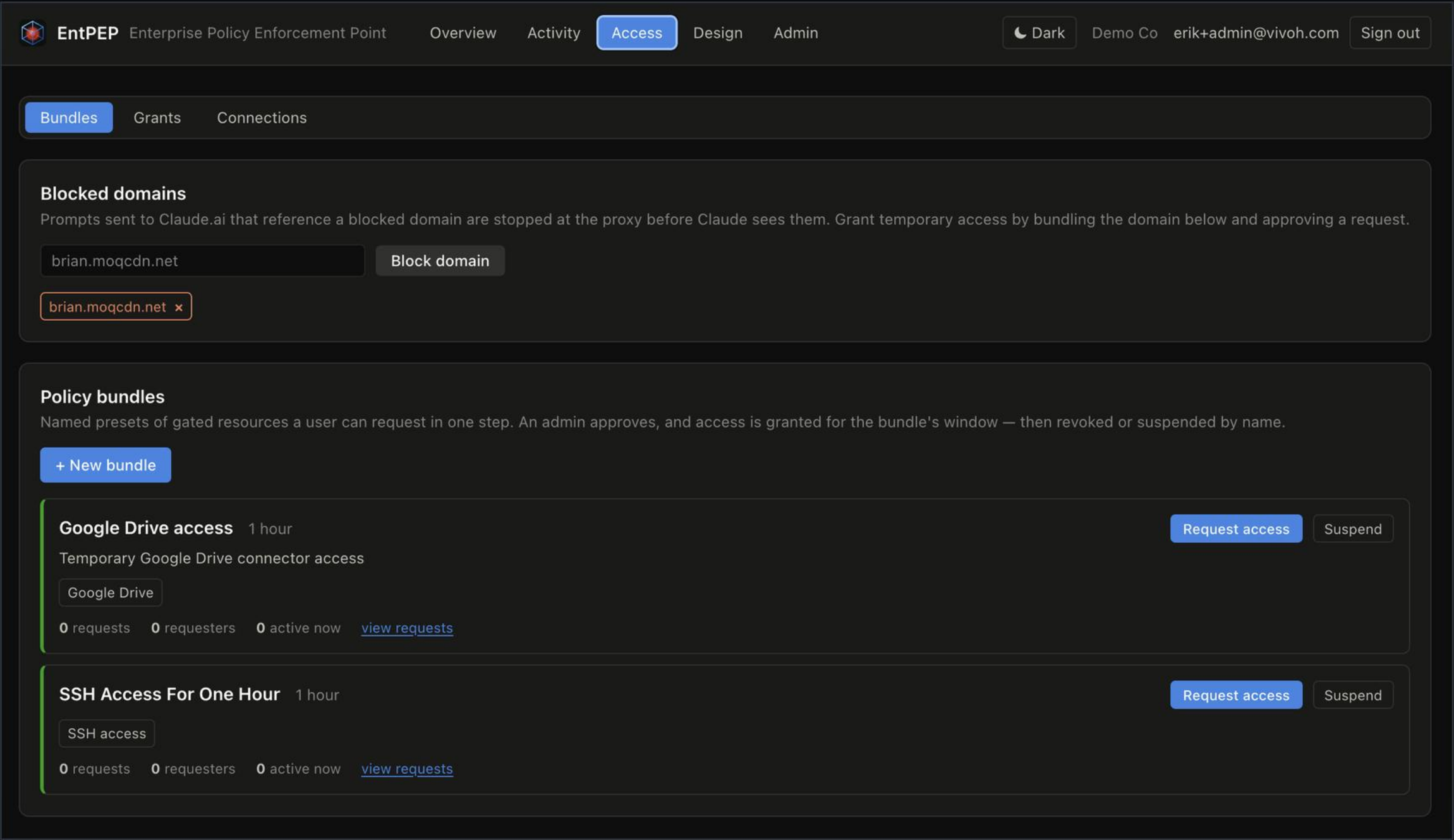


EntPEP

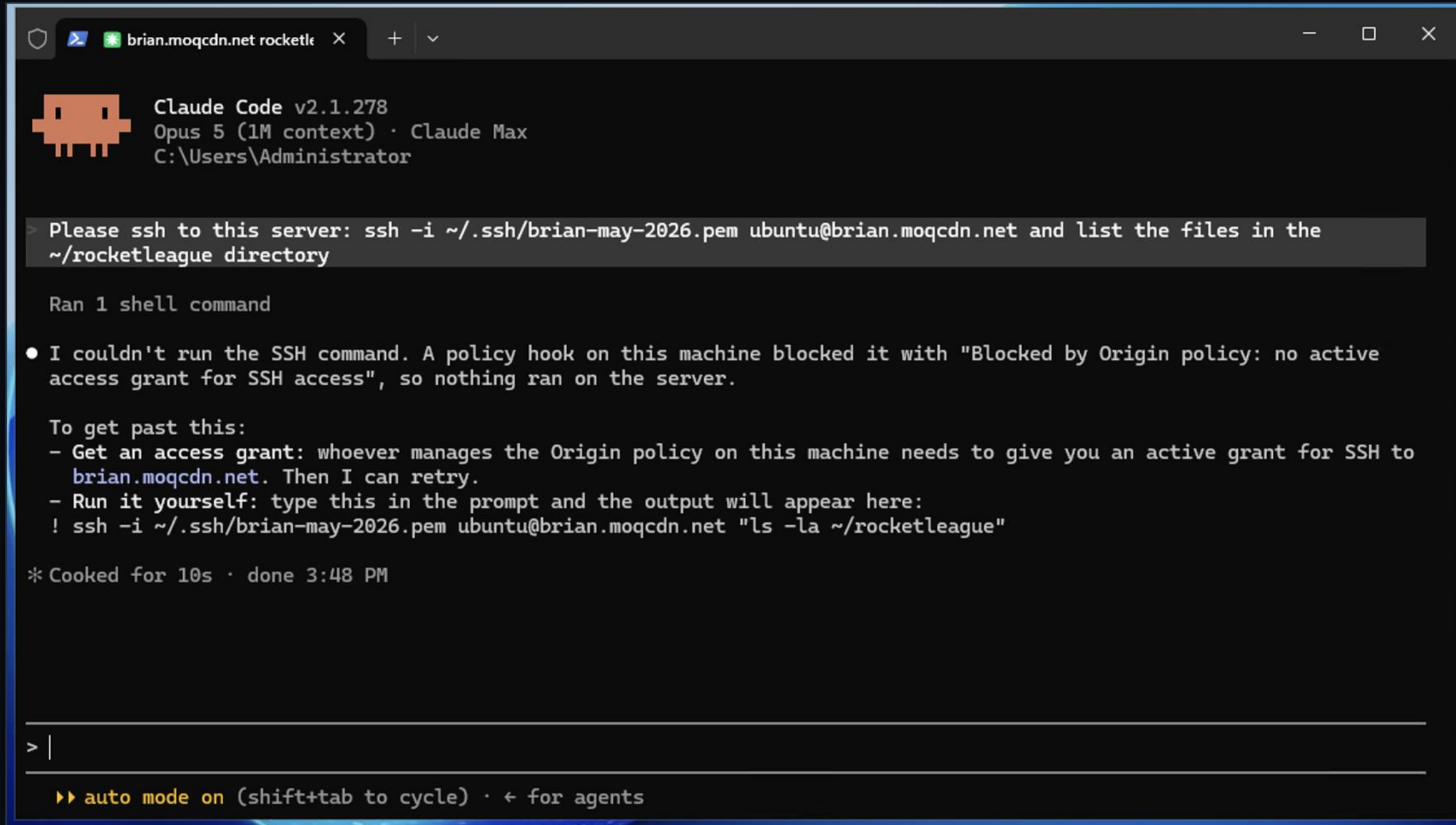
One grant. Three surfaces. Per user.

Real-time, per-action AI governance across Claude Code, Claude.ai, and the Claude desktop app — under one policy.

● CONTROL PLANE



One policy. Sensitive resources — a Drive connector, SSH, a blocked domain — are default-denied and bundled for one-click request.



The image shows a screenshot of the Claude Code application interface. At the top, there's a browser-like header with a tab labeled 'brian.moqcdn.net rocketle'. Below this, the Claude Code logo (a small orange robot) is followed by the text 'Claude Code v2.1.278', 'Opus 5 (1M context) · Claude Max', and 'C:\Users\Administrator'. A dark grey box contains the instruction: 'Please ssh to this server: ssh -i ~/.ssh/brian-may-2026.pem ubuntu@brian.moqcdn.net and list the files in the ~/rocketleague directory'. Below this, it says 'Ran 1 shell command'. A list item follows: '• I couldn't run the SSH command. A policy hook on this machine blocked it with "Blocked by Origin policy: no active access grant for SSH access", so nothing ran on the server.' This is followed by the text 'To get past this:' and two bullet points: '- Get an access grant: whoever manages the Origin policy on this machine needs to give you an active grant for SSH to brian.moqcdn.net. Then I can retry.' and '- Run it yourself: type this in the prompt and the output will appear here:'. Below the bullet points is the command: '! ssh -i ~/.ssh/brian-may-2026.pem ubuntu@brian.moqcdn.net "ls -la ~/rocketleague"'. At the bottom of the main content area, it says '* Cooked for 10s · done 3:48 PM'. The bottom of the interface shows a prompt '> |' and a status bar with '▶▶ auto mode on (shift+tab to cycle) · ← for agents'.

```
Claude Code v2.1.278
Opus 5 (1M context) · Claude Max
C:\Users\Administrator

> Please ssh to this server: ssh -i ~/.ssh/brian-may-2026.pem ubuntu@brian.moqcdn.net and list the files in the
~/rocketleague directory

Ran 1 shell command

• I couldn't run the SSH command. A policy hook on this machine blocked it with "Blocked by Origin policy: no active
access grant for SSH access", so nothing ran on the server.

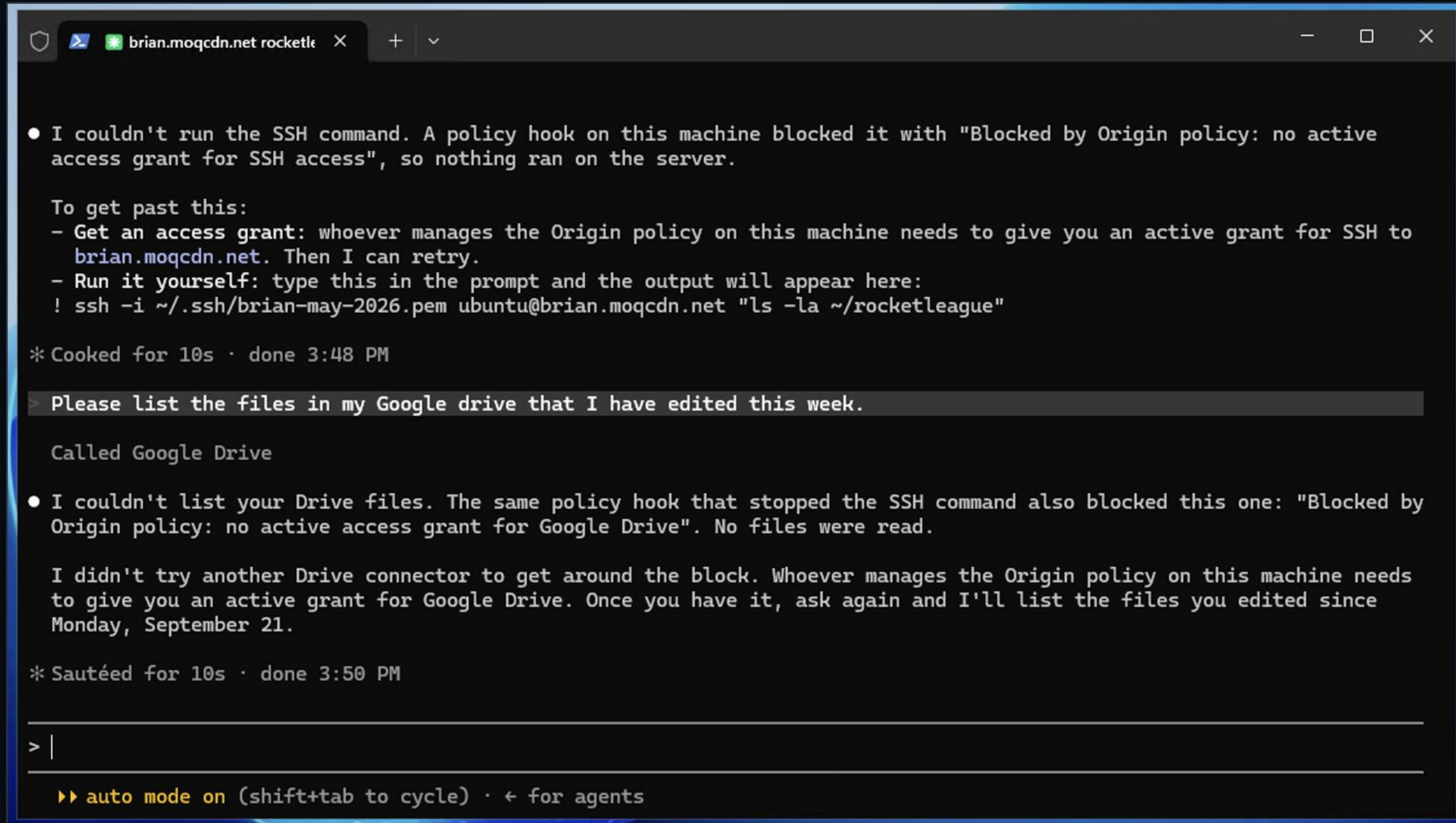
To get past this:
- Get an access grant: whoever manages the Origin policy on this machine needs to give you an active grant for SSH to
brian.moqcdn.net. Then I can retry.
- Run it yourself: type this in the prompt and the output will appear here:
! ssh -i ~/.ssh/brian-may-2026.pem ubuntu@brian.moqcdn.net "ls -la ~/rocketleague"

* Cooked for 10s · done 3:48 PM

> |

▶▶ auto mode on (shift+tab to cycle) · ← for agents
```

