Unknown Cyber Customer Setup (Azure)

Contents

[1. Open to portal.azure.com and authenticate with your company credentials. 2](#_Toc147951985)

[2. Create your App Registration 3](#_Toc147951986)

[3. Set Rights for your App Registration. 5](#_Toc147951987)

[4. Create the App Reg Secret 7](#_Toc147951988)

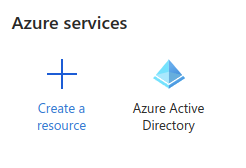
[5. Gather your information for Registering with Unknown Cyber. 9](#_Toc147951989)

[6. Setup Azure Sentinel 10](#_Toc147951990)

IMPORTANT!!!!!

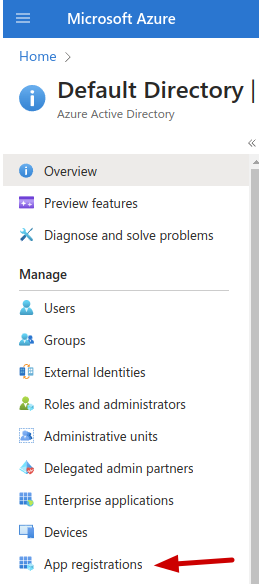
You must be a Global Administrator or have equivalent rights to complete this setup guide.

# Open to portal.azure.com and authenticate with your company credentials.

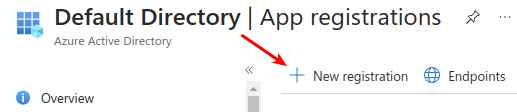


* Select Azure Active Directory

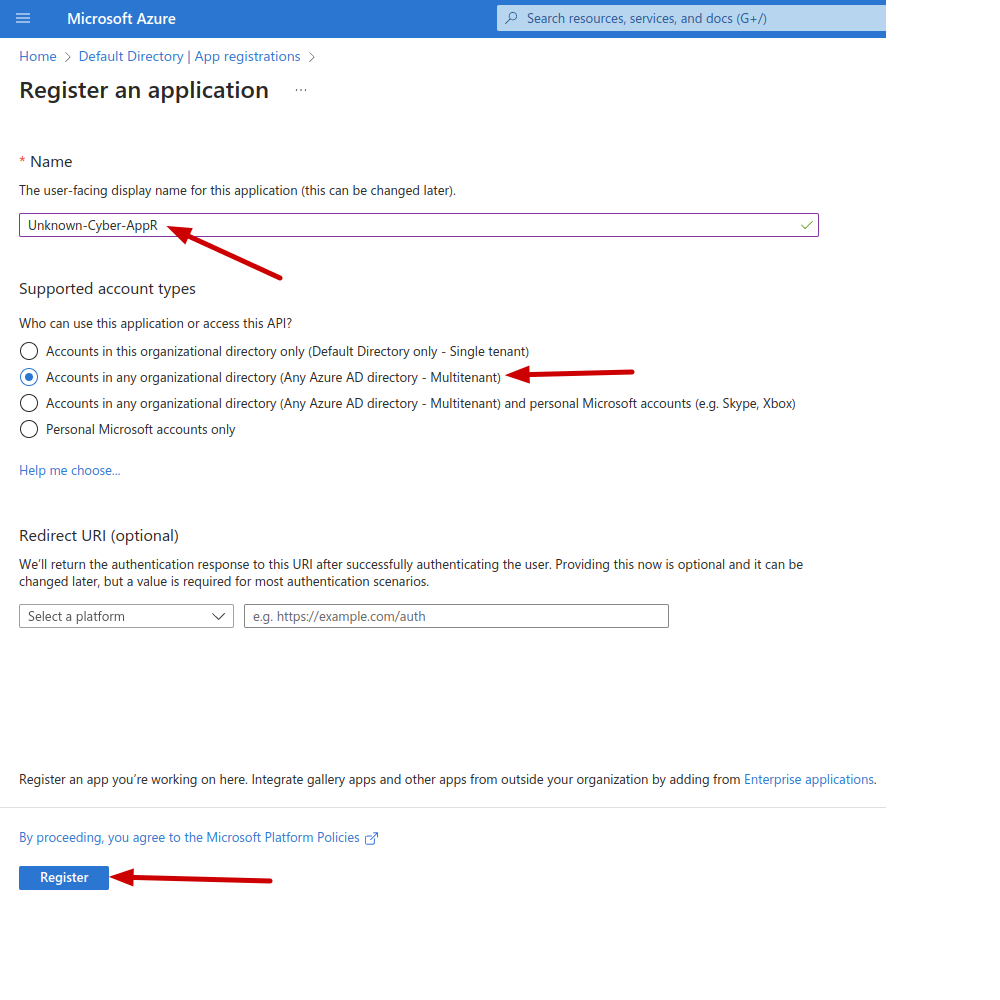
# Create your App Registration



* Scroll down and Select “App Registrations”



