White Paper

Google Workspace + IRONSCALES = A Complete Email Security Solution

IRONSCALES
SAFER TOGETHER

Introduction

This document is intended to support our enterprise client's decision to utilize IRONSCALES while recognizing they need a smooth pathway to transition their spam filtering technology. We have identified a transition strategy and specific configuration steps to maximize the utilization of their existing GWS licenses and capabilities. The goal is to help transition Spam services away from their Secure Email Gateways to native email security controls provided to you as a GWS email customer.

Contents

High-Level Implementation Strategy

This guide is intended for enterprise organizations but can be adapted to organizations of any size.

Overcommunicate

Overcommunicate what change you are making (a transition to commercialized Spam Controls), why you are making this change (extracting extra value from tools you're already paying for), when you are making this change, and how individuals can quickly receive support.

Lead from the Front

The IT organization and team members should make the switch first, so they understand any potential impact and what to expect. Collect feedback and quickly document any concerns that may have materialized. Share these documents with your support team, and make sure they know where to find this information quickly as needed.

Prepare your Team

Ensure your support team(s) and/or helpdesk are aware of the transition, support paths, common questions/concerns they may encounter, and how to respond appropriately.

Focus on VIPs

Start with VIPs of your organization. Once you successfully transitioned these employees you are less likely to face pushback from other groups of employees, as your transitioned VIPs will serve as advocates of this change.

- With VIPs, we encourage taking a white-glove approach. Have the VIP support path(s) communicated in advance personally (an email alone may NOT be effective). If possible, identify a 'war room' type location where VIPs can go to get immediate assistance.

Break up the Implementation into Manageable Pieces

If the number of VIPs is very large, consider implementing only a few VIP 'waves' at a time. People who are traditionally very resistant to change should be mixed with early adopters. Divide the waves up based on your unique knowledge of team

Start to Scale

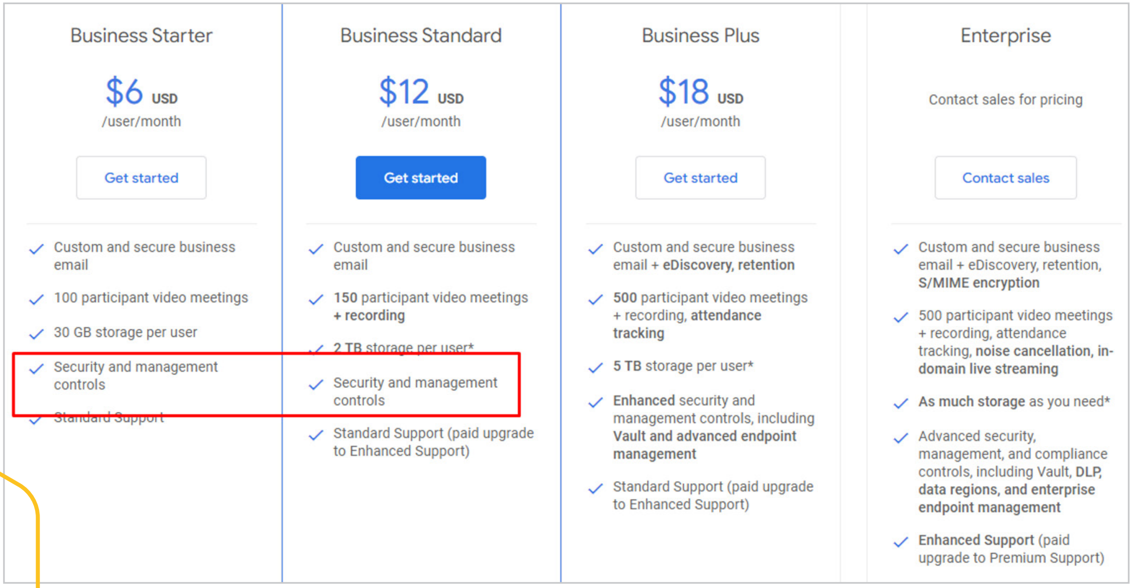
Scale up the waves for the remainder of the organization. With the VIP leaders on board, now you want to transition to larger groups. If you have many physical sites, break up the waves by function, not location. If your group waves based on location alone, the local support team will become overwhelmed, and local leadership could become resistant to this change, undermining the hard work you did with VIPs previously.

Finish Strong!

Continually add waves to the transition until complete. Remember, the objective of a successful wave is to prevent significant business disruption. Please expect users to object to or question these changes, change is always hard, and this behavior is humans doing human things. Continually focus on the goal: to make the transition as quickly as possible with the least amount of disruption or consternation within your business cycle.

