

Mail Flow Rule Evidence Worksheet

One sheet per incident. Fill it in before you change a rule, not after, because a rule change destroys the state that explains the symptom and Exchange Online keeps no version history to undo it with.

⚠ Order the Extended report in Phase 2, not at the end. It is the documented downloadable report that names the rule, and it is built from archived data.

Work through the phases in order. Each one ends with a gate that has to be true before the next starts. The rule stays untouched until Phase 5. Keep the completed sheet with the change record.

INCIDENT HEADER — COMPLETE BEFORE THIS COPY IS USED AS EVIDENCE			
Organisation / tenant	Investigator		
Date opened	Classification of this record		
Incident or ticket reference			
Change reference, if one follows			

A completed copy carries sender and recipient addresses, subjects and tenant configuration detail. Classify and store it accordingly, and redact before sharing it outside the organisation.

Version 1.7 · August 2026 · Verified against Microsoft Learn on 25 August 2026 · Message trace behaviour changed in 2026 (V2 cmdlets, no pagination, SCL demoted in cloud organizations): confirm the limits against the current documentation before relying on a figure here.

Author: Tiago S. Carvalho · tiagoscarvalho.com · Companion to the article [Troubleshooting Exchange Online Mail Flow Rules](#)



Phase 1 - Capture the symptom

Before any tool. A sender, a recipient or an Internet Message ID is enough to start: an Enhanced summary or Extended report requires at least one of those three. The timestamp with its time zone and the Network Message ID are the strongest correlation evidence, and Microsoft requires `MessageTraceId` for messages sent to more than 1,000 recipients, but neither is mandatory for every trace. Both identifiers come from the message headers, and both get the full width of the sheet: a Message-ID runs to about ninety characters with no spaces to break on, and given a quarter of a row it prints too small to read.

FIELD	VALUE	WHERE IT CAME FROM
Reported symptom, in the user's words		
Expected result		
Sender address		
Recipient address		
Timestamp and time zone		
Message-ID		
Network Message ID		
Direction, and first or repeat occurrence		

GATE 1 - ALL MUST BE TRUE BEFORE PHASE 2

- ☐ The message was forwarded as an attachment, not inline, so the original headers survived.
- ☐ A strong correlation route is recorded: Network Message ID or Internet Message ID where available; otherwise the exact sender, recipient, timestamp and time zone.
- ☐ The timestamp is written with its time zone, and compared against the admin time zone message trace will use.
- ☐ The expected result is written down before any theory was formed.
- ☐ Nothing in the rule set has been changed.



Phase 2 - Trace, and order the Extended report now

Run the Summary report for the timeline and order the Extended report in the same sitting. A Summary query can reach data up to 90 days old but can span no more than 10 days at a time; a wider window returns only an Enhanced summary or Extended report, and both can also be requested for shorter ranges. The Extended report is the documented downloadable report that names the rule, it is built from archived data, and the last 24 hours is usually not available yet.

STEP	RESULT	TIME RECORDED (UTC)
Summary report run		
Final status shown		
Extended report ordered		
Extended report received		

Message events, in order

Copy the events as the trace shows them. **Resolved** or **Expand** before delivery means the recipient changed before rules ran, and the rule set is the wrong place to look.

#	EVENT	ACTION OR DETAIL	WHAT IT TELLS YOU
1			
2			
3			
4			
5			



#	EVENT	ACTION OR DETAIL	WHAT IT TELLS YOU
6			

GATE 2 · ALL MUST BE TRUE BEFORE PHASE 3

- ☐ The Summary report was run and the final status recorded.
- ☐ The Extended report was ordered, with the time of the request written down.
- ☐ An empty trace was investigated rather than assumed: time zone, date range, then connection filtering, because messages blocked by the IP Block List never appear in message trace.
- ☐ Any Resolved or Expand event was followed to the address it produced.
- ☐ The trace was read for bifurcation: one message can become several, and each fork can meet a different outcome.



Phase 3 • The rule that fired

From the Extended report, in the `custom_data` column, find the entries prefixed `S:TRA`. Use one row per matched `S:TRA=ETR` rule entry. Copy the Rule ID, `st`, `mode`, and every `action=` value present in that entry. If multiple actions are logged, record them in the same Action cell, one action per line. The `mode` value is the only record of what the rule was doing at the time, as opposed to what the portal shows today.

RULEID (GUID)	RULE NAME TODAY	ACTION	MODE	ST (UTC)

The absence of `S:TRA` is meaningful only after you have confirmed the correct message instance, a complete and non-truncated Extended report, the correct time range, and sufficient archival delay. If any of those checks is missing, absence is not proof that no mail flow rule matched. Tick all six below before you write "no rule matched" as a finding.

SIX CONDITIONS BEFORE AN ABSENT S:TRA COUNTS AS EVIDENCE

- ☐ Correct message instance, allowing for bifurcation and distribution group expansion.
- ☐ Correct Message-ID or Network Message ID, taken from the message rather than retyped.
- ☐ Correct date, time and time zone, checked against the admin time zone message trace uses.
- ☐ Archived data already available: the last 24 hours of archived data usually is not.
- ☐ Extended report not truncated at the 1,000-row limit. A result of exactly 1,000 rows means narrow the query and run it again.
- ☐ Every AGENTINFO / `custom_data` event for the message reviewed, not only the first.

Only once all six hold does an absent entry point you elsewhere: a directory resolution, an inbox rule, a connector, or a filtering verdict.



Rules that could have matched and did not

The rule you expected to fire and did not is as important as the one that did. Severity *Not audit* hides a rule from the **Exchange transport rule report**, so silence there proves nothing. It does **not** suppress the `S:TRA` entry in the **Extended message trace**, so do not use it to explain an absence there.

RULE EXPECTED TO MATCH	PRIORITY	WHY IT DID NOT, FROM THE EVIDENCE

GATE 3 · ALL MUST BE TRUE BEFORE PHASE 4

- ☐ Every rule GUID from the Extended report has been resolved to a current rule name.
- ☐ Where a rule is absent from the Extended report, all six conditions for treating that absence as evidence have been confirmed.
- ☐ The mode recorded is the one from the trace, not the one the portal shows now.
- ☐ Any rule missing from the **transport rule report** has been checked for Severity set to Not audit. That setting does not affect the Extended message trace, so it is not an explanation for a missing S:TRA entry.
- ☐ Any rule above the suspect with Stop processing more rules enabled has been identified.
- ☐ The rule set was exported before anything else happens.



Phase 4 - Why the match came out that way

The rule is read, not changed. Record the six properties that decide behaviour, then the four things that change what the rule sees.

PROPERTY	VALUE	CONSISTENT WITH THE SYMPTOM?
State (enabled or disabled)	_____	_____
Mode (Enforce / Audit / AuditAndNotify)	_____	_____
Priority	_____	_____
StopRuleProcessing	_____	_____
SetAuditSeverity	_____	_____
RuleErrorAction	_____	_____

The four things that change what a rule sees

CHECK	RESULT	EVIDENCE
Which sender address was evaluated: header, envelope, or both	_____	_____
Was the message treated as internal? Internal requires an authenticated connection	_____	_____
Group membership: when did it last change, against a cache that refreshes about every 3 hours with no SLA	_____	_____
Headers present at rule time: rules run first in content filtering, before AV and Safe Attachments	_____	_____



Do not use SCL as proof. In cloud organizations the SCL value no longer determines whether a message is identified as spam or the action taken on it, and a bypass rule might stamp 0 or 1 rather than -1. Read `SFV:SKN`, `CAT` and `DIR` in `X-Forefront-Antispam-Report` instead.

GATE 4 · ALL MUST BE TRUE BEFORE PHASE 5

- ☐ The condition and exception logic has been read as written: conditions AND, values within a condition OR, exceptions OR.
- ☐ The message was confirmed eligible: system-generated messages, NDRs from Exchange and journal reports are never processed by rules.
- ☐ For encrypted mail, transport decryption was checked before blaming a content condition.
- ☐ Where a filtering verdict and the rule disagree, the precedence table was consulted: malware and high confidence phishing always win.
- ☐ If there is a gateway or an on-premises hop, the hybrid page of this sheet has been completed.



Hybrid and third-party gateway branch

Complete this page only when the message crossed an on-premises Exchange server or a gateway. Several symptoms have a different cause on this path.

QUESTION	ANSWER	CONSEQUENCE FOR THIS INCIDENT
Where does the MX point?		
Is Enhanced Filtering enabled on the inbound connector?		
Do SCL -1 bypass rules still exist for that connector?		
Is Centralized Mail Transport enabled?		
Routing shape: linear or non-linear		
On-premises tracking log entry, by Network Message ID		

Two combinations to check by name. After enabling Enhanced Filtering you must disable any mail flow rule that sets SCL to -1 for that connector; leaving both on produces filtering that looks configured and is not. And adding on-premises hybrid servers to Enhanced Filtering is not supported in non-linear inbound routing under Centralized Mail Transport, the `Internet → Microsoft 365 → On-premises → Microsoft 365` shape.

HYBRID GATE

- ☐ The on-premises tracking log was searched by Network Message ID, not by subject.
- ☐ On Exchange 2010 or 2013, the fallback to Message-ID was used, because NetworkMessageId is not available there.
- ☐ Double-counting was ruled out: mail returning from a gateway is treated as an entirely new message.
- ☐ EFUsers scoping was checked for proxy addresses and, in hybrid, for the mail user TargetAddress.



Phase 5 - Reproduce it safely

Only now does anything get created, and what gets created is a temporary diagnostic rule with five containment properties, not a change to the rule under investigation.

CONTAINMENT PROPERTY	VALUE USED	WHY
Mode		Audit takes no delivery action
Single test recipient		Removes everyone else from the blast radius
Unique subject token		Nobody else will send it by accident
ExpiryDate		The rule stops itself if you are pulled away
Priority		Nothing above it can pre-empt the test
Time the rule was created		Wait at least 30 minutes before testing

Audit mode is not silent. `GenerateIncidentReport` runs even in Audit and AuditAndNotify.

`GenerateNotification` runs in AuditAndNotify. If the rule you are reproducing has either action, strip it from the diagnostic copy or you will email a compliance mailbox, or a sender, on every match.

Test matrix: the negative cases are the point

TEST MESSAGE	EXPECTED	OBSERVED	EVIDENCE (TRACE EVENT, S:TRA)
Should match			
Should not match			
Internal to internal			



TEST MESSAGE	EXPECTED	OBSERVED	EVIDENCE (TRACE EVENT, S:TRA)
Reply to a matching message			
Interaction with the rule above or below			

GATE 5 · ALL MUST BE TRUE BEFORE A CHANGE IS MADE

- ☐ The diagnostic rule was created in Audit mode, scoped to one recipient, with an expiry date.
- ☐ At least 30 minutes elapsed between creating the rule and testing it.
- ☐ Both a positive and a negative test were run, and both were recorded.
- ☐ No destructive action was tested against production mail. Delete is the only irreversible one: it drops the message silently, with no copy anywhere.
- ☐ If the message was quarantined, the 30-day non-customizable retention was noted, and the fact that releasing does not resume rule evaluation.
- ☐ The diagnostic rule has been removed, or its expiry date confirmed.



Phase 6 · Root cause and the change

Root cause, in one sentence

STATED SO THAT A COLLEAGUE COULD REPEAT IT WITHOUT READING THE REST OF THIS SHEET

Before and after

PROPERTY	BEFORE	AFTER	EXPECTED OUTCOME
Rule name			
Rule GUID			
State and Mode			
Priority			
Conditions			



PROPERTY	BEFORE	AFTER	EXPECTED OUTCOME
Exceptions			
Actions			
Scope of impact, stated not implied			

Validation after the change

CHECK	RESULT	TIME (UTC)	EVIDENCE
Intended case now behaves correctly			
Negative control still behaves correctly			
The originally reported message path re-tested			

GATE 6 · ALL MUST BE TRUE BEFORE CLOSING

- ☐ The rule set was exported before the change. There is no version history in Exchange Online and no way to revert a rule to a previous state.
- ☐ Both the intended case and the negative control were validated, not just the intended case.
- ☐ At least 30 minutes were allowed after the change before validating.
- ☐ The scope of impact is written down in words, not implied by the conditions.
- ☐ The user who reported the problem has been told what the cause was.



Phase 7 · Record, roll back, monitor

Rollback position

ITEM	LOCATION	VERIFIED
Pre-change export of the rule collection		
Audit log entry for the change (RecordType ExchangeAdmin)		
Who to contact if the rollback has to happen out of hours		

Import is on notice. `Import-TransportRuleCollection` is documented as going to be deprecated from Exchange Online PowerShell. Treat the XML export as a record and a reference, not as a guaranteed one-command restore.

Standing checks worth leaving behind

CLOSING CHECKLIST

- ☐ Rules with Stop processing more rules enabled have been inventoried and the interaction understood.
- ☐ Rules in a mode other than Enforce have been reviewed, and any left in audit deliberately are recorded as such.
- ☐ Rules with Severity set to Not audit are known, so the next investigation does not read their silence as absence.
- ☐ The mail flow insights dashboard was checked for Fix slow mail flow rules and Fix possible mail loop.
- ☐ The change record references this sheet, and this sheet references the change record.
- ☐ The temporary diagnostic rule is gone.



Sign-off

APPROVAL	NAME AND ROLE	SIGNATURE OR APPROVAL REFERENCE	DATE
Investigation closed Accountable for the root cause stated above			
Change accepted Owner of the rule set after this change			
A name typed into a PDF field is not a signature and will not survive a challenge. If this copy is completed on screen, put the reference from your change or approval system in that column and keep the signed authority there.			



Sources

Every figure and quoted behaviour in this worksheet comes from Microsoft's own documentation. The load-bearing pages:

PAGE	URL
Message trace in the EAC (Report types, limits, S:TRA custom_data)	learn.microsoft.com/en-us/exchange/monitoring/trace-an-email-message/message-trace-modern-eac
Mail flow rules (Properties, logic, what rules never process)	learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules
Test mail flow rules (The 30-minute wait and the test list)	learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/test-mail-flow-rules
Manage mail flow rules (Modes, severity, the reporting gate)	learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules
Conditions and exceptions (Sender location, group cache, proxy addresses)	learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/conditions-and-exceptions
Mail flow rule actions (Destructive actions, quarantine, audit-mode exceptions)	learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions
Order of precedence (Who wins, rule versus verdict)	learn.microsoft.com/en-us/defender-office-365/how-policies-and-protections-are-combined
Anti-spam message headers (SFV, CAT, DIR, and the SCL demotion)	learn.microsoft.com/en-us/defender-office-365/message-headers-eop-mdo
Enhanced Filtering for Connectors (Skip listing, EFUsers, the SCL cleanup step)	learn.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/enhanced-filtering-for-connectors
Message tracking, on-premises (Event types and the correlating fields)	learn.microsoft.com/en-us/exchange/mail-flow/transport-logs/message-tracking
Quarantine (30 days, not customizable, admin only)	learn.microsoft.com/en-us/defender-office-365/quarantine-about
Exchange Online limits (300 rules, 8 KB per rule, 20 KB of expressions)	learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits
Diagnostics in the admin center (Visual Mail Flow, and the section it belongs to)	learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-admin-diagnostics
Search-UnifiedAuditLog (Who changed the rule)	learn.microsoft.com/en-us/powershell/module/exchangepowershell/search-unifiedauditlog
Audit search (Retention and search limits)	learn.microsoft.com/en-us/purview/audit-search

Evidence Worksheet v1.7 · Mail Flow Rule Troubleshooting · Tiago S. Carvalho · [tiagoscarvalho.com](https://www.tiagoscarvalho.com)

Free to use and share within your organisation. Verified 25 August 2026 against Microsoft Learn. Message trace behaviour changed materially in 2026; confirm limits against current documentation before relying on a figure here.