

ChannelCRM App Registration API Permissions

Customer IT overview for Microsoft 365 admin consent and tenant app provisioning

Purpose

This document describes the Microsoft 365 API permissions requested by the ChannelCRM app registration created by the CCRM App Creator.

The app registration is created in the customer's Microsoft Entra ID tenant and is used by ChannelCRM to synchronize Microsoft 365 mailbox data such as users, mail, calendar appointments, contacts, and mailbox settings.

Summary for IT

Item	Value
App registration display name	ChannelCRM
Sign-in audience	Single tenant, only the customer's own Microsoft Entra ID tenant
Permission model	Application permissions, also known as app-only permissions
Admin consent required	Yes
Access pattern	Background synchronization without an interactive signed-in user
Mail sending	Not requested through Microsoft Graph by the current implementation

Application permissions allow the application to access Microsoft 365 data as the application itself. They are not limited to the mailbox of a signed-in user unless the customer's Microsoft 365 administrator applies additional scoping, such as Exchange Online RBAC for Applications or Application Access Policies where supported.

Permissions Requested for the Customer App

API	Permission	Type	Admin consent	What it allows	Why ChannelCRM needs it
Microsoft Graph	User.Read.All	Application	Yes	Read user profiles in the tenant without a signed-in user.	Match ChannelCRM users with Microsoft 365 users and mailboxes.
Microsoft Graph	Mail.ReadWrite	Application	Yes	Read, create, update, and delete mail in mailboxes without a signed-in user. It does not grant permission to send mail.	Synchronize email data between Exchange Online and ChannelCRM.

API	Permission	Type	Admin consent	What it allows	Why ChannelCRM needs it
Microsoft Graph	Calendars.ReadWrite	Application	Yes	Read, create, update, and delete calendar events without a signed-in user.	Synchronize appointments and meetings between Outlook calendars and ChannelCRM activities.
Microsoft Graph	Contacts.ReadWrite	Application	Yes	Read, create, update, and delete contacts in mailboxes without a signed-in user.	Synchronize contacts between Exchange Online and ChannelCRM.
Microsoft Graph	MailboxSettings.Read	Application	Yes	Read mailbox settings without a signed-in user. It does not grant permission to send mail.	Read mailbox configuration such as time zone, which is required for correct calendar synchronization.
Office 365 Exchange Online	full_access_as_app	Application role	Yes	Allows EWS app-only access with full access to mailboxes.	Supports Exchange Web Services access for Exchange/Outlook synchronization scenarios still handled through EWS.

Microsoft API Resource IDs

API	Microsoft resource application ID
Microsoft Graph	00000003-0000-0000-c000-000000000000
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000

Security and Scope Notes

These permissions are tenant-wide application permissions by default. That means they can apply across all relevant mailboxes in the tenant unless the customer configures additional Microsoft 365 scoping controls.

Recommended IT review points:

- Confirm that the app registration is named ChannelCRM.
- Confirm that the listed permissions are expected before granting admin consent.
- Consider scoping mailbox access if only selected users should be synchronized.
- Review the created client secret according to the customer's normal secret rotation policy.
- Remove the app registration or revoke consent if ChannelCRM synchronization is no longer required.

Provisioning Flow

- 1 Creates or recreates the customer tenant app registration named ChannelCRM.
- 2 Adds the required API permissions listed above.
- 3 Creates a client secret for the app registration.
- 4 Stores the app ID, tenant ID, and generated secret in the relevant ChannelCRM tenant configuration endpoint.
- 5 Redirects the administrator to grant admin consent for the newly created ChannelCRM app.

Redirect URIs Configured

Redirect URI	Purpose
https://<app-creator-host>/ConsentComplete	Completion page used during the consent flow.
https://ccrm.eu.auth0.com/login/callback	ChannelCRM/Auth0 login callback.

Redirect URI	Purpose
https://auth.onchannelcrm.app/login/callback	ChannelCRM/Auth0 login callback.

Separate Permissions Used by the App Creator

The CCRM App Creator itself uses Microsoft Graph permissions during provisioning so it can create and configure the customer app registration. These setup permissions are separate from the permissions granted to the created ChannelCRM app registration.

Permission	Type	Purpose
Application.ReadWrite.All	Delegated/downstream Graph access in the App Creator	Create, update, and delete app registrations during provisioning.
Directory.ReadWrite.All	Delegated/downstream Graph access in the App Creator	Read and write directory objects needed during provisioning.

References

- Microsoft Graph permissions reference: <https://learn.microsoft.com/en-us/graph/permissions-reference>
- Exchange Online RBAC for Applications and mailbox scoping: <https://learn.microsoft.com/en-us/exchange/permissions-exo/application-rbac>
- EWS application access policy background: <https://devblogs.microsoft.com/microsoft365dev/application-access-policy-support-added-to-exchange-web-services/>