PeopleFluent Learning

Microsoft Teams Integration Guide

Contents

About this Document

Introduction

This document describes how to configure Microsoft Office 365 to integrate Microsoft Teams with PeopleFluent Learning. Microsoft Teams integration enables LMS system administrators to set up virtual classroom accounts for Teams so that learners can launch courses from the LMS that are delivered via Teams events.

Microsoft Teams integration is available with PeopleFluent-hosted (SaaS) customers with the Learning License only.

Document Information

Revision Information	
Revision Date:	October 30, 2025
Revised Document Version Number:	3.0
Details of Revision:	Updated content to reflect changes to Microsoft 365.

Microsoft Office 365 Set Up

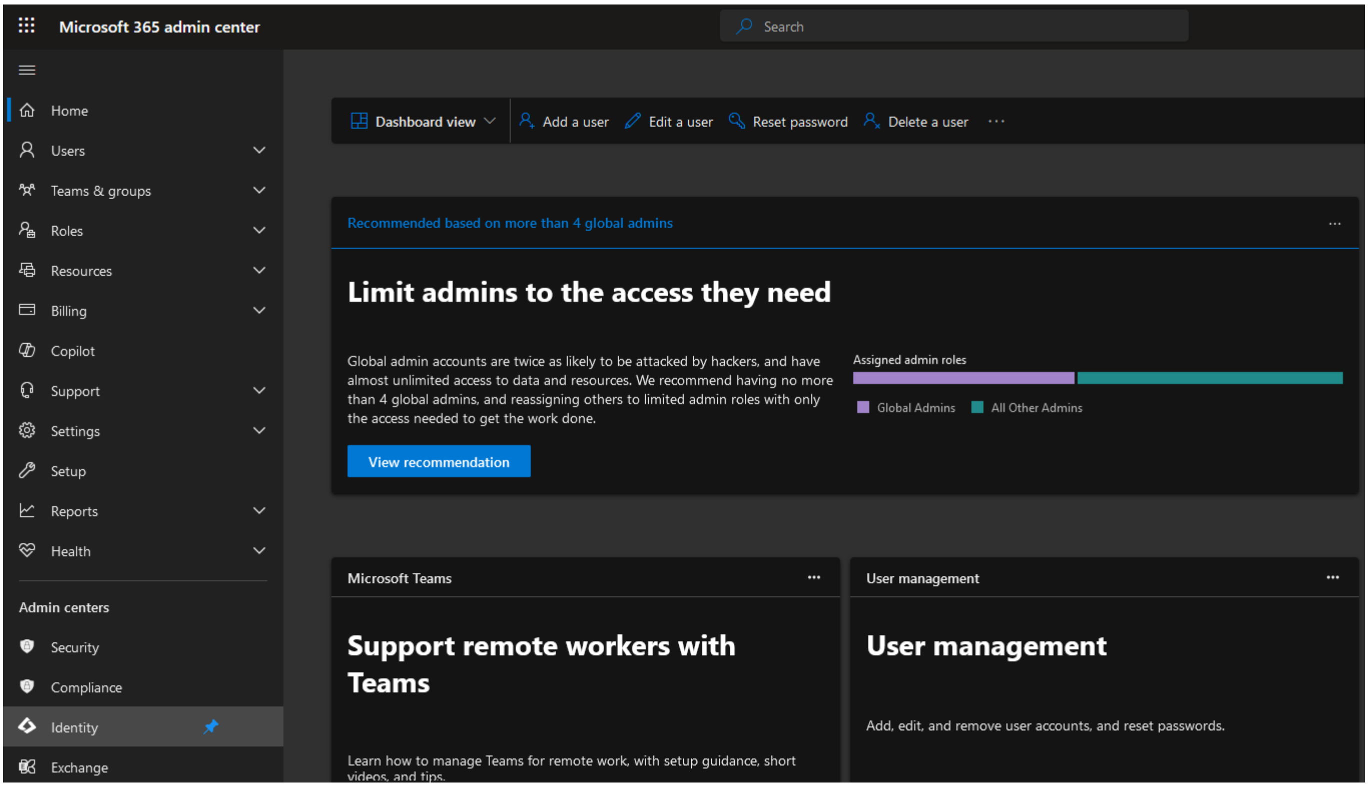
The following steps may need to be completed by whomever administers the Microsoft Office 365 accounts. Three pieces of information will be needed in the LMS, and these are noted on steps 9 and 14 below. Also, there is a URL from the LMS required on Step 7.

