MCP SERVER | NO CODE | CLOUD HOSTED

Brivo MCP for AI Agents

Manage physical security and facility access control events.

Brivo manages your physical access control and facility security using AI agents. Connect it to monitor door status, check user credentials, track access events in real time, and automate core site management actions via natural conversation.

A+ Quality Score 100/100

access-control | smart-building | physical-security | user-provisioning | door-management | facility-management

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

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.

Brivo MCP

10 tools available
Cloud-hosted on Vinkius

This MCP connects your Brivo Access account directly to your workflow. You can orchestrate complex physical security tasks—from checking a server room's current lock status to auditing who has access to the HR suite—all through simple language commands from any AI client. Forget logging into multiple portals or running complex API calls just to find out if a door is locked. Your agent handles it instantly.

Need to know why someone was denied entry? Ask your agent to retrieve historical records and audit every relevant access event. Need to update permissions? The system lets you list users, check their credentials, and even manage time-based schedules automatically. It’s about talking to your facility management systems the way you talk to a coworker.

Connecting Brivo through Vinkius means you gain one central point for all physical security operations. You get powerful, real-time insight into who's supposed to be where and whether doors are functioning correctly, right within your existing AI workflow.

Core Capabilities

01 — Get Account Info

Retrieves core information about the account or site you are connected to.

02 — Get Door Status

Checks and reports the live status (open, closed, locked) of a specific access point.

03 — Get User Details

Retrieves detailed profiles for a single user within the system.

04 — List Doors

Provides a list of all physical doors and access points monitored by Brivo.

05 — List Credentials

Generates a comprehensive inventory of all types of credentials, like cards or mobile passes.

06 — List Access Events

Fetches recent activity logs and security alarms from the facility.

07 — List Access Groups

Displays all predefined groups of access permissions used across the site.

08 — List Schedules

Retrieves time-based schedules that control automatic locking and unlocking times.

09 — List Users

Provides a complete directory of all registered people and user accounts in the system.

10 — Unlock Door

Sends an immediate command to momentarily unlock a specific door access point.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to the Brivo MCP and provide your necessary API key, username, and password.

02 Your AI client authenticates with Vinkius and establishes a secure connection to Brivo's system.

03 You ask your agent to perform an action—like 'Show me all users who can enter the data center after hours.'—and get the immediate result.

The bottom line is, you talk naturally about physical security tasks instead of writing code or navigating complex web dashboards.

Built For

Security Managers and IT Admins use this MCP to cut down on the manual effort of checking status reports and user access lists. Facilities Leads rely on it for immediate incident response, avoiding slow logins into multiple vendor portals.

Facility Manager

Needs to quickly check if a back door is secured or manually unlock an entry point for a delivery driver without leaving their primary workflow.

IT Administrator

Must audit user credentials and access groups across the entire company to ensure compliance before onboarding new staff or terminating old accounts.

Security Operations Lead

Needs a single place to review chronological security events and check if any alarms are currently active during an incident response.

What Changes When You Connect

01 Audit user credentials with the Brivo MCP. Instead of checking multiple spreadsheets, your agent lists all assigned cards or passes instantly using `list_credentials`.

02 Never manually check a dashboard again. You can get the live status of any door—like the main entrance or server room—by simply asking your agent to use `get_door_status`.

03 Incident response gets faster. Your agent pulls up historical data and security alarms using `list_access_events`, giving you immediate context on what happened.

04 Streamline user management by listing all users (`list_users`) and checking their specific access profiles without leaving your primary workflow tool.

05 Automate urgent tasks like visitor entry. You can trigger a momentary unlock for a door using the `unlock_door` tool, right from a natural conversation prompt.

Real-World Applications

Investigating Unauthorized Entry

A security lead needs to know who was in the restricted wing last night. They ask their agent, which uses `list_access_events`, and get a timeline showing only authorized entries and any alarms that tripped.

Onboarding a New Department

An IT admin needs to set up access for 15 new employees. They use the Brivo MCP to list all necessary access groups (`list_access_groups`), then retrieve profiles using `get_user`, ensuring everyone gets the right credentials.

Emergency Access Protocol

A maintenance crew needs immediate entry during an outage. The manager asks their agent to check the door status (`get_door_status`) and, upon confirmation of need, triggers a temporary unlock using `unlock_door`.

Compliance Audit Preparation

An ops lead preparing for an audit needs to review all site access rules. The agent compiles data by listing the time schedules (`list_schedules`) and checking every assigned credential type using `list_credentials`.

Patterns to Avoid

Manually cross-referencing user lists

✗ AVOID

Opening the HR system, then switching to the physical security portal, then downloading a spreadsheet and manually matching usernames or roles.

✓ INSTEAD

Use your AI client to ask it to list all users via `list_users` and retrieve their specific profiles using `get_user`. This centralizes the data without leaving your agent's chat window.

Relying on old status reports

✗ AVOID

Using a weekly PDF report that shows door statuses from 8 AM, only to find out the door was actually open an hour ago and no one noticed.

✓ INSTEAD

Ask your agent for real-time checks using `get_door_status` or review immediate activity logs with `list_access_events` when you need current data.

Forgetting time constraints

✗ AVOID

Assuming a door is always unlocked because it was open yesterday, without checking if the system schedule changed overnight.

✓ INSTEAD

Always check the site's operational window by reviewing all available schedules using `list_schedules` before assuming access status.

The Right Fit

Use this Brivo MCP if your core job involves auditing physical locations, managing employee permissions, or responding to real-time security incidents. You need the AI agent to talk directly to a professional facility management system—anything involving who can enter where and when is in scope.

Don't use it if you only need to view general building floor plans or manage internal IT tickets that aren't linked to physical access. For basic logging, a simple document repository might suffice. But if the decision hinges on whether a specific door is locked right now, or which users have been granted digital credentials, this MCP is necessary.

Brivo Access Control: Streamlining Physical Security Audits with Brivo

Right now, running a security audit means logging into the main access control portal. You'll click through user directories, pull up individual profiles to check groups, and then manually cross-reference those details against old log reports just to build a picture of compliance.

With this MCP, you tell your agent exactly what you need—like 'Show me all users in the finance department who don't have current credentials.' The AI client uses Brivo's tools to pull and compare that data for you. You get one clean, accurate summary instead of three separate reports.

Brivo Facility Management: Controlling Door Status via Brivo

Checking physical status manually is a headache. You have to remember which dashboard shows the current lock status, and then log in again just to trigger an unlock for a visitor who's arrived early.

Now, you simply ask your agent, 'Is the server room door locked?' It executes that check immediately using `get_door_status`. If it needs unlocking, the agent handles the command. You don't touch a dashboard; you just get an answer.

Brivo: 10 Tools for Physical Security and Access Control

Use these tools to list users, check door statuses, retrieve event history, and control physical access points through natural language commands.

#	TOOL	DESCRIPTION
01	`get_account_info`	Pulls core information about the site or account associated with Brivo.
02	`get_door_status`	Checks and reports the current, live status (open/closed/locked) of a specific door.
03	`get_user`	Retrieves detailed personal profiles for an individual user account in the system.
04	`list_doors`	Generates a comprehensive list of all physical access points (doors) monitored by Brivo.
05	`list_credentials`	Lists and details every type of physical or digital access credential assigned to users, such as cards or mobile passes.
06	`list_access_events`	Fetches a list of recent activity logs and security alarms for the facility.
07	`list_access_groups`	Shows all predefined logical groupings of access permissions used by the organization.
08	`list_schedules`	Retrieves the time-based schedules that control when doors can be locked or unlocked automatically.
09	`list_users`	Provides a complete roster of all people and user accounts registered within the facility management system.
10	`unlock_door`	Sends an immediate command to momentarily unlock a specified door access point.

See It in Action

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

U What are all the access points in the building and what is their current status?

Site Access Point Status Report

- **Main Entrance:** Locked (Last checked: 10:52 AM)
- **Server Room:** Open (Current occupants: None)
- **Back Exit:** Locked (Scheduled to unlock at 7:00 PM)
- **HR Suite:** Closed (Status normal)

Need me to trigger a temporary unlock on the Main Entrance? Just say the word.

U Show me all users who have access to the data center and what their credentials are.

Data Center Access Audit

USER NAME	STATUS	CREDENTIALS ASSIGNED
John Doe	Active	Key Card (ID: 901)

| Jane Smith | Suspended | Mobile Pass (Expires: 2024-12-31) |

Please check the `list_users` tool if you need a complete roster.

U What happened with access last night? Show me any alarms.

I checked the logs for unusual activity between midnight and 6 AM. Here are the events:

12:05 AM: *Alarm triggered at Loading Dock.* Reason:* Door forced open.
- **3:45 AM:** John Doe accessed Server Room (Successful).
- **None:** There were no other active alarms or denied access attempts logged during that window.

Frequently Asked Questions

01 **Can the Brivo MCP help me track who entered the building?**

Yes, it pulls up real-time and historical records of all people entering or exiting. You can see who accessed which area and exactly when they did it.

02 **How do I check if a specific door is locked right now using Brivo MCP?**

You just ask your agent to get the live status of that door. It provides an immediate, accurate report on whether the access point is open or secured.

03 **Does this Brivo MCP help with user credential management?**

Absolutely. You can list every type of credential—cards, mobile passes, etc.—assigned to users and audit who has what permissions in one place.

04 **What if I need to manually open a door quickly? Does Brivo MCP handle that?**

Yes. If you need temporary access for maintenance or a visitor, the MCP can trigger an immediate, momentary unlock on the specified door.

05 **Can I check if my team members have the right permissions to enter certain areas?**

You can list all user profiles and their assigned access groups. This helps you verify that every employee has the correct level of authorization for their job function.

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 `"brivo": { "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

Brivo 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 Brivo. 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	Brivo MCP
Server ID	`019d7563-e011-7368-8bb3-a5d85a1afca8`
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/brivo.