The Practitioner's Guide to Google Workspace Security

5 essential steps to harden your security posture

Google Workspace offers powerful built-in security features, but misconfigurations or over-looked security settings can leave any organization vulnerable.

This guide provides a deep dive Google Workspace settings related to these 5 key areas that can help you ensure robust security:

Multi-Factor Authentication (MFA) enforcement

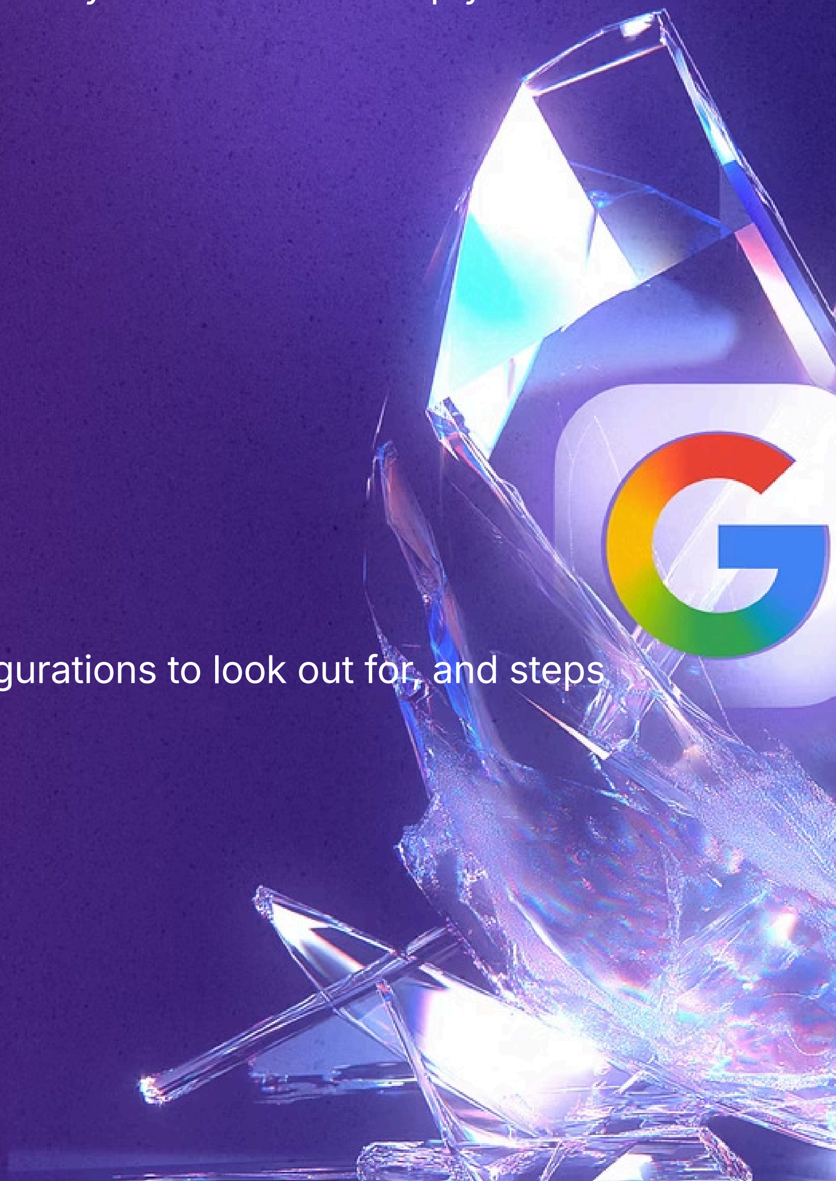
Google Drive public sharing settings

Advanced Protection Program (APP) for privileged accounts

Password strength policies

Google groups access settings

For each recommendation, we'll cover why it's important, common misconfigurations to look out for, and steps to apply secure settings.



1. Multi-Factor Authentication (MFA) enforcement

Why it matters:

Enforcing multi-factor authentication (MFA) is one of the most effective ways to prevent account breaches. MFA adds an extra layer beyond just a password, thwarting many attacks like phishing and password guessing. According to industry research, stolen credential use is the most common initial action in data breaches. The United States Cybersecurity and Infrastructure Security Agency (CISA) reports that **accounts with MFA enabled are 99% less likely to be hacked**. This underscores that if MFA is not enabled, accounts are dramatically more likely to be compromised. Google Workspace admins must ensure MFA is enabled for all users to reduce the chance of account takeover.

Common misconfigurations:

Some organizations enable MFA but don't fully enforce it for all users. In Google Workspace, it's possible for a user to register a second-factor method yet still be allowed to log in with just a password if enforcement isn't correctly configured.

Another mistake is leaving a long grace period for enrollment or having "optional" MFA, which results in many users never actually turning it on. Relying on weaker second-factor methods (like SMS texts or voice calls) can also be a mistake—these are better than nothing, but they are more susceptible to SIM-swapping and social engineering compared to stronger methods like authenticator apps or security keys.

Best practices and recommendations:

Enforce MFA for every account, especially admin accounts, with no exceptions for day-to-day use. Key recommendations include:

Turn on MFA enforcement in Admin Console

In Google's Admin Console, go to Security > Authentication > 2-Step Verification and enable enforcement for all users (after a short enrollment period).

Use strong MFA factors

Configure allowed second-step methods to exclude weaker factors. Google Workspace lets you restrict MFA methods—for instance, you can disallow SMS and voice codes (which are vulnerable) and allow only stronger methods like authenticator apps or security keys. The recommended setting is "Any except verification codes via text or phone call," which forces users to adopt more secure app-based codes or keys Even better, require security keys for your most sensitive accounts, as this provides the highest phishing resistance (though it may be impractical for all users).

Educate users

Provide guidance and training so users know how to use MFA (e.g., using Google Authenticator or phone prompts) and why it's required. Sometimes users resist changes, but emphasizing that this is a simple step that prevents the vast majority of attacks can help get buy-in.

2. Google Drive public sharing risks

Why it matters:

Google Drive makes file sharing easy—sometimes too easy. One common misconfiguration is allowing files or folders to be shared with "Anyone with the link." This public sharing option means no authentication is required to view the file; if someone obtains the link, they can access the content. While convenient for non-sensitive documents, it can be disastrous if applied to sensitive data.

Risks of public sharing:

If files are shared publicly, data leaks can occur. Sensitive documents could be indexed by search engines or discovered by malicious actors.

Common misconfigurations:

The most common mistake is using "Anyone with the link can view" as a sharing setting for files that should be internal. Often, employees select this out of convenience—they're not sure who will need access or they want to avoid dealing with permission requests.

How to secure Google Drive sharing:

IT admins should take a proactive stance on Google Drive sharing settings to prevent accidental data exposure. Here are some best practices:

Restrict or disable "Anyone with the link" sharing

In the Admin Console, you can adjust Drive sharing settings for the organization. It's highly advisable to disable the "Anyone with the link" option entirely for internal users. Most organizations rarely need truly public links. Instead, prefer options that require sign-in. If completely disabling isn't feasible (perhaps your marketing team needs to share documents publicly), consider an approach where only a certain sub-organization or group has the ability to create public links, and even then, enforce an approval process. At minimum, make "Off (restricted)" the default setting for file links so that new files aren't accidentally shared openly.

Monitor shared files

Regularly audit what files are being shared externally or publicly. Google's Security Dashboard provides a File exposure report that shows how many files are shared externally or publicly across your domain. Periodic audits (e.g., monthly or quarterly) will help catch misconfigurations early.

Educate and enforce least privilege in sharing

Train users on secure file sharing practices. They should understand the difference between "Share with specific people" vs. "Anyone with the link." Encourage a culture where employees default to the least permissive access—share with individual users or groups who need the file, rather than broad links. As a guideline, never use "Anyone with the link" for sensitive or internal data.

Consequences of misconfiguration:

The fallout from public sharing misconfigurations can be severe. Exposed internal files can lead to data breaches, regulatory compliance violations (imagine if personal data or health information is accidentally leaked), and reputational damage.

3. Advanced Protection Program (APP) for high-privilege accounts

Why use APP for admins:

Google's Advanced Protection Program (APP) is a free offering that provides Google's strongest account security settings—originally designed to protect individuals at high risk (like journalists or politicians) and now available for enterprise users. In a Workspace context, high-privilege accounts (such as super administrators or executives with access to sensitive data) should enroll in APP to benefit from its elevated protections. High-value accounts are often targeted by attackers, and the APP is specifically built to guard against targeted attacks, phishing, and account hijacking.

Google itself recommends enrolling users like IT admins, C-level executives, and others in sensitive roles in the Advanced Protection Program.

These accounts have the **"keys to the kingdom,"** so an attacker who compromises an admin can do far more damage than a regular user compromise. Thus, locking down admin accounts with APP is a smart move to drastically reduce risk.

What APP does:

The Advanced Protection Program enforces a bundle of enhanced security measures on enrolled accounts. Notable features include:

Strongest Two-Factor Authentication

APP requires the use of security keys (or passkeys) for 2-Step Verification, rather than less secure methods. Enrolled users must authenticate with a physical FIDO2 security key or equivalent, which provides phishing-resistant MFA. This stops most account takeover attempts dead in their tracks, as an attacker would need the physical key to breach the account. (Google recently enabled support for phone-based passkeys as well, offering strong security without a separate hardware key.)

Restricted third-party access

APP blocks access to your Google data by untrusted third-party apps. In practice, this means if an attacker tries to use a malicious OAuth app to trick an admin into granting access (a common phishing technique), APP will automatically prevent it unless the app is explicitly whitelisted by your organization. Only Google's own apps and trusted third-party apps can integrate with an APP-enrolled account

Enhanced scanning for threats

APP accounts get extra scrutiny on incoming emails, attachments, and downloads. Google applies more aggressive phishing and malware checks for users in APP. For example, an admin enrolled in APP might have Chrome block certain risky file types by default and have Gmail perform enhanced scans on messages, adding another layer of defense.

Tightened account recovery

To prevent attackers from using the account recovery process as a backdoor, APP makes account recovery more arduous. If an admin loses their security keys or forgets their password, the recovery requires additional verification steps and time. This mitigates the risk of someone hijacking the account by, say, impersonating the user to Google support.

4. Password strength policies

Why it matters:

Despite the push towards MFA and even passwordless technologies, strong passwords remain a fundamental security requirement. They are the first line of defense for accounts. A weak or compromised password can render other security measures ineffective. Users often choose easy-to-remember passwords that are unfortunately easy to guess. Attackers exploit this by using password spraying (trying common passwords across many accounts) and credential stuffing (using passwords leaked from other breaches). Enforcing a strong password policy in Google Workspace ensures that users create passwords that meet complexity and length requirements, making these attacks much harder to succeed. It also helps meet compliance standards that often mandate specific password controls.

Common misconfigurations:

A typical misconfiguration is simply not enabling Google Workspace's password policies—by default, some advanced password requirements are off. For instance, the "Enforce strong password" setting is OFF by default, meaning users could set very simple passwords if not changed by an admin.

Similarly, not setting a minimum password length (or leaving it at a low number like 4 or 6) is a mistake; industry practice is to require a reasonably long password (8 at absolute minimum, with many recommending 12+ characters for better security). Allowing password reuse is another misstep—if users can recycle their last password or switch between a couple of favorites, it undermines the intent of password changes.

Another potential issue is not forcing a policy update for existing passwords. Google Workspace lets you enforce new rules either at next password change or at next login. If you don't choose "at next sign-in," a user with a weak password could technically keep that password until they decide to change it on their own. Lastly, some organizations overdo one aspect (like frequent forced changes) but neglect others (like complexity), which can lead to users writing passwords down or using predictable patterns.

Google Workspace password policy settings:

As an admin, you should configure the following in Security > Password Management for your domain to enforce strong authentication:

Enforce strong passwords

Enable the option to require a strong password for all users. Google defines a strong password as one that mixes letters, numbers, and symbols (and is not on Google's list of common weak passwords). With this setting on, if a user's password is weak or common, Google will force them to change it.

Minimum password length

Set a minimum length requirement. Eight characters is the bare minimum recommended, but consider higher for better security (such as 10 or 12). Keep user experience in mind—extremely long minimums might cause pushback—but note that password length significantly increases strength. The Admin Console allows you to set a length; a common policy is minimum 8 or 10 characters.

Prevent password reuse

Make sure "Allow password reuse" is unchecked (it's unchecked by default, which means reuse is not allowed). This ensures users cannot cycle through a small set of favorite passwords. Typically, Google will remember a certain number of previous passwords (the exact number isn't shown, but you can assume at least last 5) and prevent the user from reusing them when changing to a new password.

Password expiration

Decide on a password expiration interval if required. Google Workspace allows you to expire passwords after a set number of days. Many organizations choose 90 days (the classic recommendation). Google's own guidance is that if you're unsure about forcing rotation, it's acceptable to leave it at "Never" (no expiration) because overly frequent changes can lead to worse passwords or users writing them down.

Apply policy to existing users

In the Password Management settings, there's an option to enforce the policy at next sign-in (as opposed to next password change). It's wise to check this when rolling out a new policy. That way, any user currently with a weak or non-compliant password will be forced to set a new one the very next time they log in, rather than waiting until they decide to change it on their own. This closes any loopholes for accounts that haven't changed their password in a long time.

Different policies for privileged users

Consider creating stricter password policies for admins or highly privileged accounts. Google Workspace allows different settings per organizational unit (OU).

5. Google Groups with unrestricted access

Why it matters:

Google Groups is a service within Workspace often used for mailing lists, team discussions, and permission management. However, misconfiguring Google Groups settings can inadvertently expose confidential information. The consequences of mismanaging Google Groups can be **severe data leakage**.

Common misconfigurations:

In Google Groups settings, you can control who can view topics, who can post, and who can join the group. An "unrestricted" group might allow anyone on the internet to join or view messages, or allow outside (external) members to be part of the group freely. Some organizations unintentionally leave group discussions open to the public or to the entire organization when they were meant to be confidential.

For example, if a group's access is set to "Public on the internet" for viewing, then all the messages posted in that group (which could be internal emails or files) are effectively published for anyone to read if they find the URL or the group name. Similarly, if "External members" are allowed without caution, someone could add a personal Gmail address to an internal group and receive sensitive emails. Often, these misconfigurations happen because Google Groups has many settings and the interface can be confusing, or an admin might think "nobody will find this obscure group."

Best practices for group access controls:

To avoid exposing sensitive information through Google Groups, consider the following practices:

Review group privacy settings

Audit all your Google Groups and see who can access them. For internal discussion groups (e.g., an HR group or an IT support group), the viewing access should typically be set to "Private – Only members of the group" can view messages. If you have groups that need to include external parties (like a customer forum or a partner mailing list), carefully set those to "Private" for viewing but allow external members by invitation. Google themselves urged organizations to set any groups used for internal communication to private, separate from any public groups used for external communities

Lock down membership and posting

Limit who can join and post to groups. For sensitive groups, set "Who can join" to Invite only (or at most, Only users within the organization can ask to join, which still requires approval). Do not leave it open for anyone to join. Also set "Who can post" to group members only (or a subset like managers), so outsiders can't email a group from the outside unless explicitly allowed. This prevents external spam or phishing attempts from reaching your internal groups, and it prevents the scenario where someone subscribes their personal account to an internal list without oversight.

External group communications

If a group is meant to include external people (for example, a group for a project that includes an outside contractor), use the setting to allow external members but do not allow the group to be public. This way, only the invited external users see the conversations. Clearly differentiate these groups (perhaps in the naming convention) and remind members that externals are present (to avoid accidental sharing of ultra-sensitive info on them).

Educate Google Group owners

In Google Workspace, any user can be a group owner (depending on your permissions). Those who manage Google Groups (for example, a department manager who runs a team group) might not be aware of the risks. Provide guidance or even enforce templates: for instance, when a new group is created, have a default setting of private membership and archives. If you allow users to create groups, consider restricting that ability to admins or implementing a workflow where IT reviews new groups. Encourage group owners to review their member list and settings occasionally, especially if the group was created long ago when settings might have been different. Google has improved defaults over time, but older groups might retain less secure settings.

Regular auditing and monitoring

Just like with file shares, you should regularly audit Google Groups settings.

How Nudge Security can help

Nudge Security delivers security posture management for Google Workspace as part of a comprehensive SaaS security and governance solution.

Continuous Analysis

Monitor your Google Workspace environment against security best practices

Risk Alerts

Get notified of misconfigurations and security risks as they occur

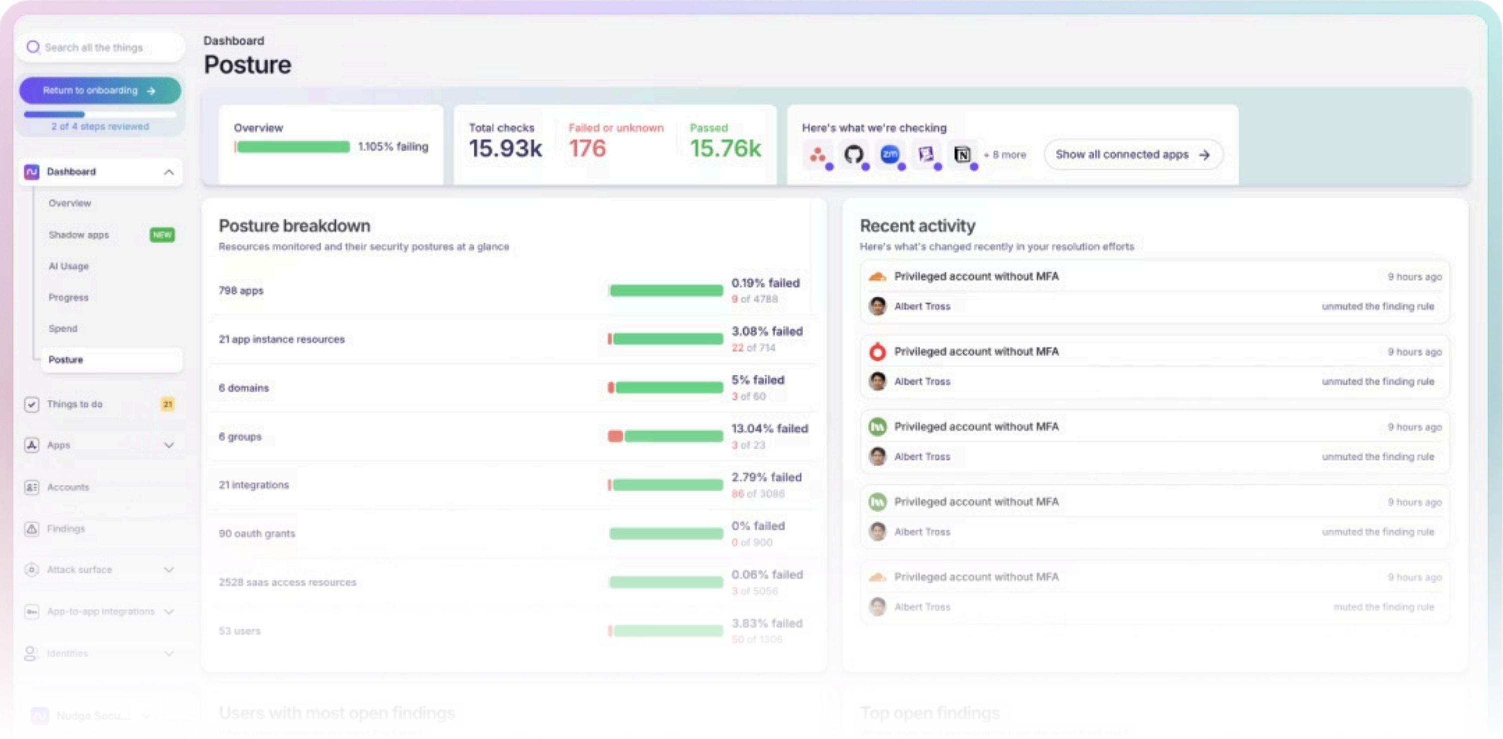
Remediation Workflows

Initiate and track remediation tasks across your team

Progress Visualization

Visualize your progress toward security posture improvements

Start a free trial now and see how Nudge Security can help you secure Google Workspace, and your entire SaaS estate.



Dashboard

Posture

Overview 1.105% failing

Total checks	Failed or unknown	Passed
15.93k	176	15.76k

Here's what we're checking

Posture breakdown

Resources monitored and their security postures at a glance

798 apps	0.19% failed 9 of 4788
21 app instance resources	3.08% failed 22 of 714
6 domains	5% failed 3 of 60
6 groups	13.04% failed 3 of 23
21 integrations	2.79% failed 86 of 3086
90 oauth grants	0% failed 0 of 900
2528 saas access resources	0.06% failed 3 of 5056
53 users	3.83% failed 50 of 1306

Recent activity

Here's what's changed recently in your resolution efforts

Privileged account without MFA	9 hours ago
Albert Tross	unmuted the finding rule
Privileged account without MFA	9 hours ago
Albert Tross	unmuted the finding rule
Privileged account without MFA	9 hours ago
Albert Tross	unmuted the finding rule
Privileged account without MFA	9 hours ago
Albert Tross	unmuted the finding rule
Privileged account without MFA	9 hours ago
Albert Tross	muted the finding rule

Users with most open findings

Top open findings