
Email Security for Gmail Message Retraction

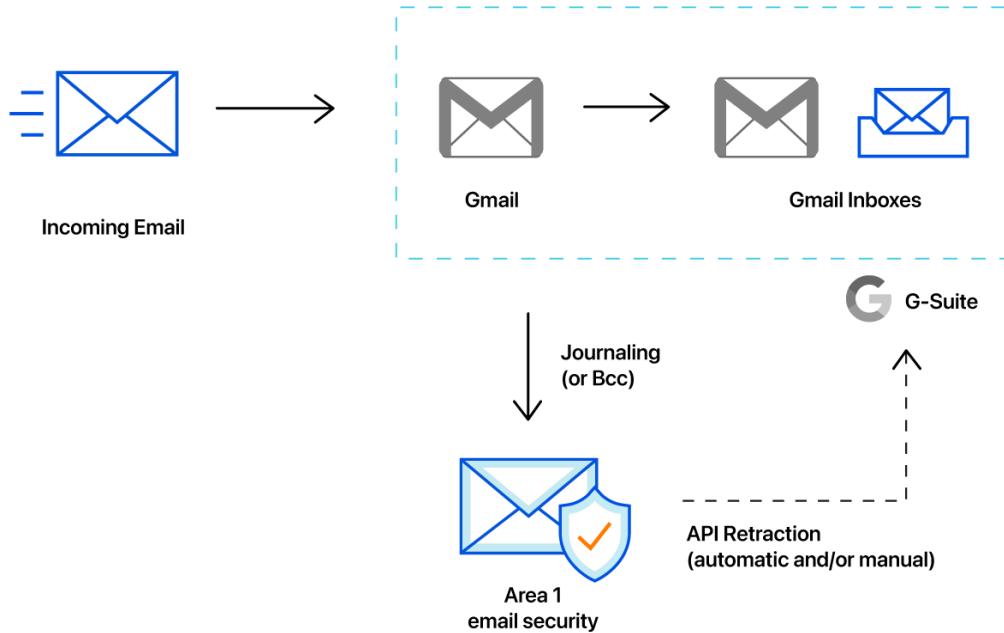
Deployment and Configuration Guide

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



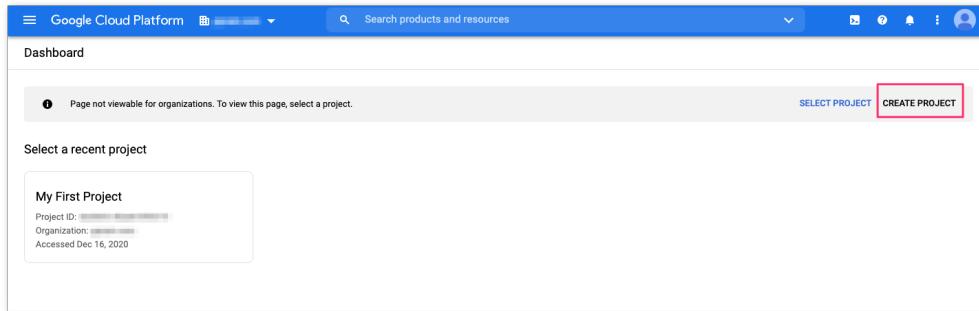
Configuration Steps

- 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

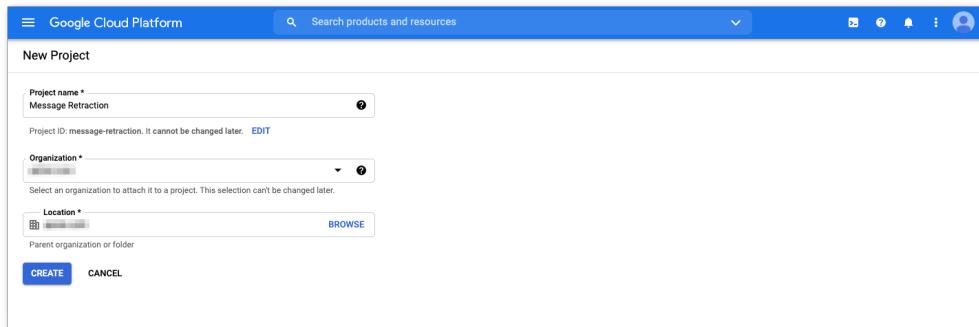
Step 1: Configure Project and Service account in GCP

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.

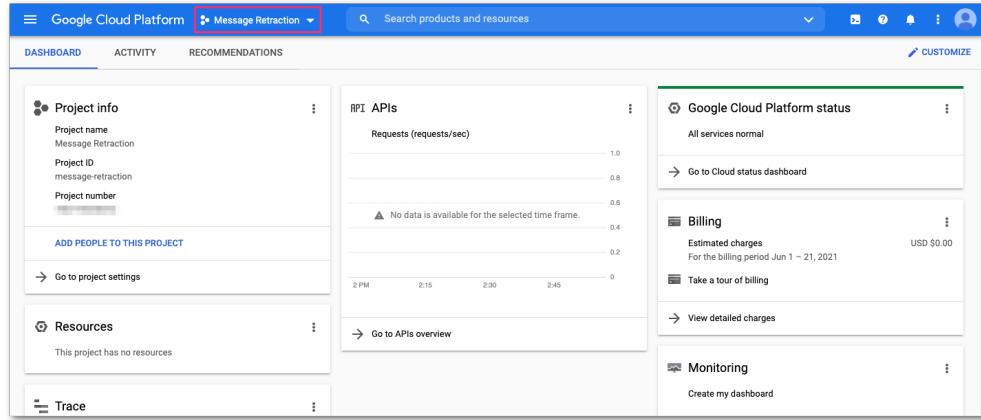
1. Access the Google Cloud Console (<https://console.cloud.google.com>). From the Dashboard, you can click the **CREATE PROJECT** button to start a new project.



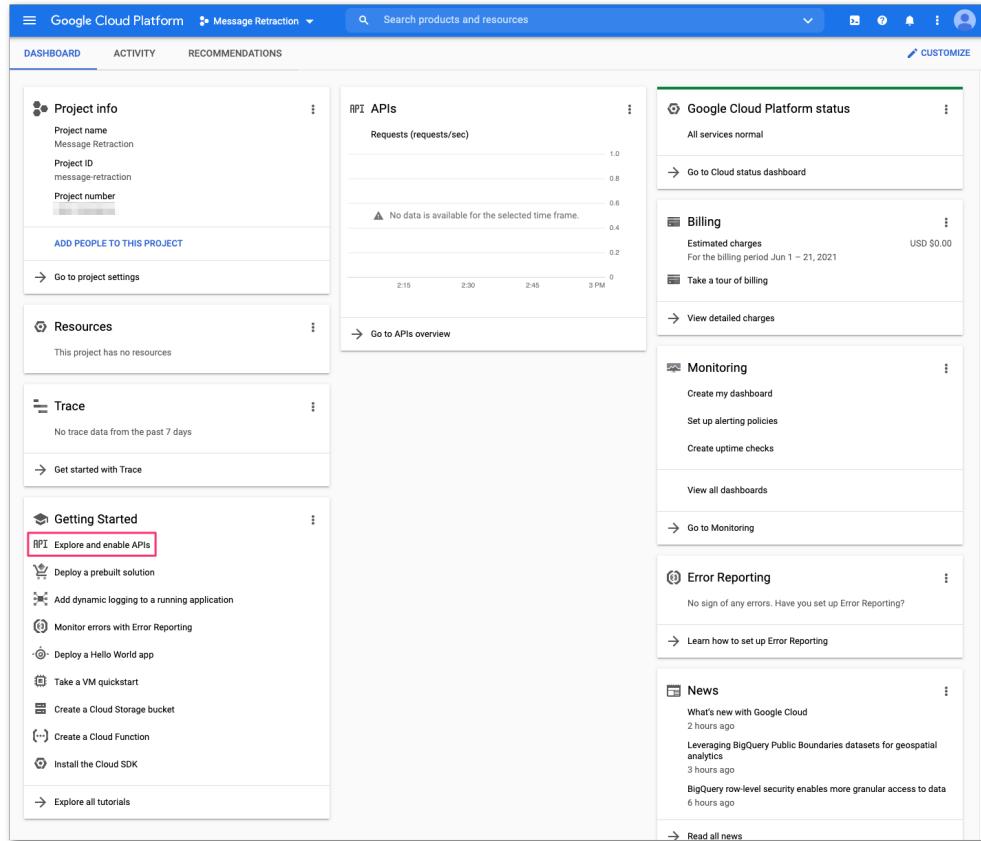
2. Provide the details for the new project and fill in with the appropriate information from your organization. Click the **CREATE** button to start your new project.



