nira

Best Practices for Document Security in Google Workspace

Best Practices for Document Security in Google Workspace

Introduction **4**
- What are Document Security Systems? 5
- Why is Document Security Important? 5

Chapter 1: Links **6**
- Link Types 7
- Permission Types 8
- What Security Risks Come with Links? 9
  - Company link Access-Risks 9
- Here's What Employees Should Know 10
  - Public link Access-Risks 11
- Set Link Sharing Permissions for Your Team 12
  - Let users share files outside of your organization 12
  - Restrict all file sharing outside of your organization 13
  - Restrict the access levels users can give to files 14
  - Control the default settings of how users share links to files 16
    - Set a Primary target audience 17
  - Link sharing defaults 18
- Here's What Employees Should Know 19

Chapter 2: Collaborators **19**
- Set Sharing Permissions for Your Team 21
  - Let users share files outside of your organization 21
  - Restrict sharing to certain domains 23
  - Restrict file sharing outside of your organization 24
- How Employees Can Set a Sharing Expiration Date 26
- What Security Risks Come from Sharing with Collaborators? 27
- Here's What Employees Should Know 28

Chapter 3: Shared Drives and Folders **28**
- What are Shared Drives? 28
  - Shared drives vs. My Drive 29
- What Security Risks Come from Using Shared Drives? 29
- Set Permissions on Shared Drives 30
  - Shared drive access levels 30
- What Admin Privileges Should You Be Aware Of? 32
  - Turn shared drive creation on or off for your organization 33
  - Control default sharing of shared drives content 35

Manage access for an existing shared drive 37
Allow users to move content to a shared drive 38
Shared Drives FAQs 41
Can users add Public links or Company links to shared drives? 41
How much visibility do users have in shared drives? 41
What kinds of accounts can be added to shared drives? 41
What happens when you suddenly stop sharing a shared drive with external parties? 41
Can I remove a collaborator on a shared drive from the documents within the shared drive? 42
How do you deal with multiple members in shared drives? 42
Can shared drives be owned across multiple domains? 42
Folders in Shared Drives 42
Move Drive folders to a shared drive as an admin 43
Restrict users from moving shared drive content outside your organization 44
Here's What Employees Should Know 45

Chapter 4: Document Retention 46
Document Retention and Policies 46
Document Retention through Google Vault 47
How Vault retention works 48
Retain files in Drive in Vault 48
How to set a custom retention rule 48
How to set a default retention rule 50
Here's What Employees Should Know 51

Chapter 5: Transferring Ownership 52
How Employees Can Transfer Ownership 52
How to Transfer Drive Files to a New Owner as an Admin 53
Transfer one file 53
Transfer all of a user's files 53
Here's What Employees Should Know 54

Chapter 6: Managing Labels 54
Turn Labels On or Off for Your Organization 55
Create Labels 56
Create Badged labels 57
Create Standard labels 58
How Employees Can Use Labels 60
Apply labels 60
View and apply labels 61
Search for files with labels 62
Manage Label Permissions 62

Here's What Employees Should Know 63

Chapter 7: Other Access Controls 64

Restrict File Access 64

Prevent Editors from re-sharing and changing access permissions 64

Prevent a file from being copied, printed, or downloaded 65

Share Content with Groups 65

Share a document with a group 66

Share outside the organization 66

View All Activity on Documents 68

Understand Inbound Documents 68

Here's What Employees Should Know 70

Chapter 8: Real-time Access Control Systems 71

Real-time Access Control System 71

Conclusion 72

About Nira 72

Glossary 73

Introduction

Google Workspace started almost by accident. What started as Gmail quickly snowballed into a suite of collaboration tools we know today as Google Workspace. Suddenly people could collaborate from anywhere and share documents on any device using Google Docs, Sheets, Slides, and more.

Google took the familiar feel of Microsoft products like Word and Excel and created versions that could be used by anyone, anywhere, anytime. It's the quintessential success story of one product being everywhere people needed it to be—functioning adeptly across mobile devices, tablets, and desktops.

Since the mid-2000s, Google has grown its market share of the productivity suites category to roughly 10%, gradually eroding Microsoft's dominant position to about 90% in 2020. And although some companies use Google Workspace on its own, even more companies are using both Microsoft and Google.

Google's tools and products are incredibly simple for companies to integrate into their daily workflows. And they're brilliant when it comes to allowing teams to work together. According to Google, almost 75% of time spent in Docs, Sheets, and Slides is collaborative.

Users of Google echo this sentiment: We surveyed 197 people about their use of Google Workspace and learned that the top two categories of words they used to describe it were "ease"/"easy" and "collaborate"/"collaboration".

This collaboration is so quick and easy that companies are seamlessly working with people across the company internally, and with external parties, too.

Before a company knows it, they have tens of thousands, hundreds of thousands—even millions of documents. These documents get shared with just as many, if not more, internal and external accounts. Documents even come inbound to a company from external vendors, partners, and customers.

