organisation name and verified domains, and which permissions were granted. Used for group-based scoping and the Check Permissions button.
Mail.Read	Read	Reads e-mails and attachments so they can be scanned for personal and sensitive data.
Files.Read.All	Read	Reads files in OneDrive and SharePoint, and who they are shared with, so they can be scanned.
InformationProtectionPolicy.Read.All	Read	Reads your Microsoft Purview sensitivity labels, so findings can be compared with how data is labelled.
Mail.Send	Send	Sends Data & More reports and notifications from a mailbox you choose. It does not read or change existing mail.

Option 2: Production (read and write)

For day-to-day use. Data & More scans all of Microsoft 365, including Teams, and carries out the policies you set up: moving sensitive mail and files to a vault, deleting data past its retention date, restoring it, tagging it and applying sensitivity labels. All permissions are required.

- **Covers:** Outlook, OneDrive, SharePoint and Teams.
- **Changes data:** only when a policy you configured says so.

- **Approval:** Global Administrator, one click.

Microsoft Graph

Permission	Access	What Data & More uses it for
User.Read.All	Read	Users and basic profile, licences and photos: whose data to scan and who owns it.
Directory.Read.All	Read	Groups and membership, Teams and their channels, organisation details, and the permission check.
Mail.ReadWrite	Read and write	Scans e-mails and attachments. Policies can move mail to the GDPRvault folder, move it back, delete or restore it, and add Outlook categories.
MailboxSettings.ReadWrite	Read and write	Creates the Outlook categories used for tagging, and tells shared mailboxes from personal ones.
Mail.Send	Send	Sends reports and notifications from a mailbox you choose.
Contacts.Read	Read	Reads Outlook contacts, so external people your employees work with are recognised as known persons.
Files.ReadWrite.All	Read and write	Scans OneDrive, SharePoint and Teams files. Policies can move files to a vault folder, delete or restore them, and apply a sensitivity label.
Sites.ReadWrite.All	Read and write	Finds SharePoint sites and document libraries, writes Data & More metadata into library columns, and restores files from the recycle bin.
Sites.FullControl.All	Manage	Adds the Data & More metadata columns to document libraries when a policy needs them.
Team.ReadBasic.All	Read	Reads basic information about Teams.
ChannelMessage.Read.All	Read	Reads posts and replies in Teams channels so they can be scanned.
Chat.Read.All	Read	Reads 1:1 and group chats in Teams so they can be scanned.
InformationProtectionPolicy.Read.All	Read	Reads your sensitivity labels, so policies can apply them and findings can be compared with them.

SharePoint

These three are granted on the SharePoint API rather than Microsoft Graph. They are used to read site groups and site owners, so findings on a site go to the people responsible for it.

Permission	Access	What Data & More uses it for
Sites.Read.All	Read	Reads SharePoint site groups and their members.
Sites.FullControl.All	Manage	Reads a site's owner group.
User.Read.All	Read	Resolves SharePoint users to people in your directory.

Scanning the Exchange Online Archive

The Online Archive is read through Exchange Web Services (EWS), which is not covered by any of the packages. If you want to scan it, also grant the **Office 365 Exchange Online** application permission `full_access_as_app`.

Option 3: Production + DLP (read and write)

Everything in Production, plus real-time data loss prevention. Microsoft 365 notifies Data & More the moment an e-mail is sent, a file is shared or a Teams message is posted. Data & More checks it against your DLP policies and can alert, hold or block it within seconds. It also covers Microsoft 365 Copilot and can alert users through a Teams bot.

- **Covers:** Production, plus real-time DLP and Copilot.
- **Changes data:** blocks, holds or restricts sharing when a DLP policy matches.
- **Approval:** Global Administrator, plus up to three one-time steps.

