DATA & MORE SUPPORT

Appregistrering och behörigheter

Data & More Compliance Solution (DMCS) ansluter till Microsoft 365 via en appregistrering i er Entra ID-klientorganisation. Ni kan välja mellan fyra sätt att ansluta. De skiljer sig åt i vad Data & More har tillåtelse att göra, från skrivskyddad skanning till realtidsbaserat dataskydd (DLP). Den här artikeln förklarar varje alternativ och samtliga behörigheter som begärs.

01
Demo
Skrivskyddad skanning av e-post och filer. Lämpligt för en provperiod.

02
Produktion
Fullständig skanning samt policyåtgärder för e-post, filer och Teams.

03
Produktion + DLP
Allt i Produktion samt realtids-DLP och Copilot.

04
Lägg till appregistrering
Ni skapar och hanterar er egen appregistrering.

- **Demo**: skrivskyddad skanning av e-post och filer. Lämpligt för en provperiod.
- **Produktion**: fullständig skanning samt policyåtgärder för e-post, filer och Teams.
- **Produktion + DLP**: allt i Produktion samt realtids-DLP och Copilot.
- **Lägg till appregistrering**: ni skapar och hanterar er egen appregistrering.

Hur samtycke fungerar

I Data & More, gå till **Inställningar → Appregistrering**. De fyra knapparna längst upp motsvarar de fyra alternativen: **Demo**, **Produktion**, **Produktion + DLP** och **Lägg till appregistrering**. De tre första använder en appregistrering som Data & More förvaltar: välj knappen för att få en samtyckeslänk, och en Microsoft 365-administratör godkänner behörigheterna för hela organisationen. Om ni inte själva är administratör ger samma skärm er möjlighet att skicka ett inbjudningsmejl till en administratör.

Samtliga behörigheter i de tre första alternativen är **programbehörigheter**. Data & More agerar som en tjänst, inte som en inloggad användare, vilket innebär att skanning fortsätter att fungera när medarbetare är frånvarande och att inga personliga lösenord används. Ni kan när som helst se och återkalla beviljade behörigheter i Entra-administrationscentret under **Företagsprogram**.

Skrivbehörigheter innebär inte automatisk radering. Raderingar kräver ett manuellt godkännandesteg i Data & More innan något tas bort.

Vem behöver godkänna

- **Global administratör** eller **Privilegierad rolladministratör**: godkänner appbehörigheterna (alla alternativ).
- **Exchange-administratör** (eller global administratör): det engångssteg som kallas "Bevilja Exchange-åtkomst" i Produktion + DLP.
- **Teams-administratör** (eller global administratör): det engångssteg som kallas "Installera Teams-bot" i Produktion + DLP.

Vad varje alternativ kan göra

Funktion	Demo	Produktion	Produktion + DLP	Lägg till appregistrering
Skanna Outlook-e-post	Ja	Ja	Ja	Ni väljer
Skanna OneDrive- och SharePoint-filer	Ja	Ja	Ja	Ni väljer

Skanna Teams-kanaler och chattar	Nej	**Ja**	**Ja**	Ni väljer
Identifiera kända personer från Outlook-kontakter	Nej	**Ja**	**Ja**	Ni väljer
Läs era känslighetsetiketter (Purview)	**Ja**	**Ja**	**Ja**	Ni väljer
Skicka rapporter och aviseringar via e-post	**Ja**	**Ja**	**Ja**	Ni väljer
Policyåtgärder: flytta till valv, radera, återställa, tagga, tillämpa etiketter	Nej	**Ja**	**Ja**	Ni väljer
Realtids-DLP för e-post, filer och Teams	Nej	Nej	**Ja**	Ni väljer
Copilot-frågor och svar	Nej	Nej	**Ja**	Ni väljer
Aviseringar i Teams från Data & More-boten	Nej	Nej	**Ja**	Ni väljer
Vem förvaltar appregistreringen	Data & More	Data & More	Data & More	Ni
Åtkomst till era data	Skrivskyddad	Läs och skriv	Läs och skriv	Enligt er tilldelning

Ni kan uppgradera till ett större alternativ senare. Välj det större alternativets knapp i Inställningar och godkänn igen; de extra behörigheterna läggs till i den befintliga appen.