Register the Application in Azure Active Directory

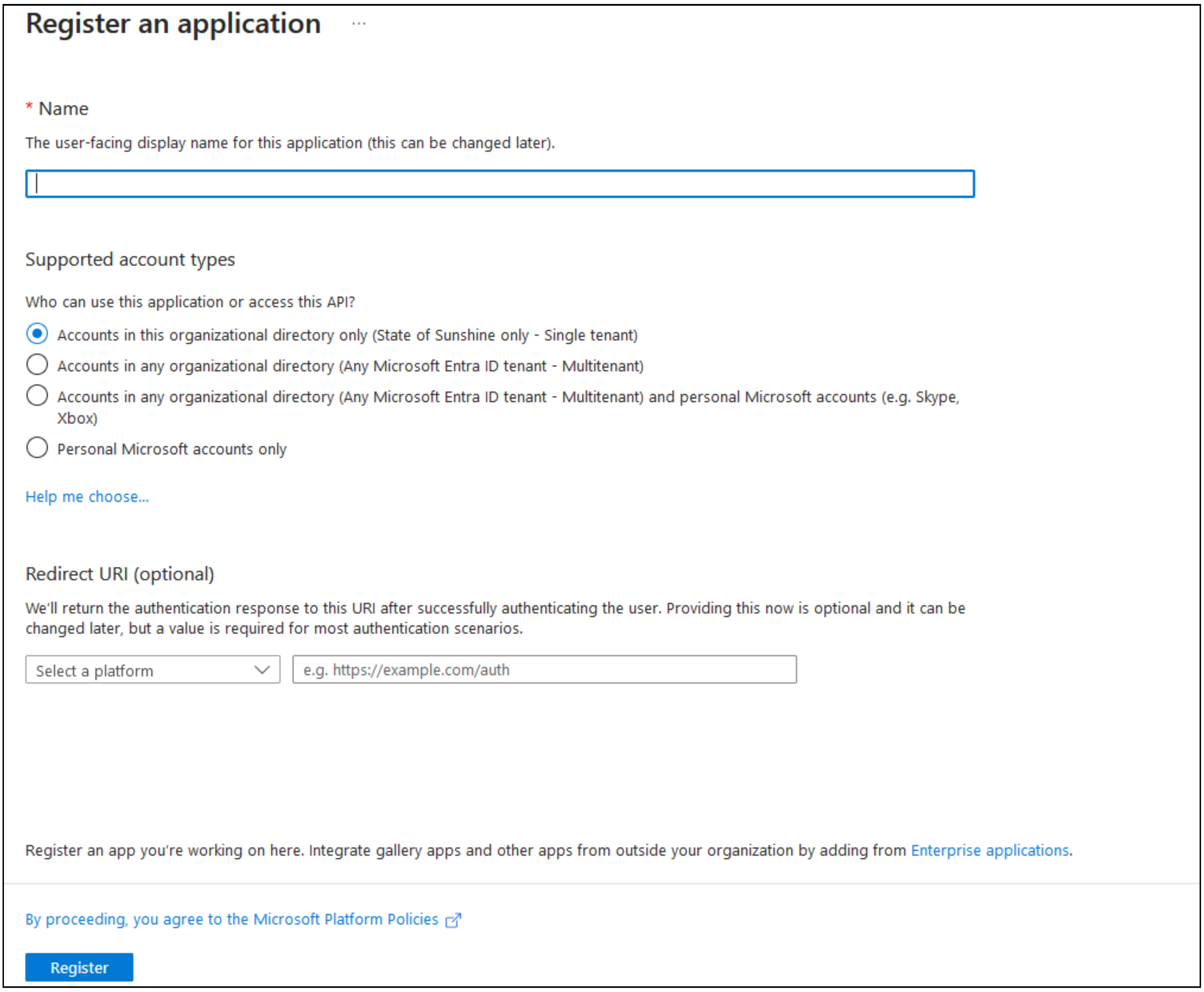
While this only needs to take place once, it is possible to create multiple "applications" in Azure Active Directory. This will be necessary for customers who have test and production LMS sites.

To register the application in Azure Active Directory:

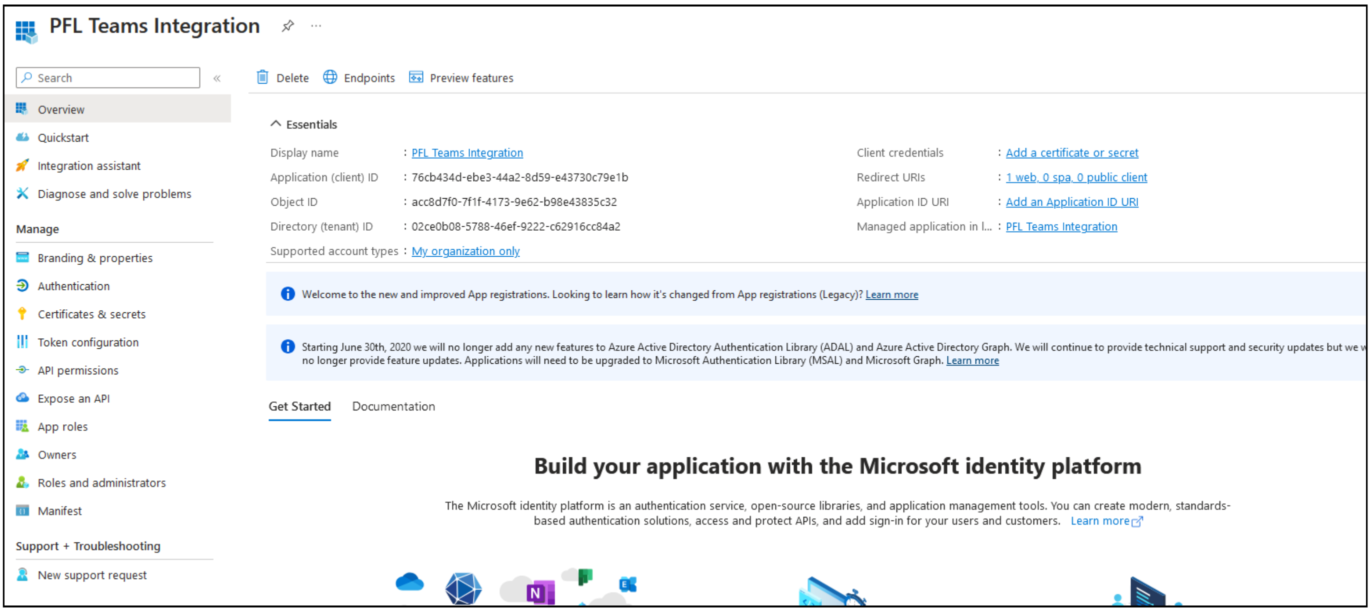
1. Log in to the Office 365 Admin Portal https://portal.office.com/adminportal/home?#/homepage.
2. On the left side, under Admin Centers, select **Identity**. The Microsoft Entra admin center opens in a new tab or window.



