GETTING STARTED GUIDE

ALCATEL-LUCENT RAINBOW™

Rainbow and Azure permissions

Ed 07

JUNE 2025

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

Contents

1 Abstract

When linked to Azure, Rainbow requires a set of permissions to be able to render the right service. This document details consent flow mechanism provided by Azure 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
- Directory search
- Meeting Scheduler

2 History

Modifications	Date	Edition
Initial Revision	2020 / 07 / 28	Ed 01
Add Teams presence and details on consent flows	2022 / 08 / 19	Ed 02
Add new authorization for Teams presence synchronization	2022 / 10 / 20	Ed 03
Add Teams V3 application	2023 / 03 / 21	Ed 04
Add list of Graph APIs and SDK	2024 / 04 / 03	Ed 05
Add Contact permission in Teams application	2025 / 03 / 14	Ed 06
Separation of Meeting Scheduler and Directory management, add Team’s activity	2025 / 06 / 01	Ed 07

3 Consent flow

3.1 User or Admin consent flows

Depending on the needed service and its required permissions, Azure can technically either require that the consent to access Azure accounts information is managed by the Azure 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 Azure administrator can decide that users are not allowed to directly request access to Azure 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 Azure configuration has been defined by the Azure admin.

Note that Azure user accounts must have the right Azure license to have a mailbox and a calendar.

Calendar and Teams presence application needs a user consent flow.

Rainbow for Teams, Mass provisioning and Directory search, Meeting Scheduler require an Admin consent as the service needs to access to some data of all user's company and rely on application's permissions.

Single Sign On needs a specific Admin action as it doesn't need a direct user consent but only an authentication.

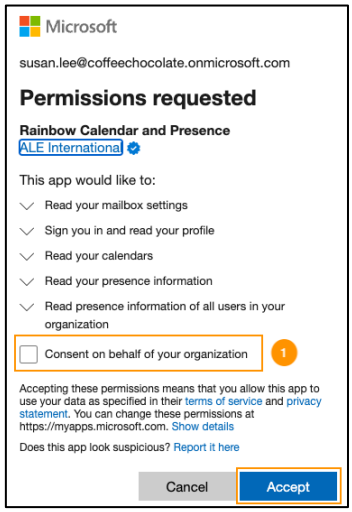
3.2 Activation of delegated permissions

Calendar and Teams presence application relies on user delegated permissions. The easiest way to allow user consent is to do it in one time using an Azure global Admin consent acting on behalf of his organization.

The first time, to be sure that all company members will have access to Rainbow services that require a user consent (Calendar and Teams presence), the Rainbow service activation must be done by an Azure Global admin. It permits to do the consent only one time and it facilitates the user experience.

The Azure Global Admin needs to enable the service: Start Rainbow and activate the calendar / presence synchronization.

As for any user, when Rainbow will require some permissions to Azure, as the user is a Global Azure, Admin, he will have the possibility to allow the application to all users in the



company.

As shown in the picture, Admin has a specific check box that permit to allow the service for all members.

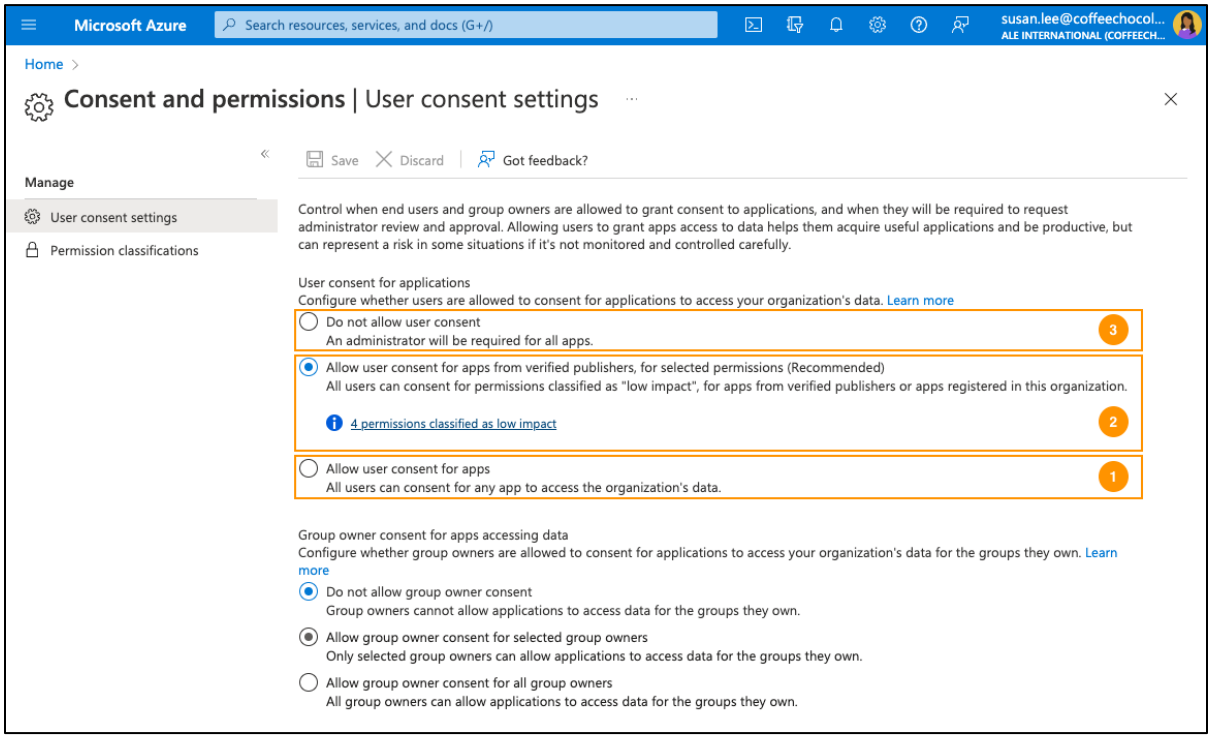
This action must be done for all services activation: typically, for Teams in a first step, and to allow the Calendar/Presence synchronization in a second step.