In addition to all Production permissions

Permission	API	Access	What Data & More uses it for
AiEnterpriseInteraction.Read.All	Microsoft Graph	Read	Reads Microsoft 365 Copilot prompts and responses so they can be checked for sensitive data. Each user needs a Microsoft 365 Copilot licence.
AuditLogsQuery.Read.All	Microsoft Graph	Read	Searches the audit log for Copilot Chat and agent activity that the Copilot export does not include.
AppCatalog.Read.All	Microsoft Graph	Read	Finds the Data & More DLP bot in your Teams app catalog.
TeamsAppInstallation.ReadWriteForUser.All	Microsoft Graph	Install	Installs the Data & More DLP bot for users in scope, so it can send them alerts in a 1:1 chat.
TeamsAppInstallation.ReadWriteForTeam.All	Microsoft Graph	Install	Installs the bot in Teams where channel alerts are needed.
Exchange.ManageAsApp	Office 365 Exchange Online	Manage	Creates and maintains the mail-flow rules that hold outgoing e-mail to external recipients until it has been checked. Data & More only manages its own rules.

One-time setup steps

Some actions cannot be granted as app permissions. You complete them once from the DLP page, signed in as an administrator.

Step	Who signs in	What it grants
Grant Exchange access	Exchange Administrator or Global Administrator	Signs in with the delegated Exchange.Manage permission and registers Data & More in Exchange Online with two Exchange roles: Transport Rules (manage its mail-flow rules) and View-Only Configuration (read your accepted domains, so internal mail is not held).
Install Teams bot	Teams Administrator or Global Administrator	Uses the delegated AppCatalog.ReadWrite.All permission once to publish the Data & More DLP bot to your organisation's Teams app catalog.
Allow Teams message deletion (optional)	Global Administrator, or each message author	Microsoft only lets a Teams message be deleted on behalf of its author. Approving the delegated ChannelMessage.ReadWrite and Chat.ReadWrite permissions for the organisation lets DLP remove a blocked message without asking each author.

Copilot DLP is alert-only: Data & More can notify about a risky Copilot conversation but does not change it.

Option 4: Add App Registration (your own app)

Some organisations prefer to create the app registration in their own tenant, so they own the credentials and decide exactly which permissions to grant. Data & More then uses that app instead of its own. Grant only what the sources and features you plan to use need; the table at the end of this section lists the minimum for each.

1. Register the app

1. Sign in to **portal.azure.com** as a Global Administrator.

2. Search for **App registrations** and select **New registration**.
3. Enter a name (for example *Data & More DMCS*) and choose **Accounts in this organizational directory only**.
4. Under **Redirect URI**, choose **Web** and enter `https://signup.dataandmore.com/api/authorized`.
5. Select **Register**.
6. Open **Authentication** and add two more **Web** redirect URIs: `https://signup.dataandmore.com/api/authorize_redirect` and your Data & More server address followed by `/api/auth/ad/login/authorized`. If your server is `https://gdpr.dataandmore.com`, that is `https://gdpr.dataandmore.com/api/auth/ad/login/authorized`. Select **Save**.

Always add both `signup.dataandmore.com` addresses, whichever package you use. They are needed for the consent and sign-in steps.

2. Add the API permissions

1. Open **API permissions** and select **Add a permission → Microsoft Graph → Application permissions**. Add the Graph permissions for your package (Demo, Production or Production + DLP above), or the minimum set for the features you want from the table below.
2. **SharePoint** (Production and Production + DLP): select **Add a permission** again, open **APIs my organization uses**, search for **SharePoint**, and add the three SharePoint application permissions.
3. **Exchange** (Production + DLP, or Online Archive): select **Add a permission → APIs my organization uses**, search for **Office 365 Exchange Online**, and add `Exchange.ManageAsApp` (DLP) and/or `full_access_as_app` (Online Archive).
4. Select **Grant admin consent** and confirm. Every permission should now show a green **Granted** status.

3. Create the credentials

1. On the app's **Overview** page, note the **Application (client) ID** and the **Directory (tenant) ID**.
2. Open **Certificates & secrets → New client secret**, add a description and expiry date, and select **Add**.
3. Copy the secret **Value** straight away. It is only shown once, and you need the value, not the secret ID. Alternatively, upload a certificate; a certificate is required to read SharePoint site groups and owners.

