DATA & MORE SUPPORT

Anwendungsregistrierung und Berechtigungen

Die Data & More Compliance Solution (DMCS) stellt über eine App-Registrierung in Ihrem Entra ID-Mandanten eine Verbindung zu Microsoft 365 her. Sie können zwischen vier Verbindungsmethoden wählen. Diese unterscheiden sich darin, was Data & More ausführen darf – von reinen Lesescans bis hin zur Echtzeit-Datenverlustprävention. In diesem Artikel werden die einzelnen Optionen und alle darin enthaltenen Berechtigungen erläutert.

01
Demo
Nur-Lese-Scan von E-Mails und Dateien. Geeignet für einen Testbetrieb.

02
Production
Vollständiger Scan sowie Richtlinienaktionen für E-Mails, Dateien und Teams.

03
Production + DLP
Alles aus Production, zusätzlich Echtzeit-DLP und Copilot.

04
Add App Registration
Sie erstellen und verwalten Ihre eigene App-Registrierung.

- **Demo**: Nur-Lese-Scan von E-Mails und Dateien. Geeignet für einen Testbetrieb.
- **Production**: Vollständiger Scan sowie Richtlinienaktionen für E-Mails, Dateien und Teams.
- **Production + DLP**: Alles aus Production, zusätzlich Echtzeit-DLP und Copilot.
- **Add App Registration**: Sie erstellen und verwalten Ihre eigene App-Registrierung.

Wie die Zustimmung funktioniert

Wechseln Sie in Data & More zu**Einstellungen → App-Registrierung**. Die vier Schaltflächen oben entsprechen den vier Optionen:**Demo**,**Production**,**Production + DLP**und**Add App Registration**. Die ersten drei Optionen nutzen eine von Data & More verwaltete App-Registrierung: Wählen Sie die entsprechende Schaltfläche, um einen Zustimmungslink zu erhalten. Ein Microsoft 365-Administrator genehmigt anschließend die Berechtigungen für Ihre gesamte Organisation. Falls Sie selbst kein Administrator sind, können Sie über denselben Bildschirm eine Einladungs-E-Mail an einen Administrator versenden.

Alle Berechtigungen in den ersten drei Optionen sind**Anwendungsberechtigungen**. Data & More agiert als Dienst und nicht als angemeldeter Benutzer. Der Scan läuft daher auch dann weiter, wenn Mitarbeitende abwesend sind, und es ist kein persönliches Passwort beteiligt. Die erteilten Berechtigungen können Sie jederzeit im Entra Admin Center unter**Unternehmensanwendungen**einsehen und widerrufen.

Schreibberechtigungen bedeuten keine automatische Löschung. Löschvorgänge durchlaufen in Data & More immer einen manuellen Freigabeschritt, bevor Daten entfernt werden.

Wer die Genehmigung erteilen muss

- **Globaler Administrator**oder**Administrator für privilegierte Rollen**: Genehmigt die App-Berechtigungen (alle Optionen).
- **Exchange-Administrator**(oder Globaler Administrator): Der einmalige Schritt „Exchange-Zugriff erteilen" in Production + DLP.
- **Teams-Administrator**(oder Globaler Administrator): Der einmalige Schritt „Teams-Bot installieren" in Production + DLP.

Was die einzelnen Optionen leisten können

Funktion	Demo	Production	Production + DLP	Add App Registration
Outlook-E-Mails scannen	Ja	Ja	Ja	Ihre Wahl
OneDrive- und SharePoint-Dateien scannen	Ja	Ja	Ja	Ihre Wahl
Teams-Kanäle und Chats scannen	Nein	Ja	Ja	Ihre Wahl
Bekannte Personen aus Outlook-Kontakten erkennen	Nein	Ja	Ja	Ihre Wahl
Ihre Vertraulichkeitsbezeichnungen lesen (Purview)	Ja	Ja	Ja	Ihre Wahl
Berichte und Benachrichtigungen per E-Mail versenden	Ja	Ja	Ja	Ihre Wahl
Richtlinienaktionen: In Tresor verschieben, löschen, wiederherstellen, kennzeichnen, Bezeichnungen anwenden	Nein	Ja	Ja	Ihre Wahl
Echtzeit-DLP für E-Mails, Dateien und Teams	Nein	Nein	Ja	Ihre Wahl
Copilot-Eingabeaufforderungen und -Antworten	Nein	Nein	Ja	Ihre Wahl
Benachrichtigungen in Teams vom Data & More-Bot	Nein	Nein	Ja	Ihre Wahl
Wer die App-Registrierung verwaltet	Data & More	Data & More	Data & More	Sie
Zugriff auf Ihre Daten	Nur Lesezugriff	Lesen und Schreiben	Lesen und Schreiben	Nach Ihrer Vorgabe

