GETTING STARTED GUIDE

ALCATEL-LUCENT RAINBOW™

Rainbow and Microsoft Entra ID Permissions

Ed 8.0

JUNE 2026

Author: Cloud Services

Alcatel-Lucent Enterprise

Disclaimer

This documentation is provided for reference purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this documentation is provided "as is" without any warranty whatsoever and to the maximum extent permitted.

In the interest of continued product development, ALE International reserves the right to make improvements to this document and the products it describes at any time without notice or obligation.

Copyright

Table of Contents

1. Abstract

When linked to Entra ID, Rainbow requires a set of permissions to be able to render the right service. This document details the consent flow mechanism provided by Entra ID and which permission is required for which service and how Rainbow uses them.

Several kinds of services exist in Rainbow and require some permissions:

- Rainbow for Teams
- Calendar and Teams presence
- Single Sign On (SSO)
- Mass Provisioning
- Meeting Scheduler
- Rainbow for Outlook
- Rainbow Personal Contact

2. History

Edition	Date	Rainbow version	Modifications
1.0	2020/07/28	-	Initial Revision
2.0	2022/08/19	-	Add Teams presence and details on consent flows
3.0	2022/10/20	-	Add new authorization for Teams presence synchronization
4.0	2023/03/21	-	Add Teams V3 application
5.0	2024/04/03	-	Add list of Graph APIs and SDK
6.0	2025/03/14	-	Add Contact permission in Teams application
7.0	2025/06/01	-	Separation of Meeting Scheduler and Directory management, add Teams activity
8.0	2026/06/17	170	Add Outlook add-in application, add Rainbow Personal Contact application; clarify Calendar and Teams Presence application permissions scenario

3. Consent Flow

3.1 User or Admin Consent Flows

Depending on the needed service and its required permissions, Entra ID can technically either require that the consent to access Entra ID accounts information is managed by the Entra ID admin (admin consent), or that it can be approved by the end user directly (user consent).

Furthermore, even for services where user consent is technically possible, the company Entra ID administrator can decide that users are not allowed to directly request access to Entra ID service, enforcing an admin consent flow.

The way the consent is given for Rainbow applications therefore depends both on the type of service, and on the way the Entra ID configuration has been defined by the Entra ID admin.

> **Note:** Entra ID user accounts must have the right Entra ID license to have a mailbox and a calendar.

- **Calendar and Teams presence** can operate in two modes depending on the administrator's choice: it normally relies on delegated permissions (Scenarios 1-3), but can alternatively be configured to use application permissions granted by the administrator for the entire organization (Scenario 4). In delegated mode, Rainbow allows the administrator to grant consent on behalf of the entire organization directly from the Rainbow admin panel, removing the individual consent prompt. However, because delegated permissions require a signed-in user context, each user must still authenticate at least once - no consent screen is shown, only a sign-in. The four scenarios are described in section 3.2 and section 4.2.
- **Rainbow for Teams**, **Mass provisioning and Directory search**, **Meeting Scheduler**, and **Rainbow Personal Contact** require an Admin consent, as the service needs to access data of all company users and relies on application permissions.
- **Single Sign On** needs a specific Admin action as it does not require a direct user consent but only an authentication.

3.2 Activation of Delegated Permissions

For Calendar and Teams presence, delegated permissions (Scenarios 1-3) differ in the level of administrator involvement:

- **Scenario 1 - default mode**: no admin action required - each user consents and signs in individually. See Annex A for details on Entra ID user consent configuration options.
- **Scenario 2 (recommended if users control their own presence sharing)**: the admin pre-authorizes from the Rainbow admin panel on behalf of the whole organization. Users only need to sign in once - no consent prompt is shown.
- **Scenario 3 (recommended if the admin wants to control presence sharing activation)**: the admin controls activation for all users and must grant delegated consent from the Rainbow admin panel. Each user still needs to sign in once.

For Scenarios 2 and 3, the Rainbow admin panel allows the administrator to enable the delegation. Microsoft then presents the standard permission consent screen. By checking "Consent on behalf of your organization", permissions are granted for all users in the company.

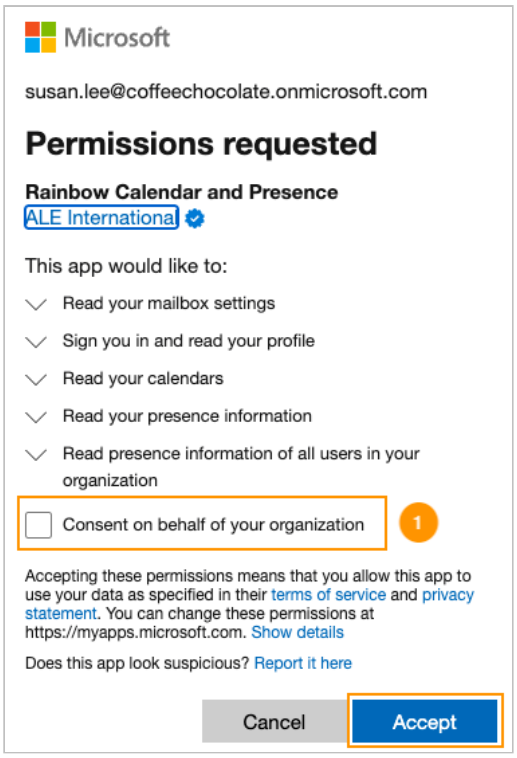


Figure 2 - Admin consent checkbox allowing service activation for all company members.

Note: Rainbow for Teams relies on both delegated and application permissions. Application permissions can only be granted using the Rainbow admin panel, which opens both kinds of permissions. If a user uses the Rainbow Teams extension before the admin has allowed permissions, Microsoft will request delegated permissions from the user. The admin still needs to take action in the Rainbow admin panel to allow the application permissions.

3.3 Activation of Application Permissions

Rainbow for Teams, Mass Provisioning + Directory search, Meeting Scheduler, and Rainbow Personal Contact rely on application permissions rather than delegated permissions. Rainbow acts as an application when calling Microsoft Graph APIs.

To grant these permissions, a Microsoft Global Administrator must enable these services using the Rainbow admin panel. It is possible to grant only one application depending on needs.