Other ways are also possible. More details are given in the following chapters.

Note: Rainbow for Teams application relies on both kind of permissions: delegated and applications. Application's permission can only be granted using the Rainbow admin panel. It will open both kind of permissions. If the user uses the Rainbow Teams extension before the admin has allowed permissions, Microsoft will request to the user the delegated permissions as described before. Admin still need to the action in Rainbow admin panel to allow other application's permissions.

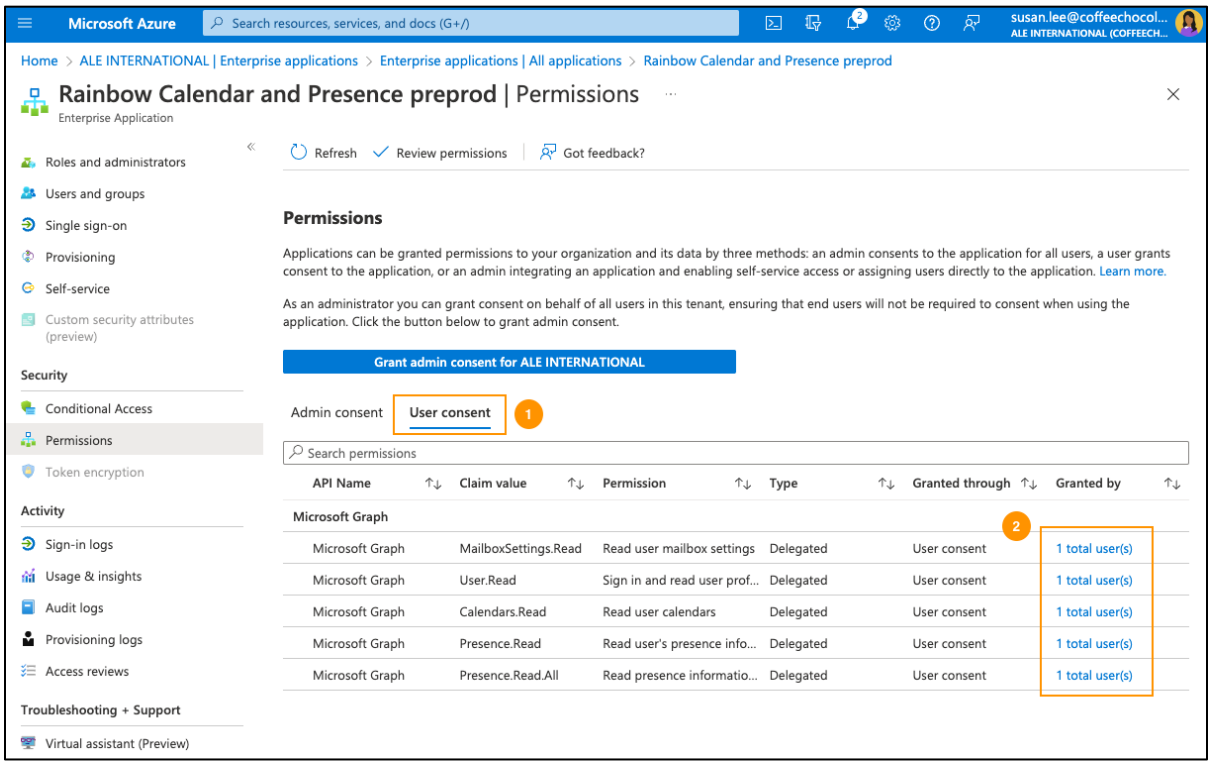
3.3 User consent flow and Admin consent requests

Azure admin can define the level of control they want to have on their user. In Azure there are three levels defined in Enterprise Applications.



From the more open to the more restrictive:

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



Some possibilities exist to delegate rights to a group of users to manage consent. It is not detailed in this document.

3.3.1 Allow user consent for apps

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

No admin action is required.

