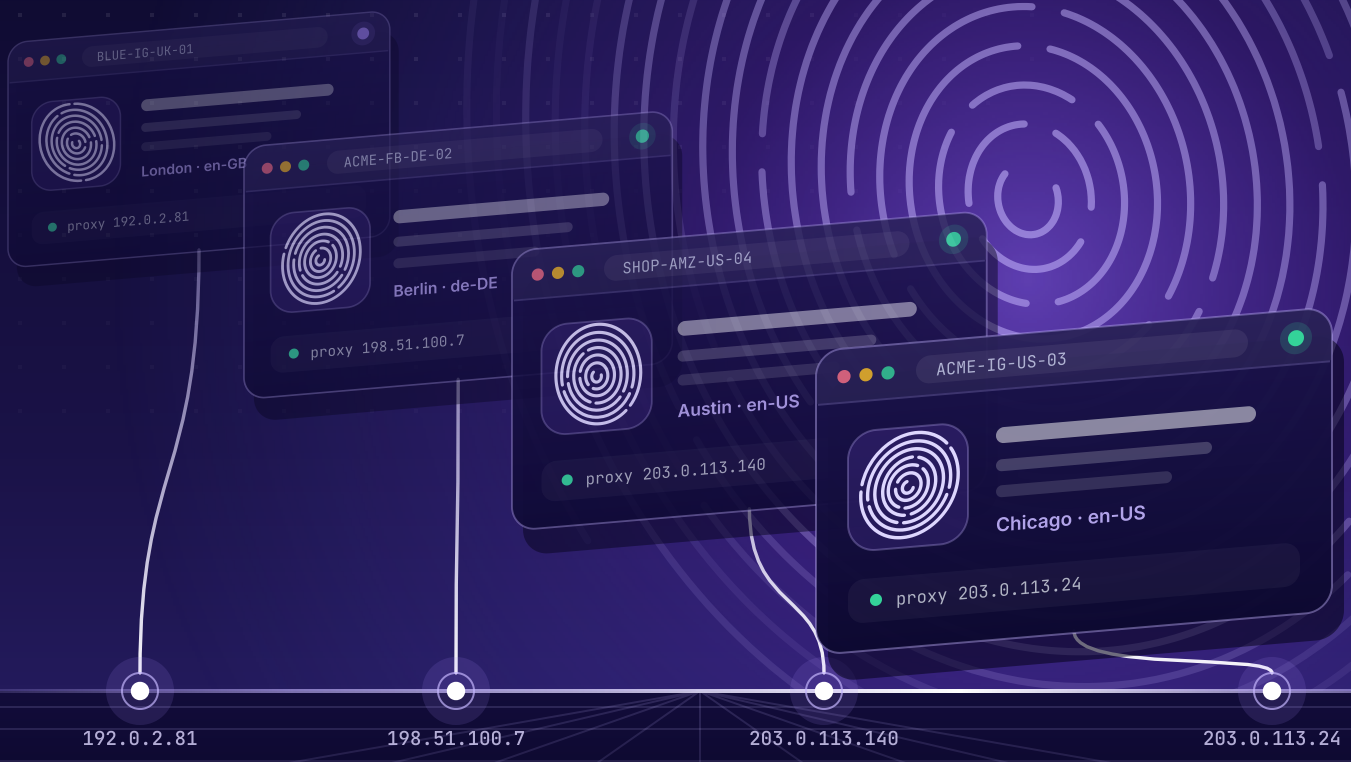
ProxyHorizon

2026 EDITION

A PROXYHORIZON FIELD GUIDE

The Antidetect Browser Handbook

Run multiple accounts safely with isolated profiles, consistent fingerprints and the right proxies.



- How fingerprinting and account linking really work
- Browser picks, proxy setups and team workflows
- Checklists, playbooks and Playwright code

BEFORE YOU BEGIN

About This Handbook

Antidetect browsers run many separate browser identities on one computer, each with its own cookies, fingerprint and IP address. Used well, they keep accounts cleanly apart. Used carelessly, they link everything you meant to separate.

Who It's For

Social and ad agencies
Client pages and ad accounts, kept separate, shared and auditable.
START WITH chapters 3, 6 and 8

E-commerce sellers
Storefronts and marketplace accounts that must stay apart.
START WITH chapters 3, 5 and 10

Affiliate marketers
Offers and ad accounts tested across markets, and kept healthy.
START WITH chapters 5, 7 and 10

QA and dev teams
Geo, language and device tests in repeatable environments.
START WITH chapters 2, 6 and 9

Privacy professionals
Work, personal and research identities kept apart from trackers.
START WITH chapters 1, 2 and 5

Automation builders
Profiles driven from code, and AI agents with stable identities.
START WITH chapters 4, 9 and 10

How to Read It

Chapters 1 to 3 explain fingerprinting and account linking. Chapters 4 to 6 turn that into a browser, a proxy plan and solid profiles. Chapters 7 to 10 cover daily operations, teams, automation and the rules. Each chapter ends with key takeaways; the appendix holds the checklists.

Signposts you'll see

Pro tip
Saves time or money.

Note
Context worth knowing.

Watch out
A common mistake to avoid.

Risk
Security or rules exposure.

Pro move
What experienced teams do.

Go deeper
A guide or free tool.

2026 Edition. Browser and proxy figures come from the ProxyHorizon directory as of November 2026. Prices change often, so check proxyhorizon.com/antidetect-browsers for live numbers. Example IPs use documentation ranges (RFC 5737), names are invented and API code uses placeholders, because every vendor's API differs. Nothing here is legal advice.

© 2026 ProxyHorizon. Share this PDF freely, unchanged and with credit.

YOUR MAP

Contents

	Why This Handbook Exists The problem antidetect browsers solve, and the mistakes this guide helps you skip.	04
01	**What an Antidetect Browser Actually Does** Three jobs per profile, and how it compares with incognito, VPNs and VMs.	05
02	**Browser Fingerprinting, Decoded** Four layers of signals, from canvas to TLS, and why consistency beats randomness.	09
03	**How Platforms Connect Accounts** The linking graph, risk scores, and what a browser can't hide for you.	15
04	**Choosing an Antidetect Browser** Eight criteria, ten browsers side by side and picks for every use case.	19
05	**Proxies: The Other Half of a Profile** One stable IP per profile, the right proxy type and nine networks to test.	24
06	**Building Profiles That Hold Up** A step-by-step build, naming, cookies and a QA check before first login.	29
07	**Warm-Up, Behavior and Account Health** A four-week warm-up, healthy habits and how to read warning signs.	34
08	**Running a Team on Profiles** Roles, shared profiles without shared passwords, SOPs and offboarding.	38
09	**Automation, APIs and AI Agents** Local APIs, Playwright and Puppeteer code, and guardrails for agents.	43
10	**Playbooks and Staying Compliant** Six setups you can copy, and the rules that keep them legitimate.	49
A	**Appendix** Launch checklist, fingerprint cheat sheet, troubleshooting, glossary and tools.	54

INTRODUCTION

Why This Handbook Exists

Picture a small agency on a Monday morning. By lunch, four client pages are asking for identity checks and two ad accounts are restricted. Nobody broke a rule on purpose. They simply ran every client from the same laptop, the same browser and the same office IP, and the platform drew a straight line between all of them.

That's the problem antidetect browsers solve. They give each account its own isolated browser, with its own storage, its own believable device fingerprint and its own proxy. Accounts that belong to different clients, stores or test cases stay as separate as they would if different people ran them on different computers.

> **The goal isn't to look like nobody. It's to look like the same somebody, every time you log in.**

The ProxyHorizon directory lists 25 antidetect browsers, and the same mistakes come up with all of them: one proxy shared by ten profiles, fingerprints randomized on every launch, brand-new accounts pushed to full speed on day one, passwords pasted into team chats. This handbook exists so you can skip them. It's opinionated where the evidence is clear and honest about the trade-offs where it isn't.

By the End, You'll Be Able To

- Explain what an antidetect browser changes, and what it can't hide.
- Read a fingerprint the way a platform does, and spot mismatches before they cost you an account.
- Choose a browser and a proxy type for your use case, budget and team size.
- Build profiles that stay consistent for the whole life of an account.
- Warm up new accounts, read health signals and respond calmly.
- Run a team on shared profiles without ever sharing a password.
- Drive profiles from Playwright, Puppeteer or Selenium, safely.

Use this responsibly

This handbook is about legitimate multi-account work: client and brand accounts, separate storefronts, testing, ad verification and privacy. Follow each platform's terms. Never use these tools for fraud, fake engagement, evading bans you earned through abuse, taking over accounts that aren't yours, or anything illegal. Chapter 10 covers the rules in detail.

01



What an Antidetect Browser Actually Does

An antidetect browser is one app that can be many browsers at once. Each profile gets its own storage, its own fingerprint and its own route to the internet, so a platform sees separate people instead of one person with many tabs. Here's how that works, and how it compares with the tools people try first.

IN THIS CHAPTER

1.1 The three jobs of every profile

1.2 Antidetect versus the alternatives

1.3 Who uses them, and for what

1.1 The Three Jobs of Every Profile

Open an antidetect browser and you won't see a browser at first. You'll see a list of **profiles**. Each one is a complete, separate browser identity: launch it and a window opens that behaves like a different computer from every other profile on your machine. To pull that off, the app does three jobs for every profile at once.

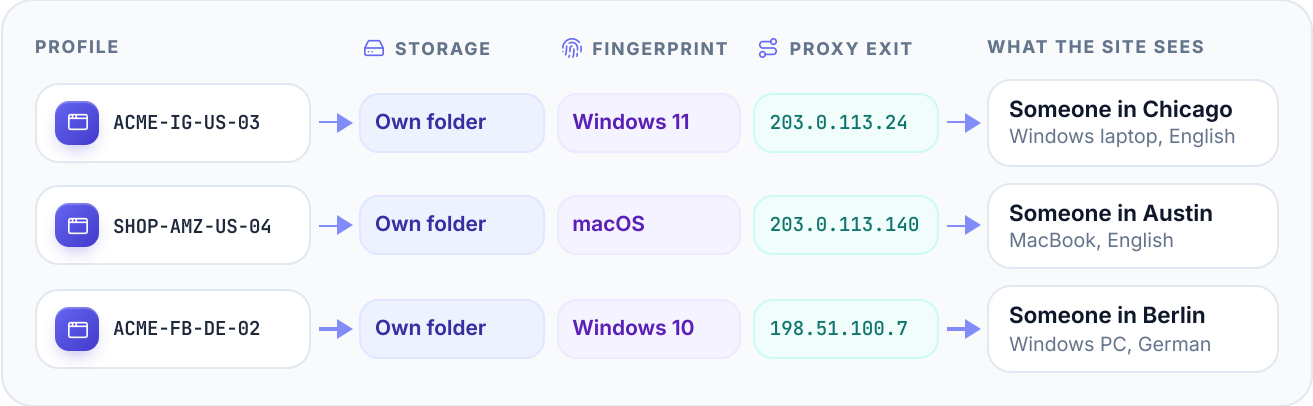


Figure 1.1 Three profiles on one laptop. Each keeps its own storage, device fingerprint and exit IP, so the platform sees three people in three places instead of one person with three tabs.

Isolate storage

Cookies, local storage, cache and saved logins live in the profile's own folder, so signing in to one account never touches another.

Present one fingerprint

Each profile reports its own device: system, screen, graphics, fonts and language, chosen to fit together and kept the same on every launch.

Route through its proxy

Every profile connects through its own proxy, so each account shows the platform a stable IP address in the right place.

Where profiles live

Profiles are stored on your computer, in the vendor's cloud, or both. Cloud sync lets a teammate open the same profile on another machine with its session intact, which is what makes team work possible (Chapter 8). It also means the vendor holds your logged-in sessions, so how they store and protect profiles is one of the questions to ask in Chapter 4.

Changed inside the engine, not on the page

Antidetect browsers are built on modified browser engines, usually Chromium and sometimes Firefox, that report the profile's values before any page code runs. Extensions that overwrite values after a page loads leave traces detection scripts look for, such as functions that no longer look native or values that differ between a page and its web workers.

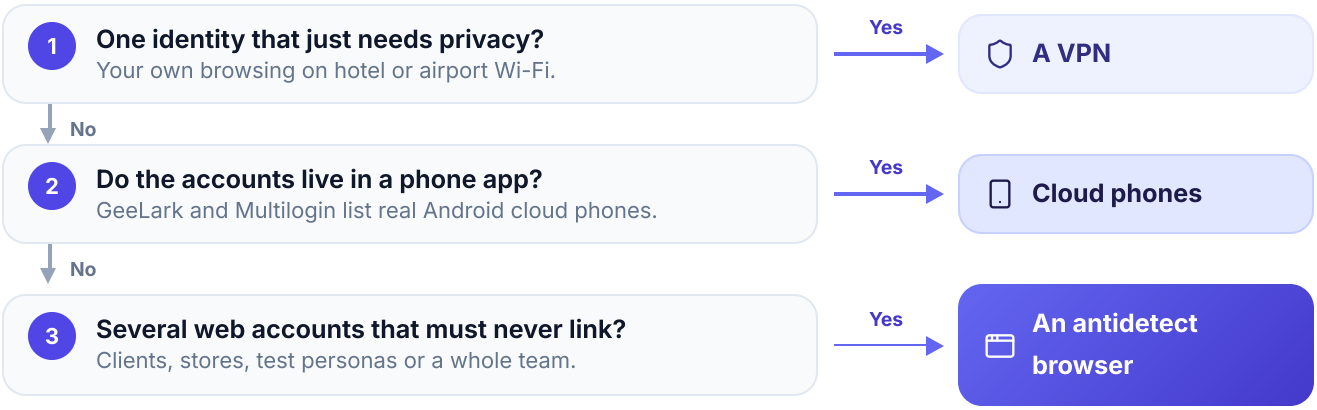
1.2 Antidetect Versus the Alternatives

Most people try incognito windows, Chrome profiles, a VPN or a virtual machine before they find antidetect browsers. Each of those separates part of an identity. Only an antidetect browser separates all three parts, for every profile, at a scale a team can actually use.

