

Access Audit for Google Ads

Prepared for: **Brightpath Digital (demo)**

Audit date: **2026-10-14**

Reviewed by: **Nicolas Su Nobrega, HumanLS**

Scope: **6**

Sample report with fictitious data; addresses are masked.

Possible active compromise

At least one finding looks like a takeover in progress (changes to users, billing, security or manager links by someone nobody recognises, or an unrecognised manager with ownership). Follow the active-compromise protocol before working through the rest of this report.

Report a compromised account to Google (https://support.google.com/google-ads/contact/compromised_account) · Guide: <https://support.google.com/google-ads/answer/9355975>

Actions taken during the session

- 10:42 · Possible takeover on Urban Fit Gym (unrecognised admin ad***@outlook.com, user-access change on 2026-10-12). Session paused; the agency administrator removed the user, signed out all sessions of the affected login and filed Google's compromised-account form. Rest of the review resumed at 11:05. Re-check at day 14.

Summary

6 Google Ads accounts reviewed live with the agency on 2026-10-14. Read-only: HumanLS changed nothing.

6 Accounts reviewed	20 Users reviewed	2 Critical	7 High	9 Medium
1 Low				

Clean-up priorities

#	Severity	Account	Finding	Action
1	Critical	Brightpath Digital MCC	Former team member lu.....@brightpath.example still has Admin access	Remove access now.
2	Critical	Urban Fit Gym	Changes by unrecognised actor «ad.....@outlook.com» (user access) on 2026-10-12	Treat as a possible compromise: follow the active-compromise protocol before anything else.
3	High	Brightpath Digital MCC	Only one trusted administrator (an.....@brightpath.example)	Add a second trusted administrator from the agency or the client.
4	High	Brightpath Digital MCC	Former team member lu.....@brightpath.example made changes on 2026-09-28	Confirm the departure date and review what was changed.
5	High	Café Luna	Pending invitation to unrecognised address se.....@gmail.com (Standard)	Revoke the invitation unless someone can vouch for it.
6	High	Roofing Pros	Unrecognised manager account linked: Growth Ads Partners (987-654-3210)	Confirm the link with the client; unlink it if nobody recognises it.
7	High	Sonrisa Dental	dr.....@sonrisadental.example (Standard) signs in with password only	Ask the user to turn on a passkey or 2-Step Verification, or remove edit access until they do.
8	High	Urban Fit Gym	Unrecognised user ad.....@outlook.com with Admin access	Confirm who this is today; if nobody can vouch for it, remove access.
9	High	Urban Fit Gym	Former team member so.....@brightpath.example still has Read-only access	Remove access now.
10	Medium	Brightpath Digital MCC	Personal email account da.....@gmail.com with Standard access	Replace with a company-domain account and remove the personal one.
11	Medium	Café Luna	2-Step Verification is not required	Admin > Access and security > Security > Authentication: require 2-Step Verification (from the manager account it can apply to every owned account).
12	Medium	Café Luna	No allowed email domains	Admin > Access and security > Security > Allowed domains: add the agency and client domains.
13	Medium	Roofing Pros	Allowed domains include a public email domain (gmail.com)	Remove the public domain from the list.

14	Medium	Roofing Pros	Changes labelled «Google Ads API» that no declared tool accounts for	Find which tool made these changes and add it to the inventory; if nobody knows, revoke its access from the tool or from the Google Account that authorised it.
15	Medium	Roofing Pros	Linked product nobody recognised: Merchant Center MC-7781	Confirm the owner or remove the link.
16	Medium	Sonrisa Dental	Only one trusted administrator (an*****@brightpath.example)	Add a second trusted administrator from the agency or the client.
17	Medium	Sonrisa Dental	dr*****@sonrisadental.example has not signed in for 208 days but keeps Standard access	Downgrade to Read-only or remove.
18	Medium	Sonrisa Dental	The client has no administrator on its own account	Recommend that one person at the client keeps Admin access.
19	Low	Reyes Law	Invitation to in****@brightpath.example pending for 55 days	Revoke it and resend only if still needed.

Across the portfolio

Note 6 accounts have three or fewer administrators listed on the account

WHY IT MATTERS: Google's help page says Multi-party approval applies to accounts with more than 3 administrators, and that read-only and API users are exempt. It does not spell out how administrators in a linked manager account count. Do not assume it protects these accounts.

WHAT TO DO: Check the Security requests tab in Access and security to see whether approvals are active.

Google help: <https://support.google.com/google-ads/answer/16891189>

Security settings

2-Step Verification required	yes
Allowed domains	brightpath.example
Administrators listed on this account	2
Linked manager accounts	none

User	Access	Sign-in	Last sign-in	Who
an••••••@brightpath.example	Admin	Passkey	2026-10-13	Agency
lu••••••@brightpath.example	Admin	2-Step	2026-06-02	Former staff
da••••••••@gmail.com	Standard	2-Step	2026-10-10	Agency
pa••••••@brightpath.example	Standard	2-Step	2026-10-14	Agency

Findings

- Critical

Former team member lu••••••@brightpath.example still has Admin access

WHY IT MATTERS: Access that outlives employment usually goes unnoticed until someone uses it.

