anoBytes | TECHNOLOGY SOLUTIONS

Set up and secure a new Google Workspace organization

A security baseline for a small business on Google Workspace Business Standard. Covers super admin accounts, 2-Step Verification, application and API access, email authentication and Gmail safety, sharing defaults, and the alert rules, measured against the CIS benchmark.

GOOGLE WORKSPACE · CIS GOOGLE WORKSPACE FOUNDATIONS BENCHMARK v1.4 · ADMIN CONSOLE · HOW-TO GUIDE

Recommendation numbers refer to the CIS Google Workspace Foundations Benchmark v1.4 (4 August 2026). Published 2026-08-14.

12 steps, first sign-in to verification

identity first, then apps, then email, then sharing

71 benchmark recommendations

of the 86 in CIS v1.4; the other 15 are in EXCEPT and DEVIATE

SCOPE

What this guide covers, and what it does not

The CIS Google Workspace Foundations Benchmark v1.4 holds 86 recommendations across five sections: Directory, Apps (Calendar, Drive and Docs, Gmail, Chat, Groups, Sites, and the Marketplace), Security, Reporting, and Rules. This guide works through all 86. It configures 71 of them on a new organization, two of those deliberately short of the benchmark's own value, lists 5 that this edition cannot reach in EXCEPT, and records 10 it declines in DEVIATE. Everything happens in the Google Admin console at `admin.google.com`, in a small number of sittings, before there are users and files to disrupt. Signing up and verifying the domain happen before this guide starts, and moving existing mail in from another provider is its own project.

The edition this guide assumes

Google Workspace Business Standard, the plan most small businesses hold. It includes shared drives, the alert center, endpoint management at the Fundamental tier, and a data region policy. It also draws a hard line: Google Vault, Google session control, data loss prevention rules, Context-Aware Access, and the security dashboard all need a higher edition. EXCEPT lists each one with the editions that carry it, so you can record them as accepted gaps before you hit one mid-setup.

The benchmark is written for Enterprise editions

Every recommendation carries one of two profiles, Enterprise Level 1 or Enterprise Level 2, and the benchmark states it was tested against Google Workspace Enterprise. There is no Business profile. That is why five Level 1 items in this guide are unreachable on Business Standard: they are Level 1 for an edition you do not have. Where a step below applies a Level 2 item, it says so.

Devices are out of scope, by the benchmark's own decision

Section 2 of the benchmark covers the Devices area of the Admin console and contains no recommendations. It says Chrome settings live in the CIS Chrome Benchmark and that mobile and endpoint settings will be covered in a future benchmark. Device management is therefore a separate project, and NEXT points at where it starts.

Why the step order matters

The second super admin account in Step 1 exists before the account recovery rules in Step 2 tighten, because turning off super admin self-recovery makes another super admin the way back in. In email, SPF and DKIM must be publishing for 48 hours before a DMARC record goes up, which is why Step 6 stages the three records rather than pasting them together.

MEASURE There is no security score, so measure these four things

Google Workspace publishes no single posture percentage. The security dashboard and the security health page, which come closest, need Enterprise Standard or Plus, Frontline Standard or Plus, Education Standard or Plus, or Enterprise Essentials Plus. On Business Standard the measuring instruments are the four below, and every one of them comes with the plan.

The security report, for per-user facts

At **Menu > Reporting > User Reports > Security**. One row per person, with 2-Step Verification enrollment and enforcement, security keys registered, external apps connected, and how much each person shares outside the organization. It answers the two questions an assessor asks first: is everyone on 2SV, and who is sharing what. Export it with the date in the filename at the end of Step 12 (CIS 5.1.1.2).

The alert center, for events

At **Menu > Security > Alert center**, included in every edition. Step 10 turns on the rules that feed it and points their email notifications at all super administrators, so the address on those accounts has to be one somebody reads.

Admin log events, for evidence

At **Menu > Reporting > Audit and investigation > Admin log events**. Every change made while working through this guide lands there with who, what, and when. That log plus the dated exports from Step 12 are the record that the baseline was built, which matters when an insurer or a client asks a year later.

The app usage report, monthly

At **Menu > Reporting > User Reports > Apps usage** (CIS 5.1.1.1). One pair of columns earns it a place here: last-used times for Gmail over IMAP and POP. Read them before Step 8 turns those protocols off, to see who was using them, and again afterwards, to see that nothing kept trying.

PREP Before you start

- A **custom domain you control** and sign-in access to its **DNS host** (DNS is the internet's name directory; its records are where Step 6's email authentication lives).
- A **password manager**, already in use, for the two super admin credentials this guide creates.
- **Two hardware security keys per administrator**, or passkeys on two separate devices. Google's own guidance is that an admin enrolls more than one key and stores the spare somewhere safe.
- The **names of your admins**. Decide now who holds a super admin account and which everyday account each of them will keep separate from it.

- A **monitored address for alerts**. Step 10 points alert email at all super administrators, so make sure that reaches a human, and add a shared address if one person leaving would silence it.
- About **three hours** for the console work, plus a **48-hour wait** built into Step 6 between publishing SPF and DKIM and adding DMARC.

MAP The twelve steps at a glance

The waits in Steps 3 and 6 spread this work over more than one sitting. This map shows where each step happens and which steps hold a wait, so the next sitting can start where the last one stopped.

STEP	WHERE	BUILT-IN WAIT
01 Create the super admin accounts	`Directory > Users`	none
02 Set the account recovery rules	`Security > Authentication`	none
03 Enforce 2-Step Verification	`Security > Authentication`	enrollment first; new users get 2 weeks
04 Set the password policy	`Security > Authentication`	none
05 Restrict application and API access	`Security > API controls; the Marketplace`	none
06 Publish SPF, DKIM, and DMARC	`your DNS host; Apps > Gmail`	48 hours of SPF and DKIM before DMARC
07 Turn on the Gmail safety settings	`Apps > Gmail > Safety`	none
08 Harden Gmail access and mail flow	`Apps > Gmail`	tell people before IMAP turns off
09 Set the sharing defaults	`Drive, Calendar, Chat, Groups, Directory, Sites`	none
10 Turn on the alert rules	`Rules`	changes can take 24 hours
11 Decide the AI settings	`Generative AI`	none
12 Verify and record the baseline	`Reporting`	48 hours after Step 6, for the email check

01 Create the super admin accounts properly

The first account is a super administrator, the role that can change anything and read anyone's calendar. The shape of these accounts is the first thing the benchmark tests, and the hardest to change once people are using them.

