# Unknown Cyber Customer Setup (Azure)

## Contents

# IMPORTANT!!!!!

You must be a Global Administrator or have equivalent rights to complete this setup guide.
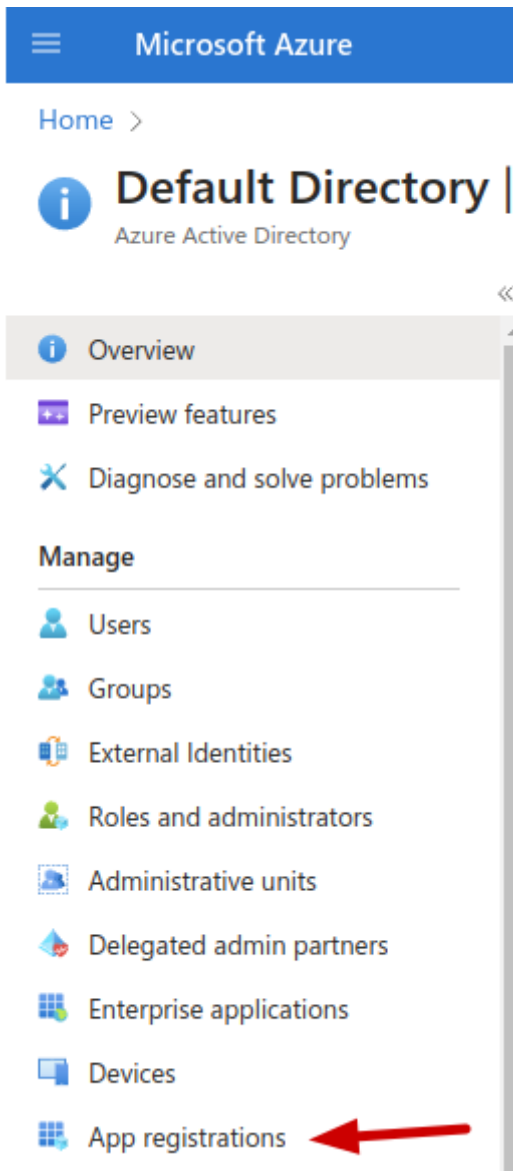
### 1. Open to portal.azure.com and authenticate with your company credentials.
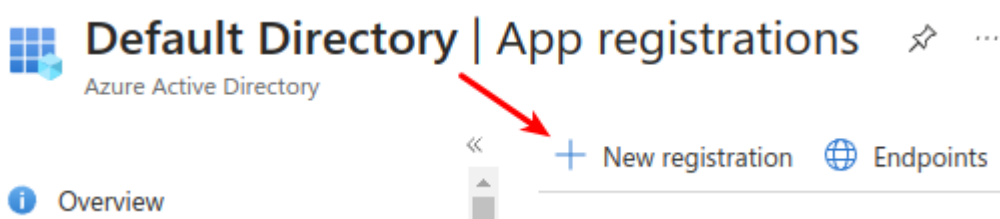
**Azure services**



- Select Azure Active Directory

## 2. 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

## 3. Set Rights for your App Registration.

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

### Request API permissions

Select an API

**Microsoft APIs**     APIs my organization uses     My APIs

Commonly used Microsoft APIs

**Microsoft Graph**
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

- Select Microsoft Graph

### Request API permissions                    ✕

❮ All APIs
Microsoft Graph
https://graph.microsoft.com/  Docs 🗗

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

- 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.