Sie können jederzeit auf eine umfangreichere Option wechseln. Wählen Sie dazu die Schaltfläche der gewünschten Option in den Einstellungen und genehmigen Sie erneut. Die zusätzlichen Berechtigungen werden der bestehenden App hinzugefügt.

Option 1: Demo (nur Lesezugriff)

Der kleinste Umfang. Data & More liest Postfächer und Dateien, um Ihnen zu zeigen, wo sich personenbezogene und vertrauliche Daten befinden. Es können jedoch keine Änderungen in Ihrem Mandanten vorgenommen werden. Verwenden Sie diese Option für einen Testbetrieb oder eine erste Bestandsaufnahme.

- **Abgedeckt:**Outlook, OneDrive und SharePoint-Dateien.
- **Daten werden geändert:**Nein, nur Berichte.
- **Genehmigung:**Globaler Administrator, ein Klick.

Berechtigung	Zugriff	Wofür Data & More sie verwendet

`User.Read.All`	Lesen	Liest die Benutzerliste und das grundlegende Profil (Name, E-Mail, Abteilung, Vorgesetzte/r), um zu ermitteln, wessen Postfächer und OneDrives gescannt werden sollen und wem die gefundenen Daten gehören.
`Directory.Read.All`	Lesen	Liest Gruppen und Gruppenmitgliedschaften, Ihren Organisationsnamen und verifizierte Domänen sowie erteilte Berechtigungen. Wird für gruppenbasierte Einschränkungen und die Schaltfläche**Berechtigungen prüfen**verwendet.
`Mail.Read`	Lesen	Liest E-Mails und Anhänge, damit diese auf personenbezogene und vertrauliche Daten gescannt werden können.
`Files.Read.All`	Lesen	Liest Dateien in OneDrive und SharePoint sowie deren Freigabeeinstellungen, damit sie gescannt werden können.
`InformationProtectionPolicy.Read.All`	Lesen	Liest Ihre Microsoft Purview-Vertraulichkeitsbezeichnungen, damit Ergebnisse mit der Datenkennzeichnung verglichen werden können.
`Mail.Send`	Senden	Sendet Data & More-Berichte und -Benachrichtigungen aus einem von Ihnen gewählten Postfach. Es werden keine vorhandenen E-Mails gelesen oder geändert.

Option 2: Production (Lesen und Schreiben)

Für den täglichen Betrieb. Data & More scannt Microsoft 365 vollständig, einschließlich Teams, und führt die von Ihnen konfigurierten Richtlinien aus: Vertrauliche E-Mails und Dateien werden in einen Tresor verschoben, Daten nach Ablauf der Aufbewahrungsfrist gelöscht, wiederhergestellt, gekennzeichnet und mit Vertraulichkeitsbezeichnungen versehen. Alle Berechtigungen sind erforderlich.

- **Abgedeckt:**Outlook, OneDrive, SharePoint und Teams.
- **Daten werden geändert:**Nur wenn eine von Ihnen konfigurierte Richtlinie dies vorgibt.
- **Genehmigung:**Globaler Administrator, ein Klick.

Microsoft Graph

Berechtigung	Zugriff	Wofür Data & More sie verwendet
`User.Read.All`	Lesen	Benutzer und grundlegendes Profil, Lizenzen und Fotos: wessen Daten gescannt werden und wem sie gehören.
`Directory.Read.All`	Lesen	Gruppen und Mitgliedschaften, Teams und deren Kanäle, Organisationsdetails sowie die Berechtigungsprüfung.
`Mail.ReadWrite`	Lesen und Schreiben	Scannt E-Mails und Anhänge. Richtlinien können E-Mails in den Ordner `GDPRvault` verschieben, zurückverschieben, löschen oder wiederherstellen sowie Outlook-Kategorien hinzufügen.
`MailboxSettings.ReadWrite`	Lesen und Schreiben	Erstellt die für die Kennzeichnung verwendeten Outlook-Kategorien und unterscheidet freigegebene Postfächer von persönlichen.
`Mail.Send`	Senden	Sendet Berichte und Benachrichtigungen aus einem von Ihnen gewählten Postfach.
`Contacts.Read`	Lesen	Liest Outlook-Kontakte, damit externe Personen, mit denen Ihre Mitarbeitenden zusammenarbeiten, als bekannte Personen erkannt werden.
`Files.ReadWrite.All`	Lesen und Schreiben	Scannt OneDrive-, SharePoint- und Teams-Dateien. Richtlinien können Dateien in einen Tresorordner verschieben, löschen oder wiederherstellen sowie eine Vertraulichkeitsbezeichnung anwenden.
`Sites.ReadWrite.All`	Lesen und Schreiben	Findet SharePoint-Websites und Dokumentbibliotheken, schreibt Data & More-Metadaten in Bibliotheksspalten und stellt Dateien aus dem Papierkorb wieder her.
`Sites.FullControl.All`	Verwalten	Fügt Dokumentbibliotheken die Data & More-Metadatenspalten hinzu, wenn eine Richtlinie diese benötigt.
`Team.ReadBasic.All`	Lesen	Liest grundlegende Informationen zu Teams.
`ChannelMessage.Read.All`	Lesen	Liest Beiträge und Antworten in Teams-Kanälen, damit diese gescannt werden können.
`Chat.Read.All`	Lesen	Liest 1:1- und Gruppenchats in Teams, damit diese gescannt werden können.
`InformationProtectionPolicy.Read.All`	Lesen	Liest Ihre Vertraulichkeitsbezeichnungen, damit Richtlinien diese anwenden und Ergebnisse damit verglichen werden können.

SharePoint

Diese drei Berechtigungen werden über die SharePoint-API und nicht über Microsoft Graph erteilt. Sie werden verwendet, um Websitegruppen und Websitebesitzer zu lesen, damit Ergebnisse zu einer Website den verantwortlichen Personen zugeordnet werden können.

Berechtigung	Zugriff	Wofür Data & More sie verwendet
`Sites.Read.All`	Lesen	Liest SharePoint-Websitegruppen und deren Mitglieder.
`Sites.FullControl.All`	Verwalten	Liest die Besitzergruppe einer Website.
`User.Read.All`	Lesen	Ordnet SharePoint-Benutzende Personen in Ihrem Verzeichnis zu.

Scannen des Exchange Online-Archivs

Das Online-Archiv wird über Exchange Web Services (EWS) ausgelesen, das von keinem der Pakete abgedeckt wird. Wenn Sie es scannen möchten, erteilen Sie zusätzlich die Anwendungsberechtigung**Office 365 Exchange Online**mit der Berechtigung `full_access_as_app` .

Option 3: Production + DLP (Lesen und Schreiben)

Alles aus Production, zusätzlich Echtzeit-Datenverlustprävention. Microsoft 365 benachrichtigt Data & More sofort, wenn eine E-Mail gesendet, eine Datei freigegeben oder eine Teams-Nachricht gepostet wird. Data & More prüft diese innerhalb von Sekunden anhand Ihrer DLP-Richtlinien und kann Benachrichtigungen senden, Inhalte zurückhalten oder blockieren. Außerdem werden Microsoft 365 Copilot abgedeckt und Benutzende über einen Teams-Bot benachrichtigt.

- **Abgedeckt:**Production, zusätzlich Echtzeit-DLP und Copilot.
- **Daten werden geändert:**Blockiert, hält zurück oder schränkt die Freigabe ein, wenn eine DLP-Richtlinie greift.
- **Genehmigung:**Globaler Administrator, plus bis zu drei einmalige Schritte.

