

# Azure Active Directory Setup Guide

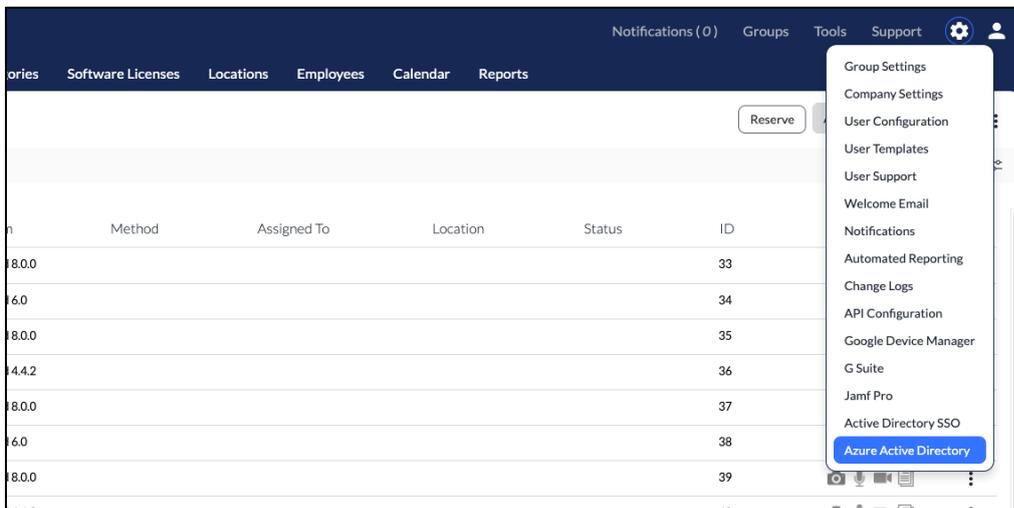
This guide will help you successfully integrate Azure Active Directory with Asset Panda.

**NOTE: You will be copying and pasting values between Azure and Asset Panda during this integration. It is recommended that you paste all values into a text (.txt) file so you do not lose them in the event of a system timeout.**

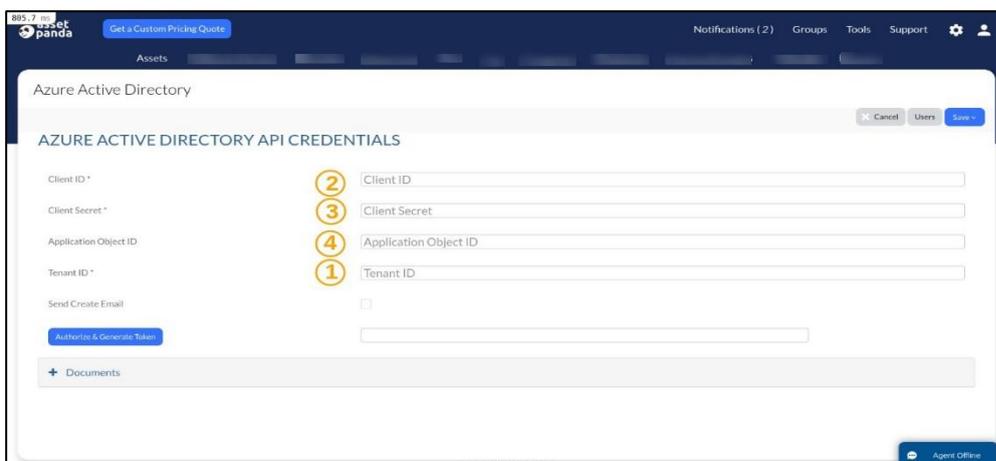
## Login to Accounts

### AssetPanda

1. Open a new tab, and then navigate to Asset Panda at <https://login.assetpanda.com>.
2. Log in to your account, click the Settings  icon, and then select **Azure Active Directory**.

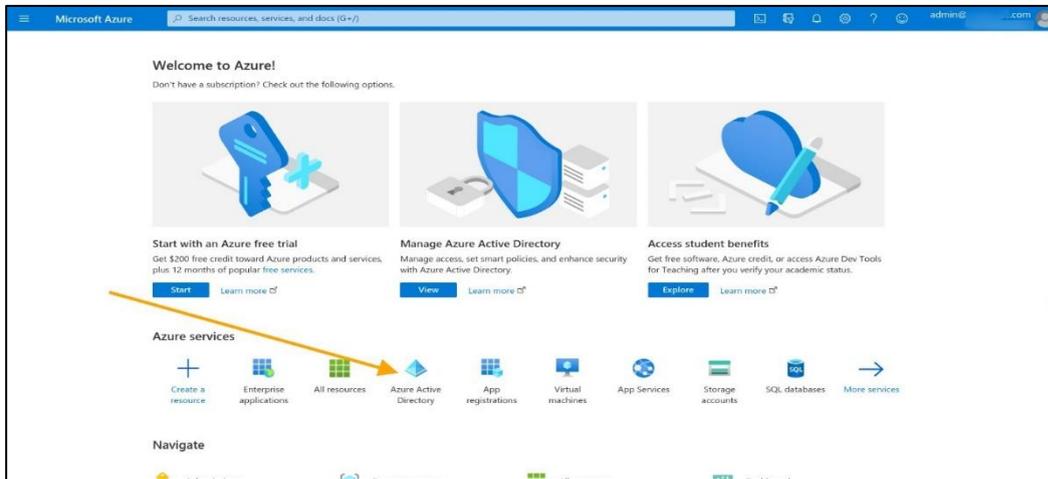


3. The **Azure Active Directory API Credentials** page displays. Keep this page and tab open, as you will refer to it again throughout the following steps.



## Microsoft Azure

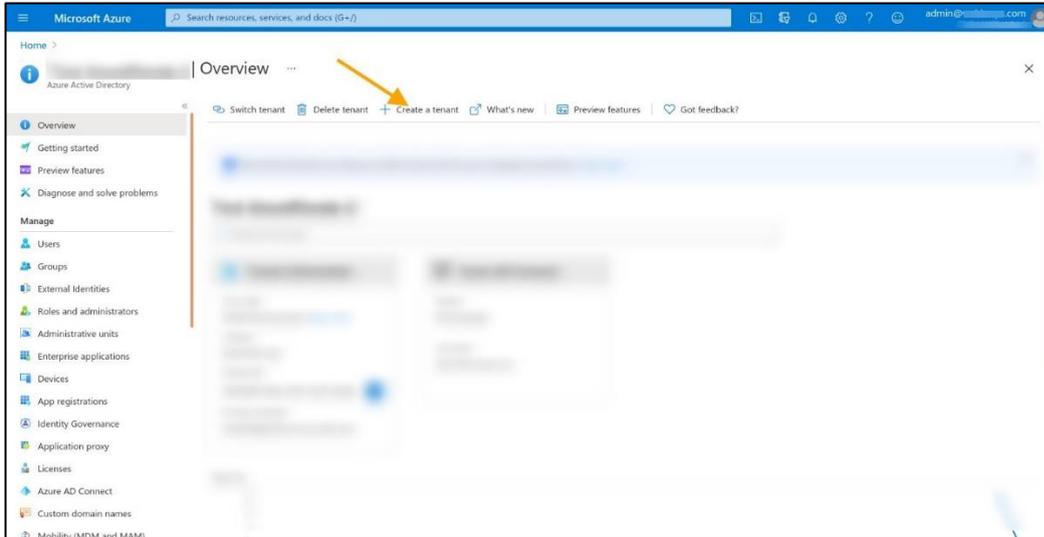
1. Open a second tab, and then navigate to Azure at <https://portal.azure.com>.
2. Log into your account, and then click **Azure Active Directory**.



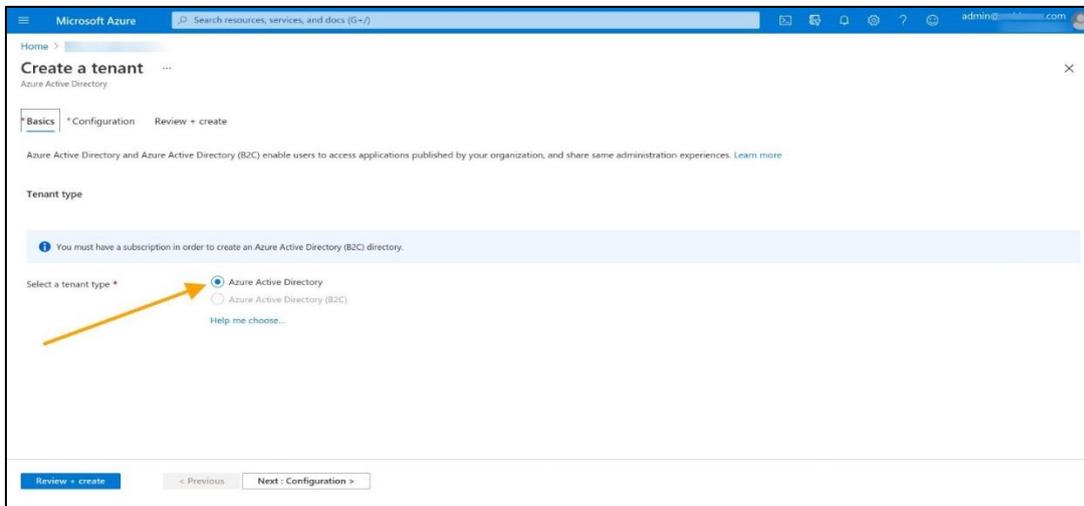
## Create Tenant

You must first create a tenant within Microsoft Azure. If you have existing tenant, skip to the **View Tenant** section. To create a tenant:

1. Select **Create a tenant**.



2. Select **Azure Active Directory**.



3. Click the **Next : Configuration** button.
4. Enter your organization-specific information into the following fields:
  - Organization name
  - Initial domain name
  - Country/Region
5. Click the **Next : Review + create** button.

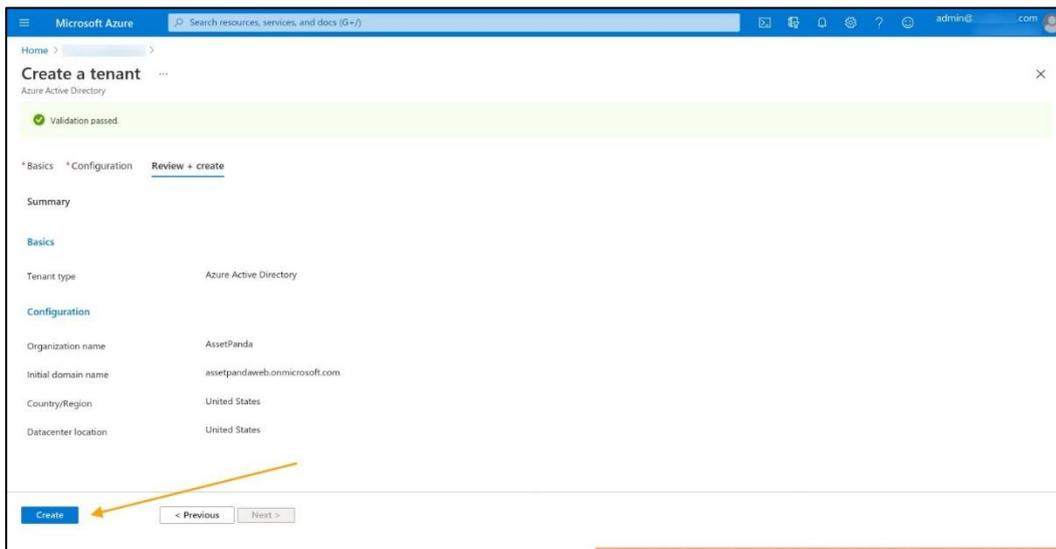
The screenshot displays the Microsoft Azure portal interface for creating a new tenant. The page title is "Create a tenant" and it is part of the "Azure Active Directory" service. The current step is "Configuration", with tabs for "Basics", "Configuration", and "Review + create".

Under "Directory details", the user is prompted to "Configure your new directory". The following fields are filled out:

- Organization name: AssetPanda
- Initial domain name: assetpandaweb (with a dropdown showing assetpandaweb.onmicrosoft.com)
- Country/Region: United States (with a dropdown showing Datacenter location - United States)

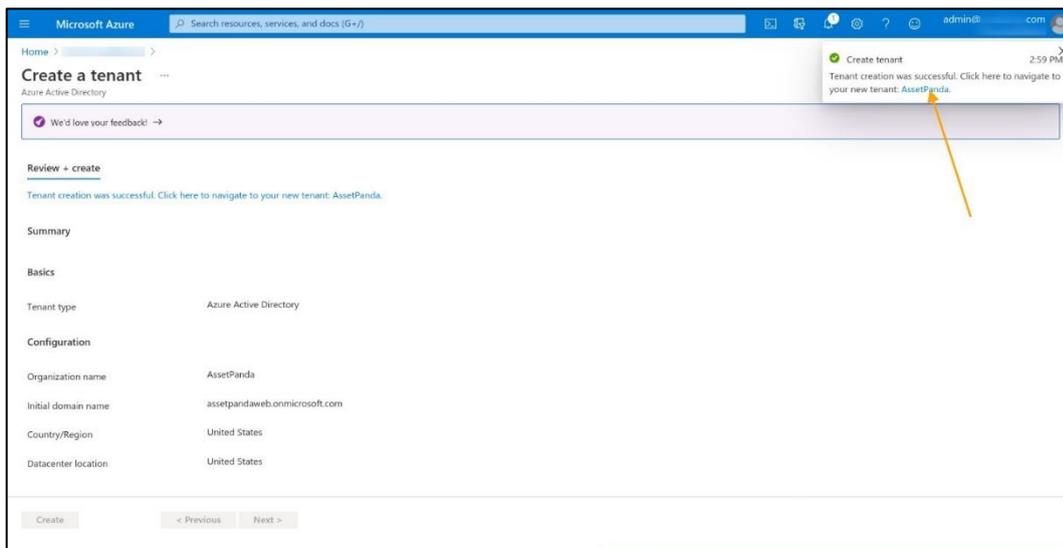
At the bottom of the page, there are three navigation buttons: "Review + create" (highlighted in blue), "< Previous", and "Next : Review + create >". A yellow arrow points to the "Next : Review + create >" button.

## 6. Click Create.



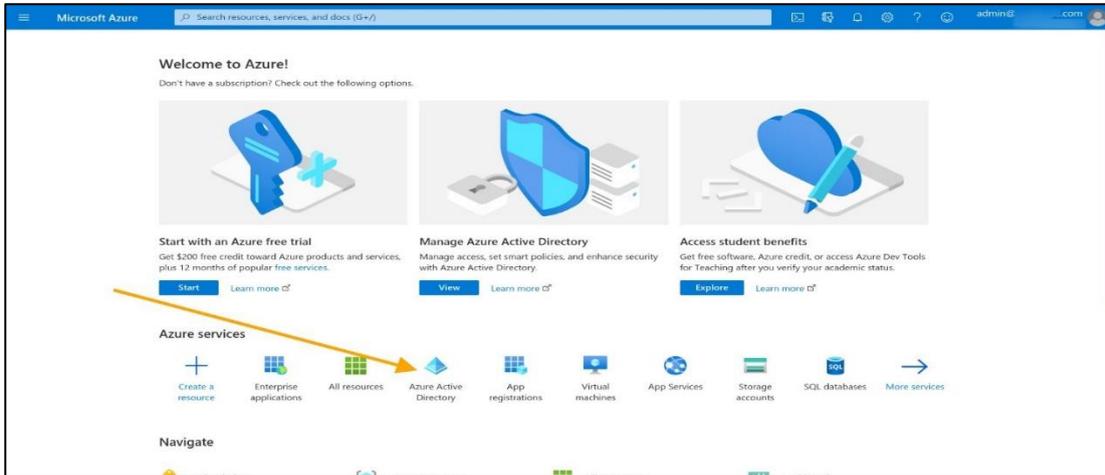
You will receive a success message once the tenant is successfully created.