While collaboration helps companies get work done and be hyper-efficient, it also brings challenges. Collaboration can quickly (and quietly, unbeknownst to a company) escalate into data breaches or leaks. Someone in an organization can share a public link and suddenly anyone on the internet has access to confidential company information. Even Company links (where all company employees can access a document) can be an issue if used improperly.

Data can get scattered across different departments within a company or shared with external vendors who are never fully offboarded. Access control becomes a full-time job for admins as a company scales.

That's exactly why we wrote this guide.

We'll go over the best practices for document security to help admins better understand the actions they can take to keep their company's Google Workspace data safe. We'll cover everything, from protecting sensitive documents to shared drives, group access, and more.

What are Document Security Systems?

When we talk about document security, we are referring to all your organization's assets (Sheets, Slides, Docs, PDFs, PPTs, Word files, shared drives, folders, etc.) that live in Google Workspace.

We'll focus specifically on the best ways to protect and secure these assets from unauthorized or unnecessary access using Google's consumer and admin tools.

We'll go over the biggest pain points we hear from IT managers and Google admins—such as how to manage shared drives, labels, and folders—and give you step-by-step instructions on how to keep your company documents secure.

Why is Document Security Important?

Documents get shared by employees at a company anywhere from dozens to thousands of times a day.

Although most employees have good intentions and aren't trying to do anything nefarious, over-sharing can and does happen all the time. People add the wrong link permissions, accidentally share with personal accounts, or even unintentionally create company documents using their own personal accounts.

This can lead to Access-Risk issues such as external vendors never being completely removed from files or confidential documents shared with public links that anyone on the internet can access without even logging in.

Accidental sharing misconfigurations or malicious data breaches can cost companies millions of dollars in revenue and legal fees and have significant reputational impacts. They can also trap admins into an endless cycle of investigations and reactive fixes.

Admins don't have a lot of time or resources to deal with these breaches and incidents, but are often expected to clean them up all the same. Unfortunately, these incidents can take months or even years to identify, investigate, and remediate. For example, the average time to identify and contain a data breach was 287 days in 2021, according to IBM.

Knowing what to do after a breach or attack is crucial, but the best data security tools enable companies to detect, investigate, and remediate risks before an event occurs.

The best approach is a proactive approach. And good document security practices will help you determine threats and vulnerabilities before they become major headaches and multi-year problems.

We'll go into the nitty-gritty of file sharing and access controls in the chapters that follow.

Chapter 1: Links

One of the easiest and fastest ways to share Google Workspace documents is through links.

Just click a button, and boom, suddenly documents can be shared using a link across a variety of tools. It's become sharing muscle memory.

Links to documents are constantly dropped into tools like Slack, GitHub, Trello, and even publicly on the web using social media, on websites, or in Google's search engines.

Links are one of the most popular ways of sharing because they are incredibly fast to create and send. No thinking about exactly who needs access, no typing in names and hitting buttons in confirmation modals. In just a few clicks, the person sharing can get a document to the people who need it.

This type of sharing can lead to Access-Risk issues, as links with sensitive information may be made visible to anyone on the internet or anyone in the company.

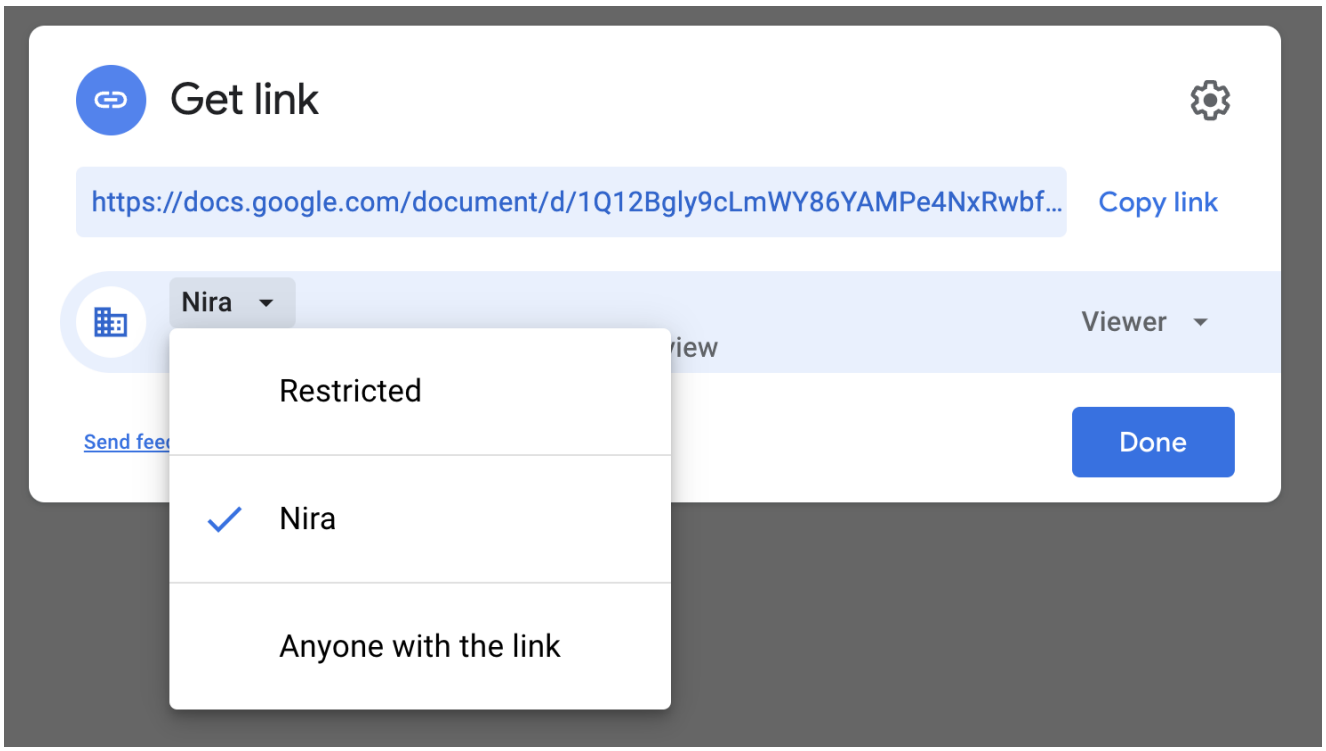
When employees create documents in Google Workspace, they are able to select from three different link types: Restricted, Anyone at the company, and Public.
Employees will also be able to further determine if the people who access the documents using the link will be Editors, Viewers, or Commenters.