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

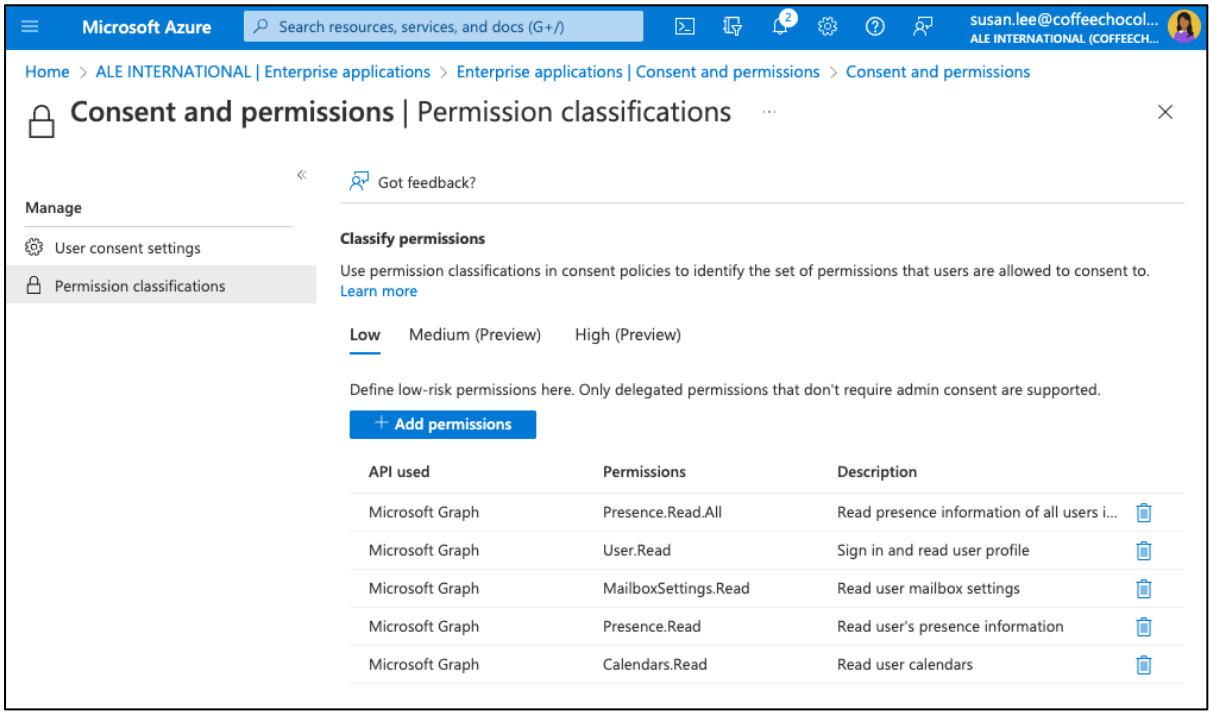
Admin can review users that enabled the application directly in Azure under the Permission of the Enterprise application.

Note: as detailed below, the admin has the possibility to allow this application for all the company (admin consent). In that case, the permission prompt is no more presented to users when they enable the Rainbow calendar, and it is no more possible to see who enabled the application in Azure.

3.3.2 Allow user for apps from verified publisher and asking for selected permissions

As recommended by Microsoft, the Azure admin have the possibility to authorize users to use application deployed by verified publisher and asking for a set of permission.

In that case the admin needs to add the list of permissions required by Rainbow calendar and Presence for example as “Low”.



Note: If the list of permissions allowed by the admin doesn’t contain all ones asked by the Rainbow application, the user will fall back in the admin consent request case as described below in 3.3.3.

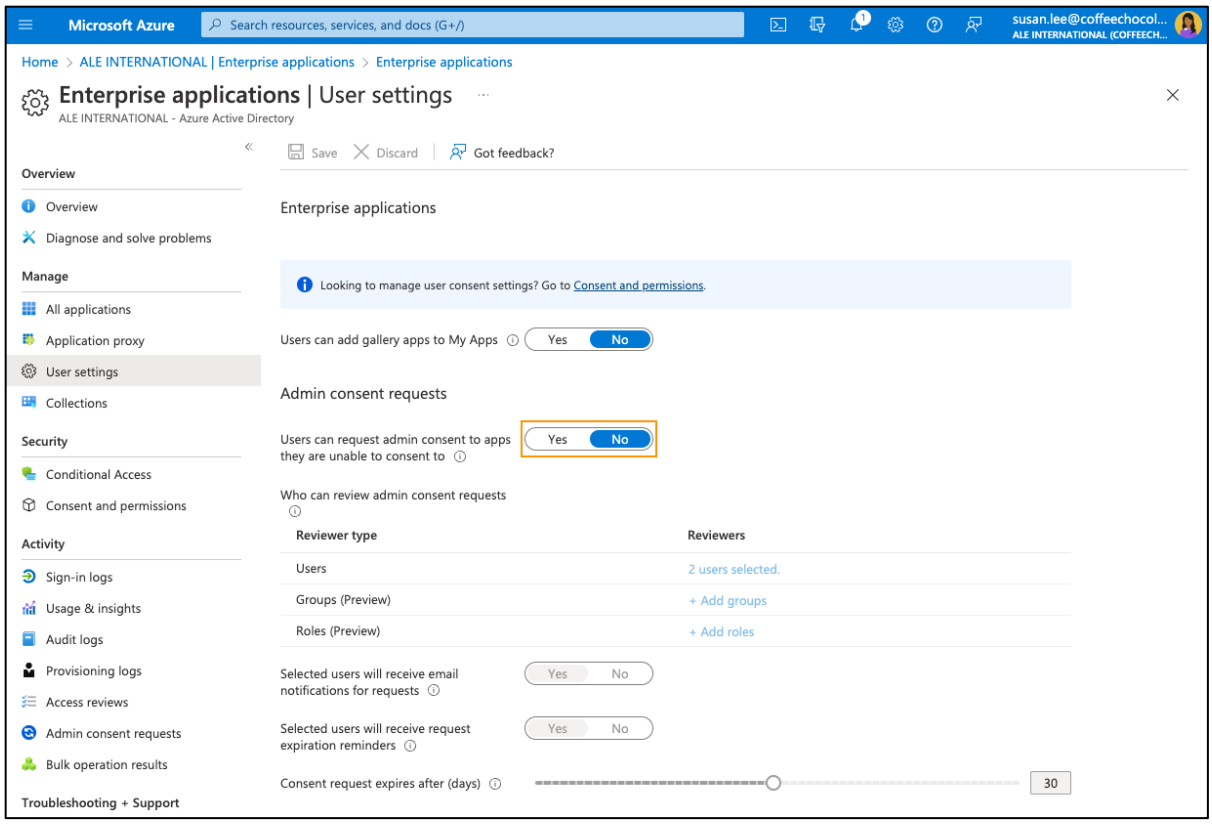
3.3.3 Do not allow user consent

The Azure admin has also the possibly to restrict access to any applications and to enforce an approval flow.

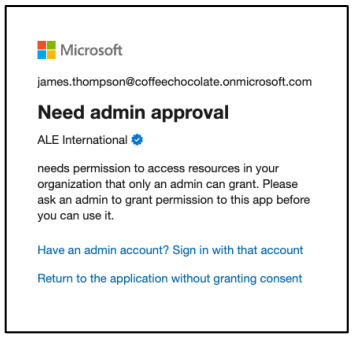
In that case, as the admin hasn’t allowed the Rainbow application for his Azure Tenant, users will see:

- Admin consent request form when they enable it on their side in Rainbow.
- if Azure Admin doesn’t authorize users to perform an admin consent request, only a screen that explain to contact their Azure admin directly.

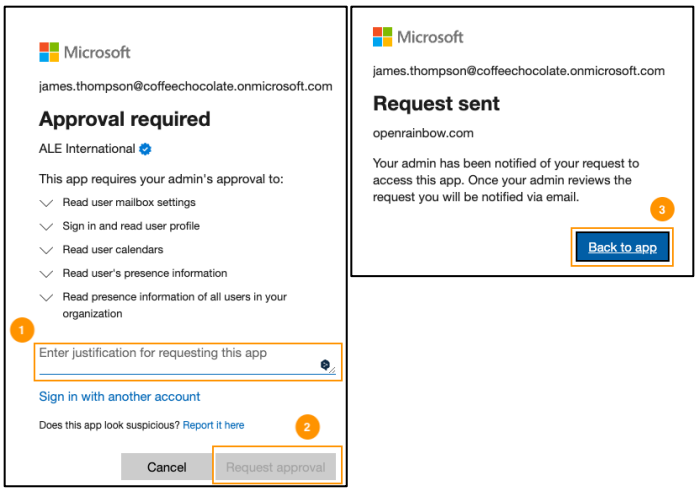
The control of the admin consent workflow is done in Enterprise application part of Azure administration.



If Admin doesn't allow admin consent request, the user will see this message when he enables Rainbow Azure integration in his Rainbow client.

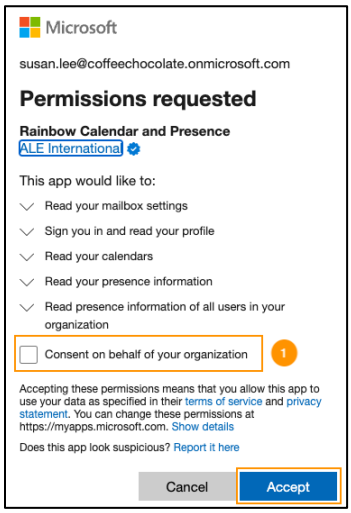


If Admin allows Admin Consent request, the user will see this message. It lets him fill a justification to the request. Admin will receive a mail from Azure. As explained in the Azure's confirmation message, when Admin accepts the request, the user receives a confirmation email from Azure. He needs to re-active Rainbow Azure integration in his Rainbow client.

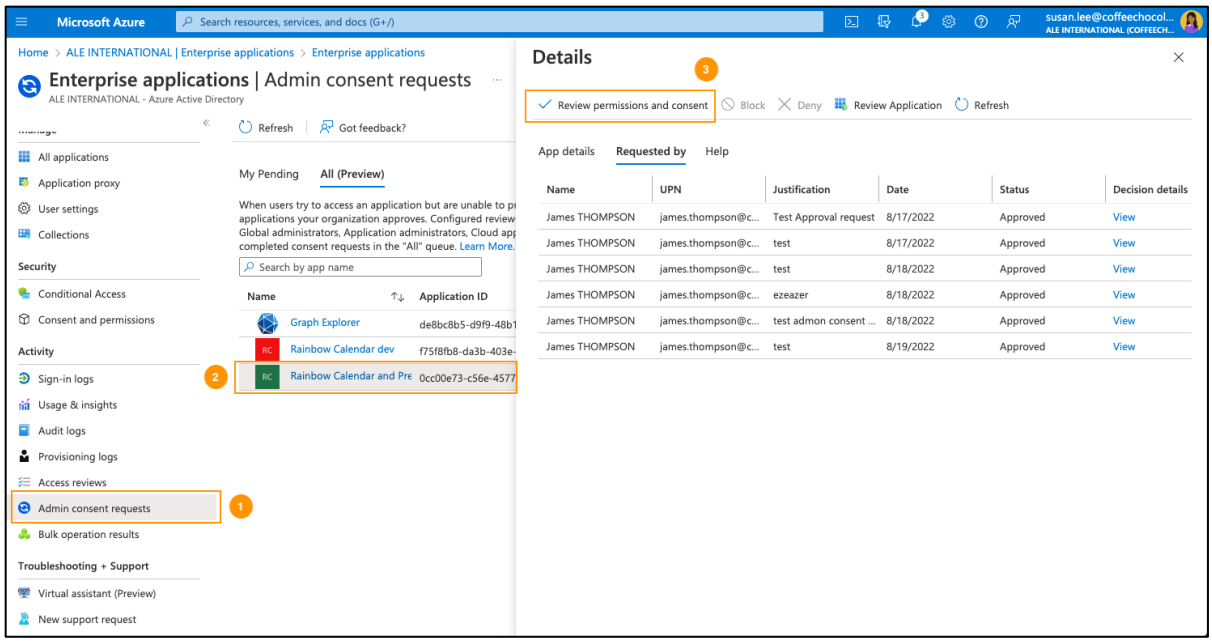


To let users to have access to the Rainbow application, admin needs to allow the Rainbow application for the whole company. This can be done in several ways.

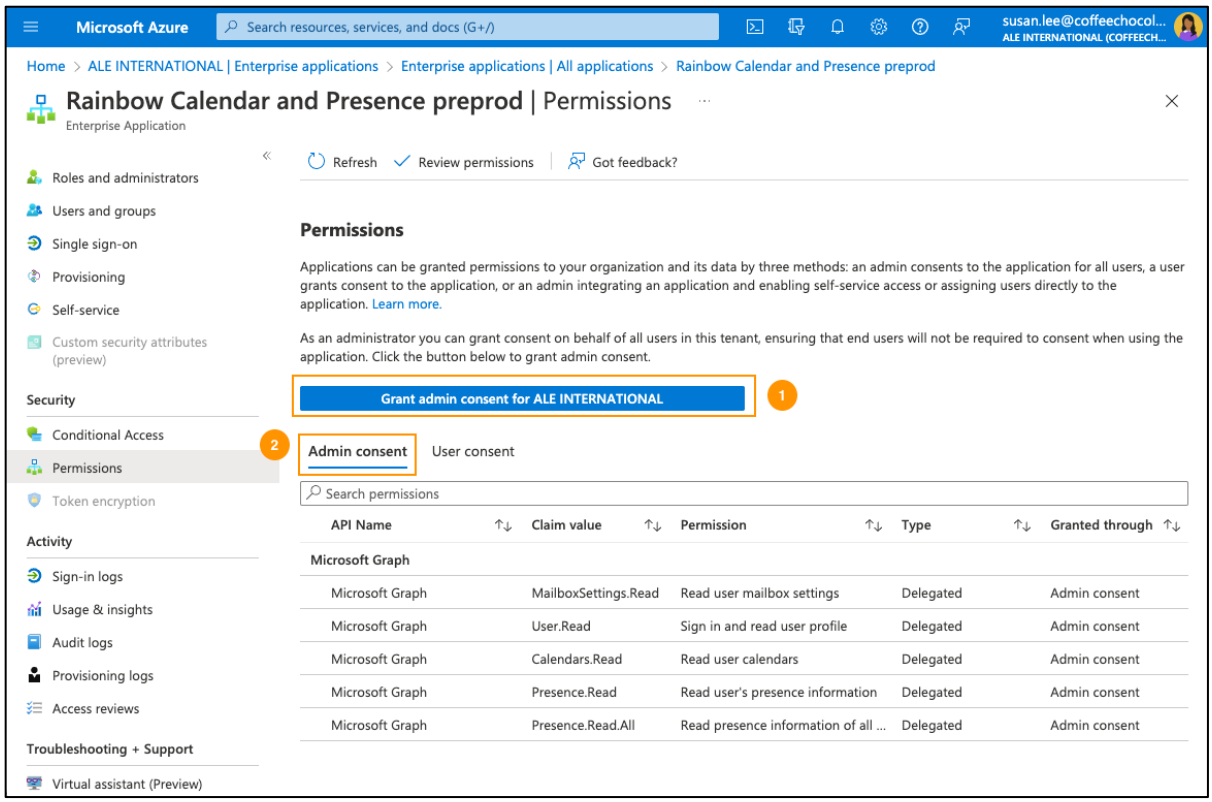
1. Admin enables the Rainbow Azure application by requesting access to Microsoft services from his own Rainbow account. As he is an admin, a specific checkbox is displayed in the permission screen that permit to allow the app for everyone in the Tenant.



2. The admin can review permission request sent by users in Azure administration panel and accept them



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



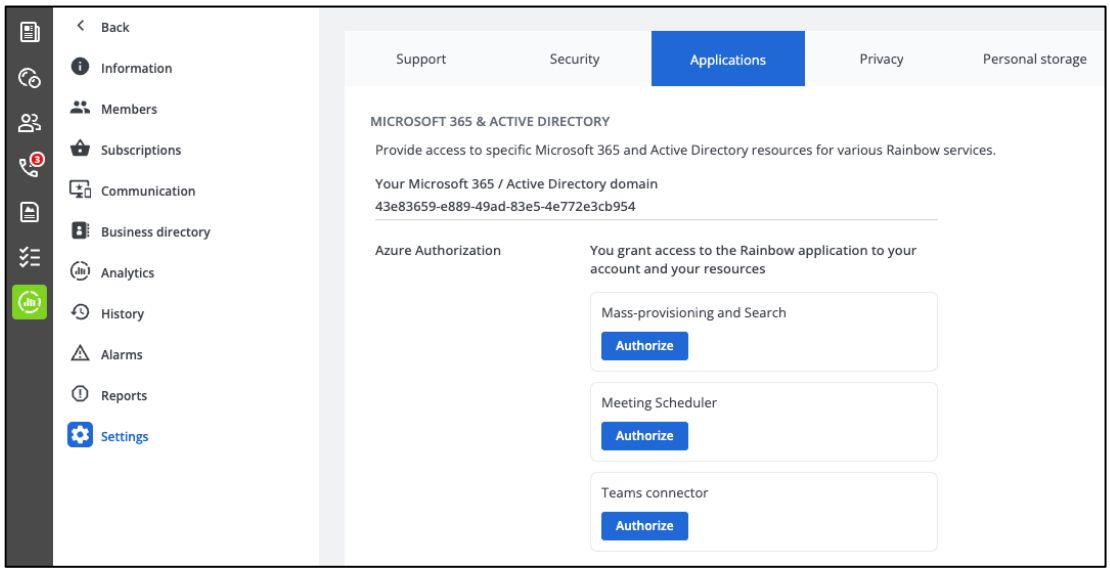
In all cases, the admin consent will be visible in Azure.