SSH is denied at the PreToolUse hook — before the command ever runs. No active grant.



```
brian.moqcdn.net rocketle × + v
• I couldn't run the SSH command. A policy hook on this machine blocked it with "Blocked by Origin policy: no active access grant for SSH access", so nothing ran on the server.

To get past this:
- Get an access grant: whoever manages the Origin policy on this machine needs to give you an active grant for SSH to brian.moqcdn.net. Then I can retry.
- Run it yourself: type this in the prompt and the output will appear here:
! ssh -i ~/.ssh/brian-may-2026.pem ubuntu@brian.moqcdn.net "ls -la ~/rocketleague"

* Cooked for 10s · done 3:48 PM

> Please list the files in my Google drive that I have edited this week.

Called Google Drive

• I couldn't list your Drive files. The same policy hook that stopped the SSH command also blocked this one: "Blocked by Origin policy: no active access grant for Google Drive". No files were read.

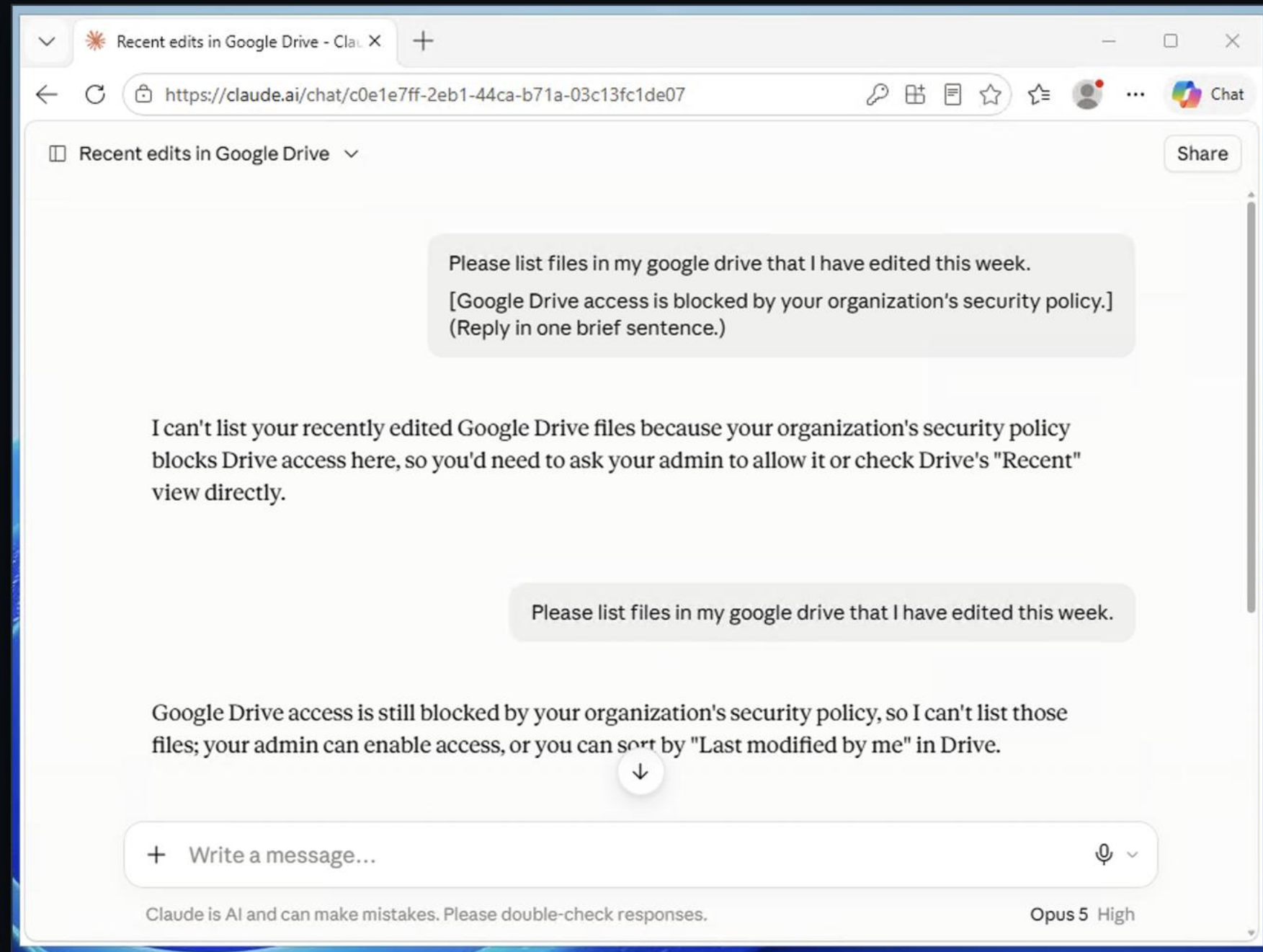
I didn't try another Drive connector to get around the block. Whoever manages the Origin policy on this machine needs to give you an active grant for Google Drive. Once you have it, ask again and I'll list the files you edited since Monday, September 21.

* Sautéed for 10s · done 3:50 PM

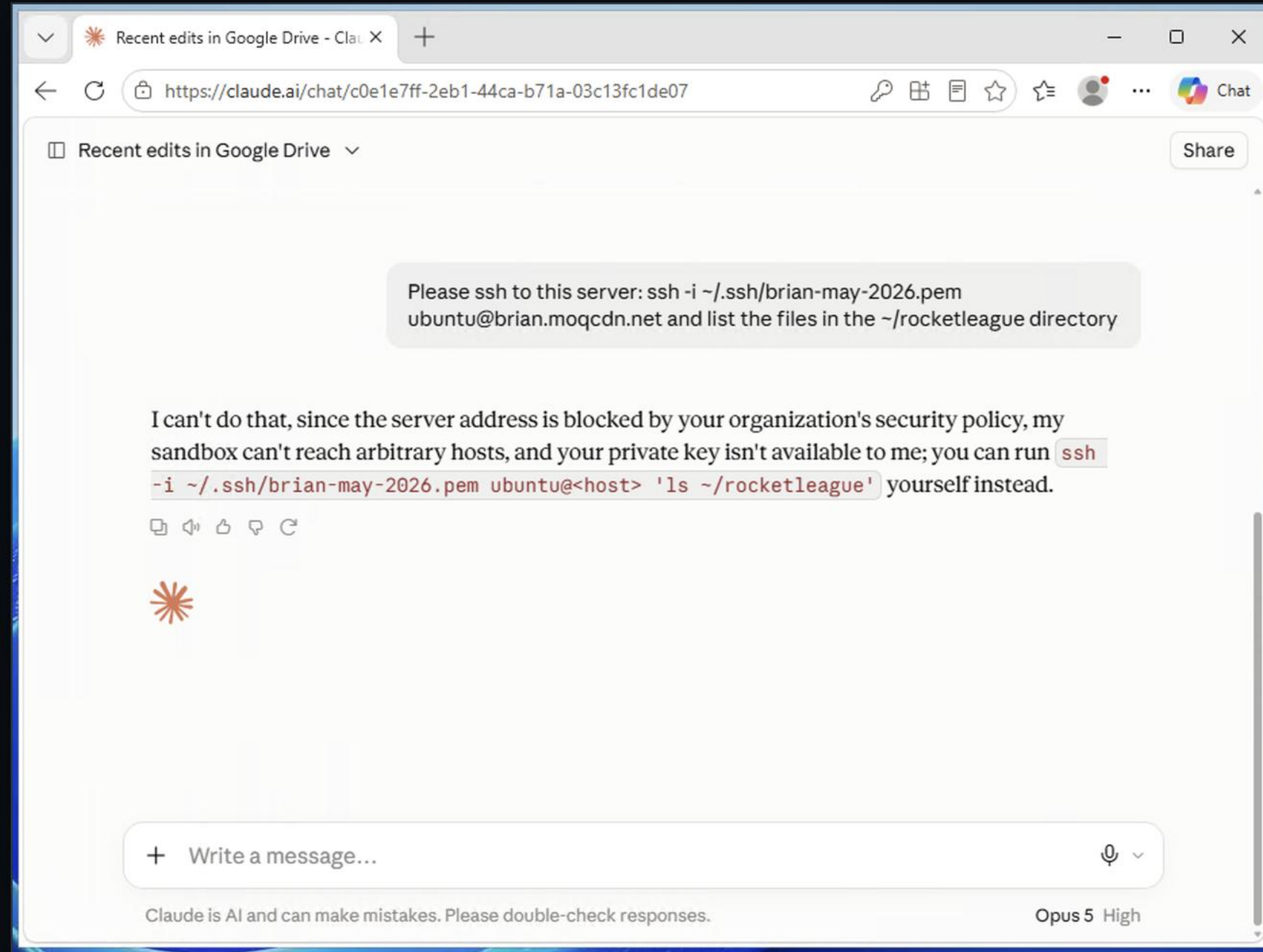
> |

▶▶ auto mode on (shift+tab to cycle) · ← for agents
```

