

Steps to GSuite Security

Enforce Secure Practices

- ☐ Set password requirements **(Priority)**
- ☐ Enforce multi-factor authentication **(Priority)**
- ☐ Use physical security tokens/keys (Yubikeys) for admin and high-value accounts
- ☐ Turn on security alerts
- ☐ Limit email fraud
- ☐ Set up auto-deletion of old emails

Manage Users

- ☐ Onboard new team members efficiently **(Priority)**
- ☐ Offboard departing team members quickly **(Priority)**
- ☐ Convert shared emails to Google Groups/Collaborative Inbox **(Priority)**
- ☐ Create groups to manage access
- ☐ Audit users regularly
- ☐ Monitor for suspicious behavior
- ☐ Isolate your superadmin accounts

Manage Documents

- ☐ Turn on Shared Drive (formerly Team Drive) **(Priority)**
- ☐ Limit Sharing Settings

Sign into your Google Admin console...

Enforce Secure Practices

1. Set password requirements (**Priority**)

Set a password length requirement of at least 12 characters. From the admin dashboard, go to Security > Password management, and set a higher minimum [password length](#) as well as strength (complexity) requirements. Warn your users that a password policy change is coming, and then be sure to check the box that says “Enforce password policy at next sign-in”.

You can also [monitor](#) the strength of user passwords. Click Security > Password monitoring from the dashboard. You will be able to see password length and strength ratings for each user. If someone is using a weak password, you can contact that user individually and ask them to change their password; or you can enforce organization-wide rules to increase password length for everyone.

2. Allow and enforce multi-factor authentication (**Priority**)

First, you will have to allow users to turn on multi-factor authentication - or 2-step verification (2SV), as Google calls it. From the G Suite Admin Console Dashboard, go to Security and then:

- Click on “Basic Settings”
- Scroll to the [Two-Step Verification setting](#)
- Click “Allow users to turn on 2-step verification”
- Click “Save Changes”

Once you have allowed users to turn on 2SV, you can enforce 2SV. Be warned that any users that have not turned on 2SV by the deadline you set will be locked out of their account. We recommend giving your domain users a heads up well in advance!

To enforce 2SV, from the G Suite Admin Console Dashboard, [go to Security and then](#):

- Click on “Basic settings”
- Scroll to the Two-Step Verification setting
- Click “Go to advanced settings to enforce 2-step verification”
- Select an organizational unit (you may want to consider making and then excluding a group of those who haven’t turned on 2SV yet, [so they don’t get locked out](#))
- Select a start date for enforcement!

Pro-tip: To make 2SV more convenient, we recommend turning on “Let users avoid repeated 2-Step Verification on trusted devices”. (Instructions here under Step 4: Select enforcement options.)

To make 2SV the most secure, you can force users to use an authentication app or a physical token. More details available under Step 4: Select enforcement options > Select a 2-Step Verification method to enforce, here.

3. Use physical security tokens/keys (Yubikeys) for admin and high-value accounts

[Security keys](#) are small hardware devices that are used for second factor authentication. They help to resist phishing threats and are the most secure form of 2SV. Make sure there is a spare security key stored in a safe place so that even if your primary key is lost or stolen, you can still access your account. Save backup codes in a password manager or locked safe.

4. Turn on security alerts

As an admin, you can keep an eye out for suspicious activity on users' accounts. GSuite offers a variety of reports, including [suspicious login activity alert](#), mobile device alerts, and other administrative changes alerts. From the Admin Console, go to Menu > Security > Security rules. Sign up for the [suspicious login activity alert](#) under "Reports" by clicking "Manage Alerts" and setting it to "ON."

Take a few moments to write down a plan for what you'll do if you get a security alert and cannot verify that the activity is legitimate. One option is to immediately call, text, or message the user (outside of GSuite) to confirm their activity. If you can't confirm that it was actually them, [suspend their account](#) and lock them out of Apps until you're sure the account hasn't been compromised.