WHAT TO DO: Remove access now.

Google help: <https://support.google.com/google-ads/answer/6372672>
- High

Only one trusted administrator (an••••••@brightpath.example)

WHY IT MATTERS: Not counting former staff or unrecognised users. If that person leaves, is locked out or is compromised, nobody else at this level can recover users. Google also pauses Multi-party approval when an account drops to a single administrator.

WHAT TO DO: Add a second trusted administrator from the agency or the client.

Google help: <https://support.google.com/google-ads/answer/16891189>
- High

Former team member lu••••~@brightpath.example made changes on 2026-09-28

WHY IT MATTERS: Activity after someone left is either a mistake in the staff list or misuse.

WHAT TO DO: Confirm the departure date and review what was changed.

Google help: <https://support.google.com/google-ads/answer/19888>

Medium Personal email account da.....@gmail.com with Standard access

WHY IT MATTERS: Personal accounts stay with the person when they leave and the agency cannot enforce its own security policy on them.

WHAT TO DO: Replace with a company-domain account and remove the personal one.

Google help: <https://support.google.com/google-ads/answer/9978556>

Security settings

2-Step Verification required	no
Allowed domains	none
Administrators listed on this account	2
Linked manager accounts	Brightpath Digital MCC (123-456-7890)

User	Access	Sign-in	Last sign-in	Who
ma...@cafeluna.example	Admin	2-Step	2026-09-30	Client
an.....@brightpath.example	Admin	Passkey	2026-10-13	Agency
pa.....@brightpath.example	Standard	2-Step	2026-10-14	Agency

Findings

High

Pending invitation to unrecognised address se.....@gmail.com (Standard)

WHY IT MATTERS: Attackers send invitations to their own addresses and wait for them to be accepted.

WHAT TO DO: Revoke the invitation unless someone can vouch for it.

Google help: <https://support.google.com/google-ads/answer/6372672>

Medium

2-Step Verification is not required

WHY IT MATTERS: Nothing forces users to add a second step, so a stolen password may be enough.

WHAT TO DO: Admin > Access and security > Security > Authentication: require 2-Step Verification (from the manager account it can apply to every owned account).

Google help: <https://support.google.com/google-ads/answer/12865295>

Medium

No allowed email domains

WHY IT MATTERS: Anyone with admin rights, including an attacker, can invite any address.

WHAT TO DO: Admin > Access and security > Security > Allowed domains: add the agency and client domains.

Google help: <https://support.google.com/google-ads/answer/12864084>

Security settings

2-Step Verification required	yes
Allowed domains	brightpath.example, sonrisadental.example
Administrators listed on this account	1
Linked manager accounts	Brightpath Digital MCC (123-456-7890)

User	Access	Sign-in	Last sign-in	Who
an*****@brightpath.example	Admin	Passkey	2026-10-13	Agency
dr*****@sonrisadental.example	Standard	Password only	2026-03-20	Client
fr*****@sonrisadental.example	Read-only	—	—	Client

Findings

- High

dr*****@sonrisadental.example (Standard) signs in with password only

WHY IT MATTERS: A phished password is enough to take this account.

WHAT TO DO: Ask the user to turn on a passkey or 2-Step Verification, or remove edit access until they do.

Google help: <https://support.google.com/google-ads/answer/12865295>
- Medium

Only one trusted administrator (an*****@brightpath.example)

WHY IT MATTERS: Not counting former staff or unrecognised users. If that person leaves, is locked out or is compromised, nobody else at this level can recover users. Google also pauses Multi-party approval when an account drops to a single administrator.

WHAT TO DO: Add a second trusted administrator from the agency or the client.

Google help: <https://support.google.com/google-ads/answer/16891189>
- Medium

dr*****@sonrisadental.example has not signed in for 208 days but keeps Standard access

WHY IT MATTERS: Unused accounts with edit rights add risk without adding work.

WHAT TO DO: Downgrade to Read-only or remove.

Google help: <https://support.google.com/google-ads/answer/9978556>
- Medium

The client has no administrator on its own account

WHY IT MATTERS: If the agency's access is lost or the relationship ends, the client depends entirely on the agency to recover its account.

WHAT TO DO: Recommend that one person at the client keeps Admin access.

Google help: <https://support.google.com/google-ads/answer/9978556>

Security settings

2-Step Verification required	yes
Allowed domains	brightpath.example, roofingpros.example, gmail.com
Administrators listed on this account	2
Linked manager accounts	Brightpath Digital MCC (123-456-7890), Growth Ads Partners (987-654-3210)

User	Access	Sign-in	Last sign-in	Who
an*****@brightpath.example	Admin	Passkey	2026-10-13	Agency
ji***@roofingpros.example	Admin	2-Step	2026-08-01	Client
re*****@callrail.example	Read-only	—	—	Approved vendor

Findings

- High

Unrecognised manager account linked: Growth Ads Partners (987-654-3210)

WHY IT MATTERS: A linked manager can manage campaigns; with ownership it can also change users. Hijackers have created MCCs in an agency's name and invited its clients into them.

WHAT TO DO: Confirm the link with the client; unlink it if nobody recognises it.

Google help: <https://support.google.com/google-ads/answer/9978556>
- Medium

Allowed domains include a public email domain (gmail.com)

WHY IT MATTERS: Allowing a public domain lets anyone with a free address be invited, which cancels the protection.

WHAT TO DO: Remove the public domain from the list.

Google help: <https://support.google.com/google-ads/answer/12864084>
- Medium

Changes labelled «Google Ads API» that no declared tool accounts for

WHY IT MATTERS: API connections are reviewed far less often than human users, and Google does not list connected apps.

WHAT TO DO: Find which tool made these changes and add it to the inventory; if nobody knows, revoke its access from the tool or from the Google Account that authorised it.

Google help: <https://support.google.com/google-ads/answer/19888>
- Medium

Linked product nobody recognised: Merchant Center MC-7781

WHY IT MATTERS: Linked products can receive account data.

WHAT TO DO: Confirm the owner or remove the link.

Google help: <https://support.google.com/google-ads/answer/9978556>

Security settings

2-Step Verification required	yes
Allowed domains	brightpath.example, reyeslaw.example
Administrators listed on this account	2
Linked manager accounts	Brightpath Digital MCC (123-456-7890)

User	Access	Sign-in	Last sign-in	Who
an*****@brightpath.example	Admin	Passkey	2026-10-13	Agency
lu***@reyeslaw.example	Admin	2-Step	2026-10-01	Client
pa*****@brightpath.example	Standard	2-Step	2026-10-14	Agency

Findings

Low

Invitation to in****@brightpath.example pending for 55 days

WHY IT MATTERS: Old invitations are forgotten and can be accepted later by whoever controls that inbox.

WHAT TO DO: Revoke it and resend only if still needed.

Google help: <https://support.google.com/google-ads/answer/6372672>

Security settings

2-Step Verification required	not captured
Allowed domains	not captured
Administrators listed on this account	3
Linked manager accounts	Brightpath Digital MCC (123-456-7890)

User	Access	Sign-in	Last sign-in	Who
an*****@brightpath.example	Admin	Passkey	2026-10-13	Agency
co*****@urbanfit.example	Admin	2-Step	2026-09-15	Client
ad*****@outlook.com	Admin	—	2026-10-12	Unrecognised
so*****@brightpath.example	Read-only	2-Step	2026-05-10	Former staff

Findings

Critical

Changes by unrecognised actor «ad*****@outlook.com» (user access) on 2026-10-12

WHY IT MATTERS: Changes to users, billing, security or manager links by someone nobody recognises are a sign of takeover.

WHAT TO DO: Treat as a possible compromise: follow the active-compromise protocol before anything else.

Google help: <https://support.google.com/google-ads/answer/9355975>

High

Unrecognised user ad*****@outlook.com with Admin access

WHY IT MATTERS: The address is not from the agency, the client or a declared vendor. Attackers add their own users after taking over an account.

WHAT TO DO: Confirm who this is today; if nobody can vouch for it, remove access.

Google help: <https://support.google.com/google-ads/answer/6372672>

High

Former team member so*****@brightpath.example still has Read-only access

WHY IT MATTERS: Access that outlives employment usually goes unnoticed until someone uses it.

WHAT TO DO: Remove access now.

Google help: <https://support.google.com/google-ads/answer/6372672>

Method and limits

- Reviewed live in a screen-share with an administrator of the agency: Admin > Access and security (users, invitations, linked manager accounts, Security tab) and Change history for the last 90 days, for every account in scope.
- Only administrators can see each user's sign-in method and last sign-in time; where it was not visible it is marked «—».
- We have not found a list of connected apps inside Google Ads. API activity is inferred from Change history, where Google says API changes might appear as «Google Ads API» or a tool name; Google also notes that some account-level changes may not be listed.
- Users of the Google payments profile (billing) are managed outside Google Ads and were not reviewed.
- This is a point-in-time review of what was shown on screen. It does not detect stolen sessions, malware or phishing in progress, and it is not a certification or a guarantee.
- HumanLS never asks for passwords, never receives access by default and never changes anything. The agency applies every action.
- HumanLS is independent and is not affiliated with or endorsed by Google.

Sources (Google Ads Help, read 2026-10-14)

- Manage access to your Google Ads account: <https://support.google.com/google-ads/answer/6372672>
- About access levels in your Google Ads account: <https://support.google.com/google-ads/answer/9978556>
- About Multi-party approval for Google Ads: <https://support.google.com/google-ads/answer/16891189>
- Manager Account Security Mandates: <https://support.google.com/google-ads/answer/12865295>
- Allowed Email Domains: <https://support.google.com/google-ads/answer/12864084>
- About change history: <https://support.google.com/google-ads/answer/19888>
- Compromised account issues: <https://support.google.com/google-ads/answer/9355975>