WAZUH – OFFICE 365 INTEGRATION

LAB CREATED BY : SAYED WAQAR ALI BACHA

Introduction:

Integrating Office 365 with Wazuh enables centralized monitoring and security management of Office 365 activities within your organization's SIEM environment. By doing so, you can track user activities, monitor login attempts, and detect suspicious behavior in real time.

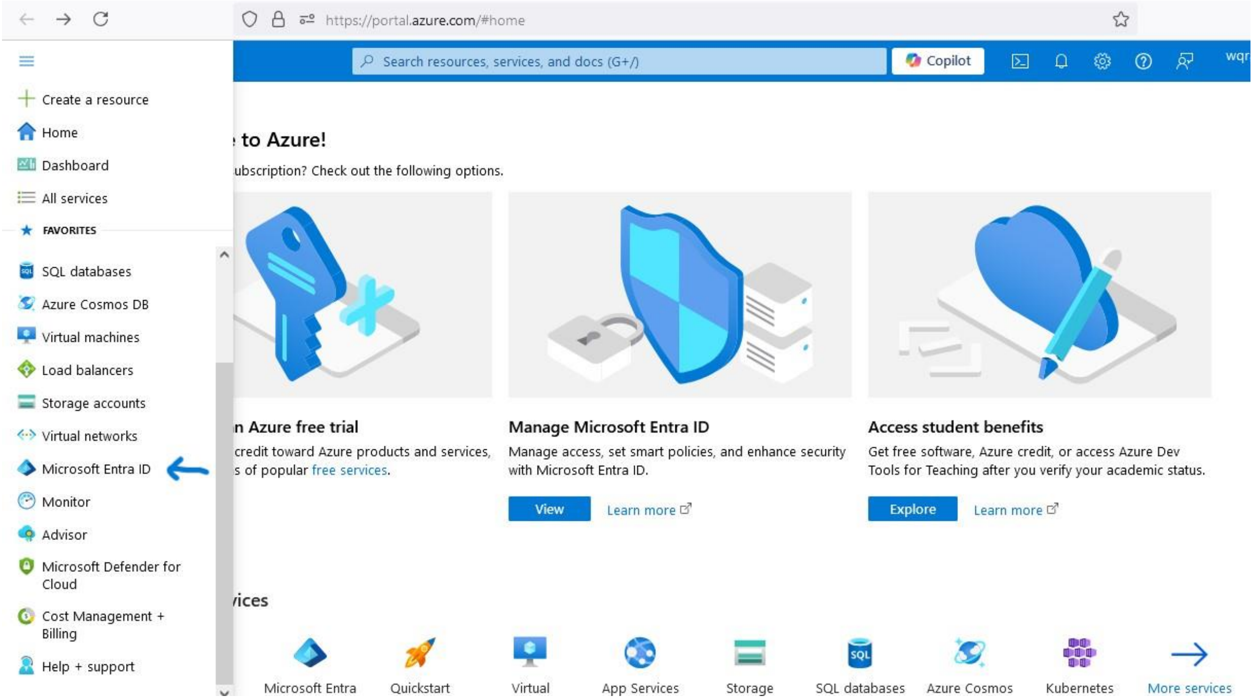
The integration allows Wazuh to collect and analyze security events from Office 365, providing insights into potential threats and compliance issues. This setup enhances the overall security posture by ensuring that events from Office 365, such as logins, file access, and administrative actions, are continuously monitored and correlated with other security events within Wazuh.

Prerequisites:

- You must have an active Office 365 subscription.
- Ensure that Wazuh is already installed and configured in your environment.
- Create and configure an Azure AD application in the Azure portal.
- Grant the necessary API permissions to the Azure AD application for accessing Office 365 logs.
- Install and configure the Wazuh Office 365 integration module**.**

Registering an app via the Azure portal :

1) Sign in to your Azure portal.
2) Click ON Microsoft Entra ID.



to Azure!

ubscription? Check out the following options.

n Azure free trial

credit toward Azure products and services, s of popular free services.

