CLOUDFLARE
AREA 1 SECURITY

Email Security for Gmail Message Retraction

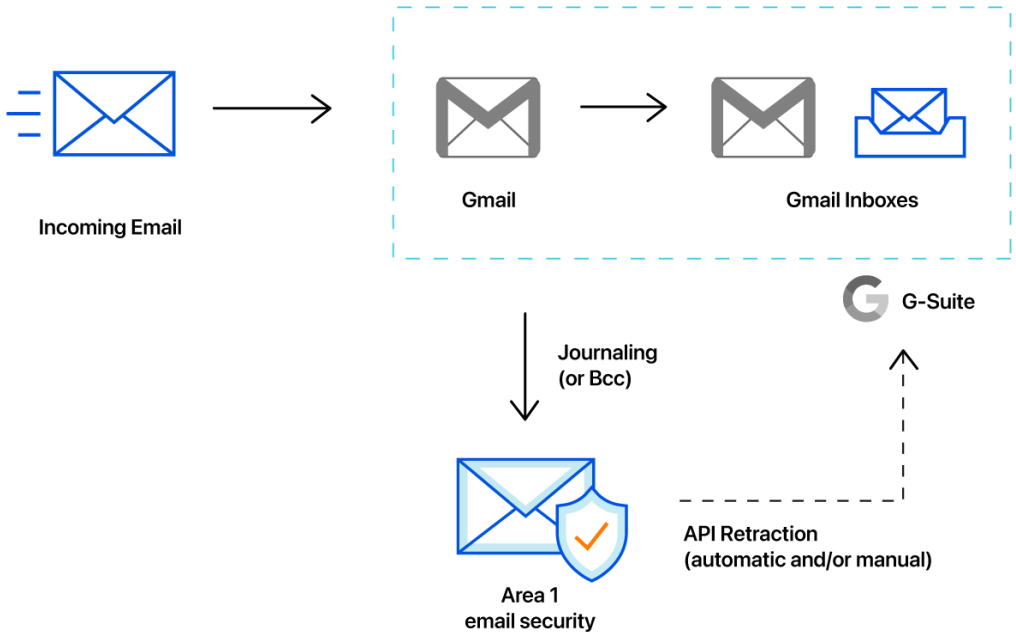
Deployment and Configuration Guide

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



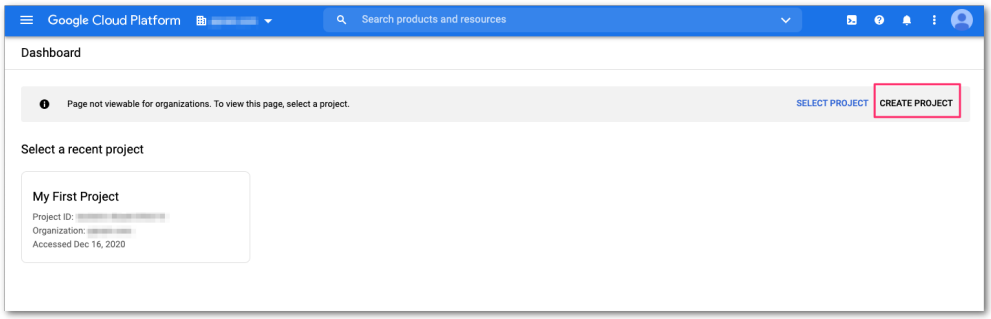
Configuration Steps

- 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

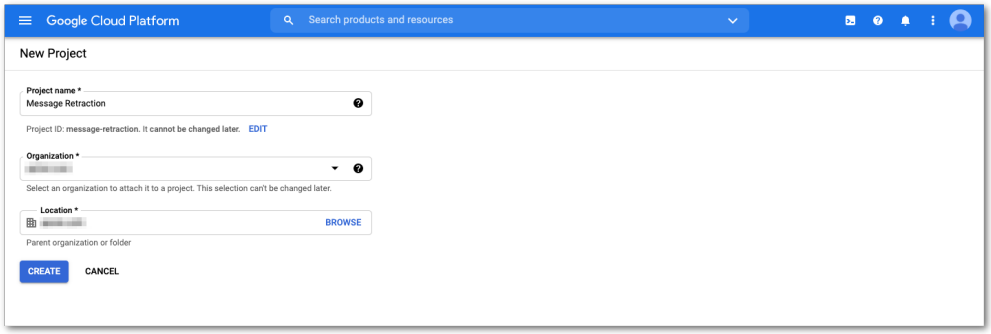
Step 1: Configure Project and Service account in GCP

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.

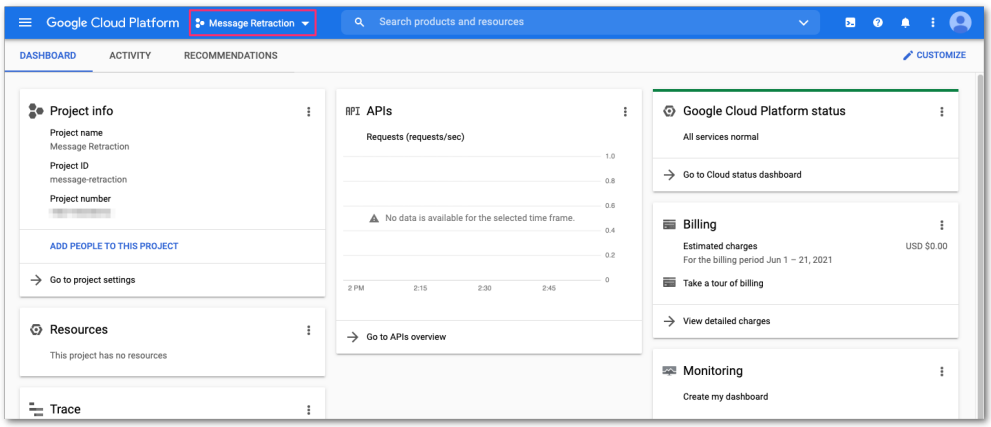
1. Access the Google Cloud Console (https://console.cloud.google.com). From the Dashboard, you can click the **CREATE PROJECT** button to start a new project.



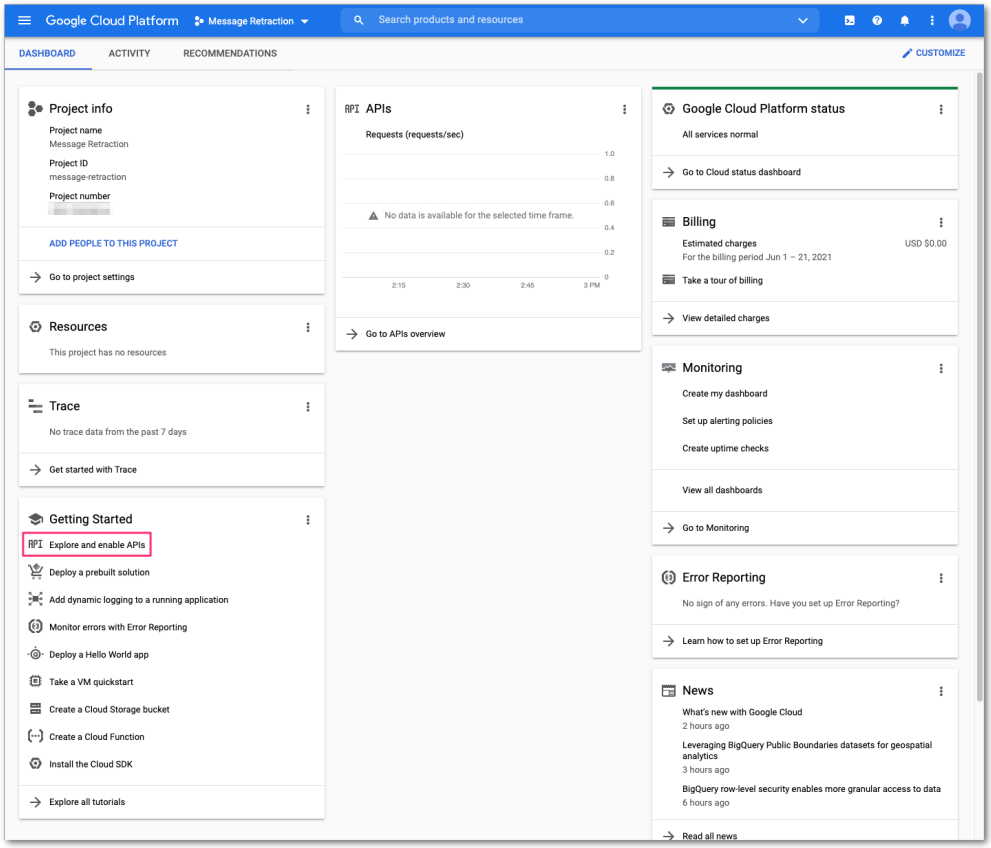
2. Provide the details for the new project and fill in with the appropriate information from your organization. Click the **CREATE** button to start your new project.



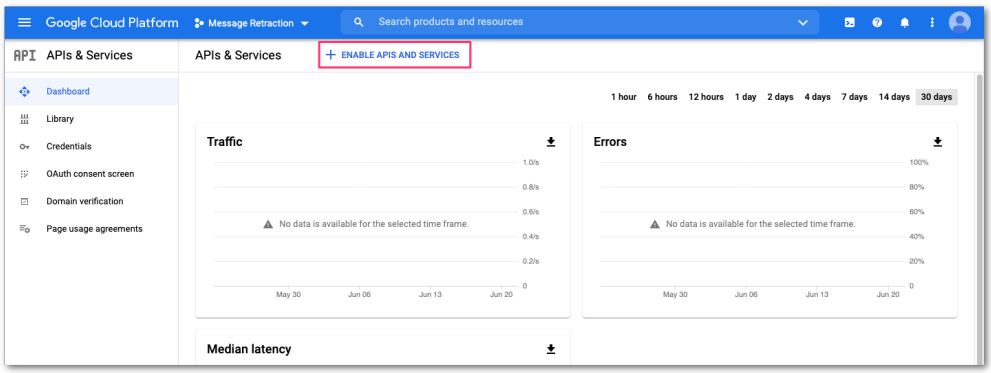
3. Once the new project has been created, the GCP console will automatically redirect you to the Project console, if not, you can use the Project selector to change to the new project you just created.



