MCP SERVER | NO CODE | CLOUD HOSTED

Files.com MCP

Manage every file, folder, and permission with conversation.

Files.com MCP gives your AI client complete control over secure enterprise file storage. Use it to coordinate complex folder structures, manage user permissions, and monitor detailed audit logs across your company's most sensitive data. It lets you move beyond clicking through web interfaces by enabling conversational commands for everything from creating new directories to checking who has access to a specific document.

A+ Quality Score 100/100

file-transfer | secure-storage | audit-logs | cloud-sync | file-metadata | collaboration

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

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

Files.com MCP

8 tools available
Cloud-hosted on Vinkius

Managing files in a large organization isn't just about storing them; it's about knowing exactly who can touch what, and when they touched it. This MCP lets you connect your AI agent directly to your Files.com secure storage account. You can talk to your client and perform complex file operations—like listing entire folder hierarchies or retrieving specific metadata for a document—all through natural conversation.

Imagine needing to check the full activity history across multiple projects, or ensuring that only members of one group can delete certain asset types. Instead of opening three different dashboards, you ask your agent. It handles the complexity, giving you immediate answers on things like user access controls or where a file was last downloaded.

By connecting this MCP via Vinkius, you give any compatible AI client the power to manage your entire digital ecosystem. You keep your data secure and audit-ready without ever needing to remember an API key or navigate complicated web forms.

Core Capabilities

01 — Map folder structures

List all folders and files within a specific path in your cloud storage.

02 — Get file details

Retrieve comprehensive metadata, including download links, for any individual file you point to.

03 — Audit access controls

List users, groups, and specific permissions to verify who can do what in the system.

04 — Track activity changes

Query real-time or historical logs to see every upload, download, or deletion that happened.

05 — Manage directories and assets

Create new folders or delete outdated files programmatically using simple commands.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius.

02 Enter your Files.com API Key and Subdomain (like yourcompany.files.com) into the connection settings.

03 Start giving commands in any compatible AI client, and it performs file operations directly against your secure storage.

The bottom line is that you treat your entire corporate file system like a single conversation with your agent.

Built For

This MCP is built for the IT Administrator who needs to prove compliance instantly, the Operations Manager tracking assets across departments, or the Compliance Officer needing an instant audit trail. If you deal with shared files and access rules, this tool solves your clicking fatigue.

IT Administrator

Quickly checks folder permissions and verifies user account access without logging into multiple admin panels.

Operations Manager

Monitors file activity history across projects and creates new folders for departmental archives directly from the workspace.

Compliance Officer

Verifies audit logs and tracks entire file lifecycle changes to prove regulatory compliance via natural language queries.

What Changes When You Connect

01 Gain full visibility into your data by listing folders across the entire structure. Instead of navigating click-by-click to find a department's directory, you simply ask your agent to run `list_folders` and see the whole map instantly.

02 Never lose track of critical assets again. Use `get_file_details` to pull complete file metadata for any document, giving you direct download links and version information in one go.

03 Prove who accessed what, when they accessed it, and if it was allowed. By querying the `list_activity_history`, you get a reliable audit trail that tracks uploads, downloads, and deletions instantly.

04 Keep your data secure by verifying access rights easily. You can run `list_permissions` to check specific user roles against folder rules without opening complex security dashboards.

05 Maintain clean governance using simple commands. Need a new archive? Use `create_folder`. Found junk assets? Run `delete_file` and keep the system tidy.

Real-World Applications

Checking for compliance violations

A Compliance Officer needs to know if any employee downloaded a sensitive contract file last month. They ask their agent to check the `list_activity_history` tool, and the AI immediately pulls a filtered log showing every user who interacted with that specific document.

Reorganizing an old department's data

An Operations Manager needs to consolidate all assets from a dissolved team. They ask their agent to run `list_folders` to map the entire directory structure, then use `create_folder` to build the new archive and move everything safely.

Onboarding a new team member

The IT Administrator needs to grant access rights. They ask the agent to run `list_users` to confirm the account exists, then use `list_permissions` to assign group-level read/write access directly, bypassing manual GUI clicks.

Recovering deleted files

An employee realizes they accidentally removed a critical folder. They instruct their agent to check the full file activity history using `list_activity_history` and get details on the deletion event, speeding up recovery efforts.

Patterns to Avoid

Manual permission checking

✗ AVOID

Logging into the web UI, manually navigating to the folder, finding the 'Permissions' tab, and cross-referencing user names against group roles.

✓ INSTEAD

Just ask your agent to run `list_permissions` on the specific directory. It gives you a clear list of every group and their exact access level in seconds.

Guessing file paths

✗ AVOID

Trying to remember if a file was stored under '/Client/2023' or '/Clients/2023', resulting in multiple failed searches.

✓ INSTEAD

Ask your agent to use `list_folders` at the root level, and then drill down into the correct path using conversational prompts. You never have to guess again.

Forgetting who owns a document

✗ AVOID

A manager can't find out which department has ownership or if specific users are blocked from seeing certain reports.

✓ INSTEAD

Run `list_users` combined with `list_permissions`. This pairing of tools quickly tells you every user and group that interacts with your files.

The Right Fit

Use this MCP if your core problem is file governance, access control, or auditing. If you need to know *who* can do *what* in a folder, or if you need to track the history of changes (uploads, deletions), this tool is perfect. It lets you run `list_activity_history` and verify permissions via `list_permissions`. Don't use it if your only goal is to search for content within file bodies—you need a dedicated document indexing service for that. If you just want to move files around without needing audit trails, standard cloud syncing tools work fine. But the moment compliance or security becomes part of the equation, this MCP gives you the necessary operational depth.

The Headache of Enterprise File Governance

Today, managing files means logging into a web portal, clicking through folder structures, and opening separate dashboards just to check who has access. To audit a single project, you often have to copy dates, cross-reference user IDs in one sheet, and then manually navigate another section to see the activity log. It’s slow, it's error-prone, and it takes up huge chunks of an engineer's day.

With this MCP, you talk to your AI agent instead. You simply ask, 'Show me all users who can edit files in the Q3 folder.' The agent runs the necessary checks—combining `list_users` with `list_permissions` —and gives you a clean, immediate list. It's not just faster; it changes the nature of the work.

Files.com MCP Gives You Complete Control Over Your File Lifecycle

You no longer have to manually track which files are old or need moving. Instead, you can ask the agent to list all folders and identify directories that haven't been touched in six months. Then, with one prompt, it runs `create_folder` for an archive and prepares assets for deletion.

The result is a system where file management isn't a series of painful clicks; it’s a conversational command. You maintain full control over your data security and structure without ever leaving the chat window.

Files.com MCP: 8 File Management Tools

These tools allow you to programmatically perform every file operation needed for enterprise governance, from listing users to deleting outdated assets.

#	TOOL	DESCRIPTION
01	`create_folder`	Creates a new folder inside your Files.com storage account.
02	`delete_file`	Removes an outdated file or entire directory from the system.
03	`get_file_details`	Retrieves all specific metadata for a given file path, including download links.
04	`list_folders`	Lists the contents and directories at any specified location in Files.com.
05	`list_user_groups`	Displays all organizational groups defined within your company's account.
06	`list_activity_history`	Retrieves a chronological list of every file action, like downloads or deletions.
07	`list_permissions`	Shows detailed access rights for users and groups on specific files or folders.
08	`list_users`	Outputs a list of all current user accounts in your Files.com organization.

See It in Action

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

U List all files in the '/Client-Projects' folder.

I've retrieved the folder contents. Inside '/Client-Projects' you have: 'Contract_v1.pdf', 'Design_Mockup.png', and 'Project_Brief.docx'. Which one would you like more details on?

U Show me the activity history for the last 24 hours.

Fetching audit logs... In the last 24 hours, there were 15 activities: 10 uploads, 3 downloads by Mike Ross, and 2 folder deletions. Would you like a detailed report on the deletions?

U Create a new folder called '/Archive-2023'.

Success! The folder '/Archive-2023' has been created in your Files.com account. You can now start moving your legacy assets into this directory.

Frequently Asked Questions

01 **How does Files.com MCP help with compliance auditing?**

It provides immediate access to historical records using `list_activity_history`. You can query specific timeframes or actions (like deletions) to generate an instant, auditable report without manual searching.

02 **What if I need to rename a folder?**

This MCP focuses on creation and deletion. While you can use `list_folders` to see the names, renaming usually requires a different tool, but you can programmatically clean up by running `delete_file` and then creating a new one.

03 **Can I check permissions for multiple folders at once using Files.com MCP?**

Yes, you can provide the agent with a list of paths, and it runs `list_permissions` against all specified locations, giving you an aggregated view of access rights.

04 **What information do I get from using list_users?**

Running this tool lists every user account in your organization. This helps administrators verify which people need to be added or removed from specific project groups before setting up new permissions.

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 `"filescom": { "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

Files.com 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 Files.com. 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	Files.com MCP
Server ID	`019dd0f0-2fe5-7232-b82f-c69dc4cde78b`
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/filescom.