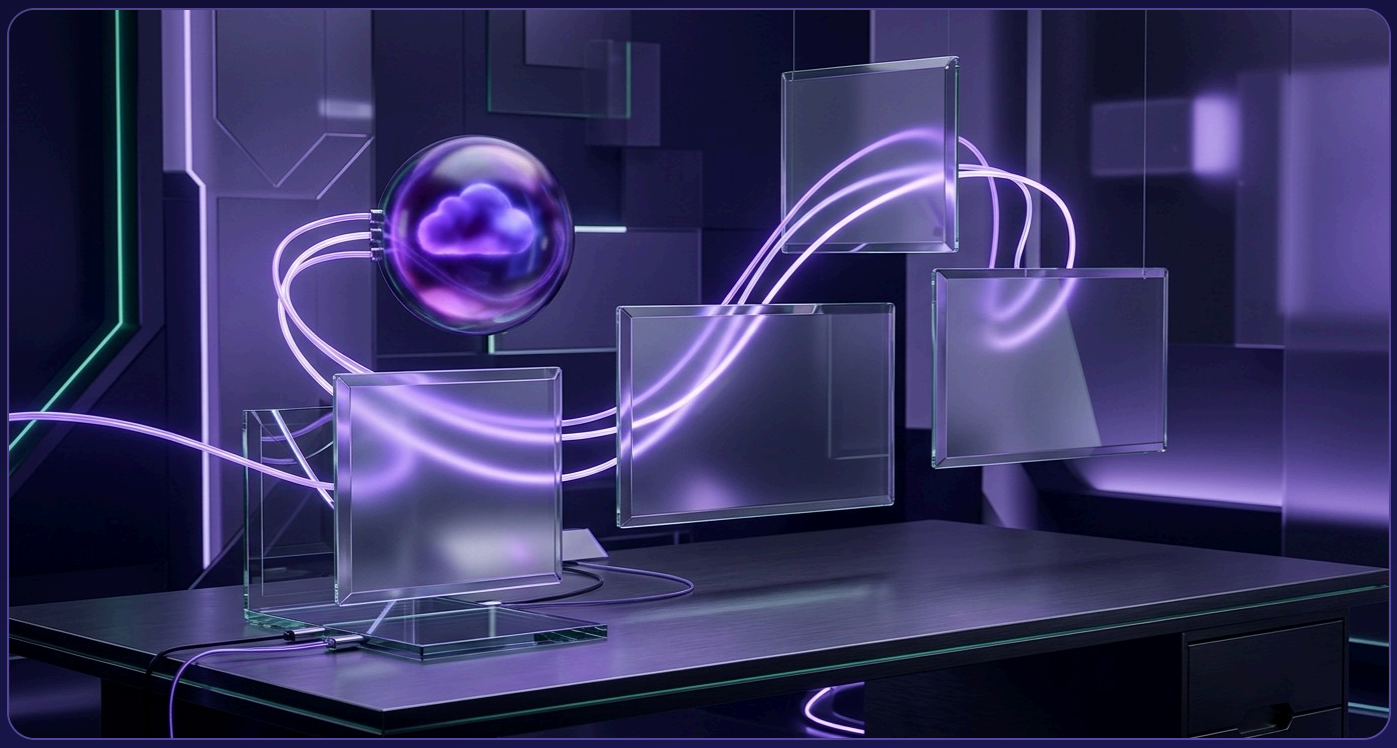
ANTHROPIC CLAUDE & WORKSPACE STUDIOS • FIELD GUIDE

Claude Cowork & Computer Use

Delegating real desktop work, cloud remote sessions, and recurring tasks without surrendering your mouse—mastering One Claude, the 3-tier tool hierarchy, Background macOS Spaces, and safety gates.

One Claude Unified Recents | 3-Tier Execution Routing | Background macOS Spaces | Scoped Local Folder Mounts | Cloud & Chrome Schedules | Human-in-the-Loop Gates



Start Anywhere, Continue Everywhere

Kick off a task on Claude Desktop, monitor live progress from iOS or Android on your commute, and review results in one unified Recents list.

Keep Your Cursor Free

Background Computer Use operates inside an isolated macOS Space behind the scenes—auto-pausing cleanly if you ever step into that window.

Fastest Tool First, Safe by Design

Claude routes through direct MCP APIs first, built-in browser second, and desktop UI clicks last—pausing for approval before payments or sends.

The “One Claude” Mental Model & Execution Routing

Instead of treating chat, browser automation, and desktop control as separate apps, Anthropic unified them into **One Claude**. Whether you open **Claude Desktop** on macOS, `claude.ai` on the web, or the **iOS/Android mobile app**, every Cowork task lives inside one synchronized **Recents** timeline backed by cloud remote sessions.

