

Graph API Envío de Email

Nombre del Patrón: Envío Email Graph API

Versión: 1.0

Realizado por: Emmanuel Jiménez Almazán

1. Contexto

Microsoft Graph es una API para web REST que permite tener acceso a los recursos del servicio Microsoft Cloud. Consideraciones:

1. [Registrar una aplicación](#)
2. Obtener tokens de autenticación para un usuario o servicio;
3. Consumo de Graph API

Para leer o escribir en recursos de Azure como usuarios o mensajes de correo electrónico, se construye una solicitud similar a la siguiente:

{HTTP method} <https://graph.microsoft.com/{version}/{resource}?{query-parameters}>

1.1 Hallazgos Claves

Requerimiento 1: [Flujo Interactivo](#). Envío de Correo Con el Remitente del propio **Usuario con acceso al aplicativo** con SSO Azure EntraID

Detalle.

1. El usuario Entra al Aplicativo mediante SSO de Azure EntraID.
2. El usuario *dentro del aplicativo*. Ejecuta **un evento** con flujo de notificación para envío de correo
3. El usuario desde el aplicativo envía el correo a la lista de destinatarios.

Requerimiento 2: [Flujo No Interactivo](#). Envío de Correo Con el Remitente de una **Cuenta de Usuario** de Proceso Aplicativa Independiente a el Usuario con acceso al aplicativo SSO Azure EntraID

Detalle

1. De forma **automatizada** (calendarizada o por la interacción con un sistema externo) se genera un evento que detona el envío del Mail desde el aplicativo
2. El aplicativo toma las credenciales (Client-Credentials) y envía el mail a la lista de destinatarios

2. Problema

Para Integrar el envío de Email a un flujo de trabajo es necesario cumplir con los límites de servicios para envío de Email

Límites de Servicio Outlook


- No superar las volúmenes permitidos por Outlook 365 (<https://learn.microsoft.com/en-us/graph/throttling-limits>)

Outlook service limits

Outlook service limits apply to the public cloud and national cloud deployments.

Limits per app ID and mailbox combination

The Outlook service applies limits to each app ID and mailbox combination - that is, a specific app accessing a specific user or group mailbox. Exceeding the limit for one mailbox doesn't affect the ability of the application to access another mailbox.

 Expand table

Limit	Applies to
10,000 API requests in a 10 minute period	v1.0 and beta endpoints
Four concurrent requests	v1.0 and beta endpoints
150 megabytes (MB) upload (PATCH, POST, PUT) in a 5-minute period	v1.0 and beta endpoints

3. Criterios

Consideraciones y Restricciones de Uso Santander

1. Que el usuario al que se le va a enviar el mail sea un usuario **interno** de Santander (Corporativo, Sucursales, etc.) que pertenezca a el directorio activo: "GFSSCORP"; Esta Solución no es para dominios de email con remitentes externos @hotmail; @gmail.
2. La solución **no** contempla Envío de Email a **Cientes** Santander
3. El aplicativo debe estar Integrado con la Autenticación Azure Entra ID y con su "EntraID Application"
4. Usuario con el que se envía el Mail debe pertenecer a el "EntraID Application"
5. El usuario con el que se desee enviar el Mail debe tener una **licencia** de Outlook Office 365
6. Flujo No Certificado: El uso de Graph Api para envío de Attachments (El Arquitecto de la Solución deberá validar este Flujo)
7. Es necesario tener un token de Azure de Autenticación Valido y Vigente

4. Solución

Graph API Send Mail Especificación

{HTTP method} <https://graph.microsoft.com/{version}/{resource}?{query-parameters}>

HTTP Request

Particularmente para consumir el API de envío de Mail se usa:

{POST} <https://graph.microsoft.com/v1.0/me/sendMail>

ó

{POST} <https://graph.microsoft.com/v1.0/users/{userPrincipal}/sendMail>

Request headers

Name	Type	Description
Authorization	string	Bearer {token}. Requerido
Content-Type	string	Requerido. Usar "application/json" para Objetos JSON Y "text/plain" para MIME content.

Request Body

Parameter	Type	Description
message	Message	El mensaje a Enviar. Requerido

NOTA: Cuando el Cuerpo se especifica en formato MIME; es necesario agregar el contenido como una cadena codificada en Base 64

