

Microsoft 365

Microsoft Office 365 integration currently supports user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs exposed by the Office 365 Management Activity API.

Procedures

To perform the setup, please confirm that you have the following access:

1. A Microsoft Office 365 account with Administrative Privileges
2. A Microsoft Azure account with Administrative Privileges

[Register a new Office 365 web application](#) To get started collecting Office 365 logs, register an Office 365 web application:

1. Log into the Office 365 portal as an Active Directory tenant administrator.
2. Click Show all to expand the left navigation area, and then click Azure Active Directory.
3. Select App Registrations, and then click + New application registration.
4. Provide the following information in the fields:
 - Name – for example, o365cytech.
 - Select Single tenant for supported account types.
 - Leave the Redirect URI blank.
 - The Audit Log Search needs to be enabled.
 - Click Register and note the Application (client) ID.

Setup Active Directory security permissions

The Active Directory security permissions allow the application you created to read threat intelligence data and activity reports for your organization.

To set up Active Directory permissions:

1. On the main panel under the new application, click API Permissions, and then click + Add a permission.
2. Locate and click on Office 365 Management APIs.
3. In Application permissions, expand and select ActivityFeed.Read, ActivityFeed.ReadDlp, ActivityReports.Read, and ServiceHealth.Read

4. Ensure all necessary permissions are selected, and then click Add permissions.
5. Click Grant admin consent, and then click Accept to confirm.
6. On the left navigation area, select Certificates & secrets, and then click + New client secret.
7. Make Sure to Copy the Value (Client Secret (Api Key) will disappear

+ New client secret

8. Description	Expires	Value ⓘ	Secret ID
testing	10/20/2023	SFH8Q~zjFaR_YJMYwLeH_vWj-0RIJP6x... ⓘ	604da4d2-bb02-4aa8-81cc-cfa5089e65... ⓘ 📋

9. Type a key Description and set the duration to Never or Maximum Grant time.
10. Click Add.
11. Click Overview to return to the application summary, and then click the link under Managed application in local directory.
12. Click Properties, and then note the Object ID associated with the application.

Revision #4

Created 23 April 2024 08:14:04

Updated 19 June 2024 06:53:45