CLOUDFLARE
AREA 1 SECURITY

POV Guide for Google G-Suite

Bcc Mode

Cloudflare Area 1 Overview

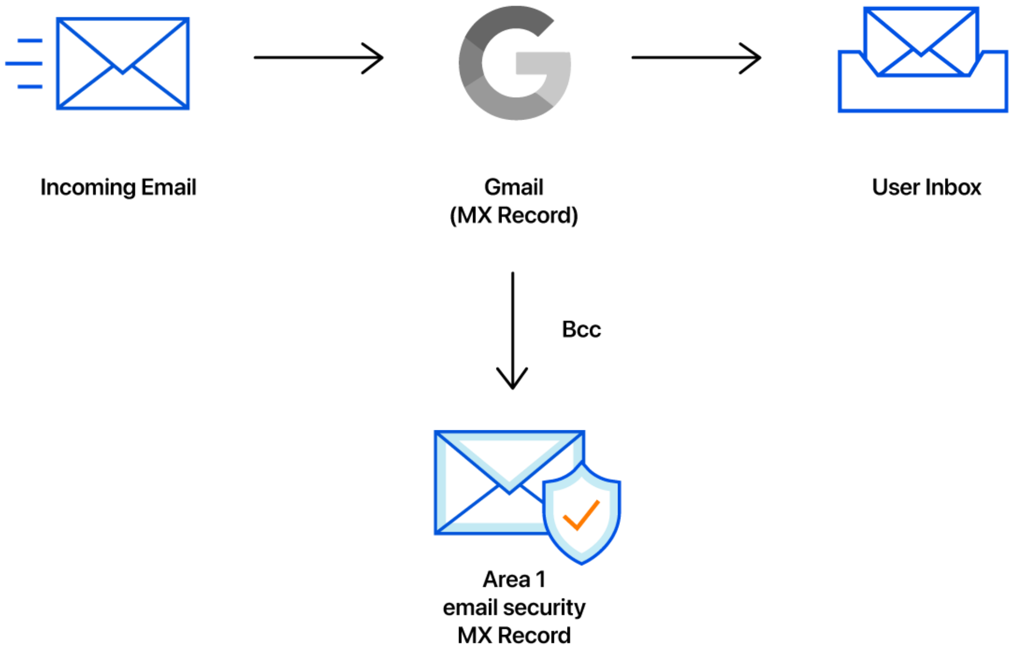
Phishing is the root cause of upwards of 90% of security breaches that lead to financial loss and brand damage. Cloudflare Area 1 is a cloud-native service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors and comprehensive attack analytics, Area 1 email security 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 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.

POV Configuration

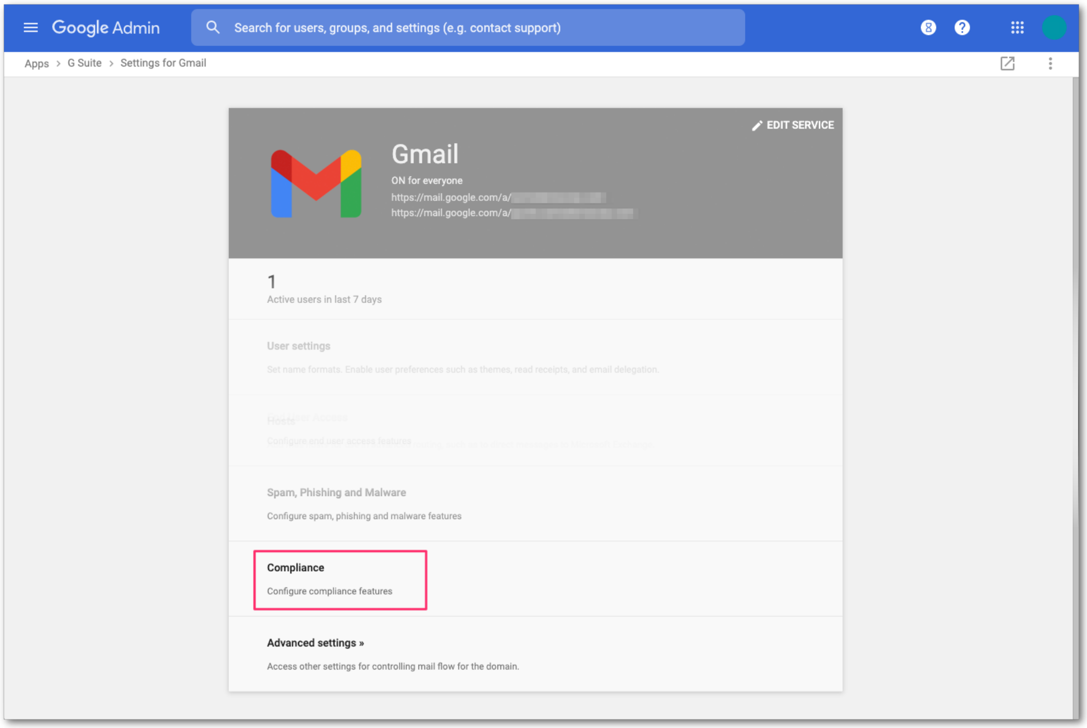
For customers using Gmail, doing a POV with Area 1 for detecting phishing emails is quick and easy to setup as detailed below.

Email Flow During POV



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

Search for users, groups, and settings (e.g. contact support)

Apps > G Suite > Settings for Gmail

EDIT SERVICE

Gmail

ON for everyone

https://mail.google.com/a/[redacted]

https://mail.google.com/a/[redacted]

1

Active users in last 7 days

User settings

Set name formats. Enable user preferences such as themes, read receipts, and email delegation.

End User Access

Configure end user access features

Hosts

Add mail routes for use in advanced routing, such as to direct messages to Microsoft Exchange.

Spam, Phishing and Malware

Configure spam, phishing and malware features

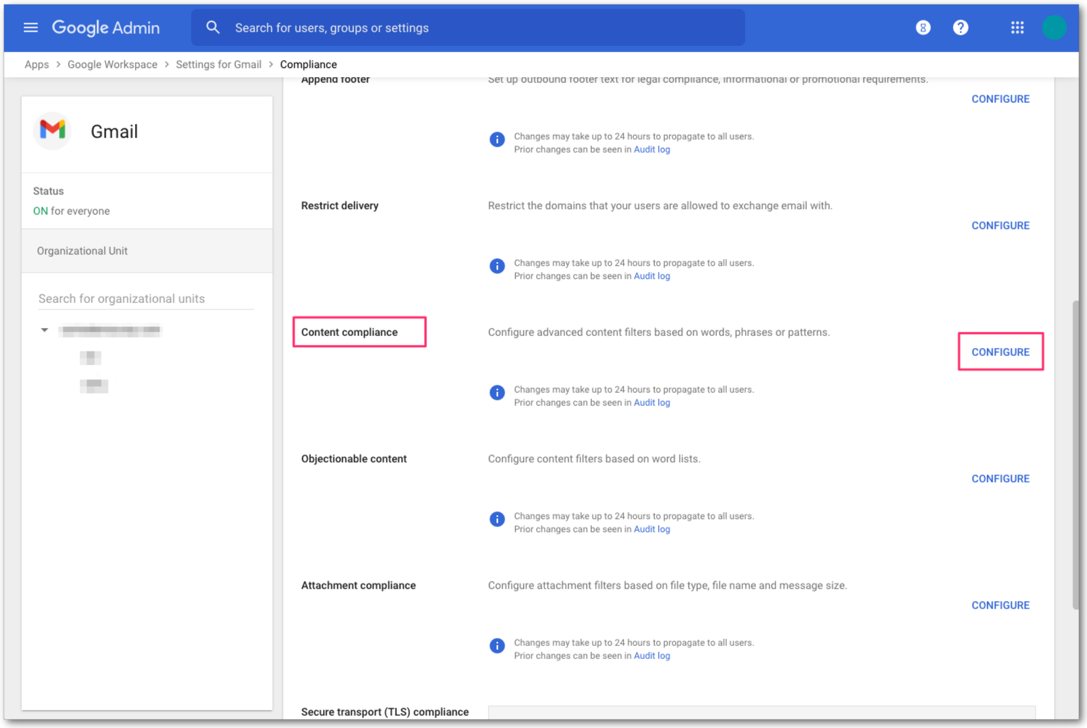
Compliance

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:



Set up outbound footer text for legal compliance, informational or promotional requirements.

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

Restrict the domains that your users are allowed to exchange email with.

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

Configure advanced content filters based on words, phrases or patterns.

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

Configure content filters based on word lists.

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

Configure attachment filters based on file type, file name and message size.

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

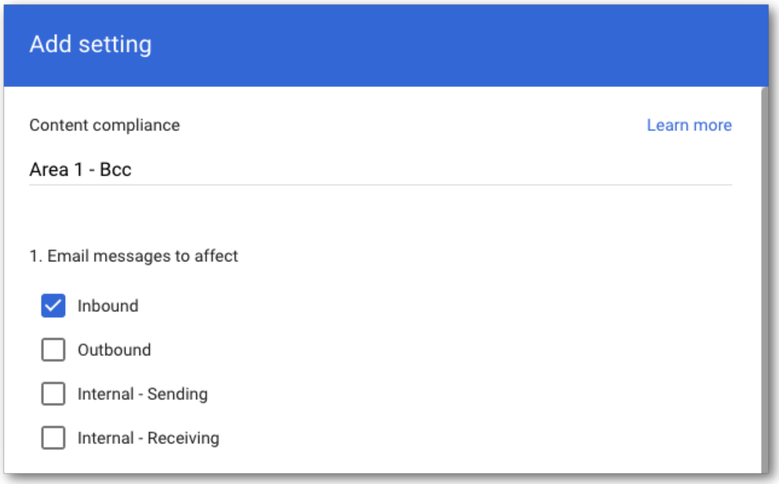
In the Configuration dialog that appears, configure the Bcc compliance rule as follows:

Configuration Steps

- Step 1: Configure Content Compliance Filter

Step 1: Configure the “Content Compliance” filter to Bcc to Area 1

1. Add and name the “Content Compliance” filter: **Area 1 - Bcc**
2. Select “Inbound” for messages to affect



Add setting

Content compliance

Learn more

Area 1 - Bcc

1. Email messages to affect

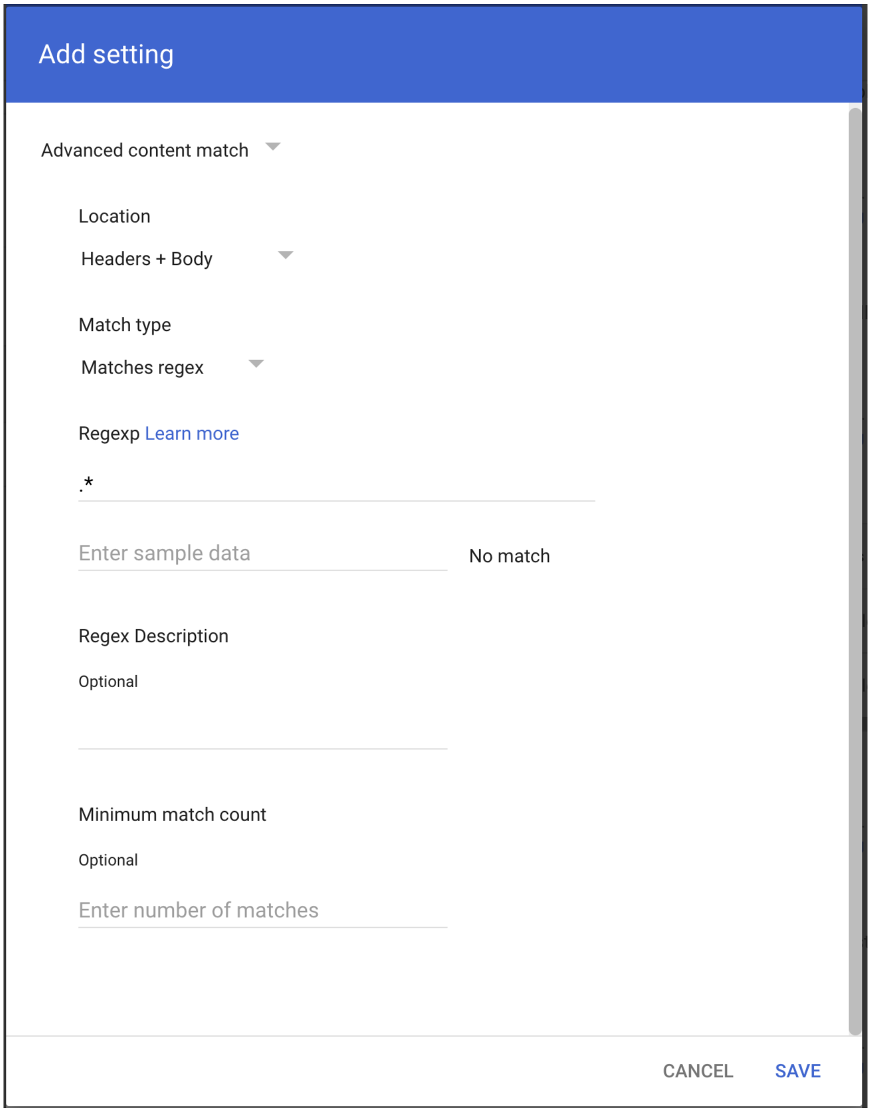
☑ Inbound

□ Outbound

□ Internal - Sending

□ Internal - Receiving

3. 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

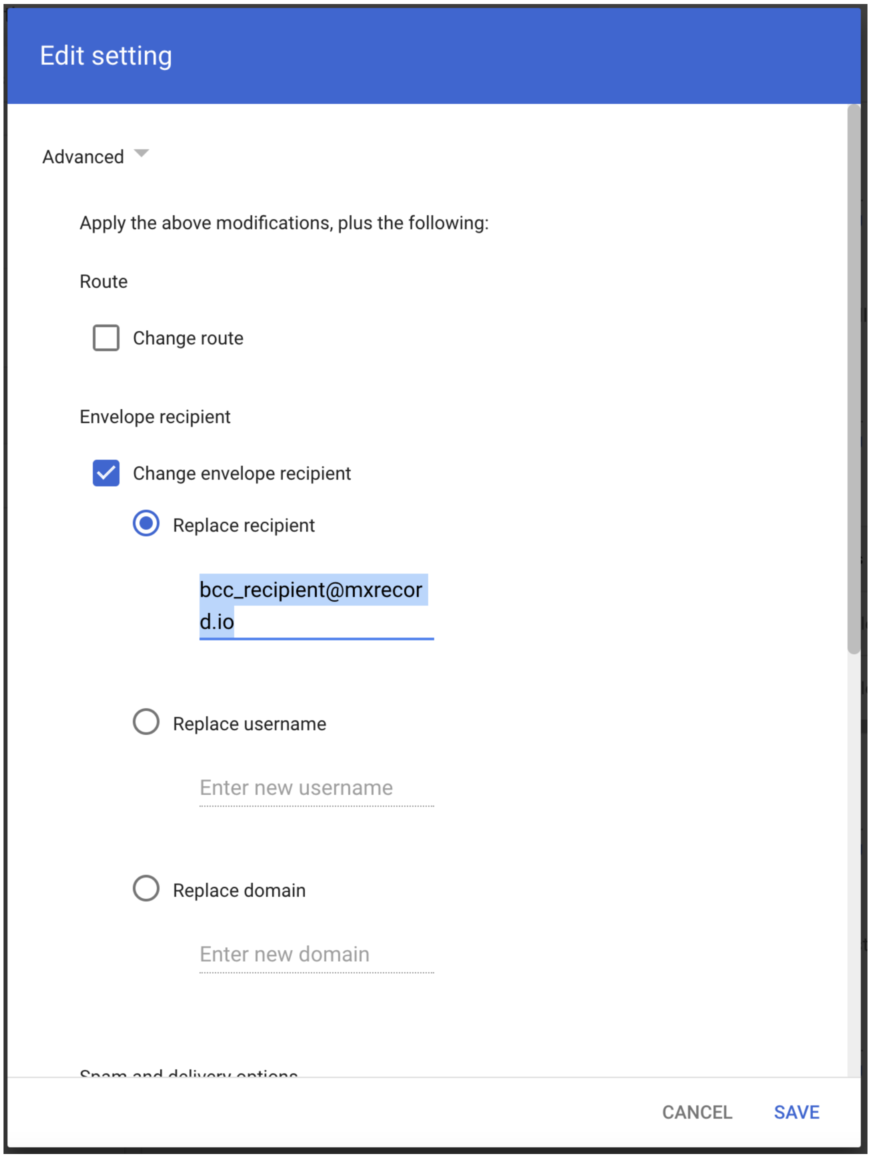
Enter number of matches

CANCEL SAVE

iv. Click SAVE to save your settings

4. 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



Edit setting

Advanced

Apply the above modifications, plus the following:

Route

☐ Change route

Envelope recipient

☑ Change envelope recipient

● Replace recipient

bcc_recipient@mxrecord.io

○ Replace username

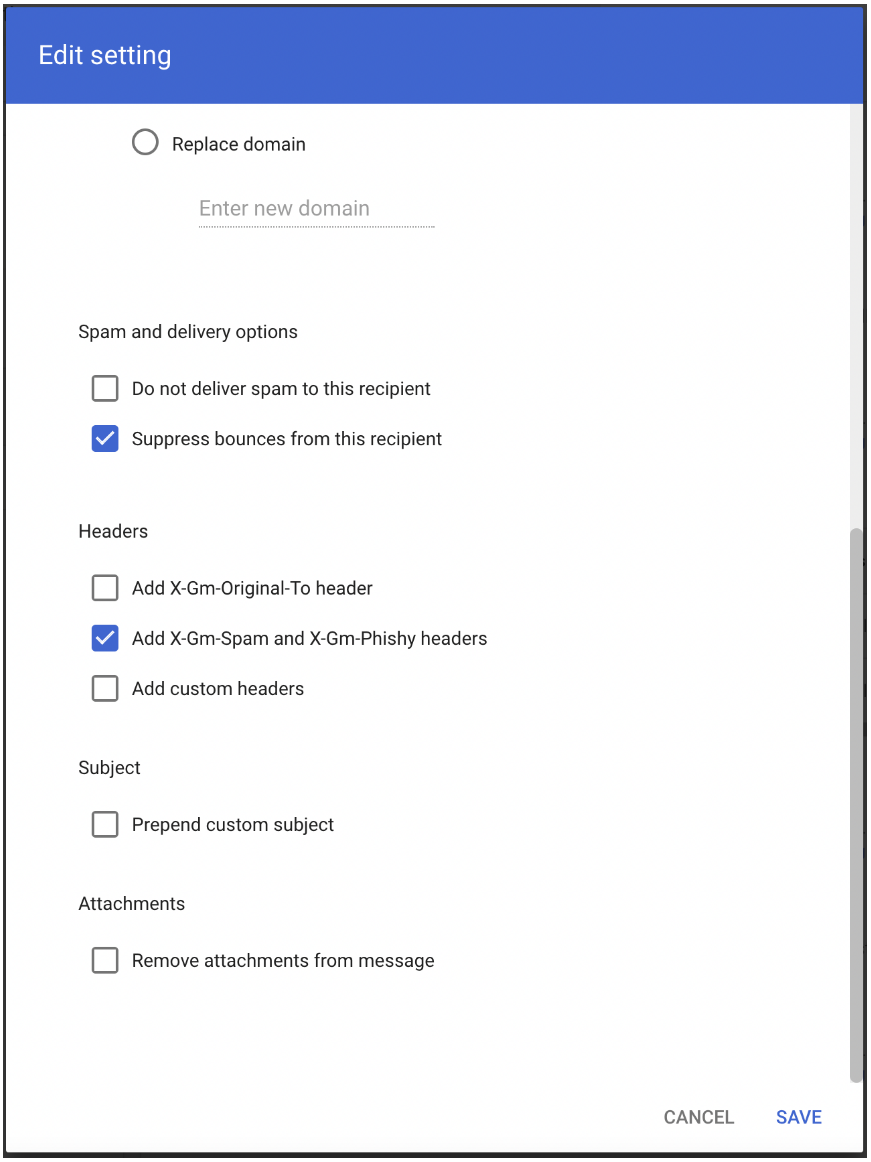
Enter new username

○ Replace domain

Enter new domain

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

○ 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

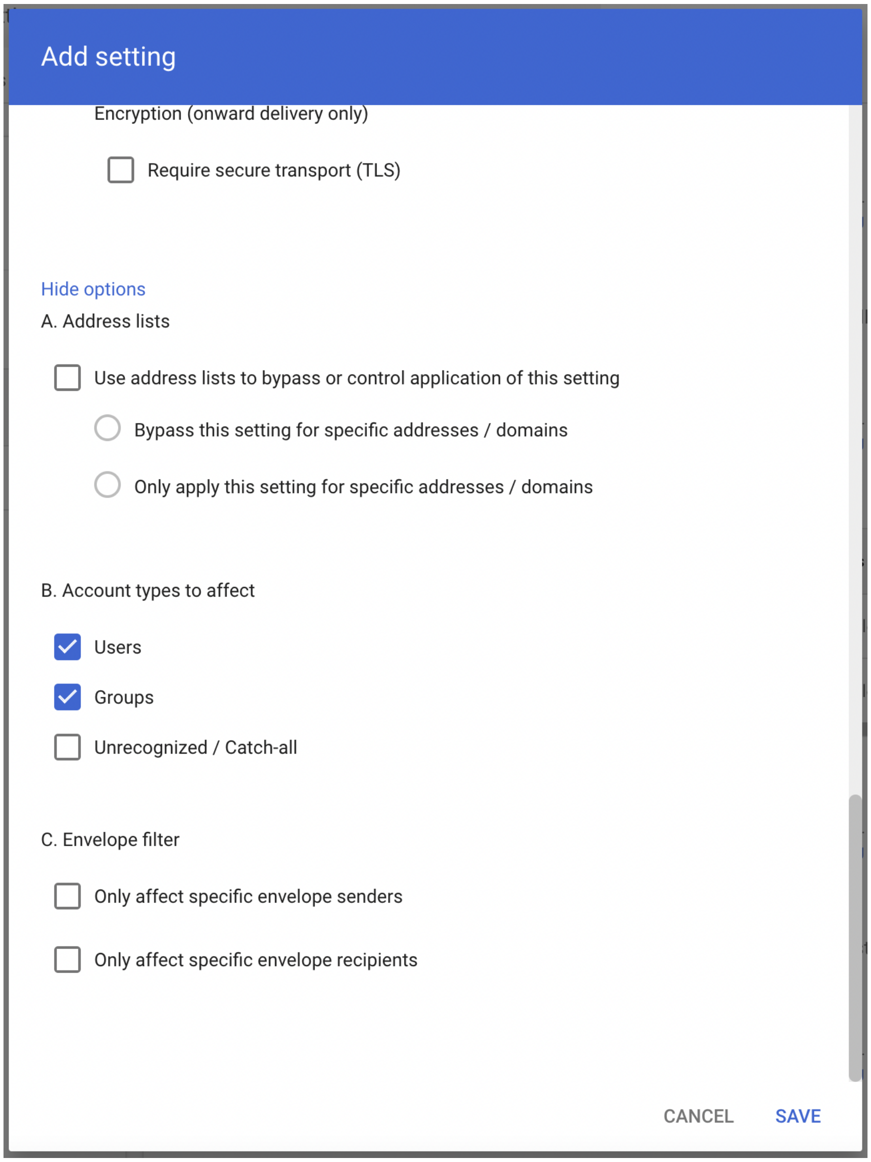
□ Prepend custom subject

Attachments

□ Remove attachments from message

vii. Click SAVE to save your settings

5. 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

○ Bypass this setting for specific addresses / domains

○ Only apply this setting for specific addresses / domains

B. Account types to affect

☑ Users

☑ Groups

□ Unrecognized / Catch-all

C. Envelope filter

□ Only affect specific envelope senders

□ Only affect specific envelope recipients

b. Click SAVE to save your settings