

Google Workspace Audit

- Audit Admin Roles – ensure principle of least privilege

Account > Admin Roles > Hover cursor over Role to “View Privileges” and “View Admins”.

The screenshot shows the Google Admin console interface. On the left, the navigation menu includes 'Admin', 'Home', 'Dashboard', 'Directory', 'Devices', 'Apps', 'Security', 'Reporting', 'Billing', 'Account', and 'Rules'. The 'Account' menu item is highlighted, and the 'Admin roles' sub-menu is selected. The main content area shows a search bar and a notification about assigning admin roles to security groups. Below this is a table of roles with columns for Role, Role description, and Type. The 'Super Admin' role is highlighted, and the 'View admins' button is visible.

Role	Role description	Type ?
Super Admin	Google Workspace Administrator Seed Role	System role
Groups Admin	Groups Administrator	System role
User Management Admin	User Management Administrator	System role
Help Desk Admin	Help Desk Administrator	System role
Services Admin	Services Administrator	System role
Android Admin	Play For Work Administrator	System role
Groups Reader BETA	Groups Reader	System role

Figure 1

- Ensure school is using email authentication.

DKIM can be found by navigating to Apps > Google Workspace > Gmail > Authenticate Email.

SPF & DMARC can be verified using mxtoolbox.com

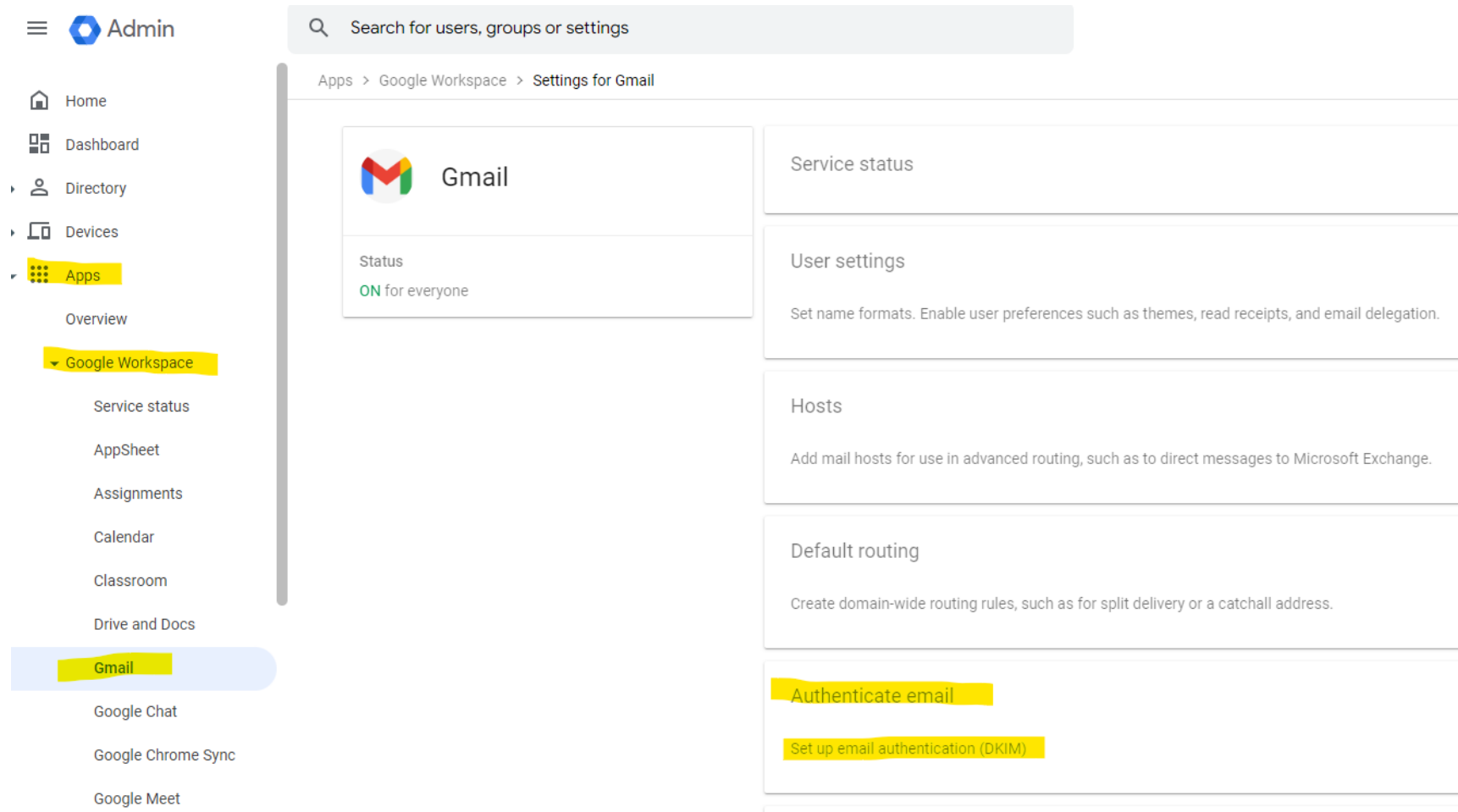


Figure 2

- To configure extra safety settings for Gmail go to Apps > Google Workspace > Gmail > Safety

Here you will find settings for “Attachments”, “Links and external images”, and “Spoofing and authentication”

