Your Guide To CLAWOLF

Understand The Screen. Follow The Workflow. Keep The Evidence.

A practical guide for people using CLAWOLF AS-OS for the first time. Chapters follow the current menu: Command Center, AS-OS Workflows, Evidence & Reporting, then Organization & Onboarding.

Before You Begin

What The Words Mean

A mission is a defined piece of security work. A runtime run is one recorded attempt to perform that work. Evidence is information supporting what happened. A report presents the recorded result and its limitations to a reviewer. Always confirm the organization, selected record and observation time before comparing screens.

How To Use Each Chapter

Read its introduction first. Understand The Screen explains panels, fields and tabs. Step By Step takes you through the task and its expected result. If Something Goes Wrong names the precise menu to revisit. Related submenu links that share one workspace are explained together, not copied into duplicate chapters.

States And Permissions

Empty means no matching record was found; unavailable means a source could not be read; blocked means a requirement prevents progress. None is a success claim. The guide does not grant a license, approve an action or execute production work. Use the owning workflow and only the controls allowed by your role.

Offline Use

The guide needs no external AI service or internet connection. Keep the downloaded copy inside approved storage. For unresolved errors retain the request reference, organization, record identity and time for your designated internal operator; never send secrets to the guide.

Manual wave-d.3 · Application 928cb37058f4fbafc21b8dbbeb40bdab6376ca46

Content Reference 1a428399dc8c40730d5a7b8b9d8d55dd2b7e0c093d75c5b1fcafc3bc248216dd

Contents In Menu Order

Command Center

1. Runtime Command 3
2. Mission Workspace 8
3. System Health 23

AS-OS Workflows

4. Detection 26
5. Investigation 29
6. Decision 32
7. Action 35
8. Governance 38
9. Learning 41

Evidence & Reporting

10. Analyst Reports 44
11. Evidence Center 48
12. Report Builder 51
13. Audit Packs 55
14. Findings & Exceptions 58
15. Export History 61
16. Decision Bundles 64
17. Investigation Bundles 67

Organization & Onboarding

18. Onboarding Progress 70
19. Organization & Tenant Profile 73
20. Admin Settings 81
21. Subscription & Entitlements 92
22. Deployment Configuration 98
23. Ecosystem Workspace 106

Appendix

24. Offline Installation Procedures 110

1. Runtime Command (Signed-In User (Read-Only))

Runtime Command is the starting point for watching security work across your organization. A runtime is one recorded attempt by AS-OS to examine information, make a decision and, where permitted, carry out an action. The central diagram shows which parts of that work have recorded activity; the surrounding cards open the workspaces used to examine it. The four lower maps summarize attack references, decision-core participation, behavioral observations and operational measurements. Use this screen to orient yourself, then open the relevant workspace rather than trying to operate the maps.

Understand The Screen

Command Bar (Signed-In User (Read-Only))

Operating Mode describes how the environment may behave; HITL describes human-in-the-loop oversight. These are governed settings, not instructions to switch them for a clearer chart. Menu On and Sidebar On are two presentations of the same navigation. Assistant opens backend-guided assistance in a separate tab. Help Tutorial opens the illustrated manual in another tab, so the original operating screen remains usable.

Five-Layer Diagram (Signed-In User (Read-Only))

Detection examines input; Decision chooses a proposed response; Action records execution; Control enforces safety and permission; Learning retains feedback. Investigation supports work across these layers. A lit function means recorded activity, not proof that every layer succeeded or a license to execute it.

Six Surrounding Cards (Signed-In User (Read-Only))

HITL Workspace opens Operating Control for human review. Workspace Selection opens the workspace selector. Activity Timeline and AS-OS Performance open the corresponding Mission Workspace sections. Evidence Report opens the reporting workflow when your role allows it. System Health opens component readiness. Read-only or unavailable cards cannot be used to bypass permissions.

Runtime Command - Continued

MITRE ATT&CK And 21 Logic Core Maps (Signed-In User (Read-Only))

MITRE ATT&CK is a classification of adversary techniques; marked cells show techniques referenced by recorded runs, not a coverage percentage. Logic cores are registered decision evaluators; their colors identify categories and their outcomes show participation. Recent activity can pulse. With no qualifying run, category colors remain but activity is not fabricated.

Behavioral Analytics And Sovereign KPI Metrics (Signed-In User (Read-Only))

Behavioral Analytics shows observed and heuristic signals, not invented user risk scores. The KPI board shows AI Detection, MTTD, MTTA, MTTC, FP Rate, Automation Rate, Average Heal Time and Heal Rate. MTTD is time to detection, MTTA to acknowledgement and MTTC to verified containment. A blank or unmeasured value means the required observations are missing; the lower counters count recorded samples, not protection quality.

Step By Step

1. Start With The Organization And Window (Signed-In User (Read-Only))

Open Command Center > Runtime Dashboard. Confirm the organization and the displayed time window before reading any status. The menu calls this Runtime Dashboard; its page heading is Runtime Command.

2. Read The Connection And Recorded Time (Signed-In User (Read-Only))

Check whether telemetry is live, polled, stale or unavailable. Live telemetry describes the connection, not a claim that a security action is currently executing. Read the run timestamp to distinguish a recent run from history.

3. Reload Recorded Activity (Signed-In User (Read-Only))

Select Reload recorded runtime activity to read the newest admitted run and its events. The button does not create a run. If the newest record is old, the screen must keep its old recorded time rather than presenting the refresh time as execution time.

Runtime Command - Continued

4. Follow The Appropriate Card (Signed-In User (Read-Only))

For a human decision open HITL Workspace; for the operational record open Workspace Selection or Activity Timeline; for infrastructure questions open System Health. Check that the destination retains the intended organization and selected record.

5. Interpret A Highlight Or Metric (Signed-In User (Read-Only))

Compare a map highlight with its recorded outcome in Mission Workspace. Do not interpret no observations as zero risk, or an available KPI sample as proof that an entire customer environment is protected.

Runtime Command - Continued

If Something Goes Wrong

All Maps Are Quiet

No qualifying runtime is recorded in the selected window.

Where To Go: Command Center > Mission Workspace > Missions

Select the relevant recorded mission and inspect its Execution Path. Do not generate synthetic activity to fill the map.

Unavailable Or Stale Telemetry

The screen cannot currently read its source, or its last successful read is too old.

Where To Go: Command Center > System Health

Check Backend readiness and Data ingestion. After the operator resolves the affected source, return here and reload recorded activity.

Evidence Report Is Read Only

Your current role does not permit the reporting destination.

Where To Go: Organization & Onboarding > Admin Settings > USERS

Ask the authorized administrator to review your assigned role; do not change account or organization to evade the restriction.

Command Bar (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Reload recorded runtime activity

Reload selects the latest admitted run for this tenant. It does not start a new run.

2. Operating mode

Read the effective mode; open Operating Control to inspect its policy, not to learn by saving changes.

What Happens

Reload refreshes recorded activity only.

2. Mission Workspace (Analyst / Operator; Authorized Actions Only)

Mission Workspace is the place to organize and follow a specific security task. A mission records an objective, the assets or systems in scope, its owner and the work needed to reach a result. It is different from a runtime: a mission may have no execution yet, or several recorded attempts. Its four tabs separate mission preparation, operating safeguards, the event history and performance measurements. Start by selecting or preparing a mission, then follow its readiness, execution and evidence instead of treating a visible button as permission to run.

Understand The Screen

Missions - Queue And Brief (Analyst / Operator; Authorized Actions Only)

The queue searches and filters missions by state and type. Select a queue item before editing it. Objective states what you want to accomplish; Mission Type classifies the work; Priority sets its handling priority; Owner identifies responsibility; Scope names the affected assets or boundary; Environment / Mode selects the intended environment; Governing Policy records the applicable policy. Adopt Run ID links a known runtime through Adopt Existing Run; it does not manufacture an execution.

Missions - Readiness (Analyst / Operator; Authorized Actions Only)

Readiness checks whether this mission has its required inputs and governing conditions. Run Readiness evaluates the selected mission; it is not Start Mission. A blocked condition remains visible with its owner and reason. Readiness is not a blanket approval for all later actions.

Missions - Execution Path And Control Gates (Analyst / Operator; Authorized Actions Only)

Execution Path lists lifecycle, checkpoint and attempts, including start, end, actor, duration and runtime receipt. Control Gates & Blockers explains the condition preventing progress, its source, owner and acknowledgement. A mission, attempt and runtime receipt are different records; use the receipt to follow the actual execution.

Mission Workspace - Continued

Missions - Mission Controls (Analyst / Operator; Authorized Actions Only)

Create New Mission creates a draft from its objective; Save Draft persists permitted edits. Adopt Existing Run associates a recorded run. Queue Mission and Start Mission are distinct transitions. Pause Mission, Resume Mission and Retry Failed Attempt operate only when their current state and policy permit. Assign / Hand Off records responsibility; Acknowledge Blocker records awareness, not resolution. Request Approval does not grant approval. Cancel Mission, Close Mission and Archive Mission have different terminal and record-retention effects. Read the disabled reason before considering any control.

Missions - Evidence & Closure (Analyst / Operator; Authorized Actions Only)

Closure criteria check a terminal lifecycle, the persisted closure record, attached evidence and unresolved exceptions. A completed attempt is not automatically a closed mission. Review the evidence links and the recorded outcome before Close Mission. Archive Mission does not mean delete its history.

Operating Control (Admin / Explicitly Delegated User; Authorized Approver For Decisions)

This tab is the governed home for mode, severity handling, approvals, confirmation, protected targets and delegation. Low is the strictest human-review threshold: low, medium, high and critical all require review. Medium reviews medium/high/critical; High reviews high/critical; Critical reviews critical. Below-threshold actions still face operating mode, protected-target, licensing and all other gates. Selecting a setting creates a draft; confirmation, a fresh authenticator code when requested, and Save are separate steps. Mode and severity changes require Admin or explicit delegation; protected-target and delegation administration require Admin. Approvals require the authority specified for the exact item. Read First! explains each effect without changing anything.

Activity Timeline (Analyst / Operator; Authorized Actions Only)

This tab is the chronological record of activity for the selected scope. Check run identity and event time, then follow the recorded stage, function and outcome. Reloading or opening this tab reads history. A connected stream and an old event are not a new execution.

Mission Workspace - Continued

AS-OS Performance (Analyst / Operator; Authorized Actions Only)

This tab explains recorded timing and performance observations. Read the sample count, window and unit before comparing values. Not measured means the required observation is absent, not a zero-duration operation. A historical median does not promise the same latency in another deployment.

Step By Step

1. Select A Mission Or Prepare A Draft (Analyst / Operator; Authorized Actions Only)

Open Command Center > Mission Workspace > Missions. Search the queue and choose the intended mission. For new work, enter a clear Objective, Mission Type, Priority, Owner, Scope, Environment / Mode and Governing Policy; use Create New Mission and then Save Draft where available.

2. Check Readiness Before Execution (Analyst / Operator; Authorized Actions Only)

Use Run Readiness on the selected mission. Read each blocker and its owner in Control Gates & Blockers. Correct profile, binding or deployment prerequisites in their owning administration screen rather than changing the mission status manually.

3. Review Operating Control (Analyst / Operator; Authorized Actions Only)

Open Operating Control. Read the currently recorded mode, protected target restrictions and approval requirements. Where human review is required, an authorized reviewer must use the approval control for this exact action and scope.

4. Use Only The Allowed Transition (Analyst / Operator; Authorized Actions Only)

Return to Missions. Review the effect and available controls, then use the applicable Queue, Start, Pause, Resume or Retry operation if authorized. A disabled control is a boundary to understand, not a reason to use another route.

Mission Workspace - Continued

5. Follow The Actual Outcome (Analyst / Operator; Authorized Actions Only)

Inspect Execution Path and Activity Timeline for the matching attempt and run. If execution fails, retain the failure reason and inspect evidence; do not call the mission successful solely because an approval was accepted.

6. Review And Close (Analyst / Operator; Authorized Actions Only)

Check Evidence & Closure, unresolved exceptions and recorded result. Use Close Mission only when its criteria and role allow it. Retain evidence before archiving according to your organization’s policy.

Mission Workspace - Continued

If Something Goes Wrong

No Mission Selected

The workspace has no selected record, so record-specific controls cannot act.

Where To Go: Command Center > Mission Workspace > Missions

Select an item in Mission Queue or create a draft. Confirm its identity in the header.

Binding Or License Required

The requested function has no usable entitlement or service binding for this organization.

Where To Go: Organization & Onboarding > Subscription & Entitlements; then Ecosystem workspace

Have an authorized administrator inspect the installed entitlement and assigned binding. Return to this mission and rerun readiness after a legitimate change.

Awaiting Approval

A person with the required authority must review the proposed action.

Where To Go: Command Center > Mission Workspace > Operating Control

Review the precise target, requested action and evidence. After the authorized decision, refresh the mission; approval does not guarantee execution success.

Failed Or Degraded Attempt

The recorded attempt stopped or did not reach its verified outcome.

Where To Go: Command Center > Mission Workspace > Missions > Execution Path

Read the checkpoint and failure reason. Check System Health if the source or executor failed; only retry after correcting the reason and confirming that Retry Failed Attempt is permitted.

Mission Queue (Analyst / Operator; Authorized Actions Only)

Isolated Demonstration - Not Your Current Tenant State



1. Search missions

Type text from a known mission title or identifier.

2. Filter by state

Select the recorded lifecycle state you want to review.

3. Adopt runtime run identifier

Copy a genuine runId from Activity Timeline or an authorized runtime record. Paste it unchanged; use Adopt only when authorized.
Illustrative Format Only: <copy your tenant's recorded runId>

What Happens

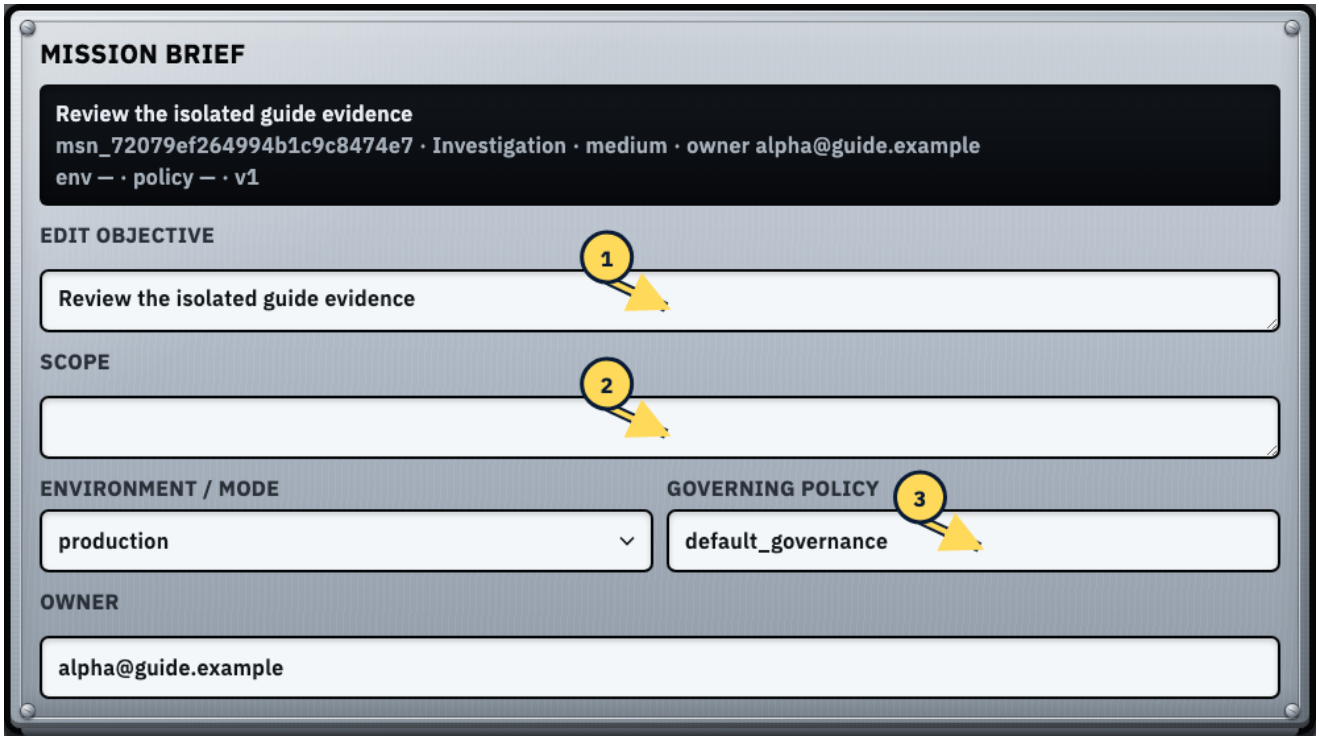
Search and filtering are read-only. Adopt persists a mission association; it does not execute the run.

Read First

Adopt changes records. Do not use an invented or another tenant's runId.

Mission Brief (Analyst / Operator; Authorized Actions Only)

Isolated Demonstration - Not Your Current Tenant State



1. Edit objective

State the intended security outcome in plain language.
Illustrative Format Only: Investigate the selected alert and retain the evidence.

2. Scope

Name the approved assets and boundary. An example is not permission to target that asset.
Illustrative Format Only: <approved asset scope>

3. Governing policy

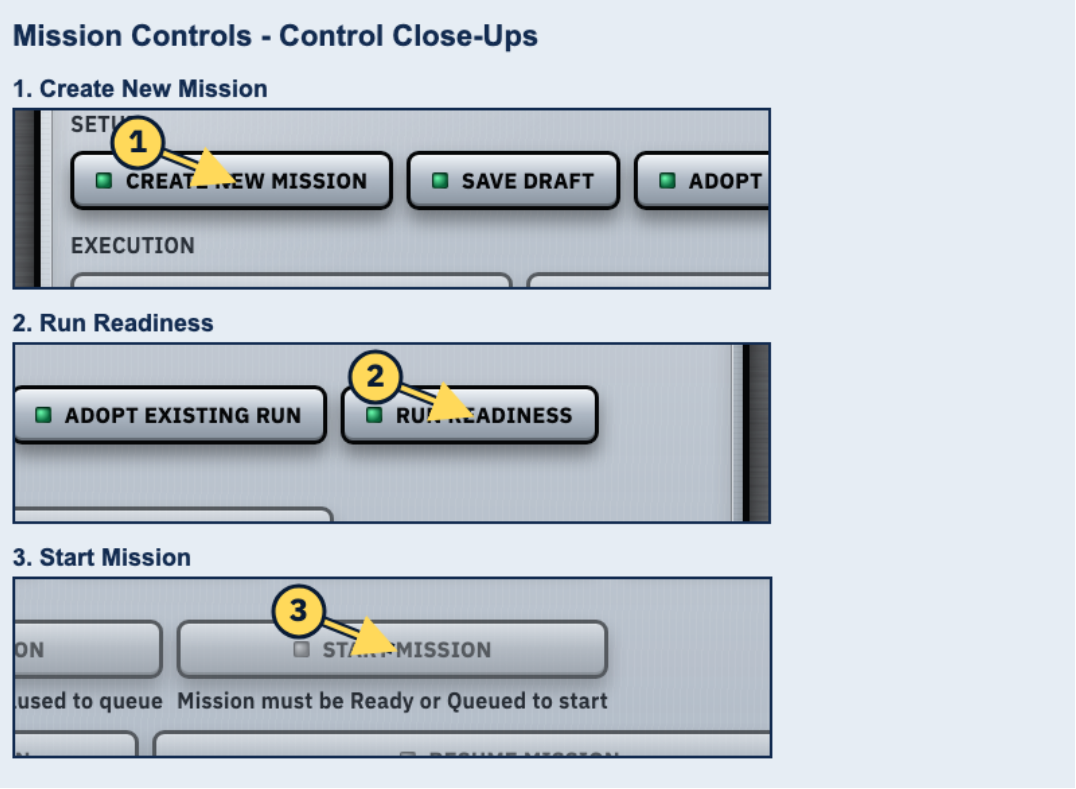
Use the policy reference approved for this organization; do not invent a policy ID.

What Happens

Saving a brief changes the selected mission; it does not prove readiness or execute actions.

Mission Controls (Analyst / Operator; Authorized Actions Only)

Isolated Demonstration - Not Your Current Tenant State



1. Create New Mission

Creates a draft from the entered objective, type, priority and scope; it does not start execution.

2. Run Readiness

Checks the selected mission's prerequisites. Inspect reasons before using Start.

3. Start Mission

Can dispatch governed work when authorized and ready. Do not press it merely to follow a tutorial.

What Happens

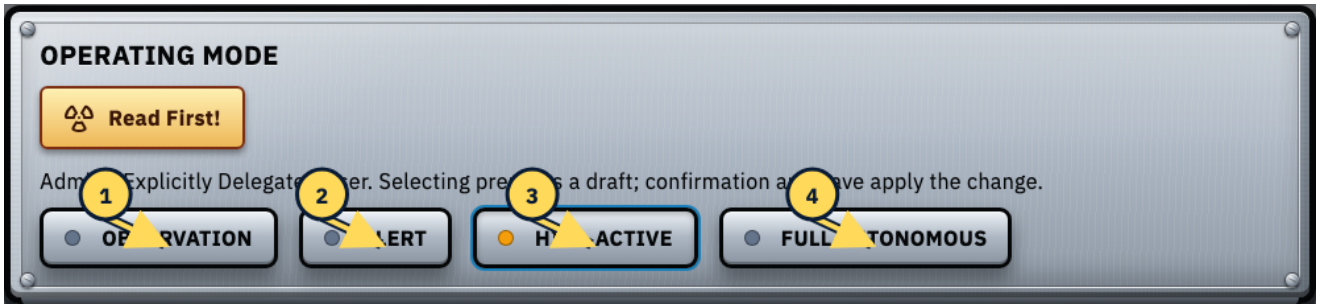
Start, resume and other offered actions can change the mission lifecycle or dispatch governed work. Inspect the recorded outcome, not only a button acknowledgement.

Read First

These are operational controls, not tutorial practice buttons.

Operating Mode (Admin / Explicitly Delegated User)

Isolated Demonstration - Not Your Current Tenant State



1. Observation

Observe and enrich without response or remediation.

2. Alert

Observe, enrich and notify without response or remediation.

3. HITL

Use the effective review threshold and stronger applicable policy.

4. Full Autonomous

Only eligible, licensed and governed work may execute; selecting this is not an execution guarantee.

What Happens

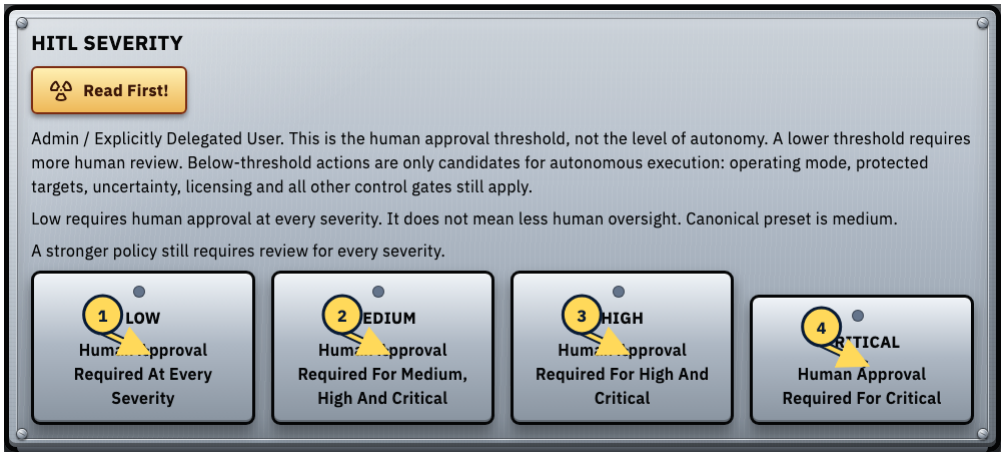
Selecting a button prepares a draft only. Read the proposed change, tick I confirm this change, enter a fresh enrolled authenticator code when requested, and press Save. Expanding authority or choosing Full Autonomous requires step-up verification. Check the effective state after saving; a configured selection is not proof that it is effective.

Read First

Selecting prepares a draft; Save changes policy. Read the effective mode after saving.

HITL Severity (Admin / Explicitly Delegated User)

Isolated Demonstration - Not Your Current Tenant State



1. Low

Human Approval Required At Every Severity

2. Medium

Human Approval Required For Medium, High And Critical

3. High

Human Approval Required For High And Critical

4. Critical

Human Approval Required For Critical

What Happens

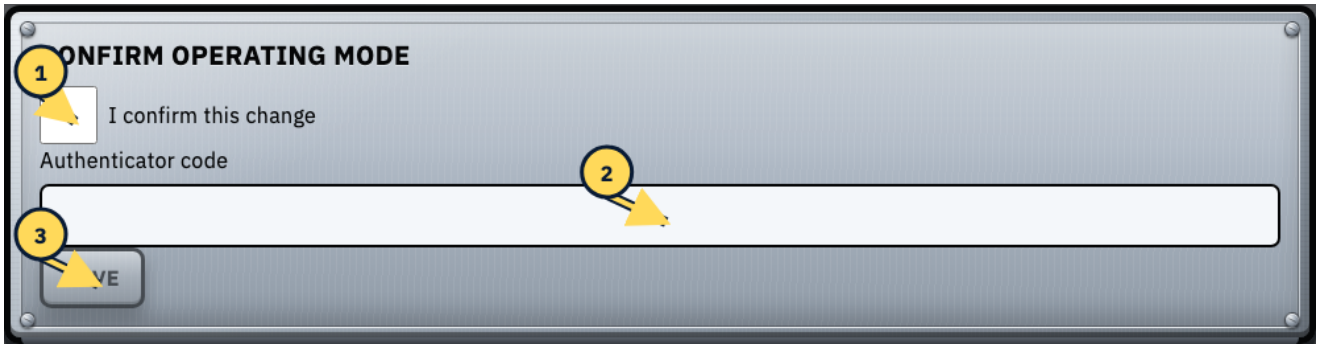
Low requires human approval at every severity. Medium reviews medium and above; High reviews high and critical; Critical reviews critical. Increasing the threshold relaxes review and requires a fresh enrolled authenticator code. Selecting a threshold does not save it: confirm, then Save. A stronger policy can still require review at every severity.

Read First

This is the human approval threshold, not the level of autonomy. A lower threshold requires more human review. Below-threshold actions are only candidates for autonomous execution: operating mode, protected targets, uncertainty, licensing and all other control gates still apply.

Confirm Operating Mode (Admin / Explicitly Delegated User)

Isolated Demonstration - Not Your Current Tenant State



1. I confirm this change

Confirm only after reviewing the draft and its operational effect.

2. Authenticator code

Enter your own current code from the enrolled authenticator when requested. Never copy a guide example or put it in Assistant.

3. Save

This is the step that submits the policy change. Read success or rejection, then check the effective state.

What Happens

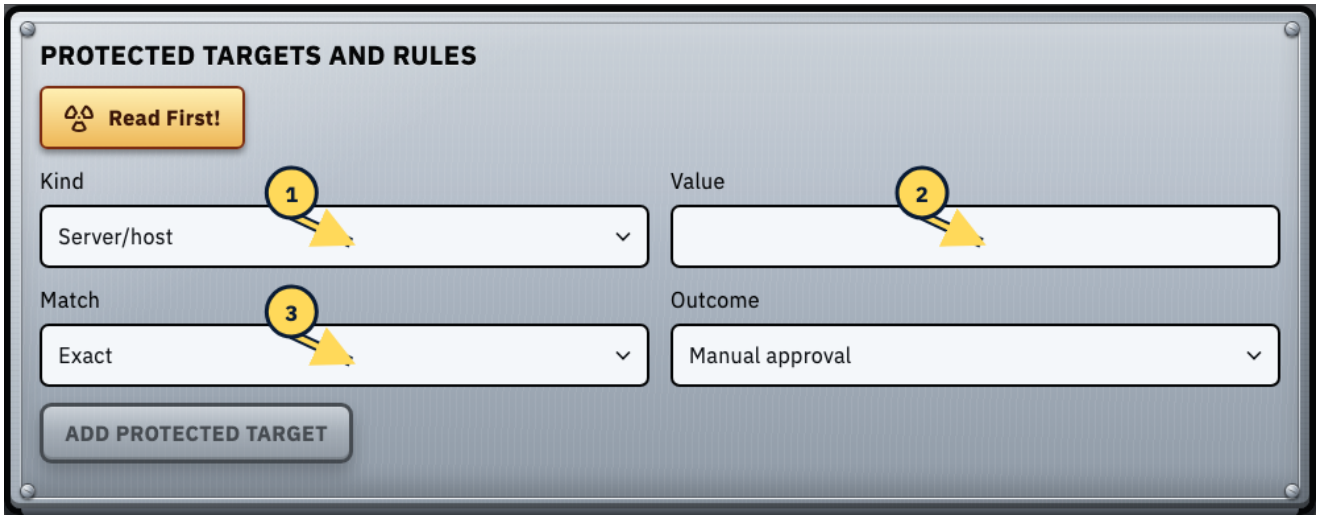
The screenshot shows a draft confirmation in an isolated demonstration; no change was saved.

Read First

Learning is not permission to change policy.

Protected Targets And Rules (Admin)

Isolated Demonstration - Not Your Current Tenant State



1. Kind

Choose the actual asset type.

2. Value

Enter an approved identifier. For a host use its recognized name; for a network use the supported address format.
Illustrative Format Only: host.example.internal (illustrative only)

3. Match / Outcome

Review matching breadth and the protection outcome before applying it.

What Happens

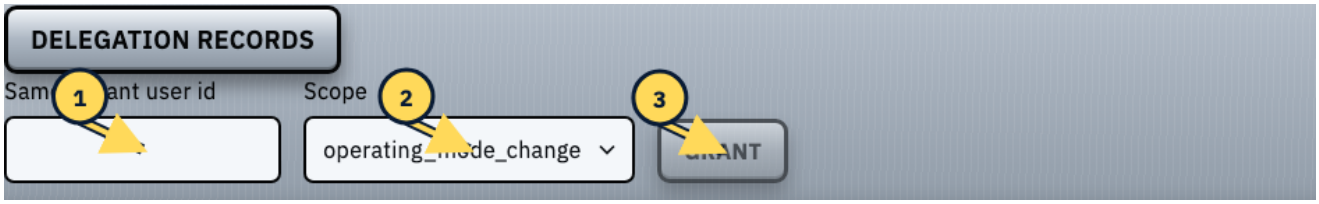
Use an approved asset identifier, not a fabricated host. Review the match scope and outcome before saving. Disabling protection requires the existing confirmation and step-up verification. Retain the result and use this same card to inspect the recorded rule.

Read First

Changing or disabling protection affects subsequent governed work.

Admin Delegation (Admin)

Isolated Demonstration - Not Your Current Tenant State



1. Same-tenant user id

Use the actual numeric ID of the intended user, not their email.
Illustrative Format Only: <recorded numeric user ID>

2. Scope

Choose operating_mode_change or hitl_severity_change; one grant does not grant both scopes.

3. Grant

Requires the existing authenticator prompt; submits the scoped grant.

What Happens

Obtain the intended numeric user ID from Admin Settings > USERS. Choose the precise scope, review identity, then follow the existing confirmation and authenticator procedure. Revoke removes that grant; it does not disable the user account.

Read First

Grant and Revoke change another user's authority. Do not use them to practice.

Activity Timeline (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Refresh

Reads recorded activity; does not start another run.

2. Mission Queue

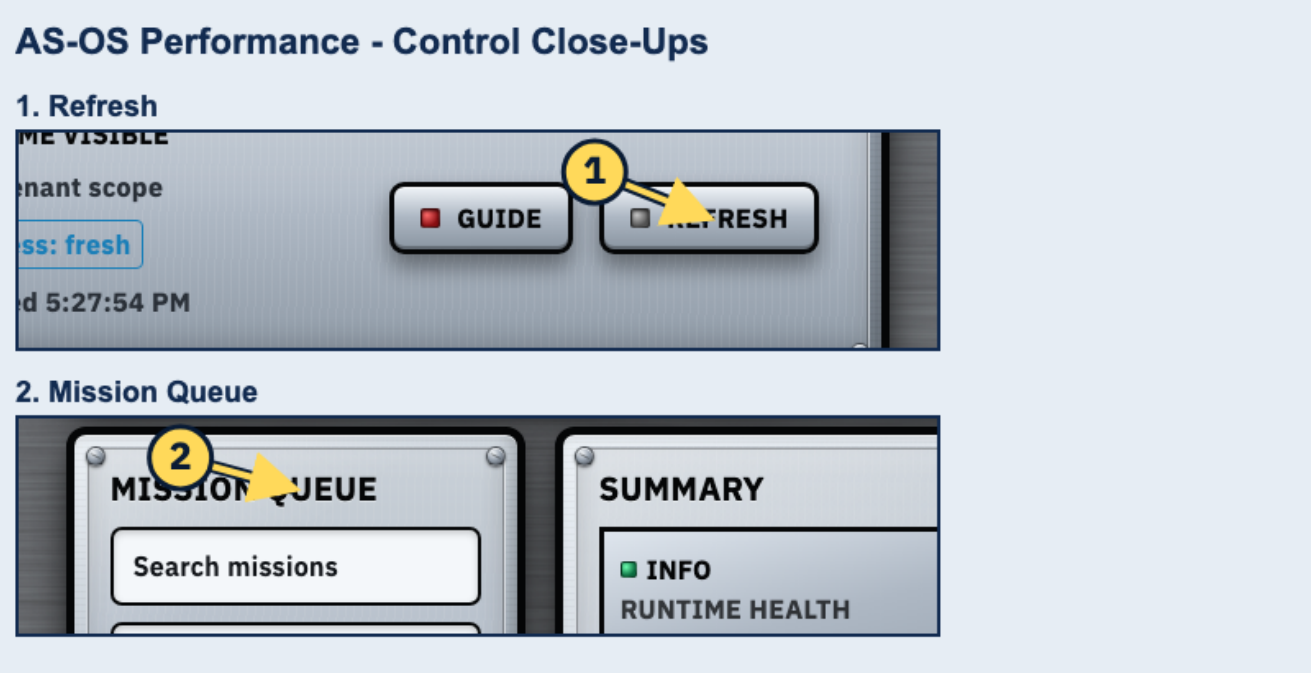
Select the intended mission; an empty draft has no executed activity.

What Happens

Review the recorded actor, time and outcome. Refresh does not make a blocked or unexecuted stage complete.

AS-OS Performance (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Refresh

Refreshes measurements for the selected recorded context.

2. Mission Queue

Choose the mission whose recorded timings you need to inspect.

What Happens

Missing measurements are not zero latency or a performance guarantee.

3. System Health (Signed-In User (Read-Only))

System Health helps you distinguish a service problem from missing configuration or missing observations. It reads the readiness reported by the runtime, backend, integrations and ingestion sources. Each domain has its own status and explanation, so one healthy component does not certify the whole deployment. You can use this screen to locate the affected domain and identify which setup workflow to revisit. It is a read-only health view, not a deployment activation or repair button.

Understand The Screen

Health Domains (Signed-In User (Read-Only))

Runtime readiness concerns the runtime prerequisites; Backend readiness concerns the service; Capability health concerns available capability observations; Kernel live state concerns the kernel; Queue / HITL depth concerns queued or human-review work; Deployment mode describes placement. Read each domain’s state and observation time separately.

Vendor Integration Health And Data Ingestion (Signed-In User (Read-Only))

An installed connector and a working feed are separate facts. Review the named vendor or source and its own reported condition. Unconfigured, unavailable and failed do not mean the same thing; an empty list is not proof that every vendor is healthy.

Claim Safety (Signed-In User (Read-Only))

This panel identifies whether displayed claims have the required observations. It prevents an absent observation from becoming an invented healthy result. Use the reported reason to identify what evidence is missing.

Step By Step

1. Confirm The Environment (Signed-In User (Read-Only))

Open Command Center > System Health and confirm the organization and observation time.

2. Locate The Affected Domain (Signed-In User (Read-Only))

Read Health domains first, then Vendor integration health and Data ingestion. Match the problem to the actual component, not the overall color.

System Health - Continued

3. Return To Its Configuration (Signed-In User (Read-Only))

For a connector or feed use Organization & Onboarding > Deployment Configuration > Ingestion Setup. For a missing service binding use Ecosystem workspace. Infrastructure recovery remains with your designated operator.

4. Verify Recovery At The Source (Signed-In User (Read-Only))

After the authorized correction, reload this view and confirm that the affected domain now reports a new successful observation. A browser refresh alone does not repair a service.

If Something Goes Wrong

Backend Readiness Is Unavailable

The health source could not be read.

Where To Go: Command Center > System Health > Backend readiness

Retain the reason and observation time for your internal operator. Do not assume that missing information means the service is healthy.

No Ingestion Observations

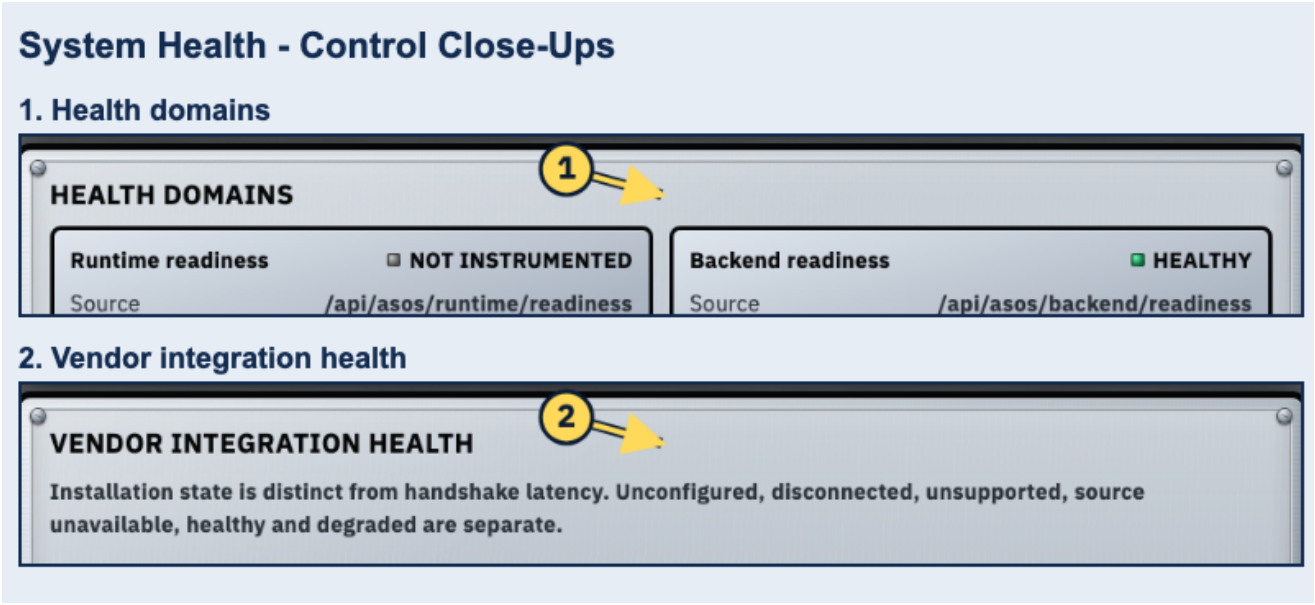
The configured source is absent, disabled or has no matching observations.

Where To Go: Organization & Onboarding > Deployment Configuration > Ingestion Setup

Check the selected method, source configuration and authorized validation result; return here after verification.

System Health (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Health domains

Review the reported source health and observation time.

2. Vendor integration health

A configured integration is not proof of live connectivity.

What Happens

Read-only health review. Return to Deployment Configuration or Admin Settings > CONNECTORS for the named configuration issue.

4. Detection (Signed-In User (Read-Only))

Detection is the workflow for understanding the information that AS-OS has examined. Telemetry means observations received from systems, logs or other configured sources. This page connects those observations with detection activity and the domain context used to interpret them. You can narrow the view to a mission or run, inspect recorded rows and follow their evidence. It does not claim that an empty feed means no threat exists, and viewing it does not start a detector.

Understand The Screen

Mission / Run Scope (Signed-In User (Read-Only))

Mission selects a recorded mission; All missions keeps the broader tenant view. Run optionally narrows the record by run ID. Clear scope removes those filters. Confirm the matching mission and run in the header before comparing panels.

Telemetry (Signed-In User (Read-Only))

Read the inputs and their recorded source, time and state. These are the observations available to the selected runtime, not a list of every system in your organization.

Detection Activity Log Ingestion (Signed-In User (Read-Only))

This band shows the recorded ingestion and detection activity represented by the workflow. A configured connector is not evidence that data arrived; follow the rows and their source state.

Domain Intelligence (Signed-In User (Read-Only))

Domain context supplies the sector, asset or policy information associated with interpreting the observations. Read what is recorded, rather than treating a reference or applicability record as a new attack detection.

Step By Step

1. Choose The Relevant Scope (Signed-In User (Read-Only))

Open AS-OS Workflows > Detection. Choose a Mission or enter the relevant Run filter. Read the header's freshness and last-read time.

2. Inspect The Input (Signed-In User (Read-Only))

Start at Telemetry. Read the source, recorded time and observation state, then open the available row detail.

Detection - Continued

3. Follow Detection Activity (Signed-In User (Read-Only))

Compare the ingestion band with the input and the selected run. If a source is unavailable, retain that reason rather than replacing it with an empty-success interpretation.

4. Read The Domain Context (Signed-In User (Read-Only))

Review Domain Intelligence for context that applies to this observation. Continue to AS-OS Workflows > Investigation if a finding needs examination, or Decision to inspect the recorded response reasoning.

If Something Goes Wrong

A Known Run Is Missing

The current mission or run filter may exclude it, or the record is not in your organization.

Where To Go: AS-OS Workflows > Detection > Mission / Run Scope

Confirm the ID in Mission Workspace. Use Clear scope for broader review; never enter another tenant's record to gain access.

Source Unavailable

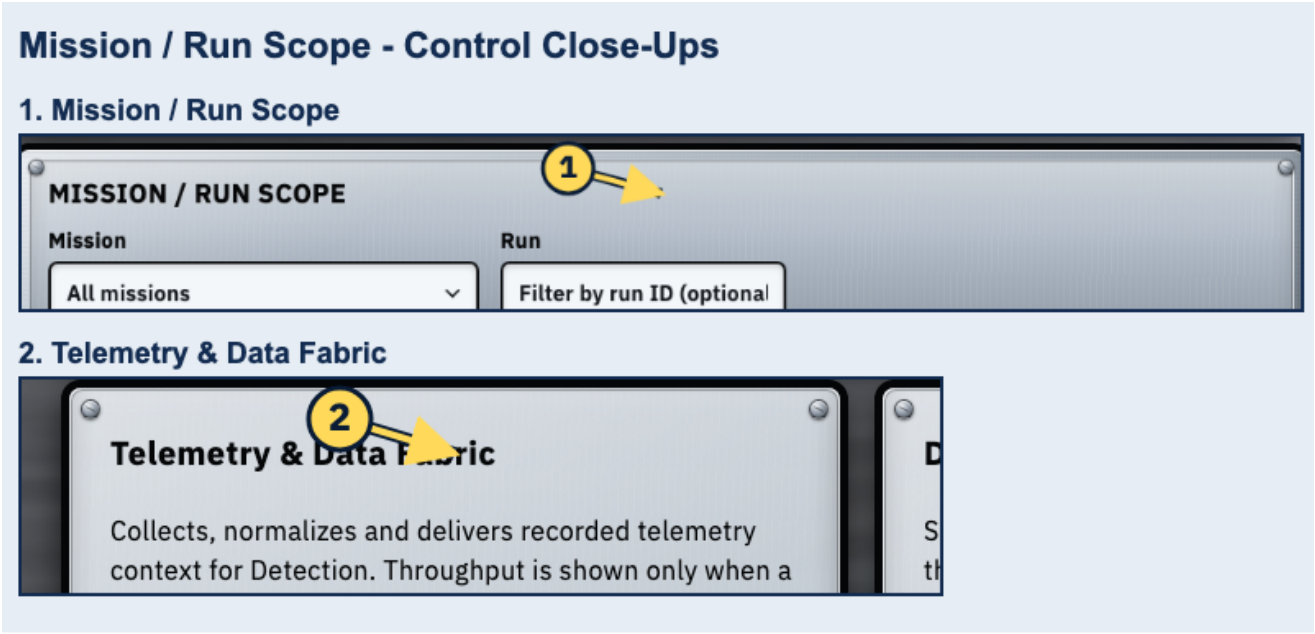
The workflow could not read the observation source.

Where To Go: Command Center > System Health; Organization & Onboarding > Deployment Configuration > Ingestion Setup

Check the source's health and configured ingestion path, then return to Detection and select Refresh.

Mission / Run Scope (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Mission / Run Scope

Select the recorded mission and run you want to inspect. Do not assume the latest tenant run belongs to another selected mission.

2. Telemetry & Data Fabric

Read source and freshness. Empty or unavailable is not successful ingestion.

What Happens

Selection filters the recorded view; it does not start detection.

5. Investigation (Analyst / Operator; Authorized Actions Only)

Investigation is the workflow for examining a suspected security event before deciding what it means. An incident is a persisted record of a security issue; an alert is an input that may need further examination. This screen lists those records and opens their investigation workspaces, where supporting context can be reviewed. The Selected run field also scopes the runtime review panels when a run is available. Investigation is a cross-layer capability, not a sixth AS-OS orchestration layer, and opening a case does not authorize containment.

Understand The Screen

Open Investigations (Analyst / Operator; Authorized Actions Only)

Each incident card shows its title, identity, time, severity and recorded status. Open workspace opens the incident’s detailed investigation. Read this run selects its linked run when one is present.

Alert Intake (Analyst / Operator; Authorized Actions Only)

Alerts are shown separately from the primary incident queue. Open in alerts is a contextual link to the alert inventory, not a replacement for the incident record. No incidents and no alerts are valid empty states, not a safety certificate.

Selected Run And Runtime Review (Analyst / Operator; Authorized Actions Only)

Use Investigation run ID only for a known run from this organization. The corresponding review panels show the available recorded context. An unselected run must not cause unrelated history to appear as this incident’s execution.

Step By Step

1. Choose An Incident (Analyst / Operator; Authorized Actions Only)

Open AS-OS Workflows > Investigation. Compare the incident title, time and severity, then select Open workspace for the record you intend to examine.

2. Build Your Understanding (Analyst / Operator; Authorized Actions Only)

In the detailed workspace read the recorded evidence, recommendations, risk and decision context that are actually available. Note unresolved gaps rather than assuming a diagnosis.

Investigation - Continued

3. Connect The Relevant Runtime (Analyst / Operator; Authorized Actions Only)

Use Read this run when offered, or enter a known run in Selected run. Confirm that the review panels belong to the same incident or runtime before interpreting an outcome.

4. Continue Through Governed Work (Analyst / Operator; Authorized Actions Only)

For approval or action, open Command Center > Mission Workspace and select the associated mission. For a persisted deliverable open Evidence & Reporting > Investigation Bundles. These are separate from investigation navigation.

If Something Goes Wrong

Incident Queue Is Empty

No incident records match the current tenant scope.

Where To Go: AS-OS Workflows > Detection

Check whether relevant input has been admitted and persisted. Do not create a case or synthetic event merely to fill the screen.

Incidents Authority Unavailable

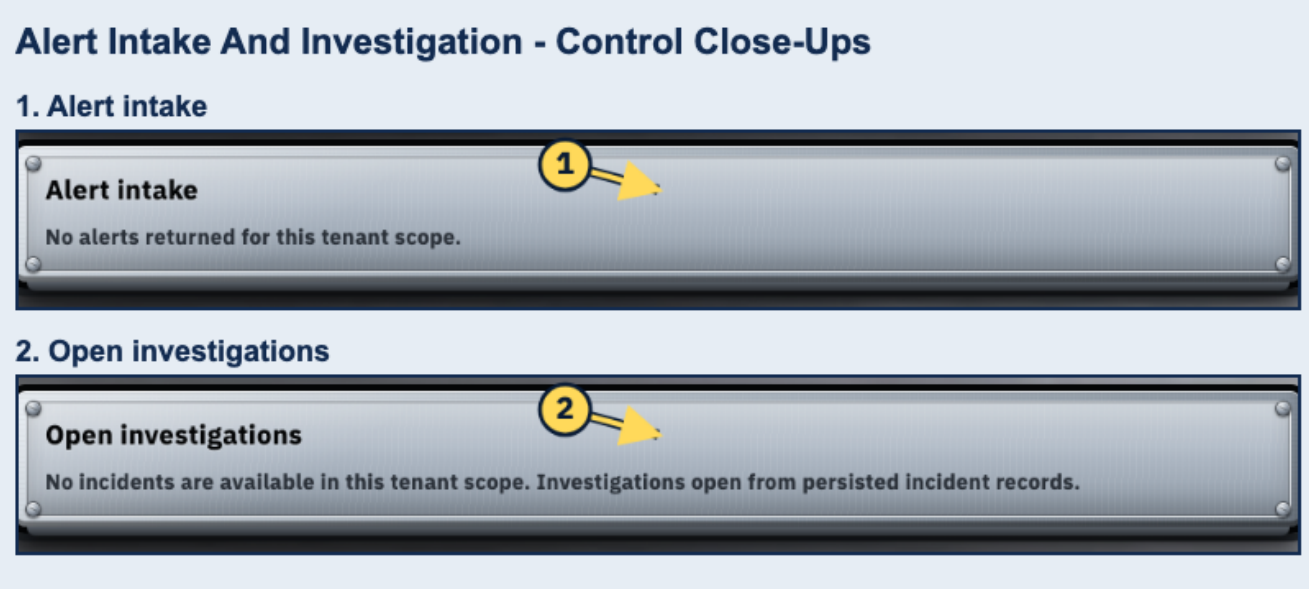
Your session cannot read the incident source.

