

AI Clearance Sample Evidence Pack

Post-approval failure: an approved AI access grant expired, review-before-expiry did not confirm continued need, and the configured Okta group still observed the user as a member. Governance Logs continuity checks pass over the retained sample audit events.

Sample - synthetic data

This is not generic marketing copy. It is a synthetic buyer-facing pack modeled on current AI Clearance outputs: Requests and request history, grant expiry, configured-group membership checks, policy evidence JSON, request CSV export, Governance Logs JSONL, and audit-chain verification metadata.

Honesty Key

Category	What it means in this pack
Product output today	AI Clearance has Requests, request history CSV export, Governance Logs, audit JSONL export, policy evidence JSON export, configured-group checks, and audit-chain verification metadata.
Sample synthetic data	Every identity, request key, policy label, group ID, timestamp, and hash value in this public pack is synthetic sample data.
Design-partner deliverable	A buyer-specific PDF narrative and evidence-pack workflow can be stood up around one real AI access process during an 8-week design-partner sprint.

Pack ID	AIC-SAMPLE-EVIDENCE-2026-06-10	Generated	2026-06-10T02:30:00Z
Scenario	Expired grant + configured-group mismatch	Continuity	Pass over retained sample events

Executive Summary

The approval record is not the control failure. The failure appears after approval: the grant reached expiry, continued need was not confirmed before expiry, and a connected-mode check still observed the user inside the configured Okta group.

Reviewer question	Evidence in this sample	State
Who requested access and why?	AIC-1042: Dana Morris requested ChatGPT Enterprise for internal engineering research.	Available
Who approved it and under what policy?	Mira Patel approved under AIC-POL-03 v7 with medium risk and a 30-day duration.	Available
Did the grant expire?	Grant expired on 2026-06-01T18:05:09Z.	Expired
Was continued need re-reviewed?	Review-before-expiry issue AIC-1088 opened. No continued-need confirmation before expiry in this sample.	Open - not confirmed before expiry
Does configured-group membership match?	Expected not_member after expiry; observed member in configured Okta group.	Mismatch
Can the audit trail be checked?	Governance Logs include prevHash, entryHash, entryMac, SHA-256, keyId, sequence, and verification summary.	Continuity pass

Boundary: this sample checks the configured Okta group only. AI Clearance does not prove provider-side app use, inspect AI prompts, assign licenses or roles by itself, replace IAM/IGA, or independently notarize audit events.

Request and Approval Evidence

This section mirrors the current request history and request detail surfaces: requester, tool, purpose, data classes, decision, policy context, grant status, and expiry.

Field	Sample value
JSM issue	AIC-1042
Requester	Dana Morris, Product Engineering
AI tool	ChatGPT Enterprise
Purpose	Approved internal engineering research. Production secrets prohibited.
Requested duration	30 days
Data classes	internal_docs; source_code_review_context
Decision	approved
Approver	Mira Patel, Security Engineering
Decision time	2026-05-01T18:03:44Z
Policy context	AIC-POL-03 v7; medium risk; manager/security approval required.

Product output today: Request history exports as CSV with requester, approver, decision, grant, expiry, lifecycle summary, and issue URL fields. The public CSV included beside this PDF adds one public sample-notice column.

Grant Lifecycle and Configured-Group Evidence

Lifecycle item	Sample state
Grant ID	grant_aic_sample_1042_chatgpt
Grant status	expired
Granted at	2026-05-01T18:05:09Z
Expires at	2026-06-01T18:05:09Z
Review-before-expiry	AIC-1088 opened on 2026-05-25; no continued-need confirmation before expiry.
Configured connector	Okta group connected mode; connectorId okta-group-chatgpt-enterprise.
Expected state after expiry	not_member
Observed state on 2026-06-03	member
Result	Configured-group mismatch; removal or exception follow-up required.

Follow-up	Sample value
Remediation / exception issue	AIC-1091
Owner	Security Engineering with IAM Operations
Due date	2026-06-05
Status	Open - access removal not confirmed after expiry.

Truth check: current AI Clearance product output can record expectedState, observedState, status, connector metadata, and post-expiry verification for configured-group checks. This sample row is Product output today when connected mode is configured; it remains bounded to the configured group.

Safe claim	Caveat
AI Clearance can record request, approval, grant, expiry, recertification/review-before-expiry, manual fulfillment, exception, and configured-group evidence where product output supports it.	The configured group must be the actual control boundary for the app, license, role, or resource.
Connected mode can add, remove, or check configured Okta/Entra group membership when configured.	This is not broad provider drift detection and not runtime AI monitoring.
Governance Logs carry hash-chain continuity metadata.	This is retained-event continuity checking, not an immutable ledger or independent notarization.

Product Surface: Requests

The Requests admin surface is where pending approvals, connector follow-up, request history, grant status, expiry, and CSV export come together. Screenshot is generated from current product terminology with synthetic scenario data.

Search

+ Create

Sample - synthetic data

AI Clearance

AI Clearance

Jira admin

Navigation

Overview

Intake & Approvals

Catalog

Connectors

Governance

Requests

Insights

Governance Logs

Requests

Refresh

Export CSV

Operate the configured AIC intake: pending reviews, connector follow-up, and request history for one AI access workflow.

Pending approvals

No pending approvals for the AIC sample intake.

Access follow-up

Approved requests usually become active immediately. Items appear here when a connector or access-removal step still needs an admin.

AIC-1042

ChatGPT Enterprise

REMOVAL PENDING

Retry sync

Mark removed

Record exception

Requester Dana Morris

Configured group mismatch: expected not_member, observed member.

Request history

Search the configured AIC intake by decision, date range, or Jira issue key.

