



An Extended Guide · No. 2081

Locking Down Google Workspace: The Admin Security Checklist

Enforce 2-Step Verification, protect the
super-admin, and close the back doors

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! Read this first — the two things that stop most attacks

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. In Google Workspace, the single highest-impact thing you can do is turn on 2-Step Verification and actually enforce it — that one move blocks the overwhelming majority of account takeovers.

Let's lock down your Google Workspace

If your business runs on Google Workspace — Gmail, Drive, Docs, Calendar, Meet — then your sign-ins are the front door to everything. This guide is a plain-English admin checklist: the handful of settings that stop most break-ins, done in an order that puts the biggest win first.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping small businesses with their technology, in plain language. You don't need to be technical to do this — you need to know which few settings matter and how to flip them, and I'll walk you through each one.

One honest heads-up: Google renames and rearranges these settings in the Admin console from time to time. I'll give you the names and paths as they stand at the time of writing, but if what you see doesn't match exactly, that's normal — look in your current Admin console or give me a call.

★ I can run this checklist with you in one visit

Turning on and enforcing 2-Step Verification and tidying up your admin settings is usually a quick job, and I'll make sure nobody gets locked out along the way. Call or text me at (330) 200-8042.

The whole checklist, on one page

If you do only these things, your Google Workspace is far safer than most small shops.

- ❑ Turn on **2-Step Verification (2SV)** and **enforce** it — not just 'allow' it — with a short enrollment period.
- ❑ For admins and high-value users, prefer **security keys or passkeys (FIDO2)** over texted codes.
- ❑ Protect your **super administrator** account above all others, and don't use it as a daily mailbox.
- ❑ Keep the **number of super-admins small** and keep a safe emergency (break-glass) admin.
- ❑ Check **recovery info, admin and login alerts**, and shut down old **app passwords / less-secure access**.
- ❑ Google is **mandating 2SV for admin accounts** — get ahead of it rather than scramble.

! 'Allow' is not the same as 'enforce'

The most common Google Workspace mistake is turning on 2-Step Verification but leaving it optional — so most people never actually set it up. You have to **enforce** it, with a grace period for enrollment, before it truly protects you.

Why 2-Step Verification is the first move

Of everything on the checklist, this is the one that does the heavy lifting. Here's why it earns the top spot.

2-Step Verification — Google's name for MFA, the second step at sign-in — means a password by itself won't get anyone in. There's a second step: a prompt on your phone, a code, or a security key. Since most account takeovers are just a stolen, reused, or guessed password, that second step shuts the door on the overwhelming majority of them in one move.

That's why 2SV is the highest-impact control you can turn on, and why Google itself has been mandating it for administrator accounts, with advance notice to admins. If you do one thing from this guide, make it turning on and enforcing 2SV.

! A password alone is not a lock anymore

Treat any Google account that has only a password as effectively unlocked. The whole point of this checklist is to make sure every account — yours, your staff's, and especially your super-admin — has that second step required, not merely offered.

How to turn on and enforce 2SV

Here's the path as it stands at the time of writing. Google moves these menus, so if yours differs, confirm in your current Admin console.

- Sign in to the **Admin console** with your super administrator account.
- Go to **Security > Authentication > 2-Step Verification**.
- Turn it on, then set it to **Enforce** — not just 'allow users to turn it on.'
- Set a short **enrollment (grace) period** so everyone has a few days to register before it's required.

The enrollment period is the kind part: it lets people set up their second step on their own time before the lock snaps shut, so nobody is surprised. For a small team you can keep that window short — there's no reason to drag it out, and the sooner it's enforced, the sooner you're protected.

✓ Settings move — the idea doesn't

If 'Authentication' or '2-Step Verification' isn't exactly where this guide says, look under Security in your Admin console or search its help. The location may shift; enforcing that second step is the thing you're after.

The difference between 'allow' and 'enforce'

This one distinction is where most of the real protection is won or lost, so it's worth a page of its own.

When you merely **allow** 2-Step Verification, you're saying 'people may turn this on if they'd like to.' In practice, most people never get around to it, so your accounts stay protected by passwords alone — which is to say, barely protected at all. You've flipped a switch but changed almost nothing.

When you **enforce** it, you're saying 'everyone must have this on to keep using their account,' with a short grace period to get set up. Now the protection is real and universal. Enforcing is the whole point — allowing is a half-measure that feels like progress without delivering it.

