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 (https://admin.google.com > 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.

1. Access the Gmail Administrative Console (https://admin.google.com/), then select Apps > Google Workspace > Gmail:
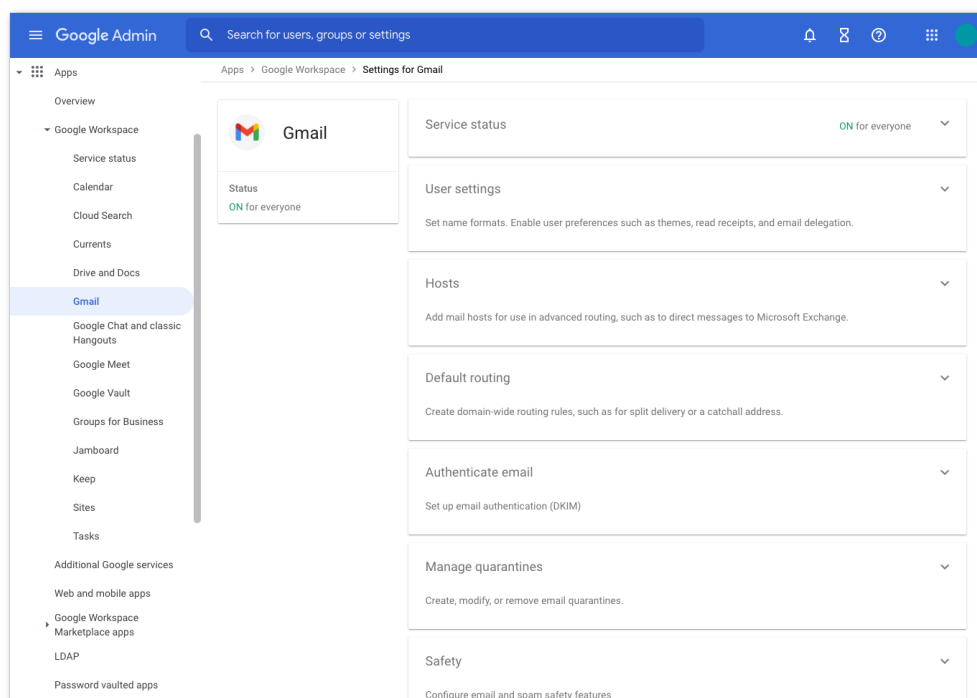
2. In the Gmail console, navigate and click on to the **Spam, Phishing, and Malware** section to access the **Inbound Gateway** configuration section:
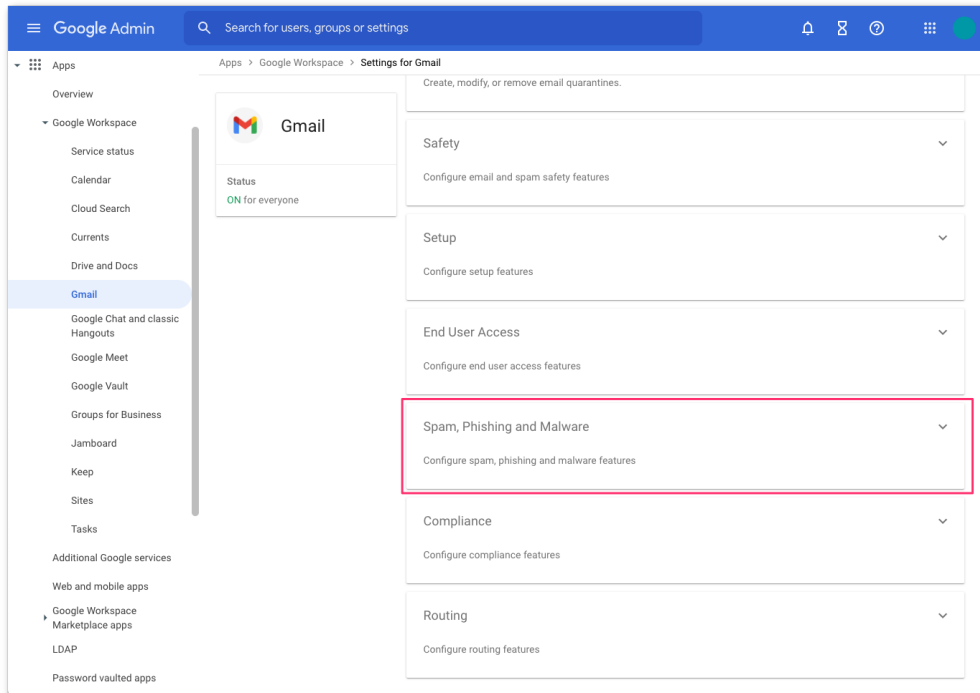
