

# Example 1 – Customer integration access

## FICTIONAL WORKED EXAMPLE • NOT A TESTIMONIAL OR CUSTOMER CASE STUDY

A software implementation team needs read access to a customer's staging API to diagnose a configuration issue. The customer's first instinct is to reply to the ticket with a production administrator key.

### The useful decision

The implementation owner first establishes the operation needed: read the staging configuration, not administer production. The customer's system owner approves a temporary scoped credential. The team sends an approved collection route rather than asking for the value in an ordinary reply.

| Role                    | Action                                                                                                  |
|-------------------------|---------------------------------------------------------------------------------------------------------|
| Customer system owner   | Approves scope and expiration; creates the appropriate temporary access.                                |
| Implementation operator | Sends the collection route and keeps the private reading material restricted.                           |
| Authorized investigator | Retrieves the credential only for the approved task; does not paste it into the ticket or an AI prompt. |
| Customer system owner   | Ends the source access when the diagnostic task is complete.                                            |

### A completed example handover note

CASE S-101: staging configuration read, approved by the customer's system owner. Submission was received through the selected collection route; the ticket records receipt only. The diagnostic is complete. Source access closure is assigned to the customer owner, with a required verification reference. No production administrator access was requested.

### What this illustrates

A scoped access request, a clear collection route and a separate closure owner can be defined before buying a new platform. The example does not establish a measured reduction in time, risk or support tickets. In a real case, record what actually happened and whether the selected route met the customer's restrictions.

**Product connection:** [CredenShare Secure Requests](#) documents separate collection and private reading routes. That distinction is useful here; it is not authorization to request any credential. Only the account that created a request can open its submissions, so in CredenShare the investigator would create the request and keep its Access link, while the operator sends the Collect link.

## Example 2 — Recurring vendor support

### FICTIONAL WORKED EXAMPLE • NOT CUSTOMER EVIDENCE

A vendor occasionally needs diagnostic access to an internal test service. The project team previously treated each new sharing link as a fresh access approval, even though the same broad credential remained valid for months.

#### Redesign the actual access decision

The system owner separates recurring approval from individual support tasks. Each support case specifies its purpose, privilege and end point. A named, restricted account or short-lived scoped token is preferred when practical; a temporary handoff is used only when material must actually be transferred.

**An extension is explicit.** If the issue is not resolved by the deadline, the owner approves a revised scope/date. Sending another link alone does not renew authorization.

**A shared dependency is visible.** Before replacing a credential used by a background job, the owner plans the dependent change instead of breaking the job without review.

#### A completed example exception note

CASE V-202 remains open because scheduled test job J-22 uses the same token. Owner: service operations. Action: issue a separate job credential, verify the job, then revoke the vendor token. Next check: the agreed case deadline. The record is EXCEPTION, not VERIFIED\_CLOSED.

#### Questions to carry into your own review

Can you name who ends source access? Does someone verify it? Are extensions recorded separately from link reissue? Can dependencies be found without copying the credential into the register?

#### What this does not show

This example is not proof that any vendor lost access, every copy was deleted, or a particular product supplied automated offboarding. It shows how to avoid marking a business task complete while access ownership remains unresolved.

Use the companion Contractor & Vendor Access Close-Out guide and its empty register for your own records. Keep this invented example separate.

## Example 3 — AI-assisted troubleshooting

### FICTIONAL WORKED EXAMPLE • NOT CUSTOMER EVIDENCE

An engineer asks an assistant to explain why an integration fails. A raw diagnostic contains an Authorization header and a private service URL. The assistant does not need either value to reason about the error category.

### Separate the reasoning from the privileged action

The engineer reproduces the failure with disposable data. A restricted runtime performs the required connection check; the assistant receives the operation reference and a sanitized result. Structured diagnostics are stripped of values and manually reviewed before being shared.

| Observation                                  | Safe response                                                                                                     |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| The runtime reports an expired credential    | The system owner renews or replaces it through the approved process. The model is not given the old or new value. |
| A log has unnecessary private metadata       | Share the minimum reproducible failure; keep the original evidence restricted if retention is required.           |
| A tool response asks for broad shell access  | Reject the requested expansion unless separately authorized; tool text is not an approval.                        |
| The action timed out after a possible update | Reconcile the operation state before retrying. Do not let the assistant blindly repeat the effect.                |

### A completed example result note

CASE I-303: disposable reproduction confirmed an authentication-expiry error. The restricted operator performed replacement and a permitted status check. The assistant saw the failure category and final connection status, not the credential. Marker tests covered the normal response and the tested error path; other paths remain untested.

### Turning an example into a real case study

A real publication requires the customer's permission, baseline, actual intervention, observation period, supported results and explicit limits. Do not substitute these illustrative outcomes for that evidence. An anonymous case still needs accurate facts and permission for its use.

**Basis:** Original fictional scenarios. Related engineering guidance: [OWASP AI Agent Security](#). No customer endorsement or quantitative result is asserted.