Alternativ 1: Demo (skrivskyddad)

Den minsta uppsättningen. Data & More läser postlådor och filer för att visa var personliga och känsliga uppgifter finns, men kan inte ändra något i er klientorganisation. Använd det för en provperiod eller en inledande bedömning.

- **Täcker:** Outlook, OneDrive och SharePoint-filer.
- **Ändrar data:** nej, endast rapporter.
- **Godkännande:** global administratör, ett klick.

Behörighet	Åtkomst	Vad Data & More använder den till
`User.Read.All`	Läs	Läser listan över användare och deras grundläggande profil (namn, e-post, avdelning, chef), så att systemet vet vilkas postlådor och OneDrives som ska skannas och vem som äger de data som hittas.
`Directory.Read.All`	Läs	Läser grupper och gruppmedlemskap, organisationsnamn och verifierade domäner samt beviljade behörigheter. Används för gruppbaserad avgränsning och knappen **Kontrollera behörigheter**.
`Mail.Read`	Läs	Läser e-postmeddelanden och bilagor så att de kan skannas efter personliga och känsliga uppgifter.
`Files.Read.All`	Läs	Läser filer i OneDrive och SharePoint samt vem de delas med, så att de kan skannas.
`InformationProtectionPolicy.Read.All`	Läs	Läser era Microsoft Purview-känslighetsetiketter, så att fynd kan jämföras med hur data är märkta.
`Mail.Send`	Skicka	Skickar Data & More-rapporter och aviseringar från en postlåda ni väljer. Den läser inte eller ändrar befintlig e-post.

Alternativ 2: Produktion (läs och skriv)

För daglig användning. Data & More skannar hela Microsoft 365, inklusive Teams, och genomför de policyer ni konfigurerar: flyttar känslig e-post och känsliga filer till ett valv, raderar data som passerat sin lagringstid, återställer den, taggar den och tillämpar känslighetsetiketter. Alla behörigheter krävs.

- **Täcker:** Outlook, OneDrive, SharePoint och Teams.
- **Ändrar data:** endast när en policy ni konfigurerat anger det.
- **Godkännande:** global administratör, ett klick.

Microsoft Graph

Behörighet	Åtkomst	Vad Data & More använder den till
`User.Read.All`	Läs	Användare och grundläggande profil, licenser och foton: vars data som ska skannas och vem som äger den.
`Directory.Read.All`	Läs	Grupper och medlemskap, Teams och deras kanaler, organisationsuppgifter samt behörighetskontrollen.
`Mail.ReadWrite`	Läs och skriv	Skannar e-postmeddelanden och bilagor. Policyer kan flytta e-post till mappen `GDPRvault`, flytta tillbaka den, radera eller återställa den samt lägga till Outlook-kategorier.
`MailboxSettings.ReadWrite`	Läs och skriv	Skapar de Outlook-kategorier som används för taggning och skiljer delade postlådor från personliga.
`Mail.Send`	Skicka	Skickar rapporter och aviseringar från en postlåda ni väljer.
`Contacts.Read`	Läs	Läser Outlook-kontakter, så att externa personer som era medarbetare samarbetar med känns igen som kända personer.
`Files.ReadWrite.All`	Läs och skriv	Skannar OneDrive-, SharePoint- och Teams-filer. Policyer kan flytta filer till en valvmapp, radera eller återställa dem samt tillämpa en känslighetsetikett.
`Sites.ReadWrite.All`	Läs och skriv	Hittar SharePoint-webbplatser och dokumentbibliotek, skriver Data & More-metadata i bibliotekets kolumner och återställer filer från papperskorgen.
`Sites.FullControl.All`	Hantera	Lägger till Data & More-metadatakolumner i dokumentbibliotek när en policy kräver det.
`Team.ReadBasic.All`	Läs	Läser grundläggande information om Teams.
`ChannelMessage.Read.All`	Läs	Läser inlägg och svar i Teams-kanaler så att de kan skannas.
`Chat.Read.All`	Läs	Läser 1:1- och gruppchattar i Teams så att de kan skannas.
`InformationProtectionPolicy.Read.All`	Läs	Läser era känslighetsetiketter, så att policyer kan tillämpa dem och fynd kan jämföras med dem.