3. Find and **Enable** the **Inbound Gateway** area. Configure the **Inbound Gateway** with the following details and click **SAVE** button at the bottom of the dialog box to save the configuration once the details have been entered.
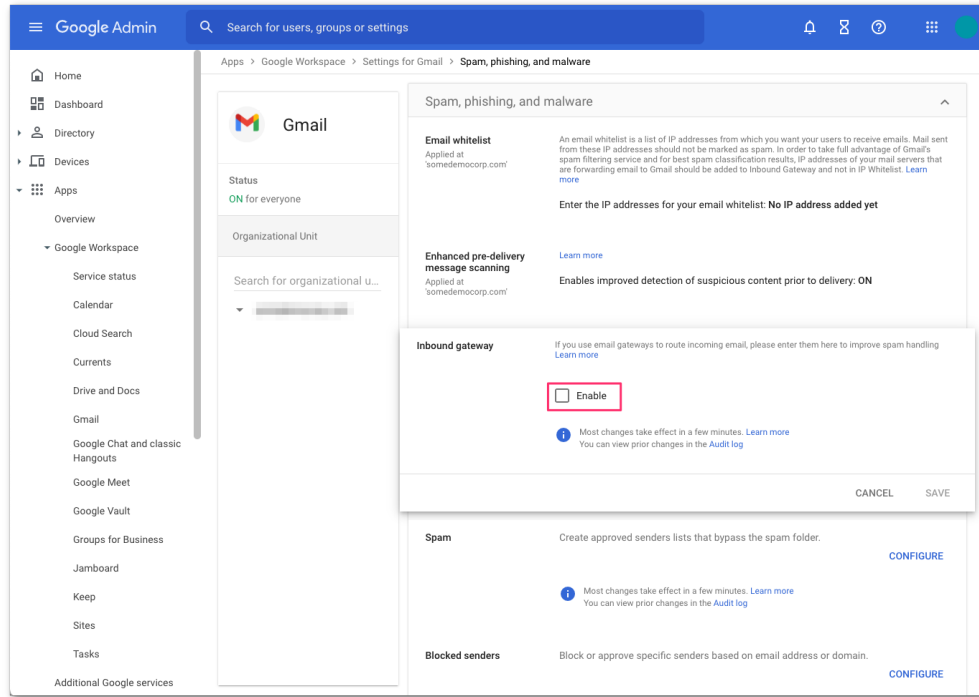
- Gateway IPs
  - Click on the **Add** link to add the following IPs:
    - 52.11.209.211
    - 52.89.255.11
    - 52.0.67.109
    - 54.173.50.115
    - 158.51.64.0/26
    - 158.51.65.0/26
    - 134.195.26.0/24
    - 52.58.35.43 (EU, if required)
    - 35.157.195.63 (EU, if required)

