

A credential went to the wrong place

FIRST-ACTIONS CARD

This card supports your existing incident process. It does not establish severity, legal notification duties or the safety of continued operation. When misuse may be ongoing, involve the responsible security/system owner immediately.

1. Stop making more copies

Do not reply with the value, quote the original message, paste it into a ticket, or feed it to an AI assistant. Ask participants not to forward it. Give the incident owner a safe case reference and the location of the original through the approved restricted route.

2. Identify what access the material provides

The issuing-system owner identifies the affected account/token, privilege, environment, validity and dependencies. A live reading link is access material too: removing the message does not establish that nobody already opened it.

3. Contain access under the incident lead

Revoke, disable or replace the affected credential as appropriate. Coordinate critical dependencies and recovery; the incident lead balances immediate containment against operational harm. Check active sessions and derived access separately when relevant. Do not wait for the ordinary project close-out date if containment is needed.

4. Preserve only authorized evidence

Record discovery time/timzone, location, safe identifier, known recipients and actions taken. Keep originals restricted as the incident policy requires. Do not create a widely shared evidence document containing the secret. Separate known facts, reports and unknown exposure.

5. Retire delivery and remove copies through the approved process

Stop the affected share/request route where appropriate and coordinate authorized message/file cleanup. Confirm received-response needs before destructive request actions. Cleanup is separate from source-access revocation; neither proves all external copies are gone.

6. Verify and assign remaining work

Retain source change and verification references, unresolved sessions/dependencies, responsible owners and next updates. The incident lead decides communication, further investigation and closure. Do not declare “no impact” from an empty access log or a deleted message.

Say this: “A credential may have been disclosed in [restricted location/reference] at [time]. Please assess the affected access and coordinate containment. I have not repeated the value here.”

Use precise language during the response

Useful messages

To the person who pasted the credential

Please do not resend or quote the value. Use [case reference] for updates. The system/security owner is assessing replacement and cleanup. Any replacement credential must use the approved route after the request and recipient are verified.

To the issuing-system owner

Please assess [restricted credential reference], its privilege and dependencies. Record the approved revocation/replacement action, verification and remaining access paths. Keep the value and any live reading link out of the response thread.

For a bounded status update

For [case], the identified [token/account] was [action] at [time], supported by [reference]. Delivery cleanup is [status]. We have not yet established [unknown]. [Owner] will provide the next update at [time].

Avoid conclusions the evidence cannot support

Instead of	Use
"It was deleted, so it is safe."	"The message was removed. Source access and possible copies are being checked."
"Nobody opened it."	"No recorded access was found within the inspected source/window; coverage limits remain."
"The token was rotated, so every session ended."	"The token changed. Session and derivative-access effects require separate verification."
"Nothing happened."	"We have established [specific facts]; [specific uncertainty] remains."

Before returning to normal work

Have the incident owner confirm the disposition. Repair the step that caused the exposure: ambiguous form wording, overbroad logging, an unsafe fallback, a mistaken reading-link placement or an unverified request. Practice the corrected route with disposable data.

Basis: Original response aid, informed by [OWASP Secrets Management](#). Product-specific request lifecycle: [CredenShare Secure Requests](#). No universal incident severity or legal conclusion is supplied.