

DARKWEB 

AZURE ACTIVE DIRECTORY

USER GUIDE

VERSION 1.0



support@idagent.com



Table of Contents

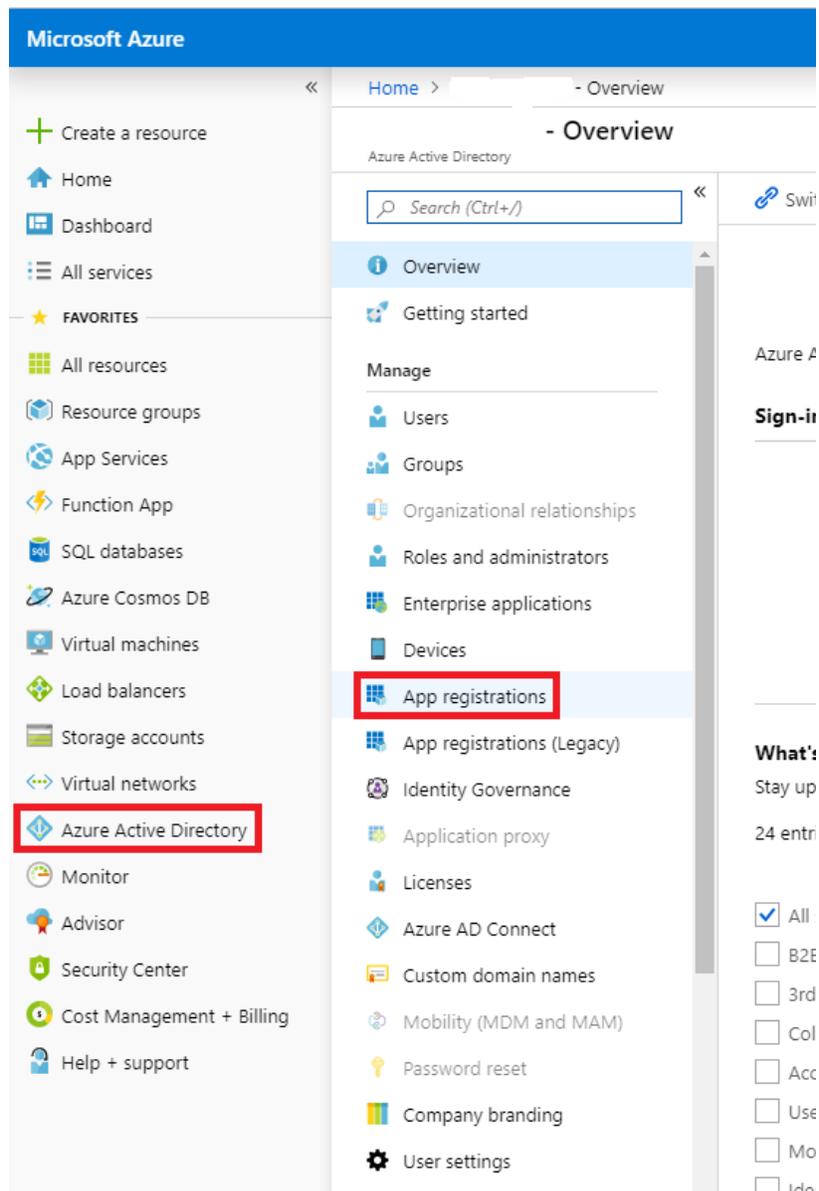
Prerequisites	2
Grant API Access to Azure AD.....	2
Authenticate with Dark Web ID.....	10
Using Active Directory in BullPhish ID.....	12