Link Types

Restricted: This type of link allows only people or groups whose email addresses have been added as collaborators to access the file, folder, or shared drive, as long as they are logged into their Google account.

Company: This type of link allows anyone at the company to access the file or folder, as long as they are logged into Google with their company email.

Public: This type of link allows anyone on the internet with the link to access the file or folder. They don't need to be signed into a Google account to access the file or folder.


Get link
https://docs.google.com/document/d/1Q12Bgly9cLmWY86YAMPe4NxRwbf...
Copy link
Nira
Viewer
Restricted
Nira
Anyone with the link
Done

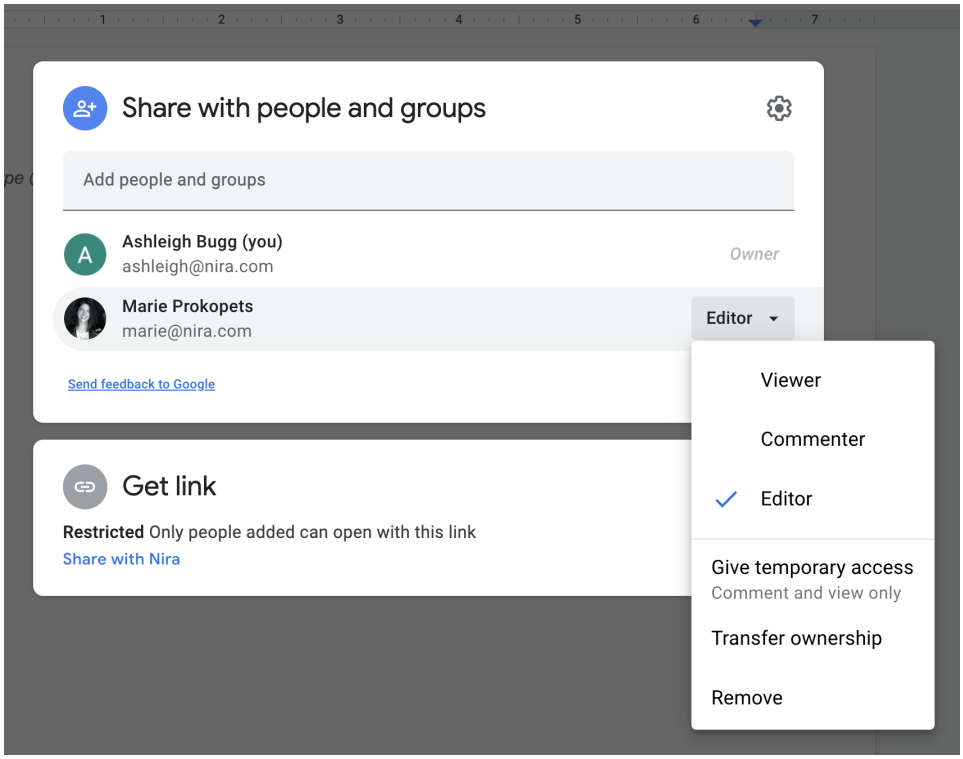
Permission Types

Viewer: The person or account can view the file but cannot make comments or edit it. Viewers cannot share the item with others and cannot see who else has access to the item.

Commenter: The person or account can view the item and make comments on it, but they cannot edit. Commenters are also unable to share the item with others or change sharing permissions.

Editor: The person or account can view, make comments, and edit the item. They can also share it with others and allow them to edit, comment, or view the item. Editors are also able to share the item with others and change sharing permissions.