SharePoint

Dessa tre beviljas via SharePoint-API:et i stället för Microsoft Graph. De används för att läsa webbplatsgrupper och webbplatsägare, så att fynd på en webbplats tilldelas de ansvariga personerna.

Behörighet	Åtkomst	Vad Data & More använder den till
`Sites.Read.All`	Läs	Läser SharePoint-webbplatsgrupper och deras medlemmar.
`Sites.FullControl.All`	Hantera	Läser en webbplats ägargrupp.

`User.Read.All`	Läs	Matchar SharePoint-användare mot personer i er katalog.

Skanning av Exchange Online-arkivet

Online-arkivet läses via Exchange Web Services (EWS), vilket inte omfattas av något av paketen. Om ni vill skanna det, bevilja även programbehörigheten **Office 365 Exchange Online** `full_access_as_app`.

Alternativ 3: Produktion + DLP (läs och skriv)

Allt i Produktion, plus realtidsbaserat dataskydd. Microsoft 365 meddelar Data & More omedelbart när ett e-postmeddelande skickas, en fil delas eller ett Teams-meddelande publiceras. Data & More kontrollerar det mot era DLP-policyer och kan avisera, hålla kvar eller blockera det inom sekunder. Det täcker även Microsoft 365 Copilot och kan avisera användare via en Teams-bot.

- **Täcker:** Produktion, plus realtids-DLP och Copilot.
- **Ändrar data:** blockerar, håller kvar eller begränsar delning när en DLP-policy matchas.
- **Godkännande:** global administratör, plus upp till tre engångssteg.

Utöver alla Produktionsbehörigheter

Behörighet	API	Åtkomst	Vad Data & More använder den till
`AiEnterpriseInteraction.Read.All`	Microsoft Graph	Läs	Läser Microsoft 365 Copilot-frågor och svar så att de kan kontrolleras för känsliga uppgifter. Varje användare behöver en Microsoft 365 Copilot-licens.
`AuditLogsQuery.Read.All`	Microsoft Graph	Läs	Söker i granskningsloggen efter Copilot Chat- och agentaktivitet som Copilot-exporten inte inkluderar.
`AppCatalog.Read.All`	Microsoft Graph	Läs	Hittar Data & More DLP-boten i er Teams-appkatalog.
`TeamsAppInstallation.ReadWriteForUser.All`	Microsoft Graph	Installera	Installerar Data & More DLP-boten för berörda användare, så att den kan skicka aviseringar i en 1:1-chatt.
`TeamsAppInstallation.ReadWriteForTeam.All`	Microsoft Graph	Installera	Installerar boten i Teams där kanalaviseringar behövs.
`Exchange.ManageAsApp`	Office 365 Exchange Online	Hantera	Skapar och underhåller de e-postflödesregler som håller kvar utgående e-post till externa mottagare tills den har kontrollerats. Data & More hanterar endast sina egna regler.

Engångssteg vid konfiguration

Vissa åtgärder kan inte beviljas som programbehörigheter. Ni utför dem en gång från DLP-sidan, inloggad som administratör.

Steg	Vem loggar in	Vad det beviljar
Bevilja Exchange-åtkomst	Exchange-administratör eller global administratör	Loggar in med den delegerade behörigheten `Exchange.Manage` och registrerar Data & More i Exchange Online med två Exchange-roller: **Transportregler** (hantera e-postflödesregler) och **Skrivskyddad konfiguration** (läsa godkända domäner, så att intern e-post inte hålls kvar).
Installera Teams-bot	Teams-administratör eller global administratör	Använder den delegerade behörigheten `AppCatalog.ReadWrite.All` en gång för att publicera Data & More DLP-boten i organisationens Teams-appkatalog.

Tillåt radering av Teams-meddelanden (valfritt)	Global administratör, eller varje meddelandeförfattare	Microsoft tillåter endast att ett Teams-meddelande raderas på uppdrag av dess författare. Genom att godkänna de delegerade behörigheterna `ChannelMessage.ReadWrite` och `Chat.ReadWrite` för organisationen kan DLP ta bort ett blockerat meddelande utan att tillfråga varje författare.

Copilot DLP är endast för aviseringar: Data & More kan avisera om en riskfylld Copilot-konversation men ändrar den inte.

Alternativ 4: Lägg till appregistrering (er egen app)

Vissa organisationer föredrar att skapa appregistreringen i sin egen klientorganisation, så att de äger autentiseringsuppgifterna och själva bestämmer exakt vilka behörigheter som ska beviljas. Data & More använder då den appen i stället för sin egen. Bevilja endast vad de källor och funktioner ni planerar att använda kräver; tabellen i slutet av det här avsnittet anger minimiuppsättningen för var och en.

1. Registrera appen

1. Logga in på **portal.azure.com** som global administratör.
2. Sök efter **Appregistreringar** och välj **Ny registrering**.
3. Ange ett namn (till exempel *Data & More DMCS*) och välj **Konton i den här organisationskatalogen endast**.
4. Under **Omdirigerings-URI**, välj **Webb** och ange `https://signup.dataandmore.com/api/authorized`.
5. Välj **Registrera**.
6. Öppna **Autentisering** och lägg till ytterligare två **Webb**-omdirigerings-URI:er: `https://signup.dataandmore.com/api/authorize_redirect` och er Data & More-serveradress följt av `/api/auth/ad/login/authorized`. Om er server är `https://gdpr.dataandmore.com`, blir det `https://gdpr.dataandmore.com/api/auth/ad/login/authorized`. Välj **Spara**.

Lägg alltid till båda `signup.dataandmore.com`-adresserna, oavsett vilket paket ni använder. De krävs för samtyckes- och inloggningsstegen.

2. Lägg till API-behörigheter

1. Öppna **API-behörigheter** och välj **Lägg till en behörighet → Microsoft Graph → Programbehörigheter**. Lägg till Graph-behörigheterna för ert paket (Demo, Produktion eller Produktion + DLP ovan), eller minimiuppsättningen för de funktioner ni vill ha från tabellen nedan.
2. **SharePoint** (Produktion och Produktion + DLP): välj **Lägg till en behörighet** igen, öppna **API:er som min organisation använder**, sök efter **SharePoint**, och lägg till de tre SharePoint-programbehörigheterna.
3. **Exchange** (Produktion + DLP, eller Online-arkiv): välj **Lägg till en behörighet → API:er som min organisation använder**, sök efter **Office 365 Exchange Online**, och lägg till `Exchange.ManageAsApp` (DLP) och/eller `full_access_as_app` (Online-arkiv).
4. Välj **Bevilja administratörsmedgivande** och bekräfta. Varje behörighet bör nu visa statusen **Beviljad** i grönt.

3. Skapa autentiseringsuppgifter

1. På appens **Översikt**-sida, notera **Program-ID (klient)** och **Katalog-ID (klient)**.
2. Öppna **Certifikat och hemligheter → Ny klienthemlighet**, lägg till en beskrivning och ett utgångsdatum, och välj **Lägg till**.
3. Kopiera hemlighetens **Värde** omedelbart. Det visas bara en gång, och ni behöver värdet, inte hemlighetens ID. Alternativt kan ni ladda upp ett certifikat; ett certifikat krävs för att läsa SharePoint-webbplatsgrupper och ägare.

4. Anslut det till Data & More

1. I Data & More, öppna **Inställningar → Appregistrering → Lägg till appregistrering** och ange klient-ID, app-ID och hemlighetsvärdet eller certifikatet. Om ni inte kan göra detta själva, skicka de tre värdena till **support@dataandmore.com** via en säker kanal.

2. Välj **Kontrollera behörigheter**. Data & More listar vilka behörigheter den hittat, markerar eventuella som saknas och visar när hemligheten eller certifikatet går ut.

