Datadog MS Defender 365 - App registrator

Introduction

azure_app_registrator.py is a python script which takes care of the following operations.

- Creates app on Azure portal
- Assign necessary permissions to run the Microsoft Defender integration on Datadog
- Grant admin consent to all these permissions
- Generate client secret
- Installs datadog-api-client library

After executing the script, an application will be created with…

- All below permissions (granted with admin consent).

  For Microsoft Graph ->

  - SecurityAlert.Read.All
  - SecurityIncident.Read.All
  - SecurityEvents.Read.All
  - ThreatHunting.Read.All
  - Directory.Read.All
  - User.Read.All

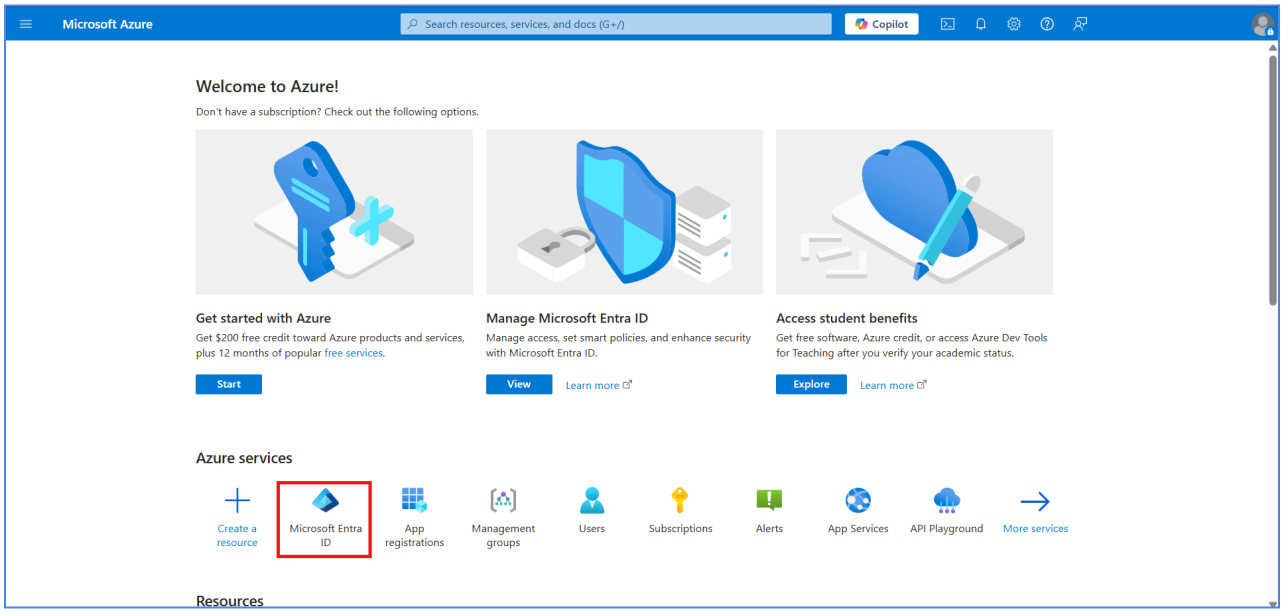
  For WindowsDefenderATP ->

  - Vulnerability.Read.All
  - Score.Read.All
  - Software.Read.All
  - Machine.Read.All
  - Alert.Read.All
- tenant_id, client_id and client_secret will be shown which user can use in conf.yaml to run this integration.
- Library **datadog-api-client** will be installed which is necessary to run this integration.

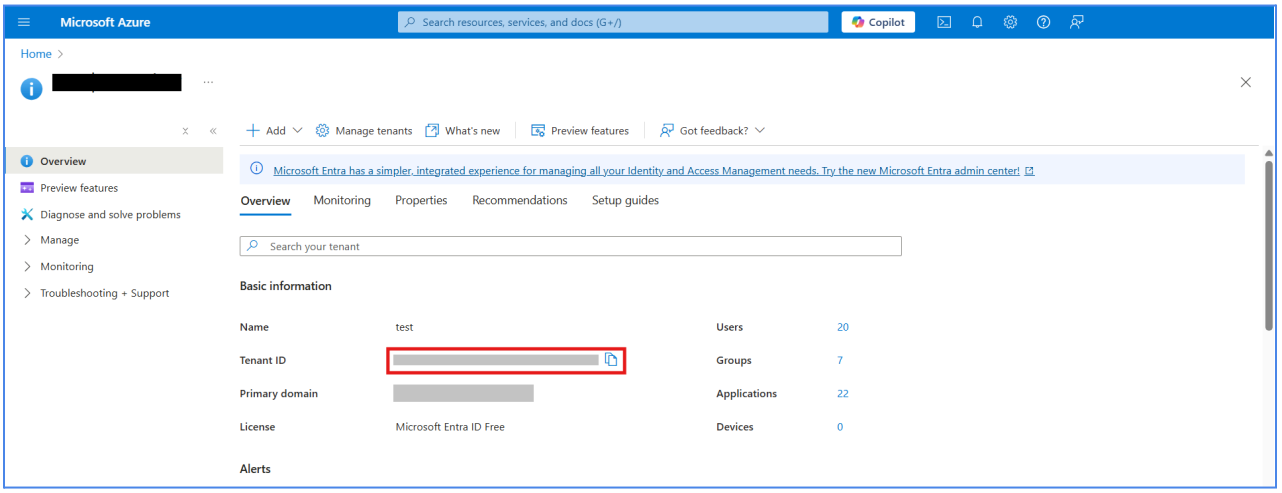
Prerequisites

You should have **tenant_id** which will be asked in this script as input.
If you don't have one, follow below steps to retrieve it. (For more information, visit how-to-find-tenant)

1. Login to your Azure portal and go to **Microsoft Entra ID.**

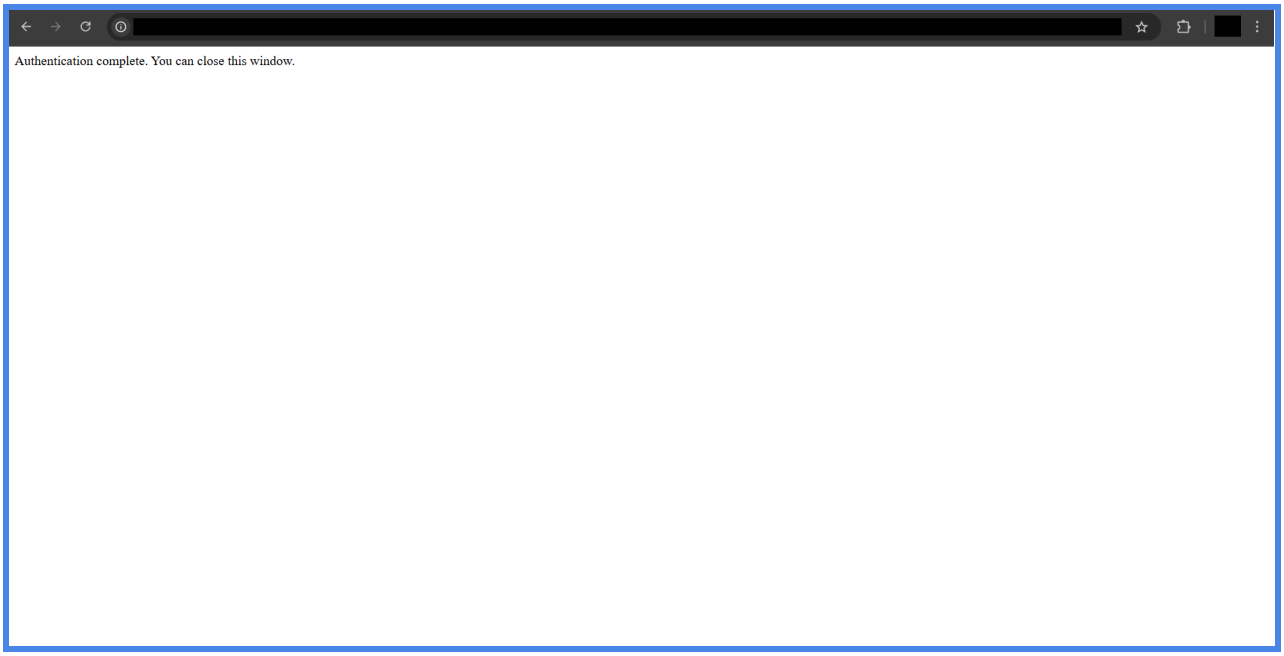


2. You will find the Tenant ID listed in the **Overview** section. Make sure to note it down.



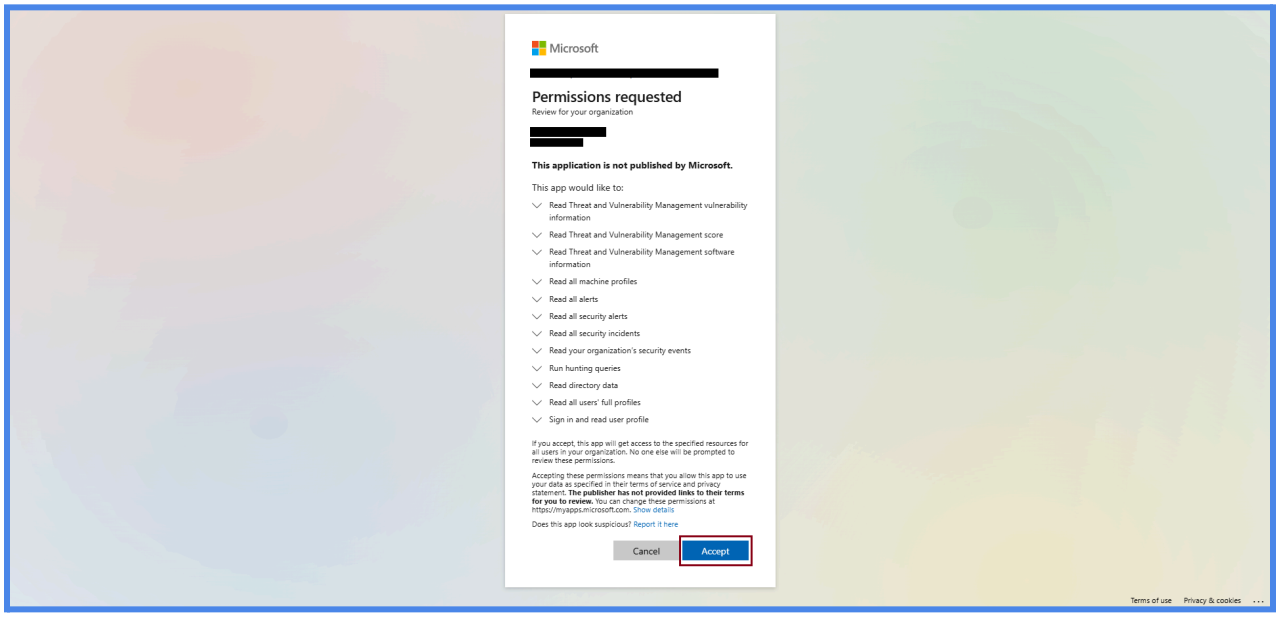
How to use this script

1. Run this command **from where the datadog-agent is installed**:
    a. **Linux:** `sudo /opt/datadog-agent/embedded/bin/python azure_app_registrator.py`
    b. **Windows**: Open command prompt **as administrator** and run below command. `"%programfiles%\Datadog\Datadog Agent\embedded3\python.exe" azure_app_registrator.py`
    c. **macOS**: `sudo /opt/datadog-agent/embedded/bin/python azure_app_registrator.py`
2. You will be prompted to enter tenant_id. Please enter the Microsoft Entra ID **tenant_id** that you copied previously.
3. After entering the **tenant_id**, you will be redirected to your browser for authentication. **Authenticate with the account on which the tenant is registered**. Upon successful authentication, you will see a page similar to the one shown below.

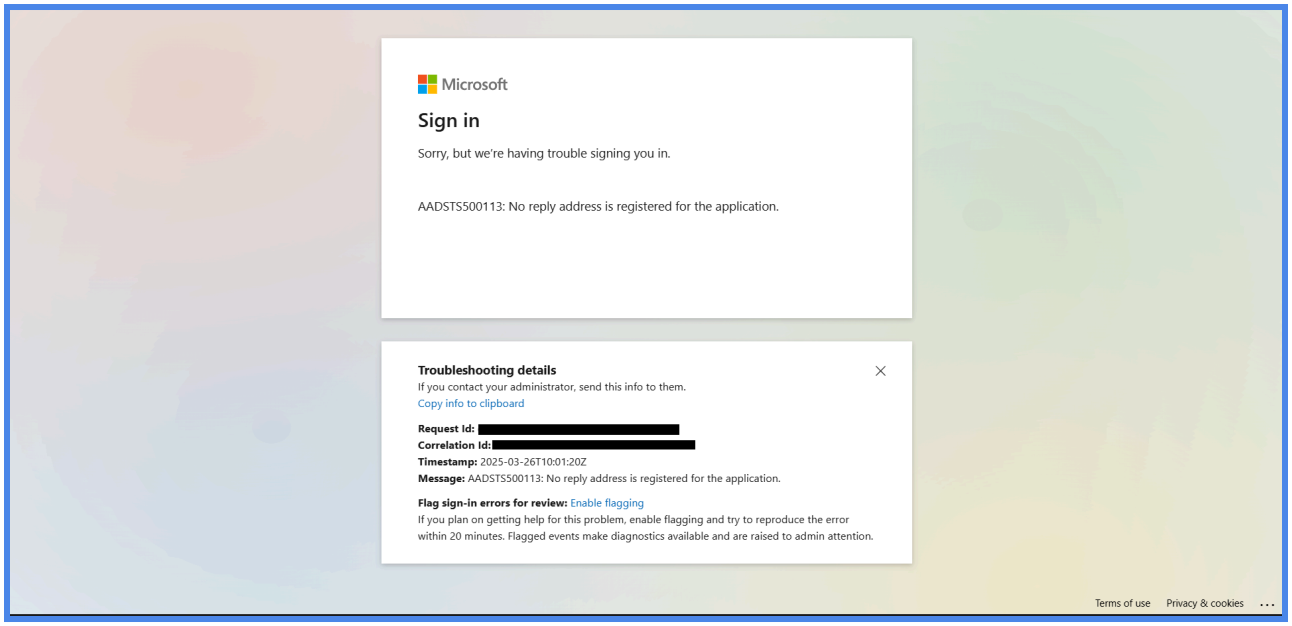


4. After authentication, an application named **datadog-ms-defender-365** will be created, and the necessary permissions will be assigned.
5. Once the permissions are granted, you will see the message **"Permissions assigned successfully."** displayed on the console.

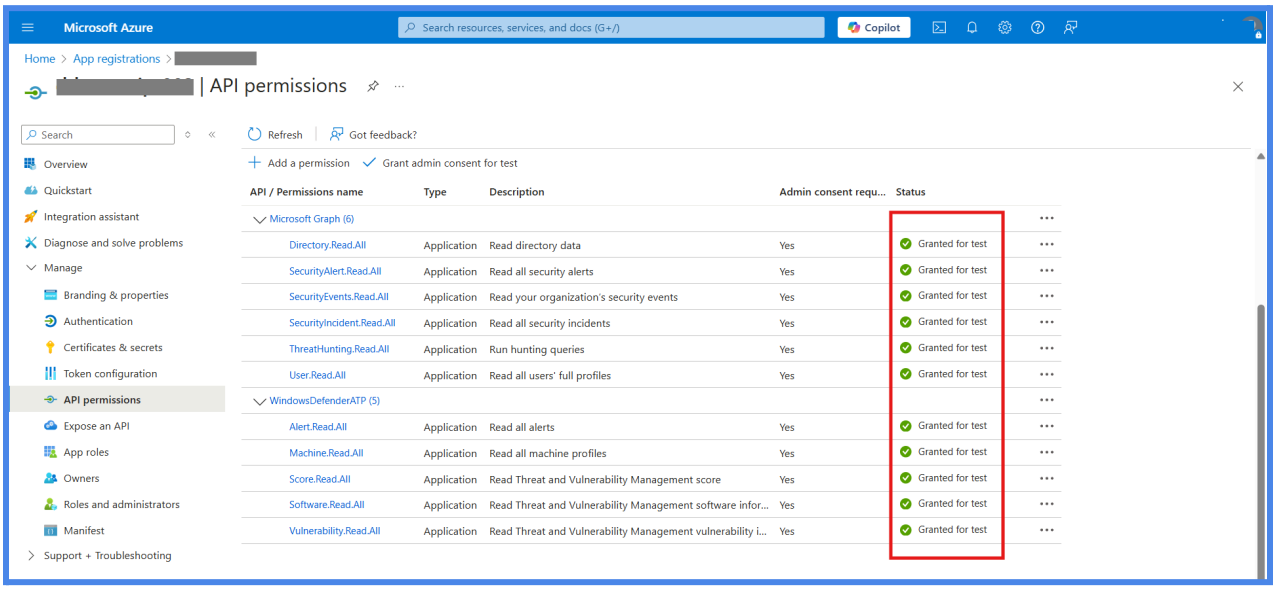
6. Next, you will be redirected to your browser to grant **admin consent**. Select the same account, and you will see a list of permissions that require admin consent, as shown in the screenshot below. Click **"Accept"** to proceed.



7. You will now see a page displaying the message *"No reply address is registered for the application."* You can safely ignore this message. If you encounter a different error message at this step, refer to the Troubleshooting section.

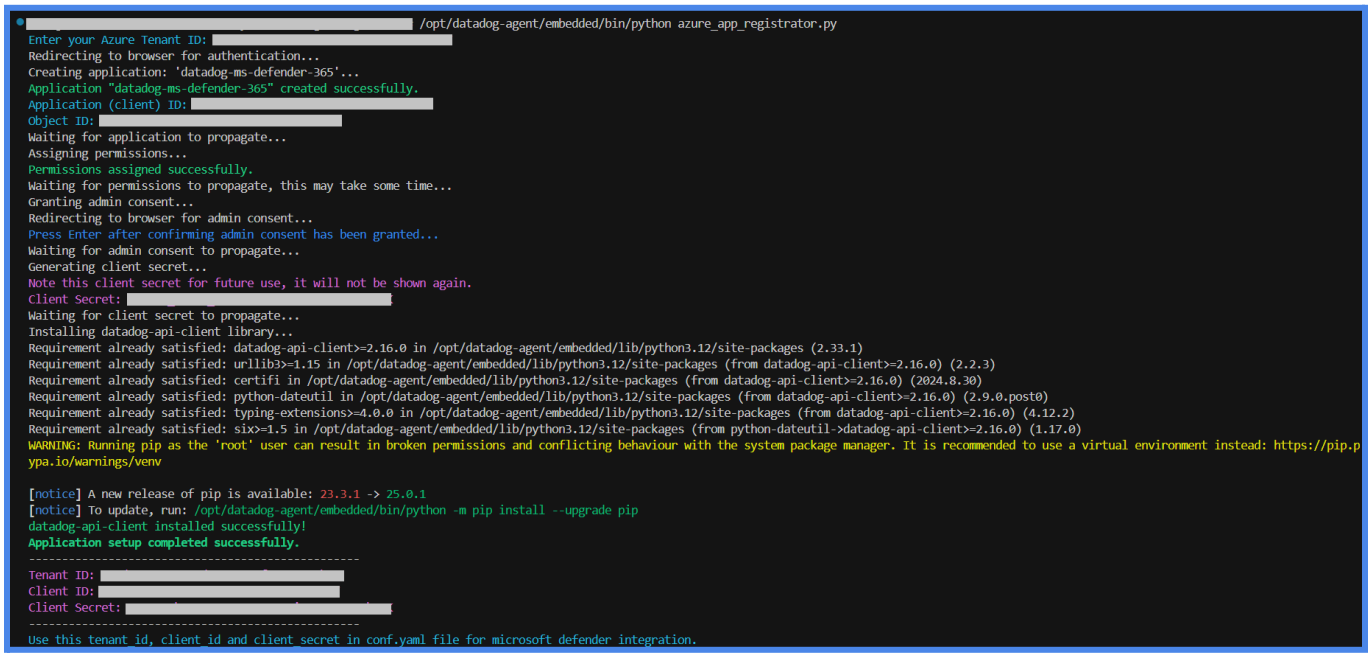


8. Go to Azure portal Now, navigate to the **Azure portal** > **App registrations** > Click on your created application **"datadog-ms-defender-365"** > **API permissions** in the left sidebar. Reload the browser window and verify that **admin consent** has been granted. You should see **“Granted for test”** under Status column.



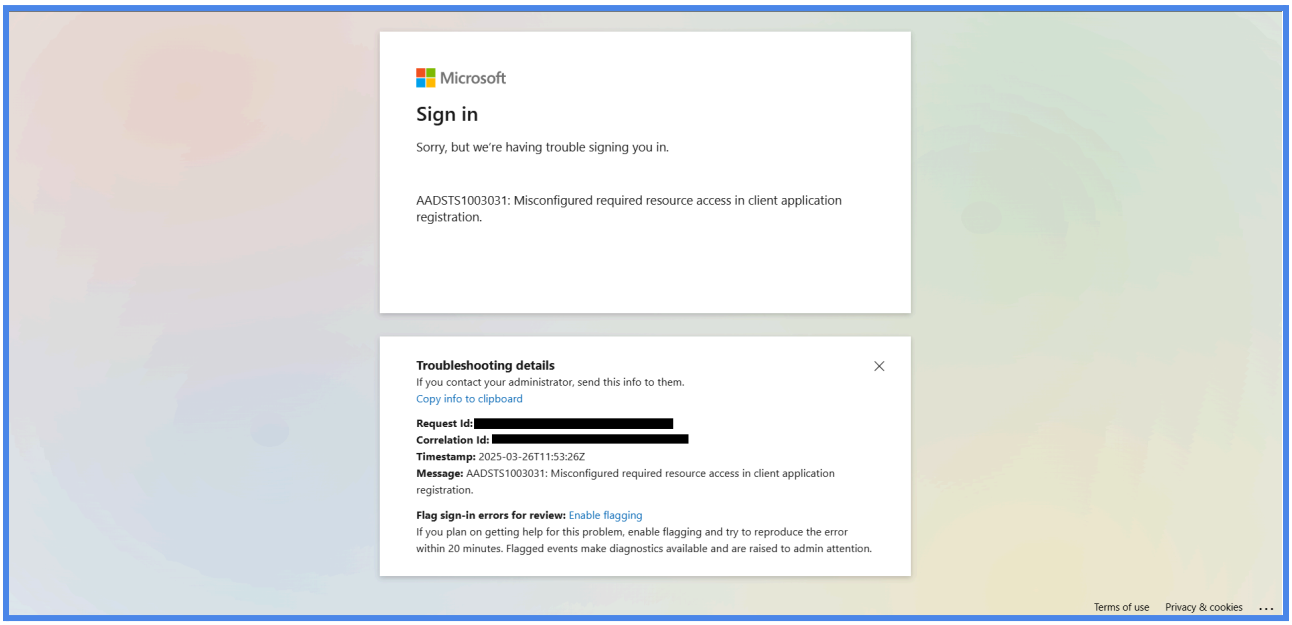
9. Return to the console and press **Enter** after verifying that admin consent has been granted for all permissions.
10. Your **client secret** will now be generated and displayed on the console. Note that this client secret is **only shown once at the time of creation** and will not be visible again in the Azure portal for security reasons. **Make sure to save it for future use.**
11. Next, the **datadog-api-client** library will be installed.
12. Once the setup is complete, you will see the message **"Application setup completed successfully."**
13. The **tenant_id** and **client_id** will also be displayed on the console. Use all three values (tenant_id, client_id, and client_secret) in the **conf.yaml** file for the **Microsoft Defender** integration.

Your console will look like this:



Troubleshooting

- If you encounter the issue below or any other problem while granting admin consent, wait for about 20 seconds and then reload this same page. The **admin consent page** should appear again. Click **"Accept"** and proceed.
- After granting admin consent, verify it by navigating to **Azure portal** > **App registrations** > Select your application **"datadog-ms-defender-365"** > **API permissions** (left sidebar). Reload the browser window and confirm that admin consent has been granted.



- If you are facing any permission related issue while running this script, run below commands before running the script
  - Linux
    - `sudo -Hu dd-agent /opt/datadog-agent/embedded/bin/pip install requests`
    - `sudo -Hu dd-agent /opt/datadog-agent/embedded/bin/pip install azure.identity`
  - Windows
    - `"%programfiles%\Datadog\Datadog Agent\embedded\python.exe" -m pip install requests`
    - `"%programfiles%\Datadog\Datadog Agent\embedded\python.exe" -m pip install azure.identity`
  - macOS
    - `sudo /opt/datadog-agent/embedded/bin/pip install requests`
    - `sudo /opt/datadog-agent/embedded/bin/pip install azure.identity`