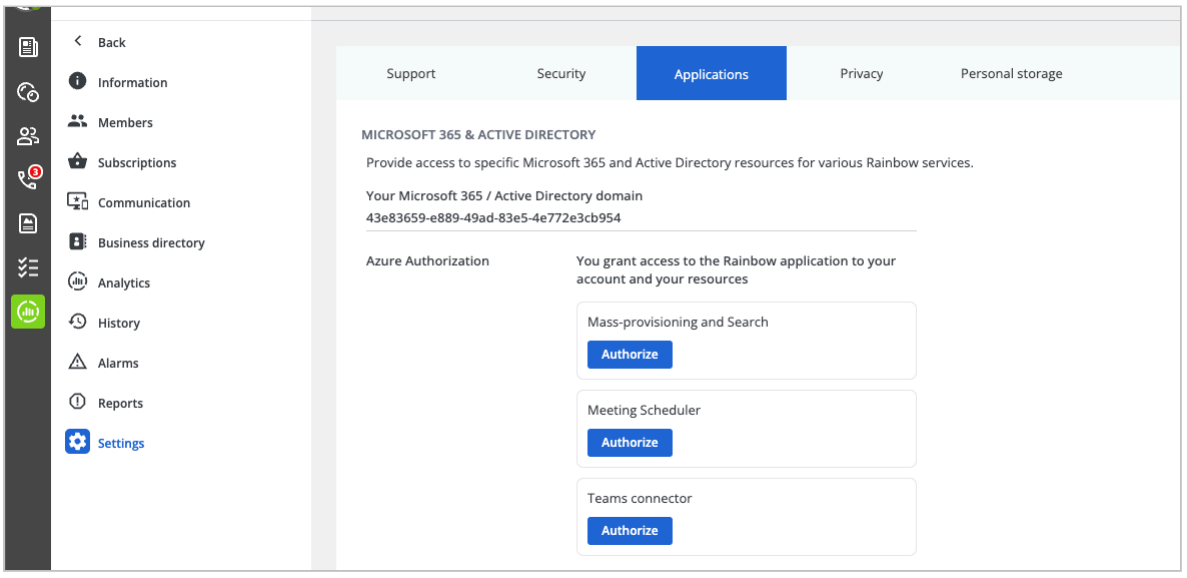


Figure 3 - Rainbow admin panel - Authorize button for Entra ID application permissions.

When the Authorize action is performed, a Microsoft login is requested to grant the needed permissions. The Microsoft account must have sufficient rights to allow them.

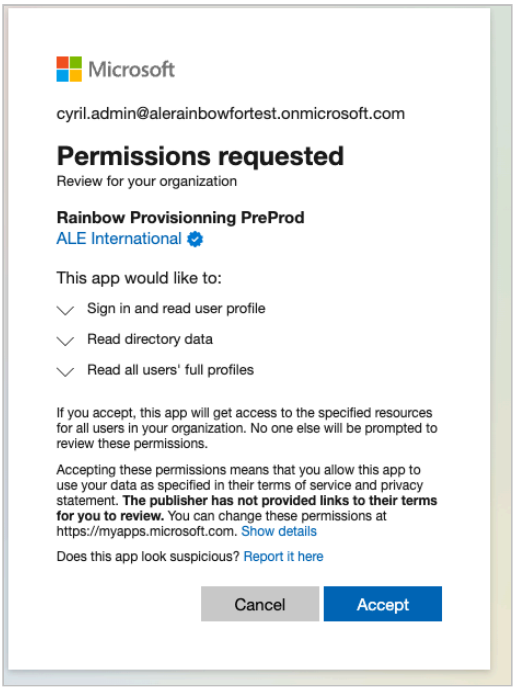


Figure 4 - Microsoft permission consent screen shown during application authorization.

The list of application permissions can then be verified in Entra ID.

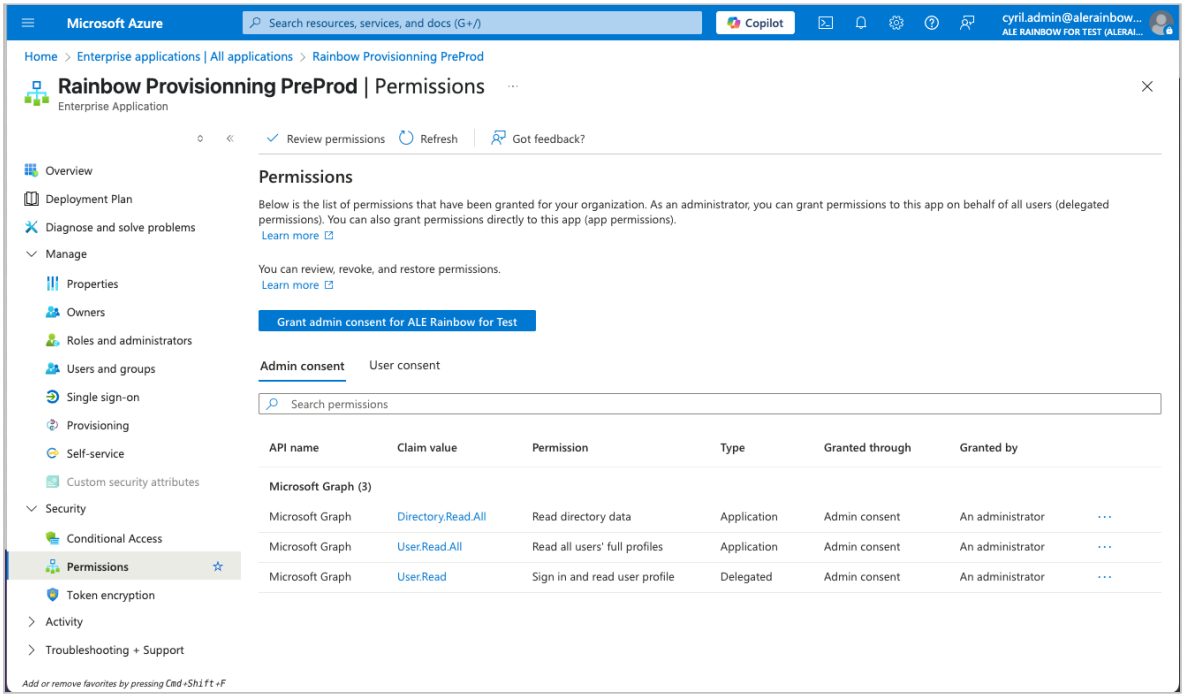


Figure 5 - Application permissions as visible in Entra ID after authorization.