Response

HTTP/1.1 202 Accepted

+++

Ejemplos

- Request

POST https://graph.microsoft.com/v1.0/me/sendMail

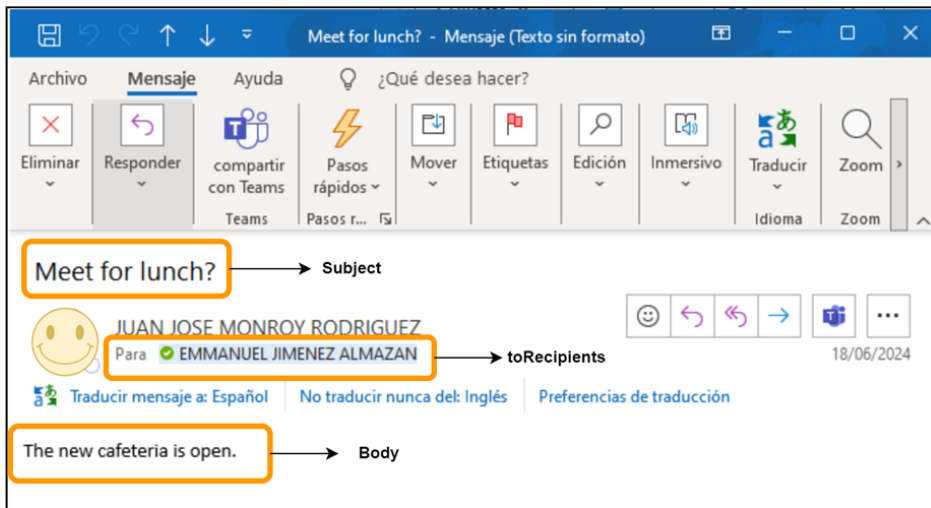
Authorization: Bearer {token}

Content-type: application/json

- Body:

```
{
  "message": {
    "subject": "Meet for lunch?",
    "body": {
      "contentType": "Text",
      "content": "The new cafeteria is open."
    },
    "toRecipients": [
      {
        "emailAddress": {
          "address": "c423860@santander.com.mx"
        }
      }
    ],
    "ccRecipients": [
      {
        "emailAddress": {
          "address": "c423860@santander.com.mx"
        }
      }
    ]
  },
  "saveToSentItems": "false"
}
```

- Resultado de Mail Enviado



😊 En este Ejemplo el Token se ha generado con el Usuario C de Juan Jose; que pertenece a el directorio GFSSCORP

- **Authorization Code Azure:**

```
0.AWIAj_DWH9bG80-dkDEB7J6GZiPiYD_Yy4tKmm2vLFZspKNjAHg.AgABAAIAAAD--
DLA3V07QrddgJg7WevrAgDs_wUA9P_1GgFQdJsxKOJeGY2muhzdD4xzS650Vd6Cxi75wpKKv00hW0ifKJw8J4-87Gw4rTIA-
oedUBC4f7Fz8lBhR_vJeFTPkv-dST5cLsrCW28-7zayGQPyXvilDsSN-
dl7kC32kVHmmdpmyu9EayotV5j1JoptYU7H4ilrynOARV3xVWVBLDJ8kh9gVtAnFimpGc-
k1NtJy8UEC_3kk3MjlyYY6T5xJLMM3ylyTThOLZCs-
6q_xB3DjySYGIZioHADt4FYjANA5C3c6kzswHSAuYtV8ApiosN73EHkNreRho_7HKRgAOLa0_SwuzLVUk_Lj9VCFk2eUB5YV
BFF758TYpHbMBO4Be3DQ7qlRanKECF0_NZoliwa-s3w216VmuW-
wevEuXMhSh9Sj5AS8AYHKVgDMimEFfevJWKvolx5FAVLLr3PQVY3jjMJwQV2kD3V7Ex2MDJjzZs48BCc2Bp9uQ66e-
zC1QW5FyV0m3CxlwtVHHpxU6i_iuAiXA7DnNI07OOrEV1txNo7CcMVRUK-rQCA5PgKHAUG4M1dk-
s8hefyJKPBMBq63RFmkHGxMCGYmQMxsaq2KCri1Mu2bZTO2_6vMywhwcEerp1aboYo1EP70wFNv7LhKydghn0OPGWA87
0UELwqCy6bHrj6jVl2dZOU6jWHTmwUPN7RcTkunwwUGjv8alb0YZqxnHx2D47E6XjdeIGKFETbFvMyMXSrw52B0QTBanqNv-
O8VY6e4x3GSE9v8kprprDNtkqgrZRZPbr5G8FQeP0xDyEpftBBZWKDLZVsnbZPB7H-
6Kd5uQUio6JR5gMW7le09W4vi7wP485HBH3bxS2bEIHpyFmbgxwV31baIMtxvvY8ZjHo6dzHO5WNmXslms-z7ouRuwVI2Vsn-
05Sg-inn_WHw5E3S5CpVAZ-NTIwRS4IAuH95hMdfPgoK8tFwTHdNp-IJi21Dsad_PW6M0d6p-
CSXpCcBkLMCAEFB1cyyug267L8ANTCdF9LvPebtF9a5QvB9hb1-gh7jTyirWXYRqrctgzw-
qEm7MU7l5aK1b7szSqVTTfAg3neH12k2eN_kXGoVyyv0Q8iFppvReODF5EZx9sos7OyOewqQQBhS3Hg_I7xB2vWadSmi76RI
G8K0P-J09sLvJm7Kbtfwh6A4ED9YbSpBbrBdh4985p-
_KKUPzgHnmL4Eg3fwl8asOiztwf0UL_TQkH08JW11ZO3DXz1n1_jjepK0Xq-
nJHtUmwOmhyGVJWx5_7kloKtKXpuRT4_udyI8KvdfE_CXDCgFa3s5OCCSguRyphOYDD82SojsWQFxxV-
HMC3WEpEBVWwTrKlp7Yj_8i-yAdDOgeKmAmG9_t7XPCcRCEaXlXoQzayB0KqJHEk-QA6SwDHs
```

- **Token Azure**

Azure Delegate Permissions

TestAppEmm API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration **API permissions** Expose an API App roles Owners Roles and administrators Manifest Support + Troubleshooting Troubleshooting

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (14)				
email	Delegated	View users' email address	No	Granted for Directorio p...
Mail.Read	Delegated	Read user mail	No	Granted for Directorio p...
Mail.Read.Shared	Delegated	Read user and shared mail	No	Granted for Directorio p...
Mail.ReadBasic	Delegated	Read user basic mail	No	Granted for Directorio p...
Mail.ReadBasic.Shared	Delegated	Read user and shared basic mail	No	Granted for Directorio p...
Mail.ReadWrite	Delegated	Read and write access to user mail	No	Granted for Directorio p...
Mail.ReadWrite.Shared	Delegated	Read and write user and shared mail	No	Granted for Directorio p...
Mail.Send	Delegated	Send mail as a user	No	Granted for Directorio p...
Mail.Send.Shared	Delegated	Send mail on behalf of others	No	Granted for Directorio p...
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Directorio p...
openid	Delegated	Sign users in	No	Granted for Directorio p...
Policy.ReadWrite.SecurityDefault	Delegated	Read and write your organization's security defaults policy	Yes	Not granted for Directo...
profile	Delegated	View users' basic profile	No	Granted for Directorio p...
User.Read	Delegated	Sign in and read user profile	No	Granted for Directorio p...

Implementación Flujo No interactivo

Prerrequisitos

- Contar con un Usuario de Proceso Aplicativo dado de alta en Ldap local México y replicado en Azure.
 - Para tener el usuario es necesario una Autorización de CISO (Ciso YAM) Ticket. Snow: QRO - GGAA - LDAP-Domain - New/Delete /Modify Service Account Al levantar el Ticket Se llena el ForSIN013. (solicitar un DomainUser con la habilidad de enviar correos desde el aplicativo veradat en AzureAD para servicios de preproduccion)
- El usuario debe contar con una licencia de Outlook 365 con la capacidad de envío de Email (Esta licencia tiene un costo para la iniciativa). En este punto es necesario analizar el detalle del tipo de licencia (E1, E2..) para mejor detalle contactar a Equipo GRUPO SOFTWARE ASSET MX SDS software_asset_mx@gruposantander.com.mx
- Revisar con Jose Miguel Flores (Alguna Regla en IronPort; para que no bloquee correos)
- Alta de cuenta de Usuario Azure. Enviar Mail a access_management_apps@produban.com.mx - ACCESS MANAGEMENT APLICACIONES PROTECT
- Ya con usuario con buzón y licencia ir con "Jonathan Sanchez Arellano" para asignar licencia office E1 a la cuenta de Usuario de proceso
- Finalmente contactar a el quipo de Administración de la plataforma Azure en México "Javier Collazo" y "FRANCISCO XAVIER GARCIA SOLIS"; para asociar el usuario a el Application y habilitar los permisos a nivel application "Application permissions" [Graph Set permissions](#)

Flujo

- El flujo de Notificación es desencadenado por el mismo aplicativo derivado de un evento No interactivo como (temporizador interno, petición de un tercero, petición de otra aplicación Interna Santander, Flujo interno que detone una notificación interna desde el aplicativo)
- De forma interna el aplicativo Obtiene las credenciales de Azure (Client Credentials: ClientId y Client Secret)
- Forma la petición para generar el Token usando client Credentials. Referencia General Azure para este flujo: <https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-client-creds-grant-flow>
 - Formar Request: invocando el servicio de creación de token; y especificando el client_id, client_secret, grant_type y scope = https%3A%2F%2Fgraph.microsoft.com%2F.default

Ejemplo

```
POST /{tenant}/oauth2/v2.0/token HTTP/1.1
Host: login.microsoftonline.com:443
Content-Type: application/x-www-form-urlencoded
query_params:

client_id=00001111-aaaa-2222-bbbb-3333cccc4444

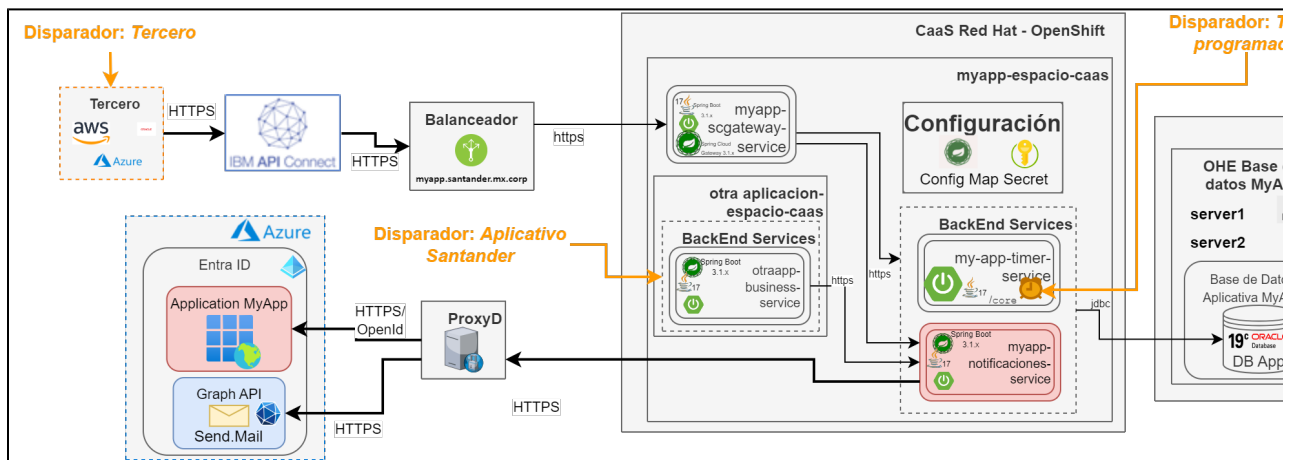
&scope=https%3A%2F%2Fgraph.microsoft.com%2F.default

&client_secret=qWgdYAmab0YSkuLlqKv5bPX

&grant_type=client_credentials
```

NOTA: Con el token se forma la petición para envío de correo desde graph API. El token se asigna en la cabecera de Authorization como Bearer Token

Representación



Azure Application Permissions

java-spring-webapp-auth | Permisos de API

Nombre de permisos/API	Tipo	Descripción	Se necesita el conse...	Estado
Microsoft Graph (15)				
Mail.Read	Delegada	Leer correo de usuario	No	Concedido para Libre
Mail.Read.Shared	Delegada	Leer correo compartido y del usuario	No	Concedido para Libre
Mail.ReadBasic	Delegada	Leer el correo básico del usuario	No	Concedido para Libre
Mail.ReadBasic.Shared	Delegada	Read user and shared basic mail	No	Concedido para Libre
Mail.ReadWrite	Delegada	Acceso de lectura y escritura al correo de usuario	No	Concedido para Libre
Mail.ReadWrite.Shared	Delegada	Leer y escribir correo compartido y del usuario	No	Concedido para Libre
Mail.Send	Delegada	Enviar correo como usuario	No	Concedido para Libre
Mail.Send	Aplicación	Send mail as any user	Sí	Concedido para Libre
Mail.Send.Shared	Delegada	Enviar correo en nombre de otros usuarios	No	Concedido para Libre
offline_access	Delegada	Mantener el acceso a los datos a los que se le ha concedi...	No	Concedido para Libre
openid	Delegada	Iniciar la sesión de usuarios	No	Concedido para Libre
profile	Delegada	Ver el perfil básico de los usuarios	No	Concedido para Libre
User.Read	Delegada	Iniciar sesión y leer el perfil del usuario	No	Concedido para Libre
User.Read.All	Delegada	Leer los perfiles completos de todos los usuarios	Sí	Concedido para Libre

5. Referencias

- Especificación de OpenID: <https://learn.microsoft.com/en-us/entra/architecture/auth-oidc>
- Crear Application Entra ID: <https://learn.microsoft.com/es-es/graph/auth-register-app-v2>
- Restricciones de Uso Outlook: <https://learn.microsoft.com/en-us/graph/throttling-limits>
- Generación de Token client credentials: <https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-client-creds-grant-flow>
- Generación de Token auth code grant: <https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-auth-code-flow>
- Graph API Set Permissions: <https://learn.microsoft.com/en-us/graph/migrate-azure-ad-graph-configure-permissions?tabs=http&pivots=entra-portal-api-permissions>
- Integración con un proyecto Spring: <https://learn.microsoft.com/es-es/azure/developer/java/spring-framework/spring-boot-starter-for-azure-active-directory-developer-guide?tabs=SpringCloudAzure4x>