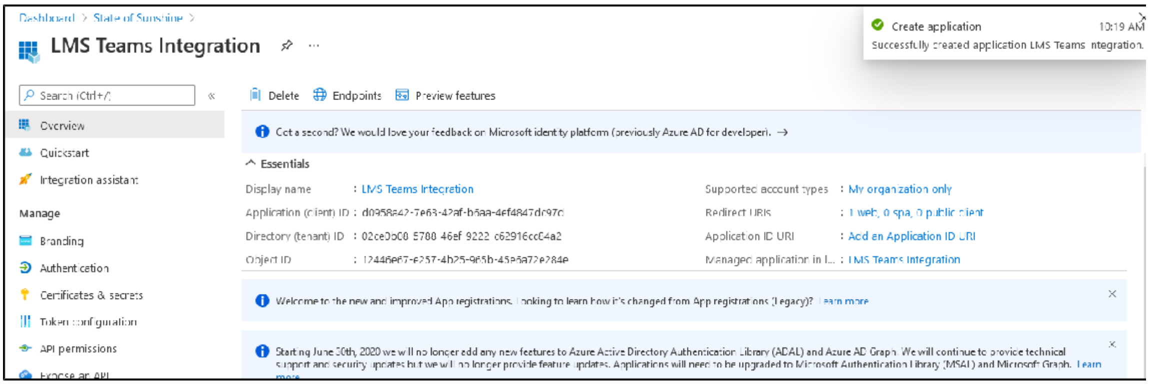
3. In the Microsoft Entra admin center, select **Identity** in the left menu.
4. Select **Applications** then **App Registrations**.
5. Select **+ New Registration**.



6. Enter a name for the Application. This can be anything, but should reflect the LMS (for example, LMS Teams Integration or something similar).
7. Select **Web** and enter the Redirect URL in the following format: http{s}://{customer.domain}/{instance}/servlet/ekp/TEAMSPROCESSOR. {customer.domain} is the full domain for the LMS (customer.netdimensions.com) while {instance} is the second part of the URL (default is "ekp" but this is often changed for customers. This can also be found in your LMS under **Manage Center > Learning > Virtual Classroom Account Setup > + Create new > Select Microsoft Teams**.