4. Permissions

The list of Entra ID permissions is documented on the Microsoft support site: https://docs.microsoft.com/en-us/graph/permissions-reference

Rainbow applications connected to the Entra ID environment use delegated and application permissions depending on the case. Permissions are required at user or administrator level.

For each required permission, this document gives the name, the permission type, and how it is used in Rainbow.

4.1 Rainbow for Teams

Application ID: `4e1de43c-e5b3-4651-af65-819d279e773d`

Rainbow for Teams is a Teams tab extension that permits access to some Rainbow services directly from Teams. To facilitate user authentication, Rainbow relies on Entra ID authentication to identify the user. Rainbow for Teams also enables missed call notifications in Teams' activity section.

Permission	Type	Rainbow usage
`profile`	Delegated	Used by Rainbow to get the language of the user.
`offline_access`	Delegated	Allows the app to see and update data even when users are not currently using the app.
`email`	Delegated	Used to link the Entra ID account to the Rainbow account using the user's email address.
`openid`	Delegated	Used to sign the user into Entra ID and allow other permissions.
`User.Read`	Delegated	Used to let the user sign in to Entra ID and allow other permissions.
`Contacts.Read`	Delegated	Used to propose a search in the user's contacts from the Rainbow Teams tab.
`TeamsActivity.Send`	Application	Used to display a notification in Teams when the user has a missed call or a new voicemail.
`User.ReadBasic.All`	Application	Used to get the email of users to link the Rainbow user having a missed call to the associated Microsoft Teams user for the activity notification.

APIs used:

- `https://login.microsoftonline.com/<tenant>/v2.0/adminconsent`
- `https://graph.microsoft.com/v1.0/teamwork/sendActivityNotificationToRecipients`

SDKs used:

- `@microsoft/teams-js`
- `@azure/msal-browser`
- `@azure/identity`

4.2 Calendar and Teams Presence

Two applications cover this feature, depending on the authorization mode configured by the administrator. See the *Rainbow Presence Synchronization with Microsoft Entra ID* guide for full deployment scenarios.

The table below summarizes the four scenarios. The Rainbow admin mode column refers to the configuration set in the Rainbow administration panel.

Scenario	Admin involvement
1 - User consent	None - each user consents and signs in individually
2 - Admin pre-authorization	Admin pre-authorizes for the whole org; users sign in once
3 - Admin-controlled activation	Admin grants delegated consent; users sign in once

4 - Application permissions	Admin grants application permissions for the whole org; no user action required

Scenarios 1, 2, 3 - Delegated permissions

Application: Rainbow Calendar and Presence - **Application ID:** `96d01656-933b-43b3-b06b-abc61ce7bcb3`

Each user authorizes Rainbow individually, or an admin grants consent on behalf of the organization. Presence synchronization is **bidirectional** (Rainbow ↔ Teams).

Permission	Type	Rainbow usage
`User.Read`	Delegated	Sign in to Entra ID and allow other permissions.
`Calendars.Read`	Delegated	Read the user's calendar to show occupancy status and duration to other users.
`MailboxSettings.Read`	Delegated	Read out-of-office state and automatic reply message to display to the user's contacts.
`Presence.Read`	Delegated	Read Teams presence to display DND status in Rainbow.
`Presence.Read.All`	Delegated	Subscribe to presence change notifications. The subscription API requires this permission - `Presence.Read` alone is insufficient.
`Presence.ReadWrite`	Delegated	Push Rainbow presence status to Teams. When a user is in a call or has set DND in Rainbow, they appear as Busy in Teams.

APIs used:

- `https://login.microsoftonline.com/common/oauth2/authorize`
- `https://login.microsoftonline.com/common/oauth2/token`
- `https://graph.microsoft.com/v1.0/me`
- `https://graph.microsoft.com/v1.0/me/presence`
- `https://graph.microsoft.com/v1.0/subscriptions`
- `https://graph.microsoft.com/v1.0/subscriptions/:id`
- `https://graph.microsoft.com/v1.0/users/:id/presence/setPresence`
- `https://graph.microsoft.com/v1.0/users/:id/calendar/calendarView`
- `https://graph.microsoft.com/v1.0/users/:id/mailboxSettings/automaticRepliesSetting`
- `https://graph.microsoft.com/v1.0/users/:id/calendar/events`
- `https://graph.microsoft.com/v1.0/users/:id/mailboxSettings`

Scenario 4 - Application permissions

Application: Rainbow Calendar and Presence (App) - **Application ID:** `baa4f282-a867-486b-8063-fbca0ee764e5`

The administrator authorizes the application for the entire organization - no individual user action is required.

> **Note - Microsoft limitation:** Presence change notification subscriptions are not supported with application permissions. Scenario 4 only supports **unidirectional** synchronization (Rainbow → Teams). Bidirectional sync requires delegated permissions (Scenarios 1–3).

Permission	Type	Rainbow usage
`Calendars.Read`	Application	Read calendars across all mailboxes to compute user occupancy.
`MailboxSettings.Read`	Application	Read mailbox settings (timezone, out-of-office) for all users.

Presence.Read.All	Application	Read Teams presence for all users.
Presence.ReadWrite.All	Application	Write Rainbow presence status to Teams for all users.
User.Read.All	Application	Read full profiles of all users in the organization.

APIs used:

- https://login.microsoftonline.com/:tenant/v2.0/adminconsent
- https://graph.microsoft.com/v1.0/users/:id
- https://graph.microsoft.com/v1.0/users/:id/presence
- https://graph.microsoft.com/v1.0/users/:id/presence/setPresence
- https://graph.microsoft.com/v1.0/users/:id/calendar/calendarView
- https://graph.microsoft.com/v1.0/users/:id/mailboxSettings/automaticRepliesSetting
- https://graph.microsoft.com/v1.0/subscriptions
- https://graph.microsoft.com/v1.0/subscriptions/:id

4.3 Single Sign On

Rainbow can leverage an external identity provider to allow users to log in to Rainbow using their Entra ID credentials. These permissions are granted by the Entra ID admin when configuring SSO with Rainbow.

When based on SAML, Rainbow needs access to the user's email address to match the corresponding Rainbow account. SAML authentication in Entra ID does not require specific permissions - only the email address is returned as a claim.