Once the admin consent is given for an application, user no longer see the permission screen when they enable the Rainbow application on their side. It is also no more possible to see details of users who enable the application in Azure' user consent tab.

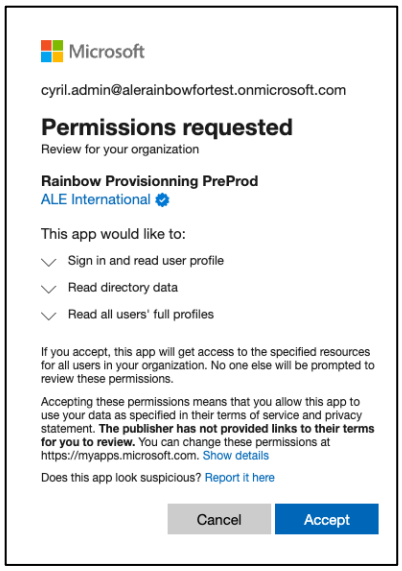
3.4 Activation of application's permissions

Rainbow for Teams, Mass Provisioning + Directory search, Meeting Scheduler rely on application permissions and not on delegated permission. Rainbow is acting as an application when calling Microsoft Graph APIs.

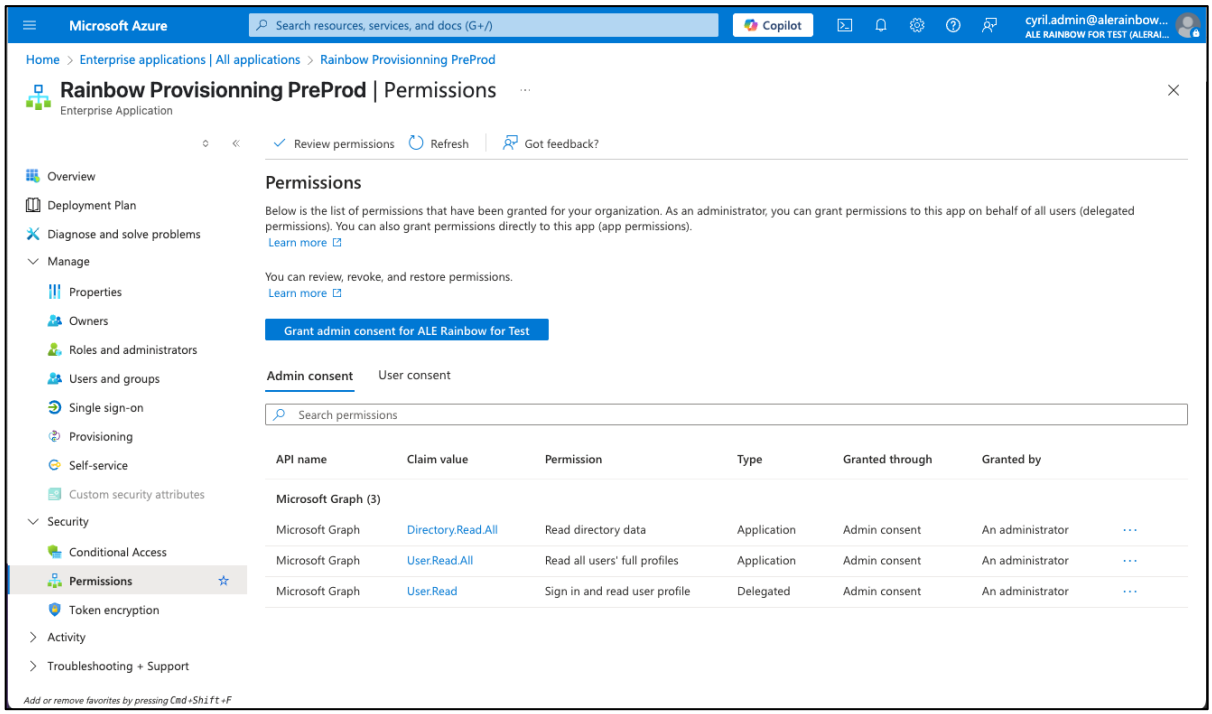
The grant these permissions, a Microsoft Global Administrator must enable these services using the Rainbow admin panel. It is possible the grant only one application depending on needs.



When the Authorize action is performed, a Microsoft login is requested to grant needed permission. The Microsoft account should have enough right to allow them.



In Azure, the list of applications permission can be verified.



4 Permissions

The list of Azure's permission is given on the Microsoft support site: https://docs.microsoft.com/en-us/graph/permissions-reference

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

For each required permission, this document gives the name, a description, which kind of permission is required, 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 permit to access to some Rainbow services directly from Teams. To facilitate the user's authentication, Rainbow relies directly on Azure authentication to identity the user. To have access to the Azure's identity of the user, Rainbow asks for some identity's related permissions. Rainbow for Teams also permits to have a missed call notification in Team's activity section. Corresponding permissions are requested at application level.

Required authorizations are:

Id	**User.profile**
Name	View users' basic profile
Description	Allows the app to see your users' basic profile (e.g., name, picture, user name, email address)
Type	Delegated permission
Rainbow usage	Used by Rainbow to get language of the user.
Id	**OpenID.offline_access**
Name	Maintain access to data you have given it access to
Description	Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.
Type	Delegated permission
Id	**OpenID.email**
Name	View users' email address
Description	Allows the app to read your users' primary email address
Type	Delegated permission
Rainbow usage	Used by Rainbow to get do the link between Azure account and rainbow account. The key is the user's email.
Id	**OpenID.openid**
Name	Sign users in
Description	Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.
Type	Delegated permission
Rainbow usage	Used to signed in the User in Azure to allow other permissions.
Id	**User.Read**
Name	Sign in and read user profile
Description	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Type	Delegated permission
Rainbow usage	Used by Rainbow to let the user to sign in to Azure and allow other permissions
Id	**Contacts.Read**
Name	Read user contacts

Description	Allows the app to read contacts in your contact folders.
Type	Delegated permission
Rainbow usage	Used to propose a search in user's contacts from the Rainbow Teams tab.
Id	**TeamsActivity.Send**
Name	Send a teamwork activity to any user
Description	Allows the app to create new notifications in users' teamwork activity feeds without a signed in user. These notifications may not be discoverable or be held or governed by compliance policies.
Type	Application's permission
Rainbow usage	Used to display a notification in teams application when the user has a missed call or a new voicemail.
Id	**User.ReadBasic.All**
Name	Read all users' basic profiles
Description	Allows the app to read a basic set of profile properties of other users in your organization without a signed-in user. Includes display name, first and last name, email address, open extensions, and photo.
Type	Application's permission
Rainbow usage	Used to get the email of users to do the link between the Rainbow user having a missed call, and the associated Microsoft Teams user to display the activity notification.

API used are:

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

SDKs used are:

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

4.2 Calendar and Teams presence

Application ID: 96d01656-933b-43b3-b06b-abc61ce7bcb3

In Rainbow, it is possible to share the calendar state to other Rainbow users. They will see if someone is currently in a meeting or not and when it will finish. When a user is out of office, other user will see the state, the return date and the out-of-office message configured in Azure. Each Rainbow user is prompted to accept to share their calendar details. They can refuse it.

Users have also the possibility to synchronize his Teams presence with Rainbow. When user is Busy or DND in Teams, he will be seen as "DND Teams" on Rainbow. And when a User is DND or Busy in Rainbow, he will be seen as Busy in Teams.

Required authorizations are:

Id	**User.Read**

Name	Sign in and read user profile
Description	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Type	Delegated permission
Rainbow usage	Used by Rainbow to let the user to sign in to Azure and allow other permissions
Id	**Calendars.Read**
Name	Read user calendars
Description	Allows the app to read events in user calendars.
Type	Delegated permission
Rainbow usage	Rainbow uses the fact that the user is occupied or not and up to when. To show the calendar presence to other users of his network.
Id	**MailboxSettings.Read**
Name	Read user mailbox settings
Description	Allows the app to the read user's mailbox settings. Does not include permission to send mail.
Type	Delegated permission
Rainbow usage	Rainbow uses the mailbox settings to get the out of office state and the associated automatic reply message to display it to other contact of his network.
Id	**Presence.Read**
Name	Read user's presence information
Description	Allows the app to read your presence information on your behalf. Presence information includes activity, availability, status note, calendar out-of-office message, timezone and location.
Type	Delegated permission
Rainbow usage	Read Teams user's presence to display a DND status Rainbow side
Id	**Presence.Read.All**
Name	Read presence information of all users in your organization
Description	Allows the app to read presence information of all users in the directory on your behalf. Presence information includes activity, availability, status note, calendar out-of-office message, timezone and location.
Type	Delegated permission
Rainbow usage	Used by Rainbow to be notified when a user's presence change. The subscription API is only available using this permission for now. It is not possible to subscribe just for the user's own presence with the Presence.Read permission.
Id	**Presence.ReadWrite**
Name	Read and write a user's presence information
Description	Allows the app to read the presence information and write activity and availability on behalf of the signed-in user. Presence information includes activity, availability, status note, calendar out-of-office message, timezone and location.
Type	Delegated permission
Rainbow usage	Used by Rainbow to push to presence status from Rainbow to Teams. When a user is in a call or has configured his status to DND in Rainbow application, he will be seen as Busy in Teams.

API used are:

- 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/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

4.3 Single Sign On

Rainbow can leverage an external identity provider to allow users to login to Rainbow using their Azure credentials. These permissions are allowed by the Azure admin when it configures the SSO with Rainbow.

When based on SAML, Rainbow needs to have access to email address of the user to match the corresponding Rainbow account. On Azure, SAML authentication is not based on permissions. No specific permission is required once SSO in configured in Azure and email address is returned as a claim.

Required authorizations when SSO is based on OIDC are:

Id	**OpenID.openid**
Name	OpenID.openid
Description	Allows users to sign into the app with their work or school accounts and allows the app to see basic user profile information.
Type	Delegated permission
Rainbow usage	It is used to allow to sign-in using Azure.
Id	**OpenID.email**
Name	Read user mailbox settings
Description	Allows the app to read your users' primary email address.
Type	Delegated permission
Rainbow usage	The email profile is retrieved to read email address to match the Rainbow login of the associated account for OIDC authentication.

Endpoint used for OIDC:

- discoveryUrl (optional): https://login.microsoftonline.com/:tenantId/v2.0/.well-known/openid-configuration
- issuer: https://login.microsoftonline.com/:tenantId/v2.0
- jwksUri: https://login.microsoftonline.com/:tenantId/discovery/v2.0/keys
- authorizationEndpoint: https://login.microsoftonline.com/:tenantId/oauth2/v2.0/authorize
- tokenEndpoint: https://login.microsoftonline.com/:tenantId/oauth2/v2.0/token
- userinfoEndpoint (optional): https://graph.microsoft.com/oidc/userinfo

- endSessionEndpoint (optional): https://login.microsoftonline.com/:tenantId/oauth2/v2.0/logout

Endpoint used for SAML:

- loginUrl: https://login.microsoftonline.com/:tenatnId/saml2
- logoutUrl (optional): https://login.microsoftonline.com/:tenantId/saml2

4.4 Rainbow Provisioning

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

Rainbow can use the Azure directory to create Rainbow users (Mass provisioning) or Search. The administrator needs to link his Rainbow company with his Azure directory and accept required authorizations.

To link Rainbow and Azure, the admin need to allow some permissions:

Id	**User.Read**
Name	Sign in and read user profile
Description	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Type	Delegated permission
Rainbow usage	Used by Rainbow to let the administrator to sign in to Azure and link the Azure tenant with Rainbow by allowing the application to access to the directory.

API used by all services linked to directory application:

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

4.4.1 Mass provisioning

Rainbow can perform an import of user's account configured in Azure to create associated Rainbow accounts. To do that, the admin allows Rainbow to read the list of users in Azure thru the administrative part of Rainbow.

Id	**User.ReadAll**
Name	Read all users' full profiles
Description	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.
Type	Application permission, administrator's consent
Rainbow usage	Permit to retrieve details of account to create Rainbow side: name, email, phone numbers

API used for Mass provisioning:

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

4.4.2 Search

Once linked with Azure directory, Rainbow users can perform a search from Rainbow in the Azure directory to make a dial by name. The search permit to find Azure's company users and shared contacts.

Id	**User.ReadAll**
Name	Read all users' full profiles
Description	Allows the app to read the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user.
Type	Application permission, administrator's consent
Rainbow usage	Permit to make a search in the Azure directory of company's user from the Rainbow client to call him using his phone number.
Id	**Directory.ReadAll**
Name	Read directory data
Description	Allows the app to read data in your organization's directory, such as users, groups and apps.
Type	Application permission, administrator's consent
Rainbow usage	Permit to make a search in the Azure directory of shared contacts from the Rainbow client to call him using his phone number.

APIs used for directory search:

- 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 when relied on their calendar availability information configured in Azure. For each slot, details such as the probability of attendance of the requested users and their status (free, tentative, busy, out of office, out of day work, out of hour work and working elsewhere) will be highlighted. This functionality does not require users' permissions, but it only requires administrator's consent.

Id	**User.Read**
Name	**Sign in and read user profile**
Description	**Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.**
Type	**Delegated permission**
Rainbow usage	**Used by Rainbow to let the administrator to sign in to Azure and link the Azure tenant with Rainbow by allowing the application to access to the directory.**
Id	**Calendars.ReadWrite**
Name	Have full access to user calendars
Description	Allows the app to create, read, update, and delete events in user calendars.
Type	Application permission

Rainbow usage	Allows to get the availability information of each participant in a bubble in order to compute available slots. An event will then be created in each participant's calendar for a chosen slot.
Id	**MailboxSettings.Read**
Name	Read user mailbox settings
Description	Allows the app to the read user's mailbox settings. Does not include permission to send mail.
Type	Application permission
Rainbow usage	It is crucial to take into consideration the time zone of users when computing available slots. To do so, Rainbow can get a user's mailbox time zone setting.

APIs used for meeting scheduler:

- 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 Directory (deprecated)

Deprecated: This application is no more used when mass provisioning / directory search or Meeting scheduler are used. It is replaced by two applications to separate the Meeting scheduler and the directory management. This evolution is required to no longer require calendar permission needed by the Meeting scheduler, when only directory services are used.

This application is replaced by:

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

If the admin restarts the activation process from the Rainbow admin interface, the new applications will be used. This application will remain on Azure side, but no more used. The admin must remove is manually from the Azure admin application management interface.

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

Rainbow can use the Azure directory for several services. He needs to link his Rainbow company with his Azure directory and accept required authorizations.

To link Rainbow and Azure, the admin needs to allow some permissions:

Id	**User.Read**
Name	Sign in and read user profile
Description	Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Type	Delegated permission, administrator's consent
Rainbow usage	Used by Rainbow to let the administrator to sign in to Azure and link the Azure tenant with Rainbow by allowing the application to access to the directory.

API used by all services linked to directory application:

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

Directory application requires a set of permissions as described in corresponding chapter of the new corresponding applications.

End of Document