PREREQUISITES

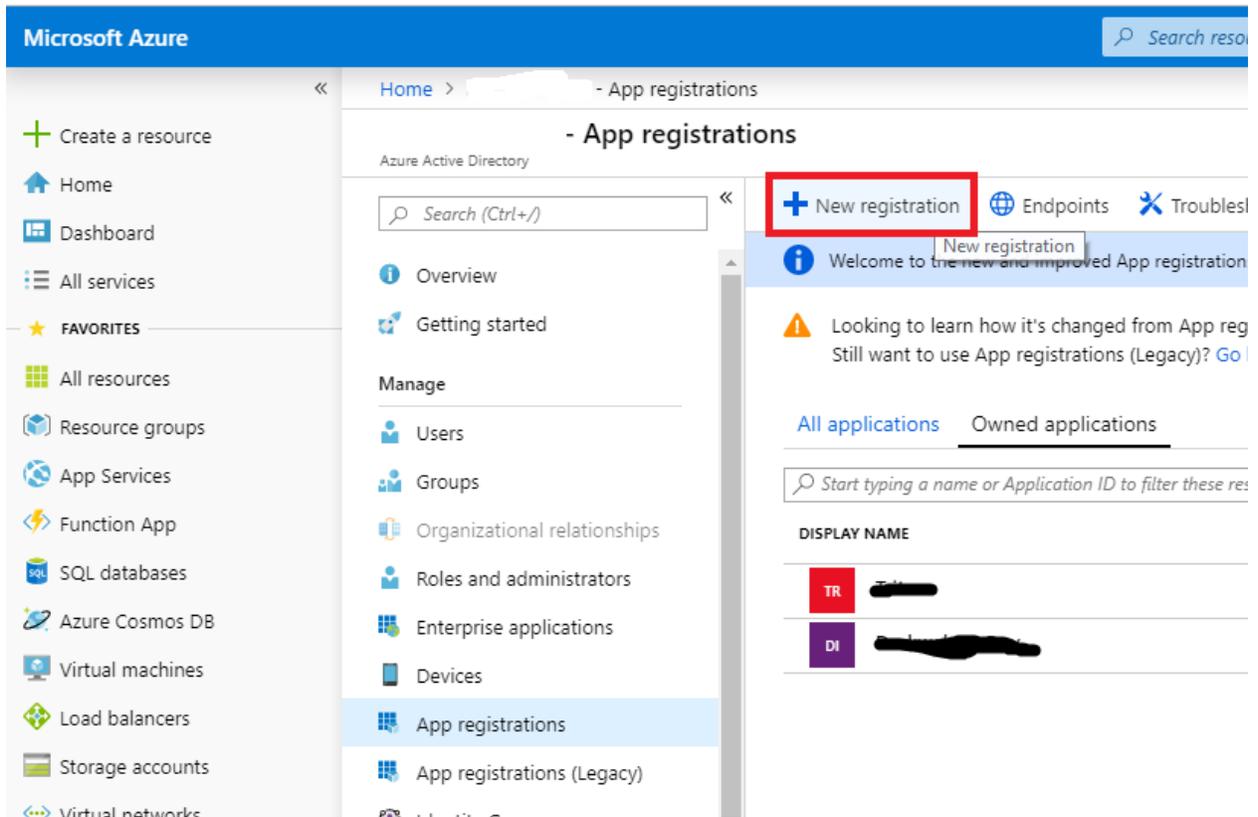
This integration is specifically for Azure’s Cloud Based Active Directory (AD). To use an Active Directory Group in Dark Web ID™ and BullPhish ID™, it will need to contain information for “givenName”, “surname”, “jobTitle”, and “mail” to translate to BullPhish ID. If “jobTitle” is null, it will default to “Employee.”

GRANT API ACCESS TO AZURE AD

1. Log into Azure Portal: <https://portal.azure.com>.
2. Click on “Azure Active Directory” in the left navigation menu.
3. Click on “App registrations” on the secondary menu.



