

MCP SERVER

NO CODE

CLOUD HOSTED

# Domo MCP for AI Agents

## Manage user access and data group memberships

Domo MCP lets your AI agent handle complex user administration directly within your BI environment. You can provision new accounts, update profiles, delete dormant users, or organize team members by creating and managing groups—all without navigating the clunky admin panels.

**F** Quality Score 14.04/100

user-administration

data-governance

analytics

identity-access

cloud-bi



# 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.

### 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.

### 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.

### 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**

Encryption at rest

**Ed25519**

PKI vault signatures

**24h TTL**

Ephemeral session keys

**V8 Isolate**

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.

### 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.

### 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.

### 06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

**FinOps**

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

**Firewall & DLP**

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

**Agent Activity**

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

**Tool Health**

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

**Incident Log**

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

Get started at [cloud.vinkius.com](https://cloud.vinkius.com) — connect your AI agent in under 60 seconds.

# Domo MCP

6 tools available

Cloud-hosted on Vinkius

Managing access in a large Business Intelligence platform is usually a tedious process of clicking through multiple tabs and screens. With this MCP connected via Vinkius, your agent bypasses that overhead entirely. You simply tell your AI client what you need done—for instance, 'Add John Doe to the Finance group' or 'Create an admin account for Sarah.' The tool handles the rest. It lets you create new users with specific roles, update profiles like job titles and locations, and control exactly who belongs in which data governance group. This means you can manage your entire user lifecycle—from initial provisioning to final removal—using natural conversation instead of complex UI workflows. You get immediate access control and a clear audit trail for every change.

---

## Core Capabilities

### 01 — Add user to group

Adds an existing user to a specified Domo group.

### 02 — Create group

Creates a brand new, empty organizational group within Domo.

### 03 — Create user

Generates a completely new user account in Domo and sends an invite email.

### 04 — Delete user

Permanently removes a user's entire account from the system.

### 05 — Remove user from group

Takes an existing user out of a specific Domo group.

### 06 — Update user

Modifies the profile details of an active Domo user account.

# One Click on Vinkius — From Prompt to Execution

Available at [vinkius.com/mcp/domo](https://vinkius.com/mcp/domo) — connect your AI agent in three steps.

- 01 Subscribe to this MCP and provide your Domo Access Token.
- 02 Connect the service credentials to your preferred AI client (like Claude or Cursor).
- 03 Tell your agent what you need done—for example, 'Update user 123's location to London.' The agent then executes the necessary API calls.

The bottom line is that once connected, your AI client acts as a direct interface into Domo's core administration functions.

---

## Built For

This MCP saves time for IT Operations and BI Administrators who deal with user churn and access control daily. If you spend time manually adding users to groups or updating profiles via the web UI, you need this. It lets your team manage data governance at scale.

### BI Administrator

Manages user accounts and ensures correct roles are assigned across different departments in Domo.

### IT Operations Engineer

Automates the entire user lifecycle, from onboarding a new employee to deprovisioning access when they leave the company.

### Team Lead / Manager

Organizes team members into specific functional groups (e.g., 'Q3 Marketing') and controls who sees which dashboards.

---

## What Changes When You Connect

- 01 Eliminate repetitive manual tasks. Instead of navigating the Domo admin panel to create a new account, you simply ask your agent to run 'create\_user' with all necessary details.

- 
- 02 Improve security governance by making membership changes instant. You can use 'add\_user\_to\_group' or 'remove\_user\_from\_group' without ever touching the UI, ensuring immediate access control.

---

  - 03 Simplify user offboarding. Running 'delete\_user' is a single command, replacing hours of clicking through multiple dashboards to revoke permissions.

---

  - 04 Maintain clean organizational structures by proactively managing groups. Use 'create\_group' when a new project requires dedicated shared visibility.

---

  - 05 Update profiles quickly and accurately. The 'update\_user' tool lets you change job titles or roles for thousands of records without manual data entry.
- 

---

## Real-World Applications

### Onboarding a New Department

A new marketing team needs access to the central dashboard. Instead of manually adding 15 users and assigning them to the 'Marketing' group, you tell your agent to create the necessary group using 'create\_group', then run 'add\_user\_to\_group' for all 15 people in one go.

### Changing a User's Role

A data analyst moves from basic reporting to administrative duties. Instead of changing their profile manually, you use 'update\_user' to change their role and then confirm they are added to the 'Admin' group.

### Handling Employee Departure

An employee leaves today and their access must be revoked immediately. You prompt your agent to execute the 'delete\_user' tool, ensuring zero lingering access or security risks across Domo's platforms.

### Auditing Access for Compliance

You need to ensure only Finance staff can access salary reports. You ask your agent to review all users, identify those who shouldn't be there, and use 'remove\_user\_from\_group' on any misassigned personnel.

---

# Patterns to Avoid

---

## Using the UI for bulk changes

### X AVOID

Manually going into Domo's admin panel to add 50 users to a new group. This is slow, prone to clicks errors, and takes up half a day.

### ✓ INSTEAD

Define the access list in your agent prompt and let it handle the bulk operations using 'add\_user\_to\_group' for every person listed. It's faster and requires zero clicking.

---

## Forgetting to update roles

### X AVOID

When a user changes jobs, you only update their profile but forget to remove them from old groups like 'Old Project Alpha'. This leaves stale access.

### ✓ INSTEAD

Always pair the 'update\_user' tool with 'remove\_user\_from\_group' to ensure both the role and the specific group membership are cleared out.

---

## Attempting manual user deletion

### X AVOID

Trying to find a user in the system settings just to delete their account. This often fails or requires multiple authorization steps.

### ✓ INSTEAD

Just use the 'delete\_user' tool. It handles the entire lifecycle of removal and ensures no orphaned records remain.

---

## The Right Fit

Use this MCP if your primary need is administrative control over user identities, group memberships, or profile data within Domo. If you frequently answer questions like 'Who needs access to X?' or 'How do I onboard a new team?', this tool is for you. Don't use it if your goal is analyzing the *data* itself; that requires different connectors. Also, don't try to use it to generate reports—it only manages who can see the data. If you need complex reporting logic or dataset transformations, look into a dedicated data processing MCP instead.

---

---

## Domo User Administration with AI Agents: Handling Access Control

Right now, adding a user to Domo requires logging into the admin panel. You have to search for the person, navigate to groups, and manually assign them. If you're doing this ten times a day across multiple projects, your day is spent clicking buttons instead of analyzing data.

With this MCP, you just tell your agent who needs access and where. It handles finding the right group, running the 'add\_user\_to\_group' operation, and confirming the assignment—all in a single prompt. You get immediate, verifiable changes to user access.

---

## Managing Domo Group Governance via AI Agents

The worst part about group management is cleanup. When a project ends, you have to remember to go back and remove everyone from the 'Project X' group. If you miss one person, they retain access, creating a security hole.

Using the agent to run 'remove\_user\_from\_group' ensures that when you decommission a team, every single user is properly detached from the old groups in bulk. Your data governance stays tight.

---

## 6 Tools for Domo User Administration and Group Governance

Use these tools through your AI client to programmatically add, remove, update, and create users and organizational groups in Domo.

#	TOOL	DESCRIPTION
01	<code>add_user_to_group</code>	Adds an existing user to a specified Domo group.
02	<code>create_group</code>	Creates a brand new, empty organizational group within Domo.
03	<code>create_user</code>	Generates a completely new user account in Domo and sends an invite email.
04	<code>delete_user</code>	Permanently removes a user's entire account from the system.
05	<code>remove_user_from_group</code>	Takes an existing user out of a specific Domo group.
06	<code>update_user</code>	Modifies the profile details of an active Domo user account.

---

## See It in Action

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

**U** We hired two new people today. Create their accounts as Participants and add them to the 'Data Science' group.



**Success.**

The following actions were completed:

- **User Accounts Created:** Alice Smith (alice@corp.com) and Bob Jones (bob@corp.com).
- **Roles Assigned:** Both users are set as 'Participant'. Invitation emails sent.
- **Group Membership:** Both accounts added to the 'Data Science' group (ID 9982). They now have access to shared resources.

**U** I need to update Jane Doe's profile because she got a promotion. Also, remove her from the old 'Marketing Beta' group.



**Update Complete.**

Jane Doe's record (ID 45021) has been successfully updated:

- **Job Title:** Senior Product Manager
- **Location:** San Francisco, CA
- **Group Change:** Removed from 'Marketing Beta'. She retains access to the core 'Product Insights' group.

Please verify her new permissions in your dashboard.

- U** We need a new group for the legal team that only sees compliance data. Create it and give me a list of all users I should add.



✔ **Group Created & Recommended.**

A new group, 'Legal Compliance Review', has been created (ID 9901).

**Suggested Members:**

- Michael Chen (Director)
- Sarah Lee (Counsel)
- David Rodriguez (Associate)

You can now run the `add_user_to_group` tool for these users, or review them manually. The group is ready for access control.

---

## Frequently Asked Questions

---

**01 How does the Domo MCP help me manage user access?**

It lets you handle all account changes—creating new users, updating profiles, and revoking access—using natural language commands. You don't have to navigate complex admin menus; your agent just executes the change directly.

**02 Can I use this MCP to onboard a large group of employees?**

Yes, you can automate bulk operations. You can create entire groups for new hires and then assign multiple users to that group in one prompt, ensuring everyone gets the right starting access.

**03 If I use this MCP, will I lose audit history?**

No. The agent records every action taken through the tools—every user created or membership changed—giving you a clear record of who did what and when for compliance purposes.

**04 Does the Domo MCP handle group permissions changes?**

Absolutely. You can establish new groups using 'create\_group' and then use other tools to precisely control which users belong in it, maintaining strict data governance.

**05 What if I just need to update a user's title or location?**

You don't need separate tools for that. The 'update\_user' capability lets you modify profile details like job title and department without affecting their core access rights.

**06 Is the Domo MCP better than using a spreadsheet to track users?**

Yes. Spreadsheets are static documents; this MCP performs live actions within Domo's system, making changes instantly and reliably without manual data entry errors.

---

# Go Live in 60 Seconds

Get your connection token from [cloud.vinkius.com](https://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 `"domo": { "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

# Domo 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](https://cloud.vinkius.com) →

[vinkius.com](https://vinkius.com) · [support@vinkius.com](mailto: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 Domo. 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	Domo MCP
Server ID	019e388d-65a8-717e-b9d0-63cc063cf7a1
Platform	Vinkius Cloud for AI Agents
Endpoint	<a href="https://edge.vinkius.com/{token}/mcp">https://edge.vinkius.com/{token}/mcp</a>

### 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/domo](https://vinkius.com/mcp/domo).