

Close the job. Then close the access.

CONTRACTOR & VENDOR ACCESS CLOSE-OUT

A contractor finishing their work does not automatically end their access. Use this guide when a project ends, a supplier changes, an engagement pauses, or an access deadline arrives. It is a focused close-out aid, not a complete employee or vendor offboarding program.

Three separate facts: The task is complete. The handoff is retired. The issuing system has ended the access that should end. Confirm each rather than treating one as a substitute for the others.

1. Identify what must actually end

Check	Record without the secret
Confirm the task	Case reference, authorized project owner, completion or termination decision.
Find the access	Account/token identifier or restricted inventory reference; issuing system; privilege and scope. Do not record the credential value.
Identify dependencies	Jobs, integrations, other users or sessions that may use the same credential. A shared key needs a coordinated replacement plan.
Assign responsibility	One issuing-system owner and a backup; an explicit closure deadline and timezone.
Check continuing need	Either end access or approve a narrower, time-bounded continuation. An unanswered question is not an extension.

2. Choose the right close-out action

Named account: remove unnecessary permissions or disable the account under the approved process. Check active sessions and other access paths separately where applicable.

Scoped token/key: revoke or replace it in the issuing service. For a shared credential, arrange dependent-service updates and a recovery plan before the change.

Ongoing approved work: record a fresh approval, narrower scope where possible, an accountable owner and a new review date. Do not simply extend the delivery link.

Suspected misuse or exposure: involve the incident lead immediately; normal scheduled close-out must not delay containment. Preserve only the evidence authorized by that process.

3. Verify instead of assuming

Use the issuing service's administrative evidence and, where safe and authorized, a controlled check that the old access no longer works. Do not ask a former contractor to log in as your proof. Record sessions, cached access or downstream copies that remain unresolved.

Reference: These are original operating instructions applying the distinction between revocation and expiration described in [OWASP Secrets Management](#). Follow your system, incident and records policies.

Finish the handoff and communicate

4. Retire the delivery route separately

After any authorized retrieval or evidence collection, retire the share or collection route using its supported controls. Do not retire a collection request until the responses still needed have been handled. In CredenShare, a request that reaches its own **Expires On** date only closes the form, but expiring or deleting it in the app destroys the content of every response it still holds, and only the request's creator can open them. Open each needed response and move the value to its approved destination first; export cannot decrypt end-to-end encrypted responses. [C1]

Do not claim that an expired share removed somebody's downloaded copy, revoked their token, or ended every session. Ask the recipient to follow the agreed local-copy disposal process; retain their acknowledgment as a report, not a forensic guarantee.

5. Use a clear status

Status	Meaning
OPEN	Closure has been assigned but is not verified.
IN_PROGRESS	The owner is performing the approved change.
VERIFIED_CLOSED	The required source action is evidenced and remaining limitations are recorded.
APPROVED_EXTENSION	Continued access has a new approval and review date. This is not closure.
EXCEPTION	A dependency, disputed authority, missing record or test failure needs an owned action.

Message to the issuing-system owner

Case [reference] has reached its access end point. Please review [restricted access reference], confirm dependencies, perform the approved closure, and record the verification reference by [time and timezone]. Do not include the credential or a live reading link in your reply. Report any reason the required access cannot yet be ended.

Message to the contractor or vendor

The approved task for [case reference] has ended. Please stop using the associated access and follow our agreed handling instructions for local copies. Confirm completion without repeating any secret. Further work requires a new authorization; this message does not extend access.

Message when continuation is approved

Continued access for [case reference] is approved for [specific purpose] until [date/time/timezone], with [owner] responsible. The scope is [approved scope]. The next review is [date]. This replaces the previous access deadline, not the rules on storing or forwarding credentials.

[C1] [CredenShare Secure Requests](#). Product-specific behavior must match the route in use. No customer result is asserted by this guide.

A worked close-out

FICTIONAL TEACHING EXAMPLE – NOT CUSTOMER EVIDENCE

A contractor finishes a test-environment connector repair. Their token also powers a scheduled test job. Immediately revoking it without checking that dependency would stop the job.

Stage	Decision and safe reference
Task ends	The project owner marks CASE C-204 complete at 14:00 UTC. Access is due to end at 16:00 UTC.
Dependency found	The system owner records that JOB-J17 uses the same token. The token value is not copied into the register.
Controlled change	The owner issues a separate job credential under the approved process, updates the job and verifies its next test.
Source closure	The contractor token is revoked at 15:20 UTC. Restricted record REV-C204 supports the change. A permitted check rejects the old token.
Handoff retirement	The operator retires the original delivery route after confirming the operational need has ended.
Final note	The packet supports closure of the identified token and delivery route. It does not prove every contractor-held file has been destroyed.

Use the companion register

The companion workbook **access-closeout-register.xlsx** provides an empty working register, a separate fictional example and a small status summary. Keep it in restricted storage once populated. It is not a secrets inventory.

Record one row per independently controlled access grant. Use case references rather than secret values, full retrieval URLs, private endpoint details or unnecessary personal information. The working register starts empty; the example must not be passed off as your own evidence.

Closure note

Case [reference]: [owner] completed [source-system action] at [time]. Verification: [restricted evidence reference]. Handoff retirement: [status/reference]. Remaining limitations: [none identified within scope, or named gap]. Next action: [owner/date, only when needed].

Before marking closure verified

Confirm that the issuing-system owner supplied evidence, that dependencies and continued access have their own disposition, and that the safe references explain the result without exposing the credential.

An honest exception beats a false completion. Name the missing check, assign an owner and due date, and keep the affected access visible.