! An optional lock is an unlocked door

If you turn on 2SV but leave it optional, don't fool yourself that you're covered — you've simply offered a lock that most people won't use. Enforce it, or you've done the work without getting the benefit.

Not all second steps are equal

2SV can use several kinds of second step. For your most important accounts, choose the strongest.

The weakest second step is a code texted to your phone — better than nothing, but a determined attacker can sometimes intercept or trick you out of it. A prompt in the Google app is stronger. The strongest of all are **security keys and passkeys (FIDO2)**, which are phishing-resistant: they're bound to the real site, so a fake login page can't capture anything reusable.

A sensible plan: standard 2SV for everyday staff, and the strongest option — a security key or passkey — for your super-admins and anyone handling especially sensitive data. Our guide on passkeys and security keys walks through exactly how to roll these out to a handful of people.

✓ Push SMS codes to the bottom of the list

If you can, steer your most valuable accounts away from text-message codes and toward a key or passkey. For everyday users a phone prompt is fine; for the keys to the kingdom, go phishing-resistant.

Guard the super administrator account

Of all your accounts, one deserves the most protection: the super administrator.

The super administrator can change everything in your Google Workspace — add and remove people, reach anyone's data, reset passwords, and rewrite security for the whole organization. If an attacker captures that one account, they have the keys to the kingdom. So it needs your strongest protection.

That means a phishing-resistant second step (a security key or passkey) if you can, a strong unique password, and — importantly — **not using it as an everyday mailbox**. Sign into the super-admin only to make admin changes, and read your daily mail from a normal account. Our guide 'Who's the Admin?' goes deeper on keeping admin and everyday accounts apart.

! Google is tightening admin sign-in

Google has been mandating 2-Step Verification for administrator accounts, with advance notice. Putting strong protection on your super-admin now means you're ahead of the requirement, not caught off guard by it.

Keep a safe 'break-glass' admin

Enforcing 2SV raises a fair worry — what if someone gets locked out? The answer is an emergency admin.

A **break-glass admin** is a spare super-admin account you create, write down, and lock away — like the little hammer behind glass by a fire exit. You never use it for daily work. It exists for the moment a regular admin is unavailable, locked out, or an account is compromised and you need a clean way back in.

Give it a strong unique password, protect it, and store its login somewhere truly safe and separate — a sealed envelope in a safe, or your password manager's most protected entry. Make sure the owner knows where it lives, and test it a couple of times a year so you know it works before you ever need it.

✓ Set it up before you enforce

Create your emergency admin as part of locking down, not after a lockout. It's cheap insurance, and it lets you enforce 2SV with confidence instead of hesitation.

Keep the super-admin count small

Every super-admin is a powerful key. The fewer you have, the less there is to lose.

It's easy for super-admin rights to accumulate — someone needed it once, a former IT helper still has it, an account was set up as admin 'to be safe.' Each of those is another password a thief could steal and another account you must guard. In a small shop, the owner plus one trusted backup is often all you need.

Open your Admin console and look at who currently holds super-admin and other admin roles. Anyone who doesn't genuinely need that power should be stepped down to a normal account. This is the same least-privilege idea from our admin-accounts guide, applied right where it matters most.

✓ Make a written list and keep it

Write down exactly who holds admin rights and why, and review it a couple of times a year. A short, current list is one of the simplest security tools you'll ever keep.

Two kinds of Google Workspace shops

The checklist is the same, but how quickly and how tightly you tune it depends on your size and how sensitive your data is.

If you're a small team

A handful of users and straightforward needs. You can enforce the essentials quickly and be done.

- Enforce 2SV with a short enrollment window — small teams can move fast.
- Keep super-admins to the owner and one backup, plus a locked-away emergency admin.
- Put a security key or passkey on the super-admin; phone prompts are fine for everyone else.
- Do the quick extras — recovery info, alerts, app passwords — in the same sitting.

If you're growing or handle sensitive data

More people, maybe donor, patient, or financial records. The same steps matter more, and a few deserve extra care.

- Push phishing-resistant keys or passkeys to more of your high-value users, not just admins.
- Watch admin and login alerts closely, and review the admin list more often.
- Be strict about shutting down old app passwords and legacy access paths.
- If an insurer or a rule applies to you, confirm exactly which controls you must be able to show.

★ Not sure how tight to set things?

Tell me how many people you have and what kind of data you handle, and I'll help you right-size the checklist — strong where it counts, simple where it can be. Call (330) 200-8042.

Check your recovery information

If you ever need to recover an account, Google leans on its recovery details — so make sure those point to you.

