

## **Email Security for Gmail**

**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: Add Area 1 IP addresses to the Inbound gateway configuration
- Step 2: Quarantine malicious detections
- Step 3: Update your domain MX records
- Step 4: Secure your email flow
- Step 5: Send Area 1 SPAM to user spam folder (optional)

#### Requirements

- Provisioned Area 1 Account
- Access to the Gmail administrator console (<u>https://admin.google.com</u> > Apps > Google Workspace > Gmail)
- Access to the domain nameserver hosting the MX records for the domains that will be processed by Area 1

# Step 1: Add Area 1 IP addresses to the Inbound gateway configuration

When Area 1 is deployed as MX records upstream of Gmail, the Inbound gateways need to be configured such that Gmail is aware that they are no longer the MX record for the domain. This is a critical step as it will allow Gmail to accept messages from Area 1.

 Access the Gmail Administrative Console (<u>https://admin.google.com/</u>), then select Apps > Google Workspace > Gmail:

≡ Google Admin Q	Search for users, groups or settings	4 Z Ø	•
🕶 🏭 Apps	Apps > Google Workspace > Settings for	or Gmail	
Overview - Google Workspace	M Gmail	Service status ON for everyone	~
Calendar Cloud Search Currents	Status ON for everyone	User settings Set name formats. Enable user preferences such as themes, read receipts, and email delegation.	~
Drive and Docs		Hosts	~
Gmail Google Chat and classic Hangouts		Add mail hosts for use in advanced routing, such as to direct messages to Microsoft Exchange.	
Google Meet			
Google Vault		Default routing	~
Groups for Business		Create domain-wide routing rules, such as for split delivery or a catchall address.	
Jamboard			_
Keep		Authenticate email	~
Sites		Set up email authentication (DKIM)	
Tasks			_
Additional Google services		Manage quarantines	~
Web and mobile apps		Create, modify, or remove email quarantines.	
Google Workspace Marketplace apps			
LDAP		Safety	~
Password vaulted apps		Configure email and spam safety features	

2. In the Gmail console, navigate and click on to the **Spam**, **Phishing**, **and Malware** section to access the **Inbound Gateway** configuration section:

≡ Google Admin	λ Search for users, groups or setting	IS	¢	8	0		
→ III Apps	Apps > Google Workspace > Settings	for Gmail					
Overview		Create, modify, or remove email quarantines.					
✓ Google Workspace	M Gmail	0.64					
Service status		Safety				~	
Calendar	Status	Configure email and spam safety features					
Cloud Search	ON for everyone					_	
Currents		Setup				~	
Drive and Docs		Configure setup features					
Gmail							
Google Chat and classic Hangouts		End User Access				~	
Google Meet		Configure end user access features					ł
Google Vault							
Groups for Business		Spam. Phishing and Malware				~	
Jamboard							
Кеер		Configure spam, phishing and malware features					
Sites							1
Tasks		Compliance				~	
Additional Google services		Configure compliance features					
Web and mobile apps							
Google Workspace Marketplace apps		Routing				~	
LDAP		Configure routing features					
Password vaulted apps			_	_			

3. Find and **Enable** the **Inbound Gateway** area. Configure the **Inbound Gateway** with the following details and click **SAVE** button at the bottom of the dialog box to save the configuration once the details have been entered.

=	Google Admin Q	Search for users, groups or setting	s	А 8 © III 💮
	Google Admin     Q     Search for users, groups or setting     Apps > Google Workspace > Settings     Directory     Directory     Directory     Google Workspace     Service status     Calendar     Cloud Search     Ourrents		s for Graail > Spam, phishing, and Spam, phishing, and Email whitelist Applied at Somedemocorp.com? Enhanced pre-delivery Applied at Somedemocorp.com?	A R      O     H
	Drive and Docs Gmail Google Chat and classic Hangouts Google Meet			Enable     Most changes take effect in a few minutes. Learn more     You can view prior changes in the Audit tog     CANCEL SAVE
	Google Vault Groups for Business Jamboard		Spam	Create approved senders lists that bypass the spam folder.
	Keep Sites			Wous changes take errect in a new minutes. Learn Mote You can view prior changes in the Audit log
	Tasks Additional Google services		Blocked senders	Block or approve specific senders based on email address or domain. CONFIGURE

- Gateway IPs
  - Click on the **Add** link to add the following IPs:
    - **52.11.209.211**
    - **52.89.255.11**
    - **52.0.67.109**
    - **54.173.50.115**
    - 158.51.64.0/26
    - 158.51.65.0/26
    - 134.195.26.0/24
    - 52.58.35.43 (EU, if required)
    - 35.157.195.63 (EU, if required)
- Select Automatically detect external IP (recommended)
- Select Require TLS for connections from the email gateways listed above

