

# Email Security for Gmail

## Message Retraction

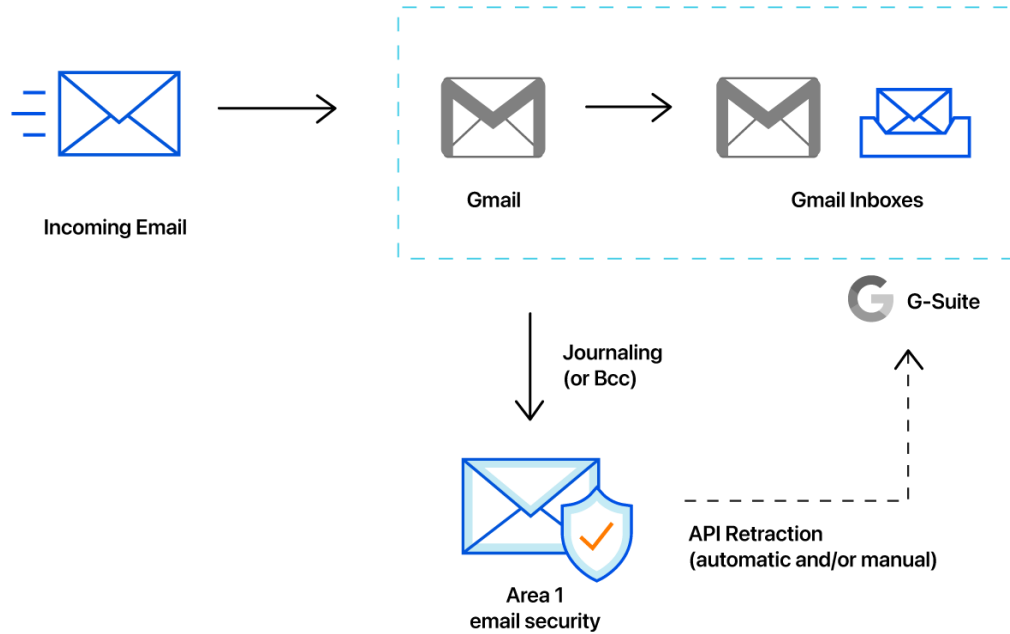
Deployment and Configuration Guide

### Area 1 Horizon Overview

Phishing is the root cause of 95% of security breaches that lead to financial loss and brand damage. Area 1 Horizon is a cloud based service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors & comprehensive attack analytics, Area 1 Horizon proactively identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Area 1 Horizon allows customers to take preemptive action against these targeted phishing attacks across all vectors - email, web and network; either at the edge or in the cloud.

## Email Flow



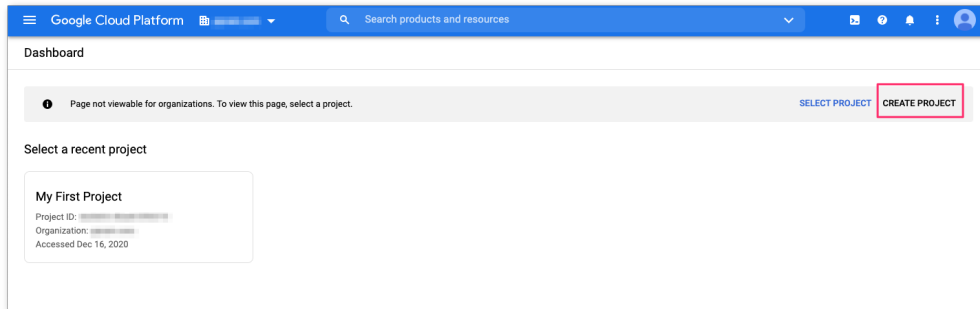
## Configuration Steps

- Step 1: Configure Project and Service account in GCP
- Step 2: Sharing the Service Account JSON Key with Area 1
- Step 3: Configure Auto-Retraction Actions in Area 1 Horizon
- Step 4: Adjust the Hop Count in Area 1 Horizon
- Step 5: Configure Bcc or Journaling in Google Workspaces
- Manual Retractions

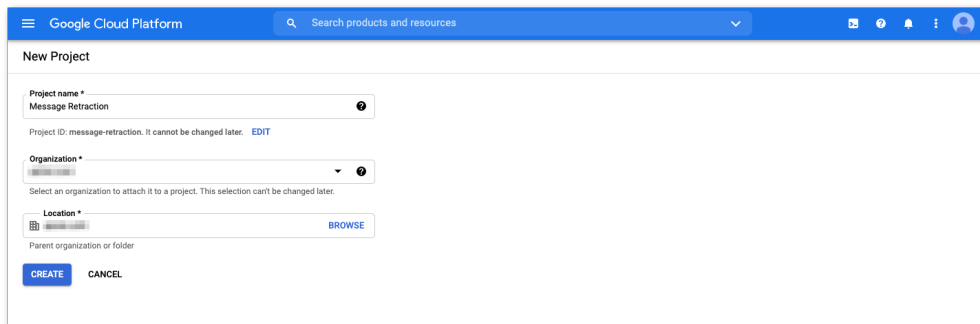
## Step 1: Configure Project and Service account in GCP

In order to allow Area 1 to retract messages from Gmail inboxes, a service account needs to be created as part of a GCP Project.

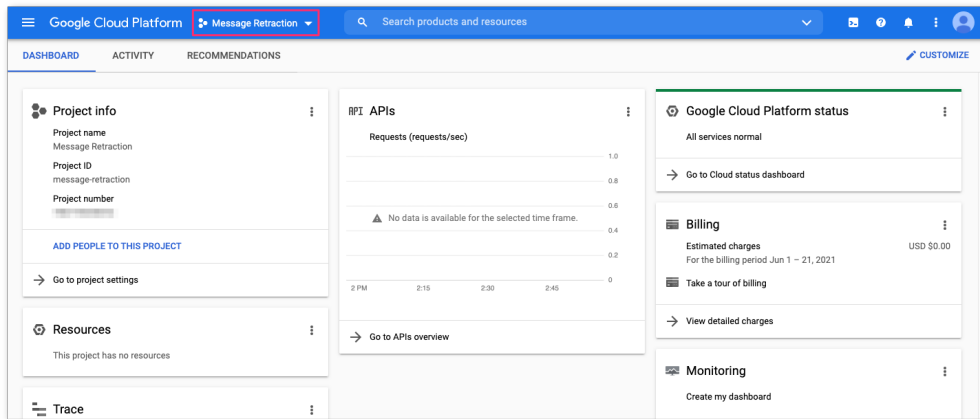
1. Access the Google Cloud Console (<https://console.cloud.google.com>). From the Dashboard, you can click the **CREATE PROJECT** button to start a new project.



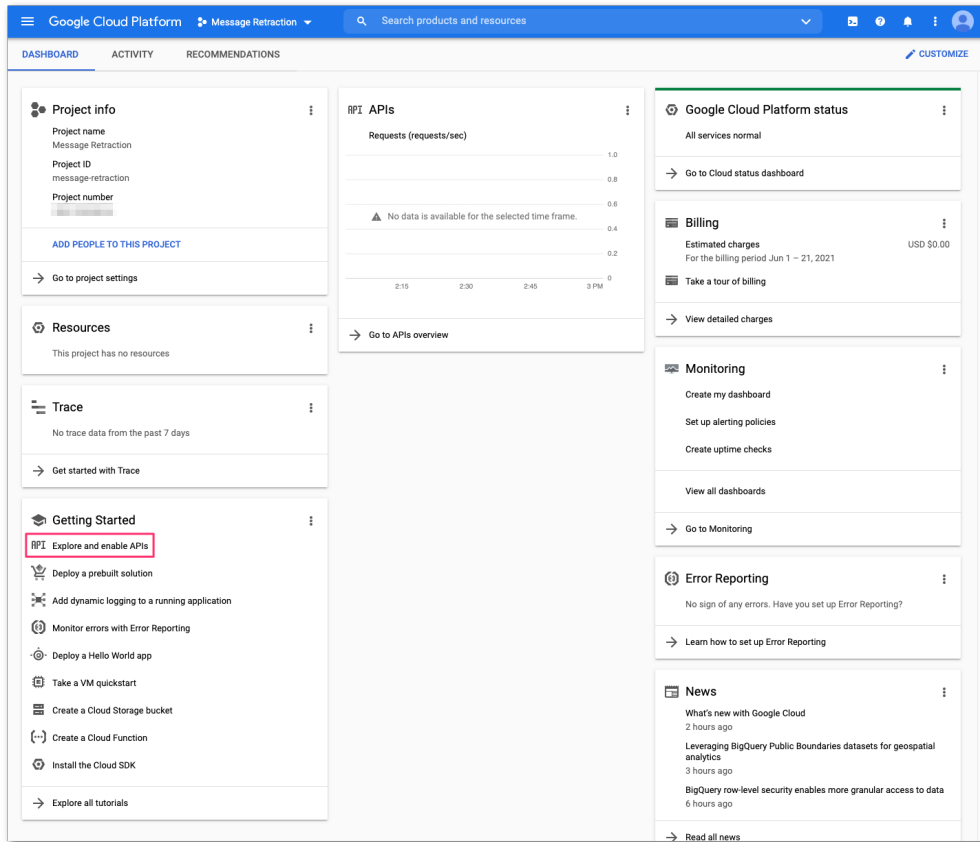
2. Provide the details for the new project and fill in with the appropriate information from your organization. Click the **CREATE** button to start your new project.



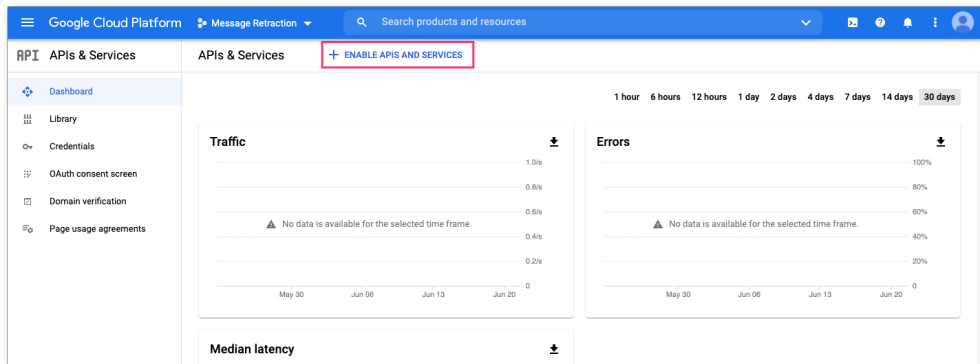
- Once the new project has been created, the GCP console will automatically redirect you to the Project console, if not, you can use the Project selector to change to the new project you just created.



