MCP SERVER | NO CODE | CLOUD HOSTED

Bitwarden MCP for AI Agents

Audit organizational collections, user groups, and access policies.

Bitwarden connects your organization's security posture directly to your AI agent. Instead of clicking through multiple web portals for compliance checks, you can ask natural questions about who has access to what, review security policies, and audit every change that happened in the vault. It gives security teams immediate visibility into collections, user groups, member status, and detailed event logs.

A+ Quality Score 100/100

password-manager | vault-management | audit-logs | identity-management | security-audit

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/bitwarden

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

Bitwarden MCP

5 tools available
Cloud-hosted on Vinkius

Need to keep up with organizational security? This MCP lets your AI agent talk directly to your Bitwarden organization data. You bypass the complex web interface entirely. Instead of manually navigating pages to audit who can access what or checking policy compliance against a checklist, you just ask your agent a question. For example, you can instantly get a list of all groups and see which users belong to them. Your AI client handles everything else, pulling detailed event logs to show exactly when an admin changed a setting or when a collection was created. Because Vinkius hosts this MCP, you connect once to your preferred AI agent—whether it's Claude, Cursor, or another compatible client—and gain full visibility across all those critical security resources.

Core Capabilities

01 — Audit organization collections

The agent reads and lists every collection in the vault to show how shared items are organized.

02 — Review administrative event logs

You pull detailed records of security activity, letting you monitor who did what and when within the organization.

03 — Verify user membership status

The agent compiles a list of all organizational members to check seat utilization and current access rights.

04 — Manage team-based group permissions

You query the system for user groups, allowing you to understand team-level access controls quickly.

05 — Check active security policies

The agent inspects current organizational policies to ensure they meet established compliance standards.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/bitwarden** — connect your AI agent in three steps.

01 Subscribe to this MCP and provide your Bitwarden Client ID and Secret credentials.

02 Connect the service to your AI client, giving it permission to access your organization's data.

03 Ask your agent a natural language question, like 'Show me all policy changes last week,' and get an instant report.

The bottom line is you skip the dashboard navigation and talk directly to your security infrastructure.

Built For

This MCP is essential for Security Administrators, IT Operations teams, and Compliance Officers. If manual auditing of access logs or policy adherence feels like a full-time job, this tool cuts through the clicks and delivers answers instantly.

Security Administrator

You use it to quickly audit event logs and verify that security policies haven't been bypassed by checking every active policy.

IT Operations Engineer

You manage user groups and organization members directly from automation workflows, tracking access without logging into the web vault.

Compliance Officer

You retrieve collections and access structures for security reporting, guaranteeing you have a complete audit trail for regulators.

What Changes When You Connect

01 Stop manually sifting through dashboards. Instead of checking multiple tabs to verify member status or group assignments, you ask your agent to list members and groups in one query.

02 Never miss a compliance flag again. By running the 'list_policies' tool via your AI client, you ensure every security standard is documented and visible for audit reporting.

03 Drastically cut down investigation time. Using 'list_events' lets you instantly pull detailed activity logs to trace back exactly who made a policy change or accessed sensitive data.

04 Gain full visibility into data sharing. Running 'list_collections' shows precisely how your vault items are grouped and shared across teams, preventing accidental exposure.

05 Automate access control checks. You can use the tools to verify both group permissions ('list_groups') and individual user seats ('list_members'), making IT cleanup faster.

Real-World Applications

Investigating a Data Leak Incident

A team member reports suspicious activity. Instead of spending hours digging through logs, you ask your agent to run 'list_events' and immediately see all recent administrative actions related to the compromised collection.

Annual Compliance Audit Prep

The compliance officer needs proof that all required security policies are in place. You use the MCP to check every active policy via 'list_policies' and generate a report showing adherence across groups and members.

Onboarding New Department Staff

When a new department starts, you need to ensure their access is minimal. You use the MCP to list all current groups ('list_groups') and check user membership ('list_members') before granting any elevated permissions.

Restructuring Shared Data Sets

The company merges two divisions, requiring a review of shared data. You use 'list_collections' to map out all current collections and then audit them against the policies ('list_policies') before moving items.

Patterns to Avoid

Only checking membership counts

✗ AVOID

A junior admin only runs a list of users to see 'how many people are in Bitwarden.' This gives zero insight into actual risk or access structure.

✓ INSTEAD

Don't just count users. Use the MCP to cross-reference members with groups ('list_members' and 'list_groups') AND check their associated policies ('list_policies') for a complete risk profile.

Relying on web UI logs

✗ AVOID

The team spends hours navigating the Bitwarden web vault to manually compile an audit report of policy changes, missing crucial context.

