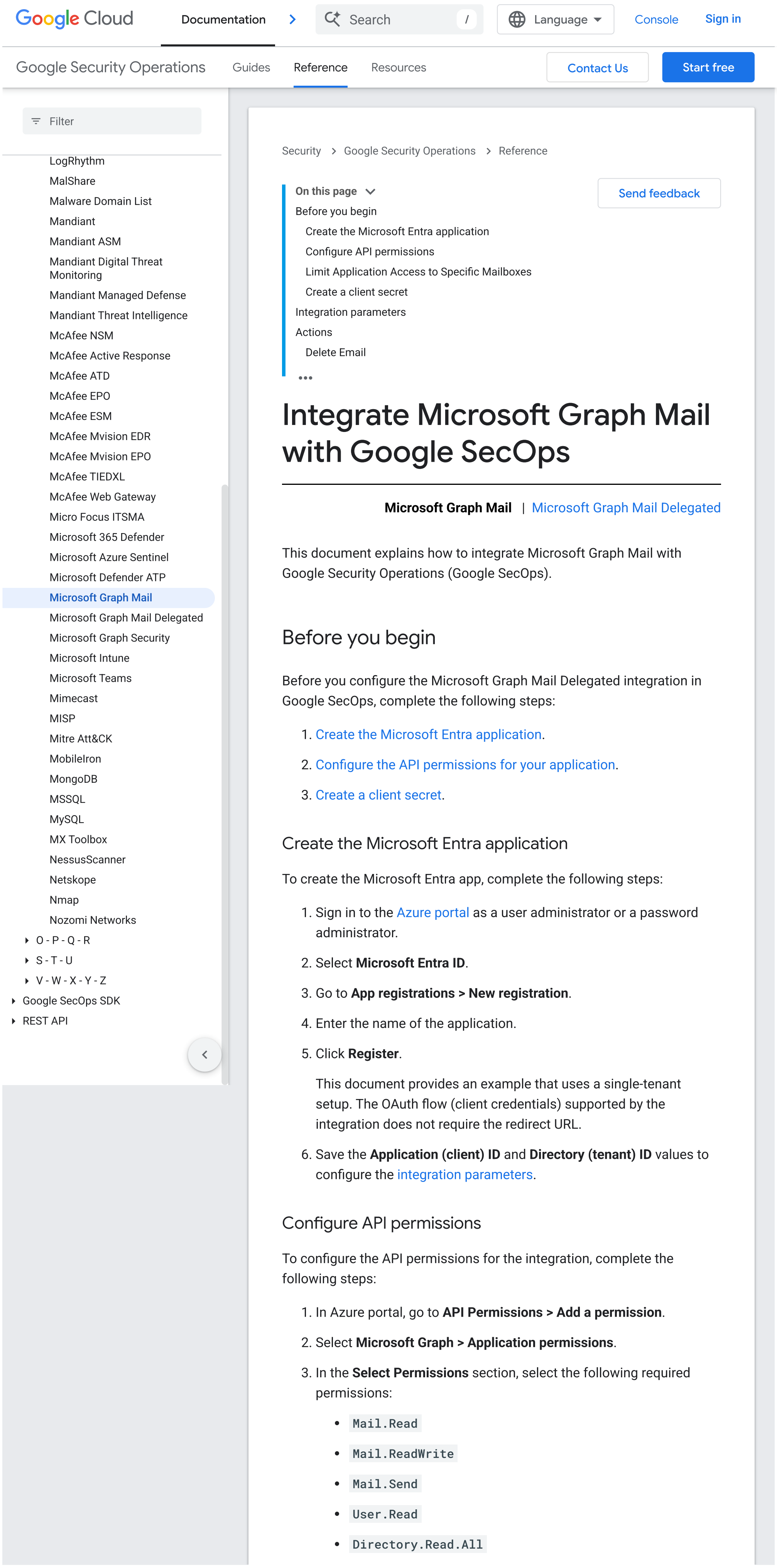
PORTFOLIO SAMPLE



Filter

LogRhythm
MalShare
Malware Domain List
Mandiant
Mandiant ASM
Mandiant Digital Threat Monitoring
Mandiant Managed Defense
Mandiant Threat Intelligence
McAfee NSM
McAfee Active Response
McAfee ATD
McAfee EPO
McAfee ESM
McAfee Mvision EDR
McAfee Mvision EPO
McAfee TIEDXL
McAfee Web Gateway
Micro Focus ITSMA
Microsoft 365 Defender
Microsoft Azure Sentinel
Microsoft Defender ATP
Microsoft Graph Mail
Microsoft Graph Mail Delegated
Microsoft Graph Security
Microsoft Intune
Microsoft Teams
Mimecast
MISP
Mitre Att&CK
MobileIron
MongoDB
MSSQL
MySQL
MX Toolbox
NessusScanner
Netskope
Nmap
Nozomi Networks
O - P - Q - R
S - T - U
V - W - X - Y - Z
Google SecOps SDK
REST API

Security > Google Security Operations > Reference

Send feedback