	. Gateway IPS	
	IP addresses / ranges	
	52.11.209.211	
	52.89.255.11	
	52.0.67.109	
	54.173.50.115	
	158.51.64.0/26	
	158.51.65.0/26	
	134.195.26.0/24	
		ADD
	<ul> <li>Automatically detect external IP (recommended)</li> </ul>	
	Reject all mail not from gateway IPs	
	Require TLS for connections from the email gateways listed above	/e
2	2. Message Tagging	
	Message is considered spam if the following header regexp mate	ches
	Most changes take effect in a few minutes. Learn more	

**Note:** Do not select **Reject all mail not from gateway IPs** until the MX records have fully propagated. Reference step 4 of this guide for more details.

4. Once saved, the administrator console will show the **Inbound Gateway** as enabled.



#### **Step 2: Quarantine malicious detections**

This optional step is highly recommended to prevent users from being exposed to malicious messages.

When messages are identified as malicious, Area 1 Horizon will insert the X-header **X-Area1Security-Disposition** into the message with the corresponding disposition. Based on the value of the **X-Area1Security-Disposition**, a **content compliance** filter can be configured to send malicious detections to an administrative quarantine. This section will outline the steps required to:

- Create an Area 1 Malicious quarantine
- Create the content compliance filter to send malicious messages to quarantine

#### **Create Area 1 Malicious Quarantine**

If you would like to send Area 1 malicious detection to a separate quarantine other than the default quarantine, you will need to create a new quarantine.



1. In the Gmail administrative console, select Manage quarantines panel:

2. Click the **ADD QUARANTINE** button to configure the new quarantine. This will bring up a pop-up for the configuration details.

	Google Admin	Q Search for users, groups or settin	ngs			¢	8	0	
ŵ	Home	Apps > Google Workspace > Setting	s for Gmail > Manage quarantines						
먊	Dashboard		Manage quarantines						^
۰ °	Directory	M Gmail	Manage quarantines						
• [0	Devices			Name	Description		A	ctions	
<b>-</b> Ⅲ	Apps	ON for everyone		Default			E	dit	
	Overview				GO TO ADMIN	QUARA	NTINE	ADD QU	ARANTINE
	Google Workspace			Most changes take e	ffect in a few minutes. Learn mo	re			
	Service status			You can view prior ch	anges in the Audit log				
	Calendar						0	ANCEL	SAVE
	Cloud Search							ANGLE	UNVL
	Currents								

- 3. In the quarantine configuration pop-up, enter the following and **SAVE** the new quarantine:
  - Name: Area 1 Malicious
  - Description: Area 1 Malicious
  - For the Inbound denial consequence, select Drop Message
  - For the Outbound denial consequence, select Drop Message

Add quarantine	
Name *	
Area 1 Malicious	
This field is required.	
Description	
Area 1 Malicious	
Quarantine reviewers group	Manage Groups
Learn more	
Select Groups	
If a group is not set or does not exist, then only super admins or o	delegated admins with
privilege "Access Admin Quarantine" can review the quarantine.	
Inbound denial consequence	
Drop Message	
Sand the default reject message	
Send the default reject message	
Outbound denial consequence	
Drop Message	
Send the default reject message	
Notify periodically when messages are quarantined	
Learn more	
It may take several minutes for changes to propagate	
n may take several minutes for changes to propagate.	
	CANCEL SAVE

 To access the newly create quarantine, click the GO TO ADMIN QUARANTINE button or access the quarantine directly by pointing your browser to <u>https://email-quarantine.google.com/adminreview</u>

=	Google Admin	Q Search for users, groups or set	lings		4	n 8 @	
ŵ	Home	Apps > Google Workspace > Setti	ngs for Gmail > Manage quarantines	3			
₽₿	Dashboard		Manage quarantines				^
• 8	Directory	Gmail	Manage guarantines				
• [0	Devices			Name	Description	Actions	
- III	Apps	Status ON for everyone		Default		Edit	
	Overview		_	Area 1 Malicious	Area 1 Malicious	Delete - Ed	it
	Google Workspace				GO TO ADMIN QUA	RANTINE ADD	UARANTINE
	Service status						
	Calendar			You can view prior changes	s in the Audit log		
	Cloud Search						
	Currents					CANCEL	SAVE
	Drive and Docs						

Once in the Admin quarantine console, you can access the **Area 1 Malicious** quarantine by clicking the corresponding quarantine on the left navigation section

≡ Admin Quarantine	Q Search for messages	?	•
All Quarantines Area 1 Malicious			
Denied Allowed			
Help Send feedback	No quarantined messages.		
Revert to the previous version			

Quarantined messages can be released as needed by an administrator.

