



ALCATEL-LUCENT RAINBOW™

Rainbow and Azure permissions

Ed 01

JULY 2020

Author: Cloud Services

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

©2020 ALE International. Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for a commercial purpose is prohibited unless prior permission is obtained from Alcatel-Lucent.

Alcatel-Lucent, OmniPCX, and OpenTouch and Rainbow are either registered trademarks or trademarks of Alcatel-Lucent.

All other trademarks are the property of their respective owners.

Contents

1	Abstract	4
2	History.....	4
3	Permissions	4
4	Calendar presence	4
5	Directory	5
5.1	Mass provisioning	6
5.2	Search	6
5.3	Meeting Scheduler.....	7
6	Contact invitation	7

1 Abstract

When linked to Azure, Rainbow requires a set of permissions to be able to render the right service. This document details which permission is required for which service and how Rainbow uses them.

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

- Calendar presence
- Single Sign On
- Mass Provisioning
- Directory search
- Contact invitation

2 History

Modifications	Date	Edition
Initial Revision	2020 / 07 / 28	Ed 01

3 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 Calendar presence

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 message configure in Azure. Each Rainbow user are prompted to accept to share their calendar details. They can refuse it.

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, user's consent
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, user's consent
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, user's consent
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	MailboxSettings.ReadWrite
Name	Read and write user mailbox settings
Description	Allows the app to create, read, update, and delete user's mailbox settings. Does not include permission to directly send mail but allows the app to create rules that can forward or redirect messages.
Type	Delegated permission, user's consent
Rainbow usage	Not documented by Azure but required to get the out of office state and the associated automatic reply message.

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 need 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 is 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, user's consent
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, user's consent
Rainbow usage	The email profile is retrieved to read email address to match the Rainbow login of the associated account for OIDC authentication.

5 Directory

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 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, 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.

5.1 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

5.2 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.

5.3 Meeting Scheduler

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	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, administrator's consent
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, administrator's consent
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.

6 Contact invitation

A user can invite his Azure contact to use Rainbow. To do that the user is prompt to share his directory with Rainbow and Rainbow will invite the list of selected contacts. This functionality is allowed depending on company privacy rules.

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, user's consent
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 user contacts.
Type	Delegated permission, user's consent
Rainbow usage	Used by Rainbow to propose a list of contact to invite and send a mail to selected ones.

End of Document