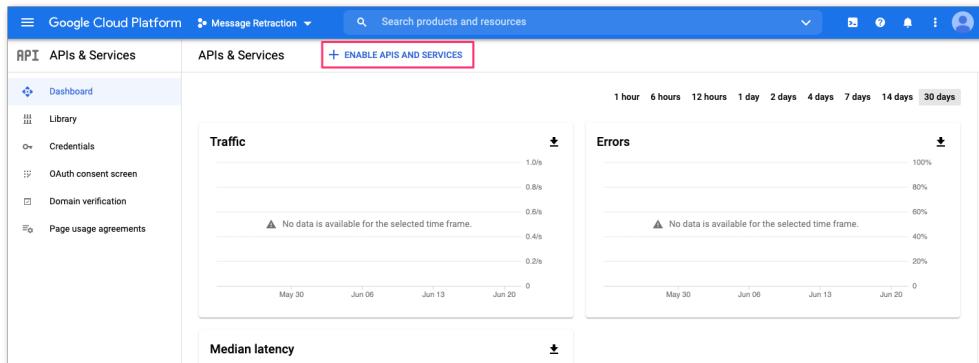
- Once the new project has been created, the GCP console will automatically redirect you to the Project console, if not, you can use the Project selector to change to the new project you just created.



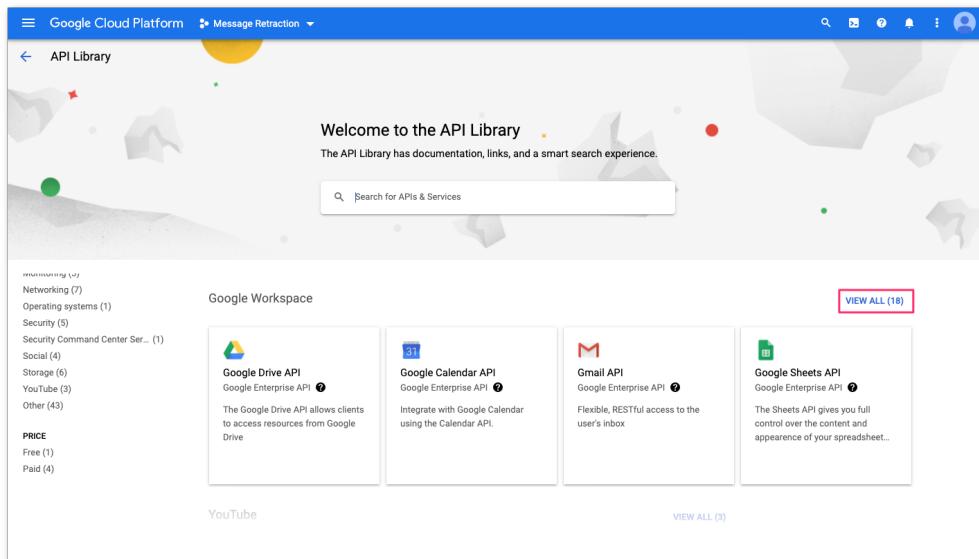
- Access the **APIs & Services** configuration console to enable API access to this project. You can find a link to the **APIs & Services** console under the **Getting Started** card:



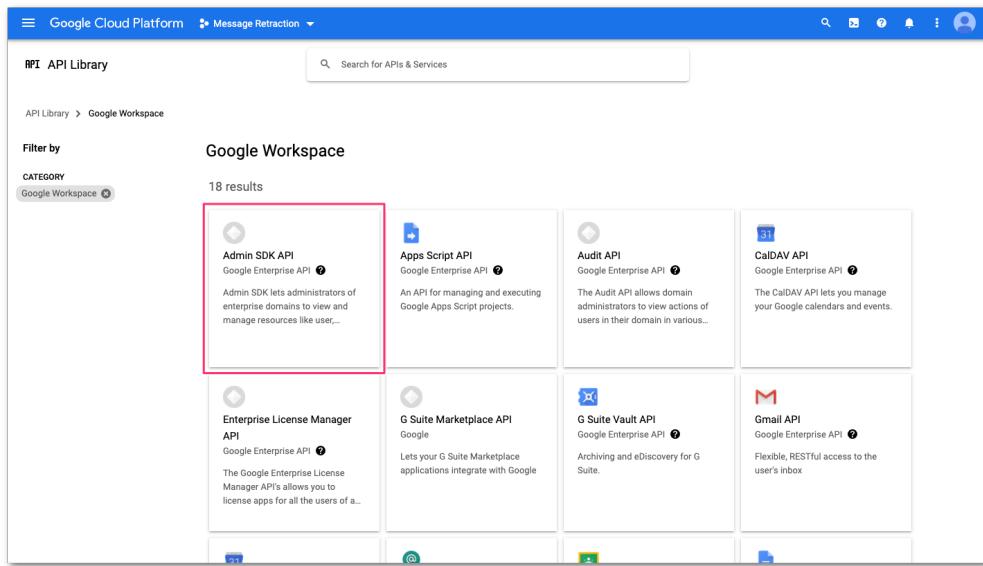
5. Click the **+ ENABLE APIs AND SERVICES** button to open the API Library.



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:

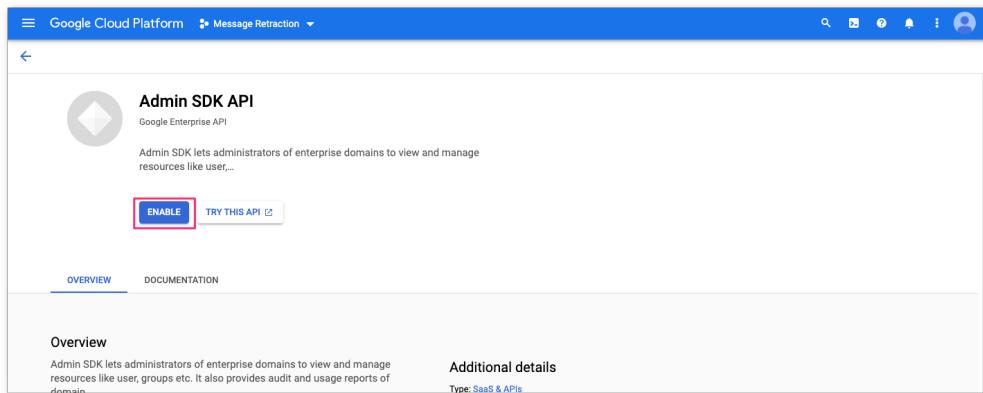


7. Select the Admin SDK API:



The screenshot shows the Google Cloud Platform API Library interface. The search bar at the top contains "Search for APIs & Services". Below it, the breadcrumb navigation shows "API Library > Google Workspace". A sidebar on the left titled "Filter by" has "Google Workspace" selected under "CATEGORY". The main area is titled "Google Workspace" and shows "18 results". The first result, "Admin SDK API", is highlighted with a red box. Other visible APIs include Apps Script API, Audit API, CalDAV API, Enterprise License Manager API, G Suite Marketplace API, G Suite Vault API, and Gmail API.

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



The screenshot shows the "Admin SDK API" detail page. At the top, there's a circular icon and the API name "Admin SDK API" with its description: "Google Enterprise API". Below that is a button labeled "ENABLE" with a red border. To its right is another button labeled "TRY THIS API". At the bottom of the page, there are two tabs: "OVERVIEW" (which is selected) and "DOCUMENTATION". The "OVERVIEW" section contains the "Overview" and "Additional details" sections. The "Additional details" section includes the "Type: SaaS & APIs" information.