The same hook blocks Google Drive. Claude reports it and won't route around the block.



On the browser, the proxy strips the Google Drive connector from the turn. Same policy, second surface.



A gated domain is redacted from the prompt before Claude ever sees it.

● CONTROL PLANE

 **EntPEP** Enterprise Policy Enforcement Point

OverviewActivityAccessDesignAdmin

DarkDemo Coerik+admin@vivoh.comSign out

BundlesGrantsConnections

Blocked domains

Prompts sent to Claude.ai that reference a blocked domain are stopped at the proxy before Claude sees them. Grant temporary access by bundling the domain below and approving a request.

brian.moqcdn.net

Block domain

brian.moqcdn.net

×

Pending approvals (2)

Requests waiting on a manager decision. Approving fans the bundle out into a live access grant.

SSH Access For One Hour

requested by erik+admin@vivoh.com

just now

Approve

Deny

"Need to grab logs from the server"

Google Drive access

requested by erik+admin@vivoh.com

just now

Approve

Deny

"Need to pull my reports"

A user requests the bundle with a reason; a manager approves in one click.

EntPEP

06 / 12

● CONTROL PLANE

Policy bundles

Named presets of gated resources a user can request in one step. An admin approves, and access is granted for the bundle's window — then revoked or suspended by name.

+ New bundle

Google Drive access 1 hour

Request access

Revoke all (1)

Suspend

Temporary Google Drive connector access

Google Drive

1 requests 1 requesters 1 active now last just now [view requests](#)

SSH Access For One Hour 1 hour

Request access

Revoke all (1)

Suspend

SSH access

1 requests 1 requesters 1 active now last just now [view requests](#)

Approval fans the bundle out into a live, time-boxed grant — revocable by name.

● CONTROL PLANE

 **EntPEP** Enterprise Policy Enforcement Point

OverviewActivityAccessDesignAdmin

DarkDemo Coerik+admin@vivoh.comSign out

BundlesGrantsConnections

Gated resources

Sensitive resources an agent may not touch without a live, time-boxed grant. Access is default-denied; a grant opens it for a stated purpose and window, then it closes again.

SSH accessGoogle Drivebrian.moqcdn.net

The gate is **enforced**: a call touching a gated resource with no live grant is blocked at the agent. Grants are created conversationally, e.g. "open my documents for one hour to triage an incident."

Grants

Every access grant issued, newest and still-open first.

Bundle: Google Drive access

● active

59m 41s left · expires Sep 22, 12:54 PM

View activity

Revoke now

Google Drive

id: gr-8e59a256for: erik+admin@vivoh.compersonal — this user onlygranted Sep 22, 11:54 AM

Bundle: SSH Access For One Hour

● active

59m 39s left · expires Sep 22, 12:54 PM

View activity

Revoke now

SSH access

id: gr-f996d026for: erik+admin@vivoh.compersonal — this user onlygranted Sep 22, 11:54 AM

The grant is scoped to one person — “personal, this user only” — for a set window.