Required permissions when SSO is based on OIDC:

Permission	Type	Rainbow usage
openid	Delegated	Allows users to sign into the app with their Entra ID account.
email	Delegated	The email address is retrieved to match the Rainbow login of the associated account for OIDC authentication.

OIDC endpoints:

- Discovery URL (optional): https://login.microsoftonline.com/:tenantId/v2.0/.well-known/openid-configuration
- Issuer: https://login.microsoftonline.com/:tenantId/v2.0
- JWKS URI: https://login.microsoftonline.com/:tenantId/discovery/v2.0/keys
- Authorization endpoint: https://login.microsoftonline.com/:tenantId/oauth2/v2.0/authorize
- Token endpoint: https://login.microsoftonline.com/:tenantId/oauth2/v2.0/token
- Userinfo endpoint (optional): https://graph.microsoft.com/oidc/userinfo
- End session endpoint (optional): https://login.microsoftonline.com/:tenantId/oauth2/v2.0/logout

SAML endpoints:

- Login URL: https://login.microsoftonline.com/:tenantId/saml2
- Logout URL (optional): https://login.microsoftonline.com/:tenantId/saml2

4.4 Rainbow Provisioning

Application ID: a8b1d6a4-8d79-4387-894d-5b27c8e1e17c

Rainbow can use the Entra ID directory to create Rainbow users (Mass provisioning) or to search the directory. The administrator needs to link their Rainbow company with their Entra ID directory and accept the required permissions.

Permission required to link Rainbow and Entra ID:

Permission	Type	Rainbow usage
User.Read	Delegated	Used to let the administrator sign in to Entra ID and link the Entra ID tenant with Rainbow by allowing the application access to the directory.

API used by all services linked to the directory application:

- https://login.microsoftonline.com/:tenant/v2.0/adminconsent

4.4.1 Mass Provisioning

Rainbow can import user accounts configured in Entra ID to create associated Rainbow accounts. To do this, the admin allows Rainbow to read the list of users in Entra ID through the administrative part of Rainbow.

Permission	Type	Rainbow usage
User.Read.All	Application	Retrieves account details to create users in Rainbow: name, email, phone numbers.

API used:

- https://graph.microsoft.com/v1.0/users

4.4.2 Search

Once linked with the Entra ID directory, Rainbow users can search the Entra ID directory from Rainbow to dial by name. The search finds Entra ID company users and shared contacts.

Permission	Type	Rainbow usage
User.Read.All	Application	Enables searching for company users in the Entra ID directory from the Rainbow client.
Directory.Read.All	Application	Enables searching for shared contacts in the Entra ID directory from the Rainbow client.

APIs used:

- https://graph.microsoft.com/beta/contacts
- https://graph.microsoft.com/v1.0/users

4.5 Rainbow Meeting Scheduler

Application ID: 4b5796e7-887a-4787-b8a3-e14769a74d35

In Rainbow, a bubble organizer can look for available slots for all or some bubble participants based on their calendar availability in Entra ID. For each slot, details such as the probability of attendance and participant status (free, tentative, busy, out of office, out of work hours, working elsewhere) are highlighted. This functionality does not require user permissions - only administrator consent.

Permission	Type	Rainbow usage
User.Read	Delegated	Used to let the administrator sign in to Entra ID and link the Entra ID tenant with Rainbow.

Calendars.ReadWrite	Application	Allows retrieval of each participant's availability to compute available slots. An event is then created in each participant's calendar for the chosen slot.
MailboxSettings.Read	Application	Used to take into consideration the timezone of users when computing available slots.

APIs used:

- https://login.microsoftonline.com/:tenant/v2.0/adminconsent
- https://graph.microsoft.com/v1.0/users/:id
- https://graph.microsoft.com/v1.0/users/:id/calendar/getSchedule
- https://graph.microsoft.com/v1.0/users/:id/mailboxSettings
- https://graph.microsoft.com/v1.0/users/:id/calendar/events

4.6 Rainbow for Outlook

Application ID: 2ed00a4d-9fc3-499f-a96e-af2077ceba2b

A Rainbow add-in is available for Outlook. It permits creating a bubble from a list of meeting participants and automatically adds a link to the composed invitation.

Permission	Type	Rainbow usage
profile	Delegated	Used by Rainbow to get the language of the user.
offline_access	Delegated	Allows the app to maintain access to data even when users are not currently using the app.
email	Delegated	Used to link the Entra ID account to the Rainbow account using the user's email address.
openid	Delegated	Used to sign the user into Entra ID and allow other permissions.
User.Read	Delegated	Used to let the user sign in to Entra ID and allow other permissions.
Calendars.ReadWrite	Delegated	Permits displaying the Rainbow add-in in the calendar view. Rainbow needs access to meeting participants to create corresponding Bubbles, and write access is required to modify the event body to add the Bubble link.
Mail.Read	Delegated	Permits displaying Rainbow in the email context of Outlook. Required by Microsoft to display the extension in the email context.

SDKs used:

- @microsoft/teams-js
- @azure/msal-browser
- @azure/identity

4.7 Directory (deprecated)

> **Deprecated:** This application is no longer used when Mass provisioning, Directory search, or Meeting Scheduler are used. It has been replaced by two separate applications to decouple the Meeting Scheduler and directory management - this avoids requiring calendar permissions when only directory services are needed.

This application has been replaced by:

- **Rainbow Provisioning** (a8b1d6a4-8d79-4387-894d-5b27c8e1e17c) - for Mass provisioning and Search.
- **Rainbow Meeting Scheduler** (4b5796e7-887a-4787-b8a3-e14769a74d35) - for Meeting Scheduler.

If the admin restarts the activation process from the Rainbow admin interface, the new applications will be used. The old application will remain in Entra ID but will no longer be used. The admin must remove it manually from the Entra ID admin application management interface.

Application ID: `994960a3-afdc-4132-a85c-faa2be7c4709`

Permissions required are identical to those described in the corresponding chapters of the replacement applications above.

API used:

- `https://login.microsoftonline.com/:tenant/oauth2`

4.8 Rainbow Personal Contact

Application ID: `31c5f992-c125-4ff0-a708-c5128c7bb3a3`

Rainbow Personal Contact enables Rainbow users to search their personal contacts stored in their Microsoft 365 mailbox directly from the Rainbow interface. The service enumerates all contact folders (including nested ones), performs full-text search across them, and retrieves contact details including photos.