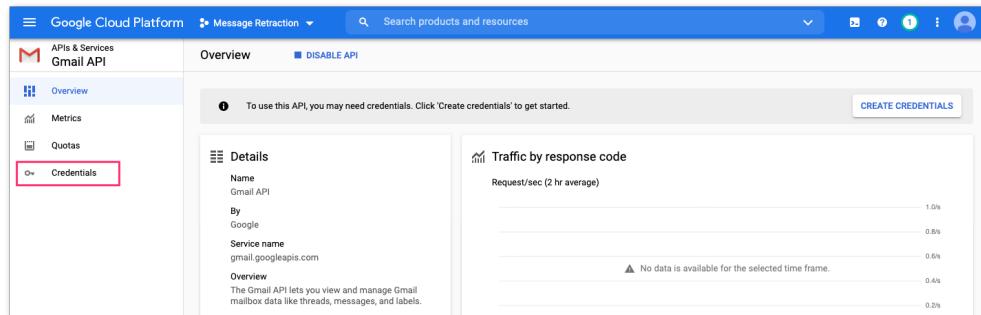
9. Return to the **Google Workspace** API library and select the **Gmail API**:

The screenshot shows the Google Cloud Platform API Library interface. The search bar at the top contains "Search for APIs & Services". Below it, the "API Library" section has a breadcrumb trail: "API Library > Google Workspace". A "Filter by" dropdown is set to "Google Workspace". The results are displayed in a grid under the heading "Google Workspace" with a count of "18 results". The "Gmail API" is highlighted with a red box. Other visible APIs include Admin SDK API, Apps Script API, Audit API, CalDAV API, Enterprise License Manager API, G Suite Marketplace API, G Suite Vault API, and Google Analytics API.

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

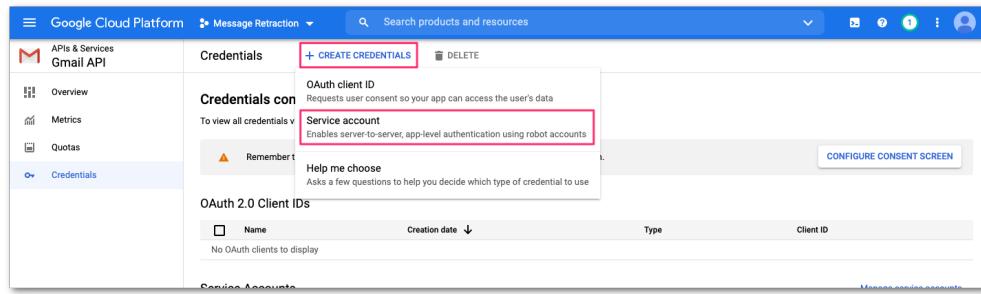
The screenshot shows the "Gmail API" overview page in the Google Cloud Platform. At the top, there's a "TRY THIS API" button. Below it, the "OVERVIEW" tab is selected, showing a brief description: "Flexible, RESTful access to the user's inbox". There are two main sections: "Overview" and "Additional details". The "Overview" section includes a "TRY THIS API" button. The "Additional details" section lists the type as "SaaS & APIs" and the last updated date as "3/18/21".

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:



The screenshot shows the Google Cloud Platform interface for the Gmail API. On the left sidebar, under 'APIs & Services', 'Gmail API' is selected. The 'Overview' tab is active. In the main content area, there's a message: 'To use this API, you may need credentials. Click "Create credentials" to get started.' Below this is a 'Details' section with fields like 'Name' (Gmail API), 'By' (Google), 'Service name' (gmail.googleapis.com), and an 'Overview' paragraph. To the right is a 'Traffic by response code' chart showing request rates over time. At the top right of the main area is a 'CREATE CREDENTIALS' button.

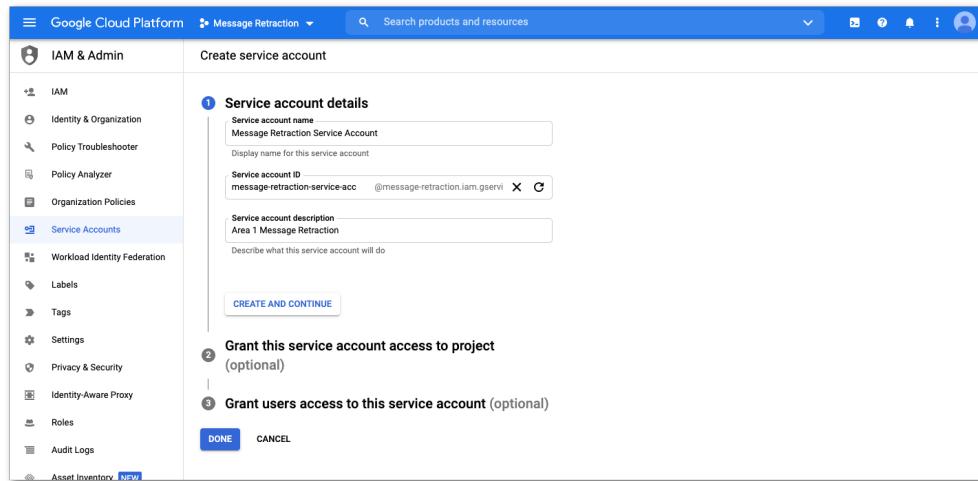
12. Click the **+ CREATE CREDENTIALS** menu option, followed by **Service account**, to start the process:



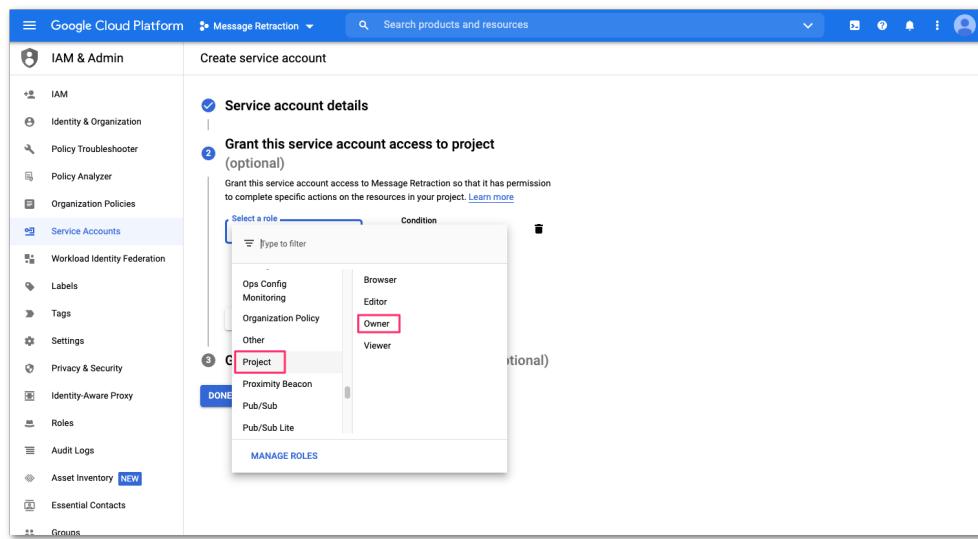
The screenshot shows the 'Credentials' page for the Gmail API. The left sidebar shows 'Overview', 'Metrics', 'Quotas', and 'Credentials'. The 'Credentials' menu item is highlighted with a red box. In the main area, there's a '+ CREATE CREDENTIALS' button. Below it, a 'Credentials type' dropdown has 'Service account' selected, which is also highlighted with a red box. Other options shown are 'OAuth client ID' and 'Help me choose'. At the bottom right is a 'CONFIGURE CONSENT SCREEN' button.