Minimibehörigheter per funktion

Funktion	Skanning (läs)	Policyåtgärder (skriv)
Alltid nödvändigt	`User.Read.All`, `GroupMember.Read.All`, `Organization.Read.All`, `Application.Read.All`	Ingen
Outlook	`Mail.Read`, `MailboxSettings.Read`	`Mail.ReadWrite`, `MailboxSettings.ReadWrite`
Exchange Online-arkiv	Exchange: `full_access_as_app`	Exchange: `full_access_as_app`
OneDrive	`Files.Read.All`	`Files.ReadWrite.All`, `Sites.ReadWrite.All`, `Sites.Manage.All`
SharePoint	`Sites.Read.All`, `Files.Read.All`; SharePoint: `Sites.Read.All` (certifikat)	`Files.ReadWrite.All`, `Sites.ReadWrite.All`, `Sites.Manage.All`
Teams-kanaler	`Channel.ReadBasic.All`, `ChannelMessage.Read.All`, `Files.Read.All`	`Files.ReadWrite.All`
Teams-chattar	`Chat.Read.All`	Ingen
Kända personer	`Contacts.Read`	Ingen
Känslighetsetiketter	`InformationProtectionPolicy.Read.All`	`Files.ReadWrite.All` (för att tillämpa)
Rapporter via e-post	Ingen	`Mail.Send`
Copilot	`AiEnterpriseInteraction.Read.All`, `AuditLogsQuery.Read.All`	Ingen
Realtids-DLP	Skanbehörigheterna för varje källa ni skyddar	Exchange: `Exchange.ManageAsApp`; Graph: `Mail.ReadWrite`, `Mail.Send`, `Files.ReadWrite.All`, `AppCatalog.Read.All`, `TeamsAppInstallation.ReadWriteSelfForUser.All`, `TeamsAppInstallation.ReadWriteSelfForTeam.All`; samt engångsstegen under Produktion + DLP

> **Tänk på:** ni ansvarar för att förnya hemligheten eller certifikatet innan det går ut; vyn **Kontrollera behörigheter** visar utgångsdatumet. Om en behörighet saknas visar den berörda källan ett åtkomstfel i stället för att misslyckas tyst. Lägg till behörigheten, bevilja administratörsmedgivande igen och kör **Kontrollera behörigheter**.

Begränsa vad Data & More kan nå

Programbehörigheter gäller för hela klientorganisationen. Om ni vill begränsa dem erbjuder Microsoft följande kontroller, och Data & More fungerar med alla:

- **Avgränsning i Data & More.** Välj vilka användare, grupper, webbplatser och Teams som varje källa täcker. Ingenting utanför avgränsningen skannas eller ändras.
- **Exchange-programåtkomstpolicy eller RBAC för program.** Begränsa `Mail.Send` och postlådeåtkomst till en e-postaktiverad säkerhetsgrupp.
- **Granskning.** Varje anrop som Data & More gör visas i era Entra-inloggningsloggar och Microsoft 365-granskningsloggen under appens namn.

Vanliga frågor

Kan Data & More läsa mina användares lösenord?

Nej. Ingen av dessa behörigheter ger åtkomst till lösenord eller inloggningsuppgifter. Data & More autentiserar sig som sin egen app, med sin egen hemlighet eller sitt eget certifikat.

Varför behöver en i huvudsak läsande produkt skrivbehörigheter?

Skrivåtkomst används endast när en policy ni konfigurerat instruerar Data & More att agera, till exempel för att flytta en känslig fil till ett valv eller radera e-post som passerat sin lagringstid. Raderingar kräver även ett manuellt godkännandesteg. Om ni endast vill ha rapporter, välj Demo eller bevilja enbart läsbehörigheter i er egen app.

Kan vi börja med Demo och uppgradera senare?

Ja. Välj **Produktion** eller **Produktion + DLP** i **Inställningar → Appregistrering** och godkänn igen. Era befintliga skanningsresultat bevaras.

Vad händer om vi tar bort en behörighet?

De funktioner som är beroende av den slutar fungera, och de berörda källorna visar ett åtkomstfel. Allt annat fortsätter att fungera. Kör **Kontrollera behörigheter** för att se vad som saknas.

Använder Data & More delegerade behörigheter (inloggad användare)?

Inget av de tre paketen innehåller delegerade behörigheter, inte ens `User.Read`. Delegerade behörigheter används endast för engångsstegen i DLP, för personliga konton (där en användare ansluter sin egen postlåda och OneDrive) samt för radering av Teams-meddelanden, vilket Microsoft endast tillåter på uppdrag av författaren.

Jag har tappat bort klienthemligheten. Kan jag se den igen?

Nej. Microsoft visar ett klienthemlighetsvärde endast en gång, direkt efter att ni skapat det. Skapa en ny hemlighet, uppdatera den i **Inställningar → Appregistrering**, och radera den gamla.