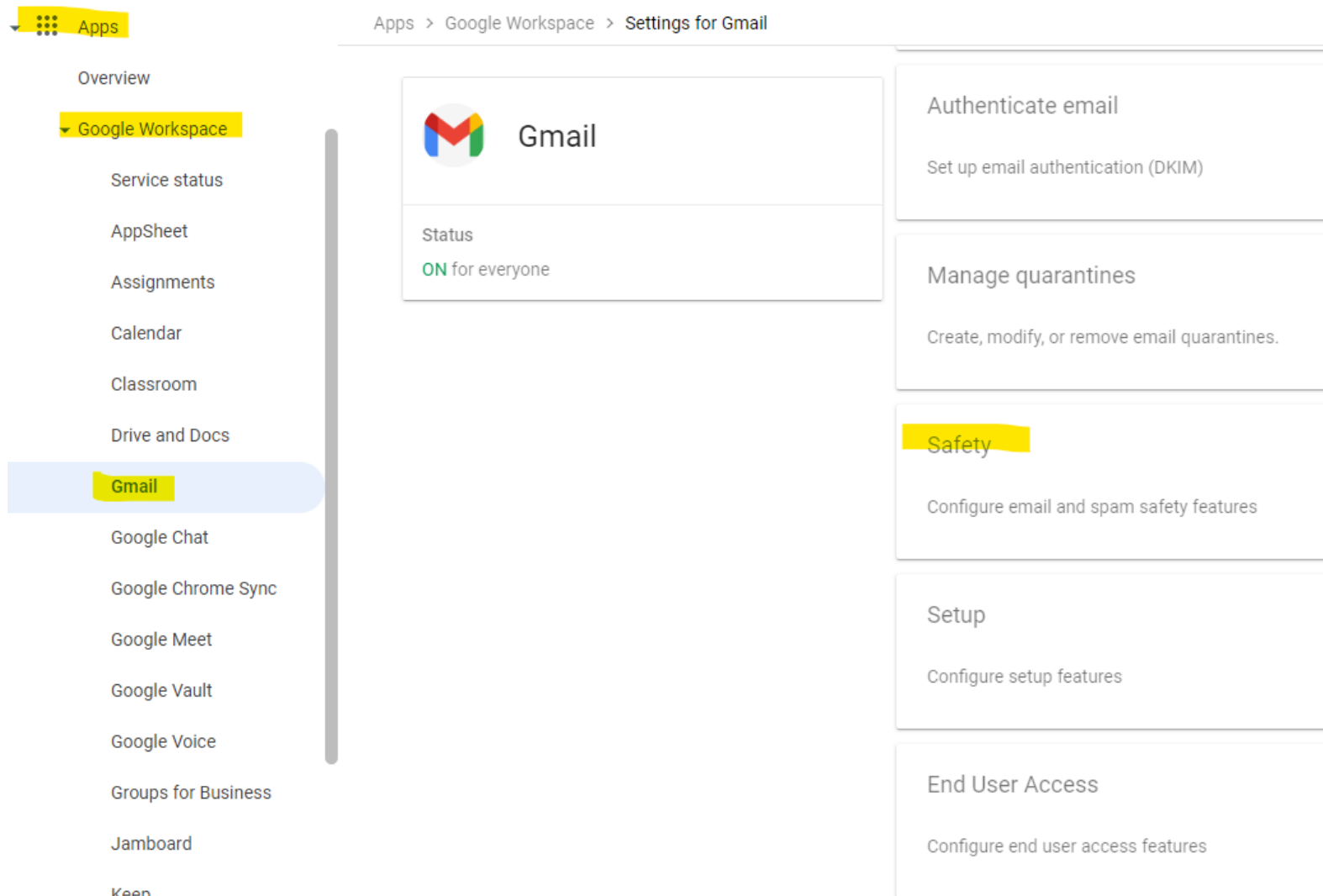


Figure 3

- End User Access - Apps > Google Workspace > Gmail > End User Access

This is where you can disable POP & IMAP access (this will prevent the use native mail clients such as Apple Mail).

This is important, because these older protocols do not support MFA.

Also in this section, you are given the option to disable automatic forwarding. Doing this, prevents Business Email Compromise (BEC) attacks. It may be that this should be disabled for some users, but not all.