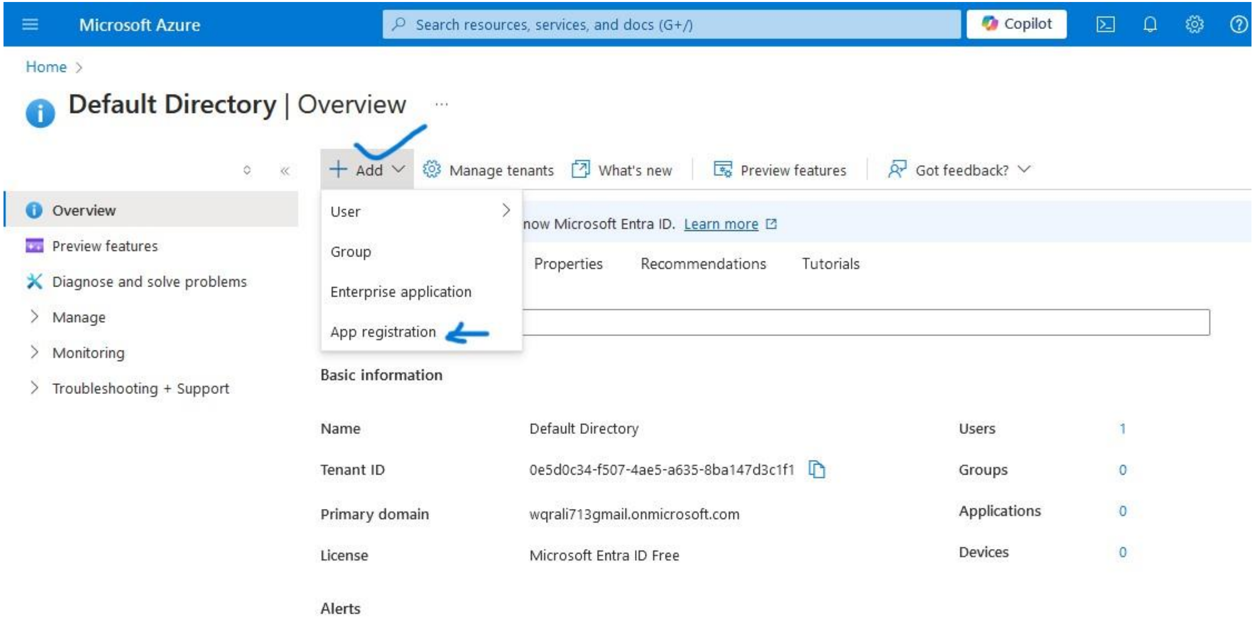
Manage Microsoft Entra ID

Manage access, set smart policies, and enhance security with Microsoft Entra ID.

Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

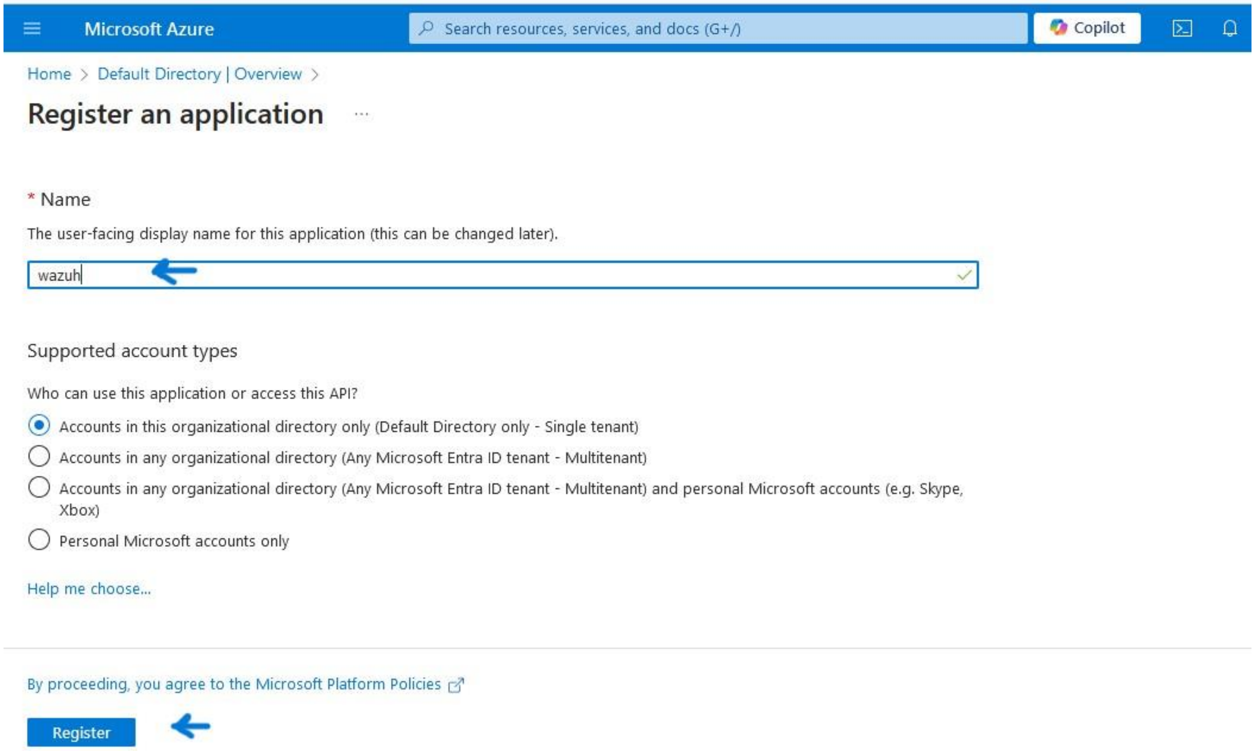
3) Click on **New registration** in the Microsoft Azure portal app registrations section**.**



Basic information

Name	Default Directory	Users	1
Tenant ID	0e5d0c34-f507-4ae5-a635-8ba147d3c1f1	Groups	0
Primary domain	wqrali713gmail.onmicrosoft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

4) Fill in the name of your application, choose the desired account type, and click on the **Register** button**.**


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Default Directory | Overview >
Register an application
Help me choose...
Register

* Name

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

wazuh

Supported account types

Who can use this application or access this API?

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

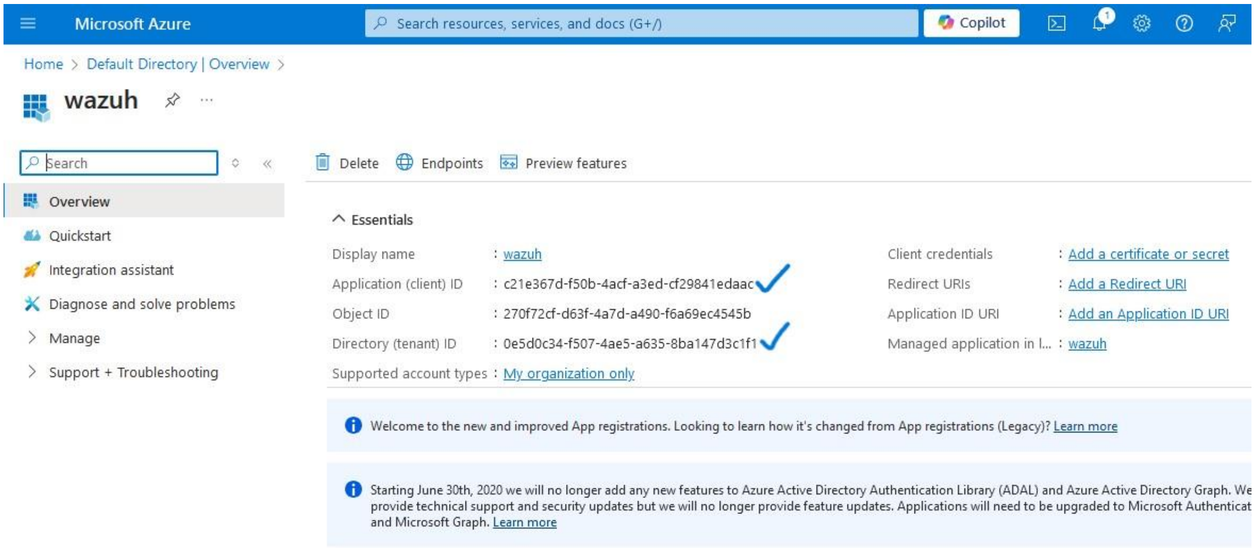
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

By proceeding, you agree to the Microsoft Platform Policies

5) Click on the **Overview** tab on the menu to view and copy the application's client and tenant IDs**.**


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Default Directory | Overview >
wazuh
Search
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Support + Troubleshooting
Delete
Endpoints
Preview features
Essentials

Display name : wazuh
Application (client) ID : c21e367d-f50b-4acf-a3ed-cf29841edaac ✓
Object ID : 270f72cf-d63f-4a7d-a490-f6a69ec4545b
Directory (tenant) ID : 0e5d0c34-f507-4ae5-a635-8ba147d3c1f1 ✓
Supported account types : My organization only

Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : wazuh

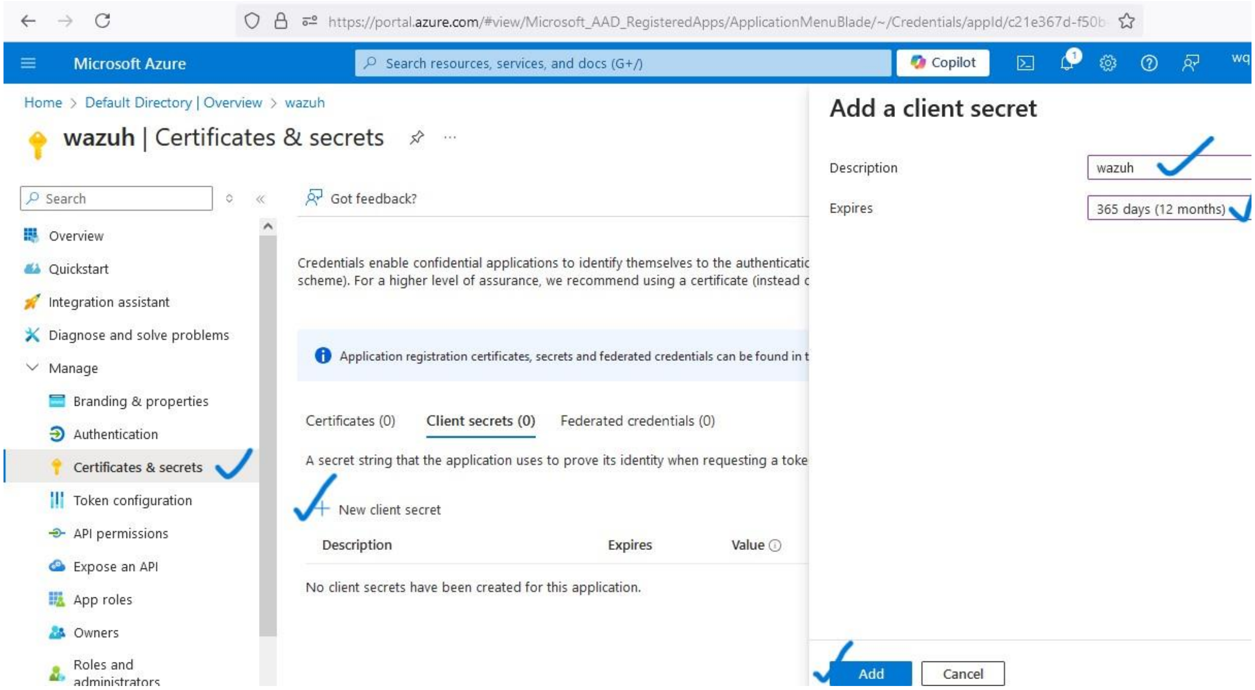
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authenticat and Microsoft Graph. Learn more

Creating certificates and secrets :

The application requires a certificate and secret to use during the authentication process.

1) Navigate to the Certificates & secrets menu and click the New client secret button. Then, fill in the Description and Expires fields of the new secret under the Add a client secret section**.**



https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/appId/c21e367d-f50b

Microsoft Azure

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

Copilot

Home > Default Directory | Overview > wazuh

wazuh | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authenticatic scheme). For a higher level of assurance, we recommend using a certificate (instead c

Application registration certificates, secrets and federated credentials can be found in t

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

A secret string that the application uses to prove its identity when requesting a toke

+ New client secret

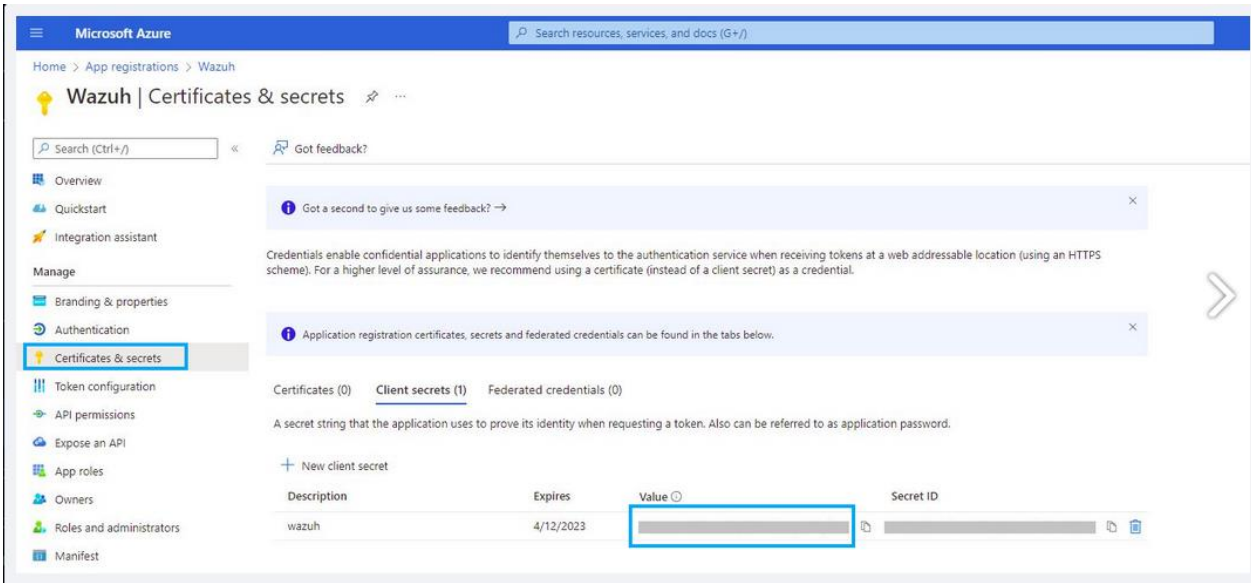
Description	Expires	Value
No client secrets have been created for this application.		

Add a client secret

Description: wazuh

Expires: 365 days (12 months)

1) Copy and save the value of the secret under the Client secrets section.



Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

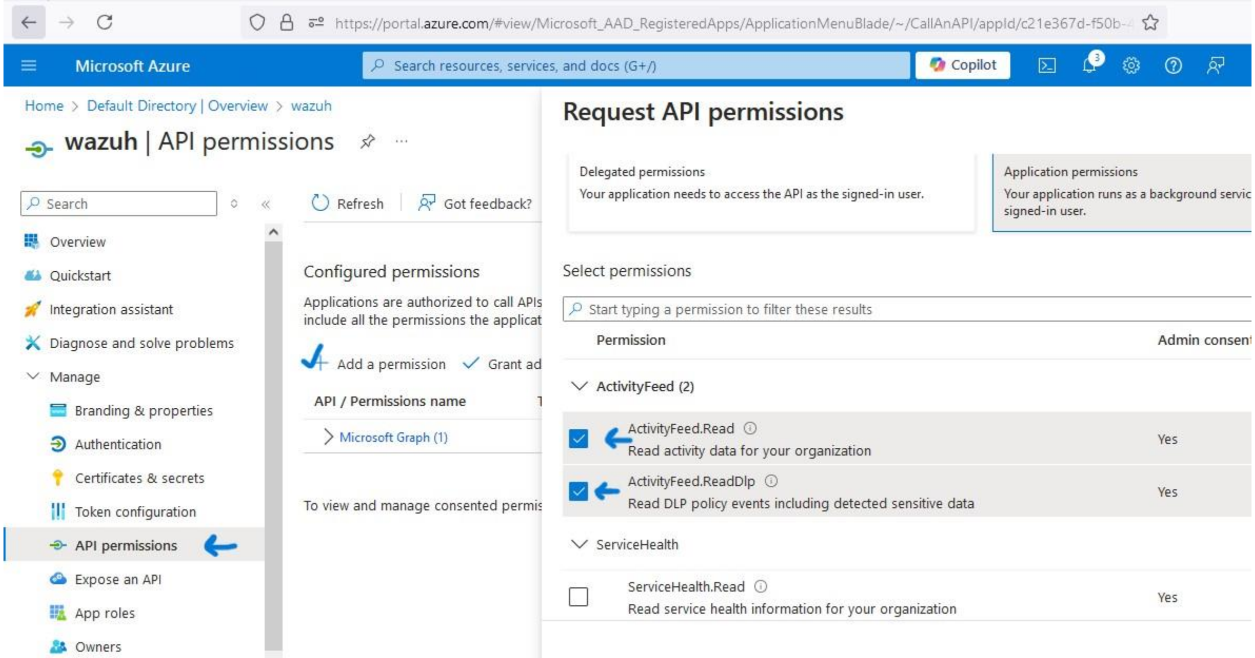
Description	Expires	Value	Secret ID
wazuh	4/12/2023	[redacted]	[redacted]

Note: Make sure you write it down because the web interface won’t let you copy it afterward.

Enabling API permissions :

Navigate to the API permissions menu and choose Add a permission.

- **Select the Office 365 Management APIs and click on Application permissions.**
- **Add the following permissions under the ActivityFeed group:**
- **ActivityFeed.Read: Read activity data for your organization.**
- **ActivityFeed.ReadDlp: Read DLP policy events including detected sensitive data.**
- **Click on the Add permissions button.**



Configured permissions

Applications are authorized to call APIs include all the permissions the applicat

API / Permissions name
Microsoft Graph (1)

To view and manage consented permis

Request API permissions

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

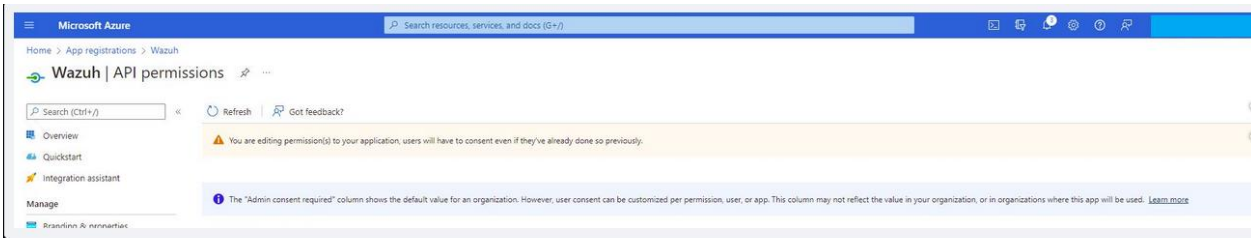
Application permissions
Your application runs as a background servic signed-in user.

Select permissions

Start typing a permission to filter these results

	Permission	Admin consent
	ActivityFeed (2)	
☑	ActivityFeed.Read Read activity data for your organization	Yes
☑	ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data	Yes
	ServiceHealth	
☐	ServiceHealth.Read Read service health information for your organization	Yes

NOTE : Admin consent is required for API permission changes.



You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

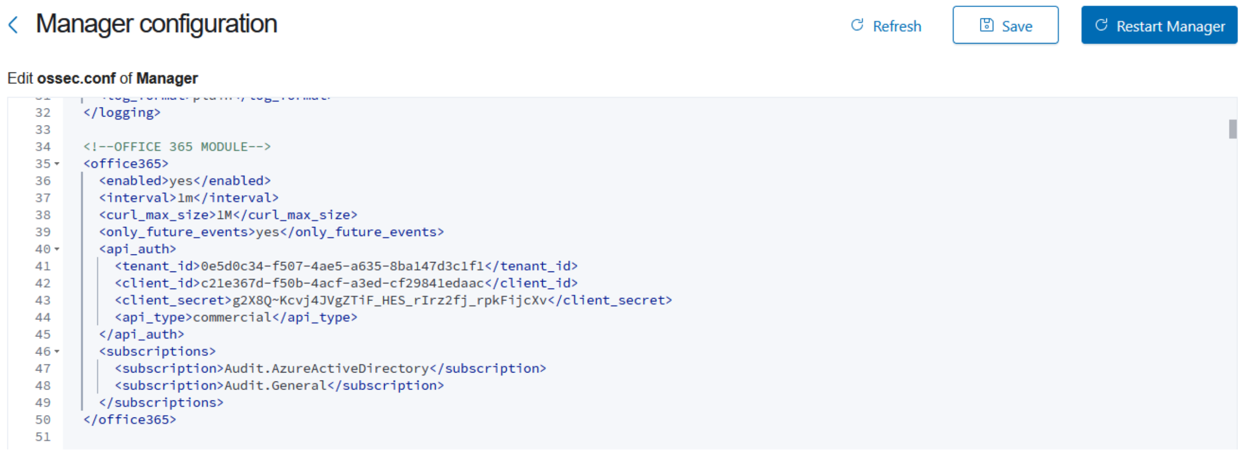
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configuring Wazuh with Office 365 APIs :

1) Go To /var/ossec/etc/ossec.conf in wazuh server and paste this lines below logging section.

```
<ossec_config>
 <office365>
   <enabled>yes</enabled>
   <interval>1m</interval>
   <curl_max_size>1M</curl_max_size>
   <only_future_events>yes</only_future_events>
   <api_auth>
     <tenant_id><YOUR_TENANT_ID></tenant_id>
     <client_id><YOUR_CLIENT_ID></client_id>
     <client_secret><YOUR_CLIENT_SECRET></client_secret>
     <api_type>commercial</api_type>
   </api_auth>
   <subscriptions>
     <subscription>Audit.SharePoint</subscription>
   </subscriptions>
 </office365>
</ossec_config>
```

2) After that make changes in Tennant id, Client id and Client secret ……



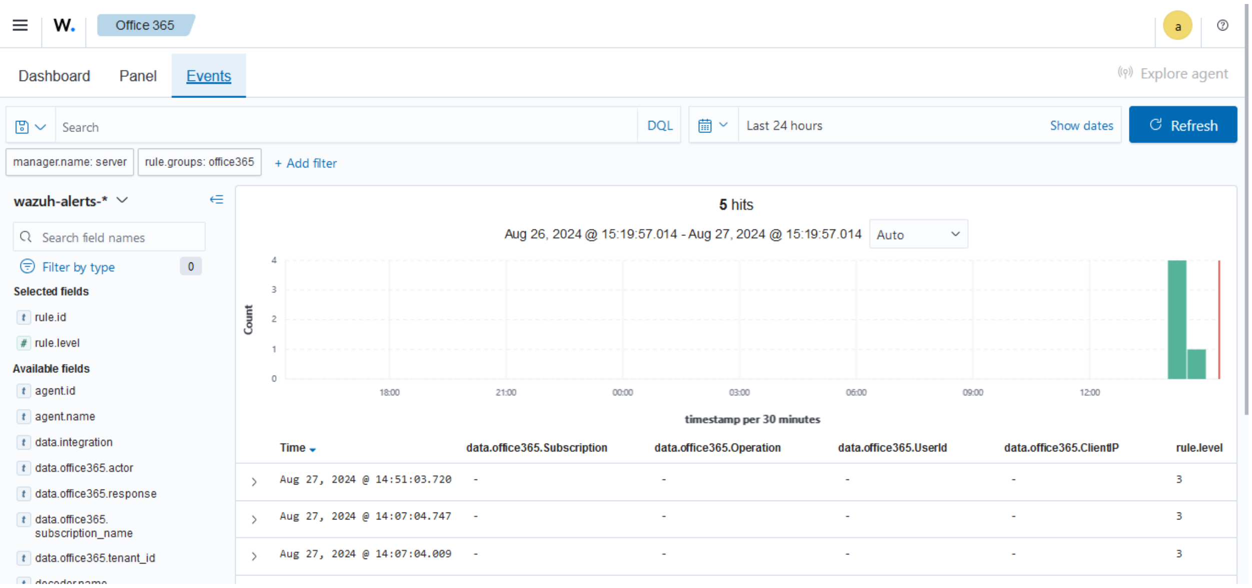
Edit **ossec.conf** of **Manager**

```
</logging>

<!--OFFICE 365 MODULE-->
<office365>
  <enabled>yes</enabled>
  <interval>1m</interval>
  <curl_max_size>1M</curl_max_size>
  <only_future_events>yes</only_future_events>
  <api_auth>
    <tenant_id>0e5d0c34-f507-4ae5-a635-8ba147d3c1f1</tenant_id>
    <client_id>c21e367d-f50b-4acf-a3ed-cf29841edaac</client_id>
    <client_secret>g2X8Q~Kcvj4JVgZTiF_HES_rIrz2fj_rpkFijcXv</client_secret>
    <api_type>commercial</api_type>
  </api_auth>
  <subscriptions>
    <subscription>Audit.AzureActiveDirectory</subscription>
    <subscription>Audit.General</subscription>
  </subscriptions>
</office365>
```

3) Save the configuration and restart wazuh manager.

➢ IF YOUR INTEGRATION IS SUCCESFULL YOU WILL SEE LOGS ON YOUR DASHBOARD..



Last 24 hours

manager.name: server | rule.groups: office365

wazuh-alerts-*

Selected fields

- rule.id
- rule.level

Available fields

- agent.id
- agent.name
- data.integration
- data.office365.actor
- data.office365.response
- data.office365.subscription_name
- data.office365.tenant_id
- decoder.name

5 hits

Aug 26, 2024 @ 15:19:57.014 - Aug 27, 2024 @ 15:19:57.014 Auto

Time	data.office365.Subscription	data.office365.Operation	data.office365.UserId	data.office365.ClientIP	rule.level
Aug 27, 2024 @ 14:51:03.720	-	-	-	-	3
Aug 27, 2024 @ 14:07:04.747	-	-	-	-	3
Aug 27, 2024 @ 14:07:04.009	-	-	-	-	3

- **Regards:**

✓ SAYED WAQAR ALI BACHA

- Follow Me On Linkedin:

✓ https://www.linkedin.com/in/waqar-ali-8a5b6b228/

- Contact Number:

✓ +92-3466052414

- Gmail:

✓ Wqrali713@gmail.com