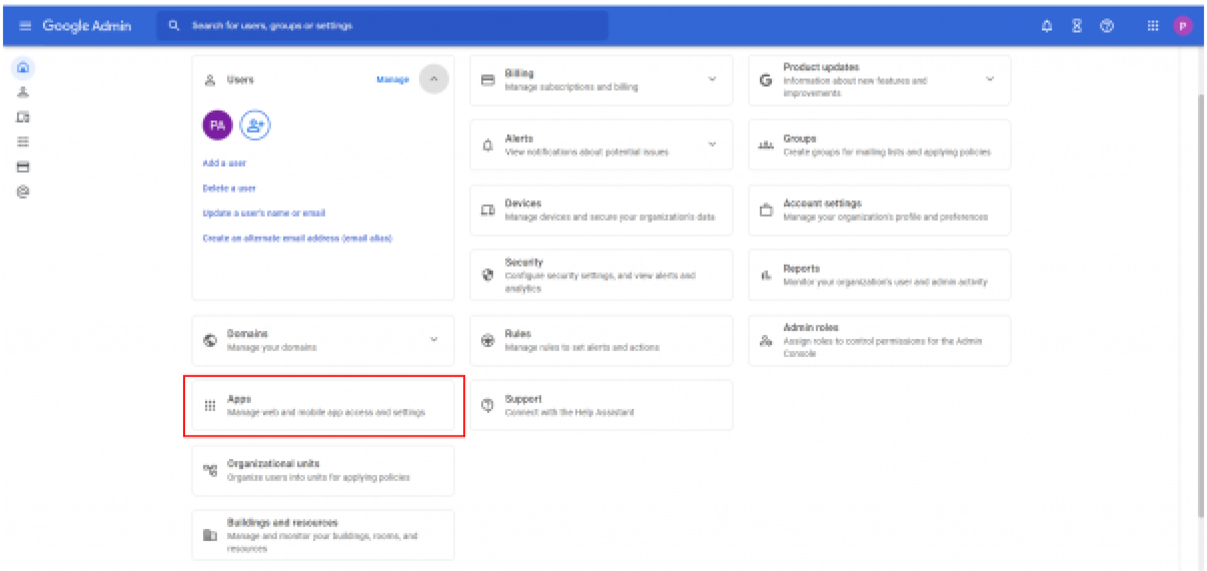
Google Workspace Whitelisting

There are several options in G Suite that can be adjusted to improve the Phishing Simulation Experience.

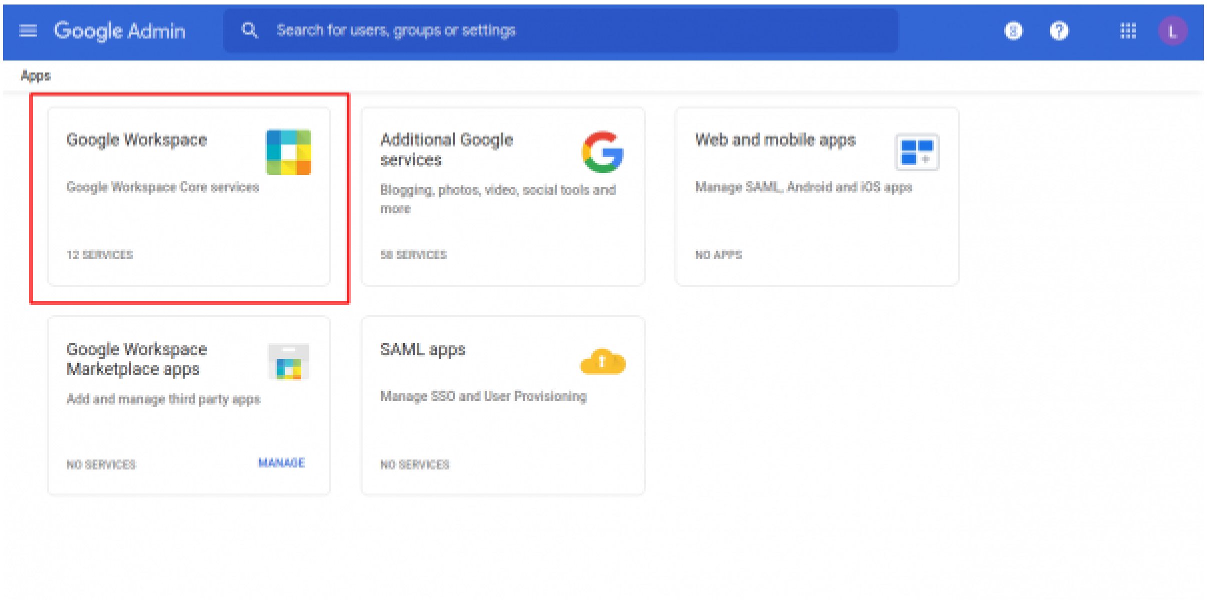
Whitelisting emails from LUCY.

Whitelist LUCY to receive emails from the appliance.

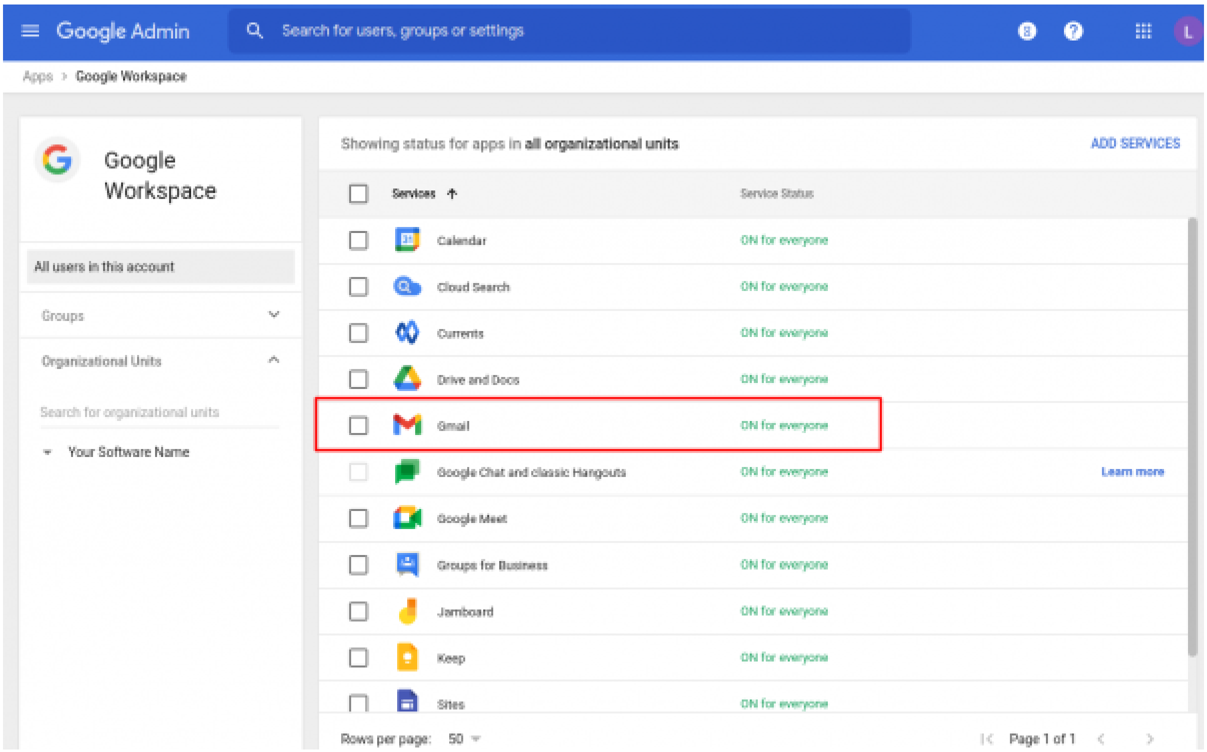
Log into admin.google.com, go to **"Apps"**:


Google Admin
Search for users, groups or settings
Users
Manage
PA
Add a user
Delete a user
Update a user's name or email
Create an alternate email address (email alias)
Billing
Manage subscriptions and billing
Product updates
Information about new features and improvements
Alerts
View notifications about potential issues
Groups
Create groups for mailing lists and applying policies
Devices
Manage devices and secure your organization's data
Account settings
Manage your organization's profile and preferences
Security
Configure security settings, and view alerts and analytics
Reports
Monitor your organization's user and admin activity
Domains
Manage your domains
Rules
Manage rules to set alerts and actions
Admin roles
Assign roles to control permissions for the Admin Console
Apps
Manage web and mobile app access and settings
Support
Connect with the Help Assistant
Organizational units
Organize users into units for applying policies
Buildings and resources
Manage and monitor your buildings, rooms, and resources

Navigate to **"Google Workspace"**:


Google Admin
Search for users, groups or settings
L
Apps
Google Workspace
Google Workspace Core services
12 SERVICES
Additional Google services
Blogging, photos, video, social tools and more
58 SERVICES
Web and mobile apps
Manage SAML, Android and iOS apps
NO APPS
Google Workspace Marketplace apps
Add and manage third party apps
NO SERVICES
MANAGE
SAML apps
Manage SSO and User Provisioning
NO SERVICES

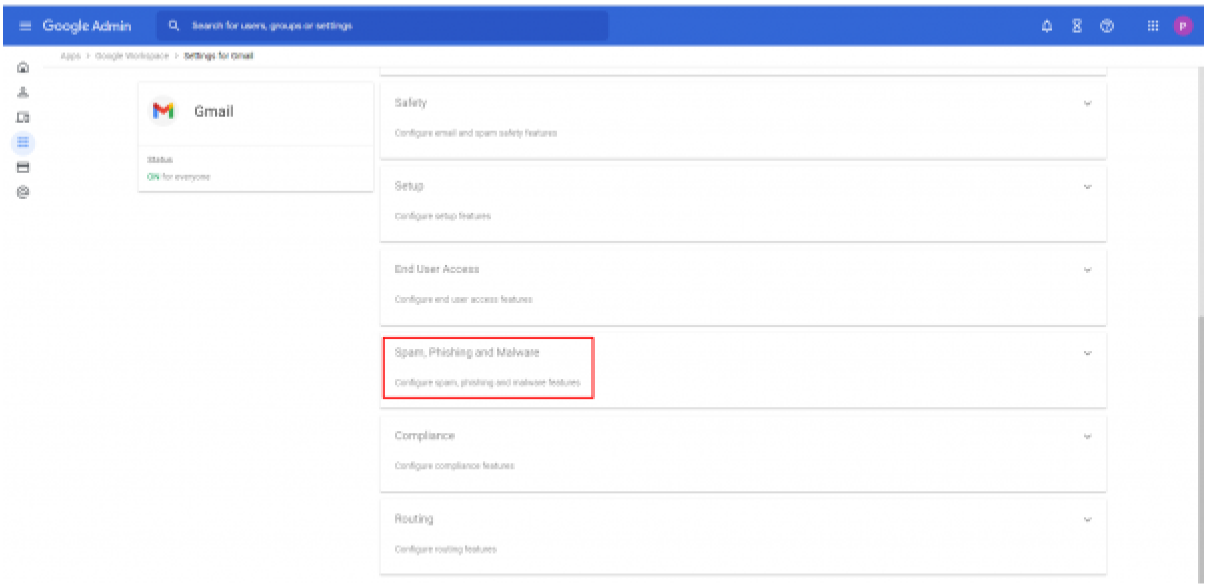
Go to **"Gmail"**:



Showing status for apps in **all organizational units**

Services	Service Status
Calendar	ON for everyone
Cloud Search	ON for everyone
Currents	ON for everyone
Drive and Docs	ON for everyone
Gmail	ON for everyone
Google Chat and classic Hangouts	ON for everyone
Google Meet	ON for everyone
Groups for Business	ON for everyone
Jamboard	ON for everyone
Keep	ON for everyone
Sites	ON for everyone

Choose the **"Spam, phishing, and malware"** at the very bottom of the list:



Google Admin
Search for users, groups or settings
Apps > Google Workspace > Settings for Gmail
Gmail
Status
ON for everyone

Safety
Configure email and spam safety features

Setup
Configure setup features

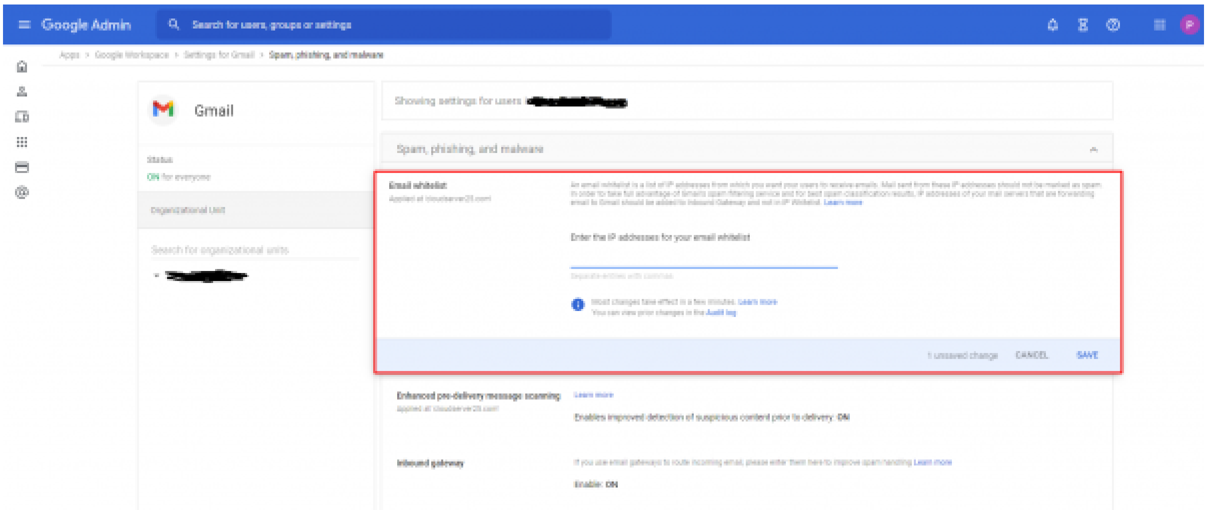
End User Access
Configure end user access features

Spam, Phishing and Malware
Configure spam, phishing and malware features

Compliance
Configure compliance features

Routing
Configure routing features

Add LUCY IPv4 to **"Email Whitelist"**. Click **"Save"**


Google Admin
Search for users, groups or settings
Apps > Google Workspace > Settings for Gmail > Spam, phishing, and malware
Gmail
Status
ON for everyone
Organizational Unit
Search for organizational units

Showing settings for users [redacted]

Spam, phishing, and malware

Email whitelist
Applied at cloudserver25.com

An email whitelist 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 Whitelist. Learn more

Enter the IP addresses for your email whitelist

Separate entries with commas

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

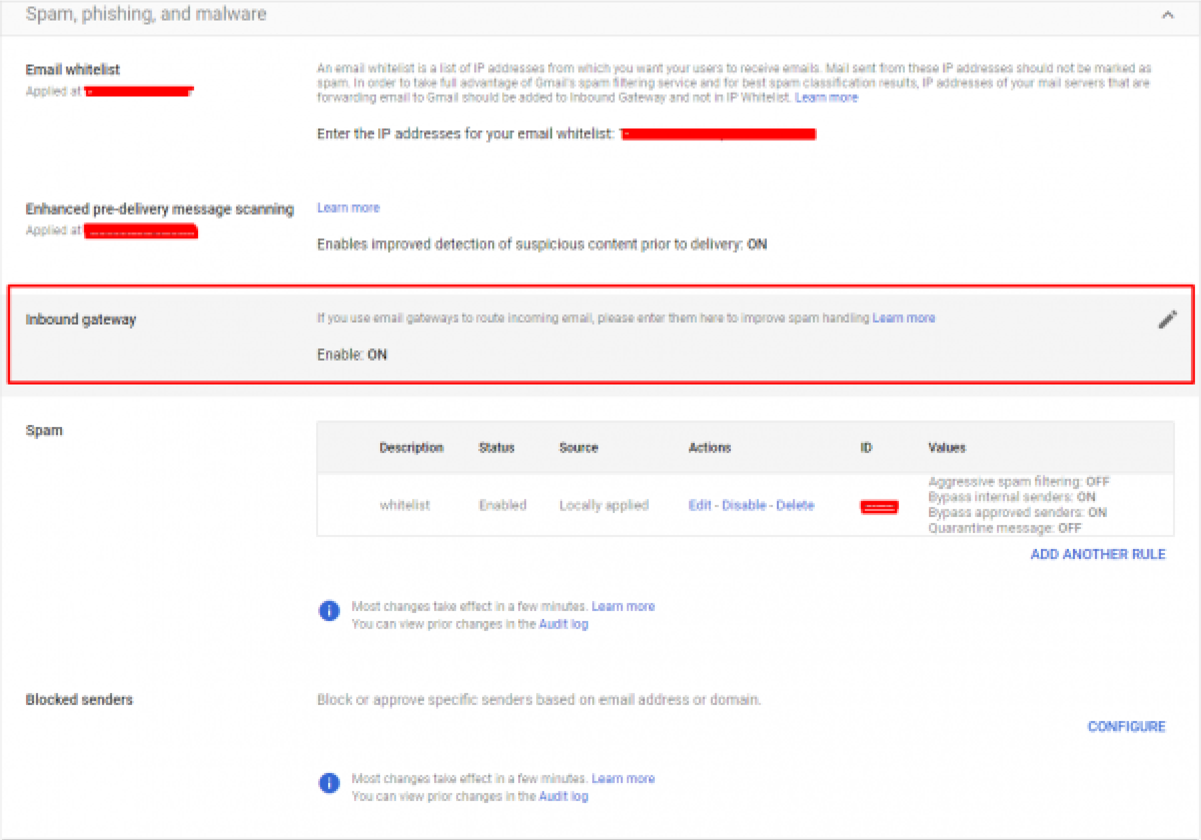
1 unsaved change CANCEL SAVE

Enhanced pre-delivery message scanning
Applied at cloudserver25.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: ON

As the result of steps above, G Suite will not reject email messages from LUCY host, however, if you do not want them to be considered as spam, please do some additional steps:

Go to **"Inbound Gateway"** configuration on the same menu.


Spam, phishing, and malware

Email whitelist
Applied at [redacted]

An email whitelist 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 Whitelist. Learn more

Enter the IP addresses for your email whitelist: [redacted]

Enhanced pre-delivery message scanning
Applied at [redacted]
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: ON

Spam

Description	Status	Source	Actions	ID	Values
whitelist	Enabled	Locally applied	Edit - Disable - Delete	[redacted]	Aggressive spam filtering: OFF Bypass internal senders: ON Bypass approved senders: ON Quarantine message: OFF

ADD ANOTHER RULE

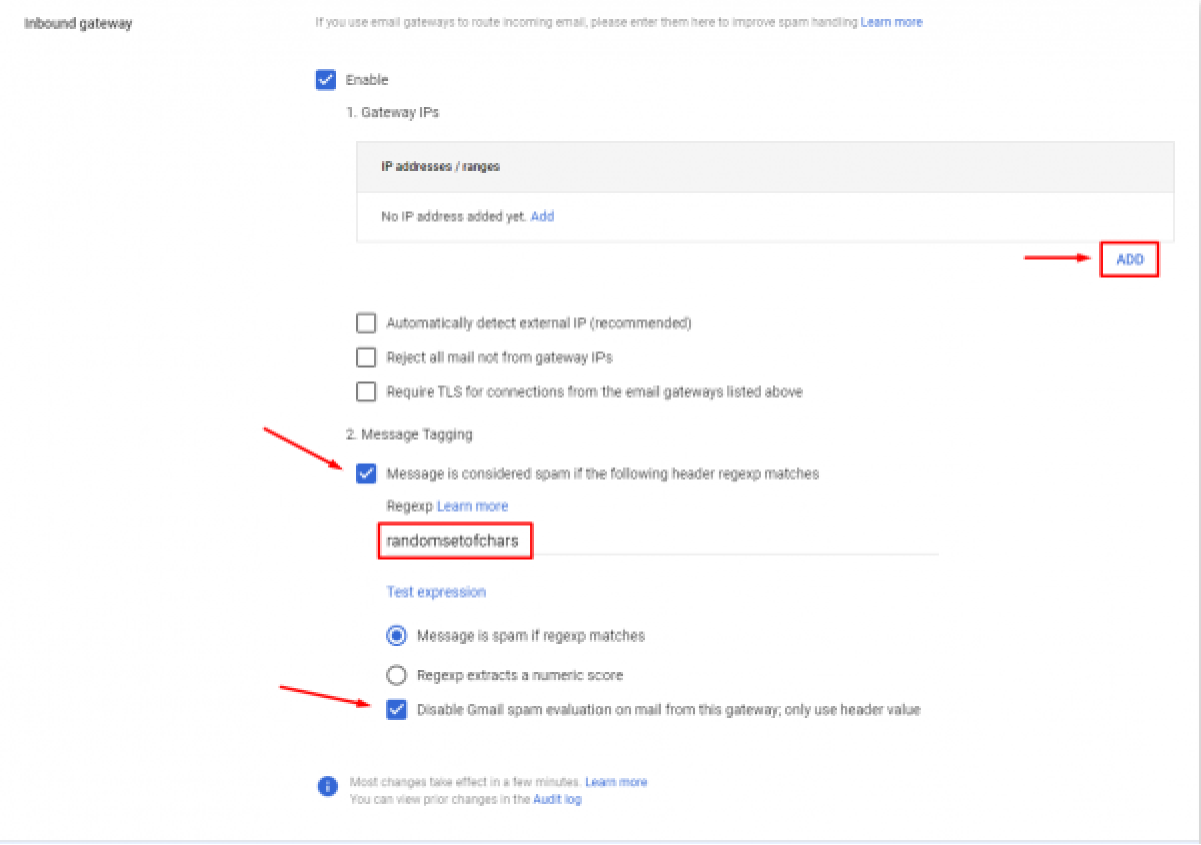
Most changes take effect in a few minutes. Learn more
You can view prior changes in the Audit log

Blocked senders
Block or approve specific senders based on email address or domain.

CONFIGURE

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

- Add LUCY IPv4.
- Activate Message Tagging.
- Add a random set of symbols to the Regular Expression field. Only emails with a header like this expression will be considered as spam.
- Check "*Disable Gmail spam evaluation on mail from this gateway; only use header value*".
- Click **"Save"**



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
No IP address added yet. Add

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

Regexp Learn more

randomsetofchars

Test expression

● Message is spam if regexp matches

○ Regexp extracts a numeric score

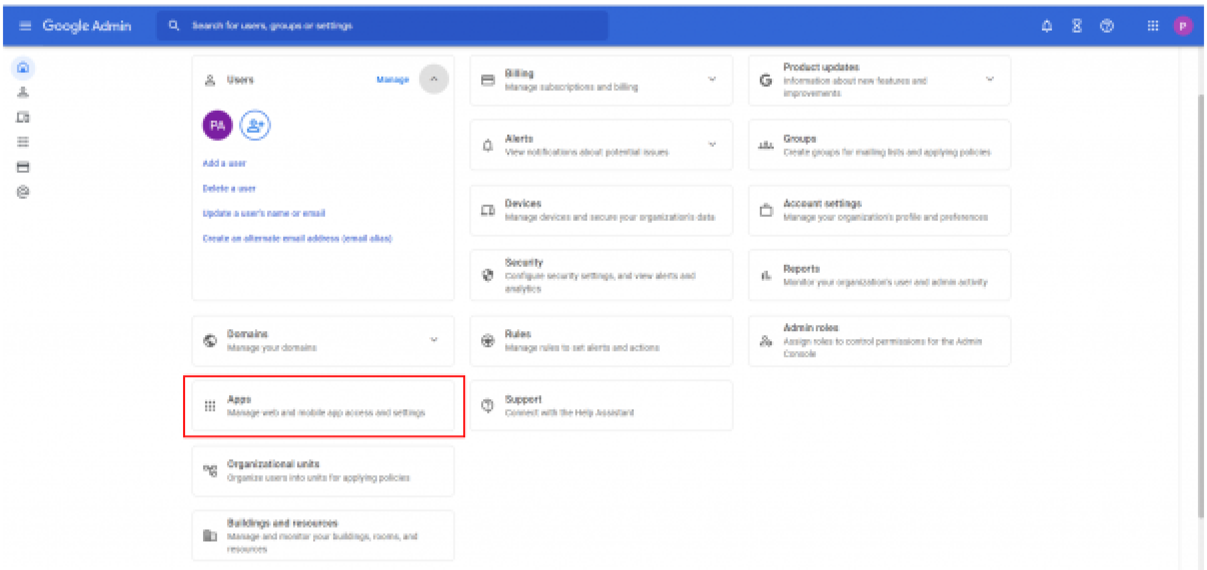
☑ Disable Gmail spam evaluation on mail from this gateway; only use header value

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

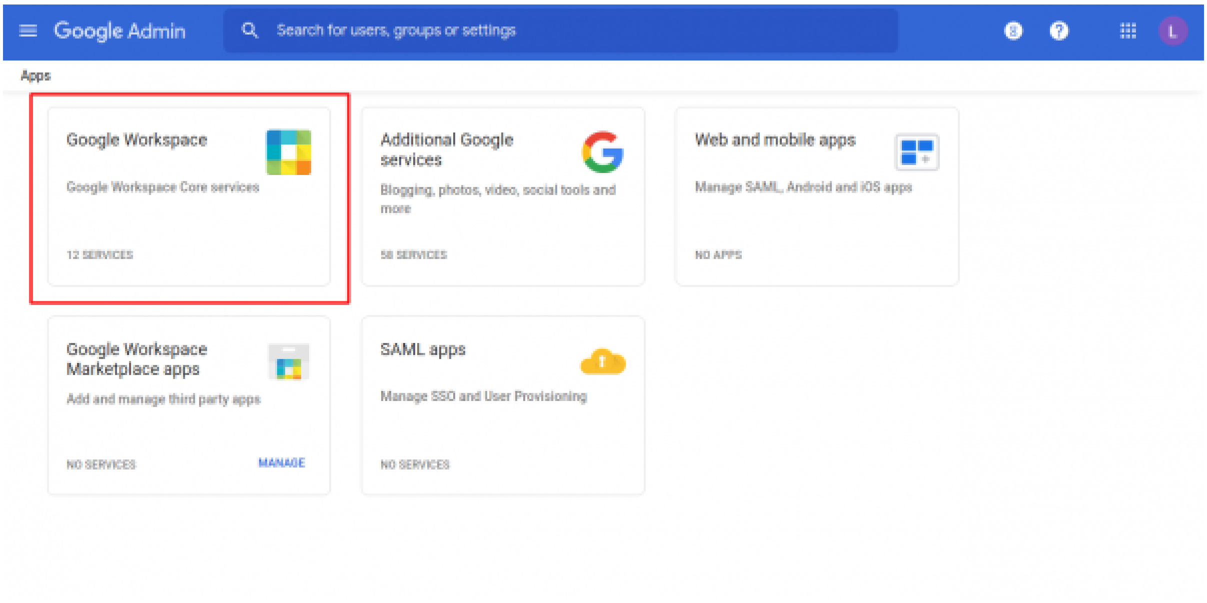
Bypassing spam by Email Header.

Inside of a campaign, it is possible to set a custom X-Mailer Header. G Suite can analyze the header to bypass SPAM detection.

Steps to configure: Log into admin.google.com, go to **"Apps"**.


Google Admin
Search for users, groups or settings
Users
Manage
PA
Add a user
Delete a user
Update a user's name or email
Create an alternate email address (email alias)
Billing
Manage subscriptions and billing
Product updates
Information about new features and improvements
Alerts
View notifications about potential issues
Groups
Create groups for mailing lists and applying policies
Devices
Manage devices and secure your organization's data
Account settings
Manage your organization's profile and preferences
Security
Configure security settings, and view alerts and analytics
Reports
Monitor your organization's user and admin activity
Domains
Manage your domains
Rules
Manage rules to set alerts and actions
Admin roles
Assign roles to control permissions for the Admin Console
Apps
Manage web and mobile app access and settings
Support
Connect with the Help Assistant
Organizational units
Organize users into units for applying policies
Buildings and resources
Manage and monitor your buildings, rooms, and resources

Go to **"Google Workspace"**.



Google Workspace
Google Workspace Core services
12 SERVICES

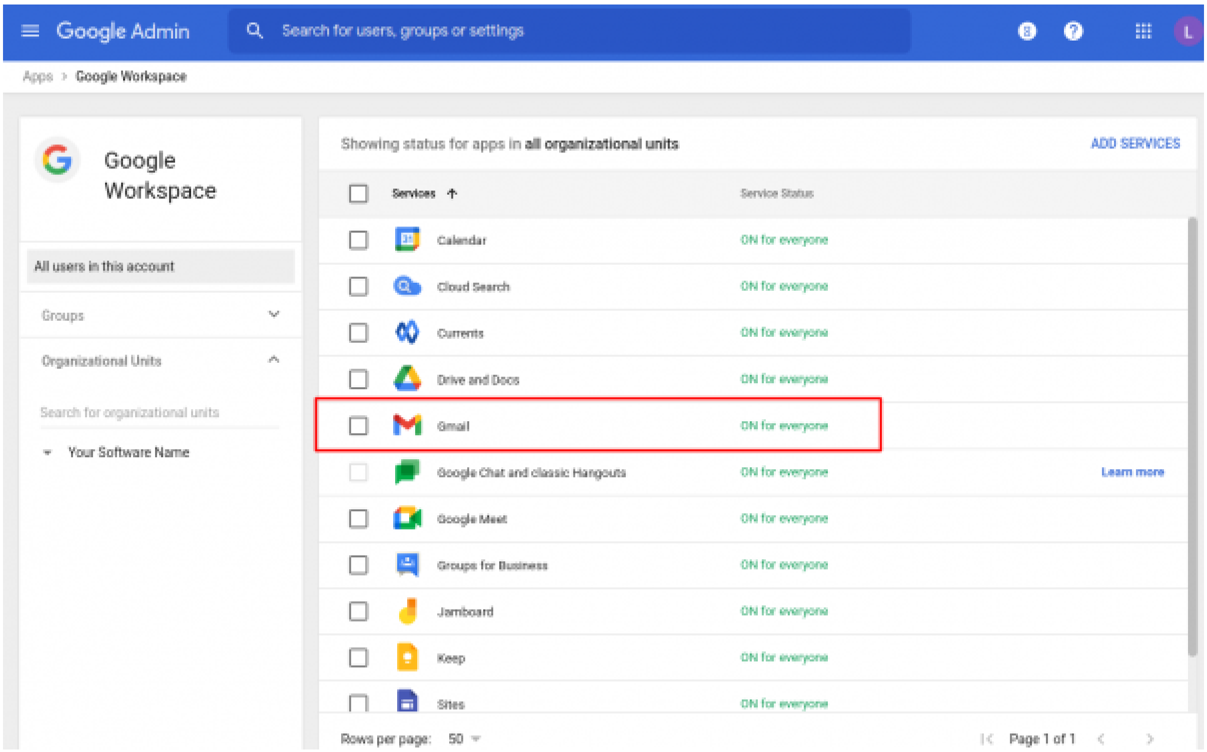
Additional Google services
Blogging, photos, video, social tools and more
58 SERVICES

Web and mobile apps
Manage SAML, Android and iOS apps
NO APPS

Google Workspace Marketplace apps
Add and manage third party apps
NO SERVICES MANAGE

SAML apps
Manage SSO and User Provisioning
NO SERVICES

Go to **"Gmail"**.

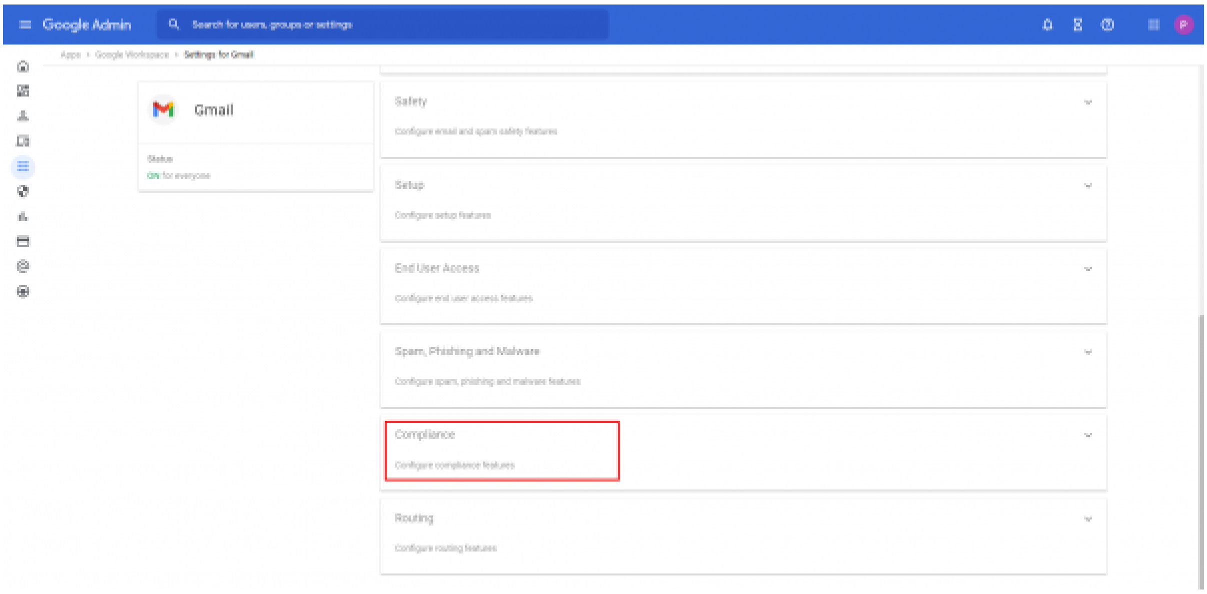


Showing status for apps in **all organizational units**

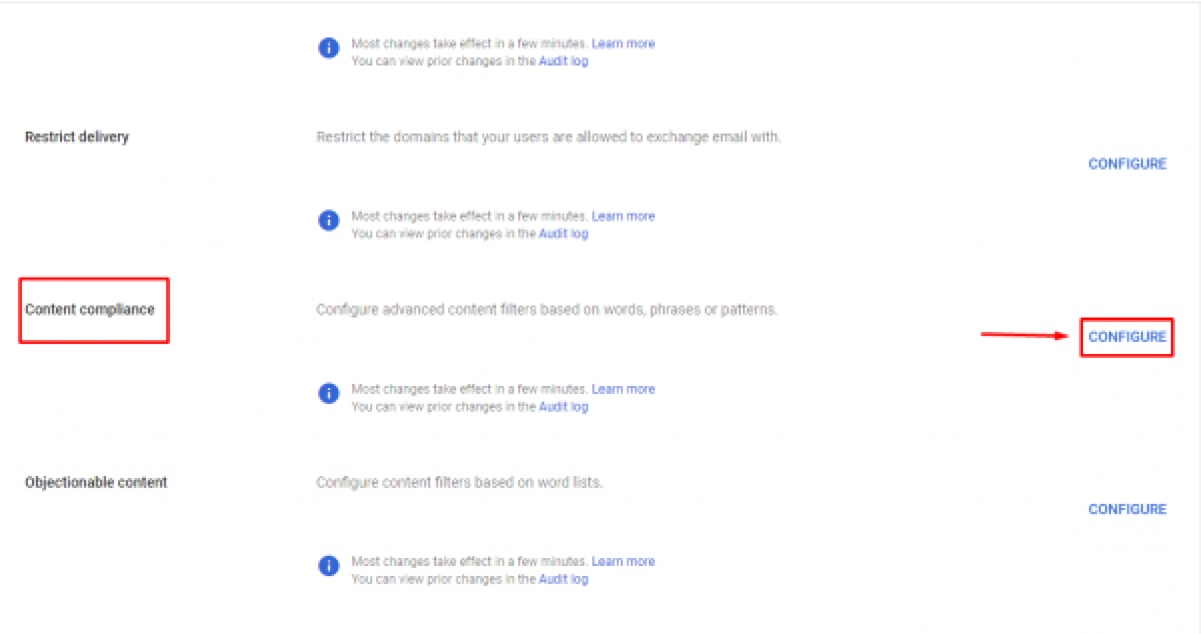
☐ Services ↑	Service Status	
☐ Calendar	ON for everyone	
☐ Cloud Search	ON for everyone	
☐ Currents	ON for everyone	
☐ Drive and Docs	ON for everyone	
☐ Gmail	ON for everyone	
☐ Google Chat and classic Hangouts	ON for everyone	Learn more
☐ Google Meet	ON for everyone	
☐ Groups for Business	ON for everyone	
☐ Jamboard	ON for everyone	
☐ Keep	ON for everyone	
☐ Sites	ON for everyone	

Rows per page: 50 Page 1 of 1

Go to **"Compliance"** at the very bottom.


Google Admin
Search for users, groups or settings
Apps › Google Workspace › Settings for Gmail
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

Go to **"Content Compliance"** and click **"Configure"**.



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

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

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

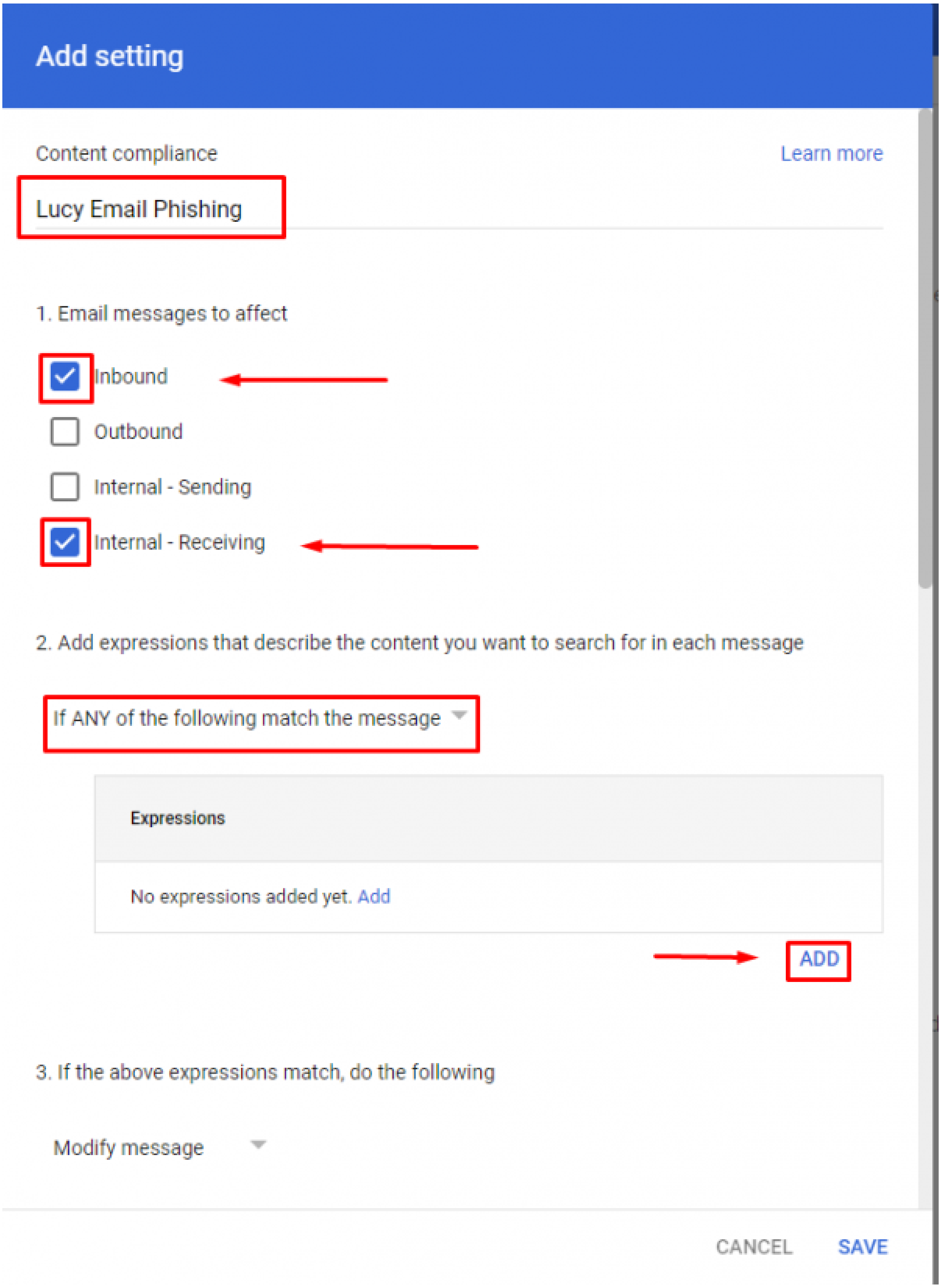
Content compliance
Configure advanced content filters based on words, phrases or patterns.
CONFIGURE

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

Objectionable content
Configure content filters based on word lists.
CONFIGURE

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

- Add description (e.g. "Lucy Email Phishing")
- Check **"Inbound"**
- Check **"Internal - receiving"**
- Select **"If ANY of the following match the message"**



Add setting

Content compliance

Lucy Email Phishing

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

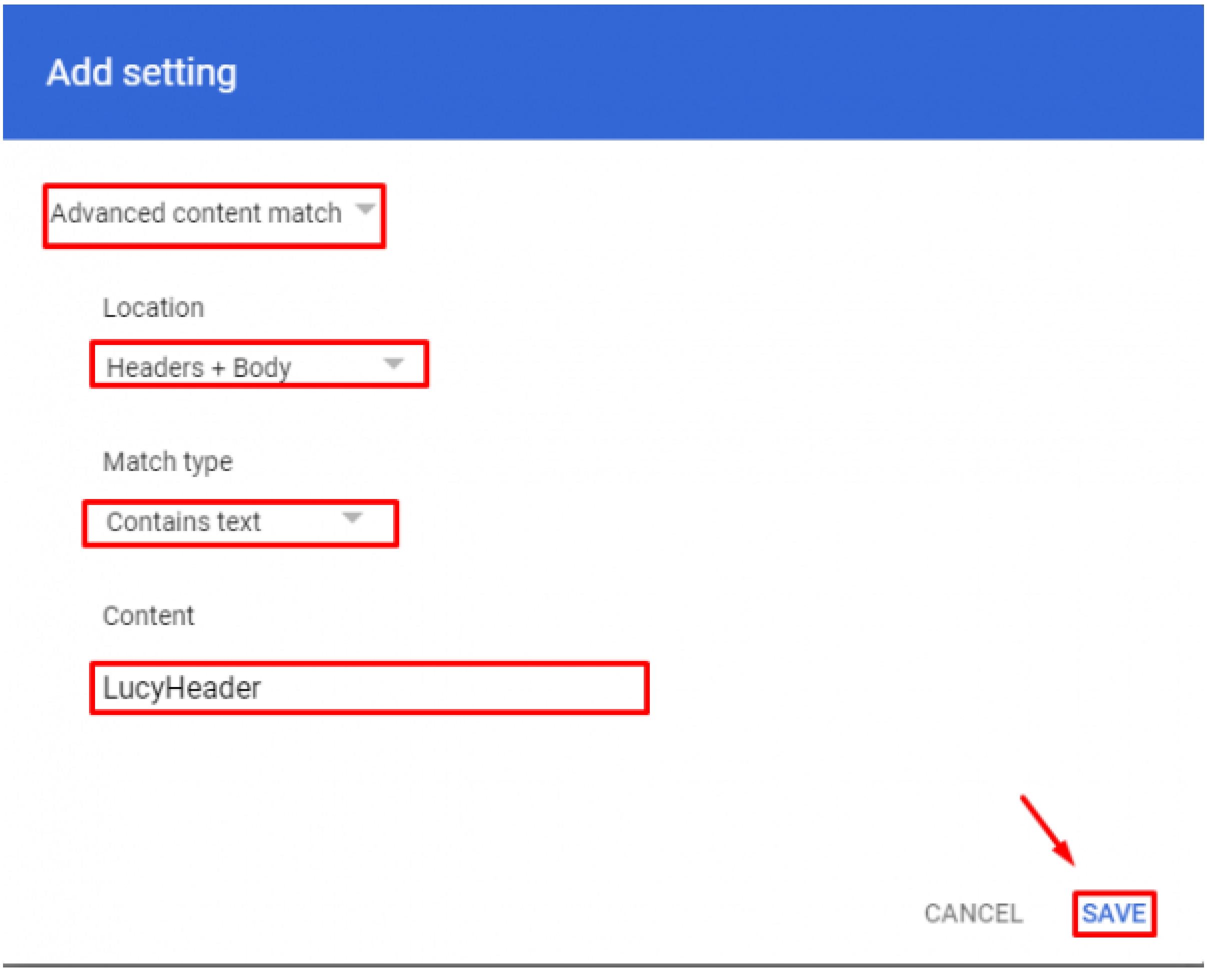
If ANY of the following match the message

Expressions
No expressions added yet. Add

3. If the above expressions match, do the following

Modify message

- Click **Add Expression** → **Advanced content match** → **Headers + Body** → **Contains text**.
- Content → Input your LUCY X-Mailer Header[1] (e.g. "LucyHeader") and click **Save**.



Add setting

Advanced content match

Location

Headers + Body

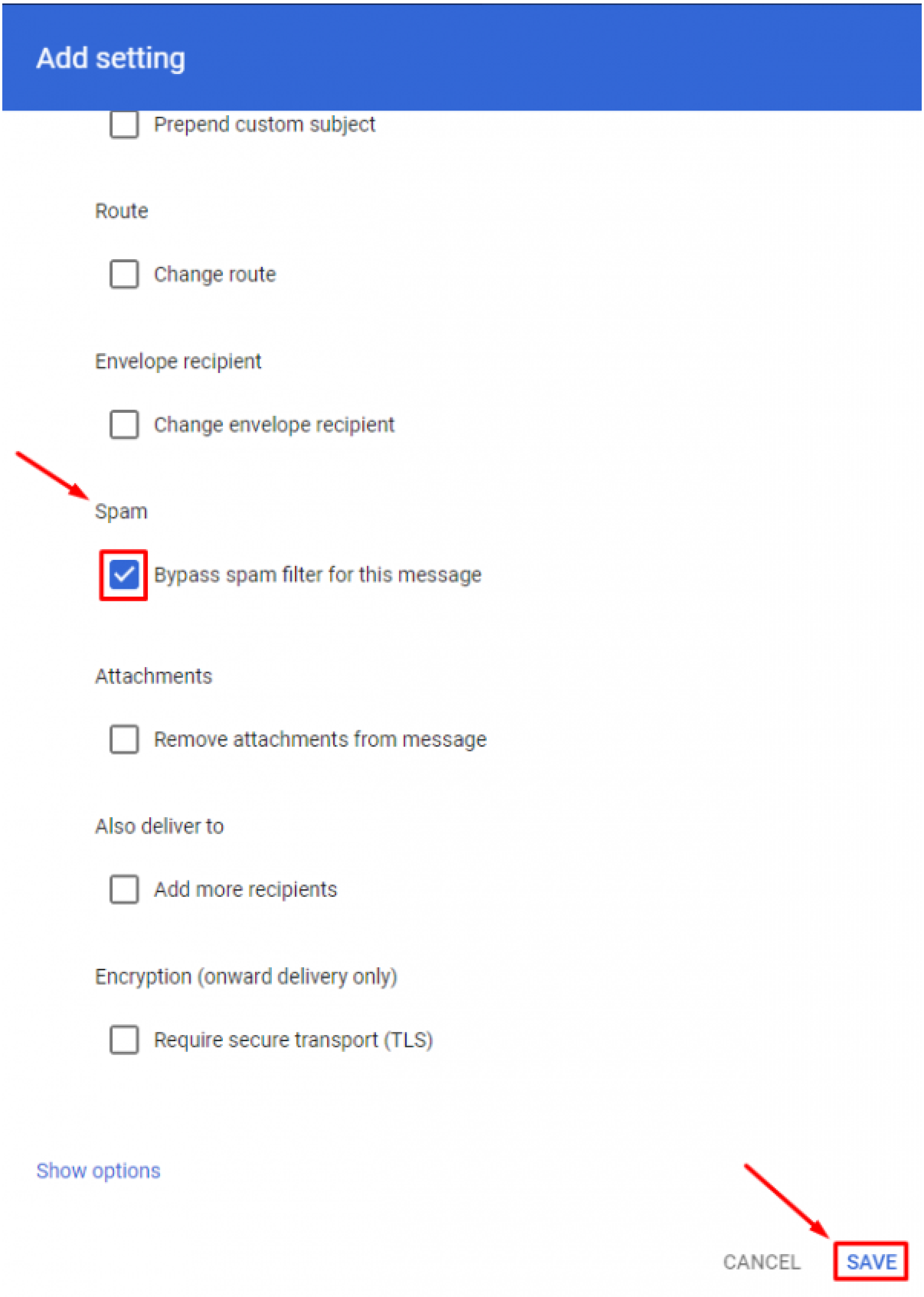
Match type

Contains text

Content

LucyHeader

- Scroll down to the **"Spam"** section and activate **"Bypass spam filter for this message"**.
- Click **"Save"**.



Add setting

☐ Prepend custom subject

Route

☐ Change route

Envelope recipient

☐ Change envelope recipient

Spam

☑ Bypass spam filter for this message

Attachments

☐ Remove attachments from message

Also deliver to

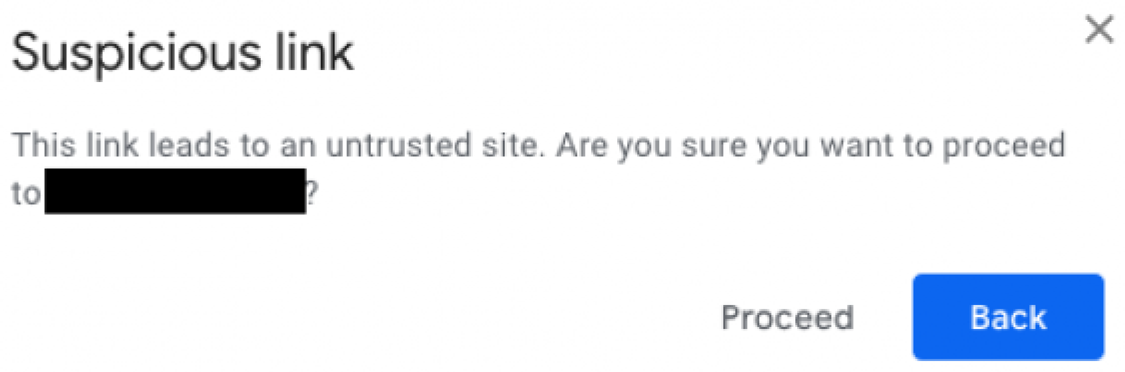
☐ Add more recipients

Encryption (onward delivery only)

☐ Require secure transport (TLS)

Suspicious link issue

Sometimes a warning pop-up window appears when you are trying to open link from LUCY email.



Suspicious link

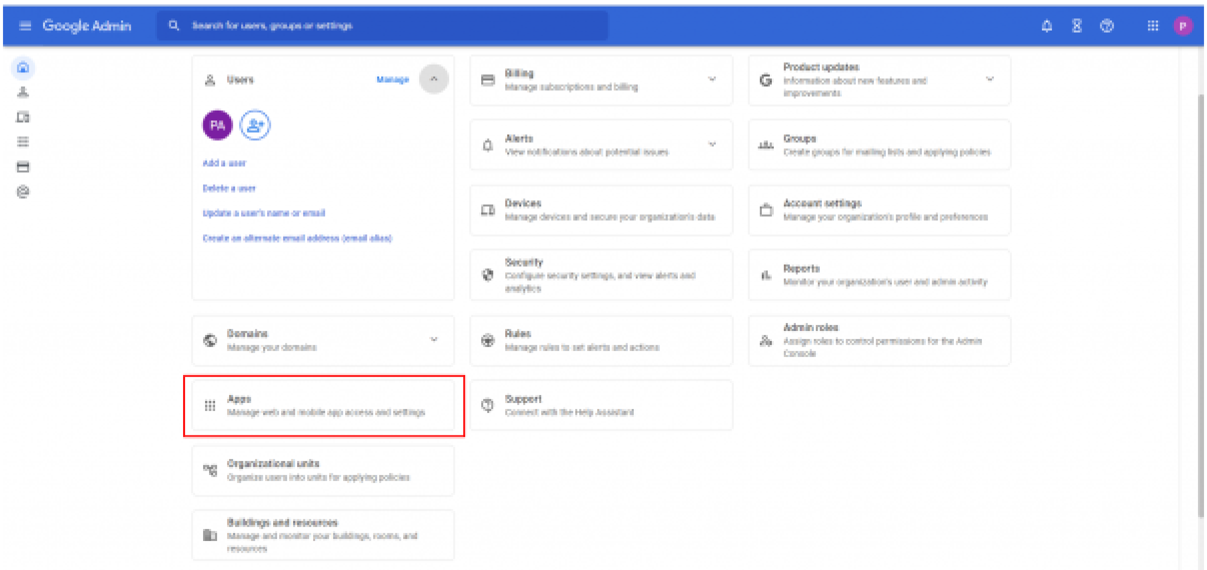
This link leads to an untrusted site. Are you sure you want to proceed to [redacted]?

First of all, please enable SSL in LUCY campaign. More info can be found here.

It can be that Let's Encrypt certificate is not enough, so we recommend to obtain a paid certificate. You can contact our support team via support@lucysecurity.com or any SSL vendor you like.

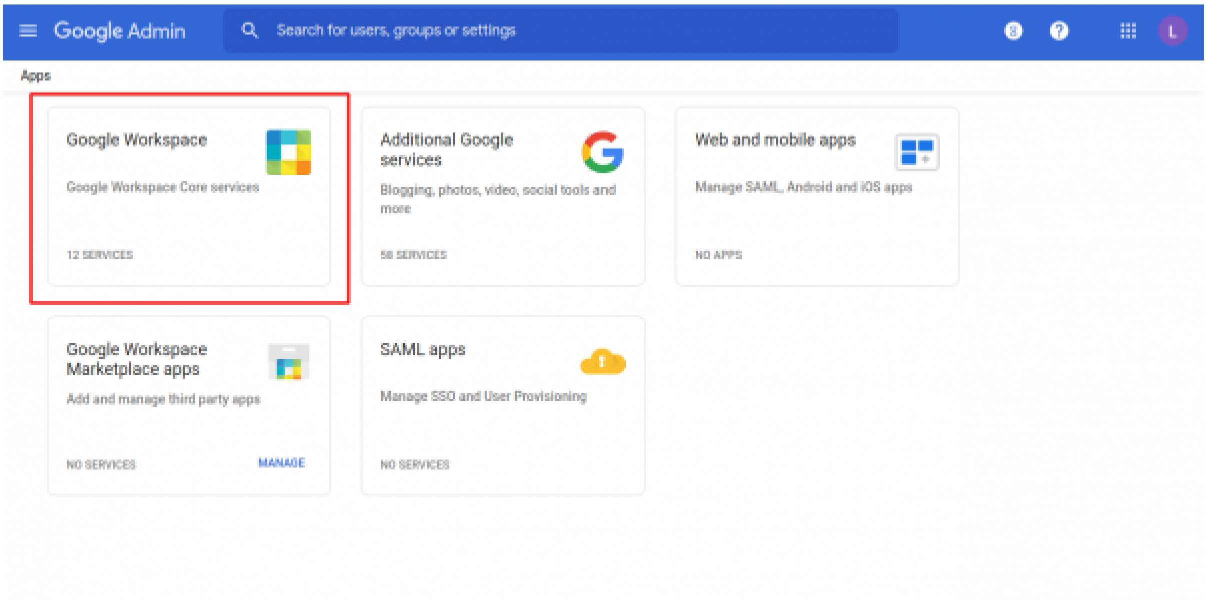
However, there are known cases when even a paid certificate can not solve the issue. In this case, you can try to disable this pop-up on G Suite side. Untrusted domains from suspicious emails still will be not affected. "Gmail clients will show a warning prompt when users click on any link in email to untrusted domains (does not work on IMAP/POP email clients). If you don't activate this feature, warnings will only be shown for clicks to untrusted domains from suspicious emails."

Steps to configure: Log into admin.google.com, go to **"Apps"**.



Google Admin
Search for users, groups or settings
Users
Manage
PA
Add a user
Delete a user
Update a user's name or email
Create an alternate email address (email alias)
Billing
Manage subscriptions and billing
Product updates
Information about new features and improvements
Alerts
View notifications about potential issues
Groups
Create groups for mailing lists and applying policies
Devices
Manage devices and secure your organization's data
Account settings
Manage your organization's profile and preferences
Security
Configure security settings, and view alerts and analytics
Reports
Monitor your organization's user and admin activity
Domains
Manage your domains
Rules
Manage rules to set alerts and actions
Admin roles
Assign roles to control permissions for the Admin Console
Apps
Manage web and mobile app access and settings
Support
Connect with the Help Assistant
Organizational units
Organize users into units for applying policies
Buildings and resources
Manage and monitor your buildings, rooms, and resources
P

Navigate to **"Google Workspace"**:



Google Workspace
Google Workspace Core services
12 SERVICES

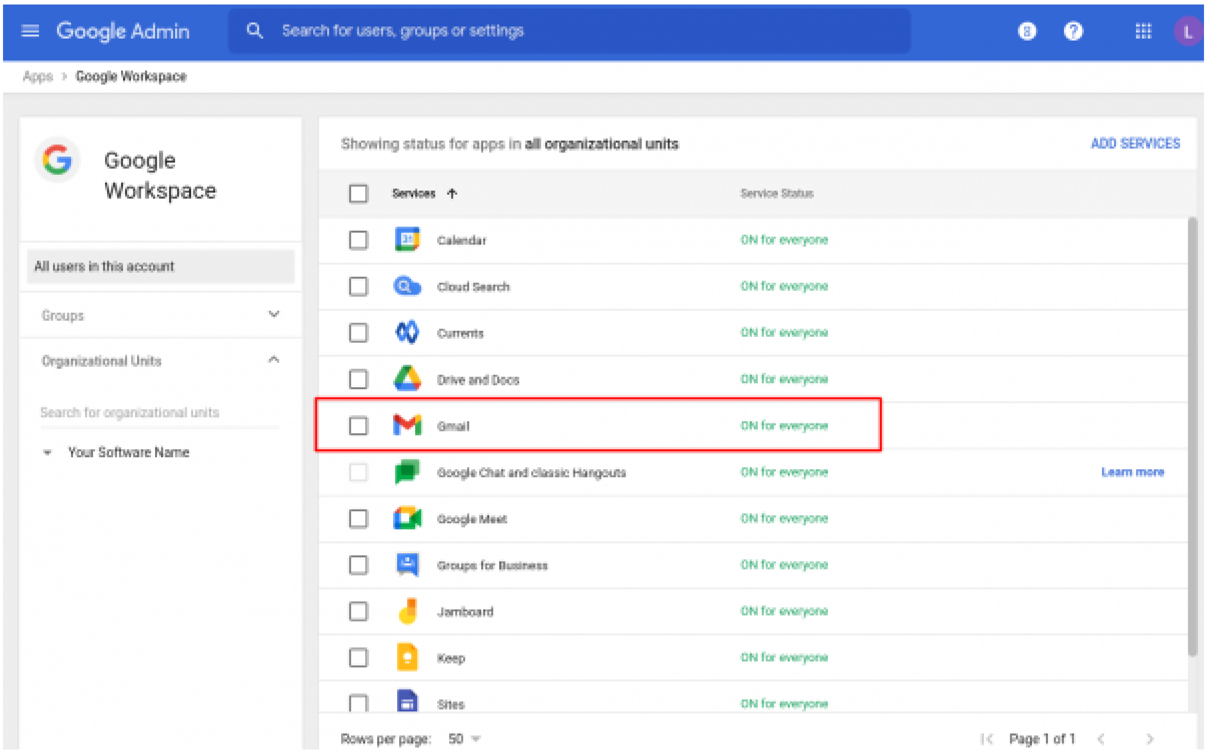
Additional Google services
Blogging, photos, video, social tools and more
58 SERVICES

Web and mobile apps
Manage SAML, Android and iOS apps
NO APPS

Google Workspace Marketplace apps
Add and manage third party apps
NO SERVICES MANAGE

SAML apps
Manage SSO and User Provisioning
NO SERVICES

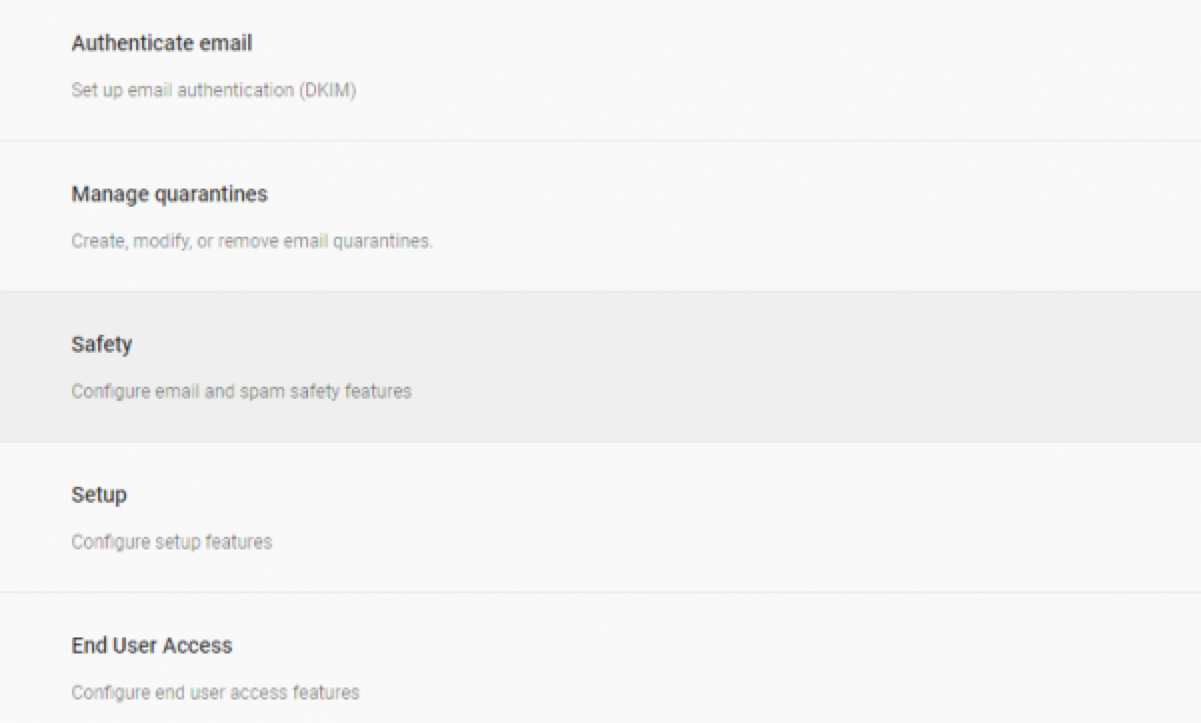
Go to **"Gmail"**.



Showing status for apps in **all organizational units**

Services	Service Status
□ Calendar	ON for everyone
□ Cloud Search	ON for everyone
□ Currents	ON for everyone
□ Drive and Docs	ON for everyone
□ Gmail	ON for everyone
Google Chat and classic Hangouts	ON for everyone
□ Google Meet	ON for everyone
□ Groups for Business	ON for everyone
□ Jamboard	ON for everyone
□ Keep	ON for everyone
□ Sites	ON for everyone

Go to **"Safety"**.



Authenticate email

Set up email authentication (DKIM)

Manage quarantines

Create, modify, or remove email quarantines.

