

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

Document Expiry Calendar MCP

Keep your compliance schedules on track without manual tracking.

Document Expiry Calendar MCP tracks document lifecycles and manages renewal windows. It calculates lead times and identifies upcoming deadlines so your AI agent can handle scheduling, task assignment, and risk assessment for expired documents automatically.

A+ Quality Score 100/100

compliance

documents

scheduling

risk-management

lifecycle



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.

Document Expiry Calendar MCP

4 tools available

Cloud-hosted on Vinkius

You can stop manually checking spreadsheets for expiring permits or licenses. This MCP acts as a proactive compliance layer for your AI client. It monitors document lifecycles by calculating renewal windows based on specific expiry dates and required lead times. Instead of you hunting for what's due, your agent can pull a chronological schedule of upcoming windows or identify exactly which tasks belong to specific owners. When a deadline is missed, the MCP provides the necessary risk assessments and remediation steps to fix the compliance gap. It's a direct way to hand off the heavy lifting of deadline management to your agent.

Core Capabilities

01 — Renewal Scheduling

Your agent uses this to map out upcoming windows before documents expire.

02 — Task Delegation

The agent identifies specific responsibilities for individual owners.

03 — Protocol Lookup

Your agent retrieves the exact materials needed for a successful submission.

04 — Risk Remediation

The agent assesses risks and provides steps when a deadline is missed.

One Click on Vinkius — From Prompt to Execution

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

- 01
- Connect the MCP to your preferred client like Claude or Cursor.
- 02
- Your agent accesses the renewal calendar to see upcoming dates.
- 03
- The agent identifies specific tasks for owners or submission requirements.
- 04
- The agent monitors for expired documents and provides remediation steps.

Connect the MCP to your client and let your agent manage the lifecycle.

Built For

This MCP is built for professionals managing high-stakes documentation and regulatory requirements.

Compliance Officers

They hand off the monitoring of expiration dates and risk assessments to the agent.

Operations Managers

They use the agent to track renewal windows and assign tasks to team members.

Legal Assistants

They rely on the agent to pull submission protocols and document requirements.

What Changes When You Connect

- 01
- Calculates renewal windows automatically based on expiry dates.
- 02
- Assigns specific tasks to owners to prevent missed deadlines.
- 03
- Provides remediation steps for expired documents.

04 Centralizes submission protocols for all document types.

Real-World Applications

Regulatory Compliance

An agent monitors business permits and alerts the team before they expire.

Risk Management

When a document expires, the agent identifies the risk and the necessary fix.

Staff Certification

The agent tracks employee health certificates and assigns renewal tasks to managers.

Document Auditing

The agent pulls a full calendar of all upcoming renewal windows for an audit review.

Patterns to Avoid

Manual spreadsheet hunting

❌ AVOID

You spend your Monday morning scrolling through rows of dates in a spreadsheet to see what expires this month.

✓ INSTEAD

Let your agent pull a chronological schedule of all upcoming windows using ``get_renewal_calendar`` instead.

Vague compliance checks

❌ AVOID

You ask your agent if the team is compliant without knowing which specific person is responsible for a specific permit.

✓ INSTEAD

Use ``get_action_owner_tasks`` to see exactly what tasks are assigned to a specific owner.

Reactive panic after expiration

❌ AVOID

A license expires and you realize you don't know what paperwork is needed to fix the gap.

✓ INSTEAD

Use ``get_document_requirements`` to find the exact protocols needed for a successful submission before the deadline hits.

The Right Fit

Connect this MCP if your team manages high-stakes permits, licenses, or staff certifications that require strict adherence to renewal windows. Do not connect it if your documentation is static or has no regulatory consequences. The decision rests on whether a missed deadline creates a measurable operational or legal risk.

Document Expiry Calendar 4 Tools

These tools manage the entire lifecycle of a document from upcoming renewal windows to post-expiry risk remediation.

#	TOOL	DESCRIPTION
01	get_action_owner_tasks	This tool pulls a list of specific tasks assigned to a particular person. Use it to see exactly what an owner needs to do to stay compliant.
02	get_document_requirements	This tool provides the specific submission protocols and materials needed for a document renewal. It tells your agent exactly what to prepare.
03	get_missed_deadline_contingencies	This tool identifies documents that have already expired. It returns risk assessments and the steps required to remediate the failure.
04	get_renewal_calendar	This tool generates a chronological schedule of all upcoming renewal windows. It gives your agent a clear view of the timeline ahead.

See It in Action

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

U Show me the renewal schedule for the next three months.



Here is your renewal calendar for the next three months: 1. Passport (Starts: 2024-10-15, Expires: 2024-11-15), 2. Driver License (Starts: 2024-12-01, Expires: 2025-01-01).

U What are the requirements to renew my Business Permit?



To renew your Business Permit, you must use the digital portal and provide a valid tax certificate and proof of address.

U What tasks are assigned to Alice?



Alice has the following upcoming tasks: Renew Health Certificate by 2024-11-20 via digital portal.

Frequently Asked Questions

01 How does the MCP handle expired documents?

It uses the `get_missed_deadline_contingencies` tool to identify expired documents and provide risk assessments and remediation steps.

02 Can I assign tasks to specific people?

Yes, the `get_action_owner_tasks` tool retrieves specific tasks assigned to a particular responsible person.

03 What information is provided for renewals?

The `get_document_requirements` tool provides the specific submission protocols and necessary materials for a document's renewal.

04 How do I see all upcoming deadlines?

You can use the `get_renewal_calendar` tool to see a chronological schedule of all upcoming renewal windows.

05 Which AI clients can use this MCP?

This MCP works with any MCP-compatible client, including Claude, Cursor, Windsurf, and VS Code.

06 How are renewal dates calculated?

The renewal start date is calculated by subtracting the document's specific lead time from its expiry date.

07 Can I see tasks assigned to a specific person?

Yes, you can use the `'get_action_owner_tasks'` tool to retrieve a list of tasks for a specific responsible owner.

08 What happens if a document expires?

You can use `'get_missed_deadline_contingencies'` to identify overdue documents and receive risk levels and remediation steps.

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>"document-expiry-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

Document Expiry 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 Document Expiry 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	October 2026
MCP Server	Document Expiry Calendar MCP
Server ID	01a0e75e-3a06-706c-86c7-a7d9b17fd4ef
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/en/ai-agent-connect/document-expiry-calendar.