Microsoft Office 365 - API Permissions

Integration Requirements

Please saved and provide this values to Cytech Support Team.

Directory (tenant) ID:

Application (client) ID:

Client Secret Value:

Steps to Verify Client's Office 365 Integration.

Step 1: Check Microsoft Entra ID

Register Your Application in Microsoft Entra ID:

- How to Locate:

    - Log in to the Azure Portal.

    - Navigate to Azure Active Directory > App registrations.

    - Check for an existing app registration.

- How to Create:

    - Click New Registration.

    - Provide a Name for the application.

    - Choose Supported Account Types (typically "Accounts in this organizational directory only").

- Enter a Redirect URI (if required).

- Click Register.

Step 2: Check API Permissions

Microsoft Graph:

- How to Locate:

  - Navigate to App registrations in the Azure Portal.

  - Select your app, then go to API Permissions.

- How to Add:

  - Click Add a permission.

  - Select Microsoft Graph > **Delegated permissions**.

  - Search for and add **User.Read**.

Office 365 Management API Permissions:

- How to Locate:

  - In **Application Permissions**, look for permissions such as:

  - **ActivityFeed.Read**

  - **ActivityFeed.ReadDLP**

  - **ServiceHealth.Read**

- How to Add:

  - Click Add a permission.

  - Select APIs my organization uses.

  - Search for Office 365 Management APIs and add the required permissions.

Grant Admin Consent:

- How to Perform:

  - In API Permissions, click **Grant admin consent** for <tenant name>.

  - **Confirm** the action.

Step 3: Verify Integration Requirements for Office 365

Application (Client) ID:

- How to Locate:

  - Go to App registrations > Select your application.

  - Copy the Application (client) ID from the overview page.

Directory (Tenant) ID:

- How to Locate:

  - In the Azure Portal, navigate to Azure Active Directory > Overview.

  - Copy the Directory (tenant) ID.

New Client Secret (Value):

- How to Create:

  - In App registrations, go to Certificates & secrets.

  - Click New client secret.

  - Add a description and expiration period, then click Add.

- Copy the Value (displayed only once).

Step 4: Enable Unified Audit Logging

Unified Audit Logging must be enabled before accessing data via the Office 365 Management Activity API.

Method 1: Using Microsoft 365 Security & Compliance Center

1. Sign in to Microsoft 365:

    - Go to https://admin.microsoft.com and sign in with your Global Admin credentials.

2. Access the Security & Compliance Center:

    - In the left-hand menu, under Admin centers, click on Security (or go directly to https://security.microsoft.com).

3. Navigate to Audit Log Search:

    - In the Security & Compliance Center, go to Search in the left-hand menu and click on Audit log search.

4. Check Audit Log Status:

    - If you see an option to search the audit log, then audit logging is already enabled.

    - If you see a banner that says "Start recording user and admin activity" or a prompt to enable auditing, it means that audit logging is not yet enabled.

5. Enable Audit Logging (if needed):

    - If audit logging is not enabled, you can click on the prompt to enable it. This will enable auditing for all activities within your Microsoft 365 environment. The process may take a few hours to be fully operational.

Method 2: Using Powershell

1.Install and Update Exchange Online Management Module

- Open PowerShell as Administrator.

- Install the module:

-->Install-Module -Name ExchangeOnlineManagement

- Update the module:

-->Update-Module -Name ExchangeOnlineManagement

- Import the module

-->Import-Module ExchangeOnlineManagement

2.Connect to Exchange Online

- Run the following command:

-->Connect-ExchangeOnline -UserPrincipalName <admin-email-address>

- Replace <admin-email-address> with the admin email. Authenticate if required.

3.Check and Enable Unified Audit Logging

Check Status:

- Run:

-->Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled

- If the output is True, Unified Audit Logging is already enabled.

Enable Logging (if needed):

- If the output is False, enable it:

-->Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true

- Verify again:

-->Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled

4.Disconnect from Exchange Online

- Run:

-->Disconnect-ExchangeOnline

If you need further assistance, kindly contact our support at **support@cytechint.com** *for prompt assistance and guidance.*

Revision #8
Created 21 January 2025 06:15:40 by Richmond Abella
Updated 2 May 2025 03:12:15 by Richmond Abella