More than one, and no more than four (CIS 1.1.1)

A single super admin is a single point of failure: lose that account and Google support becomes the only way back into your own organization. More than four adds attack surface without adding resilience. Create a second super admin under **Menu > Directory > Users**, then assign the role through **Admin roles and privileges** on the account. The benchmark is explicit that this should be a new account rather than the role added to an account someone already uses.

Super admin accounts are used only for super admin work (CIS 1.1.2)

Each administrator gets two accounts: the super admin account, and the everyday account they read mail with. Google's own guidance goes further and asks admins to sign out of the super admin account when the task is done, because an open session can be used by anything else that reaches that browser.

Everything routine runs on a delegated role

Google's administrator roles split the console into pieces: Groups Admin, User Management Admin, Help Desk Admin, Services Admin, and custom roles you build. The principle of least privilege applies here: an account gets the access it needs and no more. Each person holds the smallest role that covers their normal work, and the super admin account comes out only for the things that genuinely need it, such as billing, adding a domain, or another admin's recovery. Assign them on the person's own page, under **Admin roles and privileges**.

Write down what account recovery will ask for

If both super admin accounts become unreachable, Google's recovery flow falls back to proving you own the domain, by adding a CNAME or TXT record at your DNS host, which can take up to 24 hours to propagate. Support-assisted recovery then asks for evidence of ownership, including details such as when the account was created and when you last paid. Record those now, alongside sign-in access to the DNS host, in the same place as the emergency passwords.

02 Set the account recovery rules before anyone needs them

Two settings sit under **Menu > Security > Authentication > Account recovery**, and they deserve opposite answers.

SETTING	SET IT TO	CIS	WHY
Super admin account recovery	`Off`	`4.1.2.1`	Self-service recovery on a super admin account means a recovery phone or mailbox can hand over the whole organization. With it off, a super admin who clicks "Forgot password?" is told to contact their administrator, which is the second super admin from Step 1. Level 2. Note the default depends on edition: it is already off on Business Plus, Frontline Standard, Education Standard and Plus, Enterprise Essentials Plus, G Suite Basic, and Cloud Identity Premium, and on for everything else, including Business Standard.
User account recovery	`On`	`4.1.2.2`	For everyone who is not a super admin, self-service recovery removes the password-reset phone call, which is the hardest request for a small business to verify. Self-service recovery leans on a phone number or a secondary email address, which is why it stays limited to ordinary accounts.

Recovery details and backup codes belong in this step

`GOOGLE'S ADMIN ACCOUNT GUIDANCE, AND THE REASON STEP 3 CANNOT LOCK YOU OUT`

Every administrator adds a recovery phone number and a recovery email address to their account, and generates 2-Step Verification backup codes ahead of time, printed and stored somewhere physical. Both matter more once Step 3 enforces 2-Step Verification: an admin whose only security key is in a coat pocket at home needs the codes, and under the strictest 2-Step Verification setting users cannot generate their own codes, so an admin has to issue them. Enroll a second security key per administrator while you are here. Test a full sign-in with the second super admin account twice a year, on a calendar, and read its log afterwards.

03 Enforce 2-Step Verification

2-Step Verification (2SV, Google's name for multifactor authentication, or MFA: a second proof of identity at sign-in beyond the password) is the highest-value setting in this guide. It lives at **Menu > Security > Authentication > 2-Step Verification** and applies to whichever organizational unit you have selected, so put the admin accounts from Step 1 in their own organizational unit and configure that first, then the organization as a whole. Configuration groups can do the same job, but Google notes their availability varies by edition and by setting, so the organizational unit is the route that works everywhere.

SETTING	SET IT TO	CIS	WHY
Allow users to turn on 2-Step Verification	Checked	4.1.1.1	The permission that has to exist before anyone can enroll, and before enforcement means anything.
Enforcement	On, once people have enrolled	4.1.1.3	"On from" a chosen date is the safer route on an organization that already has users; on an empty one, On is fine today. Each person enrolls from the security page of their own Google Account.
New user enrollment period	2 weeks	4.1.1.3	A new hire gets two weeks to register a method before enforcement applies, which stops their first week becoming a support call.
Frequency: allow user to trust device	Unchecked	4.1.1.1	A trusted device stops asking for the second factor, which quietly returns a stolen laptop to password-only access.
Methods	Any except verification codes via text, phone call	4.1.1.1	Phone-based codes fall to SIM swaps and to phishing sites that relay the code in real time. The remaining methods are the authenticator app, prompts, passkeys, and security keys.
Methods, for the admin group	Only security key	4.1.1.2	Level 2, and the one Level 2 item worth taking on a first pass. Google's setting now covers passkeys as well as physical keys, and both resist phishing by design. Set the 2-Step Verification policy suspension grace period at the same time, which the benchmark puts at 1 day, and note that users can no longer generate their own backup codes under this setting.
Security codes	Don't allow users to generate security codes	4.1.1.2	Security codes exist to carry a key-based sign-in onto a platform that cannot talk to the key. Google's own guidance is that keys and passkeys used directly are more secure, so leave codes off until a specific application forces the question.

Google is making 2SV mandatory for administrators

ROLLING OUT GRADUALLY; SUPER ADMINS ARE NOTIFIED ABOUT 90 DAYS AHEAD, OTHER ADMINS ABOUT 60

Google is phasing in required 2-Step Verification for all administrator accounts. Once enforcement reaches an account that has not enrolled, Admin console reminders keep arriving from the seventh day on, mobile access to Workspace apps stops after 15 days, and web access stops after 30. Service accounts are exempt, though the admin account one impersonates has to be enrolled. Google's stated position for an administrator who cannot enable 2SV is to remove their admin rights. Doing it now, with keys in hand and backup codes printed, takes an hour and gets ahead of the rollout.