Permission	Type	Rainbow usage
`profile`	Delegated	Used to get the language of the user.
`offline_access`	Delegated	Allows the app to maintain access even when the user is not actively using the app.
`Contacts.Read`	Application	Reads contacts from the user's mailbox folders.
`MailboxFolder.Read.All`	Application	Enumerates contact folders and sub-folders in the user's mailbox.
`MailboxItem.Read.All`	Application	Reads contact items within the discovered folders.
`User.Read.All`	Application	Resolves the user identity to scope all requests to the correct mailbox.

APIs used:

- `GET /v1.0/users/{userId}/contactFolders`
- `GET /v1.0/users/{userId}/contactFolders/{folderId}/childFolders`
- `GET /v1.0/users/{userId}/contacts`
- `GET /v1.0/users/{userId}/contactFolders/{folderId}/contacts`
- `GET /v1.0/users/{userId}/contacts/{contactId}`
- `GET /v1.0/users/{userId}/contactFolders/{path}/contacts/{contactId}`
- `GET /v1.0/users/{userId}/contacts/{contactId}/photo/$value`

Annex A - User Consent Flow and Admin Consent Requests

Calendar and Teams Presence synchronization requires each user to authenticate with their Microsoft account so Rainbow can access their calendar and presence data. In Scenario 1, this is done entirely by the user without any administrator action in Rainbow.

For Scenario 1 to work, the Entra ID tenant must allow user consent for applications.

This annex describes the Entra ID user consent policies and how administrators can configure them.

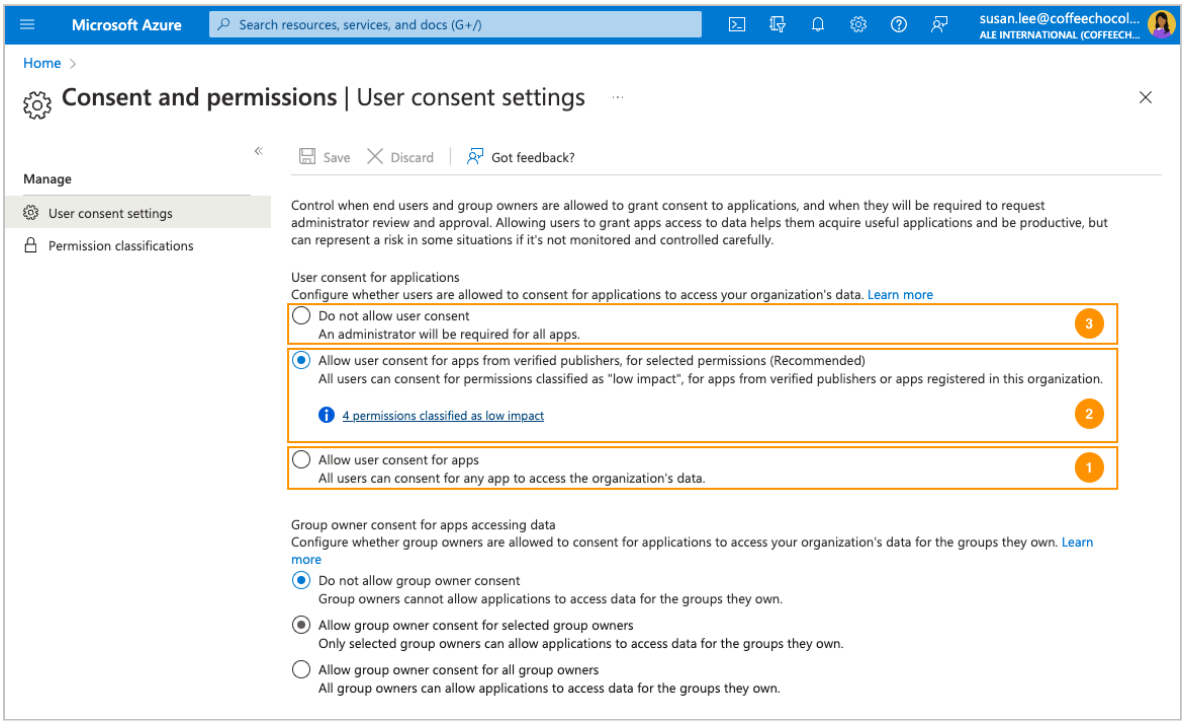


Figure A1 - Entra ID Enterprise Applications consent configuration levels.

Entra ID admins can define the level of control they want to have over their users. In Entra ID there are three levels defined in Enterprise Applications, from the most open to the most restrictive:

1. Allow user consent for apps.
2. Allow user for apps from verified publisher and asking for selected permissions.
3. Do not allow user consent.

> **Note:** Some possibilities exist to delegate rights to a group of users to manage consent. These are not detailed in this document.

A.1 Allow User Consent for Apps

If the admin allows user consent, any user declared in Entra ID can allow Rainbow applications that require user consent.

No admin action is required.

When the user enables the service in the Rainbow application, a Microsoft authentication screen is presented and the user must authenticate and accept the requested permissions.

