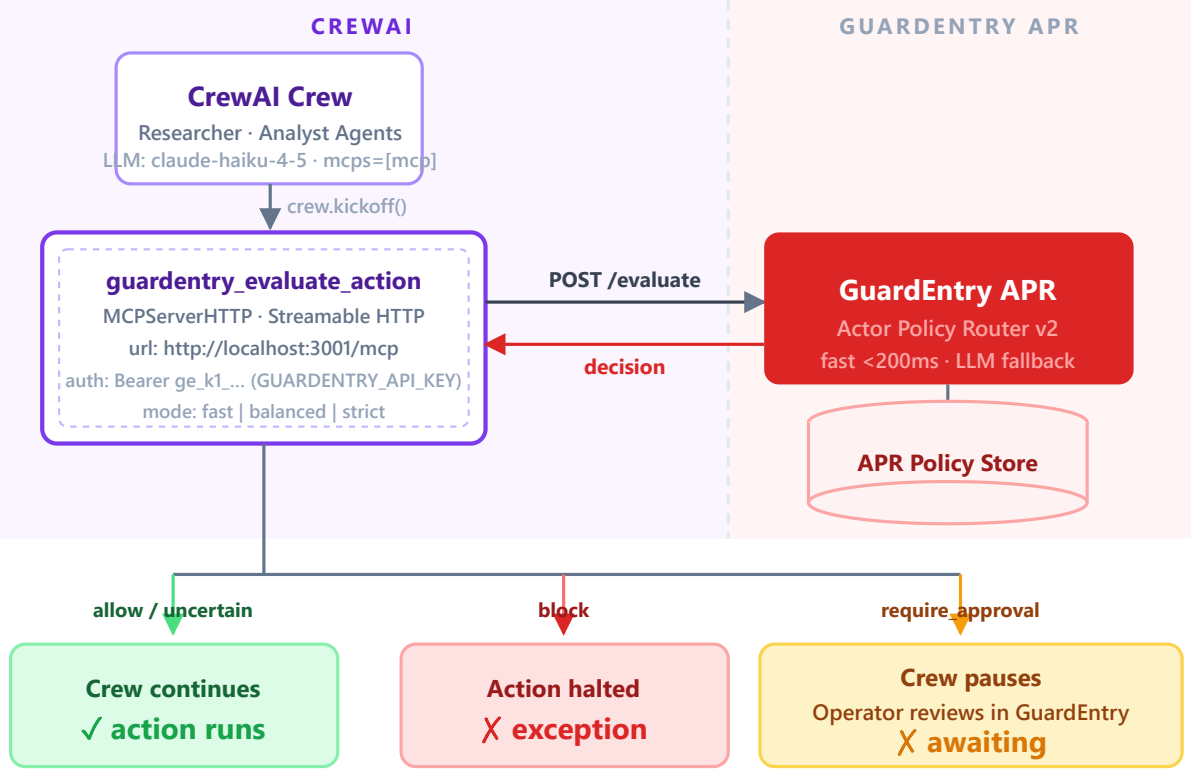
GuardEntry × CrewAI

GuardEntry APR via MCP — Integration Architecture Overview

GuardEntry MCP Server v0.2.0
CrewAI · MCPServerHTTP · Streamable HTTP
guardentry.ai · 2026-06-14

Connect CrewAI crews to **GuardEntry's Agent Policy Router** via MCP. Every action your agents propose — research queries, write operations, external API calls — is evaluated against your compliance policy before it executes. Blocked actions are logged with full reasoning, confidence score, and a deep-link audit record.



HOW IT WORKS

1. **Clone and start the MCP server.** The GuardEntry MCP server exposes `guardentry_evaluate_action` over Streamable HTTP. Set `MCP_TOOLS=guardentry_evaluate_action` to stay under Anthropic's tool-schema limit when using Claude as the CrewAI LLM.
2. **Connect agents via MCPServerHTTP.** Add the MCP server to each agent's `mcps` parameter. Auth uses a scoped API key (`ge_k1_...`) in the `Authorization: Bearer` header.
3. **APR evaluates against policies.** `fast` mode applies regex/substring rules in <200 ms. `balanced` / `strict` add LLM-assisted reasoning — for detecting data-exfiltration intents, SOC 2 / ISO 27001 control gaps, and change-window violations.
4. **Crew acts on the decision.** `allow` → agent continues. `block` → exception raised, task halted. `require_approval` → crew pauses; operator reviews in GuardEntry dashboard before re-ordering.

QUICK START

```
git clone https://github.com/guardentryai/mcp-server.git
cd mcp-server && npm install
MCP_TOOLS=guardentry_evaluate_action \
  GUARDENTRY_API_KEY=ge_k1_... npm run start:http
```

DECISION OUTCOMES

DECISION	CREW BEHAVIOR
allow	Agent action proceeds normally
block	Exception raised · task halted · logged with reasoning
require_approval	Crew pauses · operator reviews in GuardEntry
uncertain / verify	Proceeds · logged for review
unreachable	Fails open — MCP server outage won't block your crew

KEY PARAMETERS

PARAMETER	NOTES
`subject_content`	Action text to evaluate (required)
`subject_type`	task | tool_argument | prompt | plan | tool_result
`agent_id`	Agent UUID — appears in audit log

PARAMETER	NOTES
`mode`	fast | balanced | strict — default: balanced
`correlation_id`	Thread ID linking ingress + egress decisions