Scope

This document is focused on maximizing the organization's utilization of the commercialized spam controls within Gmail for Business with a Business Starter license and above, which includes Security and Management Controls. This document focuses on the configuration required to address the concern of noisy Spam while using IRONSCALES to secure your organization.



Business Starter	Business Standard	Business Plus	Enterprise
$6 USD /user/month	$12 USD /user/month	$18 USD /user/month	Contact sales for pricing
Get started	Get started	Get started	Contact sales
✓ Custom and secure business email	✓ Custom and secure business email	✓ Custom and secure business email + **eDiscovery, retention**	✓ Custom and secure business email + eDiscovery, retention, **S/MIME encryption**
✓ 100 participant video meetings	✓ **150** participant video meetings **+ recording**	✓ **500** participant video meetings + recording, **attendance tracking**	✓ 500 participant video meetings + recording, attendance tracking, **noise cancellation, in-domain live streaming**
✓ 30 GB storage per user	✓ **2 TB** storage per user*	✓ **5 TB** storage per user*	✓ **As much storage** as you need*
✓ Security and management controls	✓ Security and management controls	✓ **Enhanced** security and management controls, including **Vault and advanced endpoint management**	✓ Advanced security, management, and compliance controls, including Vault, **DLP, data regions, and enterprise endpoint management**
✓ Standard Support	✓ Standard Support (paid upgrade to Enhanced Support)	✓ Standard Support (paid upgrade to Enhanced Support)	✓ **Enhanced Support** (paid upgrade to Premium Support)

Configure anti-spam policies in Gmail for Business.

In organizations using Gmail for Business, inbound email messages can be automatically protected against spam.

NOTE

The settings outlined in this document will need to be monitored and adjusted based on your individual organization's email traffic. Please use this as a guide to assist you in your transition and assume we've tried to provide a generalized best practice that will need adjustment over time.

Gmail spam filters automatically move spam email messages (sometimes called junk mail) into users' spam folders. You can't turn off Gmail's spam filters, but you can create filters that:

- Bypass spam classification for messages received from users on an approved senders list that you create.
- Bypass spam classification for messages received from senders within your domain.
- Put spam messages in quarantine so you can review them before they're delivered to users.
- Filter bulk email more aggressively.

The Gmail AI-enhanced spam-filtering (using in-house machine learning framework, TensorFlow) capabilities block nearly 10 million spam emails every minute.

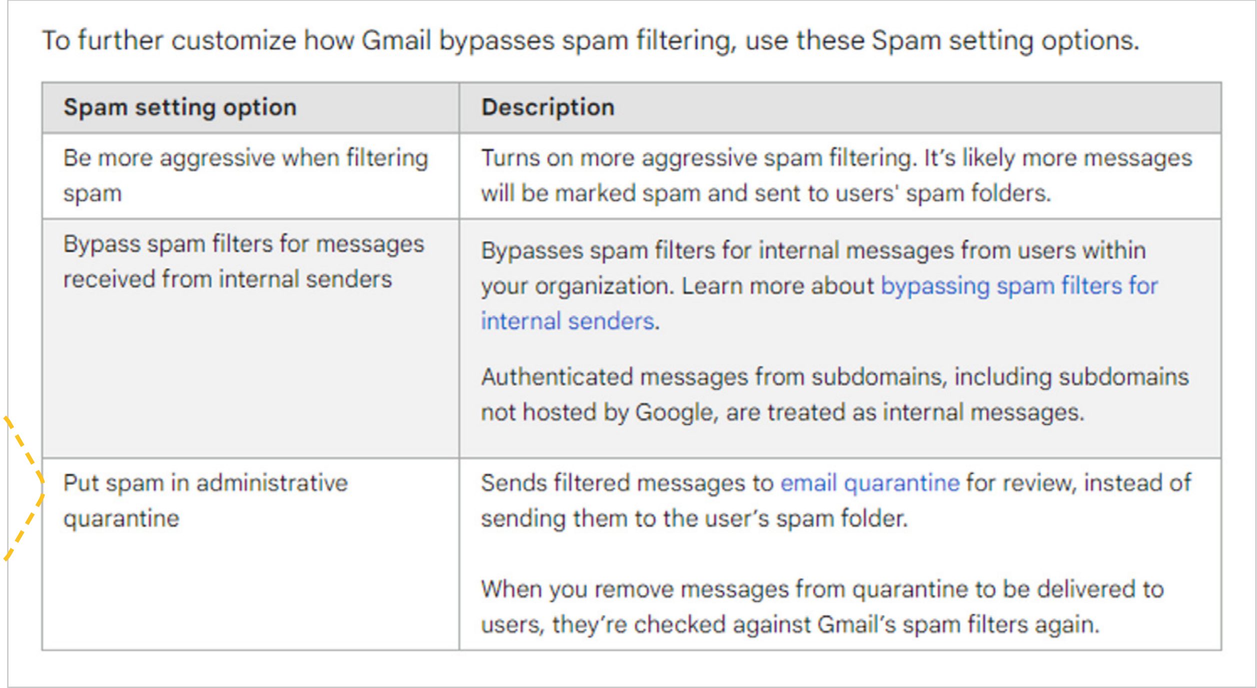
According to Google, Gmail's filtering capabilities and advanced security protections help billions of people stay safe and get things done more efficiently. By combining Google's powerful functionality with IRONSCALES, our customers have experienced a 99.9% reduction in the amount of spam reaching their end users' mailboxes.