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

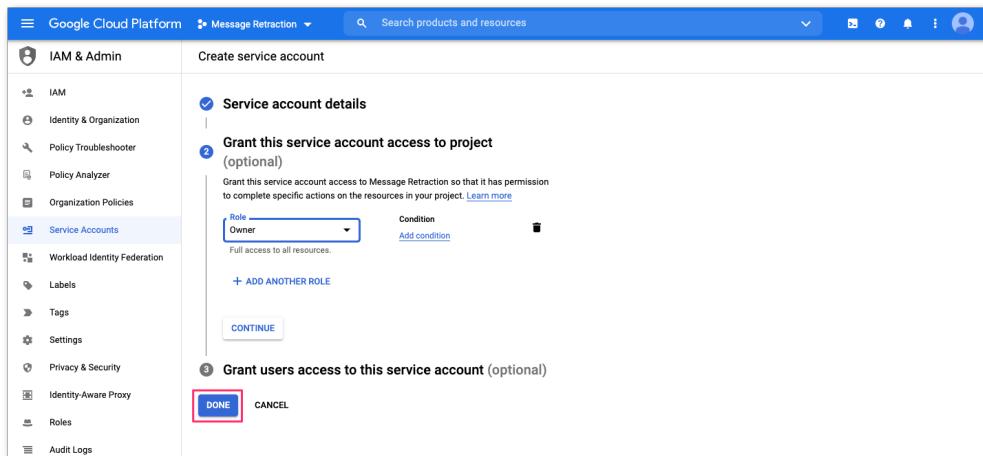
- Service account name (e.g. Message Retraction Service Account)
- Service account ID (value is automatically generated)
- Service account description (e.g. Area 1 Message Retraction)



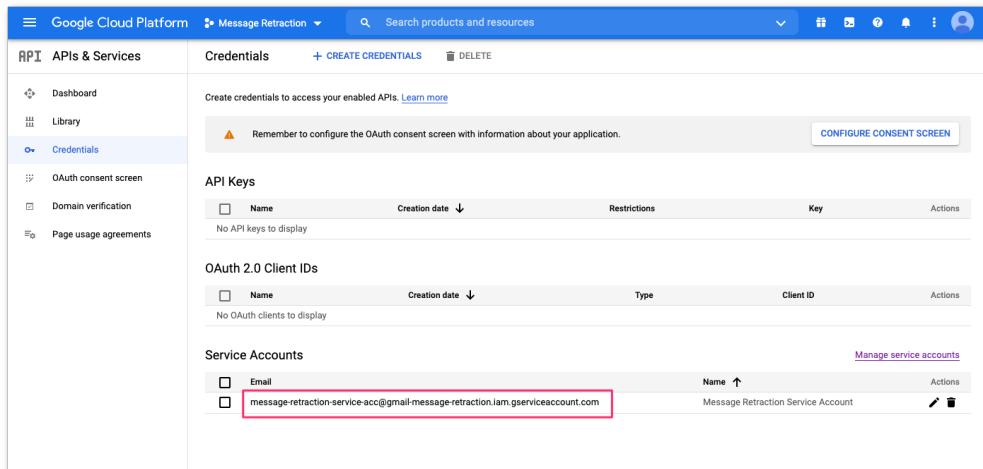
14. In the **Grant this service account access to project** section, click the **Select a role** dropdown. On the left column, find the **Project** item and select the **Owner** role on the right column:



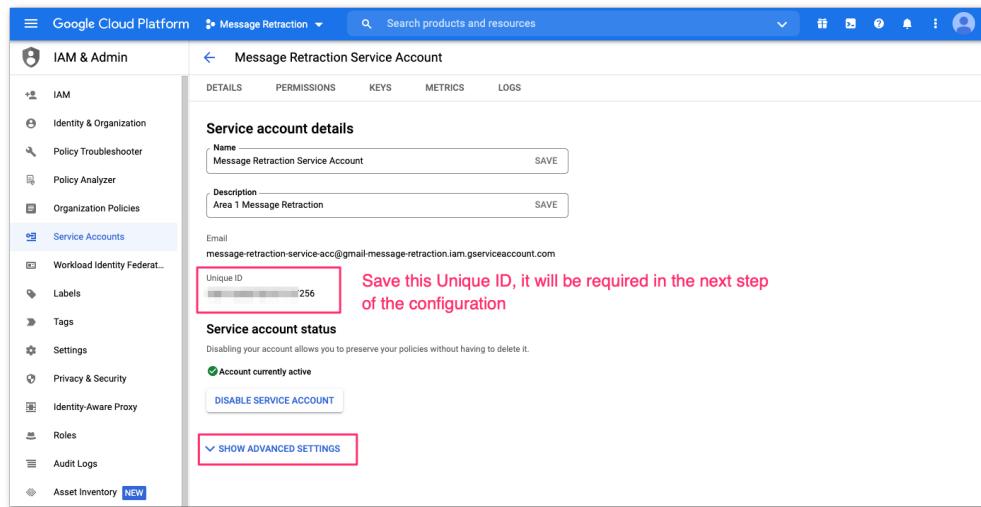
15. Once the role is assigned, click the **DONE** button to complete the setup:



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:

The screenshot shows the Google Cloud Platform IAM & Admin interface. On the left, there's a sidebar with various service links like IAM, Identity & Organization, Policy Troubleshooter, etc. The main panel is titled 'Message Retraction Service Account' under the 'Service account status' section. It shows the account is currently active. Below this, there's a 'Domain-wide Delegation' section with a warning message about caution when granting access via domain-wide delegation. A 'VIEW GOOGLE WORKSPACE ADMIN CONSOLE' button is located in this section, which is highlighted with a red rectangular box. At the bottom of the main panel, there's another section for 'Google Workspace Marketplace OAuth Client' with its own warning and a 'CONFIGURE' button. A link to 'HIDE ADVANCED SETTINGS' is at the very bottom.

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

The screenshot shows the Google Admin Console interface for 'Demo Corporation'. The left sidebar is collapsed, and the main area displays several sections:

- Users**: Shows 7 active users. Options include 'Add a user', 'Delete a user', 'Update a user's name or email', and 'Create an alternate email address (email alias)'.
- Billing**: Shows 'Manage subscriptions' and 'Payment accounts'.
- Product updates**: Lists recent changes:
 - Manage Gmail IMAP controls by group (06:30 AM)
 - Set user language programmatically with the Directory API (02:12 AM)
 - Admins can install Google Workspace Marketplace applications for specific groups (Dec 8)
 - Updated user interface for the App Access Control panel in the Admin console (Dec 8)
- Domains**: Shows the primary domain 'somedemocorp.com'. Options include 'Manage domains', 'Add a domain', and 'Change your primary domain'.

A modal window titled 'Enhance context-aware access with partner signals' is open on the right, featuring a shield icon and text about Lookout. It includes 'ENABLE PARTNER INTEGRATION' and 'DISMISS' buttons. Another modal for 'Enable advanced mobile management' is also visible.

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:

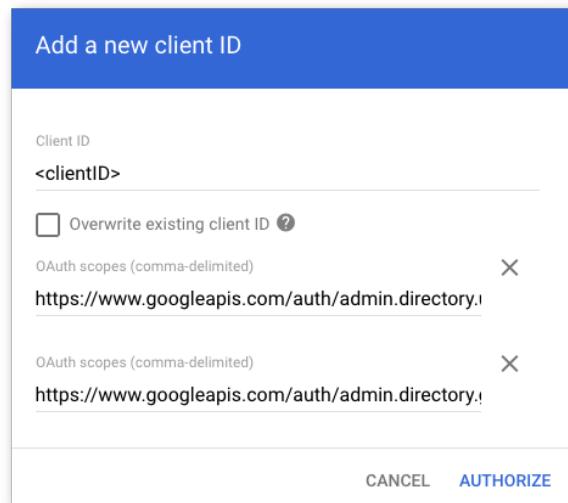
The screenshot shows the Google Admin interface under the Security section. The left sidebar has 'API controls' selected. The main content area is titled 'API controls' and contains a description of how it enables or restricts access to Google Workspace APIs. Below this is a 'Settings' section with two tabs: 'MANAGE GOOGLE SERVICES' and 'MANAGE THIRD-PARTY APP ACCESS'. Under 'MANAGE GOOGLE SERVICES', there is a message about users trying to access restricted services, a 'Message' input field, and a 'Area 1' section. The 'Area 1' section contains two settings: 'Block all third-party API access' (unchecked) and 'Trust internal, domain-owned apps' (checked). Below these is a note about apps trusted via Marketplace, Android, or iOS. At the bottom of this section are 'CANCEL' and 'SAVE' buttons. A red box highlights the 'MANAGE DOMAIN WIDE DELEGATION' button in the 'Domain wide delegation' section below. This section contains a note about developers registering clients and a link to 'MANAGE DOMAIN WIDE DELEGATION'.

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

The screenshot shows the Google Admin interface under the 'Security' section, specifically the 'API Controls' and 'Domain-wide Delegation' sub-sections. On the left, there's a sidebar with various administrative links like Home, Dashboard, Directory, Devices, Apps, Security, Reporting, Billing, Account, and Rules. The main content area has a header 'Search for users, groups or settings' and a breadcrumb path 'Security > API Controls > Domain-wide Delegation'. A blue info bar at the top states: 'Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords.' with a 'GOT IT' button. Below this, there are tabs for 'API clients' (selected), 'Add new' (highlighted with a red box), and 'Download client info'. There's also a '+ Add a filter' button. A table below lists columns for 'Name', 'Client ID', and 'Scopes'. At the bottom, there are pagination controls: 'Rows per page: 10', 'Page 1 of 1', and navigation arrows.