All decisions

AIC-1042

Apply filters

Clear filters

Issue	Requester	Tool	Submitted	Decision	Grant	Expiry
AIC-1042	Dana Morris	ChatGPT Enterprise	2026-05-01	APPROVED	EXPIRED	2026-06-01
AIC-1038	Evan Brooks	GitHub Copilot Business	2026-05-27	APPROVED	ACTIVE	2026-06-26

Current terminology reflected here: Requests, request history, Export CSV, Grant, Expiry, pending approvals, and access follow-up.

Sample - synthetic data. Not a customer record, not legal advice, not runtime AI monitoring, not an IAM/IGA replacement.

https://ardsaor.com/apps/ai-clearance/ | andrew@ardsaor.com | Request teardown: https://ardsaor.com/apps/ai-clearance/#book-teardown

Page 5

Product Surface: Governance Logs

Governance Logs expose the audit stream and verification/export controls. The synthetic screenshot shows the same six-event AIC-1042 scenario after verification has been run.

Search

+ Create

Sample - synthetic data

AI Clearance

AI Clearance

Jira admin

Navigation

Overview

Landing page with launch status...

Intake & Approvals

Portal intake, routing, SLA...

Catalog

Requestable AI tools and approval...

Connectors

Okta and Entra connector setup...

Governance

Policies, approval defaults...

Requests

Pending approvals, manual action...

Insights

Aggregated adoption visibility...

Governance Logs

Chronological audit explorer...

Governance Logs

Inspect audit events for the configured AIC intake, export evidence, and verify the audit chain.

Verify audit chain

Export audit JSONL

Export evidence pack ZIP

Export policy evidence JSON

Latest sequence

6

Recent event count

6

Last verification

Pass - 2026-06-10 02:30 UTC

Governance log explorer

Filter the AIC sample audit stream by action, request, grant, or date range.

Timestamp	Seq	Action	Actor	Integrity	Request
2026-06-03 15:21	6	connector_membership_checked	Reviewer	CHAINED	AIC-1042
2026-06-01 18:06	5	grant_expired	App	CHAINED	AIC-1042
2026-05-01 18:07	4	connector_membership_checked	App	CHAINED	AIC-1042
2026-05-01 18:05	3	grant_created	App	CHAINED	AIC-1042
2026-05-01 18:03	2	request_approved	Approver	CHAINED	AIC-1042
2026-05-01 16:42	1	request_created	App	CHAINED	AIC-1042

Current terminology reflected here: Governance Logs, Verify audit chain, Export audit JSONL, Export evidence pack, sequence, action, integrity, and event detail chain fields.

Sample - synthetic data. Not a customer record, not legal advice, not runtime AI monitoring, not an IAM/IGA replacement.
https://ardsaor.com/apps/ai-clearance/ | andrew@ardsaor.com | Request teardown: https://ardsaor.com/apps/ai-clearance/#book-teardown

Page 6

Governance Logs Export Excerpt

The public JSONL sample contains the six synthetic AIC-1042 scenario events shown on the prior page, with full prevHash, entryHash, and entryMac values. This PDF shortens digests for readability.

Seq	Action	Integrity	prevHash	entryHash
1	request_created	chained	GENESIS	4babbf9ea2ba
2	request_approved	chained	4babbf9ea2ba	7b1ee3b7a7f1
3	grant_created	chained	7b1ee3b7a7f1	5bdd99ebd5f6
4	connector_membership_checked	chained	5bdd99ebd5f6	e7daec11b25a
5	grant_expired	chained	e7daec11b25a	c3e12c8bdfb3
6	connector_membership_checked	chained	c3e12c8bdfb3	16f2e726b728

Verification Summary

Check	Sample result
Continuity	Pass: every prevHash matches the prior entryHash over retained sample events.
Entry hash	Pass: SHA-256 over the canonicalized event core.
Entry MAC	Pass: entryMac is HMAC-SHA-256 over entryHash using keyId v1 in this synthetic sample.
Entry count	6
Finding caveat	Business finding remains open: expected not_member, observed member after grant expiry.
Retention caveat	Verification covers retained chained audit events only.

Download Bundle

Artifact	Why a buyer would inspect it
Sample evidence pack PDF	Human-readable buyer artifact tying request, approval, expiry, mismatch, and Governance Logs continuity together.
Governance Logs JSONL	Machine-readable audit events with sequence, action, prevHash, entryHash, entryMac, hashAlgorithm, keyId, and integrityState.
Request/grant CSV	Current request history export shape with grant status, expiry, lifecycle summary, and issue URL.
Audit-chain verification summary JSON	Continuity check result and retained-event caveats.
Policy evidence JSON	Current product evidence-pack export shape: catalog, decision history, lifecycleEvidence, manual attestations, and audit summary.
Product screenshots ZIP	Product-surface screenshots generated from current AI Clearance terminology and synthetic scenario data, stamped as synthetic.

Design-Partner Ask

Offer: CA\$20k, 8 weeks, 3 slots. Outcome: stand AI Clearance up around one real AI access process, verify the Okta/Entra configured-group boundary or document the manual path, and produce the buyer's evidence pack around their actual audit question.

Next step: <https://ardsaor.com/apps/ai-clearance/> | Email: andrew@ardsaor.com | Request a 20-minute teardown: <https://ardsaor.com/apps/ai-clearance/#book-teardown>

Week	Design-partner output
1-2	Map one current JSM AI access workflow, request fields, approval policy, and identity-provider group boundary.
3-4	Configure catalog, policy context, expiry/review-before-expiry, and connected or manual fulfillment evidence path.
5-6	Run real request/grant/expiry/review scenarios and export Governance Logs, request history, and policy evidence JSON.
7-8	Assemble buyer-specific evidence pack, verify chain continuity, document caveats, and decide pilot/production next step.