**NOTE: This process may take a while.**

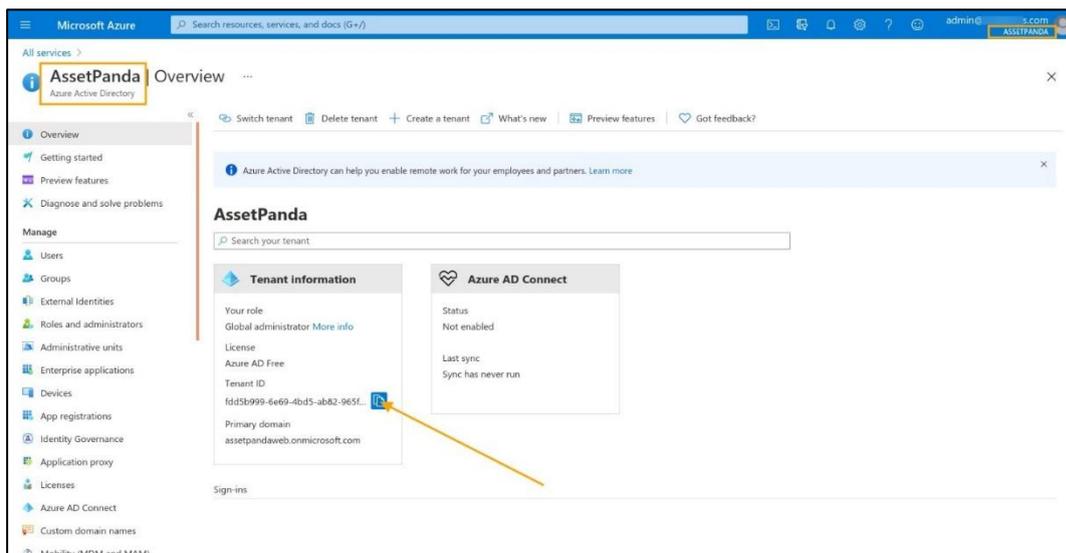


## View Tenant

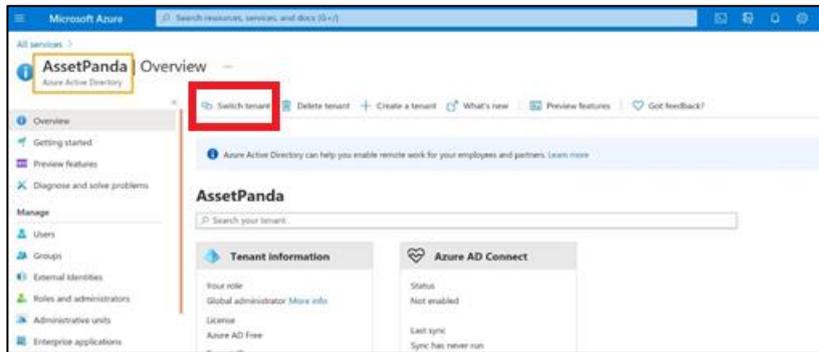
1. Navigate back to or log into your Azure Account. (If you're already logged in, click **Home**, located within in the top, left corner of your screen.)
2. Select **Azure Active Directory**.



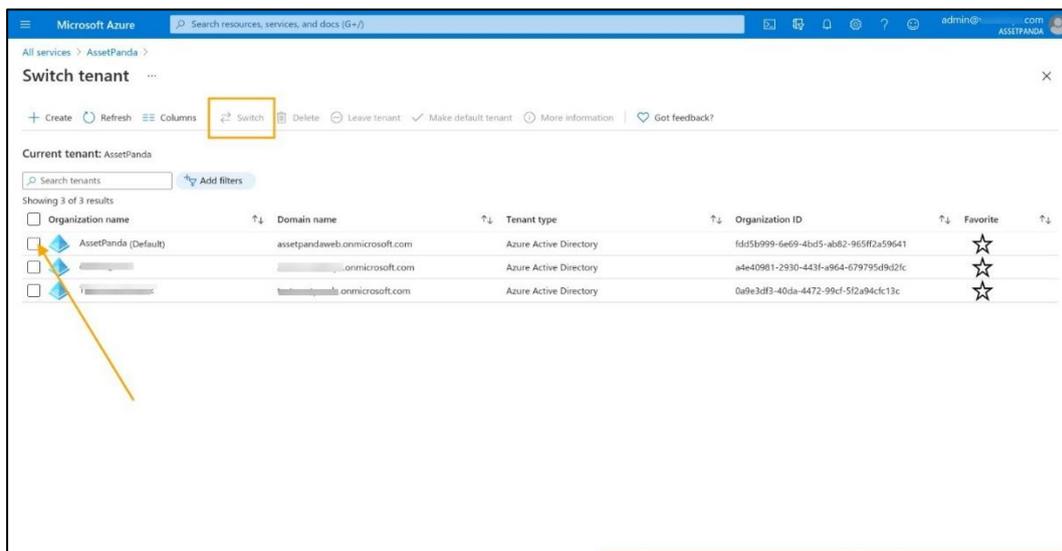
Your default **Tenant Information** displays.



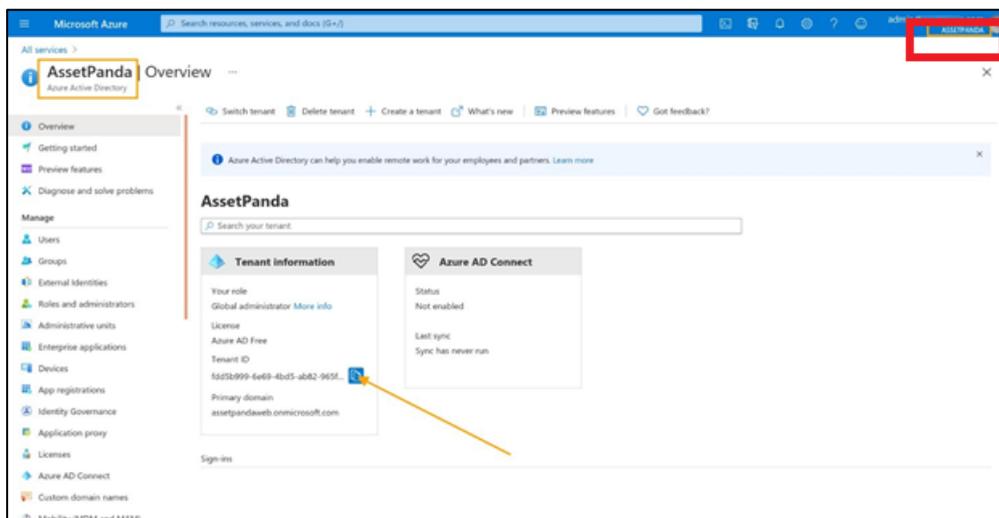
3. Click **Switch Tenant** if you would like to use a different tenant, and then select a tenant from the list.



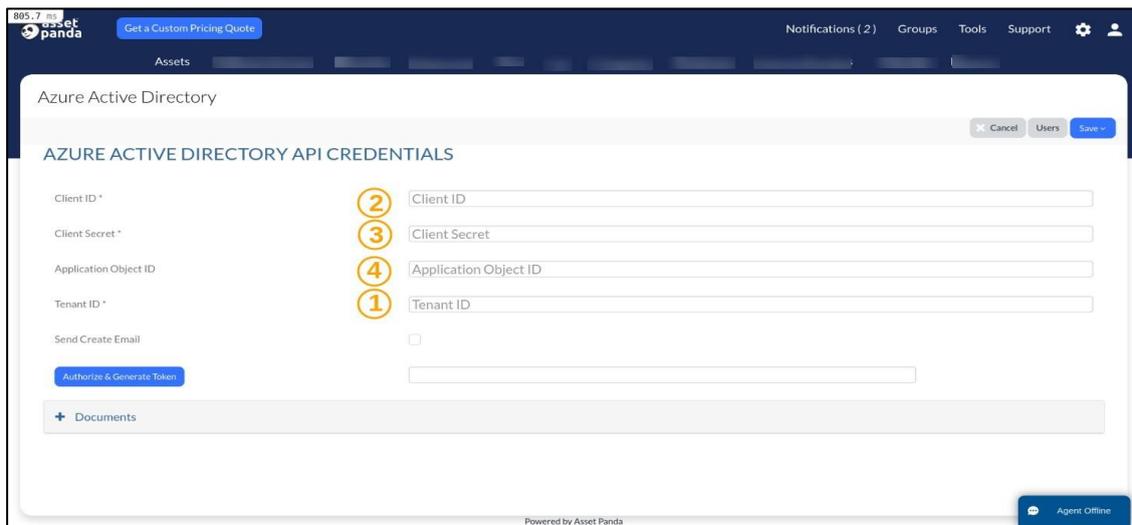
4. Click **Switch**.



5. Verify the tenant name (located in the top, right corner below your email id).
6. Click the copy icon to copy the **Tenant ID**.