The Advanced Protection Program (CIS 4.1.3.1, Level 2) is the next step up, at **Menu > Security > Authentication > Advanced Protection Program**. Enrollment is open to users by default. It enforces security keys or passkeys, blocks applications asking for high-risk permissions unless they sit on Google's default trusted list or an admin has trusted them, and turns on enhanced pre-delivery

scanning for those accounts. The Security Sandbox that Google pairs with it needs an Enterprise edition. It suits the two or three accounts that would hurt most if taken: the founder, whoever signs payments, and the super admin accounts.

04 Set the password policy

At **Menu > Security > Authentication > Password management**. Four settings, and one deliberate departure from the benchmark.

- **Enforce strong password:** checked. Google rates strength by entropy (how unpredictable the password is) and rejects passwords found in breach databases or identical to the username (CIS 4.1.5.1).
- **Minimum length:** 14 characters or more. The field accepts 8 to 100.
- **Enforce password policy at next sign-in:** checked, so the rule applies to accounts that already exist as well as to new ones.
- **Allow password reuse:** unchecked, which is already the default. Confirm it.
- **Expiration:** leave it off. This departs from the benchmark, which asks for a 365-day reset frequency.

Why expiration stays off

A DOCUMENTED DEVIATION FROM CIS 4.1.5.1, WITH TWO SOURCES BEHIND IT

Google turns password expiration off by default and says research has shown little positive impact on security. NIST Special Publication (SP) 800-63B-4, the federal guideline for authentication, goes further: verifiers shall not require subscribers to change passwords periodically, and shall force a change only where there is evidence the credential has been compromised. Scheduled expiry also collides with the strong-password rule above: people meet both by adding a digit. The strength here comes from length, the breach check, no reuse, and the 2-Step Verification enforced in Step 3. Google keeps the option for organizations whose contract or regulator names a rotation period, so set 90 or 180 days where one applies. Expiration prompts reach browser sign-ins rather than applications authenticated through OAuth, so it covers less than it appears to. Either way, record the decision and its reason in your exception register, which is how an assessor will read it.

05 Restrict application and API access

Attackers who cannot beat 2-Step Verification ask the user to hand access over instead. A mail about a shared document leads to a real Google sign-in screen for a malicious application. One approval there grants standing access to the mailbox and Drive, and the password never changes hands. These settings move every such grant through an administrator.

SETTING	SET IT TO	CIS	WHERE
Marketplace installs	`Allow users to install and run allowlisted apps`	`3.1.9.1.1`	Apps > Google Workspace Marketplace apps > Apps list > User install settings. The default lets anyone install anything from the Marketplace. The allowlist becomes a short list you maintain, and you can still allow internal apps automatically.
Google services access	`Restricted, for the services that carry your data`	`4.2.1.1`	Security > Access and data control > API controls > Manage Google Services. Restricted means only applications you have marked Trusted, or granted specific data access, can reach that service. Start with Gmail, Drive, and Calendar. Level 2, and the core of this step.
Unconfigured third-party apps	`Blocked until an admin configures them`	`beyond CIS`	Same page. The default lets anyone sign in to any third-party application with their work account. Blocking the unconfigured case is what makes the allowlist above the only route in.

SETTING	SET IT TO	CIS	WHERE
Trust internal apps	Checked	4.2.1.3	Same page. Applications your own organization owns keep working, so the restriction above lands on outside code rather than on your own scripts.
Chat apps	Off	3.1.4.4.1	Apps > Google Workspace > Google Chat > Chat apps. On by default. A chat app is a third party with access to everything said in that space.
Incoming webhooks	Off	3.1.4.4.2	Same pane, on by default. A webhook URL is a password-shaped string that anyone holding it can post through, and they leak into repositories.
Docs add-ons	Covered above	3.1.9.1.1	The Add-Ons switch is gone from the console and v1.4 withdrew the recommendation that used it. Editor add-ons install through the Marketplace, so the allowlist closes this second store too.

Two of this section's recommendations have no setting to change; they ask you to review what is there, and they land in REVIEW: connected third-party applications (CIS 4.2.1.2) and domain-wide delegation (CIS 4.2.1.4), both at Security > Access and data control > API controls. Domain-wide delegation deserves the closer look of the two, because it lets an application act as any user in the organization without that user approving anything.

06 Publish SPF, DKIM, and DMARC for every domain

Three DNS records let the world's mail servers verify mail claiming to be from your domain, and let yours reject imposters. SPF lists the servers allowed to send as your domain, DKIM puts a cryptographic signature on each message, and DMARC tells receivers what to do when both fail. They are CIS 3.1.3.2.2, 3.1.3.2.1, and 3.1.3.2.3, all Level 1. Publish them in this order.

1. SPF, today

One TXT record at the root of each sending domain, with the host set to `@`: `v=spf1 include:_spf.google.com ~all`. If a newsletter tool or your website also sends as the domain, add its include before the ending. Google recommends the soft-fail ending `~all`, which asks receivers to treat anything else as suspect rather than reject it outright, and that pairs correctly with an enforcing DMARC policy later.

2. DKIM, today

At **Apps > Google Workspace > Gmail > Authenticate email**, select the domain and click **Generate new record**. Take the 2048-bit key length where the DNS host supports it, and keep the default selector `google`. Google gives you a TXT record with a host of the form `google._domainkey`; publish it, return, and click **Start authentication**. Signing can take up to 48 hours to come into effect. A new organization is not signing with your domain's key until you do this.

