MCP SERVER | NO CODE | CLOUD HOSTED

WeCom MCP

Manage Staff, Departments, and Messages by Conversation

WeCom / 企业微信 connects your AI client directly to China's top enterprise communication platform. Your agent handles complex internal operations, letting you list departments, find user profiles, check team attendance, and send messages—all through natural conversation instead of the admin backend.

A+ Quality Score 100/100

enterprise-messaging | team-collaboration | attendance-tracking | employee-management | internal-comms | api-integration

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

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.

WeCom / 企业微信 MCP

10 tools available
Cloud-hosted on Vinkius

Managing a large organization usually means clicking through confusing dashboards just to get basic employee data or check who was supposed to clock in. This MCP lets your agent bypass all that complexity. It treats WeCom like an extension of your chat interface, letting you talk to it about your company's structure and workforce. Need to know which users belong to the 'Finance' group? Ask. Want to see who clocked in this morning? Ask. Your agent pulls data on departments, retrieves detailed employee records, checks attendance logs, or sends a quick heads-up message—all instantly. Because Vinkius hosts this MCP, you connect your preferred AI client once and gain access to all these core business functions, turning rigid enterprise tools into simple conversational commands.

Core Capabilities

01 — Audit Team Attendance

Your agent retrieves real-time check-in data for staff, letting you audit workforce activity without logging into the attendance portal.

02 — Map Organizational Structure

You can ask the MCP to list all departments and then narrow down the employee roster within any specific unit.

03 — Identify Specific Users

The agent finds people based on their details, department, or assigned organizational tags.

04 — Send Targeted Messages

You send instant text messages to any specified user directly through the chat interface.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and enter your WeCom Corp ID, App Secret, and Agent ID.

02 Connect the MCP to your AI client (Claude, Cursor, etc.).

03 Tell your agent what you need: 'What are the users in the Engineering department?' The agent processes the request and provides the data.

The bottom line is that instead of navigating complex admin backends, you just talk to it about company operations.

Built For

This MCP is for anyone whose job involves manually querying large internal databases or coordinating staff across multiple platforms. If your day includes checking who's in which department, verifying employee records, or sending group announcements, you need this.

HR Manager

Checks team attendance and verifies employee profiles by asking the agent natural language questions.

Operations Coordinator

Coordinates staff communication, sending messages to groups or individuals without leaving their primary chat interface.

IT Administrator

Retrieves system metadata about internal apps and monitors organizational structure details for troubleshooting.

What Changes When You Connect

01 Check attendance instantly. Instead of logging into a separate dashboard to see who clocked in, your agent uses `get_attendance_data` to give you real-time check-in summaries.

02 Map out staff relationships. Use `list_departments` and then `list_users` to build an accurate organizational chart without manual data exports or spreadsheet manipulation.

03 Communicate targeted updates. Send a message using `send_message` directly through your agent, ensuring the announcement hits the right person immediately, regardless of their location in the org structure.

04 Segment users precisely. Need all compliance officers? Use `list_tags` first to see available groups, then use `get_tag_users` to pull only those employees who match that tag.

05 Avoid UI overload. Your agent handles complex lookups like getting user details (`get_user`) or department info (`get_department`), so you never have to navigate the WeCom Admin Backend yourself.

Real-World Applications

The HR Audit

A manager needs to confirm which staff members are in the new 'Product Development' department and whether they all clocked in today. The agent first uses `list_departments` to verify the unit, then uses `list_users` for the roster, and finally calls `get_attendance_data` to generate a single compliance report.

The Quick Announcement

A team lead needs to notify five specific people that a policy has changed. Instead of copying their names and sending messages one by one, the agent uses `get_tag_users` to find all users with the 'Leadership' tag, then calls `send_message` once to reach everyone.

The IT Deep Dive

An admin needs to know what a specific internal app can do. They use `list_menu` and `get_app_details`, getting the exact configuration metadata without needing access to the backend system settings.

The Missing Employee Profile

A user needs Jane Doe's phone number and manager name. Instead of searching through multiple HR systems, they ask their agent, which immediately uses `get_user` to pull all the necessary details in one conversational reply.

Patterns to Avoid

Assuming a unified database

✗ AVOID

Trying to run an 'All Employees' query and expecting it to return everything, including department, tag, and attendance data simultaneously.

✓ INSTEAD

Break the request down. First, list departments using `list_departments`. Then, ask for users in that specific department using `list_users`, followed by checking their status with `get_attendance_data`.

Manual user lookup

✗ AVOID

Searching the WeCom admin interface for a person's details, which requires knowing their exact ID or department name first.

✓ INSTEAD

Just ask your agent. If you know the general group, use `get_tag_users` to find them first, then use `get_user` on the result.

Sending messages blind

✗ AVOID

Attempting to send a message using only a vague description of the person (e.g., 'the guy in marketing').

✓ INSTEAD

Always verify the user ID first, either by asking for their full profile details with `get_user` or finding them via department listing (`list_users`). Then use `send_message`.

The Right Fit

Use this MCP if your core business process revolves around internal communication and managing people within a highly structured corporate environment. If you frequently need to query organizational charts, verify employee roles by group or department, or send targeted messages based on user status, this is essential. Don't use it if you only need general messaging capabilities; for simple one-to-one chats, native WeCom features work fine. But if the task involves *data retrieval* about who works where, what their role is, or when they clocked in, then you need its specific tools like `get_attendance_data` and `list_departments`. This MCP turns a data query into a conversation.

The struggle of navigating enterprise backends

Right now, gathering simple staff information is a headache. You have to jump between the user profile page, the department list, and the attendance dashboard. It's always multi-step: click here for the group tag, then copy that ID over to the reporting tool, then manually query the name.

With this MCP, you just talk to your agent. Instead of clicking through five different screens, you ask it to check user status or find all users in a department. The data flows directly into your conversation window.

WeCom / 企业微信: Direct Access to Core Data

Specific tasks, like finding every employee who belongs to the 'Engineering' department or listing all available functional tags, used to require an admin-level query and several manual data points. Now you just ask your agent to list departments using `list_departments` or find users by tag with `get_tag_users`.

This MCP gives you instant control over complex organizational data structures. You're not limited by the platform's UI; you use natural language to access the raw facts.

WeCom / 企业微信: 10 Tools for Operations Management

Use these tools to query employee data, map organizational structure, audit attendance records, or send messages directly through your AI agent.

#	TOOL	DESCRIPTION
01	`get_app_details`	Pulls detailed information about an application agent within WeCom.
02	`get_attendance_data`	Retrieves current and past employee check-in or attendance records for specified staff members.
03	`get_department`	Fetches specific details about a named department in the organization.
04	`get_tag_users`	Lists all users who have been assigned one or more organizational tags.
05	`get_user`	Gets comprehensive profile details for a single employee using their identifier.
06	`list_departments`	Provides an exhaustive list of all departments currently set up in the organization.
07	`list_menu`	Retrieves the custom menu configurations for a specific internal application agent.
08	`list_tags`	Provides a complete list of all functional or organizational tags used by the company.
09	`list_users`	Lists all employee users who belong to a specific department or unit.
10	`send_message`	Sends a plain text message directly to any specified user within the platform.

See It in Action

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

U List all departments in our organization.

I've retrieved the organizational structure for WeCom. You have 5 primary departments, including 'Engineering', 'Marketing', and 'Sales'. Which one would you like to see the users for?

U Send a message to user 'Mario' saying 'The deployment is complete'.

Done! I've sent your message to Mario through the WeCom application. He has been notified that the deployment is complete.

U Show me the attendance data for 'mario,renato' from today.

I've retrieved the check-in data for the specified users. Mario punched in at 9:00 AM, and Renato punched in at 8:45 AM. Both are currently marked as active in the system.

Frequently Asked Questions

01 **How do I list all departments using WeCom / 企业微信 MCP?**

You ask your agent to list all departments. The tool uses `list_departments` and returns a full roster of every department name currently in your organization.

02 **Can the WeCom / 企业微信 MCP check if an employee was present today?**

Yes, you can retrieve attendance records using `get_attendance_data`. Just tell your agent which user or group you want to audit, and it pulls the check-in details.

03 **What is the difference between listing users and getting a user profile?**

Listing users (`list_users`) gives you a roster of people in one place. Getting a user profile (`get_user`) provides deep, specific details about just that single person.

04 **Does the WeCom / 企业微信 MCP handle group messaging?**

You can send messages using `send_message` to individual users or groups found via tools like `get_tag_users`, making communication centralized and traceable.

05 **Can I get details about an internal application? (WeCom / 企业微信 MCP)**

Yes. You can use `list_menu` to see the app's custom menu structure, or `get_app_details` for deeper metadata on its functionality.

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 `"wecom": { "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

WeCom / 企业微信 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 WeCom / 企业微信. 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	WeCom / 企业微信 MCP
Server ID	`019d849c-54fa-70a7-a1a7-df2b8d0d9e4a`
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/wecom.