Every account has recovery information: a backup email and phone used to help get back in if something goes wrong. The danger for a small business is stale or wrong recovery details — a former employee's phone number still listed, or a personal email nobody controls anymore. In the worst case, outdated recovery info can be a back door into an account.

Review the recovery details on your admin and important accounts and make sure they point to a current, trusted contact under your control. This is especially important for the super-admin and for any shared or service accounts.

✓ Recovery info is a key too

A recovery email or phone that belongs to someone who's left is just another way in that you didn't mean to leave open. Clean these up whenever someone departs — it pairs naturally with your offboarding checklist.

Turn on the alerts that warn you early

Good alerts mean you hear about trouble while you can still do something about it.

Google Workspace can notify you about events worth knowing: suspicious sign-ins, changes to admin settings, a new admin being created, and other unusual activity. For a small business, the most valuable ones are alerts about admin changes and about logins that look odd — a sign-in from a strange location, say.

- Make sure admin and security alerts go to an address a real person actually watches.
- Pay special attention to alerts about new admins or changed admin settings — those can signal a takeover.
- Don't let alerts pile up unread; a warning nobody reads is no warning at all.
- The exact alert names and locations may differ in your Admin console — look under the security or alerts area.

✓ An alert is only as good as who reads it

Decide now who watches the alert inbox. In a one-person shop that's you; in a team, name someone — and make sure a strange-login alert wouldn't sit unseen for a week.

Shut down app passwords and legacy access

A couple of older features can quietly let something sign in **without** your shiny new second step. Close them.

Over the years, Google has offered ways for older apps and devices to connect using just a password — things often called 'app passwords' or 'less secure app access.' The problem is that these can bypass 2-Step Verification entirely: a leaked app password could let someone in without the second step you worked to enforce.

In your Admin console, look for these older access methods and turn them off unless you have a specific, understood reason to keep one. If an old program breaks because of it, that's usually a sign the program was using an insecure sign-in and should be updated to a modern one.

! A back door undoes the front-door lock

There's little point enforcing 2SV at the front door if an old app password leaves a side door propped open. Finding and closing these legacy paths is part of making your enforcement actually hold.

If you run both Google and Microsoft

Plenty of small businesses have a foot in both camps. The ideas carry straight across.

Maybe your email is on Google Workspace but part of the business uses Microsoft 365, or you're mid-switch. The sign-in principles are identical: require a second step for everyone, protect the top admin account, keep admin separate from everyday accounts, and keep a break-glass admin. Only the menu names differ.

On the Microsoft side, the free equivalent of enforcing 2SV is called Security Defaults, and the top admin is the Global Administrator. Our companion guide 'Locking Down Microsoft 365 Sign-Ins' covers that side the same way this one covers Google. Wherever your mail lives, the enforced second step is what matters most.

★ Running a mix? I handle both

Lots of the offices I help have one foot in Google and one in Microsoft. I can lock down the sign-ins on both sides in a single visit so you're not juggling two different to-do lists. Call (330) 200-8042.

What your team will experience

Enforcing 2SV is quick for you; knowing what your people will see keeps it from feeling disruptive.

During the enrollment window, each person gets a nudge to set up their second step — a phone prompt, a code, or a key. Once it's enforced, signing in means entering their password and then confirming that second step. On trusted devices they won't be challenged constantly, so day to day it's a light touch, not a nuisance.

The only real friction is surprise, so get ahead of it. A short note to your team — 'you'll be asked to set up a second sign-in step this week, here's how, it's expected' — turns a potential help-desk rush into a non-event.

✓ Tell people before, not after

Nearly every 2SV complaint I hear traces back to no one warning the team. A day's heads-up and a one-line how-to make the whole rollout smooth.

The mistakes that leave the door cracked

A few common habits quietly undercut all this good work. Now you'll catch them.

- **Allowing 2SV instead of enforcing it** — the number-one mistake, since most people never opt in.
- **No strong protection on the super-admin**, the one account that most needs it.
- **Using the super-admin as a daily mailbox**, exposing the keys to everyday phishing.
- **Too many super-admins**, each one an extra key to lose.
- **Leaving old app passwords or legacy access on**, bypassing your enforced second step.
- **No break-glass admin**, so one lockout turns into a crisis.

! Half-done is the real risk

Most Google Workspace trouble I see isn't a wrong setting — it's a job left half-finished: 2SV allowed but not enforced, or enforced at the front door while a back door stays open. Finish the whole checklist.