Prerequisites

- You need to be assigned **Admin** permissions in **G Suite** before you can do the procedures in this article:
- To add, modify, and delete anti-spam policies, you need to be an **Administrator**

Where you can apply spam filters

- You can apply spam settings and filters per organizational unit. Settings and filters apply to all users in the organizational unit. Users in child organizations inherit the setting from the parent organization.
- Spam filter settings can't be applied to groups. Spam filter settings affect groups users who are in an organizational unit where the setting is applied.
- Gmail spam filters automatically move spam email messages (sometimes called junk mail) into users' spam folders. You can't turn off Gmail's spam filters, but you can create filters that:



To further customize how Gmail bypasses spam filtering, use these Spam setting options.

Spam setting option	Description
Be more aggressive when filtering spam	Turns on more aggressive spam filtering. It's likely more messages will be marked spam and sent to users' spam folders.
Bypass spam filters for messages received from internal senders	Bypasses spam filters for internal messages from users within your organization. Learn more about bypassing spam filters for internal senders. Authenticated messages from subdomains, including subdomains not hosted by Google, are treated as internal messages.
Put spam in administrative quarantine	Sends filtered messages to email quarantine for review, instead of sending them to the user's spam folder. When you remove messages from quarantine to be delivered to users, they're checked against Gmail's spam filters again.

Best practices for approved senders' lists

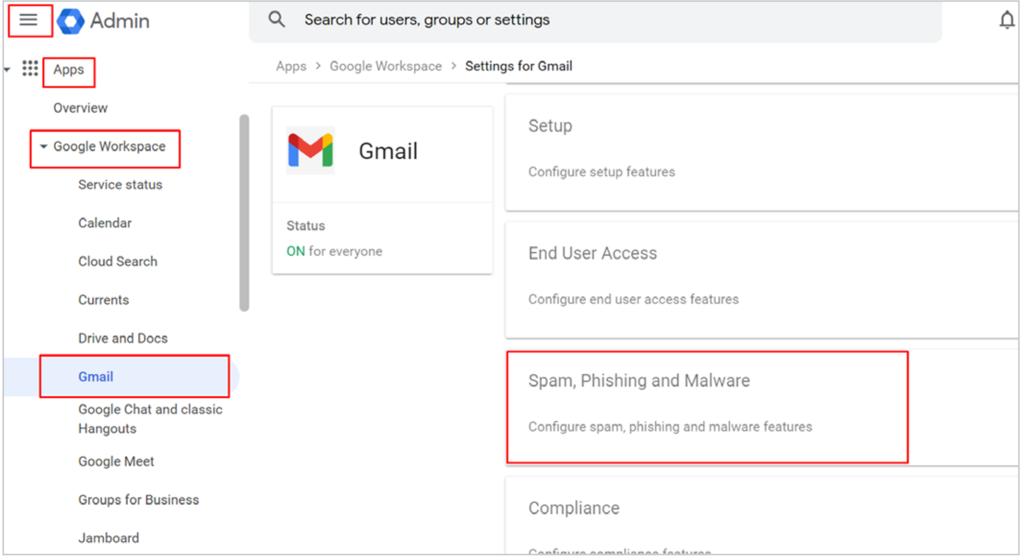
Some tips for working with approved senders' lists:

- When possible, use the same approved sender lists for multiple Gmail settings. For example, you can use the same list for **Spam** settings and **Restrict delivery** settings.
- Match From addresses with entries in the approved sender list. Gmail checks the addresses or domains against the From part of the message header, not against the **Return-Path** part of the header. For this reason, From must match an address or domain you entered in the approved senders list.
- An approved senders list that includes a domain is also applied to the subdomains.
- If the sending domain has a DMARC policy set to **reject**, the policy overrides any settings for an approved senders list.
- Approved senders' lists are subject to Gmail settings size limits.

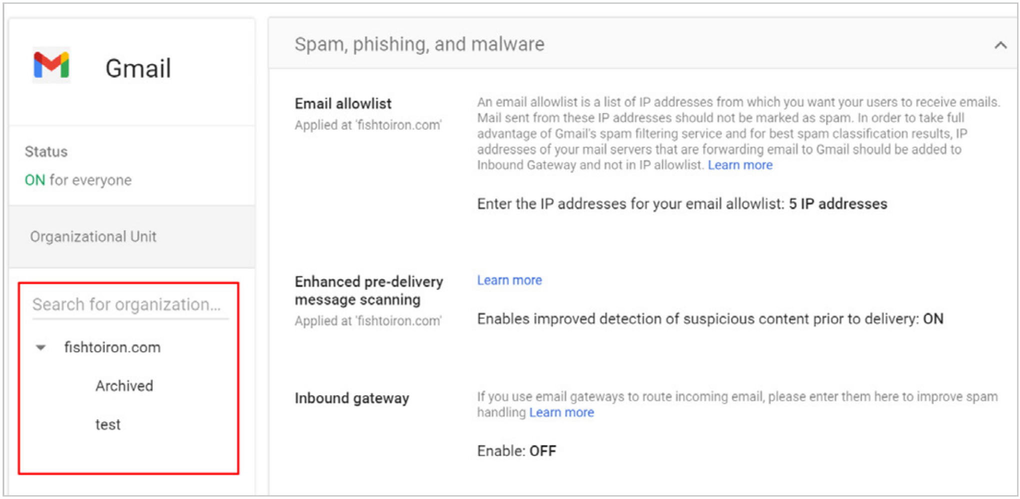
Setting Description	Google Workspace Account Limit	Learn More About These Settings
Settings: The size limit for all Gmail settings, such as Spam, Compliance, Routing settings	• 5 MB. This limit is the combined size of all Gmail settings in your Google Workspace account, after you save them and they're complied by the systems. If you rech this limit, you can't save additional settings. • 1,000 settings (not over 5 MB)	• Span filters • Content compliance • Email routing
Descriptions: The number of characters that can be used to describe settings, regular expressions, and other items.	• 1,00 characters per description	• Span filters • Content compliance • Email routing

Add a list of approved senders that bypass spam filters

1. Sign in to your [Google Admin console](#).
2. Sign in using an administrator account, not your current account
3. In the Admin console, go to
   Menu → Apps → Google Workspace → Gmail Spam, Phishing and Malware.


Admin
Search for users, groups or settings
Apps
Overview
Google Workspace
Service status
Calendar
Cloud Search
Currents
Drive and Docs
Gmail
Google Chat and classic Hangouts
Google Meet
Groups for Business
Jamboard
Apps > Google Workspace > Settings for Gmail
Gmail
Status
ON for everyone
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

4. On the left, select an Organizational Unit.



Email allowlist
Applied at 'fishtoiron.com'

An email allowlist is a list of IP addresses from which you want your users to receive emails. Mail sent from these IP addresses should not be marked as spam. In order to take full advantage of Gmail's spam filtering service and for best spam classification results, IP addresses of your mail servers that are forwarding email to Gmail should be added to Inbound Gateway and not in IP allowlist. Learn more

Enter the IP addresses for your email allowlist: **5 IP addresses**

Enhanced pre-delivery message scanning
Applied at 'fishtoiron.com'

Learn more

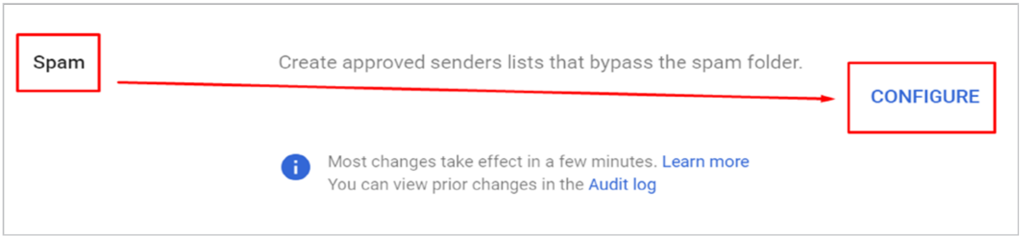
Enables improved detection of suspicious content prior to delivery: **ON**

Inbound gateway

If you use email gateways to route incoming email, please enter them here to improve spam handling Learn more

Enable: **OFF**

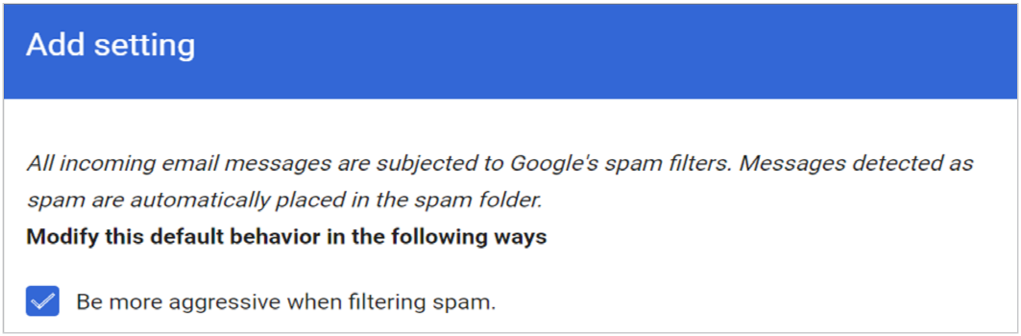
5. Point to **Spam** and click **Configure**.



Create approved senders lists that bypass the spam folder.

Most changes take effect in a few minutes. Learn more
You can view prior changes in the Audit log

6. Check the Be more aggressive when filtering spam checkbox



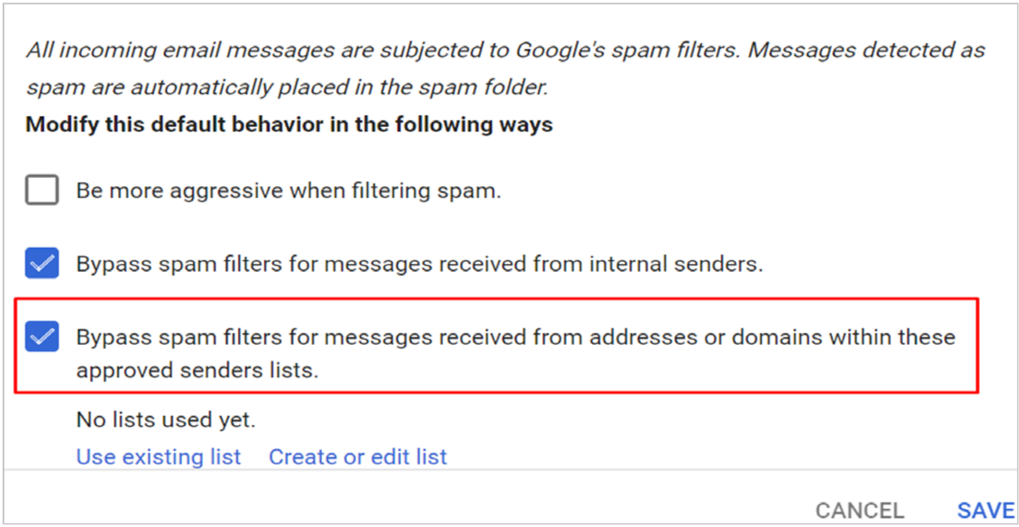
Add setting

All incoming email messages are subjected to Google's spam filters. Messages detected as spam are automatically placed in the spam folder.

Modify this default behavior in the following ways

☑ Be more aggressive when filtering spam.

7. Check the **Bypass spam filters** for messages received from addresses or domains within these approved senders lists box.



All incoming email messages are subjected to Google's spam filters. Messages detected as spam are automatically placed in the spam folder.

Modify this default behavior in the following ways

☐ Be more aggressive when filtering spam.

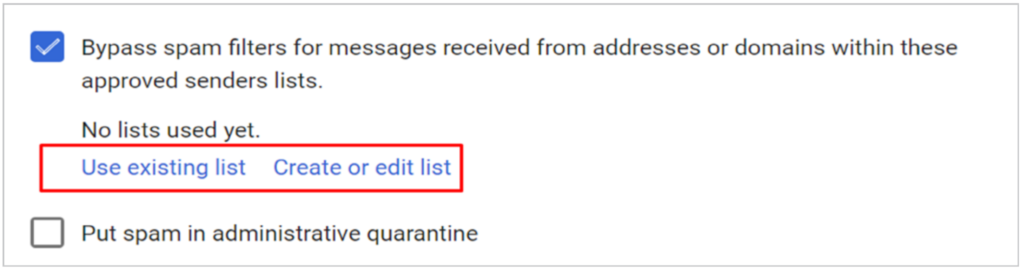
☑ Bypass spam filters for messages received from internal senders.

☑ Bypass spam filters for messages received from addresses or domains within these approved senders lists.

No lists used yet.

8. Click **Use existing list** or **Create or edit l**ist to select an existing list or create a list of approved senders. To add a new list:

9. Click **Create** or **Edit list**.

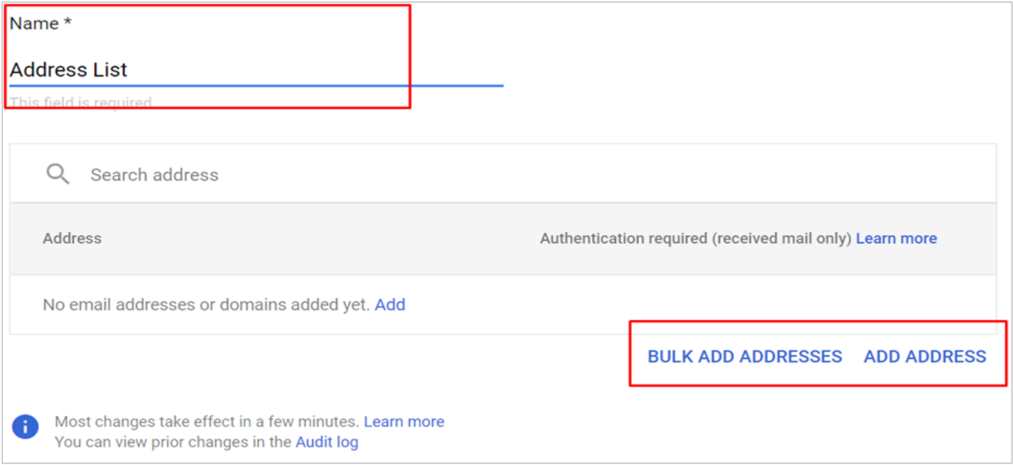


☑ Bypass spam filters for messages received from addresses or domains within these approved senders lists.

No lists used yet.

□ Put spam in administrative quarantine

10. Enter a New Name for the List



Name *

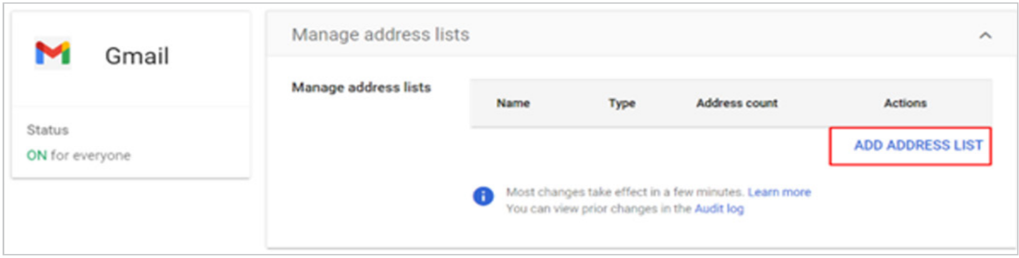
Address List

This field is required

No email addresses or domains added yet. Add

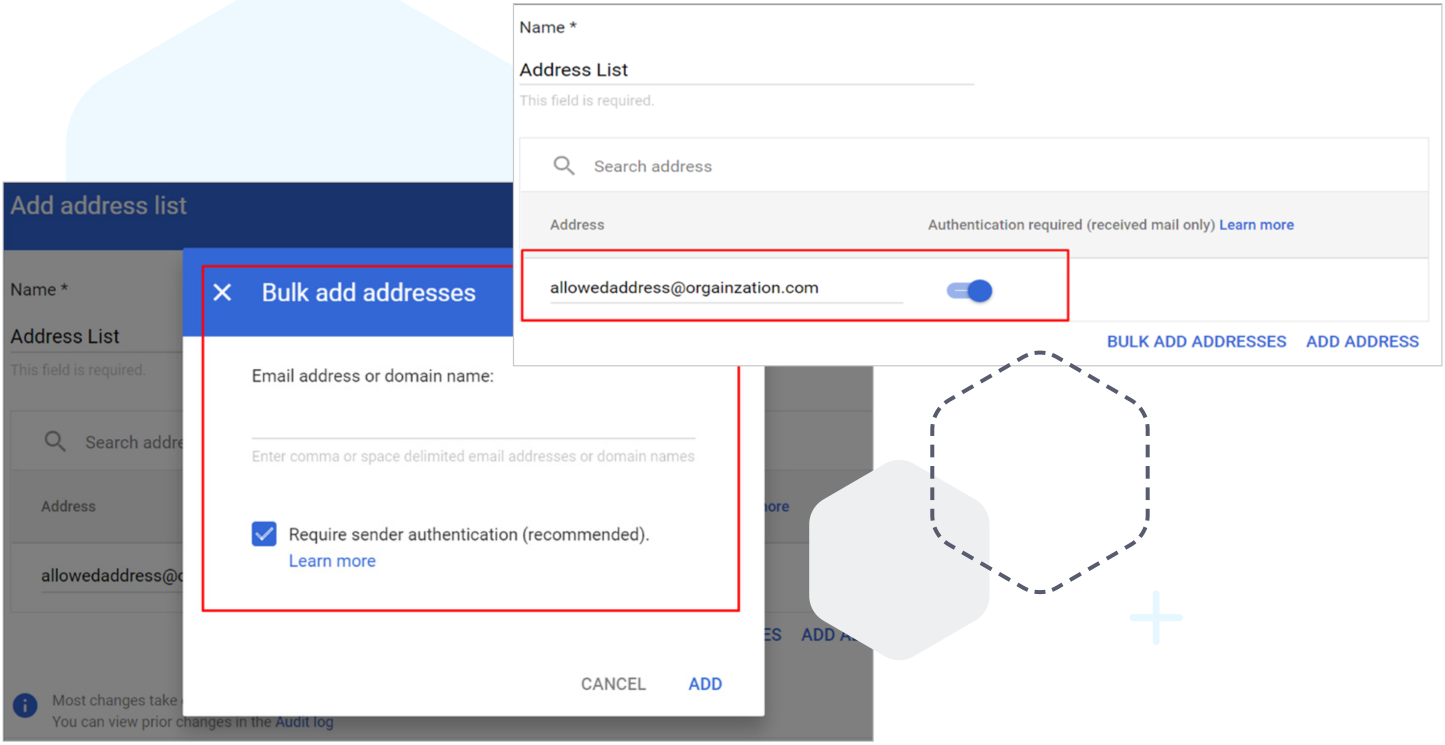
Most changes take effect in a few minutes. Learn more
You can view prior changes in the Audit log

