INTEGRATION GUIDE

Jira Integration

SHADOW AI
DISCOVERY · SECSTUDIO

Set up automatic Jira ticketing for critical & high AI-security findings — Shadow AI Discovery & SecStudio.

1 · What this integration does

When enabled, every new **critical** and **high** finding automatically opens a Jira issue with its fields pre-filled, so your engineers work security findings inside the tracker they already use. The issue is created once per finding (deduplicated), and it transitions to **Done** automatically when you resolve the finding in the dashboard. Analysts can also raise a ticket on demand from any finding.

> **Two products, one flow.** The same behaviour applies to **Shadow AI Discovery** (risks) and **SecStudio** (findings). Configuration is per-organization and set from the product's **Integrations** tab.

2 · Prerequisites

- A Jira Cloud site (`https://your-org.atlassian.net`) or Jira Server/Data Center.
- A Jira account to act as the automation identity — ideally a dedicated service account, not a person.
- Permission for that account to **create issues** (and transition them) in the target project.
- An **API token** for that account.

3 · What you'll need to collect

FIELD	WHERE TO FIND IT	EXAMPLE
Base URL	Your Jira site address	`https://acme.atlassian.net`
Account email	The automation account's login email	`ai-security@acme.com`
API token	id.atlassian.com → Security → **Create and manage API tokens**	`ATATT3xFf…`
Project key	The short key of the target project	`SEC`
Issue type	An issue type that exists in that project	`Task` or `Bug`
Default assignee	The project lead. Jira Cloud = **accountId**; Server/DC = username	`5f8a…c2`

To find an **accountId** on Jira Cloud, open the person's profile — the URL ends in their accountId — or call `/rest/api/3/user/search?query=name` .

4 · How to configure — in the dashboard (recommended)

STEP 1 Sign in as an `org-admin` and open `Integrations` in the left nav.

STEP 2 In the **Jira** card, fill in Base URL, Account email, API token, Project key, Issue type, and the Default assignee (your project lead).

STEP 3 Tick **Create Jira tickets** and click **Save**. Your API token is encrypted at rest — it is never shown again (only a masked placeholder).

STEP 4 Click **Create test ticket**. A ticket titled *"[Shadow AI] Test alert"* should appear in your project within a few seconds, and the button shows the new issue key.

5 · How to configure — self-hosted (environment)

If you self-host and prefer secrets in your secrets manager instead of the app, set these and restart. Dashboard config takes precedence when its toggle is on; otherwise the environment is used.

```
SHADOW_AI_JIRA_URL=https://acme.atlassian.net
SHADOW_AI_JIRA_EMAIL=ai-security@acme.com
SHADOW_AI_JIRA_TOKEN=ATATT3xFf...
SHADOW_AI_JIRA_PROJECT=SEC
SHADOW_AI_JIRA_ISSUETYPE=Task
SHADOW_AI_JIRA_ASSIGNEE=<accountId>            # optional
SHADOW_AI_JIRA_DONE_TRANSITION=31              # transition id → Done (optional)
SHADOW_AI_JIRA_REOPEN_TRANSITION=11            # transition id → reopen (optional)
```

For **SecStudio**, the same variables are prefixed `SECSTUDIO_JIRA_*`.

Transition IDs come from `GET /rest/api/2/issue/<KEY>/transitions` on any ticket in the project.

6 · What gets created — field mapping

Each finding is translated into a Jira issue as follows:

JIRA FIELD	POPULATED FROM
Project / Issue type	Your configured project key + issue type
Summary	`[Shadow AI] <finding title>`
Description	What/why, severity + risk score, affected assets, remediation steps, compliance controls (NIST AI RMF / OWASP LLM / ISO 42001 / EU AI Act), references
Priority	critical→Highest · high→High · medium→Medium · low→Low
Labels	`shadow-ai`, `sev-<severity>`, the risk class, and the OWASP id (e.g. `LLM02`)
Assignee	Your default assignee (the project lead), if set — otherwise left for triage

The description footer prompts your team to add project-specific fields (components, epic link, sprint). If your project rejects the priority or assignee field (common in team-managed projects), SecStudio retries automatically without them so the ticket is still created.

7 · Auto-close on resolution

When you set a finding to **Resolved / Closed / Mitigated / False-positive** in the dashboard, the linked Jira issue is transitioned to **Done** using `*_DONE_TRANSITION`. If a finding recurs, it can be reopened via `*_REOPEN_TRANSITION`. Leave these unset to manage the ticket lifecycle manually.

8 · Scope, limits & security

> **Least privilege.** Use a dedicated service account with create/transition rights on one project only — not an admin.

> **Secret handling.** The API token you enter is encrypted at rest with a key held in the deployment secret; it is never returned to the browser and never written to logs. Rotate it from id.atlassian.com and re-save at any time.

- Only **critical** and **high** findings auto-create tickets; medium/low do not (raise those manually if needed).
- One ticket per finding (deduplicated) — re-running a scan will not spam duplicates.
- No finding data leaves your environment except the ticket you send to your own Jira site.

9 · Troubleshooting

SYMPTOM	FIX
Test says `401 / 403`	Wrong email/token, or the account lacks create-issue permission on the project.
`400 … issuetype`	The issue type name doesn't exist in that project — use one that does (e.g. Task).
Ticket created but unassigned	On Jira Cloud the assignee must be an **accountId**, not a username/email.
No auto-close	Set the correct `DONE_TRANSITION` id for your project's workflow.