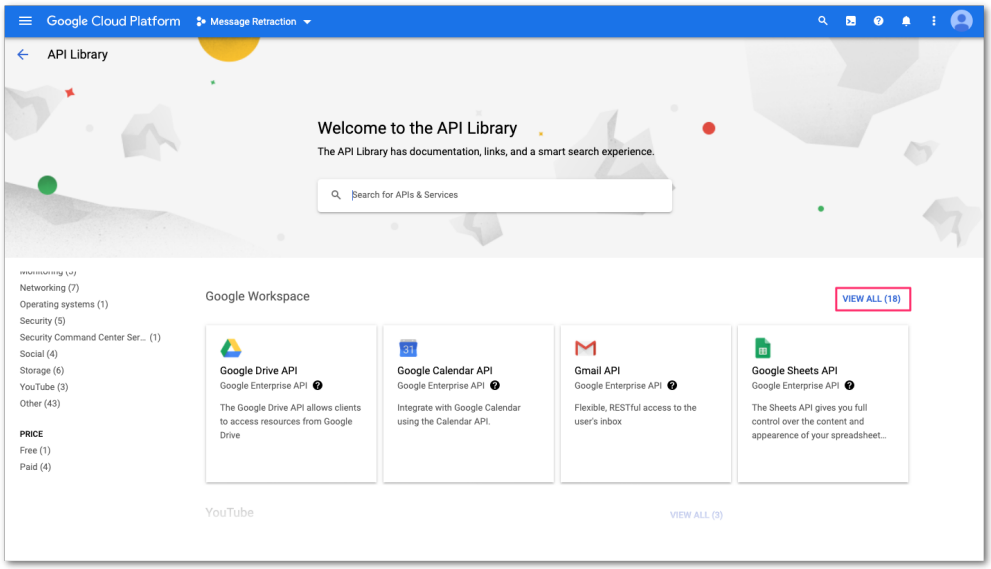
4. Access the **APIs & Services** configuration console to enable API access to this project. You can find a link to the **APIs & Services** console under the **Getting Started** card:



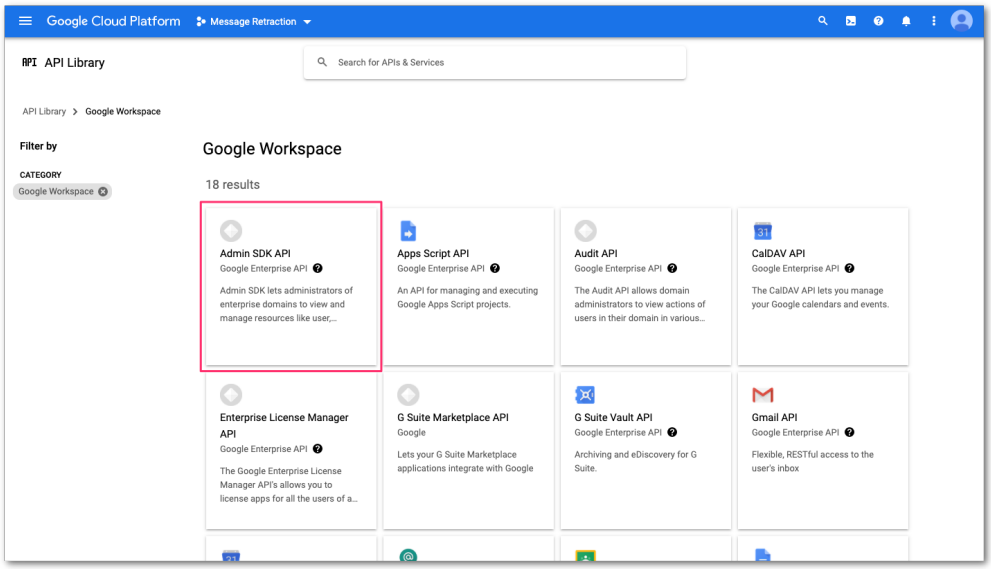
5. Click the **+ ENABLE APIS AND SERVICES** button to open the API Library.



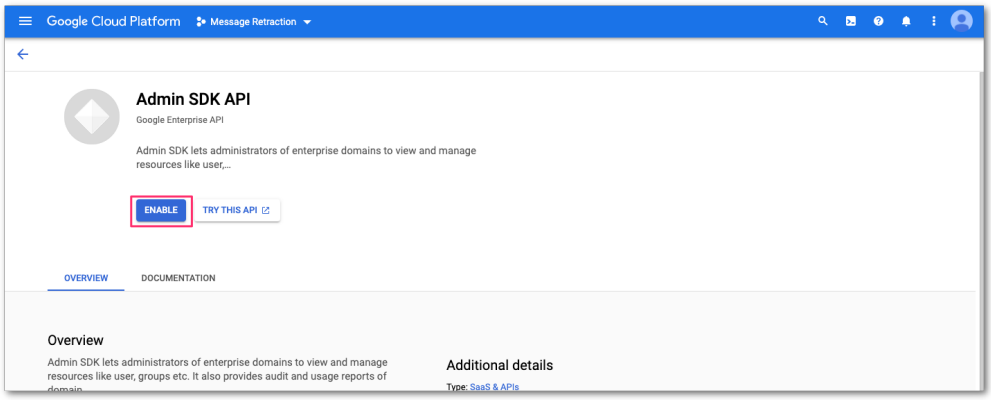
6. You will need to enable the **Admin SDK API** and the **Gmail API**. From the API Library and locate the **Google Workspace** section of the Library and click the **View All** link to access all the available APIs for Google Workspace:



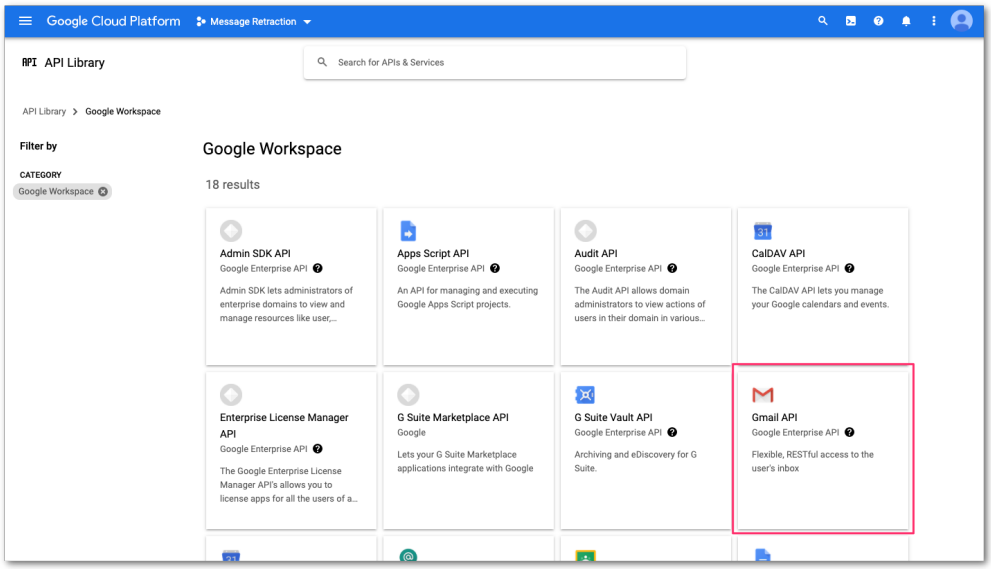
7. Select the **Admin SDK API**:



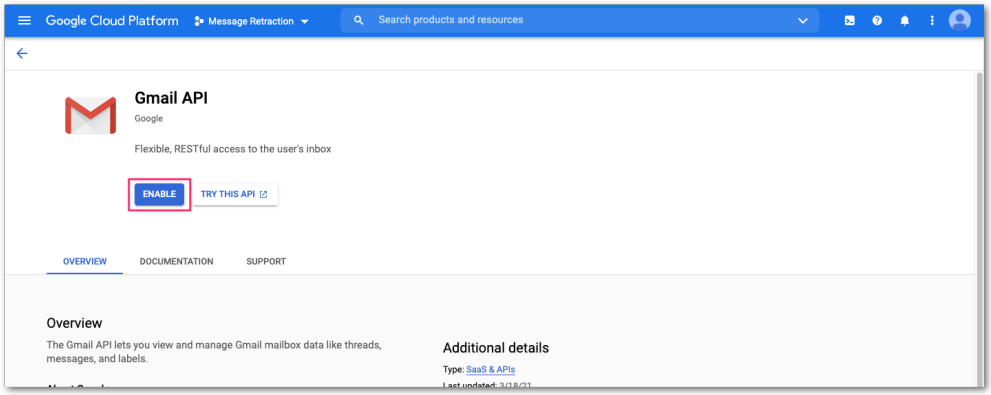
8. Click the **Enable** button to activate the **Admin SDK API**:



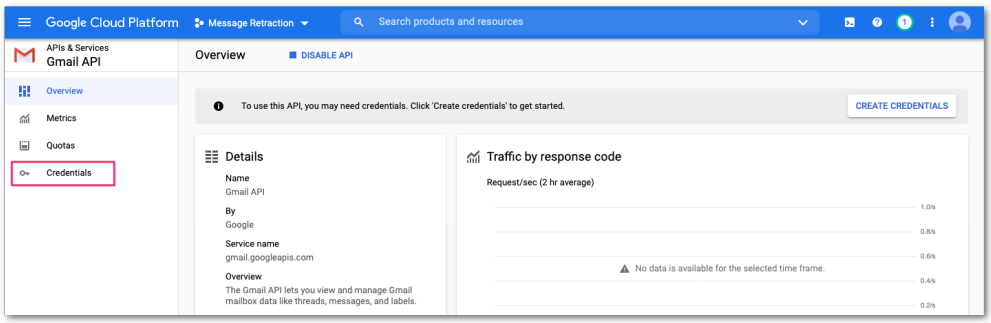
9. Return to the **Google Workspace** API library and select the **Gmail API**:



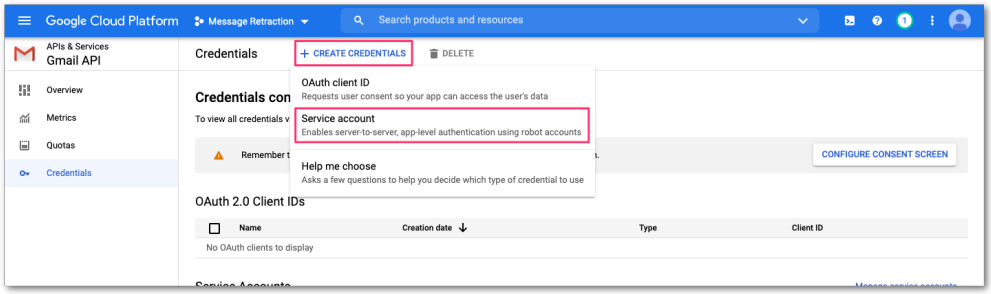
10. Click the **ENABLE** button to activate the **Gmail API**:



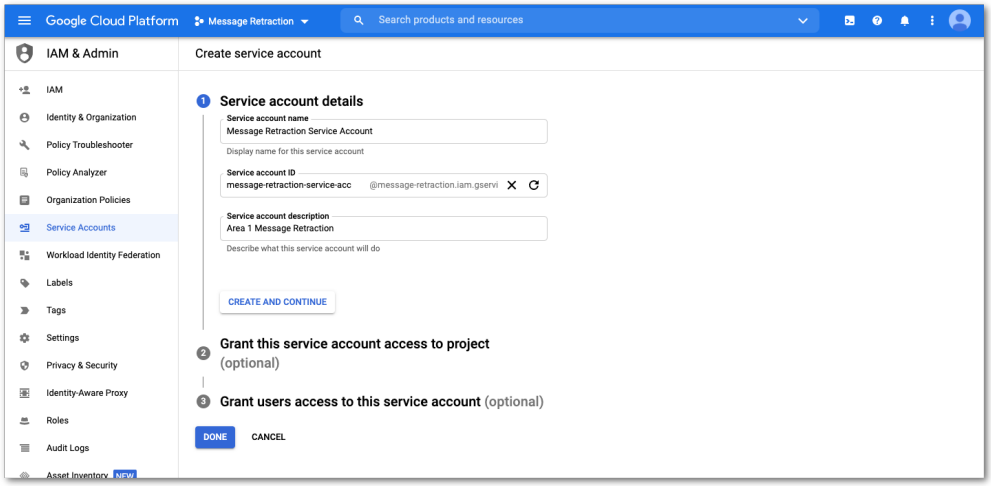
11. You will now need to create a **Service Account** to use the API. From the **Gmail API** console, click the **Credentials** option on the left navigation bar to start the process:



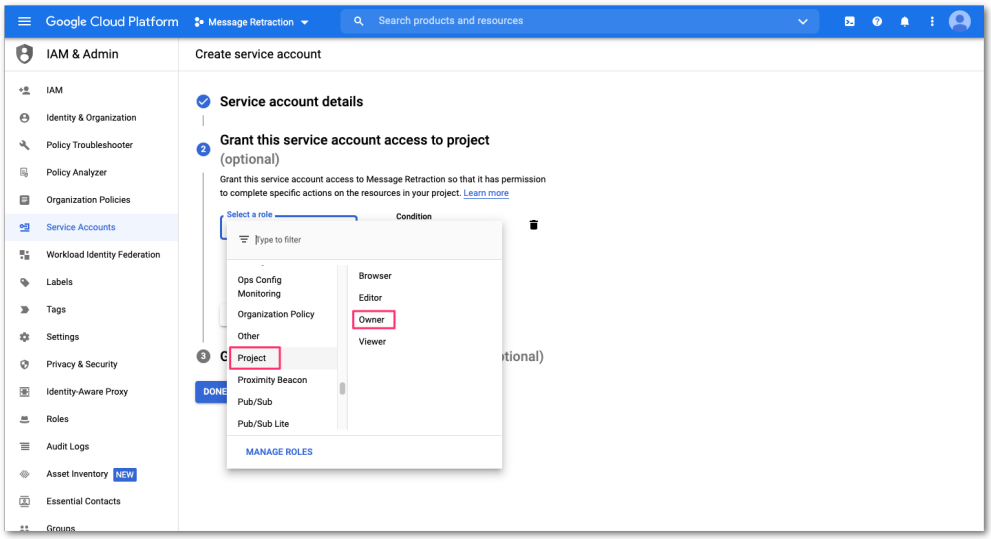
12. Click the **+ CREATE CREDENTIALS** menu option, followed by **Service account**, to start the process:



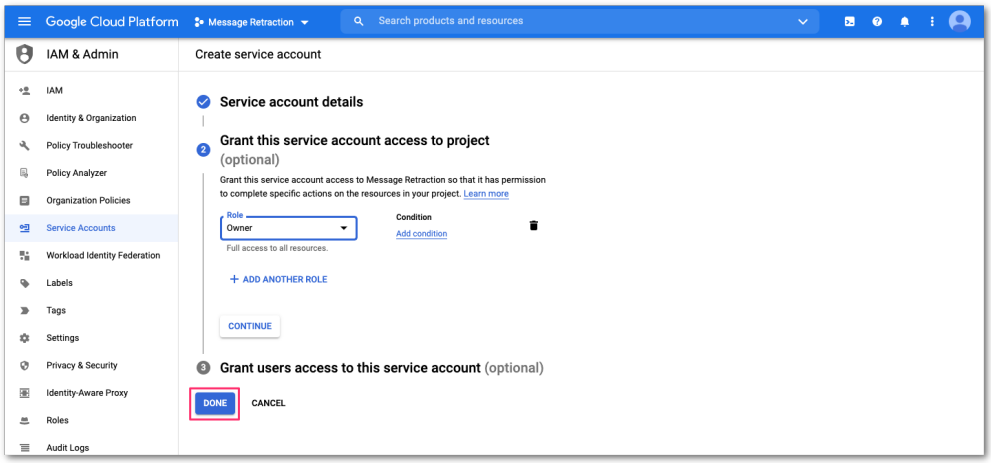
13. In the **Service account details** section, provide the details of the service account and click the **CREATE AND CONTINUE** button:
    - Service account name (e.g. Message Retraction Service Account)
    - Service account ID (value is automatically generated)
    - Service account description (e.g. Area 1 Message Retraction)



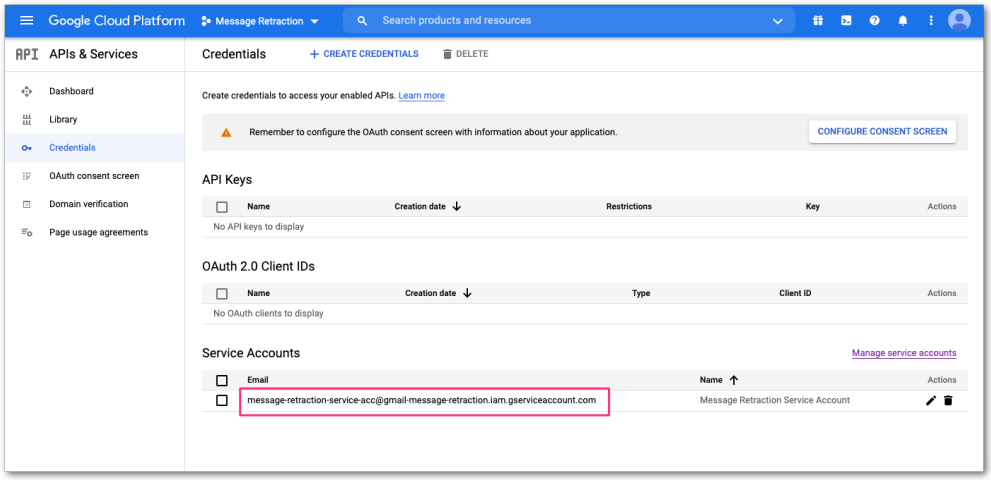
14. In the **Grant this service account access to project** section, click the **Select a role** dropdown. On the left column, find the **Project** item and select the **Owner** role on the right column:



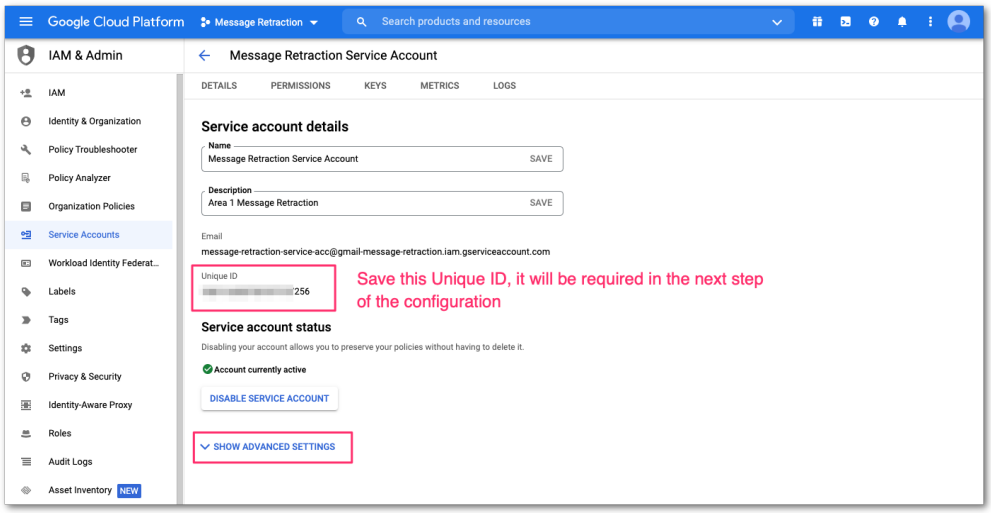
15. Once the role is assigned, click the **DONE** button to complete the setup:



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:

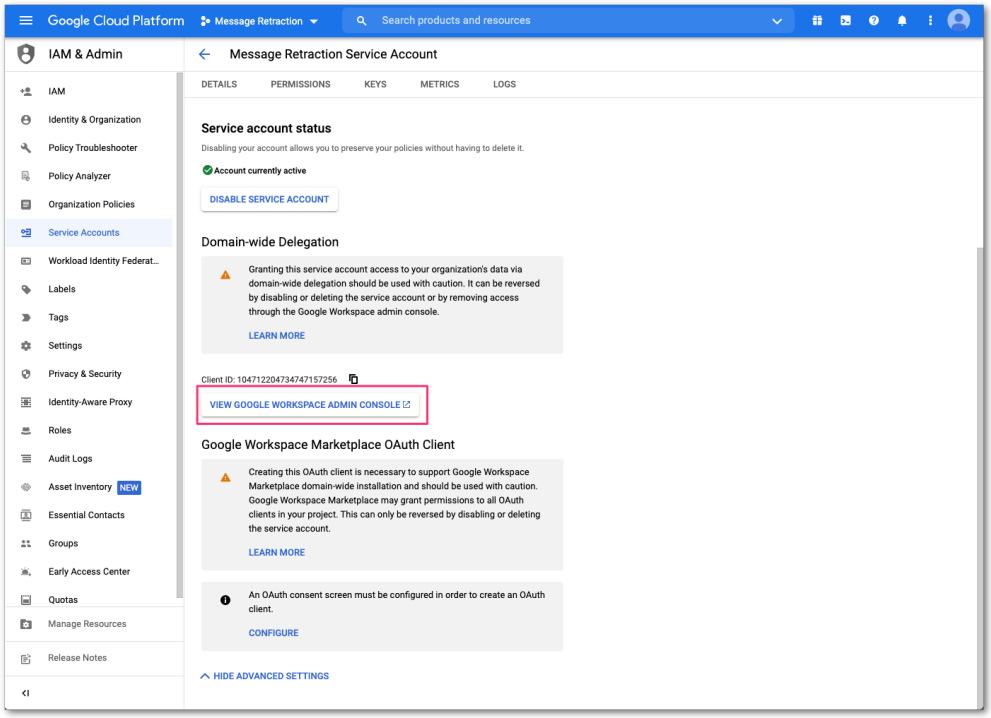


17. In the **Detail** of the service account, click the **SHOW ADVANCED SETTINGS** option to expose the advanced configuration options:

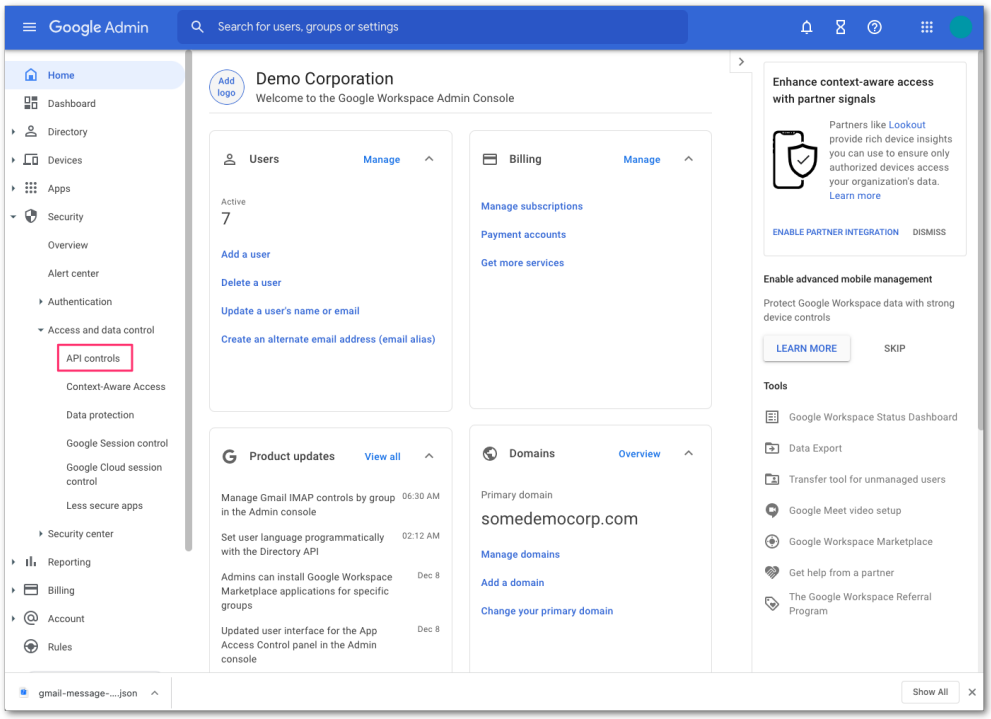


Note: Write down the **Unique ID** value as this information will be required in the configuration of the domain-wide delegation configuration in the Google Workspace configuration in the next step.