- Select **Automatically detect external IP (recommended)**
- Select **Require TLS for connections from the email gateways listed above**

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.
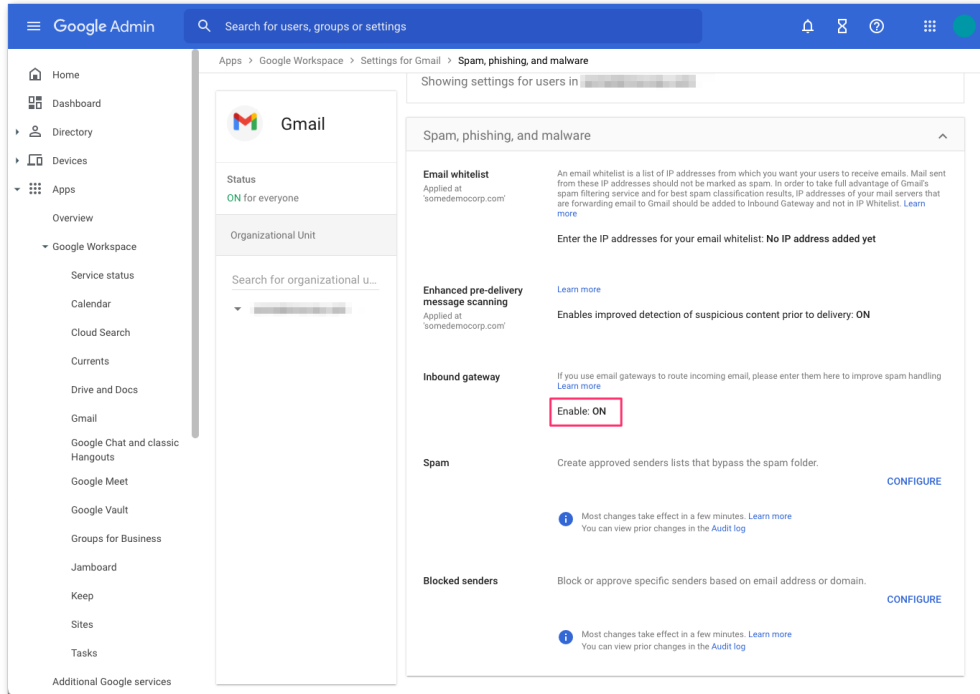
Step 2: Quarantine malicious detections

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
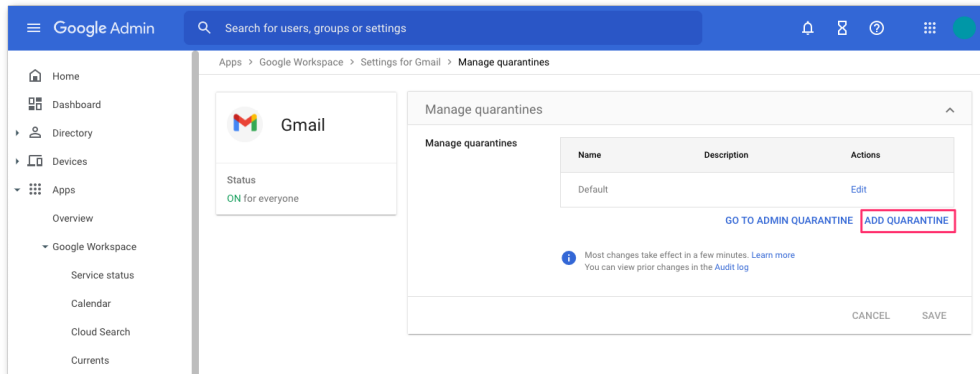
Create Area 1 Malicious Quarantine