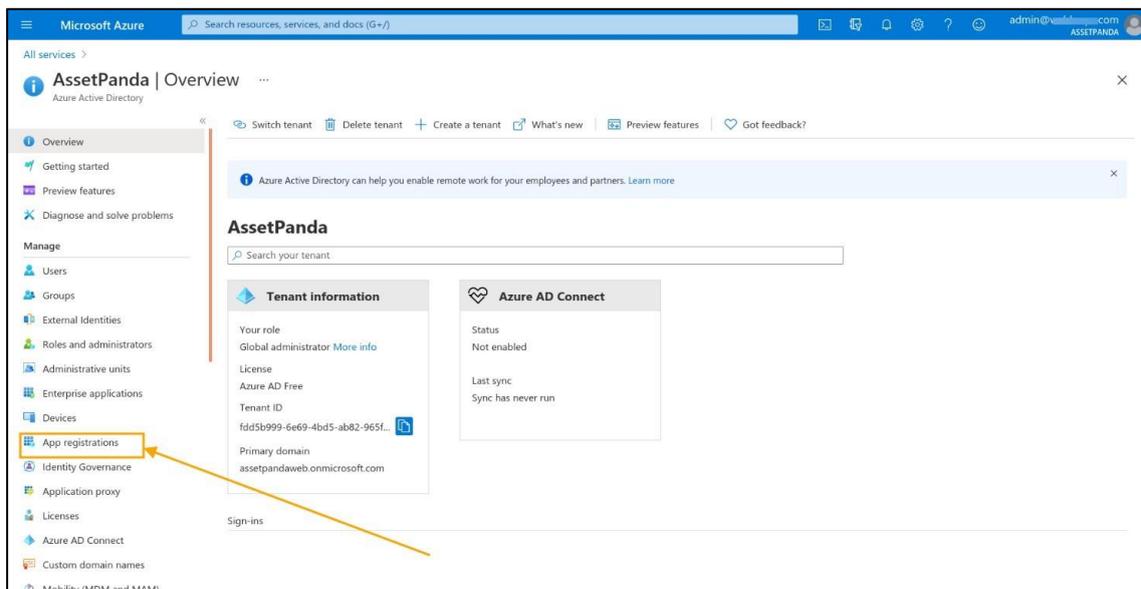


7. Navigate back to Asset Panda, and then paste the Tenant ID into the **Tenant ID** field (#1).

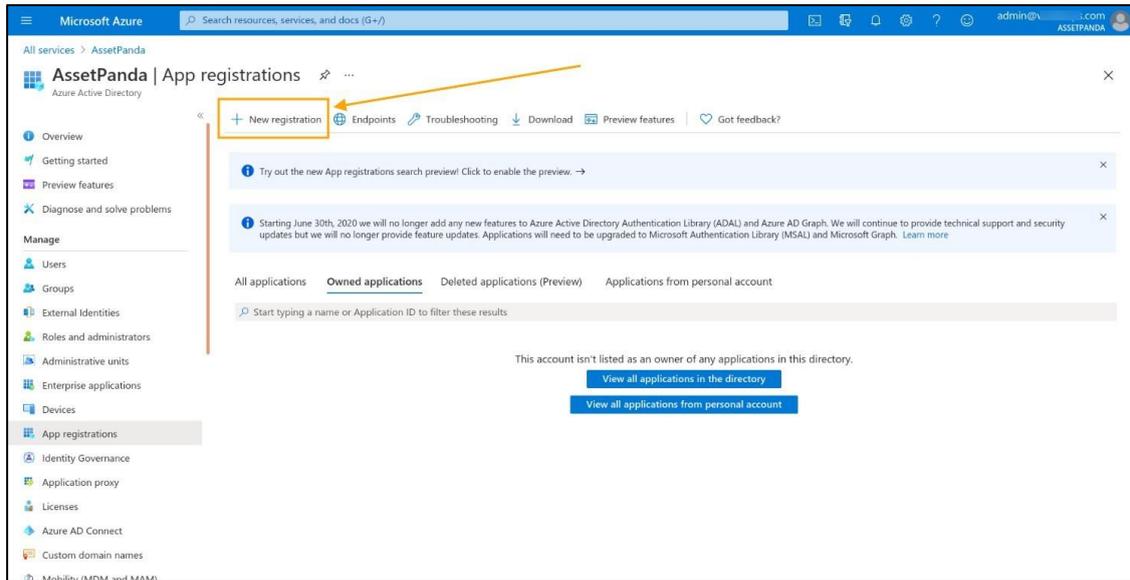


## App Registration

1. Navigate back to your Azure account, and then click **App registration**.



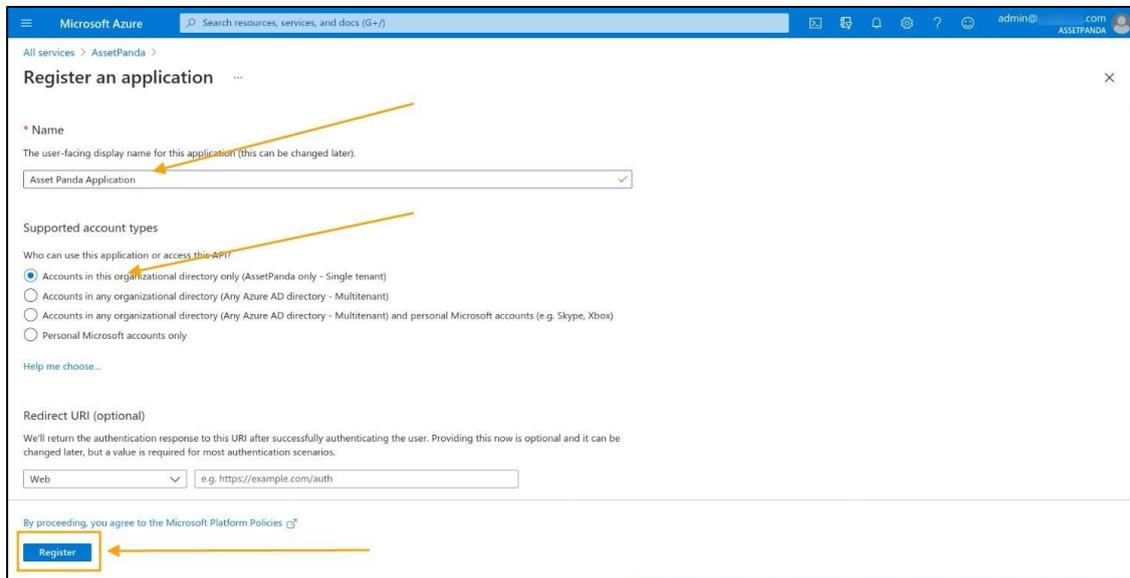
## 2. Click **New registration**.



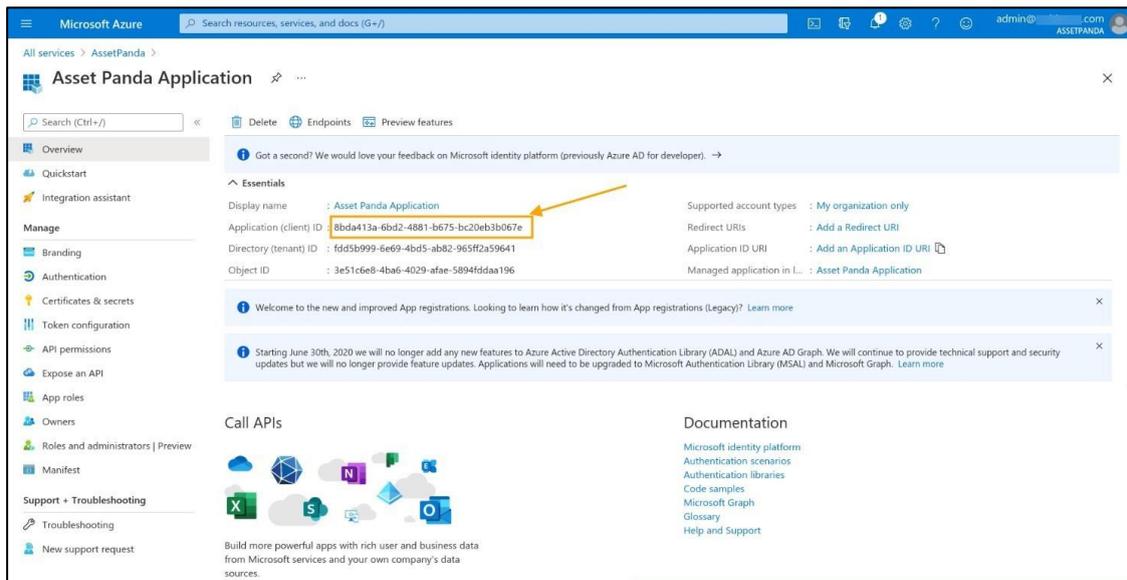
## 3. Complete the following fields:

- Name
- Supported account types – Select **Accounts in this organizational directory only (AssetPanda only – Single tenant)**

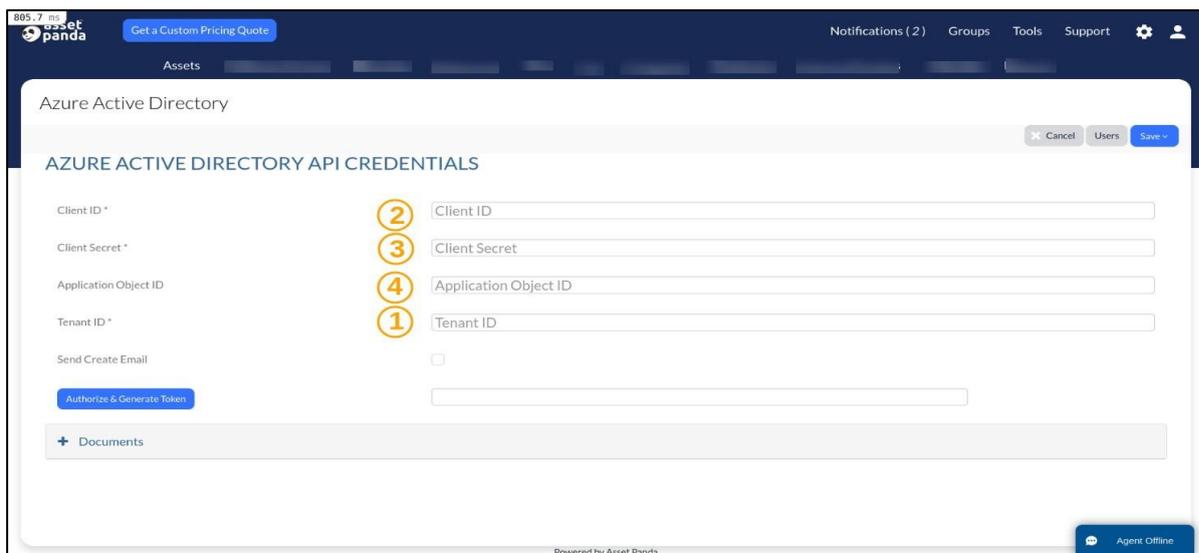
## 4. Click **Register**.



5. Copy the **Application (client ID)**.



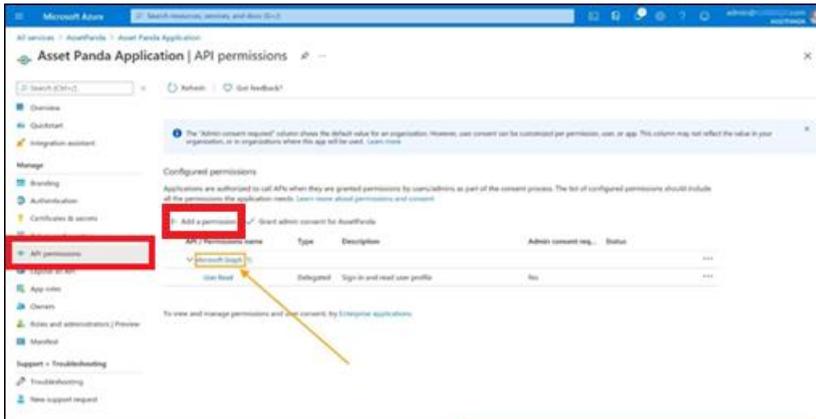
6. Navigate back to your Asset Panda account, and then paste the **Application (client ID)** into the **Client ID** field (#2).



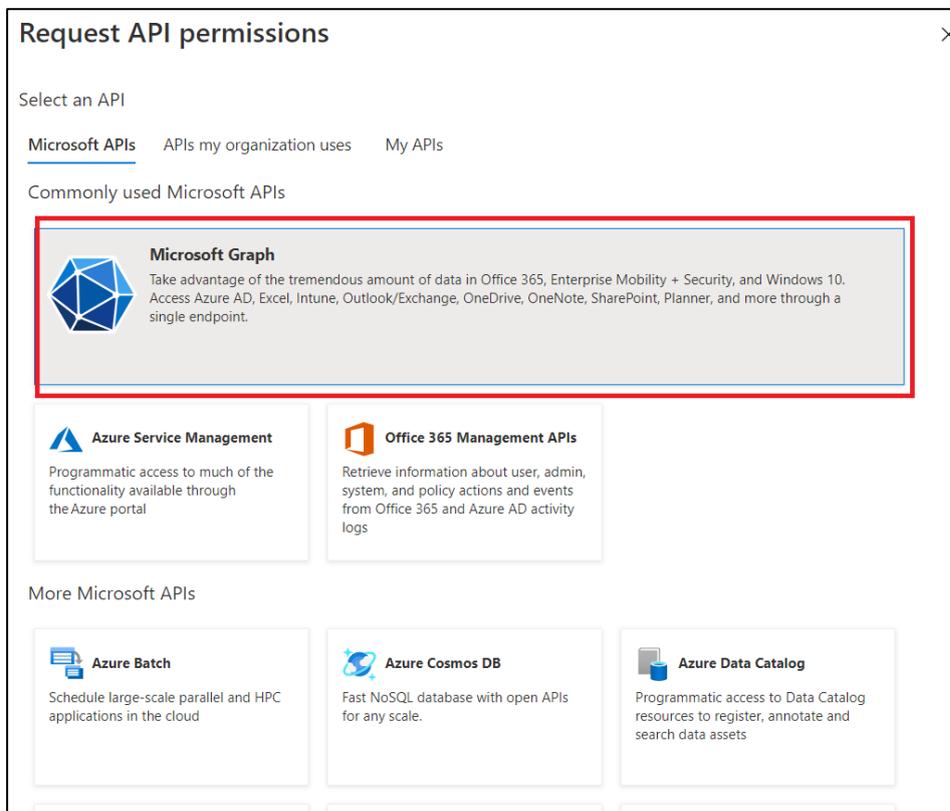
## Add API Permissions

Complete the following steps to add your API permissions.

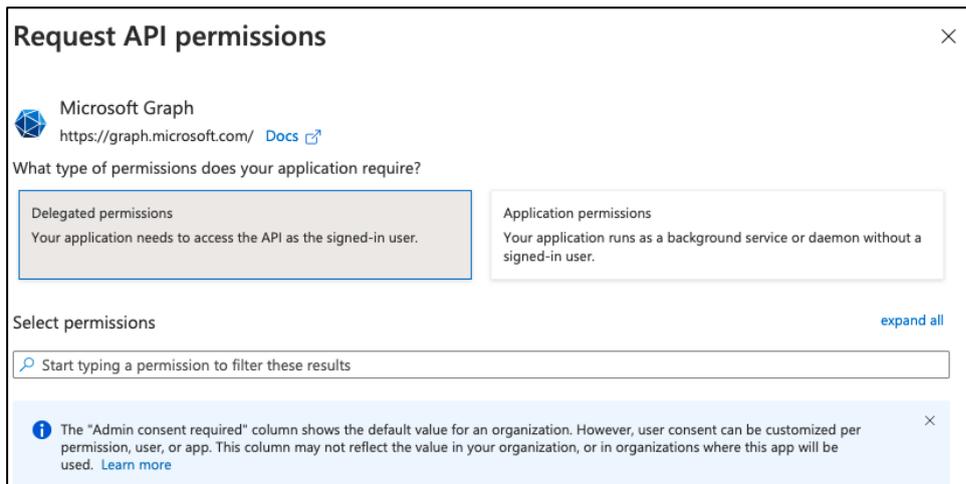
1. Navigate back to your Azure account.
2. Click **API Permissions**.  
The **User Read** permission should already be contained within the list.
3. From the **Configured permissions** section, select **Add a permission**.



4. From the **Request API permissions** page, select **Microsoft Graph** to add more permissions.

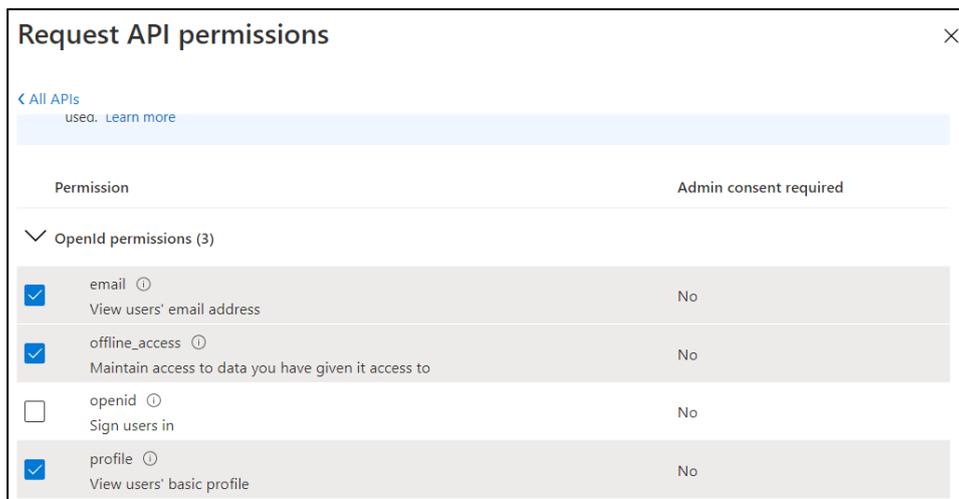


5. Select **Delegated permissions**.



6. Expand **OpenId permissions**, and then select the following values:

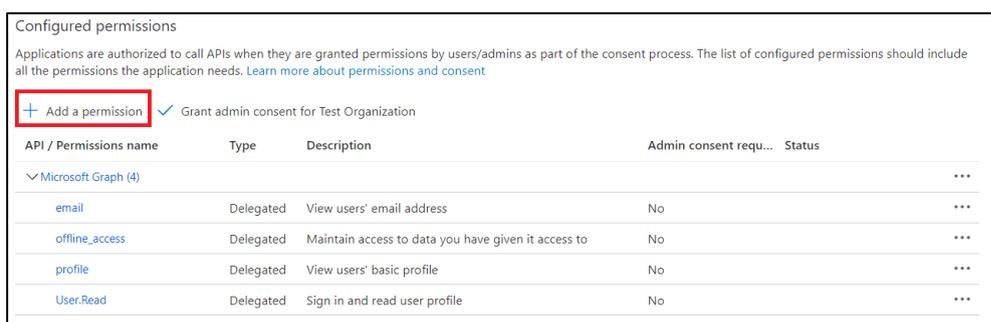
- email
- profile
- offline\_access



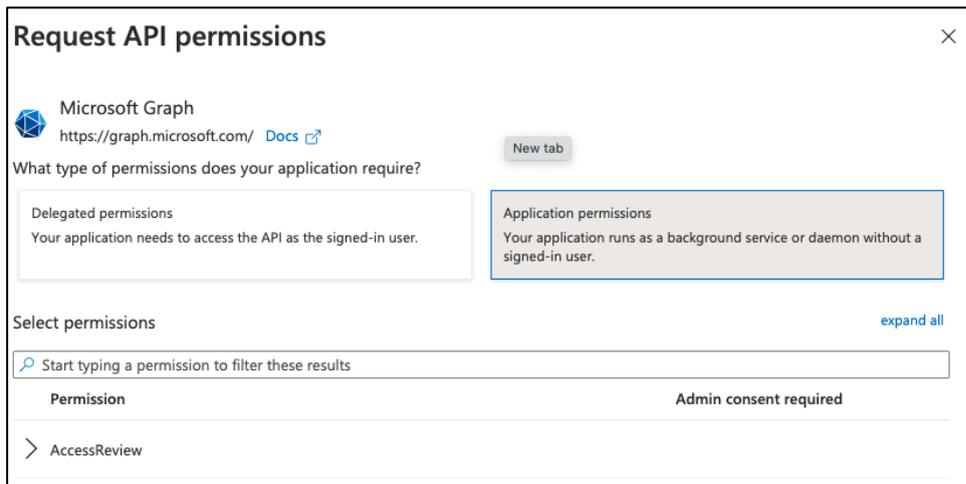
7. Click **Add Permissions**.

The Configured permissions section displays again.

8. Click **Add a permission** to add more permissions.



9. Select **Microsoft Graph** again, and then select **Application permissions**.



10. Navigate to **Group**, expand the menu, and then select:

- Group.Read.All

11. Navigate to **Directory**, expand the menu, and then select:

- Read.All

12. Navigate to **User**, expand the menu, and then select:

- Read.All

13. Navigate to **Delegated permission**, expand the menu, and then select:

- User.ReadBasic.All

14. Navigate to **Application**, expand the menu, and then select:

- Application.Read.All

15. Click **Update permissions**. A list of your selected permissions should display, as shown below.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

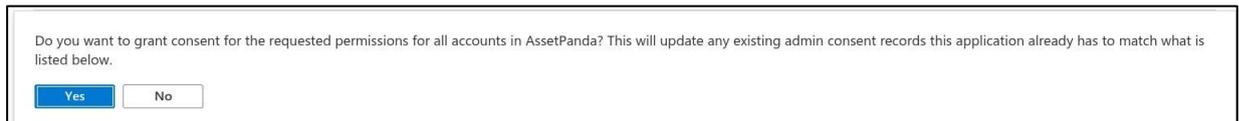
+ Add a permission ✓ Grant admin consent for Test Organization

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (8)				
Application.Read.All	Application	Read all applications	Yes	⚠ Not granted for Test Or... ⋮
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Test Or... ⋮
email	Delegated	View users' email address	No	⋮
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Test Or... ⋮
offline_access	Delegated	Maintain access to data you have given it access to	No	⋮
profile	Delegated	View users' basic profile	No	⋮
User.Read	Delegated	Sign in and read user profile	No	⋮
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Test Or... ⋮

16. Click **Grant admin consent for Default Directory** to confirm that all permissions have admin consent.



17. Click **Yes** to grant consent.



18. Confirm that the **Status** column displays the granted, admin permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

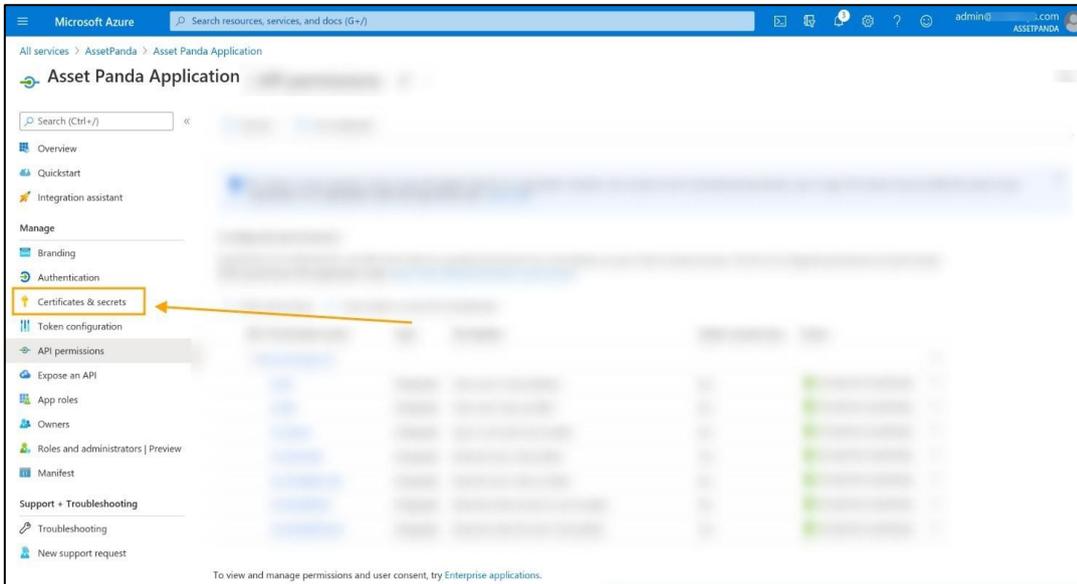
+ Add a permission ✓ Grant admin consent for Test Organization

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (8)				...
Application.Read.All	Application	Read all applications	Yes	✓ Granted for Test Organi... ..
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Test Organi... ..
email	Delegated	View users' email address	No	✓ Granted for Test Organi... ..
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Test Organi... ..
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for Test Organi... ..
profile	Delegated	View users' basic profile	No	✓ Granted for Test Organi... ..
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Test Organi... ..
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Test Organi... ..

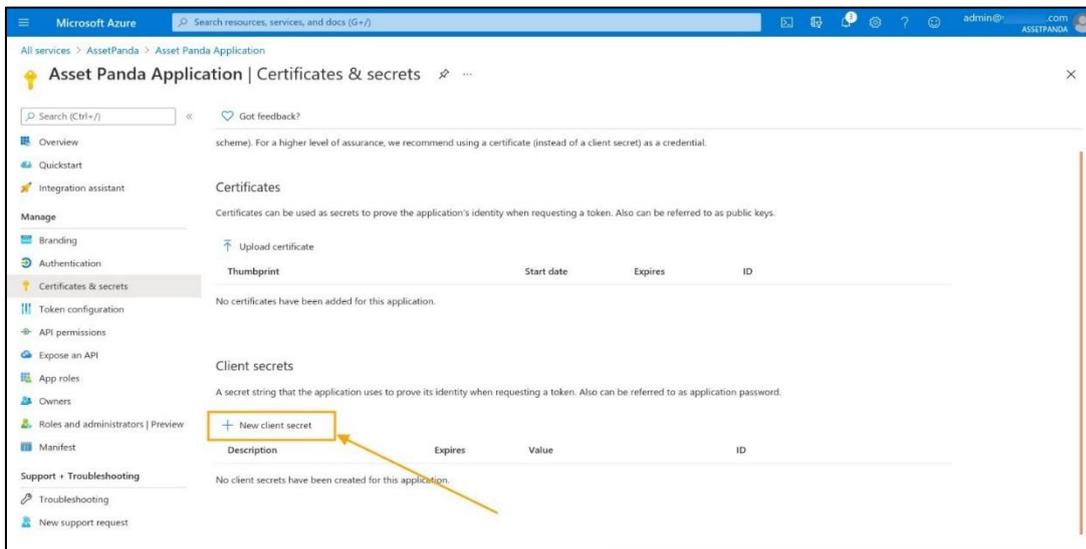
## Create Application Secret

This section will guide you through the steps of creating an application secret that will be used within Asset Panda.

1. Click **Certificates & secrets**.



2. Click **New client secret**.



3. Enter the following details within the **Client secrets** window:
  - Description
  - Expires - Select the maximum expiration option.
4. Click **Add**.

5. Copy the **Value** shown on your screen. You will not be able to do this again after this step.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value	Secret ID
APanda secret	5/20/2023	y_E2dCER81MgCyP~fjh6wpT.nRqt.f4_9B	547f941c-d3be-466d-a34a-83c4d11e281a

6. Navigate back to your Asset Panda window, and then paste the Value within the **Client Secret** field (#3).

Asset Panda

Get a Custom Pricing Quote

Notifications (2) Groups Tools Support

Assets

Azure Active Directory

AZURE ACTIVE DIRECTORY API CREDENTIALS

Client ID \*

Client Secret \*

Application Object ID

Tenant ID \*

Send Create Email

Authorized & Generate Token

+ Documents

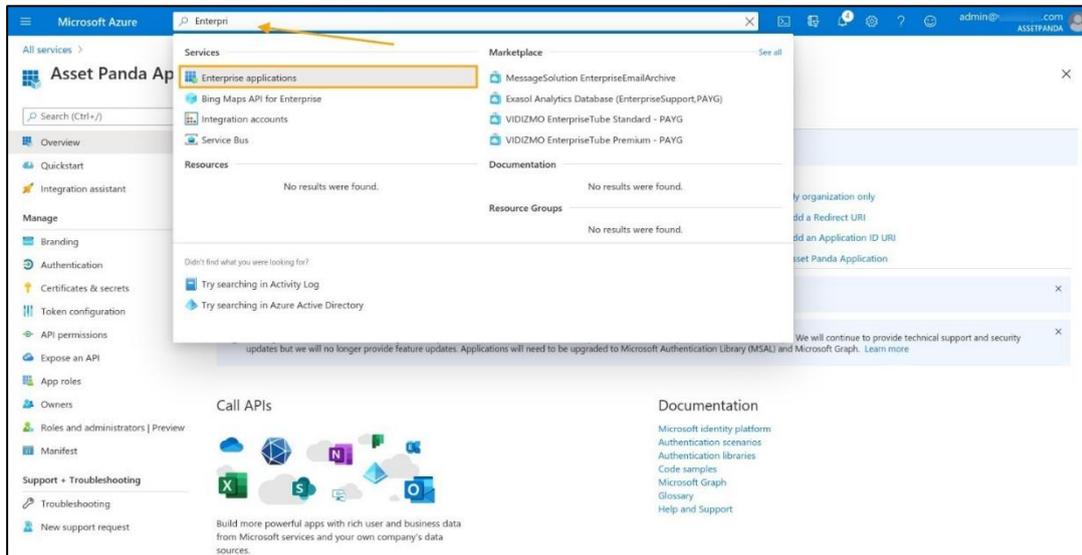
Powered by Asset Panda

Agents Offline

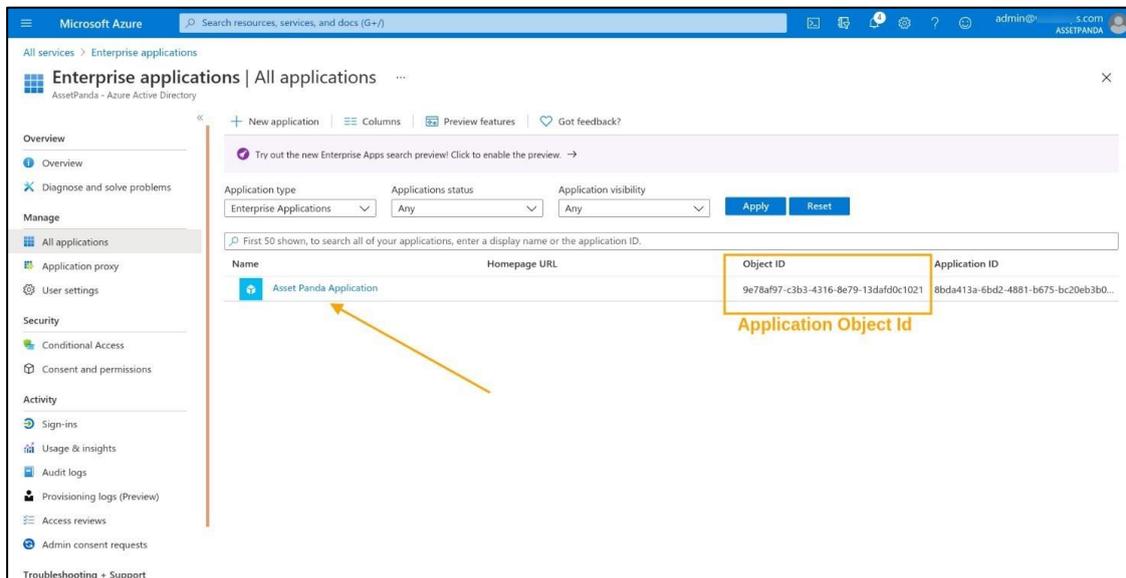
## Enterprise Application

To enable Asset Panda to sync with Active Directory users, you must first enable the application within Azure.

1. Navigate back to your Azure account.
2. Begin to type **Enterprise** within the Search box, and then select **Enterprise Applications**.



3. Locate your application, and then copy the **Object ID**.



4. Navigate back to your Asset Panda account, and then paste the Object ID within the **Application Object ID** field (#4).

The screenshot displays the 'Azure Active Directory' configuration page in the Asset Panda interface. The page title is 'AZURE ACTIVE DIRECTORY API CREDENTIALS'. It features four input fields, each with a yellow circular callout containing a number: 'Client ID' (2), 'Client Secret' (3), 'Application Object ID' (4), and 'Tenant ID' (1). Below these fields is a 'Send Create Email' checkbox and an 'Authorize & Generate Token' button. The page also includes a 'Cancel' button, a 'Users' dropdown, and a 'Save' button. A '+ Documents' section is visible at the bottom. The footer indicates 'Powered by Asset Panda' and 'Agent Offline'.

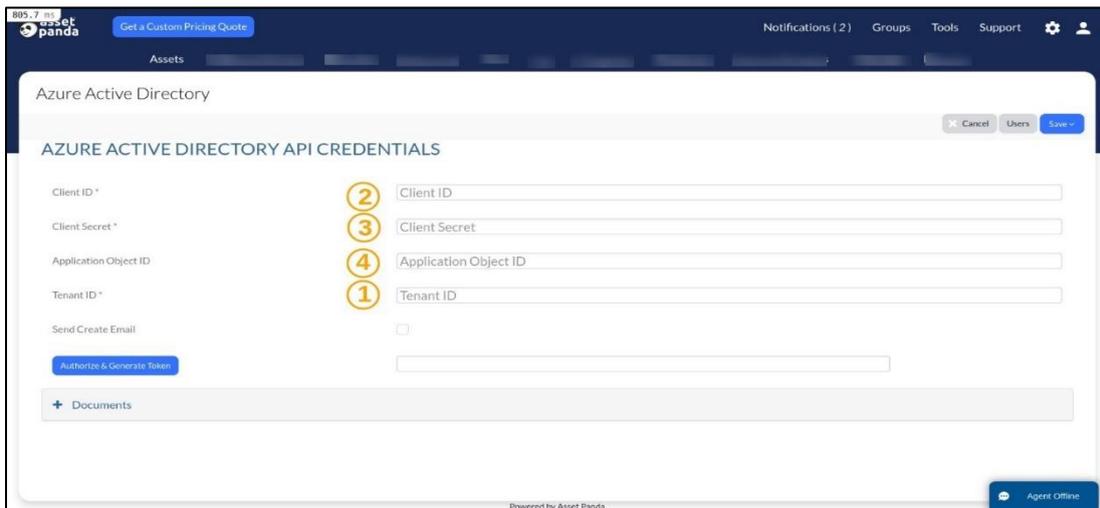
## Final Steps

The following fields should now contain information from the previous steps:

- Client ID
- Client Secret
- Application Object ID
- Tenant ID

To complete the setup process:

1. Click **Authorize & Generate Token**.



The screenshot displays the 'Azure Active Directory API CREDENTIALS' configuration page in the Asset Panda application. The page features a dark blue header with the Asset Panda logo and navigation links. The main content area is titled 'AZURE ACTIVE DIRECTORY API CREDENTIALS' and contains several input fields: 'Client ID \*' (labeled with a yellow circle '2'), 'Client Secret \*' (labeled with a yellow circle '3'), 'Application Object ID' (labeled with a yellow circle '4'), and 'Tenant ID \*' (labeled with a yellow circle '1'). Below these fields is a 'Send Create Email' checkbox and an 'Authorize & Generate Token' button. A 'Documents' section is visible at the bottom of the form area. The footer of the page includes the text 'Powered by Asset Panda' and an 'Agent Offline' status indicator.

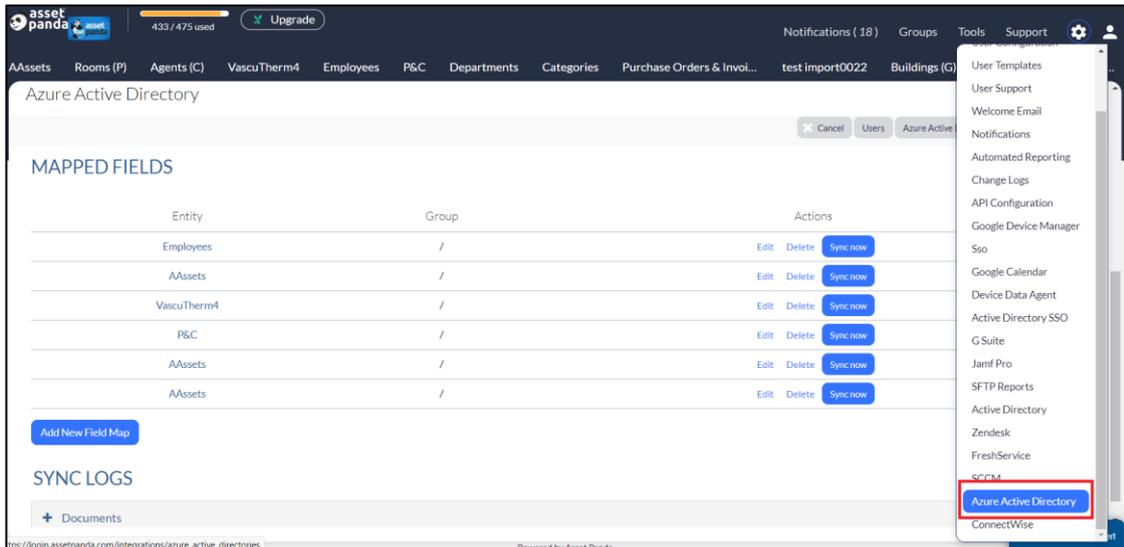
2. Click **Save**.

Azure Active Directory is now ready to use with your account. You can now copy users, create field maps, and set schedules.

## Mapped Fields

Complete the steps in this section to map (and sync) to specific groups.

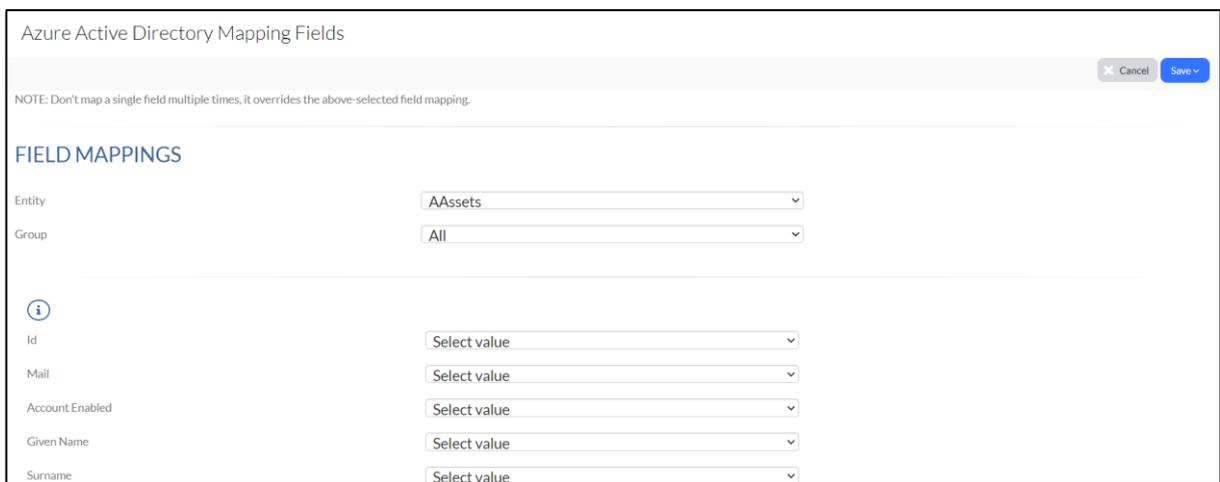
1. Click the Settings icon , and then select **Azure Active Directory** (or scroll down the **Azure Active Directory** page if you are already there and have completed all the steps in the previous sections).



2. Navigate to the **Mapped Fields** section, and then click **Add New Field Map**.



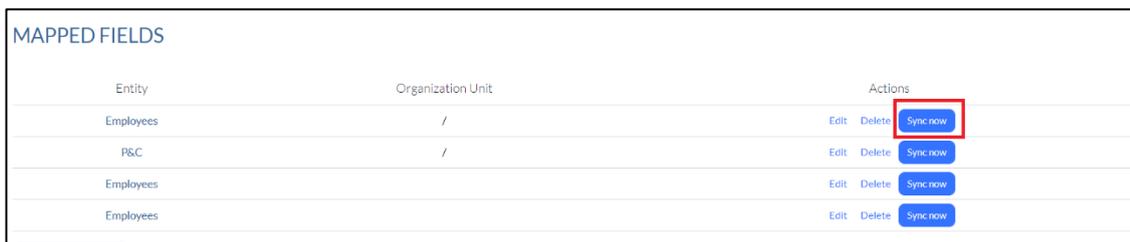
3. Select the groups you wish to map into Asset Panda.



4. Click **Save**.

You are redirected back to the **Azure Active Directory** page.

5. Scroll back to the **Mapped Fields** section, and then click **Sync Now**. (See, "Sync Individual Record" below if you wish to sync an individual record rather than a group.)



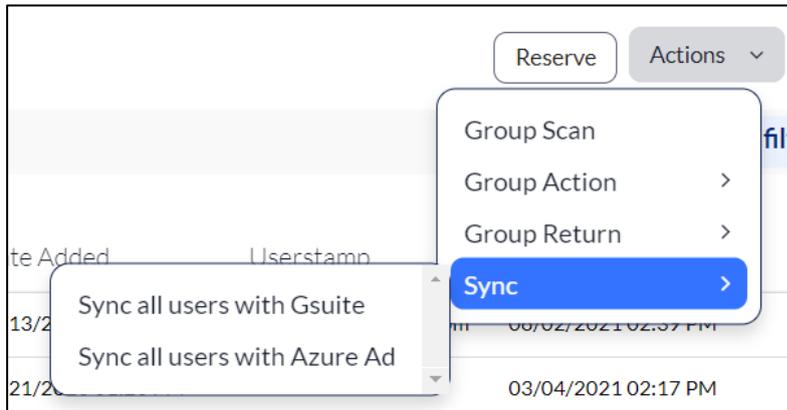
6. Your items begin to synchronize and you will receive an email once it is complete.

**NOTE: All sync information can be viewed through the Sync Logs at the bottom of the Azure Active Directory page.**

## Sync Individual Record

If you wish to sync an individual record:

1. Click **Actions** when viewing a record.
2. Select **Sync**, and then select **Sync all users with Azure Active Directory**.



**NOTE: All sync information can be viewed through the Sync Logs at the bottom of the Azure Active Director page.**