Integrate Microsoft Graph Mail with Google SecOps

Microsoft Graph Mail | Microsoft Graph Mail Delegated

This document explains how to integrate Microsoft Graph Mail with Google Security Operations (Google SecOps).

Before you begin

Before you configure the Microsoft Graph Mail Delegated integration in Google SecOps, complete the following steps:

1. Create the Microsoft Entra application.
2. Configure the API permissions for your application.
3. Create a client secret.

Create the Microsoft Entra application

To create the Microsoft Entra app, complete the following steps:

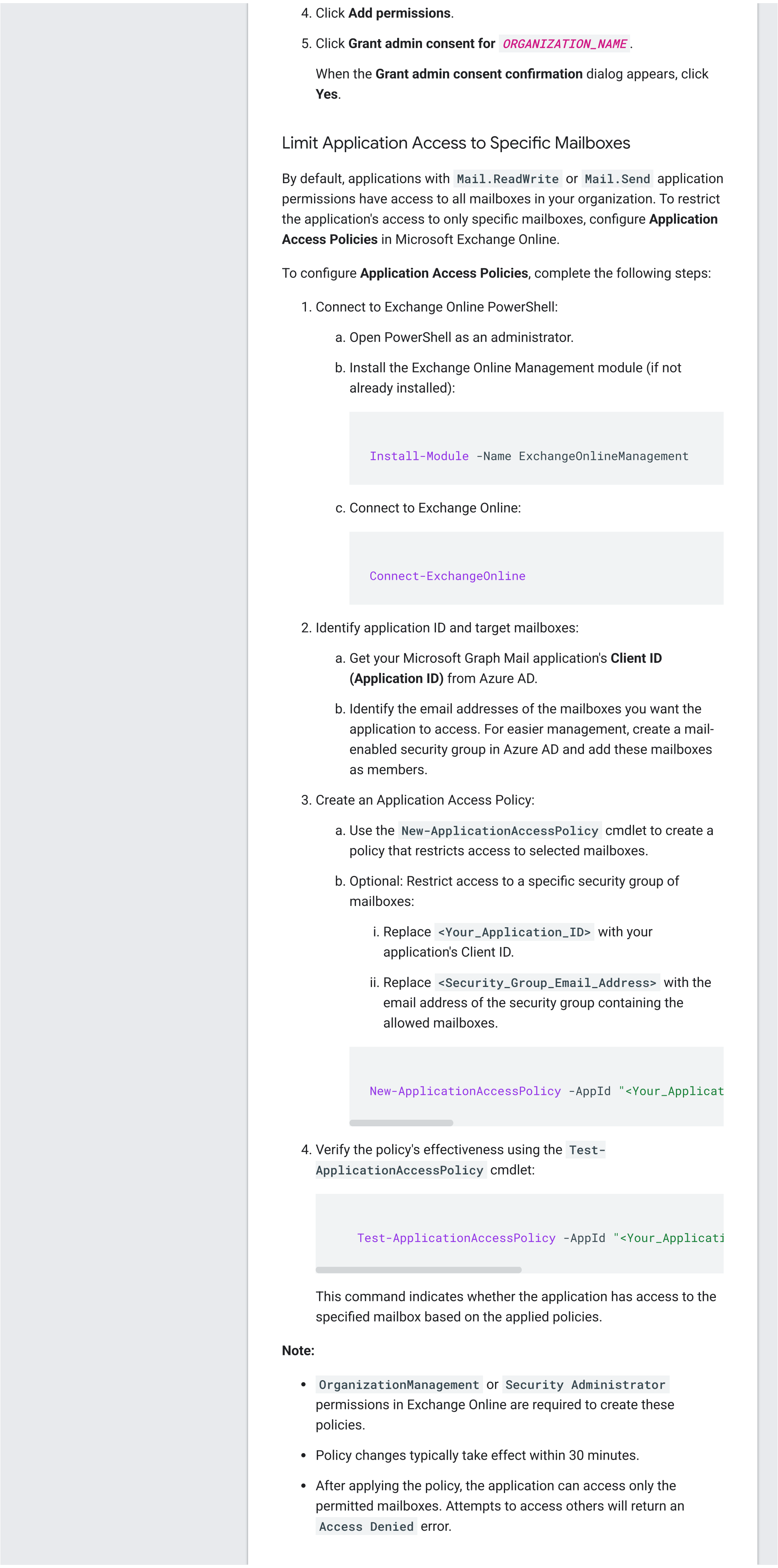
1. Sign in to the Azure portal as a user administrator or a password administrator.
2. Select **Microsoft Entra ID**.
3. Go to **App registrations > New registration**.
4. Enter the name of the application.
5. Click **Register**.