3. DMARC, in monitor mode, at least 48 hours later

Google asks for 48 hours of working SPF and DKIM before DMARC goes up. Then a TXT record at `_dmarc.example.com`: `v=DMARC1; p=none; rua=mailto:dmarc-reports@example.com`. The `p=none` policy changes no delivery. It makes receivers send you aggregate reports at the `rua` address showing who is sending as your domain, which is how you find the invoicing tool nobody mentioned. The reports arrive as XML attachments, roughly daily, and are hard to read raw; a DMARC reporting service turns them into a readable table, and Google recommends using one. After a few weeks of clean reports, move to `p=quarantine`, then to `p=reject; pct=100`. Google calls that staged progression the recommended DMARC rollout, and the aggregate reports are what tell you when each step is safe.

4. The domains that send nothing

Parked domains are spoofing targets precisely because nobody watches them. Give each an SPF record of `v=spf1 -all`, which authorizes no sender at all, and a DMARC record of `v=DMARC1; p=reject;`.

Google's sender requirements set the floor: every sender to personal Gmail addresses needs SPF or DKIM, and senders of 5,000 or more messages a day to those addresses need SPF, DKIM, and DMARC together. Verify from outside with `dig txt _dmarc.example.com` or any public checker, rather than from the console that just told you it worked.

07 Turn on the Gmail safety settings

Eleven checkboxes at **Apps > Google Workspace > Gmail > Safety** carry the largest share of this benchmark's Level 1 email controls. Several are already checked on a new organization, and the ones that are not are named below. What needs changing on all of them is the action, which defaults to leaving the message in the inbox with a warning.

GROUP	TURN ON	CIS	ACTION AND NOTES
Attachments	Encrypted attachments from untrusted senders; attachments with scripts from untrusted senders; anomalous attachment types	3.1.3.4.1.1 to 3.1.3.4.1.3	Set the action to **Move email to spam** on all three. The first two are checked by default, the third is not. An encrypted archive is the standard way to post malware past a scanner, since the scanner cannot read inside it.
Links and external images	Identify links behind shortened URLs; scan linked images; show warning prompt for any click on links to untrusted domains	3.1.3.4.2.1 to 3.1.3.4.2.3	Toggles with no action to choose. They put the real destination in front of the person before the click.
Spoofing and authentication	Domain spoofing by similar domain names; spoofing of employee names; inbound email spoofing your domain; any unauthenticated email; Groups protected from inbound spoofing	3.1.3.4.3.1 to 3.1.3.4.3.5	Set **Move email to spam** on all five. "Protect against any unauthenticated emails" is unchecked by default and is the one that pays off Step 6. Employee-name spoofing is common in invoice fraud, where the display name says the founder and the address does not.
Future settings	Apply future recommended settings automatically	beyond CIS	One checkbox per group. Google adds protections to these panes over time, and this is how a small business without a mail administrator receives them.

Three more settings sit just below, in **Spam, phishing and malware** and **Manage quarantines**:

- **Enhanced pre-delivery message scanning** (CIS 3.1.3.6.1): on. Suspicious messages are held for extra checks before delivery, at the cost of a slight delay.

- **Bypass spam filters for messages received from internal senders** (CIS 3.1.3.6.2): unchecked. A compromised internal account is exactly the sender you want filtered, and spoofed internal mail is common.
- **Notify periodically when messages are quarantined** (CIS 3.1.3.3.1): checked. When nobody reads the quarantine, people start asking for the protections to be turned off instead.

Keep the approved-sender and bypass lists empty. Every entry skips the filtering configured above, and "add our own domain to the approved list" is the classic misconfiguration that turns self-spoofing into guaranteed delivery.

08 Harden Gmail access and mail flow

Six settings under **Apps > Google Workspace > Gmail** close the paths attackers use after taking a mailbox, or instead of taking one.

SETTING	SET IT TO	CIS	WHY
Automatic forwarding	Unchecked	3.1.3.5.2	End User Access. On by default. A silent forward-everything rule is the classic persistence move after a mailbox compromise: the attacker keeps reading long after the password changes.
Per-user outbound gateways	Unchecked	3.1.3.5.3	End User Access. Stops a user routing outbound mail through a server you know nothing about, under a from-address on your domain.
Warn for external recipients	Checked	3.1.3.5.4	End User Access. Gmail marks outside recipients and warns before a reply leaves the organization, which catches the misdirected thread before it becomes a data incident.
Mail delegation	Unchecked	3.1.3.1.1	User Settings. Already unchecked on a new organization, but check it. Delegation lets one person read and send as another, which is worth granting deliberately or not at all.
POP and IMAP access	Unchecked	3.1.3.5.1	End User Access, both available by default. Level 2. Check the app usage report first, and warn people before you change it. Google's own instruction is to tell iPhone and iPad users that Gmail will stop syncing to iOS Mail, and any other client reaching the mailbox over IMAP stops too. The middle path on the same pane is to leave IMAP on and select **Restrict which mail clients users can use (OAuth mail clients only)**, which keeps phones working and shuts out anything that cannot authenticate properly.
Comprehensive mail storage	Checked	3.1.3.7.1	Compliance. Puts a copy of everything sent by other Google services into the sender's mailbox, so the archive is complete. Its full value arrives with Google Vault, which needs Business Plus; on Business Standard it still makes the mailbox itself a complete record.

Why secure transport (TLS) compliance stays off

A DOCUMENTED DEVIATION FROM CIS 3.1.3.7.2, ON GOOGLE'S OWN WARNING

The benchmark asks for the Secure transport (TLS) compliance setting to be applied to all inbound and all outbound messages. Google's documentation is explicit about what that does: outbound messages to a server without TLS bounce back with a non-delivery report, and inbound messages arriving over a non-TLS connection are rejected without anyone in your organization being told, though the outside sender does get a non-delivery report. For a small business that mails clients, suppliers, and the occasional government office, that is lost mail in both directions, and nothing on your side flags the inbound half. Gmail already attempts TLS on every connection by default. Where a specific partner requires guaranteed encryption, add that partner's domain to the setting by name, which is what the address-list option is for. Leaving it unset organization-wide is the safer configuration, and it belongs in the exception register with this reason.

The benchmark's less secure apps recommendation was overtaken by Google, and v1.4 has withdrawn it: Workspace accounts stopped supporting sign-in by username and password from third-party apps and devices on 1 May 2025, and the enforcement setting was removed from the Admin console. There is nothing to configure. What remains is the practical consequence, in HELP: the old scanner or line-of-business app that used a password now needs OAuth, the SMTP relay service, or an app password.

09 Set the sharing and collaboration defaults

Sharing settings trade security against everyday convenience, so decide them while nothing is shared yet. The stance below keeps outside collaboration working, and makes each grant a deliberate act with a name attached to it.

SETTING	SET IT TO	CIS	WHERE
Sharing outside the organization	On, with the warning checked	3.1.2.1.1.1	Drive and Docs > Sharing settings > Sharing options. External sharing keeps working, and the person doing it gets told they are doing it.
Publishing to the web	Unchecked	3.1.2.1.1.2	Same pane, checked by default. This is the setting behind every "confidential document found by search engine" story.
Access Checker	Recipients only	3.1.2.1.1.5	Same pane. When someone pastes a Drive link into Gmail, Google offers to fix the permissions. This limits that offer to the named recipients rather than to anyone with the link.
Distributing content outside the organization	Only users in your organization	3.1.2.1.1.6	Same pane, set to Anyone by default. Stops an outside collaborator moving your files into a shared drive that another company owns.
Shared drive creation	Allowed for users	3.1.2.1.2.1	Same page, Shared drive creation. v1.4 hands this decision to you, tied to DLP rules this edition cannot run. Its remediation leaves creation available, and so does this guide: files in a shared drive belong to the organization and survive the person leaving, while files in someone's My Drive do not.
Managers overriding shared drive settings	Unchecked	3.1.2.1.2.2	Same pane, checked by default. Sharing rules stay an administrator's decision instead of each drive manager's.
Non-members added to shared drive files	Unchecked	3.1.2.1.2.3	Same pane, checked by default. Membership becomes the access boundary, which is the only way a shared drive stays reviewable.

SETTING	SET IT TO	CIS	WHERE
Viewers and commenters downloading, printing, copying	Unchecked	3.1.2.1.2.4	Same pane. Level 2. Someone with view or comment access can still read the file but cannot take a copy of it.
Calendar external sharing, primary and secondary	Only free/busy information	3.1.1.1.1, 3.1.1.2.1	Calendar > Sharing settings, and General settings for secondary calendars. Primary calendars already default to free/busy; secondary calendars default to sharing all information. A full calendar leaks names, clients, and travel.
External invitation warnings	Checked	3.1.1.1.3	Calendar > Sharing settings. A prompt before an outside guest joins an internal meeting.
Chat external file sharing	No files	3.1.4.1.1	Google Chat > Chat file sharing, set to allow all files by default. Files leave through Drive, where the sharing rules above apply and the audit trail exists.
Chat externally, and external spaces	Allowlisted domains only	3.1.4.2.1, 3.1.4.3.1	Google Chat > External chat settings, and External spaces & group direct messages. Chatting with named partner domains stays available; a stranger opening a direct message does not. Both cost list upkeep, which is the trade.
Groups: access from outside	Private	3.1.6.1	Groups for Business > Sharing options. Already private by default; confirm it. Public group archives have leaked internal threads for years.
Groups: who can create groups	Only organization admins	3.1.6.2	Groups for Business > Creating groups. Anyone can create one by default. Also clear the two boxes that let group owners admit external members or accept outside mail.
Groups: default view permission	All group members	3.1.6.3	Groups for Business > Sharing options, set to all organization users by default. Other group defaults follow this one.
External directory sharing	Authenticated user basic profile fields	1.2.1.1	Directory > Directory settings > Sharing settings. The wider option shares organization data as well. This one limits what the People, Contacts, and CardDAV APIs hand to third-party applications, down to the signed-in person's own name, photo, and email address. The wider setting hands out the whole staff list, which is what a phishing campaign needs.
Google Sites	Off for everyone	3.1.7.1	Apps > Google Workspace > Sites. On by default, rarely used deliberately, and capable of publishing internal content to the web. Turn it back on for a named group if a team needs it.
External Google Groups	Off for everyone	3.1.8.1	Apps > Additional Google services > Google Groups. A legacy service that only controls whether work accounts can join groups outside your organization. It has no effect on your own groups.

One default is already correct, so check it and leave it alone: newly created Drive files default to Restricted general access, so a file reaches nobody until its owner shares it.

10 Turn on the alert rules

Google ships more than fifty system-defined rules at **Menu > Rules**, and the benchmark names eight that matter for a small organization (CIS 6.1 through 6.8). Six of the eight are already active on a new organization. The two that are off both catch an attacker consolidating a foothold.

RULE	WHAT IT CATCHES, AND WHAT TO DO	CIS
User granted Admin privilege	Inactive by default. Turn it on at Medium severity. Granting itself an admin role is how a compromised account becomes a compromised organization, and on a small team every legitimate occurrence is one you already know about.	6.4
User's password changed	Inactive by default. Turn it on at Medium severity. Noisy in a large organization; on a team of six, a password change nobody made is a phone call.	6.1
Government-backed attacks	Active. Confirm it is on and set to High. Google sends this when it believes a state-sponsored actor is targeting one of your users.	6.2
User suspended due to suspicious activity	Active. High severity. Google has already acted; the alert tells you why one of your people cannot sign in.	6.3
Suspicious programmatic login, and suspicious login	Both active. Sign-ins that look like a script rather than a person, and sign-ins that do not match the account's usual pattern.	6.5, 6.6
Leaked password	Active. Google has seen the account's password in a breach corpus. Reset it and check what else used it.	6.7
Gmail potential employee spoofing	Active. Pairs with the employee-name spoofing protection in Step 7.	6.8

For each rule, open it, edit the Actions pane, select **Send to alert center**, set the severity, and enable email notifications. The recipient list preselects all super administrators; add the monitored address from PREP so a single departure cannot silence them.

11 Decide the AI settings before your users do

Gemini features are included in Google Workspace subscriptions and are on by default. The benchmark makes no recommendation about them, so this decision is yours to make without one. Make it in the same sitting as the rest.

Where the controls are

At **Menu > Generative AI > Gemini for Workspace**, under **Feature access**, each service can be turned on or off for the whole organization or for an organizational unit. The list includes the Gemini app, note-taking in meetings, and smart features across Workspace.

The decision to make, in one sitting

Decide which features are on, for whom, and what people may put into them. A tool with access to Drive and Gmail inherits whatever the person can already reach, so the sharing work in Step 9 is what bounds it. Write the answer down before anyone asks, because the alternative is people finding their own tools, which is the harder problem. Our AI Acceptable Use Policy template covers the written half.

12 Verify and record the baseline

Read the settings back instead of trusting the screens you clicked through, and keep the read-back. Google publishes no command-line tool for the Admin console, so the manual version is a short list of console pages and two exports.

- **Security report** at **Reporting > User Reports > Security**: confirm every account shows 2-Step Verification enrolled and enforced, that admins show a security key, that external application counts are what you expect, and that external share counts are near zero on a new organization. Export to CSV with the date in the filename (CIS 5.1.1.2).
- **Apps usage report** at **Reporting > User Reports > Apps usage**: confirm the IMAP and POP last-used columns stay empty after Step 8 (CIS 5.1.1.1).
- **Admin log events** at **Reporting > Audit and investigation > Admin log events**: filter to the setup window and confirm your changes are recorded. This is the log that proves when the baseline was built.
- **Email authentication**: check SPF, DKIM, and DMARC from outside with `dig` or a public checker, 48 hours after Step 6.
- **The two rules from Step 10**: confirm both show an Alert status of On in the Rules list. Google says changes to these rules can take up to 24 hours to take effect, so check again the next day if it has not appeared.

There is a machine-readable version of this check. The Google Workspace Policy API reached general availability on 20 February 2025 and is open to all Workspace customers; a super admin can call it to read service-level settings, including Gmail, Calendar, and 2-Step Verification, which turns the quarterly drift check into a scheduled export. It is read only for these settings today, so it audits the baseline but cannot build one.

Repeat the two exports quarterly. Comparing two dated CSVs is the drift check, and it takes minutes. Those exports, the admin log, and a written note of the deviations in DEVIATE and EXCEPT are what an insurer or an assessor asks for, and they are much easier to produce in the week the organization was built than a year afterwards.

NEXT When you enroll devices

Device management is the follow-on project, and the benchmark leaves it out on purpose: its Devices section holds no recommendations. It points at the CIS Chrome Benchmark for browser settings and at a future benchmark for mobile and endpoint settings. Two things are worth knowing before you start.

- **Basic mobile management is already on.** Google turns it on by default, so a phone registers as soon as someone adds their work account. The settings are at **Menu > Devices > Mobile & endpoints > Settings > Universal**. Set the screen-lock and encryption requirements there before the first phone appears.
- **Business Standard carries the Fundamental endpoint tier.** Advanced management, which adds iOS app management and device audit logs, needs Business Plus. That is the practical reason to weigh the upgrade, alongside Google Vault.

Our Remote Work & Mobile Device Policy template pairs with that project, and the offline-access deviations in DEVIATE become worth revisiting once devices are managed.

SMALL A company of one or two

The second super admin account is still the rule

A solo founder holds one working super admin account plus a second created for the function rather than for a person, which satisfies CIS 1.1.1 and 1.1.2 without a second person on the team. Keep its security key and printed backup codes somewhere physical and separate from the laptop, so a lost key does not turn into a support case about your own domain.

Alerts need somewhere to land

A solo founder has nobody else to notice a compromised account, so the alert rules in Step 10 and the quarantine notifications in Step 7 have to reach a mailbox that gets read daily. Point them at the everyday account, since the super admin account is one you are signed out of by Step 1.

Write the deviations down

Whatever you skip, record it with the reason and a review date. An assessor reads a dated entry with a reason as a decision, and an undocumented gap as a finding. DEVIATE and EXCEPT below are already written in that shape; the exception register template on our resources page holds the fields.

HELP What breaks, and the way back

- **Nobody can sign in to a super admin account**

  Use the second super admin account from Step 1 to reset the first. If both are unreachable, recovery falls back to proving you own the domain with a DNS record, then to Google support with the ownership details from Step 1, which is why they were written down before they were needed. This is also the reason Step 2 turns super admin self-recovery off rather than relying on a recovery phone.

- **An administrator lost their security key**

  Under the "Only security key" method from Step 3, users cannot generate their own backup codes, so an admin issues them at **Directory > Users**, the person's page, then **Security > 2-step verification > Get backup verification codes**. Only a super admin can do this for another administrator's account. The alternative is moving that account to an organizational unit with a broader method until the replacement key arrives. Enroll the replacement key and revoke the lost one the same day. The spare key and printed codes from Step 2 exist to make this a ten-minute job.

- **A new app cannot connect, or Sign in with Google is refused**

  This is Step 5 working: unconfigured third-party applications are blocked, and the restricted Google services open only to applications you have configured. At **Security > Access and data control > API controls**, configure the app and choose what it gets: Trusted, Limited to the unrestricted services, or access to specific data only. A Marketplace app goes on the Step 5 allowlist instead. Grant the narrowest level that lets the app work, and record who asked for it.

- **The printer, scanner, or old line-of-business app stopped emailing**

  This one is Google's doing. Workspace accounts stopped accepting username-and-password sign-in from third-party apps and devices on 1 May 2025, and the setting that allowed it is gone from the Admin console. The supported answers are a device or application that speaks OAuth, Google's SMTP relay service configured for that sender, or an app password for the device's account, which needs 2-Step Verification turned on first. An app password then signs in without a second factor, so treat it as the fallback.

- **Mail to a partner started bouncing**

  If you enabled Secure transport (TLS) compliance despite the deviation in Step 8, that is where to look first: outbound mail to a server without TLS bounces, and inbound mail over a plain connection is rejected without any notice reaching you. Otherwise check the DMARC policy from Step 6, since moving to `p=reject` before every legitimate sender appears in the aggregate reports will drop your own newsletters or invoicing mail.

- **A legitimate forward or external share no longer works**

  Automatic forwarding is off by design (Step 8) and web publishing is off by design (Step 9). The supported answers are a group or delegated access instead of a forwarding rule, and a named share instead of a published link. Grant the narrow version rather than reopening the broad setting.

- **Offboarding is more than deleting the account**
  Suspend the account first so sessions and tokens stop, transfer Drive and Calendar ownership, remove any admin roles, check for forwarding rules and connected third-party applications the person authorized, transfer any groups they owned, and only then delete. Deleting first destroys the data you were about to transfer.

REVIEW The checks that need a recurring look

These cannot be finished in the setup sitting. They are what keeps the baseline honest as the organization fills up. Put them on a calendar now and name an owner for each.

WHAT TO REVIEW	WHERE	HOW OFTEN	CIS
Connected third-party applications	Security > Access and data control > API controls	Monthly is realistic for a small business, with anything new investigated the same day. Each entry should have a user and a reason.	4.2.1.2
Domain-wide delegation	Same page, Manage domain wide delegation	Monthly, and read every entry. A delegated application can act as any user in the organization without that user approving anything.	4.2.1.4
Security report	Reporting > User Reports > Security	Monthly: everyone still enrolled and enforced on 2SV, admins still on security keys, external shares still explainable.	5.1.1.2
Apps usage report	Reporting > User Reports > Apps usage	Monthly, focused on the IMAP and POP columns and on storage outliers.	5.1.1.1
Super admin count and delegated roles	Directory > Users, filtered to admins	Quarterly: still two to four super admins, still separate from everyday accounts, still the smallest role that covers the work.	1.1.1, 1.1.2
Alert center queue	Security > Alert center	Weekly at first, so the queue stays small enough that people keep reading it.	6.1 to 6.8
DMARC aggregate reports	The rua mailbox from Step 6	Weekly until the policy reaches p=reject, then monthly.	3.1.3.2.3
Marketplace allowlist	Apps > Google Workspace Marketplace apps	Quarterly: every allowlisted app still has an owner and a purpose.	3.1.9.1.1
Quarantine and spam verdicts	Apps > Google Workspace > Gmail > Manage quarantines	Weekly at first. False positives caught early keep people from asking for approved-sender entries later.	3.1.3.3.1
Configuration drift	The Step 12 exports, compared against the originals	Quarterly. The work is already written down; the check is whether the new output still matches.	beyond CIS

The benchmark asks for a weekly look at the connected applications, the delegation list, and the two user reports; the monthly rhythm above is sized for a small team, so record that difference with the other deviations.

EXCEPT Five recommendations Business Standard cannot reach

These need a higher edition. Log them as accepted gaps with the edition as the reason, and revisit them if the organization grows.

- **Context-Aware Access** (4.2.2.1, blocking sign-in from unapproved countries): Frontline Standard and Plus, Enterprise Standard and Plus, Education Standard and Plus, Enterprise Essentials Plus, or Cloud Identity Premium.
- **Data loss prevention (DLP) rules for Drive** (4.2.3.1): Frontline Standard and Plus, Enterprise Standard and Plus, Education Fundamentals, Standard and Plus, or Enterprise Essentials Plus. Business Standard can run the Data Protection Insights report, which scans and shows you what sensitive content exists, so use that to size the gap even though you cannot write rules against it.
- **Google session control** (4.2.4.1, shortening the 14-day web session): Business Plus, Frontline Standard and Plus, Enterprise Standard and Plus, Education Fundamentals, Standard and Plus, Enterprise Essentials Plus, G Suite Business, or Cloud Identity Premium. Google Cloud session control (4.2.5.1, Level 2) is available on Business Standard, at Security > Access and data control. It governs reauthentication for the Google Cloud console, the gcloud command line, and applications asking for Google Cloud permissions, with a frequency between 1 and 24 hours; the benchmark sets 16. Configure that and record the Workspace session length as the gap.
- **The security dashboard** (4.3.1) and **the security health page** (4.3.2): Enterprise Standard and Plus, Frontline Standard and Plus, Education Standard and Plus, or Enterprise Essentials Plus. The reports in MEASURE are the substitute.

Two more edition boundaries shape the plan without being benchmark items: Google Vault, which is where retention and eDiscovery live, needs Business Plus, and client-side encryption is not available on any Business edition. LIMITS covers what that means for data recovery.

DEVIATE Ten recommendations this guide declines, with reasons

A benchmark written for Google Workspace Enterprise assumes managed devices and a dedicated administrator. These ten are defensible there and costly here. Record each one in the exception register with the reason and a review date, and revisit them once devices are managed.

RECOMMENDATION	WHY THIS GUIDE DECLINES IT	CIS
Disable offline documents, Drive for desktop, and Gmail web offline	All three assume device policies exist to control local copies. Without endpoint management, turning them off removes offline working from a small team and moves files to personal copies instead. Revisit after the device project in NEXT.	3.1.2.2.1, 3.1.2.3.1, 3.1.3.1.2
Restrict internal calendar sharing to free/busy, primary and secondary	Level 2. A small team schedules by seeing each other's calendars. External sharing is already restricted in Step 9, which is where the exposure was.	3.1.1.1.2, 3.1.1.2.2
Disable Calendar web offline	Level 2, and the same offline-access argument as above.	3.1.1.3.1
Control document sharing by domain allowlist, and warn on it	Level 2. An allowlist model means every new client needs an admin before a file can reach them. Step 9 keeps sharing on with warnings, which suits a business whose clients change.	3.1.2.1.1.3, 3.1.2.1.1.4
Disable internal file sharing in Chat	Level 2. External Chat file sharing is off in Step 9; blocking internal sharing too pushes people to personal channels.	3.1.4.1.2
Enforce post-SSO login challenges	Level 2, and it applies to organizations using a third-party single sign-on (SSO: one sign-in across many services) provider. This baseline signs in to Google directly, so there is no post-SSO step to challenge.	4.1.4.1

Two further departures are covered where they arise rather than repeated here: password expiration stays off (Step 4, against CIS 4.1.5.1's 365-day value), and Secure transport (TLS) compliance stays unset organization-wide (Step 8, against CIS 3.1.3.7.2). Both carry a source and a reason at the point of the decision.

LIMITS What this setup does not protect against

- **A compromised endpoint.** Everything here governs the cloud side. A keylogged laptop signs in with a valid passkey, which is why the device work in NEXT is the follow-on project.
- **A user who approves the wrong thing.** Step 5 moves application grants to an administrator, which makes that administrator the target. Read consent requests as skeptically as you read invoices with changed bank details.
- **An insider with legitimate access.** The admin log investigates them afterwards and the sharing defaults limit what can leave casually. Neither prevents deliberate exfiltration by someone doing their job's normal actions.
- **Data loss and retention.** Business Standard has no Google Vault, so there is no retention policy, no legal hold, and no eDiscovery. Deleted mail and files follow the ordinary trash rules and then they are gone. Google's Data Export tool can still take a full copy of everyone's data: a super admin whose account is at least 30 days old, with 2-Step Verification on, can run it, and the export takes days and waits in a temporary bucket for 60 days, so it is a periodic snapshot rather than a backup. If your business has a retention obligation, that is the reason to move to Business Plus, and our BC/DR plan template covers the rest.
- **Losing the organization itself.** A lapsed subscription, an expired domain, or a compromised registrar account all sit outside Google Workspace. Keep the registrar and DNS host on the vendor register with their own multifactor authentication, and keep the recovery details from Step 1 where a fire at one site cannot take both copies.

DONE What you achieved

- Two to four super admin accounts, separate from everyday accounts, signed out between tasks, with delegated roles carrying the routine work and the recovery paperwork written down.
- 2-Step Verification enforced on everyone, security keys or passkeys required of administrators, device trust off, and phone-based codes ruled out ahead of Google's own mandatory enforcement.
- Application access that flows through an administrator: an allowlisted Marketplace that covers editor add-ons too, restricted Google services, and unconfigured third-party sign-ins, chat apps, and webhooks all turned off.
- Email that proves its origin with SPF, DKIM, and DMARC on every domain including the parked ones, eleven Gmail safety protections set to move threats out of the inbox rather than label them, and no path for a compromised mailbox to forward itself out.
- Sharing that stays deliberate: no web publishing, no anonymous distribution outside the organization, shared drives bounded by membership, calendars showing free and busy, chat limited to named domains, and groups closed by default.
- Alerting that reaches a person, with the two rules Google leaves off switched on, plus dated exports and an admin log that show when the baseline was built.

Where that leaves you against the benchmark

THE LINE TO PUT IN FRONT OF AN ASSESSOR OR INSURER

Seventy-one of the benchmark's 86 recommendations are addressed in the console, sixty-nine of them at the benchmark's own value; the remaining two depart from it deliberately, in Steps 4 and 8, each carrying its source at the point of the decision. Five need a higher Google Workspace edition and are listed in EXCEPT with the editions that carry them. Ten are declined with reasons in DEVIATE. Three items stay conditional until you close them: DMARC only enforces once you move it past `p=none`, 2-Step Verification enforcement counts only after people have enrolled, and the Marketplace allowlist is a list somebody has to keep. Write those, EXCEPT, and DEVIATE into the exception register, dated, and you have both the configuration and the reasoning that goes with it.

REF References

CIS Google Workspace Foundations Benchmark v1.4, 4 August 2026 · cisecurity.org/cis-benchmarks

NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management, July 2025 · pages.nist.gov/800-63-4

The Policy API is now generally available, 20 February 2025 · workspaceupdates.googleblog.com/2025/02/policy-api-general-availability.html

Winding down Google Sync and less secure apps support, updated 29 April 2025 with the final date of 1 May 2025 · workspaceupdates.googleblog.com/2023/09/winding-down-google-sync-and-less-secure-apps-support.html

The pages below are Google's admin documentation, all under knowledge.workspace.google.com:

Security checklist for small businesses (1-100 users) · /admin/security/security-checklist-for-small-businesses-1-100-users

Security best practices for administrator accounts · /admin/users/security-best-practices-for-administrator-accounts

About 2SV enforcement for admins, and Deploy 2-Step Verification · /admin/security/about-2sv-enforcement-for-admins

Recovering administrator access to your account · /admin/users/recovering-administrator-access-to-your-account

Allow super administrators to recover their password · /admin/users/allow-super-administrators-to-recover-their-password

Enforce and monitor password requirements for users · /admin/users/enforce-and-monitor-password-requirements-for-users

Protect users with the Advanced Protection Program · /admin/security/protect-users-with-the-advanced-protection-program

Control which apps access Google Workspace data · /admin/apps/control-which-apps-access-google-workspace-data

Control access to less secure apps (withdrawn 1 May 2025) · /admin/apps/control-access-to-less-secure-apps

Set up SPF, Set up DKIM, and Set up DMARC · /admin/security/set-up-dmarc

Advanced phishing and malware protection · /admin/gmail/advanced/advanced-phishing-and-malware-protection

Send email over a secure TLS connection · /admin/gmail/advanced/send-email-over-a-secure-tls-connection

Turn POP and IMAP on or off for users · /admin/sync/turn-pop-and-imap-on-or-off-for-users

Let third-party apps access Directory data · /admin/users/let-third-party-apps-access-directory-data

View and edit system-defined rules · /admin/reports/view-and-edit-system-defined-rules

Compare Business editions · /admin/getting-started/editions/compare-business-editions