Connecting People.ai and Microsoft 365

Marc Spilka
1 month ago Updated

Follow

Overview

Onboarding new users can be cumbersome when managing each user's access individually. Users must go through the process of accepting invites to the platform and authenticating with their individual accounts before they are granted access. People.ai Team Access makes it possible for administrators to get their team set up seamlessly, with no effort from the end-user.

Team Access directly connects to the team's Microsoft 365 account, allowing administrators to get everyone onboard in People.ai in the background. Administrators can specify who has access to People.ai and whose activities are captured and analyzed, directly from their Microsoft admin panel.

For the companies running Microsoft, People.ai uses Microsoft's Graph API. It is ideal for large, enterprise-grade organizations that want to onboard and manage all users at once. With the flick of a switch, People.ai can access the records of all users within a company. Additionally, with application access, it is more likely that all user data will be available at any given time (as opposed to User-Driven Access). This approach is extremely convenient but requires an administrative account to authorize access to all mailboxes in the company.

Graph API is a powerful REST API that gives access to all cloud resources in a unified way on either a user or organizational basis, depending on the consent provided.

For application access, the administrator of Microsoft 365 must authorize access to People.ai using the OAuth 2.0 authorization form on Microsoft's website. People.ai will never have access to the administrator's credentials but instead receives an authentication token valid to operate on behalf of the user.

During the integration process, the Microsoft 365 admin will be asked to consent to the following permissions:

Admin consent | User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph					
Microsoft Graph	Calendars.Read	Read calendars in all mailboxes	Application	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Application	Admin consent	An administrator
Microsoft Graph	Mail.Read	Read mail in all mailboxes	Application	Admin consent	An administrator
Microsoft Graph	Contacts.Read	Read contacts in all mailboxes	Application	Admin consent	An administrator

People.ai doesn't require write access to any resources, however, the above permissions are mandatory for application access. By default, People.ai will have access to **all** the organization mailboxes and calendars. Microsoft 365 admin can change this behavior before or after completing the above steps. The process is outlined in the next paragraph.

Setting up Team Access using MS Graph API

The process of setting up Team Access is simple and does not require Microsoft 365 admin to log into the app. Please follow these steps to set up the integration:

1. Limit People.ai application access to certain users.

This way, you can limit the users' scope **before** installing the People.ai Azure Application.

To limit the People.ai application access to a specific set of mailboxes, use the **New-ApplicationAccessPolicy** PowerShell cmdlet to configure access control (see Microsoft's documentation).

Follow these instructions to create a new application access policy to apply to the new security group.

1. First, create a **mail-enabled security group.** You will create a restrictive policy that prevents P.ai access to any mailbox not within this security group.
2. Next, connect to Exchange Online PowerShell. For details, see Connect to Exchange Online PowerShell.
3. The following script will be utilized in order to limit People.ai's access to the mail-enabled security group before installation of the Azure application.
4. Create an application access policy.
   Run the following command, replacing the PolicyScopeGroupId, and Description arguments with your **mail-enabled security group** information.

   ```
   New-ApplicationAccessPolicy \
   -AppId 6135b4c8-8900-475f-84db-b8ee65fbb329 -PolicyScopeGroupId EvenUsers@
   -AccessRight RestrictAccess \
   -Description "Restrict this app to members of distribution group EvenUsers
   ```

5. Test the newly created application access policy:

   ```
   Test-ApplicationAccessPolicy -Identity user1@contoso.com -AppId6135b4c8-89
   ```

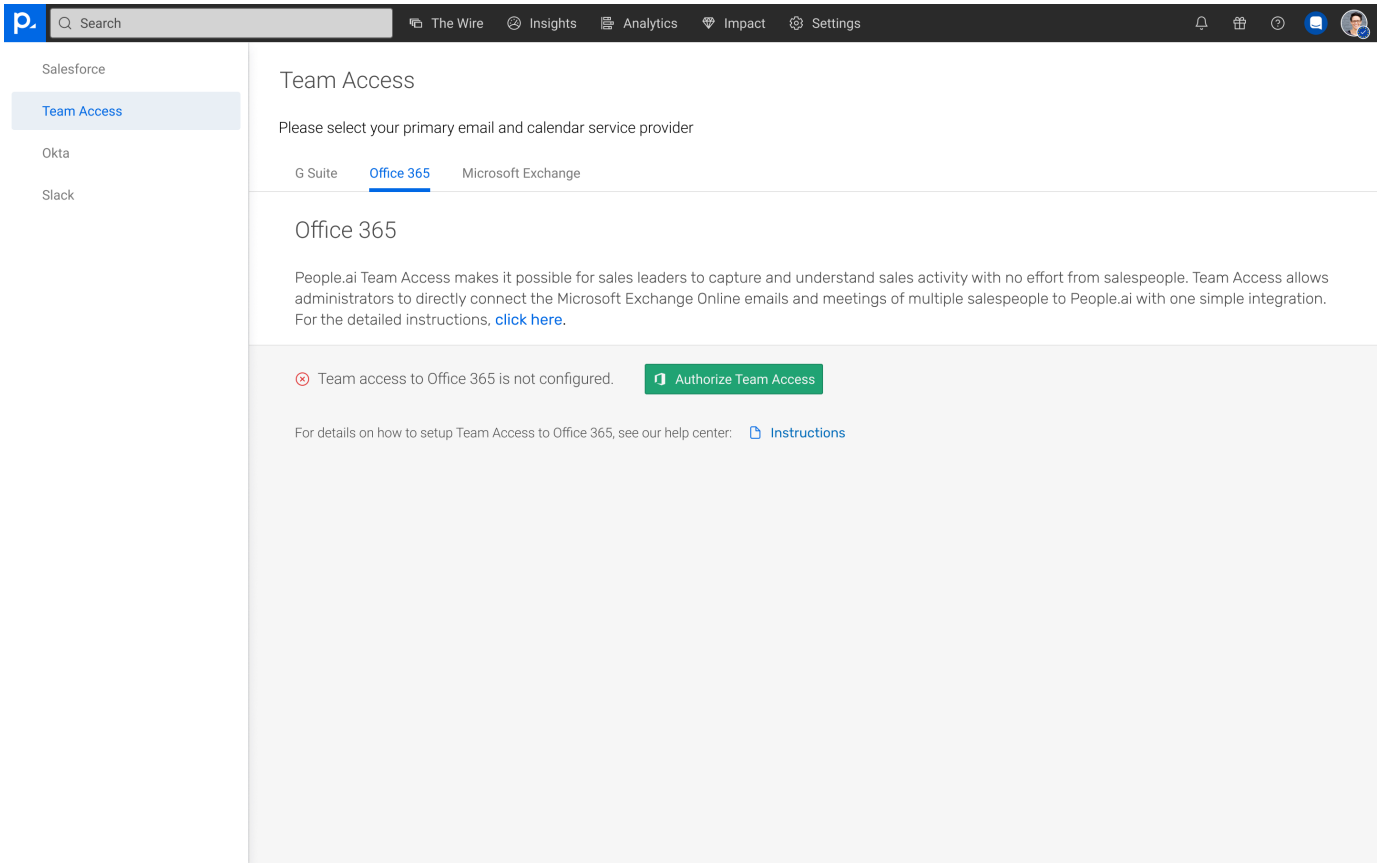
   The output of this command will indicate whether the app has access to User1's mailbox.

Please note: Changes to application access policies can take up to 30 minutes to take effect in Microsoft Graph REST API calls.

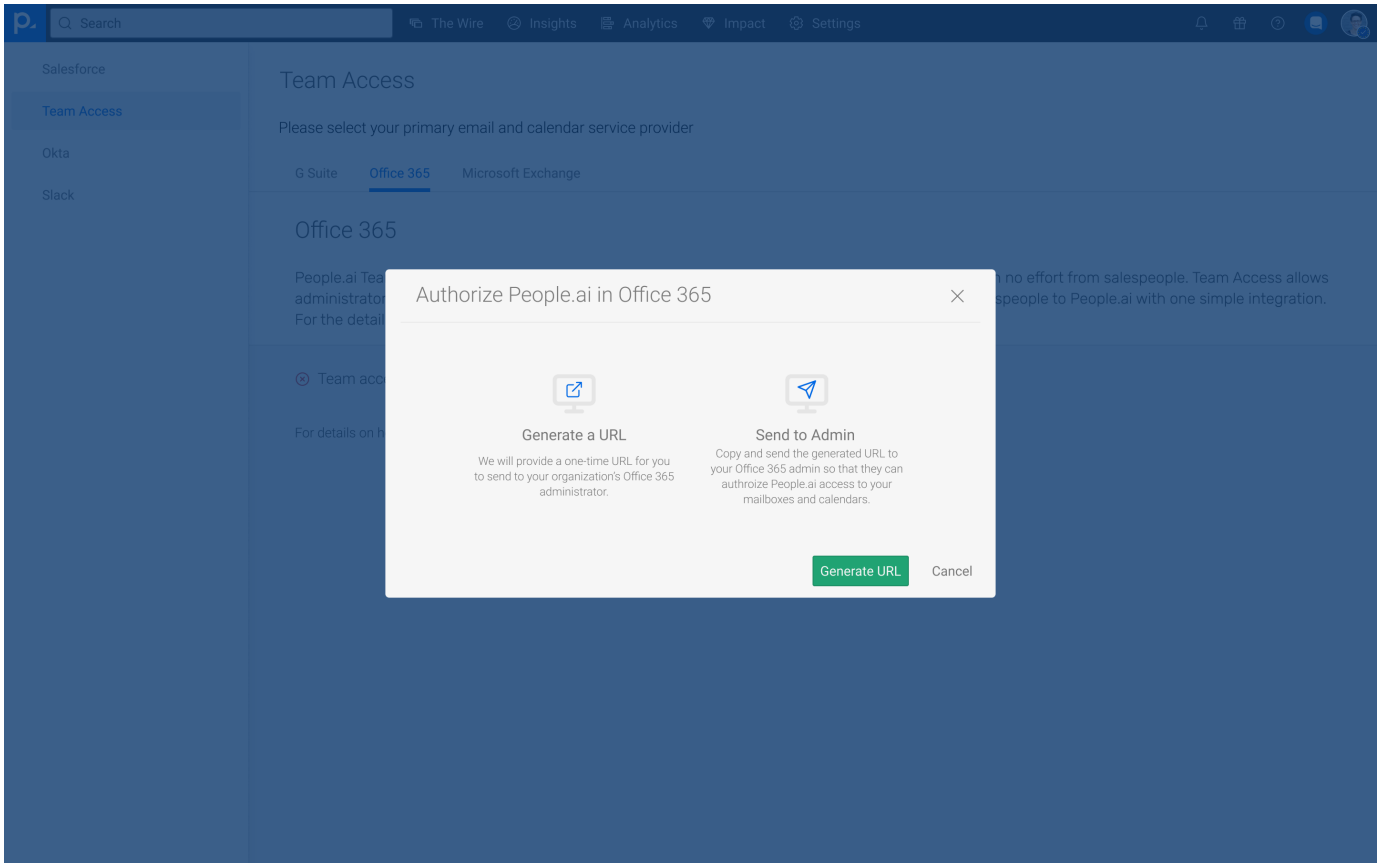
You can further limit the specific access permissions, though it is unnecessary because of the scoping in OAuth. To do so, see Supported permissions and additional resources.

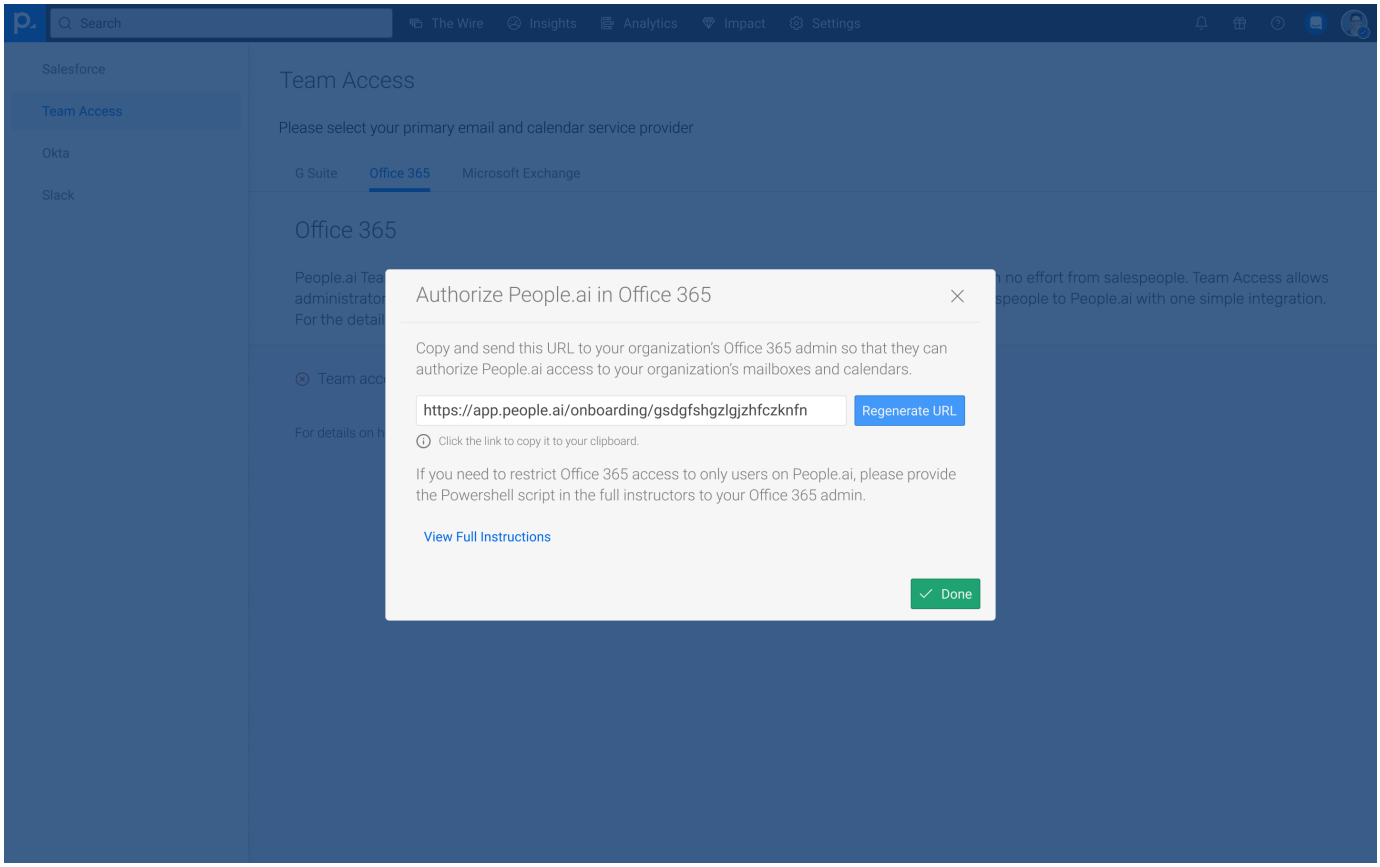
2. Give the People.ai app access to Microsoft 365

1. Log into People.ai as the application administrator.
2. Go to **Settings -> Integration -> Team Access** page and switch to **Office 365** tab:



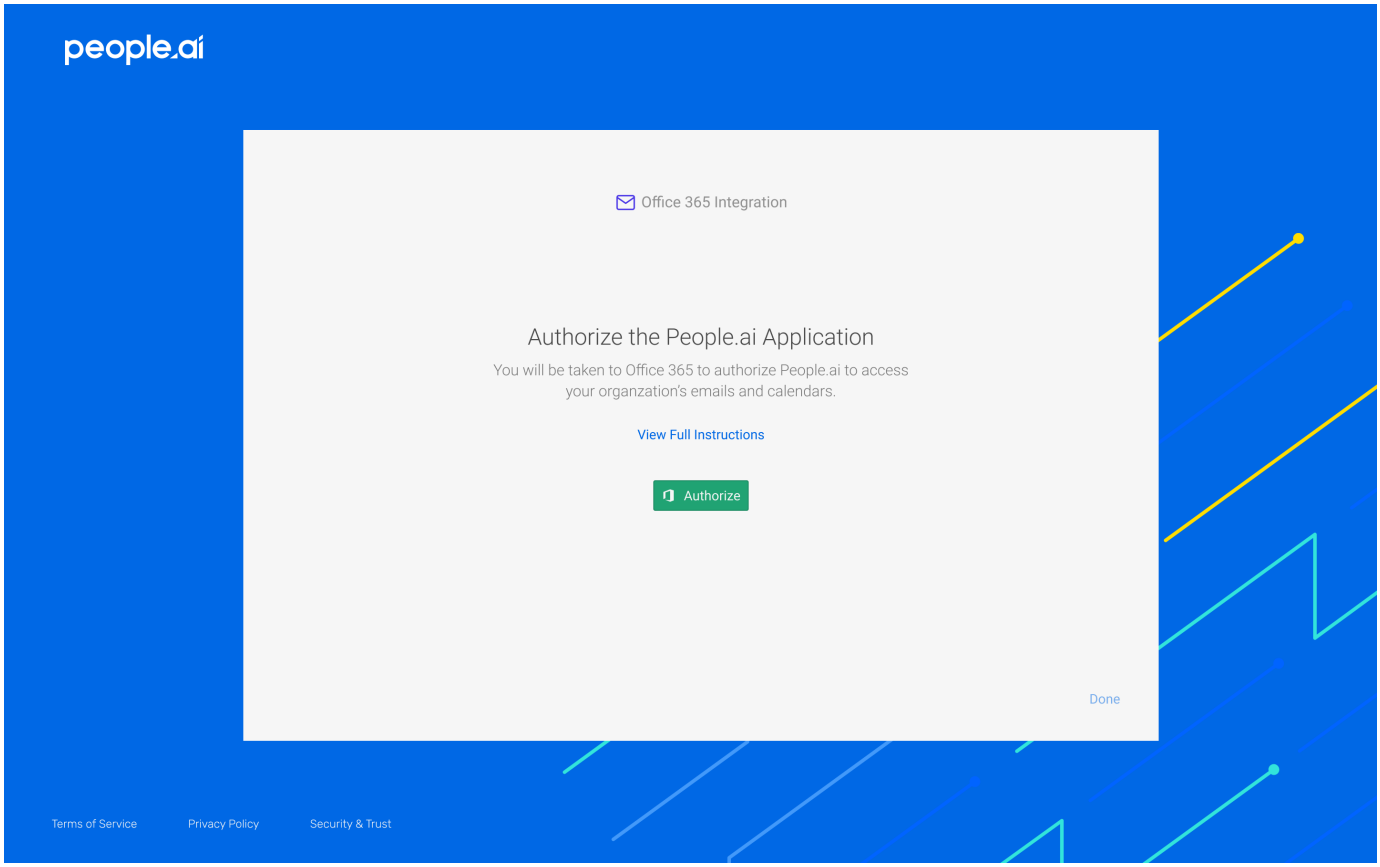
3. Click on Authorize Team Access button and generate the consent URL:

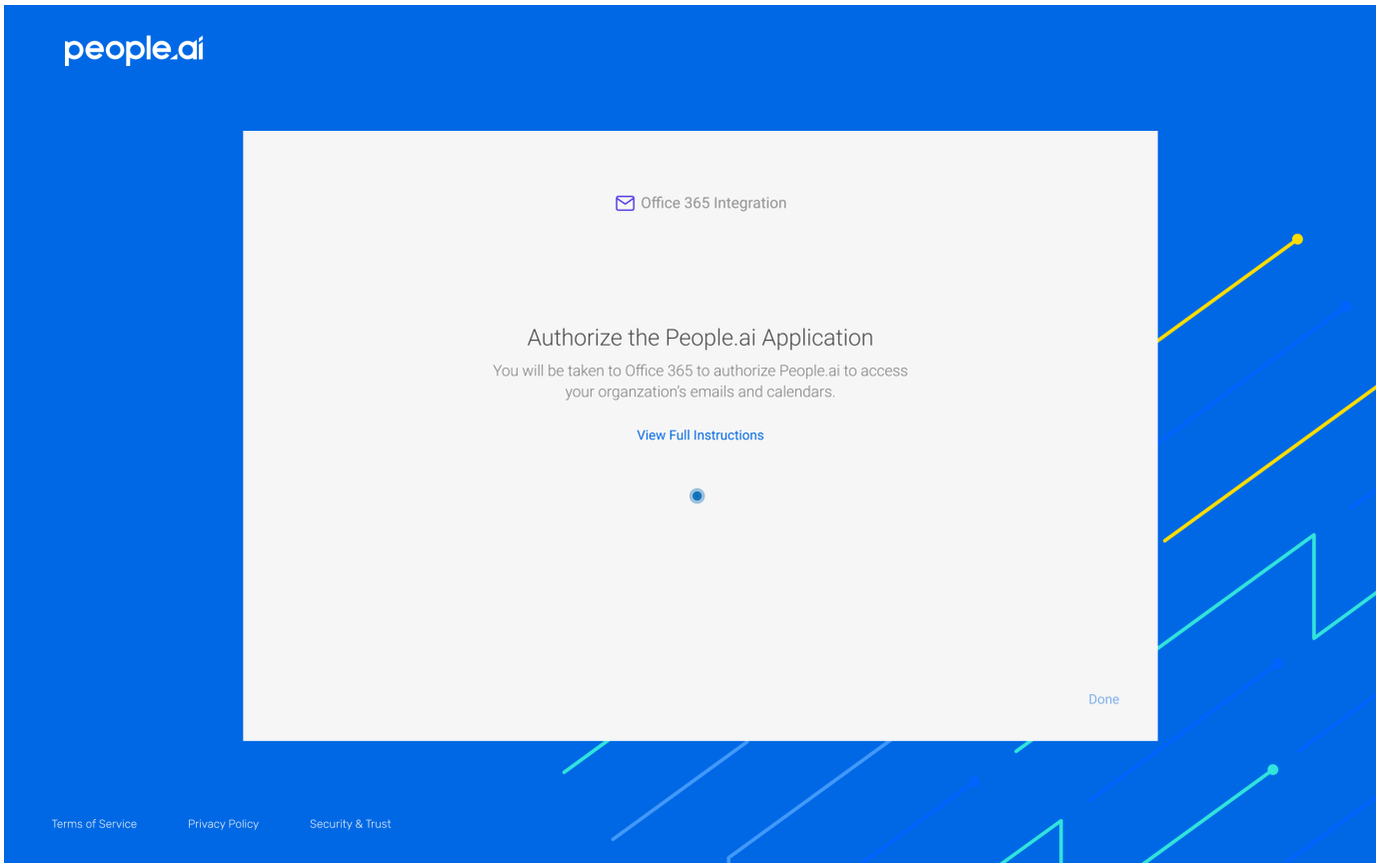


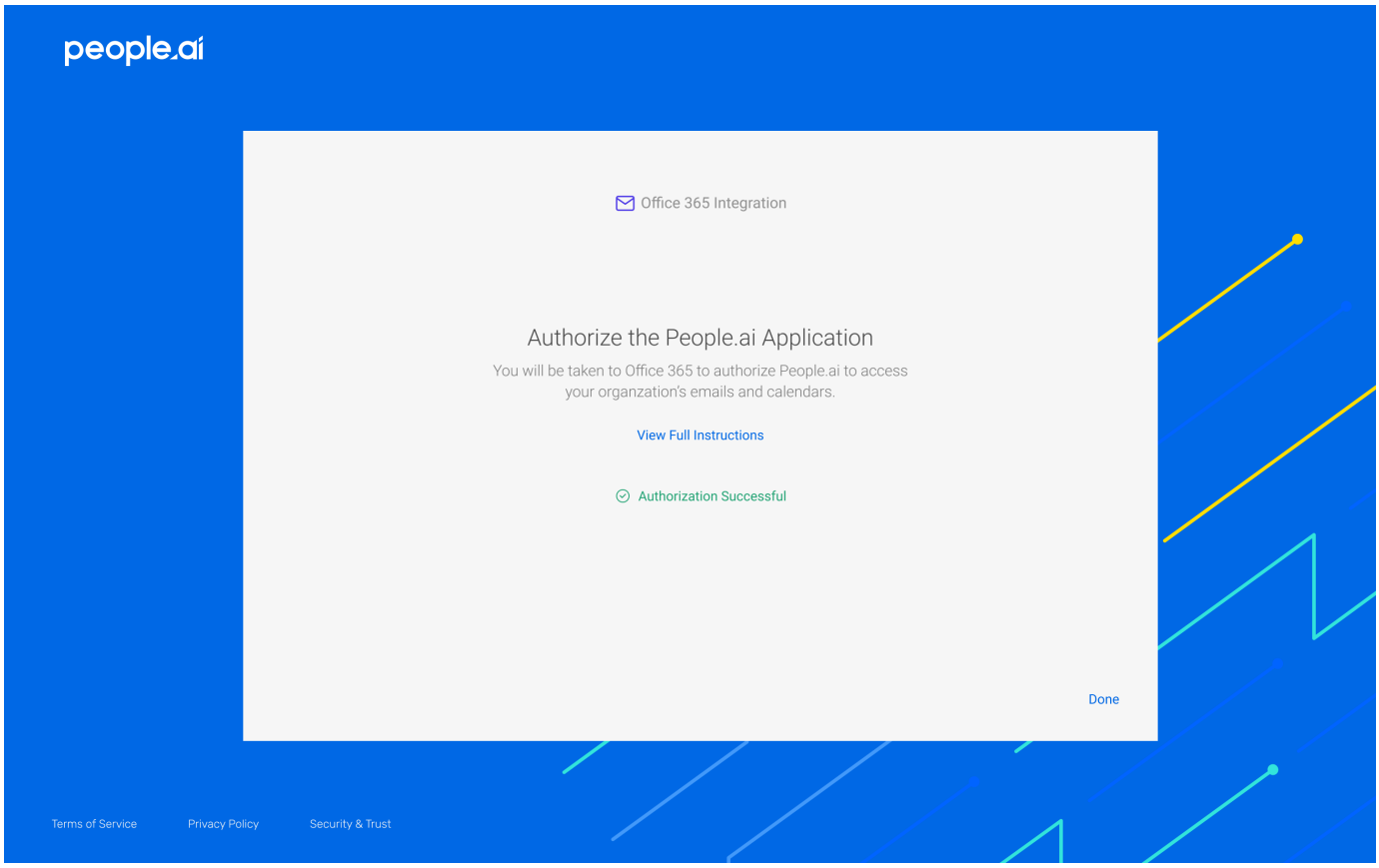


4. Send the generated URL to your organizations' Microsoft 365 administrator

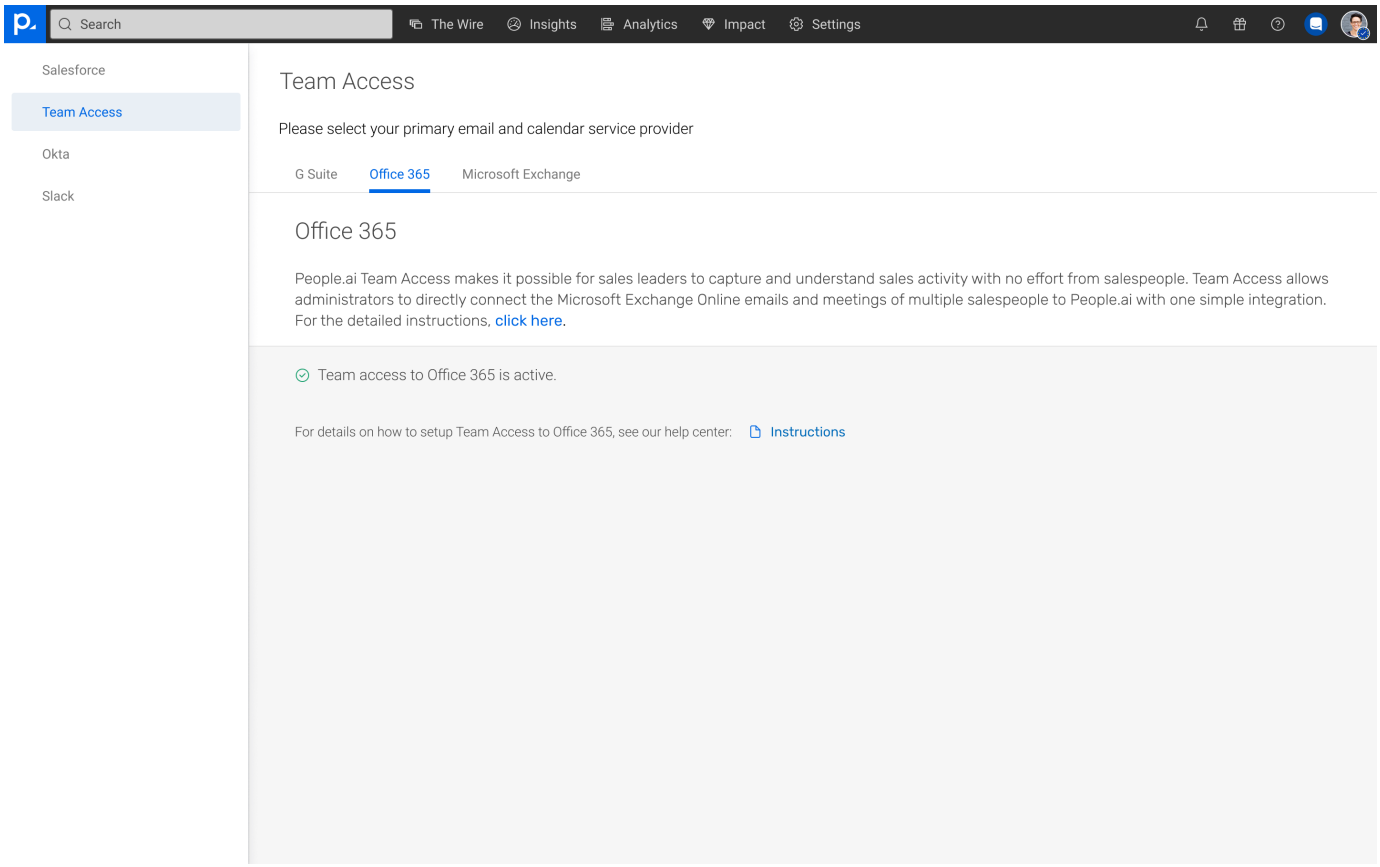
5. The Microsoft 365 administrator should log in to Microsoft 365 and follow the URL to grant permissions:







6. After successfully completing this flow, the People.ai administrator should see that Team Access is active:



Troubleshooting Tips to Consider

- Some organizations use customized authorization flows instead of the standard Microsoft 365 Single sign-on. In that case, the Microsoft 365 administrator may need to log into People.ai first to make it possible for the other users to log into People.ai.