✓ INSTEAD

Let your agent use 'list_events' directly. You get a structured, chronological feed of every security action taken, making reporting immediate.

Assuming collections are organized

✗ AVOID

A team assumes all shared data is in the main vault collection without verifying how it's actually segmented or protected.

✓ INSTEAD

Always start by running 'list_collections'. This maps out every distinct, shareable resource group, ensuring you audit the right boundaries.

The Right Fit

Use this MCP if your workflow requires continuous security auditing and deep visibility into organizational access structures. If you need to confirm who can see what, or prove compliance by tracing actions back to a specific policy, this is for you. Don't use it if you simply need to generate a list of passwords or manage individual credentials; those tools handle the core vault function. Instead, focus on using its auditing capabilities like 'list_events' and 'list_policies' to prove governance over your data.

Bitwarden MCP for AI Agents: Simplifying Security Audits

Today, an audit is a nightmare of clicks. You jump between user management panels and event logs, copy-pasting names and timestamps into spreadsheets just to prove who had access on a given date. It’s tedious, slow, and highly prone to human error.

With this MCP, you ask your agent for the report. The system gathers all necessary data—from checking group assignments through 'list_groups' to reviewing every active policy ('list_policies')—and delivers one clean summary right in your chat window.

Bitwarden MCP for AI Agents: Managing User Access and Governance

Manual access review involves checking user lists against group definitions, and then cross-referencing those with the required security policies. It's a three-step process that takes an entire afternoon.

Now, you consolidate all this data. You ask your agent to verify membership ('list_members') and check resource organization ('list_collections'). You get one definitive answer about who owns what, instantly.

5 Tools for Bitwarden: Audit Collections, Groups, & Members

Use these functions to manage and report on every aspect of your organizational vault structure, from member lists to policy details.

#	TOOL	DESCRIPTION
01	`list_collections`	Lists every shared collection in your organization's vault.
02	`list_events`	Retrieves detailed logs of administrative actions and security-related activity.
03	`list_groups`	Lists all defined user groups within the organization.
04	`list_members`	Retrieves a roster of every current member in your organization.
05	`list_policies`	Shows all active security and administrative policies set up for the vault.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U What policies are currently restricting access in the finance collections?

Policies Report: Finance Collections

We found 3 active policies affecting your financial data:

- **Policy ID F-001:** Requires MFA for all members. (Active)
- **Policy ID F-002:** Restricts export to Admin roles only. (Active)
- **Policy ID F-003:** Mandates annual password rotation. (Scheduled: Q4 2025)

You should check the full details on Policy F-002, as it's critical for compliance.

U Show me all users in the 'Engineering' group and their current permissions.

Group: Engineering

- **Members:** Alice (Owner), Bob (Admin), Charlie (User)
- **Permissions Summary:** Members have read/write access to collections, but cannot modify policies.

Note: *Based on the current system configuration, only users in 'Admins' can modify group permissions. Do you want me to check the full list of admin roles?*

U What happened with our audit logs yesterday?

Audit Trail Summary (2026-06-11)

- **Event Count:** 14 actions recorded.
- **Key Activities:** 3 user invitations, 1 policy update by 'admin@corp.com', and 7 collection read attempts.
- **Highlight:** The policy update for MFA was logged at 9:05 AM EST. Would you like to see the specific details of that change?

Frequently Asked Questions

01 **How does the Bitwarden MCP help with compliance reporting?**

The Bitwarden MCP allows your AI agent to gather all necessary evidence for an audit in one go. It checks active policies, reviews event logs, and verifies member access, giving you a comprehensive report without manual data gathering.

02 **Can I use the Bitwarden MCP to check who belongs to which group?**

Yes. The agent can query user groups and then list all members associated with those groups. This helps IT Ops quickly map out team access rights without navigating multiple screens.

03 **What if I need to audit data sharing across different teams?**

You use the MCP's collection listing capability to see every shared resource group in your vault. You can then check which policies govern those collections, providing a full picture of data segmentation.

04 **Is this Bitwarden MCP better than manually checking logs?**

Absolutely. Instead of viewing raw log entries, the agent processes them for you. It highlights key actions and summarizes event logs, saving hours of manual investigation time.

05 **Does the Bitwarden MCP support multiple organizations or only one?**

It connects to a single specified organization using your client credentials. This ensures that all audit trails and resource reports are accurate for the defined scope.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"bitwarden": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

Bitwarden is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

vinkius.com · support@vinkius.com

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Bitwarden. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	Bitwarden MCP
Server ID	`019e386d-751c-7172-b2cb-33d864f53f4e`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/bitwarden.

© 2026 Vinkius · vinkius.com · support@vinkius.com