

Choose the Right Access or Sharing Method

A two-page decision guide. Start with the task below. The right answer may be an existing identity, vault or secrets-management capability, rather than another sharing tool.

First, establish the task

Name the approved recipient, the action they need to perform, the system owner and the permitted duration. Do not start with "How do I send this password?" when the person could be granted a suitable named role instead.

Work through these decisions in order

Decision	Choose this approach	Check before proceeding
1. Can a named account, invitation or delegated role do the job without transferring a reusable secret?	Use the source system's approved access-management route.	Correct privileges, owner, end date and removal process.
2. Is a person obtaining continuing access to an existing credential already managed in an approved password manager?	Use the approved vault's access-sharing capability where suitable.	Its permissions, recipient support and revocation behavior fit the task.
3. Does an application need to retrieve a secret repeatedly at runtime?	Use the approved application secrets manager or equivalent managed identity pattern.	Runtime authorization, rotation, dependencies and failure handling. A temporary link is not a secrets store.
4. Must somebody provide a credential you do not yet hold?	Use an approved protected collection request.	Minimum information, receiving operator, submission route, response lifetime and continuity.
5. Do you already hold a credential that an authorized recipient needs for a bounded handoff?	Use an approved temporary sharing mechanism.	Recipient restrictions, delivery window, permitted destination and source-access closure.
6. Is the task really to share a diagnostic excerpt?	First remove secrets and unrelated data. Use an approved text-transfer path for what remains.	Review the actual content and ownership requirements; "sanitized" is not a guarantee.

None fits, or a mandatory control is unavailable? Ask the system/security owner to approve an alternative. Do not move to ordinary email, a public paste or a shared personal login just to finish faster.

Four facts to keep separate Authorization says who may use the system. Transfer moves a value. Storage keeps it available for later use. Evidence records what was approved or observed. One tool does not automatically perform all four jobs.

The decision order is a recommended workflow, not a product ranking or a universal security standard. Review stricter organizational and customer requirements first. General background: [OWASP Secrets Management](#).

Apply the choice to a real situation

Four completed examples

Situation	Recommended starting choice	What still needs an owner
A colleague needs ongoing access to the finance application.	A named application account or delegated role; no shared personal password.	Source-system permissions, review and removal.
An integration service needs a database credential on every start.	The approved runtime secrets-management route or managed identity where supported.	Rotation, workload permissions and service continuity.
A customer must provide a scoped staging API token for onboarding.	A dedicated protected collection request, if delegation does not meet the task.	Receiving operator, correct scope, response handling and customer-side revocation.
A contractor must use an existing scoped credential for a two-hour diagnostic.	A protected temporary handoff to the authorized person, if a named account is not suitable.	Intended storage/use, dependencies, task end and source-system access closure.

These are illustrative decisions, not findings about a particular organization.

What a temporary link does not settle

An expired link does not revoke a password or token already retrieved. Have the issuing-system owner verify the access change when needed. Do not equate message deletion with containment or source-access closure.

A view event is not business authorization. Establish the intended recipient and approved purpose separately. A recipient acknowledgment also does not prove that no additional copy exists.

A preset is not an enforced policy. Inspect the actual protections for the chosen route and recipient. Test unfamiliar paths with disposable data before relying on them.

Where CredenShare fits

CredenShare documents **Secure Shares** for sending a value you hold and **Secure Requests** (Business and Enterprise) for collecting one somebody else holds. Send the submitter the **Collect link**; the **Access link** carries the decryption key and stays with the request's creator. [C1]

Use the product only where its verified controls fit the chosen handoff. It does not replace your source system's access-management duties or the approved long-term storage for the credential.

Record the decision in one useful sentence

For [case reference], [system owner] approved [recipient or workload] to perform [task] using [selected method], with [scope and duration]. [Owner] will verify access closure or the next review. The credential remains in [approved protected destination], not in this note.

Keep that note free of the value, live reading links and unnecessary personal details. If scope or duration changes, obtain the required new approval rather than silently issuing another link.

[C1] CredenShare: [Secure Requests and when to use a Share](#). Product distinction checked 29 September 2026. [General lifecycle background: OWASP](#). Examples and decision sequence are original guidance, not a certification or a review of your systems.