Safety

Configure email and spam safety features

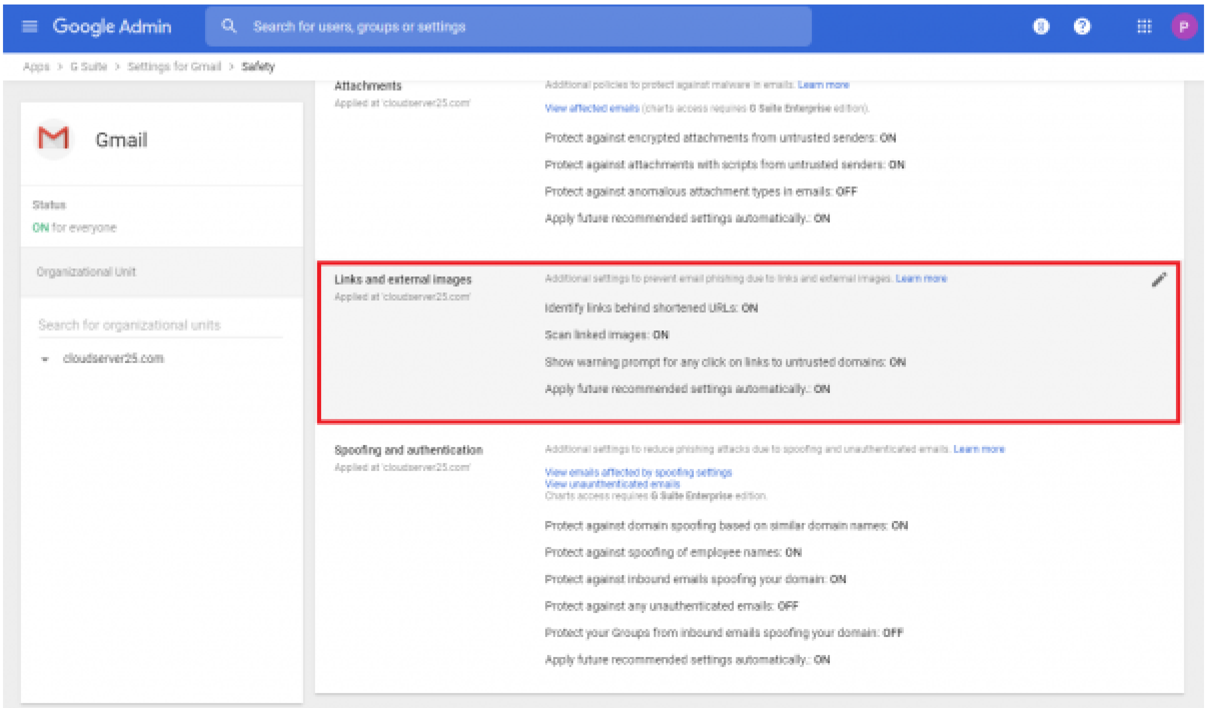
Setup

Configure setup features

End User Access

Configure end user access features

Go to **"Links and external images"**.



Google Admin
Search for users, groups or settings
Apps > G Suite > Settings for Gmail > Safety
Gmail
Organizational Unit
Search for organizational units
cloudserver25.com

Status
ON for everyone

Attachments
Applied at 'cloudserver25.com'

Additional policies to protect against malware in emails. Learn more

View affected emails (charts access requires G Suite Enterprise edition).

Protect against encrypted attachments from untrusted senders: ON

Protect against attachments with scripts from untrusted senders: ON

Protect against anomalous attachment types in emails: OFF

Apply future recommended settings automatically.: ON

Links and external images
Applied at 'cloudserver25.com'

Additional settings to prevent email phishing due to links and external images. Learn more

Identify links behind shortened URLs: ON

Scan linked images: ON

Show warning prompt for any click on links to untrusted domains: ON

Apply future recommended settings automatically.: ON

Spoofing and authentication
Applied at 'cloudserver25.com'

Additional settings to reduce phishing attacks due to spoofing and unauthenticated emails. Learn more

View emails affected by spoofing settings
View unauthenticated emails
Charts access requires G Suite Enterprise edition.

Protect against domain spoofing based on similar domain names: ON

Protect against spoofing of employee names: ON

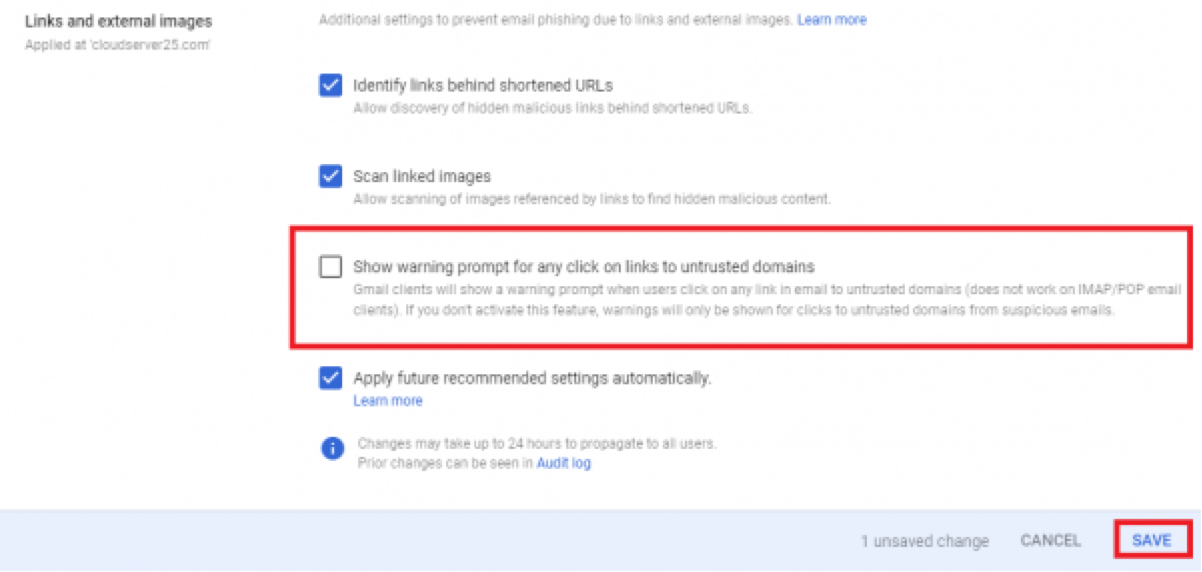
Protect against inbound emails spoofing your domain: ON

Protect against any unauthenticated emails: OFF

Protect your Groups from inbound emails spoofing your domain: OFF

Apply future recommended settings automatically.: ON

Deactivate **"Show warning prompt for any click on links to untrusted domains"** and click **"Save"**.



Links and external images
Applied at 'cloudserver25.com'

Additional settings to prevent email phishing due to links and external images. Learn more

☑ Identify links behind shortened URLs
Allow discovery of hidden malicious links behind shortened URLs.

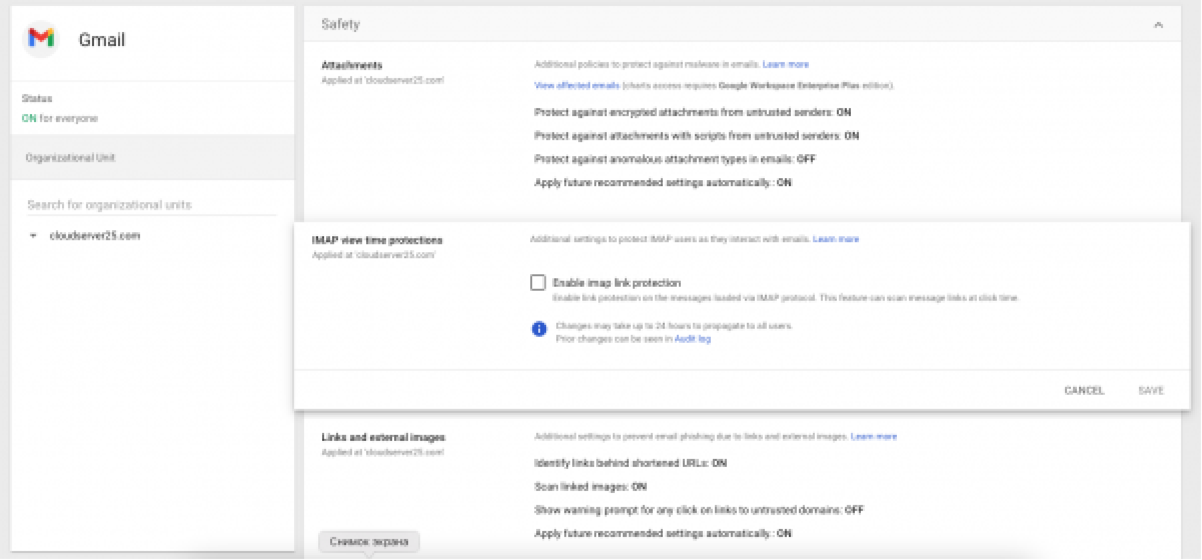
☑ Scan linked images
Allow scanning of images referenced by links to find hidden malicious content.

☐ Show warning prompt for any click on links to untrusted domains
Gmail clients will show a warning prompt when users click on any link in email to untrusted domains (does not work on IMAP/POP email clients). If you dont activate this feature, warnings will only be shown for clicks to untrusted domains from suspicious emails.

☑ Apply future recommended settings automatically.
Learn more

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

Gsuite can scan links inside of phishing simulation emails which can cause false-positives. The feature is called **"IMAP view time protections"**.



Attachments
Applied at 'cloudserver25.com'

Additional policies to protect against malware in emails. Learn more
View affected emails (charts access requires Google Workspace Enterprise Plus edition).

Protect against encrypted attachments from untrusted senders: ON
Protect against attachments with scripts from untrusted senders: ON
Protect against anomalous attachment types in emails: OFF
Apply future recommended settings automatically : ON

IMAP view time protections
Applied at 'cloudserver25.com'

Additional settings to protect IMAP users as they interact with emails. Learn more

☐ Enable imap link protection
Enable link protection on the messages loaded via IMAP protocol. This feature can scan message links at click time.

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

Links and external images
Applied at 'cloudserver25.com'

Additional settings to prevent email phishing due to links and external images. Learn more

Identify links behind shortened URLs: ON
Scan linked images: ON
Show warning prompt for any click on links to untrusted domains: OFF
Apply future recommended settings automatically : ON

[1]

LUCY X-Mailer Header is being configured in your campaign, message section, find more here

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=gsuite_whitelisting

Last update: **2021/12/21 19:41**