MCP SERVER | NO CODE | CLOUD HOSTED

# Everbridge Critical Management MCP

## Track Incident Timelines and Contact Details in Chat.

Everbridge Critical Management connects your AI agent directly to enterprise emergency communication systems. Use it to track active incidents, check notification delivery status across thousands of contacts, and monitor organizational crisis data using natural language prompts.

A+ Quality Score 100/100

emergency-notifications | crisis-response | incident-management | alerting | public-safety

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/everbridge-critical-management

SCAN TO VIEW

# The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

# Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

# Everbridge Critical Management MCP

10 tools available
Cloud-hosted on Vinkius

When a major incident hits, you don't have time to log into five different portals just to see if everyone got the alert. This MCP gives your agent direct visibility into critical event management (CEM) systems. You can ask about an active incident timeline and get immediate details on severity levels and response logs. Need to know who needs calling? Your agent will pull contact profiles, checking their work email, personal phone, and group memberships all in one go. It also tracks every broadcast, letting you see if the message was delivered successfully or if contacts haven't confirmed receipt yet. This kind of deep operational oversight is exactly what Vinkius makes possible, bringing complex enterprise systems into your conversational flow. You manage an entire crisis response strategy simply by asking questions.

## Core Capabilities

**01 — Audit Crisis Health**

Get a high-level summary of recent notification volume and current active incidents.

**02 — Track Notification Delivery Status**

Check the specific delivery success rates, failure counts, and confirmation status for any broadcast.

**03 — List Contacts and Groups**

Retrieve full lists of registered contacts or all configured distribution groups across the organization.

**04 — Monitor Incident Timelines**

Get detailed settings, severity levels, and historical timelines for specific critical incidents.

**05 — Identify High-Risk Contacts**

Find the full communication profile and multiple contact methods (phone, email) for any individual person.

## One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/everbridge-critical-management** — connect your AI agent in three steps.

01 Connect your AI client using your Everbridge Organization ID, API Username, and API Password.

02 Authorize the connection to grant access to crisis management data.

03 Ask a natural language question, like 'What's the status of the last weather warning?' or 'List all high-severity incidents.'

The bottom line is you get instant answers about your organization's critical communications and contacts without touching a dashboard.

## Built For

This MCP is built for people who manage communication during high-stakes, time-sensitive events. If you live in the world of emergency operations or corporate risk management, this tool cuts through the complexity.

**Crisis Manager**

They use this MCP to quickly check notification statuses and incident timelines when they are on-site during a crisis.

**Emergency Operations Team Lead**

They use it in chat to research contact groups and distribution lists while coordinating an active event, instead of hunting through internal directories.

**Safety & Security Director**

They monitor organization-wide crisis metadata, tracking response metrics instantly without needing a dedicated dashboard view.

## What Changes When You Connect

01 You stop cross-referencing spreadsheets. Need to know the status of a broadcast? Use `get_notification_detailed_status` to see exactly who got the alert, how many confirmed receipt, and which contacts failed delivery.

02 Forget jumping between contact databases and incident logs. You can list all active incidents using `list_critical_incidents`, then immediately drill down into specific details with `get_incident_detailed_data` —all in one chat session.

03 Contact data is rarely simple. Instead of just getting a name, use `get_contact_profile_and_methods` to pull every communication channel for a person: their work phone, personal mobile, and group memberships.

04 Crisis audits used to take hours of manual reporting. Now, run a quick overview with `quick_crisis_event_audit` and get an immediate summary of overall crisis health metrics.

05 You don't have to search through every contact list manually. Simply use `list_contact_distribution_groups` to see all the communication channels available in your organization.

# Real-World Applications

**Checking Post-Event Communication**

A team member asks, 'What was the delivery status for the hurricane warning?' The agent runs `list_critical_notifications` and then uses `get_notification_detailed_status`, showing 98% successful delivery and listing the specific groups that missed the alert.

**On-Demand Contact Research**

A coordinator needs to reach a new employee. They ask, 'Give me John Smith's full contact details.' The agent executes `get_contact_profile_and_methods` and reports his primary phone number, work email, and that he belongs to the 'West Coast Team' group.

**Immediate Incident Triage**

A supervisor asks, 'Are there any high-priority incidents right now?' The agent runs `list_high_severity_incidents` immediately, identifying an active system outage and providing the associated timeline using `get_incident_detailed_data`.

**Auditing Organizational Readiness**

A safety director asks, 'Show me all potential contacts for the R&D building.' The agent runs `list_critical_contacts`, providing a comprehensive list that includes their membership in various distribution groups using `list_contact_distribution_groups`.

## Patterns to Avoid

### Using separate portals for data

✗ AVOID

Logging into the Everbridge web portal to view incident history, then opening a secondary database just to check contact groups.

✓ INSTEAD

Use this MCP. Ask your agent directly: 'What were the high-severity incidents and who are the key contacts associated with them?' The tool handles both `list_critical_incidents` and `list_contact_distribution_groups` in one command.

### Assuming universal contact info

✗ AVOID

Just having a name and an email address, but not knowing if they also have a work phone or are part of the 'Executive' distribution group.

✓ INSTEAD

Don't guess. Use `get_contact_profile_and_methods`. This function retrieves all known communication channels for that contact, ensuring you don't miss the best way to reach them.

### Asking 'Did it go out?' generically

✗ AVOID

A vague query like, 'Was the last alert successful?' which gives no details on failure rates.

✓ INSTEAD

Be specific. Ask: 'What was the delivery status for the message sent yesterday?' The agent runs `get_notification_detailed_status` and provides hard metrics like success percentage.

## The Right Fit

Use this MCP if your core pain point involves monitoring communications during a crisis, especially when that data is spread across incident logs, contact directories, and notification reports. You need to know *who* was notified, *when*, and *if* they received it.

Don't use this MCP if you only need basic messaging capabilities; for simple chat or internal message sending, a general communication tool works fine. However, if your task requires deep, verifiable data—like listing all contacts ( `list_critical_contacts` ) or getting the full timeline of an incident ( `get_incident_detailed_data` )—you must use this specialized MCP to ensure you get enterprise-grade accuracy.

## The mess of manual crisis communications tracking is a nightmare.

Right now, handling an incident means juggling multiple screens. You have to copy a notification ID from one dashboard into another system just to check its delivery status. Then you have to open the contact database, search for key personnel by name, and manually confirm which distribution group they belong to before drafting a follow-up message. It's slow, it’s prone to human error, and when seconds count, that friction costs real time.

With this MCP connected via Vinkius, you just talk to your agent. You tell it what happened, and it handles the cross-referencing. Instead of logging into separate portals, you get a single, conversational answer detailing both the incident status and the communication success rates.

## Everbridge Critical Management delivers instant operational oversight.

You eliminate the need to run multiple manual reports. You don't have to click through `list_critical_incidents` just to find severity levels, and then separately query contact groups using `list_contact_distribution_groups` . All that metadata is available instantly.

What changes is certainty. Your agent gives you definitive answers about who knows what, when they know it, and if the system itself was able to get the message out.

# Everbridge Critical Management: 10 Tools

These tools let you govern everything from listing active incidents to verifying the exact delivery status of critical emergency notifications.

| # | TOOL | DESCRIPTION |
|---|---|---|
| 01 | `get_everbridge_org_metadata` | Retrieves operational limits and core organizational information for your Everbridge account. |
| 02 | `get_contact_profile_and_methods` | Pulls the full communication profile, including multiple methods like phone or email, for a named contact. |
| 03 | `get_incident_detailed_data` | Retrieves the entire timeline and detailed settings for any specific critical incident. |
| 04 | `get_notification_detailed_status` | Provides a full breakdown of delivery success rates, statistics, and recipient counts for a broadcast notification. |
| 05 | `quick_crisis_event_audit` | Generates an immediate overview summary covering recent notifications and active incidents. |
| 06 | `list_critical_contacts` | Returns a list of every contact registered in your organization's address book. |
| 07 | `list_contact_distribution_groups` | Provides a complete listing of all configured contact distribution groups within the system. |
| 08 | `list_high_severity_incidents` | Identifies and lists incidents that are currently flagged with high severity levels. |
| 09 | `list_critical_incidents` | Lists all active and historical critical incidents recorded by the system. |
| 10 | `list_critical_notifications` | Retrieves a list of every broadcast notification that has been sent via Everbridge. |

# See It in Action

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

**U** List all active critical incidents.

I've found 2 active incidents: 'Building Fire - North Wing' (Severity: High) and 'System Outage - HQ' (Severity: Medium). Would you like to see the notification history for the Building Fire?

**U** Check delivery status for notification ID '1234567'.

Notification ID '1234567' (Subject: Weather Warning) was sent to 500 contacts. 485 were successfully delivered (97%) and 120 contacts have confirmed receipt. Should I list the contacts who haven't confirmed yet?

**U** Show me the contact details for 'John Doe'.

John Doe (External ID: 998877) has 3 communication methods: Mobile (SMS/Call), Work Email, and Personal Phone. They are a member of the 'Emergency Response Team' group. Would you like the full profile for this contact?

# Frequently Asked Questions

01 **How does Everbridge Critical Management MCP check contact details?**

It pulls detailed profiles for any person using `get_contact_profile_and_methods`. This means you don't just get an email address; you get their full communication profile, including secondary numbers and group memberships.

02 **What if I need to check multiple incidents at once?**

You can list all active or historical events using `list_critical_incidents`. Then, for each one, you can run `get_incident_detailed_data` to get the full timeline and severity report.

03 **Can this MCP tell me if a message was successfully delivered?**

Yes. Use `get_notification_detailed_status`. This tool provides specific metrics on delivery rates, confirming how many people received the alert versus those who haven't confirmed receipt.

04 **Is this only for large corporations?**

No. It works with any organization that uses Everbridge for critical communication. The MCP simply exposes the tools to your agent, regardless of company size.

05 **What is the difference between `list_critical_contacts` and getting a profile?**

`list_critical_contacts` gives you a simple list of names. You must use `get_contact_profile_and_methods` to get the actual, detailed communication methods for any single person on that list.

# 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 `"everbridge-critical-management": { "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

# Everbridge Critical Management 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 Everbridge Critical Management. 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 | Everbridge Critical Management MCP |
| Server ID | `019d7593-3bac-725f-8f62-a5890321c317` |
| 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/everbridge-critical-management.