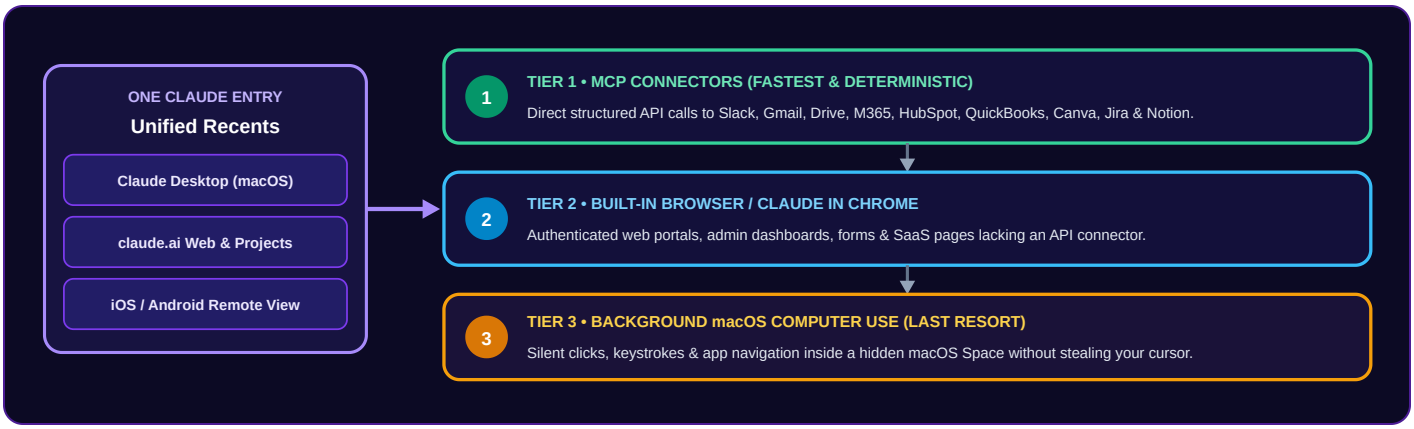
Quick Navigation

1. One Claude & 3-Tier Routing Model p. 2
2. Plans, macOS Setup & Tool Matrix p. 3
3. Annotated Cowork Workspace UI Tour p. 4
4. The 3-Tier Tool Hierarchy Deep Dive p. 5
5. Task Anatomy & Scoped Folder Mounts p. 6
6. Background macOS Computer Use p. 7
7. Two Recurring Schedule Engines p. 8
8. 5 Real-World Copy-Paste Recipes p. 9
9. Governance, Privacy & Safety Gates p. 10
10. Cross-Tool Morning Briefing Pipeline p. 11
11. Troubleshooting Clinic & Pre-Flight p. 12
Golden Rule: API First, Clicks Last All

Cloud Remote Sessions vs. Local Desktop Reach

When a Cowork task relies on web connectors (Gmail, Slack, Notion, HubSpot, Drive) or research, it runs inside an encrypted **cloud remote session**—so you can start it from your phone or close your laptop lid while Claude finishes. Whenever a task needs files in a mounted local folder or native macOS apps without APIs, Claude Desktop executes locally using scoped permissions and Background Spaces.

Architecture: 3-Tier Execution Routing Waterfall



Why Routing Matters: Never Burn Screen Pixels When an API Exists

An MCP call pulls 50 Slack messages or 200 HubSpot deals in 800 milliseconds with zero UI ambiguity. Claude reserves Computer Use exclusively for legacy desktop software, multi-app macOS workflows, and portals without connectors.

Plan Tiers, macOS Grants & Ecosystem Decision Matrix

Cowork and Computer Use span **Pro**, **Max**, **Ultra**, **Team**, and **Enterprise** subscriptions, pairing cloud remote execution with explicit, revocable macOS permissions whenever local files or desktop windows are involved.

1 Subscription Tiers & Nov 2026 Rollout

- **Pro, Max & Ultra:** Full Cowork access, cloud remote sessions, Chrome tasks, connector file transfers (beta, Nov 24), and Monthly Recap (`Reflect`, GA Nov 24).
- **Team & Enterprise:** Shared MCP catalogs, zero training, and **Computer Use (beta, Nov 20, 2026)** governed by Org Owners with SSO and audit logs.
- **Desktop Channels (Nov 17):** Pick `Stable` (default) or daily `Latest` in Claude Desktop settings to control rollout cadence.
- **Cloud vs. Local Rule:** Cloud sessions survive closed laptops; local mounts & UI automation require Desktop open and awake.

2 60-Second macOS Permission Setup

1. Install **Claude Desktop for macOS** and toggle on **Cowork & Computer Use** inside `Settings → Capabilities`.
2. Open `System Settings → Privacy & Security → Screen & System Audio Recording` and enable **Claude** (lets Claude read background app state).
3. Open `Privacy & Security → Accessibility` and enable **Claude** (grants isolated click and keystroke dispatch).
4. Grant per-task **Local Folder Mounts** only to dedicated working directories like `~/Documents/Invoices`—never root `~/`.

One-Minute Check: Cloud Remote Session vs. Local Desktop Execution

Ask yourself one question before hitting Run: *"Does this task touch a folder on my hard drive or a native macOS app?"* If **No** (Gmail, Drive, Slack, HubSpot, web portals), Claude runs in a **Cloud Remote Session** you can monitor from your phone. If **Yes**, keep your Mac awake and mount only the exact folder needed.

Ecosystem Decision Matrix: Picking the Right Anthropic Worker

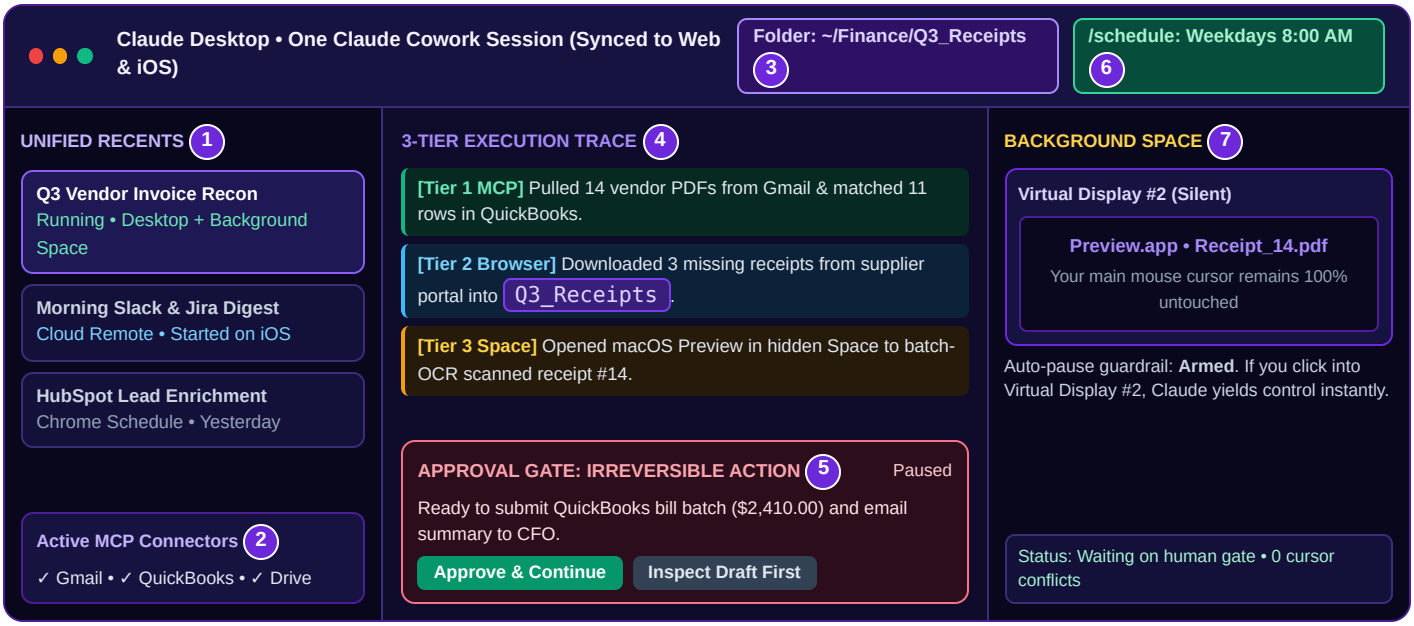
Anthropic Tool	Sweet Spot & Input Surface	Speed & Reliability	Auth & Device Scope	Best Used For
Claude Cowork *Orchestration Hub*	Multi-step knowledge work across connectors, mounted files, and web/UI fallbacks.	**Adaptive:** Picks fastest tier automatically per sub-step.	Cloud remote + local Mac folders; viewable on Mobile.	Expense triage, client onboarding, weekly ops briefings.
Claude in Chrome *Browser Extension*	DOM-aware navigation inside your active Chrome profile with existing logins.	**High:** Reads structured page elements instead of guessing pixels.	Runs locally inside your signed-in Chrome browser.	Web portal forms, CRM updates, recurring tab scraping.
Computer Use *Background macOS UI*	Desktop apps without APIs (Keynote, Preview, legacy ERP, Finder batches).	**Moderate:** Visual inspection + background Space clicks.	Local macOS Desktop with Screen & Accessibility grants.	Native app exports, GUI-only installers, cross-app drag/save.
MCP Connectors *Direct Tool APIs*	Slack, Gmail, Drive, M365, HubSpot, QuickBooks, Canva, Jira & Notion.	**Instant & Exact:** Zero brittle selectors or screen lag.	OAuth / Org allowlisted in cloud or Desktop.	Searching emails, filing Jira issues, syncing QuickBooks rows.
Claude Code *Terminal & Git Agent*	Software repositories, shell scripts, builds, git branches, and test suites.	**Blazing Fast:** Native CLI, diff edits, and test verification.	Local terminal or cloud sandbox repositories.	Building features, refactoring codebases, CI debugging.

Rule of Thumb: Start in Cowork, Let Claude Choose the Tier

You do not have to micromanage whether Claude opens an MCP tool or a browser tab. State your outcome, connect your approved MCP tools, mount a tight local folder if required, and let Cowork escalate down the 3-tier waterfall only when needed.

Annotated Tour: Inside the Claude Cowork Workspace

One unified window connects your cross-device **Recents** feed, active connector badges, scoped local folder mounts, live Background macOS Space previews, and human-in-the-loop safety gates.



1 **Unified Recents Rail:** Every Cowork task syncs across Desktop, `claude.ai`, and mobile apps in real time.

2 **Connector Pill Strip:** Shows live OAuth-verified MCP tools (Gmail, Slack, QuickBooks, Drive) ready for Tier 1 calls.

3 **Scoped Folder Badge:** Confirms the exact local directory mounted for read/write work—everything outside stays invisible.

4 **3-Tier Execution Trace:** Transparently logs whether each step ran via MCP API, built-in browser, or desktop Space.

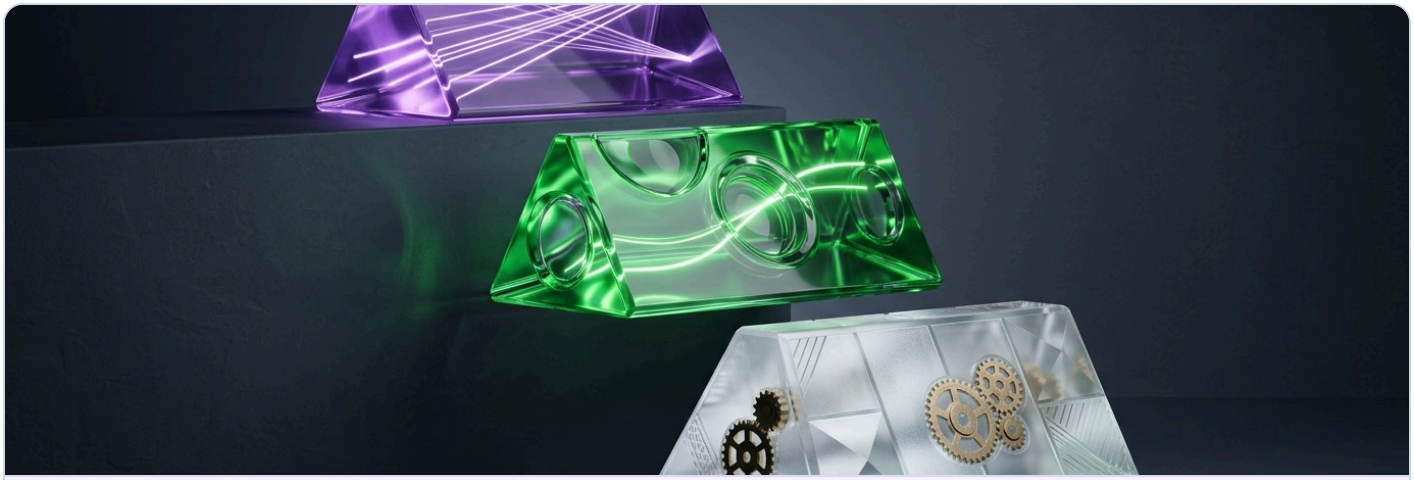
5 **Human-in-the-Loop Gate:** Hard-pauses before irreversible actions (payments, outbound emails, deletions) for one-click approval.

6 `/schedule` **Runner Badge:** Converts any proven one-off Cowork workflow into an hourly, daily, weekday, or weekly automation.

7 **Background macOS Space Preview:** Shows a live thumbnail of Claude's isolated virtual workspace so you can inspect progress visually without giving up your keyboard or cursor.

Mastering the 3-Tier Tool Hierarchy

Great Cowork operators think in layers. Rather than asking Claude to click around your screen for data that already lives behind a clean API, you guide workflows through a cascading waterfall: structured MCP pipes first, browser lenses second, and desktop pixels third.



Top-Down Precision Waterfall: Tier 1 MCP connectors deliver instant structured JSON; Tier 2 built-in browser handles authenticated portals; Tier 3 Computer Use steps in only when native desktop UI interaction is mandatory.

1 Tier 1: MCP Connectors

First stop for SaaS systems of record. Zero screen parsing, full pagination, and cloud remote compatibility.

Native roster: Slack, Gmail, Google Drive, Microsoft 365, HubSpot, QuickBooks, Canva, Jira & Notion.

2 Tier 2: Built-In Browser

Steps in when a vendor portal, HR dashboard, or supplier invoice site has no MCP API.

Two flavors: Cowork's built-in sandbox browser, or **Claude in Chrome** reusing your live session cookies.

3 Tier 3: Computer Use

The tactile fallback for local macOS apps, custom Finder moves, or legacy desktop software.

Key strength: Operates inside a background macOS Space so you keep working uninterrupted.

Always State Connector Preference in Multi-App Tasks

When a workflow touches both SaaS and desktop apps, explicitly name your Tier 1 connectors: *"Read messages via Slack MCP and pull slides from Google Drive MCP; only open Chrome if a vendor link requires portal login."* That one sentence cuts task runtime by up to 80% and prevents unnecessary screen captures.

Prompt & Task Anatomy + Scoped Folder Mounts

Vague prompts like *"clean up my invoices"* invite guesswork. Combining five explicit building blocks—Goal, Scope, Connectors, Fallback, and Confirmation Gate—gives Claude crystal-clear guardrails on the very first run.

The 5-Part Cowork Task Anatomy

[1. Goal & Deliverable] Reconcile all March contractor invoices into a clean reconciliation CSV and draft summary email. **[2. Scope / Folder Mount]** Read and write strictly inside the mounted `~/Finance/March_Recon` folder. **[3. Preferred Connectors]** Pull invoice attachments via Gmail MCP and match vendor IDs against QuickBooks MCP. **[4. Browser / Desktop Fallback]** If a portal link lacks an attachment, download the PDF via Claude in Chrome; use macOS Preview only for scanned OCR. **[5. Confirmation Gate]** Pause and show me a line-item summary before posting any QuickBooks bills or sending the CFO email.

Task Component	What It Governs During Execution	Risk When Left Unspecified
Goal & Deliverable	Defines exact output artifact (CSV, Slack digest, Jira ticket batch, renamed files).	Claude stops mid-way or produces chat prose instead of saved files.
Scope / Folder Mount	Restricts local filesystem reach to one dedicated working directory.	Broad mounts risk scanning personal docs or writing to wrong folders.
Preferred Connectors	Pins Tier 1 MCP APIs (Slack, Drive, M365, Notion, Jira) before touching browsers.	Slow pixel clicking inside a web app when an instant API exists.
Browser / Desktop Fallback	Names exact Tier 2 portal or Tier 3 macOS app permitted when APIs fall short.	Claude aborts at the first login wall or guesses the wrong local app.
Confirmation Gate	Forces a hard pause before payments, sends, deletes, or production writes.	Unreviewed batch actions dispatch before you verify edge cases.

Three Proven Local Folder Mount Patterns

A The Quarantine Drop-Box

Mount only `~/Cowork_Inbox/`. Drag raw PDFs, screenshots, or exports in; let Claude rename, extract CSVs, and place finished results into `~/Cowork_Inbox/Done/`.

B Read-Only Reference + Output

Grant read access to `~/Client_Assets/` and write access only to `~/Client_Deliverables/` so original brand kits or contracts can never be overwritten.

C Zero-Local Cloud Mode

Skip mounting any local folder at all when working between Drive, Notion, Slack, and HubSpot—keeping the entire run inside a portable cloud remote session.

Never Mount `~/`, `~/Desktop`, or Password Managers

Keep local folder mounts surgical. A dedicated per-workflow folder acts as a physical blast-radius boundary and prevents stray temporary files from cluttering your desktop.

Background macOS Computer Use Without Hijacking Your Mouse

Earlier desktop agents locked you out of your own Mac, yanking your mouse cursor across the screen every two seconds. Claude's **Background macOS Computer Use** runs clicks, scrolling, and keystrokes inside a hidden Space while your active cursor stays completely yours.



Isolated Dual-Layer Execution: Write emails or edit code on your primary display while Claude quietly drives desktop apps inside an off-screen macOS workspace behind frosted isolation.

How Background Spaces & Auto-Pause Safety Work

1 Hidden macOS Space Isolation

When Tier 3 activates, Claude Desktop spins up target app windows inside a separate virtual Space. Screenshot inspection and synthetic pointer/keyboard events route directly to that Space—so your active window focus never flickers.

2 Automatic Input-Interference Yielding

If you switch into Claude's working window, move the mouse over its active target, or type on the keyboard inside that Space, Claude detects user input immediately, **auto-pauses**, and hands control back to you cleanly.

Best Practices for Smooth Background Desktop Runs

Keep target apps signed in before launching a batch, avoid locking your Mac screen (use a dim display sleep timer instead of lock-on-idle), and watch the live thumbnail in Claude's sidecar whenever you want to verify a multi-step native export without switching Spaces.

Two Recurring Engines: Cowork `/schedule` vs. Chrome Schedules

Once a manual workflow works reliably, promote it to autopilot. Anthropic gives you two distinct scheduling engines—knowing which one runs with your laptop lid closed and which one relies on your live browser cookies prevents missed morning runs.

A Cowork Scheduled Tasks (`/schedule`)

- **Cadences:** Run **hourly**, **daily**, **weekdays**, or **weekly** directly from any Cowork thread via `/schedule` or the Schedule button.
- **Cloud Remote Tasks (Lid Closed OK!):** Workflows using only Tier 1 MCP connectors (Slack, Gmail, Drive, Jira, Notion, HubSpot) execute in Anthropic's cloud even while your MacBook is asleep in a backpack.
- **Local Folder & macOS Tasks:** Any schedule touching local mounted files or Tier 3 Computer Use queues until Claude Desktop is open and your Mac is awake.

B Chrome Scheduled Tasks

- **Purpose-Built for Web Portals:** Runs recurring workflows through **Claude in Chrome** inside your authenticated browser profile.
- **Zero Re-Authentication Friction:** Ideal for SSO-protected vendor dashboards, bank/carrier portals, competitor pricing checks, and recurring web form submissions that lack MCP APIs.
- **Device Requirement:** Because it uses your live Chrome profile and session cookies, your computer and Chrome must be awake at the scheduled trigger window.

Side-by-Side Comparison: Choosing Your Automation Engine

Dimension	Cowork `/schedule` (Cloud & Desktop)	Chrome Scheduled Tasks
Runs With Laptop Lid Closed?	**Yes** for pure MCP/cloud jobs; **No** if local files or macOS UI are needed.	**No** (requires local Mac awake with Chrome running).
Primary Execution Tier	Tier 1 MCP Connectors + local mounts / Tier 3 Spaces.	Tier 2 DOM-level browser navigation in signed-in tabs.
Best Cadence Fit	7:30 AM weekday executive briefings, hourly triage, weekly Notion rollups.	Daily portal CSV downloads, weekly SaaS billing PDF fetches, form fills.
Mobile Review & Alerts	Results appear immediately in **One Claude Recents** on iOS/Android.	Synced to Recents once the local Chrome run completes.

```
/schedule weekdays at 07:45 AM — Summarize unread urgent Gmail threads + #eng-incidents Slack messages from the last 24h, cross-check open P1 Jira blockers, and post a 5-bullet briefing card to my morning briefing thread. Cloud MCP only; no local folders.
```

Pro Pattern: Split Cloud Briefings From Local Desktop Runs

Keep your 7:30 AM executive digest purely on MCP connectors so it finishes in the cloud before you even flip open your MacBook. Schedule heavy local PDF exports or Chrome portal scrapes for 9:15 AM when you are already at your desk.

5 Real-World Copy-Paste Cowork Recipes

Paste any recipe below directly into Claude Desktop or `claude.ai`. Each prompt names its exact connectors, folder bounds, fallback tier, and safety approval gate so you get repeatable results with zero surprises.

Recipe & Use Case	Copy-Paste Prompt (Tier-Aware & Gated)	Execution Path & Output
1. Month-End Receipt Reconciliation *Finance & Ops*	`Search Gmail MCP for vendor receipts from the last 30 days, download PDFs into mounted ~/Finance/Receipts, match amounts against QuickBooks MCP open bills, and export discrepancies to recon.csv. Pause for my approval before creating or paying any QuickBooks bill.`	Tier 1 MCP + local mount; outputs `recon.csv` and holds writes behind a safety gate.
2. Cloud Morning Executive Briefing */schedule Weekdays*	`/schedule weekdays 7:30 AM: Read overnight Slack #leadership mentions, urgent Gmail threads from VIP clients, and Jira P0/P1 blockers via MCP. Draft concise 3-line replies for my top 4 emails in Gmail Drafts without sending, and save a 1-page briefing note in Notion.`	100% Cloud Remote Session (runs with laptop closed); synced to iOS Recents.
3. Portal Invoice Fetcher *Chrome Schedule*	`Using Claude in Chrome on my signed-in carrier portal tab, navigate to Billing → Statements, download the latest PDF into ~/Downloads/Carrier_Bills, rename it YYYY-MM_Carrier.pdf, and log the total into our Drive MCP Expenses Sheet. Stop if MFA is prompted.`	Tier 2 Chrome DOM + Tier 1 Drive MCP; pauses cleanly on unexpected MFA challenges.
4. Legacy Desktop Export Batch *Background Space*	`In Background macOS Computer Use, open each .key deck inside ~/Decks/Q2_Archive using Keynote, export to PDF at high quality into ~/Decks/PDF_Out, and close the window cleanly. Do not touch my foreground screen; pause if any font-missing dialog blocks export.`	Tier 3 hidden macOS Space; batch-renders native Keynote files while you keep working.
5. New Hire Onboarding Pack *HR & Enablement*	`Read our Onboarding_Checklist in Notion MCP, create a personalized 30-60-90 Doc in Google Drive MCP for Maya Chen (Product Eng), pull her Canva welcome banner link via Canva MCP, and draft a Slack welcome post for review. Do not post to Slack until I click Approve.`	Pure Tier 1 multi-MCP orchestration; prepares all assets with zero premature sends.

Test Once Manually, Then Wrap With `/schedule`

Never schedule an untested prompt straight onto daily autopilot. Run the recipe interactively once, watch which tier each step picks in the trace, verify the output files, and then attach `/schedule`.

Draft Mode Is the Best Safety Multiplier

Notice Recipes #2 and #5 ask Claude to create *Gmail Drafts* or stage posts rather than sending live. You get 95% of the labor saved while keeping 100% editorial sign-off.

Governance, Privacy & Human-in-the-Loop Safety Gates

Giving an AI agent access to your email, files, and desktop buttons demands clear boundaries. Anthropic pairs **least-privilege folder mounts** and **macOS privacy switches** with mandatory confirmation gates before irreversible actions occur.

1 Irreversible-Action Confirmation Gates

- **Hard Pause Categories:** Financial transfers, invoice payments, outbound customer emails, bulk file deletions, and permission changes trigger an explicit pause card.
- **Preview Before Commit:** Every gate displays the exact dollar amount, recipient list, or file path so you can approve, edit, or cancel in one click.
- **Admin Policy Locks:** Team and Enterprise admins can mandate approval gates on external MCP writes even if a prompt omits them.

2 Defending Against Indirect Prompt Injection

- **Untrusted Web Tabs & PDFs:** Random web pages, scraped forums, or external vendor emails can hide adversarial text trying to hijack browser actions.
- **Session Isolation:** Close sensitive banking, password manager, and admin tabs before letting Chrome tasks browse unfamiliar third-party sites.
- **Least-Privilege Connectors:** Connect only the specific MCP tools needed for a workflow; revoke unused OAuth tokens quarterly.

Security & Permission Hygiene Across Surfaces

Control Layer	Recommended Safe Configuration	Common Anti-Pattern to Avoid
Local Folder Mounts	Dedicated per-task folder (e.g., `~/Work/Invoices`) mounted just for that job.	Mounting your entire home directory (`~/`), `Documents`, or `.ssh` keys.
macOS OS Permissions	Grant Screen Recording & Accessibility only to verified Claude Desktop; audit monthly (**no sandbox** sits between Computer Use and allowed desktop apps).	Leaving unattended unlocked Macs running open-ended third-party web scraping.
Outbound Comms & Spend	Create drafts or stage carts first; require explicit click-to-send confirmation.	Instructing “auto-reply and pay all invoices without asking.”
Enterprise Governance	Org-approved MCP allowlist, Team/Enterprise Computer Use toggle (beta, Nov 20), zero-training guarantee, SSO & audit logs.	Connecting unvetted community MCP binaries holding production credentials.

What to Do If a Scraped Page Looks Suspicious

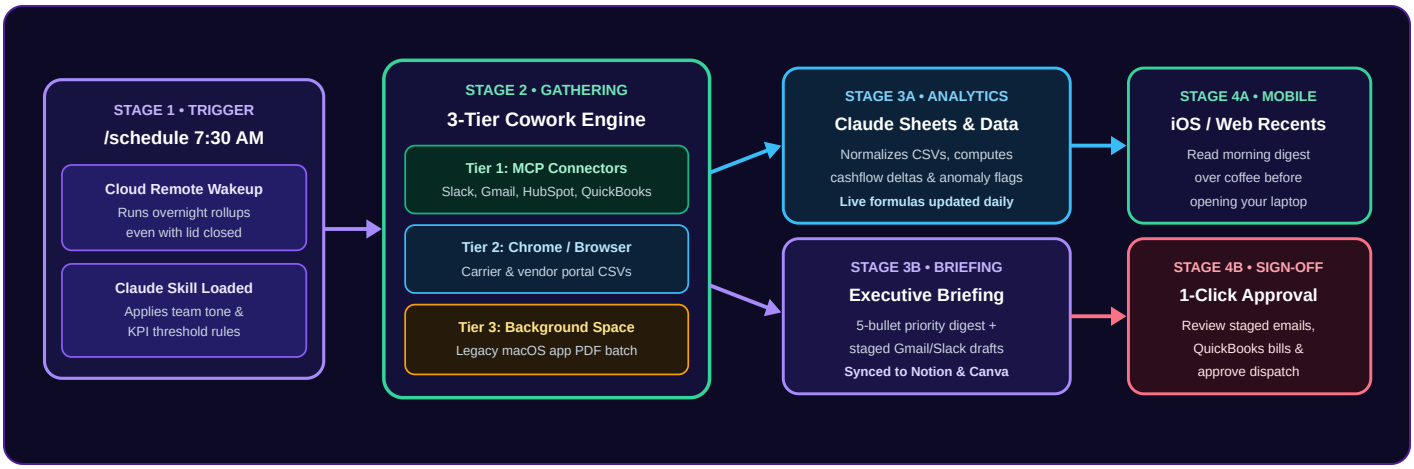
If Claude pauses and warns about unexpected instructions inside an email, PDF, or webpage—or tries to navigate toward an unrelated domain—click **Stop** immediately. Close the untrusted tab, revoke any temporary folder mount if not needed, and inspect the execution trace before restarting from a clean prompt.

Never Store Secrets in Plain-Text Prompts

Do not paste API keys, passwords, or credit card numbers directly into chat or scheduled prompts. Rely on official OAuth MCP connectors or sign in manually once inside Chrome before starting a browser task.

Cross-Tool Synergy: Automated Morning Briefing & Ops Loop

Cowork reaches its peak leverage when it acts as the conductor across Anthropic's entire studio—combining **MCP Connectors**, **Background Computer Use**, **Claude Skills**, and **Claude Sheets / Data** into one seamless daily loop.



How the 4 Stages Compound Every Morning

1 Overnight Cloud Rollup Before You Wake

At 7:30 AM, `/schedule` triggers in the cloud, pulling Slack, Gmail, HubSpot, and QuickBooks metrics via MCP using your saved **Claude Skill** formatting rules.

2 Automatic Local Handoff at Your Desk

Once you open Claude Desktop at 9:00 AM, any local steps—like Chrome vendor CSV downloads or Background Space PDF exports—run quietly without touching your active cursor.

3 Instant Claude Sheets & Data Modeling

Raw CSVs flow straight into **Claude Sheets** where formulas flag invoice variances, budget burn, and overdue receivables automatically.

4 Commute Review + 1-Click Approval

Skim the finished briefing inside **One Claude Recents** on iOS or Android, then tap **Approve** only on the drafted replies and payments you want shipped.

Pair Recurring Cowork Runs With Custom Claude Skills

Save your team's naming conventions, spreadsheet column schemas, and tone-of-voice rules inside a reusable **Claude Skill** so every scheduled briefing arrives formatted identically every single morning.

Troubleshooting Clinic & Pre-Flight Checklist

Use this diagnostic table whenever a macOS permission blocks a click, a scheduled task skips overnight, or Claude picks a slow UI route instead of an API—followed by our 6-point pre-flight checklist.

Symptom / Issue	Root Cause	10-Second Fix
1. Computer Use fails to click or read a desktop window	macOS Screen Recording or Accessibility toggle missing/stale after an app update.	Open `System Settings → Privacy & Security`, toggle **Claude** off and back on in both `Screen Recording` and `Accessibility`, then relaunch Desktop.
2. Background task keeps pausing mid-run	You moved the mouse inside Claude's active Space or typed during execution.	That is the **input-interference safety pause** working as designed; leave the Space undisturbed and click **Resume** in the Cowork pane.
3. `/schedule` task did not run overnight	Task depended on a local mounted folder, Chrome tab, or Tier 3 app while laptop slept.	Split pure MCP work into a cloud-only `/schedule` job, or schedule local/Chrome tasks during awake desk hours with Mac sleep disabled.
4. Claude clicks around Chrome instead of using Slack/Drive	MCP connector was disconnected or prompt omitted preferred Tier 1 tools.	Re-authenticate the connector under `Settings → Connectors` and name it explicitly (e.g., *"Use Gmail MCP and Drive MCP first"*).
5. Task stops with "Folder Access Denied"	Output path sits outside the folder mounted for the current Cowork session.	Grant a scoped mount to the exact working directory (e.g., `~/Finance/March_Recon`) or direct outputs into the mounted folder.
6. Chrome task stalls at an SSO or MFA prompt	Session cookie expired or portal requires hardware key / authenticator tap.	Sign into the portal manually in your Chrome tab first, complete MFA, then click **Continue** in Claude's task bar.
7. Cowork features missing on Team or Enterprise account	Organization administrator has not enabled Desktop Computer Use or specific MCPs.	Ask an Org Owner/Primary Owner to review `Organization settings → Capabilities` and allowlist required connectors.

6-Point Pre-Flight Checklist Before Delegating

- ☑ **1. Verify Tier 1 MCPs First:** Connect Slack, Gmail, Drive, Notion, Jira, or QuickBooks so Claude uses instant APIs before browsers or clicks.
- ☑ **2. Check macOS Privacy Grants:** Confirm **Claude** is enabled under both `Screen Recording` and `Accessibility` on macOS.
- ☑ **3. Mount a Tight Sandbox Folder:** Point local tasks at a dedicated subfolder like `~/Cowork_Inbox`—never root `~/`.
- ☑ **4. Add an Explicit Approval Gate:** Require a pause before payments, outbound sends, or deletes; prefer draft mode for comms.
- ☑ **5. Match Engine to Sleep State:** Keep `/schedule` overnight jobs pure-cloud MCP; run Chrome/local schedules while your Mac is awake.
- ☑ **6. Test Once Before Scheduling:** Run every new recipe manually once, inspect the 3-tier execution trace, then promote to `/schedule`.

Final Takeaway: Delegate Execution, Keep Command

One Claude unites cloud speed, browser reach, and quiet background macOS Spaces under one roof. Use APIs first, keep folder mounts narrow, guard irreversible steps with approval gates, and let your cursor stay yours.