MCP SERVER | NO CODE | CLOUD HOSTED

ServiceNow MCP

Manage IT service records via conversation.

ServiceNow MCP connects your AI client to the enterprise IT Service Management backbone. Manage everything from P1 incidents and service requests to change approvals and CMDB lookups using natural conversation. Stop navigating complex dashboards; just ask your agent to handle it.

A+ Quality Score 100/100

itsm | incident-management | service-catalog | workflow-automation | enterprise-service-management | cmdb

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

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.

ServiceNow MCP

10 tools available
Cloud-hosted on Vinkius

The ServiceNow MCP lets you manage your entire IT operational lifecycle through simple chat commands, treating your AI client like an internal ITSM command center. Instead of clicking through multiple tabs on a massive dashboard, you talk to the system. You can query open tickets by priority or SLA breach status using one prompt. Need to escalate? Just ask it to create a new incident record. Want to know if that database upgrade is safe? The agent queries the CMDB and tells you what CI relationships exist. Everything—from submitting a service request to reviewing complex change approvals—is handled conversationally. Connect this MCP through Vinkius, your #1 catalog, and give your AI agent hands-on access to every corner of ServiceNow's record system. It turns IT operations from manual data entry into dialogue.

Core Capabilities

01 — Search for known issues

It searches the Knowledge Base using simple keywords, returning article numbers and summaries that help resolve incidents.

02 — Track active service disruptions

You can list open incidents with specific filters like priority or assignment group to see exactly what needs fixing right now.

03 — Manage system changes

The MCP lets you create new change requests, check the risk level, and track them until they are approved by CAB.

04 — Audit infrastructure assets

Query the CMDB to find specific configuration items or map relationships between different pieces of hardware and software.

05 — Update ticket details

You update existing records, specifying only the fields you need changed—no more opening a record just to change one status flag.

One Click on Vinkius — From Prompt to Execution

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

01 First, subscribe to this MCP and enter your organization's specific ServiceNow instance URL and credentials.

02 Next, authorize your AI client. This gives your agent direct read/write access to the core ITSM tables (incidents, changes, requests).

03 Finally, start chatting with your agent. You tell it what you need—e.g., 'List all P1 incidents assigned to Network Ops'—and it executes the required queries and actions.

The bottom line is that once set up, your AI client handles complex IT processes using natural language commands instead of requiring you to navigate a dozen dashboards and forms.

Built For

IT Service Managers who are sick of manually cross-referencing data across multiple dashboards. DevOps Engineers tired of losing time on ticket triage. Help Desk Analysts who want to resolve complex issues without constantly switching screens.

Help Desk Analyst

They use the MCP to search the knowledge base for quick answers and update incident records instantly via chat, speeding up first-call resolution.

DevOps Engineer

They create change requests or query CMDB relationships directly from their workflow agent, eliminating manual data entry into ticketing systems.

IT Service Manager

They monitor the health of service delivery by querying open incidents and tracking SLA compliance status without running reports.

What Changes When You Connect

01 Triage incidents faster. Instead of opening the dashboard, you just ask your agent to list open P1 incidents by assignment group using `list_incidents` and get a clean summary immediately.

02 Automate change control. You can create an entire change request using `create_record`, specifying type and risk level, then track it through approvals without lifting a finger on the UI.

03 Pinpoint infrastructure issues. Need to know if the web server is related to the database error? Use `query_cmdb` to explore CI relationships across your environment instantly.

04 Resolve tickets with knowledge. Instead of guessing where the answer is, use `search_knowledge` and get relevant articles right in the chat window for self-service resolution.

05 Handle records programmatically. You can update any existing ticket or request using `update_record`, specifying only the single field that needs changing—no manual record navigation required.

Real-World Applications

A P1 incident hits, and you need to know who owns it.

The agent handles this: 'List all open incidents where the priority is 1.' It immediately returns a list of active tickets. You then ask, 'Which team needs to pick up INC0012345?' This bypasses navigating complex ticket dashboards and gets you straight to actionable data.

A developer needs to document a new application setup.

The agent handles this: 'Create a new record for the app in CMDB.' The tool uses `create_record` to log the asset, including all necessary details. This ensures the CI is documented correctly from the start of the project lifecycle.

You need to find out what services are impacted by a known outage.

The agent handles this: 'Query CMDB for all applications related to the main database server.' It uses `query_cmdb` to map dependencies, letting you see the full blast radius of the failure without manual tracing.

A service request needs a minor field correction.

The agent handles this: 'Update SC0098765 by changing the fulfillment status to Approved.' It uses `update_record` to hit that specific record and change only one field, leaving all other data intact.

Patterns to Avoid

Assuming full visibility

✗ AVOID

Trying to list every single user account or service without knowing the exact table name. You end up getting an error because you don't know where to start.

✓ INSTEAD

Don't try to manually navigate through tables. Instead, use `query_table` and specify filters like 'department=IT' to narrow down your search scope instantly.

Over-relying on the GUI

✗ AVOID

You spend ten minutes clicking from the incident dashboard to the related change request form, then copying a number somewhere else.

✓ INSTEAD

Just ask your agent. Use `list_incidents` and follow up with 'What is the associated change request?' The MCP handles the cross-referencing for you.

Forgetting record IDs

✗ AVOID

You know a problem exists, but you don't have its `sys_id`. You can't update it or get details.

✓ INSTEAD

Don’t worry about the ID. First, use `list_incidents` to find the ticket number and then ask the agent to retrieve the full record using that information.

The Right Fit

Use this MCP if your primary pain points revolve around managing structured IT data: incidents, changes, or configuration items. If you spend time querying asset relationships (CMDB) or tracking complex workflows (CAB approvals), this is for you. Don't use it if all you need to do is browse documentation; then `search_knowledge` handles that fine. However, if your goal is purely reporting—like generating a PDF of last month's metrics without querying the data

first—you might be better off with a dedicated analytics tool instead of using these record-level tools.

The headache of the manual IT service workflow

Today, managing an incident means jumping between at least four separate dashboards. You open the ticket to check priority, click over to the CMDB to see what assets are involved, then switch tabs to find a related knowledge article. If you need to update anything, you have to copy and paste IDs across multiple forms just to make sure everything is logged correctly.

With this MCP, that entire sequence vanishes. You tell your agent, 'Figure out why the VPN dropped for Joe in accounting.' The agent handles checking `list_incidents`, cross-referencing assets via `query_cmdb`, and suggesting articles from `search_knowledge`—all without you clicking anything.

Get immediate control with ServiceNow MCP

The ability to manage records means no more manual status updates. Instead of finding the change request, opening it, and changing 'Status: Pending' to 'Status: Approved,' you simply tell your agent to perform the action.

Your IT team gains immediate control over its service data. You talk to ServiceNow using plain English; the MCP translates that into precise actions like running `create_record` or `update_record`, making complex operations as simple as a chat message.

ServiceNow with 10 Tools

Use these tools to perform specific actions across your entire ServiceNow instance—from creating new assets to listing open tickets.

#	TOOL	DESCRIPTION
01	`create_record`	This tool allows you to create a brand new record in key tables like incident, change request, or service catalog requests.
02	`search_knowledge`	It searches the ServiceNow Knowledge Base and returns matching articles with their KB numbers so you know where to find solutions.
03	`update_record`	You modify an existing record by specifying only the exact fields and values that need changing, leaving everything else untouched.
04	`delete_record`	This action removes a ServiceNow record entirely; you'll be warned because this change can't be undone.
05	`query_table`	It lets you run custom queries against any table using advanced filters, including looking up related fields across the system.
06	`count_records`	This tool quickly counts how many records exist in a specific ServiceNow table without having to fetch every single one of them.
07	`get_record`	You retrieve all available information for a single record just by providing its system ID.
08	`list_incidents`	It lists multiple incidents and lets you filter the results by criteria like priority, state, or assignment group.
09	`list_change_requests`	This tool fetches a list of change requests, allowing filtering based on risk level or current state.
10	`query_cmdb`	You search the CMDB for configuration items like servers or applications using common names or IDs.

See It in Action

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

U Show me all P1 incidents that are unassigned.

Found 4 unassigned P1 incidents: 1. INC0012345 — 'Email Service Down' (opened 2h ago), 2. INC0012350 — 'VPN Authentication Failure' (opened 45min ago), 3. INC0012352 — 'ERP Integration Timeout' (opened 30min ago), 4. INC0012355 — 'Database Replication Lag' (opened 15min ago). Would you like me to assign any of these?

U Create a normal change request for 'Database Upgrade to v15' assigned to the DBA team.

Change request CHG0045678 has been created successfully. Type: Normal, Risk: Moderate, Assignment Group: DBA Team, Short Description: 'Database Upgrade to v15'. It is now pending CAB approval. Would you like me to add implementation notes?

U Search the knowledge base for 'VPN connection issues'.

Found 3 relevant knowledge articles: 1. KB0098765 — 'VPN Troubleshooting Guide' (Last updated: March 2026, 45 views), 2. KB0098770 — 'Corporate VPN Setup for Remote Workers', 3. KB0098780 — 'Known VPN Issues After Security Patch 2026-Q1'. Would you like me to show the resolution steps from any of these?

Frequently Asked Questions

01 **How does the ServiceNow MCP handle CMDB data?**

The MCP uses `query_cmdb` to let you search common configuration items like servers and applications. It can also explore relationships, showing how different assets depend on each other.

02 **Can I use the ServiceNow MCP to track P1 incidents?**

Yes, you can list open P1 incidents by using `list_incidents`. This lets you filter results immediately by priority or assignment group for quick triage.

03 **What if I need to change a ticket field, but don't know the sys_id?**

You first use `list_incidents` or `get_record` to find the record ID. Once you have that ID, you can then use `update_record` to modify specific fields.

04 **Does ServiceNow MCP help with change approvals?**

Yes, it supports managing changes. You can use `create_record` to draft a request and track its status through the system's defined approval workflows.

05 **Is this MCP only for viewing data?**

No, it lets you do more than just view. You can also execute actions like `create_record` to open new tickets or `update_record` to change the status of existing ones.

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 `"servicenow": { "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

ServiceNow 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 ServiceNow. 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	ServiceNow MCP
Server ID	`019d7606-8d14-724c-8de9-a94231dc89b1`
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/servicenow.