4. Create the App Reg Secret

Home > Default Directory | App registrations

### UC-GraphAPI-Test

Search

- Overview
- Quickstart
- Integration assistant

**Manage**

- Branding & properties
- Authentication
- Certificates & secrets ⬅
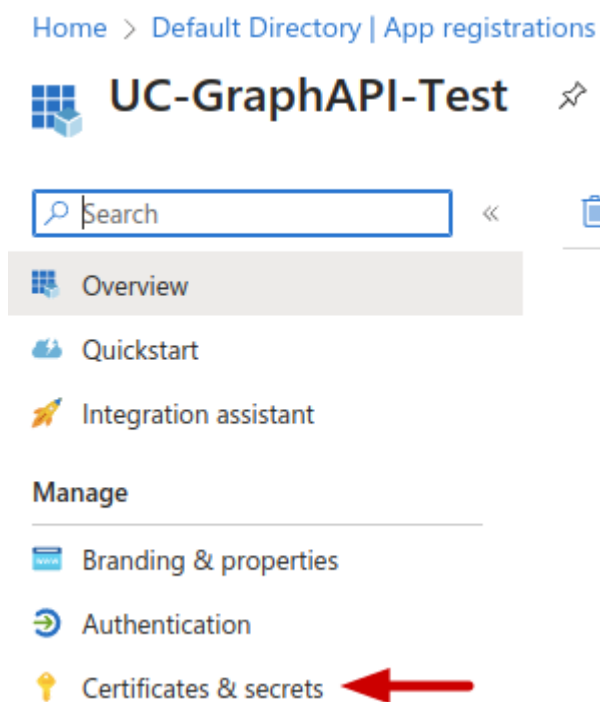
- Select "Certificates and secrets"

Application registration certificates, secrets and federated credentials can be

**Certificates (0)**   **Client secrets (1)**   Federated credentials (0)

A secret string that the application uses to prove its identity when requestin

+ New client secret ⟵

- Click "New client secret"

## Add a client secret                                    ✕

Description                    UnknownCyberSecret

Expires                        Recommended: 180 days (6 months)    ⌄

- Description "UnknownCyberSecret" is recommended
- Click Add

| Description | Expires | Value ⓘ | Secret ID |
|---|---|---|---|
| thisismysecret | 1/20/2024 | | |
| UnknownCyberSecret | 2/17/2024 | | |

- 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.)

Home > Default Directory | App registrations >

### UC-GraphAPI-Test 📌 ⋯

🔍 Search «

🔲 Overview

🔷 Quickstart

🚀 Integration assistant

**Manage**

🖼 Branding & properties

🗑 Delete   🌐 Endpoints   🔲 Preview features

⌃ **Essentials**

Display name          : UC-GraphAPI-Test
Application (client) ID :
Object ID             :
Directory (tenant) ID  :

- Copy the "Application (client) ID
- Copy the "Directory (tenant) ID
- Proceed to Unknown Cyber Portal Setup and have the:
  - o Application ID
  - o Tenant ID
  - o Secret Value

6. Setup Azure Sentinel

## RECOMMENDED (Optional) – Enable Microsoft Sentinel

- Open "Microsoft Sentinel" from your Azure Portal.



- Click "Create"



- Click "Create a new workspace"

# Create Log Analytics workspace   ···

Basics   Tags   Review + Create
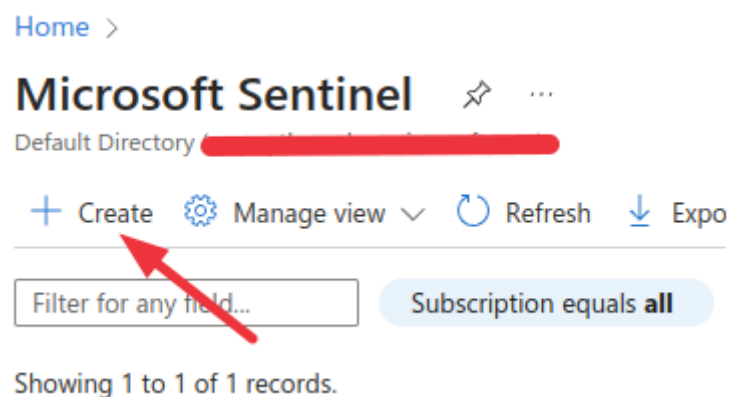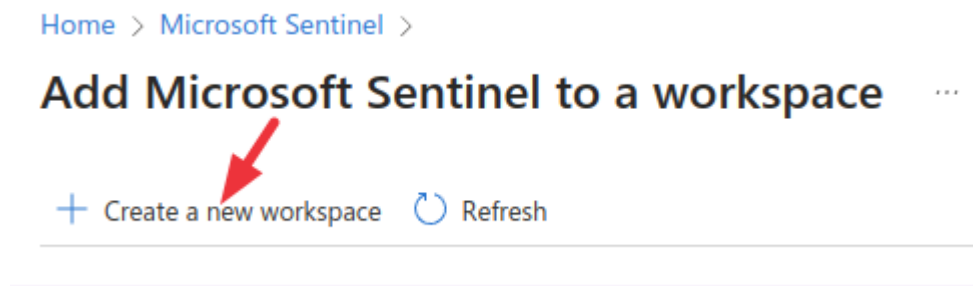
> ℹ A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations   ✕
> you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

| | |
|---|---|
| Subscription * ⓘ | Azure subscription 1 ⌄ |
| Resource group * ⓘ | ▬▬▬▬ ⌄ |
| | Create new |

**Instance details**

| | |
|---|---|
| Name * ⓘ | Unknown-Cyber-IOC ✓ |
| Region * ⓘ | East US 2 ⌄ |

- 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"

# Add role assignment ···

Role·   Members·   Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own cu
Assignment type

**Job function roles**   Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

🔍 Microsoft                                    ✕   Type : **All**    Category : **All**

| Name ↑↓ | Description ↑↓ |
|---|---|
| Microsoft Sentinel Contributor | Microsoft Sentinel Contributor |

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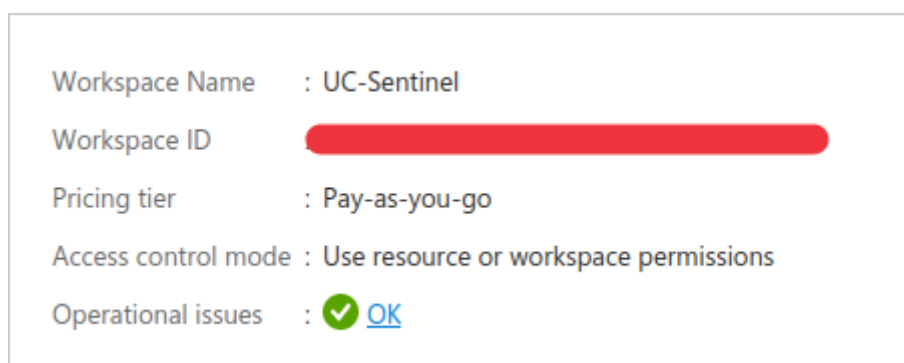- Move to Review and Assign, then click on "Review + assign"

Configuration

🔵 Workspace manager (Preview)

🟦 Data connectors

🧪 Analytics

🖼 Watchlist

⚙️ Automation

⚙️ Settings

- Select "Settings" Under Configuration inside Sentinel

- Select "Workspace Settings"

Workspace usage report

Pricing    Settings    Workspace settings >
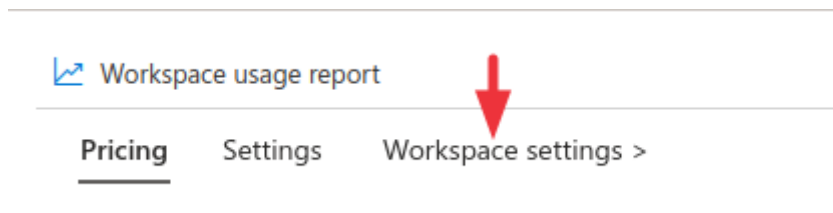
- Copy the "Workspace ID" for use in linking Sentinel to Unknown Cyber for receiving IOC feeds

Workspace Name    : UC-Sentinel

Workspace ID

Pricing tier    : Pay-as-you-go

Access control mode : Use resource or workspace permissions

Operational issues    : ✔ OK

- You can now proceed with the portal setup.