11. Scroll to the bottom of **Manage address lists**, and click **Add address list or Bulk Add Addresses**.



Most changes take effect in a few minutes. Learn more
You can view prior changes in the Audit log

12. Enter email addresses or domain names. Use a space or comma between each entry.



Add address list

Bulk add addresses

Email address or domain name:

Enter comma or space delimited email addresses or domain names

☑ Require sender authentication (recommended). Learn more

CANCEL ADD

Name *

Address List

This field is required.

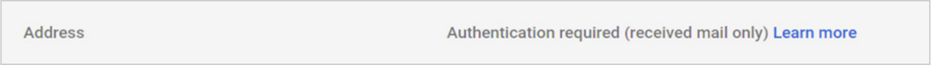
Search address

Address	Authentication required (received mail only) Learn more
allowedaddress@orgainzation.com	●

BULK ADD ADDRESSES ADD ADDRESS

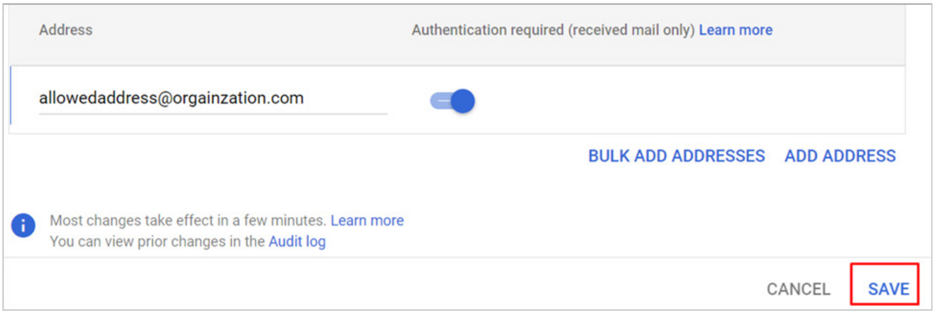
Most changes take effect in a few minutes.
You can view prior changes in the Audit log

13. (Optional) To bypass this setting for approved senders that don't have authentication, you can turn off **Authentication required** for each user. These bypass the SPF and DKIM authentication.



Address	Authentication required (received mail only) Learn more

14. Click **Save** to save the new address list.



Address	Authentication required (received mail only) Learn more
allowedaddress@orgainzation.com	●

BULK ADD ADDRESSES ADD ADDRESS

Most changes take effect in a few minutes. Learn more
You can view prior changes in the Audit log

CANCEL SAVE

15. It can take up to 24 hours for your changes to take effect. You can track changes in the Admin console audit log.

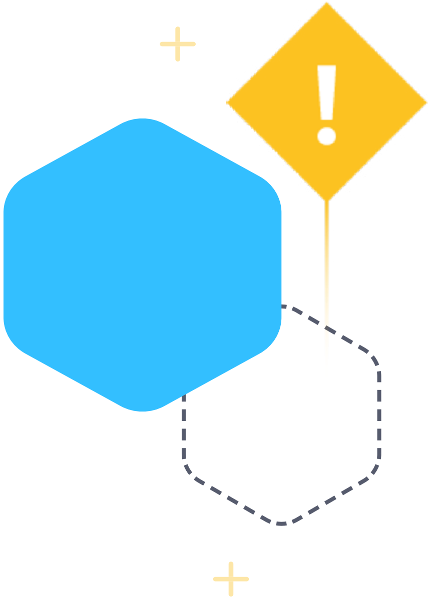
What if I get spam or malware from someone on the approved senders list?

