# Investigate Automatic Email Forwarding

Use one copy per forwarding route. Type into the fields or print the form. Record times in UTC.
Keep exact addresses and original exports in the restricted case file. Use evidence references here.

## Identify the Mailbox and Route

**Case reference**

**Investigator / team**

**Mailbox or shared mailbox reference**

**Alert / first observation (UTC)**

**Where was it found? Record the rule or setting ID and whether it was enabled.**

Check inbox rules, mailbox forwarding and organisation-wide mail flow rules as relevant.

**Destination reference / internal or external**

**Destination owner / business purpose claimed**

**What mail qualifies? Record conditions, exceptions, actions and whether a copy is kept.**

## Check the Authority for This Route

Use a known contact method independent of the affected mailbox. Compare the exact route with the approval.

**Approval / ticket / policy reference**

**Verified approver / channel / date**

**Which details match or differ? Include destination, message scope, policy and expiry or review date.**

### If forwarding may still be exposing sensitive mail

Tell the incident lead immediately. Preserve what you can safely capture and record the change time.
The authorised responder can contain an active route while another investigator collects evidence.

# Preserve the Evidence

Save original exports with restricted access. For each item record its reference, source, collector and UTC time. For searches, include filters, dates and time zone. Note coverage gaps even when a search returns no rows.

**Case reference**

**Restricted evidence location / custodian**

## Record Three Independent Observations

### 1. Configuration snapshot

Record the setting or rule ID, state, destination and scope before any change. Record any capture delay.

**Snapshot reference / collector / capture time (UTC)**

### 2. Change history and sign-in context

Record the audit operation, actor and timestamp. Record relevant sign-ins separately and note any gaps.

**Audit and sign-in references / collector / observed change / search window (UTC)**

### 3. Message trace

Check the specific recipient and the recorded delivery event. A rule can exist even if delivery was blocked.

**Trace / message ID, destination reference, status, UTC window and matching count**

**What exposure does the evidence support? Record the time span, mail types and uncertainty.**

**What remains unavailable? Record retention, access, missing events or time windows to revisit.**

Microsoft guidance on mailbox rule audit records

Microsoft guidance on message trace

# Decide and Hand Over

Choose the outcome supported by the evidence today. An unverified route can still need urgent action. Keep the case open until the owner verifies mail flow and records the outcome.

**Case reference**

**Decision owner / decision time (UTC)**

## Choose the Outcome

- ○ **Authorised exception**
  Approval covers the exact route, scope and dates. Record the owner and review or expiry date.
- ○ **Suspicious or unauthorised route**
  The owner denies it, the route conflicts with approval, or evidence suggests abuse. Escalate promptly.
- ○ **Unresolved**
  Evidence is incomplete or contradictory. Assign the next check and a deadline. Escalate active risk.

**Reason for this outcome / strongest supporting or conflicting evidence references**

## Containment and Handover

**Action authorised / taken, by whom and when (UTC), or reason for retaining the route**

**Post-change verification / UTC time / expected business mail flow / evidence reference**

**Who takes over, when (UTC), next action and review date? Include any privacy or fraud referral.**

Microsoft playbook for suspicious email forwarding