

Microsoft 365 mail troubleshooting

A practical sequence for investigating Exchange Online delivery problems.

1. Capture one specific example

Record sender, recipient, UTC time, message subject and Message-ID if available. Establish whether the issue affects inbound, outbound or internal mail; one user or many; one domain or many. Keep the original nondelivery report (NDR) and headers.

2. Check service and recipient state

Review Microsoft 365 service health. Confirm the recipient address, mailbox and applicable licence/service configuration. Compare webmail with the desktop client to distinguish service-side delivery from a local display or sync issue.

3. Trace the message

In the Exchange admin center, open Mail flow > Message trace. Search by sender, recipient and a suitably narrow time range. Inspect the event details, not just the summary status. Trace visibility, available detail and retention depend on the current service and your role.

Interpret the result

Delivered does not guarantee that the user sees the message in Inbox. Review rules, forwarding, Junk Email and quarantine where applicable.

Deferred / pending: inspect the reported reason and later events.

Failed / rejected: read the full error and the system that generated it.

4. Read the complete NDR

Capture the enhanced status code, diagnostic text and generating server. Check the documented meaning of that exact error. Common causes include an invalid recipient, policy restrictions, routing problems, authentication or temporary delivery issues. Avoid diagnosing from the numeric code alone.

5. Validate DNS and authentication

Compare MX and Autodiscover with the intended deployment. Check that SPF covers every legitimate sender and that the actual DKIM selectors resolve correctly. Inspect DMARC alignment in a real message. Use tenant-provided values; third-party gateways, hybrid routing and sovereign clouds can differ.

6. Follow the actual route

Review connectors, accepted-domain settings, transport rules and gateway logs when relevant. For suspected filtering, check quarantine and security-policy results with an authorised administrator. Keep the evidence before making a change.

Escalation evidence

Provide the UTC window, affected addresses, Message-ID, trace details, full NDR and relevant headers. Redact unrelated personal data. Record recent changes and compare a successful message with a failed one. Test a targeted correction rather than changing multiple policies together.

References (click to open): [Microsoft: message trace](#) | [Microsoft: NDRs and SMTP errors](#) | [Microsoft: external DNS records](#)