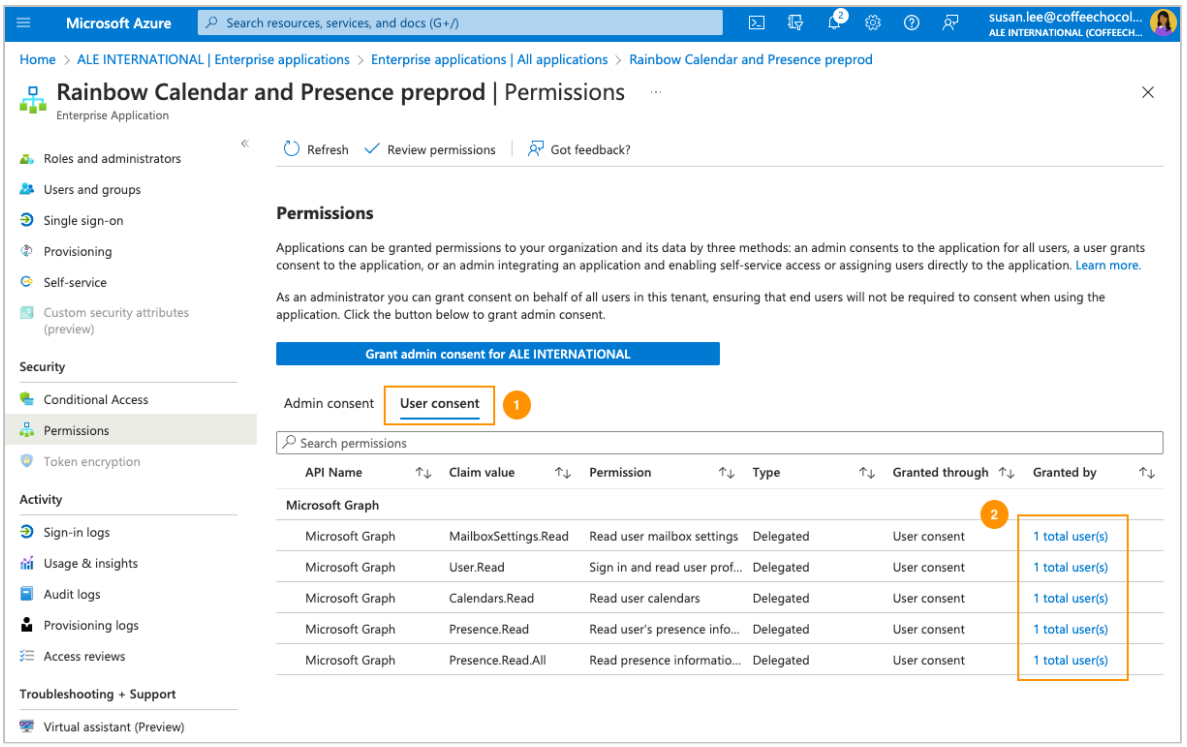


Figure A2 - Admin can review users who enabled the application under the Permission tab of the Enterprise application.

> **Note:** The admin has the possibility to allow this application for all company users (admin consent). In that case, the permission prompt is no longer presented to users when they enable the Rainbow calendar, and it is no longer possible to see who enabled the application in Entra ID.

A.2 Allow User for Apps from Verified Publisher and Asking for Selected Permissions

As recommended by Microsoft, the Entra ID admin has the possibility to authorize users to use applications deployed by a verified publisher and asking for a specific set of permissions.

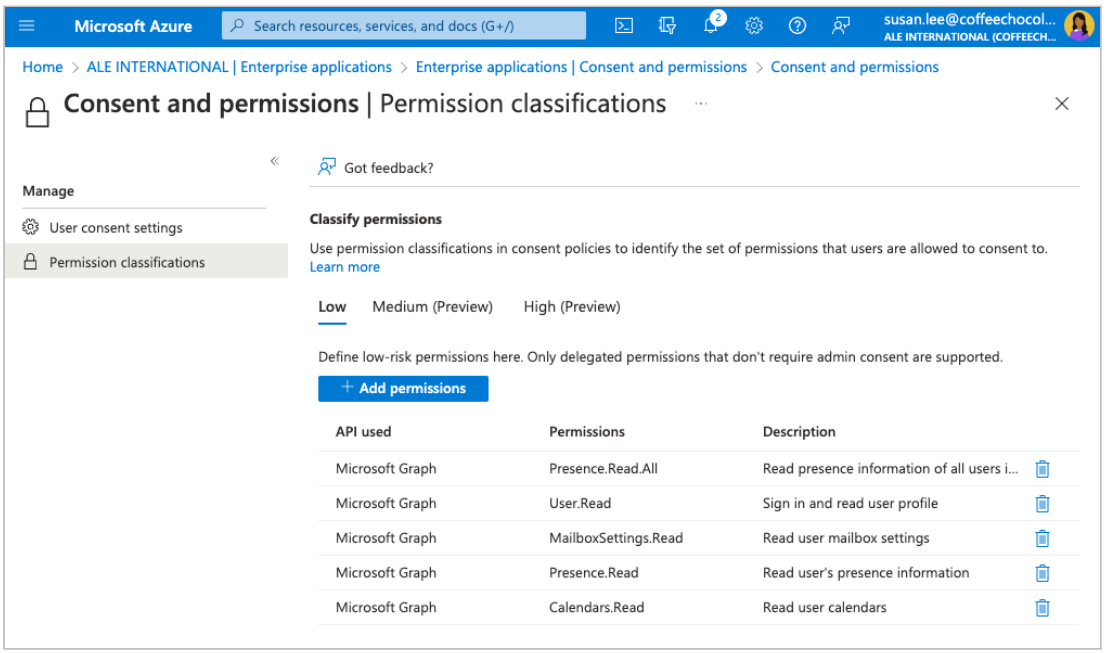


Figure A3 - Admin configures the list of allowed permissions for verified publishers.

In that case the admin needs to add the list of permissions required by Rainbow Calendar and Presence as "Low".

> **Note:** If the list of permissions allowed by the admin does not contain all permissions asked by the Rainbow application, the user will fall into the admin consent request flow described in section A.3.

A.3 Do Not Allow User Consent

The Entra ID admin can also restrict access to any application and enforce an approval flow.

In that case, since the admin has not allowed the Rainbow application for their Entra ID tenant, users will see:

- An admin consent request form when they enable it in Rainbow.
- If the Entra ID admin does not authorize users to perform an admin consent request, only a screen explaining they must contact their Entra ID admin directly.

The control of the admin consent workflow is done in the Enterprise Applications section of Entra ID administration.

