SHOMAR SECURITY PLATFORM

MCP Agent Operations Guide

Controlled agent automation for reporting, remediation, compliance, procurement, and enterprise operations.

Document Control
Audience: Bank admins, security teams, compliance teams, audit teams, developers, and approved agent operators
Classification: Customer-facing technical guide
Generated: August 01, 2026
Website: https://shomar.io
Application: https://app.shomar.io

Shomar is a security and compliance evidence platform for regulated Nigerian and African teams. It combines security scanning, findings operations, compliance evidence, customer-controlled scanning, and auditor-ready reporting in one operating workspace.

Contents

1. Purpose and Operating Model

Shomar exposes an MCP-compatible JSON-RPC endpoint for controlled security, compliance, reporting, remediation, procurement, and enterprise operations.

The MCP surface is intentionally narrower than raw product APIs. Every call is authenticated, tenant-scoped, scope-checked, RBAC-checked, constrained by API-key policy, and written to the agent invocation ledger.

Control	How it works	Outcome
Tenant isolation	Organization ID is required and enforced on every tool call.	Agents cannot cross customer boundaries.
Scoped API keys	Keys carry explicit scopes such as mcp:invoke, enterprise:read, reports:read, and playbooks:execute.	Each agent receives only the reach it needs.
Policy constraints	Allowed tools, projects, scan types, report types, daily side-effect limits, and read-only mode can be set per key.	Keys remain useful without becoming broad admin credentials.
Approvals	Side-effect tools can create approval requests instead of executing immediately.	Automation stays governed.
Audit ledger	Arguments are redacted, results are summarized, and invocations are logged.	Security and audit teams can reconstruct agent activity.

2. Enterprise MCP Tool Catalog

Enterprise tools give approved agents visibility into Shomar's operating posture and the ability to perform controlled enterprise operations.

Tool	Purpose	Side effect
enterprise.status_get	Read queues, quotas, SLA, connectors, evidence vault, and readiness controls.	No
enterprise.capacity_simulate	Model multi-tenant scan demand against live policy and worker pools.	No
enterprise.policy_simulate	Preview scope and constraint decisions before a key is shared.	No
enterprise.evidence_verify	Verify checksum and signature integrity for evidence-vault records.	No
enterprise.autoscale_recommend	Recommend worker-pool scaling from queue depth and saturation.	No
enterprise.connector_health	Check ticketing, SIEM, source-control, productivity, and evidence connector readiness.	No
enterprise.attestation_generate	Generate a signed attestation manifest for audit, regulator, or procurement use.	Yes
enterprise.siem_export	Export or dry-run a security/compliance event to SIEM.	Yes
enterprise.ticket_sync	Sync queued downstream tickets to configured connectors.	Yes
enterprise.dr_drill_run	Record DR drill proof with RPO/RTO and evidence checks.	Yes
enterprise.controls_update	Update enterprise operating controls. Approval required by default.	Yes

3. Agent Playbooks

Playbooks package common bank workflows into structured plans and optional controlled actions.

Playbook	Primary owner	Output
Triage all critical findings	Security lead	Finding list, project breakdown, task and retest sequence.
Prepare bank audit pack	Compliance lead	Auditor/regulator summaries, evidence context, attestation next action.
Close this compliance gap	Compliance officer	Gap evidence checklist and optional controlled update.
Generate remediation sprint	Engineering manager	Sprint plan and optional remediation tasks.
Retest fixed vulnerabilities	Security engineer	Retest candidates and optional targeted retests.
Prepare vendor procurement response	Procurement/compliance	VSQ, DPA checklist, evidence context, enterprise posture.
Summarize customer security posture	CISO or account team	Executive summary across findings, compliance, evidence, and capacity.

4. Smoke and Regression Checks

Production smoke checks should validate initialize, tool discovery, required enterprise/playbook tools, status, capacity simulation, policy simulation, connector health, and a customer posture playbook.

```
python scripts/production/mcp_enterprise_smoke.py --api-url https://app.shomar.io --token <enterprise_mcp_key>
```

Safety default
Run playbooks in dry-run mode first. Side-effect service-account actions should create approval requests unless an approved human operator executes them directly.