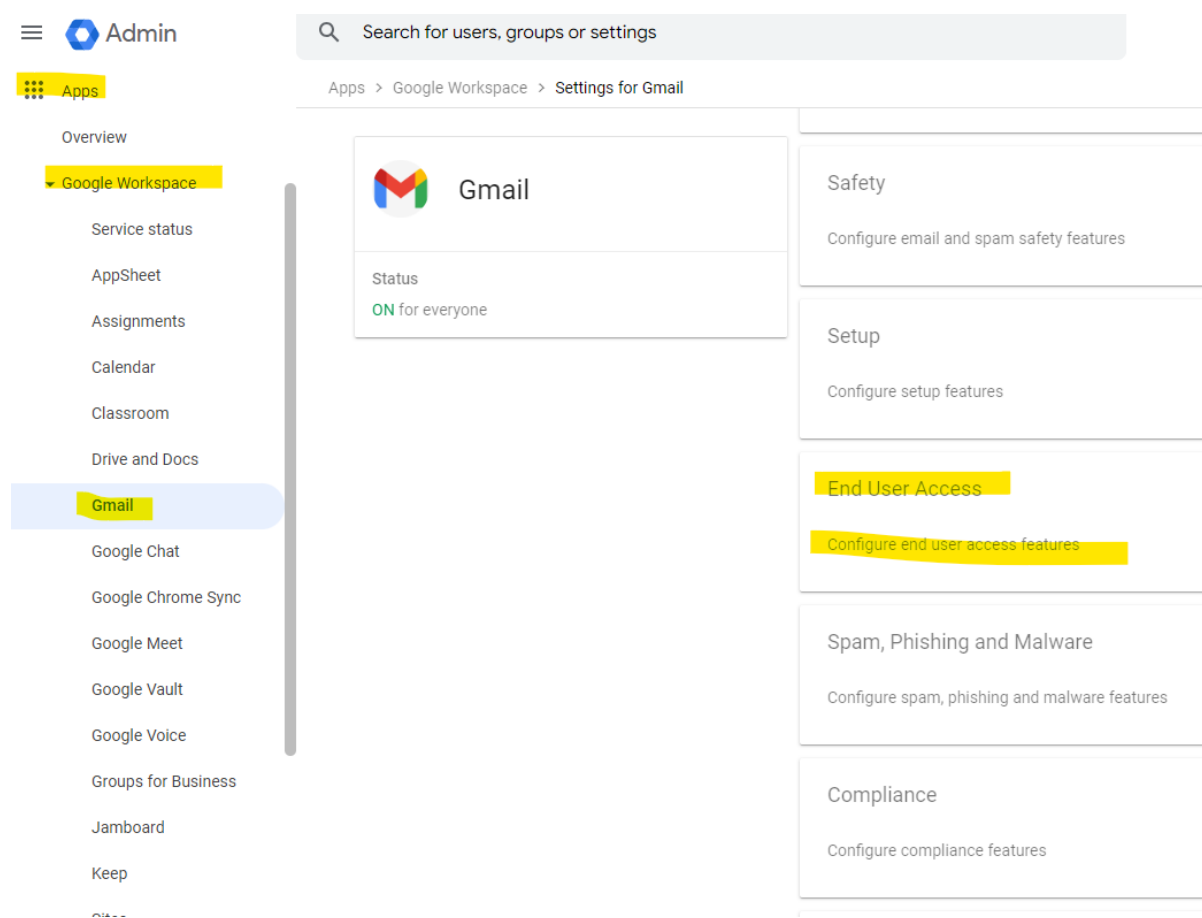


Figure 4

- Also, in Settings for Gmail is “Spam, phishing, and malware” Apps > Google Workspace > Gmail > Spam, phishing, and malware

Turn on “Enhanced pre-delivery message scanning” this will delay mail by a few seconds, giving Google’s filter a little longer to catch spam, phishing, and malware before it lands in the inbox.