Zusätzlich zu allen Production-Berechtigungen

Berechtigung	API	Zugriff	Wofür Data & More sie verwendet
`AiEnterpriseInteraction.Read.All`	Microsoft Graph	Lesen	Liest Microsoft 365 Copilot-Eingabeaufforderungen und -Antworten, damit diese auf vertrauliche Daten geprüft werden können. Jede Benutzerin und jeder Benutzer benötigt eine Microsoft 365 Copilot-Lizenz.
`AuditLogsQuery.Read.All`	Microsoft Graph	Lesen	Durchsucht das Überwachungsprotokoll nach Copilot Chat- und Agent-Aktivitäten, die der Copilot-Export nicht enthält.
`AppCatalog.Read.All`	Microsoft Graph	Lesen	Findet den Data & More-DLP-Bot in Ihrem Teams-App-Katalog.
`TeamsAppInstallation.ReadWriteForUser.All`	Microsoft Graph	Installieren	Installiert den Data & More-DLP-Bot für betroffene Benutzende, damit dieser ihnen Benachrichtigungen in einem 1:1-Chat senden kann.
`TeamsAppInstallation.ReadWriteForTeam.All`	Microsoft Graph	Installieren	Installiert den Bot in Teams, wo Kanalbenachrichtigungen erforderlich sind.
`Exchange.ManageAsApp`	Office 365 Exchange Online	Verwalten	Erstellt und verwaltet die E-Mail-Flussregeln, die ausgehende E-Mails an externe Empfänger zurückhalten, bis diese geprüft wurden. Data & More verwaltet ausschließlich eigene Regeln.

Einmalige Einrichtungsschritte

Einige Aktionen können nicht als App-Berechtigungen erteilt werden. Diese werden einmalig von der DLP-Seite aus durchgeführt, während Sie als Administrator angemeldet sind.

Schritt	Wer sich anmeldet	Was erteilt wird
Exchange-Zugriff erteilen	Exchange-Administrator oder Globaler Administrator	Meldet sich mit der delegierten Berechtigung `Exchange.Manage` an und registriert Data & More in Exchange Online mit zwei Exchange-Rollen: **Transportregeln** (zur Verwaltung der eigenen E-Mail-Flussregeln) und **Schreibgeschützte Konfiguration** (zum Lesen Ihrer akzeptierten Domänen, damit interne E-Mails nicht zurückgehalten werden).
Teams-Bot installieren	Teams-Administrator oder Globaler Administrator	Verwendet die delegierte Berechtigung `AppCatalog.ReadWrite.All` einmalig, um den Data & More-DLP-Bot im Teams-App-Katalog Ihrer Organisation zu veröffentlichen.
Teams-Nachrichtenlöschung erlauben (optional)	Globaler Administrator oder jede/r Nachrichtenautor/in einzeln	Microsoft erlaubt das Löschen einer Teams-Nachricht nur im Namen ihres Autors bzw. ihrer Autorin. Durch die Genehmigung der delegierten Berechtigungen `ChannelMessage.ReadWrite` und `Chat.ReadWrite` für die Organisation kann DLP eine blockierte Nachricht entfernen, ohne jede/n Autor/in einzeln zu fragen.

Copilot-DLP ist nur auf Benachrichtigungen beschränkt: Data & More kann über ein riskantes Copilot-Gespräch informieren, nimmt jedoch keine Änderungen daran vor.

Option 4: Add App Registration (eigene App)

Einige Organisationen bevorzugen es, die App-Registrierung in ihrem eigenen Mandanten zu erstellen, um die Anmeldeinformationen selbst zu verwalten und genau festzulegen, welche Berechtigungen erteilt werden. Data & More verwendet dann diese App anstelle der eigenen. Erteilen Sie nur die Berechtigungen, die für die von Ihnen geplanten Quellen und Funktionen erforderlich sind. Die nachstehende Tabelle enthält die jeweiligen Mindestanforderungen.

1. App registrieren

1. Melden Sie sich bei **portal.azure.com** als Globaler Administrator an.
2. Suchen Sie nach **App-Registrierungen** und wählen Sie **Neue Registrierung**.
3. Geben Sie einen Namen ein (z. B. *Data & More DMCS*) und wählen Sie **Nur Konten in diesem Organisationsverzeichnis**.
4. Wählen Sie unter **Umleitungs-URI** die Option **Web** und geben Sie `https://signup.dataandmore.com/api/authorized` ein.
5. Wählen Sie **Registrieren**.
6. Öffnen Sie **Authentifizierung** und fügen Sie zwei weitere **Web**-Umleitungs-URIs hinzu: `https://signup.dataandmore.com/api/authorize_redirect` sowie Ihre Data & More-Serveradresse gefolgt von `/api/auth/ad/login/authorized`. Wenn Ihr Server `https://gdpr.dataandmore.com` ist, lautet die URI `https://gdpr.dataandmore.com/api/auth/ad/login/authorized`. Wählen Sie **Speichern**.

Fügen Sie immer beide `signup.dataandmore.com`-Adressen hinzu, unabhängig vom gewählten Paket. Diese werden für die Zustimmungs- und Anmeldeschritte benötigt.

2. API-Berechtigungen hinzufügen

1. Öffnen Sie **API-Berechtigungen** und wählen Sie **Berechtigung hinzufügen → Microsoft Graph → Anwendungsberechtigungen**. Fügen Sie die Graph-Berechtigungen für Ihr Paket (Demo, Production oder Production + DLP, siehe oben) oder die Mindestberechtigungen für die gewünschten Funktionen aus der nachstehenden Tabelle hinzu.
2. **SharePoint** (Production und Production + DLP): Wählen Sie erneut **Berechtigung hinzufügen**, öffnen Sie **Von meiner Organisation verwendete APIs**, suchen Sie nach **SharePoint** und fügen Sie die drei SharePoint-Anwendungsberechtigungen hinzu.
3. **Exchange** (Production + DLP oder Online-Archiv): Wählen Sie **Berechtigung hinzufügen → Von meiner Organisation verwendete APIs**, suchen Sie nach **Office 365 Exchange Online** und fügen Sie `Exchange.ManageAsApp` (DLP) und/oder `full_access_as_app` (Online-Archiv) hinzu.
4. Wählen Sie **Administratorzustimmung erteilen** und bestätigen Sie. Jede Berechtigung sollte nun den grünen Status **Erteilt** anzeigen.

3. Anmeldeinformationen erstellen

1. Notieren Sie sich auf der **Übersichtsseite** der App die **Anwendungs-ID (Client-ID)** und die **Verzeichnis-ID (Mandanten-ID)**.
2. Öffnen Sie **Zertifikate & Geheimnisse → Neuer geheimer Clientschlüssel**, geben Sie eine Beschreibung und ein Ablaufdatum ein und wählen Sie **Hinzufügen**.
3. Kopieren Sie den **Wert** des Geheimnisses sofort. Er wird nur einmal angezeigt, und Sie benötigen den Wert, nicht die Geheimnis-ID. Alternativ können Sie ein Zertifikat hochladen. Ein Zertifikat ist erforderlich, um SharePoint-Websitegruppen und -besitzer zu lesen.

4. Mit Data & More verbinden

1. Öffnen Sie in Data & More **Einstellungen → App-Registrierung → Add App Registration** und geben Sie die Mandanten-ID, die Client-ID sowie den geheimen Schlüssel oder das Zertifikat ein. Falls Sie dies nicht selbst durchführen können, übermitteln Sie die drei Werte über einen sicheren Kanal an **support@dataandmore.com**.
2. Wählen Sie **Berechtigungen prüfen**. Data & More listet die gefundenen Berechtigungen auf, kennzeichnet fehlende und zeigt an, wann der geheime Schlüssel oder das Zertifikat abläuft.

Mindestberechtigungen je Funktion

Funktion	Scan (Lesen)	Richtlinienaktionen (Schreiben)
Immer erforderlich	`User.Read.All`, `GroupMember.Read.All`, `Organization.Read.All`, `Application.Read.All`	Keine

Outlook	`Mail.Read` , `MailboxSettings.Read`	`Mail.ReadWrite` , `MailboxSettings.ReadWrite`
Exchange Online-Archiv	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` (Zertifikat)	`Files.ReadWrite.All` , `Sites.ReadWrite.All` , `Sites.Manage.All`
Teams-Kanäle	`Channel.ReadBasic.All` , `ChannelMessage.Read.All` , `Files.Read.All`	`Files.ReadWrite.All`
Teams-Chats	`Chat.Read.All`	Keine
Bekannte Personen	`Contacts.Read`	Keine
Vertraulichkeitsbezeichnungen	`InformationProtectionPolicy.Read.All`	`Files.ReadWrite.All` (zum Anwenden)
Berichte per E-Mail	Keine	`Mail.Send`
Copilot	`AiEnterpriseInteraction.Read.All` , `AuditLogsQuery.Read.All`	Keine
Echtzeit-DLP	Die Scan-Berechtigungen für jede zu schützende Quelle	Exchange: `Exchange.ManageAsApp` ; Graph: `Mail.ReadWrite` , `Mail.Send` , `Files.ReadWrite.All` , `AppCatalog.Read.All` , `Tea` sowie die einmaligen Schritte unter Production + DLP

> **Bitte beachten Sie:**Sie sind dafür verantwortlich, den geheimen Schlüssel oder das Zertifikat vor dem Ablauf zu erneuern. Das Ablaufdatum wird in der Ansicht**Berechtigungen prüfen**angezeigt. Fehlt eine Berechtigung, zeigt die betroffene Quelle einen Zugriffsfehler an, anstatt stumm zu scheitern. Fügen Sie die Berechtigung hinzu, erteilen Sie die Administratorzustimmung erneut und führen Sie**Berechtigungen prüfen**aus.

Den Zugriff von Data & More einschränken

Anwendungsberechtigungen gelten für den gesamten Mandanten. Wenn Sie den Zugriff eingrenzen möchten, bietet Microsoft die folgenden Steuerungsmöglichkeiten, mit denen Data & More vollständig kompatibel ist:

- **Einschränkung in Data & More.**Wählen Sie aus, welche Benutzenden, Gruppen, Websites und Teams von der jeweiligen Quelle erfasst werden. Inhalte außerhalb des definierten Bereichs werden weder gescannt noch geändert.
- **Exchange-Anwendungszugriffsrichtlinie oder RBAC für Anwendungen.**Schränken Sie`Mail.Send`und den Postfachzugriff auf eine E-Mail-aktivierte Sicherheitsgruppe ein.
- **Überwachung.**Jeder Aufruf, den Data & More ausführt, erscheint in Ihren Entra-Anmeldeprotokollen und im Microsoft 365-Überwachungsprotokoll unter dem Namen der App.

Häufig gestellte Fragen

Kann Data & More die Passwörter meiner Benutzenden lesen?

Nein. Keine dieser Berechtigungen gewährt Zugriff auf Passwörter oder Anmeldedaten. Data & More authentifiziert sich als eigene App mit einem eigenen geheimen Schlüssel oder Zertifikat.

Warum benötigt ein hauptsächlich lesendes Produkt Schreibberechtigungen?

Schreibzugriff wird nur dann verwendet, wenn eine von Ihnen konfigurierte Richtlinie Data & More zur Aktion veranlasst – beispielsweise um eine vertrauliche Datei in einen Tresor zu verschieben oder eine E-Mail nach Ablauf der Aufbewahrungsfrist zu löschen. Löschvorgänge durchlaufen zudem einen manuellen Freigabeschritt. Wenn Sie nur Berichte benötigen, wählen Sie Demo oder erteilen Sie in Ihrer eigenen App ausschließlich Leseberechtigungen.

Können wir mit Demo starten und später upgraden?

Ja. Wählen Sie in**Einstellungen → App-Registrierung**die Option**Production**oder**Production + DLP**und genehmigen Sie erneut. Ihre vorhandenen Scan-Ergebnisse bleiben erhalten.

Was passiert, wenn wir eine Berechtigung entfernen?

Die davon abhängigen Funktionen werden deaktiviert, und die betroffenen Quellen zeigen einen Zugriffsfehler an. Alle anderen Funktionen bleiben weiterhin verfügbar. Führen Sie**Berechtigungen prüfen**aus, um festzustellen, was fehlt.

Verwendet Data & More delegierte Berechtigungen (angemeldete Benutzende)?

Keines der drei Pakete enthält delegierte Berechtigungen, nicht einmal`User.Read` . Delegierte Berechtigungen werden nur für die einmaligen DLP-Schritte, für persönliche Konten (bei denen Benutzende ihr eigenes Postfach und ihren eigenen OneDrive verbinden) sowie für das Löschen von Teams-Nachrichten verwendet, das Microsoft nur im Namen der jeweiligen Autorin oder des jeweiligen Autors erlaubt.

Ich habe den geheimen Clientschlüssel verloren. Kann ich ihn erneut einsehen?

Nein. Microsoft zeigt den Wert eines geheimen Clientschlüssels nur einmal an, direkt nach dessen Erstellung. Erstellen Sie einen neuen geheimen Schlüssel, aktualisieren Sie ihn unter**Einstellungen → App-Registrierung**und löschen Sie den alten.