# Create a content compliance filter to send malicious messages to quarantine

1. To configure the **content compliance filter** access the **Compliance** configuration panel:

≡ Google Admin	Q Search for users, groups or set	tings	Ģ	8	0	
✓ Ⅲ Apps Overview	Apps > Google Workspace > Settin	ngs for Gmail Create, modify, or remove email quarantines.				
✓ Google Workspace Service status	M Gmail	Safety				~
Calendar	Status ON for everyone	Configure email and spam safety features				
Currents		Setup				~
Drive and Docs		Configure setup features				
Google Chat and classic Hangouts		End User Access				~
Google Meet Google Vault		Configure end user access features				
Groups for Business		Spam, Phishing and Malware				~
Jamboard Keep		Configure spam, phishing and malware features				
Sites		Compliance				~
Tasks Additional Google services		, Configure compliance features				
Web and mobile apps Google Workspace		Routing				
Marketplace apps		Configure routing features				•
Password vaulted apps						

2. In the **Compliance** section, navigate to the **Content compliance** area and click the **CONFIGURE** button to start the configuration:



A configuration dialog will pop-up for the configuration details.

- 3. In the **Content compliance filter** configuration, enter the following:
  - Name: Quarantine Area 1 Malicious
  - In the Email message to affect section, select Inbound
  - In the Add expression that describe the content you want to search for in each message section, configure the following:
    - Click **Add** to add the condition
      - Match drop down, select Advanced content match
      - Location, select **Full headers**
      - Match type, select Contains text
      - Content, enter X-Area1Security-Disposition: MALICIOUS
    - Click **SAVE** to save the condition
  - In the If the above expression match, do the following section, click the action dropdown and select Quarantine message and select the Area 1 Malicious quarantine that was created in the previous step.

Add setting
1. Email messages to affect
✓ Inbound
Outbound
Internal - Sending
Internal - Receiving
2. Add expressions that describe the content you want to search for in each message If ANY of the following match the message $^{\!$
Expressions
Location: Full headers
Contains text. A Area (Security-Disposition: MALICIOUS
ADD
3. If the above expressions match, do the following Quarantine message 💌
Move the message to the following quarantine:
Area 1 Malicious 👻
Notify sender when mail is quarantined (onward delivery only)
CANCEL SAVE

• Once configured, click the **SAVE** button to save the content compliance filter

4. Once saved, the console will update with the newly configured **content compliance filter**.

≡ Google Admin	Q Search for users, groups or settings		¢ 8 ⊚ ₩ 🜑
A	Apps > Google Workspace > Settings f	or Gmail > Compliance	
E Home		Append footer	Set up outbound footer text for legal compliance, informational or promotional
Dashboard	M Gmail		CONFIGURE
Directory	Ginai		Most shannes take offert is a few minutes. Leave more
Devices			Vous changes take effect in a tew minutes. Learn more You can view prior changes in the Audit log
✓ ₩ Apps	Status ON for everyone		
Overview		Restrict delivery	Restrict the domains that your users are allowed to exchange email with.
▼ Google Workspace	Organizational Unit		CONFIGURE
Service status	Search for organizational u		Most changes take effect in a few minutes. Learn more You can view prior changes in the Audit log
Calendar	-		
Cloud Search		Content compliance	
Currents			Description Status Source Actions
Drive and Docs			Quarantine Area 1 Malicious Enabled Locally applied Edit - Disable - Delete
Gmail			ADD ANOTHER RULE
Google Chat and classic Hangouts			Most changes take effect in a few minutes. Learn more     You can view prior changes in the Audit log
Google Meet			
Google Vault		Objectionable content	Configure content filters based on word lists.
Groups for Business			CONFIGURE
Jamboard			Most changes take effect in a few minutes. Learn more
Кеер			<ul> <li>You can view prior changes in the Audit log</li> </ul>
Sites		Attachment compliance	Configure attachment filters based on file time, file name and massage size
Tasks		Attachment compliance	Configure attachment mens based on me type, life fidthe and message size.
Additional Google services			Most changes take effect in a few minutes. Learn more

If you'd like to quarantine the other dispositions, simply repeat the above steps and use the following strings for the other dispositions:

- X-Area1Security-Disposition: MALICIOUS
- X-Area1Security-Disposition: SUSPICIOUS
- X-Area1Security-Disposition: SPOOF
- X-Area1Security-Disposition: UCE

If desired, you can create a separate quarantine for each of the dispositions.