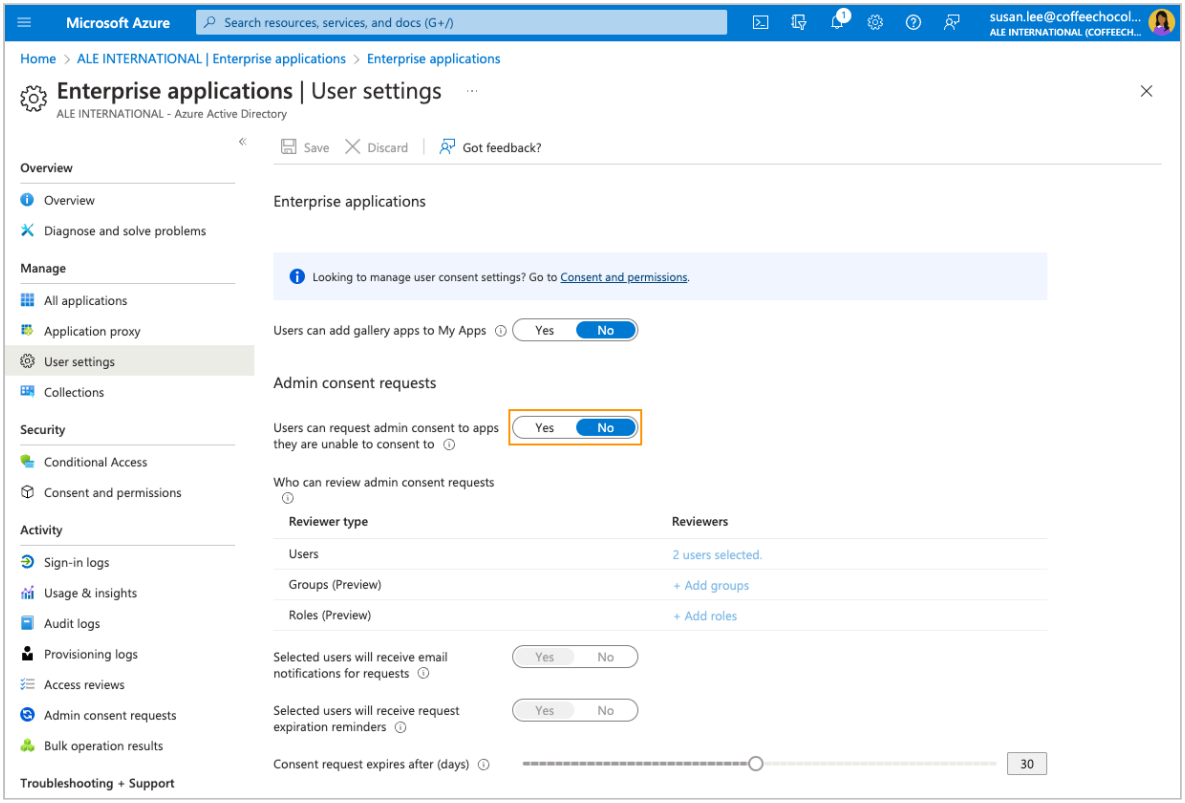


Figure A4 - Enterprise Applications settings to control user consent.

If the admin does not allow admin consent requests, the user will see this message when enabling the Rainbow Entra ID integration:

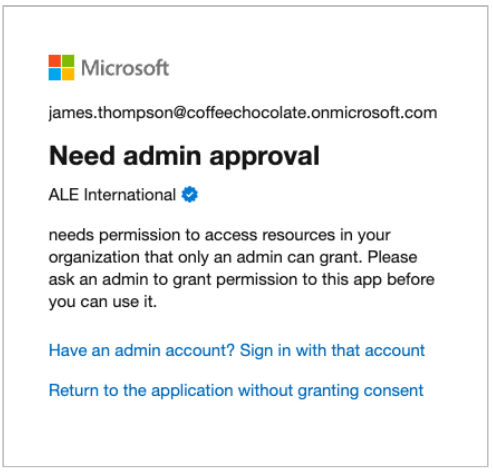


Figure A5 - Message shown to user when admin consent requests are not allowed.

If the admin allows admin consent requests, the user will see this message, which lets them fill in a justification. The admin will receive an email from Entra ID. Once the admin accepts the request, the user receives a confirmation email and must re-activate the Rainbow Entra ID integration.

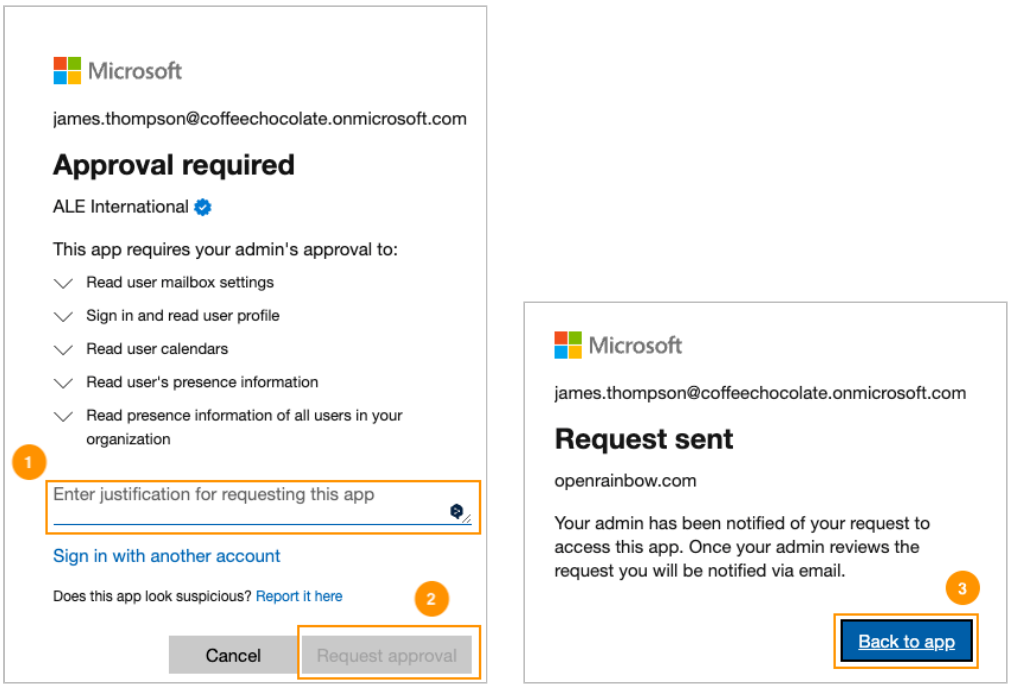
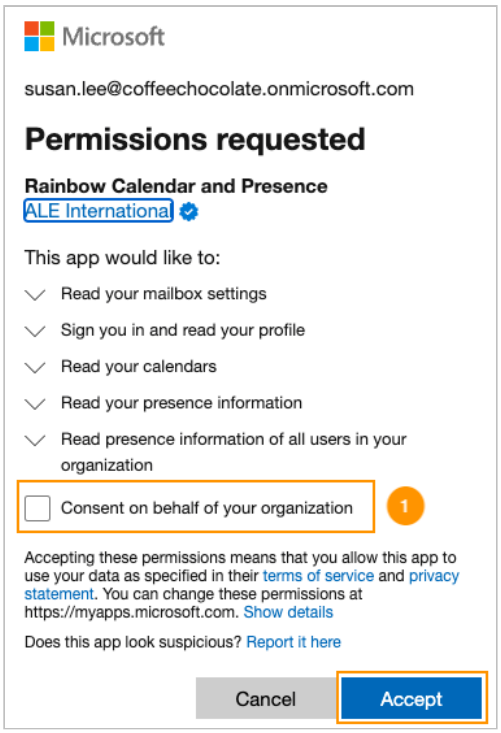


Figure A6 - Admin consent request form (left) and confirmation message (right).