	Storage	Fingerprint	IP address	Scale	Best for
Incognito window	⊙ Temporary	⊗ Shared	⊗ Shared	One at a time	Logged-out checks
Chrome profiles	✓ Separate	⊗ Shared	⊗ Shared	A handful	Work vs personal
Session tools	✓ Separate	⊗ Shared	⊗ Shared	Many tabs	Juggling logins
VPN	⊗ Shared	⊗ Shared	⊙ One for all	One identity	Public Wi-Fi privacy
Proxy in a browser	⊗ Shared	⊗ Shared	✓ Separate	One per browser	Geo checks
Virtual machine	✓ Separate	⊙ Looks virtual	⊙ Via a proxy	A few per PC	System isolation
Cloud phone	✓ Separate	✓ Real Android	⊙ Via a proxy	Paid per device	Mobile-only apps
Antidetect browser	✓ Per profile	✓ Per profile	✓ Per profile	Hundreds+	Accounts at scale

"Shared" means every window or tab shows the same value, so accounts opened there can be linked. Session tools such as Ghost Browser and SessionBox One split cookies per tab but not the fingerprint, which is why the ProxyHorizon directory says Ghost Browser isn't a full antidetect engine.

Which tool fits your job?



Go deeper: Antidetect Browser vs VPN vs Proxy · Cloud Phone vs Antidetect Browser

1.3 Who Uses Them, and for What

Antidetect browsers have a reputation problem, because a tool that keeps an agency's clients apart can also be misused. But the legitimate uses are broad and ordinary, and they're what this handbook is about. Here's who relies on them day to day.

Agencies

Each client's pages and ad accounts in their own profiles, shared with the team, so one client's trouble never spreads to the next.

E-commerce sellers

Separate brands, storefronts and regional marketplace accounts that are allowed to coexist, each in its own profile.

Affiliates and media buyers

Offers, landing pages and campaigns tested market by market, from profiles that match each market.

Ad verification

Ads and landing pages checked exactly as users in each city and on each device type see them, to catch fraud and cloaking.

QA and localization

Prices, languages, consent banners and layouts tested per country, in environments the whole team can reuse.

Automation and AI agents

Scripts and agents given stable, isolated browser identities that they can reuse across tasks.

Privacy-minded professionals use them too: journalists, researchers and consultants who keep work, personal and research browsing in separate compartments so trackers can't join them up.

What it isn't for

An antidetect browser doesn't change what a platform allows. If a platform permits one account per person, a second profile doesn't make a second account legitimate. And no setting makes fraud, fake engagement or getting around a ban acceptable. Chapter 10 draws those lines precisely.

KEY TAKEAWAYS

- Every profile does three jobs: separate storage, one coherent fingerprint and its own proxy.
- Antidetect engines change values inside the browser, which holds up far better than extensions or scripts.
- Incognito, Chrome profiles, VPNs and virtual machines each separate only part of an identity.
- The tool is for legitimate multi-account work, always within each platform's rules.

Go deeper: How Antidetect Browsers Work · **Use case:** Multi-Account Management

02



Browser Fingerprinting, Decoded

Websites can recognize a browser without a single cookie, by reading dozens of small facts about it and combining them into a fingerprint. This chapter takes a fingerprint apart layer by layer, shows why consistency matters more than randomness, and gives you free tools to test your own.

IN THIS CHAPTER

2.1 Anatomy of a fingerprint

2.2 Canvas, WebGL and audio

2.3 The network layer and WebRTC

2.4 Consistency beats randomness

2.5 Test your own fingerprint

2.1 Anatomy of a Fingerprint

A fingerprint is the combined answer to a simple question: what kind of device and browser is this? No single answer gives you away, since millions of people run Chrome on Windows. But combine the screen, graphics card, installed fonts, timezone, language and a few dozen other values, and the combination narrows things down fast, often to a single browser. The values come from four layers.

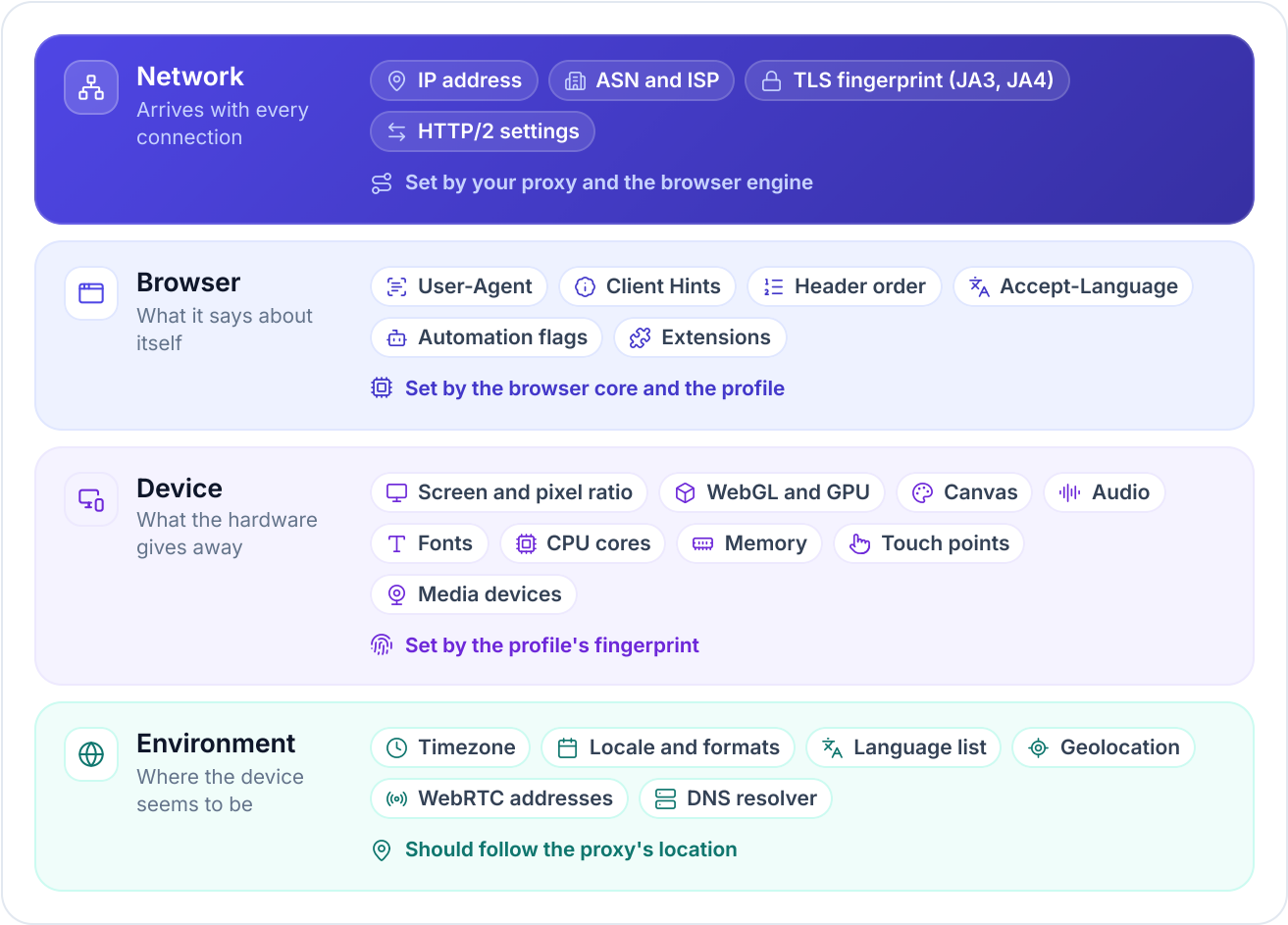


Figure 2.1 Four layers, one story. A platform can read all of them in the first second of a visit, and it checks that they agree with each other.

The layers aren't equally easy to control. Network values come from your proxy and from the engine's own networking code, so no profile setting can fix a bad IP. Device values come from real hardware, which is why good antidetect browsers build profiles from data collected on real devices instead of inventing numbers.

Think in stories, not values

A platform isn't asking whether your screen is 1920 × 1080. It's asking whether a Windows laptop with Intel graphics, US English and Central Time, connecting from a home ISP in Chicago, is a believable person. Every value you set should fit that one story.

2.2 Canvas, WebGL and Audio

The most distinctive device signals come from asking the browser to do some work and measuring the result. Graphics cards, drivers, operating systems and font renderers each produce slightly different output from identical instructions, and those differences are stable enough to recognize a device again.

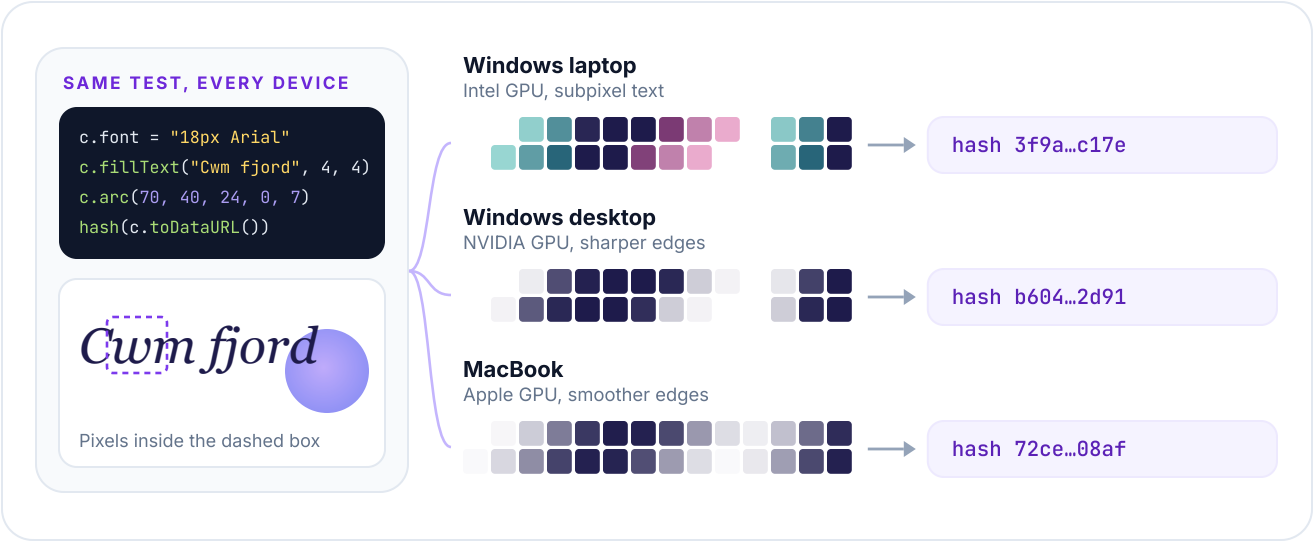


Figure 2.2 One set of canvas instructions, three devices. Differences in anti-aliasing and color handling change the pixels, and the hash of those pixels is what gets compared. Hashes are illustrative.

Canvas

A script draws hidden text and shapes, reads back the pixels and hashes them. Fonts, smoothing and the GPU all shift the result.

WebGL

Names the graphics card and driver, lists hundreds of capability limits, and renders 3D scenes whose output varies by GPU.

Audio

Generates a tone offline, runs it through audio processing and sums the samples. Tiny floating-point differences identify the stack.

Noise isn't a disguise on its own

Some tools add random noise to canvas or audio output. If the noise changes every session, the profile matches no real device and changes identity on every launch. Use a mode that keeps each profile's result stable, or values recorded from real hardware, and check that the WebGL renderer name fits the operating system the profile claims.

Go deeper: How Canvas, WebGL and AudioContext Fingerprinting Works

2.3 The Network Layer and WebRTC

Before a page runs a single script, the connection itself has already described your client. During the TLS handshake the browser lists the encryption options and extensions it supports, in its own way. Hashing that list gives a **TLS fingerprint**, known as JA3 or its successor JA4. HTTP/2 adds another: the settings and priorities a client sends when it opens a connection.

Signal	What it reveals	Who controls it
IP address and ASN	Network type (home, mobile or data center) and rough location	Your proxy
TLS fingerprint	The real client software, whatever the User-Agent claims	Browser engine
HTTP/2 settings and header order	Whether the client is a real browser or a code library	Browser engine
WebRTC	Your real public or local IP, even behind a proxy	Profile setting
DNS resolver	Which network is really doing your lookups	Proxy and engine

This is where antidetect browsers beat scripts. Each profile runs a real browser engine, so its TLS and HTTP/2 fingerprints genuinely belong to Chrome or Firefox. The engine's version still has to match what the User-Agent claims, which is one more reason to keep the browser core current. Chrome ships a new major version about every four weeks.

WebRTC: the leak that skips the proxy

WebRTC lets browsers make real-time audio and video connections. To do that, it discovers your network addresses, sometimes outside the proxy's path. Antidetect browsers give you a mode for each profile:

Mode	What a page sees	Use it when
Altered	The proxy's public IP, and no local addresses	Almost always: the default for account profiles
Disabled	No WebRTC at all	Rarely; a missing feature is unusual for a real browser
Real	Your actual addresses	Never behind a proxy

Check WebRTC in every new profile

Open My Fingerprint inside the profile. The WebRTC section should show the proxy's IP or nothing at all, never your home or office address.

