MCP SERVER | NO CODE | CLOUD HOSTED

Frontify MCP

Manage every asset and brand guideline from conversation.

Frontify connects your AI agent directly to your Digital Asset Management (DAM) system, letting you manage brand guidelines, audit metadata, and orchestrate entire project lifecycles using natural conversation. You can list all active workspaces, update asset details across brands, check usage limits, or invite team members—all without clicking through complex portals.

A+ Quality Score 100/100

digital-asset-management | brand-guidelines | creative-collaboration | metadata-management | workspace-orchestration

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

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.

Frontify MCP

10 tools available
Cloud-hosted on Vinkius

Connecting your Frontify account lets you treat your digital assets like a simple database query. Instead of navigating deep folders and manually checking metadata fields, your agent handles it all. You can start by listing every active workspace to figure out where specific project files live. From there, you can pull detailed records for any asset or check the precise rules governing brand guidelines across different departments. Need to update a title or description? Just tell your agent; it modifies the global asset boundaries for you using GraphQL logic. You'll also manage people and permissions—check who has access or invite new users directly into project workspaces. If an asset needs to go, your agent can permanently delete it. This kind of deep integration is what Vinkius offers across its catalog, letting any MCP-compatible client give you true control over brand assets through conversation.

Core Capabilities

01 — Discovering project structures

List all attached structured rules to view and explore collaborative workspaces.

02 — Managing asset details

Retrieve detailed metadata for any project asset or update global attributes like titles and descriptions.

03 — Auditing brand compliance

Identify specific brand rules or documentation trees to ensure assets meet design standards.

04 — Controlling user access

Check your team's current identity schemas and invite new users into designated project workspaces.

05 — Running advanced queries

Use native GraphQL strings to run custom, highly specific data searches across the DAM.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your Frontify Domain and Access Token in the Vinkius Marketplace.

02 Connect your preferred AI agent (like Claude or Cursor) to the integrated client.

03 Start giving natural language instructions, like 'Show me all brand guidelines for Q3,' and let your agent execute the necessary reads and writes.

The bottom line is that you get a single conversational interface to manage every aspect of your digital asset life cycle.

Built For

This MCP is for Brand Managers, Content Marketers, and Creative Directors who spend too much time clicking through complex DAM portals just to find a guideline or update an asset name. If you're tired of manually checking permissions or running ad-hoc reports on asset metadata, this tool saves hours.

Brand Manager

Using this MCP, they can quickly audit brand portals and ensure all published assets follow current style rules without navigating multiple documentation trees.

Content Marketer

They use the agent to look up specific guidelines or update asset metadata for campaigns across various global namespaces using natural language prompts.

Creative Director

A director can check team access and audit who has permission to view assets in critical project workspaces, verifying permissions in real-time.

What Changes When You Connect

01 Avoid tedious manual navigation. You can list all workspace projects or retrieve project assets just by asking your agent, skipping the complex folder hierarchy entirely.

02 Maintain perfect brand compliance instantly. The MCP lets you list brand guidelines to verify that any team member uses the correct rules for UI/UX constraints before publishing.

03 Update metadata globally without logging into multiple tools. Use patch_asset_metadata to change titles or descriptions across all global asset boundaries in one go.

04 Control user permissions easily. Need someone added? The invite_workspace_user tool sends automated access checks and places new users directly into the right project workspace.

05 Deep diagnostic capability. If you're a developer, execute_graphql_payload lets you test complex queries against the DAM using native GraphQL strings.

06 Monitor usage limits instantly. Use get_account_limits to check specific picture constraints or media quotas before launching a major campaign.

Real-World Applications

Onboarding a new designer

A creative director needs to grant access to a newly hired contractor. Instead of emailing manual links, they ask their agent to use invite_workspace_user for the contractor's email and the specific project workspace. The MCP handles the role routing automatically.

Preparing for an audit

A brand manager needs to prove compliance across all global brands. They ask the agent to list_native_brands, then run list_brand_guidelines to pull every current documented rule set and check against asset metadata.

Cleaning up old assets

A marketing team is retiring an entire product line. They ask their agent to identify all related project assets via get_project_assets, confirm they are safe to remove, and then use wipe_media_asset to permanently take them offline.

Troubleshooting asset access

A developer notices a user can't see an asset. They check the structural matching using list_platform_users to verify the correct identity schema, and then use get_account_limits to ensure the account hasn't hit its picture quota.

Patterns to Avoid

Manually updating metadata

✗ AVOID

A marketer has 50 assets across 3 brands and needs to change the description. They open the DAM, find Brand A's project, download the list, update a spreadsheet, and then manually upload 15 times.

✓ INSTEAD

Instead, tell your agent to run patch_asset_metadata for all necessary attributes, specifying the changes across the required brand namespaces. It handles the bulk mutation safely.

Guessing the correct API call

✗ AVOID

A developer writes a complicated GraphQL query, but misses one nested relationship field (like 'parent_folder'). The request fails with an ambiguous error code.

✓ INSTEAD

Use execute_graphql_payload to test and debug your exact custom queries against bounded routing spaces. This ensures the complex structure you need is properly validated before deployment.

Forgetting project scope

✗ AVOID

A user wants to delete a file but isn't sure which 'global namespace' it belongs to, so they try deleting it via a general account cleanup tool and fail.

✓ INSTEAD

First, use list_workspace_projects to identify the correct structured rules. Then, use get_project_assets on that specific project before attempting any deletion or mutation.

The Right Fit

Use this MCP if your workflow requires deep interaction with multiple layers of asset data—you need to read metadata, check user permissions, and update content across defined projects. If you frequently ask questions like 'Which assets belong to Brand X, owned by User Y, that haven't been updated in 90 days?' then this is for you.

Don't use this if all you need is a simple file upload or basic viewing of an asset. For those tasks, a standard DAM viewer will suffice. If your task involves complex data filtering, querying multiple interconnected records (like checking both project assets AND brand guidelines), or performing mass updates across different brands, then the granular control provided by tools like list_brand_guidelines and execute_graphql_payload is necessary.

The struggle of cross-platform asset governance

Today, updating a key piece of brand documentation—like the approved usage text for a new product line—requires painful manual steps. You log into the DAM portal, find the right global namespace, navigate through potentially dozens of nested folders to locate the correct project schema, and then manually edit the metadata field, hoping you didn't miss any related assets in other brand portals.

With this MCP, that entire process becomes a conversation. You simply tell your agent, 'Update the usage text for Product Line Z.' The system executes the necessary mutations across all relevant asset boundaries, ensuring every linked piece of content is updated without you ever touching a folder structure.

Frontify MCP: Total control over brand assets

You eliminate the need to jump between separate systems just to check permissions or audit guidelines. Instead of checking roles in one place and metadata in another, your agent orchestrates it all—you can list_platform_users for an identity audit and then run get_project_assets on the same day.

The result is a single source of truth visible through natural language. You stop managing clicks and start directing outcomes.

Frontify: 10 Tools for DAM Management

Use these tools to discover, audit, update, and control every aspect of your digital assets and brand guidelines directly from your AI agent.

#	TOOL	DESCRIPTION
01	`wipe_media_asset`	Permanently removes specific media assets from the system.
02	`execute_graphql_payload`	Runs advanced, custom queries inside the Headless Frontify DAM using GraphQL code.
03	`get_account_limits`	Checks your account's internal limits for specific types of media content.
04	`get_project_assets`	Retrieves a list and details of all assets tied to a given project workspace.
05	`list_native_brands`	Identifies the major, global namespaces registered in your account.
06	`list_brand_guidelines`	Finds specific brand rules and documentation trees that dictate usage constraints.
07	`list_workspace_projects`	Lists all defined project schemas to help you discover available collaborative workspaces.
08	`list_platform_users`	Retrieves a structural list of all identity records and user accounts in the system.
09	`invite_workspace_user`	Automatically adds an email address to a specified project workspace, granting them access.
10	`patch_asset_metadata`	Updates general metadata for assets across the system, such as changing titles or descriptions.

See It in Action

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

U List all projects in my Frontify workspace

Retrieving projects... I found 3 active workspaces: 'Logo Guidelines', 'Q2 Marketing Campaign', and 'Social Media Assets'. Which one would you like to explore for assets?

U Show me the brand guidelines for 'Acme Corp'

Retrieving guidelines... For 'Acme Corp', I found 2 registered portals: 'Global Brand Identity' and 'Technical Design System'. I can retrieve specific UI/UX constraints or rules from either portal for you.

U Invite 'designer@example.com' to project 'abc-123'

Invitation sent! I've commanded Frontify to add designer@example.com to project abc-123. They will receive an email to join the workspace and access the assets immediately.

Frequently Asked Questions

01 **How do I use Frontify MCP to check my storage limits?**

You use the get_account_limits tool. Simply ask your agent to inspect the deep internal arrays mitigating specific picture constraints, and it will report back exactly what you're nearing.

02 **Can Frontify MCP update multiple asset descriptions at once?**

Yes, that's what patch_asset_metadata does. You can tell your agent to substitute attributes like titles or descriptions across many global assets simultaneously.

03 **What if I need to run a query not listed in Frontify MCP?**

Use execute_graphql_payload. This tool lets you input native GraphQL strings, giving you access to the entire depth of your DAM's routing spaces for advanced queries.

04 **Does Frontify MCP help with user onboarding?**

It does. You can use invite_workspace_user to automatically send validation checks and add a new team member to the correct project workspace with one command.

05 **Which tool do I use to see what projects exist?**

Use list_workspace_projects. This tool enumerates all attached structured rules, giving you a full overview of every collaborative workspace available in your account.

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 `"frontify": { "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

Frontify 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 Frontify. 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	Frontify MCP
Server ID	`019d75a1-8dac-73ed-aef1-6cd10706aaf4`
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/frontify.