The checklist, in the right order

Here's the whole job with the biggest wins first. Work top to bottom.

- ☐ Confirm who your **super-admins** are and that the count is small.
- ☐ Create and lock away a **break-glass admin**.
- ☐ Turn on and **enforce** 2-Step Verification with a short enrollment window.
- ☐ Put a **security key or passkey** on the super-admin and other high-value accounts.
- ☐ Check **recovery info** and make sure **alerts** reach a real person.
- ☐ Shut down old **app passwords / less-secure access**, and move the super-admin out of daily email.

Work through it and you'll have the essentials done in an afternoon. If any step gives you pause — especially avoiding a lockout — that's exactly the kind of thing I'm glad to handle with you on a call or a visit.

How to know it actually took effect

A few quick checks confirm the protection is really on — not just switched somewhere in a menu.

- Sign out and back in as a normal user — you should be required to do the second step.
- Confirm 2SV shows as **enforced**, not merely allowed.
- Try the super-admin — it should demand its strong second step every time.
- Confirm your break-glass account's login and second step both work.
- Check that old app passwords and legacy access are off.

✓ Test it the way a thief would

The simplest proof is to try signing in with just a password. If Google stops you and insists on the second step — and there's no old app-password back door around it — an attacker with a stolen password is stopped too.

Keeping it current over time

Sign-in security isn't set-and-forget. A light yearly touch keeps it solid as things change.

A couple of times a year, confirm your admin list is still short and correct, that 2SV is enforced for everyone (including new hires), that recovery details are current, and that your break-glass account still works. When someone leaves, disable their account and clean up their recovery info promptly — our offboarding guide makes that a same-day habit.

Also keep half an eye on Google's own changes. They regularly tighten defaults, move settings, and expand where 2SV is required for admins. When a new requirement appears, it's almost always nudging you toward something safer — go with it rather than hunting for a way around it.

✓ Pair it with your other yearly checks

This review sits naturally alongside your backup test, your admin-account review, and your insurance renewal. Doing them together makes one tidy security habit you won't forget.

The checklist, in one view

Keep this handy — it's the whole job summarized.

Step	What it does	Priority
Enforce 2SV	Required second step	Do first
Protect super-admin	Guard the keys	Do first
Break-glass admin	Avoid lockout	Do early
Keys/passkeys	Phishing-resistant	High-value first
Recovery and alerts	Close gaps, warn early	Same sitting
Kill app passwords	Shut back doors	Don't skip

★ **Want it done right, without the lockout worry?**

I'll enforce 2SV with you, protect your super-admin, set up a break-glass account, and close the old back doors so nobody's ever stuck. Call or text (330) 200-8042.

Common Questions

The questions I hear most from owners locking down Google Workspace.

Q: What's the single most important step?

Enforcing 2-Step Verification — not just allowing it. It's the highest-impact control, it stops most account takeovers, and Google is mandating it for admins anyway. Set a short enrollment window and make it required.

Q: Isn't turning 2SV on enough? Why 'enforce'?

Because 'on but optional' means most people never set it up, so your accounts stay password-only. Enforcing requires everyone to have it (with a grace period), which is the only version that actually protects you.

Q: What if someone gets locked out?

That's what the break-glass admin is for — a spare, locked-away super-admin you can fall back on. Keep it written down safely, protect it, and test it a couple of times a year.

Q: Are text-message codes good enough?

They're better than nothing, but for admins and high-value users prefer a security key or passkey (FIDO2). Those are phishing-resistant — a fake login page can't capture anything reusable. See our passkeys guide.

★ Still have a question?

There's no silly question here. Call or text me at (330) 200-8042 and I'll give you a straight, plain-English answer — and I don't sell Google licenses, so it's just honest advice.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made locking down your Google Workspace feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't worry about memorizing anything.

When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I'm a tech helper, not a lawyer or your insurance agent — for the legal and insurance pieces I'll help you understand the questions and line up the right professional.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

The Admin Security Checklist

Biggest wins first

	Why it matters	When
Enforce 2SV	Stops takeovers	Do first
Protect super-admin	Guards the keys	Do first
Break-glass admin	Avoids lockout	Do early
Kill app passwords	Shuts back doors	Don't skip

Enforce -- don't just allow. An optional lock is an unlocked door.