4. Connect it to Data & More

1. In Data & More, open **Settings → App registration → Add App Registration** and enter the tenant ID, client ID and the secret value or certificate. If you cannot do this yourself, send the three values to **support@dataandmore.com** through a secure channel.
2. Select **Check Permissions**. Data & More lists which permissions it found, flags any that are missing, and shows when the secret or certificate expires.

Minimum permissions per feature

Feature	Scan (read)	Policy actions (write)
Always needed	<code>User.Read.All</code> , <code>GroupMember.Read.All</code> , <code>Organization.Read.All</code> , <code>Application.Read.All</code>	None
Outlook	<code>Mail.Read</code> , <code>MailboxSettings.Read</code>	<code>Mail.ReadWrite</code> , <code>MailboxSettings.ReadWrite</code>
Exchange Online Archive	Exchange: <code>full_access_as_app</code>	Exchange: <code>full_access_as_app</code>
OneDrive	<code>Files.Read.All</code>	<code>Files.ReadWrite.All</code> , <code>Sites.ReadWrite.All</code> , <code>Sites.Manage.All</code>

SharePoint	Sites.Read.All, Files.Read.All; SharePoint: Sites.Read.All (certificate)	Files.ReadWrite.All, Sites.ReadWrite.All, Sites.Manage.All
Teams channels	Channel.ReadBasic.All, ChannelMessage.Read.All, Files.Read.All	Files.ReadWrite.All
Teams chats	Chat.Read.All	None
Known persons	Contacts.Read	None
Sensitivity labels	InformationProtectionPolicy.Read.All	Files.ReadWrite.All (to apply)
Reports by e-mail	None	Mail.Send
Copilot	AIEnterpriseInteraction.Read.All, AuditLogsQuery.Read.All	None
Real-time DLP	The scan permissions of each source you protect	Exchange: Exchange.ManageAsApp; Graph: Mail.ReadWrite, Mail.Send, Files.ReadWrite.All, AppCatalog.Read.All, TeamsAppInstallation.ReadWriteSelfForUser.All, TeamsAppInstallation.ReadWriteSelfForTeam.All; plus the one-time steps under Production + DLP

Keep in mind: you are responsible for renewing the secret or certificate before it expires; the **Check Permissions** view shows the expiry date. If a permission is missing, the related source shows an access error instead of failing silently. Add the permission, grant admin consent again, and run **Check Permissions**.

Limit what Data & More can reach

Application permissions apply to the whole tenant. If you want to narrow them, Microsoft offers these controls, and Data & More works with all of them:

- **Scope in Data & More.** Choose which users, groups, sites and Teams each source covers. Nothing outside the scope is scanned or changed.
- **Exchange application access policy or RBAC for Applications.** Restrict Mail.Send and mailbox access to a mail-enabled security group.
- **Audit.** Every call Data & More makes appears in your Entra sign-in logs and the Microsoft 365 audit log under the app's name.

Common questions

Can Data & More read my users' passwords?

No. None of these permissions give access to passwords or sign-in credentials. Data & More authenticates as its own app, with its own secret or certificate.

Why does a read-mostly product need write permissions?

Write access is only used when a policy you configured tells Data & More to act, for example to move a sensitive file to a vault or delete e-mail past its retention date. Deletions also go through a human approval step. If you only want reports, choose Demo, or grant read permissions only in your own app.

Can we start with Demo and upgrade later?

Yes. Select **Production** or **Production + DLP** in **Settings → App registration** and approve again. Your existing scan results are kept.

What happens if we remove a permission?

The features that depend on it stop, and the affected sources show an access error. Everything else keeps working. Run **Check Permissions** to see what is missing.

Does Data & More use delegated (signed-in user) permissions?

None of the three packages contains delegated permissions, not even `User.Read`. Delegated permissions are only used for the one-time DLP steps, for personal accounts (where a user connects their own mailbox and OneDrive), and for deleting Teams messages, which Microsoft allows only on behalf of the author.

I lost the client secret. Can I see it again?

No. Microsoft shows a client secret value only once, right after you create it. Create a new secret, update it in **Settings → App registration**, and delete the old one.

<https://support.dataandmore.com/en/knowledge/it-setup-onboarding/rights-overview>