Owner: The person who creates the item is usually the owner. However, ownership can be transferred from the creator to other parties who then control its access permissions. Owners are able to view, comment, edit, move the item, and set sharing permissions for other users. We'll go over transferring ownership in chapter 5.



In the next few sections, we'll learn more about Company and Public links. This includes security issues, what employees need to know, and how different departments should use these link types.

What Security Risks Come with Links?

Company link Access-Risks

Company links grant access to anyone in your company, and when employees use this link setting, it can have unintended security consequences.

Suddenly, everyone in the company can access salary information or someone's private performance improvement plan. Even confidential executive-owned files about company strategy can accidentally be shared with everyone in the organization.

And even though documents might start out as accessible to people at your company, if everyone in the company has Editor-level access, they could still share with personal accounts or external accounts. We'll cover this in more detail in the Sharing via Collaborators chapter.

We've learned that company links are misused more often than people think. It's common for companies to not realize that confidential documents are accessible by anyone within the company.

So when should Company links be used? Only when documents or folders are meant for consumption by everyone in the entire company. For example, a holiday schedule should have a Company link, as should all compliance policies that employees agree to each year and need to look back on.

When shouldn't they be used? Whenever the contents of the documents and folders are not meant to be shared with everyone in the entire company. That's because it's easier than ever to share document links within collaboration tools like Slack or Teams, and then suddenly, sensitive documents can spread like wildfire.

For example, severance information should not be available to anyone in the company and should be restricted to only those who need to see it. The same goes for customer contracts or employee offer letters. But this doesn't always happen.

For this reason, departments that tend to create more confidential information such as Finance, Legal, or Human Resources, will need to be extra careful when using Company links.

They may need to share something with the whole company, like vacation policies, but they should grant everyone in the company Viewer or Commenter access rather than Editor access. Other documents, especially those with sensitive information like salaries, should always be restricted and locked down.

For best security practices, finance documents should never have Company links, with the exception of documents that need to be distributed widely.

And if an employee is sharing something like a budget proposal with the rest of their department, it is best to assign Viewer or Commenter access only, so that team members can't accidentally share with external parties or personal accounts.

However, this method may be unrealistic as Finance departments often need to collaborate cross-functionally.

One way to safely do this is through Groups, where you can limit how sensitive or confidential information is shared (see the Other Access Controls chapter for more).

To sum it up, any departments that primarily work on confidential information should limit their use of Company links.

Here's What Employees Should Know

- Company links should be used sparingly.
- Confidential documents should never have Company links.
- Company links should only be used when a document needs to be viewable by every employee in the company.
- For documents meant to be shared with specific people in the company, employees should add in those people's emails as collaborators and make sure the document is restricted to only those people.
- When adding Company links to documents, employees should select the least access privileges that people need. For example, only people who need to edit a document should get Editor access. Others should receive Commentor or Viewer access.

Public link Access-Risks

Just like Company links have become muscle memory for sharing documents within a company, Public links are the easiest, fastest way to share documents and folders externally. That's exactly why they are so risky.

Companies should use Public links sparingly, even when working with vendors.

A Public link on a document means that anyone on the internet can see the document, and they don't even need to log in to a Google account.

If the Public link allows Editor access, anyone that views it can also make changes to the document or sharing permissions—meaning they can invite other accounts to collaborate on the document.

The best rule is that documents can have Public links if the information in the documents or folders is not confidential and can be made public without any implications for the company.

For example, Lydia from the Content team needs to quickly share a document with a freelance writer that the company has contracted.

She's been communicating with the writer through the company's external Slack channel and quickly drops the link in a direct message for the writer to access. The writer messages her asking for editing permissions so they can get to work.

Rather than adding the writer's email to the document, Lydia changes their access to "Anyone with the link" and sets it to Editor. The company document is now open to anyone on the internet to view, edit, or change sharing permissions as they wish.

If the contents of the document are not confidential and there would be no issues if anyone on the internet saw the document, then this use of Public links would be unnecessary but fine. However, if Lydia was working with the freelancer on a critical future announcement like an acquisition or a secret new feature, then using a Public link would be very risky.

When it comes to departments, some should use Public links sparingly, while others should never use them at all.

For example, most documents created by executive leadership teams should not have Public links, while Marketing might have more reasons to use them.

Meanwhile, departments like Finance, HR, and Legal should not use Public links except under exceptional circumstances or for very specific reasons (like during recruiting).

Set Link Sharing Permissions for Your Team

Depending on their Google Workspace plan, admins are able to control how users share links. We'll briefly go over the permissions you can set for your employees and how to do it in your Admin console.

Let users share files outside of your organization

Supported editions include Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; G Suite Business; Nonprofits; Essentials.

For sharing outside your organization, admins can decide if users can make files visible for anyone with the link under the "Sharing options" section in "Sharing settings." This means that when sharing outside of your organization is allowed, your employees can make files public for anyone who has access to the link.

How to do it

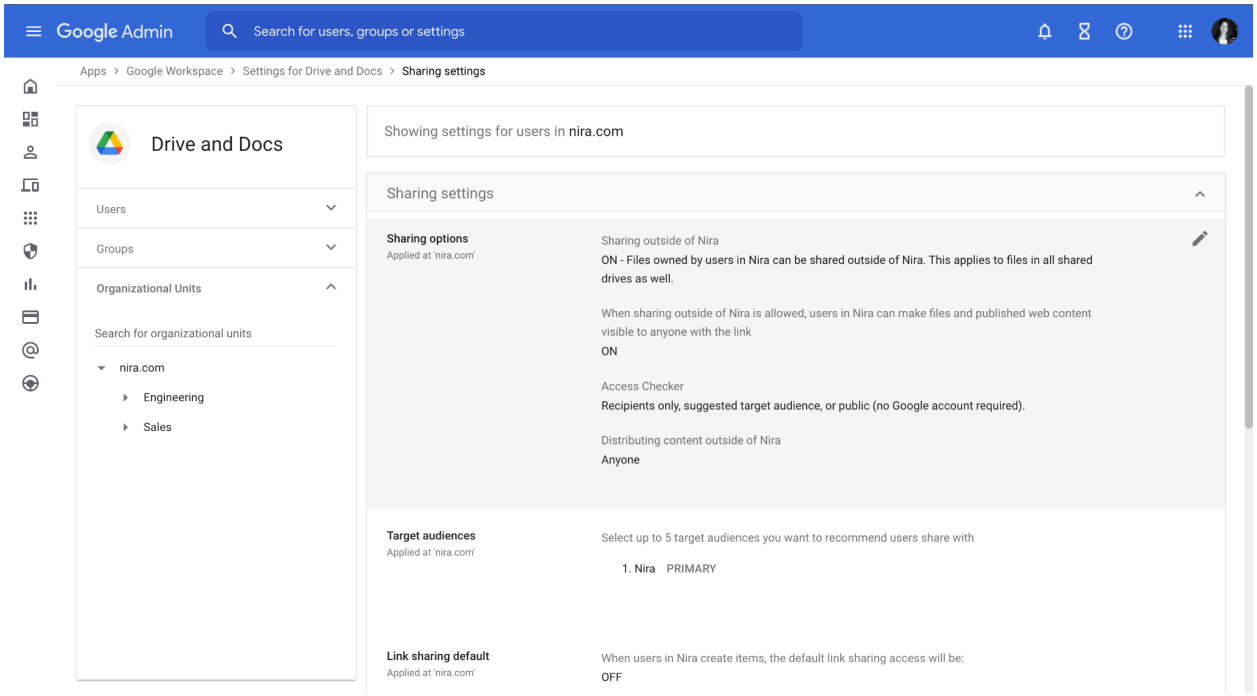
1. Within the admin panel, go to: "Apps" > "Google Workspace" > "Drive and Docs" > "Sharing settings" > "Sharing options"

    - You can either apply the setting to everyone in the organization by leaving the top organizational unit selected, or you can choose a child organizational unit that allows you to apply different permissions to select people under an organizational unit or a configuration group.

      For more information on organizational units and groups, check the glossary at the end of this guide.

2. You will then see "Sharing outside of your organization" and click "On."

    This sharing option will allow users to make files and published web content visible to anyone with the link.



Restrict all file sharing outside of your organization

Supported editions include Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; G Suite Business; Essentials.

What is it?

When you set this permission, you can keep users from sharing outside your organization for certains items including links to files stored in Drive.

You can even go further and make it so employees cannot receive files from accounts outside of your organization. This means your users cannot open or edit files from outside of your organization or in third-party storage systems.

Why it matters

This method can be useful for keeping company data safe by regulating the links employees can share and receive.

However, although it is possible to lock down external sharing via links and receiving of files coming inbound from outside of the organization, this leads to risks of its own.

For example, employees may try workarounds to share or open documents, such as copying the document to a personal account and then sharing, or using an unsanctioned application to create documents. It's typically better to educate your employees about best practices instead of locking everything down.

How to do it

1. In the Admin panel, go to: “Apps” > “Google Workspace” > “Drive and Docs” > “Sharing settings” > “Sharing options”

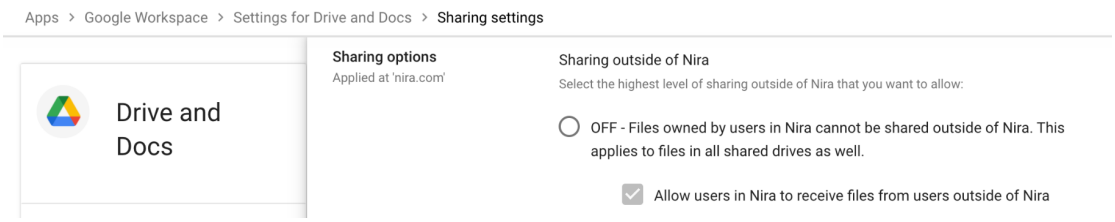
    - You can apply the setting to everyone in the organization by leaving the top organizational unit selected. Or, you can choose a child organizational unit or a configuration group.