4. Click “New registration.”

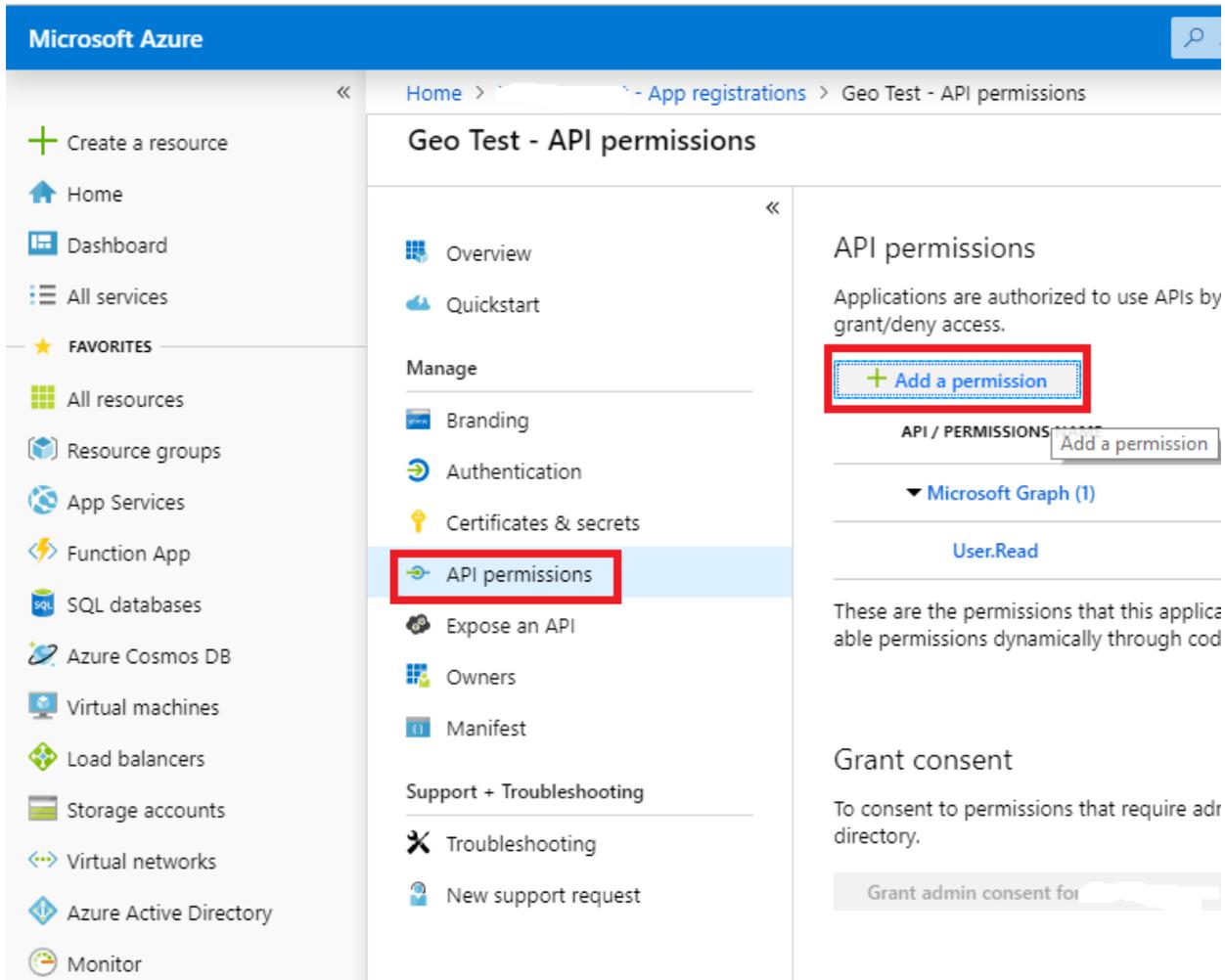


5. On the “Register an application” page, provide application name, and select “Accounts in any organizational directory” from the “Supported account types” radio button list.

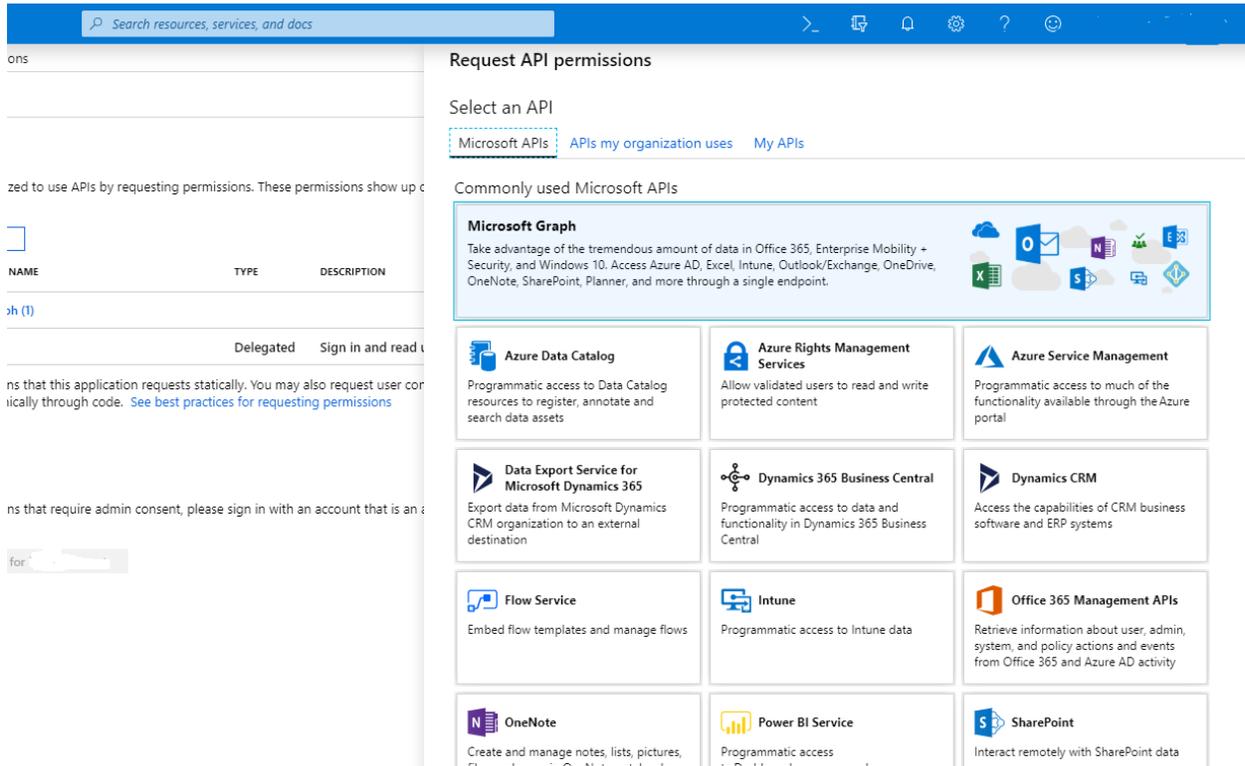
The screenshot displays the Microsoft Azure portal interface for registering an application. The left-hand navigation pane includes options like 'Create a resource', 'Home', 'Dashboard', and 'All services'. The main content area is titled 'Register an application' and contains the following sections:

- Name:** A required field with the label '* Name'. Below it, a text box contains 'Your Application Name' and a green checkmark icon.
- Supported account types:** A section titled 'Supported account types' with the subtext 'Who can use this application or access this API?'. It features three radio button options:
 - Accounts in this organizational directory only
 - Accounts in any organizational directory
 - Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)A link 'Help me choose...' is provided below the options.
- Redirect URI (optional):** A section titled 'Redirect URI (optional)' with the subtext 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' It includes a dropdown menu set to 'Web' and a text box containing the URI 'https://myapp.com/auth'.

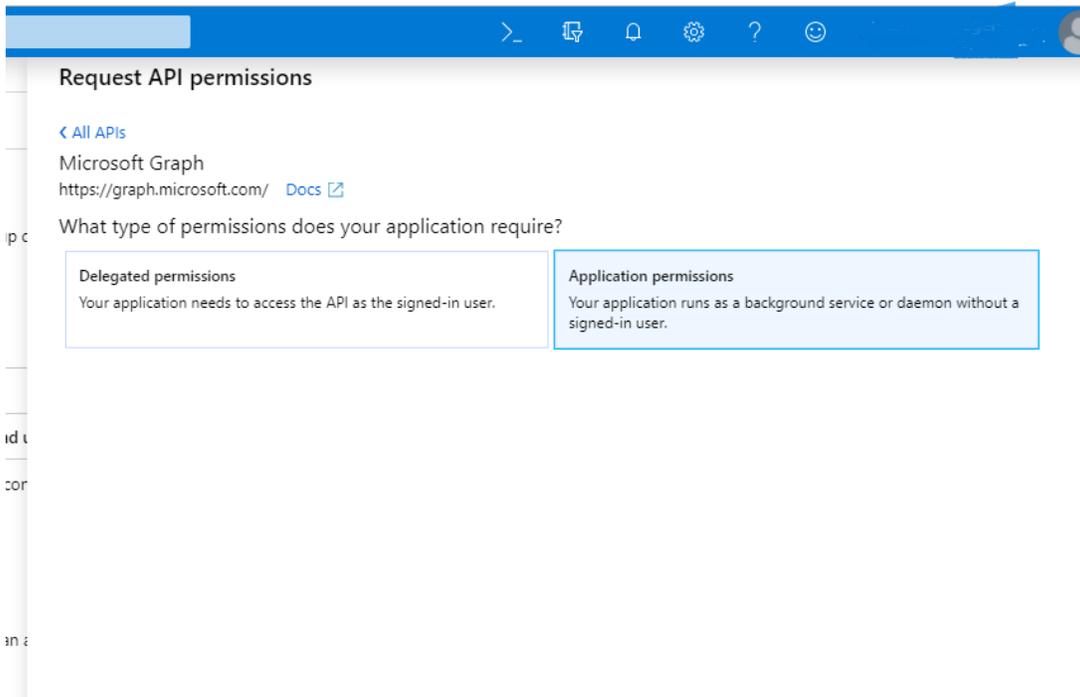
6. **Application ID, Tenant ID**, and Object ID are displayed. These will be needed to authenticate in Dark Web ID (Not Pictured).
7. Click “API permissions.”
8. Click “Add a permission.”



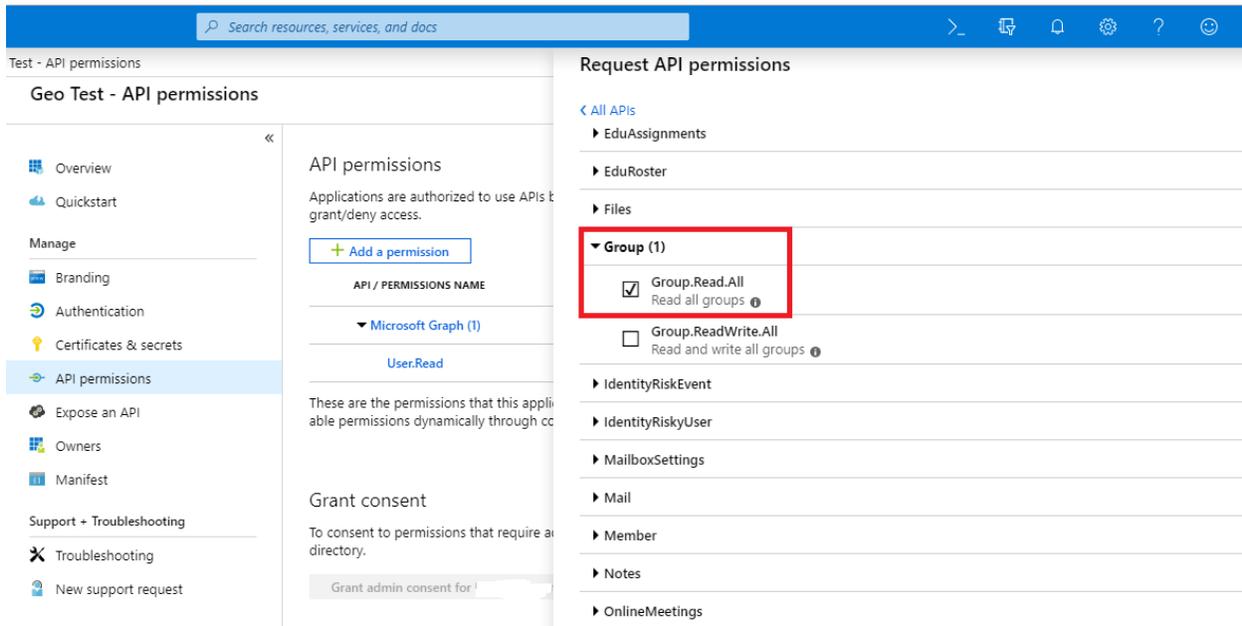
9. On the right-side menu, click “Microsoft Graph.”



10. Click “Application permissions.”

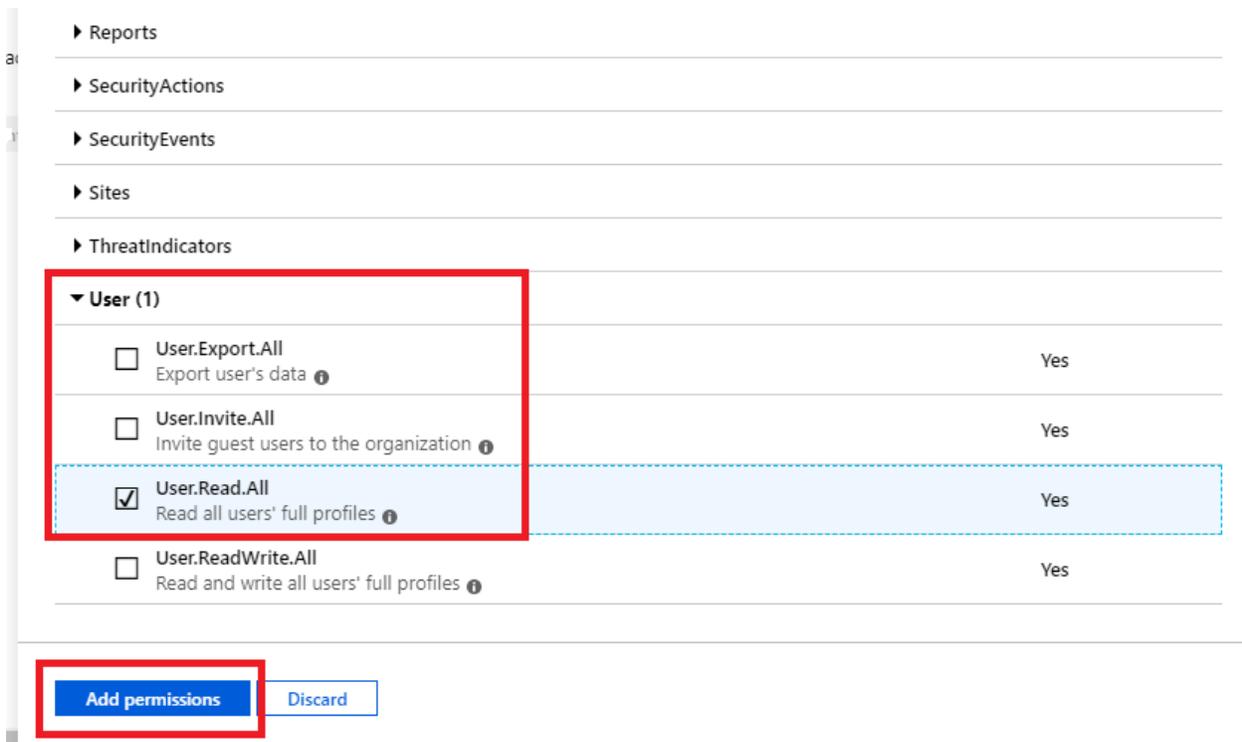


11. Scroll down to “Group”, expand it, select “Group.Read.All.”



12. Scroll down to “User”, expand it, select “User.Read.All.”

13. Click “Add permissions.”

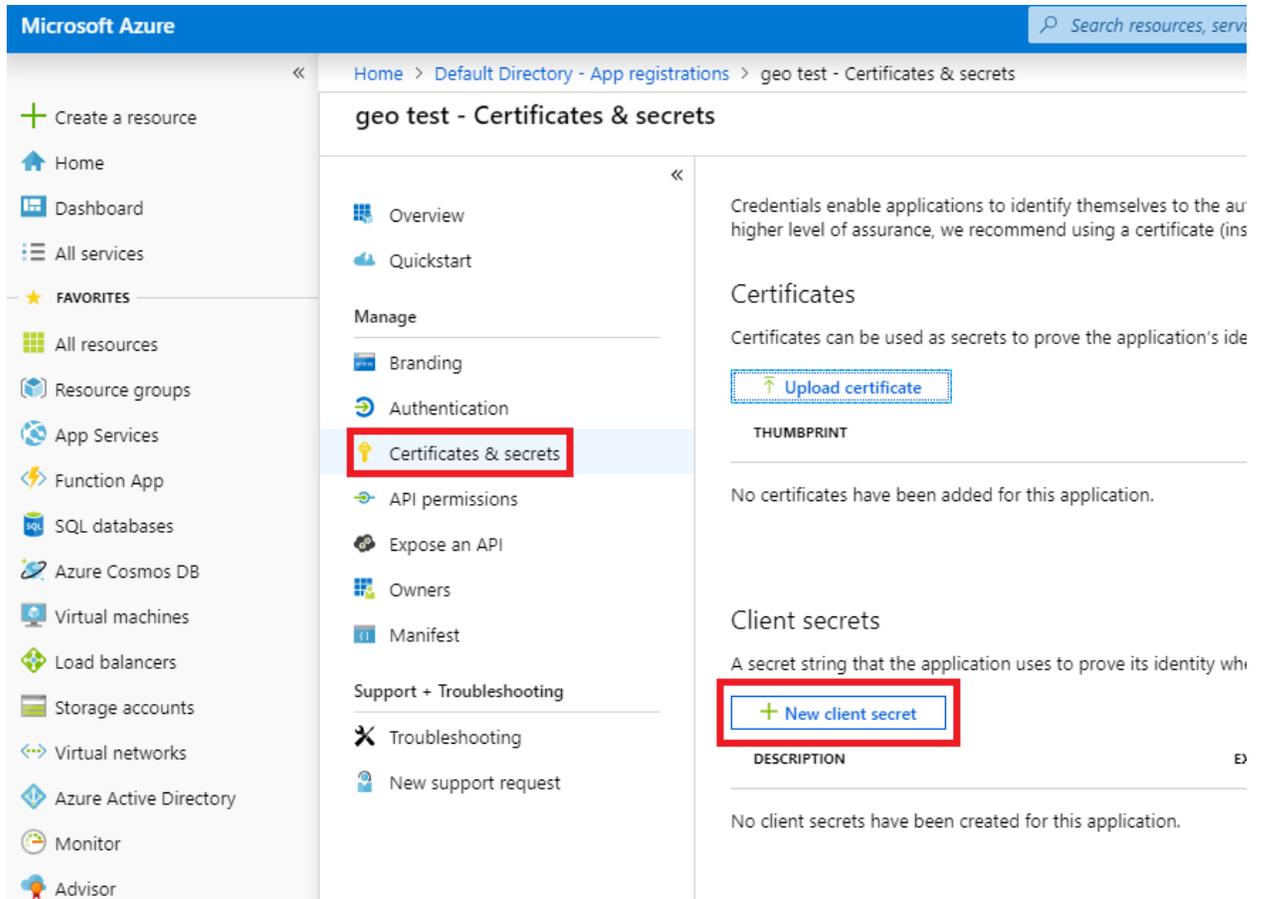


14. From the API Permissions page, click “Grant admin consent for Default Directory” button. This action requires admin level access.

The screenshot shows the Microsoft Azure portal interface. The left-hand navigation pane includes options like 'Create a resource', 'Home', 'Dashboard', and 'All services'. The main content area is titled 'Darweb ID Test - API permissions'. It features a sub-menu with 'Overview', 'Quickstart', and 'Manage' (which includes 'API permissions'). The 'API permissions' section displays a table of permissions for 'Microsoft Graph (5)'. Below the table, there is a 'Grant consent' section with a button labeled 'Grant admin consent for Default Directory' highlighted by a red box. Another button with the same text is visible at the bottom right of the page.

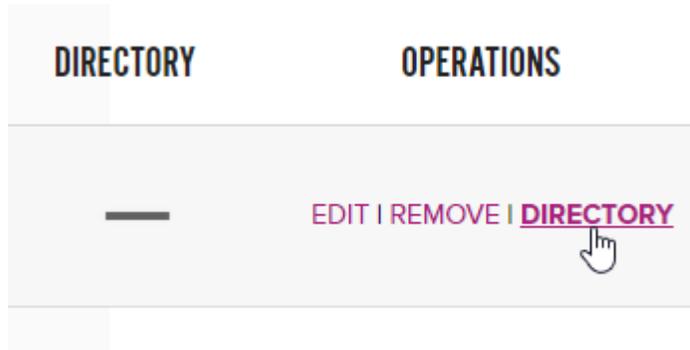
API / PERMISSIONS NAME	TYPE	DESCRIPTION
▼ Microsoft Graph (5)		
Directory.ReadWrite.All	Application	Read and
Group.Read.All	Application	Read all g
Group.ReadWrite.All	Application	Read and
User.Read	Delegated	Sign in an
User.ReadWrite.All	Application	Read and

15. Click on “Certificates & secrets.”
16. Click “New client secret.” This Secret will be needed to authenticate with Dark Web ID. **Important: The Client Secret is only visible at this time and should be safely recorded or used, as it will not be retrievable later.**



AUTHENTICATE WITH DARK WEB ID

17. Log in to secure.darkwebid.com.
18. Click “Directory” next to the Organization you would like to associate with your Active Directory.



19. Enter the Tenant ID and Client ID from step 6 and the Client Secret from step 16.

DIRECTORIES

Credentials

Tenant Id *

Active Directory Tenant Id

Client Id *

Active Directory Client Id

Client Secret *

Active Directory Client Secret

DISCARD CHANGES

SUBMIT



20. Select which AD Group you would like to associate with your Organization and spot check the first 20 entries to confirm it is correct. Click Submit.

DIRECTORIES

Credentials +

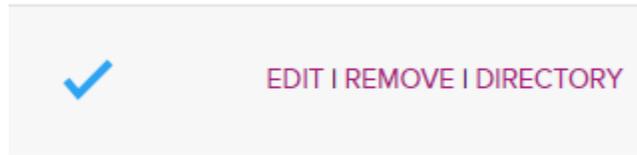
Group Selection *

All 

First 20 Users in this Group -

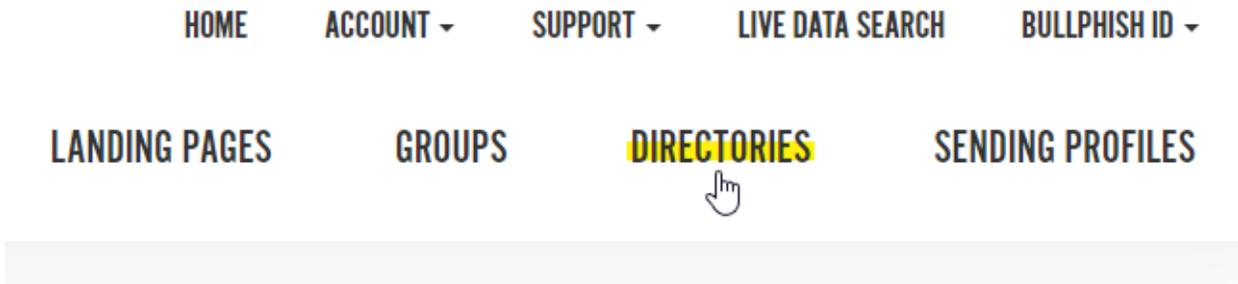
FIRST NAME	LAST NAME	POSITION
------------	-----------	----------

21. If successful, you should receive a visual indicator on the Partner Dashboard next to that Organization. This Active Directory Group can now be used in BullPhish ID.



USING ACTIVE DIRECTORY IN BULLPHISH ID

22. Navigate to BullPhish ID (Phishing or Training) and click on “Directories.”



23. Select the Organization | Active Directory Group combination you would like to import.

IMPORT DIRECTORY

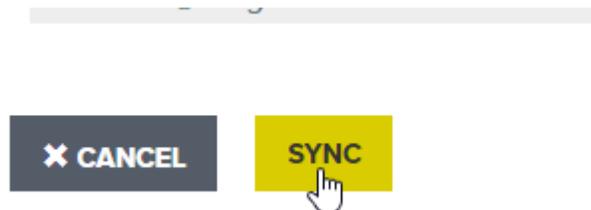
Associated Organizations with Directory *

ID Agent Org | All

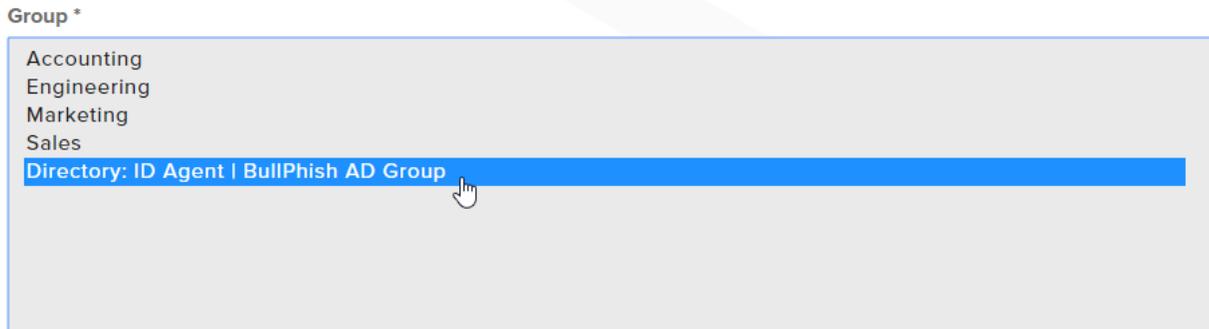
Select the Organization's Directory you would like to import.



24. If you received any errors, you can make adjustments in your Azure Active Directory group to address, then re-sync within BullPhish ID by clicking “View” on a Directory, then “Sync.”



25. Use the Active Directory Group to create a campaign! **The Active Directory Group will automatically sync with Azure upon campaign creation before any campaign emails are sent.**



If you have questions or need further assistance, please contact your Partner Success Manager or email support@idagent.com.