

M C P S E R V E R

N O C O D E

C L O U D H O S T E D

Claim Deadline Calendar MCP

Keep insurance claim timelines and document deadlines on track.

Claim Deadline Calendar MCP handles the math and scheduling for insurance claim processing. It calculates notice windows, tracks document submission deadlines, and flags urgent risks based on incident dates. Your AI client uses this to manage complex timelines and ensure you meet every compliance requirement without manual date tracking.

A+ Quality Score 98.33/100

claims

deadlines

insurance

scheduling

compliance



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 — connect your AI agent in under 60 seconds.

Claim Deadline Calendar MCP

4 tools available

Cloud-hosted on Vinkius

Managing insurance claims means juggling strict notice windows and document submission deadlines. This MCP takes the guesswork out of those timelines. You provide an incident date and the specific policy requirements, and your agent builds a complete, chronological schedule. It accounts for business-day logic so your deadlines align with standard working schedules.

You can use it to spot high-risk claims that are approaching a deadline or to check if a specific piece of paperwork is still pending. Instead of manually calculating dates in a spreadsheet, you just ask your AI client to run the numbers. It's a direct way to ensure you don't miss a filing window or a required document submission. Whether you're tracking a single incident or managing a batch of claims, this MCP keeps the critical dates front and center.

Core Capabilities

01 — Timeline Generation

Your agent creates a full schedule of deadlines based on a single incident date.

02 — Risk Assessment

The AI identifies claims that are at risk of missing a critical filing window.

03 — Document Tracking

Your agent monitors which specific documents are still required for a claim.

04 — Reminder Planning

The AI produces a list of dates for when you need to be notified to act.

05 — Business Day Logic

The tool applies standard working schedules to all calculated deadlines.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/en/ai-agent-connect/claim-deadline-calendar — connect your AI agent in three steps.

01 Connect the MCP to your preferred client like Claude or Cursor via Vinkius.

02 Provide the incident date and policy window requirements to your agent.

03 The agent uses the MCP tools to calculate timelines and risk levels.

04 Review the generated schedules or risk alerts directly in your chat interface.

Connecting this MCP to your AI client gives your agent immediate access to insurance scheduling logic.

Built For

This MCP is built for professionals managing insurance lifecycles who need to ensure strict adherence to policy timelines.

Claims Adjusters

They hand off incident details to the AI to generate filing schedules.

Insurance Case Managers

They use the AI to monitor document readiness and risk status.

Compliance Officers

They rely on the AI to verify that all notice windows are being met.

What Changes When You Connect

01 Calculates notice windows and document deadlines automatically.

02 Flags urgent escalations based on real-time claim progress.

03 Uses business-day logic to prevent scheduling errors.

04 Tracks pending paperwork status through a single interface.

Real-World Applications

New Claim Intake

Input an incident date to immediately get a full schedule of all upcoming deadlines.

Document Auditing

Check the status of specific required documents to see what is still missing.

Risk Management

Identify which claims are approaching a deadline to prevent missed filings.

Notification Planning

Create a list of reminder dates to stay ahead of critical claim milestones.

Patterns to Avoid

Manual date tracking

❌ AVOID

You try to calculate every notice window and business day deadline in a spreadsheet after an incident occurs.

✓ INSTEAD

Let your agent build the entire schedule at once using `calculate_claim_timeline`.

Reactive deadline management

❌ AVOID

You only check if a claim is overdue after the filing window has already closed.

✓ INSTEAD

Use `evaluate_late_risk_status` to identify claims that need immediate attention before they become problems.

Ignoring document status

❌ AVOID

You assume all paperwork is submitted and only realize a file is incomplete during a final audit.

✓ INSTEAD

Run `validate_document_readiness` to see exactly which specific documents are still pending or at risk.

The Right Fit

Insurance professionals managing strict policy timelines should connect this MCP. If your team relies on manual spreadsheets to track notice windows, you need this. Avoid this if your claims process has no fixed regulatory or policy-driven deadlines.

Claim Deadline Calendar Tools

These tools automate the calculation of filing windows and monitor the status of required claim documentation.

#	TOOL	DESCRIPTION
01	evaluate_late_risk_status	This tool identifies urgent actions by comparing the current date against the claim's progress. It flags claims that need immediate attention to avoid missing a deadline.
02	get_reminder_schedule	This tool generates a filtered list of specific dates for notifications. It tells your agent exactly when to alert you to take action.
03	validate_document_readiness	This tool checks the status of required paperwork. It identifies which document deadlines are still pending or currently at risk.
04	calculate_claim_timeline	This tool builds a full chronological schedule of all critical deadlines. It uses the incident date to map out every necessary reminder and filing window.

See It in Action

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

U Generate a claim timeline for an incident on 2024-05-01 with a 10-day notice window and a document deadline for 'Police Report' at 15 days.



The claim timeline has been generated. The policy notice deadline is 2024-05-11 and the Police Report must be submitted by 2024-05-16.

U What are the urgent risks for my claim if today is 2024-05-10 and my notice deadline was 2024-05-11?



An Urgent risk is active because the policy notice deadline is within 1 business day.

U Check if my documents are ready. I have already submitted 'ID Card'.



The 'ID Card' is marked as completed. The 'Medical Report' is currently pending.

Frequently Asked Questions

01 How does this MCP handle weekends?

The MCP uses business-day logic to ensure all calculated deadlines follow standard working schedules.

02 Can I use this with Claude or Cursor?

Yes, you can connect this MCP to any MCP-compatible client including Claude, Cursor, and Windsurf.

03 What information do I need to provide to start?

You typically need to provide an incident date and the specific notice or document deadlines required by the policy.

04 Does this MCP host the data?

Vinkius hosts and manages the MCP, so you don't need to set up your own hosting or manage credentials.

05 How does it identify urgent claims?

It uses the `evaluate_late_risk_status` tool to compare the current date against the claim's progress and deadlines.

06 How do I generate a full claim schedule?

Use the ``calculate_claim_timeline`` tool with the incident date, notice window, and required document deadlines.

07 Can I account for weekends and holidays?

Yes, by setting the ``businessDayOnly`` parameter to true in the ``calculate_claim_timeline`` tool, all deadlines will skip weekends and holidays.

08 How can I check if a claim is at risk of missing a deadline?

You can use ``evaluate_late_risk_status`` to identify urgent actions or ``validate_document_readiness`` to see which documents are pending or at risk.

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 <code>"claim-deadline-calendar": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

Claim Deadline Calendar 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 Claim Deadline Calendar. 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	September 2026
MCP Server	Claim Deadline Calendar MCP
Server ID	01a0e04d-29a7-736e-b3ba-23134bae76cb
Platform	Vinkius Cloud for AI Agents
Endpoint	<code>https://edge.vinkius.com/{token}/mcp</code>

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/en/ai-agent-connect/claim-deadline-calendar.