To give users access to the Rainbow application, the admin needs to allow it for the whole company. This can be done in several ways:

1. The admin enables the Rainbow Entra ID application by requesting access to Microsoft services from their own Rainbow account. As an admin, a specific checkbox is displayed in the permission screen to allow the app for everyone in the tenant.



2. The admin can review permission requests sent by users in the Entra ID administration panel and accept them.

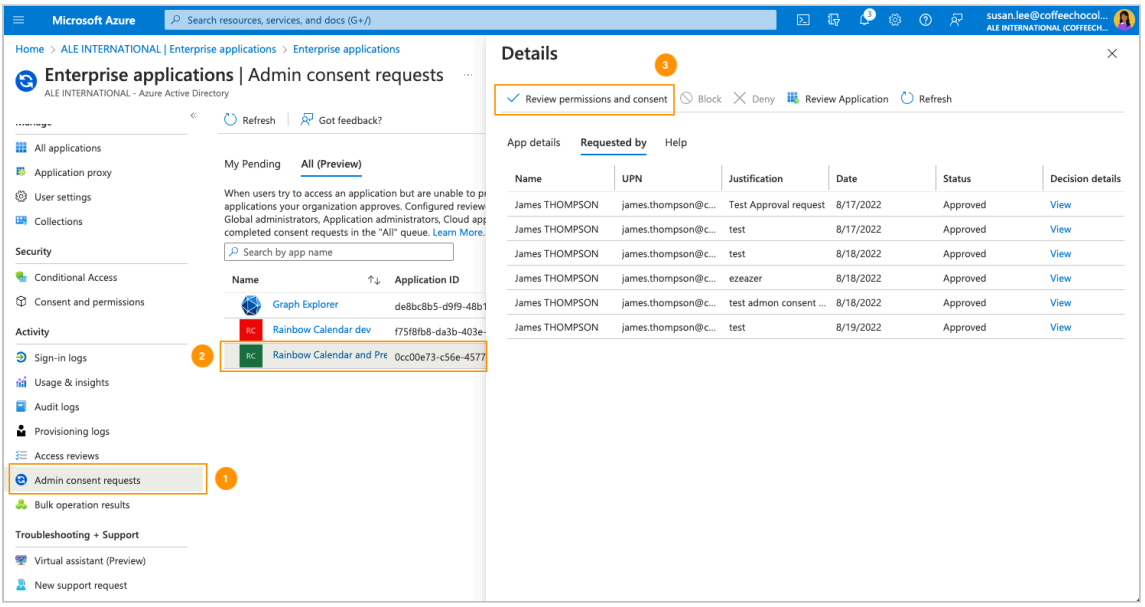


Figure A7 - Admin reviews pending user consent requests in Entra ID.

3. The admin can directly go to the Rainbow application description in Entra ID and allow it for everyone.

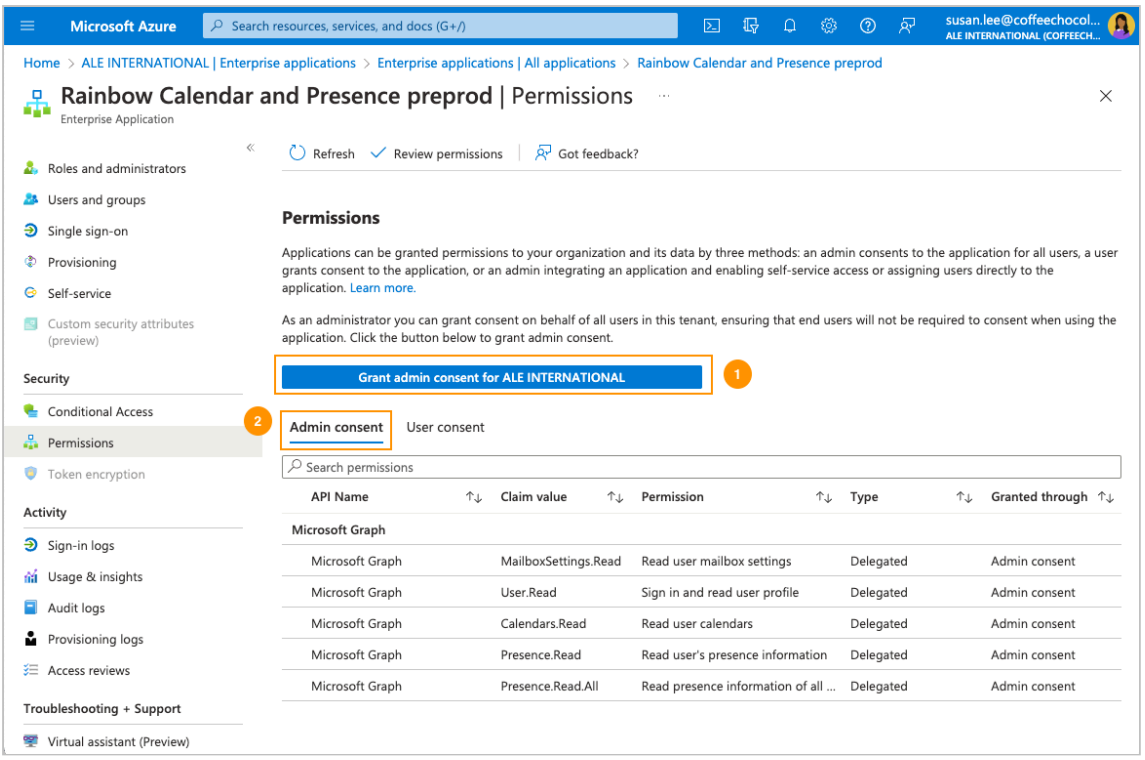


Figure A8 - Admin grants consent directly from the application registration page.

In all cases, the admin consent will be visible in Entra ID.

Once admin consent is given for an application, users no longer see the permission screen when they enable the Rainbow application. It is also no longer possible to see details of users who enabled the application in Entra ID's user consent tab.

End of Document