**Note:** Google handles Groups (i.e. distributions lists) differently from user mail accounts. The compliance filters actions are limited to "Users" account type. If you heavily use Google Groups (i.e. distribution lists), quarantining malicious messages using the Area 1 quarantine is the recommended method to ensure full protection.

### Step 3: Update your domain MX records

Instructions to update your MX records will depend on the DNS provider you are using. You will want to replace the existing Google MX records with the Area 1 hosts.

MX Priority Host		
1	aspmx.l.google.com.	
5	alt1.aspmx.l.google.com.	
5	alt2.aspmx.l.google.com.	
10	alt3.aspmx.l.google.com.	
10	alt4.aspmx.l.google.com.	

Typical default MX records when using Gmail:

Updated your domain MX records using Area 1:

MX Priority	Host
10	mailstream-east.mxrecord.io
10	mailstream-west.mxrecord.io
50	mailstream-central.mxrecord.mx

When configuring the Area 1 MX records, it's important to configure both hosts with the same MX priority, this will allow mail flows to load balance between the hosts.

For European customers, update your MX records to:

MX Priority	Host
10	mailstream-eu1.mxrecord.io
20	mailstream-east.mxrecord.io
20	mailstream-west.mxrecord.io
50	mailstream-central.mxrecord.mx

The European region will be the primary MX, with a fail-over to the US regions. If you wish to exclusively use the European region, simply update with only the European host. Once the MX records updates complete, the DNS updates may take up to 36 hours to fully propagate around the Internet. Some of the faster DNS providers will start to update records within minutes. The DNS update will typically reach the major DNS servers in about an hour.

#### Step 4: Secure your email flow

After 36 hours, the MX record DNS update will have sufficiently propagated across the Internet. It is now safe to secure your email flow. This will ensure that Gmail only accepts messages that are first received by Area 1. This step is highly recommended to prevent threat actors from using cached MX entries to bypass Area 1 by injecting messages directly into Gmail.

 To secure your deployment, edit the **Inbound gateway** configuration in the Gmail advanced configuration console (see step 1) and enable the **Reject all mail not from gateway IPs** option. Save the configuration to close the dialog. Save once more to commit and activate the configuration change in the Gmail advanced configuration console.

Inbound gateway	If you use email gateways to route incoming email, please enter them here to improve spam handling Learn more
	Enable 1. Gateway IPs
	IP addresses / ranges
	52.11.209.211
	52.89.255.11
	52.0.67.109
	54.173.50.115
	158.51.64.0/26
	158.51.65.0/26
	134.195.26.0/24
	ADD
	Automatically detect external IP (recommended)
	Reject all mail not from gateway IPs
	Require TLS for connections from the email gateways listed above
	2. Message Tagging
	Message is considered spam if the following header regexp matches
	Most changes take effect in a few minutes. Learn more You can view prior changes in the Audit log

#### Step 5: Send Area 1 SPAM to user spam folder (optional)

Unlike the configuration in step 2, where the message can be sent to an administrative quarantine. This optional step can be configured to send messages that are identified as SPAM by Area 1 to the user's **Spam** folder.

- 1. Access the **Inbound gateway settings** from the **Advanced settings** for Gmail (see step 1) and edit the **Inbound gateways**.
- 2. In the **Message Tagging** section, select the **Message is considered spam if the following header regexp matches** to enable the setting.
- 3. In the Regexp section, enter the string X-Area1Security-Disposition: UCE

Inbound gateway If y	If you use email gateways to route incoming email, please enter them here to improve spam handling Learn more
	Enable
	IP addresses / ranges
	52.11.209.211
	52.89.255.11
	52.0.67.109
	54.173.50.115
	158.51.64.0/26
	158.51.65.0/26
	134.195.26.0/24
	ADD
	Automatically detect external IP (recommended)
	<ul> <li>Reject all mail not from gateway IPs</li> <li>Require TLS for connections from the email gateways listed above</li> </ul>
	2. Message Tagging
	Message is considered spam if the following header regexp matches
	X-Area1Security-Disposition: UCE
	Test expression
	Message is spam if regexp matches
	<ul> <li>Regexp extracts a numeric score</li> <li>Disable Gmail spam evaluation on mail from this gateway; only use header</li> </ul>
	value
	Most changes take effect in a few minutes. Learn more     You can view prior changes in the Audit log

4. Click the **SAVE** button to save the updated configuration