Email rejected for cross-domain spoofing (550 5.7.1)

Fix email rejections caused by cross-domain spoofing protection: understand the '550 5.7.1' error and adapt your MX Plan or Web Hosting setup

Objective

If you send an email through **MX Plan**, **Zimbra**, or the email service bundled with a **Web Hosting** plan, and the sender address uses a different domain than the one you authenticated with, OVHcloud rejects the message — a protection against *cross-domain spoofing* enforced from **20 July 2026**.

This guide helps you understand the rejection, confirm the cause, and adapt your configuration so your emails go through again.

Requirements

- An OVHcloud email offering: **MX Plan**, **Zimbra**, or the email service bundled with a **Web Hosting** plan

Instructions

Identifying the issue

Rejected messages return this notification:

```
550 5.7.1 Rejected by policy: From header domain does not align with authenticat
```

This happens when the domain in the **From** address (the address you send *as*) differs from the domain you **authenticated** with (the mailbox credentials used to log in and send). Sending from an address on the **same** domain as your authentication mailbox is unaffected and keeps working.

Same domain

AUTHENTICATED WITH
`john.smith@mydomain.ovh`

sends as

FROM ADDRESS
`contact@mydomain.ovh`

RESULT **Delivered**

SPF · DKIM · DMARC aligned

Different domain

AUTHENTICATED WITH
`john.smith@mydomain.ovh`

sends as

FROM ADDRESS
`contact@example.com`

RESULT **Rejected — 550 5.7.1**

Alignment broken

You're likely hitting this if you:

- Send emails from an address on a different domain than your authentication mailbox
- Manage generic addresses (`contact@` , `support@` , `noreply@`) on a separate domain
- Run a **bot, script, or application** that sends with a sender domain different from the authentication domain
- Send emails **on behalf of a third party** (e.g. a service provider invoicing with their client's domain)
- Centralise sending for **multiple brands or entities** that use distinct domains from a single email infrastructure

Why is this blocked?

These three standards, now widely adopted, are why cross-domain spoofing can no longer be allowed:

Standard	Role
SPF (Sender Policy Framework)	Verifies that the sending server is authorised by the sender domain
DKIM (DomainKeys Identified Mail)	Adds a cryptographic signature linked to the sending domain
DMARC (Domain-based Message Authentication)	Combines SPF and DKIM and defines what happens on failure

Sending as a different domain than the one you authenticate with breaks this alignment; blocking it protects the reputation of your domains and the deliverability of your legitimate messages.

Resolving the rejection

Recommended fix — create a mailbox on the domain you send from

Create a mailbox on the domain you want to send from, then authenticate with it to send. Technically, a **single mailbox is enough**: once created, it can authenticate and send from **any address on that same domain**, since same-domain spoofing is unaffected by this block.

Set up the domain on a **Zimbra Starter** plan — see our Getting started with the Zimbra solution guide — then create a mailbox on it.

> ⚠ **Same-domain spoofing is a security risk, and it will soon become disableable by your domain administrator.** Right now, any mailbox on the domain can send as any other address on that same domain — a single set of credentials exposes every address, with no per-address audit trail. OVHcloud is preparing a setting that lets domain administrators turn this capability off entirely; a setup that depends on one shared mailbox impersonating several addresses will break once it's disabled. Don't build on it — prefer:
>
> - **One mailbox per address** you actually send from, or
> - A delegation feature that grants controlled access to an existing mailbox without sharing its password

- **Generic address:** you have `john.smith@mydomain.ovh` on MX Plan and want to send from `contact@example.com`. Create a mailbox, e.g. `mary.johnson@example.com`, on that domain, then authenticate with it to send as `contact@example.com`.
- **Multiple entities:** your company manages two brands, one on `mydomain.ovh` and another on `example.com`. If you currently send all mail from a single mailbox on `mydomain.ovh`, create a mailbox on `example.com` for the second brand.
- **Sending on behalf of a third party:** your agency sends communications for a client on `example.com` from your own domain. Create a mailbox on `example.com` to authenticate and send with addresses from that domain.

Alternative fix if you stay within the same domain

If all your addresses already share one domain, this block isn't your cause — re-check Identifying the issue above, since the rejection must be coming from a different address/domain pairing than you expect. For managing several identities on that single domain, use these native features instead of a shared mailbox:

Need	Feature	Available on
Send *as* another address on the same domain	**Send As**	Exchange
Send *on behalf of* someone on the same domain	**Send on Behalf**	Exchange
Share access to a mailbox without sharing the password	**Access**	Exchange
Send to a group of contacts	**Mailing List** (MX Plan) or Exchange groups	MX Plan, Exchange

If the issue persists

If you've adjusted your configuration and messages are still rejected with the same `550 5.7.1` error:

- Double-check the address you authenticate with against the **From** address actually used by your sending application or device — a mismatch is easy to miss in bulk or automated setups.
- Allow a few minutes for a newly created mailbox or configuration change to propagate before retesting.
- Contact OVHcloud support with the rejected message's full headers, the authentication address used, and the intended **From** address.

Go further

To manage aliases and redirections on an existing address, see Using email aliases and redirections.

Find out more about Zimbra Starter ↗.

To go deeper on the underlying standards, see How to improve email security with an SPF record, How to improve email security with a DKIM record, and How to improve email security with a DMARC record.

Join our community of users ↗.