Go deeper: TLS Fingerprinting · What Is a WebRTC Leak? · **Glossary:** JA3 Fingerprint

2.4 Consistency Beats Randomness

Early privacy tools randomized everything, every time. That fails for account work, because real people are boringly consistent: same laptop, same browser, same timezone, visit after visit. A profile with a new graphics card every Tuesday doesn't look private. It looks fake.

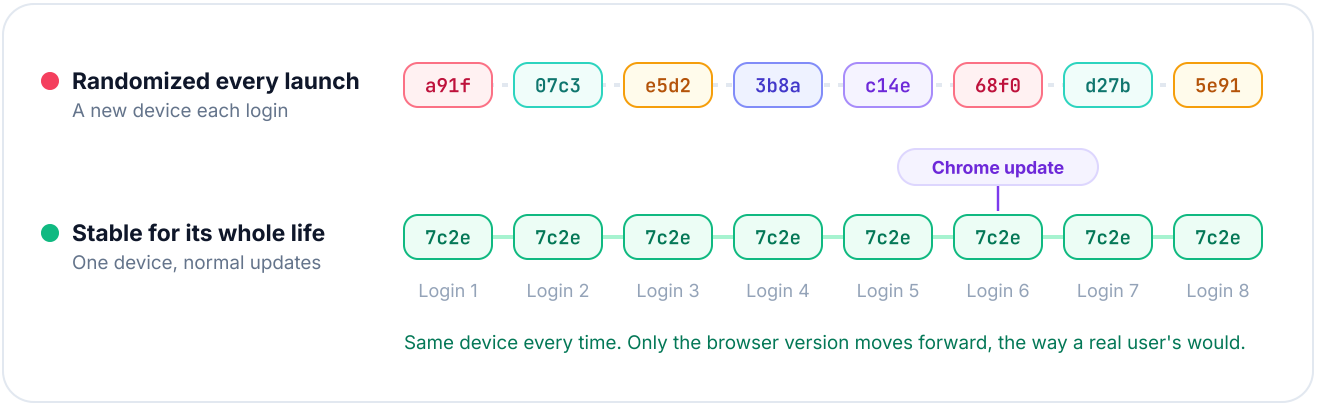


Figure 2.4 Real devices change slowly and for ordinary reasons, like a browser update. A profile should too. Fingerprint hashes are illustrative.

Mismatches that give a profile away

Mismatch	What it tells the platform	Fix
Firefox User-Agent, but Client Hints headers present	A Chromium browser in disguise; Firefox doesn't send them	Pick the engine that matches the browser you claim
German IP, US English, New York timezone	Someone hiding where they really are	Auto-match location settings to the IP
macOS User-Agent with Windows-only fonts	A spoofed operating system	Use the OS template's font set
Mobile User-Agent, desktop screen, no touch	A desktop pretending to be a phone	Use a mobile profile or a cloud phone
WebRTC shows a different IP from the proxy	A proxy user, plus their real address	Set WebRTC to altered
Same canvas hash on two "different" profiles	One device behind both accounts	A fresh fingerprint for every profile
Chrome version months behind current	A frozen or outdated identity	Keep the browser core updated

One mismatch rarely sinks an account by itself

Platforms add signals up (Chapter 3). But mismatches are the cheapest problems you'll ever fix, so clear every one before a first login.

2.5 Test Your Own Fingerprint

Don't trust a profile until you've looked at it the way a website does. Run these checks inside every new profile, and again after you change its proxy or update its browser core.

1. **Check the IP from inside the profile.** My IP should show the proxy's address and city, never yours.
2. **Look up the network.** IP Lookup shows the ASN, ISP and connection type. A residential or ISP proxy should belong to a consumer provider, not a hosting company.
3. **Read the full fingerprint.** My Fingerprint lists what the profile reveals, from User-Agent and screen to timezone, language and WebRTC. Hunt for anything that contradicts the IP.
4. **Decode the User-Agent.** Paste it into the User-Agent Parser and confirm the browser, version and operating system are the ones you intended.
5. **Compare two profiles, then restart both.** Their canvas and WebGL results should differ from each other, and each should stay identical after a restart.

My Fingerprint
Everything a profile reveals, WebRTC included.

What Is My IP
The exit IP and location a site sees.

IP Lookup
ASN, ISP, location and connection type.

User-Agent Parser
Browser, version and OS from any UA.

Test the profile, not your everyday browser

Open the tools from inside the profile you're checking. Results from your normal browser tell you about your own machine, not about the identity a platform will see.

"Unique" isn't a red flag

Fingerprint test pages often report that a browser is unique. Most real browsers are, so that alone means little. The real red flags are contradictions between layers and values that change between sessions.

KEY TAKEAWAYS

- Fingerprints span four layers: network, browser, device and environment.
- Canvas, WebGL and audio measure real hardware, so real-device data beats invented values.
- TLS and HTTP/2 fingerprints come from the engine, which must match the User-Agent.
- Consistency beats randomness: one believable identity per profile, kept stable.

Go deeper: Browser Fingerprinting Explained · Browser Fingerprint Test Tools

03



How Platforms Connect Accounts

Platforms rarely catch a multi-account setup by looking at one account. They look for links between accounts: an IP here, a payment card there, a login pattern that repeats. This chapter maps those links, explains how risk scores add up, and is honest about what an antidetect browser can and can't hide.

IN THIS CHAPTER

3.1 The linking graph
3.2 How risk scores add up
3.3 What a profile can hide, and what it can't

3.1 The Linking Graph

Think of a platform's view of your accounts as a graph. Every account is a node, and every shared detail is an edge between two of them. One edge might be coincidence, since families share Wi-Fi. A dense cluster of edges looks like one operator running many accounts, and when one of them gets restricted, the rest are judged together.

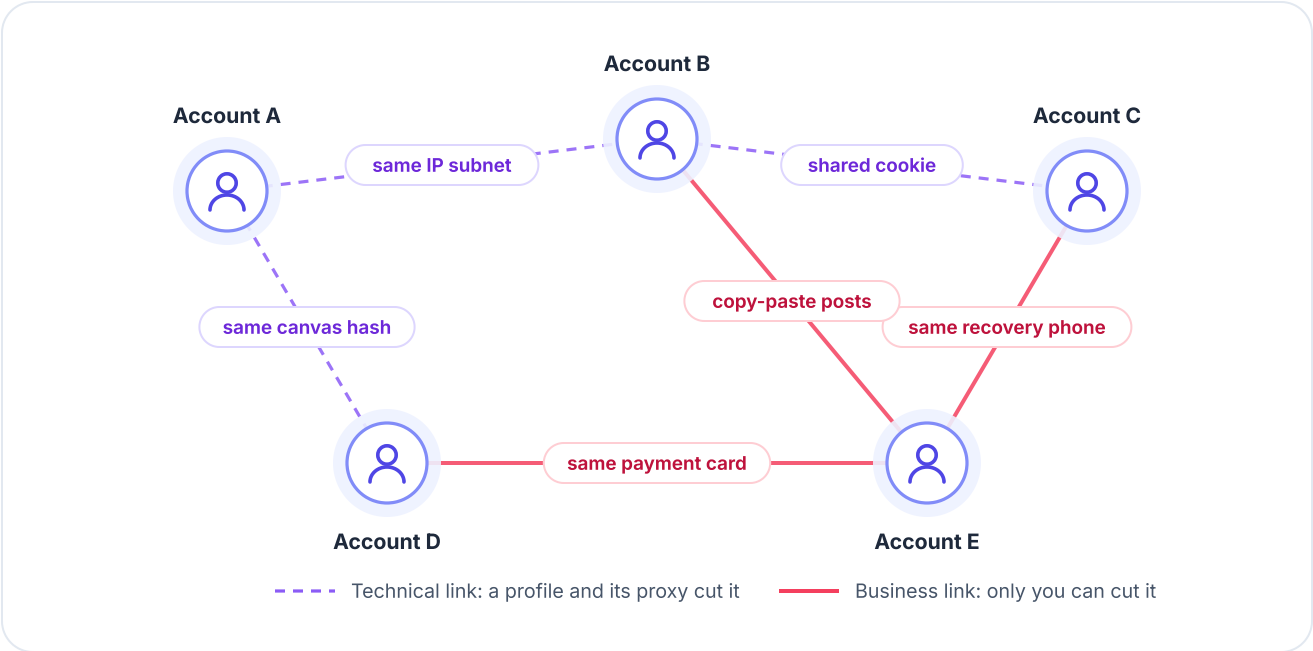


Figure 3.1 Five accounts, six links. Profiles and proxies remove the dashed links. The solid ones are created by people, and only people can remove them.

The signals platforms compare

Shared IPs and subnets
Accounts on one address, or on neighbors in the same block.

Device fingerprints
The same canvas hash, GPU and fonts behind "strangers".

Cookies and storage
An ID that survives from one account's login to the next.

Login timing
Accounts that sign in one after another, in the same order daily.

Payment methods
One card or billing address funding several ad accounts or stores.

Phones and emails
Recovery details and verification numbers reused across accounts.

Behavior and content
Identical posts, listings or creatives, and identical click paths.

Connections
The same friends, followers or contacts around every account.

3.2 How Risk Scores Add Up

Platforms keep the details private, but most large ones run risk systems that work along similar lines. Each signal nudges an account's risk score up or down, and the score decides what happens next. New accounts have little history to offset a bad signal, so their scores swing fastest.

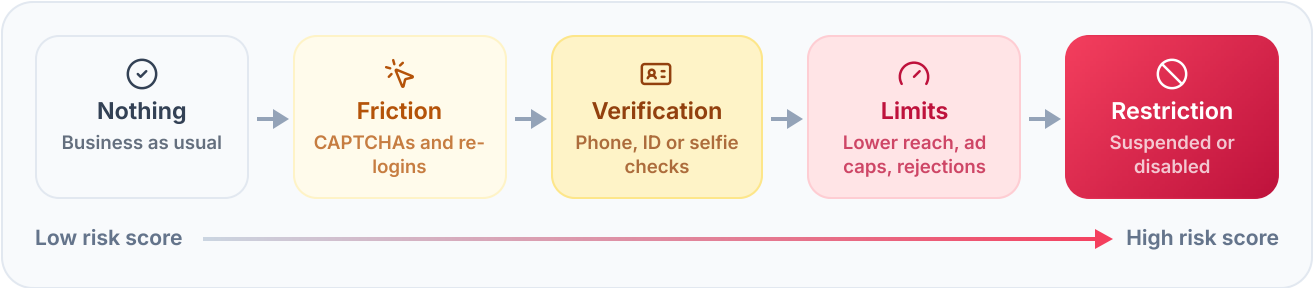


Figure 3.2 How platforms typically respond as an account's risk score climbs. Every platform draws its own lines, and many accounts move back down once the cause is fixed.

Pushes a score up

- A brand-new account doing a lot, fast
- Location signals that contradict each other
- An IP with a poor reputation or a hosting ASN
- Links to accounts that were restricted
- Many accounts on one card, phone or email
- Machine-perfect timing and repeated actions

Pulls a score down

- Account age and a steady, consistent history
- Verified email and phone that really belong to it
- The same device and location, login after login
- Genuine engagement from real people
- Normal spending and payment patterns
- Verifications completed honestly

Links are judged in context

A household with three accounts on one Wi-Fi network isn't suspicious. Thirty accounts on one IP is. Risk systems weigh how many accounts share a signal and how unusual that is, not just whether something is shared.

When one account gets flagged

1. **Pause, don't push.** Stop automation and bulk actions on that account and on anything that might be linked to it.
2. **Audit the links.** Compare its proxy, fingerprint, payment method, phone and email with your other accounts, using the table in section 3.3.
3. **Fix the cause, then appeal.** Use the platform's official review process, and keep everything else about the account unchanged while it runs.

3.3 What a Profile Can Hide, and What It Can't

An antidetect profile with its own proxy cuts the technical links: shared devices, shared storage and shared IPs. It can't cut the links you create yourself. If two profiles pay with the same card, the platform doesn't need a fingerprint to connect them.

Signal	Profile and proxy cut it?	What you have to do
IP address and subnet	Yes	Give every profile its own proxy, and never share one
Device fingerprint	Yes	Keep it stable, and never clone one profile into many
Cookies and storage	Yes	One account per profile, never two
Login timing	Partly	Don't open every account at the same time, in the same order
Payment methods	No	Separate billing per client or business, as each platform requires
Phones and emails	No	Genuine recovery details that belong to each account's owner
Behavior and content	No	Original content per account, and no copy-paste campaigns

Separation isn't a license

Keeping accounts apart is about preventing false links between accounts that are allowed to exist, such as different clients' pages. It doesn't make a banned user's new account legitimate. If a platform removed you for abuse, the honest route is its appeal process, not a new profile.

Map your own graph

List every account in a sheet with its profile, proxy IP, payment method, phone and recovery email. Any value that appears twice is an edge a platform can see too.

KEY TAKEAWAYS

- Platforms link accounts through shared signals, then judge linked accounts together.
- Risk scores rise with mismatches, sudden activity and links to restricted accounts, and fall with age and consistency.
- Profiles and proxies cut technical links. Payment, phone, email, behavior and content are on you.

Go deeper: How Social Media Platforms Detect Multiple Accounts · How Anti-Bot Systems Detect Bots

04



Choosing an Antidetect Browser

The ProxyHorizon directory lists 25 antidetect browsers, from free tools to enterprise platforms. This chapter gives you eight criteria that separate them, a side-by-side snapshot of ten widely used options, clear picks for teams, budgets, mobile work and automation, and a way to run a fair trial.

IN THIS CHAPTER

4.1 Eight criteria that matter
4.2 The directory at a glance
4.3 Picks by use case
4.4 Running a fair trial

4.1 Eight Criteria That Matter

Feature lists all look alike. These eight questions are where browsers really differ. Weight the first two most heavily: a cheap browser with a weak fingerprint costs you accounts, and lost accounts are the most expensive outcome there is.

