

Connect D3 domain intelligence to Claude and other AI assistants

Version 1.0 · March 2026 · domain-due-diligence.com

Client	URL / Info	Support
Claude Code	claude.ai/code	Full MCP support
Claude Desktop	claude.ai/download	Full MCP support
Claude for Work	Via org settings	Team-wide config
Custom MCP client	MCP 2024-11-05+	SSE transport

INTRODUCTION

The D3 MCP server implements the Model Context Protocol (MCP), allowing AI assistants such as Claude to directly invoke D3 domain intelligence tools. Users can ask natural-language questions like "Check if mybrand.com is available" or "Run a security audit on example.com" and Claude will orchestrate the scan automatically.

SETUP & CONFIGURATION

Step 1 — Create an API key in **Settings** → **API & MCP**. Copy the plaintext (shown once only) and complete the sandbox checklist.

Step 2a — Configure Claude Code (~/.claude/claude_desktop_config.json):

```
# claude_desktop_config.json
```

```
{
  "mcpServers": {
    "d3": {
      "url": "https://api.domain-due-diligence.com/api/mcp/sse",
      "headers": {
        "Authorization": "Bearer d3_live_your_key_here"
      }
    }
  }
}
```

Step 2b — Claude Desktop: open **Settings** → **Developer** → **MCP Servers** and add:

```
Server URL: https://api.domain-due-diligence.com/api/mcp/sse
Header name: Authorization
Header value: Bearer d3_live_your_key_here
```

AVAILABLE TOOLS

MCP

Start a D3 scan. Returns a scanId — poll get_scan_status for progress.
tools/scan_domain

Parameter	Type	Required	Description
domain	string	yes	Domain name or brand (e.g. "example.com")
product	string	yes	explorer security_audit valuation due_diligence
tlds	string[]	—	TLD list e.g. ["com","nl"]

```
{ "domain": "example.com", "product": "security_audit" }

# Response
{ "scan_id": "cm7x...", "status": "QUEUED", "credits_debited": 7 }
```

MCP

Check status: QUEUED, RUNNING, COMPLETED or FAILED.
tools/get_scan_status

Parameter	Type	Required	Description
scan_id	string	yes	The scanId returned by scan_domain

```
{ "scan_id": "cm7x..." }

# Response when complete
{ "scan_id": "cm7x...", "status": "COMPLETED", "overall_score": 78 }
```

MCP

Get the full D3 Certified Report for a completed scan.
tools/get_scan_report

Parameter	Type	Required	Description
scan_id	string	yes	The scanId of a completed scan

```
{ "scan_id": "cm7x..." }
# Returns full report with connectors, AI summary, SHA-256 hash
```

MCP

List all scan products with credit costs. No parameters required.
tools/list_scan_products

```
{ } // no parameters

# Response
{ "products": [ { "slug": "explorer", "credit_cost": 5 }, ... ] }
```

MCP

Quick brand/domain availability check across multiple TLDs (5 credits).
tools/check_availability

Parameter	Type	Required	Description
brand	string	yes	Brand name or domain SLD (e.g. "mybrand")
tlds	string[]	—	Defaults to ["com", "nl", "be", "net", "org"]

```
{ "brand": "mybrand", "tlds": ["com", "nl", "be"] }
```

TYPICAL WORKFLOW

A complete scan workflow involves three tool calls:

1	scan_domain	Start the scan — get a scanId
2	get_scan_status	Poll every 15–30s until COMPLETED
3	get_scan_report	Retrieve full results and AI summary

Example Claude conversation:

```
User: Run a security audit on example.com and summarise the risks

Claude: [calls scan_domain - product="security_audit"]
Scan started (scan_id: cm7x...). Checking status...

[calls get_scan_status - RUNNING, waiting 20s...]
[calls get_scan_status - COMPLETED]
[calls get_scan_report]

Overall score: 78/100 (Medium risk)
- DNS & Email: DKIM missing (score 72)
- WHOIS: Domain expires 2030, DNSSEC signed (score 85)
- Typosquatting: 8 lookalikes detected (score 65)
SHA-256 hash: a3f9d2c1...
```

SANDBOX MODE

All new API keys start in sandbox mode. All MCP tools return realistic mock data based on example.com — instantly, 0 credits. Complete the sandbox checklist in Settings → API & MCP and click "Activate production" next to the MCP section.