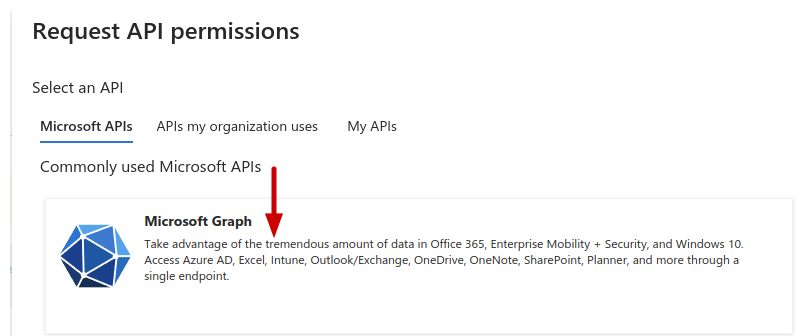
* Select New Registration



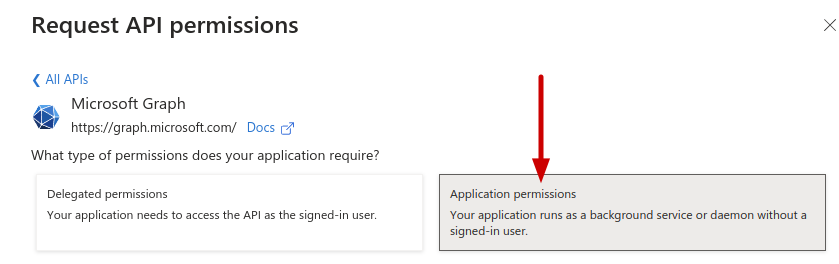
* We recommend the naming convention “Unknown-Cyber-AppR-CustomerName”
* Set for Multi-Tenant
* Click Register

# Set Rights for your App Registration.

* Open the Newly Created App Registration.
* Click on Add a Permission

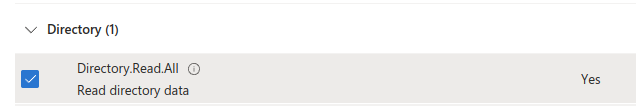


* Select Microsoft Graph



* Set to Application Permissions

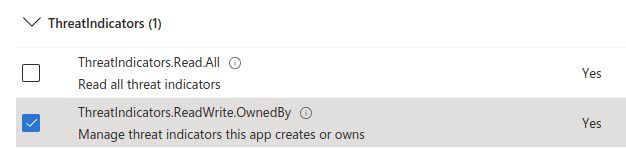
NOTE – *You can assign permissions individually and then click Add Permissions or select all permissions and then click Add Permissions. This guide users the latter method.*



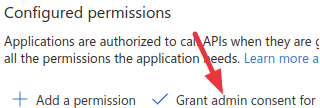
* Select Directory.Read.All



* Select “Mail → Mail.Read”

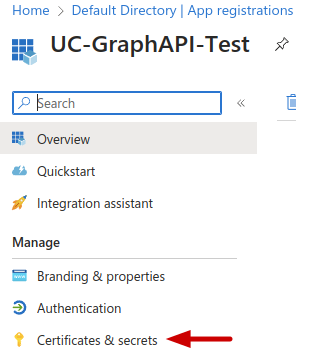


* Select “ThreatIndicators → ThreatIndicators.ReadWrite.OwnedBy”(NOTE – This is only needed if leveraging Sentinel for the Unknown Cyber IOC feed)
* Click “Add permissions” at the bottom of the screen.

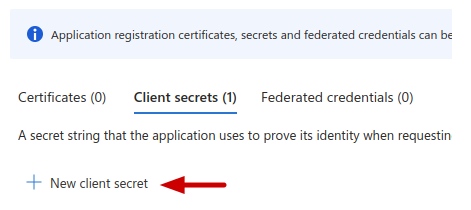


* Ensure that all permissions have “Grant admin consent for Default Directory (or your selected directory)” has a check mark, if not click the + Next to Grant and go through the wizard.

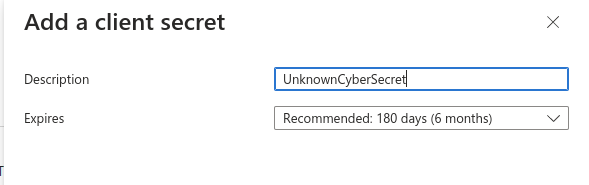
# Create the App Reg Secret



* Select “Certificates and secrets”



* Click “New client secret”

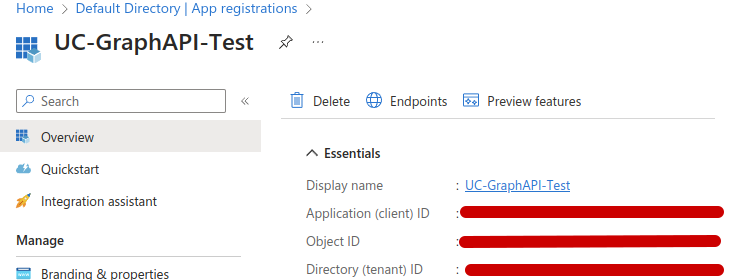


* Description “UnknownCyberSecret” is recommended
* Click Add

# Gather your information for Registering with Unknown Cyber.



* Click the Copy Icon in the “Value” Column and store that value securely. (NOTE: This value is only visible and able to be copied after initial creation.)

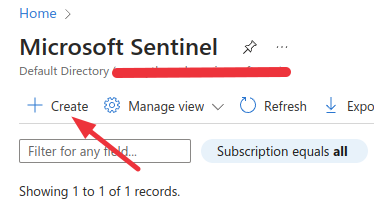


* Copy the “Application (client) ID
* Copy the “Directory (tenant) ID
* Proceed to Unknown Cyber Portal Setup and have the:
  + Application ID
  + Tenant ID
  + Secret Value

# Setup Azure Sentinel

**RECOMMENDED (Optional) – Enable Microsoft Sentinel**

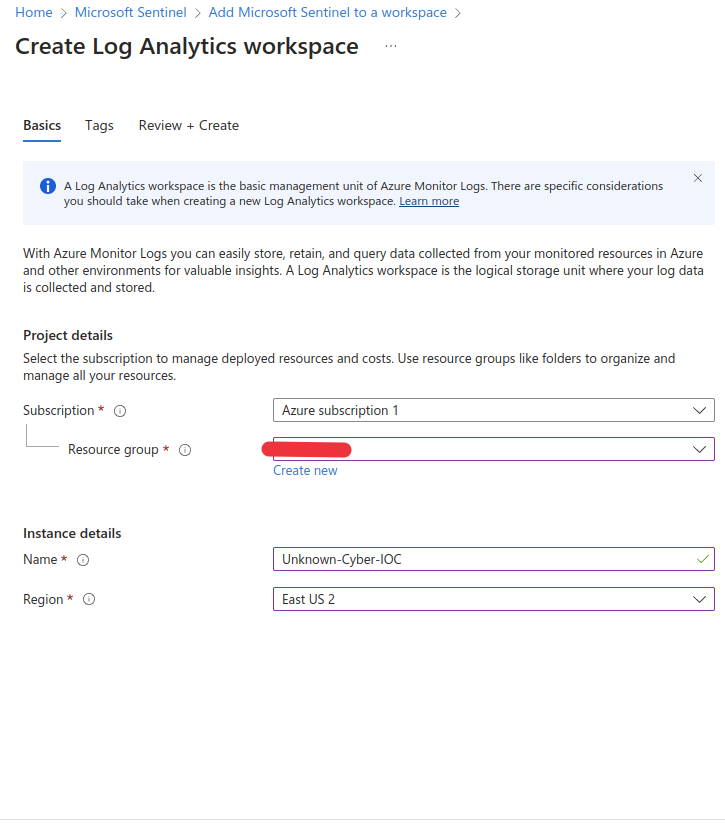
* Open “Microsoft Sentinel” from your Azure Portal.



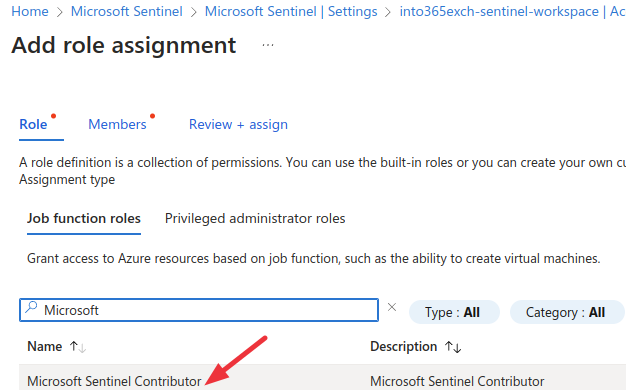
* Click “Create”



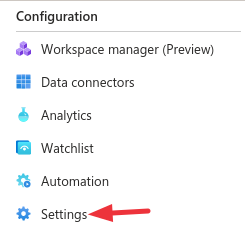
* Click “Create a new workspace”



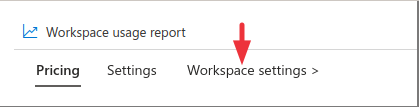
* Fill out the details in the Screen then click “Review + Create” wait for the validation to show green. Then click Create.
* Open your newly created Microsoft Sentinel Workspace and navigate to “Access Control (IAM) using the lefthand column.
* Click on “Add - > Add Role Assignment”



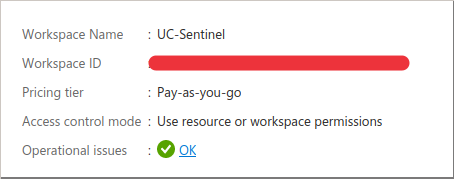
* Select “Microsoft Sentinel Contributor” for the Role
* For the Member, choose the App Reg you created earlier in this document.
* Move to Review and Assign, then click on “Review + assign”



* Select "Settings" Under Configuration inside Sentinel
* Select "Workspace Settings"



* Copy the "Workspace ID" for use in linking Sentinel to Unknown Cyber for receiving IOC feeds



* You can now proceed with the portal setup.