

# **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.

≡ Google Cloud Platform 🗈	▼ Q Search products a	id resources	~	5.	0	۰	÷	9
Dashboard								
Page not viewable for organizations. To vi	iew this page, select a project.		s	ELECT PROJI	ст с	REATE	PROJEC	л
Select a recent project								
My First Project Project ID: Organization: Accessed Dec 16, 2020								

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.

	age Retraction 👻	Q Search products and resources		× 2 0	+ E 🙆
DASHBOARD ACTIVITY RECOMMEN	IDATIONS				CUSTOMIZE
Project info Project name Message Retraction	I	RPI APIs Requests (requests/sec)	1	<ul> <li>Google Cloud Platform status</li> <li>All services normal</li> </ul>	:
Project ID message-retraction Project number		No data is available for the selected time frame.	0.8	→ Go to Cloud status dashboard	
ADD PEOPLE TO THIS PROJECT			0.4 0.2	Estimated charges For the billing period Jun 1 - 21, 2021	¥ USD \$0.00
→ Go to project settings		2 PM 2:15 2:30 2:45	0	Take a tour of billing	
Resources  This project has no resources	:	→ Go to APIs overview		→ View detailed charges	
- Trace	1			Create my dashboard	

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:

HBOARD ACTIVITY RECOMMENDATION	S		CUSTOM
Project info Project name Message Retraction	:	RPI APIs : O Google Cloud Platform status Requests (requests/sec) All services normal	÷
Project ID message-retraction Project number		G to Cloud status dashboard	
		No data is available for the selected time frame.  0.4  Billing	:
ADD PEOPLE TO THIS PROJECT		0.2 Estimated charges For the billing period Jun 1 – 21, 2021	USD \$0.00
Go to project settings		2:15 2:30 2:45 3 PM	
Resources	:	Contro APIs overview	
This project has no resources		Sector and the sector	:
<b>T</b>		Create my dashboard	
No trace data from the past 7 days	:	Set up alerting policies	
Gat started with Trace		Create uptime checks	
	_	View all dashboards	
Getting Started	:	ightarrow Go to Monitoring	
Deploy a prebuilt solution		(i) Error Reporting	:
Add dynamic logging to a running application		No sign of any errors. Have you set up Error Reporting?	,
Monitor errors with Error Reporting		-> Learn how to set up Error Reporting	
Deploy a Hello World app			
F I ake a vm quickstart		News	:
Create a Cloud Function		what s new winn Google Cloud 2 hours ago	
Install the Cloud SDK		Leveraging siguuery Public Boundaries datasets for ge analytics 3 hours ago	iospatiai
		BigQuery row-level security enables more granular acce	ess to data

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

≡	Google Cloud Platform	Description → Q. Search products and resources ✓ D Q .	: 🙆
API	APIs & Services	APIs & Services + ENABLE APIS AND SERVICES	
¢	Dashboard	1 hours 1 hours 1 days 2 days 7 days 14 days	30 days
毌	Library		
0+	Credentials	Traffic ± Errors	±
57	OAuth consent screen	1.05	2%
7	Domain verification	0.8%	
Ξo	Page usage agreements	No data is available for the selected time frame.      O.4/s	%
		0.2/8	5
		۵ مند ۵۵ مند 30 مند 30 May 30 May 30 مند 30 مند 30 May 30 مند	
		Median latency ±	

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:

	Se Message Retraction ▼			९ 🖪 🖲 🕴 🕻
← API Library	• The API Libra Q. Beard	e to the API Library	nart search experience.	
momoring (y) Networking (7) Operating systems (1) Security (5)	Google Workspace			• VIEW ALL (18)
Security Command Center Ser (1) Social (d) Stotrage (6) YouTube (3) Other (43) PRICE Free (1) Paid (4)	Coogle Drive API Google Drive API Google Drive API The Google Drive API allows clients to access resources from Google Drive	Google Calendar API Google Enterprise API  Coogle Enterprise API Coogle Calendar using the Calendar API.	Crnail API Google Enterprise API Flexible, RESTful access to the user's inbox	Image: Strategy of the strateg
	YouTube		VIEW ALL (3)	

