

Whitelist in Google Workspace

Whitelisting Simulated Phishing in Google Workspace (Gmail)

For Secure Practice Simulation Emails

This step-by-step guide is intended for **Google Workspace administrators** to allow simulated phishing emails from **Secure Practice** by properly configuring Gmail to recognize and accept messages from specific IP addresses.

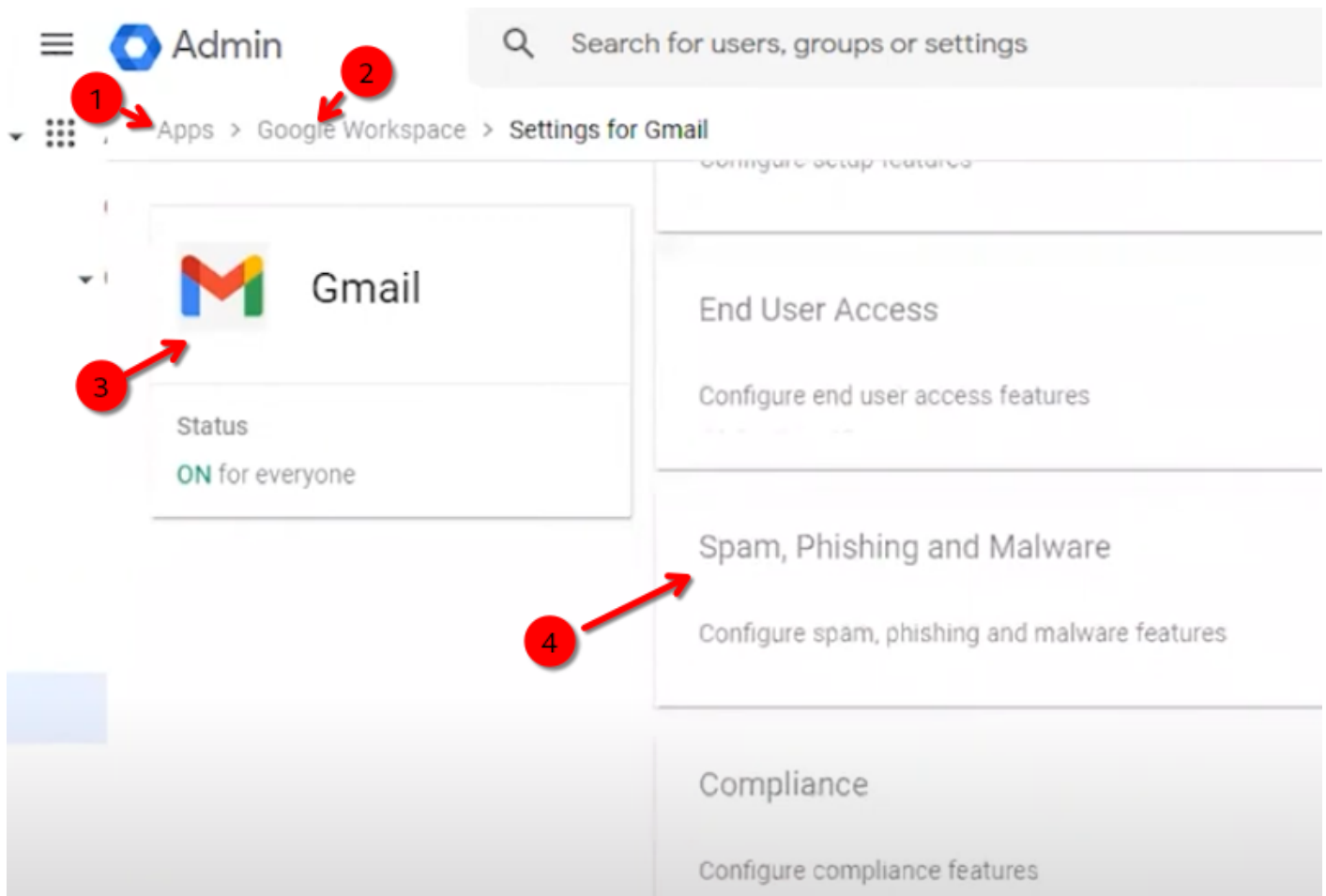
“ **Note:** You must have an **admin role** in the Google Workspace Admin Console to perform these actions.

Step 1: Access the Admin Console

1. Visit <https://admin.google.com>
2. Sign in using your **administrator account**

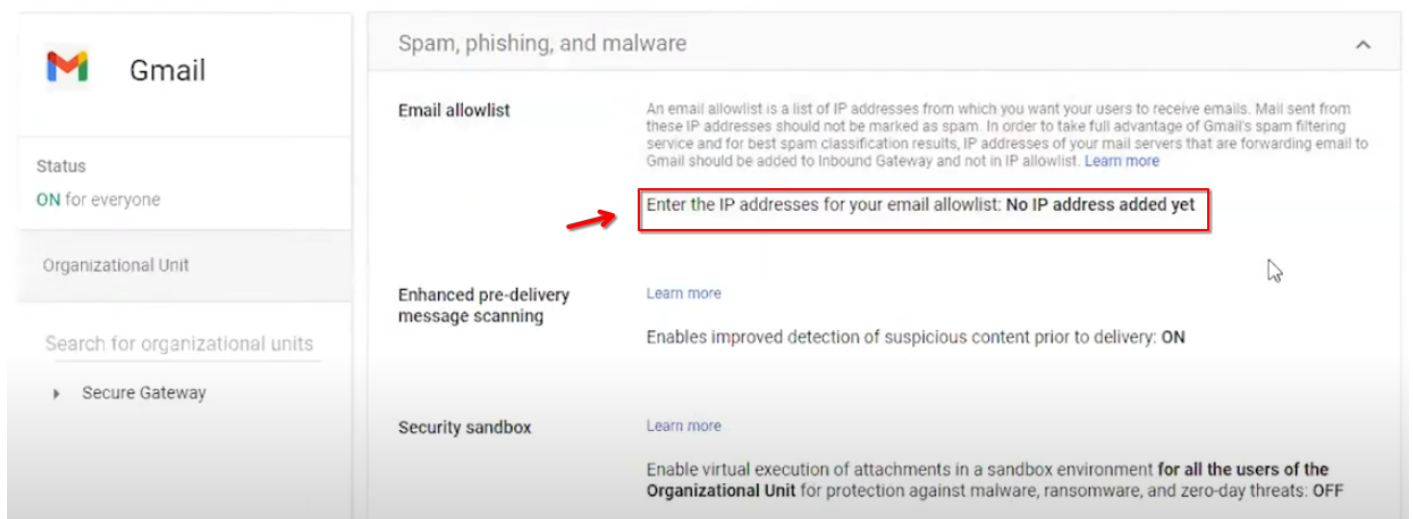
Step 2: Navigate to Gmail Settings

1. In the left-hand menu, go to:
Apps → Google Workspace → Gmail
2. Under Gmail settings, click on **Spam, Phish and Malware**



Step 3: Add IPs to the Email Allowlist

1. Click on **Email allowlist**
 - **35.153.237.243(Mail Server)**
 - **107.22.65.180(Landing Page)**
2. Enter the following IP addresses:
3. Click **Save**



Step 4: Configure Inbound Gateway

This step ensures that Gmail treats the IP addresses above as **internal senders**, preventing SPF or DMARC validation and suppressing warnings to end-users.

1. Scroll down to the **Inbound Gateway** section
2. If not already enabled, click the **Enable** button
3. In the **Gateway IPs** field, enter the same IP addresses listed earlier
4. Optional:
 - Enable **Automatic detect external IP**
 - **Do not** enable "Reject all mail not from gateway IPs" unless already required—this may block all mail delivery if not properly configured
 - Enable **Require TLS for connections**

The screenshot shows the Gmail administrative interface for the 'Secure Gateway' section. The left sidebar contains the Gmail logo, status 'ON for everyone', and a search bar. The main content area is titled '1. Gateway IPs'. It features an 'Enable' checkbox (callout 1), a text input field for 'IP addresses / ranges' (callout 2) with a placeholder 'No IP address added yet. Add' and an 'ADD' button, and three unchecked checkboxes: 'Automatically detect external IP (recommended)' (callout 3), 'Reject all mail not from gateway IPs', and 'Require TLS for connections from the email gateways listed above' (callout 4). Below this is the '2. Message Tagging' section (callout 5), which has a checked checkbox 'Message is considered spam if the following header regexp matches', a 'Regexp Learn more' link, and a text input field containing the string 'brksjrumcldotrcgsfbvn'. A 'Test expression' button is located at the bottom of this section.

Step 5: Configure Message Tagging

1. Under the **Message Tagging** section:
 - Check "**Message is considered spam if the following header regexp matches**"
 - Enter a **unique, random string** : fg2jl0ah45oahtTK56SGD23fhk2k
 - Check "**Disable Gmail spam evaluation**"

This ensures Gmail skips its spam analysis for messages from the configured IPs.

2. Message Tagging

☒ Message is considered spam if the following header regexp matches

Regexp [Learn more](#)

[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

Step 6: Bypass Spam Filters for Trusted Senders

1. Still under Gmail settings, go to the **Spam** section
2. Click **Configure** to create a spam filter bypass rule
3. Check: **"Bypass spam filters for messages received from addresses or domains"**
4. Click **Create or edit list** and add the following senders:
 - slackj.com
 - ttrelli.com
 - airbnd.cc
 - attlassians.com
 - eebbey.com
 - lastpass.net
 - my1psswords.com
 - zooms.cc
5. For flexibility, uncheck **"Authentication required"** for
6. Save the address list and the new spam bypass policy

Add setting

Spam

Learn more

Secure Practice

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.

Secure Practice (2)

Don't use

Use existing list

Create or edit list

☐

Put spam in administrative quarantine

Default

CANCEL

SAVE

Step 7: Adding Message Header in Compliance

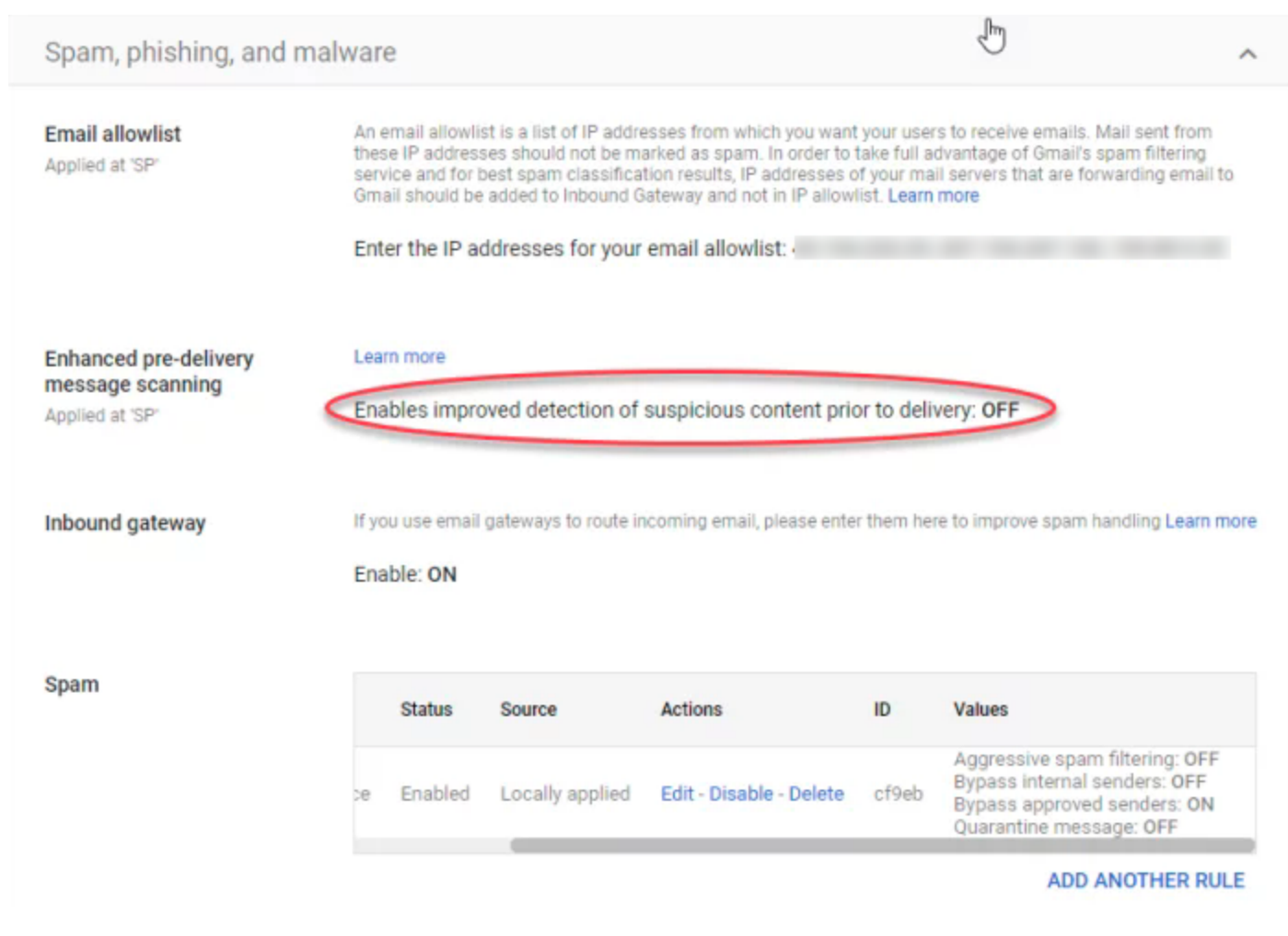
1. Navigate to the **Compliance** section in the Google Workspace Admin console.
2. Go to the **Content Compliance** subsection.
3. Click **Configure** or **Add Another**, depending on whether a rule has already been added. This will open the **Add Setting** pop-up window.
4. In the **Content compliance** field, provide a clear description for the rule, such as **"CyTech Whitelisting"**.
5. Under **Email messages to affect**, check the **Inbound** box.
6. In the **Expressions** section, click **Add** to open a new pop-up window.
7. In the first drop-down menu, select **Metadata match**.
8. From the **Attribute** drop-down menu, choose **Source IP**.
9. In the **Match type** drop-down menu, select **Source IP is**.
10. In the value field, enter one of CyTech's IP addresses.
 - **35.153.237.243(Mail Server)**
 - **107.22.65.180(Landing Page)**
11. In the **Headers** section, check the **Add custom headers** option.

12. Click **Add** in the **Custom headers** field.
13. In the **Header key** field, enter: **X-PHISHTEST**
14. In the **Header value** field, enter: **CYTECH**
15. Click **Save**.
16. Review all configured settings, then click **Save** again to apply the rule.

Optional: Temporary Adjustment for Quicker Testing

Google offers a feature called **Enhanced Pre-Delivery Message Scanning**.

While not recommended to disable permanently, you may consider turning it off briefly to speed up testing and configuration validation.



Spam, phishing, and malware

Email allowlist
Applied at 'SP'

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:

Enhanced pre-delivery message scanning
Applied at 'SP'

[Learn more](#)

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

Inbound gateway

If you use email gateways to route incoming email, please enter them here to improve spam handling [Learn more](#)

Enable: **ON**

Spam

Status	Source	Actions	ID	Values
Enabled	Locally applied	Edit - Disable - Delete	cf9eb	Aggressive spam filtering: OFF Bypass internal senders: OFF Bypass approved senders: ON Quarantine message: OFF

[ADD ANOTHER RULE](#)

Additional Systems in Use?

If your organization uses other email or security filtering systems, please refer to the [Whitelisting Phishing Overview](#) and ensure proper bypass configurations are in place across all layers.

Reference Documentation Link: <https://securepractice.co/guides/whitelisting-google>

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #5

Created 27 May 2025 10:22:28 by Richmond Abella

Updated 27 May 2025 14:51:28 by Richmond Abella