   This document provides an example that uses a single-tenant setup. The OAuth flow (client credentials) supported by the integration does not require the redirect URL.
6. Save the **Application (client) ID** and **Directory (tenant) ID** values to configure the integration parameters.

Configure API permissions

To configure the API permissions for the integration, complete the following steps:

1. In Azure portal, go to **API Permissions > Add a permission**.
2. Select **Microsoft Graph > Application permissions**.
3. In the **Select Permissions** section, select the following required permissions:
   - `Mail.Read`
   - `Mail.ReadWrite`
   - `Mail.Send`
   - `User.Read`
   - `Directory.Read.All`



4. Click **Add permissions**.
5. Click **Grant admin consent for** `ORGANIZATION_NAME`.

   When the **Grant admin consent confirmation** dialog appears, click **Yes**.

Limit Application Access to Specific Mailboxes

By default, applications with `Mail.ReadWrite` or `Mail.Send` application permissions have access to all mailboxes in your organization. To restrict the application's access to only specific mailboxes, configure **Application Access Policies** in Microsoft Exchange Online.

To configure **Application Access Policies**, complete the following steps:

1. Connect to Exchange Online PowerShell:
   a. Open PowerShell as an administrator.

   b. Install the Exchange Online Management module (if not already installed):

   ```
   Install-Module -Name ExchangeOnlineManagement
   ```

   c. Connect to Exchange Online:

   ```
   Connect-ExchangeOnline
   ```

2. Identify application ID and target mailboxes:
   a. Get your Microsoft Graph Mail application's **Client ID (Application ID)** from Azure AD.

   b. Identify the email addresses of the mailboxes you want the application to access. For easier management, create a mail-enabled security group in Azure AD and add these mailboxes as members.

3. Create an Application Access Policy:
   a. Use the `New-ApplicationAccessPolicy` cmdlet to create a policy that restricts access to selected mailboxes.

   b. Optional: Restrict access to a specific security group of mailboxes:

      i. Replace `<Your_Application_ID>` with your application's Client ID.

      ii. Replace `<Security_Group_Email_Address>` with the email address of the security group containing the allowed mailboxes.

   ```
   New-ApplicationAccessPolicy -AppId "<Your_Applicat
   ```

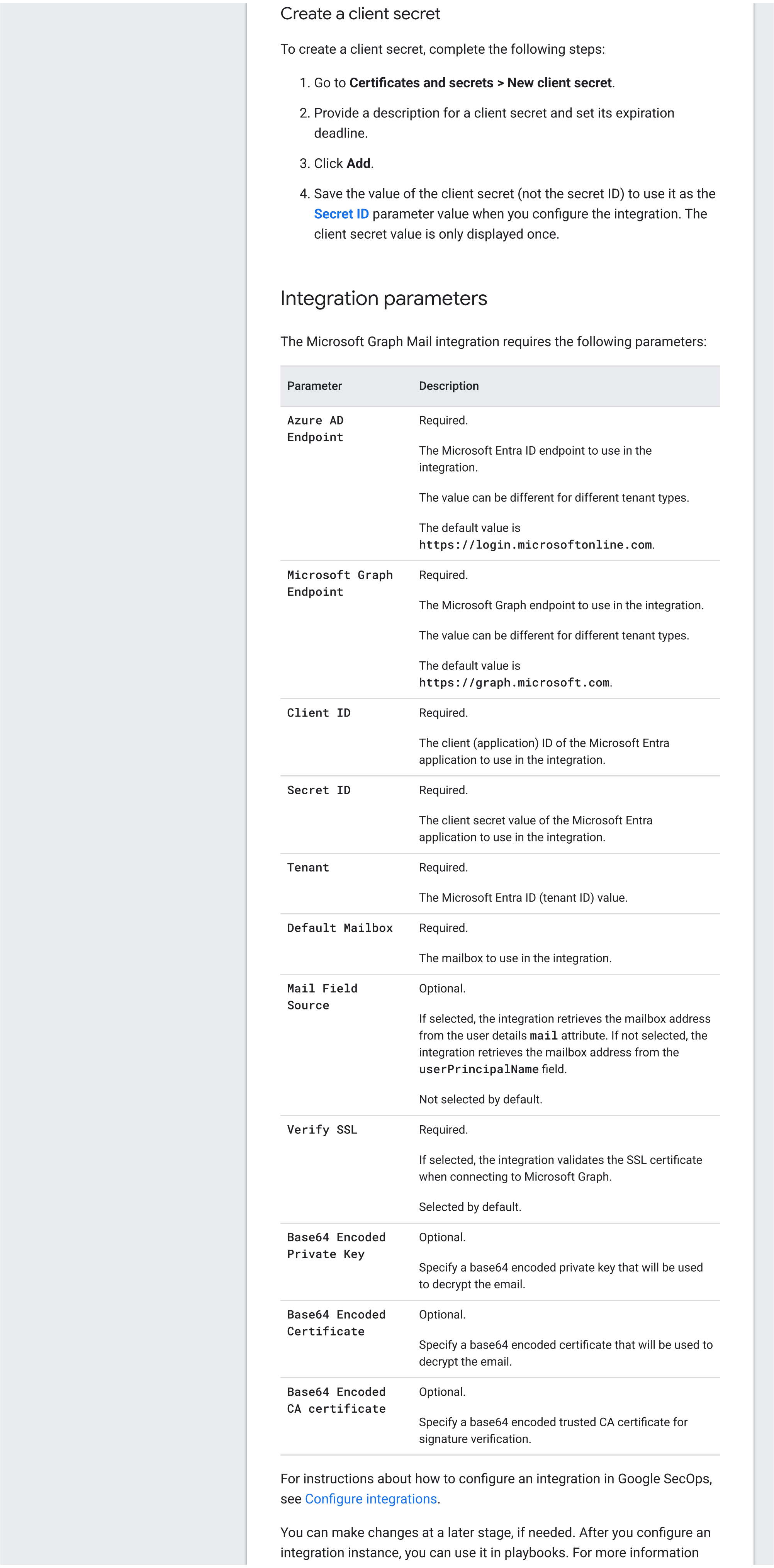
4. Verify the policy's effectiveness using the `Test-ApplicationAccessPolicy` cmdlet:

   ```
   Test-ApplicationAccessPolicy -AppId "<Your_Applicati
   ```

   This command indicates whether the application has access to the specified mailbox based on the applied policies.

