How to stop trusted sender emails from going to Spam in the Admin Panel

Use this article when a user reports that emails from a trusted sender are landing in the Spam folder.

Start by checking the **Incoming Logs**. The logs show why the message was flagged. In most cases, you can fix the issue by using **Whitelist & Deliver** from the logs. In special cases, such as failed SPF or rotating sender addresses, you may need to edit the whitelist entry.

Before you start

Log in to the Admin Panel before following these steps. You need access to the affected domain and permission to view Incoming Logs and manage whitelist entries.

At a glance: the four steps

1. **Diagnose** in the Admin Panel → Logs → Incoming Logs (find the message, read the Spam Score / SPF / DNSBL columns).
2. **Apply the quick fix**: select the message and click **Whitelist & Deliver**. This creates a domain-level whitelist entry with safe defaults.
3. **Handle the special case** if the message failed SPF or the sender's setup is broken: edit the whitelist entry under **Filtering → Whitelist** and adjust **Ignore SPF** or **Apply to Headers**.
4. **Verify** the change took effect by re-checking Incoming Logs for a new email from the same sender and confirming the whitelist entry is present.

> **Alternative path:** from the Webmail, the user can right-click the Spam message andchoose **Deliver to Inbox**. See detailed steps and skip Steps 1-3 entirely.

Step 1. Diagnose: check the Incoming Logs

The Incoming Logs show every email received by the domain in the last 60 days, with the delivery status and the scoring data the filter used to make its decision. This is your starting point for any "why did this go to Spam" question.

1. Go to **Logs → Incoming Logs**.
2. Select the **Domain**, **Start Date**, and **End Date**.
3. Add a filter to narrow down the sender: most often **Envelope From**, **Header From**, or **To** (the recipient).
4. Click **Search**.

How to read the results

Find the message in question and look at these columns:

Column	What it tells you
Status	`delivered`, `spam`, `rejected`, or `undelivered`. If it's `spam`, the message was placed in the user's Spam folder.
Spam Score	The filter's spam rating. The higher the score, the more spam-like the message looked to the filter. A high score on a legitimate sender usually means content patterns, links, or sending reputation tripped the filter.
SPF	Check whether SPF passed, failed, or soft-failed. Failed SPF often means the sender's mail server is not authorized in the sender domain's SPF record.
DNSBL	Whether the sending IP appeared in a DNS blacklist. If yes, the sender's mail server has a reputation problem with one or more blacklist providers.
IP	The IP the message was sent from. You'll need this if you decide to whitelist by IP later.

Column	What it tells you
Envelope From	The actual SMTP sender: **this is the address the filter uses for whitelisting and blacklisting**, not the friendly "From" shown in the email client. Hover the column to see the Header From for comparison.

> **Envelope From vs Header From**
>
> These are two different addresses and they often don't match. The filter only ever matches against the **Envelope From**.
>
> - **Envelope From** is the technical sender used in the SMTP transaction. Marketing platforms, transactional email services, and ESPs commonly use bounce/return-path addresses here — for example: `011edab60c-edb126-55h4-4555-b5ym-139af41f-0000@bounce.stripe.com`
> - **Header From** is the friendly address shown in the email client — for example: `Stripe <notifications@stripe.com>`
>
> If you manually whitelist `notifications@stripe.com` (Header From), the filter will **not** match incoming Stripe messages, because their Envelope From is under `bounce.stripe.com`. The reliable approach is to use **Whitelist & Deliver** directly from the Incoming Logs - the system copies the correct Envelope From for you.
>
> If you have to whitelist manually, copy the value from the **Envelope From** column.

Once you've identified why the message was flagged (high Spam score / SPF fail / DNSBL / mismatched From), move to Step 2.

Step 2. The quick fix: Whitelist & Deliver from Incoming Logs

For most cases, this is all you need.

1. In the **Incoming Logs** results, check the box next to the message (or messages) from the trusted sender.
2. Click **Whitelist & Deliver**.

This does two things at once:

- **Delivers** the message immediately to the user's Inbox.
- **Creates a domain-level whitelist entry** under **Filtering → Whitelist**, using the correct **envelope-from** address (so you don't have to figure out which header the filter is keyed on).

The new entry uses safe defaults: **Check Virus = Yes**, **Ignore SPF = No**, **Apply to Headers = No**. For most senders, those defaults are exactly what you want - you're done.

When the quick fix is not enough

If the original message failed SPF or the sender has a broken setup, the default whitelist entry won't deliver future emails; the filter will keep rejecting them on SPF grounds. In that case, continue to Step 3.

Step 3. Edit the whitelist entry for special cases

After Step 2, the whitelist entry exists but may need adjustments. Find it under **Admin Panel → Filtering → Whitelist**, select the recipient's domain from the list and search for the sender's address. Click the edit icon.

Case A: The sender's SPF is failing

If the diagnosis in Step 1 showed `SPF = fail` or `softFail` and you trust the sender enough to deliver their mail anyway:

> Before settling for this workaround long-term, consider asking the sender to fix their SPF - see The proper long-term fix below. Whitelisting is the right answer when mail needs to flow today, but it doesn't solve the underlying problem.

1. Open the whitelist entry under **Admin Panel → Filtering → Whitelist**.
2. Set **Ignore SPF** to **Yes**.
3. In the **IP** field, enter the **sender's actual IP** — copy it from the **IP** column in Incoming Logs for the offending message. If the sender publishes a known sending range, you can enter a subnet in CIDR notation instead, e.g. `203.0.113.0/24`.
4. Click **Update** (or **Add Whitelist**).

This is the recommended approach: the SPF bypass applies **only** to messages coming from that specific IP or range. A spoofer sending from anywhere else will still be blocked by SPF, so you keep most of the protection.

> **Last resort:** If the sender's IPs are genuinely unpredictable and you can't get a usable list from them, enter `1.2.3.4` in the **IP** field. This is our convention for telling the system *ignore SPF from any IP for this sender* - the entry will match no matter where the message comes from.
> Treat this as an extreme measure. It removes the IP scope entirely, which means anyone who can spoof the sender's address will pass SPF as far as your filter is concerned. Use it only when:
> - You've confirmed the sender is genuinely legitimate, **and**
> - You've ruled out the alternatives above (specific IP, CIDR range, or a published sending-IP list).

Case B: The Envelope From is unusable. Whitelist by header instead

Some senders simply can't be whitelisted by Envelope From, because that address rotates per-send or doesn't belong to them. The classic example:

>

> **The third-party email service case (SendGrid, Mailchimp, HubSpot, Postmark, etc.)**
>
> A small business sends all of their mail through SendGrid. The **Envelope From** of every message is something like `bounce-9f8e7d6c@sendgrid.net` - it rotates per-send, and it belongs to the service, not to the business. The `From:` **header**, however, consistently shows the business: `hello@trusted-small-business.com`.
>
> If you whitelist the bounce address, you'll either miss the next message (rotation) or - if you tried to whitelist the bounce domain - end up trusting every SendGrid customer on the planet, spammers included. Neither is acceptable. The correct fix is to whitelist the business's `From:` header address and turn on Apply to Headers.

Other situations where the same pattern applies:

- **Mailing lists** that rewrite the Envelope From to a list-bounce address (`mailman-bounces@lists.example.org`) but preserve the original sender in `From:`.
- **Forwarded mail** where the Envelope From becomes the forwarder's address but `From:` keeps the original sender.
- **Genuinely broken senders** whose bounce / return-path setup is random per-send, but whose `From:` header is consistent and correct.

How to do it:

1. In Incoming Logs, hover the **Envelope From** column to reveal the **Header From** and copy the address part — e.g. `hello@trusted-small-business.com`, not `Trusted Business <hello@...>`.
2. In **Admin Panel → Filtering → Whitelist**, click **New** and create an entry with this address. **Do not use Whitelist & Deliver from Incoming Logs for this case** — it captures the Envelope From, which is the wrong address here.
3. Set **Apply to Headers** to **Yes**.
4. Leave **Ignore SPF** at **No** unless you also have a confirmed SPF failure to handle.
5. Click **Add Whitelist**.

What Apply to Headers does technically: the filter normally matches only against the Envelope From. With this flag on, it also checks the `From:` headers — so the whitelisted address matches if it appears in any of those fields, even when the Envelope From is unrelated.

> **Why this is risky: read before flipping the flag** The `From:` header is the easiest field in an email for an attacker to forge. There's no protocol-level binding between `From:` and the actual sender — SPF, DKIM, and DMARC all exist precisely because `From:` can't be trusted on its own.

> When Apply to Headers is on, the filter will deliver any message that *claims* to be from the whitelisted address in its `From:` header, regardless of who actually sent it. A phisher who knows you've whitelisted `accounts@important-vendor.com` with this flag can spoof that header from anywhere and walk straight past the spam filter.
>
> Use Apply to Headers only when:
>
> - You've confirmed the Envelope From genuinely can't be whitelisted (it rotates, or it belongs to a shared third-party service), **and**
> - You trust the sender enough to accept the spoofing risk.

Save and you're done

Click **Update** (or **Add Whitelist** if you're creating a fresh entry instead of editing). Move to Step 4 to verify.

The proper long-term fix: ask the sender to repair their setup

Whitelisting on our side is always a workaround - the root cause sits on the sender's end. Their SPF, DKIM, or DMARC setup is misconfigured, and that misconfiguration affects every recipient they email, not just our users. Until they fix it, you'll have to keep maintaining the whitelist entry, and the safety trade-offs (Ignore SPF, Apply to Headers) keep accumulating.

Before settling for the workaround long-term, suggest that the affected user contact the sender and ask them to repair their DNS. Most senders don't realise their mail is landing in spam folders elsewhere. A polite heads-up often leads to a quick fix on their side, and to better deliverability for them everywhere, not just to our domain.

For large institutions with no contact path (banks, government bodies, healthcare providers), this isn't realistic - the workarounds in Case A and Case B are likely your only practical option.

Email template the user can adapt and send

Hi [sender name],

I wanted to flag something — your recent emails to me have been landing in my Spam folder. My email provider tells me the cause is that your domain's **SPF check is failing**. In plain terms, that usually means the server you're sending from isn't authorised in your domain's SPF DNS record.

If you have someone managing your domain or email setup, could you ask them to look at the following:

- **SPF record**: confirm that the SPF TXT record on your domain (`[sender-domain.com]`) includes the IP or sending service you're actually sending from. The IP my provider saw your last message come from was `[IP from Incoming Logs]`.
- **DKIM**: enable DKIM signing for your outgoing mail if it isn't already in place.
- **DMARC**: publish a DMARC record. Not strictly required, but it improves deliverability everywhere, not just to me.

A free check at `https://mxtoolbox.com/spf.aspx` or `https://www.mail-tester.com` will show what's currently wrong and what to change.

I've put a temporary workaround on my side so I keep receiving your mail, but the long-term fix really sits with you — and once it's done, you'll see better deliverability across the board.

Thanks, [your name]

Alternative path: let the user self-serve from Webmail

This is the path we recommend when the end user wants to handle it themselves, no admin involvement needed.

1. In **Webmail**, open the **Spam** folder.
2. Find the message from the trusted sender.
3. **Right-click** the message and choose **Move to Inbox folder**.

4. A confirmation pop-up will appear: "*Do you trust this sender? Are you sure you want to whitelist this sender: ...?*"
5. Click **Yes**.

This creates a **user-level** whitelist entry: it applies only to that user's mailbox, not the whole domain. The message is moved to the Inbox immediately.

> **Only do this for senders you genuinely trust.** The pop-up asks for a reason: spammers sometimes spoof familiar addresses, so don't whitelist a sender just because the name looks right.

Step 4. Verify the change worked

There are three quick checks:

Check 1: The entry exists with the settings you expect

Go to **Admin Panel → Filtering → Whitelist**, search for the sender's address, and confirm:

- The entry is there.
- **Ignore SPF** and **Apply to Headers** are set correctly for the case you handled.
- For domain-level entries, the *Username* column is empty.

Check 2: Ask the sender to send a fresh test email

Then go back to **Logs → Incoming Logs**, search by the sender's address, and look at the most recent message:

- **Status** should now be `delivered` (not `spam`).
- The message should land in the recipient's Inbox.

Check 3: If a test email isn't possible

Use **Logs → Incoming Logs** with a date range *after* you made the whitelist change, search by the sender's address, and confirm any new emails show `Status = delivered`.

Viewing whitelist entries

After you make a change, you can confirm the entry exists.

Go to **Admin Panel → Filtering → Whitelist** and select the domain. By default this shows only domain-level entries.

To also see entries that individual users have added for themselves, tick **Include Users Whitelist**. The combined report shows:

- **Domain-level entries** : no value in the *Username* column. These apply to every user on the domain.
- **User-level entries** : the user's address appears in the *Username* column. These apply only to that user.

This is the canonical view for understanding "what's currently whitelisted on this domain, by whom, with what settings."

Decision shortcut

What you saw in Incoming Logs	What to do
High Spam Score, SPF passed, DNSBL clean	Step 2: `Whitelist & Deliver`. Defaults are fine.

What you saw in Incoming Logs	What to do
SPF failed	Step 2, then Step 3 Case A .
IP listed in DNSBL	Step 2. If it keeps failing, whitelist by IP via **Filtering → IP Access List**.
Envelope From is unusable (rotates per-send, belongs to a third-party relay like SendGrid, or is a mailing-list bounce address) but you trust the address in the `From:` header	Try Step 2. If it keeps failing, manually whitelist the `From:` header address with Step 3, Case B (Apply to Headers).
End user only wants their own mailbox fixed	Alternative path: let the user self-serve from Webmail.

Troubleshooting: The message still goes to Spam

If the message still arrives as `spam` after whitelisting, the most likely causes are:

- **The sender is now sending from a different Envelope From.** Marketing platforms and transactional services (SendGrid, Mailchimp, HubSpot, Postmark, etc.) rotate per-send envelope addresses — e.g. `bounce12435@hubspot.com`, then `bounce98712@hubspot.com`. A whitelist on the previous exact address won't match the new one, and whitelisting the bounce *domain* would expose you to every other customer of that service, including spammers. The correct fix is to whitelist the sender's `From:` header address with `Apply to Headers = Yes` - see Step 3, Case B.
- **The sender is now sending from a different IP.** Re-check the `IP` column in Incoming Logs for the latest message. Update the entry with the new IP, or expand it to a CIDR range if the sender uses several addresses. As a last resort, use `1.2.3.4` to ignore SPF from any IP - but only after the safer options are exhausted (see Step 3, Case A).
- **The user has a user-level blacklist or filter rule blocking the sender.** User-level settings are more specific than domain-level and take precedence over a domain-level whitelist. A user-level block will always win. Check `Admin Panel → Filtering → Blacklist` and check **Include Users Blacklist**. Check for entries matching the sender's domain or email address.
- **You whitelisted the Header From instead of the Envelope From** — e.g. you whitelisted `notifications@stripe.com` but Stripe's Envelope From is under `bounce.stripe.com`. See the Envelope From vs Header From callout in Step 1.

Related pages

- Incoming Logs: Track All Incoming Email
- Manage Whitelists and Blacklists (domain level)
- Whitelist / Blacklist by IP: IP Access List
- Settings: Domain Spam Filtering (defaults that apply when no whitelist entry matches)
- User Panel → Whitelist or Blacklist an e-mail address

Revision #6
Created 14 May 2026 19:38:23 by Admin
Updated 14 May 2026 23:01:40 by Admin