1. Fingerprint quality and updates

Real-device fingerprints that pass the Chapter 2 tests, and a core that follows Chrome's four-week release cycle.

2. Engines

Chromium only, or Firefox and mobile engines too. Match the engine to the browser each profile claims to be.

3. Price per profile

The monthly price divided by profiles you'll actually use, plus paid seats for teammates.

4. Team features

Roles, shared profiles without shared passwords, audit logs and two-factor sign-in.

5. Automation API

A local or cloud API for Playwright, Puppeteer or Selenium. Check which plans include it.

6. Proxy integration

HTTP and SOCKS5 support, bulk import, a built-in checker and auto-matched location settings.

7. Cloud sync and security

Where profiles are stored, how they're encrypted, and what happens to your data if you leave.

8. Operating systems

Windows, macOS and Linux apps, plus Android or web access if your team needs them.

Engines named in directory listings

Browser	Engines listed	Why it matters
Multilogin	Mimic (Chromium), Stealthfox (Firefox)	Chrome and Firefox identities from one app
AdsPower	Chromium and Firefox kernels	Both major desktop browsers
GoLogin	Orbita (Chromium)	Chrome identities, plus an Android app
Kameleo	Chroma, Junglefox, Android, iOS	Desktop and mobile fingerprints
Octo Browser	Custom Chromium	A deep focus on one engine

Ask about the update lag

Ask each vendor how long its core trails a new stable Chrome release, and check the changelog. Cores that ship weeks late leave every profile looking dated.

4.2 The Directory at a Glance

Ten widely used antidetect browsers from the ProxyHorizon directory, in alphabetical order. Ratings are ProxyHorizon's community and editorial ratings out of 5. Starting prices are entry prices and change often, so check the live listing before you buy.

25
antidetect browsers in the directory

15+
listings with a free plan

$0–100
monthly entry prices

4 weeks
between Chrome major versions

Browser	Rating	From	Free plan	Systems	Known for
AdsPower	★ 4.5	$5.40/mo	5 profiles	Win, macOS, Linux	No-code RPA, local API, team roles
Dolphin Anty	★ 4.4	Free	10 profiles	Win, macOS, Linux	Built for affiliate and ad teams, automation API
GeeLark	★ 4.2	$1.99/profile	Yes	Web, Win, macOS	Real Android cloud phones, built-in RPA
GoLogin	★ 4.1	$4.50/mo	3 profiles	Win, macOS, Linux, Android	Orbita engine, cloud profiles, API
Kameleo	★ 4.3	€59/mo	Check listing	Win, macOS, Android, iOS	Mobile fingerprints, four engines, local REST API
Linken Sphere	★ 4.4	$100/mo	No	Win, macOS, Linux	Sphere 2 engine; HTTP, SOCKS5 and SSH proxies
Multilogin	★ 4.5	$19/mo	5 profiles	Win, macOS, Linux	Two engines, cloud phones, built-in proxies
Nstbrowser	★ 4.3	Free	Yes	Win, macOS, Linux	Cloud browser cluster, CDP, built-in unblocker
Octo Browser	★ 4.5	$29/mo	No	Win, macOS	Fingerprint depth, team roles, 2FA, audit logs
Undetectable	★ 4.2	$49/mo	Yes	Win, macOS, Linux	Real-device fingerprint library, local API

ProxyHorizon directory, November 2026. Alphabetical order implies no ranking. Live prices at proxyhorizon.com/antidetect-browsers; compare any two at proxyhorizon.com/compare/browsers, or answer a few questions at proxyhorizon.com/find-browser.

4.3 Picks by Use Case

There's no single best antidetect browser, but there's usually a clear best fit. Start your trial with the two or three that match your situation. Each pick below rests on the features in its directory listing.

Teams and agencies

Roles, sharing and an audit trail

- **Octo Browser** — Team roles, 2FA and audit logs — $29/mo
- **AdsPower** — Team roles and no-code RPA — $5.40/mo
- **Multilogin** — Built-in proxies on every plan — $19/mo

Pick on permissions and logs first. An agency's biggest risk is a person, not a fingerprint.

Free or budget start

Learn the workflow before you pay

- **Dolphin Anty** — Free plan with 10 profiles — Free
- **GoLogin** — Free plan with 3 profiles — $4.50/mo
- **BitBrowser** — Large free tier, RPA, local API — Free

Enough to build, test and warm up a handful of accounts before you commit to a paid plan.

Mobile and cloud phones

For app-first platforms

- **GeeLark** — Real Android cloud phones — $1.99/profile
- **Kameleo** — Android and iOS engines — €59/mo
- **Multilogin** — Cloud phones beside desktop profiles — $19/mo

If the account lives in a phone app, give it a phone, not a desktop pretending to be one.

Automation and scraping

APIs, CDP and cloud browsers

- **Nstbrowser** — Cloud browser cluster with CDP — Free
- **Kameleo** — Local REST API — €59/mo
- **Octo Browser** — Selenium, Playwright, Puppeteer — $29/mo

Confirm the API is on the plan you'll buy: Multilogin's, for example, isn't on its free plan.

Picks are a shortlist, not a ranking

They match listing features to common jobs. Your own trial, on your own platforms, decides. Prices are entry prices from the ProxyHorizon directory, November 2026.

Compare: Multilogin vs GoLogin · AdsPower vs GoLogin · AdsPower vs Multilogin

4.4 Running a Fair Trial

Most antidetect browsers offer a free plan, a trial or a cheap first month. Use it to test the things that matter, on the platforms you actually use, with the same setup in every candidate.

1. **Shortlist two or three browsers** from the picks that match your use case.
2. **Build the same three profiles in each:** same OS templates, same proxies, same locations.
3. **Run the Chapter 2 tests in every profile** and note each mismatch: IP, ASN, WebRTC, timezone, language, canvas and WebGL.
4. **Restart every profile twice** and confirm the fingerprint didn't change.
5. **Compare the core version** with the current Chrome release.
6. **Test the team features with a colleague:** share a profile, revoke access, read the audit log.
7. **If you automate, connect Playwright** through the API on the plan you'd actually buy.

PRICE PER ACTIVE PROFILE

```
(plan price + paid seats) ÷ profiles in real use
```

WORKED EXAMPLE

```
$99 plan for 100 profiles, 60 in use:
$1.65 each, not $0.99
```

The worked example uses round, hypothetical numbers to show the math. Use your own plan and headcount.

Red flags that end a trial early

- ⊗ Fingerprints that change on restart
- ⊗ No clear answer on where profiles are stored
- ⊗ The API missing from the plan you'd buy
- ⊗ A core several Chrome versions behind
- ⊗ No two-factor sign-in for the workspace
- ⊗ No way to export profiles if you leave

KEY TAKEAWAYS

- ✓ Judge browsers on fingerprint quality and core freshness first; price comes after.
- ✓ Shortlist from the directory, then trial two or three on your own platforms.
- ✓ Count price per active profile, including seats and the plan the API needs.

Go deeper: How to Choose an Anti-Detect Browser · Top Anti-Detect Browsers

05



Proxies: The Other Half of a Profile

A perfect fingerprint behind the wrong IP still gets accounts linked. This chapter covers the network side of every profile: why each one needs its own stable IP, which proxy type suits which job, how to make location settings agree with the IP, and nine networks worth testing.

IN THIS CHAPTER

5.1 One profile, one stable IP
5.2 The right proxy type for each job
5.3 Nine networks worth testing
5.4 Match the profile to its IP

5.1 One Profile, One Stable IP

Real people don't change countries between clicks. A home IP stays the same for days or weeks, and when it changes, it usually moves to another address from the same provider in the same area. An account that signs in from a new address on every visit looks like it's being passed around, which is exactly what an account takeover looks like.

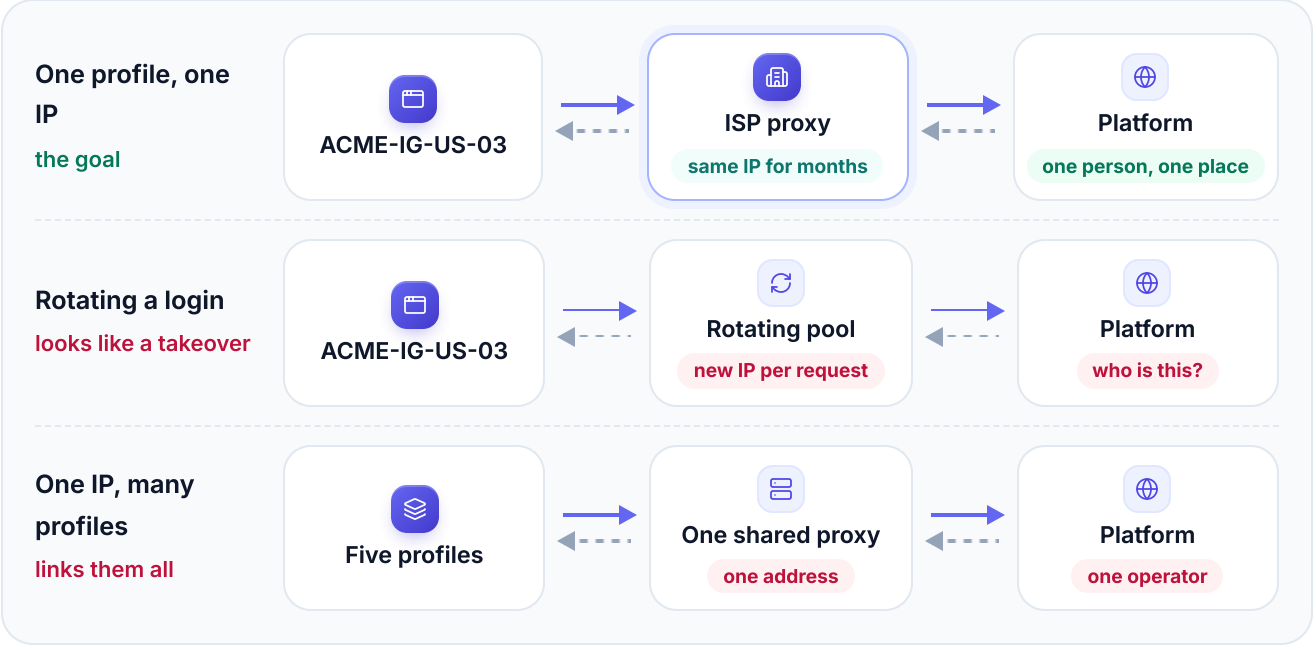


Figure 5.1 The IP is half of a profile's identity. Keep it stable and keep it private to one profile, or the best fingerprint in the world won't help.

Two rules follow: never share a proxy between profiles, and never rotate the IP of a logged-in account. If a proxy dies, replace it with one of the same type in the same city, and expect the platform to notice, the way it notices a user who switches internet providers.

Sticky sessions for accounts

Residential and mobile proxies usually come through a gateway that hands out a new IP per connection unless you ask it to hold one, which is called a sticky session. Lengths vary by provider, from minutes to many hours. For accounts, prefer a static ISP or dedicated mobile IP. If you use residential, take the longest stable session on offer, pin it to one city and reuse the same session ID for that profile.

Rotation is for scraping, not accounts

Rotating residential proxies are perfect for collecting public pages, where every request stands alone. For anything you log into, stability wins.

5.2 The Right Proxy Type for Each Job

Each proxy type borrows its trust from a different kind of network and suits a different kind of account. Higher rungs look more like ordinary users and cost more, so match the rung to the job.

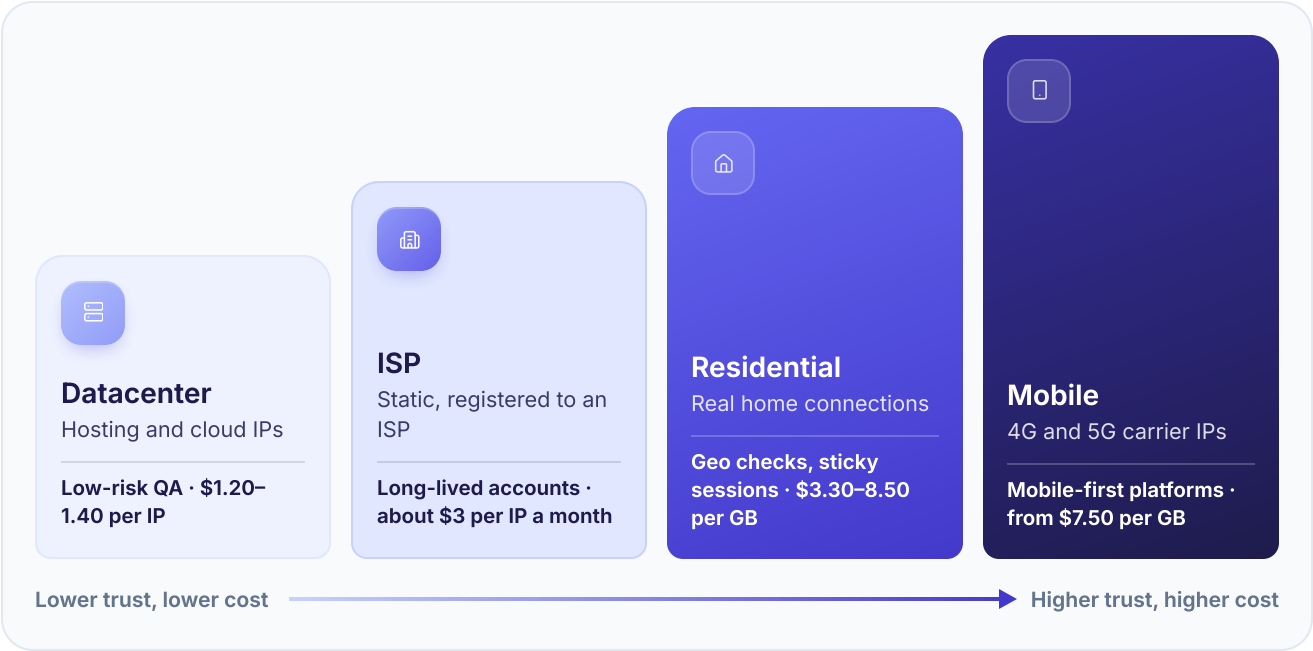


Figure 5.2 Four rungs, four jobs. Entry prices are ranges across the nine providers in section 5.3, from the ProxyHorizon directory, November 2026.

Job	Proxy type	Session	Why
Client social accounts	ISP or dedicated mobile	Static, one per account	Months on one clean IP
Store and marketplace accounts	ISP	Static, in the store's country	Stability beats variety
Mobile-first platforms	Mobile	Dedicated or long sticky	Carrier IPs are what apps expect
Ad and landing-page checks	Residential, some mobile	Short sticky per check	Many places, real-user views
QA and localization	Datacenter, then residential	Sticky per test run	Cheap where sites don't mind
Public web scraping	Datacenter or residential	Rotating	No login to protect

Why mobile IPs are trusted, and shared

Carriers put many subscribers behind each public IP, so blocking one hits real customers. That's why mobile IPs are trusted, and why their history is partly other people's.

5.3 Nine Networks Worth Testing

A neutral shortlist from the ProxyHorizon directory, in alphabetical order. For account work, look first at ISP, mobile and long sticky-session options. For checks and scraping, pool depth in your locations matters more.

Bright Data

Enterprise web data platform: every proxy type, plus scraper APIs and datasets.

Residential · ISP · Datacenter · Mobile

RESIDENTIAL POOL	RESIDENTIAL FROM
72M+	$5.04/GB

Decodo

Formerly Smartproxy. An easy dashboard and broad coverage across every type.

Residential · ISP · Datacenter · Mobile

RESIDENTIAL POOL	MOBILE FROM
115M+	$8/GB

Geonode

Developer-friendly residential proxies with unlimited-bandwidth plans.

Residential

RESIDENTIAL POOL	RESIDENTIAL FROM
30M+	$4/GB

IPRoyal

Residential traffic that never expires, plus ISP and mobile options.

Residential · ISP · Datacenter · Mobile

RESIDENTIAL POOL	RESIDENTIAL FROM
32M+	$7/GB

NodeMaven

Quality-filtered IPs and long sticky sessions, a natural fit for profiles.

Residential · Mobile

RESIDENTIAL POOL	RESIDENTIAL FROM
30M+	$3.50/GB

Oxylabs

Premium enterprise network across every type, plus scraper APIs.

Residential · ISP · Datacenter · Mobile

RESIDENTIAL POOL	RESIDENTIAL FROM
100M+	$8/GB

PYProxy

SOCKS5 per-IP pricing, static ISP proxies and an unlimited daily plan.

Residential · ISP · Datacenter

RESIDENTIAL POOL	ISP FROM
90M+	$3/IP

SOAX

Clean pools with city and ISP-level targeting, residential and mobile.

Residential · Mobile

RESIDENTIAL POOL	MOBILE FROM
155M+	$8.50/GB

Webshare

Affordable self-serve datacenter plans for low-risk QA, plus residential.

Datacenter · Residential

DATACENTER POOL	DATACENTER FROM
400K+	$2.99/mo

Product types, pools and entry prices from the ProxyHorizon directory, November 2026. Alphabetical; no ranking implied. Live numbers at proxyhorizon.com/proxies.

5.4 Match the Profile to Its IP

An IP carries a location, and every location setting in the profile has to agree with it. Most antidetect browsers fill these in from the proxy automatically. Let them, then check the result, because auto-detection is only as good as the IP database behind it.

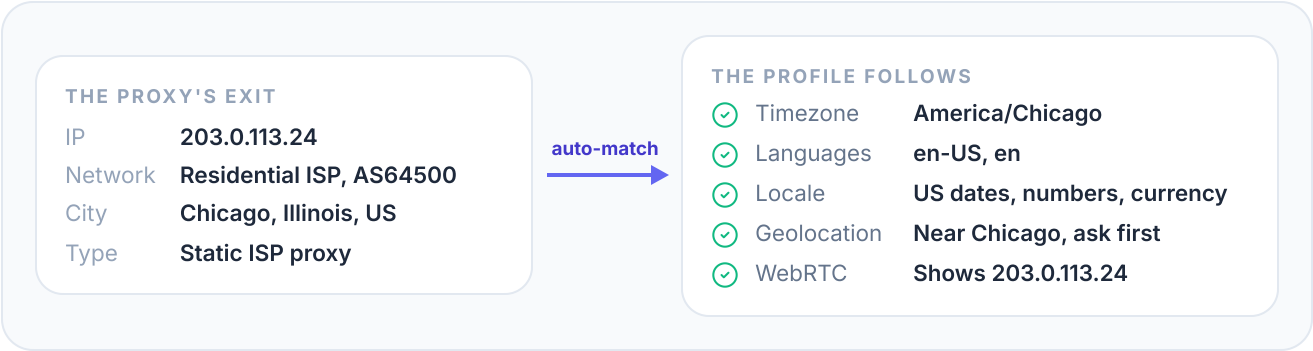


Figure 5.3 Five settings, one location. If any of them points somewhere else, the profile tells two stories at once.

HTTP or SOCKS5?

Both work for browsing in every major antidetect browser, so use what your provider recommends.

Protocol	Carries	Typical format	Use it when
HTTP(S) proxy	Web traffic, HTTPS tunneled	`http://user:pass@host:port`	The default for profiles
SOCKS5	Any TCP connection, UDP if supported	`socks5://user:pass@host:port`	A tool needs more than web traffic
SSH tunnel	TCP through a server you control	`user@host` plus a key	Your own servers, where supported

Convert proxy lists in seconds

Bulk importers each want their own format. The free Proxy Format Converter switches between them, and Proxy Checker tests each proxy first.

KEY TAKEAWAYS

- One profile, one stable IP. Never share proxies or rotate a logged-in account.
- ISP for long-lived accounts, mobile for app-first platforms, residential for checks, datacenter for low-risk QA.
- Let the profile follow the IP: timezone, languages, locale, geolocation and WebRTC.

Go deeper: Proxies With an Antidetect Browser · Sticky vs Rotating Sessions

06



Building Profiles That Hold Up

A profile is a promise to keep the same identity for the life of an account. This chapter walks through building one step by step, naming and organizing hundreds of them, moving existing accounts in safely, and checking every profile before anyone logs in.

IN THIS CHAPTER

6.1 Build a profile, step by step

6.2 Names, cookies and extensions

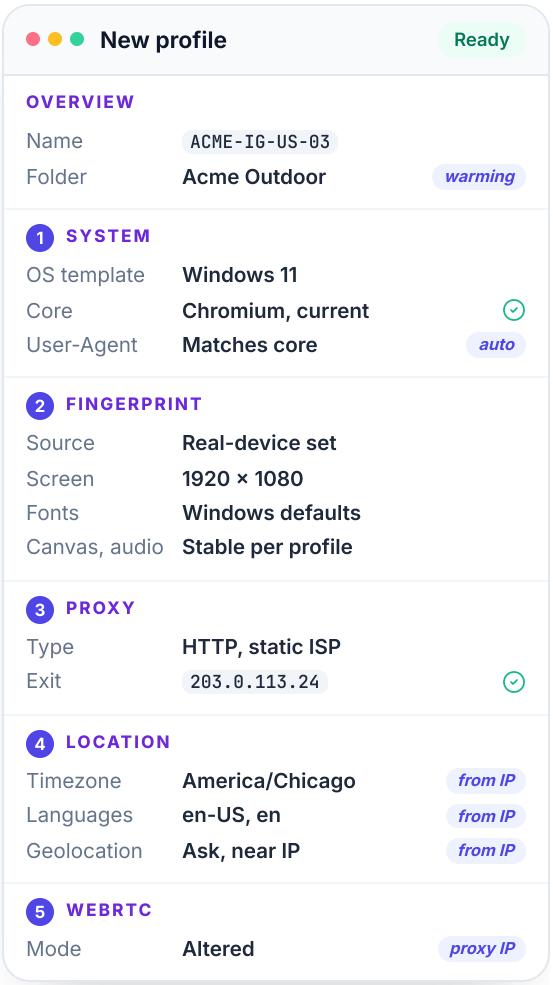
6.3 Verify before the first login

6.4 Common mistakes and fixes

6.1 Build a Profile, Step by Step

Every antidetect browser lays out its "new profile" screen differently, but the decisions are the same. Make them in this order: the system decides the fingerprint, and the proxy decides the location.

1. **Pick the OS template.** Choose the system the account's owner would plausibly use, and keep it for life.
2. **Generate the fingerprint from real-device data.** Let the browser pick a matching screen, GPU, fonts and hardware. Don't hand-edit single values.
3. **Attach the proxy.** Paste it in, run the built-in check and confirm the exit city.
4. **Let location follow the IP.** Timezone, languages, locale and geolocation all come from the proxy.
5. **Set WebRTC to altered,** so it reports the proxy's IP and nothing else.
6. **Keep fonts and screen realistic:** the template's font set and a common resolution for that system.
7. **Name, tag and save,** then run the checks in section 6.3 before anyone logs in.



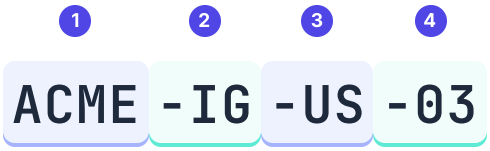
Save the recipe, not the fingerprint

Once a profile passes every check, save its settings as a template for the next account of the same kind. Each new profile still gets its own unique fingerprint; only the recipe repeats.

Account type	OS template	Proxy	Watch for
Desktop social or ad account	Windows or macOS	Static ISP	Owner's real location
Mobile-first app account	Android cloud phone	Mobile	Touch, screen, carrier agree
Marketplace seller account	Seller's usual OS	Static ISP	One country for life
QA or test persona	Per test case	Datacenter or residential	Reset between runs

6.2 Names, Cookies and Extensions

At ten profiles you remember which is which. At two hundred you won't. A naming convention makes every profile findable, and it prevents the costliest slip in multi-account work: opening the right account in the wrong profile.



1. **Client or brand.** Who the account belongs to, so folders and billing line up.
2. **Platform.** A short code: IG, FB, TT, AMZ, LI.
3. **Market.** The proxy's country, which never changes for this profile.
4. **Sequence.** Two digits, never reused after a profile is retired.

Figure 6.2 One name, four facts. Anyone on the team can tell who owns the account, where it lives and which platform it's for before they click.

Moving an existing account in

An established account moved into a new profile meets the platform as a new device either way. Importing that account's own cookies, exported from the browser it uses today, lets the profile continue the session instead of starting cold. Most antidetect browsers accept cookies in JSON or Netscape text format. Build the profile with a proxy in the account's usual city, import, confirm you're signed in, and complete any verification the platform asks for. From then on, the account lives only in that profile.

Only your own cookies

Import cookies only for accounts you own or manage with permission. Session cookies are logins: using someone else's is account takeover, and cookie bundles sold online tie your profile to strangers and whatever they did.

Extensions: fewer is safer

Reasonable in a profile

- Your team's password manager
- A tool the account's owner really uses
- Installed only from the official store

Keep out of profiles

- VPN or proxy extensions that fight the profile
- "Spoofer" add-ons that contradict the engine
- One identical extension set on every profile

6.3 Verify Before the First Login

A profile that leaks on its first login can link an account before it has done anything. Run this check inside every new profile, fix every failed line before anyone signs in, and run it again after any proxy, core or machine change.

- [ ] Exit IP is the proxy's, in the expected city
- [ ] Timezone matches the IP's location
- [ ] WebRTC shows the proxy IP, or nothing
- [ ] User-Agent matches the core version and OS
- [ ] Fonts match the OS template
- [ ] Fingerprint unchanged after a restart
- [ ] Name, folder, tags and notes filled in
- [ ] ASN matches the proxy type you paid for
- [ ] Languages and Accept-Language fit the market
- [ ] Geolocation is near the IP, or set to ask
- [ ] Screen size is common for that system
- [ ] Canvas and WebGL differ from other profiles
- [ ] No extensions the account doesn't need
- [ ] Credentials in the password manager, not notes

Profile check: ACME-IG-US-03		7 of 8 passed
IP and city	203.0.113.24, Chicago, US	Pass
Network	AS64500, residential ISP	Pass
Timezone	America/Chicago	Pass
Languages	en-US, en	Pass
WebRTC	Shows 203.0.113.24 only	Pass
Canvas	Unique among the team's 48 profiles	Pass
Fonts	Two macOS-only fonts on a Windows template	Fix
Restart	Same fingerprint after two restarts	Pass

Figure 6.3 An example check log. One failed line is enough to hold the first login until it's fixed.

What goes in the profile notes

- The account's owner and purpose, and who on the team runs it
- Proxy provider, IP and city, and the date they were assigned
- Where the login and 2FA details live in the password manager, never the details themselves
- Warm-up start date and the current status tag
- Every verification, restriction or appeal, with its date

Free tools: My Fingerprint · IP Lookup · User-Agent Parser

6.4 Common Mistakes and Fixes

Almost every linked or restricted account traces back to one of these. They're all cheap to avoid and expensive to discover after the fact.

Mistake	Why it hurts	Fix
One proxy shared by several profiles	Links every account on it at the network layer	One dedicated proxy per profile
Rotating IPs on a logged-in account	Looks like an account takeover	Static ISP or the longest sticky session
New random fingerprint every launch	A device that changes identity daily	One stable fingerprint for the profile's life
Cloning one profile for many accounts	Identical canvas and WebGL hashes	A fresh fingerprint for each profile
Two accounts in one profile	Shared cookies link them instantly	One account per profile, always
Moving a profile to another country	An impossible journey overnight	Keep the proxy's country for life
Timezone left on your real location	Location signals contradict each other	Let location settings follow the IP
Signing in "just once" from your phone	Your real device and IP join the account's history	Use the profile, or a paired cloud phone
Full activity on day one	New accounts with heavy activity score as risky	Warm up over three to four weeks (Chapter 7)
Free or public proxies	Inherited abuse history, and traffic others can read	A reputable paid provider (section 5.3)

KEY TAKEAWAYS

- Build in order: system, real-device fingerprint, proxy, then location settings that follow the IP.
- Name, tag and document every profile; keep credentials in a password manager.
- Import cookies only for accounts you own, and keep extensions to a minimum.
- Check every profile before its first login, and keep the result in its notes.

Go deeper: Antidetect Browser Mistakes Beginners Make · **Glossary:** Browser Profile

07



Warm-Up, Behavior and Account Health

A new account has no history, so platforms watch it closely. Warming up simply means using a new account the way a real new user would, and letting trust build before you ask it to do heavy lifting. Here's a four-week plan, the habits that keep accounts healthy, and what to do when one isn't.

IN THIS CHAPTER

7.1 How accounts build trust

7.2 A four-week warm-up

7.3 Reading health signals

7.1 How Accounts Build Trust

Every account starts at zero: no history, no network of real connections and no record of signing in from the same place. Platforms fill that gap with caution, which means lower limits, more checks and less benefit of the doubt. Trust grows with time and consistent use, and activity that outruns it draws attention.



Figure 7.1 A conceptual picture, not a platform formula. What an account can safely do grows with its history; a sudden burst on day one overshoots that and invites verification checks.

Habits that keep accounts healthy

Same profile, every session
Never open the account anywhere else, including your own phone "just once".

A steady routine
Sign in at similar local times. Real people have routines, and so should accounts.

Human pace
No bursts of identical actions. Spread the work through the session as a person would.

Original content
Write for each account. Duplicated posts, listings or ad copy link accounts together.

Clean session endings
Close profiles properly so they save, and never run one profile on two machines at once.

Official tools first
Use the platform's business suites, partner access and APIs wherever it offers them.

7.2 A Four-Week Warm-Up

This is a general pattern, not a magic formula. Adjust it to each platform's rules and to what a real user of that account would do. The point is honest, ordinary use that builds history, never tricks that fake it.

Week 1

Settle in

Sign in only from the account's profile. Complete the profile honestly, confirm the email and phone, and browse like a new user: read, follow a few relevant accounts, save a post or two. No ads and no bulk actions.

CHAPTERS 5 AND 6

Week 2

Start taking part

Post original content at a modest pace and reply to real comments. Keep sessions at similar times of day, from the same profile and IP.

SECTION 7.1 HABITS

Week 3

Build a normal rhythm

Raise activity gradually toward the account's intended level. Connect the business tools the platform offers, such as its business suite or an ad account, through official channels.

CHAPTER 8 FOR TEAM ACCESS

Week 4

Go to work, carefully

Begin regular operations. For ads, start with modest budgets and policy-compliant creatives, and raise spend in steps while results and account health hold steady.

CHAPTER 10 PLAYBOOKS

Never part of a warm-up

- Bought followers, likes, reviews or engagement
- Mass following and unfollowing
- Automated likes, follows or comments
- Trading fake interactions between your own accounts

Established accounts need continuity, not a warm-up

When you move an existing account into a profile, keep its country and its routine, and expect one verification prompt as the platform meets the new device. Complete it honestly, then change nothing else for a while.

7.3 Reading Health Signals

Accounts rarely go from fine to banned without warning. They send signals first, and the right response is almost always to slow down and fix the cause, not to push through.

Signal	What it usually means	How to respond
CAPTCHAs on every login	The session looks automated, or the IP has a poor reputation	Check the proxy and fingerprint; slow down
Phone or email verification	The platform saw a new device or location	Complete it honestly, then keep device and IP stable
Identity or selfie check	A higher risk score, often from links to other accounts	Complete it if the account is genuinely yours; audit the links
Reach or impressions drop	Content or behavior looks spammy	Pause automation and repeats; post original work
Ad rejections or spend limits	A policy problem, or a new ad account with little history	Fix the ad, then use the official review
"Try again later" action blocks	Too many actions, too fast	Stop that action for a day or more; lower the pace
Several accounts flagged at once	They're linked by something shared	Audit proxies, fingerprints, payment and recovery details
Restricted or disabled	A serious or repeated violation	Appeal officially; never open a replacement to get around it

Never "fix" a restriction with a new account

When a platform restricts an account, the legitimate paths are its appeal process or accepting the decision. Creating a new account to get around enforcement breaks almost every platform's terms, and this handbook won't help you do it.

KEY TAKEAWAYS

- New accounts start with no trust; let activity grow with the account's history.
- Warm up over three to four weeks with honest, ordinary use, then raise activity in steps.
- Treat verifications and limits as signals: slow down, fix the cause, appeal officially.

Go deeper: How to Warm Up Accounts in an Antidetect Browser · How to Run Multiple Instagram Accounts

08



Running a Team on Profiles

The moment a second person touches your profiles, you have a security question and a consistency question. This chapter covers roles and permissions, sharing access without sharing passwords, the folders and procedures that keep a team consistent, and clean handovers when people move on.

IN THIS CHAPTER

8.1 Roles and permissions
8.2 Share profiles, not passwords
8.3 Folders, tags and SOPs
8.4 Handover and offboarding

8.1 Roles and Permissions

Give every person the least access their job needs. Team-ready antidetect browsers let you define roles; the names vary from tool to tool, but the pattern below works almost everywhere.

Permission	Owner	Admin	Team lead	Operator
Billing and plan	✓	—	—	—
Invite and remove members	✓	✓	—	—
Create and delete profiles	✓	✓	Own folders	—
Edit fingerprint and proxy	✓	✓	—	—
Open assigned profiles	✓	✓	✓	✓
Export cookies or profiles	✓	✓	—	—
Read the audit log	✓	✓	Own team	—
Manage API keys	✓	✓	—	—

A sample agency team

Take an agency running 40 client profiles. One owner handles billing. Two admins build profiles, buy proxies and hold the API keys. Each client lead manages their own client's folder. Operators post and reply in the profiles assigned to them, and never see a fingerprint setting or a password.

Separate the builders from the users

The people who build profiles and assign proxies shouldn't be the people who use them all day. Settings stay stable, and mistakes get caught before a login instead of after one.

Two-factor sign-in and audit logs

Turn on two-factor sign-in for every workspace member, and read the audit log weekly: who opened which profile, when and from where. Octo Browser's directory listing, for example, highlights 2FA and audit logs.

Use the platform's own team tools too

Many platforms offer multi-user access of their own: business suites for social pages, manager accounts for ads, user permissions in seller dashboards. Use them alongside profiles. They give each teammate a login the platform recognizes, with permissions it can enforce.

8.2 Share Profiles, Not Passwords

The old way to share an account was to paste its password into a chat. The antidetect way is to share the profile: a teammate opens it, the session is already signed in, and they never see the password at all. Some tools go further: VMLogin's directory listing highlights password-hidden profile sharing.



Figure 8.2 Access moves with the profile, not with the password. Revoke the operator's access and nothing about the account has to change.

Where credentials should live

- **A team password manager** with a vault per client, so access follows the client, not the person.
- **Two-factor seeds** stored in that manager or on a business-owned device, never on one employee's personal phone.
- **Recovery emails and phone numbers** that belong to the client or the business, not to a member of staff.

One profile, one person at a time

Two people opening the same profile at once can corrupt its saved session, and to the platform it looks like two devices on one account. Check that nobody else has a profile open before you launch it, and close it properly when you finish.

Profile access is account access

Anyone who can open a profile can act as that account. Treat profile sharing like handing over keys: assign it per person, review it monthly and revoke it the day someone's role changes.

Clients and contractors

Give outsiders the narrowest access that works: a role in the platform's own business tools, or one shared profile with editing and export turned off. Never hand a contractor the whole workspace, and set an end date on their access the day you grant it.

8.3 Folders, Tags and SOPs

Consistency is what keeps accounts healthy, and teams are where consistency breaks. A predictable structure and a written procedure for each kind of account put it back.

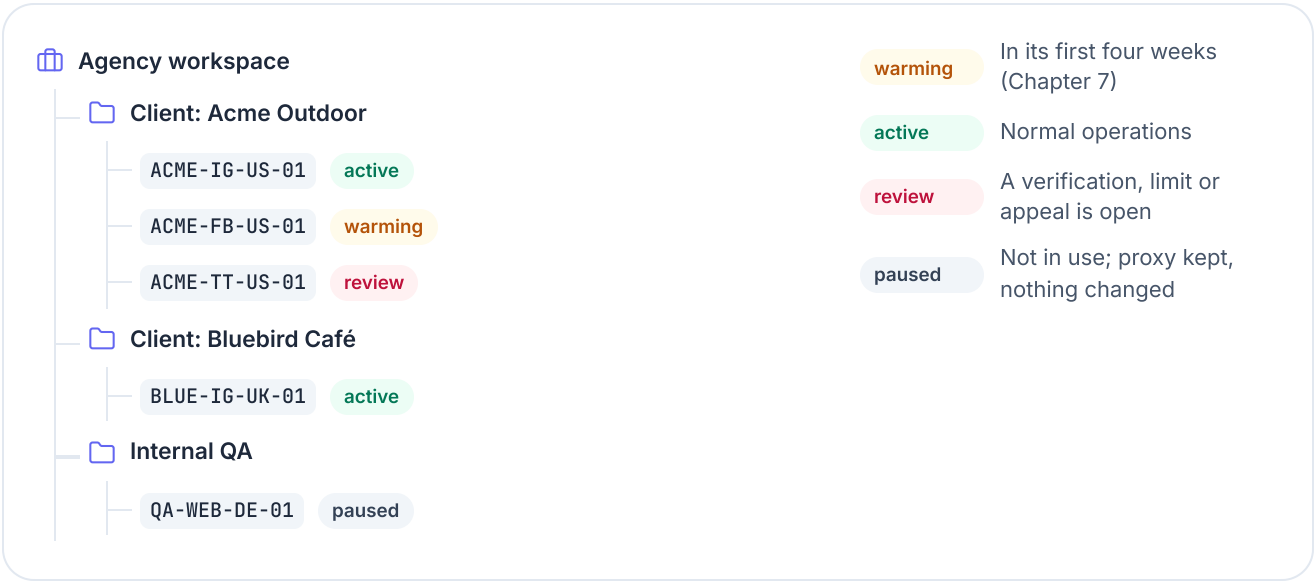


Figure 8.3 One folder per client and one status tag per profile. Filter by "review" every morning and you have a health board in seconds.

A one-page SOP for every account type

PURPOSE AND OWNER
Why the account exists and who is accountable for it

DAILY ROUTINE
Sign-in window, tasks and the limits per session

ESCALATION
Who to tell when a verification or restriction appears

SETUP
Profile template, proxy type and the market it lives in

NEVER IN THIS PROFILE
Other accounts, personal browsing, new extensions

HANDOVER NOTES
Anything the next person needs on day one

Example: a client Instagram account

PURPOSE AND OWNER
Organic posts and replies for Acme Outdoor's US page; owned by the Acme lead

DAILY ROUTINE
One session, 9 to 11 a.m. Central: post from the approved calendar, reply to comments

ESCALATION
Any verification prompt or reach drop goes to the Acme lead the same day

SETUP
Windows 11 template, static ISP proxy in Chicago, profile `ACME-IG-US-01`

NEVER IN THIS PROFILE
Other Acme accounts, personal browsing, new extensions, automation

HANDOVER NOTES
Calendar link, brand voice guide and the last 30 days of issues

8.4 Handover and Offboarding

People change roles and leave. Plan for it on day one, and a departure takes an afternoon instead of turning into a crisis. Share the routine duties out so nothing depends on one person's memory.

Task	Who	How often
Read the audit log	Admin	Weekly
Check status tags and health signals	Team lead	Daily
Re-test proxies and fingerprints	Admin	Monthly, and after any change
Update browser cores	Admin	When the vendor ships one
Review who can open which profiles	Owner	Monthly
Rotate shared credentials	Owner	Quarterly, and on every departure
Re-read each platform's terms	Team lead	Quarterly

Handing over

- [ ] Reassign the person's profiles and folders
- [ ] Walk the new owner through each SOP and its notes
- [ ] Confirm each profile opens without a new sign-in
- [ ] Record the change, with the date, in each profile's notes

Offboarding

- [ ] Remove them from the antidetect workspace
- [ ] Revoke their password-manager vaults
- [ ] Rotate passwords and 2FA they could reach
- [ ] Rotate proxy credentials and API keys they used
- [ ] Read their last 30 days in the audit log

KEY TAKEAWAYS

- Give each role the least access it needs, and separate profile builders from daily users.
- Share profiles, not passwords; keep credentials and 2FA in business-owned vaults.
- Folders, status tags and one-page SOPs keep a team consistent.
- Offboard in an afternoon: revoke, rotate, then read the audit log.

Go deeper: Antidetect Browser Team Management

09



Automation, APIs and AI Agents

Most serious antidetect browsers can be driven from code, and the pattern is the same everywhere: start a profile through a local API, get a debugging address back, and attach Playwright, Puppeteer or Selenium to it. This chapter shows that pattern, the habits that keep automated accounts safe, and where AI agents fit.

IN THIS CHAPTER

9.1 How local APIs work

9.2 Python and Playwright

9.3 Node.js and Selenium

9.4 Safe automation patterns

9.5 RPA builders and AI agents

9.1 How Local APIs Work

When an antidetect app is running, it usually also runs a small web server on your own machine, on `127.0.0.1`. Your script asks it to start a profile. The app launches that profile's browser with its fingerprint and proxy, then returns an address where your automation library can take control through the Chrome DevTools Protocol (CDP).

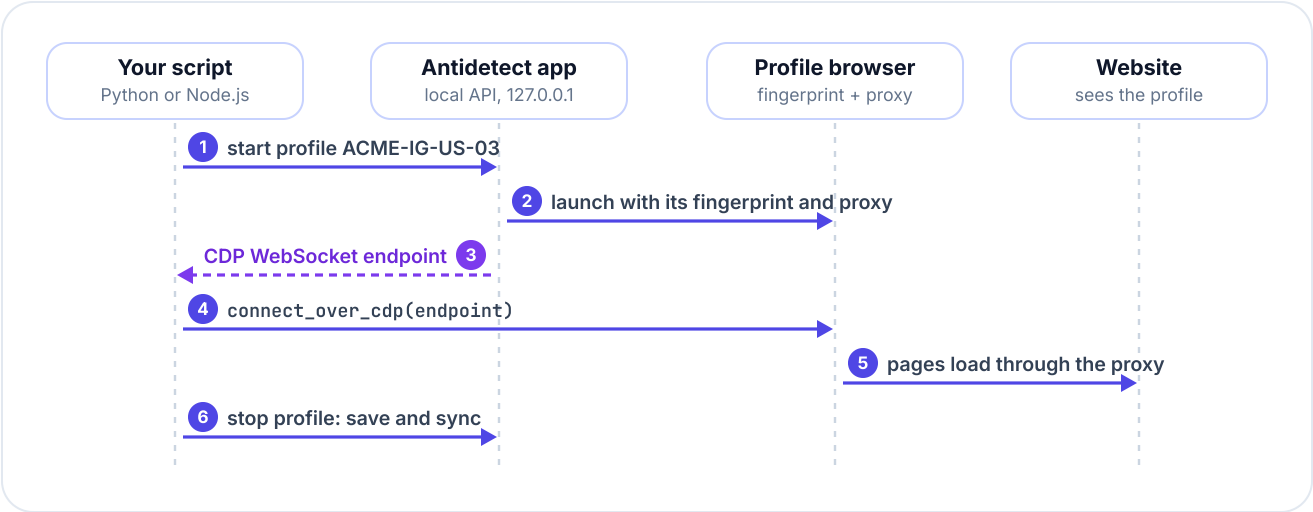


Figure 9.1 Six steps, any vendor. Only step 1 and step 6 are vendor-specific; everything in between is standard CDP.

1. **Start.** Call the local API with the profile's ID. The app opens the browser with the profile's own fingerprint, proxy and cookies.
2. **Connect.** Read the WebSocket endpoint from the response and attach your library to it over CDP.
3. **Work in the existing context.** The profile's cookies and settings live there.
4. **Stop through the API,** not by killing the process, so the app saves and syncs the profile.

> ⚠ **Every vendor's API is different**
>
> Ports, paths, parameters, response fields and authentication differ between browsers, and some plans don't include the API. This chapter's code uses marked placeholders; take the real values from your vendor's docs.

What to look for in your vendor's docs

Item	What you need from it
Start call	The profile ID it expects, and where the response puts the WebSocket endpoint or debug port
Stop call	How to close a profile so it saves and syncs
Access and limits	Any key the API needs, which plans include it, and how many profiles can run at once

9.2 Python and Playwright

Here's the whole pattern in Python. The two helpers marked as placeholders stand in for your vendor's start and stop calls; everything after them is standard Playwright, including a check that stops the run when a person needs to step in.

Python · Playwright over CDP (placeholder API)

```python
import requests
from playwright.sync_api import sync_playwright

# PLACEHOLDER API. Every antidetect browser has its own local API: replace the
# port, paths, parameters and response fields with the ones in your vendor's docs.
LOCAL_API = "http://127.0.0.1:PORT"

def start_profile(profile_id):
    """Launch a profile and return its CDP WebSocket endpoint."""
    r = requests.get(f"{LOCAL_API}/placeholder/start",
                     params={"profile": profile_id}, timeout=120)
    r.raise_for_status()
    return r.json()["ws_endpoint"]            # placeholder field name

def stop_profile(profile_id):
    requests.get(f"{LOCAL_API}/placeholder/stop",
                 params={"profile": profile_id}, timeout=60)

def needs_human(page):                        # CAPTCHA or verification: stop
    text = page.inner_text("body").lower()
    return any(w in text for w in ("captcha", "verify", "unusual activity"))

profile = "ACME-IG-US-03"
ws = start_profile(profile)
try:
    with sync_playwright() as p:
        browser = p.chromium.connect_over_cdp(ws)
        context = browser.contexts[0]         # the profile's own context and cookies
        page = context.pages[0] if context.pages else context.new_page()
        page.goto("https://example.com/dashboard")
        if needs_human(page):
            raise RuntimeError(f"{profile} needs a human")
        print(page.title())
finally:
    stop_profile(profile)                     # let the app save and sync the profile
```

Use `browser.contexts[0]`, not `new_context()`

A new context starts empty, without the profile's cookies, and may skip its proxy and settings. The existing context is the profile.

9.3 Node.js and Selenium

In Node.js, Puppeteer attaches with `puppeteer.connect()`, and Playwright with `chromium.connectOverCDP()`. Pass `defaultViewport: null` to Puppeteer, or it resizes every page to 800 × 600 and contradicts the profile's screen.

Node.js · Puppeteer (placeholder API)

```
import puppeteer from 'puppeteer-core';

// PLACEHOLDER API: swap in your vendor's real port, path and response field.
const LOCAL_API = 'http://127.0.0.1:PORT';
const id = 'ACME-IG-US-03';

const res = await fetch(`${LOCAL_API}/placeholder/start?profile=${encodeURIComponent(id)}`);
if (!res.ok) throw new Error(`start failed: ${res.status}`);
const { ws_endpoint } = await res.json();               // placeholder field name

const browser = await puppeteer.connect({
  browserWSEndpoint: ws_endpoint,
  defaultViewport: null,                                // keep the profile's own screen size
});
const page = (await browser.pages())[0] ?? (await browser.newPage());
await page.goto('https://example.com/dashboard');
console.log(await page.title());

await browser.disconnect();                             // leave the browser to the app
await fetch(`${LOCAL_API}/placeholder/stop?profile=${encodeURIComponent(id)}`);
```

Selenium attaches through a debugger address instead of a WebSocket. Most vendors return one from the start call and ship a chromedriver that matches the profile's browser core.

Python · Selenium (placeholder values)

```
from selenium import webdriver
from selenium.webdriver.chrome.service import Service

options = webdriver.ChromeOptions()
options.debugger_address = "127.0.0.1:DEBUG_PORT"      # from your vendor's start response
service = Service("/path/to/matching/chromedriver")    # must match the profile's core
driver = webdriver.Chrome(service=service, options=options)
driver.get("https://example.com/dashboard")
```

Connect to the profile as it is

Launch flags, viewport emulation, custom user agents and "stealth" plugins all change what the profile reports. Attach, use what's there, and let the antidetect browser own the fingerprint.

9.4 Safe Automation Patterns

Automation multiplies whatever you do, good habits and bad ones. These patterns keep automated profiles looking like what they should be: people doing ordinary work at an ordinary pace.

Pattern	Why it matters	How
One session per account	Two sessions at once look like two devices	A lock per profile ID in your job queue
Human pacing	Perfectly even timing is a script signature	Random waits in realistic ranges; no bursts
The profile as it is	Overrides contradict the fingerprint	Existing context; no custom UA or viewport
Hard limits	A runaway loop can burn an account fast	Caps on actions, pages and minutes per run
Stop on friction	CAPTCHAs and checks are warnings	Pause the account and alert a person
Log every run	You can't fix what you can't see	Profile, start, stop, actions and outcome
Official APIs first	Many platforms restrict automation on accounts	Use the platform's API wherever one exists

One log line per automated run

```
{"ts": "2026-11-21T09:14:03Z", "profile": "ACME-IG-US-03", "task": "reply-to-comments",
 "actions": 12, "minutes": 9, "friction": false, "outcome": "ok", "operator": "script-v3"}
```

Python · human pacing between actions

```python
import random, time

def human_pause(low=1.5, high=6.0):
    """Wait a random, human-scale interval between two actions."""
    time.sleep(random.uniform(low, high))     # never a fixed interval
```

Automation has to stay inside the rules

Many platforms prohibit automated actions on accounts, or allow them only through official APIs. Never automate fake engagement, mass messaging, bulk account creation or anything else a platform's terms forbid. If a task would break the rules done by hand, a script doesn't make it acceptable.

9.5 RPA Builders and AI Agents

Not every team writes code. AdsPower, GeeLark, Hidemyacc, DICloak and Genlogin all list RPA or no-code automation in the ProxyHorizon directory: you assemble steps such as open a page, wait, click and type, then run them across profiles. The patterns from section 9.4 apply unchanged.

AI agents driving profiles

An AI agent adds a model that decides what to do next: read the page, choose an action, check the result. Pointed at an antidetect profile, an agent inherits a stable identity, a signed-in session and a matching proxy, which makes multi-step tasks far more reliable than a fresh headless browser. It also inherits responsibility for everything it does in that account.

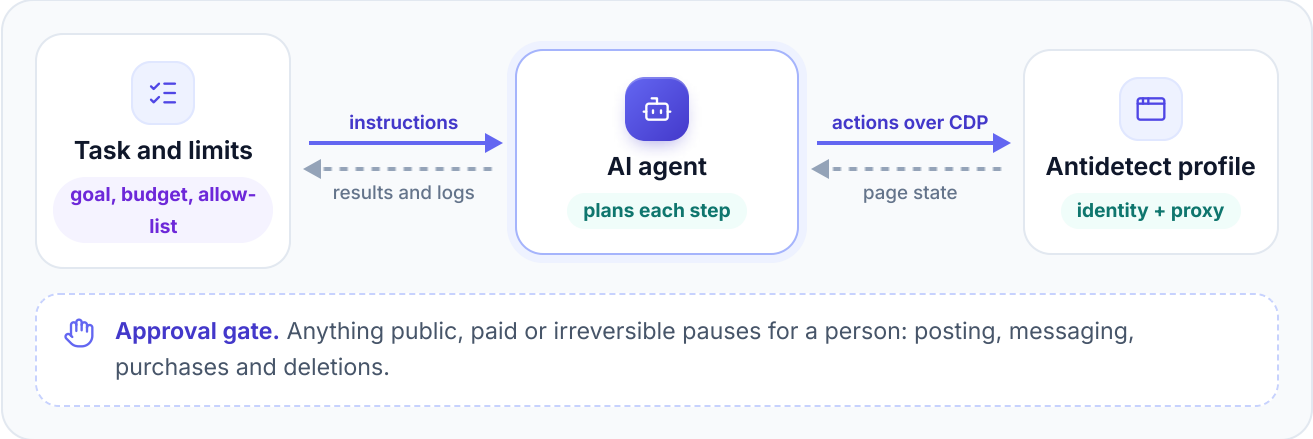


Figure 9.5 The agent decides; the profile supplies a consistent identity; a person approves anything that can't be undone.

Guardrails for agents

- One agent, one profile, one task at a time.
- Allow-list the sites and actions each agent may use.
- Cap steps, minutes and spend per task, and stop on any verification prompt.
- Keep a full action log that a person can review.

KEY TAKEAWAYS

- Start through the local API, connect over CDP, use the existing context, stop through the API.
- Never let your automation library override the profile's settings.
- Pace like a person, cap everything, stop on friction, and keep agents on a short leash.

Go deeper: How AI Agents Manage Browser Profiles · Best Antidetect Browsers for AI Agents

10



Playbooks and Staying Compliant

Six setups you can copy, one for each job antidetect browsers do best, followed by the rules that keep all of it legitimate. Each playbook names the proxy, the browser features that matter and the pitfall that catches most teams.

IN THIS CHAPTER

10.1 Agencies and e-commerce
10.2 Affiliates and ad verification
10.3 QA, geo testing and scraping
10.4 Staying compliant

10.1 Agencies and E-Commerce

Social media agency

Client pages, profiles and ad accounts, run by a team

PROXY	BROWSER FIT	PROFILES
ISP or dedicated mobile, in the client's country	**Team roles, sharing, audit logs**	**One per client account**

1. **Use the platform's business tools first.** Agency access through official business suites and partner permissions beats signing in as the client wherever it's offered.
2. **A folder per client and a profile per account,** named with the convention from section 6.2.
3. **Share profiles, not passwords.** Operators open assigned profiles; credentials stay in the vault.
4. **Keep clients fully separate:** their own proxies, payment details and recovery contacts.

CLASSIC PITFALL
One client's restricted ad account linked to the rest through a shared agency card or office IP.

WATCH THIS NUMBER
Verification prompts per account per month.

E-commerce, several stores

Separate brands, storefronts and regional marketplace accounts

PROXY	BROWSER FIT	PROFILES
Static ISP in each store's main market	**Stable fingerprints, cloud sync**	**One per store account**

1. **Check each marketplace's rules first.** Amazon, for example, expects one selling account unless there's a legitimate business need for more.
2. **One profile and one static IP per store,** in the store's main market, for the store's whole life.
3. **Keep business details genuinely separate** where the rules require it: legal entity, bank and contact details.
4. **Never sign in to two stores from one profile,** and don't clone listings word for word across stores.

CLASSIC PITFALL
Opening a second store "just to check something" from the first store's profile.

WATCH THIS NUMBER
Account health warnings per store.

10.2 Affiliates and Ad Verification

Affiliate marketing and media buying

Campaign testing across offers, markets and ad accounts

PROXY	BROWSER FIT	PROFILES
ISP for ad accounts, residential for research	Ad-team tooling, bulk setup	One per ad account, plus research

1. **Keep research and accounts apart.** Browse competitors and landing pages from research profiles, never from ad-account profiles.
2. **Match every ad account's profile** to the market it buys in.
3. **Follow the ad platform's policies** on creatives, landing pages and claims. Compliant ads protect an account more than any browser setting.
4. **Raise spend in steps** once an account has history, with legitimate, consistent billing.

CLASSIC PITFALL
Opening a fresh ad account after a rejection instead of fixing the ad.

WATCH THIS NUMBER
Disapproval rate per ad account.

Ad verification and brand safety

Placements, creatives and landing pages, as real users see them

PROXY	BROWSER FIT	PROFILES
Residential and mobile, by city and carrier	Mobile fingerprints, screenshots	One per market and device type

1. **Build a profile matrix:** every market and device type the campaign targets.
2. **Load ads the way users do,** with location settings matched to each exit IP.
3. **Capture evidence:** screenshots, redirect chains and final landing pages.
4. **Catch cloaking** by comparing what clean residential IPs see with what datacenter IPs see.

CLASSIC PITFALL
Checking mobile placements from a desktop profile.

WATCH THIS NUMBER
Markets and devices covered per campaign.

Use cases: Affiliate Marketing · Ad Verification · Social Media

10.3 QA, Geo Testing and Scraping

QA and geo testing

Localization, prices, consent banners and device variations

PROXY	BROWSER FIT	PROFILES
Datacenter where allowed, else residential	**API, templates, Playwright**	**One per market and device case**

1. **Turn your test matrix into profile templates:** market, system and device class.
2. **Drive the checks through the local API** and Playwright, as in Chapter 9.
3. **Assert location in every run:** currency, language, consent banner and prices.
4. **Reset test accounts between runs,** or keep a fixed test persona per profile.

CLASSIC PITFALL
Testing a region with your own timezone and language left in place.

WATCH THIS NUMBER
Pass rate per market.

Web scraping with a real browser

Public pages that need JavaScript and a believable browser

PROXY	BROWSER FIT	PROFILES
Rotating residential, or datacenter for lenient sites	**Cloud browsers, CDP**	**Disposable, one per worker**

1. **Use a browser only where you need one.** Plain HTTP clients are cheaper when pages don't need JavaScript.
2. **Treat profiles as workers, not accounts:** rotate IPs freely when nothing is signed in.
3. **Collect public data only,** and respect robots.txt, rate limits and each site's terms.
4. **Block heavy assets and cap pages per job** to keep proxy bills down.

CLASSIC PITFALL
Scraping while signed in, which ties the job to an account and its terms.

WATCH THIS NUMBER
Cost per valid page.

Go deeper: The Scraping Blueprint (free eBook) · Best Antidetect Browsers for Scraping

10.4 Staying Compliant

General information, not legal advice. Laws and platform terms differ by country and change often; for anything high-stakes, ask a lawyer.

Most trouble with antidetect browsers doesn't come from the browser. It comes from what people do with it. Start with each platform's own rules, because they decide how many accounts you may run and how teams should share them.

Platform	What its rules say about multiple accounts	Built for teams instead
Facebook	One personal account per person	Pages and Meta Business Suite
Instagram	Up to five accounts can be added and switched in the app	Business accounts with shared access
LinkedIn	One account per person, in your real name	Company pages with page admins
Amazon selling	One selling account, unless there's a legitimate business need for more	User permissions in Seller Central
Google Ads	Several ad accounts are normal for agencies and brands	Manager accounts

Plain-language summaries of published terms and help pages, checked November 2026. Terms change, so read the current version before you act.

Never acceptable, whatever the tool

- Fraud, including fake identities used to deceive people
- Getting around bans you earned through abuse
- Spam, scams, harassment or impersonation
- Fake engagement: bought likes, follows, reviews or ratings
- Taking over accounts that aren't yours, or stolen cookies
- Anything illegal where you or your audience are

Where ProxyHorizon draws the line

Antidetect browsers are infrastructure for legitimate work: client accounts, separate businesses, testing, verification and privacy. Privacy laws such as the GDPR still apply to customer data, and nothing here is meant to dodge a platform's enforcement.

KEY TAKEAWAYS

- Every playbook rests on the same base: one profile, one stable IP, one account, honest use.
- Each platform's terms decide what's allowed; official team tools come first.
- Fraud, fake engagement, ban evasion and account takeover are never acceptable.

APPENDIX A

Profile Launch Checklist

Print this page, or copy it into your team's SOP template. Every box should be ticked before an account's first login, and the weekly and monthly lists keep it that way.

Before the first login

- [ ] Browser chosen and trialed on your own platforms
- [ ] OS template fits the account's owner
- [ ] Fingerprint generated from real-device data
- [ ] One dedicated proxy, right type, right city
- [ ] Timezone, languages and geolocation follow the IP
- [ ] WebRTC set to altered and tested
- [ ] Fingerprint stable across two restarts
- [ ] Only the extensions this account needs
- [ ] Named, foldered, tagged "warming"
- [ ] Credentials and 2FA in the business vault
- [ ] Recovery email and phone belong to the owner
- [ ] Platform's terms checked for multiple accounts

Every week

- [ ] Status tags and health signals reviewed
- [ ] Audit log read for unusual access
- [ ] Proxies answering, in the same city
- [ ] Automation logs checked for friction

Every month

- [ ] Fingerprint and WebRTC re-tested per profile
- [ ] Browser core updated where the vendor shipped one
- [ ] Profile access reviewed person by person
- [ ] Shared credentials rotated if anyone left
- [ ] Each platform's terms re-read for changes

Browser trial scorecard

Criterion (section 4.1)	Weight	Browser A	Browser B	Browser C
Fingerprint quality and updates	×2			
Engines	×2			
Price per active profile	×1			
Team features	×1			
Automation API on your plan	×1			
Proxy integration	×1			
Cloud sync and security	×1			
Operating systems	×1			
Total (score each 1 to 5)	**/50**			

APPENDIX B

Fingerprint Cheat Sheet

Every major parameter a platform can read, what it gives away, and the setting that keeps a profile believable. When in doubt, choose the value a real device of the template's type would report.

Parameter	What it reveals	Recommended setting
IP address and ASN	Location, network type, reputation	A dedicated ISP, mobile or residential IP in the account's market
TLS and HTTP/2	The real client software	A current, real browser engine, never a script
User-Agent	Browser, version and OS	Matches the core version and the OS template
Client Hints	Brand, version and platform	Consistent with the User-Agent; absent on Firefox profiles
Languages	Preferred languages, in order	The market's language, from the IP
Timezone and locale	Where the clock and formats say you are	From the IP
Geolocation	Precise position, with permission	Near the IP, and ask before sharing
WebRTC	Public and local IP addresses	Altered: the proxy's IP only
Screen and pixel ratio	Device class and display	A common resolution for the OS template
Canvas	Differences in the rendering stack	Stable per profile, from real output or consistent noise
WebGL vendor and renderer	Graphics card and driver	A real GPU that fits the OS template
Audio	Differences in the audio stack	Stable per profile
Fonts	Installed fonts, and so the OS	The template's default font set
CPU cores and memory	Hardware class	Realistic for the device; Firefox doesn't report memory
Touch points	Touchscreen or not	Zero on desktop; real values on mobile
Media devices	Cameras and microphones	A plausible count for the device
Automation flags	A browser under remote control	Off: let the engine handle it, and add no automation launch flags

Check any profile against this sheet: proxyhorizon.com/tools/my-fingerprint

APPENDIX C

Troubleshooting

Start with the symptom, check the likely cause first, and change one thing at a time so you know what fixed it.

Symptom	Likely cause	Fix
Profile shows your real IP	Proxy not applied, or it failed silently	Re-run the proxy check; confirm the protocol and fields
WebRTC shows your real IP	WebRTC mode left on real	Set it to altered and test again
Timezone or language doesn't match	Auto-match off, or a wrong IP database entry	Re-detect from the proxy; set by hand if the data is wrong
407 Proxy Authentication Required	Wrong credentials or unencoded characters	Re-copy them; encode `@ : / #` in passwords
Proxy check passes, sites time out	A slow or dying exit	Test it with Proxy Checker; ask for a replacement in the same city
Verification on every login	The device or IP changes between sessions	One profile and one IP; compare sessions for changes
Fingerprint changes on restart	Noise mode set to random	Switch to a stable mode, or rebuild the profile
Signed out after closing	Profile not saved or synced; process killed	Close through the app or API; check sync status
Teammates see different sessions	Profile opened on two machines	One person at a time; wait for sync before reopening
Automation sees an 800 × 600 window	The library overrode the viewport	Puppeteer: `defaultViewport: null`; Playwright: existing context
Selenium can't attach	chromedriver doesn't match the core	Use the driver your vendor ships for that core
Several accounts restricted at once	A shared link: IP, card, phone or content	Audit them with the table in section 3.3

Keep a change log per profile

Most mysteries turn out to be a change nobody wrote down: a new proxy, a core update, a teammate's extension. A dated line in the profile's notes turns a guessing game into a two-minute fix.

APPENDIX D

Glossary

Antidetect browser

An app that runs many isolated browser profiles, each with its own storage, fingerprint and proxy.

ASN

The network an IP belongs to, which reveals whether it's a home ISP, a mobile carrier or a data center.

Browser core

The modified engine, usually Chromium or Firefox, that a profile runs on. Its version should track real releases.

Browser fingerprint

The combination of device, browser and network details that can identify a browser without cookies.

Browser profile

One isolated browser identity: storage, fingerprint and proxy together. One profile per account.

Canvas fingerprint

A hash of hidden drawing output, which varies with GPU, drivers and fonts.

CDP

The Chrome DevTools Protocol, which Playwright and Puppeteer use to control a running profile.

Client Hints

Headers in which Chromium-based browsers describe their brand, version and platform.

Cloud phone

An Android device in a data center that you control remotely, for app-based accounts.

ISP proxy

A static IP registered to an internet provider, hosted on fast servers. Ideal for long-lived accounts.

JA3 and JA4

Hashes of how a client opens TLS connections, used to recognize the real software behind a request.

Local API

A small web server the antidetect app runs on your machine so code can start and stop profiles.

Mobile proxy

An IP from a 4G or 5G carrier, shared by many subscribers and highly trusted.

Noise

Small changes added to canvas or audio output. Safe only when it stays stable per profile.

Residential proxy

An IP from a real home connection, usually rotating or sticky through a gateway.

SOCKS5

A proxy protocol that carries any TCP connection, and UDP where the provider supports it.

Sticky session

A gateway holding the same exit IP for a set time instead of rotating it.

WebGL fingerprint

The graphics card's name and limits, plus 3D rendering output that varies by GPU.

WebRTC leak

Your real IP exposed through the browser's real-time communication feature, despite a proxy.

Longer definitions with examples for 80+ terms live in the ProxyHorizon Glossary at proxyhorizon.com/glossary.

APPENDIX E

Free Tools and Further Reading

Everything below is free on ProxyHorizon, and the browser tools need no account.

Free tools for profile work

My Fingerprint	What a profile reveals	What Is My IP	The exit IP a site sees
IP Lookup	ASN, ISP and location	User-Agent Parser	Browser, version and OS
Proxy Checker	Speed and uptime	Proxy Format Converter	Lists for bulk import
Password Generator	Strong account passwords	Random User-Agent	Current, realistic UAs

Directories, comparisons and finders

Antidetect browsers	25 rated listings	Compare browsers	Any two, side by side
Find My Browser	A quick-fit quiz	Proxy providers	Tested and compared

Guides worth reading next

- How Antidetect Browsers Work
- How to Choose an Antidetect Browser
- Proxies With an Antidetect Browser
- Warming Up Accounts
- Antidetect Team Management
- Antidetect Browsers for Affiliates
- Antidetect Browsers for Dropshipping
- How Cloud Phones Work With Proxies

Antidetect browsers reward the teams that treat them as discipline rather than magic. One profile per account, one stable IP per profile, honest use and clean records: do those well and most problems never start.

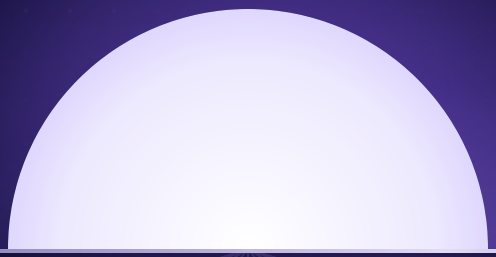
Browser directory | Compare browsers | Free tools | Multi-account guide

ProxyHorizon

Compare confidently. Implement correctly.

ProxyHorizon is the independent directory and resource hub for proxies, VPNs and antidetect browsers: expert-tested comparisons, free tools and practical guides to choose and use them.

- Compare 25 antidetect browsers
- Free proxy and network tools
- In-depth, fact-checked guides



MORE FREE EBOOKS FROM PROXYHORIZON

The Ultimate Proxy Handbook
Choose, run and scale proxies

The Scraping Blueprint
Collect web data that lasts

Proxies for AI Agents and LLM Data
Web access for AI builders

Lead Generation with Public Web Data
Prospect lists, responsibly

© 2026 PROXYHORIZON · THE ANTIDETECT BROWSER HANDBOOK