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** (the input field accepts comma separated values):
 - i. <https://www.googleapis.com/auth/admin.directory.user.readonly>,
<https://www.googleapis.com/auth/admin.directory.group.readonly>,
<https://www.googleapis.com/auth/admin.directory.user.alias.readonly>,
<https://www.googleapis.com/auth/gmail.labels>,
<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:

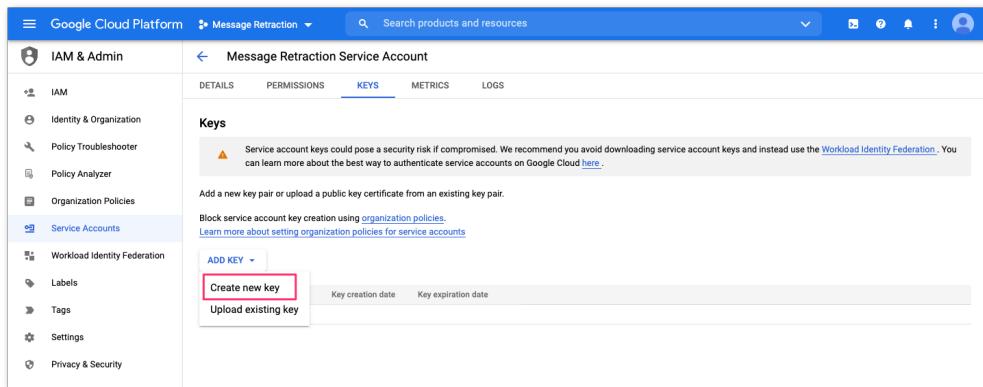
The screenshot shows the Google Cloud Platform (GCP) IAM & Admin interface. On the left, a sidebar lists various administrative tools under the heading 'IAM & Admin'. The 'Service Accounts' option is highlighted with a red box. The main content area is titled 'Message Retraction Service Account' and displays the details for a specific service account. The account's email is listed as 'message-retraction-service.acc@gmail-message-retraction.iam.gserviceaccount.com'. Below this, there is a 'Service account status' section indicating it is 'Account currently active'. A 'DISABLE SERVICE ACCOUNT' button is present. The next section, 'Domain-wide Delegation', contains a warning about granting domain-wide delegation and a 'LEARN MORE' link. At the bottom of this section is a 'Client ID' field showing '104712204734747157256' with a copy icon. A 'VIEW GOOGLE WORKSPACE ADMIN CONSOLE' button is also available. The final section, 'Google Workspace Marketplace OAuth Client', includes a warning about creating an OAuth client for Google Workspace Marketplace, a 'LEARN MORE' link, and a 'CONFIGURE' button.

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**:

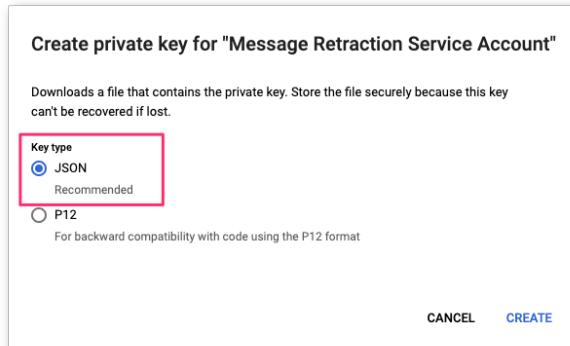
The screenshot shows the Google Cloud Platform IAM & Admin Service Accounts page. On the left, there's a sidebar with various options like IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, and Service Accounts (which is selected). The main area displays 'Service accounts for project "Message Retraction"'. A single service account is listed: 'message-retraction-service-acc@message-retraction.iam.gserviceaccount.com'. To the right of this account, a context menu is open, and the 'Manage keys' option is highlighted with a red box.

Email	Status	Name	Description	Key ID	Key creation date	Domain wide delegation	Actions
message-retraction-service-acc@message-retraction.iam.gserviceaccount.com	Enabled	Message Retraction Service Account	Area 1 Message Retraction	No keys		View Client	<ul style="list-style-type: none">Manage detailsManage permissionsManage keys (highlighted)View metricsView logsDisableDelete

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.

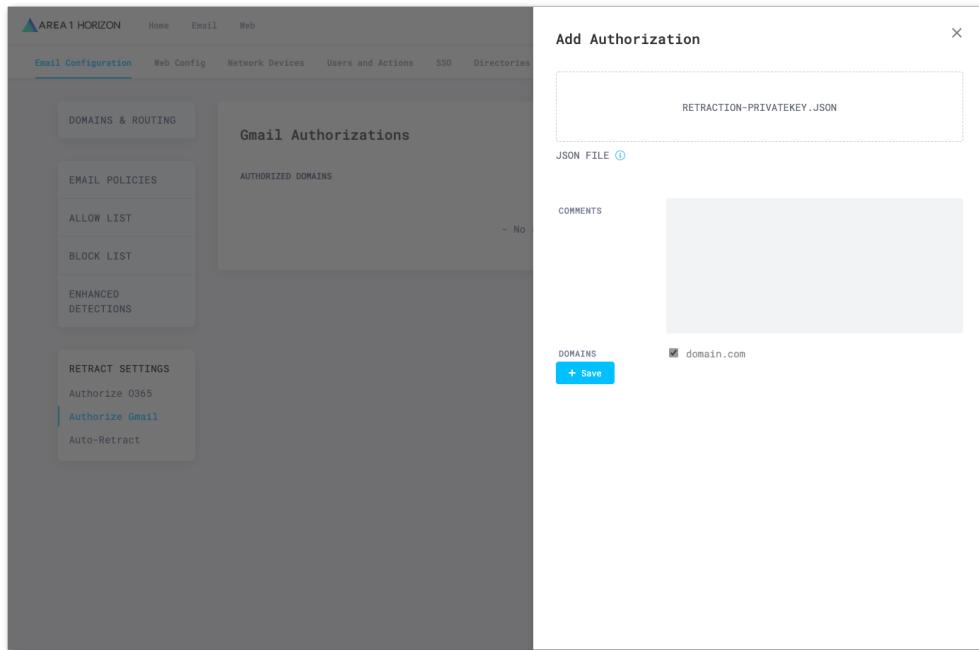
Step 2: Sharing the Service Account JSON Key with Area 1

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.

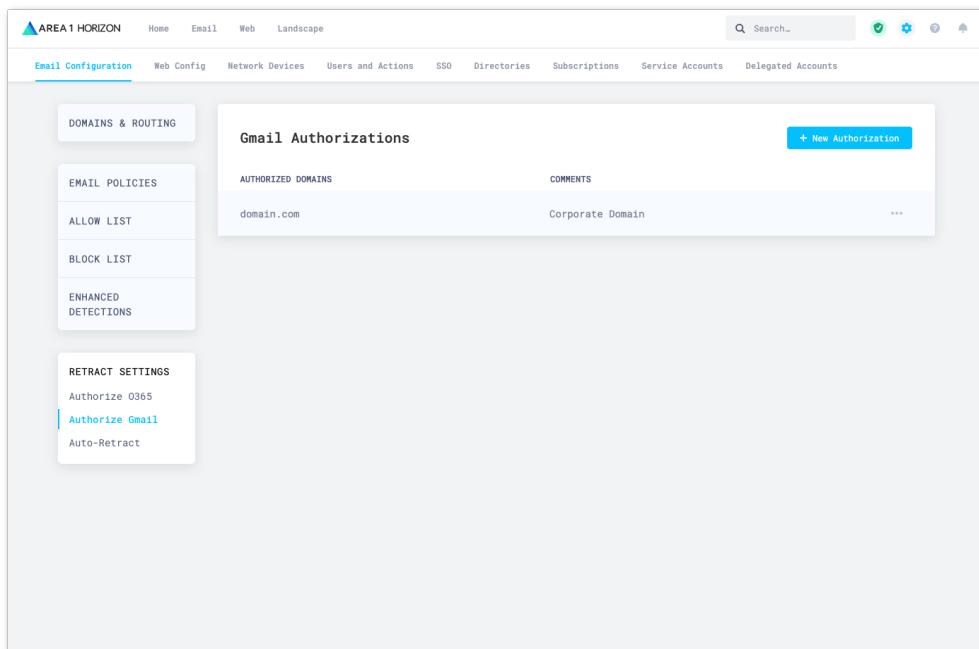
The screenshot shows the 'Email Configuration' page with the 'Gmail Authorizations' section selected. On the left, there's a sidebar with 'DOMAINS & ROUTING', 'EMAIL POLICIES' (which is currently selected), 'ALLOW LIST', 'BLOCK LIST', 'ENHANCED DETECTIONS', and 'RETRACT SETTINGS'. Under 'RETRACT SETTINGS', the 'Authorize 0365' and 'Authorize Gmail' options are listed, with 'Authorize Gmail' highlighted by a red box. The main area displays a table titled 'Gmail Authorizations' with columns 'AUTHORIZED DOMAINS' and 'COMMENTS'. A message at the bottom states '- No results to display -'. The top right of the page has a search bar and three small icons.

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:

The screenshot shows the 'Email Configuration' page in the 'Area 1 HORIZON' portal. The left sidebar has sections for 'DOMAINS & ROUTING', 'EMAIL POLICIES', 'ALLOW LIST', 'BLOCK LIST', and 'ENHANCED DETECTIONS'. The 'RETRACT SETTINGS' section is expanded, showing 'Authorize O365', 'Authorize Gmail', and 'Auto-Retract' (which is selected). The main content area is titled 'Auto-retract' and contains a table for managing automatic retract (clawback) settings. The table has columns for 'DISPOSITION', 'NO ACTION', 'TRASH', 'JUNK EMAIL', 'SOFT DELETE (USER RECOVERABLE)', and 'HARD DELETE (ADMIN RECOVERABLE)'. Rows are listed for 'Malicious', 'Spam', 'Bulk', 'Suspicious', and 'Spoof', each with a green checkmark in the 'NO ACTION' column. A blue 'Edit' button is located in the top right corner of the table area. Below the table is a section titled 'Phish Submission Response' with a toggle switch and a descriptive text about machine learning margin scores.

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.

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

DISPOSITION	NO ACTION	TRASH
Malicious	<input checked="" type="checkbox"/>	-
Spam	<input checked="" type="checkbox"/>	-
Bulk	<input checked="" type="checkbox"/>	-
Suspicious	<input checked="" type="checkbox"/>	-
Spoof	<input checked="" type="checkbox"/>	-

Phish Submission Response

With Phish Submission Response enabled, Horizon will automatically retract messages reported by your users that are found to be malicious. This feature uses machine learning margin scores by adding the user as an additional neuron into our neural network.

Update Auto-retract Settings

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

DISPOSITION	NO ACTION	TRASH	JUNK EMAIL	SOFT DELETE (USER RECOVERABLE)	HARD DELETE (ADMIN RECOVERABLE)
Malicious	-	<input checked="" type="checkbox"/>	-	-	-
Spam	-	-	<input checked="" type="checkbox"/>	-	-
Bulk	-	-	<input checked="" type="checkbox"/>	-	-
Suspicious	<input checked="" type="checkbox"/>	-	-	-	-
Spoof	<input checked="" type="checkbox"/>	-	-	-	-

Phish Submission Response

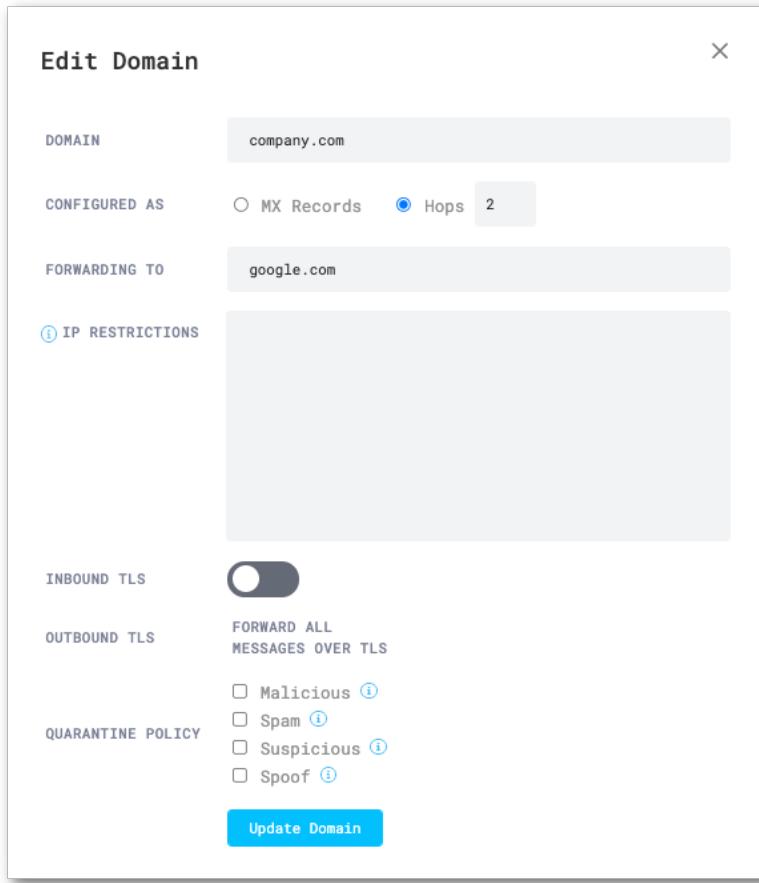
With Phish Submission Response enabled, Horizon will automatically retract messages reported by your users that are found to be malicious. This feature uses machine learning margin scores by adding the user as an additional neuron into our neural network.

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:

The screenshot shows the 'Email Configuration' page with the 'DOMAIN & ROUTING' tab selected. Under 'DOMAINS & ROUTING', the 'Domains' sub-tab is active. The main table displays 'All Domains' with one entry: 'company.com' forwarded to 'google.com'. The 'POSITION' column for 'company.com' is highlighted with a red box and contains the value 'MX Record'. The 'TLS' column indicates 'Inbound' and 'Outbound' with green status icons. On the left sidebar, other options like 'Allow List', 'Block List', and 'Enhanced Detections' are visible. At the bottom left is a 'RETRACT SETTINGS' button.

- 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.



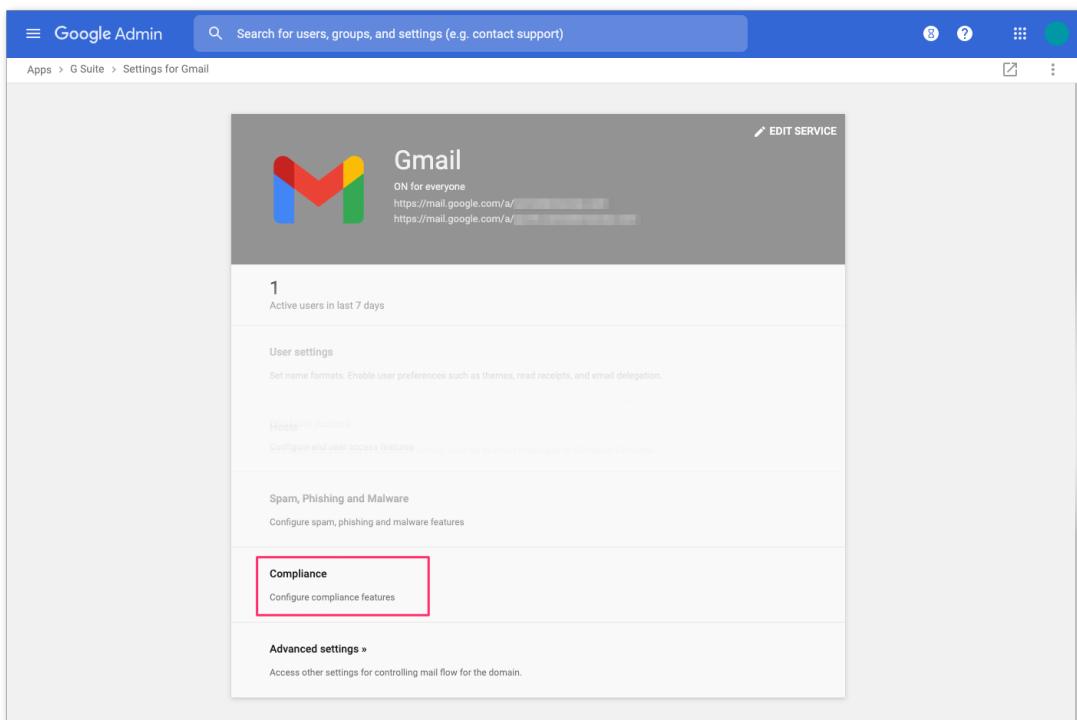
Note: If you have an existing SEG deployed as the MX record, you will need to adjust the hop count accordingly. Please contact Support if you need any assistance identifying the correct hop count.

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:

The screenshot shows the Google Admin interface under the 'Compliance' tab. On the left, there's a sidebar for 'Gmail' with sections for 'Status' (ON for everyone) and 'Organizational Unit'. Below that is a search bar for 'Search for organizational units'. The main content area is titled 'Appends footer' with a sub-section 'Content compliance' highlighted by a red box. To the right of 'Content compliance' is a 'CONFIGURE' button also highlighted with a red box. Other sections visible include 'Restrict delivery', 'Objectionable content', 'Attachment compliance', and 'Secure transport (TLS) compliance', each with their own 'CONFIGURE' buttons.

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

The screenshot shows the 'Add setting' dialog for 'Content compliance'. At the top, it says 'Area 1 - Bcc'. Below that, it lists '1. Email messages to affect' with four options: 'Inbound' (checked), 'Outbound', 'Internal - Sending', and 'Internal - Receiving'. There is also a 'Learn more' link.

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/>.

Add setting

Advanced content match ▾

Location
Headers + Body

Match type
Matches regex

Regexp [Learn more](#)

`.*`

Enter sample data No match

Regex Description
Optional

Minimum match count
Optional

Enter number of matches

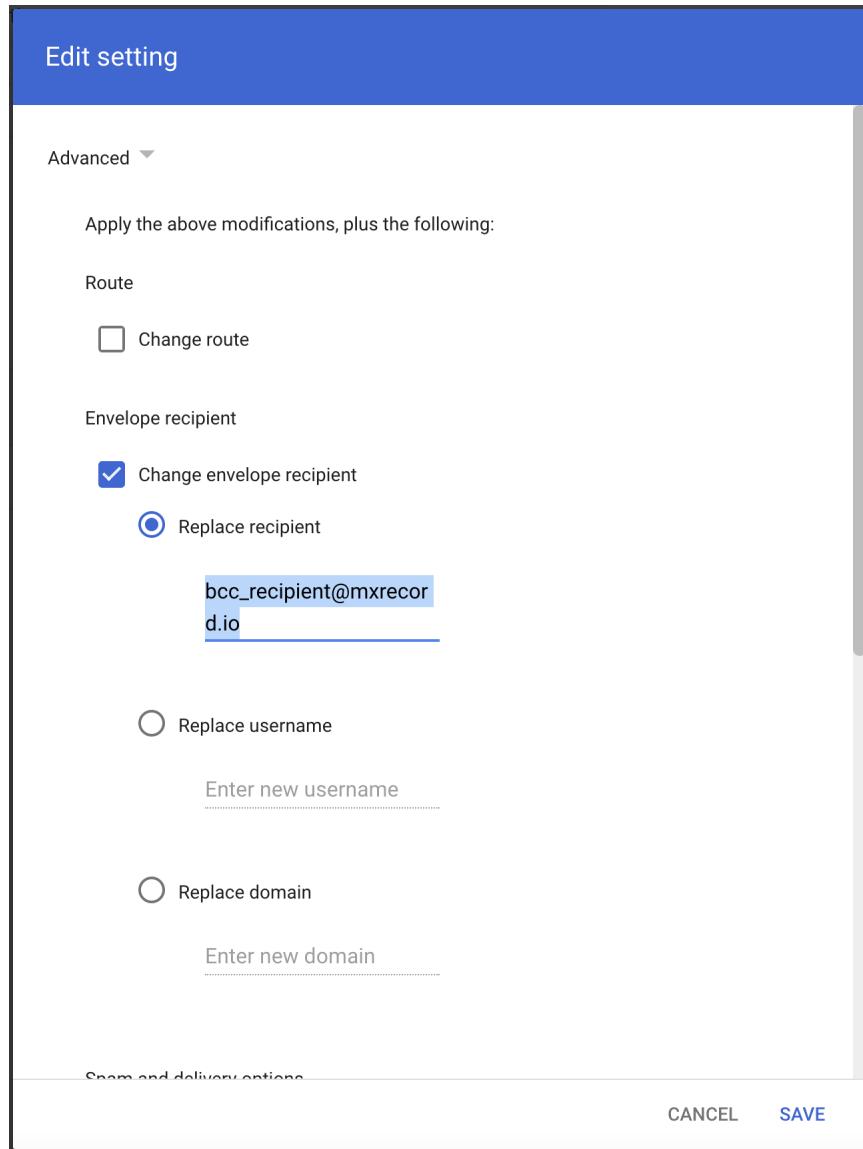
CANCEL [SAVE](#)

iv. Click **SAVE** to save your settings

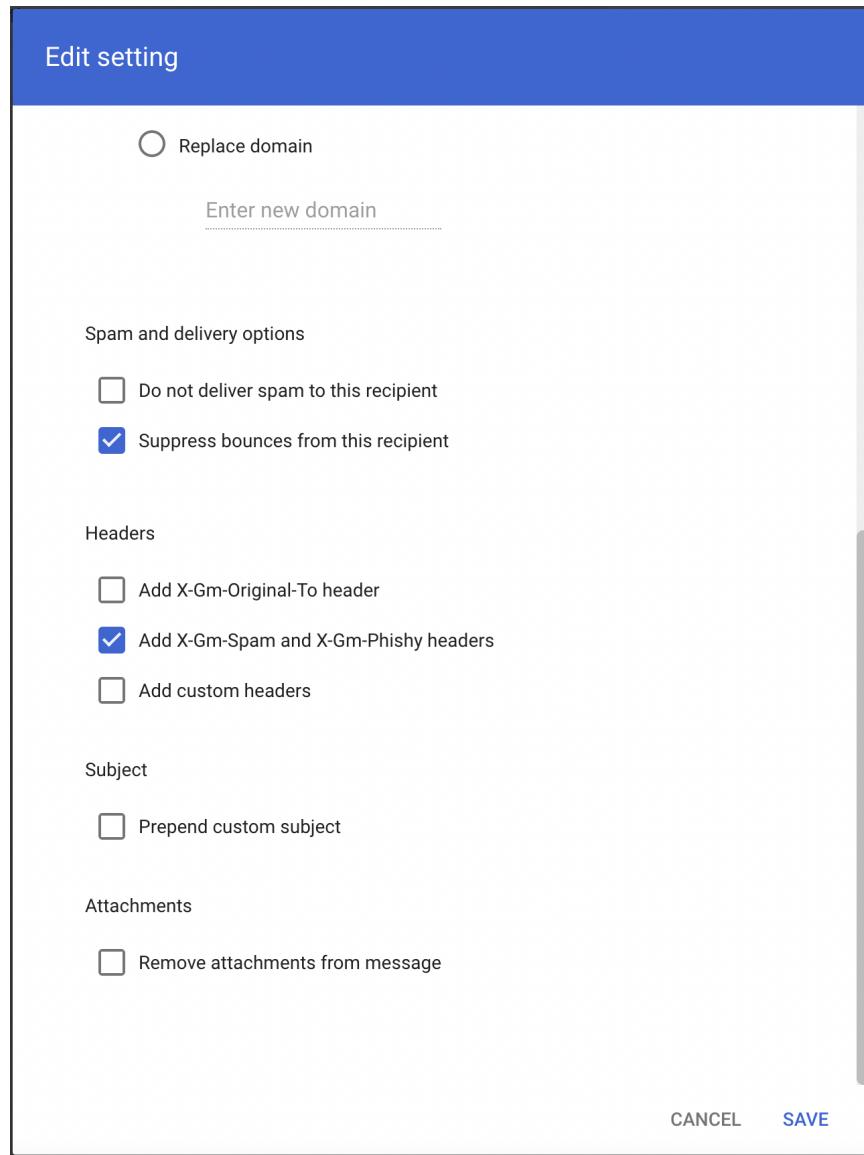
7. In section “3. If the above expressions match, do the following” make the following changes.
- a. Under **Also deliver to** check “Add more recipients”

- 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>

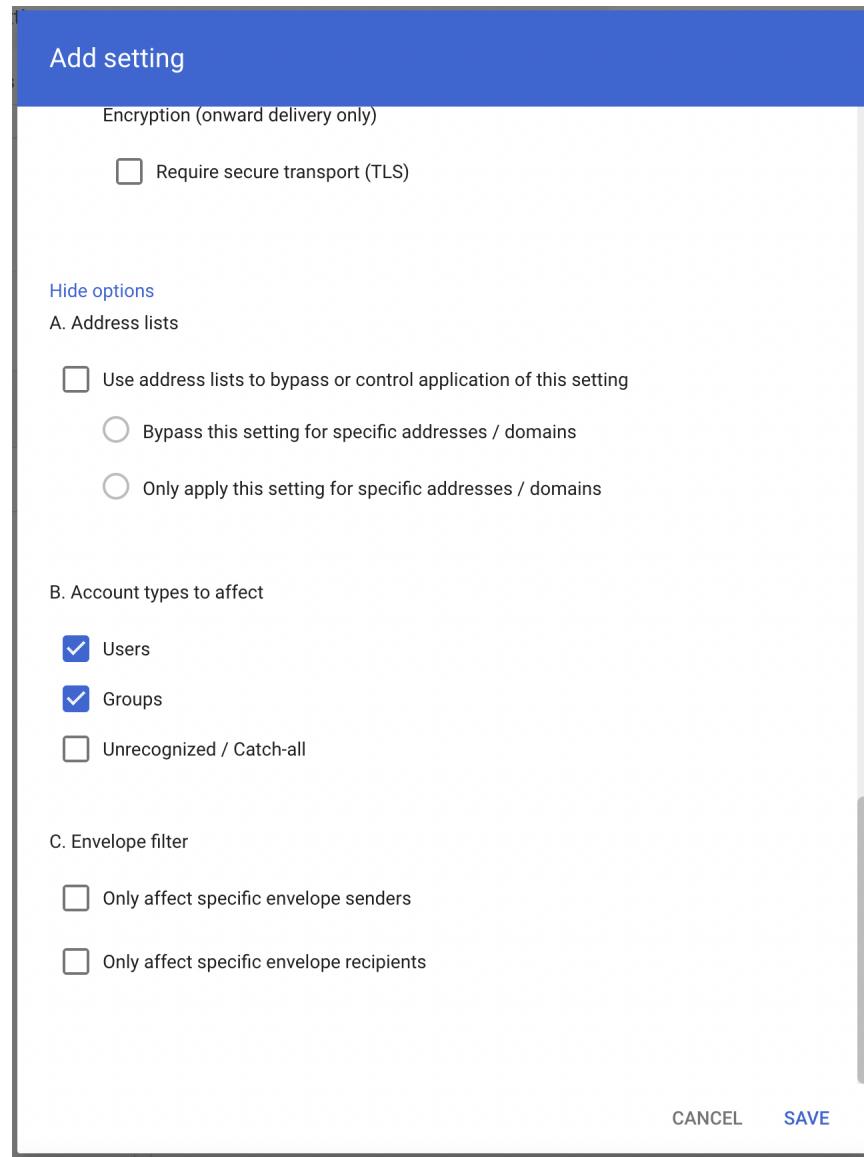
If you are located in the EU or GDPR applies to your organization, replace the “@mxrecord.io” domain in the bcc recipient with “@mailstream-eu1.mxrecord.io”, this will force email to be processed in Germany under compliance with GDPR. E.g. bcc_recipient@mailstream-eu1.mxrecord.io



- 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”

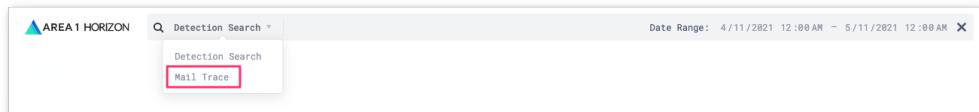


- b. Click SAVE to save your settings

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.

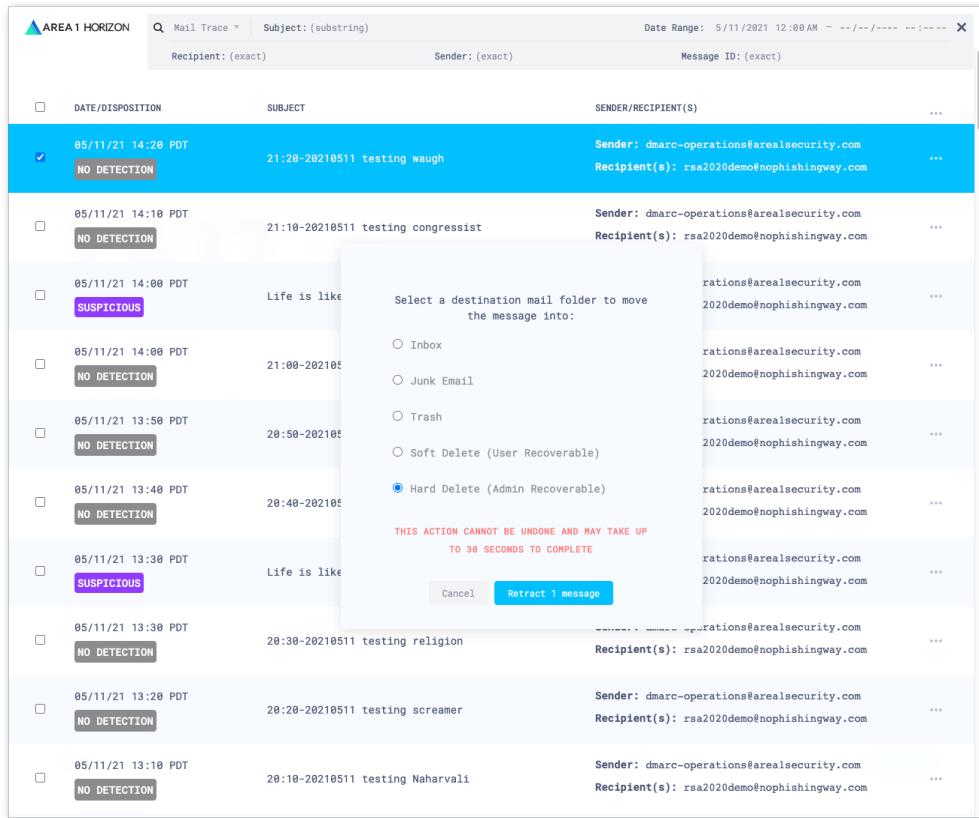
1. To manually retract a message, you will first need to find the message to retract. Access the Mail Trace search function by clicking the Search bar on top of the portal and using the dropdown to change the search type to Mail Trace:



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:



- 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:

The screenshot shows a list of messages in the Mail Trace interface. Each message row includes the date, time, subject, and detection status (e.g., NO DETECTION, SUSPICIOUS). The last message in the list has a green box at the bottom right containing the text "The message was successfully retracted."

DATE/DISPOSITION	SUBJECT	SENDER/RECIPIENT(S)
05/11/21 14:20 PDT NO DETECTION	21:20-20210511 testing waugh	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 14:10 PDT NO DETECTION	21:10-20210511 testing congressist	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 14:00 PDT SUSPICIOUS	Life is like a box of chocolates Pearl...	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 14:00 PDT NO DETECTION	21:00-20210511 testing Acipenseroidae	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:50 PDT NO DETECTION	20:50-20210511 testing apathistical	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:40 PDT NO DETECTION	20:40-20210511 testing uncolleged	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:30 PDT SUSPICIOUS	Life is like a box of chocolates Pearl...	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:30 PDT NO DETECTION	20:30-20210511 testing religion	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:20 PDT NO DETECTION	20:20-20210511 testing screamer	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
05/11/21 13:10 PDT NO DETECTION	20:10-20210511 testing Naharvali	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com The message was successfully retracted.