Allow vs. Enforce

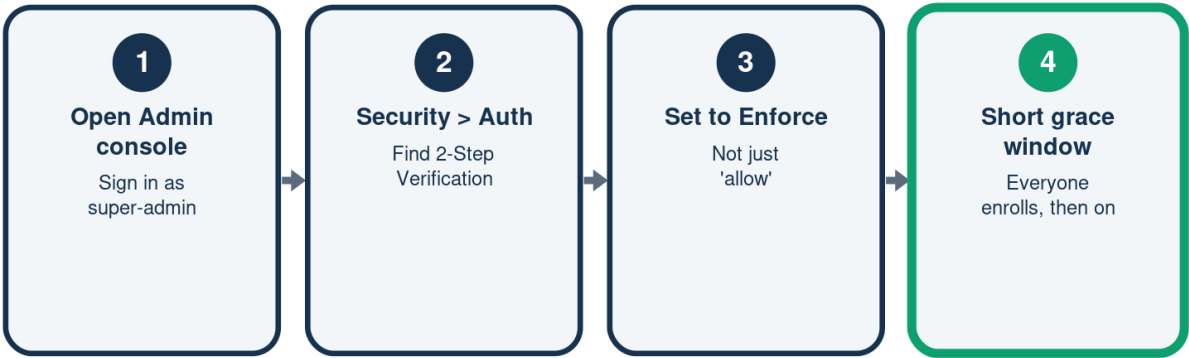
Where the real protection is won

	Allow 2SV	Enforce 2SV
Who sets it up	A few who opt in	Everyone
Real protection	Little	Full
Grace period	N/A	Short window
Feels like progress	Yes	Yes -- and is

'On but optional' means most people stay password-only.

Enforcing 2SV

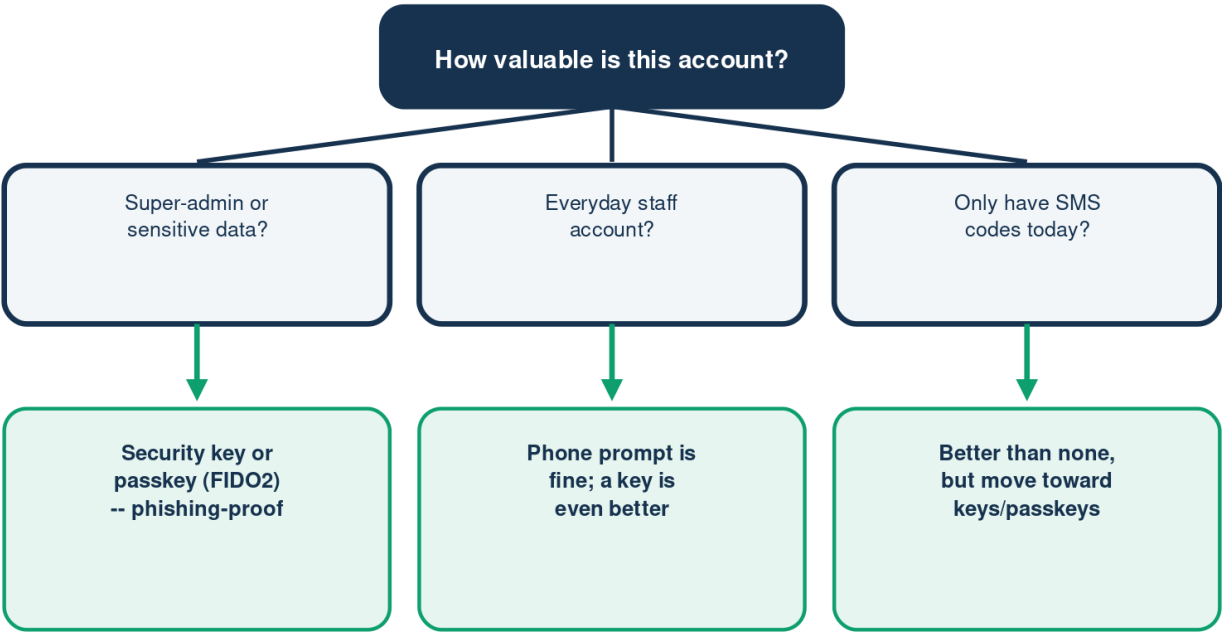
The path as of writing -- confirm in your Admin console



Warn your team first; keep the enrollment window short.

Which Second Step?

Match the strength to the account



Steer your most valuable accounts away from text-message codes.

Illustration - a schematic, not to scale. Your setup may differ.



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will
make it right -- or refund it. No awkwardness,
no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



A Note From Bill

A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech