

Unknown Cyber Customer Setup (Azure)

Contents

1. Open to portal.azure.com and authenticate with your company credentials.	2
2. Create your App Registration	3
3. Set Rights for your App Registration.	5
4. Create the App Reg Secret.....	7
5. Gather your information for Registering with Unknown Cyber.....	9
6. Setup Azure Sentinel	10

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



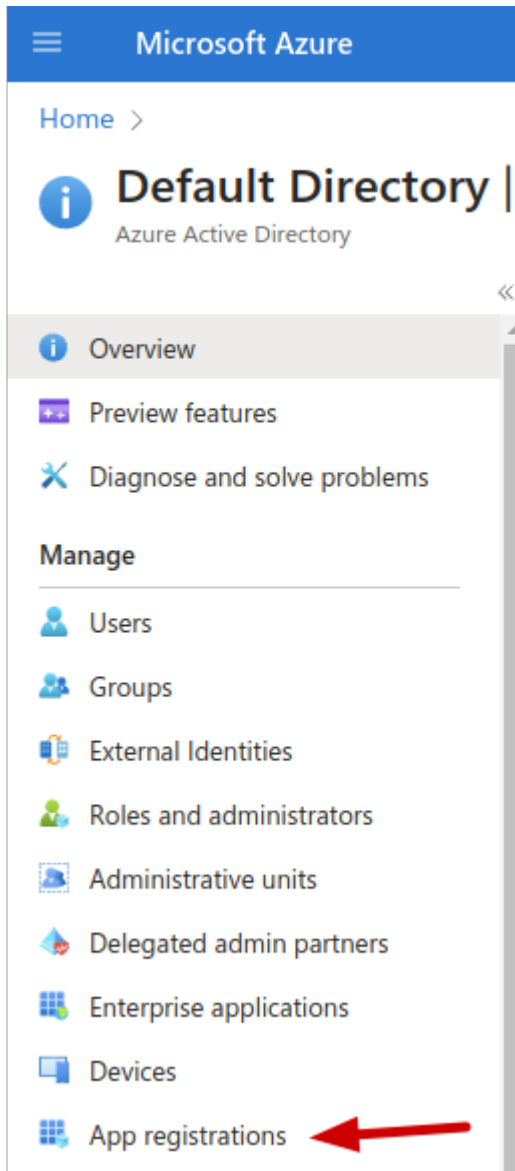
Create a
resource



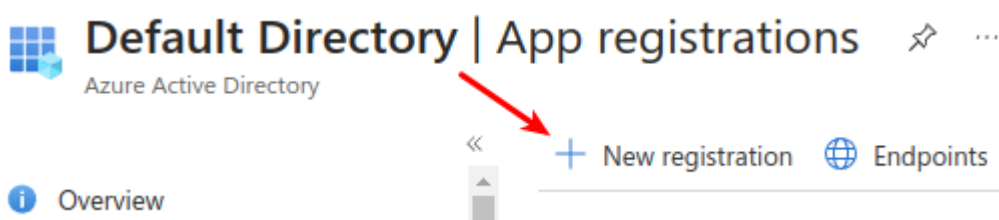
Azure Active
Directory

- ☐ Select Azure Active Directory

2. Create your App Registration



☐ Scroll down and Select “App Registrations”



☐ Select New Registration

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Default Directory | App registrations >

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

Unknown-Cyber-AppR ✓

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (Default Directory only - Single tenant)

☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

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.

Select a platform ▼ e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

- ☐ 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 uses the latter method.*

▼ Directory (1)		
<input checked="" type="checkbox"/>	Directory.Read.All ⓘ Read directory data	Yes

- ☐ Select Directory.Read.All

▼ Mail (1)		
<input checked="" type="checkbox"/>	Mail.Read ⓘ Read mail in all mailboxes	Yes

- ☐ Select “Mail → Mail.Read”

▼ ThreatIndicators (1)		
<input type="checkbox"/>	ThreatIndicators.Read.All ⓘ Read all threat indicators	Yes
<input checked="" type="checkbox"/>	ThreatIndicators.ReadWrite.OwnedBy ⓘ Manage threat indicators this app creates or owns	Yes

- ☐ 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.

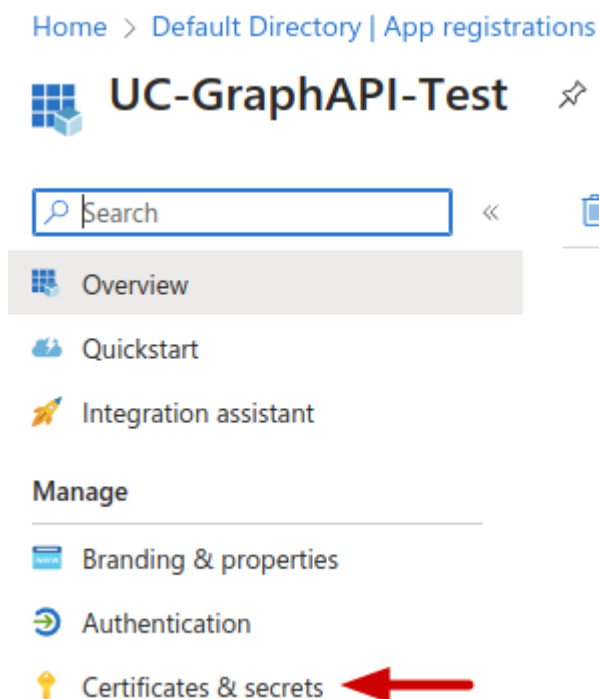
Configured permissions

Applications are authorized to call APIs when they are granted all the permissions the application needs. [Learn more about permissions](#)


[+ Add a permission](#)
[✓ Grant admin consent for](#)

- ☐ 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




- ☐ 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	<input type="text" value="UnknownCyberSecret"/>
Expires	<div>Recommended: 180 days (6 months) </div>

☐ Description “UnknownCyberSecret” is recommended



☐ Click Add




5. Gather your information for Registering with Unknown Cyber.


Description	Expires	Value ⓘ	Secret ID
thisismysecret	1/20/2024	[REDACTED]	[REDACTED]
UnknownCyberSecret	2/17/2024	[REDACTED]	[REDACTED]


- ☐ 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 <<  Delete  Endpoints  Preview features

 Overview

 Quickstart

 Integration assistant

Manage

 Branding & properties

Essentials

Display name : [UC-GraphAPI-Test](#)

Application (client) ID : [REDACTED]

Object ID : [REDACTED]

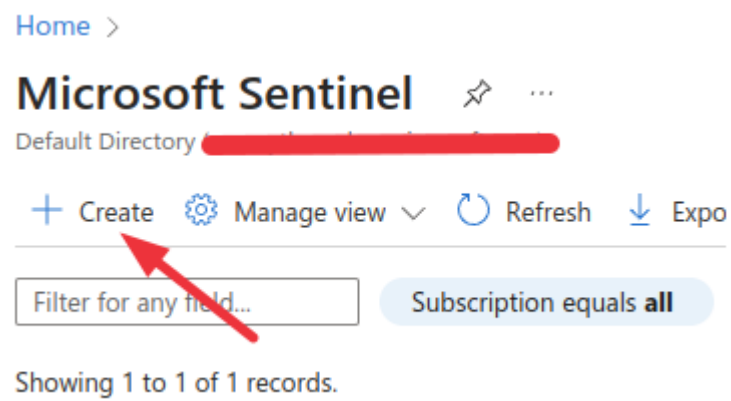
Directory (tenant) ID : [REDACTED]

- ☐ 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

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 * ⓘ [Redacted] ▼

[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 custom role. Select the role type you want to use.







Job function roles Privileged administrator roles

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

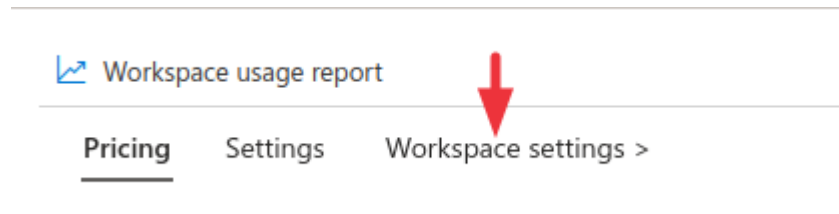
<input type="text" value="Microsoft"/>	×	Type : All	Category : All
Name ↑↓		Description ↑↓	
Microsoft Sentinel Contributor		Microsoft Sentinel Contributor	

- ☐ 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”

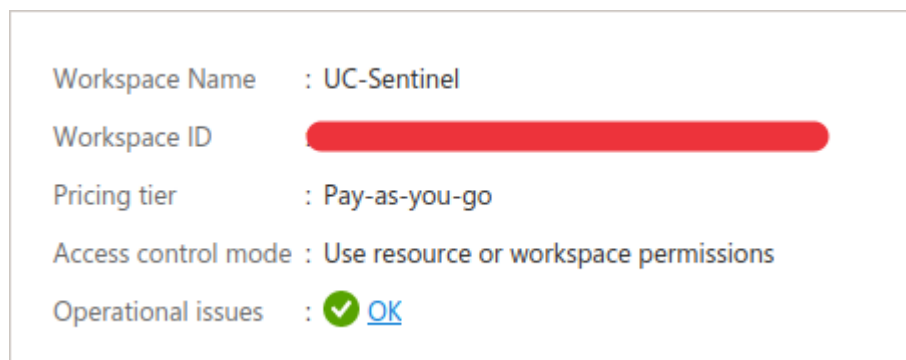
Configuration

-  Workspace manager (Preview)
-  Data connectors
-  Analytics
-  Watchlist
-  Automation
-  Settings

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



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



- You can now proceed with the portal setup.