OpsAtlas
OPERATIONAL RUNBOOKS BY SMALLWOOD ENTERPRISES
Reliable cloud operations documentation

Exchange Online Mail Flow Failure

Microsoft 365 Administration Runbook 04

Microsoft 365 Administration Runbooks

2026-05-29

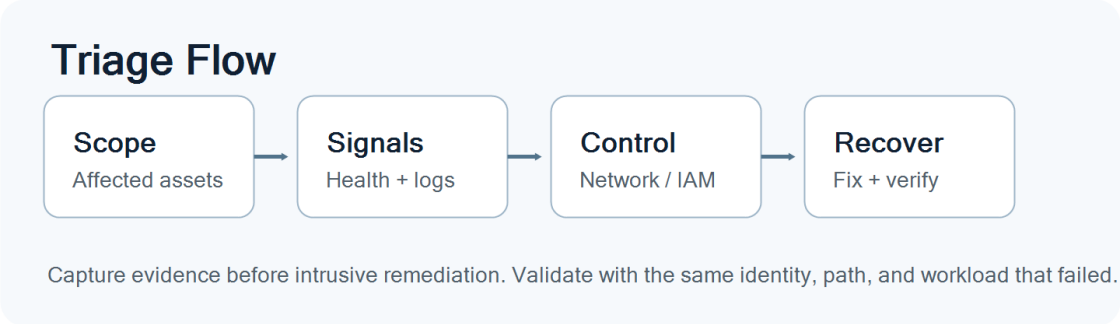
Table of Contents

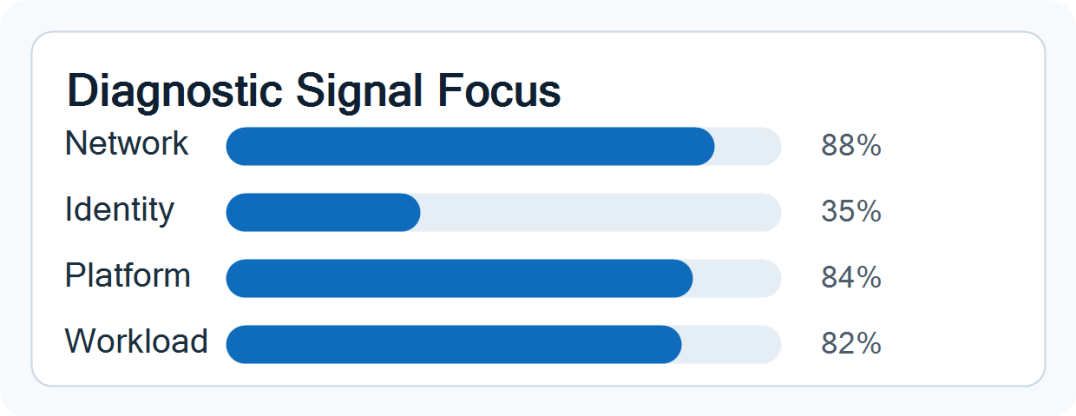
Exchange Online Mail Flow Failure

Microsoft 365 Administration Runbook 04
Audience: Microsoft 365 administrators, service desk escalation teams, MSP administrators, and IT operations leads
Severity guide: Sev 1 when tenant-wide access, mail flow, collaboration, identity, security, or regulated data is blocked; Sev 2 when a department, workload, or high-priority user is impaired with a workaround.
Incident objective: Restore inbound, outbound, or internal mail flow by using message trace, NDR analysis, connectors, transport rules, accepted domains, DNS, and protection policies.

> **Operator note:** Capture who is affected, when it started, exact error text, device/service identifiers, request IDs, screenshots, and before/after evidence.

Prefer the smallest reversible change that restores service, then replace emergency access with a durable fix.





Common Symptoms

- Users report missing, delayed, bounced, or quarantined mail.
- External recipients reject mail or sender receives NDR.
- Only one domain, connector, or application relay path fails.

First 15 Minutes

- Collect sender, recipient, subject, message ID, NDR, time zone, and timestamps.
- Run message trace for both sender and recipient.
- Check quarantine, transport rules, connectors, accepted domains, and DNS records.
- Review service health and protection reports.
- Separate user mailbox rules from transport pipeline issues.

Command Starters

Replace placeholders before running. Use the approved admin context and record output in the ticket.

```
Get-MessageTrace -SenderAddress <sender> -RecipientAddress <recipient>
```

```
Get-MessageTraceDetail -MessageTraceId <id> -RecipientAddress <recipient>

Get-TransportRule

Get-InboundConnector; Get-OutboundConnector
```

Decision Path

If you find...	Do this next
Delivered to mailbox	Investigate mailbox rules, junk, focused inbox, client sync, or user search.
Failed with NDR	Use NDR code to fix DNS, recipient, connector, or policy.
Quarantined	Review threat reason before release.
Connector path fails	Check TLS cert, smart host, IP allow, and route.

Remediation Actions

- Fix incorrect transport rules or connector settings with change control.
- Release false positives only after policy review.
- Correct SPF/DKIM/DMARC or accepted-domain records as needed.
- Escalate tenant-wide delivery impact as incident.

Validation Checklist

- Test message succeeds through intended path.
- Message trace shows delivered or expected disposition.
- Transport change is documented with before/after evidence.

Evidence to Attach

- User, device, service, tenant, location, IP/network, timestamps, and exact error text.
- Screenshots, logs, health/status evidence, message traces, policy results, or admin-center audit entries.
- Before/after configuration for identity, licensing, endpoint, network, mailbox, policy, or device changes.
- Approval record for any emergency permission, data restore, policy bypass, account unlock, deletion, rollback, or public exposure.

Customer-Facing Summary Template

What happened: `<brief customer-safe description>`
Impact: `<users/services/locations affected and time range>`
Root cause: `<confirmed root cause or current leading cause>`
Resolution: `<fix applied and validation completed>`

Prevention: `<monitoring, guardrail, training, policy, or knowledge-base follow-up>`

Reference Anchors

- Exchange Online message trace
- Mail flow best practices