MCP SERVER | NO CODE | CLOUD HOSTED

Digify MCP for AI Agents

Audit document access and track data room activity

Digify lets your AI agent manage secure files, monitor activity within virtual data rooms, and audit document access. Instead of manual reporting, you can track who views sensitive documents, review viewing rights, and get detailed engagement statistics instantly.

A+ Quality Score 100/100

data-room | document-security | access-control | engagement-analytics | file-tracking | compliance

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026

vinkius.com/mcp/digify

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.

Digify MCP

10 tools available
Cloud-hosted on Vinkius

You don't want to juggle multiple dashboards or wait for compliance reports to manually check file access. Digify connects the leading document security platform directly into your AI workflow. This lets you treat secure files and data room activity like a natural conversation. You can ask your agent who viewed an M&A proposal, how long they spent on it, and if their viewing rights are still active—all in real time. The system handles listing protected assets or monitoring collaboration across entire data rooms with minimal input from you. When connected via Vinkius, the Digify MCP gives your AI client a single pane of glass view over all your sensitive corporate documents, making compliance checks faster and more reliable than ever before.

Core Capabilities

01 — List and Check File Security Metadata

The agent retrieves usage limits and detailed security information for your entire Digify account.

02 — Monitor Virtual Data Room Activity

You can get a complete overview of a specific data room, including its member list and current collaborative activity.

03 — Audit File Viewing Statistics

The system provides detailed analytics showing exactly who viewed your file and for how long they stayed on it.

04 — Quick Security Audit Summary

Get a fast, high-level summary that combines both file view counts and current security access rights.

05 — List All Uploaded Secure Files

The agent generates a comprehensive list of every secure file currently stored in your Digify account.

06 — Identify File Recipients and Rights

You can list everyone who has access to a specific secure document and what their exact viewing permissions are.

One Click on Vinkius — From Prompt to Execution

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

01 First, you connect the Digify integration to your AI client using your Vinkius subscription. You'll need to provide your unique Digify API Key.

02 Next, you tell your agent what you need—for example, 'Who viewed the Q3 financials and for how long?' The agent then calls the necessary tool within the MCP.

03 Finally, the AI client processes the raw data from Digify and presents a natural language answer detailing who accessed the file, when they did it, and their specific permissions.

The bottom line is you get to audit complex document security and collaboration through simple conversation with your agent.

Built For

Legal, Compliance, and Corporate Development teams use this MCP when they need undeniable proof of who touched a sensitive file or needs an immediate status report on data room activity. If you deal with M&A, IP, or regulated client information, this is for you.

Legal Counsel

You check access logs to prove compliance and immediately verify the viewing rights of sensitive legal documents.

Compliance Officer

You run regular audits to track document lifecycles, identify expired files, and monitor overall security metadata for regulatory reporting.

Business Development Manager

You monitor prospect engagement with sales decks or proposals by checking detailed file access statistics on the fly.

What Changes When You Connect

01 Instant Compliance Checks: Instead of manually checking permissions, you can use the `list_file_recipients` tool to instantly verify who has been granted access to a secure asset.

02 Deep Analytics on Engagement: The `get_file_access_statistics` tool tells you exactly how long and from where every user viewed your file, turning raw data into actionable insights for sales.

03 Full Data Room Oversight: You can use `list_virtual_datarooms` to get a list of all active data rooms, ensuring no project is running without proper monitoring.

04 Streamlined File Management: Use the `list_secure_files` tool to pull a complete inventory of your assets, helping you quickly spot what needs updating or archiving.

05 Automated Risk Mitigation: The agent can use `list_expired_secure_files` to identify documents that are past their due date, reducing organizational risk before it becomes a problem.

Real-World Applications

M&A Due Diligence Cleanup

Your agent runs a check using `list_secure_files` to inventory all documents related to the merger. It then uses `get_file_access_statistics` on key files, giving you an immediate report showing which external parties viewed the financials and for how long.

Sales Proposal Monitoring

A BD professional asks their agent to check engagement with a client proposal. The agent uses `get_file_access_statistics` and provides metrics on multiple recipients, letting you know which specific files received the most attention.

Compliance Audit Preparation

The compliance team asks for all currently protected assets. The agent uses both `list_secure_files` and `quick_file_audit`, providing a consolidated report on asset counts, security settings, and potential risks.

Data Room Access Review

You need to confirm who can view the pitch deck. The agent uses `list_file_recipients` against a specific file to list every person with access, allowing you to immediately revoke unnecessary permissions.

Patterns to Avoid

Ignoring Expiration Dates

✗ AVOID

A user manually checks the Digify dashboard and only sees files that are currently active. They miss the risk of assets nearing expiration.

✓ INSTEAD

Ask your agent to run `list_expired_secure_files`. This tool specifically searches for files reaching their end date, ensuring you address compliance risks proactively.

Missing Access Scope

✗ AVOID

A user assumes everyone who was part of the data room has current viewing rights and doesn't check permissions.

✓ INSTEAD

Use `get_dataroom_details` to see all members, then use `list_file_recipients` against a key document. This confirms both membership and specific file access.

Treating Data as Static

✗ AVOID

A team assumes that because they uploaded the documents months ago, nothing has changed regarding who viewed them or if the files are still necessary.

✓ INSTEAD

Ask your agent to run `get_file_access_statistics` and cross-reference it with `quick_file_audit`. This gives you a fresh view of usage metrics alongside current security status.

The Right Fit

Use Digify if your primary need is deep, auditable tracking of document activity and access control across data rooms. For example, use this MCP when checking who viewed an M&A proposal or running a compliance check on file expiration dates. Don't use it if you simply need to store files; that's basic cloud storage. If your goal is general communication history tracking (e.g., 'who emailed whom'), look at messaging integration tools instead.

This MCP focuses purely on the security lifecycle and usage metrics of protected documents.

Digify MCP for AI Agents: Monitoring Corporate Data Room Security

Manually managing secure files means clicking through dashboards, compiling spreadsheets of member lists, and cross-referencing viewing rights. You spend hours gathering reports just to answer one question: 'Did that external party see the final version?'

With this MCP, you tell your agent what you need —like monitoring a specific data room's members or checking detailed document analytics. The result is an immediate, conversational summary of security status and activity logs.

Digify MCP for AI Agents: Managing Compliance & File Access Control

Today, compliance requires multiple manual steps: listing all documents, checking their expiration dates, verifying the current recipient list, and then manually running an audit of who viewed them.

Now, you ask your agent to 'Audit the project data room for compliance.' It runs `list_secure_files`, identifies expired items using `list_expired_secure_files`, checks permissions with `list_file_recipients`, and compiles everything into one report.

Digify MCP: 10 Tools for Document Security Auditing

Use these tools to list assets, check access rights, retrieve detailed viewing statistics, and audit virtual data rooms in a single conversation.

#	TOOL	DESCRIPTION
01	`get_security_account_metadata`	Retrieves usage limits and general metadata for your entire Digify account.
02	`get_dataroom_details`	Pulls detailed settings, including the member list, for a specific virtual data room.
03	`get_secure_file_details`	Gets deep information and security rules attached to any individual secure file.
04	`get_file_access_statistics`	Retrieves detailed metrics showing exactly who viewed a file and for how long they spent viewing it.
05	`quick_file_audit`	Generates a quick summary combining both the view count and current security rights of a file.
06	`list_virtual_datarooms`	Provides a complete list of all virtual data rooms currently set up in your account.
07	`list_expired_secure_files`	Identifies secure files that have reached their predefined expiration date.
08	`list_secure_files`	Lists every single secure file you have uploaded and stored in Digify.
09	`list_file_recipients`	Shows all people who were granted access to a specific, protected document.
10	`search_secure_files`	Searches for secure files using keywords found in the file's filename.

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 viewing history for the 'Investor Pitch Deck' file.

📊 **File View Audit: Investor Pitch Deck**

USER	COMPANY	VIEWS COUNT	LAST VIEWED
john@firm.com	Global Capital	45	Today, 10:32 AM
jane@corp.com	Acme Holdings	18	Yesterday, 3:00 PM
sam@partner.net	Beta Group	9	Last week

Summary: The file has been viewed by 3 distinct parties over the last month.

U What's the status of our 'Q4 Financial Data Room'? Are there any access issues or members who haven't logged in?

🔎 **Data Room Status: Q4 Finance**

- **Files:** 78 secured documents.
- **Active Members:** 12 people (including your team).
- **Recent Activity:** 5 new files added this week.
- **Audit Note:** Two members, 'user_x' and 'user_y', have not accessed the room since last month.

Would you like to remove their viewing rights?

U List all secure assets we own and tell me if any of them are nearing expiration.

📁 **Digify Asset Inventory Report**

Found 124 total secured files.

- ✅ **Active & Good:** 105 files (Expiration: > 90 days).
- ⚠️ **Needs Review:** 12 files (Expires in 30-90 days). [See file IDs for details.]
- ❌ **Expired/Archived:** 7 files. These require immediate review and possible deletion.

Frequently Asked Questions

01 **How does Digify help me track who accessed sensitive documents?**

Digify provides detailed analytics showing exactly which users viewed the file, how long they kept it open, and from what geographical location. This gives you an auditable trail of every interaction.

02 **Can Digify help me manage multiple data rooms for different projects?**

Yes. You can list all virtual data rooms using the MCP to see everything your company is currently managing, making oversight simple and comprehensive.

03 **Is Digify good for compliance audits of file permissions?**

Absolutely. It lets you verify every recipient who has access to a document and what their specific rights are (view only, download allowed, etc.), which is crucial for legal proof.

04 **What if I need to know if any of my secure files have passed their expiration date?**

You can use the MCP to run a report that specifically identifies all secured assets that have reached or are nearing their predetermined expiration date, allowing you to mitigate risk early.

05 **Does Digify track activity for corporate development teams during M&A?**

Yes. It monitors member lists and collaborative activity within virtual data rooms, giving your team a clear picture of who is engaged with the deal materials.

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 `"digify": { "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

Digify 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 Digify. 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	Digify MCP
Server ID	`019d7585-ed41-70c5-b146-74116dedea75`
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/digify.