Where To Go: Organization & Onboarding > Admin Settings > USERS

Ask the administrator to inspect your role and account state. Return to Investigation after normal access is restored.

Alert Intake And Investigation (Analyst / Operator; Authorized Actions Only)

Isolated Demonstration - Not Your Current Tenant State



1. Alert intake

Use an offered alert from this tenant; verify its identity and severity.

2. Open investigations

Select the intended record and read persisted context before following its workflow.

What Happens

An offered intake action can create or adopt an investigation; reviewing a recorded run is read-only.

6. Decision (Signed-In User (Read-Only))

Decision explains the response that AS-OS proposed for recorded security work. It separates the input context from risk and confidence assessments and from the gate or policy that governs the proposal. Confidence describes support for a decision; it is not an execution success percentage. You can select a mission or run, inspect the reason and supporting rows, and identify whether a human decision is still required. Use this page to understand a proposal before following it into the owning action or approval workflow.

Understand The Screen

Decision Context (Signed-In User (Read-Only))

Read the situation and inputs associated with the selected mission or run. Confirm their identity before interpreting a proposal.

Risk & Confidence Evaluation (Signed-In User (Read-Only))

Read the recorded risk, confidence and evidence limitations. Missing values must remain unavailable; a colored state does not justify inventing a score.

Gate / Policy Decisions (Signed-In User (Read-Only))

A gate is a condition that must permit an operation before it can proceed. Inspect the verdict and policy reason: allow, denial, human review or a restricted path are not interchangeable outcomes.

Step By Step

1. Select The Record (Signed-In User (Read-Only))

Open AS-OS Workflows > Decision. Choose Mission and, if needed, Run in Mission / Run Scope.

2. Read Context Before The Verdict (Signed-In User (Read-Only))

Inspect Decision Context and its supporting rows. Confirm the recorded time and freshness.

Decision - Continued

3. Assess The Proposal (Signed-In User (Read-Only))

Review Risk & Confidence Evaluation together with Gate / Policy Decisions. Identify what the proposal permits and what evidence or human decision remains missing.

4. Follow The Owning Workflow (Signed-In User (Read-Only))

For human review use Command Center > Mission Workspace > Operating Control. For execution results use AS-OS Workflows > Action. For a persisted decision deliverable use Evidence & Reporting > Decision Bundles.

If Something Goes Wrong

Human Review Required

The current gate does not permit autonomous execution.

Where To Go: Command Center > Mission Workspace > Operating Control

Have the authorized reviewer examine the same target, proposal and evidence. Refresh Decision after the supported approval path; do not change the verdict manually.

Decision Context Is Missing

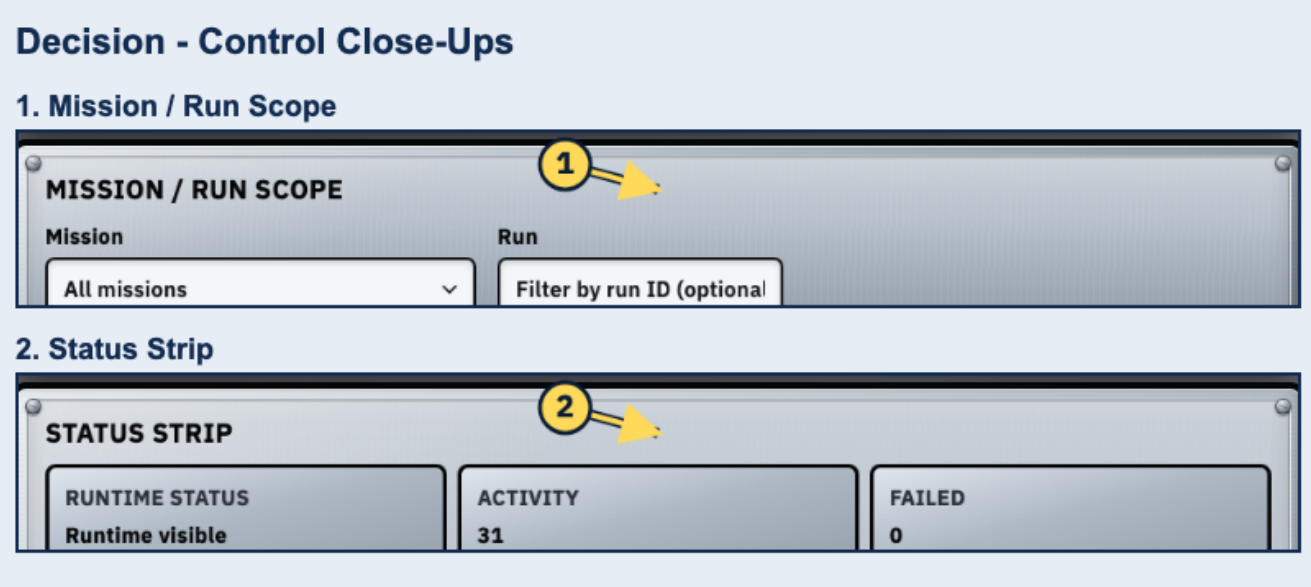
No corresponding recorded decision is available for this scope.

Where To Go: AS-OS Workflows > Decision > Mission / Run Scope

Confirm the selected record in Mission Workspace and remove an incorrect filter. Missing context is not an allow verdict.

Decision (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Mission / Run Scope

Choose the intended recorded mission/run.

2. Status Strip

Read the persisted result and its limitations. A missing result does not mean execution succeeded.

What Happens

These workflow projections inspect recorded work. Use Mission Workspace for authorized changes or approvals.

7. Action (Signed-In User (Read-Only))

Action shows the operational work proposed or attempted after a decision. A queued action is a request to do something; an execution is an attempt; a verified result is evidence that the expected effect was observed. This page keeps those stages separate so you can see where work stopped. Select a mission or run to inspect its action queue, execution orchestration and resulting evidence. Reading an action record does not retry it or grant permission to operate its target.

Understand The Screen

Action Queue (Signed-In User (Read-Only))

Read proposed or queued work and its current state. A queue item is not proof that an executor ran.

Execution Orchestration (Signed-In User (Read-Only))

Review how the recorded attempt progressed and which governing condition applied. Approval, execution and verification are distinct stages.

Action Results & Evidence (Signed-In User (Read-Only))

Read the recorded outcome and available evidence. A successful request or accepted approval is not automatically verified containment. Preserve failure and missing-postcondition information.

Step By Step

1. Set The Scope (Signed-In User (Read-Only))

Open AS-OS Workflows > Action and select the intended Mission or Run. Check header identity and freshness.

2. Follow A Queue Item (Signed-In User (Read-Only))

Read its requested operation and state in Action Queue. Inspect available detail rather than treating a count as completion.

Action - Continued

3. Compare Attempt And Result (Signed-In User (Read-Only))

Follow Execution Orchestration into Action Results & Evidence. Confirm the target, recorded time, receipt and observed outcome refer to the same attempt.

4. Resolve Or Review In Its Owner (Signed-In User (Read-Only))

If the attempt needs approval or retry, return to Mission Workspace and its Operating Control or Mission Controls. For a report of the recorded execution, use Evidence & Reporting > Action Execution Reports.

If Something Goes Wrong

Approved But Failed

Human authorization permitted an attempt, but execution did not reach the required outcome.

Where To Go: Command Center > Mission Workspace > Missions > Execution Path

Read the actual failure and related health or executor condition. Do not count authorization as successful action.

No Result Evidence

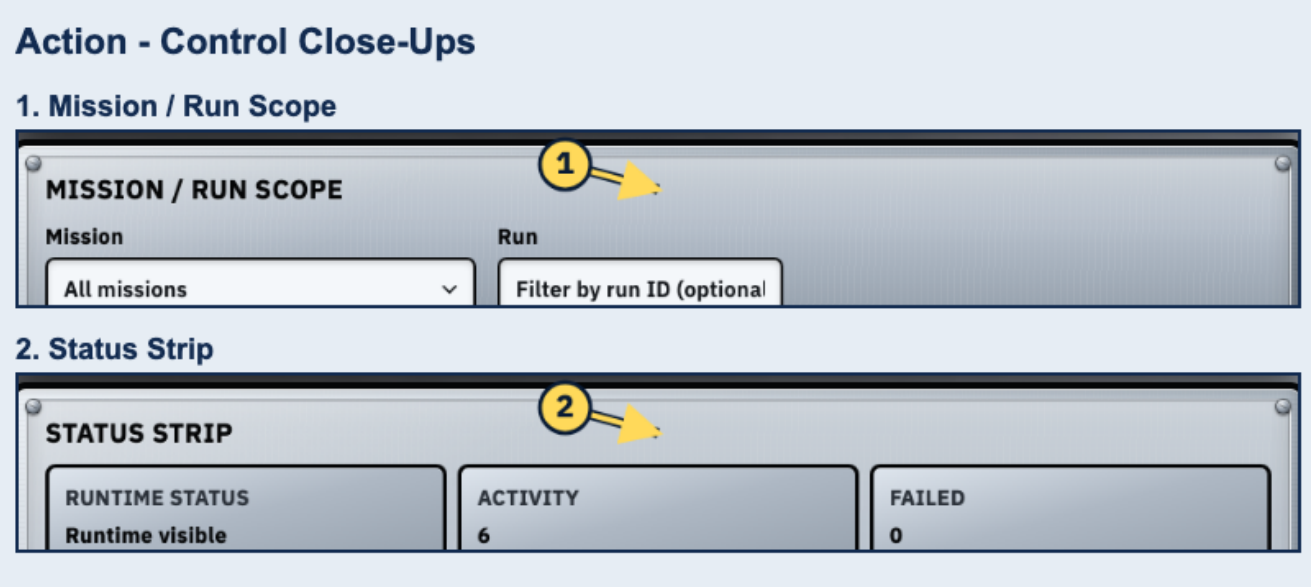
The required receipt or observed postcondition is absent.

Where To Go: Evidence & Reporting > Evidence Center

Inspect the matching evidence record and gaps. Return to the owning mission for unresolved verification; do not label it completed from the queue alone.

Action (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Mission / Run Scope

Choose the intended recorded mission/run.

2. Status Strip

Read the persisted result and its limitations. A missing result does not mean execution succeeded.

What Happens

These workflow projections inspect recorded work. Use Mission Workspace for authorized changes or approvals.

8. Governance (Signed-In User (Read-Only))

Governance explains the safeguards applied to recorded runtime work. A guardrail is a rule that limits what the system may do; an approval gate requires an authorized person or condition before an operation proceeds. This screen shows runtime guardrails, approval and gate controls, and source integrity for the selected scope. You can inspect why an operation was allowed, restricted or blocked, but the page does not replace the approval workflow. Governance is the customer menu label for the Control layer; it is not a new sixth layer.

Understand The Screen

Runtime Guardrails (Signed-In User (Read-Only))

Read restrictions and their source for the selected operation. Protected assets, allowed scope and mode constraints must be evaluated before action.

Approval & Gate Control (Signed-In User (Read-Only))

Read the current control outcome and its relationship to human review. A past human requirement and the current post-review gate may differ; human involvement must not be erased from the record.

Source / Integrity Control (Signed-In User (Read-Only))

Review whether the supporting source and evidence integrity are available. Available data, verified integrity and permitted execution are different claims.

Step By Step

1. Select The Governed Record (Signed-In User (Read-Only))

Open AS-OS Workflows > Governance. Choose the Mission or Run whose action you are reviewing.

2. Read The Applicable Restriction (Signed-In User (Read-Only))

Inspect Runtime Guardrails and identify the protected target, scope or policy condition that applies.

Governance - Continued

3. Review Approval And Integrity (Signed-In User (Read-Only))

Compare Approval & Gate Control with Source / Integrity Control. Read missing requirements and the recorded reason before interpreting an allow or denial.

4. Make Changes Only In Their Workflow (Signed-In User (Read-Only))

Use Command Center > Mission Workspace > Operating Control for authorized review or control changes. Use Evidence Audit Reports or Control Verdict Reports for persisted supporting records.

If Something Goes Wrong

Blocked By A Protected Target

A governing rule restricts this target or operation.

Where To Go: Command Center > Mission Workspace > Operating Control

Ask the authorized owner to review the restriction and requested scope. Do not remove protection simply to make a run continue.

Integrity Not Available

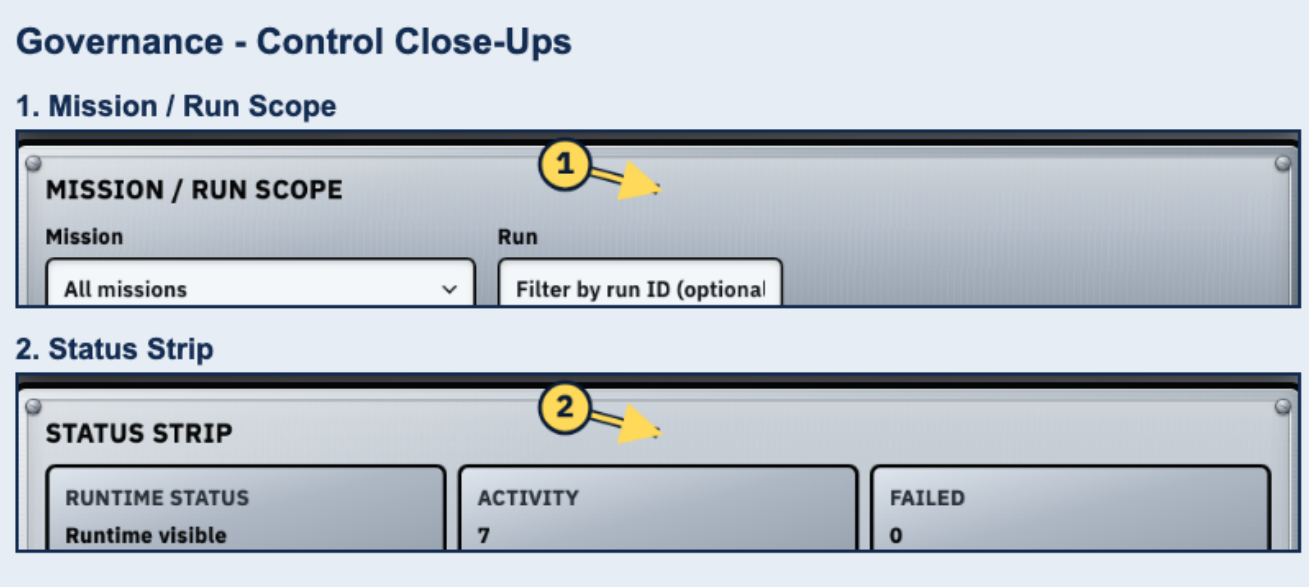
The required source or integrity evidence cannot be read.

Where To Go: Evidence & Reporting > Evidence Center

Review the matching record and Missing proof / gaps. Return to Governance only after the source condition has been resolved or explicitly retained as a limitation.

Governance (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Mission / Run Scope

Choose the intended recorded mission/run.

2. Status Strip

Read the persisted result and its limitations. A missing result does not mean execution succeeded.

What Happens

These workflow projections inspect recorded work. Use Mission Workspace for authorized changes or approvals.

9. Learning (Signed-In User (Read-Only))

Learning shows recorded feedback retained from security work. Feedback is information about what happened and how well a decision or action matched the observed result. This page separates captured feedback from patterns and from knowledge or playbook evolution. You can inspect what was recorded for the selected mission or run without assuming that every observation changed a production policy. An empty learning view means no matching feedback is available, not that the system has already learned everything.

Understand The Screen

Feedback Capture (Signed-In User (Read-Only))

Read outcome feedback linked to the recorded work. It is evidence for review, not automatic authorization to change policy.

Pattern Learning (Signed-In User (Read-Only))

Review the recorded patterns and their supporting scope. A suggested or observed pattern is different from a deployed policy change.

Knowledge / Playbook Evolution (Signed-In User (Read-Only))

Inspect the available knowledge or playbook records and their actual state. Do not infer promotion, verification or production activation from a visible entry.

Step By Step

1. Choose The Scope (Signed-In User (Read-Only))

Open AS-OS Workflows > Learning. Select the Mission and optional Run; check freshness and recorded identity.

2. Start With The Outcome (Signed-In User (Read-Only))

Read Feedback Capture and identify the underlying execution or decision outcome.

Learning - Continued

3. Follow Its Learning Records (Signed-In User (Read-Only))

Compare Pattern Learning with Knowledge / Playbook Evolution. Note whether the record is merely observed, proposed or actually persisted with a governed outcome.

4. Retain The Evidence (Signed-In User (Read-Only))

For the source result return to Action or Mission Workspace > Activity Timeline. For an auditable output follow the corresponding Evidence & Reporting workflow rather than claiming a policy update from this screen.

If Something Goes Wrong

No Feedback

The selected record has no matching captured feedback.

Where To Go: Command Center > Mission Workspace > Activity Timeline

Check whether the relevant attempt and outcome were recorded. Return to Learning after a genuine observation exists.

Unexpected Pattern

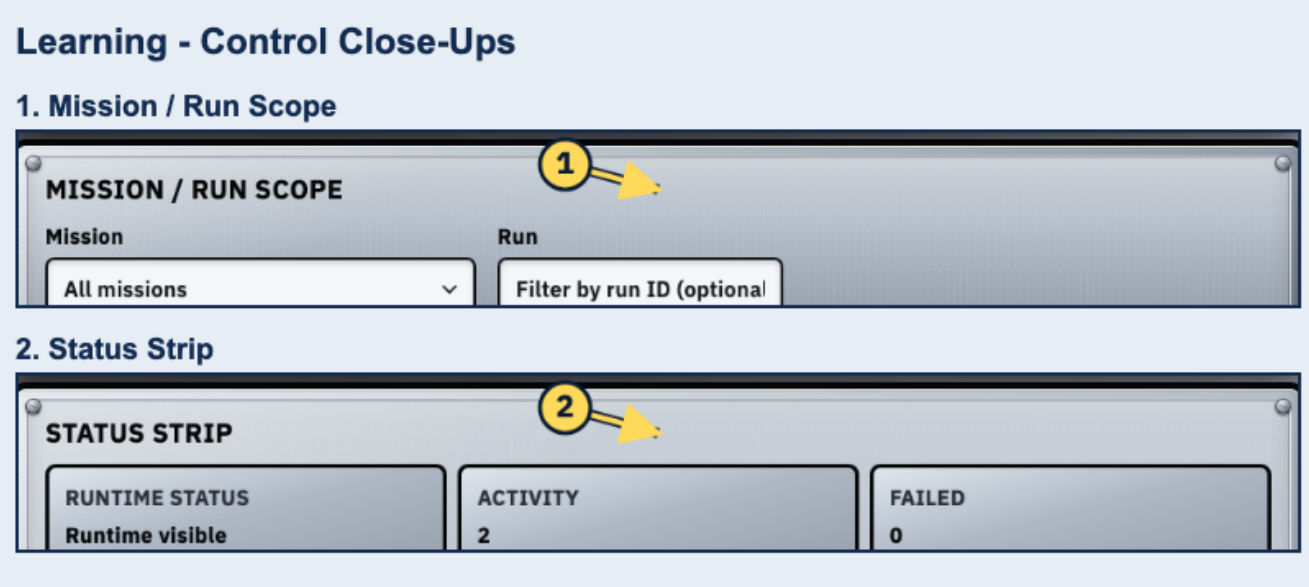
The view may include a broader mission or tenant scope than intended.

Where To Go: AS-OS Workflows > Learning > Mission / Run Scope

Confirm the selected Mission and Run. Compare the pattern with its own supporting record before drawing a conclusion.

Learning (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Mission / Run Scope

Choose the intended recorded mission/run.

2. Status Strip

Read the persisted result and its limitations. A missing result does not mean execution succeeded.

What Happens

These workflow projections inspect recorded work. Use Mission Workspace for authorized changes or approvals.

10. Analyst Reports (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Analyst Reports turns recorded security work into a deliverable that another person can review. A report brings together the available decisions, control results, executions and evidence for the displayed scope. Report Draft, Evidence Coverage and Customer-ready explain whether that material can support an output. Review Draft opens the current draft; Evidence Gaps identifies proof or delivery conditions that still need attention. Use this screen to review readiness before generating or sending a report: preparation and delivery do not prove that every security action succeeded.

Understand The Screen

Report Readiness And Review Draft (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Read the reported readiness and Customer-ready state before selecting Review Draft. A draft is a document under review, not a signed-off outcome. The Evidence review tab concerns the recorded source material; the report review area concerns its proposed output.

Evidence Gaps And Report Draft Readiness (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Read the tenant identity, evidence completeness and each gap. Missing source material, a blocked gate and unavailable delivery require different recovery. Sensitive raw evidence is not displayed here; a summary does not replace the original authorized record.

Report Center And Families (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Evidence Audit Reports, Control Verdict Reports and Action Execution Reports use this workspace with a report-family selection. They emphasize proof, control permission or execution attempts respectively; they are not separate identical report engines. Review the current family and the controls actually offered in Report Center.

Report Actions (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Generate PDF prepares the allowed output. Export Runtime Proof Dossier packages its proof. Send Email, Slack and Teams use separately configured outbound channels when permitted. Read each disabled reason, classification and recipient before acting; never route sensitive evidence through an unapproved channel.

Analyst Reports - Continued

Step By Step

1. Open The Required Family (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Open Evidence & Reporting > Analyst Reports, or the required report-family submenu. Confirm the displayed organization and source scope.

2. Review Readiness (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Read Report Draft, Evidence Coverage and Customer-ready. Select Review Draft to inspect the proposed document rather than assuming that a status tile is the document itself.

3. Resolve The Named Gap (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Read Evidence Gaps and Report Draft Readiness. For missing operational proof return to Mission Workspace > Evidence & Closure or Evidence Center; for channel readiness use the owning connector or SMTP configuration.

4. Use The Authorized Output (Analyst / SOC Operator / SOC Lead / CISO / Admin)

When its gate and your role permit, use Generate PDF or Export Runtime Proof Dossier, then inspect the produced artifact. Send Email, Slack or Teams only with an approved destination and ready channel. Check the resulting file or receipt; output generation is not a separately recorded approval.

Analyst Reports - Continued

If Something Goes Wrong

Report Is Not Customer-Ready

The current scope lacks required proof or readiness.

Where To Go: Evidence & Reporting > Analyst Reports > Evidence Gaps

Read the specific missing condition and return to its owning mission, evidence screen or channel configuration. Do not invent evidence to enable an output.

Reporting Access Denied

Your role or entitlement does not permit this report workflow.

Where To Go: Organization & Onboarding > Admin Settings > USERS; Subscription & Entitlements

Ask the authorized administrator to check your role and installed capability. A viewer must not bypass the reporting route.

Delivery Unavailable

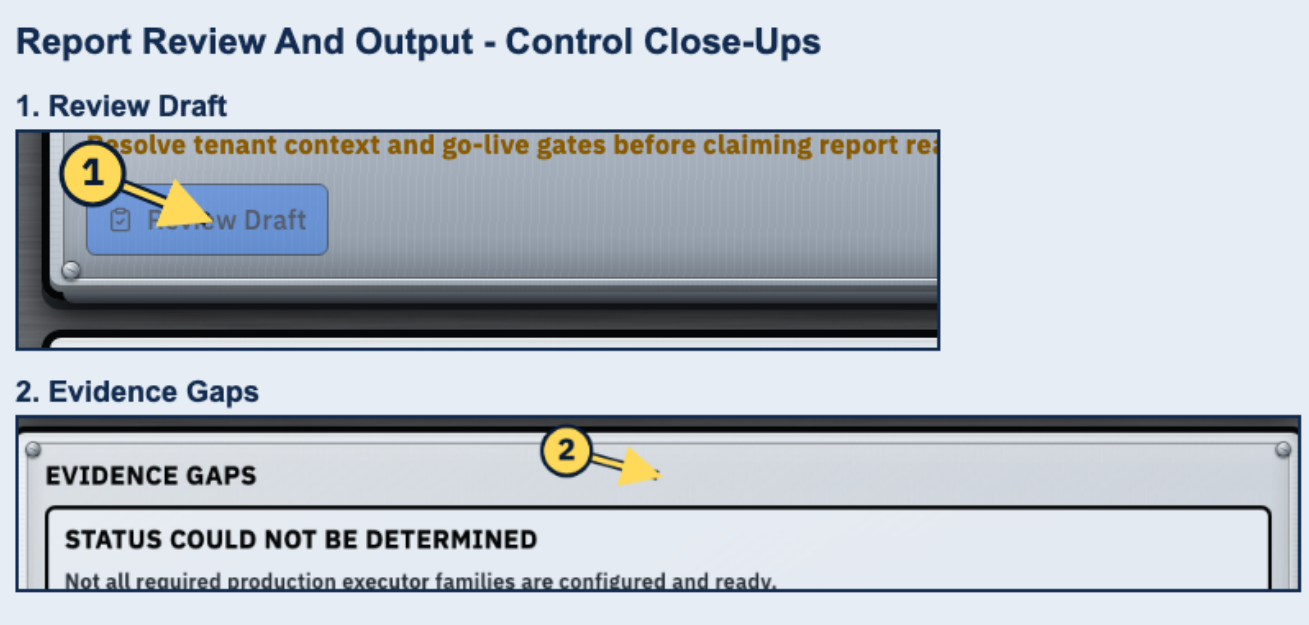
The configured delivery channel is not ready or the output is gated.

Where To Go: Organization & Onboarding > Admin Settings > CONNECTORS

Have the authorized operator inspect the configured channel. Use only a permitted local download when offered; do not upload incident evidence to an external service.

Report Review And Output (Analyst / SOC Operator / SOC Lead / CISO / Admin)

Isolated Demonstration - Not Your Current Tenant State



1. Review Draft

Opens the current draft for inspection, not approval.

2. Evidence Gaps

Read why evidence or delivery is incomplete. Return to the source workflow; never treat a blocked report as complete.

What Happens

PDF generation, dossier export and external delivery remain separate gated actions. A disabled action requires its stated prerequisite, not another role guessed by the guide.

11. Evidence Center (Signed-In User (Read-Only))

Evidence Center is the inventory of records used to support security decisions and reports. Evidence can describe an observation, a decision, an execution or another recorded source; it is not the same as an assertion that an action succeeded. The page lets you filter the inventory, inspect a selected record and see missing proof. Integrity describes whether the necessary integrity information is present, while freshness describes whether the source is recent enough for its policy. Use this screen to understand what can actually support a report and what still needs attention.

Understand The Screen

Scope And Inventory (Signed-In User (Read-Only))

Use the displayed scope and filters to narrow records by their source, state or related mission/run. Select an inventory row to open Evidence detail. The record’s title, time and reference identify what you are reviewing.

Missing Proof / Gaps (Signed-In User (Read-Only))

This panel lists evidence conditions that have not been satisfied. A missing-integrity record, unavailable source and absent record require different recovery. Do not hide gaps by assuming every visible record is verified.

Evidence Detail (Signed-In User (Read-Only))

Read source, identity, timestamps, integrity and freshness information for the selected record. Copying a reference helps another authorized reviewer locate it; it does not export the source data or grant access.

Step By Step

1. Set The Evidence Scope (Signed-In User (Read-Only))

Open Evidence & Reporting > Evidence Center. Confirm the organization and filter for the intended mission, run or evidence type.

2. Inspect One Record (Signed-In User (Read-Only))

Select a row in Evidence inventory. Read Evidence detail and compare its identity and time with the security work you intend to report.

Evidence Center - Continued

3. Check Gaps And Integrity (Signed-In User (Read-Only))

Review Missing proof / gaps and distinguish unavailable data from absent proof. Keep any unresolved condition with the record.

4. Continue To A Report (Signed-In User (Read-Only))

For a prepared document use Report Builder. For the underlying operation return to Mission Workspace or the relevant AS-OS Workflow. Evidence Center does not execute actions.

If Something Goes Wrong

Inventory Is Empty

No evidence matches this organization and filter.

Where To Go: Evidence & Reporting > Evidence Center > Scope / Filters

Clear an incorrect filter, then verify the source mission in Mission Workspace. Do not interpret an empty list as successful verification.

Integrity Missing

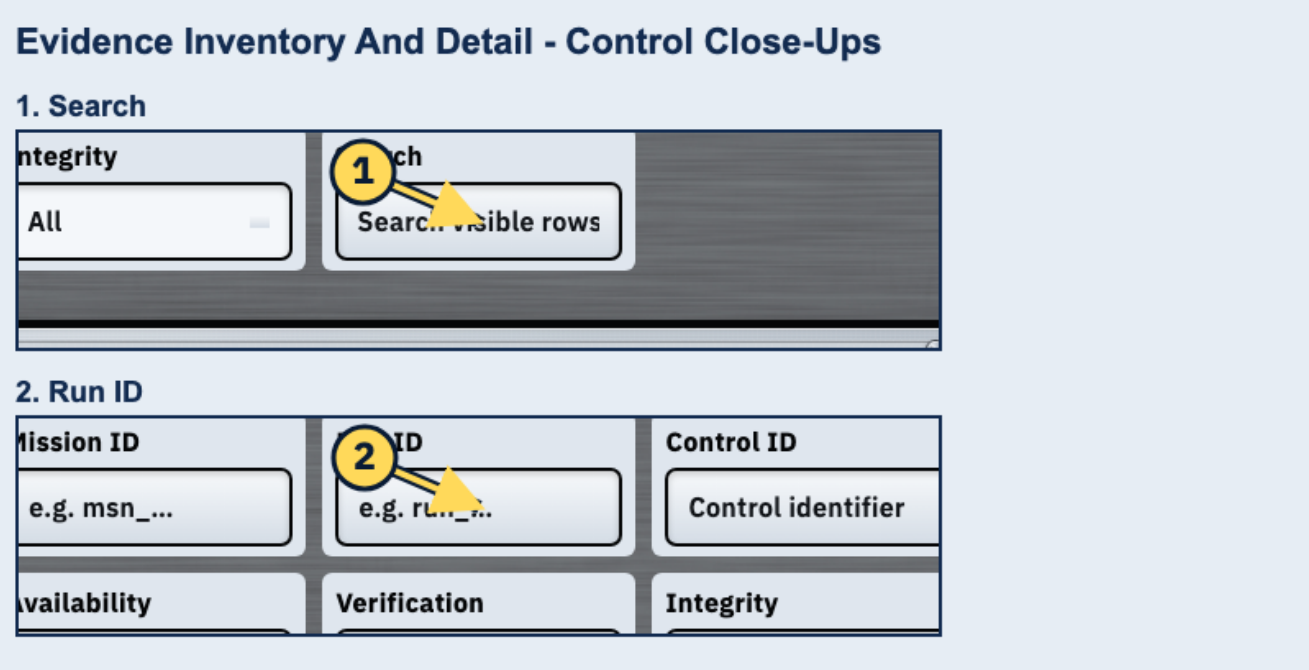
The required integrity reference is absent for that record.

Where To Go: Command Center > Mission Workspace > Missions > Evidence & Closure

Ask the responsible operator to inspect the original evidence and its capture path. Keep the gap visible until the source supplies the required proof.

Evidence Inventory And Detail (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Search

Select your intended tenant-scoped record and narrow the list with offered filters.

2. Run ID

Copy the genuine recorded identifier from your authorized mission/run or report. Paste it unchanged to narrow this view; filtering creates no new evidence.

What Happens

Inspecting records or filtering does not execute security work.

12. Report Builder (Analyst / Operator; Authorized Actions Only)

Report Builder assembles an evidence-based document for a defined purpose and audience. You choose its type, title, framework, classification and scope, then review the included evidence and findings. A framework defines the reporting criteria; choosing one does not certify legal compliance. The Section Manifest previews what the document will contain, while Export readiness identifies conditions that prevent a complete output. Use this workflow to prepare and inspect a report; a separately authorized approver remains responsible for sign-off.

Understand The Screen

Report Configuration (Analyst / Operator; Authorized Actions Only)

Report type chooses the document purpose. Title is the human-readable name. Framework chooses applicable reporting criteria; Classification controls the sensitivity label. Scope and criteria states the boundary being described. Prepared by comes from your signed-in identity and cannot be typed as another person. Approved by stays pending until the separate approval record exists.

Section Manifest (Analyst / Operator; Authorized Actions Only)

The manifest lists the document sections and their available source content. Review the scope, evidence, findings, integrity legend and limitations before generating. A section title does not prove its source is complete.

Included Evidence And Findings (Analyst / Operator; Authorized Actions Only)

Inspect the actual selected items and their detail. Check dates, references and unresolved conditions. Findings describe recorded issues; evidence supports claims about those issues.

Export Readiness (Analyst / Operator; Authorized Actions Only)

Read every missing requirement. Allow incomplete export permits only a watermarked draft, not a customer-ready document or an approval shortcut. The Generate control remains governed by the reported requirements and your permissions.

Report Builder - Continued

Step By Step

1. Choose The Reporting Purpose (Analyst / Operator; Authorized Actions Only)

Open Evidence & Reporting > Report Builder. Select Report type, give a clear Title and choose Framework and Classification according to the intended audience.

2. Describe The Scope (Analyst / Operator; Authorized Actions Only)

Complete the scope and criteria and the available period or mission/run selections. Verify that Prepared by is your current signed-in identity.

3. Review The Included Material (Analyst / Operator; Authorized Actions Only)

Read Section Manifest, Included evidence and Included findings. Inspect item detail and resolve mistaken selections before output.

4. Resolve Missing Requirements (Analyst / Operator; Authorized Actions Only)

Read Export readiness. Return to Evidence Center for proof gaps or Findings & Exceptions for unresolved issues. If an incomplete draft is legitimately required, use the explicitly labeled watermarked option and keep its limitations.

5. Generate And Review The Result (Analyst / Operator; Authorized Actions Only)

Use the available Generate control when permitted. Inspect the produced document and Export History. Do not treat preparation as approval or send a watermarked draft as a finalized customer report.

Report Builder - Continued

If Something Goes Wrong

Generate Is Disabled

Required scope or proof is missing, or permission is insufficient.

Where To Go: Evidence & Reporting > Report Builder > Export readiness

Read the named missing condition. Correct configuration here, evidence in Evidence Center, or findings in Findings & Exceptions before trying again.

Sign-Off Is Pending

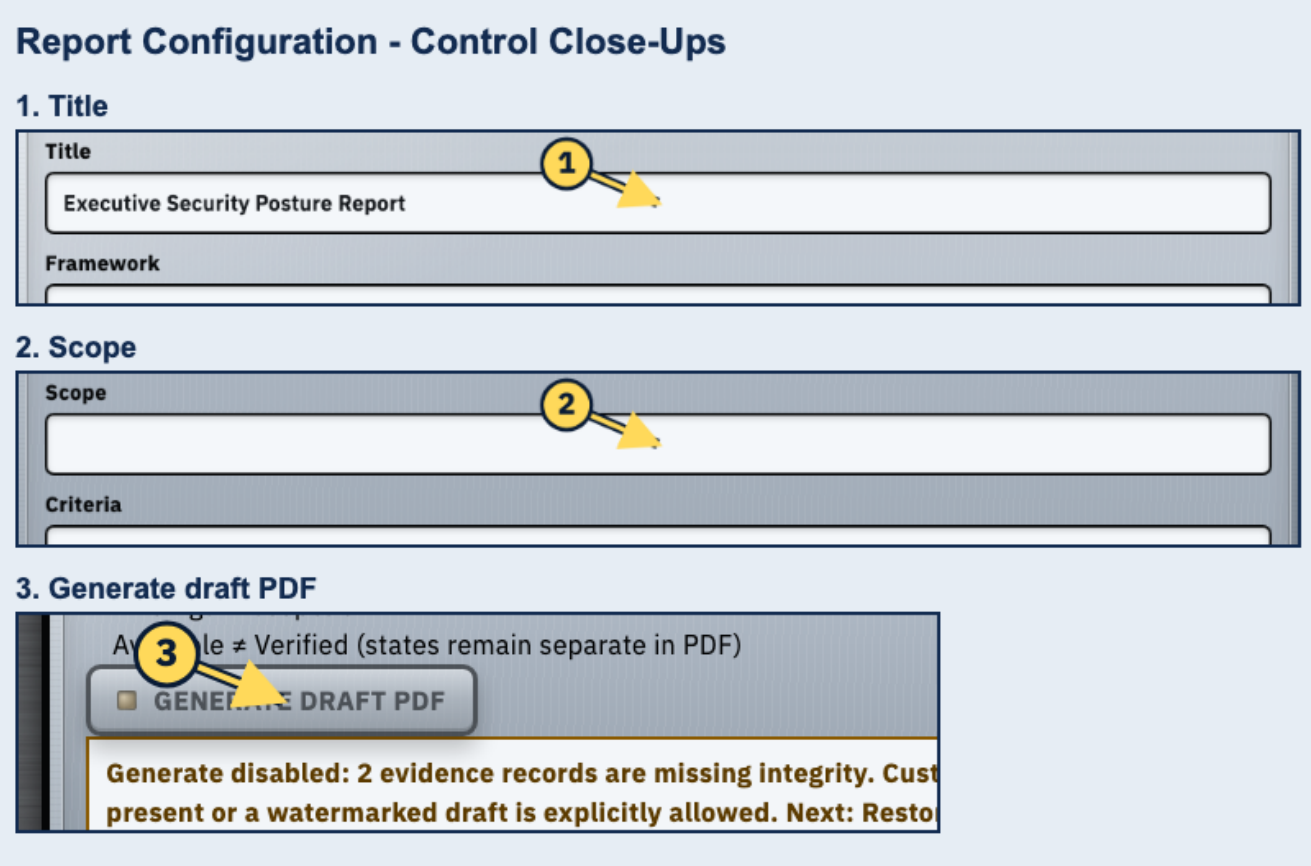
Preparation and approval are separate authorities.

Where To Go: Evidence & Reporting > Report Builder; your organization’s authorized approval procedure

Have the designated approver review the exact digest and version using the supported procedure. Do not enter an invented Approved by identity.

Report Configuration (Analyst / Operator; Authorized Actions Only)

Isolated Demonstration - Not Your Current Tenant State



1. Title

Give the report a clear name.
Illustrative Format Only: Review Of The Selected Mission (illustrative)

2. Scope

Describe the approved scope; choose framework and classification for the audience.

3. Generate draft PDF

Read export readiness first. Incomplete output is a watermarked draft, not an approved report.

What Happens

Generate prepares an output under the existing readiness checks; it does not approve it.

13. Audit Packs (Analyst / Operator; Authorized Actions Only)

Audit Packs groups evidence and findings into a named collection for a review or audit. A pack has a purpose, framework and reporting period so a reviewer understands what the collection covers. Its completeness panel shows the material present and any remaining gaps. You can inspect existing packs and use the offered preparation form when your role permits it. Creating a pack organizes records; it does not make missing proof appear or certify the organization as compliant.

Understand The Screen

Preparation Form (Analyst / Operator; Authorized Actions Only)

Pack name identifies the collection; Purpose explains why it is being prepared; Framework sets the review context; Period start and end define its window. The selected mission/run and included items must refer to the intended organization.

Audit Packs Inventory (Analyst / Operator; Authorized Actions Only)

Select a persisted pack to inspect its recorded contents. Keep the pack identity and period with any downstream review.

Pack Completeness / Gaps (Analyst / Operator; Authorized Actions Only)

Read which required records exist and which remain missing. Completeness of a collection and verified operational success are different conclusions.

Step By Step

1. Inspect Existing Packs (Analyst / Operator; Authorized Actions Only)

Open Evidence & Reporting > Audit Packs and select the intended pack, if one already exists.

2. Define A New Pack When Authorized (Analyst / Operator; Authorized Actions Only)

Enter its name, purpose, framework and period in the offered preparation form. Review the intended mission/run and evidence scope before using the create control.

Audit Packs - Continued

3. Review Its Contents (Analyst / Operator; Authorized Actions Only)

Inspect the resulting pack and Pack completeness / gaps. Compare included evidence and findings with the declared purpose.

4. Retain Its Limits (Analyst / Operator; Authorized Actions Only)

Resolve missing records through Evidence Center or the owning mission. Store the approved output inside the organization's permitted evidence boundary.

If Something Goes Wrong

Pack Is Incomplete

The collection lacks required evidence or contains unresolved gaps.

Where To Go: Evidence & Reporting > Evidence Center; Findings & Exceptions

Review the named records and their sources. Do not remove an inconvenient requirement to obtain a complete label.

Wrong Reporting Period

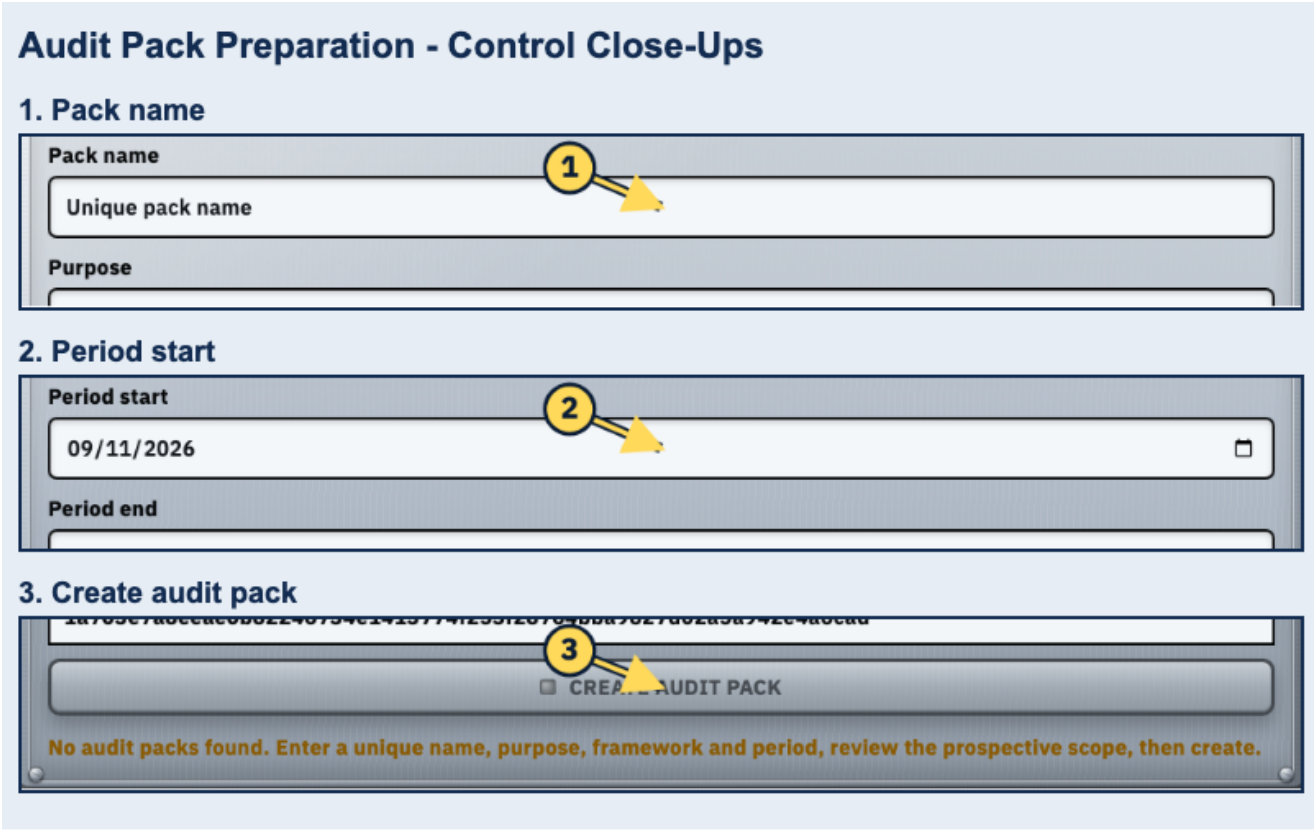
The pack scope does not match the intended review.

Where To Go: Evidence & Reporting > Audit Packs > Preparation Form

Review the period before creating another collection and retain the original history according to your policy.

Audit Pack Preparation (Analyst / Operator; Authorized Actions Only)

Isolated Demonstration - Not Your Current Tenant State



1. Pack name

Name the collection and explain its review purpose.

2. Period start

Use the intended period and check that end follows start.
Illustrative Format Only: YYYY-MM-DD

3. Create audit pack

Review included records and gaps after authorized creation.

What Happens

Create persists a collection; completeness and verified success are separate.

14. Findings & Exceptions (Analyst / Operator; Authorized Actions Only)

Findings & Exceptions records issues that a reviewer needs to understand or resolve. A finding identifies a documented condition; an exception records a condition that has not been resolved or is being handled under explicit authority. This page shows responsibility, severity, status and links to supporting evidence or reports. You can inspect priority items and use permitted editing controls for a selected record. Changing a finding's text or status must not be confused with repairing the underlying security condition.

Understand The Screen

Findings And Exceptions Inventory (Analyst / Operator; Authorized Actions Only)

Select a row to read the issue, recorded owner and current state. Severity describes importance; status describes its handling stage.

Overdue / High Severity (Analyst / Operator; Authorized Actions Only)

Use this panel to prioritize issues with time or severity concerns. A priority label does not grant permission to bypass the owning workflow.

Linked Evidence / Report References (Analyst / Operator; Authorized Actions Only)

Follow references to understand the source of the finding. Review the actual evidence before changing its handling state or preparing a report.

Step By Step

1. Choose A Finding (Analyst / Operator; Authorized Actions Only)

Open Evidence & Reporting > Findings & Exceptions and select the issue you are reviewing.

2. Read Its Responsibility And Proof (Analyst / Operator; Authorized Actions Only)

Check owner, severity, status and linked evidence. Confirm that the reference supports the stated issue.

Findings & Exceptions - Continued

3. Apply Only A Permitted Update (Analyst / Operator; Authorized Actions Only)

Use the selected finding's offered controls when your role allows them. Record the appropriate handling information; do not declare a technical fix merely by editing a status.

4. Verify The Underlying Resolution (Analyst / Operator; Authorized Actions Only)

Return to the owning mission or source workflow for the actual repair evidence. Then review the updated finding and any report that cites it.

If Something Goes Wrong

Finding Has No Supporting Evidence

The issue may be recorded, but the required proof is missing.

Where To Go: Evidence & Reporting > Evidence Center

Inspect the linked source and missing proof. Retain the limitation rather than inventing a supporting result.

Overdue Item

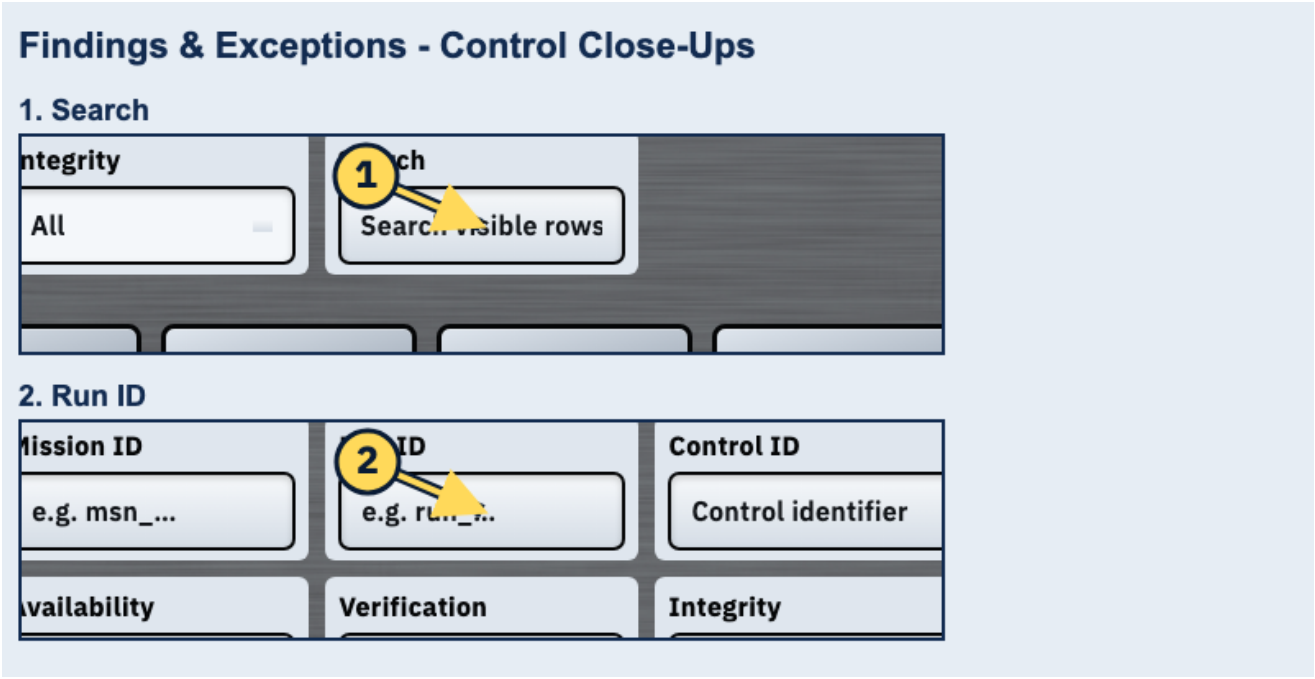
The recorded owner has not completed the required handling within its stated period.

Where To Go: Evidence & Reporting > Findings & Exceptions > Selected Finding

Review responsibility and the recorded deadline with the authorized owner. Escalate internally; changing severity is not resolution.

Findings & Exceptions (Analyst / Operator; Authorized Actions Only)

Isolated Demonstration - Not Your Current Tenant State



1. Search

Select your intended tenant-scoped record and narrow the list with offered filters.

2. Run ID

Copy the genuine recorded identifier from your authorized mission/run or report. Paste it unchanged to narrow this view; filtering creates no new evidence.

What Happens

Inspecting records or filtering does not execute security work.

15. Export History (Signed-In User (Read-Only))

Export History is the record of report outputs that were requested or generated. It helps you identify which report version produced a file, who requested it and whether generation succeeded. A digest is a fingerprint used to identify the artifact; it is not a claim that its contents are correct. You can filter the history, inspect a selected export and review failed outputs. Use this record to trace an output rather than assuming that pressing Generate created a usable file.

Understand The Screen

Filters (Signed-In User (Read-Only))

Export ID and Report ID locate known records. Artifact digest locates a file fingerprint or snapshot. Family / format narrows the output type; Status separates generated, pending and failed outputs; Requester identifies the actor; Period narrows recorded time.

Export History And Failed Exports (Signed-In User (Read-Only))

Select an output record to inspect it. Failed exports remain failures; a historical successful file does not repair a later failed attempt.

Selected Export Metadata (Signed-In User (Read-Only))

Read the output identity, source report, recorded status and integrity references. Keep the version and classification with any approved transfer.

Step By Step

1. Locate The Output (Signed-In User (Read-Only))

Open Evidence & Reporting > Export History. Use the known Export ID, Report ID or artifact digest, or the available status and period filters.

2. Inspect Metadata (Signed-In User (Read-Only))

Select the matching record. Compare its source report, version, requester, classification and generation state with the file you intend to use.

Export History - Continued

3. Handle A Failed Attempt (Signed-In User (Read-Only))

Read Failed exports and retain the reason. Return to Report Builder to correct a missing source or configuration rather than using a different old file as if it were the same output.

4. Retain And Transfer Safely (Signed-In User (Read-Only))

Keep the original output and its references in approved local storage. Follow controlled-media and recipient procedures for any transfer.

If Something Goes Wrong

No Matching Export

The filters exclude the record or no output was persisted.

Where To Go: Evidence & Reporting > Export History > Filters

Clear an incorrect ID or period, then inspect Report Builder’s generation result. Do not infer a file exists from a button click.

Failed Export

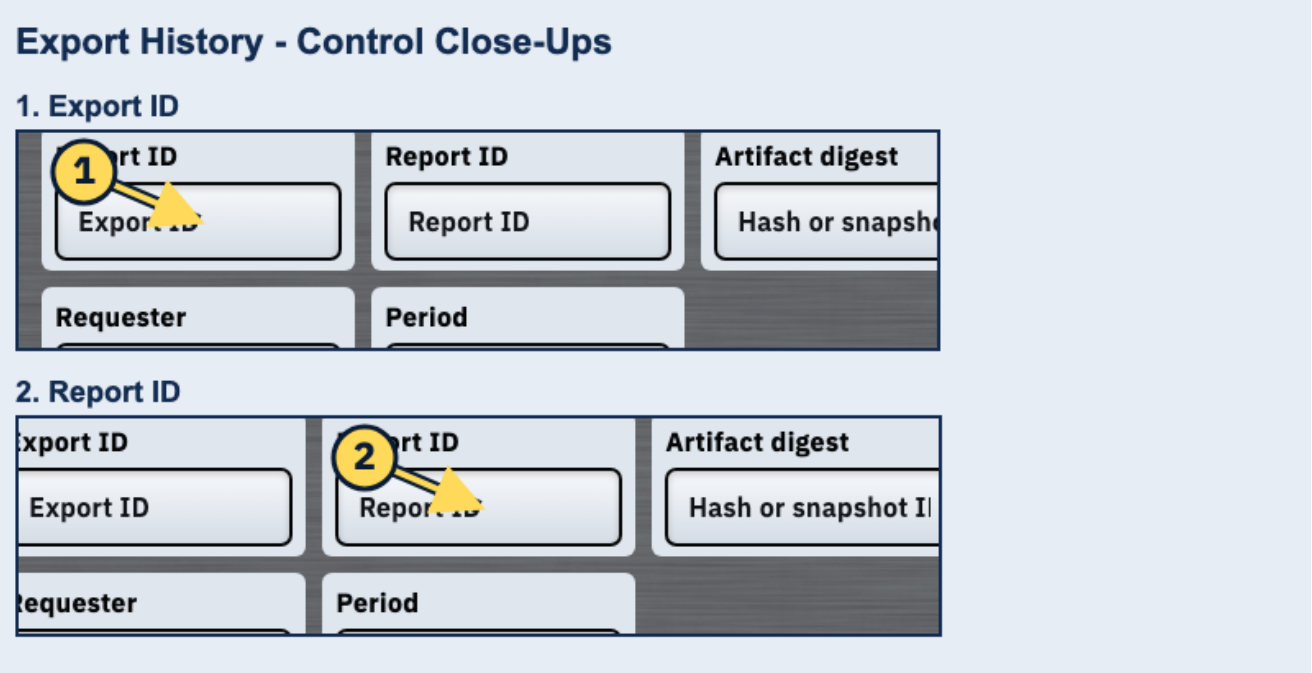
Generation did not produce the required output.

Where To Go: Evidence & Reporting > Report Builder > Export readiness

Resolve the recorded condition and use the supported generation path. Preserve the failed history and distinguish the new attempt.

Export History (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Export ID

Select your intended tenant-scoped record and narrow the list with offered filters.

2. Report ID

Copy the genuine recorded identifier from your authorized mission/run or report. Paste it unchanged to narrow this view; filtering creates no new evidence.

What Happens

Inspecting records or filtering does not execute security work.

16. Decision Bundles (Signed-In User (Read-Only))

Decision Bundles are persisted collections that explain a recorded security decision. They gather the decision context and supporting evidence into a deliverable that a reviewer can inspect. The inventory is not a live alert feed and does not create a new decision when you open it. You can filter bundles, select one and inspect its evidence, classification and review state. Use a bundle to understand what was recorded and what remains unverified before relying on the decision.

Understand The Screen

Bundle Filters (Signed-In User (Read-Only))

Search can locate a title, run, campaign or hash. Threat classification describes the assessed threat; Data classification describes sensitivity. Severity, review state, time and sort controls narrow the inventory, not the underlying evidence.

Bundle Inventory (Signed-In User (Read-Only))

Select a persisted bundle and confirm its run, title and creation time. Empty inventory means no matching deliverable is persisted; it is not a detection-quality result.

Bundle Detail (Signed-In User (Read-Only))

Read the sections and any available evidence graph reference. A ready record, complete source information and a verified outcome are distinct facts. Use only the offered authorized download controls.

Step By Step

1. Find The Decision (Signed-In User (Read-Only))

Open Evidence & Reporting > Decision Bundles. Filter or search for the known decision run or title.

2. Select Its Bundle (Signed-In User (Read-Only))

Choose the inventory row and confirm its scope, sensitivity and recorded review state.

Decision Bundles - Continued

3. Review The Supporting Sections (Signed-In User (Read-Only))

Read the decision context and supporting evidence. Follow an available source link to compare it with Decision or the owning mission.

4. Use The Deliverable Within Its Scope (Signed-In User (Read-Only))

Retain unresolved gaps with any approved download. Keep the original bundle identity when referring to it in an internal review.

If Something Goes Wrong

Bundle Not Entitled

The required operational reporting capability is not available for this tenant.

Where To Go: Organization & Onboarding > Subscription & Entitlements; Ecosystem workspace

Have the authorized administrator inspect the installed capability and binding. Do not bypass the bundle route.

No Bundle For A Known Run

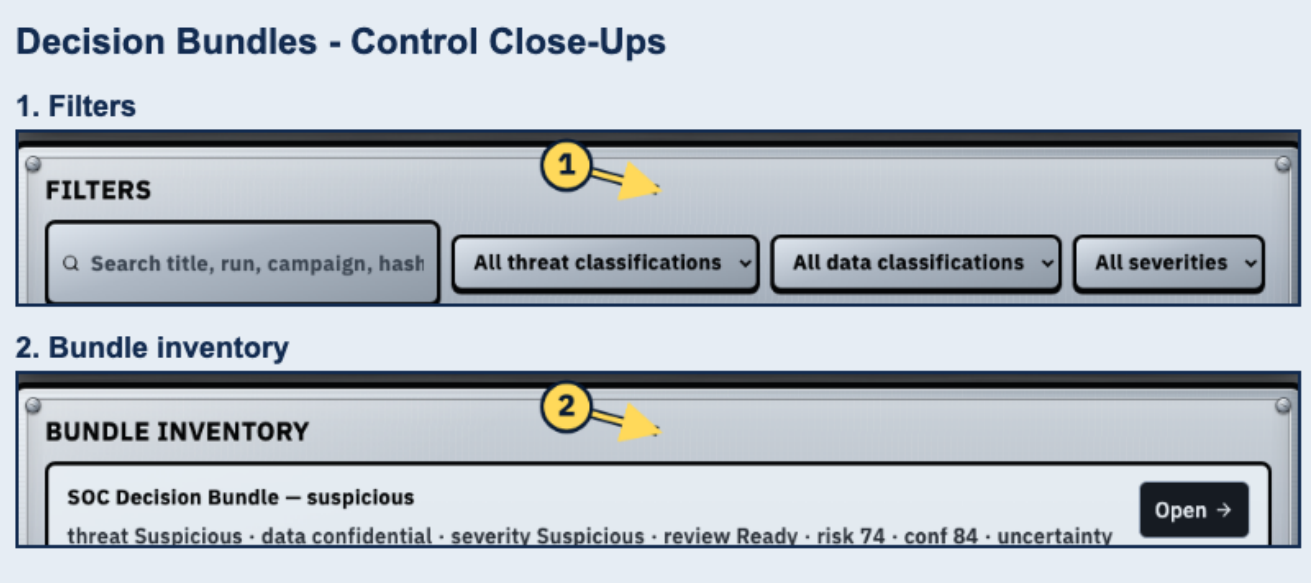
The deliverable may not have materialized or the filter may be incorrect.

Where To Go: Evidence & Reporting > Analyst Reports; Command Center > Mission Workspace

Check the report lifecycle and source run. A visible runtime does not prove that a bundle was persisted.

Decision Bundles (Reporting Roles)

Isolated Demonstration - Not Your Current Tenant State



1. Filters

Use the known run or bundle reference from the owning mission.

2. Bundle inventory

Open the persisted bundle and compare source, completeness and recorded time.

What Happens

Viewing a bundle does not create evidence or approve work.

17. Investigation Bundles (Signed-In User (Read-Only))

Investigation Bundles collect the recorded findings and evidence of an investigation into a reviewable deliverable. An investigation examines an issue; its bundle documents the recorded result and supporting material. The inventory can be searched by identity, threat context and review state. Detail includes the available investigation sections and completeness information rather than a promise that every question was resolved. Use this workspace to review or retain an investigation output, not to execute containment.

Understand The Screen

Investigation Filters (Signed-In User (Read-Only))

Use the available root-cause, MITRE, asset, identity, finding, owner and verification filters along with search, time and classification. MITRE identifies referenced attack techniques; root-cause status describes whether the source actually established a cause.

Inventory And Completeness (Signed-In User (Read-Only))

Select a persisted investigation bundle and read its recorded completeness conditions. Missing investigation material stays missing even when the bundle itself is visible.

Investigation Detail (Signed-In User (Read-Only))

Read hypotheses, findings, supporting evidence and any available source reference. A proposed explanation is not automatically a confirmed root cause or verified remediation.

Step By Step

1. Locate The Investigation Output (Signed-In User (Read-Only))

Open Evidence & Reporting > Investigation Bundles. Search the known run or title and narrow with the relevant available filters.

2. Confirm Scope And Classification (Signed-In User (Read-Only))

Select the bundle and read its organization, source identity, time and data sensitivity.

Investigation Bundles - Continued

3. Review Completeness And Findings (Signed-In User (Read-Only))

Examine the recorded investigation sections and unresolved gaps. Compare the supporting record with AS-OS Workflows > Investigation.

4. Retain The Recorded Conclusion (Signed-In User (Read-Only))

Use permitted download controls and retain limitations with the output. Hand off any required action to the associated mission's governed workflow.

If Something Goes Wrong

Root Cause Not Established

The investigation record does not yet support a confirmed cause.

Where To Go: AS-OS Workflows > Investigation > Open workspace

Review the hypotheses and evidence for the same incident. Do not promote an incomplete explanation into a confirmed cause in the report.

Required Section Missing

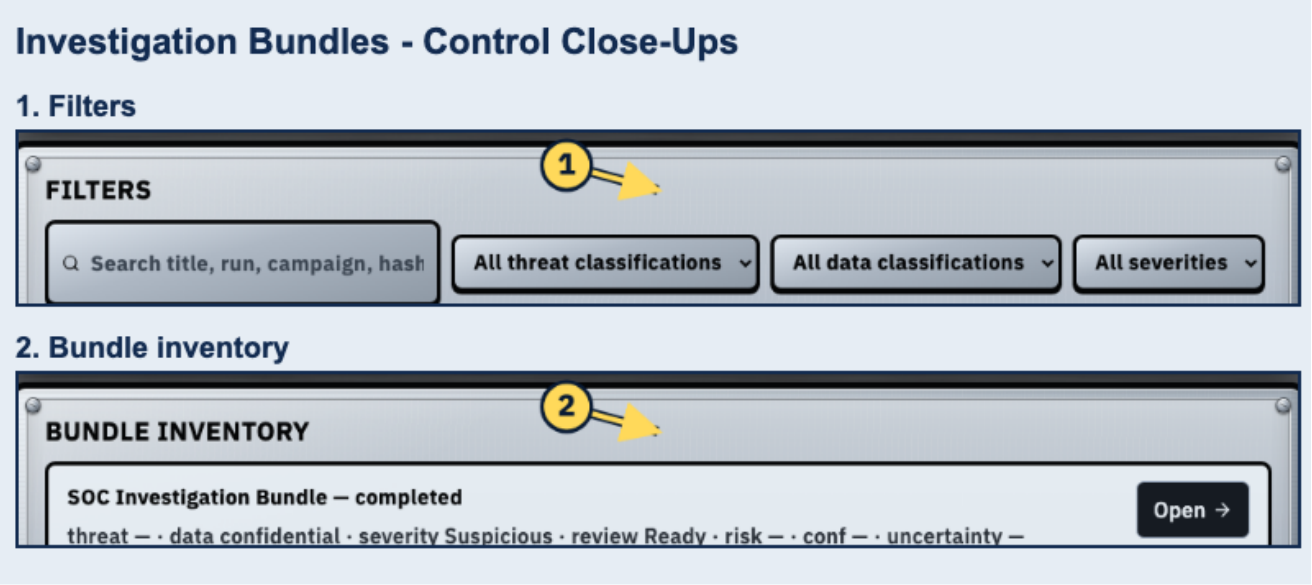
The investigation deliverable lacks material required by its completeness contract.

Where To Go: Evidence & Reporting > Evidence Center

Inspect the missing source and return to the investigation owner for its legitimate capture or documented limitation.

Investigation Bundles (Reporting Roles)

Isolated Demonstration - Not Your Current Tenant State



1. Filters

Use the known run or bundle reference from the owning mission.

2. Bundle inventory

Open the persisted bundle and compare source, completeness and recorded time.

What Happens

Viewing a bundle does not create evidence or approve work.

18. Onboarding Progress (Signed-In User (Read-Only))

Onboarding Progress is the checklist for preparing this organization to use CLAWOLF safely. It shows which setup responsibilities are complete, partial, blocked or not started, based on recorded backend facts. The order begins with customer identity and entitlement, then deployment, governance, ingestion and action readiness. Each step identifies its owner, missing condition and next destination so you do not need to guess where to configure it. This page summarizes progress; it does not perform every setup task or certify production merely because a card is visible.

Understand The Screen

Progress Counters (Signed-In User (Read-Only))

Completed, Partial, Not started, Blocked, Backend unavailable, Not applicable and Waived have different meanings. Not applicable excludes a condition that does not apply; Waived is an explicit recorded exception, not an assumption made by the guide.

Ordered Setup Steps (Signed-In User (Read-Only))

Customer / Tenant Selection identifies the organization. Subscription & Entitlement Activation establishes the permitted capability. Deployment Mode Selection and Runtime Configuration establish placement and mode. Governance Onboarding / Binding connects permitted services. Ingestion Setup prepares input. Executor / Action Readiness prepares authorized action. Review / Evidence / Go-Live reviews the resulting readiness.

Step Detail And Provenance (Signed-In User (Read-Only))

Each card reports fields complete, dependencies, owner, blocked reason and next action. Provenance identifies the recorded sources behind the summary. A completion percentage is not proof of live customer connectivity.

Step By Step

1. Review The First Incomplete Step (Signed-In User (Read-Only))

Open Organization & Onboarding > Onboarding Progress. Confirm your organization, then follow the earliest incomplete step whose dependencies are satisfied.

Onboarding Progress - Continued

2. Open Its Owning Screen (Signed-In User (Read-Only))

Use the card's offered destination. Complete identity in Organization & Tenant Profile, licensing in Subscription & Entitlements and deployment stages in Deployment Configuration as directed.

3. Respect Dependencies And Ownership (Signed-In User (Read-Only))

Read the step's owner and blocking reason. Do not bypass license or governance requirements by configuring a later executor first.

4. Return And Recheck (Signed-In User (Read-Only))

After saving in the owning workflow, return to Onboarding Progress and refresh. Confirm the stored state changed; if its source is unavailable, keep that distinction visible.

If Something Goes Wrong

A Step Stays Partial

Required fields or dependencies remain incomplete.

Where To Go: Organization & Onboarding > Onboarding Progress > Affected Step

Read its required-field counts and next action; return to that named owning screen and complete the missing condition.

Backend Unavailable

The progress source could not be read.

Where To Go: Command Center > System Health

Have the responsible operator check the affected service, then refresh onboarding. Do not mark the step complete from memory.

Onboarding Progress (Admin; Other Roles Read-Only Where Offered)

Isolated Demonstration - Not Your Current Tenant State



1. VIEW

Opens the owning configuration screen; it does not complete the stage.

What Happens

Work through the displayed dependency order. Completed, pending, blocked and unavailable have different meanings; inspect the recorded reason.

19. Organization & Tenant Profile (Admin; Other Roles Read-Only Where Offered)

Organization & Tenant Profile records who your organization is and the context that should govern its security work. A tenant is an organization's isolated working boundary, so changing this profile affects that organization rather than another customer. Profile captures identity, sector, jurisdiction, applicability and operational restrictions; Domain Intelligence shows the activation derived from that stored context. Licensing, Billing, Entitlements and Audit show related lifecycle records without turning profile visibility into commercial authority. Complete and review this information carefully because an incorrect sector, country or protected asset can lead to the wrong operating context.

Understand The Screen

Profile - Identity And Operating Context (Admin; Other Roles Read-Only Where Offered)

Tenant Identity identifies the legal organization. Review country, legal name, sector and sub-industry using the offered fields. Contacts and locations identify responsibility and operating footprint. Asset and response restrictions describe infrastructure that needs protection or a human decision; do not guess these facts.

Domain Intelligence (Admin; Other Roles Read-Only Where Offered)

This tab shows activation derived from the sector, jurisdiction and applicability facts saved in Profile. To change an applicability answer, return to Profile and its Regulatory Applicability Details; this activation review is not that editing form. Unknown is unresolved; No, None and None Apply are explicit answers. Mandatory instruments cannot be removed while the applicability result includes them. Needs More Information asks for missing context; Recommended, Optional and Customer Selected are distinct from mandatory obligations.

Licensing (Admin; Other Roles Read-Only Where Offered)

Read assigned package and lifecycle information for the selected organization. Commercial assignment and execution authority remain separate; a profile editor is not automatically a manufacturer signing authority.

Organization & Tenant Profile - Continued

Billing (Admin; Other Roles Read-Only Where Offered)

Review recorded commercial and billing information. A displayed price or record is not evidence that payment or provisioning completed.

Entitlements (Admin; Other Roles Read-Only Where Offered)

Inspect the capability activation state and its prerequisites. Visibility of a domain does not mean it is licensed, bound or permitted to execute.

Audit (Admin; Other Roles Read-Only Where Offered)

Review recorded profile and lifecycle changes, their actor and time. Use this history to distinguish a saved change from a draft. Tenants in the navigation points to this same profile workspace and does not require a second identical chapter.

Step By Step

1. Confirm The Tenant (Admin; Other Roles Read-Only Where Offered)

Open Organization & Onboarding > Organization & Tenant Profile. Where an authorized tenant selector is offered, confirm its identity before editing; switching with unsaved changes may require an explicit discard confirmation.

2. Complete Identity And Technology Facts (Admin; Other Roles Read-Only Where Offered)

In Profile, Organization Name is the working name; Legal Name identifies the legal entity. Deployment Type is placement, not operating authority. Customer Type classifies the relationship; Employee Range records organization size. Select actual Data Types Handled, Regulated Data Types and Cloud Providers. None is an explicit answer, not an unfinished field. Critical Systems names the systems whose availability matters.

3. Complete Sector And Applicability (Admin; Other Roles Read-Only Where Offered)

Select Industry / Sector before Sub-industry. Business Criticality describes the importance of operations. Primary Country and compliance jurisdictions shape applicability. Review Regulatory Applicability Details and Applicable Regulatory Instruments & Frameworks; answer the offered questions from actual facts. Save and Lock applies the offered completion conditions. Do not substitute Unknown with No to clear a blocker.

Organization & Tenant Profile - Continued

4. Review Domain Intelligence And Lifecycle (Admin; Other Roles Read-Only Where Offered)

Open Domain Intelligence to review activation derived from the stored profile. Licensing and Entitlements show the recorded commercial capability; use Subscription & Entitlements for its owning operation. Billing shows Commercial Summary, Billing Account, Handoff Queue and Invoices. Currency, cadence, payment terms, due days and tax fields describe billing, not security policy; only an authorized billing actor may use its offered edit controls.

5. Confirm The Saved State (Admin; Other Roles Read-Only Where Offered)

Reopen Profile and check Audit for the actor, time and changed record. Audit pagination and Export CSV concern the displayed history. Keep any exported data inside approved storage. Review completion and lock conditions before using them; do not lock an incomplete draft merely to change a progress label.

Organization & Tenant Profile - Continued

If Something Goes Wrong

Needs More Information

The applicability calculation lacks an answer required for this context.

Where To Go: Organization & Onboarding > Organization & Tenant Profile > Profile > Regulatory Applicability Details

Answer the named question from the organization's actual facts. Unknown must not be substituted with No just to remove a blocker.

Entitlement Is Inactive

The organization profile and commercial activation are separate.

Where To Go: Organization & Onboarding > Subscription & Entitlements

Inspect the installed capability and activation prerequisites with the authorized administrator; then review its binding in Ecosystem workspace.

Unsaved Changes On Tenant Switch

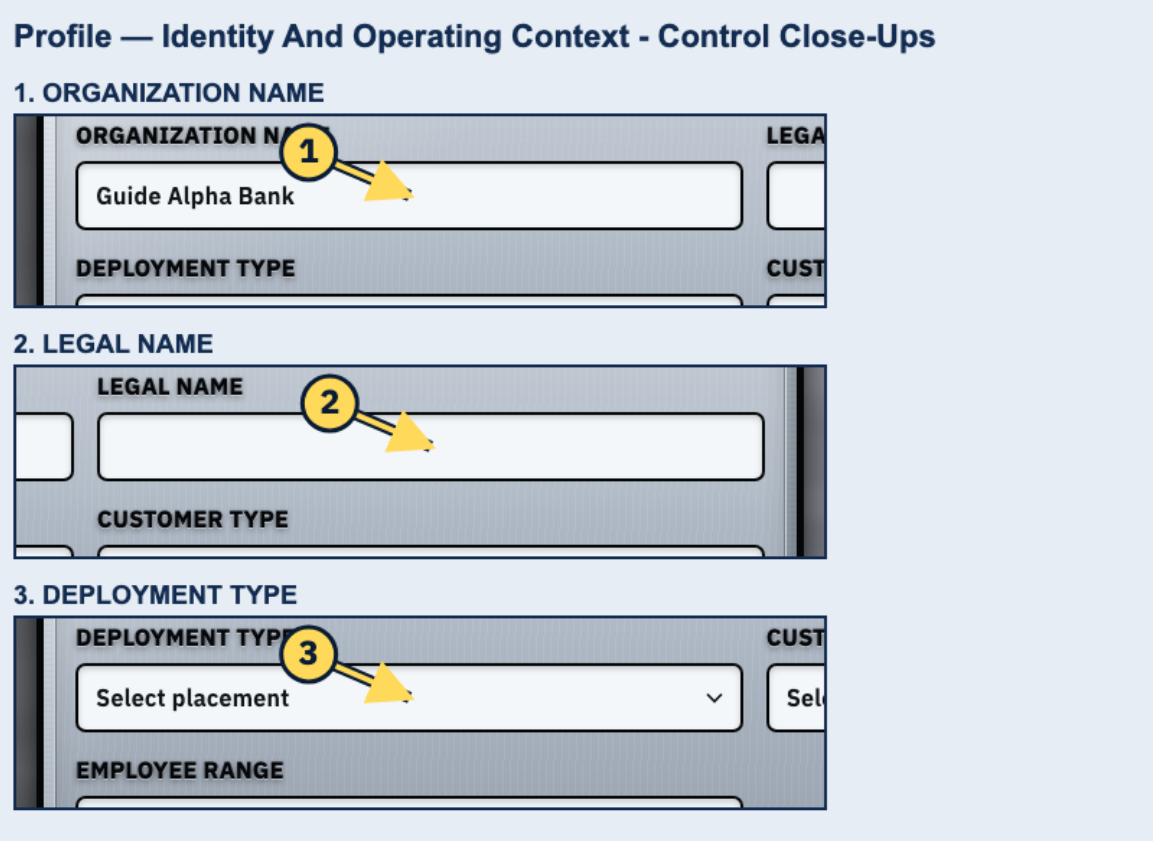
The new selection would discard the current draft.

Where To Go: Organization & Onboarding > Organization & Tenant Profile > Profile

Save the intended changes first, or explicitly discard them after review. Never apply one organization's draft to another tenant.

Profile - Identity And Operating Context (Admin; Other Roles Read-Only Where Offered)

Isolated Demonstration - Not Your Current Tenant State



1. ORGANIZATION NAME

Use the organization’s approved identity and contact details.

2. LEGAL NAME

Choose the actual jurisdiction, sector and operating context; they are policy inputs, not decorative labels.

3. DEPLOYMENT TYPE

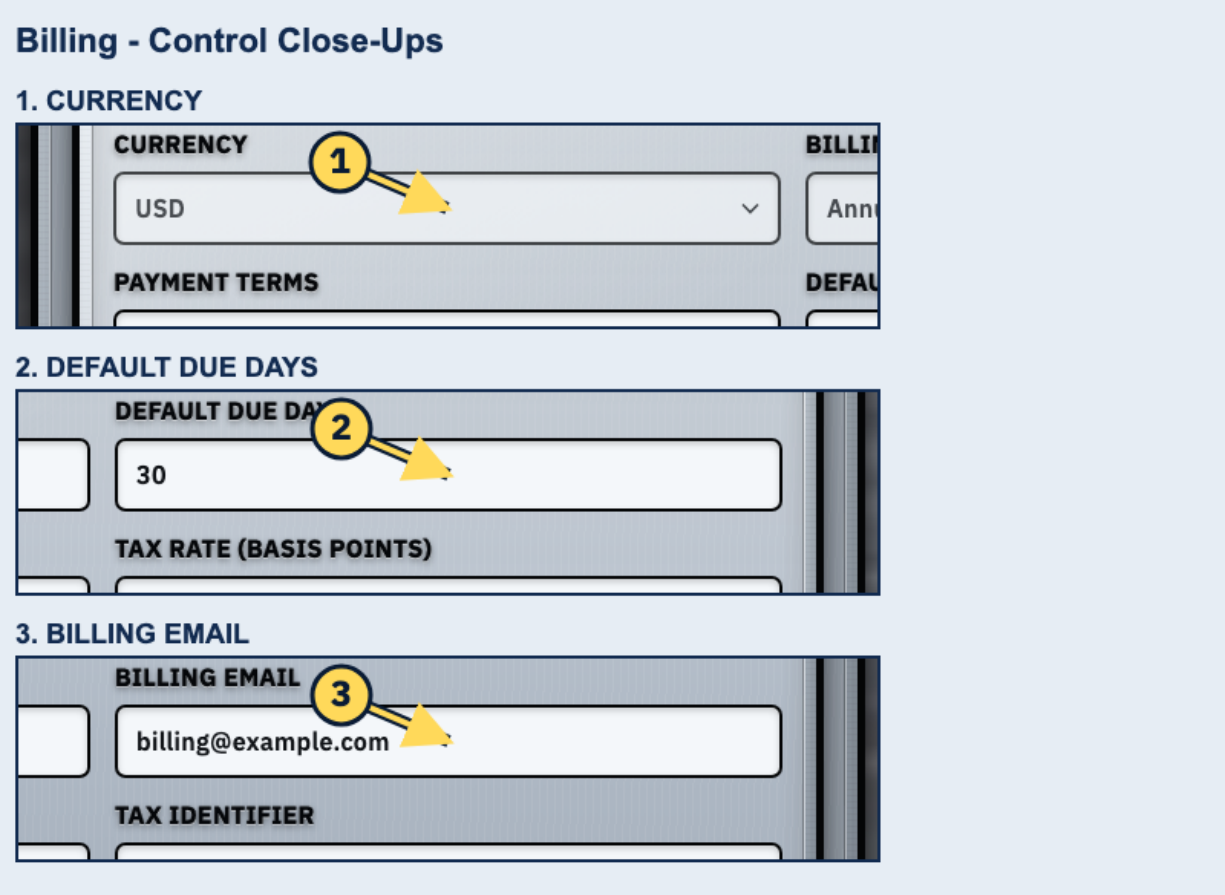
Select the actual placement. Saving or locking this profile is a separate operation; review those steps before using it.

What Happens

Saving changes organization context; locking/unlocking remains separately governed.

Billing (Admin; Other Roles Read-Only Where Offered)

Isolated Demonstration - Not Your Current Tenant State



1. CURRENCY

Choose the approved billing currency.

2. DEFAULT DUE DAYS

Enter the contractual number of days, not a date.

3. BILLING EMAIL

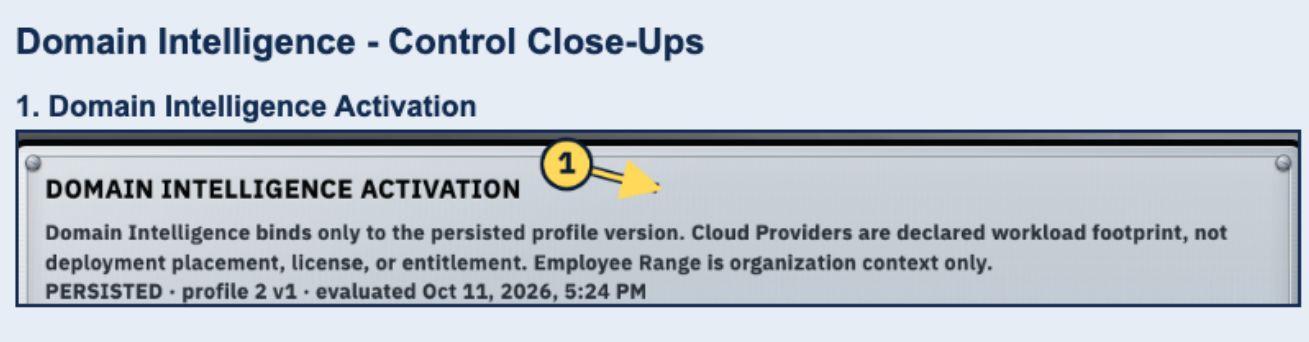
Enter the approved billing contact address.
Illustrative Format Only: billing@example.invalid (illustrative only)

What Happens

Use the tab's offered save action only when authorized. Export JSON / CSV reads recorded data; it does not send an invoice.

Domain Intelligence (Admin; Other Roles Read-Only Where Offered)

Isolated Demonstration - Not Your Current Tenant State



1. Domain Intelligence Activation

Read the persisted jurisdiction/sector context and completeness.

What Happens

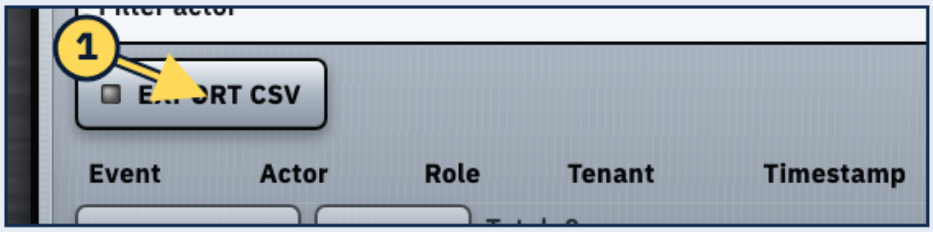
A stored domain selection is policy context, not a claim of regulatory compliance. Correct missing context in Profile before retrying.

Audit (Signed-In User (Read-Only))

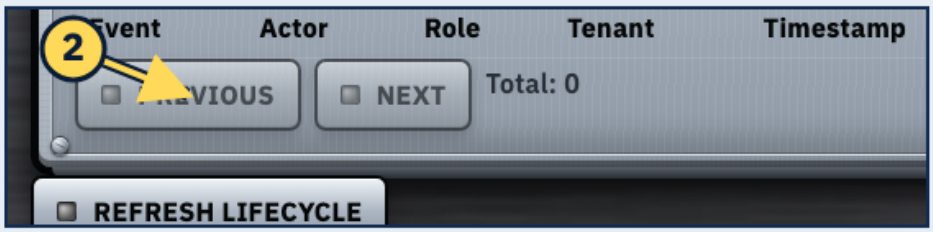
Isolated Demonstration - Not Your Current Tenant State

Audit - Control Close-Ups

1. Export CSV



2. Previous



1. Export CSV

Downloads the displayed audit history; does not change it.

2. Previous

Reads the prior available page of records.

What Happens

Keep exported organization history in approved storage.

20. Admin Settings (Admin; Other Roles Read-Only Where Offered)

Admin Settings is the organization’s administration workspace for accounts, permissions, identity providers, security, connectors and credentials. A role is a set of permissions; an identity provider is a service used for sign-in; a connector links a supported outside system. The six tabs keep those responsibilities separate while retaining the same organization scope. An authorized administrator can inspect records and use the offered controls, but some operations need a separate approval, confirmation or higher permission. Never paste a password, recovery code or stored secret into the Guided Assistant to resolve an administration issue.

Understand The Screen

USERS - Invite And Inspect (Admin; Other Roles Read-Only Where Offered)

Invite User requests identity and role information for a new account. Select a row in Users to open User Admin Detail. Review account status, assigned role, organization and MFA state before using any lifecycle control. A pending invitation is not an active account.

USERS - Lifecycle Controls (Admin; Other Roles Read-Only Where Offered)

ASSIGN ROLE changes permitted responsibility; ACTIVATE and SUSPEND affect account availability; OFFBOARD ends the intended lifecycle. FORCE MFA RE-ENROLL requires the user to enroll again. REVOKE SESSIONS ends sessions; RESEND INVITE sends another invitation through the configured channel. CREDENTIAL APPROVAL, ACCESS REVIEW and TITLE / MANAGER address their specific administrative records. Read confirmation and protected-owner restrictions; do not remove the last required privileged administrator.

ROLES & RBAC (Admin Reads; Platform Owner Changes Role Definitions)

RBAC means role-based access control. Select a role and read Role Detail & Permission Matrix before changing it. Permissions determine actions rather than just menu visibility. Protected system roles and privileged changes remain governed by the existing controls.

SSO & IDENTITY (Admin; Other Roles Read-Only Where Offered)

SSO is single sign-on. SSO & Identity Catalog lists configured identity-provider records; IdP Detail shows the selected provider. Review protocol, domain and permitted configuration. TEST CONNECTION, VERIFY DOMAIN and SCIM SYNC have separate purposes; SCIM concerns identity provisioning, not proof that sign-in succeeded.

Admin Settings - Continued

SECURITY / MFA (Admin; Other Roles Read-Only Where Offered)

MFA means multi-factor authentication: an additional verification beyond a password. Inspect the organization’s security and enrollment requirements. Recovery and re-enrollment are controlled procedures, not ways to bypass the second factor.

CONNECTORS (Admin; Other Roles Read-Only Where Offered)

Inspect connector installations and configuration using the supported catalog. An install record is not proof of live vendor connectivity. Review the test or health result offered by the owning integration. Use the Credential Vault for secrets rather than embedding them in guide text.

CREDENTIAL VAULT (Admin; Other Roles Read-Only Where Offered)

Store Credential records a permitted credential and its environment. Credential Reference List identifies records without displaying stored secrets. Credential Detail and Vault Actions operate on the selected reference. A local decryptability result is not a live vendor-connection test. Read approval, lock or update conditions before using a vault action.

Step By Step

1. Choose The Account Or Permission Task (Admin; Other Roles Read-Only Where Offered)

Open Admin Settings > USERS. Enter the invited person’s Email, Name, Role and Department; Invite User sends an invitation, not immediate verified access. Search Users locates a record; select it before using lifecycle controls. In ROLES & RBAC, New Role Name identifies a new permitted role. Select its Permission Matrix and review actual permissions before saving; a role name alone does not grant capability.

2. Configure Identity Carefully (Admin; Other Roles Read-Only Where Offered)

In SSO & IDENTITY choose provider Type and a descriptive Name. Entity ID / Issuer identifies the provider; SSO URL is its sign-in endpoint; SAML Certificate / Metadata is write-only trust material. Allowed Domains restricts identity scope. SCIM Endpoint and its write-only Token concern provisioning. Claims / Group-role Map maps supplied identity claims to permitted roles. The JIT Provisioning Flag is explicitly stored-only, not proof of automatic provisioning. Test Connection, Issue Domain Challenge, Confirm Challenge and Sync Now have different results; inspect each actual response.

Admin Settings - Continued

3. Review MFA And Exceptions (Admin; Other Roles Read-Only Where Offered)

In SECURITY / MFA, Set Up Authenticator enrolls your account's second factor. Organization metrics and Users Requiring Action identify outstanding enrollment. Enforce MFA changes the organization requirement only through its offered authority. A governed exception needs the named Identity, Reason and Expiry; it is not an indefinite bypass. Recovery, Force Re-enroll and Revoke Sessions require their owning permission and confirmation.

4. Configure A Connector And Its Mail Channel (Admin; Other Roles Read-Only Where Offered)

In CONNECTORS, choose the supported vendor category and installation. For Customer SMTP, Mail Server and Port identify the approved server; Username and Password authenticate; Sender Address and Name identify outgoing messages. TLS Mode chooses STARTTLS or implicit TLS; CA Certificate supplies approved trust when required. Save stores configuration, Test Connection tests the connection, Send Test Email attempts actual delivery, and Disable stops use. These results are separate. A successful connection does not prove mailbox delivery.

5. Approve Only The Intended Endpoint (Admin; Other Roles Read-Only Where Offered)

Approved Endpoint Access restricts where a connector may communicate. Select Connector Installation and enter HTTPS Hostname, Port, any permitted IPv4 CIDR, Customer CA Vault Reference and Existing Credential Vault Reference. Capability Scope defines permitted use; Fresh Authenticator Code supplies the required step-up check. Create, Replace, Enable, Disable and Remove have different effects. Confirm the exact destination and inspect the recorded result; do not approve a broad destination to bypass a connection failure.

6. Store And Read Back A Credential Safely (Admin; Other Roles Read-Only Where Offered)

Use CREDENTIAL VAULT > Store Credential for the supported secret type and environment. Select its reference to inspect detail and permitted actions without revealing the secret. Keep passwords, tokens and certificates in the designated write-only inputs. Reopen the affected user, provider, connector or vault detail and its audit record after a permitted operation; a toast or local decryptability result is not proof that a vendor connected.

Admin Settings - Continued

If Something Goes Wrong

User Cannot Open A Workflow

Account state, role permissions, Terms, entitlement or binding may prevent access.

Where To Go: Organization & Onboarding > Admin Settings > USERS / ROLES & RBAC

Check the actual account and assigned role first. Use Subscription & Entitlements for licensing and Ecosystem workspace for bindings; do not grant broad privileges just to remove an error.

SSO Test Or Domain Verification Fails

The configured provider or domain does not satisfy the selected test.

Where To Go: Organization & Onboarding > Admin Settings > SSO & IDENTITY > IdP Detail

Review the reported condition and the configured protocol, domain and credential reference with the identity administrator. Do not assume SCIM synchronization proves sign-in.

Vault Action Is Denied

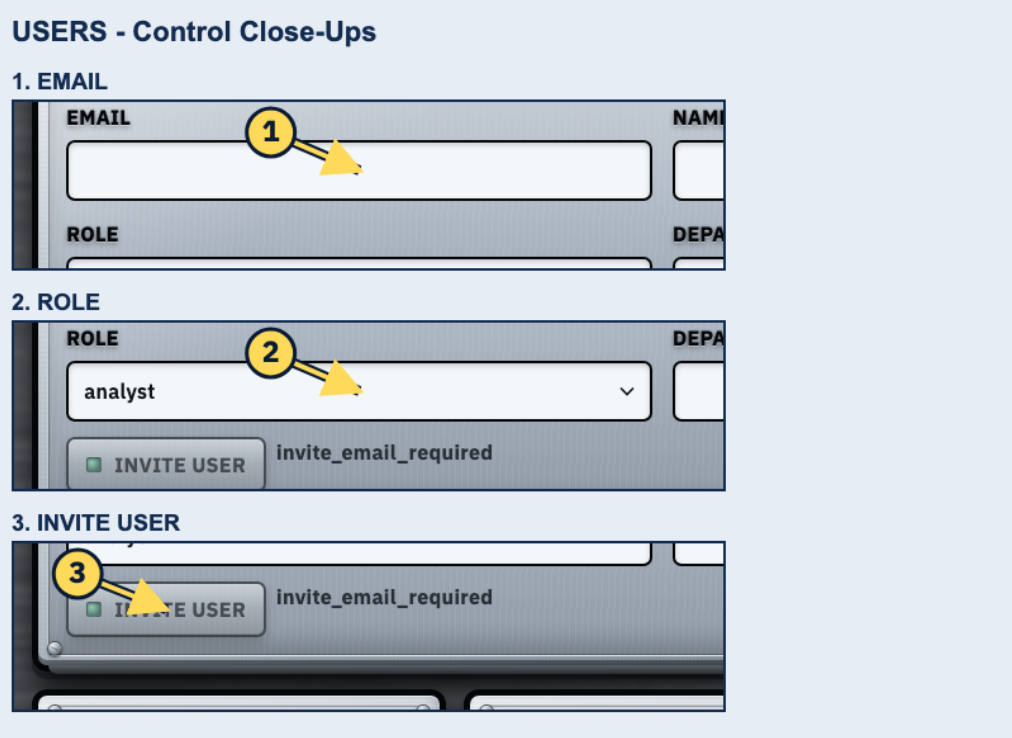
The selected reference, environment or permission does not allow this operation.

Where To Go: Organization & Onboarding > Admin Settings > CREDENTIAL VAULT > Credential Detail

Check the correct reference and the named approval or lock condition. Do not copy the secret to another field or an external channel.

USERS (Admin)

Isolated Demonstration - Not Your Current Tenant State



1. EMAIL

Find the intended user by their own email or displayed identity.

2. ROLE

Use the approved account and permitted role; do not create a platform-owner role inside a customer tenant.

3. INVITE USER

Read the effect before changing status, resetting access or revoking sessions.

What Happens

User lifecycle actions affect another person’s access. Role definition changes, where offered, require Platform Owner authority.

Read First

Do not use account-management actions as tutorial practice.

ROLES & RBAC (Admin Reads; Platform Owner Changes Definitions)

Isolated Demonstration - Not Your Current Tenant State



1. NEW ROLE NAME

Use an approved descriptive role name. Customer administration does not grant platform-owner role-definition authority.

2. CREATE ROLE

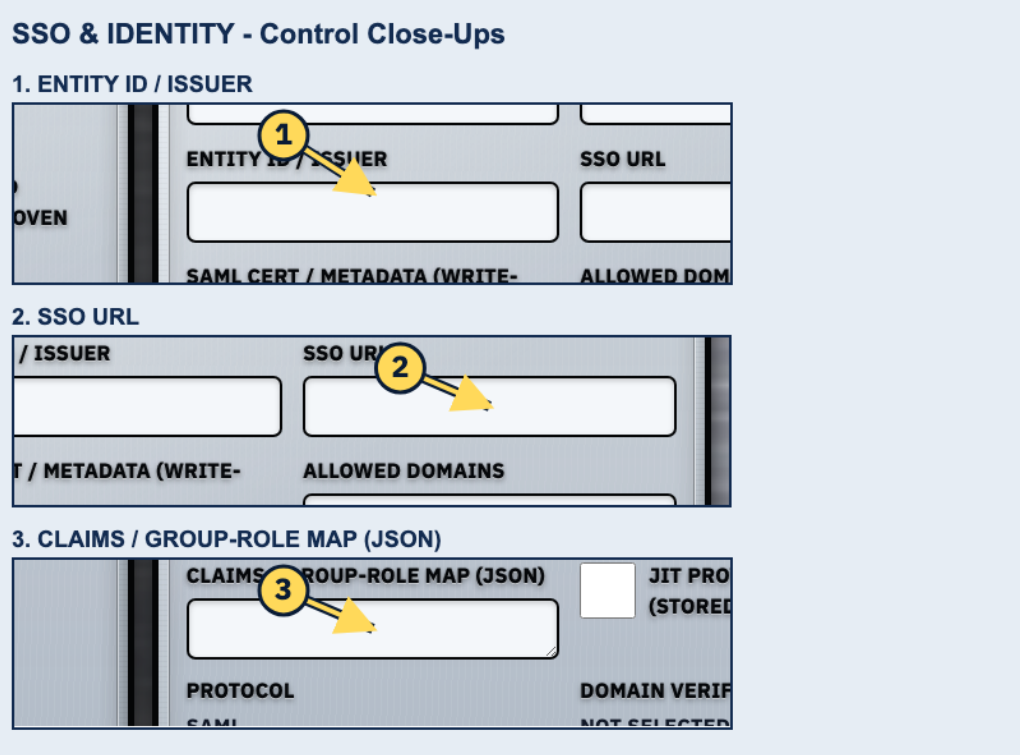
Only the platform owner can create the supported role definition; a visible field is not permission.

What Happens

Review permissions individually. Role labels alone do not prove execution authority.

SSO & IDENTITY (Admin)

Isolated Demonstration - Not Your Current Tenant State



1. ENTITY ID / ISSUER

Copy the issuer from your approved identity-provider configuration; do not guess it.

2. SSO URL

Use the provider's exact supported HTTPS endpoint.
Illustrative Format Only: https://idp.example.invalid/... (format only)

3. CLAIMS / GROUP-ROLE MAP (JSON)

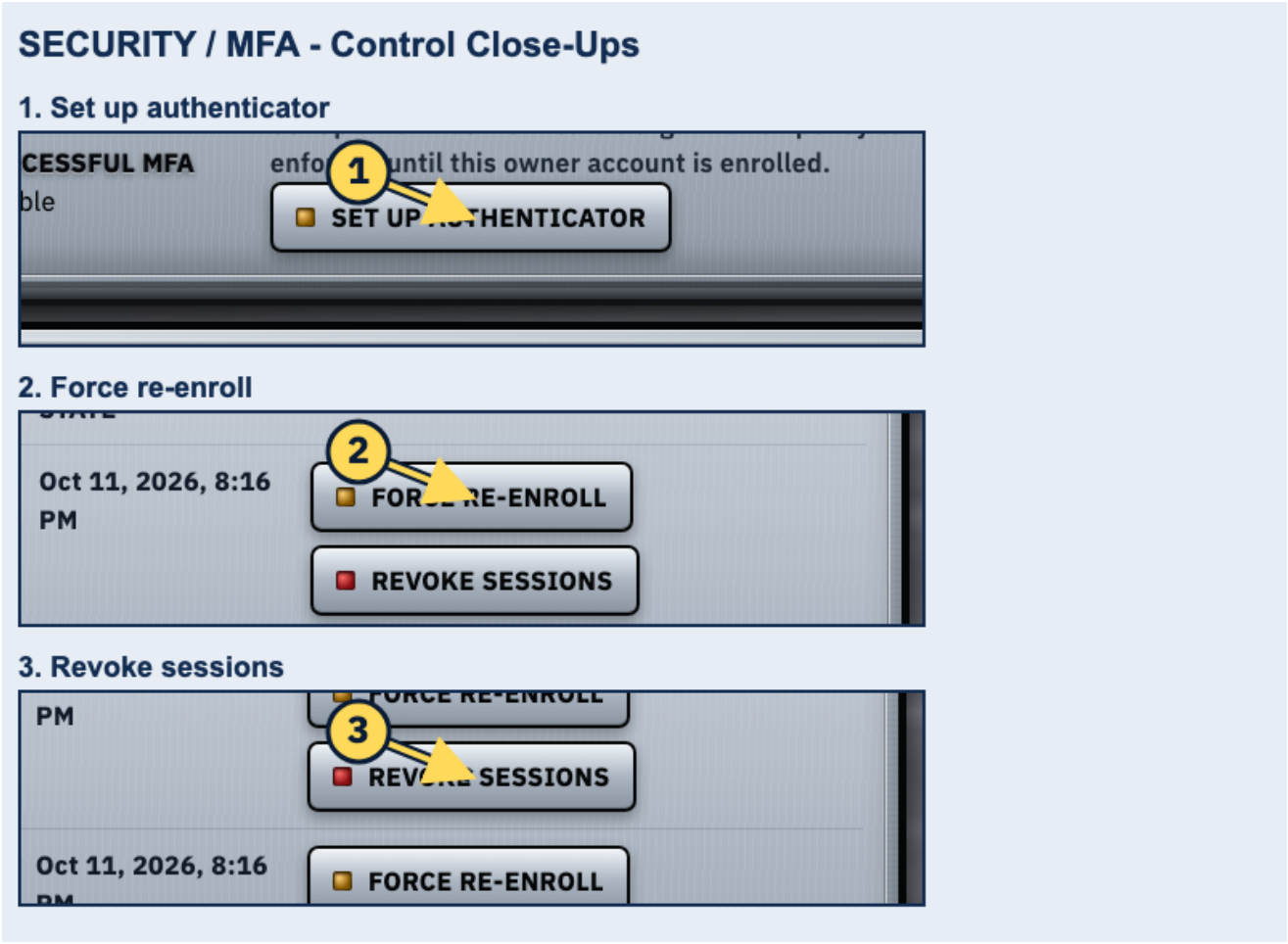
Enter the supported JSON mapping, not prose. Obtain the approved mapping from your identity administrator.
Illustrative Format Only: {"<approved claim>": "<approved value>"} (JSON shape only; do not submit these placeholders)

What Happens

Saving stores configuration. JIT flag is stored only; do not infer that toggling it enables an unproven authentication flow. Never put SAML/SCIM secrets in Assistant.

SECURITY / MFA (Admin; Enrollment For Own Account)

Isolated Demonstration - Not Your Current Tenant State



1. Set up authenticator

Starts your own supported enrollment; keep its secret out of help questions.

2. Force re-enroll

Invalidates the selected person's MFA setup under existing controls.

3. Revoke sessions

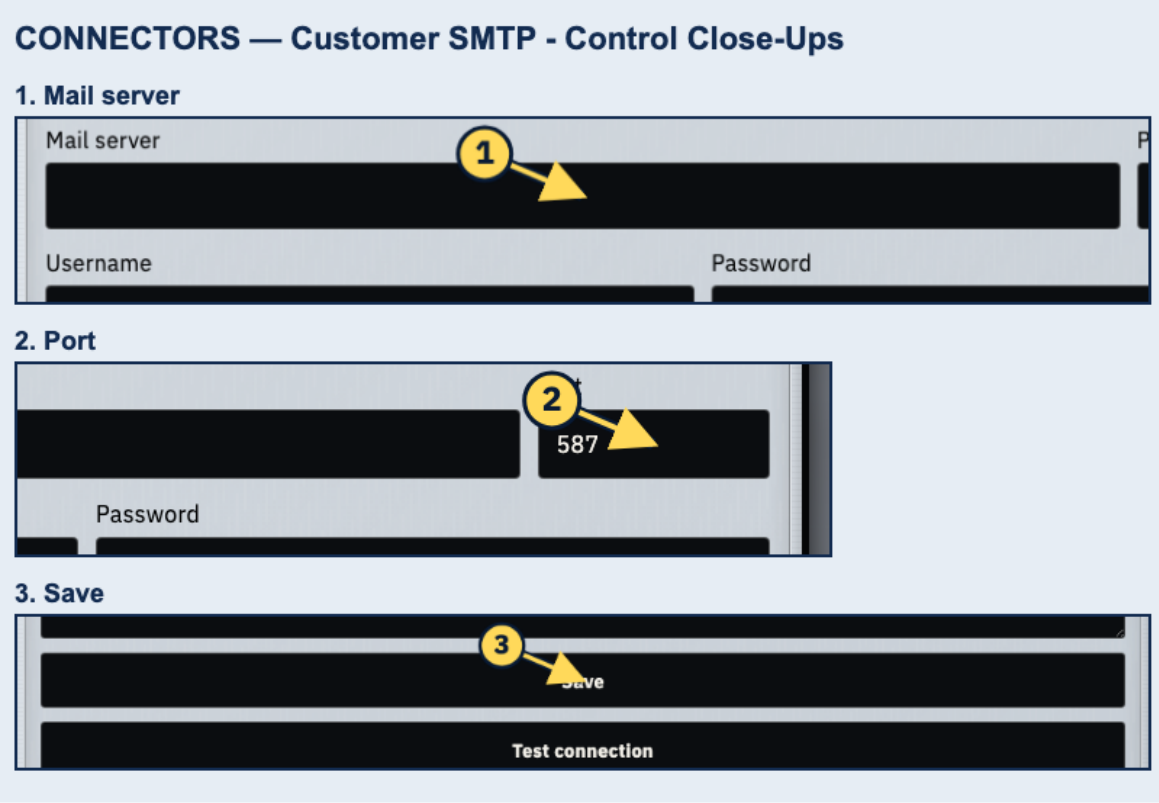
Ends that person's sessions; confirm identity before using it.

What Happens

Reset/revoke can interrupt access. Do not practice these actions on another user.

CONNECTORS - Customer SMTP (Admin)

Isolated Demonstration - Not Your Current Tenant State



1. Mail server

Enter the organization's approved SMTP hostname, not a web page URL.
Illustrative Format Only: smtp.example.invalid (format only)

2. Port

Use the provider's port matching the selected TLS mode.
Illustrative Format Only: 587 with STARTTLS; 465 with Implicit TLS (confirm your provider)

3. Save

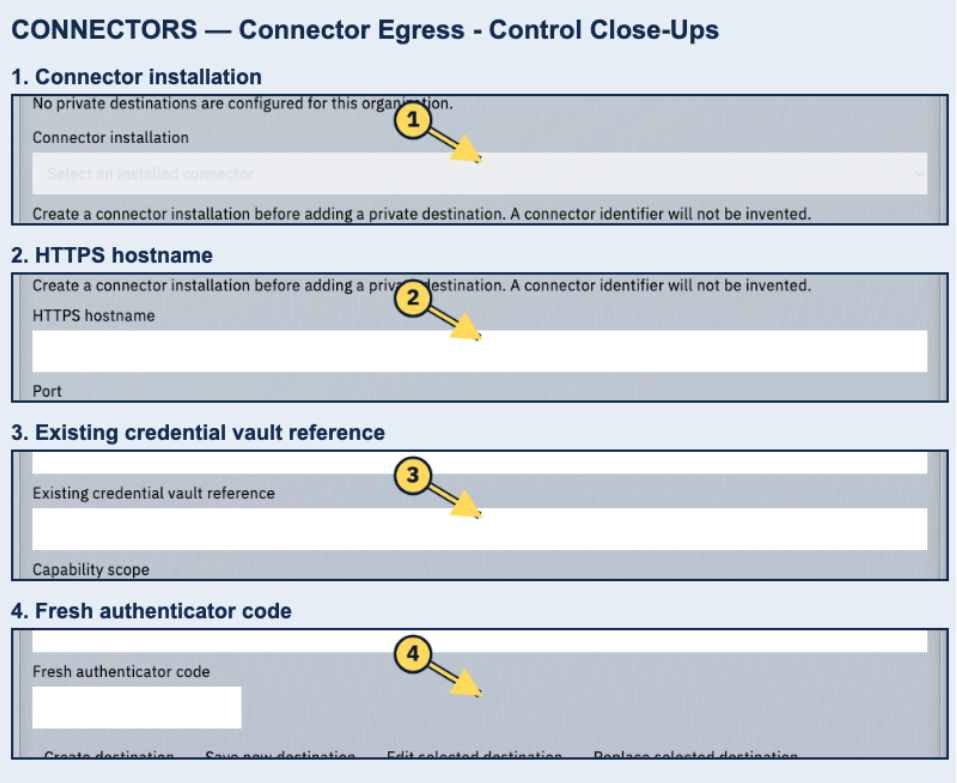
Stores the supplied configuration; Test connection and Send test email are separate network/ delivery actions.

What Happens

A successful Save does not prove mailbox delivery. Correct server, port, TLS, trust and sender in this same card before retesting. Secrets are write-only; never paste them into Assistant.

CONNECTORS - Connector Egress (Admin)

Isolated Demonstration - Not Your Current Tenant State



1. Connector installation

Select the actual installed connector.

2. HTTPS hostname

Use its approved exact destination hostname.

3. Existing credential vault reference

Use an existing permitted vault reference, not its raw secret.

4. Fresh authenticator code

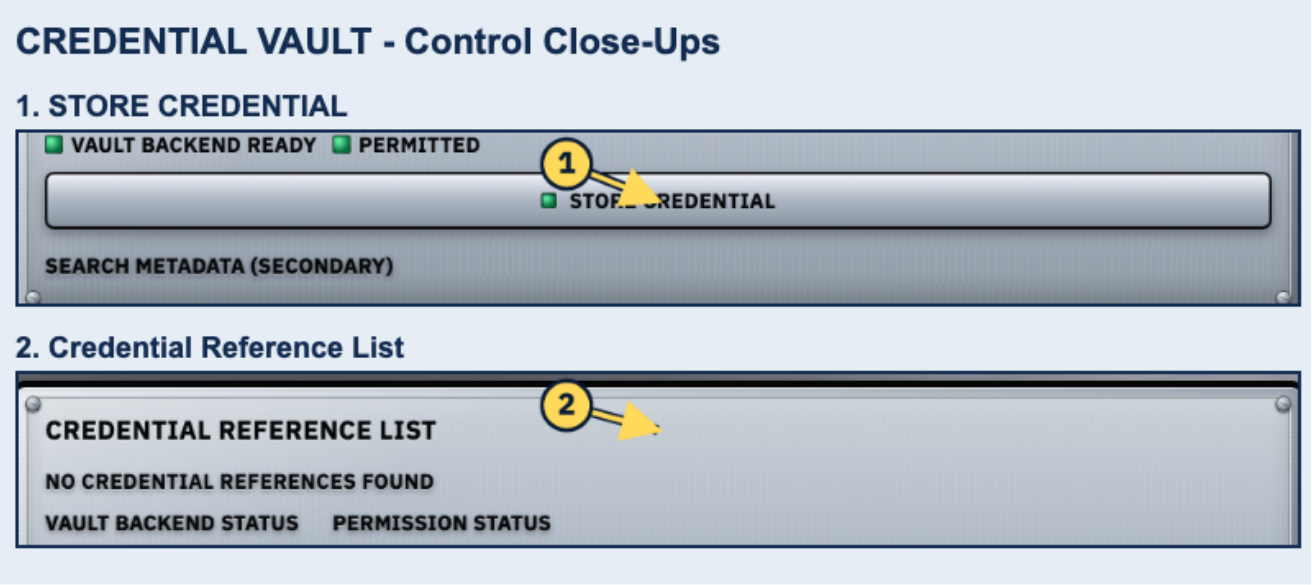
Use your own current enrolled code when the gated operation requires it.

What Happens

Review destination, scope and trust before allowing egress. A vault reference is not an authorization override.

CREDENTIAL VAULT (Admin)

Isolated Demonstration - Not Your Current Tenant State



1. STORE CREDENTIAL

Opens the supported credential-entry procedure; do not submit a tutorial example.

2. Credential Reference List

Use the stored reference in its owning connector workflow, not the secret value.

What Happens

The vault supports authorized storage and references. Stored secrets must not be exposed to screenshots, PDF or questions.

21. Subscription & Entitlements (Admin; Other Roles Read-Only Where Offered)

Subscription & Entitlements explains the commercial capabilities available to this organization. A subscription records a purchased or assigned product lifecycle; an entitlement records which capability may be used under its conditions. The catalog and quote workflow describe commercial options, while current subscriptions and entitlements show recorded state. Billing and Lifecycle / Audit retain related commercial records. Use this page to identify the intended capability and its activation conditions, remembering that a listed product still needs a valid binding and execution permission before runtime use.

Understand The Screen

Catalog (Admin; Other Roles Read-Only Where Offered)

Review the versioned product catalog, SKU and offered capability. Starter, Core and Governance are commercial packages, not AS-OS layers. A catalog entry is not an installed subscription.

Configure / Quote (Admin; Other Roles Read-Only Where Offered)

Choose the offered product and permitted options to prepare a quote through this workflow. Configuration and quote preparation are not activation, payment completion or manufacturer-signed provisioning.

Current Subscriptions - Offline License And Licensing Audit (Admin; Other Roles Read-Only Where Offered)

Inspect Current subscriptions, Offline license and Licensing audit. Evaluation and purchased production states are separate. The offered signed-artifact apply procedure consumes the input for this organization and installation; it does not create a manufacturer signature. Follow the packaged enrollment, custody-checkpoint capture and audit verification procedure where displayed; retain its original files and receipts inside the approved boundary.

Entitlements (Admin; Other Roles Read-Only Where Offered)

Read the allowed capability and its active, missing, expired or otherwise reported state. Installation and service-binding constraints still apply. Tenant identity, Licensed packages, Billing references, Provisioning summary, Recent lifecycle events, Entitlements mirror and Entitlement ledger describe related records, not independent permission to execute.

Subscription & Entitlements - Continued

Billing (Admin; Other Roles Read-Only Where Offered)

Review the stored billing records and their actual status. A displayed amount is not proof of collection or successful service activation.

Lifecycle / Audit (Admin; Other Roles Read-Only Where Offered)

Review the actor, time and record of commercial changes. Retain application and issuance receipts under the organization’s approved local procedure. Manufacturer production signing remains outside the customer runtime.

Step By Step

1. Identify The Capability (Admin; Other Roles Read-Only Where Offered)

Open Organization & Onboarding > Subscription & Entitlements > Catalog and locate the required product or capability.

2. Inspect The Installed State (Admin; Other Roles Read-Only Where Offered)

Open Current Subscriptions and Entitlements. Confirm the intended organization, lifecycle, validity and capability rather than relying on menu visibility.

3. Use The Appropriate Commercial Path (Admin; Other Roles Read-Only Where Offered)

Prepare a quote only through Configure / Quote. Where offline issuance is required, obtain the authorized manufacturer-signed artifact and follow the installed apply workflow; the manufacturer private key is not an installation input.

4. Check Binding And Readiness (Admin; Other Roles Read-Only Where Offered)

Review the corresponding binding in Ecosystem workspace and the relevant onboarding prerequisite. Return to the blocked mission only after the actual entitlement and binding are usable.

5. Retain The Receipt (Admin; Other Roles Read-Only Where Offered)

Review Lifecycle / Audit and preserve the relevant receipt in controlled local records. A rejected application or quote is not activation.

Subscription & Entitlements - Continued

If Something Goes Wrong

Feature Is Visible But Runtime Is Denied

Visibility, licensing, entitlement and execution authorization are separate.

Where To Go: Organization & Onboarding > Subscription & Entitlements > Entitlements; Ecosystem workspace

Inspect the capability's current state and assigned binding. Have the authorized administrator resolve the named condition without bypassing admission.

Artifact Rejected Or Expired

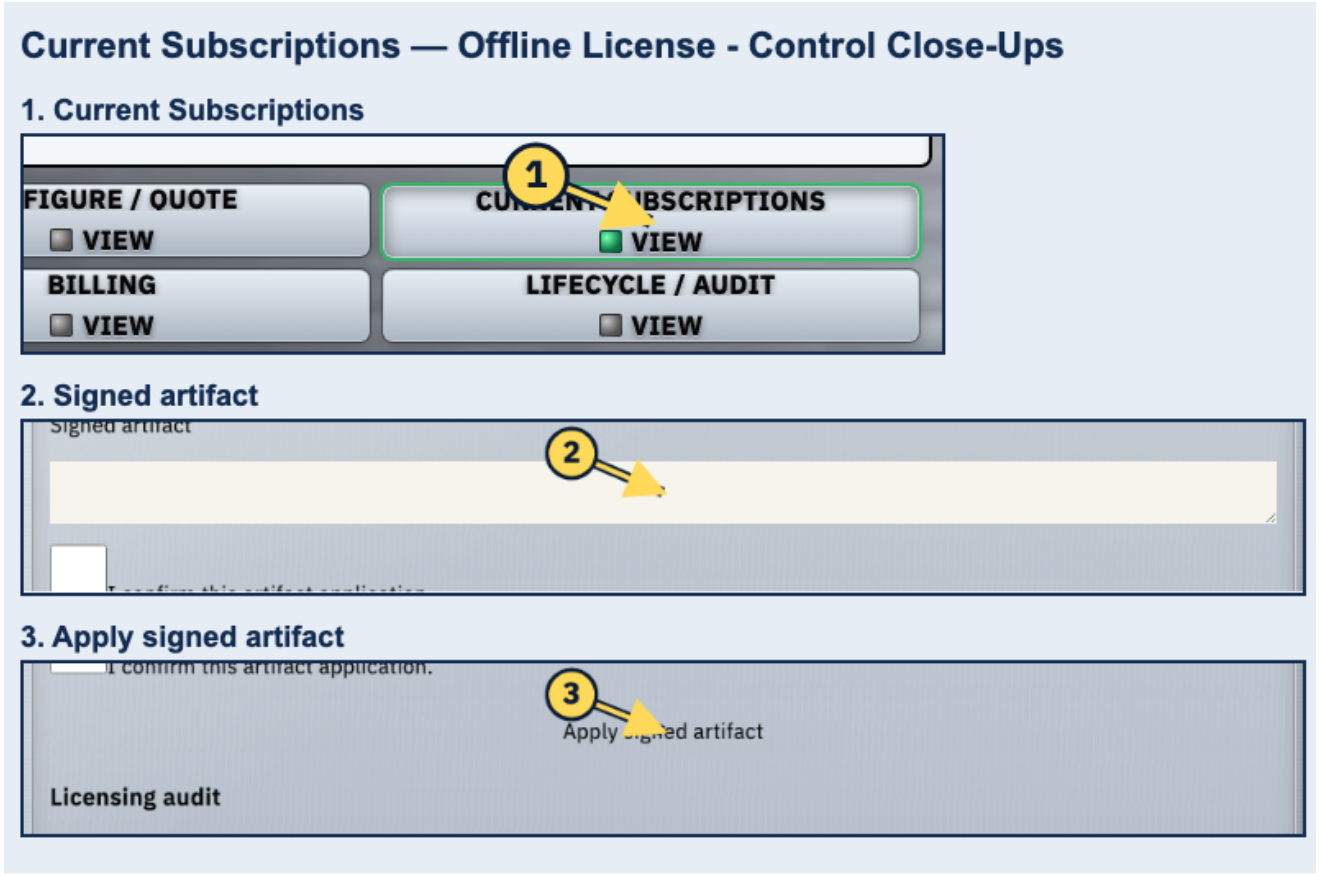
The signed input does not satisfy its validity or installation conditions.

Where To Go: Organization & Onboarding > Subscription & Entitlements > Entitlements

Check the supplied artifact against its intended organization and installation through the approved issuance procedure. Do not edit or re-sign it in the customer runtime.

Current Subscriptions - Offline License (Admin; Other Roles Read-Only Where Offered)

Isolated Demonstration - Not Your Current Tenant State



1. Current Subscriptions

Open the tab and inspect installation, validity and evaluation versus production.

2. Signed artifact

Use the original manufacturer-authorized artifact, unchanged.

3. Apply signed artifact

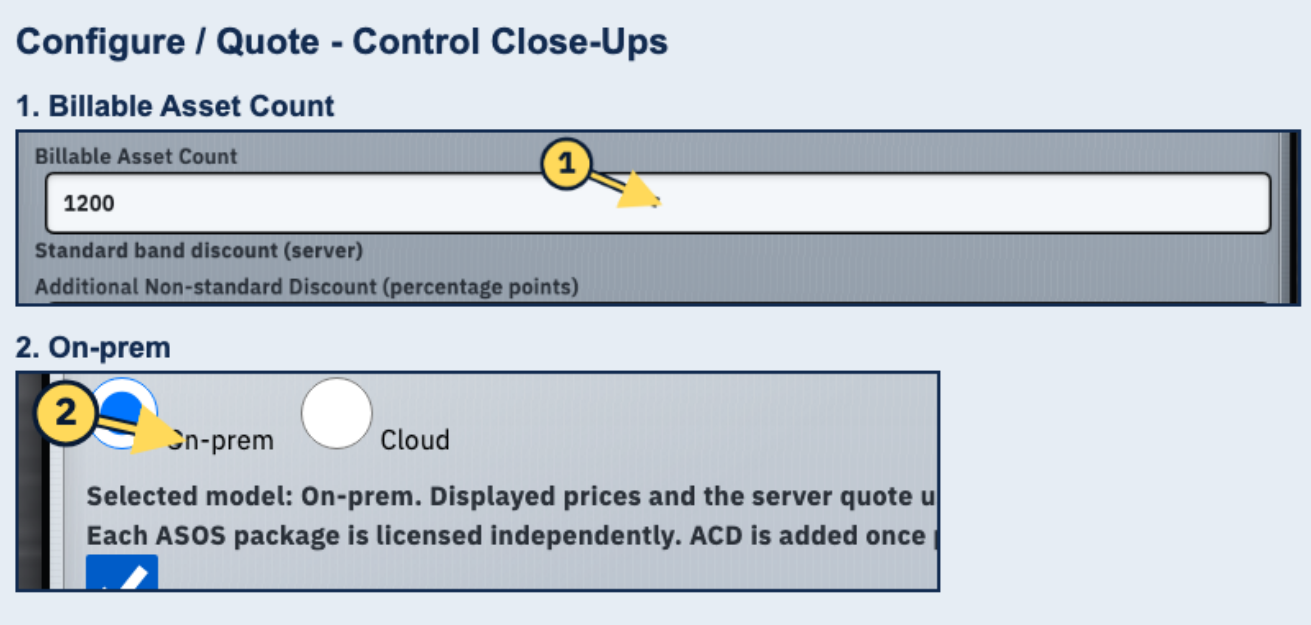
Review and confirm only for its intended installation; inspect the receipt or rejection.

What Happens

Applying an artifact changes licensing state; viewing or exporting its audit does not issue a production license.

Configure / Quote (Admin; Other Roles Read-Only Where Offered)

Isolated Demonstration - Not Your Current Tenant State



1. Billable Asset Count

Use the actual approved billable asset count.
Illustrative Format Only: 100 (illustrative count only)

2. On-prem

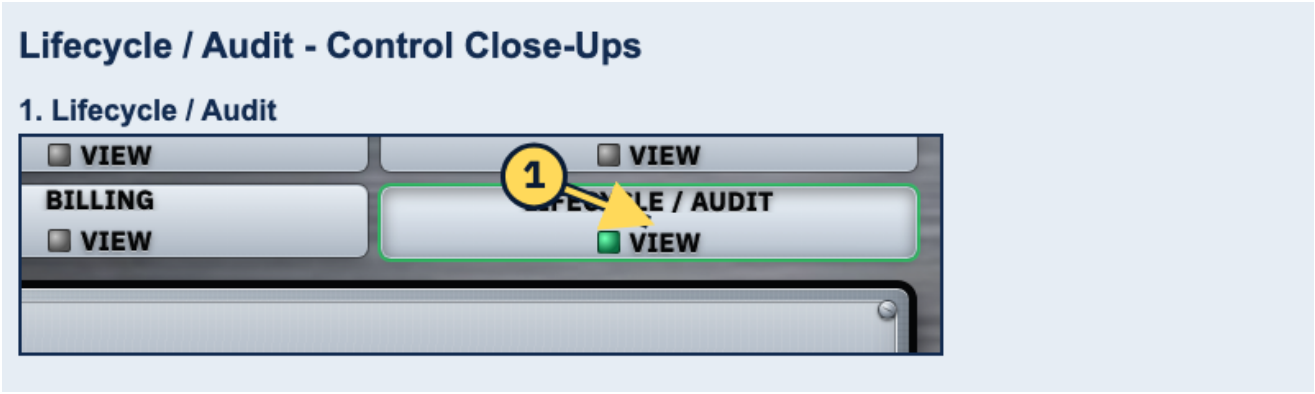
Choose actual placement; quotation is not activation.

What Happens

The displayed price and scope are a quote. Only the supported commercial/enrollment path creates activation.

Lifecycle / Audit (Signed-In User (Read-Only))

Isolated Demonstration - Not Your Current Tenant State



1. Lifecycle / Audit

Read the recorded lifecycle and licensing decisions.

What Happens

History is not permission to extend an expired license or issue a new one.

22. Deployment Configuration (Admin; Other Roles Read-Only Where Offered)

Deployment Configuration prepares the environment in which this organization will run CLAWOLF. It separates where the system is installed from how it is allowed to operate and how the engagement is staged. Its seven-step workflow then binds governance, configures incoming data and checks authorized action readiness before go-live review. You can use the offered forms and validation controls to record configuration and inspect the corresponding evidence. A saved setting, available connector or open go-live page is not proof that the customer environment has been activated.

Understand The Screen

1. Deployment Mode (Admin; Other Roles Read-Only Where Offered)

Choose the supported placement for the intended environment, such as cloud, on-premises or air-gapped where offered. This concerns location and connectivity, not permission for autonomous action.

2. Runtime Configuration (Admin; Other Roles Read-Only Where Offered)

Review the intended runtime configuration and operating mode. Observation, alert-only or human-reviewed operation restrict behavior differently. Do not choose a more powerful mode merely to make a test pass.

3. Engagement Mode (Admin; Other Roles Read-Only Where Offered)

Record the engagement context, such as evaluation or production where offered. Commercial authorization and environment placement remain separate.

4. Governance Onboarding (Admin; Other Roles Read-Only Where Offered)

Review the governing profile, service binding and required controls. A binding connects the permitted service to its organization and use; an administrator’s visibility does not create one.

5. Ingestion Setup (Admin; Other Roles Read-Only Where Offered)

Choose the supported input method and source. Webhook, API pull, collector, syslog/event feed, document upload and execution callback have different contracts. Use actual source details and authorized credential references; do not assume a configured source is sending data.

Deployment Configuration - Continued

6. Executor / Action Readiness (Admin; Other Roles Read-Only Where Offered)

An executor performs a permitted operation on a target. Review control binding, target restrictions, credential readiness and the offered validation result before allowing actions. A connector install alone is not verified execution.

7. Base-Live & Go (Admin; Other Roles Read-Only Where Offered)

Review the collected readiness and evidence in the final stage. Resolve named blockers through their owning steps. Activation is an authorized operation for the intended environment, not a status the guide can set.

Step By Step

1. Start With Identity And Entitlement (Admin; Other Roles Read-Only Where Offered)

Open Organization & Onboarding > Onboarding Progress and verify the preceding identity and subscription requirements. Then open Deployment Configuration.

2. Record Placement And Runtime Context (Admin; Other Roles Read-Only Where Offered)

Complete Deployment Mode, Runtime Configuration and Engagement Mode in order. Review the saved environment and intended behavior.

3. Bind Governance Before Input And Action (Admin; Other Roles Read-Only Where Offered)

Review Governance Onboarding. Use the authorized service assignment and policy; do not create a commercial grant as a side effect of testing.

4. Configure And Validate Input (Admin; Other Roles Read-Only Where Offered)

Open Ingestion Setup, select the supported method and provide only its required configuration. Store credentials in the owning vault and inspect the real validation result.

Deployment Configuration - Continued

5. Review Action Readiness (Admin; Other Roles Read-Only Where Offered)

Open Executor / Action Readiness. Check the exact target, required authorization and observed test result. Keep unavailable customer connections as unavailable until configured.

6. Review Go-Live Evidence (Admin; Other Roles Read-Only Where Offered)

Open Base-Live & Go, inspect prerequisites and the supported confirmation path. Return to Onboarding Progress and System Health to read the recorded result; preserve local evidence and recovery procedures.

Deployment Configuration - Continued

If Something Goes Wrong

Governance Binding Required

The capability is not connected to an authorized service assignment.

Where To Go: Organization & Onboarding > Ecosystem workspace; Deployment Configuration > Governance Onboarding

Have the authorized owner inspect the existing assignment and binding. Do not bypass licensing or grant new commercial authority to obtain a test result.

Connector Or Ingestion Test Fails

The selected source could not satisfy its own validation contract.

Where To Go: Organization & Onboarding > Deployment Configuration > Ingestion Setup; Admin Settings > CREDENTIAL VAULT

Review the method, source URL and permitted credential reference with the operator. Keep secrets out of screenshots, questions and external support channels.

Go-Live Is Blocked

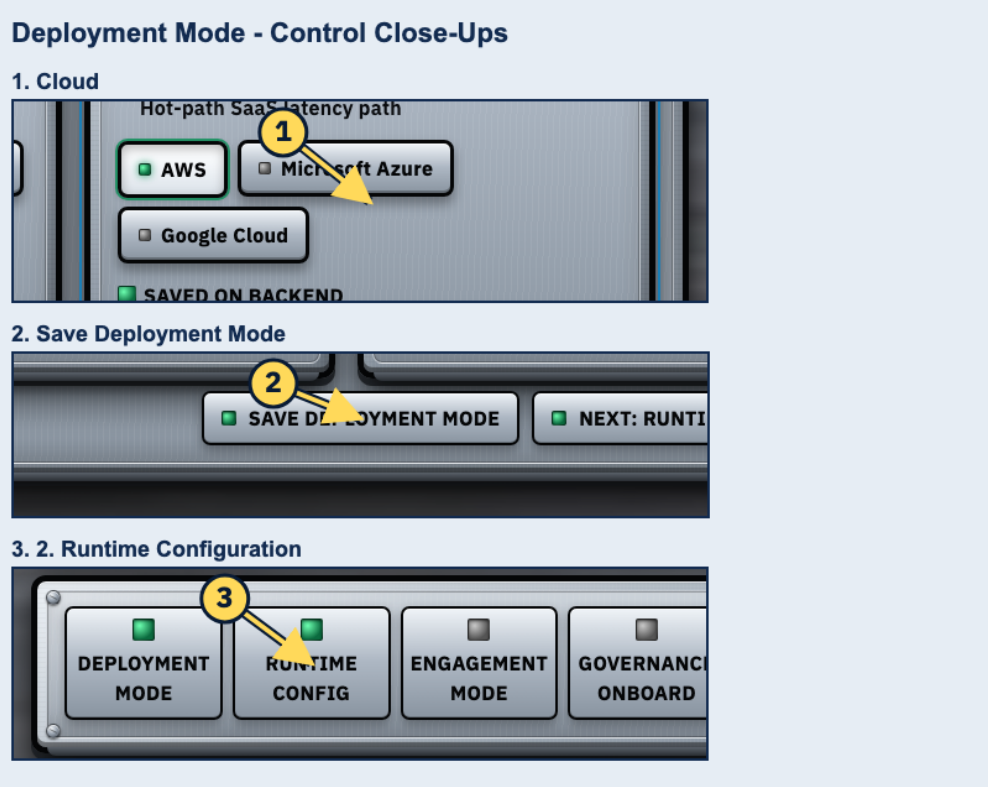
One or more required setup, evidence or authority conditions remain unsatisfied.

Where To Go: Organization & Onboarding > Deployment Configuration > Base-Live & Go

Read each named prerequisite and return to its indicated stage. Do not report deployment success from configuration alone.

Deployment Mode (Admin; Other Roles Read-Only Where Offered)

Isolated Demonstration - Not Your Current Tenant State



1. Cloud

Choose the real deployment model and hosting boundary.

2. Save Deployment Mode

Saves this configuration; does not install or activate a customer environment.

3. 2. Runtime Configuration

Continue in the displayed seven-step order. Review each prerequisite and readiness result.

What Happens

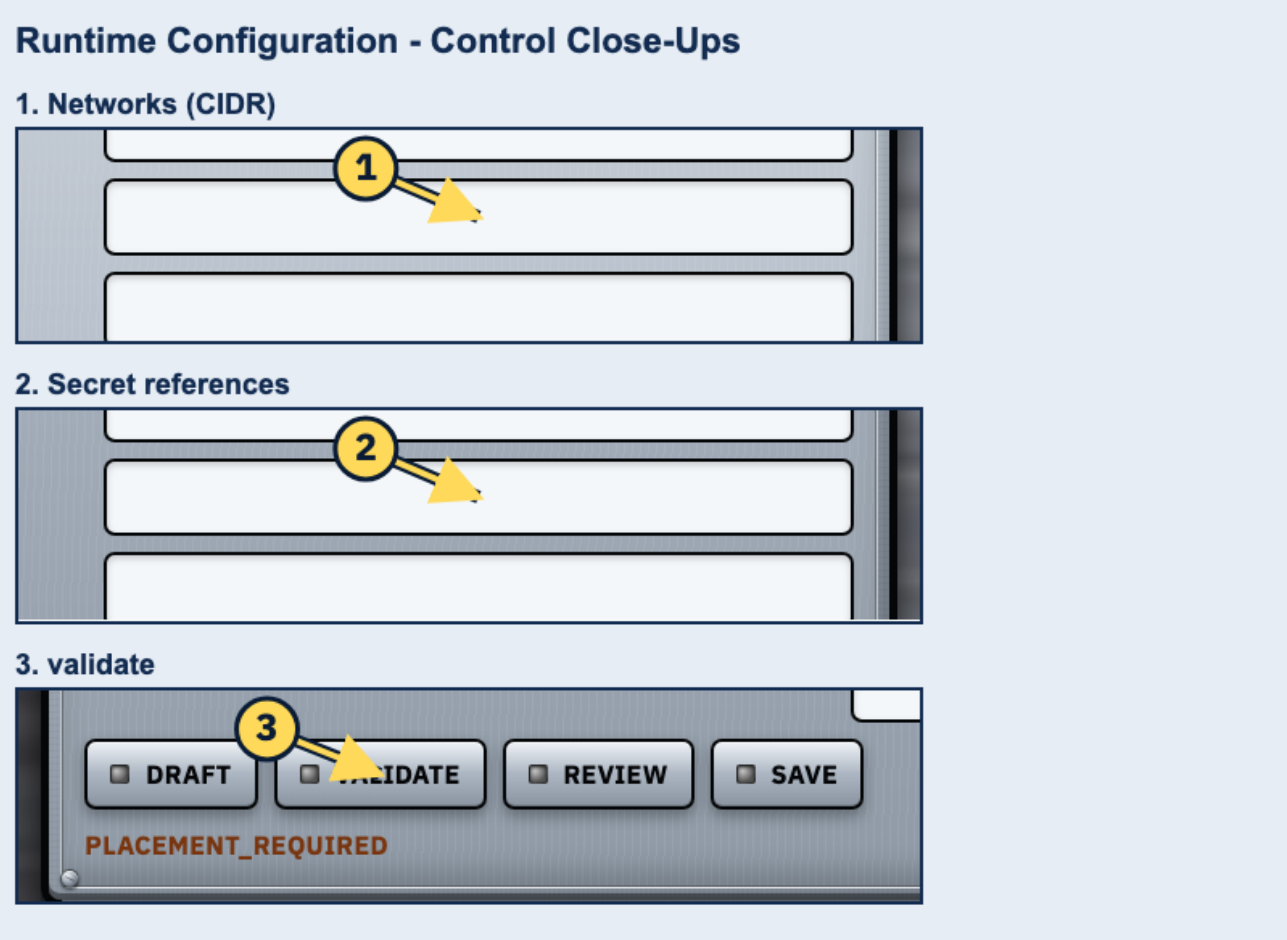
Each configuration or activation control has its own gate. Customer credentials and live transition are not supplied by the guide.

Read First

Do not press deploy, approve, rollback or live-transition controls to learn their meaning.

Runtime Configuration (Admin / Authorized Deployment Operator)

Isolated Demonstration - Not Your Current Tenant State



1. Networks (CIDR)

Use approved network ranges, in CIDR format.
Illustrative Format Only: 10.20.0.0/16 (illustrative only)

2. Secret references

Use stored references, not raw credentials.

3. validate

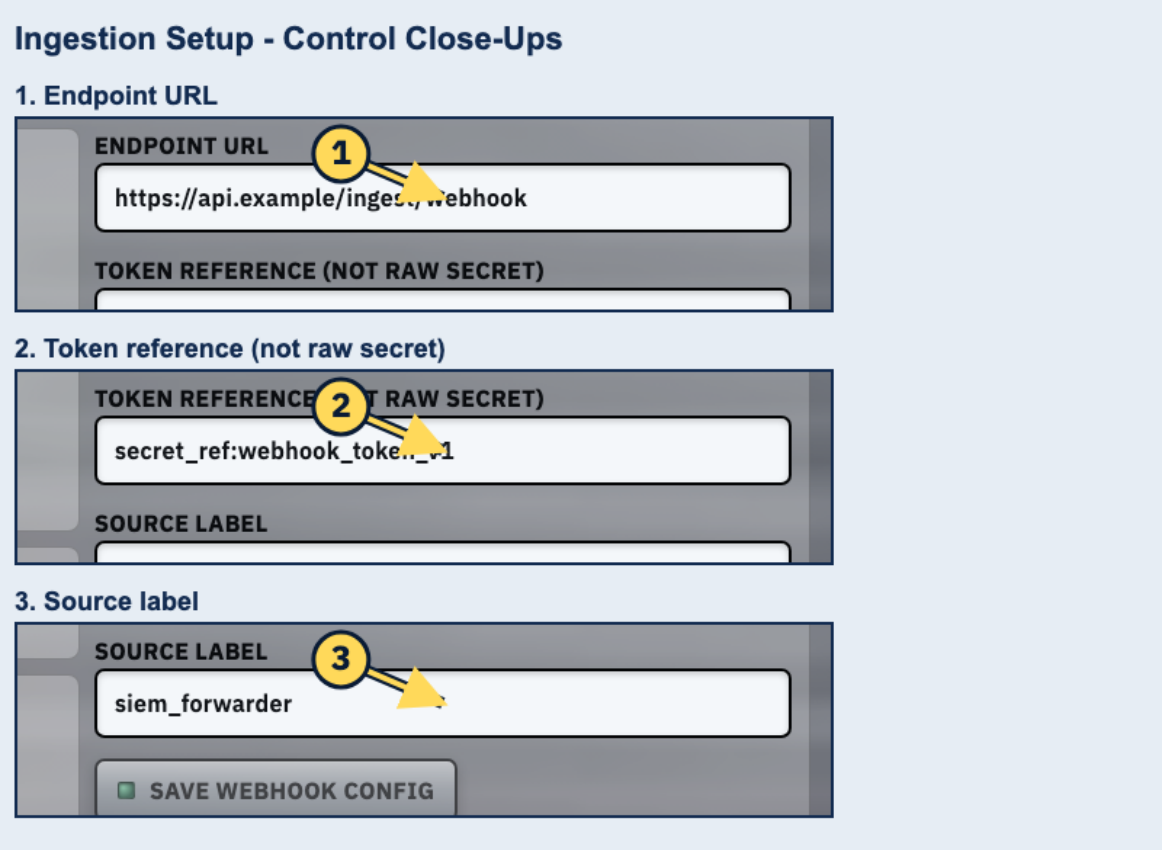
Runs the offered configuration validation; draft and validation are distinct.

What Happens

Validation checks the stored inputs; it does not install infrastructure or authorize live execution.

Ingestion Setup (Admin / Authorized Deployment Operator)

Isolated Demonstration - Not Your Current Tenant State



1. Endpoint URL

Use the approved source endpoint in the supported URL format.
Illustrative Format Only: https://source.example.invalid/... (format only)

2. Token reference (not raw secret)

Use an approved vault reference.

3. Source label

Give the source an identifiable name.
Illustrative Format Only: Corporate Identity Logs (illustrative)

What Happens

Configured ingestion is not proof of delivered telemetry. Check its offered readiness result and source health.

Base-Live & Go (Authorized Deployment Approver / Operator)

Isolated Demonstration - Not Your Current Tenant State



1. Grant approval (reason + expiry required)

Read the scope, reason and expiry before the supported approval.

2. Authorize live transition (feature flag + all proofs required)

Requires the existing feature flag and every proof; this can change operational readiness.

What Happens

These are protected live-transition controls, not tutorial buttons. A waiver cannot be treated as completed proof.

23. Ecosystem Workspace (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Ecosystem Workspace is the control tower for service relationships and bindings that your role is authorized to inspect. A binding connects a permitted service to an organization, environment and lifecycle; it is not merely a connector or catalog entry. This workspace brings together customer lifecycle, responsibility, renewal, commercial health and deployment facts. Its local navigation separates Bindings, Partner fleet and, for internal roles, Internal operations. Use the authorized tenant or partner selector carefully because the displayed facts and available actions belong to that selection, not every customer.

Understand The Screen

Bindings And Authorized Selection (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Select only an organization or partner offered by Authorized tenant or partner. Check Tenant context before inspecting a binding. No assignment means no authorized relationship for this scope; it does not justify entering another customer ID.

Customer Lifecycle And Partner Responsibility (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Read which actor owns the customer relationship and lifecycle operation. A partner assignment and the customer’s runtime entitlement are distinct.

Renewal, Commercial Health And Deployment (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Review recorded tasks, entitlement and commercial health, operational issues and deployment state. A displayed record is not proof that renewal or activation succeeded.

Partner Fleet And Internal Operations (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Partner fleet is a scoped relationship view, not the Partner Portal self-service home. Internal operations is shown only to authorized internal users. Provider operations, offboarding, remote support and cost observations remain governed by their offered controls and recorded evidence.

Ecosystem Workspace - Continued

Step By Step

1. Confirm Authorized Context (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Open Organization & Onboarding > Ecosystem workspace. Select an offered Authorized tenant or partner and read its displayed relationship.

2. Inspect The Relevant Binding (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Review Bindings and the selected service detail. Confirm capability, environment, lifecycle and recorded prerequisites.

3. Review Responsibility And Health (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Read customer lifecycle, partner responsibility, renewal tasks and entitlement/deployment state for this selection.

4. Use Only The Owning Operation (Assigned Customer / Partner Staff; Platform Owner For Internal Operations)

Follow an offered authorized control or link when required. Return to Subscription & Entitlements for commercial state or Deployment Configuration for setup; refresh this workspace afterward.

Ecosystem Workspace - Continued

If Something Goes Wrong

No Assignment

Your current session has no authorized relationship for the selected scope.

Where To Go: Organization & Onboarding > Ecosystem workspace > Authorized tenant or partner

Choose an offered scope or request assignment review through your internal administrator. Do not substitute a foreign tenant ID.

Partial Availability

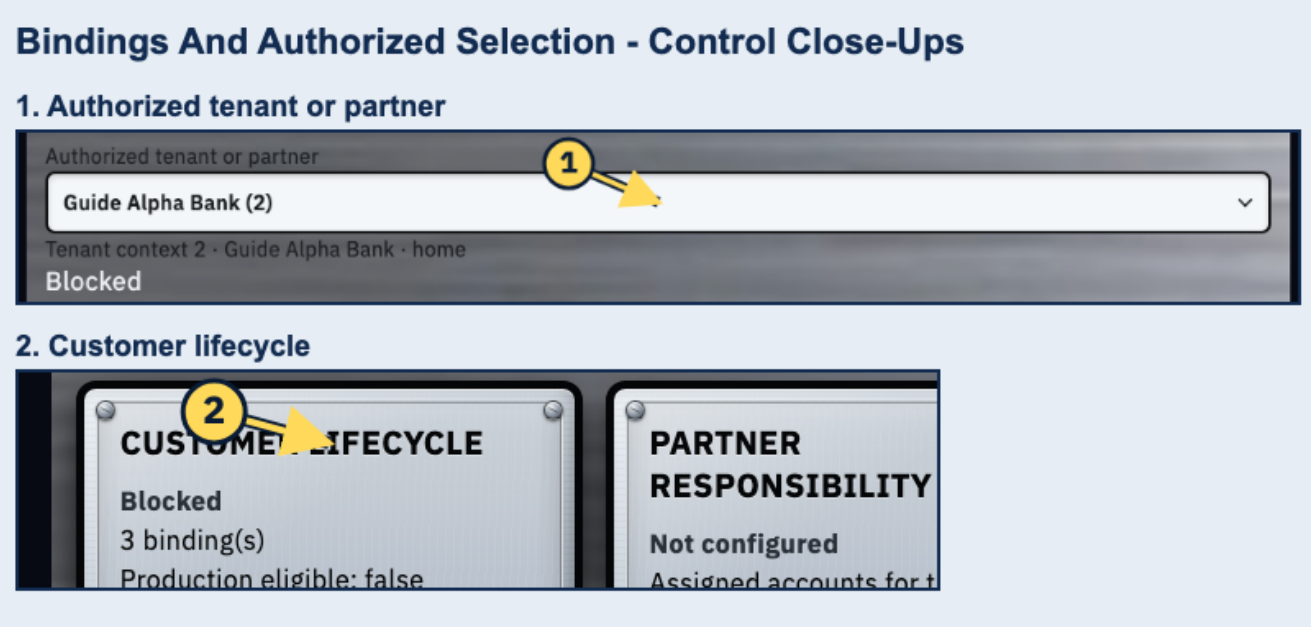
One source in the relationship view could not be read.

Where To Go: Organization & Onboarding > Ecosystem workspace > Recovery actions

Use the offered retry for the affected source and retain its request reference. Do not treat the remaining visible panels as proof that all sources are healthy.

Bindings And Authorized Selection (Assigned Customer / Partner Staff)

Isolated Demonstration - Not Your Current Tenant State



1. Authorized tenant or partner

Select only the assigned customer and installation.

2. Customer lifecycle

Read commercial, enrollment and deployment state without conflating them.

What Happens

The assigned scope and each operation’s permission govern changes; visibility does not create a binding or entitlement.

24. Offline Installation Procedures (Admin; Other Roles Read-Only Where Offered)

An offline installation keeps configuration, licensing and evidence inside the organization's approved boundary. Controlled media is the authorized transfer path when internet access is unavailable or prohibited. Supplier signatures, artifact identity and operator custody must be checked before import or export. Backup and restore are infrastructure procedures owned by a designated operator, not the Guided Assistant. Use the installed package's approved commands and retain original receipts and recovery references.

Understand The Screen

Internal Responsibility (Admin; Other Roles Read-Only Where Offered)

The designated infrastructure operator owns backup, restore and custody. The reporting operator owns evidence scope and classification. Only the authorized issuer signs production licenses; runtime administration does not create manufacturer authority.

Step By Step

1. Import Through Controlled Media (Admin; Other Roles Read-Only Where Offered)

Use only media and transfer stations approved by your organization. Before import, the designated operator checks the supplier signature, file digest, intended installation and release, and records custody. Use the product's existing import or apply workflow; reject altered, unexpected or expired artifacts. Never disable signature checks to make an import pass.

2. Export Inside The Approved Boundary (Admin; Other Roles Read-Only Where Offered)

Select only the required evidence and review its contents for secrets and sensitive data. Use approved bank-local storage or controlled media, record the recipient and custody, and retain the verification receipt. Do not upload customer data to an internet service or external support channel.

Offline Installation Procedures - Continued

3. Back Up Locally (Admin; Other Roles Read-Only Where Offered)

Your designated infrastructure operator uses the deployment's approved local backup procedure for the database, evidence and required configuration. Record the backup time and integrity reference, protect access and retain it according to policy. The guide does not create a backup or claim one exists.

4. Restore With The Authorized Operator (Admin; Other Roles Read-Only Where Offered)

Confirm the exact installation, approved backup, integrity and recovery authorization. Follow the installed deployment's local restore procedure, then verify sign-in, tenant scope, recorded runtime and evidence. Do not reset evaluation clocks, entitlements or audit custody to obtain a working screen.

5. Apply An Offline License (Admin; Other Roles Read-Only Where Offered)

Review the signed artifact's customer, installation, image or release binding and validity. Use the existing Subscription & Entitlements apply workflow with the required role. Check the resulting entitlement and retain its receipt. The manufacturer private key remains outside the customer runtime.

6. Retrieve Incident Evidence (Admin; Other Roles Read-Only Where Offered)

Select the incident, mission or decision and check its organization and recorded time. Use Evidence & Reporting with an authorized role. Keep the original record and verification references under retention or legal hold; missing evidence stays missing, and an export is not proof that an action succeeded.

If Something Goes Wrong

Verification Or Import Fails

The artifact or its intended installation does not satisfy the check.

Where To Go: Organization & Onboarding > Subscription & Entitlements / Deployment Configuration; Evidence & Reporting > Export History

Retain the rejection and compare the original signed input, installation, trust file and custody checkpoint with the approved procedure. Do not reset clocks, edit signatures or waive verification.