Note:

- `OrganizationManagement` or `Security Administrator` permissions in Exchange Online are required to create these policies.
- Policy changes typically take effect within 30 minutes.
- After applying the policy, the application can access only the permitted mailboxes. Attempts to access others will return an `Access Denied` error.



Create a client secret

To create a client secret, complete the following steps:

1. Go to **Certificates and secrets > New client secret**.
2. Provide a description for a client secret and set its expiration deadline.
3. Click **Add**.
4. Save the value of the client secret (not the secret ID) to use it as the **Secret ID** parameter value when you configure the integration. The client secret value is only displayed once.

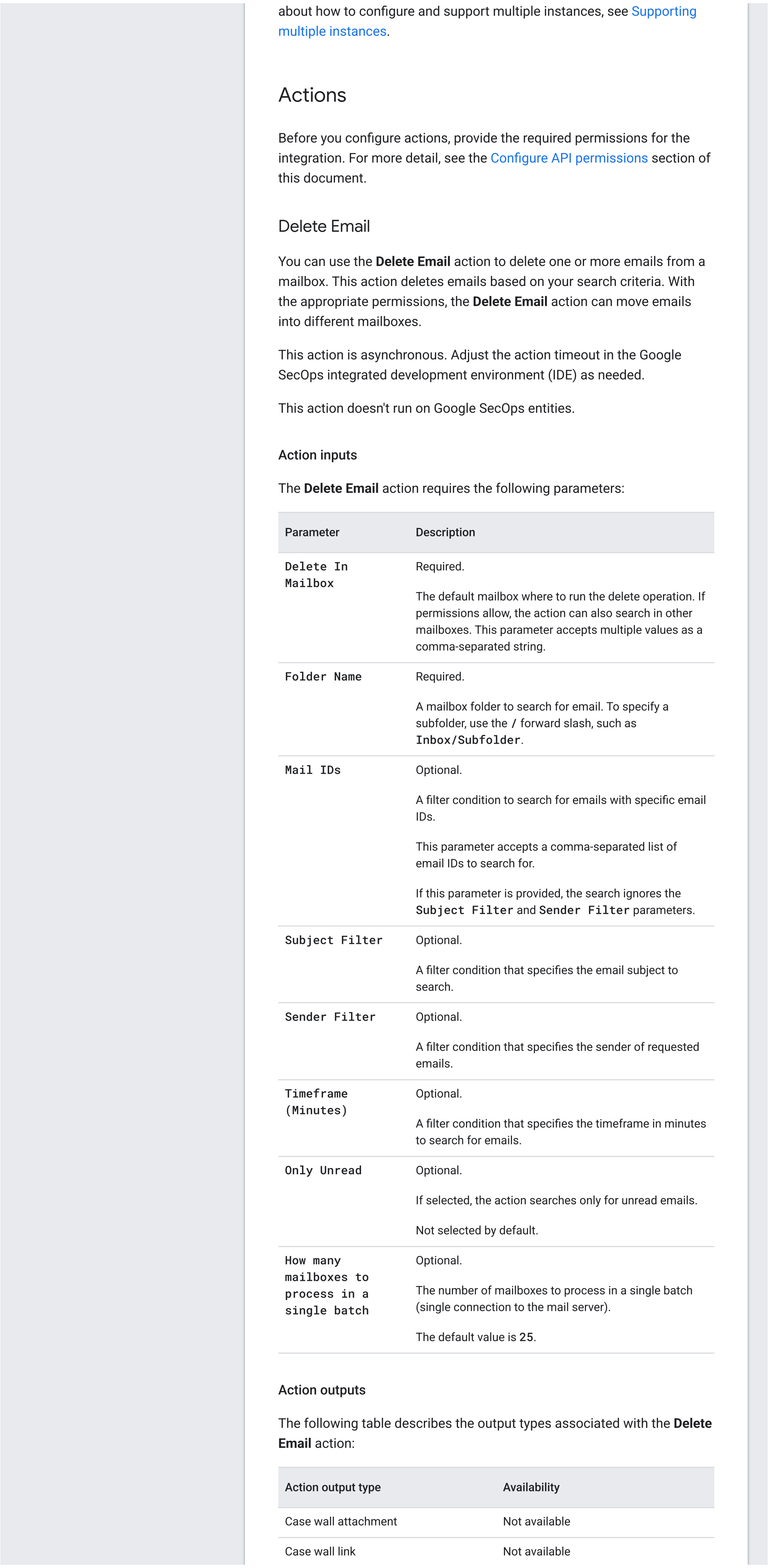
Integration parameters

The Microsoft Graph Mail integration requires the following parameters:

Parameter	Description
`Azure AD Endpoint`	Required. The Microsoft Entra ID endpoint to use in the integration. The value can be different for different tenant types. The default value is `https://login.microsoftonline.com`.
`Microsoft Graph Endpoint`	Required. The Microsoft Graph endpoint to use in the integration. The value can be different for different tenant types. The default value is `https://graph.microsoft.com`.
`Client ID`	Required. The client (application) ID of the Microsoft Entra application to use in the integration.
`Secret ID`	Required. The client secret value of the Microsoft Entra application to use in the integration.
`Tenant`	Required. The Microsoft Entra ID (tenant ID) value.
`Default Mailbox`	Required. The mailbox to use in the integration.
`Mail Field Source`	Optional. If selected, the integration retrieves the mailbox address from the user details `mail` attribute. If not selected, the integration retrieves the mailbox address from the `userPrincipalName` field. Not selected by default.
`Verify SSL`	Required. If selected, the integration validates the SSL certificate when connecting to Microsoft Graph. Selected by default.
`Base64 Encoded Private Key`	Optional. Specify a base64 encoded private key that will be used to decrypt the email.
`Base64 Encoded Certificate`	Optional. Specify a base64 encoded certificate that will be used to decrypt the email.
`Base64 Encoded CA certificate`	Optional. Specify a base64 encoded trusted CA certificate for signature verification.

For instructions about how to configure an integration in Google SecOps, see Configure integrations.

You can make changes at a later stage, if needed. After you configure an integration instance, you can use it in playbooks. For more information



about how to configure and support multiple instances, see Supporting multiple instances.

Actions

Before you configure actions, provide the required permissions for the integration. For more detail, see the Configure API permissions section of this document.

Delete Email

You can use the **Delete Email** action to delete one or more emails from a mailbox. This action deletes emails based on your search criteria. With the appropriate permissions, the **Delete Email** action can move emails into different mailboxes.

This action is asynchronous. Adjust the action timeout in the Google SecOps integrated development environment (IDE) as needed.

This action doesn't run on Google SecOps entities.

Action inputs

The **Delete Email** action requires the following parameters:

Parameter	Description
`Delete In Mailbox`	Required. The default mailbox where to run the delete operation. If permissions allow, the action can also search in other mailboxes. This parameter accepts multiple values as a comma-separated string.
`Folder Name`	Required. A mailbox folder to search for email. To specify a subfolder, use the `/` forward slash, such as `Inbox/Subfolder`.
`Mail IDs`	Optional. A filter condition to search for emails with specific email IDs. This parameter accepts a comma-separated list of email IDs to search for. If this parameter is provided, the search ignores the `Subject Filter` and `Sender Filter` parameters.
`Subject Filter`	Optional. A filter condition that specifies the email subject to search.
`Sender Filter`	Optional. A filter condition that specifies the sender of requested emails.
`Timeframe (Minutes)`	Optional. A filter condition that specifies the timeframe in minutes to search for emails.
`Only Unread`	Optional. If selected, the action searches only for unread emails. Not selected by default.
`How many mailboxes to process in a single batch`	Optional. The number of mailboxes to process in a single batch (single connection to the mail server). The default value is `25`.

Action outputs

The following table describes the output types associated with the **Delete Email** action:

Action output type	Availability
Case wall attachment	Not available
Case wall link	Not available