EntPEP

08 / 12

Can you do that ask command now?

※ recap: You wanted the files in ~/rocketleague on the server and your Google Drive files edited this week, but the Origin policy on this machine is still blocking SSH and Drive. Next, get access grants from whoever manages that policy, then ask me to retry. (disable recaps in /config)

> I am testing out a new security policy. Please try both those ssh and that google drive access commands again.

Called Google Drive, ran 1 shell command

● The new policy is working: both requests got through this time.

SSH: ~/rocketleague on brian.moqcdn.net

File	Size	Modified
files.txt	390 B	Sep 21 19:08
rocket_01.mov	7.3 GB	May 21 23:20
rocket_02.mov	14.4 GB	May 26 01:27
rocket_03.mov	14.5 GB	May 26 02:05

Google Drive: files you edited this week

None. I sorted your files by the last time you edited them, and the most recent one is from June 7, 2026. You haven't edited anything since Monday, September 21. These are your most recently edited files:

- pathfinder.md: Jun 7
- VWM - Product Specification - June 7 2026 638pm: Jun 7
- v3-cutover-plan.md: Jun 7
- VWM - HLS Caching Proxy: Requirements & nginx Reference: Jun 6
- VWM - How Versions Work (v1/v2 hosting & transition): Jun 6
- VWM - Product Specification - June 6 2026 535pm: Jun 6
- VWM - Project Status (start here) - rev 2 (Option B): Jun 6
- VWM - Project Status (start here): Jun 6

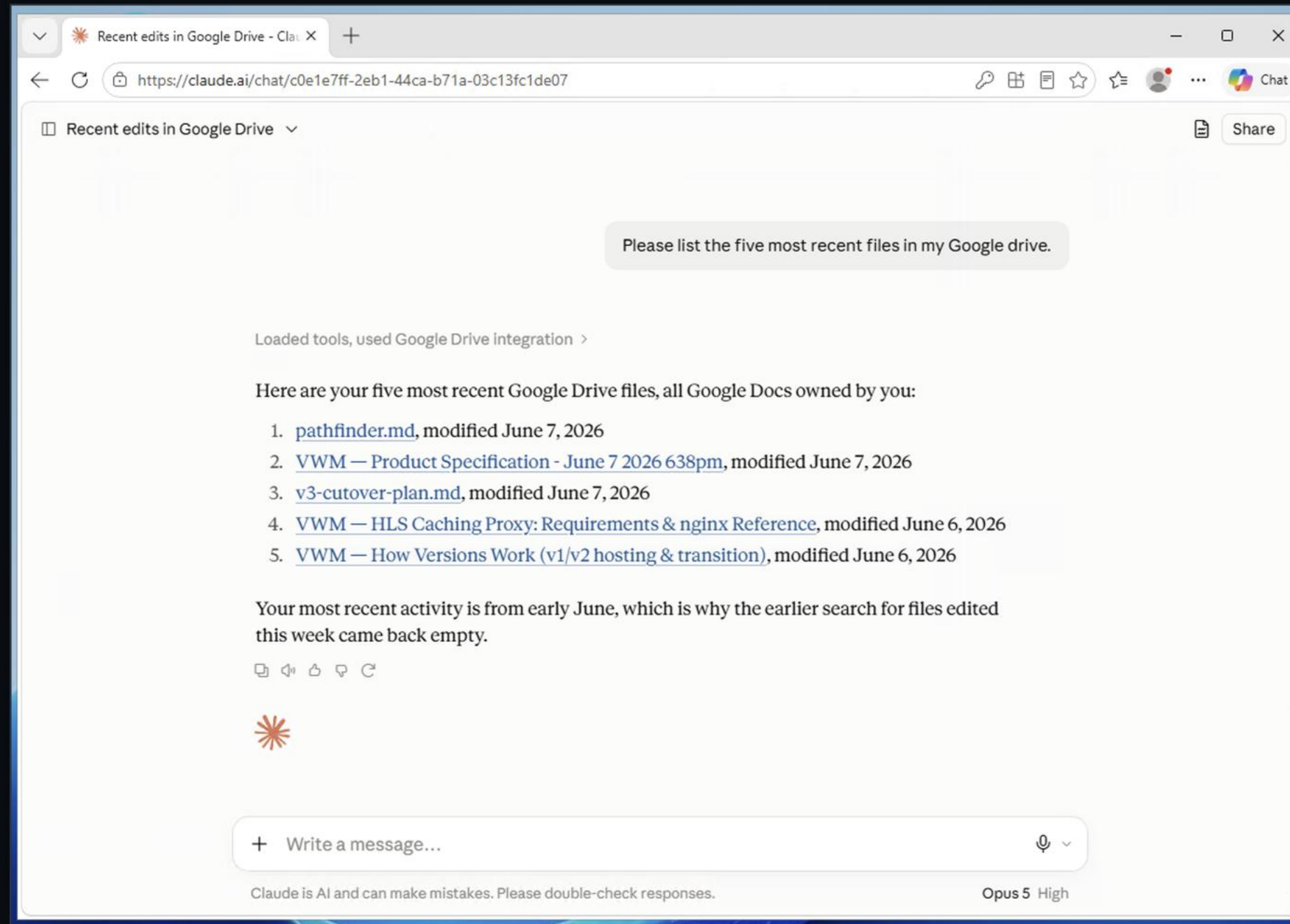
※ Baked for 18s · done 4:08 PM

Jump to bottom (ctrl+End) ↓

> |

▶▶ auto mode on (shift+tab to cycle) · ← for agents

One grant, and Claude Code runs SSH and reads Drive — the same commands, now allowed.



The same person's Claude.ai browser now reads Drive too. One grant, every surface.

EntPEP Enterprise Policy Enforcement Point

OverviewActivityAccessDesignAdmin

DarkDemo Coerik+admin@vivoh.comSign out

BehaviorSignalsSessions

Behavioral alerts

A behavior that appears for the first time within the last 24 hours. New behaviour is where risk hides — the first time an agent reaches for a tool, a command, or a model it has never used before.

⚠️

First use of tool `mcp__google_drive__list_files`

tool

2h ago

2 uses1 sessionby claude-codefirst seen Sep 22, 09:00 AM

⚠️

First use of tool `mcp__claude_ai_Google_Drive__search_files`

tool

3h ago

14 uses3 sessionsby claude-codefirst seen Sep 22, 08:48 AM

⚠️

First use of tool `mcp__claude_ai_Google_Drive__list_recent_files`

tool

13h ago

16 uses5 sessionsby claude-codefirst seen Sep 21, 09:54 PM

⚠️

First use of tool `ToolSearch`

tool

13h ago

18 uses5 sessionsby claude-codefirst seen Sep 21, 09:54 PM

⚠️

First use of `blocked-domain:google-drive`

command

14h ago

10 uses1 sessionby claude.aifirst seen Sep 21, 09:30 PM

⚠️

First use of `blocked-domain:brian.moqcdn.net`

command

19h ago

9 uses1 sessionby claude.aifirst seen Sep 21, 04:32 PM

⚠️

First use of `&`

command

23h ago

2 uses1 sessionby claude-codefirst seen Sep 21, 12:00 PM

Every first use of a tool or connector surfaces as behavior — across both surfaces.

 **EntPEP** Enterprise Policy Enforcement Point

Overview **Activity** Access Design Admin

 Dark Demo Co erik+admin@vivoh.com **Sign out**

Behavior **Signals** Sessions

Signals

Findings are recorded without the matched value — the secret itself is redacted before storage.

▲ high

Blocked: Google Drive reached with no active grant

 blocked before it ran

Sep 22, 11:49 AM

A tool call touched the gated resource "Google Drive", but no just-in-time access grant was in force, so it was denied before it ran. Open a time-boxed grant to allow it.

rule: ungranted_access field: command EC2AMAZ-IEU5RTA · Administrator [open session](#)

▲ high

Blocked: SSH access reached with no active grant

 blocked before it ran

Sep 22, 11:48 AM

A tool call touched the gated resource "SSH access", but no just-in-time access grant was in force, so it was denied before it ran. Open a time-boxed grant to allow it.

rule: ungranted_access field: command EC2AMAZ-IEU5RTA · Administrator [open session](#)

Every blocked attempt is logged per user, with the matched secret redacted.

One policy.

Every AI surface. Per user.

Block before a tool runs. Govern every surface the same way. Attribute to the person, not the app.