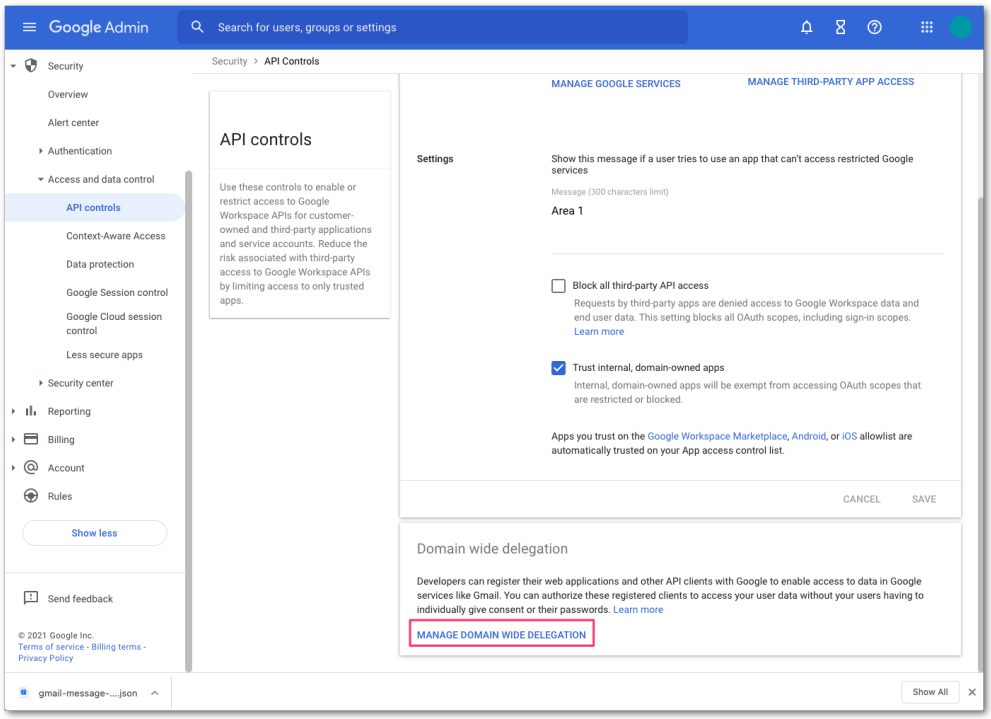
18. In the **ADVANCED SETTINGS**, click the **VIEW GOOGLE WORKSPACE ADMIN CONSOLE** button to configure the Domain-wide delegation. This will open a new window to the Google admin console:



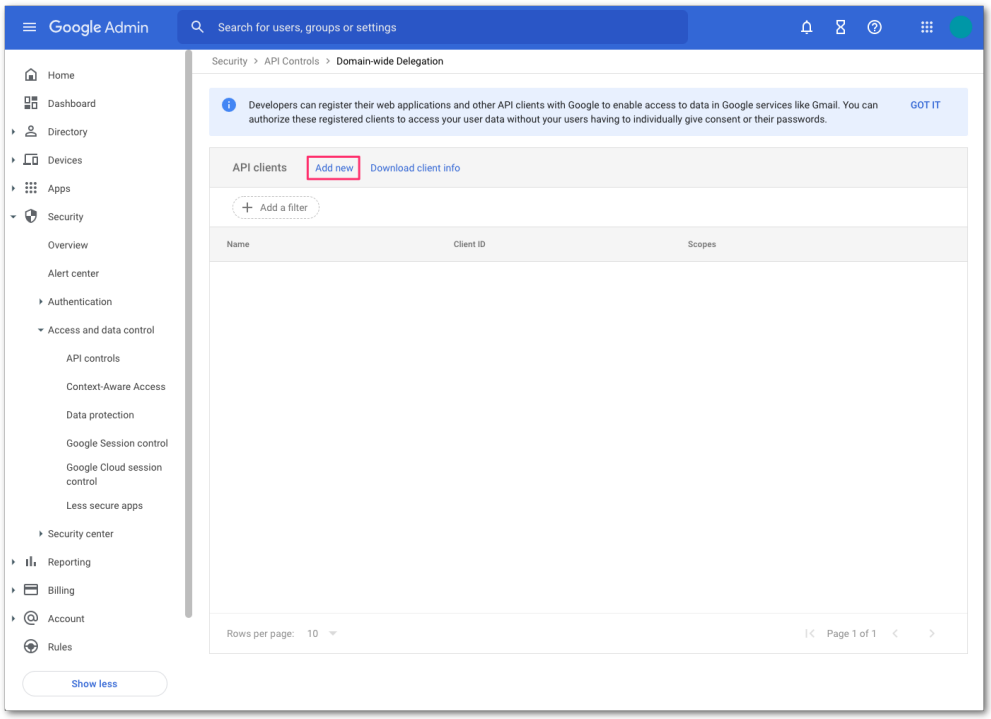
19. In the **Google Admin Console**, access the **API controls** by navigating to **Security >> Access and data control**:



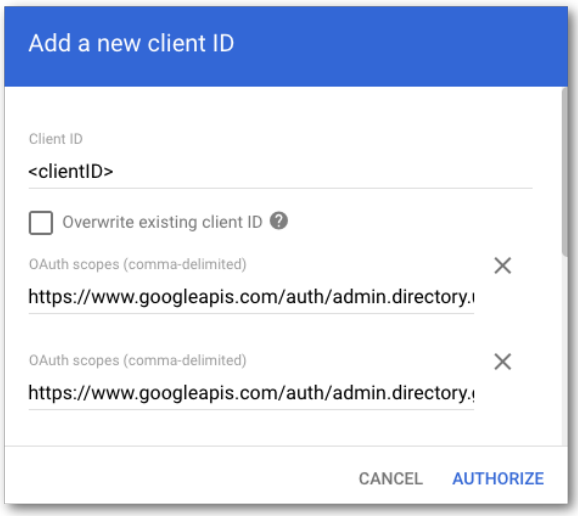
20. In the **API controls**, navigate to the **Domain wide delegation** section and click the **MANAGE DOMAIN WIDE DELEGATION** link to add the service account:



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

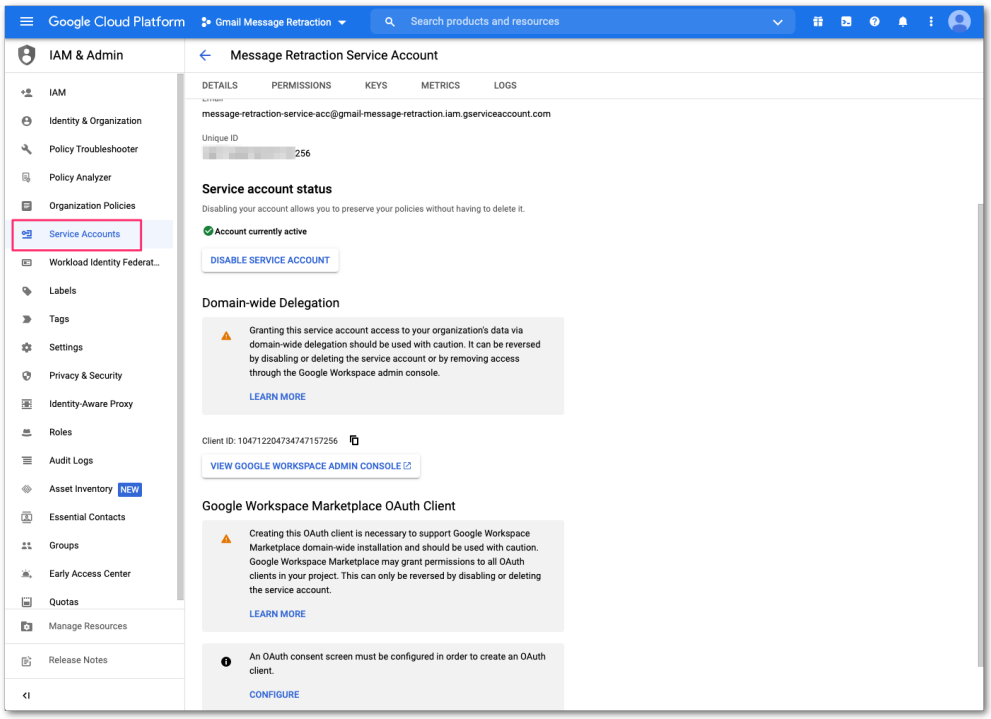


22. In the **Add a new client ID** configuration dialog box:
    - Enter your **client ID** (this is the Client ID saved from the previous step)
    - Enter the following **OAuth scopes**:
        i. https://www.googleapis.com/auth/admin.directory.user.readonly
        ii. https://www.googleapis.com/auth/admin.directory.group.readonly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

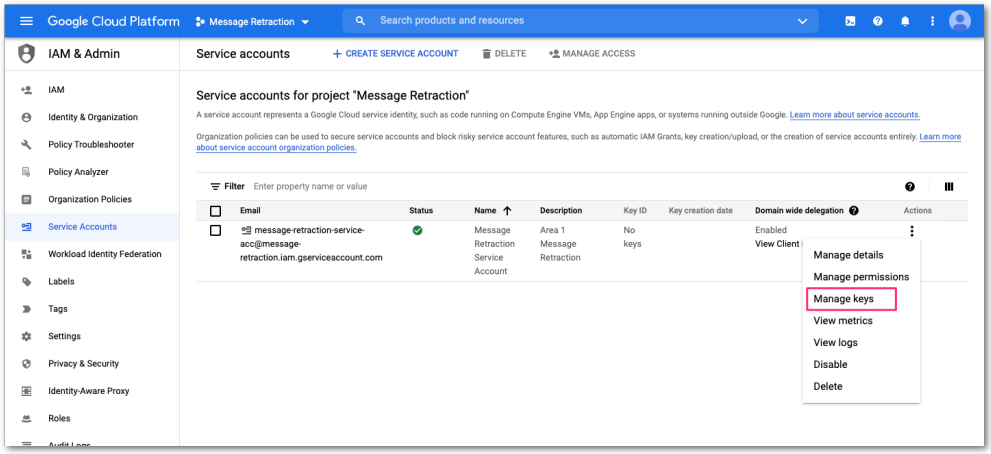


- Click **AUTHORIZE** to complete the configuration

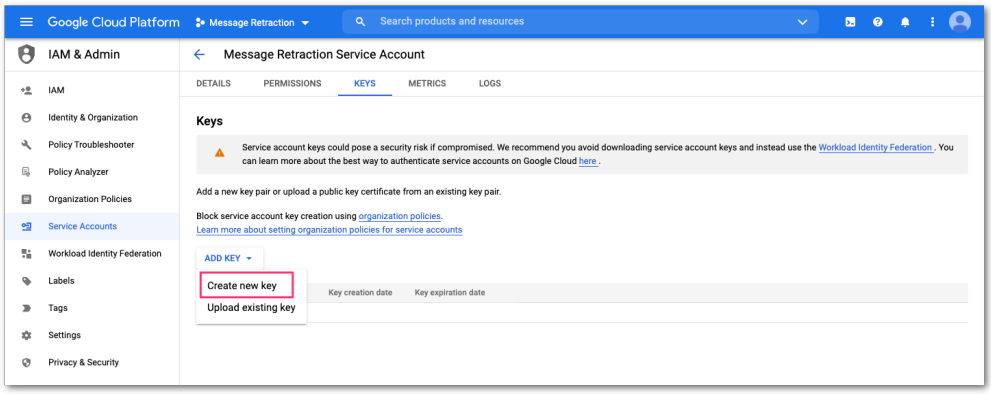
23. Return to the GCP Console and click the **Service Accounts** configuration option to return to the service account screen:



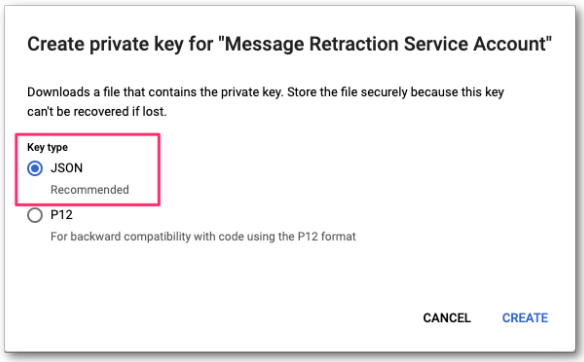
24. From the Service account configuration panel, you will need to create an API key, click the ⋮ button on the right side of the service account and select **Manage keys**:



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.

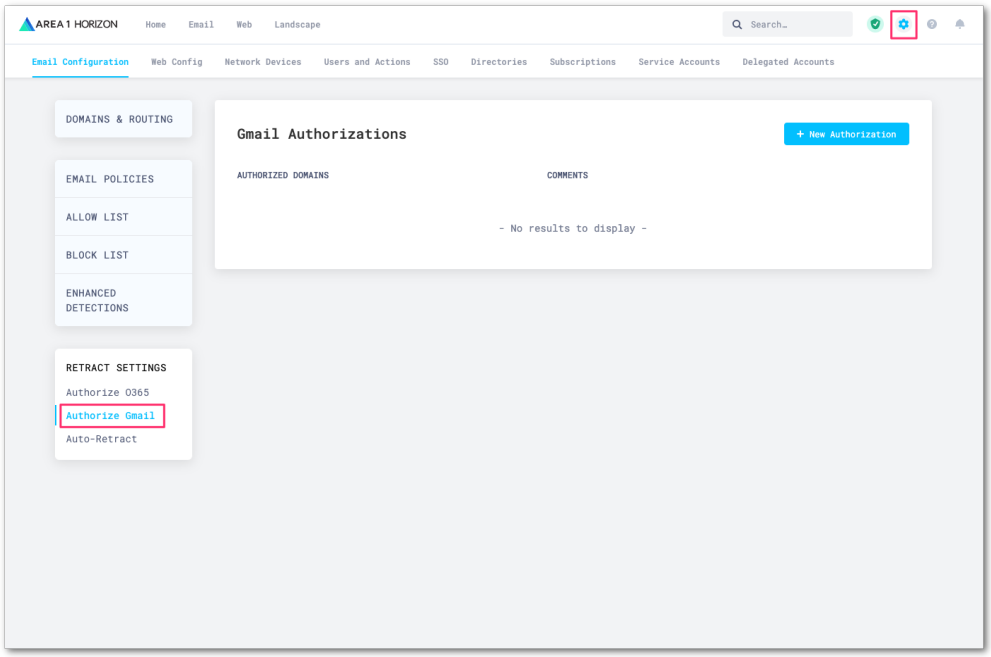


Note: Save the key in a secure location as it allows access to your cloud resources
Note: This key will need to be shared with Area 1 as part of the configuration process in the next step.

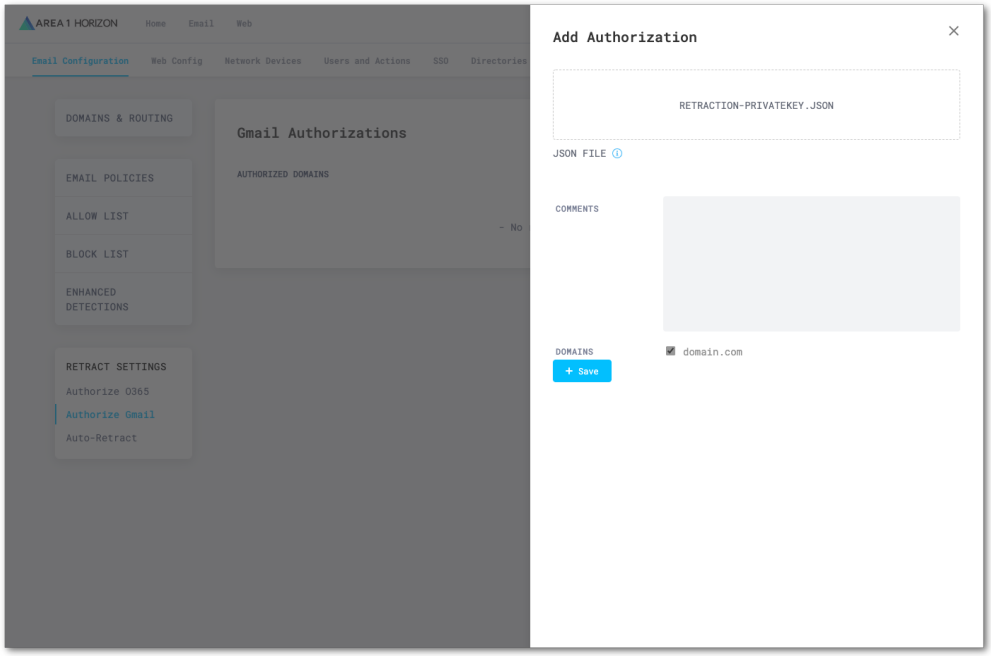
Step 2: Sharing the Service Account JSON Key with Area 1

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

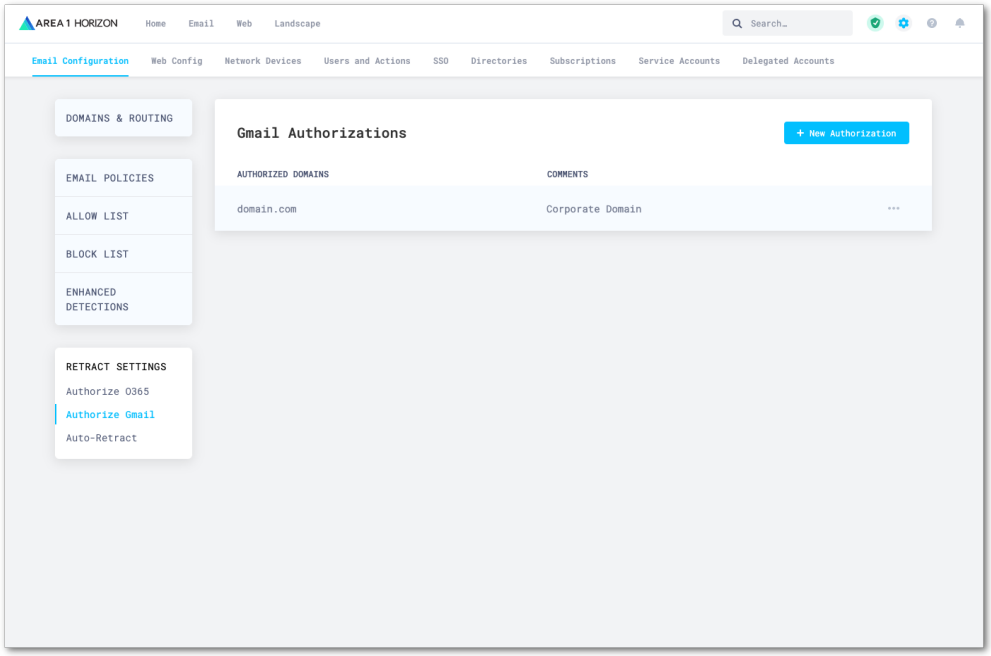
1. From the **Email Configuration** page, navigate to the **RETRACTION SETTINGS** portion of the configuration, select the **Authorize Gmail** option.



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



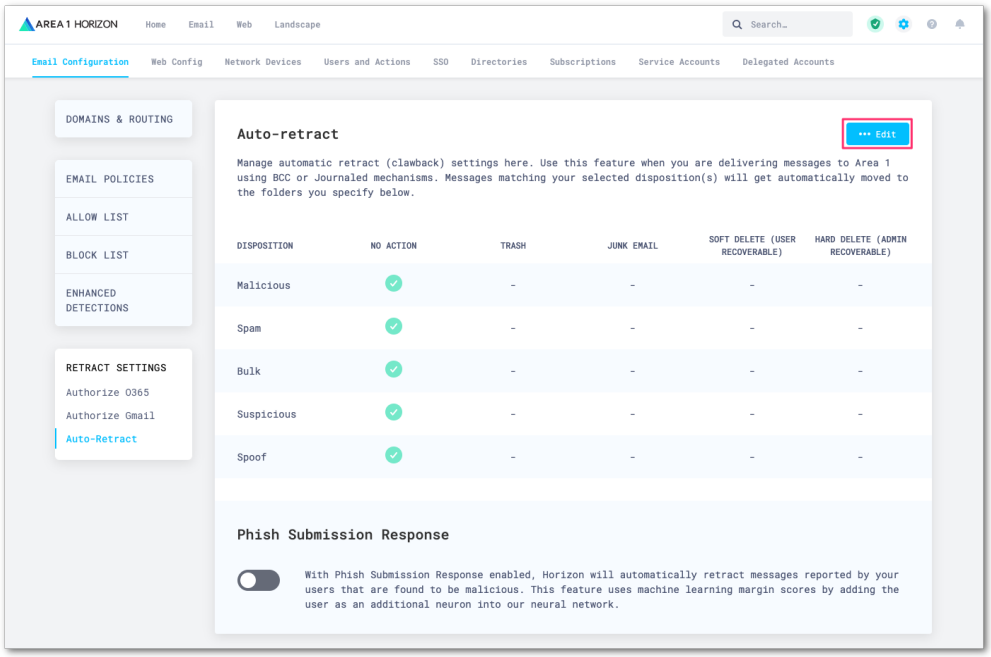
Click into the **AUTHORIZATION DATA (JWT)** box and select the JSON private key file.
Under the **Domains** section, specify which domain this private key belongs to.
Click **+Save** button to save the configuration



Step 3: Configure Auto-Retraction Actions in Area 1 Horizon

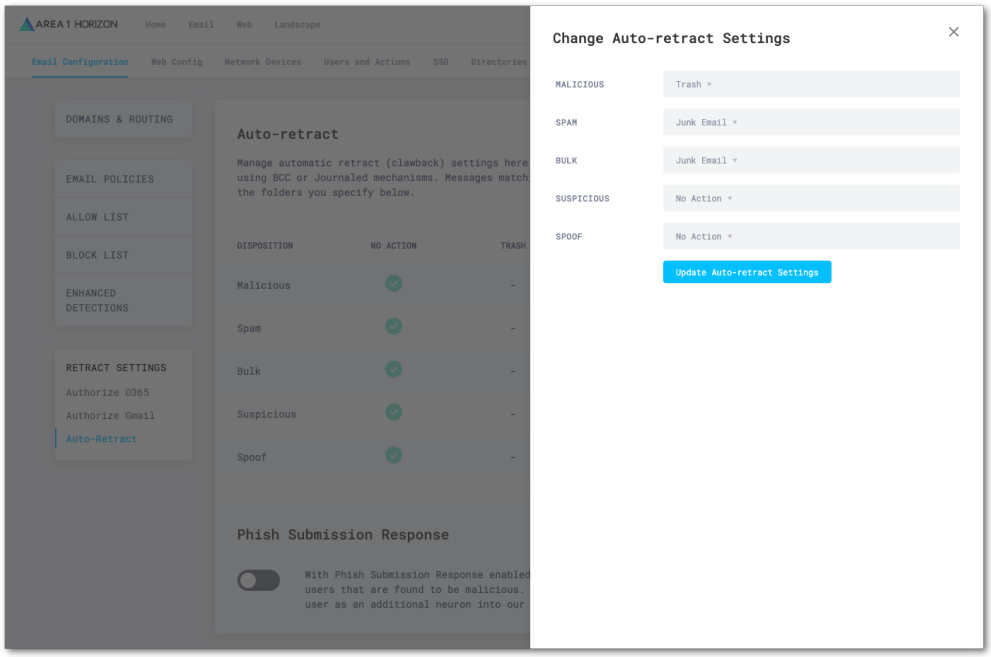
In the Area 1 Portal, you will need to configure the auto-retraction behavior for each disposition. Note that automatic retraction is not available when Area 1 is deployed as MX. From the **Email Configuration** page, navigate to the **RETRACTION SETTINGS** portion of the configuration:

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:

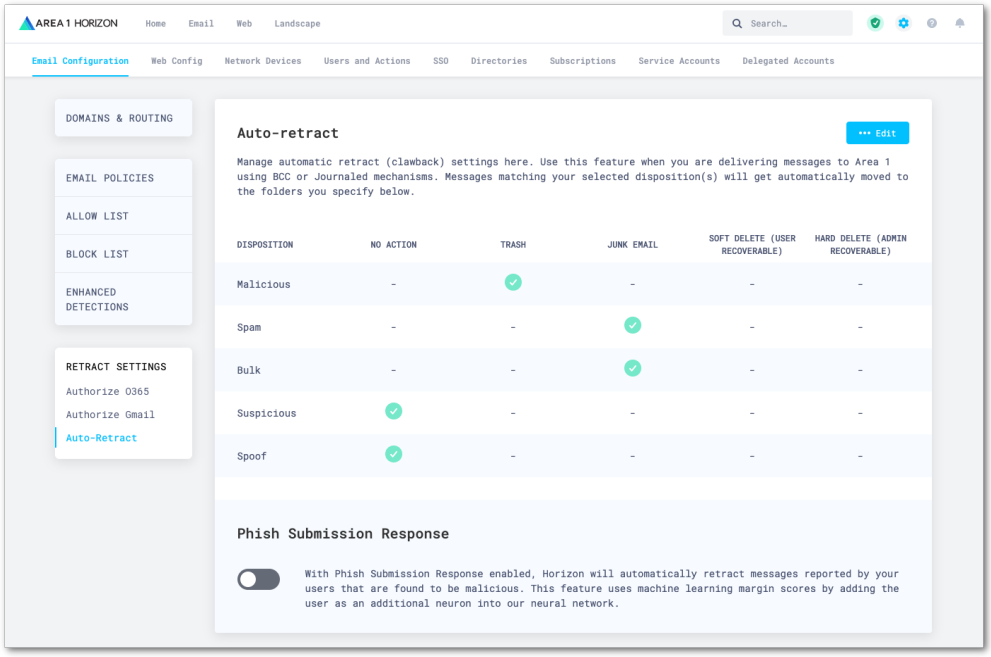


Note: You must be an Area 1 Horizon Enterprise customer in order to access the **RETRACTION SETTINGS** configuration panel. If the setting is not available, please contact customer support at **support@area1security.com**.

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

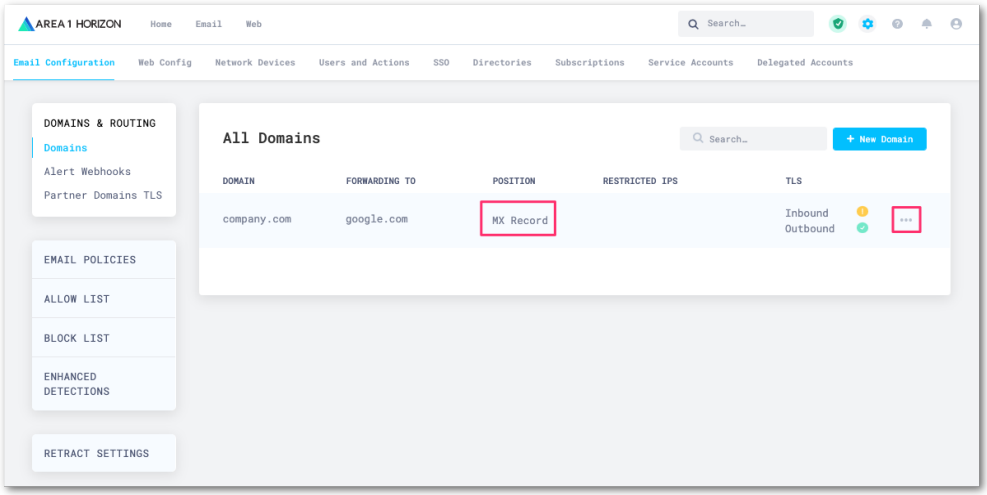


3. Once saved, the configuration table will update with the selected behaviors:

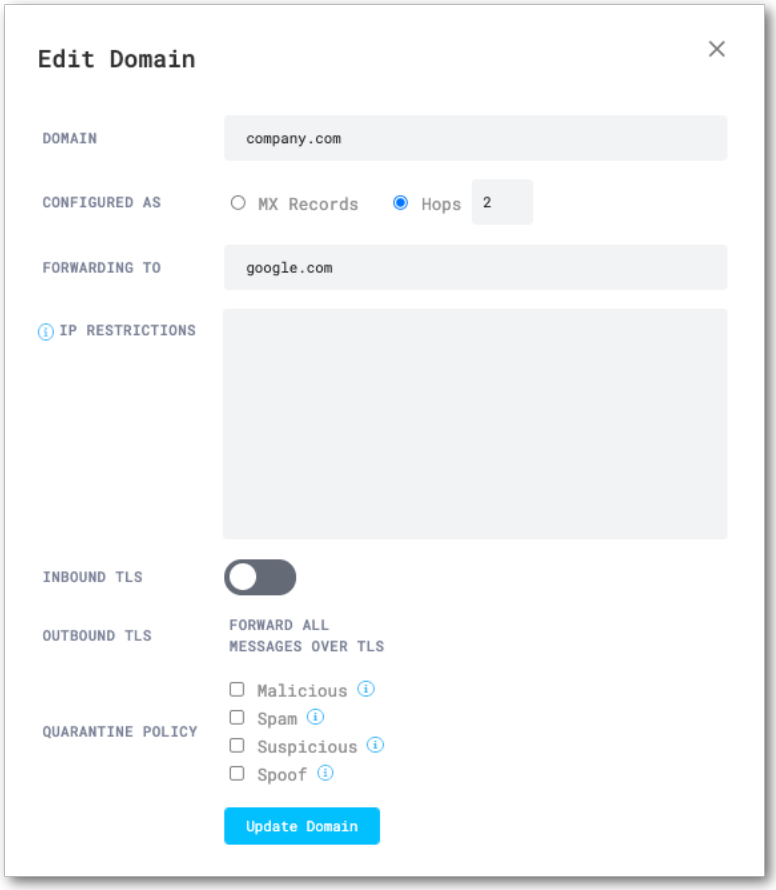


Step 4: Adjust the Hop Count in Area 1 Horizon

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.



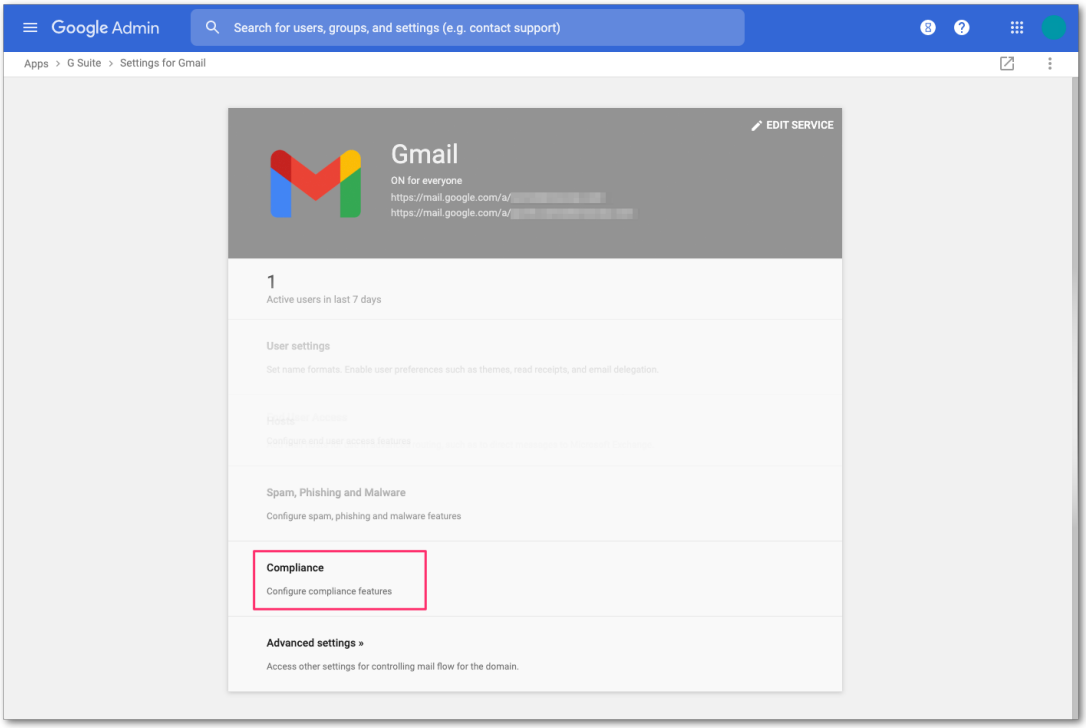
Note: If you have an existing SEG deployed as the MX record, you will need to adjust the hop count accordingly. Please contact Support if you need any assistance identifying the correct hop count.

Step 5: Configure Bcc or Journaling in Google Workspaces

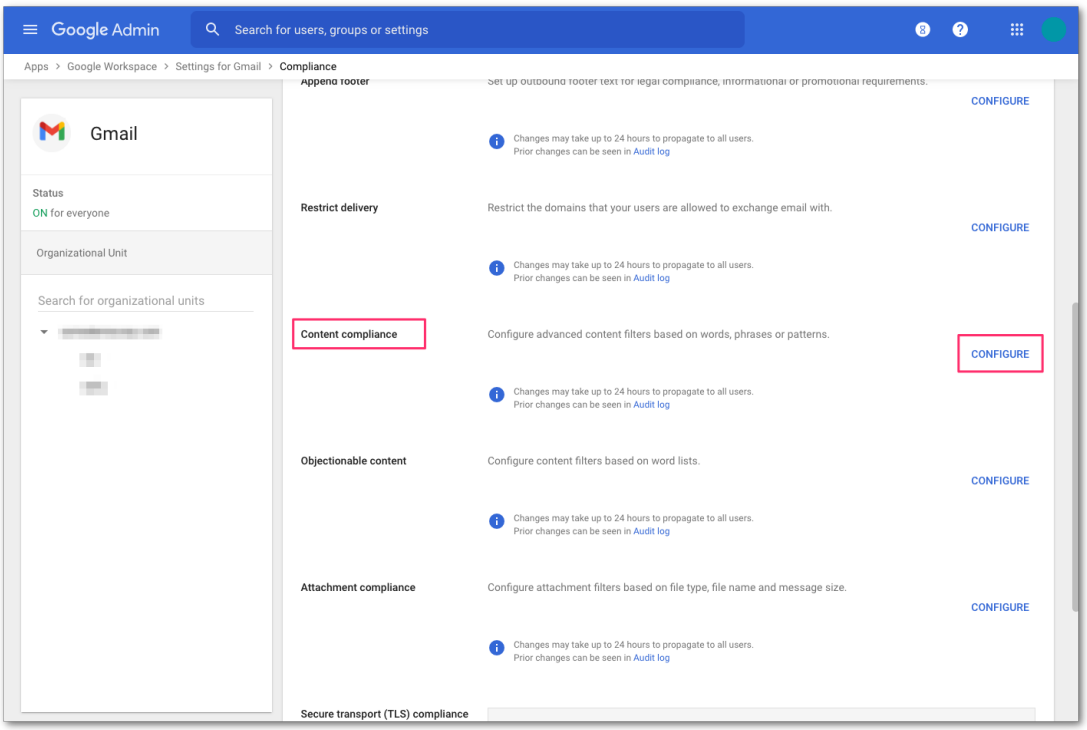
In order for Area 1 Horizon to be able to automatically retract messages, copies of the inbound messages must be sent to Area 1 for inspection. Note that automatic retraction is not available when Area 1 is deployed as MX. Messages can be sent to Area 1 using a **Bcc compliance rule** or **message journaling**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

Configure Bcc Compliance Rule

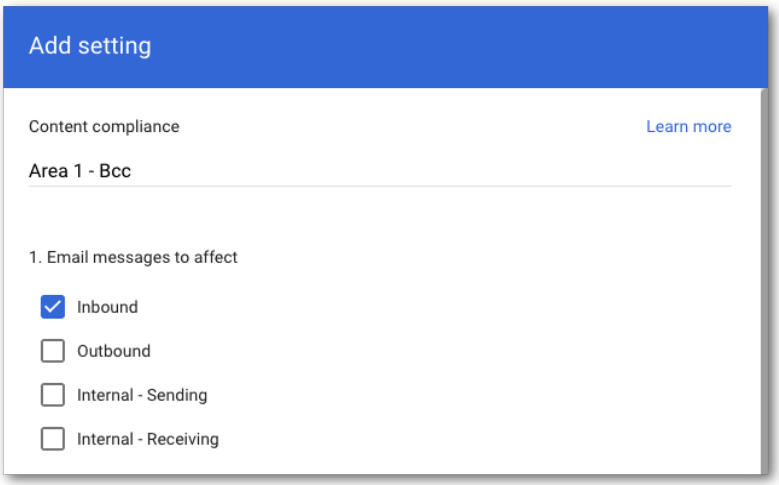
1. To configure the Bcc compliance rule, start from the **Gmail Administrative Console** and access the **Compliance** configuration option:



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

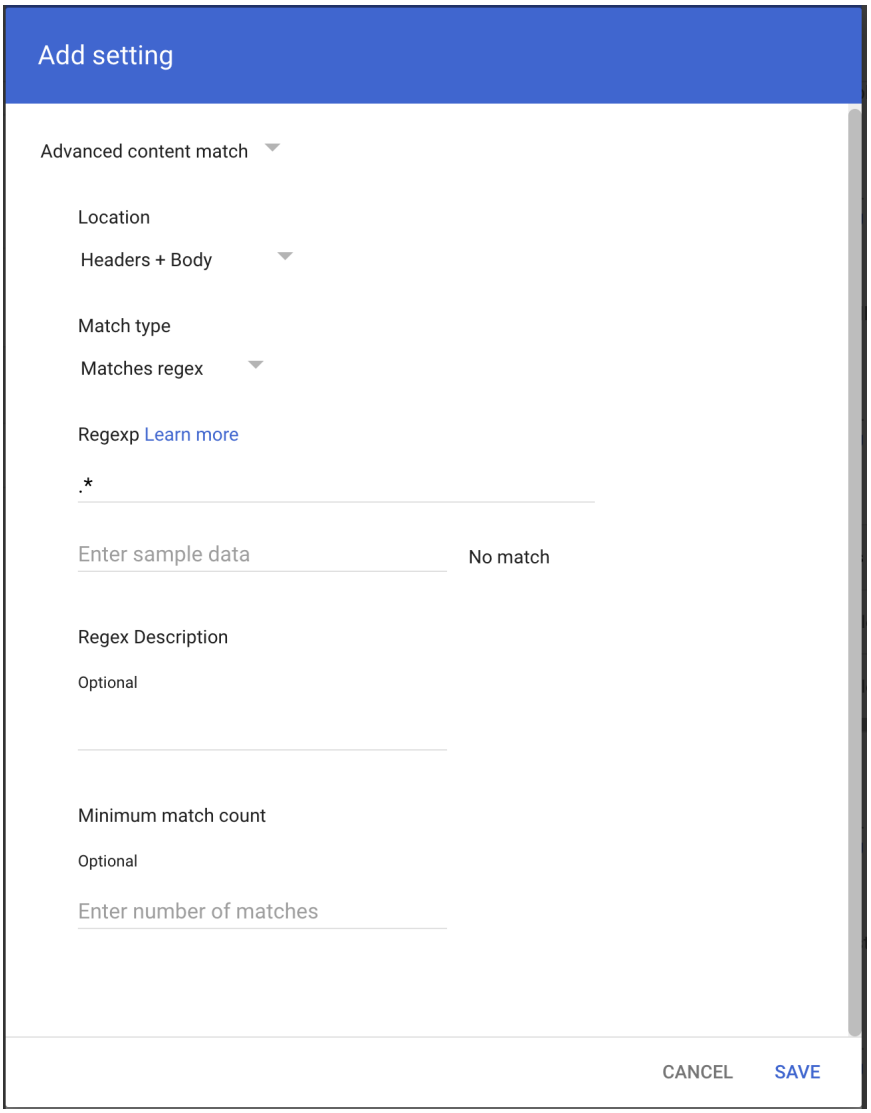


3. In the Configuration dialog that appears, configure the Bcc compliance rule as follows:
4. Add and name the “Content Compliance” filter: **Area 1 - Bcc**
5. Select “Inbound” for messages to affect



6. Add the recipients that will have their messages Bcc’d to Area 1

a. Click “Add” to configure the expression
b. Select “Advanced content match”
    i. For **Location**, select “Headers + Body”
    ii. For **Match type** select “Matches regex”
    iii. For **Regexp** enter “.*” (without quotes)
        1. You can customize the regex as needed and test within the admin page or on sites like https://regexr.com/.

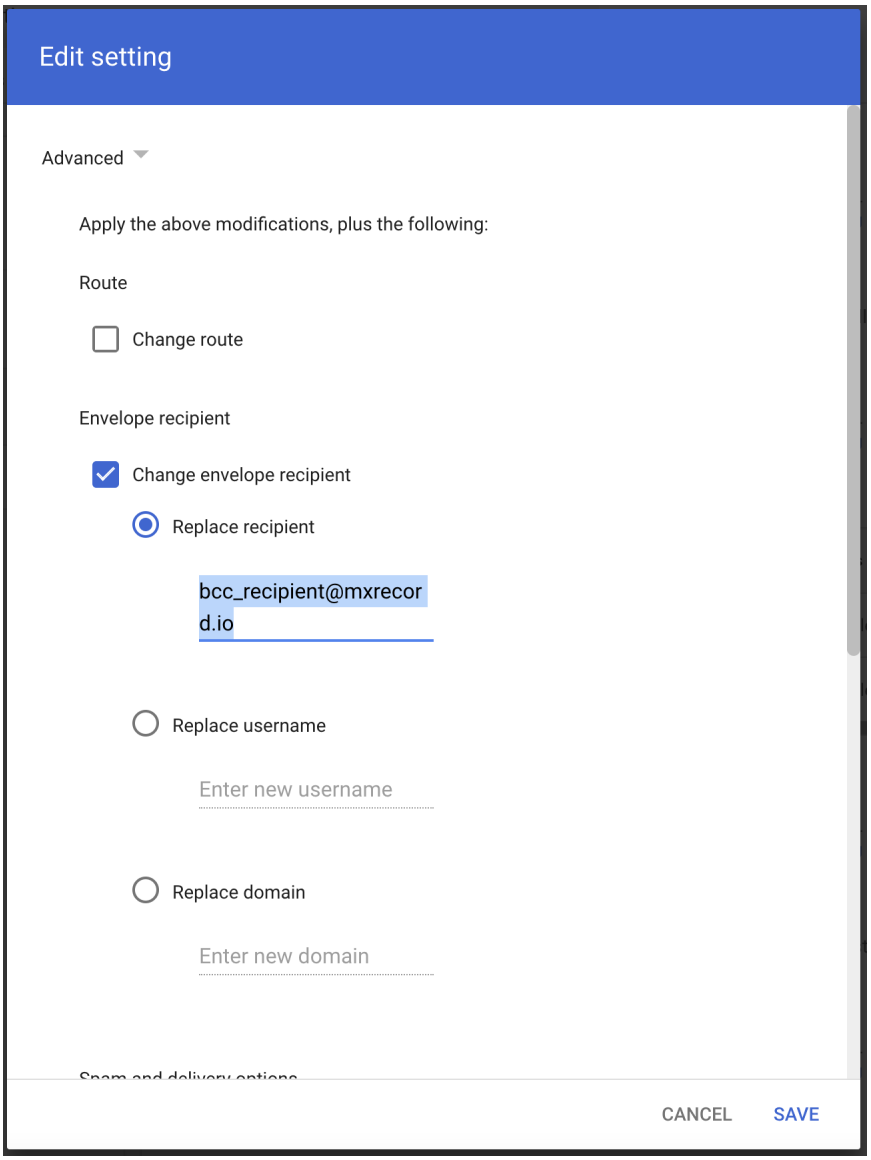


    iv. Click SAVE to save your settings

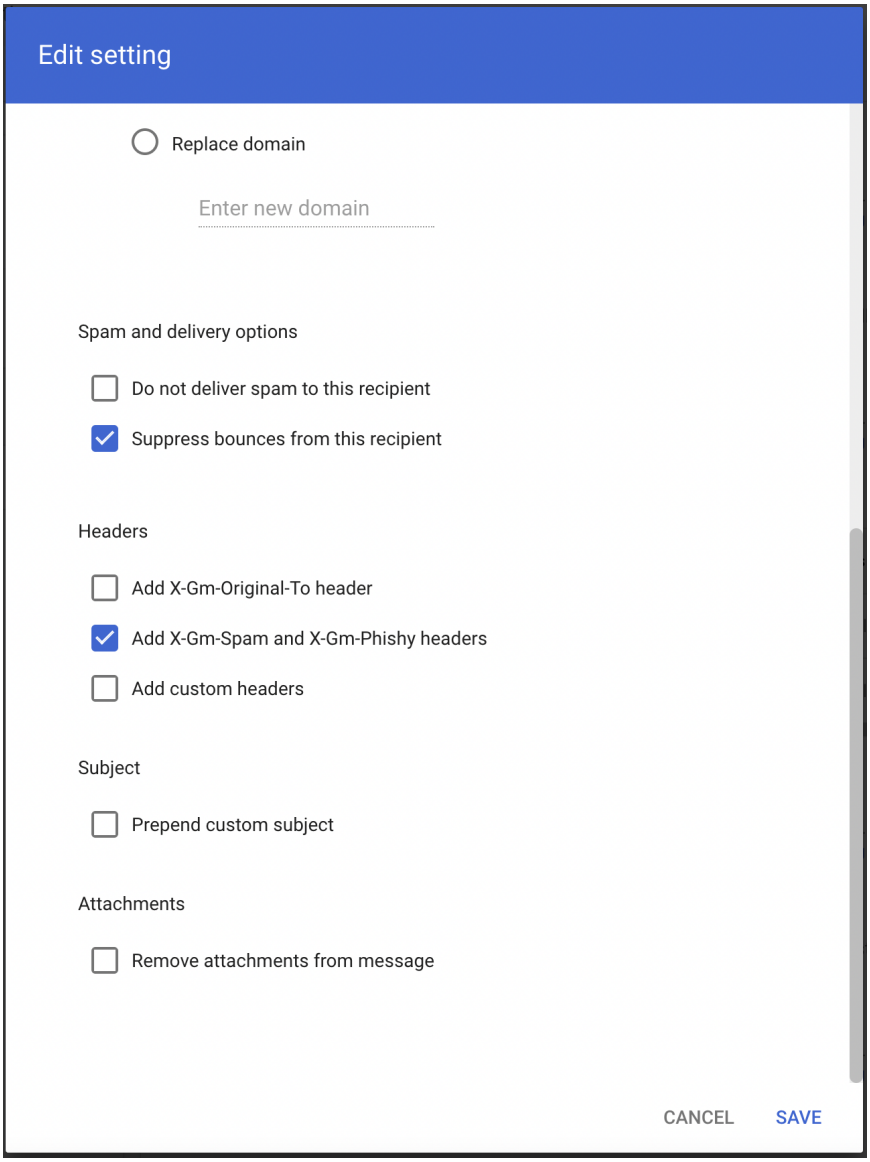
7. In section “3. If the above expressions match, do the following” make the following changes.
    a. Under **Also deliver to** check “Add more recipients”

i. Under **Recipients** click “Add”
ii. Change the setting to **Advanced**
iii. Under **Envelope recipient** check “Change envelope recipient”
iv. Under **Replace recipient** add the recipient bcc address. E.g. bcc_recipient@mxrecord.io
    1. This address is specific to each customer tenant and can be found in your Portal at https://horizon.area1security.com/support/service-addresses

       If you are located in the EU or GDPR applies to your organization, replace the “@mxrecord.io” domain in the bcc recipient with “@mailstream-eu1.mxrecord.io”, this will force email to be processed in Germany under compliance with GDPR. E.g. bcc_recipient@mailstream-eu1.mxrecord.io

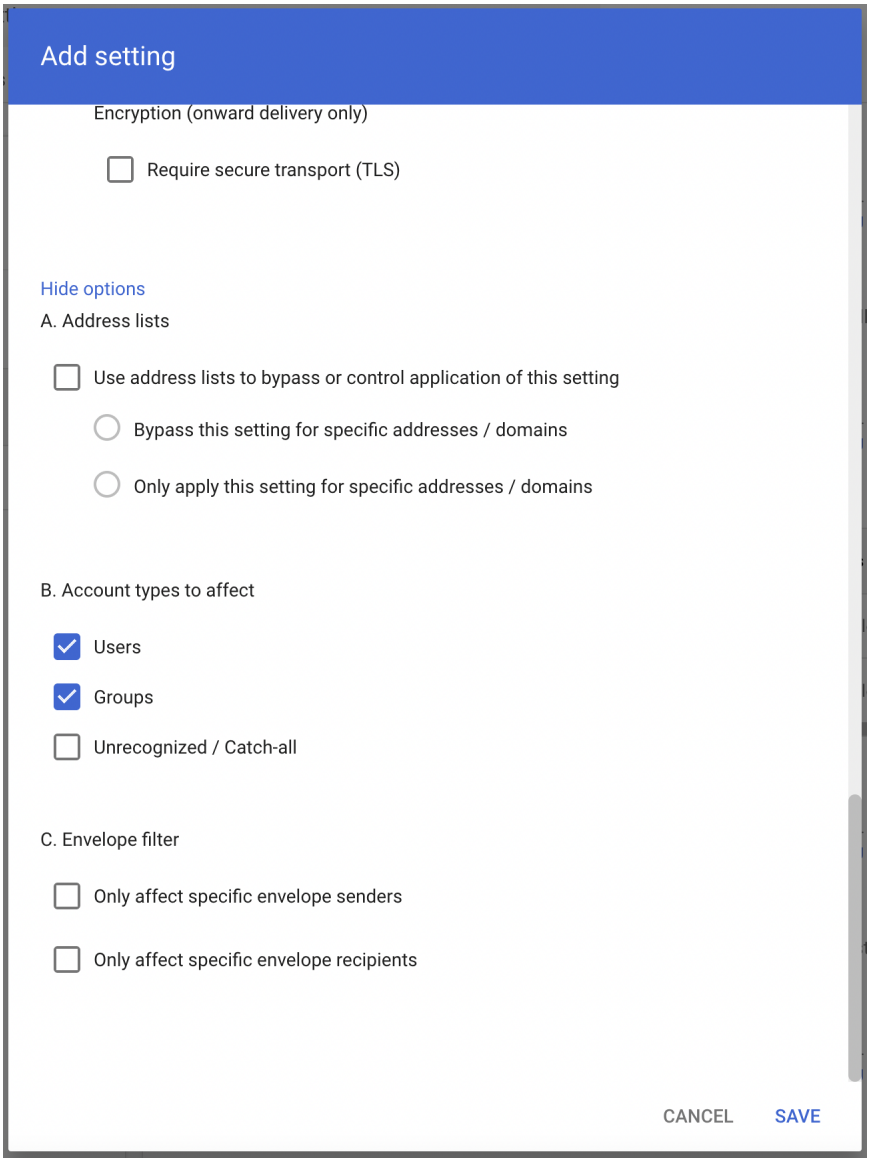


v. Under **Spam and delivery options** uncheck “Do not deliver spam to this recipient”
vi. Under **Headers** check “Add X-Gm-Spam and X-Gm-Phishy headers”



vii. Click SAVE to save your settings

8. Scroll to the bottom and select “Show options”
    a. Under **Account types to affect** check “Groups”

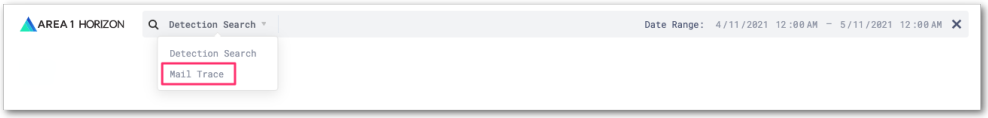


b. Click SAVE to save your settings

Manual Message Retraction

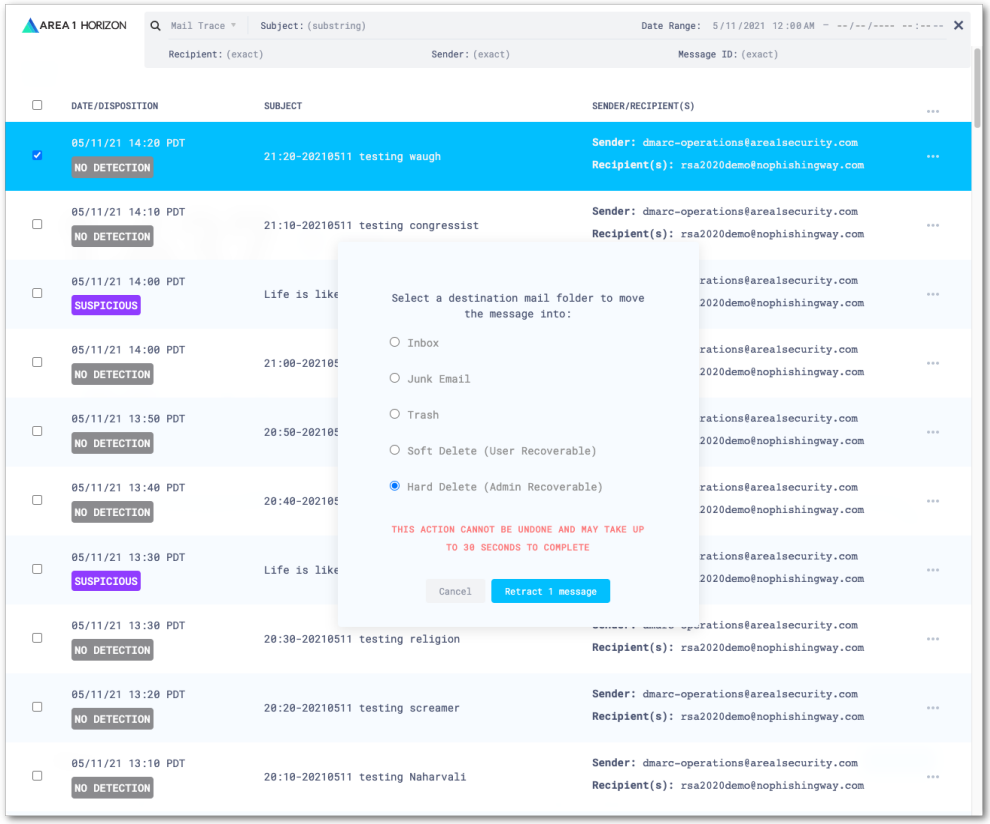
When retraction is enabled, this also allows you to manually retract messages that were not automatically retracted, for example a message was inadvertently sent to a few recipients and you've been requested to remove the message from their inbox.

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: