Free Professional Email Setup Guide

Get a professional email like `support@yourdomain.com` for free. Receive it in your normal Gmail. Reply from Gmail, and people see your domain name — not your Gmail address.

Cost: $0. No paid email hosting. No paid plan.

What you need before starting

1. A domain you own (example: `yourdomain.com`)
2. The domain's DNS managed on Cloudflare (free plan is fine)
3. A normal Gmail account (example: `youraccount@gmail.com`)

How it works

Two separate halves. This is the important idea:

Receiving mail — Cloudflare Email Routing takes mail sent to `support@yourdomain.com` and forwards it to your Gmail inbox. Free.

Sending mail — Cloudflare cannot send mail. So we use a free SMTP provider (Brevo). Gmail connects to Brevo and sends your message with your domain as the sender. Free, 300 emails per day.

You need both. One alone is not enough.

Why Brevo for sending

Free options compared:

1. Brevo — 300 emails/day free forever. Real SMTP. Custom domain DKIM. Works with Gmail. Best choice.
1. SMTP2GO — 1000 emails/month free. Also good. Use if Brevo fails.
1. Mailjet — 200/day free. Works, but weaker delivery reputation.
1. SendGrid — free plan removed. Skip.
1. Zoho Mail free — no SMTP access on free plan. Cannot work with Gmail. Skip.

STEP 1 — Check your current DNS first

Do not skip this. You must know what is already there, so you do not break your website.

Run these in a terminal (replace `yourdomain.com`):

```
dig +short MX yourdomain.com
dig +short TXT yourdomain.com
dig +short TXT _dmarc.yourdomain.com
dig +short A yourdomain.com
```

Or just look at your Cloudflare DNS page.

Write down what you find:

1. MX records — if you already use another email service (Google Workspace, Zoho, etc.), STOP. Adding Cloudflare MX will break it. You cannot have two mail providers on the same domain.
1. SPF record — a TXT record starting with `v=spf1`. Note it down.
1. DMARC record — a TXT record at `_dmarc`.
1. A / CNAME records — your website. We will not touch these.

If you have no MX, no SPF, no DMARC — perfect, clean start.

The one rule that breaks everything

A domain can have only ONE SPF record.

If you end up with two TXT records starting with `v=spf1`, every SPF check fails and your mail goes to spam. If you need to add something to SPF, edit the existing record. Never create a second one.

STEP 2 — Turn on Cloudflare Email Routing

1. Cloudflare dashboard → pick your domain → Email → Email Routing
2. Click Get started
3. Cloudflare shows the DNS records it will add:

1. 3 MX records (`route1/2/3.mx.cloudflare.net`)
1. 1 TXT record for SPF
1. 1 TXT record for DKIM (`cf2024-1._domainkey`)

1. Check the screen for any "conflicting records will be removed" warning. If it wants to delete something you need, stop and check it.
2. Accept. Cloudflare adds the records itself.

The MX priority numbers are random for each domain. That is normal.

STEP 3 — Add your destination and rule

Enabling Email Routing is not enough. Many people stop here and wonder why nothing arrives. You must do both of these:

A. Destination Addresses tab

1. Add your Gmail: `youraccount@gmail.com`
1. Cloudflare sends a verification email to that Gmail
1. Open Gmail and click the verify link
1. Status must change from `Pending` to `Verified`

B. Routing rules tab

1. Click Create routing rule
1. Email pattern: `support` @ `yourdomain.com`
1. Action: Send to an email
1. Destination: your Gmail
1. Save

Catch-all: leave it Disabled. Catch-all accepts mail to every possible address at your domain, and spammers find those fast.

TEST 1 — Does receiving work?

From a different email account, send a mail to `support@yourdomain.com`.

Do not send from the same Gmail that receives the forward. Gmail hides mail you send to yourself, and you will think it failed.

It should arrive in your Gmail within a minute.

If nothing arrives, open the Activity Log tab in Cloudflare Email Routing. It shows exactly where the mail stopped.

Do not continue until TEST 1 passes. Later, Gmail sends a confirmation code to `support@yourdomain.com`. If forwarding is broken, you will never receive that code.

STEP 4 — Create a Brevo account

Go to brevo.com and sign up. Free plan.

Then: Settings → Senders, Domains & IPs → Domains → Add a domain

1. Domain name: `yourdomain.com` (no `www`, no `https://`)
2. Branded subdomain: type `mail`

Optional, but do it. It makes your links use your domain instead of Brevo's, and it helps your mail look trustworthy. Make sure `mail` is not already used in your DNS.

1. Setup method: choose Manual, not Automatic.

Automatic logs into your DNS and adds records by itself. It often adds a second SPF record, which breaks all your mail. Manual keeps you in control.

Brevo now shows about 7 records. They look like this:

```
TXT    @                 brevo-code:xxxxxxxxxxxx
CNAME  brevo1._domainkey  b1.yourdomain-com.dkim.brevo.com
CNAME  brevo2._domainkey  b2.yourdomain-com.dkim.brevo.com
TXT    _dmarc             v=DMARC1; p=none; rua=mailto:...
CNAME  mail               ...brand.brevosend.com
CNAME  r.mail             ...r.brand.brevosend.com
CNAME  img.mail           ...img.brand.brevosend.com
```

Your exact values will be different. Copy yours from your own screen.

Note about SPF

Brevo does not ask for an SPF record. That is correct and normal. Brevo sends using its own return address, so SPF is checked against Brevo's domain, and DMARC still passes because of DKIM.

Some old guides tell you to add `include:spf.brevo.com` to your SPF. Don't. It does nothing useful here, and it allows every other Brevo customer's servers to send email using your domain name. Leave your SPF as it is.

STEP 5 — Add the Brevo records to Cloudflare

Go to Cloudflare → DNS → Records.

Add each record from Brevo. For every record:

Proxy status must be "DNS only" (grey cloud), not proxied (orange).

Proxying a DKIM or mail record breaks it completely.

Faster way

Cloudflare has an Import button that accepts a BIND file. Put all records in one text file and upload it once:

```
yourdomain.com. 3600 IN TXT "brevo-code:xxxxxxxxxxxx"
_dmarc.yourdomain.com. 3600 IN TXT "v=DMARC1; p=none; rua=mailto:..."
brevo1._domainkey.yourdomain.com. 3600 IN CNAME b1.yourdomain-com.dkim.brevo.com.
brevo2._domainkey.yourdomain.com. 3600 IN CNAME b2.yourdomain-com.dkim.brevo.com.
mail.yourdomain.com. 3600 IN CNAME mail-yourdomain-com.brand.brevosend.com.
r.mail.yourdomain.com. 3600 IN CNAME mail-yourdomain-com.r.brand.brevosend.com.
img.mail.yourdomain.com. 3600 IN CNAME mail-yourdomain-com.img.brand.brevosend.com.
```

Note the dots at the end of CNAME values. They matter.

When importing, leave "Proxy imported DNS records" unchecked.

Check your work

```
dig +short TXT yourdomain.com | grep -c "v=spf1"
```

The answer must be 1. If it says 2, delete one immediately.

STEP 6 — Authenticate the domain in Brevo

Back in Brevo, on the records page:

1. Click Verify records
2. Every record should show a green "values match" message
3. Click Authenticate domain

Status should become Authenticated and Branded.

DNS can take a few minutes. If verification fails, wait and retry.

STEP 7 — Get your SMTP key

Brevo → Settings → SMTP & API → SMTP tab

You will see:

```
SMTP Server   smtp-relay.brevo.com
Port          587
Login         xxxxxxxx@smtp-brevo.com
```

Click Generate SMTP key. Copy it. Brevo shows it only once.

Security

This key can send email as your domain. Treat it like a password.

1. Never commit it to git
1. Never put it in code or a `.env` file you share
1. Never post it in a screenshot or chat
1. Store it in a password manager

If it leaks, delete it in Brevo and generate a new one.

Also: do not turn on Brevo's "block unauthorized IP addresses" option. Gmail sends from Google servers whose IPs change all the time. Turning it on will break your sending.

STEP 8 — Set up Gmail

Gmail → Settings (gear) → See all settings → Accounts and Import → Send mail as → Add another email address

First screen:

```
Name            Your Support Name
Email address   support@yourdomain.com
Treat as alias  CHECKED
```

Should "Treat as an alias" be checked?

Yes, check it.

"Alias" means the address belongs to the same person. When checked, Gmail sends a clean `From: support@yourdomain.com` and nothing else.

If you uncheck it, you are telling Gmail "I am sending on behalf of someone else." Gmail then adds a hidden `Reply-To` header pointing at your personal Gmail address. Everyone who replies would see your Gmail address. That defeats the whole purpose.

Second screen:

```
SMTP Server   smtp-relay.brevo.com
Port          587
Username      xxxxxxxx@smtp-brevo.com
Password      your SMTP key
Connection    Secured connection using TLS
```

Click Add. Gmail sends a confirmation code to `support@yourdomain.com`. It arrives in your Gmail through Cloudflare forwarding. Paste the code.

Last step, very important:

On the same settings page, select:

```
(•) Reply from the same address the message was sent to
```

Now when someone writes to `support@yourdomain.com` and you hit Reply, Gmail automatically replies as `support@yourdomain.com`.

If you want this to be your main address, click make default.

Testing — do all of these

Do not tell anyone it works until all six pass.

TEST 1 — Receiving From another email account, send to `support@yourdomain.com`. It should arrive in your Gmail.

TEST 2 — Sending In Gmail, compose a new mail. Change the "From" to `support@yourdomain.com`. Send to another account you own. The receiver must see `support@yourdomain.com`.

TEST 3 — Replying Reply to the mail from TEST 1. Check your Sent folder. The From must be `support@yourdomain.com`, not your Gmail.

TESTS 4, 5, 6 — SPF, DKIM, DMARC

Send a mail from `support@yourdomain.com` to a Gmail account. Open it, click the three dots, choose Show original. You want to see:

```
SPF:    PASS
DKIM:   PASS   with domain yourdomain.com
DMARC:  PASS
```

The DKIM domain must be your domain. If it says `brevo.com`, your domain authentication did not finish. Go back to STEP 6.

You can also send to a free checker like mail-tester.com for a full report and a spam score.

Also check these

No "via" text. In Gmail, your mail should show as `support@yourdomain.com` alone. If it shows `support@yourdomain.com via brevo.com`, DKIM is not signing with your domain. Fix STEP 6.

No Reply-To header. In "Show original", search for `Reply-To`. There should be none. If you see your personal Gmail address there, go back and check the "Treat as alias" checkbox in STEP 8.

No Sender header. Same check. There should be no `Sender:` line showing your Gmail address.

Make DMARC stronger later

Start with `p=none`. It only watches and reports, it blocks nothing.

After all six tests pass and you have sent mail normally for about a week, edit your `_dmarc` TXT record:

```
v=DMARC1; p=quarantine; rua=mailto:...
```

Wait another week or two, then:

```
v=DMARC1; p=reject; rua=mailto:...
```

`reject` means anyone faking your domain gets blocked. Do not jump straight to `reject` — if something is misconfigured, you will silently block your own real mail.

Common problems

Nothing arrives at my new address Destination address is probably still `Pending`. Open your Gmail and click Cloudflare's verification link.

Mail arrives but goes to spam Check DMARC is set and DKIM passes. New domains also need time and normal sending activity to build reputation.

Gmail rejects my SMTP password Two possibilities. You used your Brevo account password instead of the generated SMTP key. Or Brevo has not finished reviewing your new free account — new accounts sometimes wait a few hours before SMTP works.

All my mail suddenly fails Check for two SPF records:

```
dig +short TXT yourdomain.com | grep "v=spf1"
```

Only one line is allowed.

My website went down You edited or deleted an A or CNAME record. Email setup only needs MX, TXT and mail-related CNAME records. Restore your website records.

Limits to know

- Brevo free: 300 emails per day. Fine for support mail.
- Cloudflare Email Routing: receiving only. It can never send.
- Cloudflare forwards mail, it does not store it. Your Gmail is the real mailbox.
- You can add more addresses (`hello@`, `billing@`) as extra routing rules, all forwarding to the same Gmail, for free.

Quick summary

1. Check existing DNS. Note MX, SPF, DMARC.
2. Turn on Cloudflare Email Routing.
3. Add destination Gmail, verify it, create the routing rule.
4. TEST 1 — make sure receiving works.
5. Create Brevo account, add domain, choose Manual setup.
6. Add Brevo's records to Cloudflare as DNS only.
7. Verify and authenticate in Brevo.
8. Generate SMTP key.
9. Add "Send mail as" in Gmail, alias CHECKED, TLS port 587.
10. Turn on "Reply from the same address".
11. Run all six tests.
12. Later, raise DMARC to quarantine, then reject.

Total cost: nothing.