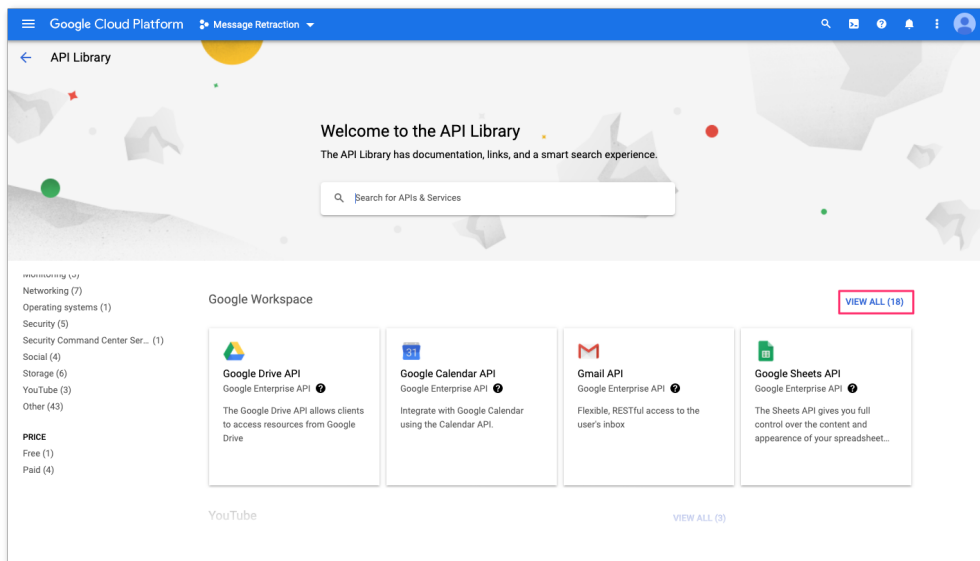
- Access the **APIs & Services** configuration console to enable API access to this project. You can find a link to the **APIs & Services** console under the **Getting Started** card:



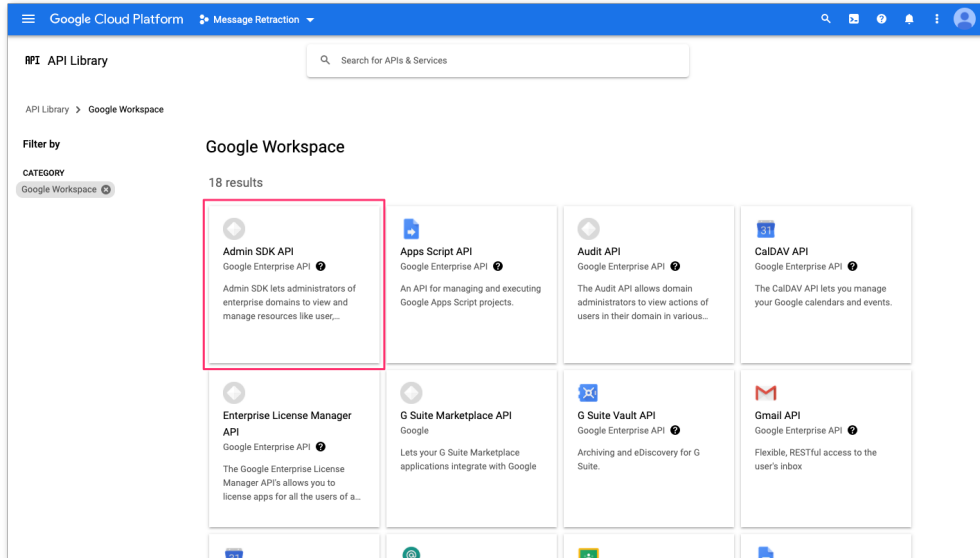
5. Click the **+ ENABLE APIS AND SERVICES** button to open the API Library.



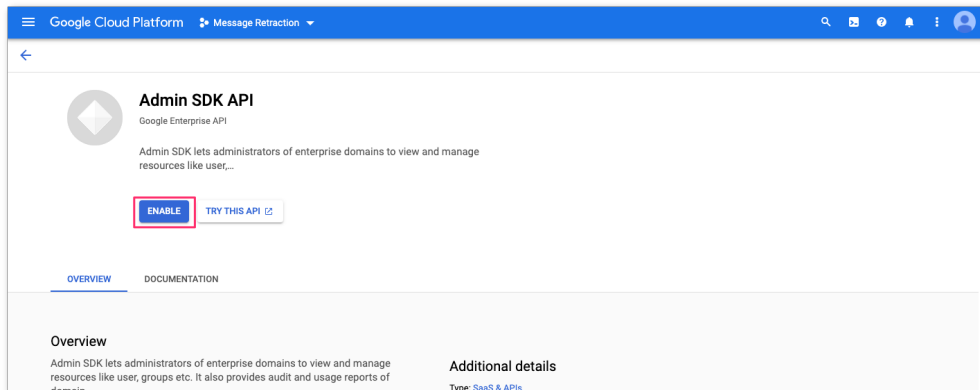
6. You will need to enable the **Admin SDK API** and the **Gmail API**. From the API Library and locate the **Google Workspace** section of the Library and click the **View All** link to access all the available APIs for Google Workspace:



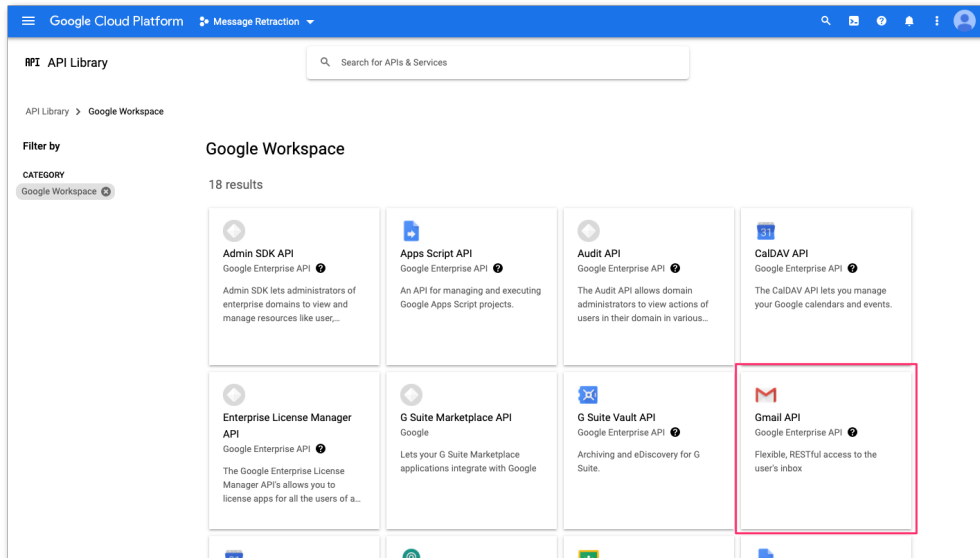
7. Select the **Admin SDK API**:



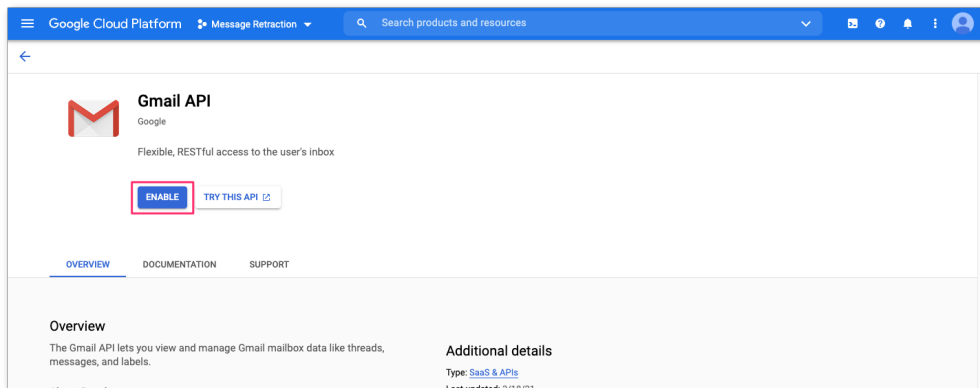
8. Click the **Enable** button to activate the **Admin SDK API**:



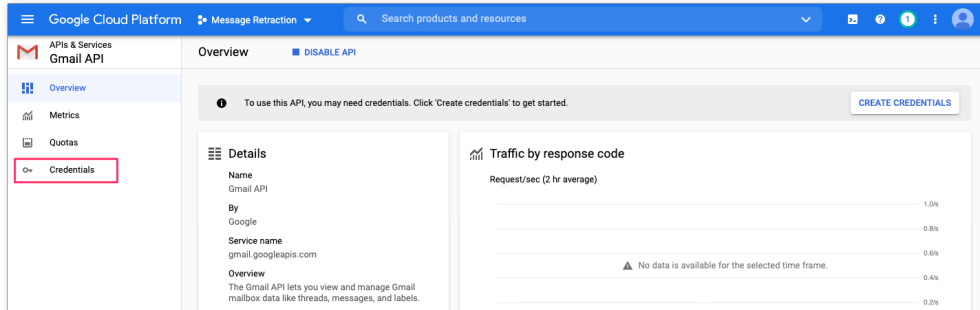
9. Return to the **Google Workspace** API library and select the **Gmail API**:



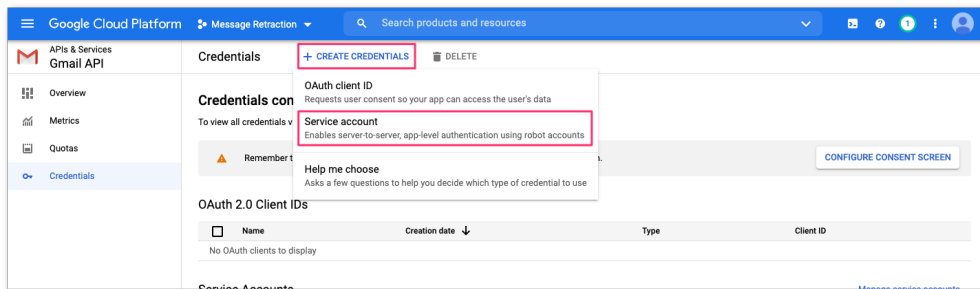
10. Click the **ENABLE** button to activate the **Gmail API**:



11. You will now need to create a **Service Account** to use the API. From the **Gmail API** console, click the **Credentials** option on the left navigation bar to start the process:



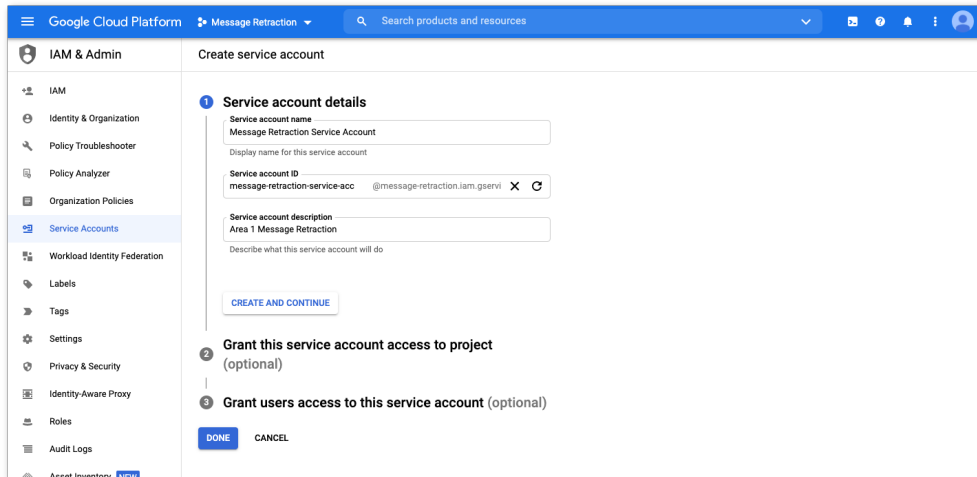
12. Click the **+ CREATE CREDENTIALS** menu option, followed by **Service account**, to start the process:



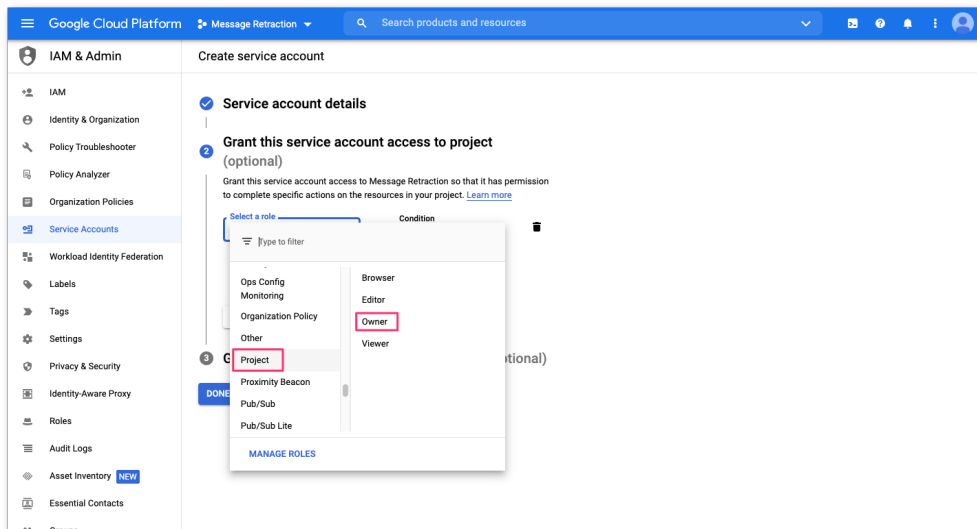


13. In the **Service account details** section, provide the details of the service account and click the **CREATE AND CONTINUE** button:

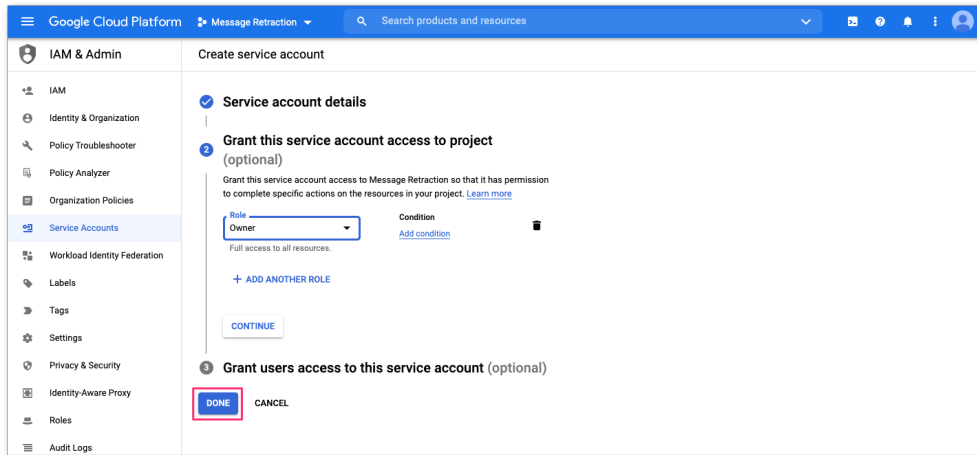
- Service account name (e.g. Message Retraction Service Account)
- Service account ID (value is automatically generated)
- Service account description (e.g. Area 1 Message Retraction)



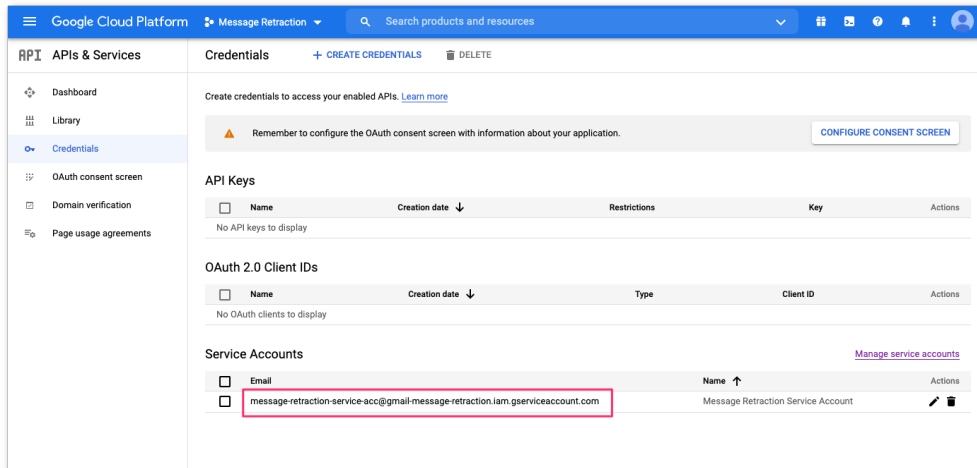
14. In the **Grant this service account access to project** section, click the **Select a role** dropdown. On the left column, find the **Project** item and select the **Owner** role on the right column:



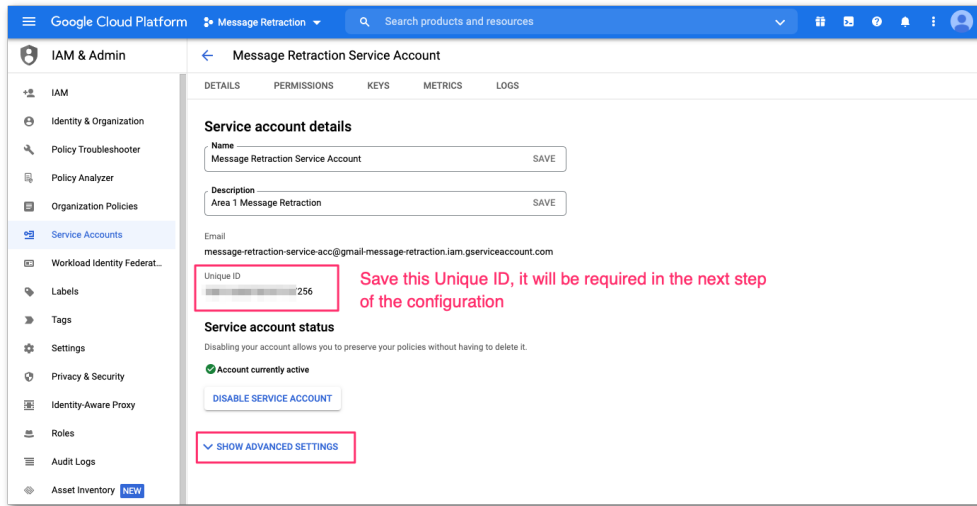
15. Once the role is assigned, click the **DONE** button to complete the setup:



16. Once the role assignment has been saved, you will be returned to the API credential configuration console. Click the newly created service account to configure the Domain-wide delegation:

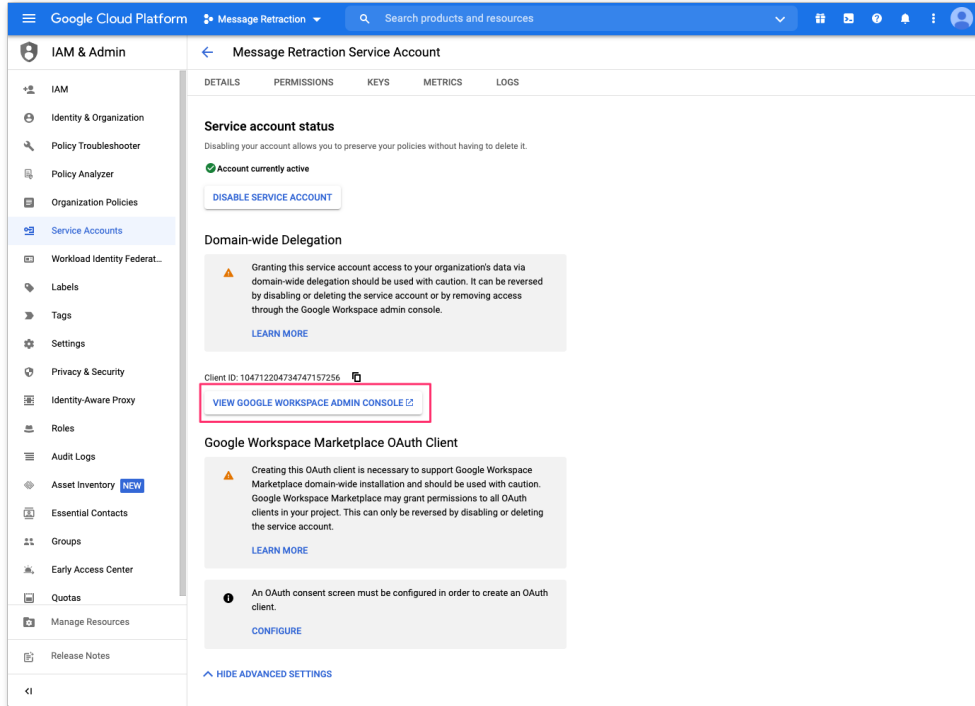


17. In the **Detail** of the service account, click the **SHOW ADVANCED SETTINGS** option to expose the advanced configuration options:

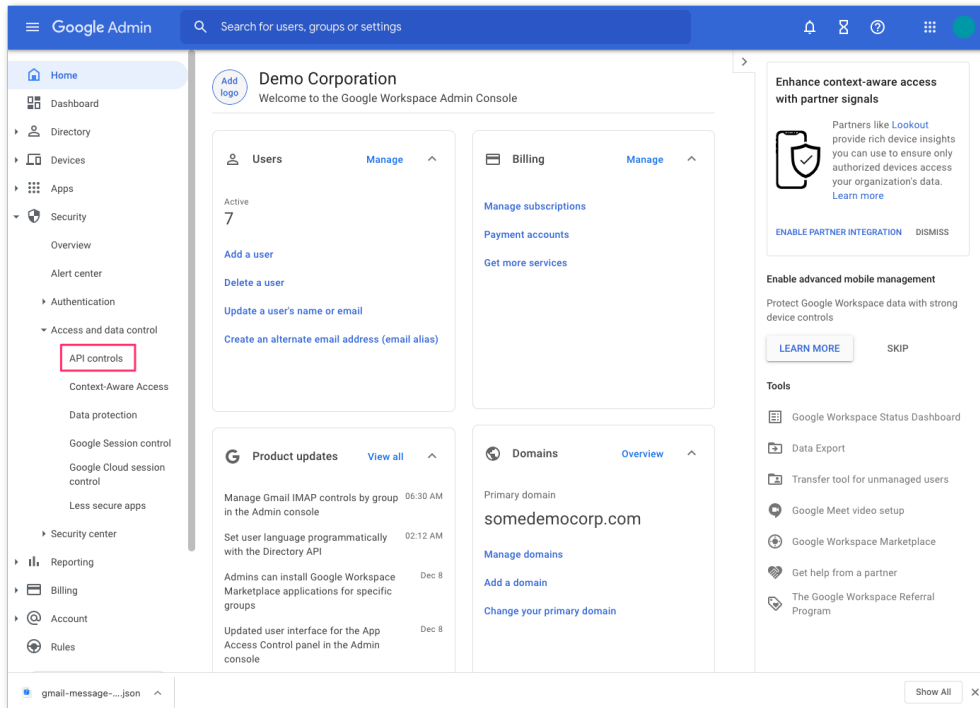


**Note:** Write down the **Unique ID** value as this information will be required in the configuration of the domain-wide delegation configuration in the Google Workspace configuration in the next step.

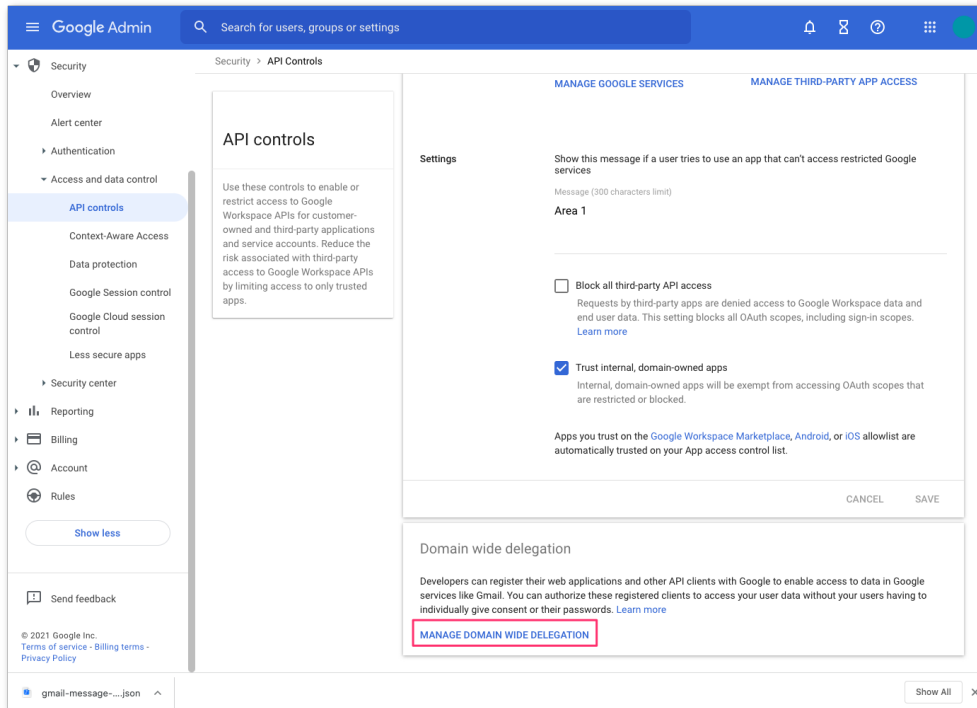
18. In the **ADVANCED SETTINGS**, click the **VIEW GOOGLE WORKSPACE ADMIN CONSOLE** button to configure the Domain-wide delegation. This will open a new window to the Google admin console:



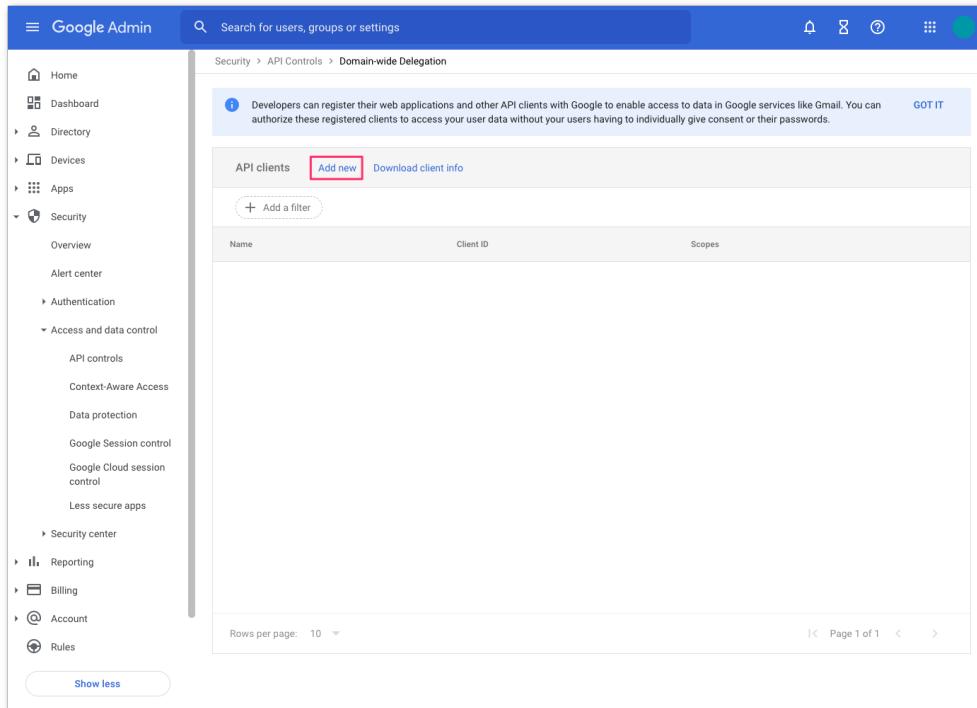
19. In the **Google Admin Console**, access the **API controls** by navigating to **Security >> Access and data control**:



20. In the **API controls**, navigate to the **Domain wide delegation** section and click the **MANAGE DOMAIN WIDE DELEGATION** link to add the service account:

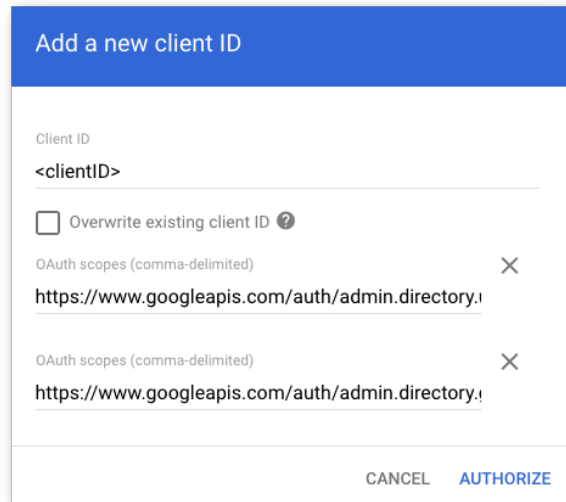


21. In the **Domain-wide Delegation** configuration panel, click **Add new** to add a new client ID:



22. In the **Add a new client ID** configuration dialog box:

- Enter your **client ID** (this is the Client ID saved from the previous step)
- Enter the following **OAuth scopes**:
  - i. <https://www.googleapis.com/auth/admin.directory.user.readonly>
  - ii. <https://www.googleapis.com/auth/admin.directory.group.readonly>
  - iii. <https://www.googleapis.com/auth/admin.directory.user.alias.readonly>
  - iv. <https://www.googleapis.com/auth/gmail.labels>
  - v. <https://mail.google.com/>

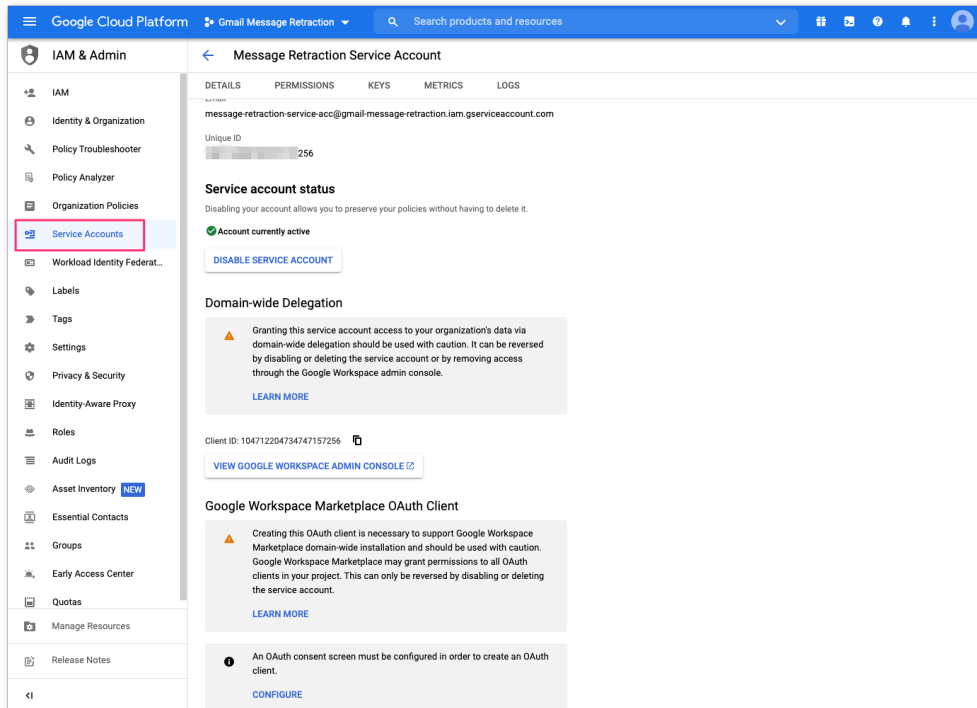



The screenshot shows a dialog box titled "Add a new client ID". It contains a text input field for "Client ID" with the placeholder "<clientID>". Below this is a checkbox for "Overwrite existing client ID" with a help icon. There are two "OAuth scopes (comma-delimited)" fields, each containing the URL "https://www.googleapis.com/auth/admin.directory," and a close button (X). At the bottom right, there are two buttons: "CANCEL" and "AUTHORIZE".

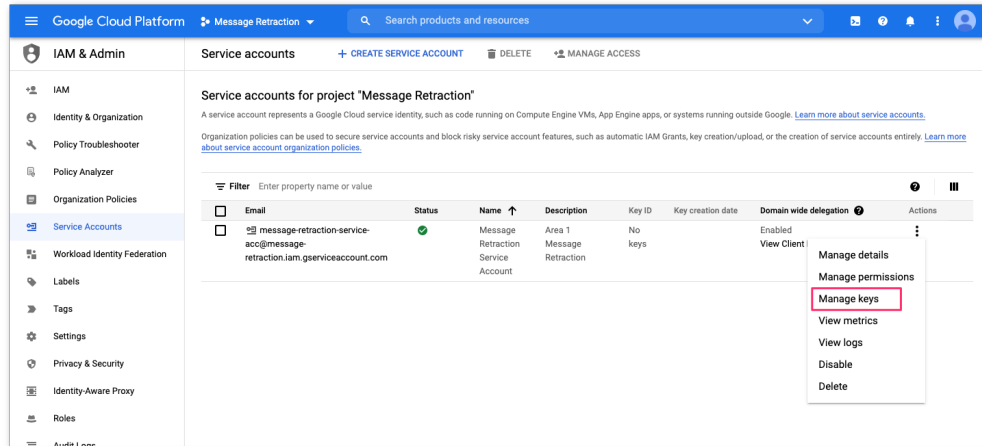
- Click **AUTHORIZE** to complete the configuration



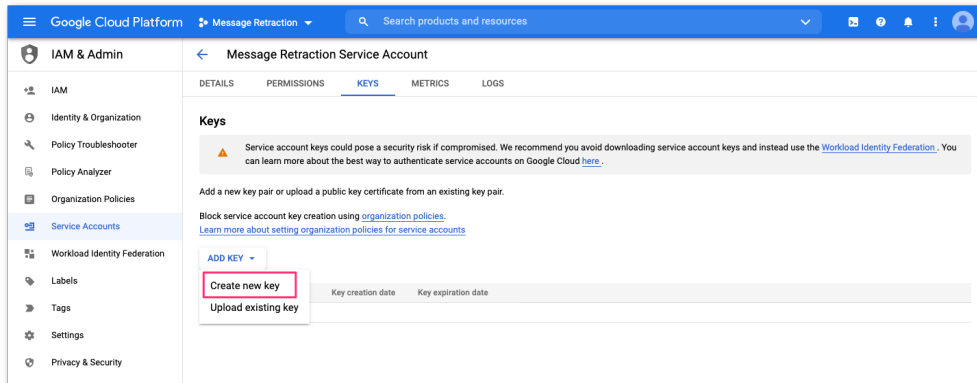
23. Return to the GCP Console and click the **Service Accounts** configuration option to return to the service account screen:



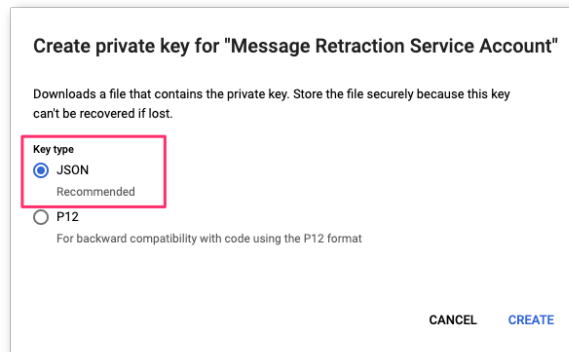
24. From the Service account configuration panel, you will need to create an API key, click the  button on the right side of the service account and select **Manage keys**:



25. In the **Keys** configuration panel, create a new key by selecting the **Create new key** option under the **ADD KEY** dropdown:



26. Create the **private key** using the **JSON** format and click **CREATE** to generate the key.



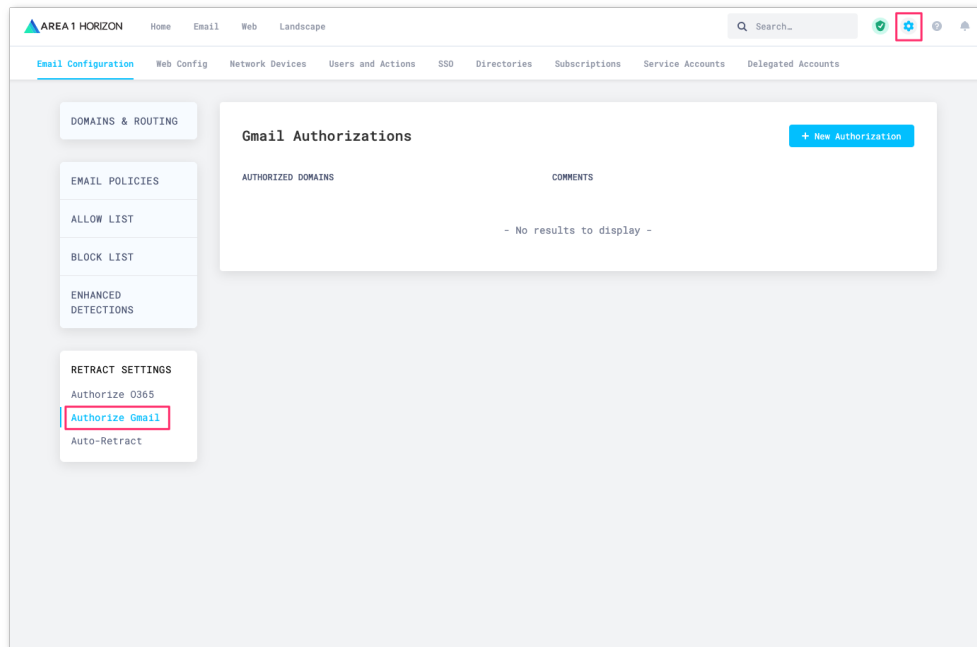
**Note:** Save the key in a secure location as it allows access to your cloud resources

**Note:** This key will need to be shared with Area 1 as part of the configuration process in the next step.

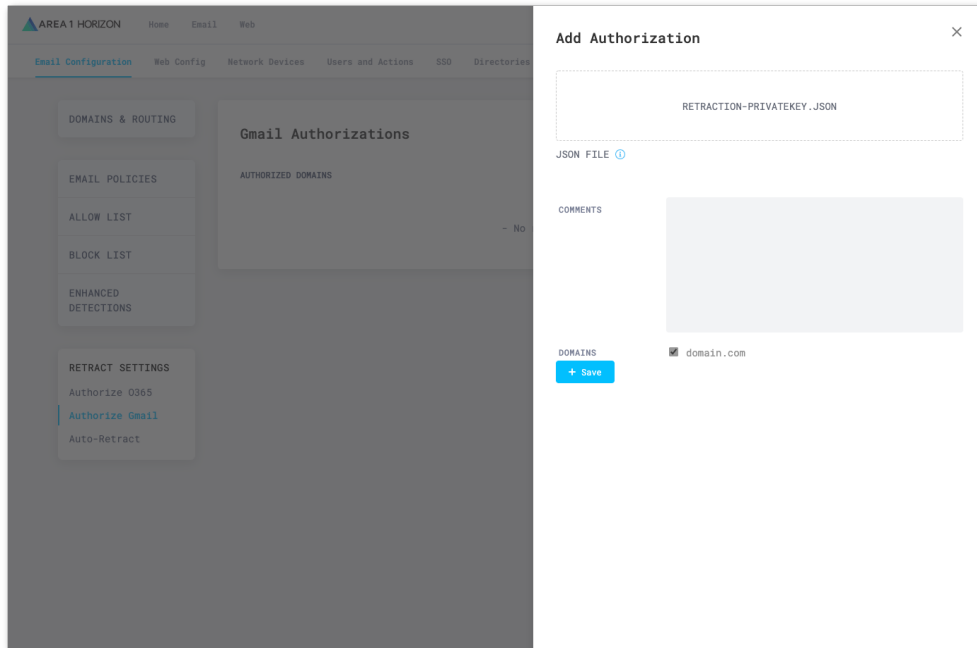
## Step 2: Sharing the Service Account JSON Key with Area 1

The Private Key that was generated in the previous step needs to be uploaded to Area 1 so retractions can be executed.

1. From the **Email Configuration** page, navigate to the **RETRACTION SETTINGS** portion of the configuration, select the **Authorize Gmail** option.

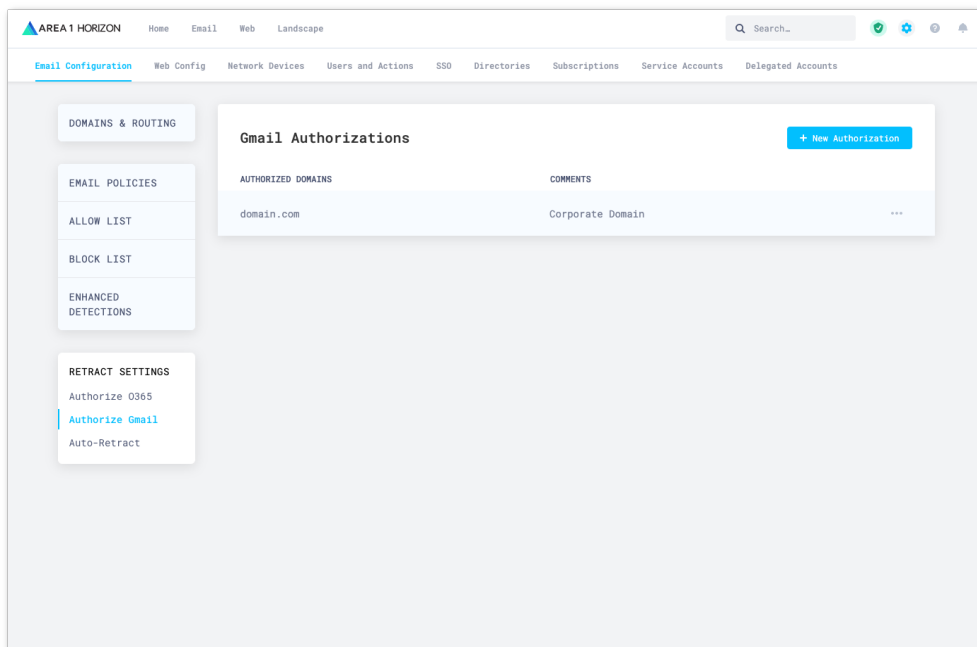


2. Click the **+ New Authorization** button to upload the JSON private key.



Click into the **AUTHORIZATION DATA (JWT)** box and select the JSON private key file.

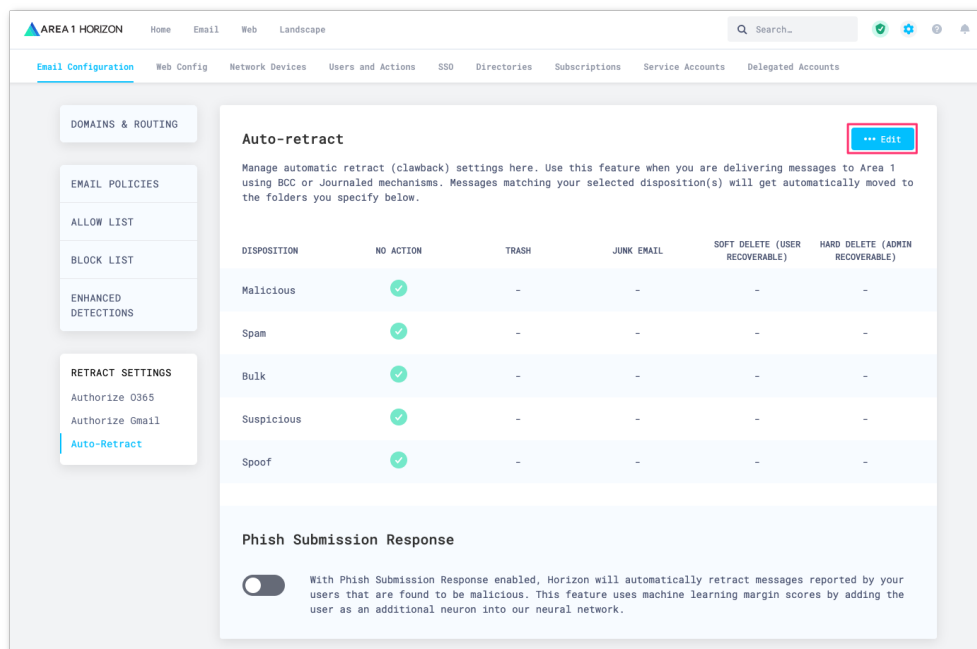
Under the **Domains** section, specify which domain this private key belongs to. Click **+Save** button to save the configuration



## Step 3: Configure Auto-Retract Actions in Area 1 Horizon

In the Area 1 Portal, you will need to configure the auto-retraction behavior for each disposition. Note that automatic retraction is not available when Area 1 is deployed as MX. From the **Email Configuration** page, navigate to the **RETRACTION SETTINGS** portion of the configuration:

1. Click the **Auto-Retract** option on the left navigation bar to access the retraction behavior setting. By default, no actions are taken against any of the dispositions. To modify the behaviors, click the **Edit** button:

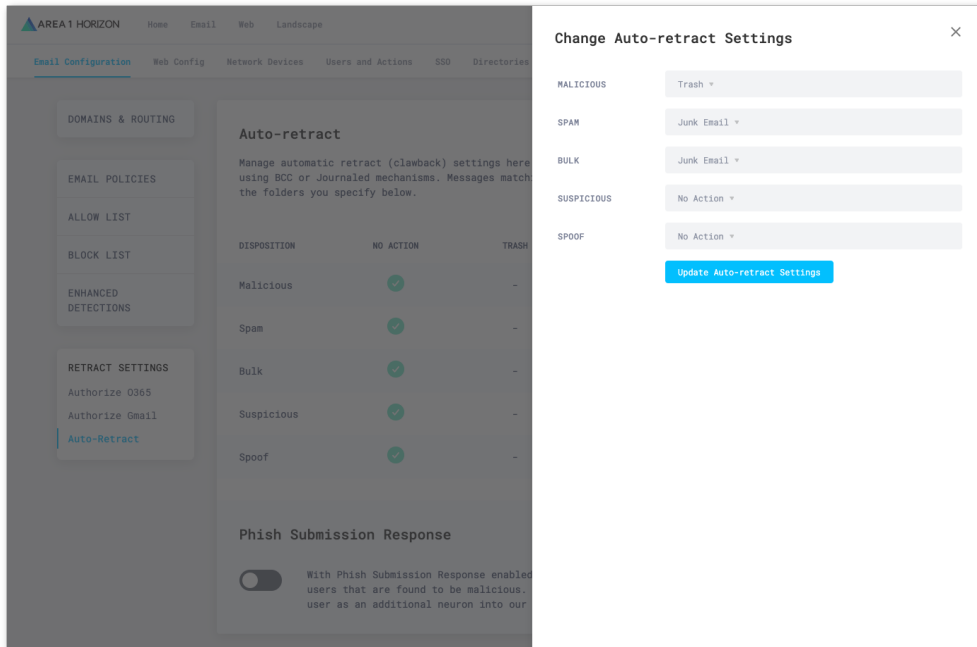


The screenshot shows the 'Auto-retract' configuration page in the Area 1 Horizon portal. The page has a left-hand navigation menu with sections for 'DOMAINS & ROUTING', 'EMAIL POLICIES', and 'RETRACT SETTINGS'. Under 'RETRACT SETTINGS', 'Auto-Retract' is selected. The main content area is titled 'Auto-retract' and includes an 'Edit' button. Below the title is a table with columns for 'DISPOSITION', 'NO ACTION', 'TRASH', 'JUNK EMAIL', 'SOFT DELETE (USER RECOVERABLE)', and 'HARD DELETE (ADMIN RECOVERABLE)'. The table lists five dispositions: Malicious, Spam, Bulk, Suspicious, and Spoof, each with a green checkmark in the 'NO ACTION' column and dashes in the others. Below the table is a 'Phish Submission Response' section with a toggle switch and explanatory text.

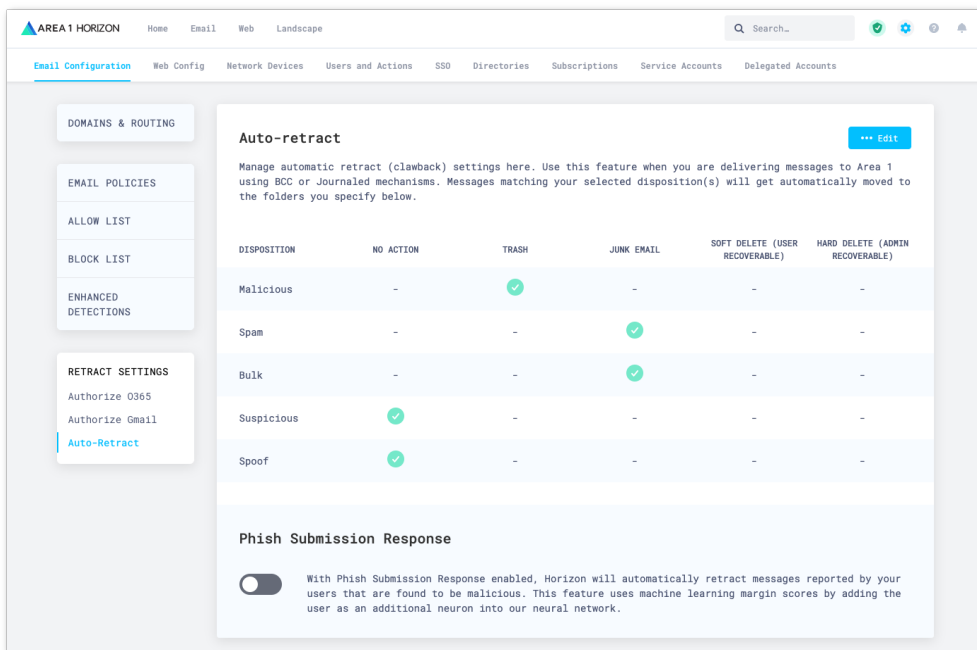
DISPOSITION	NO ACTION	TRASH	JUNK EMAIL	SOFT DELETE (USER RECOVERABLE)	HARD DELETE (ADMIN RECOVERABLE)
Malicious	✓	-	-	-	-
Spam	✓	-	-	-	-
Bulk	✓	-	-	-	-
Suspicious	✓	-	-	-	-
Spoof	✓	-	-	-	-

**Note:** You must be an Area 1 Horizon Enterprise customer in order to access the **RETRACTION SETTINGS** configuration panel. If the setting is not available, please contact customer support at [support@area1security.com](mailto:support@area1security.com).

- Select the appropriate remediation behavior for each dispositions and save your selection by clicking the **Update Auto-retraction Settings**:

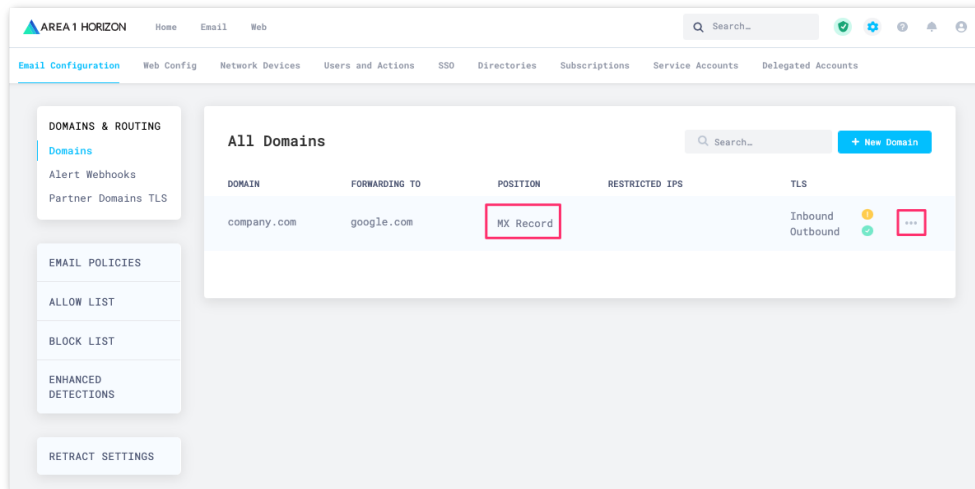


- Once saved, the configuration table will update with the selected behaviors:



## Step 4: Adjust the Hop Count in Area 1 Horizon

Since Area 1 is not configured as the MX record for your domains, you will need to adjust Area 1's position (hop count) relative to Area 1's position in the email processing order. From the **Email Configuration** page, under **DOMAIN & ROUTING**, select the **Domain** option and verify the position:





- For standalone Gmail only deployments, the value should be set to **2**. To update the hop count, click the ... button on the right side of the domain you want to update and adjust the **Hops** count to 2. Then, click the **Update Domain** button to update the configuration.

The screenshot shows a configuration window titled "Edit Domain" with a close button (X) in the top right corner. The window contains the following fields and options:

- DOMAIN:** A text input field containing "company.com".
- CONFIGURED AS:** Two radio button options: "MX Records" (unselected) and "Hops" (selected). To the right of "Hops" is a small input field containing the number "2".
- FORWARDING TO:** A text input field containing "google.com".
- IP RESTRICTIONS:** A section with an information icon (i) and a large, empty light gray rectangular area below it.
- INBOUND TLS:** A toggle switch that is currently turned off.
- OUTBOUND TLS:** A section with the text "FORWARD ALL MESSAGES OVER TLS".
- QUARANTINE POLICY:** A section with four unchecked checkboxes: "Malicious", "Spam", "Suspicious", and "Spooof". Each checkbox has an information icon (i) to its right.
- Update Domain:** A blue button at the bottom center of the window.

**Note:** If you have an existing SEG deployed as the MX record, you will need to adjust the hop count accordingly. Please contact Support if you need any assistance identifying the correct hop count.



## Step 5: Configure Bcc or Journaling in Google Workspaces

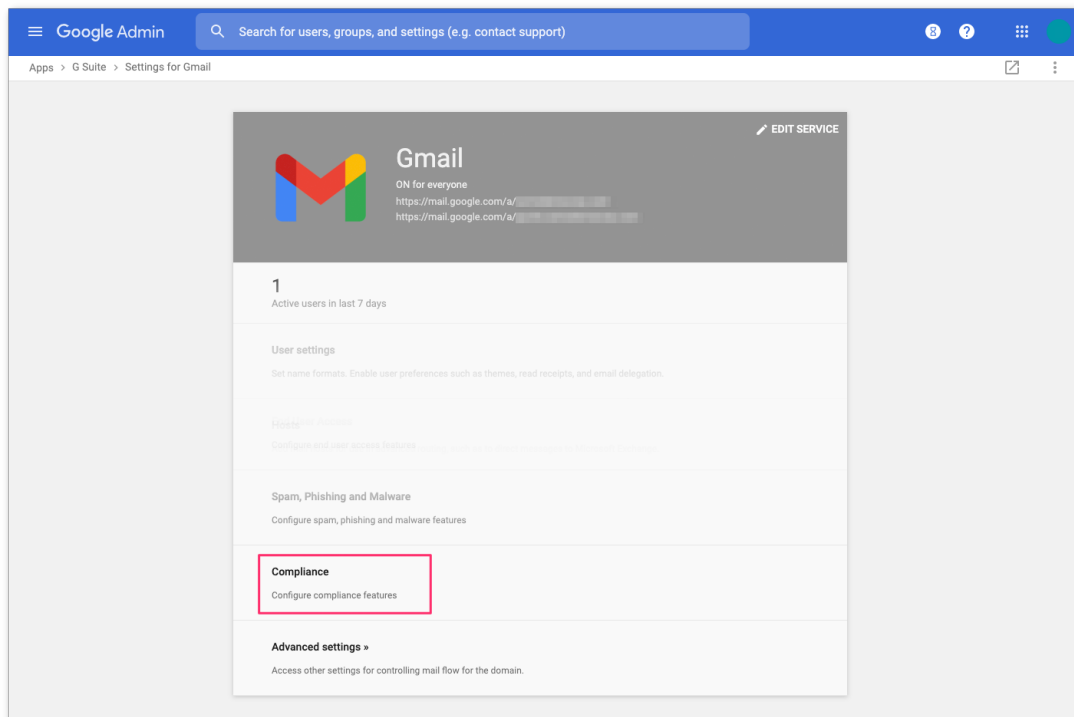
In order for Area 1 Horizon to be able to automatically retract messages, copies of the inbound messages must be sent to Area 1 for inspection. Note that automatic retraction is not available when Area 1 is deployed as MX. Messages can be sent to Area 1 using a **Bcc compliance rule** or **message journaling** method.

Either methods work equally well, the method to use will be dependent on the Google licenses you have purchased:

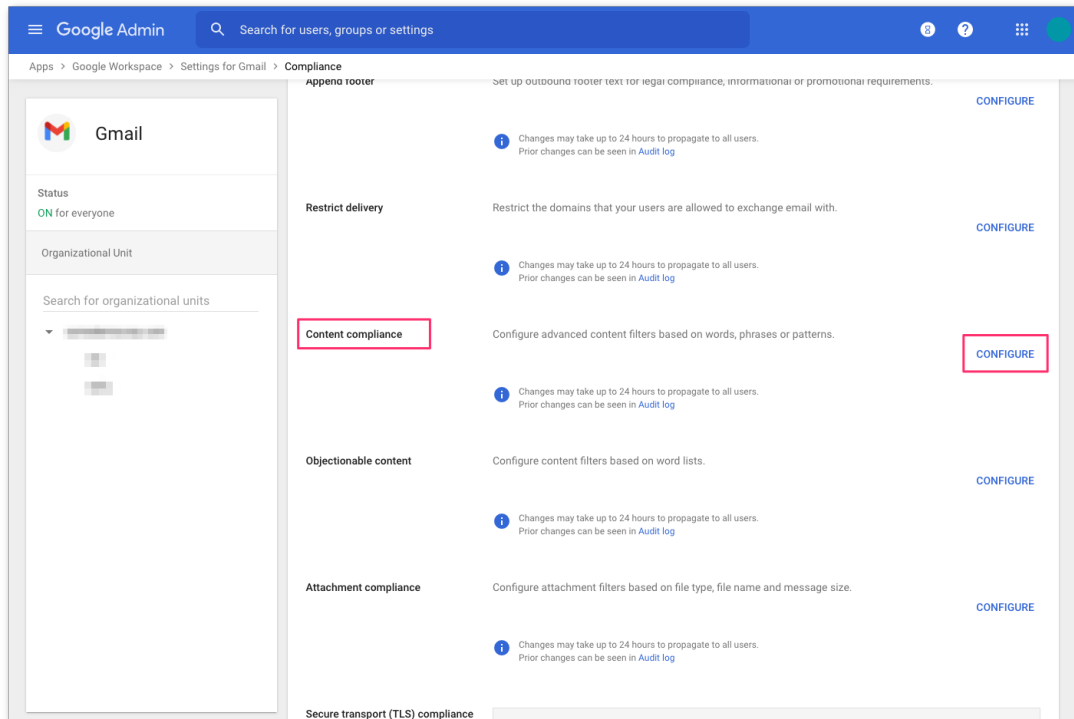
- The Bcc method is available to all tiers of paid Google licenses.
- The journaling method is **only** available to Google Enterprise users, if you have a mix of Business and Enterprise licenses, use the Bcc method.

### Configure Bcc Compliance Rule

1. To configure the Bcc compliance rule, start from the **Gmail Administrative Console** and access the **Compliance** configuration option:

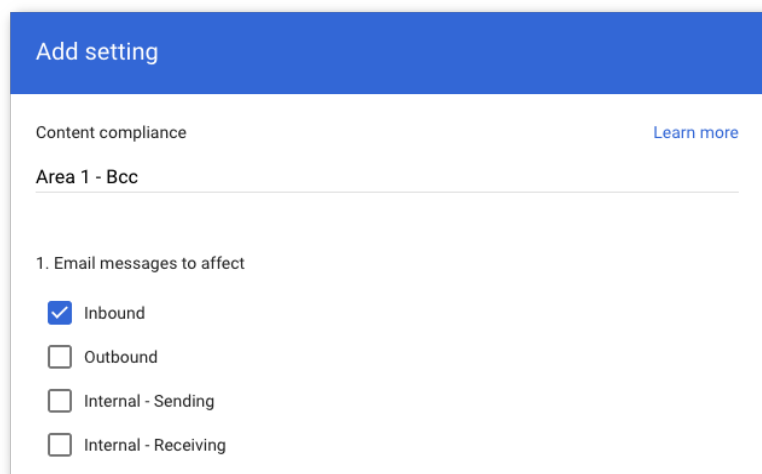


2. In the **Compliance** section of the configuration, navigate down the list and click the **CONFIGURE** button the right of the **Content Compliance** section:



3. In the Configuration dialog that appears, configure the Bcc compliance rule as follows:

- Name the Content Compliance filter **Area 1 - Bcc**
- In the first section **1. Email messages to affect**, select **Inbound**



In the **2. Add expression that describe the content you want to search for in each message** section, configure the conditions where the rule will trigger:

- a. Click **Add** to configure the expression
- b. Select **Advanced content match**
  - i. For **Location**, select “Any envelope recipient”
  - ii. For **Match type**, select **Ends with**
  - iii. For **Content**, enter your email domain (e.g. company.com)
  - iv. Click **SAVE** to save your settings

The screenshot shows a dialog box titled "Add setting" with a blue header. Below the header, there is a section titled "Advanced content match" with a dropdown arrow. Underneath, there are three fields: "Location" with a dropdown menu showing "Any envelope recipient", "Match type" with a dropdown menu showing "Ends with", and "Content" with a text input field containing "company.com". At the bottom right of the dialog, there are two buttons: "CANCEL" and "SAVE".

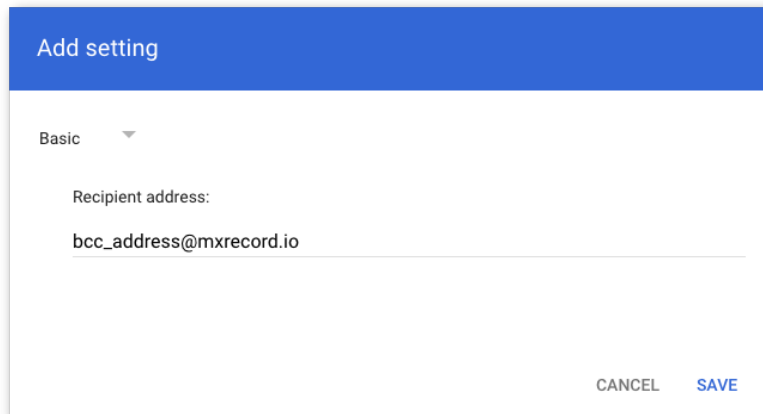
4. Repeat the previous step to additional domains to your list. Ensure that the search condition is set to **If Any of the following match the message**, this will apply an **OR** to the trigger conditions. Below is an example with 2 email domains:

The screenshot shows a section titled "2. Add expressions that describe the content you want to search for in each message". Below the title, there is a dropdown menu showing "If ANY of the following match the message". Underneath, there is a table with two rows of expressions:

Expressions
Location: Any envelope recipient Ends with: company.org
Location: Any envelope recipient Ends with: company.com

At the bottom right of the table, there is an "ADD" button.

5. In the **3. If the above expressions match, do the following** section, navigate down the list and select the **Also deliver to** action:
  - a. Add the recipient Bcc address (this will be provided by Area 1). Keep the recipients setting to **Basic**.
  - b. Click **SAVE** to save the the recipient



Add setting

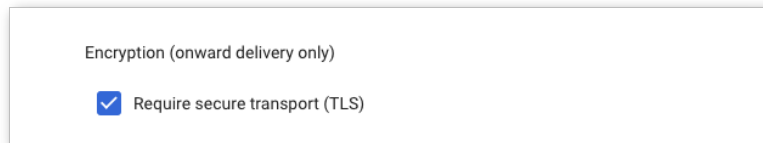
Basic ▾

Recipient address:

bcc\_address@mxrecord.io

CANCEL SAVE

6. If TLS delivery is desired, select the **Require Secure Transport (TLS)** option under the **Encryption (onward delivery only)** section.



Encryption (onward delivery only)

Require secure transport (TLS)

7. Click **SAVE** at the bottom of the **Add setting** dialog box to save the content compliance filter.

**Add setting**

Change envelope recipient

Spam

Bypass spam filter for this message

Attachments

Remove attachments from message

Also deliver to

Add more recipients

**Recipients**

Deliver to: bcc\_address@mxrecord.io  
Do not deliver spam to this recipient  
Suppress bounces from this recipient

[ADD](#)

Encryption (onward delivery only)

Require secure transport (TLS)

[Show options](#)

[CANCEL](#) [SAVE](#)

8. The rule will be activated once the filter is saved:

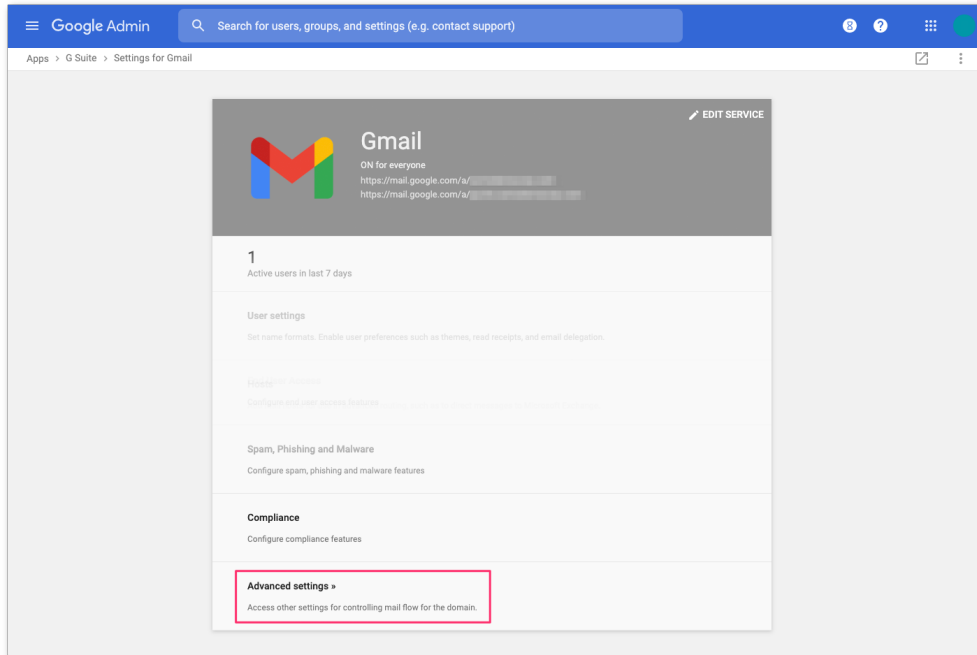
Description	Status	Source	Actions	ID	Messages	Matches	Consequences
Area 1 - Bcc	Enabled	Locally applied	<a href="#">Edit</a> - <a href="#">Disable</a> - <a href="#">Delete</a>	114a0	Inbound	2	Modify message Additional delivery: 1 Require secure transport (TLS)

[ADD ANOTHER RULE](#)

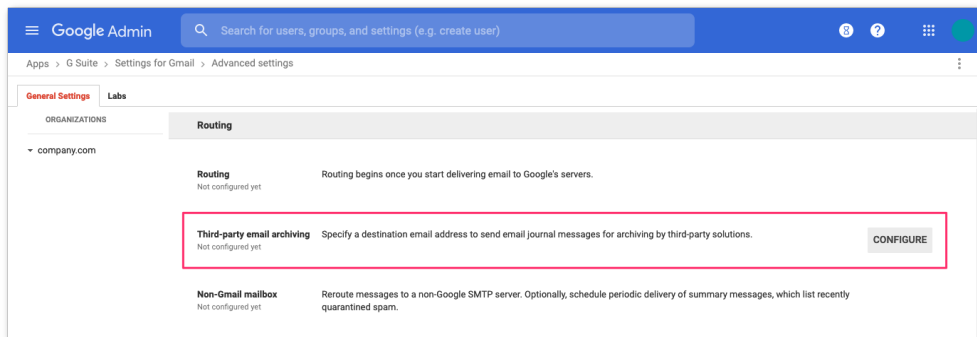
## Configure Journaling Rule

To configure Journaling, you will need to access the Gmail Administrative Console from the main Google Admin page (<https://admin.google.com>).

1. Start from the **Gmail Administrative Console** and select the **Advanced settings** option at the bottom of the Gmail Console:



2. In the Advanced configuration console, under the **Routing** section, navigate to the **Third-party email archiving** setting and click the **CONFIGURE** button to start the configuration:





3. In the configuration dialog, provide a short description of the rule and the address where to send the journal messages:

**Note:** The **Journal address** will be provided to you by Area 1.

The screenshot shows a dialog box titled "Add setting" with a close button (X) in the top right corner. The main heading is "Third-party email archiving" with a "Help" link to its right. Below this, the text "Area 1 Journaling" is displayed. A horizontal line separates the header from the configuration area. The first step is "1. Send journal messages to this email address", followed by the email address "company@journaling.mxrecord.io" entered in a text field. Below the text field is another horizontal line. At the bottom of the dialog, there is a yellow warning icon followed by the text "Third-party email archiving setting applies to G Suite Enterprise users only". In the bottom right corner, there are two buttons: "CANCEL" and "ADD SETTING".

4. Click the **ADD SETTING** button to validate your configuration.
5. Once added, a new entry will be visible in your configuration:

The screenshot shows a configuration list entry for "Third-party email archiving" under the heading "Area 1 Journaling". The status "Locally applied" is shown to the left of the heading. To the right of the heading, the text "Email journal destination email address: company@journaling.mxrecord.io" is displayed. Below this, there is a yellow warning icon followed by the text "This rule only applies only to licensed users with the appropriate G Suite offering."

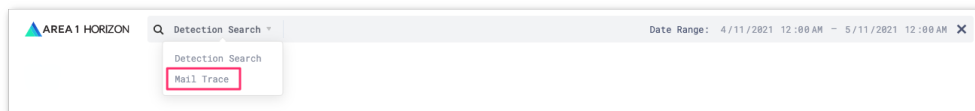
6. To confirm and activate the configuration. You will need to click the **SAVE** button located at the lower right corner of the browser window.

The screenshot shows the bottom of a browser window with a settings summary. It includes three items: a blue checkmark icon with the text "Do not delete email and chat messages automatically.", a yellow warning icon with the text "The auto-deletion setting applies to chat and email messages in the user's inbox and archived messages. It does not apply to messages in the Trash folder, which are deleted permanently after the specified number of days.", and a blue checkmark icon with the text "Changes will take some time to propagate to users. Prior changes can be seen in Audit log". In the bottom right corner, there are two buttons: "DISCARD" and "SAVE".

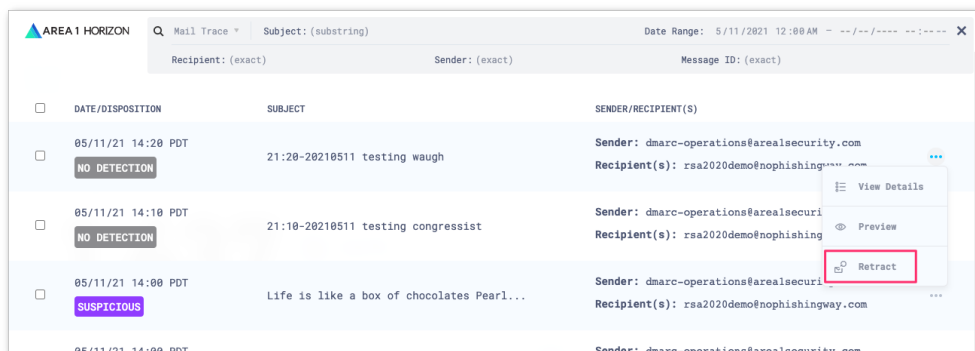
# Manual Message Retraction

When retraction is enabled, this also allows you to manually retract messages that were not automatically retracted, for example a message was inadvertently sent to a few recipients and you've been requested to remove the message from their inbox.

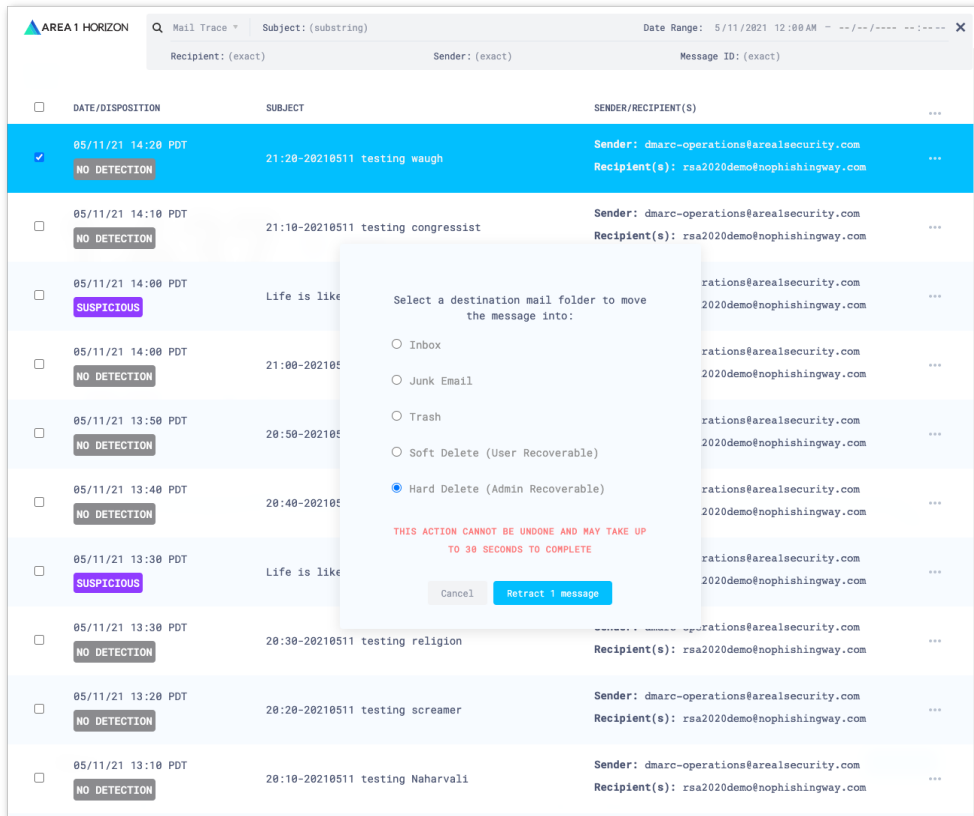
1. To manually retract a message, you will first need to find the message to retract. Access the Mail Trace search function by clicking the Search bar on top of the portal and using the dropdown to change the search type to Mail Trace:



2. This will update the search dialog and allow you to search for the messages to retract, once you have entered the correct search parameters, you will be presented with the messages that match the search criteria. To retract a single message, click the ... icon associated with the message and select the **Retract** option. If you'd like to retract multiple messages, you can select the messages in question by clicking the associated checkbox on the left side of the results:



3. Clicking the **Retract** action, will bring up a dialog giving you the option to decide where you want to retract the message:



4. Once you click the **Retract Message** button, if the message was successfully retracted, you will receive a positive confirmation on the lower right corner of the Portal:

