

Customer Credential Request Starter Kit

A procedure and six messages for an authorized support or onboarding task. Use your organization's approved collection mechanism. **No CredenShare purchase is required to use the general guidance.** Creating CredenShare Secure Requests requires a Business or Enterprise plan; first-time Business subscribers can start a 14-day free trial. The submitter needs no paid plan; sign-in depends on the request settings below.

The working rule The conversation coordinates the task. The approved collection route carries the credential. A named system owner decides who may use it and when that access ends.

1. Ask whether the credential needs to move

Start with the task, not a request for a password. Prefer a named invitation, delegated role or a narrowly scoped temporary token when that can achieve the same result. Do not request a person's primary password, recovery code or broad production administrator credential simply because that is convenient. [G1]

Agree the task, environment, privileges, authorized contact, receiving operator, storage and access end condition. A ticket number is context, not approval.

2. Follow one complete collection process

Step	What the operator does	What stays in the ordinary work item
Authorize	Confirm the customer owner approved the task and access scope. Verify an unexpected request through an established contact route.	Safe case reference and approval reference.
Prepare	Choose the receiving operator first. That operator creates the dedicated collection request from their own account, in the correct context, with appropriate controls.	Operator, intended purpose and due date; no Access link.
Deliver	Send only the approved submission route to the verified customer contact. Deliver any separate passcode independently.	Request sent; safe reference to the case.
Receive	Retrieve through the authorized path. Use or store the value only in the approved destination.	Receipt status, not the credential.
Complete	Confirm whether the requested task succeeded. Request corrections through the same controlled process.	Task result and any unresolved issue.
Close	Have the source-system owner end temporary access when required. Retire the collection/handoff separately.	Each closure, its owner and supporting reference.

3. Know which link you are sending

With CredenShare **Secure Requests**, send the **Collect link** for submission. Keep the **Access link** private: it carries the decryption key. Save it somewhere durable before you close the creation screen. Without it, responses can be read only in the browser that created the request or on a device activated for zero-knowledge custody. On any other device, paste it into the request's submission viewer to read responses. Never send it to the submitter or forward it to colleagues.

A submitter needs an account only when the creator requires sign-in, or when a request created through the API requires two-factor authentication. [C1]

Keep secrets out of this kit, screenshots, email replies, ordinary tickets and AI prompts. A live Access link is sensitive access material too. Follow stricter organizational or customer requirements where they apply.

Send the request and acknowledge receipt

Copy-ready wording. Replace every bracketed field before sending. Choose only the information needed for the agreed task. Use your normal organizational signature. These are task messages, not a marketing sequence.

Initial request

Subject: Access needed for [case reference / agreed task]

Hi [name],

To complete [agreed task] in [environment], we need the access approved by [system owner]. Please use a named invitation or delegated role when that meets the requirement. If a credential is necessary, provide only the scoped [credential type] for [minimum privileges], with access ending at [time and timezone / agreed condition].

Submit it through this approved collection route: [COLLECTION LINK ONLY]. Do not reply with the credential or send recovery material. If this request is unexpected, verify it through our established contact route before submitting anything.

Once submitted, reply with [case reference] only. [Named operator/team] will use the information solely for the agreed task. Please contact us first if the requested scope is not available.

Reminder for an agreed, outstanding request

Subject: Access request for [case reference]

Hi [name],

The approved access for [case reference] is still outstanding, so [task] remains on hold. Please use the collection route in our verified earlier message; do not send the value in this reply.

If the scope, owner or timing has changed, let us know before submitting. We can agree a revised next step instead of requesting broader access.

Use this only while the request is still expected and appropriate. Do not turn it into an indefinite follow-up sequence. Confirm the submission route is usable before directing the customer back to it.

Receipt acknowledgment

Subject: Information received for [case reference]

Hi [name],

We received the information for [case reference] through the approved route. [Operator/team] will use it for [agreed task] and confirm the result without repeating the value.

[System owner] remains responsible for ending temporary access at [agreed time or condition]. We will let you know when the task is complete.

Receipt is not validation. Use "received" only after the authorized operator confirms receipt. Do not say "working" or "verified" until an appropriate authorized check has actually passed.

Handle corrections and closure

A credential arrived in the ticket or email

Subject: Please pause credential sharing in [case reference]

Hi [name],

A credential was included in the ordinary conversation for [case reference]. Please do not resend or quote it. We are notifying the responsible security/system owner to assess the exposure and the appropriate replacement or revocation action.

Any replacement should come through a new, verified collection request. We will coordinate removal of the exposed material under the applicable incident and records process. Deleting a message alone does not establish that the credential is safe to keep using.

Do not copy the value into replies or diagnostic tools. Follow your incident procedure, coordinate containment with the owner and consider service dependencies. [G1]

A correction is needed

Subject: Correction needed for [case reference]

Hi [name],

We could not complete [authorized task] because [non-sensitive issue, such as insufficient approved scope or incorrect environment]. Please confirm the intended scope with [system owner].

Do not send a broader credential in reply. Once approved, use [verified collection route / newly issued collection request] for the correction. Keep the values out of screenshots and ordinary messages.

A timeout does not establish an invalid credential. Describe the observed problem, not an assumed cause.

The task is complete; source access needs closure

Subject: Task complete; access closure for [case reference]

Hi [name],

[Agreed task] is complete. Please have [system owner] end the temporary access under the agreed procedure, taking any dependencies into account, and confirm completion using a safe reference only.

We will separately retire the handoff/collection under our approved process. That does not revoke the credential in the source system. If access must continue, please obtain a new documented approval and review date.

Check the two lifetimes before closing a request

CredenShare documents the form's scheduled end separately from the lifetime of submitted responses. Using **Expire request now** destroys every submission's content at once; the submission records stay as an audit trail, but their content cannot be recovered. Before you use it, open each response you still need in the submission viewer and move the value to its approved protected destination. The request page's export cannot decrypt end-to-end encrypted submissions, so do not rely on it as a copy. Never copy credentials into this kit or the ordinary work item. [C1]

Use disposable data for demonstrations; never a customer's live credential.

A worked example you can reuse

Fictional teaching example. No real customer, credential or test result is represented.

An onboarding team must verify a staging connection. The customer authorizes a temporary read-only integration token rather than providing a personal administrator password.

Decision	Completed example
Case and task	ONB-104: verify a staging connection; no production writes.
Approval	Customer system owner recorded in approval AP-104.
Receiving operator	Named onboarding operator, who creates the request from their own account; no shared personal login.
Access scope	Staging only; read-only permissions needed for the check.
Access boundary	Customer owner to revoke after the check, no later than 16:00 UTC on the agreed day.
Collection instructions	Dedicated submission form. Access link kept private, outside the ticket.
Allowed destination	Authorized test runtime / protected store for the agreed task, not a personal note.
Result	Operator confirms the check completed; the credential is not copied into the case.
Closure	Source owner records revocation and its verification. Handoff retirement is recorded separately.

Configure your first real request

For this example, consider **case reference**, **environment**, **scoped integration credential**, and **access end condition**. Remove information already known or unnecessary. Do not collect extra credentials "just in case."

Agree recipient verification, form lifetime, response lifetime, operator access and absence coverage. **Create the request from the account that will receive the value.** Only that account can read the request's submissions; team owners and admins cannot, and reading cannot be delegated. Plan for absence before you create the request: if the intended receiver may be unavailable, have someone who will be available create it from their own account, or use another approved workflow. Never use a shared login.

Confirm the procedure with a disposable rehearsal

Use **TRAINING-NOT-A-REAL-SECRET** in a nonproduction exercise. Check submission, authorized retrieval and the receipt message. Rehearse an expired request without weakening the process. The operator should explain the next safe action, not merely open a page.

If you cannot establish the required operator access, recipient restrictions or continuity route, pause the request and choose an approved alternative. Do not share a personal account to bypass the problem.

References and scope

[C1] [CredenShare: Secure Requests](#). Product-specific link, plan and lifecycle details were checked against the CredenShare documentation and updated on 2 October 2026. Product behavior can change; confirm current behavior in the documentation before relying on a particular control.

[G1] [OWASP: Secrets Management Cheat Sheet](#). Background on least privilege, lifecycle and exposure response. The operating procedure, examples and messages here are CredenShare-authored guidance, not requirements issued by OWASP.

This resource is not a personalized assessment, a certification or a promise that all external copies have been removed. Adapt the wording to the customer's approved access and records processes.