Trusted ARC Sealers — Microsoft 365

Trusted ARC Sealers — Microsoft 365

When this guide applies

The standard Hermes-as-relay-MX deployment expects the customer's downstream mail server (the relay target) to **allowlist Hermes by IP or hostname** and accept Hermes-forwarded mail without re-running upstream auth checks. That's how Mimecast, Proofpoint, Barracuda customers deploy those products; Hermes works the same way. In that deployment model, you do NOT need a Trusted ARC Sealer configuration because the receiver doesn't run its own auth checks against Hermes-forwarded mail in the first place.

This guide applies when:

- The customer's downstream MX is M365, AND
- For policy reasons the M365 admin **cannot** simply allowlist Hermes (some compliance frameworks require all inbound mail to be re-checked, even from trusted gateways), AND
- Hermes-forwarded mail is being quarantined or rejected by M365 due to broken upstream `ARC-Message-Signature` body hash (`arc=fail` / `cv=fail`) or broken original-sender DKIM (`dkim=fail`) caused by Hermes body modification (External Sender Banner, disclaimer, etc.)

In that specific scenario, M365's Trusted ARC Sealers feature lets the M365 admin tell their tenant "accept Hermes's seal as authoritative even when the math fails" — which is the receiver-side equivalent of IP allowlisting for the auth check.

The same scenario is also relevant for **cross-org forwarding cases** where a Hermes-served message later hops through another Hermes-untrusting gateway before final delivery (e.g.

customer A's Hermes forwards to customer B's M365 tenant, customer B's tenant doesn't allowlist customer A's Hermes IP).

Background: why this comes up

When Hermes modifies a message body — banner injection, disclaimer injection, S/MIME or PGP rewrap — the modification invalidates any cryptographic signature whose body hash was computed over the original bytes. This affects both the original sender's `DKIM-Signature` and any prior `ARC-Message-Signature` from upstream sealers (M365, Workspace, Mimecast, Proofpoint, Exclaimer, etc.). Hermes's own ARC seal at the post-content-filter re-injection point is mathematically valid (it's computed over the modified body) but honestly records `cv=fail` on the chain it can no longer body-validate.

A correctly-configured downstream MX allowlists Hermes and ignores these signals; this guide is for the cases where allowlisting isn't an option.

What this fixes (and what it doesn't)

Symptom	Trusted ARC Sealer helps?
M365 receiver quarantines forwarded mail with `arc=fail` from Hermes	Yes — M365 will accept Hermes's seal as authoritative
M365 receiver delivers but flags forwarded mail as spam due to DMARC fail-on-forward	Yes — DMARC alignment is rescued via the trusted seal
Non-M365 downstream MX (Gmail Workspace, on-prem Exchange, third-party SEG) rejects	No — those have their own trust mechanism (Gmail uses an internal list; on-prem typically has none)
Outbound mail from Hermes users to external recipients fails DKIM	No — that's a DKIM key/DNS issue, not an ARC trust issue

Identity requirements

To add Hermes to the M365 Trusted ARC Sealers list, the receiving M365 tenant administrator needs to know **the ARC signing domain Hermes uses** — the `d=` value in Hermes's `ARC-Seal:` header. Find this in the Hermes admin UI under **Content Checks > ARC Settings**: it's the domain on the active row in the *Gateway ARC Signing Identity* card.

The domain must also have a valid public key published in DNS at `<selector>._domainkey.<domain>` (this is what M365 fetches to verify the seal signature before deciding whether to trust the seal). If DNS isn't right, the math fails before the trust check even runs.

Configuration steps (M365 admin)

Run in Exchange Online PowerShell connected to the tenant:

```
# Connect (if not already)
Connect-ExchangeOnline

# Inspect existing trusted sealers
Get-ArcConfig

# Add Hermes's signing domain to the trusted list
Set-ArcConfig -Identity Default `
  -ArcTrustedSealers "your-hermes-signing-domain.example.com"
```

If multiple gateways need to be trusted, comma-separate the list:

```
Set-ArcConfig -Identity Default `
  -ArcTrustedSealers "hermes.example.com","mimecast.example.com"
```

To remove a sealer, set the property to a comma-separated list that omits the entry.

Verification

After configuration:

1. Send a test message from an ARC-sealing upstream system through Hermes (relay-mode domain) to a mailbox on the configured M365 tenant.
2. Open the message in Outlook on the Web → ellipsis menu → **View → View message source**.
3. Look for the `Authentication-Results` header chain that M365 added:
   - `arc=pass` with the `oar=` field referencing Hermes's signing domain confirms the trust list took effect.
   - `arc=fail` with a note about `original-authres` indicates the trust list did NOT match (most likely cause: domain mismatch or DNS not published).

Troubleshooting

Problem	Check
`Get-ArcConfig` returns `ArcTrustedSealers` as empty after Set	Confirm you're connected to the right tenant; verify with `Get-OrganizationConfig | Select Identity`
Test mail still shows `arc=fail` in M365	Wait up to 60 min for the trust config to propagate; recheck DNS for the Hermes selector
Hermes's seal shows `cv=pass` but M365 still rejects	Not an ARC issue — check Connection Filter / Anti-spam policies on the M365 side

Related

- ARC Settings — Hermes-side ARC configuration
- Email flow — full pipeline with ARC placement
- Microsoft official docs: Trusted ARC Sealers in Exchange Online

---

Revision #48
Created 2026-05-31 12:52:34 UTC by Dino Edwards
Updated 2026-06-20 13:33:19 UTC by Dino Edwards