Polyguard

Polyguard PreScreen: Sending Trust Check Emails From Your Domain

By default, the Trust Check invitation that Polyguard emails to your candidates is sent from `alerts@polyguard.ai`, with your company name as the display name. This guide sets up sending from an address on your own domain instead, for example `careers@example.com`. Candidates see your domain, their replies reach your team, and the mail is authenticated as yours (DKIM, and SPF through a bounce subdomain).

You need someone who can edit your domain's DNS records and someone who can create a mailbox and set up forwarding. The hands-on work takes about 30 minutes; DNS changes usually take effect within an hour, and Amazon confirms the domain within minutes of the records resolving (up to 72 hours in rare cases).

Throughout this guide, `example.com` stands for your domain.

How it works

Polyguard sends mail through Amazon SES from Polyguard's own AWS account. For SES to send mail as your domain, three things are needed:

1. **DKIM signing delegated to SES.** You publish three CNAME records. SES then signs each message with a key under your domain, so receiving mail servers see `d=example.com` in the signature. This is what satisfies your DMARC policy.
2. **A bounce subdomain (recommended).** You publish an MX record and an SPF record on a subdomain such as `bounce.example.com`. SES uses it as the envelope sender, so SPF also passes and aligns with your domain, and delivery failures come back to that subdomain (SES handles them).
3. **A real mailbox** at the sender address, forwarding to Polyguard. Candidate replies, delivery notices, and Amazon's verification messages arrive there.

Nothing changes for your existing mail. The records are additive: your current MX, SPF, and DKIM records for your own mail servers stay exactly as they are. You do not need to add anything to your domain's root SPF record.

Step 1: Choose the sender address

Pick a role address on your domain, such as `careers@example.com`, `recruiting@example.com`, or `talent@example.com`.

- **Use a mailbox someone reads.** Candidates reply to these emails. Avoid `noreply@` addresses.
- **Do not use a person's address.** The mailbox is shared with Polyguard (Step 2), and the address outlives any one employee.
- **A subdomain works too** (for example `careers@jobs.example.com`) if you prefer to keep this mail separate from your primary domain. The DNS records in Step 3 then go on that subdomain.

Send the chosen address to your Polyguard contact. Polyguard creates the sender identity and returns the DNS record values used in Step 3.

Step 2: Create the mailbox and forward it to Polyguard

Create the address in your mail system (a shared mailbox, a group, or an alias on an existing mailbox all work) and forward **all** incoming mail to:

```
alerts+<your-company-slug>@polyguard.ai
```

Keep a copy in your own mailbox if you want your recruiting team to see replies directly. The forwarded copy lets Polyguard see candidate replies, delivery problems, and any verification messages from Amazon.

Notes for common mail systems:

- **Google Workspace.** Either create a Google Group for the address and add the Polyguard address as an external member (the group's settings must allow external members), or create the address as an alias on a user and add a Gmail filter that forwards matching mail. Forwarding to an external address must be allowed by your Workspace admin.
- **Microsoft 365.** Create a shared mailbox and set forwarding to the Polyguard address, keeping a copy. External forwarding is blocked by default: your admin needs to allow it in the outbound spam policy for this mailbox.

A confirmation email may be sent to the forwarding target when you set this up. Polyguard receives it and completes the confirmation; you do not need to do anything further.

Step 3: Publish DNS records

Polyguard sends you the exact values after creating the identity. The records below show the shape; the `<token>` values are unique to your domain.

3a. DKIM (required)

Three CNAME records:

Type	Name	Value
CNAME	`<token1>._domainkey.example.com`	`<token1>.dkim.amazonses.com`
CNAME	`<token2>._domainkey.example.com`	`<token2>.dkim.amazonses.com`
CNAME	`<token3>._domainkey.example.com`	`<token3>.dkim.amazonses.com`

- Many DNS providers append the zone name automatically. If yours does, enter only `<token1>._domainkey` as the name; otherwise the record ends up at `<token1>._domainkey.example.com.example.com` and verification never completes.
- **Cloudflare:** set the proxy status to **DNS only** (grey cloud) on each CNAME. Proxied CNAMEs do not resolve for mail servers.
- Any TTL is fine.

3b. Bounce subdomain (recommended)

Choose a subdomain that carries no other records and no mailboxes, such as `bounce.example.com`, and publish:

Type	Name	Value
MX	`bounce.example.com`	priority `10`, `feedback-smtp.us-west-2.amazonses.com`
TXT	`bounce.example.com`	`v=spf1 include:amazonses.com ~all`

This makes the envelope sender (the address delivery failures return to) live on your domain, so SPF passes and aligns with the `From` domain under DMARC.

Without this step, mail still authenticates through DKIM and passes DMARC, but the envelope sender is an `amazonses.com` address. Adding `include:amazonses.com` to your root domain's SPF record does **not** achieve the same thing and is not needed.

3c. Check your DMARC policy

Look up your DMARC record:

```
dig TXT _dmarc.example.com +short
```

- With `p=quarantine` or `p=reject`, the DKIM records in 3a are what make Polyguard's mail pass. Do not enable the sender in Polyguard before DKIM is verified (Step 4), or receiving servers will reject the mail.
- `adkim=s` (strict DKIM alignment) is fine: the `From` domain and the DKIM domain are the same domain.

- `aspf=s` (strict SPF alignment) means SPF alignment fails when the bounce subdomain is used, since strict alignment requires an exact domain match. DKIM alignment still passes DMARC, so nothing else is needed.
- If you have no DMARC record, none is required for this to work.

Step 4: Tell Polyguard, then verify together

Once the records are published, tell your Polyguard contact. Polyguard then:

1. Confirms the records resolve and that Amazon reports the domain as **Verified** with DKIM **Successful**.
2. Sets the sender address on your PreScreen app.
3. Sends you a test Trust Check invitation.

Check the test message:

- The `From` header shows your address and your display name.
- In the message headers (Gmail: "Show original"; Outlook: "View message source"), `Authentication-Results` includes `dkim=pass` with `header.d=example.com`, `dmarc=pass`, and, if you completed 3b, `spf=pass`.
- Replying to the test lands in the mailbox from Step 2 and is forwarded to Polyguard.

From this point every Trust Check invitation and reminder for your candidates is sent from your address.

After setup

- **Keep the records in place.** If the DKIM CNAMEs are removed, Amazon marks the domain unverified. Polyguard's system then falls back to sending from `alerts@polyguard.ai` so candidates are still reached, and Polyguard will contact you to restore the records.
- **Display name.** The name shown next to the address is set by your own admins in the Polyguard Console (Settings > PreScreen > Branding > "Trust Check email sender name").
- **Changing the address.** Another address on the same domain needs no DNS change; tell Polyguard and update the mailbox forwarding. A different domain repeats Steps 1 to 4.
- **Reputation.** Because the mail is signed with your domain, spam complaints from recipients count against your domain's reputation as well as Polyguard's. Only candidates who applied to one of your roles receive these messages.

Record summary

Purpose	Type	Name	Value
DKIM	CNAME	`<token1>._domainkey.example.com`	`<token1>.dkim.amazonses.com`
DKIM	CNAME	`<token2>._domainkey.example.com`	`<token2>.dkim.amazonses.com`
DKIM	CNAME	`<token3>._domainkey.example.com`	`<token3>.dkim.amazonses.com`
Bounce domain	MX	`bounce.example.com`	`10 feedback-smtp.us-west-2.amazonses.com`
Bounce domain	TXT	`bounce.example.com`	`v=spf1 include:amazonses.com ~all`

Mailbox: `careers@example.com` (your chosen address), forwarding to `alerts+<your-company-slug>@polyguard.ai`.

Troubleshooting

Verification still pending after a day. Check each CNAME with `dig CNAME <token1>._domainkey.example.com +short`; it should return `<token1>.dkim.amazonses.com`. The usual causes are the zone name appended twice, a proxied record in Cloudflare, or a typo in a token.

`dmarc=fail` in the test message headers. The DKIM signature is not from your domain, which means the sender was enabled before DKIM finished verifying, or a CNAME is wrong. Fix the record and ask Polyguard to resend the test.

Candidates report the mail in spam. A newly sending domain has no history with the large mailbox providers. It settles as candidates open and reply to the messages. Make sure Step 3b is complete so both SPF and DKIM pass.

Forwarded copies fail DMARC at polyguard.ai. Expected: forwarding rewrites the envelope and often the message, which breaks the original authentication. It only affects the copy forwarded to Polyguard and has no effect on candidate delivery.