



TalentLink Smart Calendar – Outlook-OAuth & MS Teams Integration FAQs

November 2021

Login/Generic Account

- The app is registered on our side
- The customer needs to create a generic user account (for example: talentlink.calendar@customername.com)
- The generic user account should be a cloud user since we are using Microsoft API and thus we are calling the cloud services
- Regarding the OAuth method - OAuth2.0 is the only accepted auth method. We are using MS Graph API, and we are not able to use Azure AD Single Sign On.

Permissions

- This generic user accounts acts as a service principle so only for this specific calendar we will require the following access permissions:

1. *User.ReadBasic.All*

this allows us to see free/busy slots for each user via the generic user account

2. *Calendars.ReadWrite*

this allows us to create a web meeting event in the calendar.

These rights are displayed on the consent screen during oauth authorization.

For creating events we need Calendars.ReadWrite permission

What does this permission mean: access to the calendar for the generic user account

part of our consent screen:

This app would like to:

✓ Read all users' basic profiles

✓ Have full access to your calendars

considering the above, we never ask for access to other users calendars

description for creating event:

<https://docs.microsoft.com/en-us/graph/api/user-post-events?view=graph-rest-1.0&tabs=http>

description what "Calendars.ReadWrite" means: (it is for the user's calendar, not for all users)

<https://docs.microsoft.com/en-us/graph/api/calendar-get?view=graph-rest-1.0&tabs=http>

description why admin needs to grant consent:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?tabs=azure-portal>

What is the additional account used for and how it will work?

The additional account in Azure is required, because we are using it to communicate with MS Graph API on behalf of this user. The generic user account should be a cloud user since we are using Microsoft API and thus we are calling the cloud services
OAuth2.0 is the only accepted auth method. We are using MS Graph API, and we are not able to use Azure AD Single Sign On.

The customer can setup a non admin account with password expiration (optional)
The customer needs to create a service principle.
The app is registered on our side

The license required for the additional account can be any license that allows Exchange Online. (We – CSOD - set this up for our demo system using an O365 E5 license)

When Talentlink makes the API Call will it be coming from a particular subnet?

Yes, it will be from our subnet.

Is MFA (multi factor authorisation) applicable for the integration?

MFA is not necessarily required after successful authorization since we are using OAuth2.

However, if you want to use MFA this can be configured on the customer's side and our smartcalendar IP can be whitelisted - which is {"ip":"18.196.234.76"}

I am the GSA and I cannot approve the authorization?

Due to the company's IT security policy it may be the case that someone from IT or the Azure administrator has to approve the integrations

This can be done in two ways:

- 1) Directly in Azure via the administrator
- 2) Someone from IT with the rights to approve the integration can get a (temporary) user access to Talentlink. Only one role is required called "Administration only"

Then you need to go to Settings > Company Configuration > Smart Meeting Configuration
> Select the integration connection or create a new one with the login (which is the name of the generic user account) and click on "OAUTH Authorization & Save"

The authorization has been approved but I still cannot see any free/busy slots?

- 1) Make sure your mailbox is not inactive, soft-deleted, or is hosted on-premise
- 2) If you are having a hybrid setup of Microsoft 365 with an on-premise exchange server, please look at hybrid-rest-support once if you are not missing anything
- 3) Check if a license may not be activated for this account