

Microsoft 365 Email Relay Setup for Alpine Technology

Oct 5, 2026 · @Nick

This guide lets Alpine Technology send email from your own domain, such as `invoices@yourcompany.com`, through your Microsoft 365 tenant. Your administrator creates a connector that trusts one IP address supplied by Alpine Technology and adds that IP to your SPF record. No passwords, accounts or app permissions are shared. Setup takes about 30 minutes.

Before you start

You will need:

- A Microsoft 365 administrator who can create connectors in the Exchange admin center (Exchange Administrator or Global Administrator role).
- Access to edit your domain's DNS records, usually at your domain registrar or DNS host.
- **The sending IP address from Alpine Technology.** Contact Alpine Technology support and ask for the "Microsoft 365 relay IP address." Use only the IP they give you, and use it exactly as provided.

In the steps below, replace `yourcompany.com` with your domain and `<ALPINE-IP>` with the IP Alpine Technology provided.

Step 1: Choose a sender address

Pick the address your recipients will see email come from, for example

`invoices@yourcompany.com` or `noreply@yourcompany.com`.

- It must use a domain already verified in your Microsoft 365 tenant. Addresses ending in `.onmicrosoft.com` will not work reliably and are rate-limited by Microsoft.
- It does not need to be a licensed mailbox. If you want to receive replies, create it as a free shared mailbox; otherwise replies will bounce.

Step 2: Create the inbound connector

The connector tells Microsoft 365 to accept and relay mail that arrives from Alpine Technology's IP address.

Option A: Exchange admin center

1. Sign in to the Exchange admin center at admin.exchange.microsoft.com.
2. Go to **Mail flow** → **Connectors** and select **Add a connector**.
3. Set **Connection from** to "Your organization's email server" and **Connection to** to "Office 365". Select **Next**.
4. Name it `Alpine Technology Relay`, leave it turned on, and select **Next**.
5. Choose **By verifying that the IP address of the sending server matches one of the following IP addresses**, enter `<ALPINE-IP>`, select **+**, then **Next**.
6. Review and select **Create connector**.

Option B: PowerShell

```
Connect-ExchangeOnline

New-InboundConnector -Name "Alpine Technology Relay" `
  -ConnectorType OnPremises `
  -SenderDomains * `
  -SenderIPAddresses <ALPINE-IP> `
  -RestrictDomainsToIPAddresses $true
```

The connector can take up to 30 minutes to take effect.

Step 3: Update your SPF record

Adding Alpine Technology's IP to your SPF record tells recipients' mail servers that it may send for your domain. Without it, messages are likely to land in spam or be rejected.

1. Sign in to wherever your domain's DNS is managed (your registrar, a DNS service such as Cloudflare, or the Microsoft 365 admin center under **Settings** → **Domains** if Microsoft hosts your DNS).
2. Find the existing **TXT** record on your root domain whose value starts with `v=spf1`.
3. Edit that record and add `ip4:<ALPINE-IP>` directly after `v=spf1`, keeping everything else.
4. Save the record.

Example:

	SPF value
Before	<code>v=spf1 include:spf.protection.outlook.com -all</code>
After	<code>v=spf1 ip4:<ALPINE-IP> include:spf.protection.outlook.com -all</code>

Edit the existing record; never add a second `v=spf1` record, because two SPF records cause all SPF checks to fail. If you have no SPF record at all, create a TXT record on the root domain (host `@`) with the "After" value.

To confirm the change, run this after a few minutes:

```
Resolve-DnsName -Type TXT yourcompany.com | Where-Object { $_.Strings -like "v=spf1*" }
```

Step 4: Send these details to Alpine Technology

Once Steps 1 to 3 are done, email Alpine Technology support with the following:

Item	Example	How to find it
Sender address	invoices@yourcompany.com	Chosen in Step 1
Display name	Your Company Billing	The name recipients should see
Reply-to address (optional)	support@yourcompany.com	Where replies should go, if different from the sender
MX endpoint	yourcompany-com.mail.protection.outlook.com	Run <code>Resolve-DnsName -Type MX yourcompany.com</code> and copy the NameExchange value
Confirmation	Connector and SPF updated on [date]	Steps 2 and 3

Alpine Technology will configure its system to send through your MX endpoint and let you know when to test.

Step 5: Test and confirm

Alpine Technology will send test messages to addresses you provide. Include at least one address **outside** your organization, such as a personal Gmail or Outlook.com account. A message to your own domain can arrive even when the connector is not working, so only an external delivery proves the setup.

For each test message, check that:

- It arrives in the inbox, not spam.
- It shows your chosen sender address and display name.
- Replying goes to the expected address.

To confirm SPF passed, open the message headers (in Gmail: ☰ → **Show original**) and look for **SPF: PASS** with `<ALPINE-IP>`.

Troubleshooting

Symptom or error	Likely cause	Fix
550 5.7.64 TenantAttribution; Relay Access Denied	The connector does not match Alpine Technology's IP, or it has not taken effect yet	Check the IP in the connector matches exactly; wait 30 minutes and retest
550 5.7.1 or 5.7.606 rejection from your tenant	Sender address is not on a domain verified in your tenant	Use an address on a verified domain (Step 1)
Message lands in spam, or SPF shows FAIL or SOFTFAIL	IP missing from SPF, or two SPF records exist	Recheck Step 3; ensure exactly one <code>v=spf1</code> record
Internal test works but external does not	Connector missing or misconfigured	Recheck Step 2

If problems continue, send Alpine Technology the full error text and the time of the failed test.

Removing access later

To stop Alpine Technology sending on your behalf, disable or delete the **Alpine Technology Relay** connector in **Mail flow → Connectors**, and remove **ip4:<ALPINE-IP>** from your SPF record. Mail from that IP is refused for external recipients as soon as the connector is removed.