7. Select the Admin SDK API:

	💲 Message Retraction 👻			९ 🖪 🛛 🗍 🕂	9
RPI API Library	Q. Search 1	or APIs & Services			
API Library > Google Workspace					
Filter by	Google Workspace				
CATEGORY Google Workspace	18 results	7			
	Admin SDK API Google Enterprise API Admin SDK lets administrators of enterprise domains to view and manage resources like user,	Apps Script API Google Enterprise API  An API for managing and executing Google Apps Script projects.	Audit API Google Enterprise API The Audit API allows domain administrators to view actions of users in their domain in various	CaDAV API Google Enterprise API The CaDAV API tes you manage your Google calendars and events.	
	Content of the second s	G Suite Marketplace API Google Lets your G Suite Marketplace applications integrate with Google	G Suite Vault API Google Enterprise API C Archiving and eDiscovery for G Suite.	Conal API Google Enterprise API © Flexible, RESTful access to the user's inbox	
	(57)				

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

≡	Google Cloud	l Platform 🔹 Message Retraction 👻	۹	۶.	?	٠	: (	9
÷								
		Admin SDK API Google Enterprise API Admin SDK lets administrators of enterprise domains to view and manage resources like user TRY THIS API @						
	OVERVIEW	DOCUMENTATION						
	Overview							
	Admin SDK lets a resources like use domain	administrators of enterprise domains to view and manage er, groups etc. It also provides audit and usage reports of Type: SasS & APIs	_	_	_			

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

	n 💲 Message Retraction 👻			९ 🖬 🥹 🌲	: 2
API API Library	Q. Search	for APIs & Services			
API Library > Google Workspace					
Filter by	Google Workspace				
CATEGORY Google Workspace	18 results				
	Admin SDK API Google Enterprise API • Admin SDK Ites administrators of enterprise domains to view and manage resources like user,	Cosple Enterprise API Cosple Enterprise API Cosple Enterprise API Cosple Enterprise API Cosple Appa Script projects.	Audit API Google Enterprise API The Audit API allows domain administrators to view actions of users in their domain in various	CAIDAV API Google Enterprise API @ The CaIDAV API lets your manage your Google calendars and events.	
	Conterprise License Manager API Google Enterprise API The Google Enterprise License Manager APIs allows you to License apps for all the users of a	G Suite Marketplace API Google Lets your G Suite Marketplace applications integrate with Google	CSuite Vauit API Google Enterprise API C Archiving and eDiscovery for G Suite.	Cmail API Google Enterprise API O Plexible, RESTful access to the user's inbox	

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

≡	Google Cloud Plat	form 💲 Message Retraction 👻	Q Search products and resources	~	۶.	0	٠	÷ (	
÷									
	Goo Flex	<b>nail API</b> <sup>gle</sup> xible, RESTful access to the user's inbox							
	E	VABLE TRY THIS API							
	OVERVIEW DO	ICUMENTATION SUPPORT							_
	Overview								
_	The Gmail API lets you view and manage Gmail mailbox data like threads, messages, and labels.		hreads, Additional details Type: <u>SanS &amp; APIs</u> Lest.undstad: 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:

=	Google Cloud Platform	Search product	s and resources	5 0 1 i 🙆
Μ	APIs & Services Gmail API	Overview DISABLE API		
:: 	Overview Metrics	To use this API, you may need credentials. Click 'Crea	ate credentials' to get started.	CREATE CREDENTIALS
•	Quotas Credentials	E Details Name Grani API	ଲୀ Traffic by response code Request/sec (2 hr average)	
		By Google Service name gmail.googleapis.com Overview	▲ No data is available for the selected time frame.	1.0% 0.8% 0.6%
		The Gmail API lets you view and manage Gmail mailbox data like threads, messages, and labels.		0.2/8

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

≡	Google Cloud Platform	- Message Retraction		v 🛛 🛛 🕄 🕰	
Μ	APIs & Services Gmail API	Credentials	+ CREATE CREDENTIALS		
99	Overview	Credentials con	OAuth client ID Requests user consent so your app can access the user's data		
<b>M</b>	Metrics	To view all credentials v	Service account Enables server-to-server, app-level authentication using robot accounts		
	Quotas	A Remember t	Help me sheepe		CONFIGURE CONSENT SCREEN
0+	Credentials		Asks a few questions to help you decide which type of credential to use		
		OAuth 2.0 Client II	Os		
		Name Name	Creation date 🗸	Туре	Client ID
		No OAuth clients to di	splay		
		Service Accounts			Managa papilas appointe

- 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)

=	Google Cloud Platform	Search products and resources	
θ	IAM & Admin	Create service account	٦
• <u>#</u>	IAM	Service account details	
Θ	Identity & Organization	Service account name Messan Batration Survive Account	
٩	Policy Troubleshooter	Display name for this service account	
6	Policy Analyzer	Service account ID	
₽	Organization Policies		
연고	Service Accounts	Area 1 Message Retraction	
₩å	Workload Identity Federation	Describe what this service account will do	
۹	Labels		
	Tags	CREATE AND CONTINUE	
٠	Settings	Grant this service account access to project	
0	Privacy & Security	(optional)	
	Identity-Aware Proxy	Grant users access to this service account (optional)	
	Roles		
Ξ	Audit Logs	DARE CARVEL	
	Asset Inventory NEW		_

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:

≡	Google Cloud Platform	Search products and resources	~	э.	8	٠	: 🙆	
θ	IAM & Admin	Create service account						
•=	IAM	Service account details						
4	Policy Troubleshooter	Grant this service account access to project						
6	Policy Analyzer	Grant this service account access to Message Retraction so that it has permission						
	Organization Policies	to complete specific actions on the resources in your project. Learn more						
<u>0</u>	Service Accounts	Select a role Condition						
5	Workload Identity Federation	Pype to inter						
۹	Labels	Ops Config Browser Monitoring Entitor						
	Tags	Organization Policy Owner						
۵	Settings	Other Viewer						
0	Privacy & Security	C Project Itional)						
	Identity-Aware Proxy	DONE Proximity Beacon Pudr/Sub						
	Roles	Pub/Sub Lite						
Ξ	Audit Logs	MANAGE ROLES						
	Asset Inventory NEW							
8	Essential Contacts							

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

≡	Google Cloud Platform	★ Message Retraction
θ	IAM & Admin	Create service account
•=	IAM	Service account details
٩	Policy Troubleshooter	Grant this service account access to project     (optional)
E,	Policy Analyzer	Grant this service account access to Message Retraction so that it has permission to complete specific actions on the resources in your project. Learn more
⊑ 12	Service Accounts	Role Condition
54	Workload Identity Federation	Full access to all resources.
٠	Labels	+ ADD ANOTHER ROLE
>	Tags	CONTINUE
*	Settings	
0	Privacy & Security	Grant users access to this service account (optional)
	Roles	DONE CANCEL
≡	Audit Logs	

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:

≡	Google Cloud Platform	🐌 Message Retraction 👻	Q Search products and resources		v ii 🗷 0	🔺 E 🙆
API	APIs & Services	Credentials + CRE	ATE CREDENTIALS			
<\$	Dashboard	Create credentials to access your	enabled APIs. Learn more			
ш	Library	A Remember to configu	re the OAuth concept corean with information about	it your application	CONFIGURE CON	ISENT SODEEN
0+	Credentials	A Remember to comiga	e die OAddi consent screen with mormation abo	your application.		ICENT CORLEN
17	OAuth consent screen	API Keys				
V	Domain verification	Name Name	Creation date	Restrictions	Key	Actions
= <sub>0</sub>	Page usage agreements	No API keys to display				
		OAuth 2.0 Client IDs				
		Name	Creation date 🔸	Туре	Client ID	Actions
		No OAuth clients to display				
		Service Accounts			Manage	service accounts
		Email		Nar	ne 个	Actions
		message-retraction-se	rvice-acc@gmail-message-retraction.iam.gservice	account.com Me	ssage Retraction Service Account	/ 1

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

≡	Google Cloud Platform	Search products and resources	~	ŧ:	э.	?	۰	÷	9
θ	IAM & Admin	← Message Retraction Service Account							
+ <u>e</u>	IAM	DETAILS PERMISSIONS KEYS METRICS LOGS							
Θ	Identity & Organization	Service account details							
٩	Policy Troubleshooter	Name							
Ę	Policy Analyzer	Description							
	Organization Policies	Area 1 Message Retraction SAVE							
<u>•</u> =	Service Accounts	Email							
	Workload Identity Federat	message-retraction-service-acc@gmail-message-retraction.iam.gserviceaccount.com							
٠	Labels	Save this Unique ID, it will be required in the next step of the configuration							
•	Tags	Service account status							
۰	Settings	Disabling your account allows you to preserve your policies without having to delete it.							
0	Privacy & Security	Ø Account currently active							
æ	Identity-Aware Proxy	DISABLE SERVICE ACCOUNT							
	Roles								
Ξ	Audit Logs	V STORFAUVAULU SLITINGS							
•	Asset Inventory NEW								

**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**:

≡ Google Admin	Q Search for users, groups or settings		4 8 Ø III 🌑
Home Home Dashboard Dashboard  A Directory  Coversiew Alert center Authentication Access and data control API controls Context-Aware Access	Demo Corporation Welcome to the Google Workspace Admin     Users     Manage     Active     7     Add a user Delete a user Update a user's name or email Create an alternate email address (email alias)	n Console           Billing         Manage           Manage subscriptions         Payment accounts           Get more services         Get more services	Chance context-aware access with partner signals For the signal of the context is the
Data protection Google Session control Google (Dud session control Less secure apps - Security center - II. Reporting - Billing - O Account - Rules	✔ Product updates         View all         ▲           Manage Gmail IMAP controls by group         06.30 AM         ■           In the Admin console         02.12 AM         ■           Set user language programmatically         02.12 AM         ■           Marketplace applications for specific groups         Dec 8         ■           Updated user interface for the App Access Control panel in the Admin console         Dec 8         ■	C Domains Overview A Primary domain Somedemocorp.com Manage domains Add a domain Change your primary domain	<ul> <li>Google Workspace Status Dashboard</li> <li>Data Export</li> <li>Transfer tool for unmanaged users</li> <li>Google Meet video setup</li> <li>Google Workspace Marketplace</li> <li>Get help from a partner</li> <li>The Google Workspace Referral Program</li> </ul>
🚊 gmail-messagejson \land			Show All X

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:

≡ Google Admin	Q Search for users, groups or settings			φB	0	•
👻 😯 Security	Security > API Controls	MAN	AGE GOOGLE SERVICES	MANAGE THIRD-PARTY AF	PP ACCESS	
Overview Alert center Authentication	API controls	Settings Show	/ this message if a user tries to	use an app that can't access restric	ted Google	
Access and data control      API controls      Context-Aware Access     Data protection     Google Session control     Google Cloud session     control     Less secure apps     Security center     II. Reporting     Billing     @ Account	Use these controls to enable or restrict access to Google Workspace APIs for customer- owned and third-party applications and service accounts. Reduce the risk associated with third-party access to Google Workspace APIs by limiting access to only trusted apps.	servi Messa Area □ □ 1 Apps autor	ces age (100 characters limit) 1 Block all third-party API access Requests by third-party apps ar end user data. This setting bloc Learn more Trust internal, domain-owned apps w are restricted or blocked. up that internal, domain-owned apps w are restricted or blocked.	e denied access to Google Workspr kes all OAuth scopes, including sign pps ill be exempt from accessing OAuth pace Marketplace, Android, or iOS a cess control list.	ice data an in scopes. I scopes th	d at
Rules     Show less     Sond feedback     Source alling terms -     Privacy Policy		Domain wide delegation Developers can register their web ap services like Gmail. You can authori individually give consent or their pas MANAGE DOMAIN WIDE DELEGATION	splications and other API clients there registered clients to ac severeds. Learn more DN	CAN s with Google to enable access to d	CEL :	le to
gmail-messagejson ^						Show All X

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

≡ Google Admin Q	Search for users, groups or setting	s		ф 8 @	₩ ●
Home	Security > API Controls > Domain-wide	Delegation			
Dashboard	Developers can register their well     authorize these exclusions	applications and other API clients with Goo	ogle to enable access to data in Google servi	ces like Gmail. You can	GOT IT
Directory	authorize these registered clients	s to access your user data without your user	s naving to individually give consent or their j	passwords.	
▶ □ Devices	API clients Add new Dow	nload client info			
Apps					
👻 😯 Security	+ Add a filter				
Overview	Name	Client ID	Scopes		
Alert center					
<ul> <li>Authentication</li> </ul>					
<ul> <li>Access and data control</li> </ul>					
API controls					
Context-Aware Access					
Data protection					
Google Session control					
Google Cloud session control					
Less secure apps					
<ul> <li>Security center</li> </ul>					
▶ II. Reporting					
Billing					
Account	D			Li Barritati	
Rules	kows per page: 10 👻			IS Page 1 of 1	
Show less					

#### 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/

Client ID	
<clientid></clientid>	
Overwrite existing client ID 🖉	
OAuth scopes (comma-delimited)	×
https://www.googleapis.com/auth/adm	in.directory.
OAuth scopes (comma-delimited)	×
https://www.googleapis.com/auth/adm	in.directory.

• 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:

≡	Google Cloud Platform	Search products and resources	~	-	э.	0	۰	: 🙎	
θ	IAM & Admin	← Message Retraction Service Account							]
+ <u>e</u>	IAM	DETAILS PERMISSIONS KEYS METRICS LOGS							
Θ	Identity & Organization	message-retraction-service-acc@gmail-message-retraction.iam.gserviceaccount.com							
٩	Policy Troubleshooter	Unique ID 256							
B	Policy Analyzer	Service account status							
	Organization Policies	Disabling your account allows you to preserve your policies without having to delete it.							ł
크	Service Accounts	S Account currently active							ł
E	Workload Identity Federat	DISABLE SERVICE ACCOUNT							ł
۹	Labels	Domain-wide Delegation							ł
	Tags	Grantian this service account access to your amanization's data via							
۰	Settings	domain-wide delegation should be used with caution. It can be reversed by disabling or deleting the service account or by removing access							ł
Ø	Privacy & Security	through the Google Workspace admin console.							ł
<b>.</b>	Identity-Aware Proxy	LEARN MORE							
*	Roles	Client ID: 104712204734747157256 🛛 🚹							
≡	Audit Logs	VIEW GOOGLE WORKSPACE ADMIN CONSOLE							ł
$\otimes$	Asset Inventory NEW								ł
2	Essential Contacts	Google Workspace Marketplace OAuth Client							ł
21	Groups	Creating this OAuth client is necessary to support Google Workspace Marketplace domain-wide installation and should be used with caution.							ł
ж,	Early Access Center	Google Workspace Marketplace may grant permissions to all OAuth clients in your project. This can only be reversed by disabling or deleting							
	Quotas	the service account.							ł
0	Manage Resources	LEARN MURE							
D)	Release Notes	An OAuth consent screen must be configured in order to create an OAuth client.							ł
<1		CONFIGURE		_		_			

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**:

=	Google Cloud Platform	🐌 Mess	sage Retraction 👻	٩	Search products a	nd resources				×	~	۶.	0	۰	: (	
θ	IAM & Admin	Servic	e accounts +	CREATE	SERVICE ACCOUNT	👕 DELETE	◆ <u>■</u> MANAGE A	ACCESS								
• <u>*</u>	IAM	Servic	e accounts for projec	ct "Me:	ssage Retraction	,										
Θ	Identity & Organization	A service	account represents a Google C	Cloud serv	vice identity, such as code	e running on Com	oute Engine VMs, App	p Engine apps,	or systems running out	tside Google. <mark>Lea</mark>	m more a	bout ser	vice ad	counts.		
٩	Policy Troubleshooter	Organizat about ser	tion policies can be used to sec rvice account organization polic	cure servi cies.	ce accounts and block ris	sky service accou	nt features, such as a	utomatic IAM	Grants, key creation/up	load, or the creat	on of ser	vice acco	ounts e	ntirely. Le	earn mo	re
E,	Policy Analyzer													-		
	Organization Policies	Ŧ	ilter Enter property name or	r value	0	N	Bernsteller	M	Marca and an allow	Barrista		•		0		
<u>•</u> =	Service Accounts		email e∃ message-retraction-se	ervice-	Status	Message	Area 1	No	Key creation date	Enabled	uelegatic	u U		:	19	
74	Workload Identity Federation		acc@message- retraction.iam.gserviceacc	count.co	m	Retraction Service	Message Retraction	keys		View Client	Mana	ige det	ails			
	Labels					Account					Mana	ige per	missi	ons		
	Tags										Mana	ige key	s			
۵	Settings										View	metric: logs	S			
0	Privacy & Security										Disat	le				
	Identity-Aware Proxy										Delet	e				
	Roles															
	Audit Loop															

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

=	Google Cloud Platform	🕽 Message Retraction 👻 🔍 Search products and resources V 🛛 🛛 🖈 🗄 🙆
θ	IAM & Admin	← Message Retraction Service Account
•=	IAM	DETAILS PERMISSIONS KEYS METRICS LOGS
Θ	Identity & Organization	Keys
٩	Policy Troubleshooter	Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. You
R,	Policy Analyzer	can learn more about the best way to authenticate service accounts on Google Cloud here.
	Organization Policies	Add a new key pair or upload a public key certificate from an existing key pair.
연필	Service Accounts	Block service account key creation using organization policies. Learn more about setting organization policies for service accounts
5	Workload Identity Federation	ADD KEY +
۰	Labels	Create new key
	Tags	Upload existing key
۵	Settings	
Ø	Privacy & Security	

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

Key type JSON Recommended P12 For backward compatibility with code using the P12 format	ant be recovered i	lost.	,		
	ey type JSON Recommended P12 For backward co	mpatibility with cod	le using the P12 forr	nat	

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

DOMAINS & ROUTING     Imail Authorizations       EMAIL POLICIES     Authorizations       ALLOW LIST     - No results to display -       BLOCK LIST     - No results to display -       ENHANCED     - No results to display -       RETRACT SETTINGS     - No results to display -       Introductions     - No results to display -	DOMAINS & ROUTING     EMAIL POLICIES   ALLOW LIST   BLOCK LIST   EMAANCED   DETECTIONS     RETRACT SETTINGS   Authorize Gmail   Authorize Gmail   Authorize Tract		g Network Devices Osers and Accions	SSU Directories Subscriptions	Service Accounts	beregated Accounts		
EMAIL POLICIES     AUTHORIZED DOMAINS     COMMENTS       ALLOW LIST     - No results to display -       BLOCK LIST       ENTANCED DETECTIONS	EMAIL POLICIES     AUTHORIZED DOMAINS     COMMENTS       ALLOW LIST     - No results to display -       BLOCK LIST       ENHANCED DETECTIONS	DOMAINS & ROUTING	Gmail Authorizations			+ New Autho	rization	
ALLOW LIST BLOCK LIST ENHANCED DETECTIONS Authorize 0365 Authorize Gmail Auto-Retract	ALLOW LIST BLOCK LIST ENHANCED DETECTIONS RETRACT SETTINGS Authorize Gmsil Authorize Gmsil Authorize Tat	EMAIL POLICIES	AUTHORIZED DOMAINS	COMMENTS				
BLOCK LIST ENHANCED DETECTIONS RETRACT SETTINGS Authorize 0365 Authorize Gmail Auto-Retract	BLOCK LIST ENHANCED DETECTIONS Authorize 0365 Authorize Gmail Auto-Retract	ALLOW LIST		- No results to displ	ay -			
ENHANCED DETECTIONS RETRACT SETTINGS Authorize 0365 Authorize Gmail Auto-Retract	ENHANCED DETECTIONS RETRACT SETTINGS Authorize 0365 Authorize Gmail Auto-Retract	BLOCK LIST						
RETRACT SETTINGS Authorize 0365 Authorize Gmail Auto-Retract	RETRACT SETTINGS Authorize 0365 Authorize Omsil Auto-Retract	ENHANCED DETECTIONS						
Authorize 0365 Authorize Gmail Auto-Retract	Authorize 0365 Authorize Gmsil Auto-Retract	RETRACT SETTINGS						
Auto-Retract	Auto-Retract	Authorize 0365						
		Auto-Retract						

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

AREA 1 HORIZON Home Emai	1 Web	Add Authorization	×
		RETRACTION-PRIVATEKEY.JSON	
DOMAINS & ROUTING	Gmail Authorizations		
EMAIL POLICIES	AUTHORIZED DOMAINS	JSON FILE ()	
ALLOW LIST		COMMENTS	
BLOCK LIST			
ENHANCED DETECTIONS			
		DOMAINS 🗹 domain.com	
RETRACT SETTINGS		+ Save	
Auto-Retract			

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

DOMAINS & ROUTING	Gmail Authorizations			+ New Autho	rizatio	m	
EMAIL POLICIES	AUTHORIZED DOMAINS	COMMENTS					
ALLOW LIST	domain.com	Corporate Dom	ain				
BLOCK LIST							
ENHANCED DETECTIONS							
RETRACT SETTINGS							
Authorize 0365							
Auto-Retract							

### **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:

 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:

DOMAINS & ROUTING	Auto-retrac	t				••• Edit
EMAIL POLICIES	Manage automatic using BCC or Jou the folders you	c retract (clawback) s urnaled mechanisms. Me specify below.	ettings here. Use s ssages matching you	his feature when you ir selected dispositi	are delivering mes on(s) will get auto	sages to Area 1 matically moved to
ALLOW LIST						
BLOCK LIST	DISPOSITION	NO ACTION	TRASH	JUNK EMAIL	SOFT DELETE (USER RECOVERABLE)	HARD DELETE (ADMIN RECOVERABLE)
ENHANCED	Malicious	0	-	-	-	-
DETECTIONS	Spam	0	-	-	-	-
RETRACT SETTINGS	Bulk	0	-	-	-	-
Authorize Gmail	Suspicious	0	-	-	-	-
Auto-Retract	Spoof	0	-	-	-	-
	Phish Submi	ssion Response	ponse enabled, Hori	zon will automatical:	ly retract messages	reported by your

**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**:

	N Home Email	Web Landscape			Change Auto-	retract Settings	×
Email Configurat:	ion Web Config ——			Directories	MALICIOUS	Trash *	
DOMAINS	& ROUTING	Auto-retrac	t		SPAM	Junk Email *	
EMAIL PO		Manage automatic using BCC or Jou	retract (clawback) s	ettings here ssages match:	BULK	Junk Email *	
ALLOW LI		the folders you	specity below.		SUSPICIOUS	No Action *	
BLOCK LI		DISPOSITION	NO ACTION	TRASH	SPOOF	No Action *	
ENHANCED		Malicious		-		Update Auto-retract Settings	
		Spam		-			
RETRACT	SETTINGS	Bulk		-			
Authoriz	e Gmail	Suspicious		-			
Auto-Ret		Spoof					
		Phish Submi	ssion Response				
		With users user	Phish Submission Resp s that are found to be as an additional neur	onse enabled malicious. on into our			

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

11 Configuration Web Config	g Network Devices Us	ers and Actions SSO	Directories Sub	scriptions Service A	ccounts Delegated Ac	counts	
DOMAINS & ROUTING	Auto-retrac	t				••• Edit	
EMAIL POLICIES	Manage automatic using BCC or Jou the folders you	retract (clawback) s rnaled mechanisms. Me specify below.	ettings here. Use ssages matching yo	this feature when you ur selected dispositi	u are delivering mes ion(s) will get auto	sages to Area 1 matically moved to	
ALLOW LIST	DISPOSITION	NO ACTION	TRASH	JUNK EMAIL	SOFT DELETE (USER RECOVERABLE)	HARD DELETE (ADMIN RECOVERABLE)	
ENHANCED	Malicious	-	0	-	-	-	
DETECTIONS	Spam	-	-	0	-	-	
RETRACT SETTINGS Authorize 0365	Bulk	-	-	0	-	-	
Authorize Gmail	Suspicious	0	-	-	-	-	
	Spoof	0	-	-	-	-	
	Phish Submi	ssion Response Phish Submission Resp that are found to bu as an additional neur	ponse enabled, Hori e malicious. This f ron into our neural	zon will automatical eature uses machine network.	ly retract messages learning margin scor	reported by your es by adding the	

### 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:

AREA1 HORIZON Home Er	nail Web			Q Search	- 0	• • •
Email Configuration Web Config	Network Devices	Users and Actions SSO	Directories Subs	criptions Service Accounts	Delegated Accounts	
DOMAINS & ROUTING	All Domains	3		Q Search	1	New Domain
Alert Webhooks	DOMAIN	FORWARDING TO	POSITION	RESTRICTED IPS	TLS	
Partner Domains ILS	company.com	google.com	MX Record		Inbound Outbound	• ···
EMAIL POLICIES						
ALLOW LIST						
BLOCK LIST						
ENHANCED DETECTIONS						
RETRACT SETTINGS						

• 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.

Edit Domain		×
DOMAIN	company.com	
CONFIGURED AS	O MX Records   Hops 2	
FORWARDING TO	google.com	
() IP RESTRICTIONS		
INBOUND TLS		
OUTBOUND TLS	FORWARD ALL MESSAGES OVER TLS	
QUARANTINE POLICY	<ul> <li>Malicious <sup>1</sup></li> <li>Spam <sup>1</sup></li> <li>Suspicious <sup>1</sup></li> <li>Spoof <sup>1</sup></li> </ul>	
	Update Domain	

**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:

≡ Google Admin	earch for users, groups, and settings (e.g. contact support)		8	?		
Apps > G Suite > Settings for Gmail					Z	:
Apps > G Suite > Settings for Gmail	Image: Strategy of the strategy	✓ EDIT SERVICE				
	Spam, Phishing and Malware Configure spam, phishing and malware features					
	Compliance Configure compliance features Advanced settings > Access other settings for controlling mail flow for the domain.					

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

≡ Google Admin Q Sear	ch for users, groups or settings	0	? ₩
Apps > Google Workspace > Settings for Gma	<ul> <li>Compliance</li> <li>Appena tooter</li> </ul>	Set up outbound tooter text for legal compliance; informational or promotional requirements.	CONFIGURE
M Gmail		Changes may take up to 24 hours to propagate to all users.     Prior changes can be seen in Audit log	
Status ON for everyone	Restrict delivery	Restrict the domains that your users are allowed to exchange email with.	CONFIGURE
Organizational Unit		Changes may take up to 24 hours to propagate to all users.     Prior changes can be seen in Audit log	
Search for organizational units	Content compliance	Configure advanced content filters based on words, phrases or patterns.	CONFIGURE
-		Changes may take up to 24 hours to propagate to all users.     Prior changes can be seen in Audit log	
	Objectionable content	Configure content filters based on word lists.	CONFIGURE
		Changes may take up to 24 hours to propagate to all users. Prior changes can be seen in Audit log	
	Attachment compliance	Configure attachment filters based on file type, file name and message size.	CONFIGURE
		Changes may take up to 24 hours to propagate to all users.     Prior changes can be seen in Audit log	
	Secure transport (TLS) compliance	0	

- 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

Add setting	
Content compliance	Learn more
Area 1 - Bcc	
<ol> <li>Email messages to affect</li> <li>Inbound</li> <li>Outbound</li> <li>Internal - Sending</li> <li>Internal - Receiving</li> </ol>	

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 <u>https://regexr.com/</u>.

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. <u>bcc\_recipient@mxrecord.io</u>
  - This address is specific to each customer tenant and can be found in your Portal at <u>https://horizon.area1security.com/support/service-addresses</u>

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. <u>bcc\_recipient@mailstream-eu1.mxrecord.io</u>

Edit setting				
Advanced 🔻				
Apply the above modifications, plus the following:				
Route				
Change route				
Envelope recipient				
Change envelope recipient				
Replace recipient				
bcc_recipient@mxrecor d.io				
O Replace username				
Enter new username				
O Replace domain				
Enter new domain				
Sham and delivery entions				
	CANCEL	SAVE		

- 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"

Edit setting		
O Replace domain		
Enter new domain		
Spam and delivery options		
Do not deliver spam to this recipient		
Suppress bounces from this recipient		
Headers		
Add X-Gm-Original-To header		
Add X-Gm-Spam and X-Gm-Phishy headers		
Add custom headers		
Subject		
Prepend custom subject		
Attachments		
Remove attachments from message		
	CANCEL	SAVE

- vii. Click SAVE to save your settings
- 8. Scroll to the bottom and select "Show options"
  - a. Under Account types to affect check "Groups"

Add setting		
Encryption (onward delivery only)		
Require secure transport (TLS)		
Hide options		
A. Address lists		
Use address lists to bypass or control application of this setting		
O Bypass this setting for specific addresses / domains		
Only apply this setting for specific addresses / domains		
P. Account turned to officiat		
B. Account types to affect		
Vusers		
Groups		
Unrecognized / Catch-all		
C. Envelope filter		
Only affect specific envelope senders		
Only affect specific envelope recipients		
	CANCEL	SAVE

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.

 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:

AREA 1 HORIZON	$\boldsymbol{Q}$ Detection Search $^{\scriptscriptstyle (2)}$	Date Range: 4/11/2021 12:00 AM - 5/11/2021 12:00 AM 🗙
	Detection Search 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:

AR	EA1 HORIZON	Q	Mail Trace *	Subject: (substring)	Date Range: 5/11/2021 12:00 AM =//:	×
			Recipient: (exact	:) Sender: (exact)	Message ID: (exact)	
	DATE/DISPOSIT	ION		SUBJECT	SENDER/RECIPIENT(S)	
	05/11/21 14 NO DETECTIO	:20 N	PDT	21:20-20210511 testing waugh	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishinguaar com In View Details	
	05/11/21 14	:10 N	PDT	21:10-20210511 testing congressist	Sender: dmarc-operations@arealsecuri  Recipient(s): rsa2020demo@nophishing  Preview	
	05/11/21 14 SUSPICIOUS	:00	PDT	Life is like a box of chocolates Pearl	Sender: dmarc-operations@arealsecuri Recipient(s): rsa2020demo@nophishingway.com	
	95/11/21 14	·aa	PDT		Sender: dmarc-operations@arealsecurity.com	

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:

AREA1 HORIZON Q Mail Trace * Subject: (substring) Date Range: 5/11/2021 12:00 AM//				Date Range: 5/11/2021 12:00 AM =// 🗙
	Recipient: (exact		ct) Sender:(exact)	Message ID: (exact)
	DATE/DISPOSIT	TION	SUBJECT	SENDER/RECIPIENT(S)
	05/11/21 14 NO DETECTIO	1:20 PDT	21:20-20210511 testing waugh	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
0	05/11/21 14 NO DETECTIO	1:10 PDT	21:10-20210511 testing congressist	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 14 SUSPICIOUS	:00 PDT	Life is like a box of chocolates Pearl	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 14 NO DETECTIO	1:00 PDT	21:00-20210511 testing Acipenseroidei	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 13 NO DETECTIO	1:50 PDT	20:50-20210511 testing apathistical	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 13 NO DETECTIO	1:40 PDT	20:40-20210511 testing uncolleged	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 13 SUSPICIOUS	:30 PDT	Life is like a box of chocolates Pearl	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 13 NO DETECTIO	1:30 PDT	20:30-20210511 testing religion	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 13 NO DETECTIO	1:20 PDT	20:20-20210511 testing screamer	Sender: dmarc-operations@arealsecurity.com Recipient(s): rsa2020demo@nophishingway.com
	05/11/21 13 NO DETECTIO	1:10 PDT	20:10-20210511 testing Naharvali	Sender: dmarc-oper Recipient(s): rae2 The message was successfully retractéd.
	05/11/01 10	LOG DOT		Condex, James