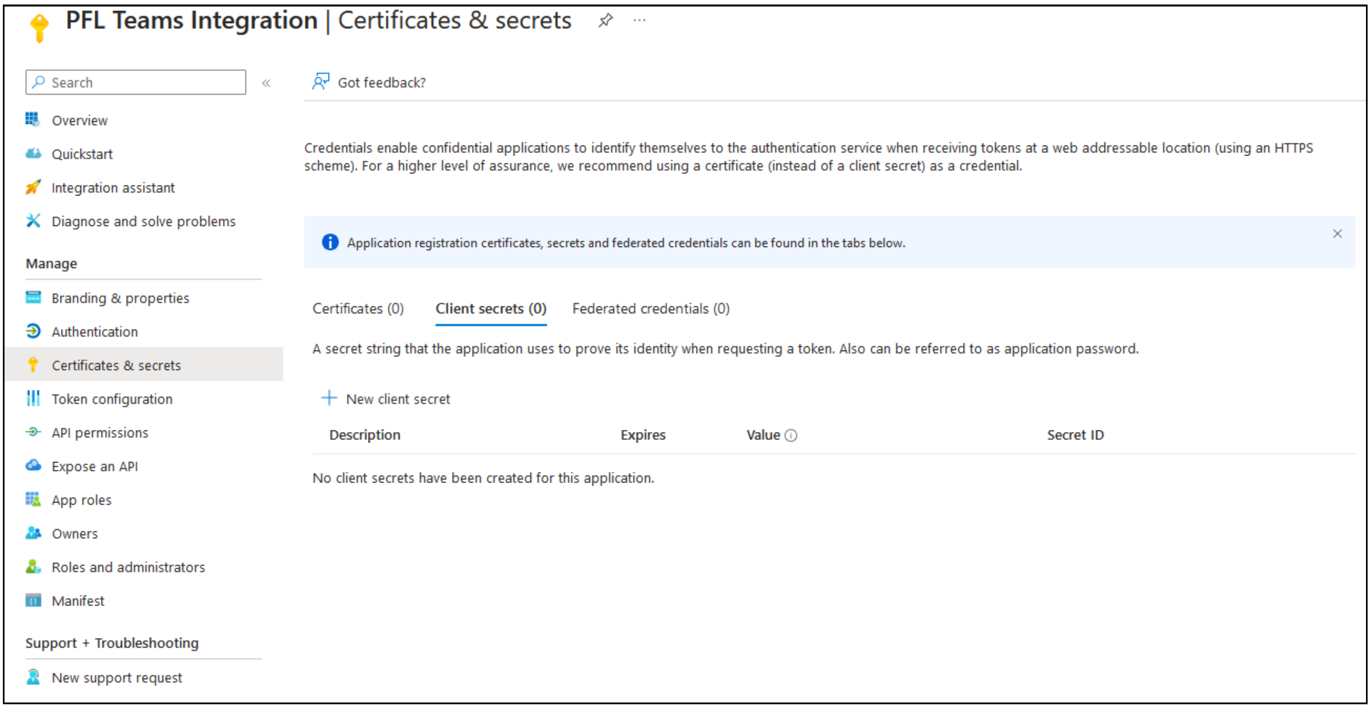


8. If not already open, open the App registration page.

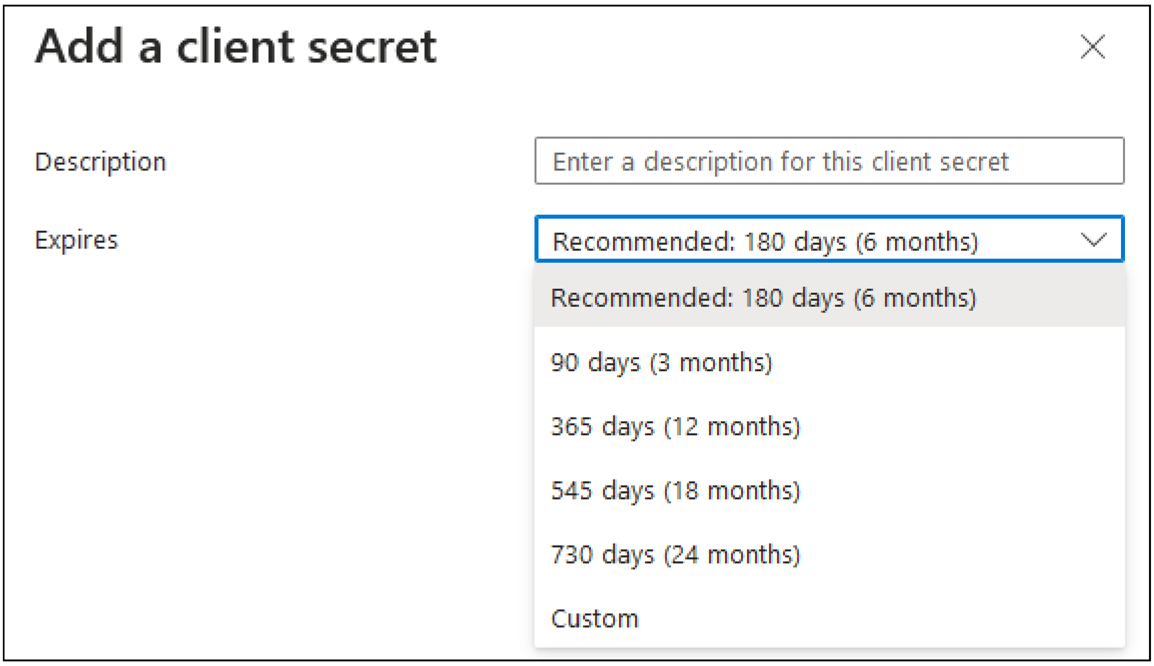


9. Copy the *Application (client) ID* and the *Directory (tenant) ID*. These values are needed as part of the Virtual Classroom Account Setup (see below) fields, *Client ID* and *Tenant ID*.

10. Select **Certificates & secrets** from the Manage menu on the left.



11. At the bottom, click **+ New client sec**.



12. Description is optional. Select an option to specify if or when the secret expires. Note that if the secret expires, a new secret will need to be created.
13. Click **Add**.

14. Copy the **Value** of the secret you just created, not the ID. The client secret value is needed as part of the Virtual Classroom Account Setup below.

Set API Permissions

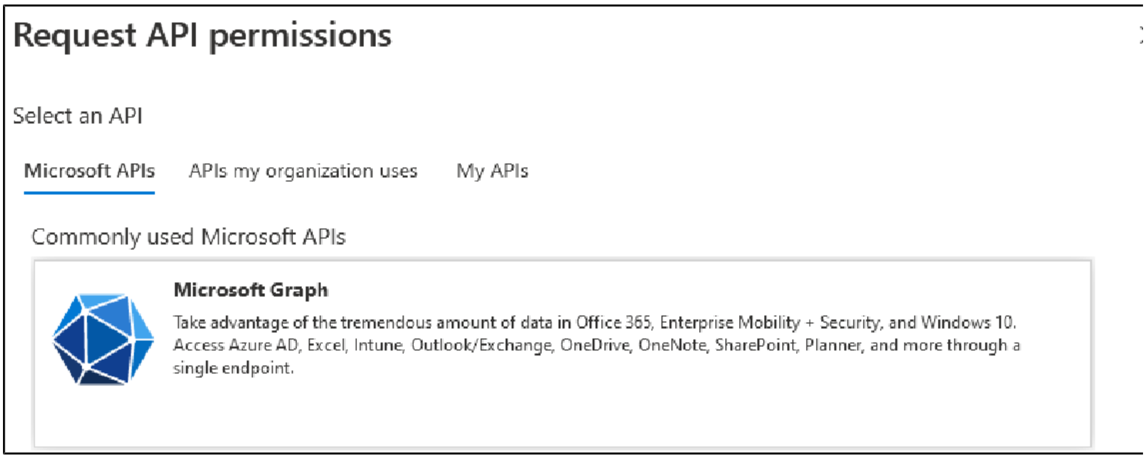
Virtual Classroom

You will need to set the following API permissions:

- **OnlineMeetings.ReadWrite** - Grants full access (read and create/update) to online meetings that the signed-in user organizes. It allows the ability to read existing meetings the user has scheduled, create new online meetings, update meeting details (time, participants, etc.) and delete meetings.
- **OnlineMeetingArtifact.Read.All** - Grants read access to meeting artifacts across all users in the tenant, which is used for attendance reports.
- **offline_access** - Grants access to a refresh token in addition to the access token. An access token usually expires within an hour, however a refresh token can be used without requiring re-authorization.

To set the API permissions

1. In the App Registrations page for the app, click the **API Permissions** link under Manage.
2. Click **Add a permission**. When the options appear, select **Microsoft Graph**.



3. Select **Delegated Permissions**.
4. Scroll down (or search) to locate and select the parameters specified above.

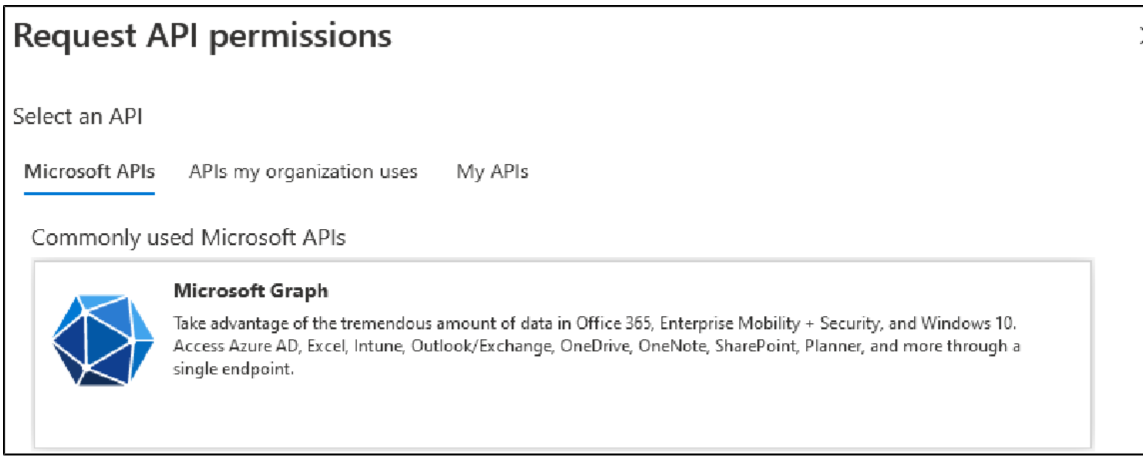
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted fo
OnlineMeetingArtifact.Read.A	Delegated	Read user's online meeting artifacts	No	Granted fo
OnlineMeetings.ReadWrite	Delegated	Read and create user's online meetings	No	Granted fo

Notifications

- **Chat.Create** — Allows an app to create new one-on-one or group chats on behalf of a user.
- **Chat.ReadWrite** — Grants full read and write access to all chats the signed-in user is a member of, including sending and editing messages.
- **Chat.ReadWrite.All** — Allows an app to read and write all chat content in the organization, regardless of membership.
- **ChatMember.ReadWrite.All** — Enables an app to add, remove, or update members in any chat across the organization.
- **ChatMessage.Send** — Permits an app to send messages in any chat the signed-in user can access.
- **TeamsAppInstallation.ReadForUser** — Lets an app read which Teams apps are installed for the signed-in user.
- **User.Read.All** — Allows reading of basic profile information for all users in the organization.

To set the API permissions:

1. In the App Registrations page for the app, click the **API Permissions** link under Manage.
2. Click **Add a permission**. When the options appear, select **Microsoft Graph**.



3. Select **Delegated Permissions**.

4. Scroll down (or search) to locate and select the parameters specified above.

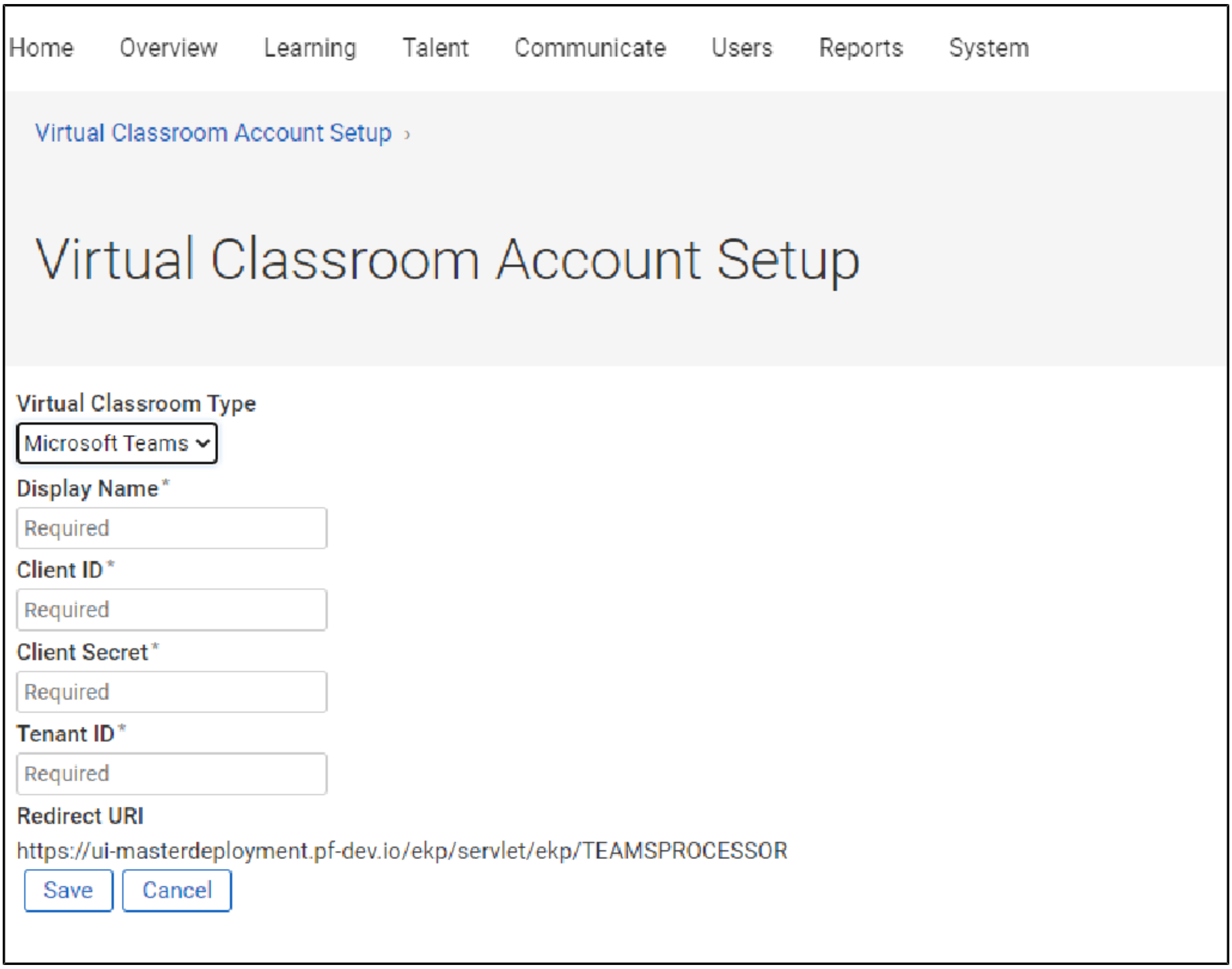
Microsoft Graph (7)				
Chat.Create	Delegated	Create chats	No	Granted for
Chat.ReadWrite	Delegated	Read and write user chat messages	No	Granted for
Chat.ReadWrite.All	Application	Read and write all chat messages	Yes	Granted for
ChatMember.ReadWrite.All	Application	Add and remove members from all chats	Yes	Granted for
ChatMessage.Send	Delegated	Send user chat messages	No	Granted for
TeamsAppInstallation.ReadFo	Delegated	Read user's installed Teams apps	No	Granted for
User.Read.All	Application	Read all users' full profiles	Yes	Granted for

Once the information above is set up, everything else is done within the LMS. It is up to each customer how many Applications to register in Azure Active Directory. Only one is needed per LMS site because of the Redirect URL in Step 7.

LMS Set Up

Virtual Classroom Account Set Up

To set up a Microsoft Teams Virtual Classroom Account, go to **Manage Center > Learning > Catalog General Settings > Virtual Classroom Account Setup**. Accounts can be created, edited or deleted.



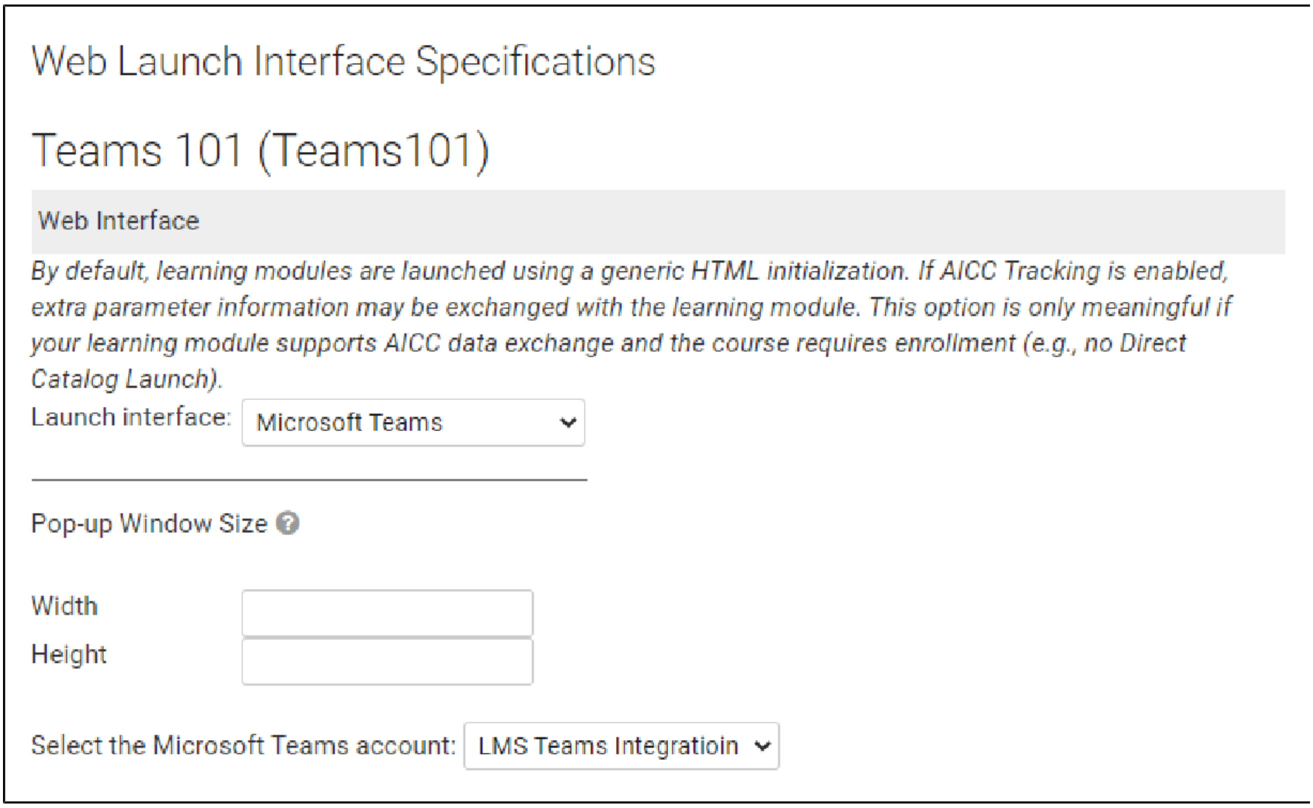
For Microsoft Teams, the entries are:

- **Display Name** - This is used in the LMS to display the account. It is used when creating a Virtual Classroom Session.
- **Client ID** - This is the client id created in Azure Active Directory above (step 9).
- **Client Secret** - This is client secret created in Azure Active Directory above (step 14).
- **Tenant ID** - This is the tenant id created in Azure Active Directory above (step 9).

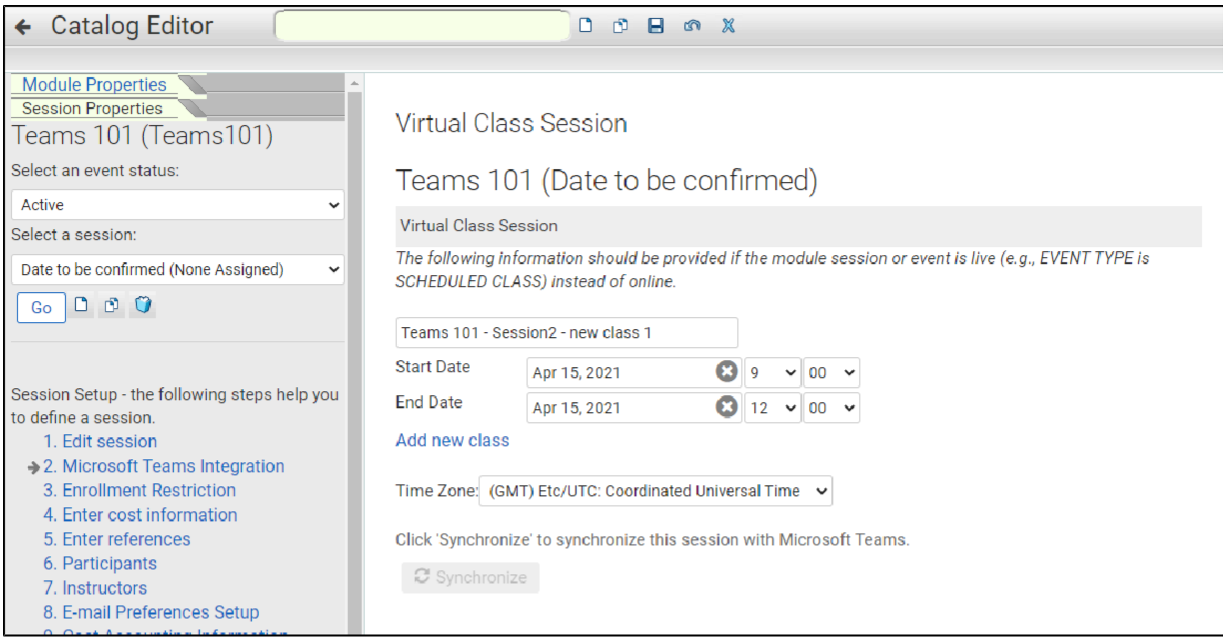
Enter the values and click **Save**.

Create Virtual Classroom Module

1. Go to **Manage Center > Learning > Create Learning Module**. In the Catalog Editor, select Virtual Classroom and enter a Module ID.
2. To designate the Teams account, go to **4.1 Define Launch Properties** and select **Microsoft Teams** and then select the Microsoft Teams account as set up above. There can be more than one account.



3. Once the Launch Interface is designated, create a session and go to **2. Microsoft Teams Integration**.



4. Give the class a title and designate the dates and times. Additional classes can be added here.
5. Click the **Save** icon in the header. After saving, the Synchronize button is activated.
6. The logged in administrator will authorize the integration by logging into the Office 365 account (it not already logged in). This step may be repeated depending on the time between creating sessions. This is required for the application to integrate.

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="ekp.example.com">
      <Path name="ekp/servlet/ekp/remoteUserAuthenticator"
requireSession="true" authType="shibboleth"/>
    </Host>
  </RequestMap>
</RequestMapper>
```

```
<Location /ekp/servlet/ekp/remoteUserAuthenticator>
 AuthType shibboleth
 ShibRequestSetting requireSession 1
 require valid-user
</Location>
```

7. After this step, click Synchronize again. The Copy Join URL button appears. This can be populated into communications if necessary. This will also be the URL enrolled learners will see after clicking Launch from their Current Courses (Current Enrollments).

Notification Set Up

MS Teams Configuration on the Organization Level

> The Microsoft application used for notifications can be the same application used for virtual classrooms.

Users who have Unrestricted access to the **Microsoft Teams Application Configuration** permission can create and manage configurations.

Create a New Configuration

1. Go to **Manage Center > Users > User Manager > Microsoft Teams Application Configuration**.
2. Click **+ Create Microsoft Teams Application**.
3. Configure the fields:

> You will need the MS Teams Application Client ID, Client Secret and Tenant ID to complete this task. Have this information handy.

- **Name** - enter a name for the application. This text will be displayed to users to select an application in the user profile.
- **Description (optional)** - enter a description.
- **Application Client ID** - enter the Client ID.
- **Application Client Secret** - enter the Client Secret.
- **Application Tenant ID** - enter the Application Tenant ID.

4. The application is active by default. Clear the **Active** field if you do not want it to be active immediately.
5. Click **Save**.

Set User-Specific Access Permissions

You can assign permissions to specific users, user groups, roles and more allowing them to access an application configuration.

1. On the Microsoft Teams Application Configuration page, locate the appropriate option and take one of the following actions.
   - Click the action menu and select **Permissions**.
   - Click the action menu and select **Edit** and then click the **Permissions** button.
2. Configure the permissions as necessary.
   - **Read Only** allows view-only access to the configuration.
   - **Unrestricted** further allows the user to update permissions, update and delete the configuration.
3. Click **Save**.

Delete a Configuration

To delete a configuration, locate the appropriate option and take one of the following actions:

- Click the action menu and select **Delete**.
- Click the action menu and select **Edit** and then click the **Delete** button.

> Configurations that are currently in use can't be deleted.

Set Up MS Team Notifications in another User's Profile

> In order to set up notifications in your own user profile, your role must have unrestricted access the **Notifications** permission.

1. Go **Manage Center > Users > User Manager > Users**.
2. Locate and open the appropriate user profile.
3. Open the **Notifications** tab. Scroll to the **Microsoft Teams Notifications** section.
4. In the **Enable Microsoft Teams Notifications** field select *Yes*.
5. In the **Select notifications to send to Microsoft Teams** field, choose one of the following options:
   - **Only notifications sent TO me** - choose this option to get notifications only when the user is a direct recipient of the notification.
   - **Both notifications sent TO me and where I am copied** - choose this option to also send notifications when the user CC'ed.

4. In the **Microsoft Teams Application** field, select the appropriate MS Teams configuration.
5. Click **Submit**.

Set Up MS Teams Notifications in Your Own User Profile

> In order to set up notifications in your own user profile, your role must have unrestricted access the **Notifications** permission.

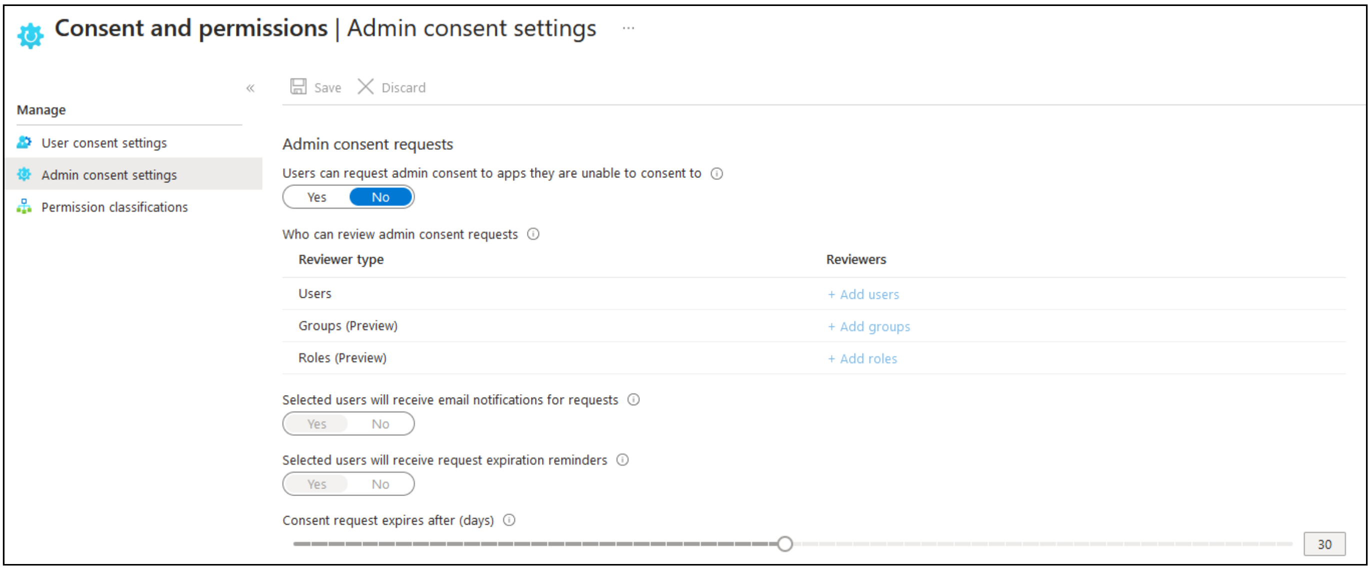
1. Go to **My Profile** and click the **Notifications** tab.
2. In the **Enable Microsoft Teams Notifications** field select *Yes*.
3. In the **Select notifications to send to Microsoft Teams** field, choose one of the following options:
   - **Only notifications sent TO me** - choose this option to get notifications only when you are the direct recipient of the notification.
   - **Both notifications sent TO me and where I am copied** - choose this option to also receive notifications when you are CC'ed.

4. In the **Microsoft Teams Application** field, select the appropriate MS Teams configuration.
5. Click **Submit**.

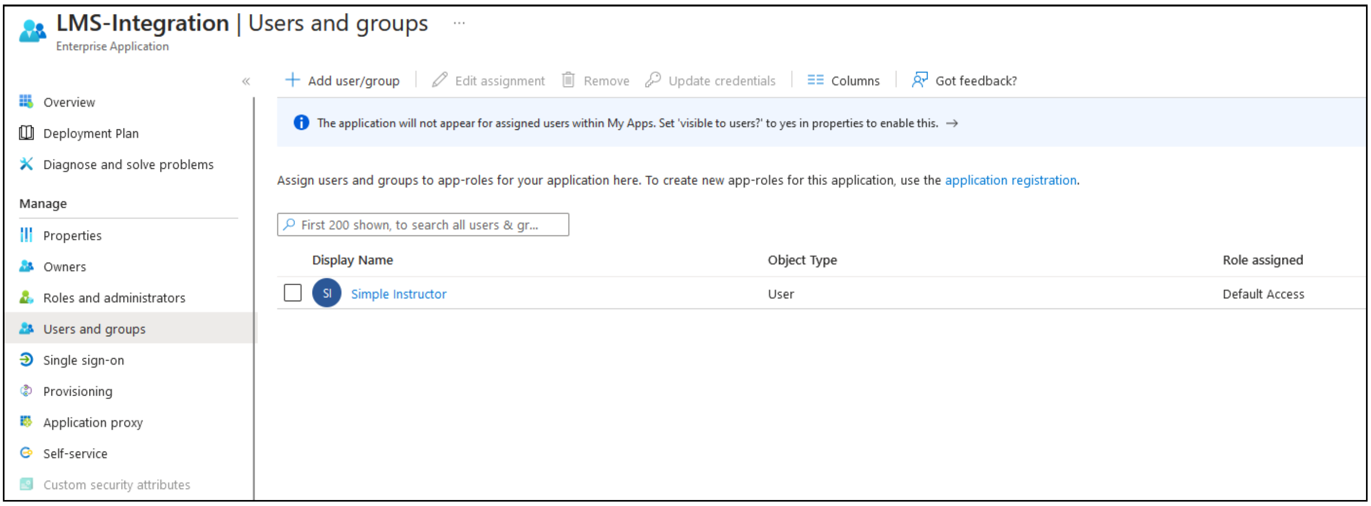
Troubleshooting

This appendix provides additional configuration steps for organizations that do not allow users to consent to apps accessing company data on their behalf.

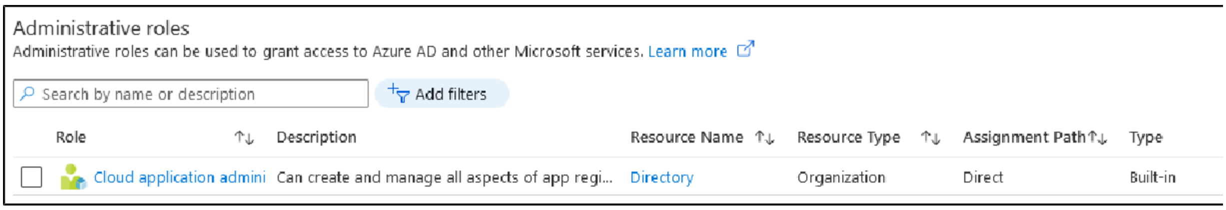
In the Microsoft Entra admin center, go to **Enterprise Applications > Consent and permissions > Admin consent settings** and confirm **Users can consent to apps accessing company data on their behalf** is set to No.



If so, then specific users will need to be permitted to access the integration. Go to **Enterprise applications**, select the specific application, and then select Users and groups to add a user.



Select the user and assign them the *Cloud application administrator* role. This is a default role that allows access to the application.



Legal Notice

Website: peoplefluent.com