DARKWEB ID

AZURE ACTIVE DIRECTORY USER GUIDE

VERSION 1.0

IDAGENT
A Kaseya COMPANY

support@idagent.com

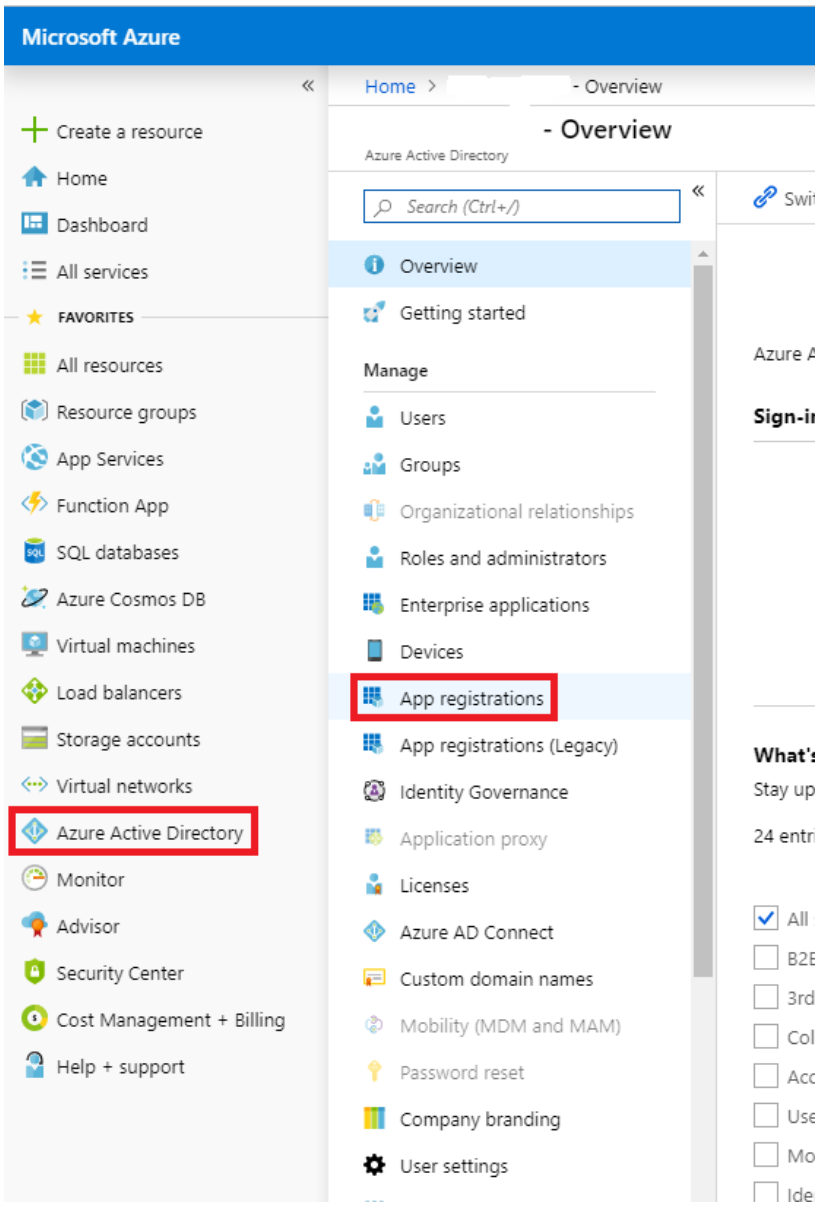
Table of Contents

PREREQUISITES

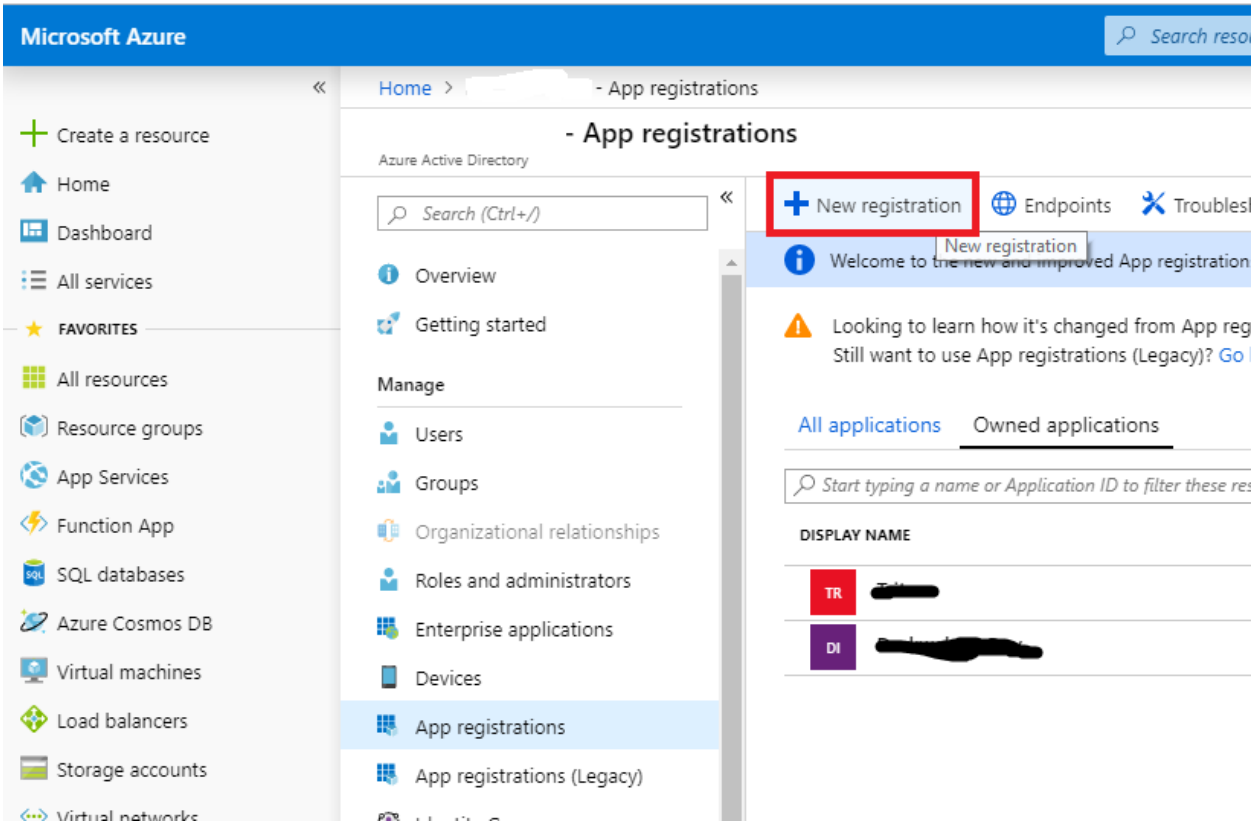
This integration is specifically for Azure's Cloud Based Active Directory (AD). To use an Active Directory Group in Dark Web ID™ and BullPhish ID™, it will need to contain information for "givenName", "surname", "jobTitle", and "mail" to translate to BullPhish ID. If "jobTitle" is null, it will default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

GRANT API ACCESS TO AZURE AD

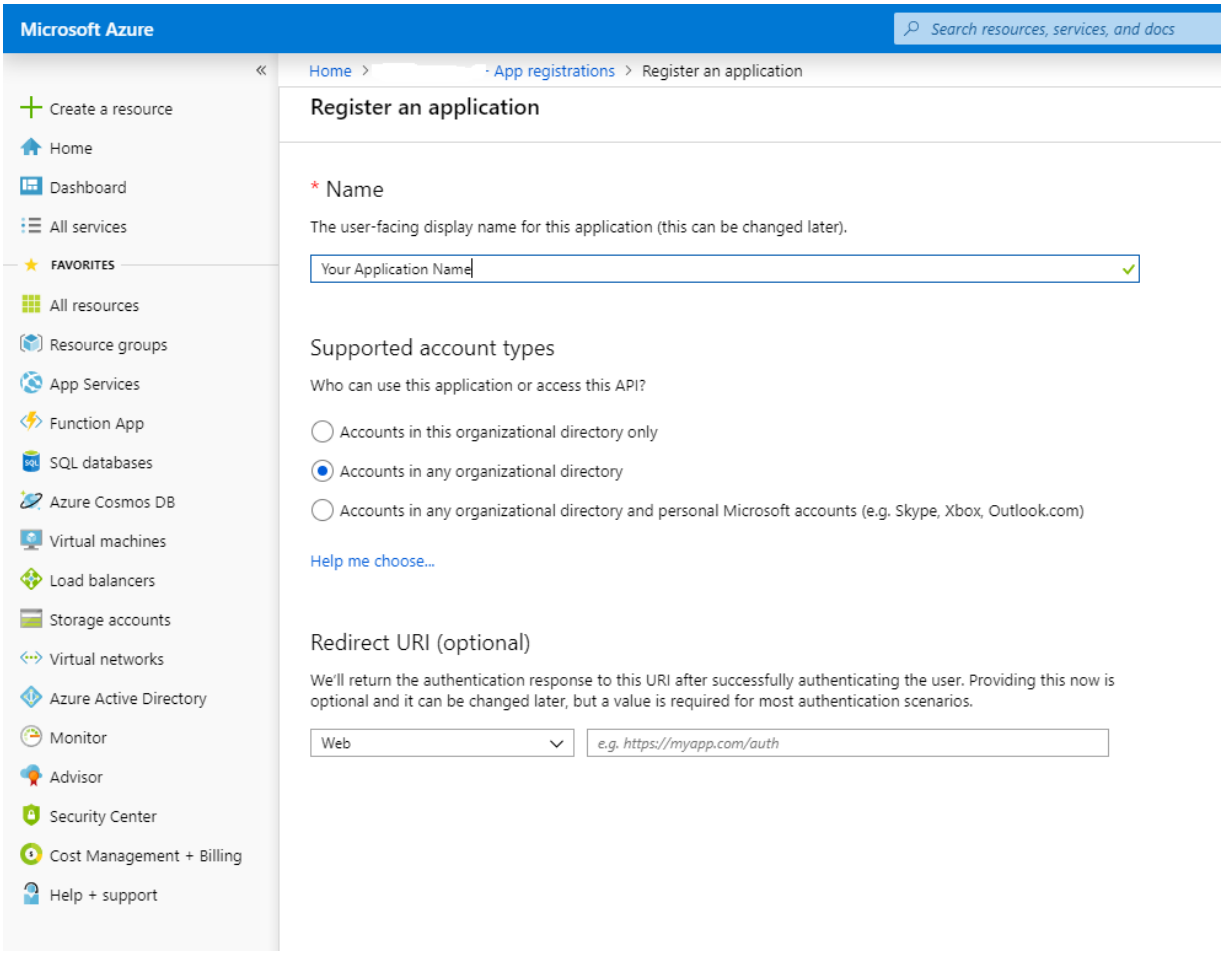
1. Log into Azure Portal: https://portal.azure.com.
2. Click on "Azure Active Directory" in the left navigation menu.
3. Click on "App registrations" on the secondary menu.



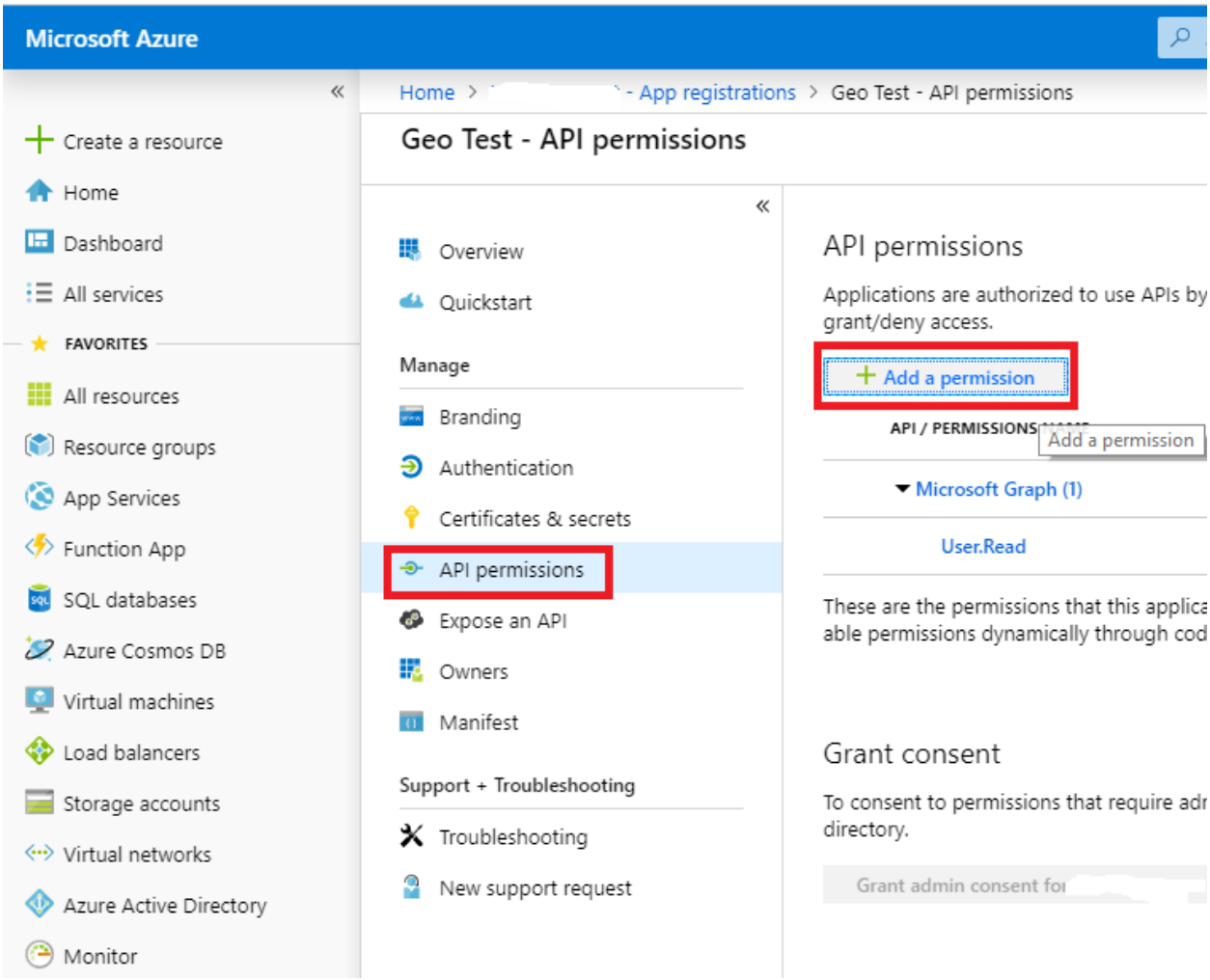
4. Click “New registration.”



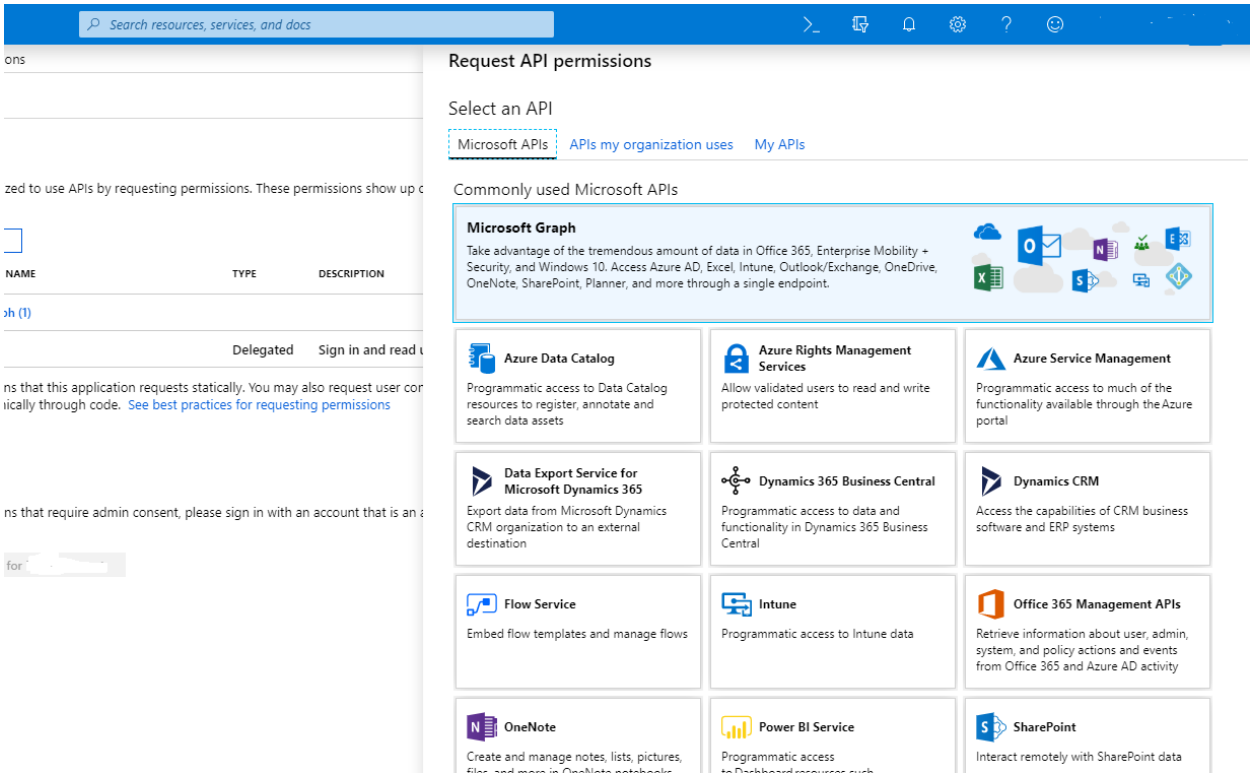
5. On the “Register an application” page, provide application name, and select “Accounts in any organizational directory” from the “Supported account types” radio button list.



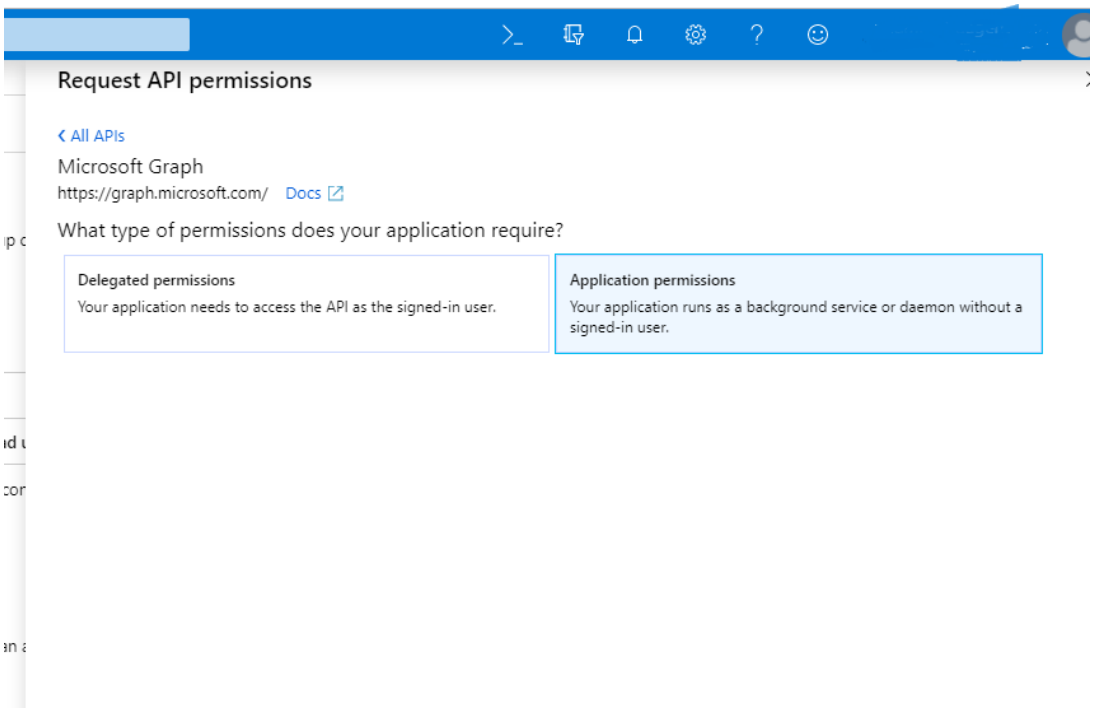
6. **Application ID, Tenant ID,** and Object ID are displayed. These will be needed to authenticate in Dark Web ID (Not Pictured).
7. Click “API permissions.”
8. Click “Add a permission.”



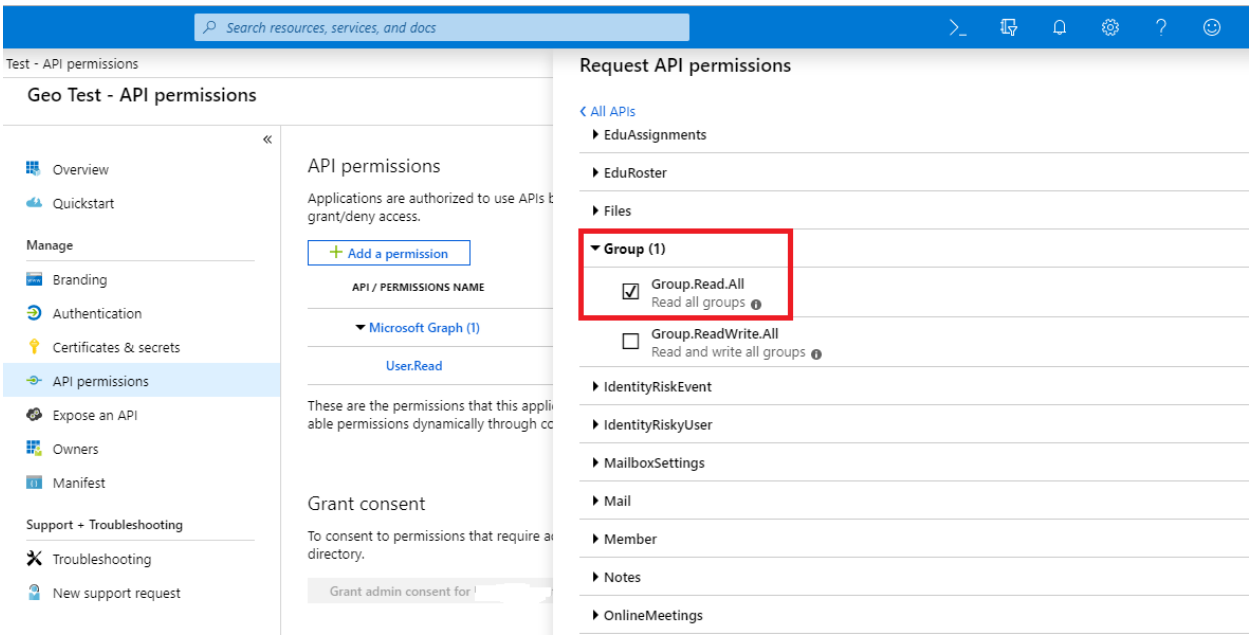
9. On the right-side menu, click “Microsoft Graph.”



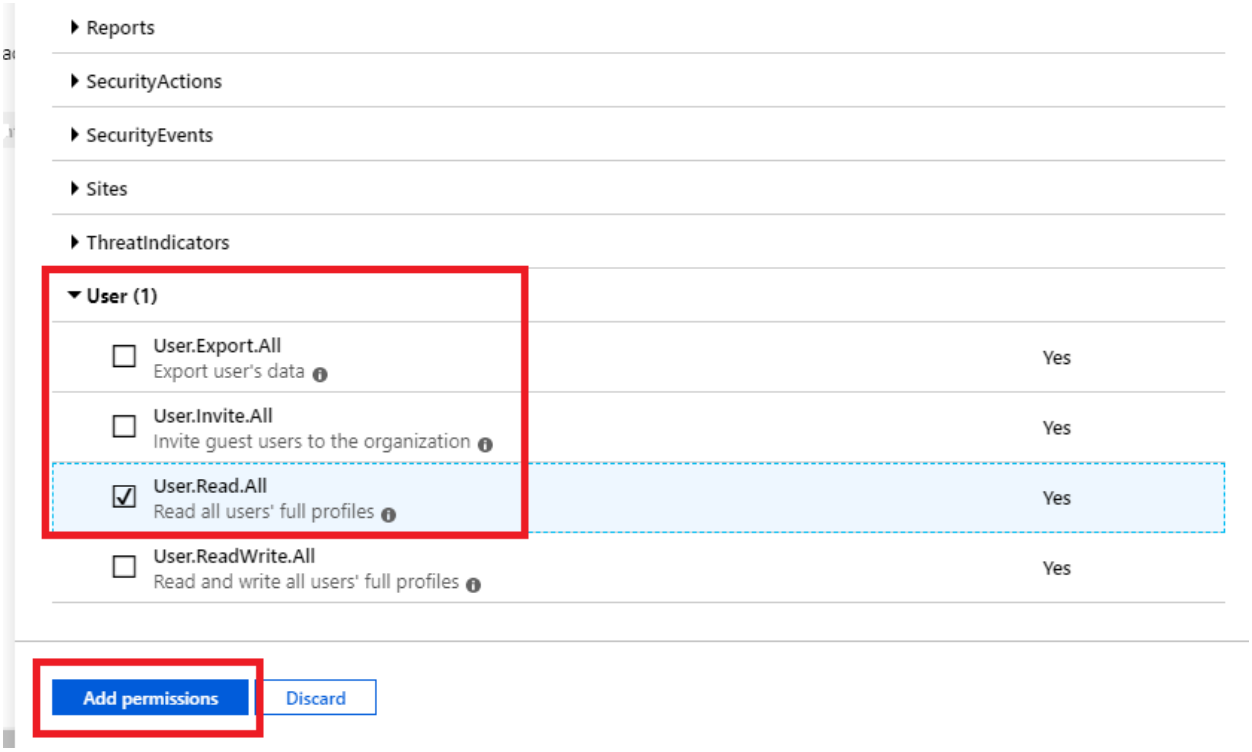
10. Click “Application permissions.”



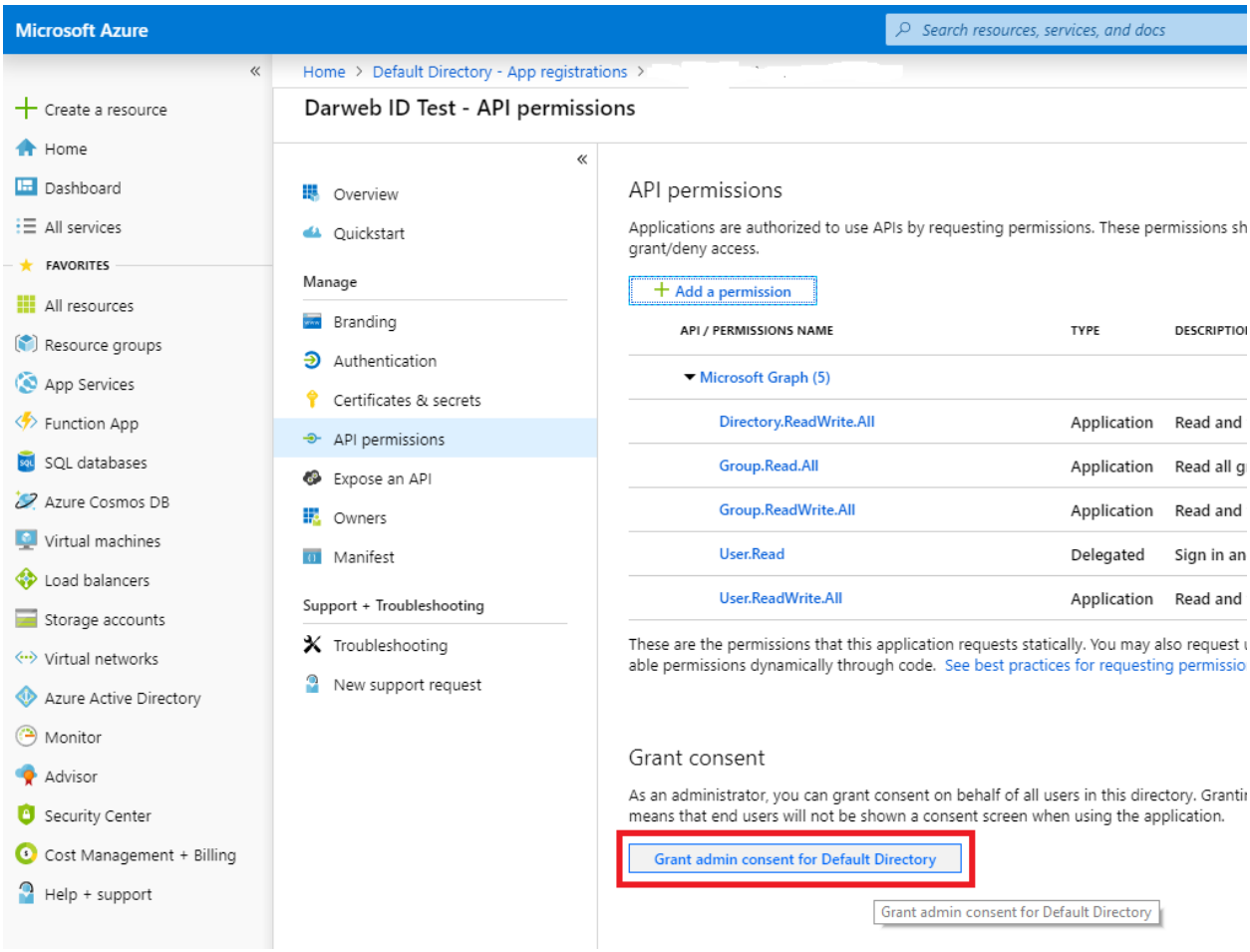
11. Scroll down to “Group”, expand it, select “Group.Read.All.”



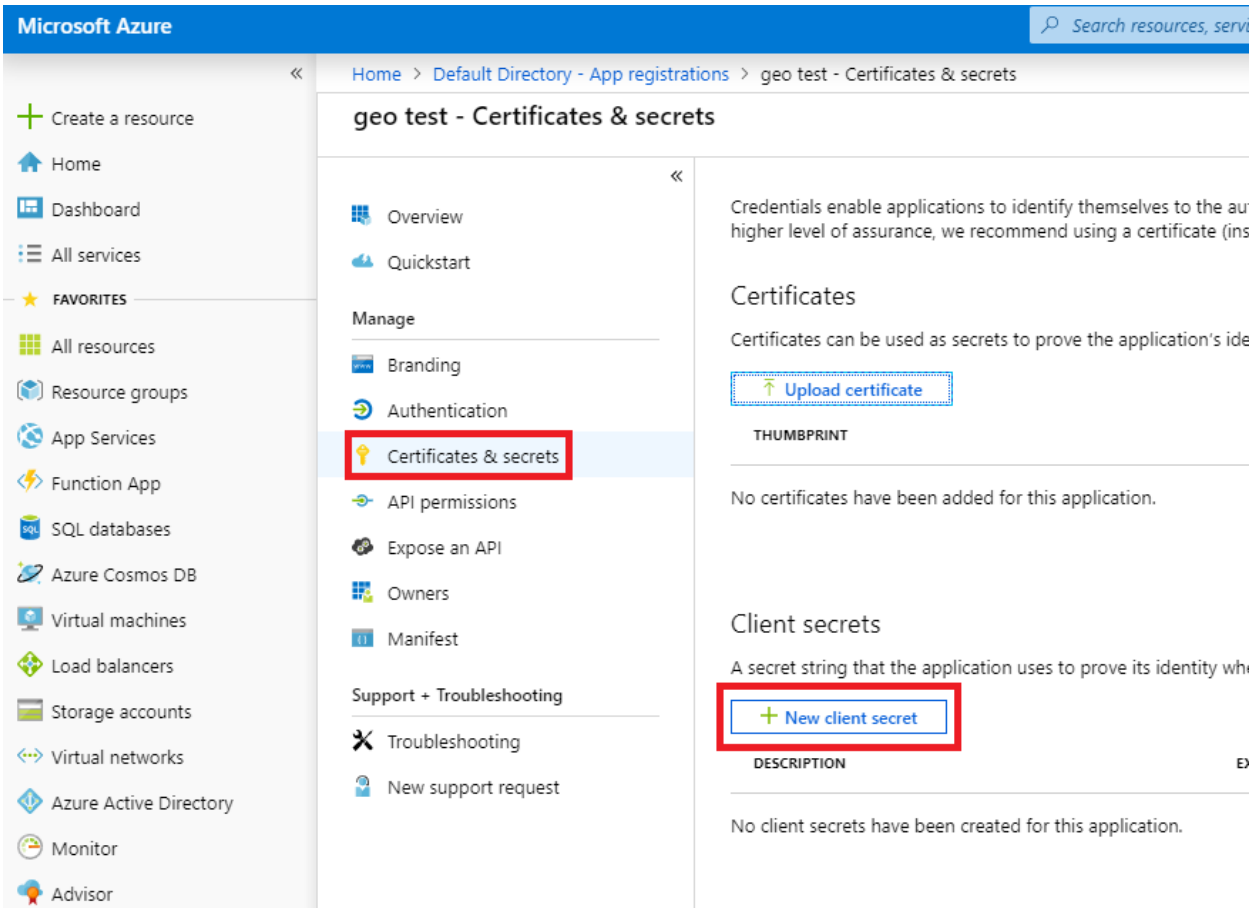
12. Scroll down to “User”, expand it, select “User.Read.All.”
13. Click “Add permissions.”



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

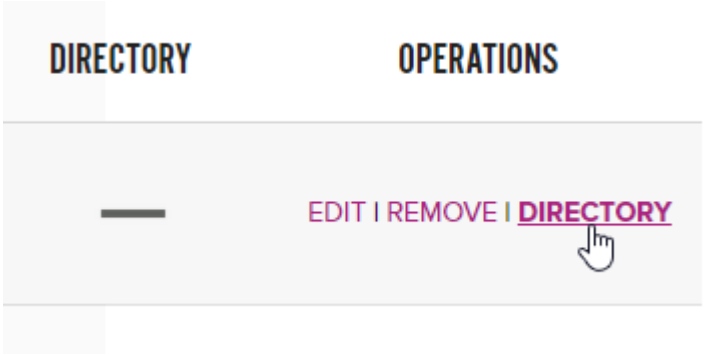


15. Click on “Certificates & secrets.”
16. Click “New client secret.” This Secret will be needed to authenticate with Dark Web ID. **Important: The Client Secret is only visible at this time and should be safely recorded or used, as it will not be retrievable later.**

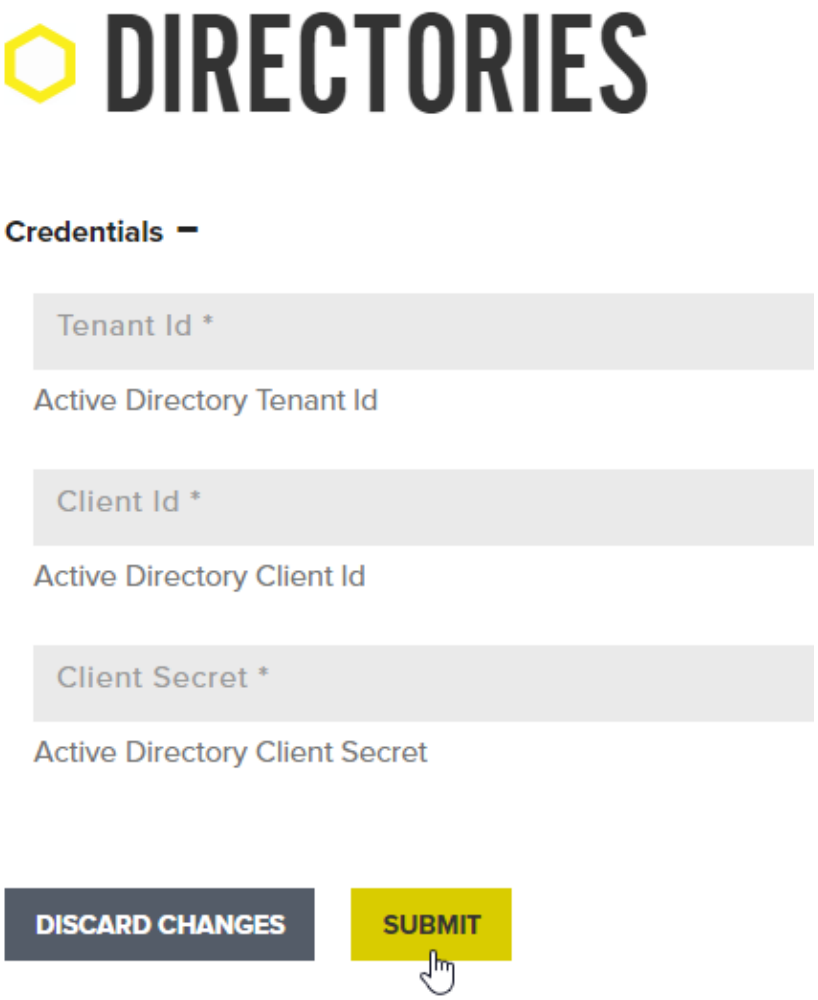


AUTHENTICATE WITH DARK WEB ID

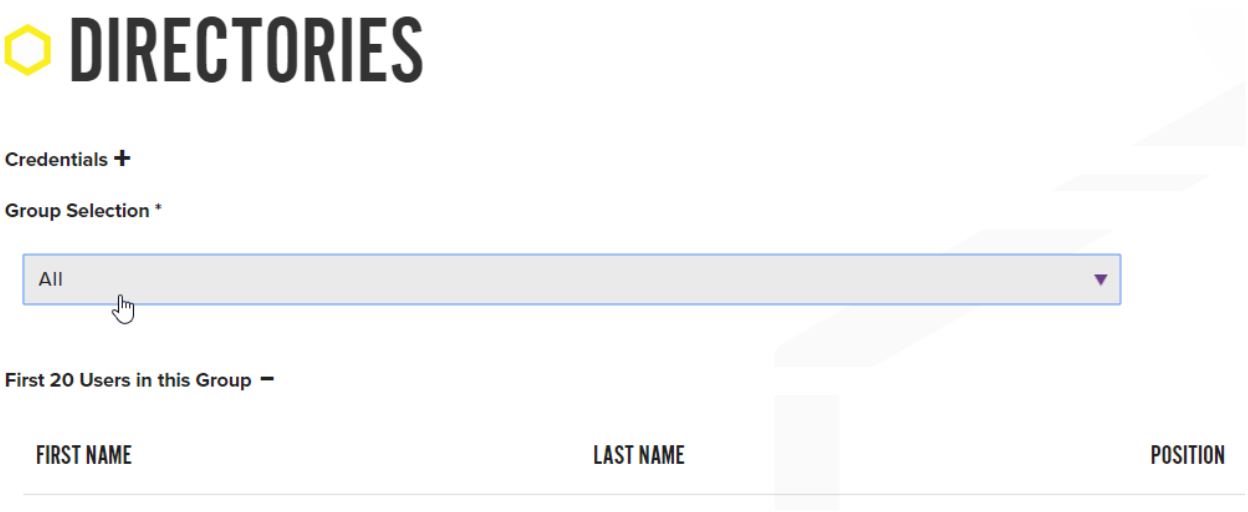
17. Log in to secure.darkwebid.com.
18. Click “Directory” next to the Organization you would like to associate with your Active Directory.



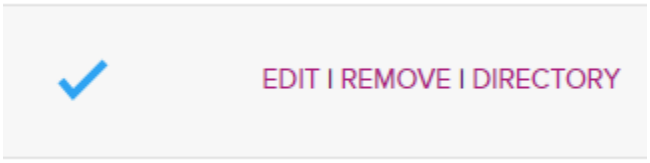
19. Enter the Tenant ID and Client ID from step 6 and the Client Secret from step 16.



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.

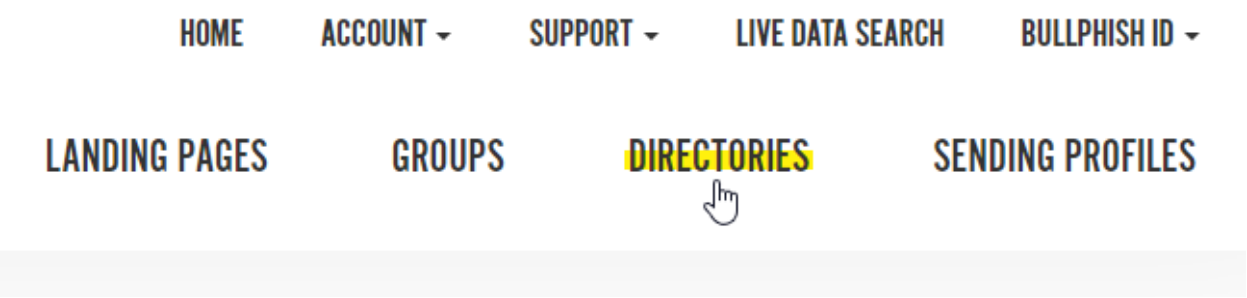


21. If successful, you should receive a visual indicator on the Partner Dashboard next to that Organization. This Active Directory Group can now be used in BullPhish ID.



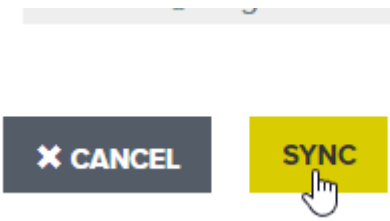
USING ACTIVE DIRECTORY IN BULLPHISH ID

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

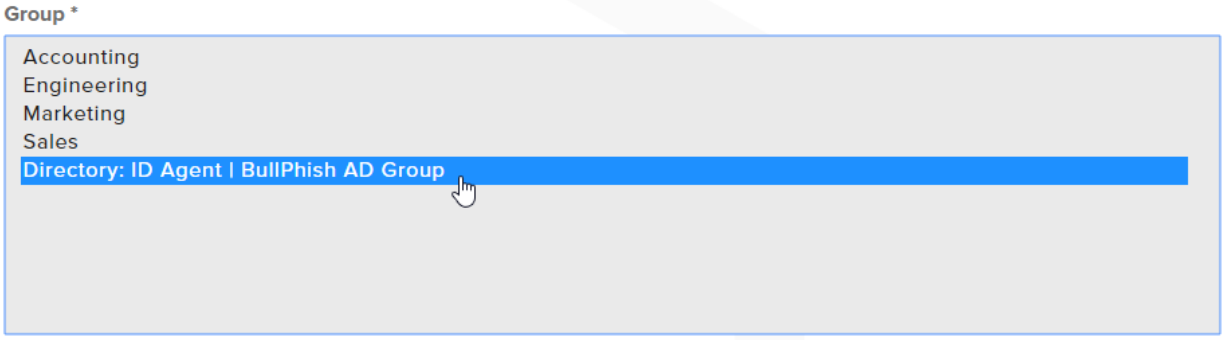


23. Select the Organization | Active Directory Group combination you would like to import.

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.