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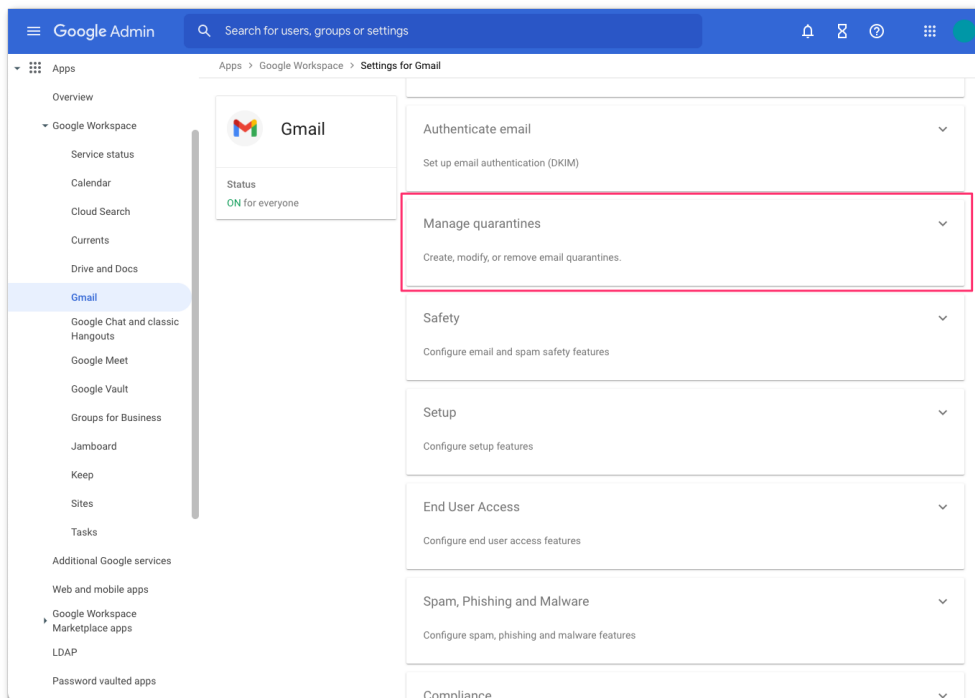
2. Click the **ADD QUARANTINE** button to configure the new quarantine. This will bring up a pop-up for the configuration details.

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**

4. To access the newly create quarantine, click the **GO TO ADMIN QUARANTINE** button or access the quarantine directly by pointing your browser to https://email-quarantine.google.com/adminreview
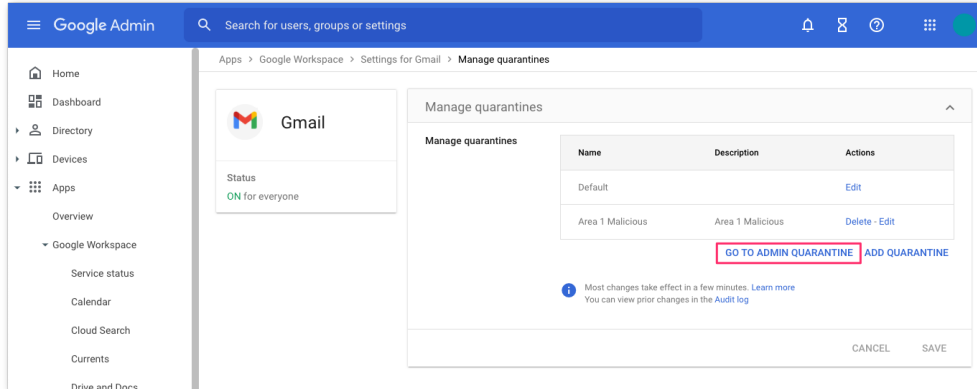
Once in the Admin quarantine console, you can access the **Area 1 Malicious** quarantine by clicking the corresponding quarantine on the left navigation section
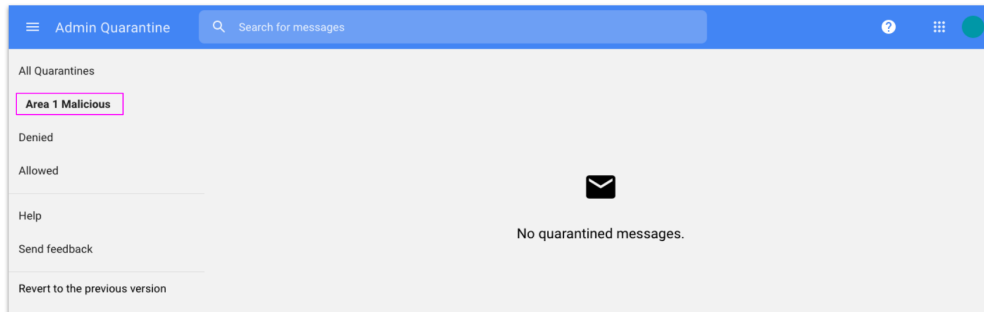
Quarantined messages can be released as needed by an administrator.

