

AI Agent

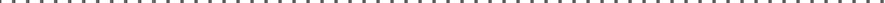
- [Claude-Skills-📄📄📄📄📄](#)
- [Claude Code Skills 📄📄](#)
- [Agent Skill 📄📄📄📄](#)
- [Claude Skill📄Skill Creator](#)

Claude-Skills-

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 



Skill []-[] Claude [] Skills [] Claude []

Skills  Claude 

Skills Skills Skill



- Skills 
-  Skill  MCP 
- 
-  Skills



- Claude [Progress bar]
- Claude [Progress bar]

Skills 1-2 MCP Skills + MCP 3

--	--	--	--	--	--	--	--

[illegible]

- | | | | | | |
|--|--|--|--|--|--|
| | | | | | |
|--|--|--|--|--|--|

Skills

--	--	--	--	--	--	--

- token

Claude Skills Skill Skills

Skills □ Claude.ai □ Claude Code □ API ██████████ ———— ███████ Skill ███████

🔗 MCP 🔗🔗Skills + 🔗🔗

“🔗 🔗 MCP 🔗🔗🔗 Skills🔗🔗🔗——🔗🔗🔗🔗🔗🔗

🔗🔗🔗🔗 MCP 🔗🔗🔗🔗🔗🔗Skills 🔗🔗🔗——🔗🔗🔗🔗🔗🔗 Claude 🔗🔗🔗🔗

🔗🔗🔗

MCP 🔗🔗🔗🔗🔗🔗🔗🔗

Skills 🔗🔗🔗🔗🔗🔗🔗🔗

🔗🔗🔗🔗🔗🔗🔗🔗🔗🔗🔗🔗

🔗🔗🔗🔗

MCP🔗🔗	Skills🔗🔗
🔗 Claude 🔗🔗🔗Notion🔗Asana🔗Linear 🔗	🔗 Claude 🔗🔗🔗🔗
🔗🔗🔗🔗🔗	🔗🔗🔗🔗
Claude 🔗	Claude 🔗🔗

🔗🔗 MCP 🔗🔗🔗

🔗 Skills🔗

- 🔗🔗 MCP🔗🔗🔗🔗
- 🔗🔗"🔗🔗🔗 X"
- 🔗🔗
- 🔗🔗🔗🔗🔗🔗
- 🔗🔗🔗🔗🔗🔗🔗🔗

🔗 Skills🔗

- 🔗🔗🔗🔗🔗🔗
- 🔗🔗🔗
- 🔗🔗🔗🔗🔗
- 🔗🔗🔗🔗

--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Skill ☐ ☐ ☐ 2-3 ☐ ☐ ☐ ☐ ☐ ☐

□□□□□□□□

□□□□□□"□□□□□□"□"□□□□□□"

□□

1. □ Linear□□ MCP□□□□□□□□
2. □□□□□□□□
3. □□□□□□□
4. □ Linear □□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□

--	--	--	--

- 
- 
-  MCP 
- 

☐ Skill ☐

☐ Anthropic

[illegible]

front-end-design skill docx pptx xlsx ppt Skills

“ [] Web [] artifact [] ”

--	--	--	--	--

- 2 □ □ □ □ □ □ □ □

skillcreator skill

--	--	--	--	--

- 3 □□MCP □□

sentry-code-review skill Sentry

--	--	--	--	--

-  MCP 
- 
- 
-  MCP 



目录

- Skill 90% 技能
 - 技能 10-20 技能 Skill 技能 vs. 技能
- X 技能
 - 技能 Skill 技能 token 技能
- 技能 0 API 技能
 - 技能 MCP 技能

目录

- 技能 Claude 技能
 - 技能
- 技能
 - 技能 3-5 技能
- 技能
 - 技能

目录

目录

```
your-skill-name/  
├─ SKILL.md          # 技能 Skill 技能  
├─ scripts/          # 技能技能  
|   └─ process_data.py # 技能  
|   └─ validate.sh    # 技能  
├─ references/        # 技能技能  
|   └─ api-guide.md   # 技能  
|   └─ examples/      # 技能  
└─ assets/            # 技能技能  
    └─ report-template.md # 技能
```

目录

SKILL.md 技能

- SKILL.md 技能
- 技能SKILL.MD技能skill.md 技能

Skill 技能

- `kebab-case: notion-project-setup`
- `Notion Project Setup`
- `notion_project_setup`
- `NotionProjectSetup`

README.md

- Skill README.md
- SKILL.md references/
- GitHub README——

YAML Frontmatter

YAML frontmatter Claude Skill

```
---
name: your-skill-name
description: What it does. Use when user asks to [specific phrases].
---
```

name

- kebab-case
-
-

description

- - Skill
 -
- 1024
- XML<>
-
-

license

- Skill ☐☐☐☐☐
- MIT ☐ Apache-2.0

compatibility ☐ ☐ ☐ ☐

- 1-500
-

metadata

metadata:

author: ProjectHub

version: 1.0.0 mcp-server: projecthub

--	--	--	--

Frontmatter 

- XML `<>` `[]`
- `[]` "claude" `[]` "anthropic" `[]` Skills `[]`

[illegible]

Skills

Description

Anthropic Claude Skill

--	--	--

$$[\begin{array}{|c|c|c|c|} \hline & & & \\ \hline \end{array}] + [\begin{array}{|c|c|c|c|} \hline & & & \\ \hline \end{array}] + [\begin{array}{|c|c|c|c|} \hline & & & \\ \hline \end{array}]$$

description

--

 —

--	--	--	--	--	--

description: Analyzes Figma design files and generates developer handoff documentation. Use when user uploads .fig

files, asks for "design specs", "component documentation", or "design-to-code handoff".

 —   

description: Manages Linear project workflows including sprint planning, task creation, and status tracking. Use when user mentions "sprint", "Linear tasks", "project planning", or asks to "create tickets".

 —   

description: End-to-end customer onboarding workflow for PayFlow. Handles account creation, payment setup, and subscription management. Use when user says "onboard new customer", "set up subscription", or "create PayFlow account".

 description

description: Helps with projects.

description: Creates sophisticated multi-page documentation systems.

description: Implements the Project entity model with hierarchical relationships.

 frontmatter  Markdown  

 Skill         

name: your-skill
description: [...]

Your Skill Name

Instructions

Step 1: [First Major Step]

Clear explanation of what happens.

```
```bash
```

```
python scripts/fetch_data.py --project-id PROJECT_ID
```

```
Expected output: [describe what success looks like]
```

```
```
```

(Add more steps as needed)

Examples

Example 1: [common scenario]

User says: "Set up a new marketing campaign"

Actions:

1. Fetch existing campaigns via MCP
2. Create new campaign with provided parameters

Result: Campaign created with confirmation link

(Add more examples as needed)

Troubleshooting

Error: [Common error message]

Cause: [Why it happens]

Solution: [How to fix]

(Add more error cases as needed)



Run ``python scripts/validate.py --input {filename}`` to check data format.

If validation fails, common issues include:

- Missing required fields (add them to the CSV)
- Invalid date formats (use YYYY-MM-DD)



Validate the data before proceeding.



Common Issues

MCP Connection Failed

If you see "Connection refused":

1. Verify MCP server is running: Check Settings > Extensions
2. Confirm API key is valid
3. Try reconnecting: Settings > Extensions > [Your Service] > Reconnect



Before writing queries, consult ``references/api-patterns.md`` for:

- Rate limiting guidance
- Pagination patterns
- Error codes and handling





Skills

- ☐ **Claude.ai**
- ☐ **Claude Code**
- ☐ **Skills API**

Skill Skill Skill

“

Skill Claude Skill Claude



Skills

1.

Skill

- ☐
- ☐
- ☐

- "Help me set up a new ProjectHub workspace"

- "I need to create a project in ProjectHub"

- "Initialize a ProjectHub project for Q4 planning"

- "What's the weather in San Francisco?"

- "Help me write Python code"

- "Create a spreadsheet" (unless ProjectHub skill handles sheets)

2. □□□□

□□□\$skill □□□□□□□□

□□□□

- □□□□□□
- API □□□□
- □□□□□□□□
- □□□□□□□□

□□□

Test: Create project with 5 tasks

Given: Project name "Q4 Planning", 5 task descriptions

When: Skill executes workflow

Then:

- Project created in ProjectHub
- 5 tasks created with correct properties
- All tasks linked to project
- No API errors

3. □□□□

□□□\$skill □□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□

□□□□

Without skill:

- User provides instructions each time
- 15 back-and-forth messages
- 3 failed API calls requiring retry
- 12,000 tokens consumed

With skill:

- Automatic workflow execution
- 2 clarifying questions only
- 0 failed API calls
- 6,000 tokens consumed

skill-creator Skill

Anthropic `skill-creator` Skill Skills MCP 2-3 Skill-

Skills

- Skills
- frontmatter SKILL.md
-

Skills

-
- /
- Skill

- Skill skill-creator
- "Use the issues & solution identified in this chat to improve how the skill handles [specific edge case]"

"Use the skill-creator skill to help me build a skill for [your use case]"

skill-creator Skills

Skills

- Skill
-
-

“ description —

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

- Skill

| | | | | | | |
|--|--|--|--|--|--|--|
| | | | | | | |
|--|--|--|--|--|--|--|
- | | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|
- | | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

“ ”

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

- 
- API 
- 

“ ”

| | | | | | | | | |
|--|--|--|--|--|--|--|--|--|
| | | | | | | | | |
|--|--|--|--|--|--|--|--|--|

[illegible]

□□□□□□2026 □ 1 □□

Skills

1.  Skill 
2.        
3.  Claude.ai  Settings > Capabilities > Skills 
4.    Claude Code skills 

Skills

- Skills 2025 12 18
-
-

| | | | |
|--|--|--|--|
| | | | |
|--|--|--|--|

API Skills

Skills Skills API Skill

- /v1/skills Skills
- container.skills Skills Messages API
- Claude Console
- Claude Agent SDK

API vs. Claude.ai

| Skills | Claude.ai / Claude Code |
|--------|-------------------------|
| | Claude.ai / Claude Code |
| | Claude.ai / Claude Code |
| Skills | API |
| | API |
| | API |

API Skills Code Execution Toolbeta Skills

- Skills API
- Skills
- Agent SDK Skills

GitHub Skill READMESkill Skill README.md

1. GitHub

- Skills
- README
-

2. MCP Skills

- MCP Skills
- Skills
- Skills

3. Skills

Installing the [Your Service] skill

1. Download the skill:

- Clone repo: `git clone https://github.com/yourcompany/skills`
- Or download ZIP from Releases

2. Install in Claude:

- Open Claude.ai > Settings > skills
- Click "Upload skill"
- Select the skill folder (zipped)

3. Enable the skill:

- Toggle on the [Your Service] skill
- Ensure your MCP server is connected

4. Test:

- Ask Claude: "Set up a new project in [Your Service]"

Skills

Skills README Skill

"The ProjectHub skill enables teams to set up complete project workspaces in seconds — including pages, databases, and templates — instead of spending 30 minutes on manual setup."

"The ProjectHub skill is a folder containing YAML frontmatter and Markdown instructions that calls our MCP server tools."

MCP + Skills

"Our MCP server gives Claude access to your Linear projects. Our skills teach Claude your team's sprint planning workflow. Together, they enable AI-powered project management."



Skills

vs.

Home Depot

Skills

- "Skill MCP Skill
- "Notion MCP" → Skill Claude Skill

Skills

1

Workflow: Onboard New Customer

Step 1: Create Account

Call MCP tool: `create\_customer`

Parameters: name, email, company

Step 2: Setup Payment

Call MCP tool: `setup\_payment\_method`

Wait for: payment method verification

Step 3: Create Subscription

Call MCP tool: `create\_subscription`

Parameters: plan_id, customer_id (from Step 1)

Step 4: Send Welcome Email

Call MCP tool: `send\_email`

Template: welcome_email_template

□□□□

- □□□□□
- □□□□□□
- □□□□□
- □□□□□□

□□ 2□□ MCP □□

□□□□□□□□

□□□□□□

Phase 1: Design Export (Figma MCP)

1. Export design assets from Figma
2. Generate design specifications
3. Create asset manifest

Phase 2: Asset Storage (Drive MCP)

1. Create project folder in Drive
2. Upload all assets
3. Generate shareable links

Phase 3: Task Creation (Linear MCP)

1. Create development tasks
2. Attach asset links to tasks
3. Assign to engineering team

Phase 4: Notification (Slack MCP)

1. Post handoff summary to #engineering

2. Include asset links and task references

□□□□

- □□□□□
- MCP □□□□□
- □□□□□□□
- □□□□□

□□ 3□□□□□

□□□□□□□□

□□□

Iterative Report Creation

Initial Draft

1. Fetch data via MCP
2. Generate first draft report
3. Save to temporary file

Quality Check

1. Run validation script: `scripts/check\_report.py`
2. Identify issues:
 - Missing sections
 - Inconsistent formatting
 - Data validation errors

Refinement Loop

1. Address each identified issue
2. Regenerate affected sections
3. Re-validate
4. Repeat until quality threshold met

Finalization

1. Apply final formatting
2. Generate summary
3. Save final version

□□□□

- □□□□□□
- □□□□
- □□□□
- □□□□□□□□

□□ 4 □□□□□□□□□□

□□□□□□□□□□□□□□

□□□□

```
## Smart File Storage

### Decision Tree
1. Check file type and size
2. Determine best storage location:
  - Large files (>10MB): Use cloud storage MCP
  - Collaborative docs: Use Notion/Docs MCP
  - Code files: Use GitHub MCP
  - Temporary files: Use local storage

### Execute Storage
Based on decision:
- Call appropriate MCP tool
- Apply service-specific metadata
- Generate access link

### Provide Context to User
Explain why that storage was chosen
```

□□□□

- □□□□□□
- □□□□
- □□□□□□□□

□□ 5 □□□□□□□□

```
## Payment Processing with Compliance

### Before Processing (Compliance Check)
1. Fetch transaction details via MCP
2. Apply compliance rules:
  - Check sanctions lists
  - Verify jurisdiction allowances
  - Assess risk level
3. Document compliance decision

### Processing
IF compliance passed:
  - Call payment processing MCP tool
  - Apply appropriate fraud checks
  - Process transaction
ELSE:
  - Flag for review
  - Create compliance case

### Audit Trail
- Log all compliance checks
- Record processing decisions
- Generate audit report
```

- ██████████
- █████
- ██████
- █████

SKILL.md

####

- #### SKILL.md#####
- `ls -la` ##### SKILL.md

##"Invalid frontmatter"

###YAML ###

####

```
# ---#####
name: my-skill
description: Does things

# ---#####
name: my-skill
description: "Does things

# 
---
name: my-skill
description: Does things
---
```

##"Invalid skill name"

#####

```
# 
name: My Cool Skill

# 
name: my-cool-skill
```

Skill ###

Skill #####

description Description /

| | | | | | | |
|--|--|--|--|--|--|--|
| | | | | | | |
|--|--|--|--|--|--|--|

- "Helps with projects"
-
-

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

□ Claude □ "When would you use the [skill name] skill?" Claude □□ description □□□□□□□□□□

Skill

| | | | | | |
|--|--|--|--|--|--|
| | | | | | |
|--|--|--|--|--|--|

Skill

| | | | | | | | |
|--|--|--|--|--|--|--|--|
| | | | | | | | |
|--|--|--|--|--|--|--|--|

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

1.

description: Advanced data analysis for CSV files. Use for statistical modeling, regression, clustering. Do NOT use for simple data exploration (use data-viz skill instead).

2. ☐ ☐ ☐ ☐

| | | |
|--|--|--|
| | | |
|--|--|--|

description: Processes documents

| | | |
|--|--|--|
| | | |
|--|--|--|

description: Processes PDF legal documents for contract review

3. ☐ ☐ ☐ ☐

description: PayFlow payment processing for e-commerce. Use specifically for online payment workflows, not for general financial queries.

MCP

| | | | |
|--|--|--|--|
| | | | |
|--|--|--|--|

Skill ☐☐ MCP ☐☐

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

1. `!mcp`
 - Claude.ai Settings > Extensions > []
 - [] "Connected" []
2. []
 - API []
 - []/[]
 - OAuth token []
3. [] MCP
 - [] Claude [] MCP [] Skill []
 - "Use [Service] MCP to fetch my projects"
 - [] MCP [] Skill
4. []
 - Skill [] MCP []
 - [] MCP []
 - []

| | | | | | |
|--|--|--|--|--|--|
| | | | | | |
|--|--|--|--|--|--|

Skill ☐☐ Claude ☐☐☐☐

| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|

1. 
- 
 - 
 - 
2. 
- 
 - 
 - 
3. 

Make sure to validate things properly

☐

CRITICAL: Before calling `create_project`, verify:

- Project name is non-empty
- At least one team member assigned
- Start date is not in the past

Office skills

4. " " 10

Performance Notes

- Take your time to do this thoroughly
- Quality is more important than speed
- Do not skip validation steps

SKILL.md

Skill

- Skill
- Skills
-

1. SKILL.md
 - references/
 -
 - SKILL.md 5,000
2. Skills
 - 20-50 Skills
 -
 - Skill "

Skill API

Anthropic

-
- Skills

- [API](#)
- [MCP](#)

[Links](#)

- [Introducing Agent Skills](#)
- [Engineering Blog: Equipping Agents for the Real World](#)
- [Skills Explained](#)
- [How to Create Skills for Claude](#)
- [Building Skills for Claude Code](#)
- [Improving Frontend Design through Skills](#)

[Skills](#)

[Skills](#)

- [GitHubanthropics/skills](#)
- [Anthropic Skills](#)

[skill-creator](#)

[skill-creator skill](#)

- [Claude.ai](#) [Claude Code](#)
- [Skills](#)
- [Help me build a skill using skill-creator"](#)

[skill-creator](#)

- [skill-creator Skills](#)
- [Review this skill and suggest improvements"](#)

[skill-creator](#)

[skill-creator](#)

- [Claude Developers Discord](#)

[Bug](#)

- [GitHub Issuesanthropics/skills/issues](#)
- [Skill](#)

00 A0000000

0000000000 Skill0000000000 skill-creator skill 0000000000000000

0000

- ☐ 00 2-3 000000
- ☐ 00000000 MCP
- ☐ 000000 Skills
- ☐ 000000

000000

- ☐ 0000 kebab-case 00
- ☐ SKILL.md 00000000
- ☐ YAML frontmatter [--- 00
- ☐ name 000kebab-case00000000
- ☐ description 00000WHAT00000WHEN
- ☐ XML < >
- ☐ 0000000
- ☐ 00000
- ☐ 0000
- ☐ 000000

0000

- ☐ 0000000000
- ☐ 000000000000
- ☐ 000000000000
- ☐ 00000
- ☐ 000000000000
- ☐ 0000 .zip 00



- ☐ [] [] [] [] [] [] [] []
- ☐ [] [] [] [] [] [] / [] [] [] [] [] []
- ☐ [] [] [] [] [] []
- ☐ [] [] description [] [] [] []
- ☐ [] metadata [] [] [] [] [] []

[] B[YAML Frontmatter



```
---
name: skill-name-in-kebab-case
description: What it does and when to use it. Include specific
trigger phrases.
---
```



```
name: skill-name
description: [required description]
license: MIT # [ ] [ ] [ ] [ ] [ ] [ ]
allowed-tools: "Bash(python:*) Bash(npm:*) WebFetch" # [ ] [ ] [ ] [ ] [ ] [ ]
metadata: # [ ] [ ] [ ] [ ] [ ] [ ]
  author: Company Name
  version: 1.0.0
  mcp-server: server-name
  category: productivity
  tags: [project-management, automation]
documentation: https://example.com/docs
support: support@example.com
```



- `name` YAML `name: my-project`
- `description` metadata `description: A sample project`
- `description` `description: 1024 characters`



- XML `<?xml version="1.0" encoding="UTF-8" ?>`
- YAML `name: my-project` YAML `name: my-project`
- `"claude"` `"anthropic"` `skills: [ ]`

My Career Skill Set

My Skills

- **Document Skills** - PDF, DOCX, PPTX, XLSX
- **Example Skills** - `skills: [ ]`
- **Partner Skills Directory** - `skills: [ ]` Asana, Atlassian, Canva, Figma, Sentry, Zapier

Claude Code Skills

Skills Claude Code extension points

Skills Skill

Anthropic Claude Code Skills Skills

Skills

Skills Agent Skills Skills

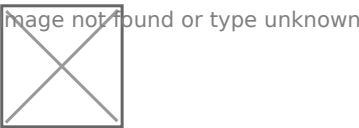
Skills" markdown Skills

Claude Code Skills hooks

Claude Code Skills

Skills Skills Skills Skills

Skill



1. API

SDK Skills Claude Code Skills

- billing-lib — footguns
- internal-platform-cli — CLI
- frontend-design — Claude

2. 技能

技能は Skills、Playwright、tmux

Skills Claude Skills

Claude Skill

- signup-flow-driver — →
- checkout-verifier — Stripe UI
- tmux-cli-driver — TTY

3. 技能

Skills Skills ID

- funnel-query — "→" user_id
- cohort-compare —
- grafana — UID→

4. 技能

Skills Skills Skills MCP Model Context Protocol S

- standup-post — GitHub Slack → delta-only
- create-<ticket-system>-ticket — schema Slack
- weekly-recap — PR + + →

5. 技能

boilerplate Skills Skills scaffolding Sk

- new-<framework>-workflow — / /
- new-migration —

- `create-app` — `XXXXXXXXXXXXXXXXXXXX`

6. `XXXXXXXX`

`XXXXXXXXXXXXXXXXXXXX` Skills `XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX` Skills `XXXXXXXXXXXXXXXXXXXX` GitHub Action `XXXX`

`XXXX`

- `adversarial-review` — `XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX` subagent `XXXX` Claude Code `XXXX`
- `code-style` — `XXXXXXXXXXXX` Claude `XXXXXXXX`
- `testing-practices` — `XXXXXXXXXXXXXXXX`

7. CI/CD `XXXX`

`XXXXXXXXXXXX` Skills `XXXX` Skills `XXXXXX` Skills `XXXXXX`

`XXXX`

- `babysit-pr` — `XXXX` PR → `XXXXXX` CI → `XXXXXX` → `XXXXXX`
- `deploy-<service>` — `XX` → `XXXX` → `XXXXXXXXXXXXXXXX` → `XXXXXXXXXX`
- `cherry-pick-prod` — `XXXXXXXX` `worktree` → `cherry-pick` → `XXXX` → `XXXX` PR

8. `XXXX`

`XXXXXXXXXXXX` Slack `XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX` Skills `XX`

`XXXX`

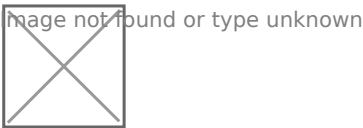
- `<service>-debugging` — `XXXXXXXXXX` → `XXXXXXXXXXXXXXXXXXXX`
- `oncall-runner` — `XXXX` → `XXXXXX` → `XXXXXXXXXX`
- `log-correlator` — `XXXXXX` ID `XXXXXXXXXXXXXXXXXXXX`

9. `XXXXXX`

`XXXXXXXXXXXX` Skills — `XXXXXXXXXXXXXXXXXXXXXXXXXXXX` Skills `XXXXXXXXXXXXXXXXXXXX`

`XXXX`

- `<resource>-orphans` — `XXXXXX` Pod/Volume → `XX` Slack → `XXXX` → `XXXX` → `XXXX`
- `dependency-management` — `XXXXXXXXXXXX`
- `cost-investigation` — `"XXXX/XXXXXXXXXXXX"` `XXXXXXXXXXXXXXXX`



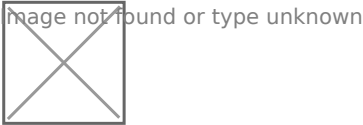
☐ Skill ☐

[Skill Creator](#) ☐ Claude Code ☐ Skills ☐

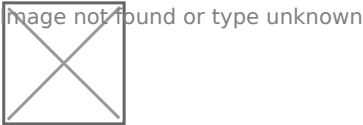


Claude Code ☐ Claude ☐ Skill ☐ Claude ☐

[frontend design](#) ☐ Skill ☐ — ☐ Anthropic ☐ Claude ☐ Inte



☐ Skill ☐ Claude ☐ Skill ☐ Skill ☐



☐ Skill ☐ markdown ☐ Context Engineering ☐ progressive dis

☐ Context Engineering ☐ 2025 ☐ Andrej Karpathy ☐

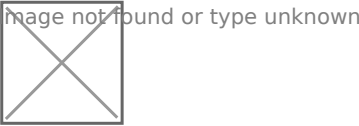
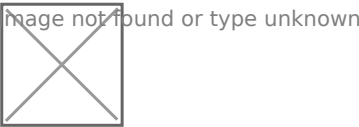
☐ mar [references/api.md](#) ☐

☐ [assets/arkdown](#) ☐

☐ Claude ☐

Claude

Claude Skills Claude



Skills Slack Skill Claude Slack

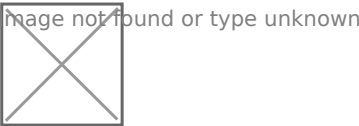
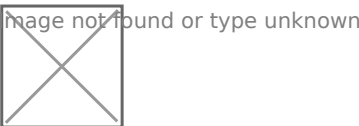
config.json Skill

AskUserQuestion Claude

description

Claude Code Skill "Claude Skill" Skill

description "Skill" Claude "Skill" description if-then



Skills JSON SQLite

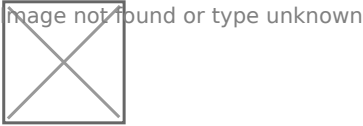
standup-post Skill standups.log Claude

Skill Skill Skill

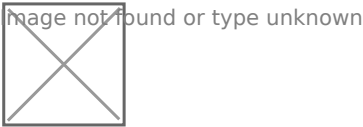


[[Claude [Claude []]

[Skill [Claude []]



Claude []]



Skills [Skill [On Demand Hooks []]



- /careful — [PreToolUse [B rm -rf DROP TABLE [force-pus kubectl delete []]
- /freeze — [Edit/Write []]



Skills []]

[.agents/skills/ [Git [Skills []]

Skills

[Skills [Skill [CSV [Skill [CSV [Agent Skills [Skill []]

Skills []]

A horizontal array of 20 slots. The first 5 slots are grouped under the label 'PreToolUse'. The next 5 slots are grouped under the label 'Skill'. The next 5 slots are grouped under the label 'Skills'. The remaining 5 slots are empty.



Skills □ AI ▢▢▢AI Agent□□□□□□□□□□□□□□□□□□□□

Skills Skills Skills

Agent Skill

SKILL.md — YAML 30 Agent Claude Code Gemini CLI Cui
Skill SKILL.md FastAPI Skill
Skill Anthropic Vercel Google — Ag
ADK

- Tool Wrapper Agent
- Generator
- Reviewer
- Inversion Agent
- Pipeline

alt text not found or type unknown

Tool Wrapper

Agent API Skill Agent

alt text not found or type unknown

SKILL.md references/

Agent conventions.md Agent

```
# skills/api-expert/SKILL.md
---
name: api-expert
description: FastAPI FastAPI REST API Pydantic
metadata:
  pattern: tool-wrapper
  domain: fastapi
---

FastAPI
```

##

'references/conventions.md' FastAPI

##

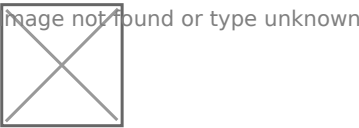
- 1.
- 2.
- 3.

##

- 1.
- 2.
- 3.
- 4. Annotated

Generator

Agent " " "



assets/ references/ Agent API

Skill Agent

```
# skills/report-generator/SKILL.md
---
name: report-generator
description: Markdown
metadata:
  pattern: generator
  output-format: markdown
---


```


references/style-guide.md

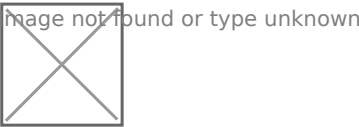
assets/report-template.md

-
-
-

Markdown

Reviewer

references/review-checklist.md



Agent Python OWASP Skill

Skill Agent

```
# skills/code-reviewer/SKILL.md
---
name: code-reviewer
description: Python Bug
metadata:
  pattern: reviewer
  severity-levels: error,warning,info
---

Python

references/review-checklist.md

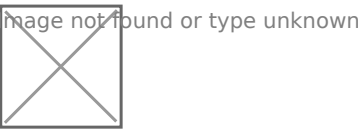

```

```
#####  
- #####  
- #####error#####warning#####info#####  
- #####  
- #####
```

```
#####  
- **##*#####  
- **##*##### error## warning### info#  
- **##*##1-10 #####  
- **###*#####
```

#####Inversion#

Agent #####Agent ##### Agent #####



#####"#####"#### Agent #####A

Skill##### Agent

```
# skills/project-planner/SKILL.md  
  
---  
  
name: project-planner  
  
description: #####"#####"#####"  
metadata:  
  pattern: inversion  
  interaction: multi-turn  
  
---  
  
#####  
  
## # ---#####  
  
#####
```

- Q1" " "
- Q2" " "
- Q3" " "

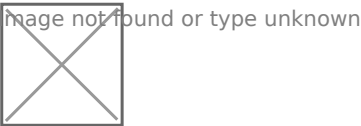
—

- Q4" " "
- Q5" " "
- Q6" " "

—

- 1. 'assets/plan-template.md'
- 2.
- 3.
- 4. " "
- 5.

Pipeline



Agent

—Agent

```
# skills/doc-pipeline/SKILL.md
---
name: doc-pipeline
description: Python API  API 
metadata:
  pattern: pipeline
```

— — —

[illegible]

Python "API"

- `'references/docstring-style.md'` `██████`[illegible][illegible][illegible]

☐ 'assets/api-doc-template.md' ☐ API ☐

☐ 'references/quality-checklist.md' ☐ ☐ ☐ ☐[illegible][illegible]

—



image not found or type unknown

| 項目 | 内容 |
|---------|----|
| Agent 名 | 太郎 |
| 性別 | 男 |
| 年齢 | 25 |

| Agent | Skills |
|-------|--------|
| Agent | |
| | |



Skill SkillToolset Agent ADK

Agent



Agent Skills [Go to ADK Agent Development Kit](#) Agent

Claude Skill Skill Creator

```
---
name: skill-creator
description: Create new skills, modify and improve existing skills, and measure skill performance. Use when
users want to create a skill from scratch, edit, or optimize an existing skill, run evals to test a skill, benchmark
skill performance with variance analysis, or optimize a skill's description for better triggering accuracy.
---
```

Skill Creator

A skill for creating new skills and iteratively improving them.

At a high level, the process of creating a skill goes like this:

- Decide what you want the skill to do and roughly how it should do it
- Write a draft of the skill
- Create a few test prompts and run `claude-with-access-to-the-skill` on them
- Help the user evaluate the results both qualitatively and quantitatively
 - While the runs happen in the background, draft some quantitative evals if there aren't any (if there are some, you can either use as is or modify if you feel something needs to change about them). Then explain them to the user (or if they already existed, explain the ones that already exist)
 - Use the `eval-viewer/generate_review.py` script to show the user the results for them to look at, and also let them look at the quantitative metrics
- Rewrite the skill based on feedback from the user's evaluation of the results (and also if there are any glaring flaws that become apparent from the quantitative benchmarks)
- Repeat until you're satisfied
- Expand the test set and try again at larger scale

Your job when using this skill is to figure out where the user is in this process and then jump in and help them progress through these stages. So for instance, maybe they're like "I want to make a skill for X". You can help narrow down what they mean, write a draft, write the test cases, figure out how they want to evaluate, run all the prompts, and repeat.

On the other hand, maybe they already have a draft of the skill. In this case you can go straight to the eval/iterate part of the loop.

Of course, you should always be flexible and if the user is like "I don't need to run a bunch of evaluations, just vibe with me", you can do that instead.

Then after the skill is done (but again, the order is flexible), you can also run the skill description improver, which we have a whole separate script for, to optimize the triggering of the skill.

Cool? Cool.

Communicating with the user

The skill creator is liable to be used by people across a wide range of familiarity with coding jargon. If you haven't heard (and how could you, it's only very recently that it started), there's a trend now where the power of Claude is inspiring plumbers to open up their terminals, parents and grandparents to google "how to install npm". On the other hand, the bulk of users are probably fairly computer-literate.

So please pay attention to context cues to understand how to phrase your communication! In the default case, just to give you some idea:

- "evaluation" and "benchmark" are borderline, but OK
- for "JSON" and "assertion" you want to see serious cues from the user that they know what those things are before using them without explaining them

It's OK to briefly explain terms if you're in doubt, and feel free to clarify terms with a short definition if you're unsure if the user will get it.

Creating a skill

Capture Intent

Start by understanding the user's intent. The current conversation might already contain a workflow the user wants to capture (e.g., they say "turn this into a skill"). If so, extract answers from the conversation history first — the tools used, the sequence of steps, corrections the user made, input/output formats observed. The user may need to fill the gaps, and should confirm before proceeding to the next step.

1. What should this skill enable Claude to do?
2. When should this skill trigger? (what user phrases/contexts)
3. What's the expected output format?

4. Should we set up test cases to verify the skill works? Skills with objectively verifiable outputs (file transforms, data extraction, code generation, fixed workflow steps) benefit from test cases. Skills with subjective outputs (writing style, art) often don't need them. Suggest the appropriate default based on the skill type, but let the user decide.

Interview and Research

Proactively ask questions about edge cases, input/output formats, example files, success criteria, and dependencies. Wait to write test prompts until you've got this part ironed out.

Check available MCPs - if useful for research (searching docs, finding similar skills, looking up best practices), research in parallel via subagents if available, otherwise inline. Come prepared with context to reduce burden on the user.

Write the SKILL.md

Based on the user interview, fill in these components:

- **name:** Skill identifier
- **description:** When to trigger, what it does. This is the primary triggering mechanism - include both what the skill does AND specific contexts for when to use it. All "when to use" info goes here, not in the body. Note: currently Claude has a tendency to "undertrigger" skills -- to not use them when they'd be useful. To combat this, please make the skill descriptions a little bit "pushy". So for instance, instead of "How to build a simple fast dashboard to display internal Anthropic data.", you might write "How to build a simple fast dashboard to display internal Anthropic data. Make sure to use this skill whenever the user mentions dashboards, data visualization, internal metrics, or wants to display any kind of company data, even if they don't explicitly ask for a 'dashboard.'"
- **compatibility:** Required tools, dependencies (optional, rarely needed)
- **the rest of the skill :)**

Skill Writing Guide

Anatomy of a Skill

```
skill-name/  
├─ SKILL.md (required)  
│   └─ YAML frontmatter (name, description required)  
│       └─ Markdown instructions  
└─ Bundled Resources (optional)  
    └─ scripts/ - Executable code for deterministic/repetitive tasks
```


- └─ references/ - Docs loaded into context as needed
- └─ assets/ - Files used in output (templates, icons, fonts)

Progressive Disclosure

Skills use a three-level loading system:

1. **Metadata** (name + description) - Always in context (~100 words)
2. **SKILL.md body** - In context whenever skill triggers (<500 lines ideal)
3. **Bundled resources** - As needed (unlimited, scripts can execute without loading)

These word counts are approximate and you can feel free to go longer if needed.

Key patterns:

- Keep SKILL.md under 500 lines; if you're approaching this limit, add an additional layer of hierarchy along with clear pointers about where the model using the skill should go next to follow up.
- Reference files clearly from SKILL.md with guidance on when to read them
- For large reference files (>300 lines), include a table of contents

Domain organization: When a skill supports multiple domains/frameworks, organize by variant:

```
cloud-deploy/  
└─ SKILL.md (workflow + selection)  
└─ references/  
    └─ aws.md  
    └─ gcp.md  
    └─ azure.md
```

Claude reads only the relevant reference file.

Principle of Lack of Surprise

This goes without saying, but skills must not contain malware, exploit code, or any content that could compromise system security. A skill's contents should not surprise the user in their intent if described. Don't go along with requests to create misleading skills or skills designed to facilitate unauthorized access, data exfiltration, or other malicious activities. Things like "roleplay as an XYZ" are OK though.

Writing Patterns

Prefer using the imperative form in instructions.

Defining output formats - You can do it like this:

```
## Report structure
```

ALWAYS use this exact template:

```
# [Title]
```

```
## Executive summary
```

```
## Key findings
```

```
## Recommendations
```

Examples pattern - It's useful to include examples. You can format them like this (but if "Input" and "Output" are in the examples you might want to deviate a little):

```
## Commit message format
```

```
**Example 1:**
```

Input: Added user authentication with JWT tokens

Output: feat(auth): implement JWT-based authentication

Writing Style

Try to explain to the model why things are important in lieu of heavy-handed musty MUSTs. Use theory of mind and try to make the skill general and not super-narrow to specific examples. Start by writing a draft and then look at it with fresh eyes and improve it.

Test Cases

After writing the skill draft, come up with 2-3 realistic test prompts — the kind of thing a real user would actually say. Share them with the user: [you don't have to use this exact language] "Here are a few test cases I'd like to try. Do these look right, or do you want to add more?" Then run them.

Save test cases to `evals/evals.json`. Don't write assertions yet — just the prompts. You'll draft assertions in the next step while the runs are in progress.

```
{
  "skill_name": "example-skill",
  "evals": [
    {
      "id": 1,
      "prompt": "User's task prompt",
      "expected_output": "Description of expected result",
      "files": []
    }
  ]
}
```

```
]
}
```

See `references/schemas.md` for the full schema (including the `assertions` field, which you'll add later).

Running and evaluating test cases

This section is one continuous sequence — don't stop partway through. Do NOT use `/skill-test` or any other testing skill.

Put results in `<skill-name>-workspace/` as a sibling to the skill directory. Within the workspace, organize results by iteration (`iteration-1/`, `iteration-2/`, etc.) and within that, each test case gets a directory (`eval-0/`, `eval-1/`, etc.). Don't create all of this upfront — just create directories as you go.

Step 1: Spawn all runs (with-skill AND baseline) in the same turn

For each test case, spawn two subagents in the same turn — one with the skill, one without. This is important: don't spawn the with-skill runs first and then come back for baselines later. Launch everything at once so it all finishes around the same time.

With-skill run:

Execute this task:

- Skill path: `<path-to-skill>`
- Task: `<eval prompt>`
- Input files: `<eval files if any, or "none">`
- Save outputs to: `<workspace>/iteration-<N>/eval-<ID>/with_skill/outputs/`
- Outputs to save: `<what the user cares about — e.g., "the .docx file", "the final CSV">`

Baseline run (same prompt, but the baseline depends on context):

- **Creating a new skill:** no skill at all. Same prompt, no skill path, save to `without_skill/outputs/`.
- **Improving an existing skill:** the old version. Before editing, snapshot the skill (`cp -r <skill-path> <workspace>/skill-snapshot/`), then point the baseline subagent at the snapshot. Save to `old_skill/outputs/`.

Write an `eval_metadata.json` for each test case (assertions can be empty for now). Give each eval a descriptive name based on what it's testing — not just "eval-0". Use this name for the directory too.

If this iteration uses new or modified eval prompts, create these files for each new eval directory — don't assume they carry over from previous iterations.

```
{
  "eval_id": 0,
  "eval_name": "descriptive-name-here",
  "prompt": "The user's task prompt",
  "assertions": []
}
```

Step 2: While runs are in progress, draft assertions

Don't just wait for the runs to finish — you can use this time productively. Draft quantitative assertions for each test case and explain them to the user. If assertions already exist in `evals/evals.json`, review them and explain what they check.

Good assertions are objectively verifiable and have descriptive names — they should read clearly in the benchmark viewer so someone glancing at the results immediately understands what each one checks. Subjective skills (writing style, design quality) are better evaluated qualitatively — don't force assertions onto things that need human judgment.

Update the `eval_metadata.json` files and `evals/evals.json` with the assertions once drafted. Also explain to the user what they'll see in the viewer — both the qualitative outputs and the quantitative benchmark.

Step 3: As runs complete, capture timing data

When each subagent task completes, you receive a notification containing `total_tokens` and `duration_ms`. Save this data immediately to `timing.json` in the run directory:

```
{
  "total_tokens": 84852,
  "duration_ms": 23332,
  "total_duration_seconds": 23.3
}
```

This is the only opportunity to capture this data — it comes through the task notification and isn't persisted elsewhere. Process each notification as it arrives rather than trying to batch them.

Step 4: Grade, aggregate, and launch the viewer

Once all runs are done:

1. **Grade each run** — spawn a grader subagent (or grade inline) that reads `agents/grader.md` and evaluates each assertion against the outputs. Save results to `grading.json` in each run directory. The `grading.json` expectations array must use the fields `text`, `passed`, and `evidence` (not `name`/`met`/`details` or other variants) — the viewer depends on these exact field names. For assertions that can be checked programmatically, write and run a script rather than eyeballing it — scripts are faster, more reliable, and can be reused across iterations.
2. **Aggregate into benchmark** — run the aggregation script from the skill-creator directory:

```
python -m scripts.aggregate_benchmark <workspace>/iteration-N --skill-name <name>
```

This produces `benchmark.json` and `benchmark.md` with `pass_rate`, time, and tokens for each configuration, with mean $\pm$ stddev and the delta. If generating `benchmark.json` manually, see `references/schemas.md` for the exact schema the viewer expects. Put each with `_skill` version before its baseline counterpart.

3. **Do an analyst pass** — read the benchmark data and surface patterns the aggregate stats might hide. See `agents/analyzer.md` (the "Analyzing Benchmark Results" section) for what to look for — things like assertions that always pass regardless of skill (non-discriminating), high-variance evals (possibly flaky), and time/token tradeoffs.
4. **Launch the viewer** with both qualitative outputs and quantitative data:

```
nohup python <skill-creator-path>/eval-viewer/generate_review.py \  
  <workspace>/iteration-N \  
  --skill-name "my-skill" \  
  --benchmark <workspace>/iteration-N/benchmark.json \  
  > /dev/null 2>&1 &  
VIEWER_PID=$!
```

For iteration 2+, also pass `--previous-workspace <workspace>/iteration-<N-1>`.

Cowork / headless environments: If `webbrowser.open()` is not available or the environment has no display, use `--static <output_path>` to write a standalone HTML file instead of starting a server. Feedback will be downloaded as a `feedback.json` file when the user clicks "Submit All Reviews". After download, copy `feedback.json` into the workspace directory for the next iteration to pick up.

Note: please use `generate_review.py` to create the viewer; there's no need to write custom HTML.

5. **Tell the user** something like: "I've opened the results in your browser. There are two tabs — 'Outputs' lets you click through each test case and leave feedback, 'Benchmark' shows the quantitative comparison. When you're done, come back here and let me know."

What the user sees in the viewer

The "Outputs" tab shows one test case at a time:

- **Prompt:** the task that was given
- **Output:** the files the skill produced, rendered inline where possible
- **Previous Output** (iteration 2+): collapsed section showing last iteration's output
- **Formal Grades** (if grading was run): collapsed section showing assertion pass/fail
- **Feedback:** a textbox that auto-saves as they type
- **Previous Feedback** (iteration 2+): their comments from last time, shown below the textbox

The "Benchmark" tab shows the stats summary: pass rates, timing, and token usage for each configuration, with per-eval breakdowns and analyst observations.

Navigation is via prev/next buttons or arrow keys. When done, they click "Submit All Reviews" which saves all feedback to `feedback.json`.

Step 5: Read the feedback

When the user tells you they're done, read `feedback.json`:

```
{
  "reviews": [
    {"run_id": "eval-0-with_skill", "feedback": "the chart is missing axis labels", "timestamp": "..."},
    {"run_id": "eval-1-with_skill", "feedback": "", "timestamp": "..."},
    {"run_id": "eval-2-with_skill", "feedback": "perfect, love this", "timestamp": "..."}
  ],
  "status": "complete"
}
```

Empty feedback means the user thought it was fine. Focus your improvements on the test cases where the user had specific complaints.

Kill the viewer server when you're done with it:

Improving the skill

This is the heart of the loop. You've run the test cases, the user has reviewed the results, and now you need to make the skill better based on their feedback.

How to think about improvements

1. **Generalize from the feedback.** The big picture thing that's happening here is that we're trying to create skills that can be used a million times (maybe literally, maybe even more who knows) across many different prompts. Here you and the user are iterating on only a few examples over and over again because it helps move faster. The user knows these examples in and out and it's quick for them to assess new outputs. But if the skill you and the user are codeveloping works only for those examples, it's useless. Rather than put in fiddly overfitty changes, or oppressively constrictive MUSTs, if there's some stubborn issue, you might try branching out and using different metaphors, or recommending different patterns of working. It's relatively cheap to try and maybe you'll land on something great.
2. **Keep the prompt lean.** Remove things that aren't pulling their weight. Make sure to read the transcripts, not just the final outputs — if it looks like the skill is making the model waste a bunch of time doing things that are unproductive, you can try getting rid of the parts of the skill that are making it do that and seeing what happens.
3. **Explain the why.** Try hard to explain the **why** behind everything you're asking the model to do. Today's LLMs are *smart*. They have good theory of mind and when given a good harness can go beyond rote instructions and really make things happen. Even if the feedback from the user is terse or frustrated, try to actually understand the task and why the user is writing what they wrote, and what they actually wrote, and then transmit this understanding into the instructions. If you find yourself writing ALWAYS or NEVER in all caps, or using super rigid structures, that's a yellow flag — if possible, reframe and explain the reasoning so that the model understands why the thing you're asking for is important. That's a more humane, powerful, and effective approach.
4. **Look for repeated work across test cases.** Read the transcripts from the test runs and notice if the subagents all independently wrote similar helper scripts or took the same multi-step approach to something. If all 3 test cases resulted in the subagent writing a `create_docx.py` or a `build_chart.py`, that's a strong signal the skill should bundle that script. Write it once, put it in `scripts/`, and tell the skill to use it. This saves every future invocation from reinventing the wheel.

This task is pretty important (we are trying to create billions a year in economic value here!) and your thinking time is not the blocker; take your time and really mull things over. I'd suggest writing

a draft revision and then looking at it anew and making improvements. Really do your best to get into the head of the user and understand what they want and need.

The iteration loop

After improving the skill:

1. Apply your improvements to the skill
2. Rerun all test cases into a new `iteration-<N+1>/` directory, including baseline runs. If you're creating a new skill, the baseline is always `without_skill` (no skill) — that stays the same across iterations. If you're improving an existing skill, use your judgment on what makes sense as the baseline: the original version the user came in with, or the previous iteration.
3. Launch the reviewer with `--previous-workspace` pointing at the previous iteration
4. Wait for the user to review and tell you they're done
5. Read the new feedback, improve again, repeat

Keep going until:

- The user says they're happy
 - The feedback is all empty (everything looks good)
 - You're not making meaningful progress
-

Advanced: Blind comparison

For situations where you want a more rigorous comparison between two versions of a skill (e.g., the user asks "is the new version actually better?"), there's a blind comparison system. Read `agents/comparator.md` and `agents/analyzer.md` for the details. The basic idea is: give two outputs to an independent agent without telling it which is which, and let it judge quality. Then analyze why the winner won.

This is optional, requires subagents, and most users won't need it. The human review loop is usually sufficient.

Description Optimization

The description field in SKILL.md frontmatter is the primary mechanism that determines whether Claude invokes a skill. After creating or improving a skill, offer to optimize the description for better triggering accuracy.

Step 1: Generate trigger eval queries

Create 20 eval queries — a mix of should-trigger and should-not-trigger. Save as JSON:

```
[
  {"query": "the user prompt", "should_trigger": true},
  {"query": "another prompt", "should_trigger": false}
]
```

The queries must be realistic and something a Claude Code or Claude.ai user would actually type. Not abstract requests, but requests that are concrete and specific and have a good amount of detail. For instance, file paths, personal context about the user's job or situation, column names and values, company names, URLs. A little bit of backstory. Some might be in lowercase or contain abbreviations or typos or casual speech. Use a mix of different lengths, and focus on edge cases rather than making them clear-cut (the user will get a chance to sign off on them).

Bad: "Format this data", "Extract text from PDF", "Create a chart"

Good: "ok so my boss just sent me this xlsx file (its in my downloads, called something like 'Q4 sales final FINAL v2.xlsx') and she wants me to add a column that shows the profit margin as a percentage. The revenue is in column C and costs are in column D i think"

For the **should-trigger** queries (8-10), think about coverage. You want different phrasings of the same intent — some formal, some casual. Include cases where the user doesn't explicitly name the skill or file type but clearly needs it. Throw in some uncommon use cases and cases where this skill competes with another but should win.

For the **should-not-trigger** queries (8-10), the most valuable ones are the near-misses — queries that share keywords or concepts with the skill but actually need something different. Think adjacent domains, ambiguous phrasing where a naive keyword match would trigger but shouldn't, and cases where the query touches on something the skill does but in a context where another tool is more appropriate.

The key thing to avoid: don't make should-not-trigger queries obviously irrelevant. "Write a fibonacci function" as a negative test for a PDF skill is too easy — it doesn't test anything. The negative cases should be genuinely tricky.

Step 2: Review with user

Present the eval set to the user for review using the HTML template:

1. Read the template from `assets/eval_review.html`
2. Replace the placeholders:

- `__EVAL_DATA_PLACEHOLDER__` → the JSON array of eval items (no quotes around it — it's a JS variable assignment)
 - `__SKILL_NAME_PLACEHOLDER__` → the skill's name
 - `__SKILL_DESCRIPTION_PLACEHOLDER__` → the skill's current description
3. Write to a temp file (e.g., `/tmp/eval_review_<skill-name>.html`) and open it: `open /tmp/eval_review_<skill-name>.html`
 4. The user can edit queries, toggle should-trigger, add/remove entries, then click "Export Eval Set"
 5. The file downloads to `~/Downloads/eval_set.json` — check the Downloads folder for the most recent version in case there are multiple (e.g., `eval_set (1).json`)

This step matters — bad eval queries lead to bad descriptions.

Step 3: Run the optimization loop

Tell the user: "This will take some time — I'll run the optimization loop in the background and check on it periodically."

Save the eval set to the workspace, then run in the background:

```
python -m scripts.run_loop \  
--eval-set <path-to-trigger-eval.json> \  
--skill-path <path-to-skill> \  
--model <model-id-powering-this-session> \  
--max-iterations 5 \  
--verbose
```

Use the model ID from your system prompt (the one powering the current session) so the triggering test matches what the user actually experiences.

While it runs, periodically tail the output to give the user updates on which iteration it's on and what the scores look like.

This handles the full optimization loop automatically. It splits the eval set into 60% train and 40% held-out test, evaluates the current description (running each query 3 times to get a reliable trigger rate), then calls Claude to propose improvements based on what failed. It re-evaluates each new description on both train and test, iterating up to 5 times. When it's done, it opens an HTML report in the browser showing the results per iteration and returns JSON with `best_description` — selected by test score rather than train score to avoid overfitting.

How skill triggering works

Understanding the triggering mechanism helps design better eval queries. Skills appear in Claude's `available_skills` list with their name + description, and Claude decides whether to consult a skill based on that description. The important thing to know is that Claude only consults skills for tasks it can't easily handle on its own — simple, one-step queries like "read this PDF" may not trigger a skill even if the description matches perfectly, because Claude can handle them directly with basic tools. Complex, multi-step, or specialized queries reliably trigger skills when the description matches.

This means your eval queries should be substantive enough that Claude would actually benefit from consulting a skill. Simple queries like "read file X" are poor test cases — they won't trigger skills regardless of description quality.

Step 4: Apply the result

Take `best_description` from the JSON output and update the skill's SKILL.md frontmatter. Show the user before/after and report the scores.

Package and Present (only if `present_files` tool is available)

Check whether you have access to the `present_files` tool. If you don't, skip this step. If you do, package the skill and present the .skill file to the user:

```
python -m scripts.package_skill <path/to/skill-folder>
```

After packaging, direct the user to the resulting `.skill` file path so they can install it.

Claude.ai-specific instructions

In Claude.ai, the core workflow is the same (draft → test → review → improve → repeat), but because Claude.ai doesn't have subagents, some mechanics change. Here's what to adapt:

Running test cases: No subagents means no parallel execution. For each test case, read the skill's SKILL.md, then follow its instructions to accomplish the test prompt yourself. Do them one at a time. This is less rigorous than independent subagents (you wrote the skill and you're also running it, so you have full context), but it's a useful sanity check — and the human review step compensates. Skip the baseline runs — just use the skill to complete the task as requested.

Reviewing results: If you can't open a browser (e.g., Claude.ai's VM has no display, or you're on a remote server), skip the browser reviewer entirely. Instead, present results directly in the conversation. For each test case, show the prompt and the output. If the output is a file the user needs to see (like a .docx or .xlsx), save it to the filesystem and tell them where it is so they can download and inspect it. Ask for feedback inline: "How does this look? Anything you'd change?"

Benchmarking: Skip the quantitative benchmarking — it relies on baseline comparisons which aren't meaningful without subagents. Focus on qualitative feedback from the user.

The iteration loop: Same as before — improve the skill, rerun the test cases, ask for feedback — just without the browser reviewer in the middle. You can still organize results into iteration directories on the filesystem if you have one.

Description optimization: This section requires the `claude` CLI tool (specifically `claude -p`) which is only available in Claude Code. Skip it if you're on Claude.ai.

Blind comparison: Requires subagents. Skip it.

Packaging: The `package_skill.py` script works anywhere with Python and a filesystem. On Claude.ai, you can run it and the user can download the resulting `.skill` file.

Updating an existing skill: The user might be asking you to update an existing skill, not create a new one. In this case:

- **Preserve the original name.** Note the skill's directory name and `name` frontmatter field -- use them unchanged. E.g., if the installed skill is `research-helper`, output `research-helper.skill` (not `research-helper-v2`).
- **Copy to a writable location before editing.** The installed skill path may be read-only. Copy to `/tmp/skill-name/`, edit there, and package from the copy.
- **If packaging manually, stage in `/tmp/` first,** then copy to the output directory -- direct writes may fail due to permissions.

Cowork-Specific Instructions

If you're in Cowork, the main things to know are:

- You have subagents, so the main workflow (spawn test cases in parallel, run baselines, grade, etc.) all works. (However, if you run into severe problems with timeouts, it's OK to run the test prompts in series rather than parallel.)
- You don't have a browser or display, so when generating the eval viewer, use `--static <output_path>` to write a standalone HTML file instead of starting a server. Then proffer a link that the user can click to open the HTML in their browser.

- For whatever reason, the Cowork setup seems to disincline Claude from generating the eval viewer after running the tests, so just to reiterate: whether you're in Cowork or in Claude Code, after running tests, you should always generate the eval viewer for the human to look at examples before revising the skill yourself and trying to make corrections, using `generate_review.py` (not writing your own boutique html code). Sorry in advance but I'm gonna go all caps here: **GENERATE THE EVAL VIEWER BEFORE** evaluating inputs yourself. You want to get them in front of the human ASAP!
 - Feedback works differently: since there's no running server, the viewer's "Submit All Reviews" button will download `feedback.json` as a file. You can then read it from there (you may have to request access first).
 - Packaging works — `package_skill.py` just needs Python and a filesystem.
 - Description optimization (`run_loop.py` / `run_eval.py`) should work in Cowork just fine since it uses `claude -p` via subprocess, not a browser, but please save it until you've fully finished making the skill and the user agrees it's in good shape.
 - **Updating an existing skill:** The user might be asking you to update an existing skill, not create a new one. Follow the update guidance in the `claude.ai` section above.
-

Reference files

The `agents/` directory contains instructions for specialized subagents. Read them when you need to spawn the relevant subagent.

- `agents/grader.md` — How to evaluate assertions against outputs
- `agents/comparator.md` — How to do blind A/B comparison between two outputs
- `agents/analyzer.md` — How to analyze why one version beat another

The `references/` directory has additional documentation:

- `references/schemas.md` — JSON structures for `evals.json`, `grading.json`, etc.
-

Repeating one more time the core loop here for emphasis:

- Figure out what the skill is about
- Draft or edit the skill
- Run `claude-with-access-to-the-skill` on test prompts
- With the user, evaluate the outputs:
 - Create `benchmark.json` and run `eval-viewer/generate_review.py` to help the user review them
 - Run quantitative evals
- Repeat until you and the user are satisfied
- Package the final skill and return it to the user.

Please add steps to your TodoList, if you have such a thing, to make sure you don't forget. If you're in Cowork, please specifically put "Create evals JSON and run `eval-viewer/generate_review.py` so human can review test cases" in your TodoList to make sure it happens.

Good luck!