If you get spam or malware from an approved sender:

- If an approved sender sends spam, the messages are delivered to the recipient's inbox, not to the spam folder. Bypassed messages display a banner: "This message wasn't sent to Spam because of your organization's settings."
- If an approved sender's message has a virus or is part of an email attack, Google's virus filters prevent it from reaching your users.
- Ask the sender to set up DMARC so their valid messages are delivered to the inbox, and not sent to spam.

With advanced settings, you can:

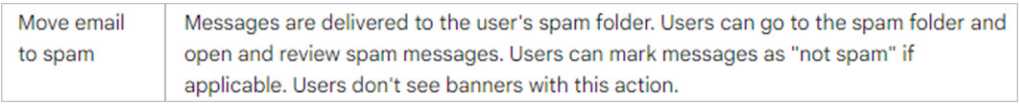
- Automatically turn on and apply future recommended settings. This ensures maximum protection for email and attachments for your domain.
- Provide the strongest level of protection for a domain or organizational unit by turning on all security options.
- Customize security settings by checking only the options you want to turn on. Unchecking all options turns off all advanced security settings for the domain or organizational unit.
- Specify an action for each security option you turn on. If you don't select an action, the default action is applied to the security option.



Important to note:

- Other spam settings - These advanced security features work independently of other spam settings you might have previously turned on. For example, even if you've listed a domain as a safe sender in spam settings, the enhanced security features are still applied.
- Quarantine action — When you select Quarantine for any of the advanced security settings, the quarantine you select applies only to incoming messages. This is true even when the quarantine you select specifies actions to take on outgoing messages. Allowlist settings don't override the Quarantine option.
- Warning banners — Warning banners (yellow box) appear only on Gmail web. Third-party apps do not display a warning banner.

How selecting Spam Action affects users:



Move email to spam	Messages are delivered to the user's spam folder. Users can go to the spam folder and open and review spam messages. Users can mark messages as "not spam" if applicable. Users don't see banners with this action.

Gmail Spam Filter - FAQs

Does Gmail have a spam filter?

Gmail has a built-in spam filter that automatically moves certain messages into a spam folder. You cannot turn it off, but you can customize where messages from certain email addresses may end up. This is a useful tool so that you are not constantly bombarded by unwelcome advertisements and junk mail.

Where is my spam filter in Gmail?

To find your spam folder, log into your Gmail account and look at the panel on the left. You should see folders for your main inbox, promotions, updates, and more. Continue to scroll down and you will see the spam folder. If you d on't see it, click on the "more labels" option and it should show up below your other folders.

How do I set up a spam filter in Gmail?

Setting your spam filter in Gmail is relatively simple. First, click on the Settings icon that looks like a gear. Then, navigate to “Filters and Blocked Addresses.” Choose “Create New Filter.” Click in the “From” section, and type in the email address from the sender that you want to keep out of your spam folder. Finally, click “Create Filter,” and you will now be able to view messages from this sender without navigating to the spam folder.

How do I unblock spam in Gmail?

This is another easy task that is like the last one. Go to the Settings icon that resembles a gear. From there, click on Settings. Then, click “Filters and Blocked Addresses.” You will now see a list of all of the email addresses that you have blocked on your account. Scroll to the email address that you want to unblock and click on “Unblock” on the right-hand side. Gmail will ask you to confirm that you want to unblock the sender. Click “Unblock” again, and you will now be able to receive messages from this sender.

Does Gmail automatically delete spam?

When spam first comes in, Gmail sends it to the spam folder without deleting it. However, any spam that has been sent to the spam folder for more than 30 days will be deleted automatically. This is a nice feature because it allows you to check your spam folder for certain messages that may not belong there. If it was automatically deleted, you may never receive a message that you have been waiting for. You can also manually delete the messages in your spam folder, or you can create custom filters that will automatically delete messages from certain domains or senders.

Related topics

Spam and authentication

- Advanced phishing and malware protection
- How sender authentication protects your domain
- Set up and manage email quarantines
- Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy

IRONSCALES

SAFER TOGETHER

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

To learn more, please visit **www.ironscales.com** today!