Create a content compliance filter to send malicious messages to quarantine

1. To configure the **content compliance filter** access the **Compliance** configuration panel:
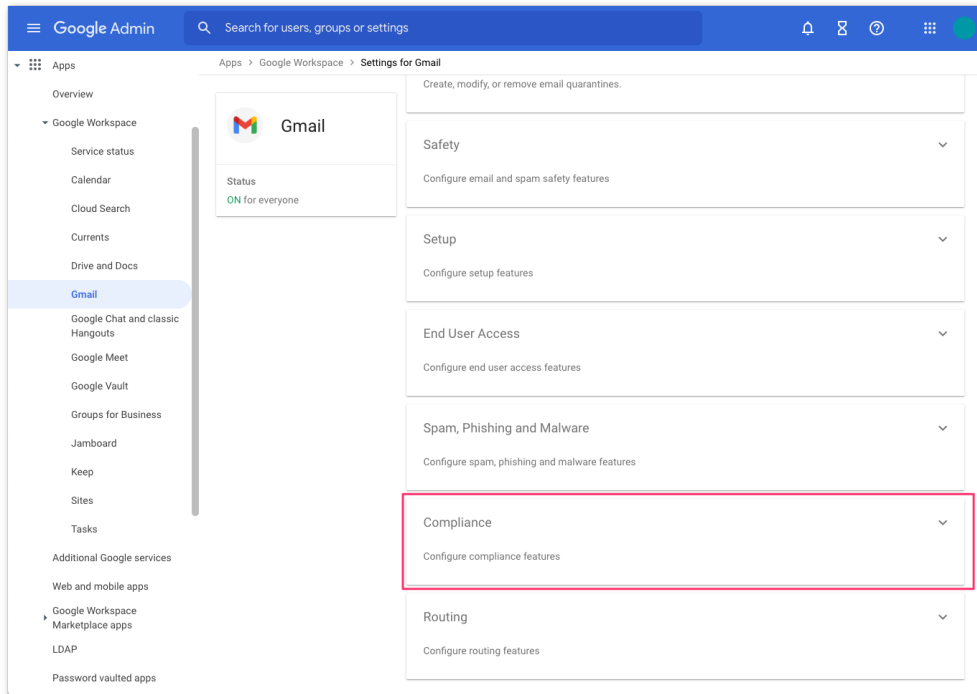
2. In the **Compliance** section, navigate to the **Content compliance** area and click the **CONFIGURE** button to start the configuration:
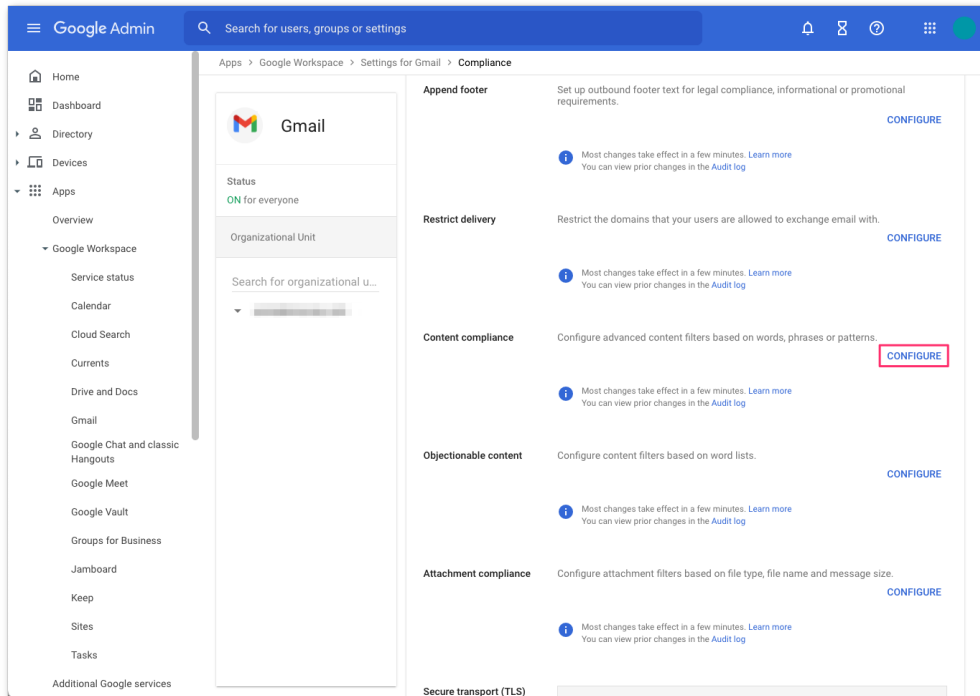

A configuration dialog will pop-up for the configuration details.

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.

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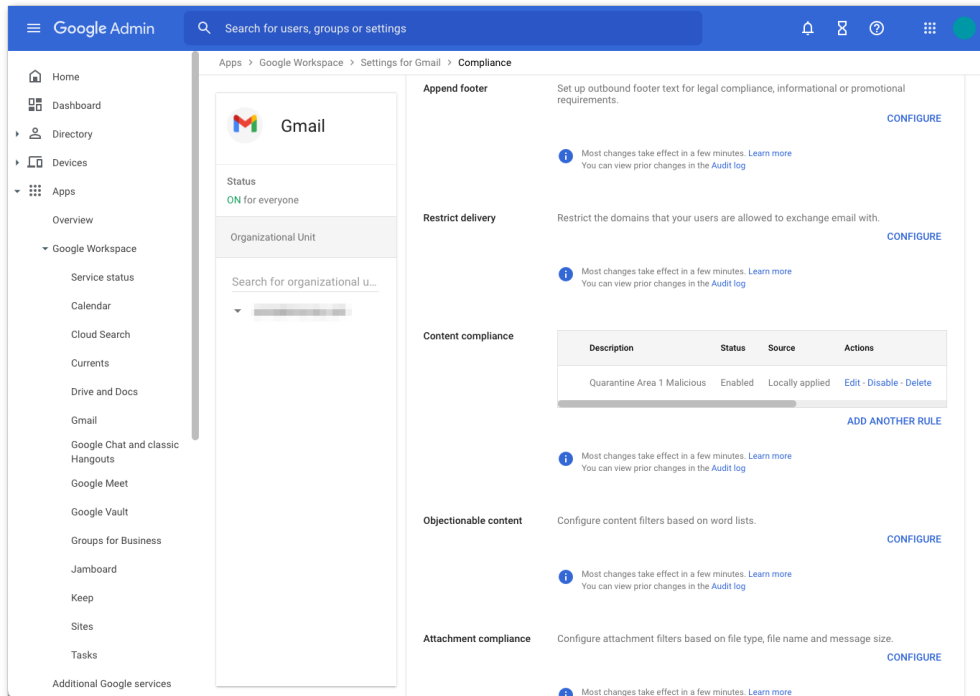
If you'd like to quarantine the other dispositions, simply repeat the above steps and use the following strings for the other dispositions:

- 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.

Typical default MX records when using Gmail:

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.

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.

1. 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.

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**

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