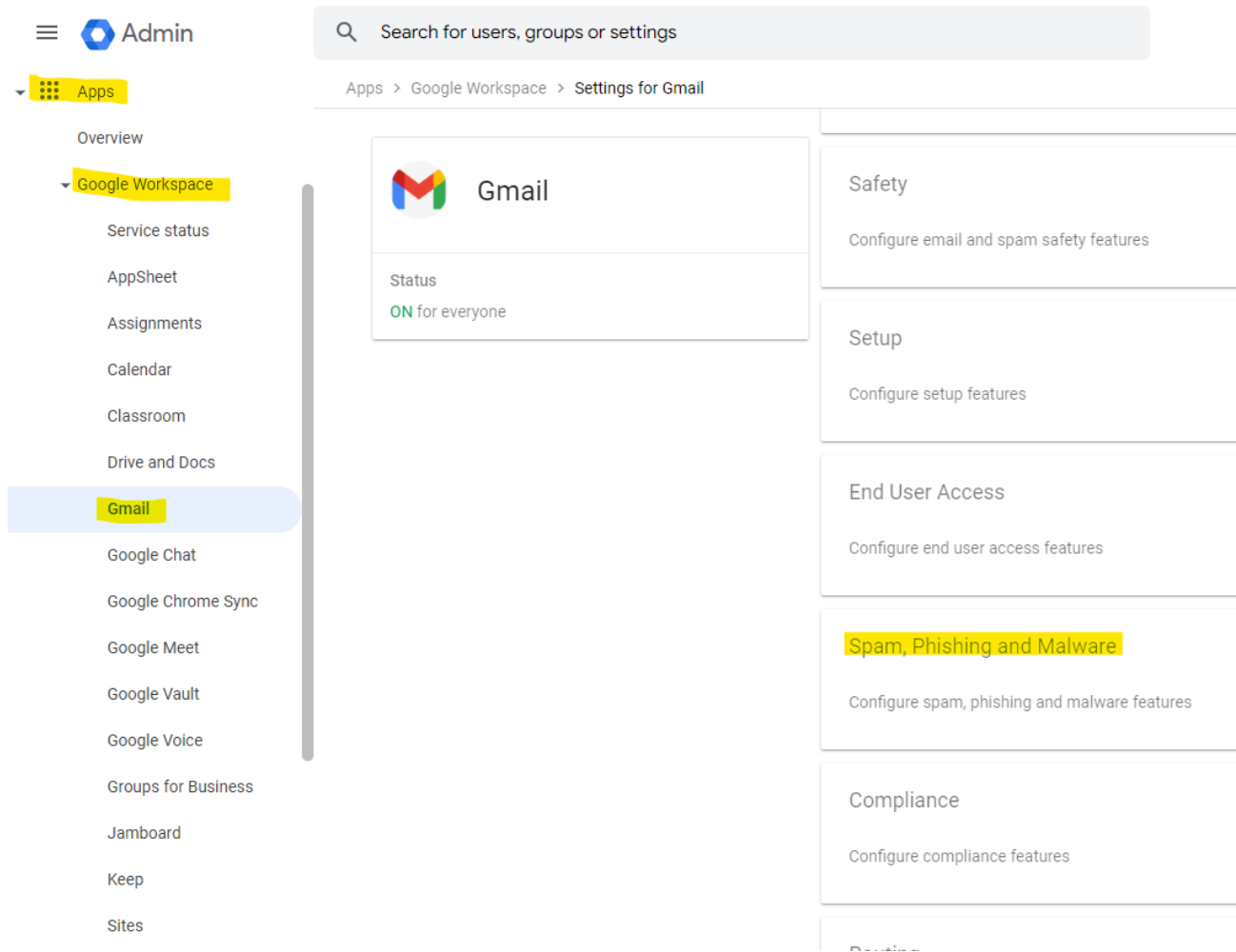


Figure 5

- Compliance - Apps > Google Workspace > Gmail > Compliance

Content Compliance – can be set to quarantine emails that contain certain words, phrases, or pattern. For example, you can set it to detect and quarantine an email (inbound or outbound) if a social security number is present in the message.

In the next few images we will walk through creating a rule that will prevent users from emailing social security numbers, including pictures of them.

First we navigate to Gmails compliance settings, this can be achieved by following *Figure 6*.

Apps

Overview

Google Workspace

Service status

AppSheet

Assignments

Calendar

Classroom

Drive and Docs

Gmail

Google Chat

Google Chrome Sync

Google Meet

Google Vault

Google Voice

Groups for Business

Jamboard

Keep

Sites

Tasks

Additional Google services



Gmail

Status

ON for everyone

Safety

Configure email and spam safety features

Setup

Configure setup features

End User Access

Configure end user access features

Spam, Phishing and Malware

Configure spam, phishing and malware features

Compliance

Configure compliance features

Routing

Configure routing features

Figure 6

Once there, ensure Optical Character Recognition

is enabled. This will allow Google to scan images for text. *See Figure 7*

The screenshot displays the 'Compliance' settings page in the Google Admin console. At the top, there is a header 'Compliance' with an upward arrow. Below the header is a blue banner with an information icon and the text: 'To check how these settings are affecting email delivery and troubleshoot potential issues, go to [Email Log Search](#). GOT IT'. The main content area is divided into several sections:

- Email and chat auto-deletion:** Applied at 'rbsd.k12.ar.us'. The setting is 'Do not delete email and chat messages automatically.' A warning icon indicates that the auto-deletion setting applies to email and chat messages in the user's inbox and archived messages, but not to messages in the Trash folder.
- Optical Character Recognition (OCR):** Applied at 'rbsd.k12.ar.us'. The setting is 'Enable OCR for email attachments: ON'. A warning icon indicates that the OCR setting applies only to licensed users with the appropriate Google Workspace offering.
- Comprehensive mail storage:** Inherited. The setting is 'Ensure that a copy of all sent and received mail is stored in associated users' mailboxes: OFF'.
- Append footer:** Set up outbound footer text for legal compliance, informational or promotional requirements. A 'CONFIGURE' button is located at the bottom right of this section.

At the bottom of the page, there is an information icon and the text: 'Most changes take effect in a few minutes. [Learn more](#). You can view prior changes in the [Audit log](#)'.

Figure 7

Next, scroll down to Content Compliance and press “Configure.” See *Figure 8*

The screenshot shows a configuration interface with three main sections. Each section includes an information icon, a description, and a 'CONFIGURE' button. The 'Content compliance' section is highlighted with a yellow background.

Section	Description	Action
Restrict delivery	Restrict the domains that your users are allowed to exchange email with.	CONFIGURE
Content compliance	Configure advanced content filters based on words, phrases or patterns.	CONFIGURE
Objectionable content	Configure content filters based on word lists.	CONFIGURE

Restrict delivery

Most changes take effect in a few minutes. [Learn more](#)
You can view prior changes in the [Audit log](#)

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

CONFIGURE

Content compliance

Most changes take effect in a few minutes. [Learn more](#)
You can view prior changes in the [Audit log](#)

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

CONFIGURE

Objectionable content

Most changes take effect in a few minutes. [Learn more](#)
You can view prior changes in the [Audit log](#)

Configure content filters based on word lists.

CONFIGURE

Figure 8

Give your rule a descriptive name, so when you see it later or another tech comes across it, it will be clear what the rule is doing. For this rule, we select “Outbound.” Once that is done, you’ll need to add an expression.

Add setting

Content compliance [Learn more](#)

PII - Data Leak Prevention - Social Security

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

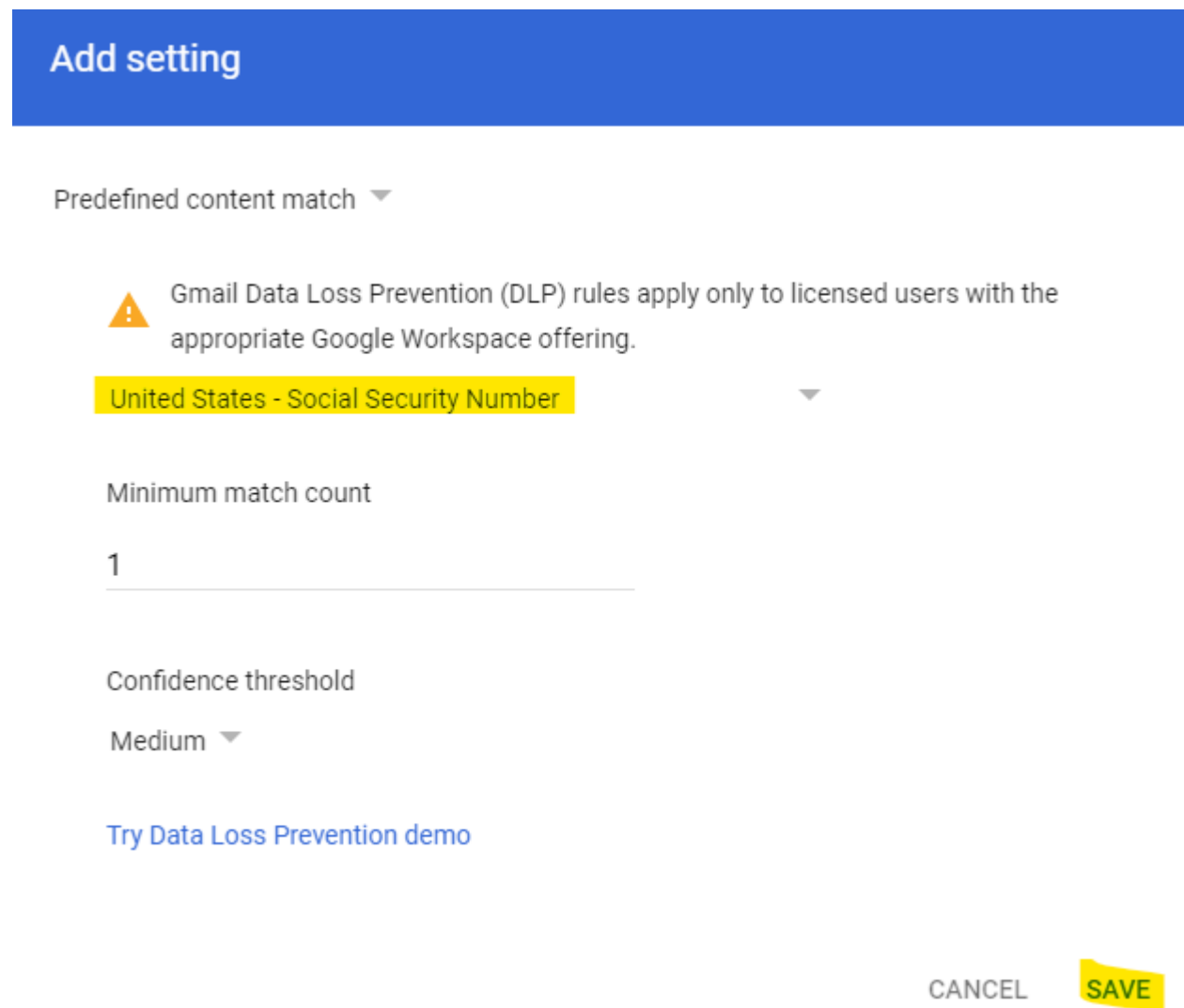
If ANY of the following match the message ▼

Expressions
No expressions added yet. Add

[ADD](#)


Figure 9

Once you've selected "add expression", you'll be brought to the following window, select "predefined content match" and choose "United States – Social Security Number."



Add setting

Predefined content match ▼

 Gmail Data Loss Prevention (DLP) rules apply only to licensed users with the appropriate Google Workspace offering.

United States - Social Security Number ▼

Minimum match count

1

Confidence threshold

Medium ▼

[Try Data Loss Prevention demo](#)

CANCEL **SAVE**

Figure 10

On the third setting for content compliance, we need to tell Google what to do if the rule is violated. In my example, I'm setting the rule to reject. You can also use the modify option, which allows you to apply several different measures such as removing the attachment, enforce TLS, etc. If you choose reject, you'll need to add a rejection notice for your end users that violate the policy. *See Figure 11*

ADD

3. If the above expressions match, do the following

Reject message ▼

Customize rejection notice

Optional

Contents of your email violated our data loss prevention rule & therefore was rejected. Contact the tech department for guidance.

Show options

CANCEL SAVE

Figure 11

- Security – Security > Authentication > Password management

Here you can force strong passwords, password length requirements, disallow reuse, and set expirations.

- Security – Security > Less Secure Apps

This is where you can prevent users from accessing your domains Google Services from insecure apps. It is recommended that you turn this on. Being that these third-party apps may not have the same sign-in security standards as Google. If two-factor is enabled Less Secure Apps are disabled automatically.

- Security > 2-Step Verification


Two-factor must be enabled from the Google Admin console so that users may set it up on their end. *See Figure 11*

Turn on 2-Step Verification

With 2-Step Verification, also called two-factor authentication, you can add an extra layer of security to your account in case your password is stolen. After you set up 2-Step Verification, you can sign in to your account with:

- Your password
- Your phone

Allow 2-Step Verification

1. Open your [Google Account](#) .
2. In the navigation panel, select **Security**.
3. Under “How you sign in to Google,” select **2-Step Verification** > **Get started**.
4. Follow the on-screen steps.

Tip: If you use an account through your work, school, or other group, these steps might not work. If you can’t set up 2-Step Verification, [contact your administrator for help](#).

Verify it’s you with a second step

After you turn on 2-Step Verification, you must complete a second step to verify it’s you when you sign in. To help protect your account, Google will ask that you complete a specific second step.