5. Limit email fraud with advanced security settings

Phishing is one of the most common attacks on small non-profits. GSuite offers default warnings against phishing and scams that are robust. You can increase your security even more with a few different email settings:

- [Turn on enhanced pre-delivery message scanning.](#)
- [Turn on attachment protection](#)
 - Go to Apps > GSuite > Gmail > Safety > Attachments
 - Turn on "Protect against attachment with scripts from untrusted senders"
 - Turn on "Protect against anomalous attachment types in emails"
- [Turn on links & external images protection](#)
 - Go to Apps > GSuite > Gmail > Safety > Links and external images
 - Turn on "Identify links behind shortened URLs"
 - Turn on "Scan linked images"
 - Turn on "Show warning prompt for any click on links to untrusted domains"

- Authenticate your email domain and prevent spoofing by using DKIM, SPF, and DMARC. Documentation that will guide you through setting them all up is at <https://support.google.com/a/topic/4388154>.
 - Enhance security for outgoing email by authenticate your email domain with [DKIM](#) (DomainKeys Identified Mail Standards)
 - From your admin console, click Apps > Google Apps > Gmail > Authenticate email. If you have multiple domains, select which one you want to make a key for, then click “Generate new record.” The domain will automatically be added to the DNS records if you bought your domain from a Google Apps partner. Otherwise, you’ll have to [add it manually](#). Finally, [turn it on](#) by going to Apps > Google Apps > Gmail > Authenticate email, and clicking “Start Authentication.”
 - Configure [SPF Records](#) to help prevent spoofing. Configure it from your [Admin console](#).
 - Once you have SPF records set up, you’ll be able to use [DMARC](#) to enhance security for forged spam.
- Once you have set up DKIM, SPF, and DMARC, you can go back to Apps > GSuite > Gmail > Safety and scroll to the Spoofing and authentication section.

6. Set up auto-deletion of old emails

If regular email deletion after a certain number of months or years is part of your data retention plan, you can [turn on email deletion](#) for all users in the GSuite Admin Console. You can customize the length of time after which all emails are deleted, and whether they are moved to the trash folder first or permanently deleted right away. You can exempt emails with specific labels from this rule.

Manage Users

7. Onboard new team members efficiently (**Priority**)

When you add a new user, let “minimum access required” be your guide: only give the users the bare minimum of permissions they need to do their work. Take a few moments to open a spreadsheet and think about all the categories of users (staff, volunteer, board member...) or, if your organization is small enough, write down the roles of everyone in the organization. Who needs to get an @yourdomain email when they start? Who needs access to certain Drive documents, but not an email? Create a flow chart or a checklist for new team members in each category. Bring this document to your next team meeting to get team input and buy-in so you can consistently manage new GSuite account provisioning.

Pro-tip: Create a Google Form for new users to submit when they need a new account. Ask for first name, last name, personal email, and role, and any other information you need to create a new account with the right permissions.

8. Offboard departing team members quickly (**Priority**)

If the email account is staying active but not being used, set up an away message and any forwarding rules, and change the password. If the email account is transferring to a new owner, change the password.

If the email account will no longer be used, you have two options for offboarding a user.

- Suspend a user: You will have access to all documents and emails, and will have to continue paying for this user.
- Delete a user: This permanently removes all documents and emails, except for documents created in Shared Drives. You have 20 days to reverse the deletion before it is permanent.

Pro-tip: If you delete or suspend a user, you can add their email address as an alias to another account so that important emails aren't missed.

9. Create groups to manage access

If you find yourself with consistent groups of people who need the same level of minimum permissions to do their work, you can control their access more efficiently by categorizing users or devices into [organizational units](#).

You may also want to create Google Groups to manage access to Drive documents. You can [create Google Groups](#) and give appropriate document access to the Group's email address. When a new person onboards or offboard, you can just add or remove their email from the Google Group rather than adding or removing them to each individual file.

Google Groups can also be used to manage shared email accounts. Everyone who needs access to the email address can be added to a Google Group. Using the “send as” feature, individuals can use their own emails to reply as the shared account. This is detailed below.

10. Convert shared emails to Google Groups/Collaborative Inbox

Shared emails - i.e., when multiple people log in and check the same email - present a security threat from an account hygiene standpoint as well as a data management standpoint. Shared inboxes mean shared passwords, which end up being communicated via text, email, or other insecure means when users need to log in. Two-factor authentication is challenging, if not impossible, to enforce. It's also challenging to onboard and offboard users from shared inboxes; offboarding requires changing the password for all users, exacerbating the password sharing issues above. If a shared inbox is compromised, it's harder to trace the source of the attack and to cut off access for the attacker, especially if this is the organization's only or most important inbox.

Luckily, Google offers solutions that you can use as an alternative to sharing emails. Say, for example, your organization currently uses `team@mydomain.com` as your shared inbox. First, rename the email account that you want to convert into a group. In our example, we'd rename `team@mydomain` to `old-team@mydomain.com`. Google will automatically make `team@mydomain` an alias for the account; delete this alias. Go to groups.google.com and [create a Google Group](#) with the old shared email account - `team@mydomain.com`. Add members to the Google Group who you would like to see all emails to `team@mydomain`, and be sure to check the permissions settings to allow people outside your domain to email the group.

If you'd like to delete the old shared email, but save the messages in someone else's inbox, you can use POP settings to import old and new messages into a different inbox. Instructions are available [here](#).

11. Audit users regularly.

Once a quarter, audit your list of users. Open your complete list of GSuite users, and check last activity date. Are there any accounts that haven't been used in over a month? Anyone who has left the organization but whose account wasn't deleted?

For any shared accounts, check with the primary supervisor of the account if it has become inactive. Before deleting, check with the team to make sure it's not still public or active.

12. Monitor for suspicious behavior

You want to check login activity, file storage amount, and sharing for any odd behavior or spikes. Check weekly or monthly and get a feel for what is normal for your organization so you can

notice any changes in patterns. Set a calendar reminder to check your [account activity report](#) and your [audit log](#) from the GSuite Admin portal.

13. Isolate your superadmin accounts

Your superadmin accounts (those that can create new users and reset passwords) should not be email accounts you use everyday. Create a separate account for your regular email and a separate account for administration - for example, admin-jane@example.com and jane@example.com. Log in to the superadmin account only to complete admin functions, and log out as soon as you are done. Be sure to save the superadmin password where at least one other person has access to it, or create at least two superadmin accounts, so that if your account is lost or compromised, the organization can continue operating their GSuite. For admin tasks you find yourself repeating often - like creating a new account or resetting a password - consider making an admin account with the necessary privileges to complete those tasks, while keeping a superadmin account for permanent admin tasks like deleting a user.

Manage Documents

14. Turn on Shared Drive (formerly Team Drive) **(Priority)**

Using Shared Drives to store your organizations' files ensures that no matter who comes and goes, the organization will always retain file ownership of all documents. For some reason, the default on GSuite is to prevent users from making team drives. You have to un-prevent them in order to start using shared drives. Instructions from Google are [here](#).

- From your Admin Console, head to Apps > GSuite > Drive and Docs.
- Make sure that [Drive is turned on](#) (click More and then ON for Everyone).
- Select Sharing Settings.
- Under Shared drive creation, uncheck "Prevent users in your organization from creating new shared drives."
- After you click save, these changes will take 24 hours to go into effect.

15. Limit sharing settings

The safest way to share documents from your team's Shared Drive is by sending invitations to trusted individuals only.

You want to make sure that Link Sharing is off so that team members don't inadvertently make documents public. As iEcology [explains](#), "Unless you change the default behavior of your G Suite, whenever anyone clicks "Get sharable link" on a folder or file, they will create a link that is open to anyone, without needing to sign into a Google account. You can and should change this default behavior so that "Get sharable link" can be used to copy-paste a document link without changing the existing permissions on the item." Instructions for finding these settings are [here](#); at; under Link Sharing, choose "OFF."

Team members will still be able to share documents, but they will have to intentionally change the file's permissions using the "Share" button in order to do so.

In the same part of your admin portal for [setting Drive users' sharing permissions](#), you can enable a warning before users share files with external people.

You'll also want to scroll down to the settings for Access Checker - this is the feature that makes sure all recipients of an email have access to a Google file being shared or linked to in that email. Ensure that Access Checker is configured "for Recipients only" so that files linked to in emails aren't made public.