2. When you see “Sharing outside of your organization,” click “Off.”

3. After you restrict file-sharing, you have the additional option to stop employees from receiving files from users outside of your organization. They cannot open or edit files from outside of your organization or in third-party storage systems.

    Just uncheck the “Allow users in your organization to receive files from users outside of your organization” box.

4. Click “Save.”



Restrict the access levels users can give to files

Supported editions for this feature: Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; G Suite Business; Essentials.

What is it?

Admins can control the level of access users can give other users when they are prompted to share files. Employees are asked if they want to share files with additional people when they attempt to share a file but not everyone has access.

For example, an employee tries to send a document link that they hadn’t previously shared with their coworker in a Gmail message or a Google chat.

Or they want to attach a document link to a calendar invite for their team, but not everyone on the team has access to the file. They will then receive a prompt asking if they want to share the file.

How much power employees have will depend on if they own the file. If they aren't the owner, it will depend on the actual file owner's organizational unit and its sharing permissions. If they share multiple files and different organizational unit settings apply, the options come from the least permissive organizational unit.

Why it matters
It can be difficult to work collaboratively when you need to share a document and the recipients haven't been granted access.

However, there might have been a good reason they weren't given that access in the first place. The document may contain sensitive data like PII or strategic information like marketing and sales plans that shouldn't be shared with just anyone with the link.

Being able to mediate the levels of access users can grant helps combat further issues down the road. However, this can also lead to employees trying workarounds, which is why, as always, employee education, plus access control measures taken by admins, are key.

How to do it

1. Within the Admin panel, go to: "Apps" > "Google Workspace" > "Drive and Docs" > "Sharing settings" > "Sharing options"
    - To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select a child organizational unit or a configuration group.
2. Click "Sharing options."
3. You can then use "Access Checker" and choose an option:

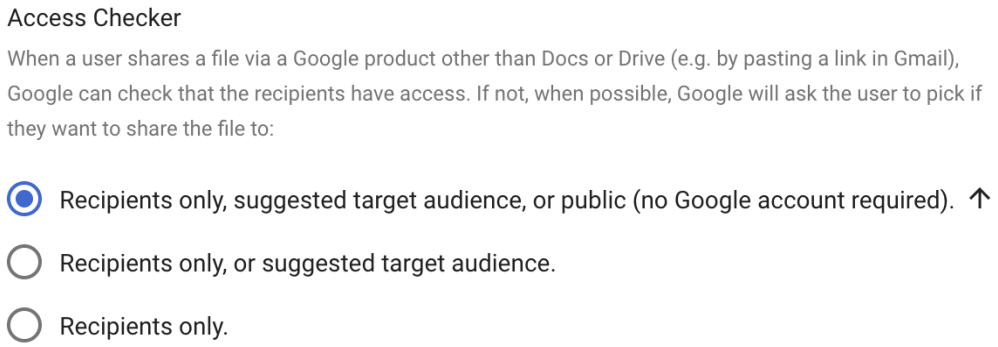
    Recipients only, your organization, or public—Employees can grant access to anyone who has the link. This is the least restrictive setting; it's available only if sharing is turned on for your organization, and you allow employees to publish files online.

    Note: if you have target audiences set up, you can choose the suggested target audience. You will find more information on setting a target audience in the following section.

Recipients only or your organization—Employees can grant access to required recipients and anyone in your organization who has the link.

Note: if you have target audiences set up, you can choose the suggested target audience.

Recipients only—This is the most restrictive setting. Users can only give access to required recipients. However, if the file has been shared with other people, they will still have access.



Control the default settings of how users share links to files

Please note that only these Google Workspace plans come with this permission: *Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; G Suite Business; and Essentials.*

Admins on the plans listed above can control how users share links to files in My Drive. This does not apply to files and folders within shared drives, which we'll go over in the Shared Drives chapter.

As an admin, you can apply these permissions to everyone in the company, or you can apply policies to specific users through an organizational unit or to a group of users through a configuration group.

In your Admin console, you will have the ability to set default link sharing settings in several ways. For example, you may turn it "OFF" automatically, so that only the owner, and then those they choose to share with, has access to the document. You can also set it to "ON-Anyone at your organization with the link" which allows anyone at your company to access the document if they have the link or "ON-Anyone with the link," which allows anyone in your organization to search for and view the file.

Set a Primary target audience

You can go a step further when setting up your organization's permissions and create "target audiences." These are basically groups of people, such as the Marketing department or a Sales team, that you can recommend your users share with.

You will create a "primary target audience'' and then can add multiple secondary target audiences, up to five in all.

By setting up a target audience, you have an added level of protection when configuring sharing privileges.

How to do it

1. You will first create a target audience: "Directory" > "Target audiences."
2. Click "Create target audience."
3. Under "Name," write a name for the target audience, such as Sales or Engineering.
4. Under "Description," you can write a quick blurb explaining the target audience.
5. Click "Create."
   Then, you can add members to the target audience. This step may be completed later if you're not sure yet which users you need to add. However, make sure you have added some members before applying the target audience to a Google service.
6. Click "Add members."
   If you have the Service Settings Admin privilege, you may apply your target audience to a Google service. You can create and apply up to five target audiences for a specific service.
7. Click "Apply to Google services," and select a service. In this case, you will set it for "Drive and Docs."

Remember: To make the primary target audience appear as the default link-sharing option to users, make sure link sharing is turned on.

You have the option to "Create another" target audience, for a total of five target audiences.

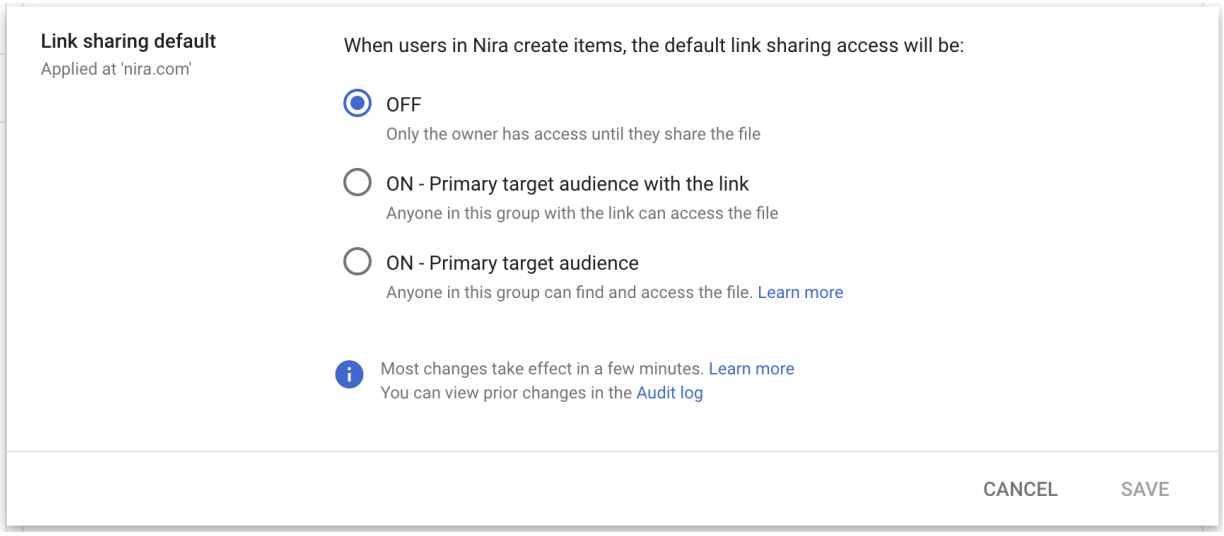
8. Click "Done."

Link sharing defaults

Now, when a user creates a document, admins can decide what the default settings for link sharing will be.

They can either turn them “OFF” which will only allow the owner of the document to have automatic access, or they can turn it “ON” for a “Primary target audience” or “ON” for a “Primary target audience with the link.”

1. In the Admin console, you will go to “Apps” > “Google Workspace” > “Drive and Docs,” and then select “Sharing settings” and then “Link sharing default.”



2. Here are the three link sharing default settings you can select from:

    - **OFF:** Only the file owner and people the owner has shared the file with can access the file.
    - **ON-Primary target audience with the link:** Only those in your primary target audience who have the link can access.
    - **ON-Primary target audience:** Anyone in your primary target audience can find and access the file.
3. You will then save your permissions, but be aware that it can take up to 24 hours for the changes to take effect.

It’s important to note that employees are used to collaborating freely and if their habits get hampered, they can use workarounds to be able to share documents, which can lead to other Access-Risk issues.

Instead of immediately locking down employees' permissions, the method that we've found to work best is to educate employees and give them visibility of security risks related to link sharing. And to control access to Google Workspace documents by using a real-time access control system.

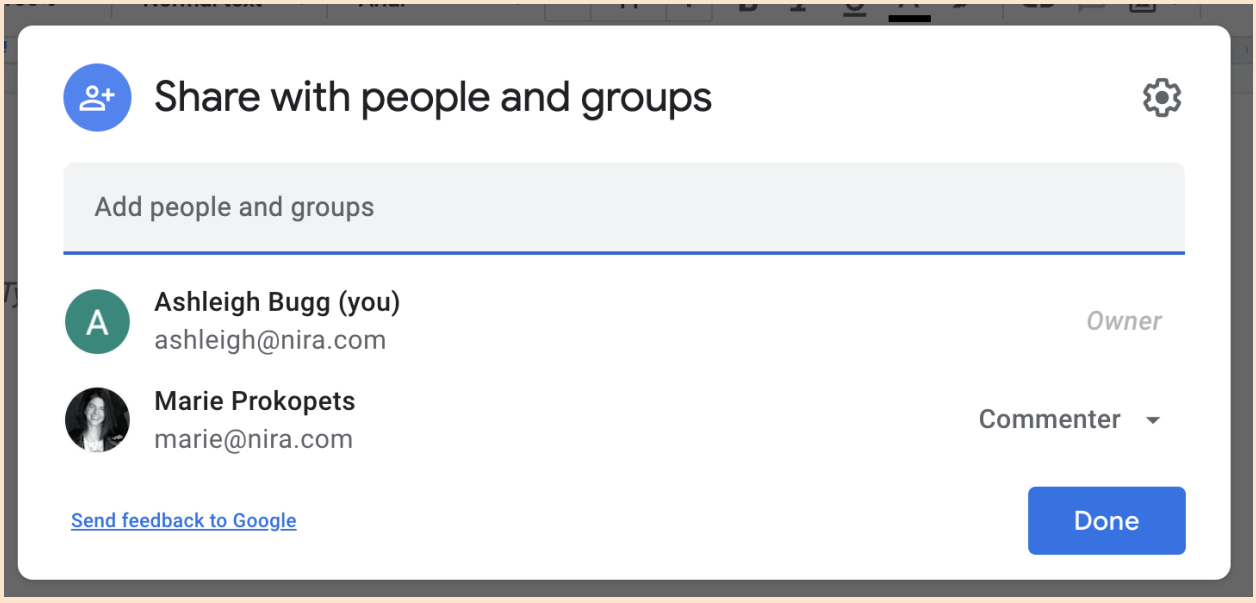
Here's What Employees Should Know

- Restricted links should be the default, and it's best to limit sharing as much as possible without interrupting collaboration.
- Company links should only be used when everyone in the company should have access to the document.
- Public links should only be used when there is a valid business need and anyone on the internet can access the document without any repercussions to the company.
- Never put confidential information in documents with Company or Public links.
- HR, legal, finance, and executive-level staff should avoid using Company or Public links.
- Always use Public links with caution, even when working with trusted vendors or contractors.

Now that we've gone over the types of sharing using links, let's get more in-depth by examining how sharing documents with different internal and external collaborators affects security.

Chapter 2: Collaborators

We've looked at quick and secure ways to share documents using links. Now we'll go further by diving in to sharing with specific people and groups.



This type of sharing includes with internal collaborators within the company, outside collaborators from other domains, and personal email account collaborators (i.e. Gmail or Yahoo accounts).

Employees can also share with groups. For example, everyone at the company or everyone in a specific department at the company.

Sharing with collaborators is simple and quick, but it also comes with security concerns, as more and more people can be added to drives, folders, and documents. Issues stem from a lack of oversight as old documents are forgotten, and access is never removed.

As an admin, you can help alleviate some risk by setting prompts that ask employees to reconsider if they want to share outside of their organization.

However, unless you have enabled specific controls to keep them from doing so, they may ignore the warning messages.

And if they give a personal or outside domain account Editor permissions, the account-holders can then share with more people or even change the sharing permissions to public, allowing anyone on the internet access.

It may seem like employees have malicious intent when sharing with personal or outside domain accounts, but that's rarely the case.

For example, Roberto on the Marketing team has a document he wants to share with a new vendor who is helping the company with social media.

He shares with the vendor and gives them full editing rights. That vendor in turn gives everyone at their company editing permissions by sharing with a group email address, rather than with the specific people working on the project. Anyone in their company can now view or even make changes to the sharing permissions for the document.

Once the project is finished, the vendor is never properly removed from the document, and everyone at the external company still has access.

This may seem like a low-level risk if the information is just a quick brainstorming session for social media.

But what happens when extremely confidential information from the financial or legal departments accidentally gets shared?

Departments that share sensitive information such as Finance and HR should only be sharing classified documents with outside collaborators when required. They should also be very careful when sharing with those inside the company.

We recommend keeping documents with extremely sensitive information locked down and not giving internal collaborators editing permissions unless absolutely necessary, as well as removing access when possible.

Set Sharing Permissions for Your Team

As an admin, you can apply various sharing permissions to everyone in the company or through an organizational unit or a configuration group.

We'll go over the permissions you can set for your employees, why they matter, and how to do it in your Admin console.

Let users share files outside of your organization

What is it?
When you turn this permission on, you may choose from several sharing options. For example, you can warn users when they are about to share outside of their organization or let employees send sharing invitations to people outside your organization who don't have a Google account.

Why it matters
Your employees are going to need to share outside of your company eventually, whether it be with third-party vendors, customers, or other external stakeholders. They may also be

collaborating with people who haven't used Google Workspace and don't have Google accounts set up. Allowing these permissions will help them easily work with others and do their jobs. It will also let them be more aware of who they're sharing with and why. For example, giving a warning message can mitigate risky behavior without automatically locking down privileges that interrupt employee workflows.

How to do it

1. "Apps" > "Google Workspace" > "Drive and Docs" > "Sharing settings" > "Sharing options"

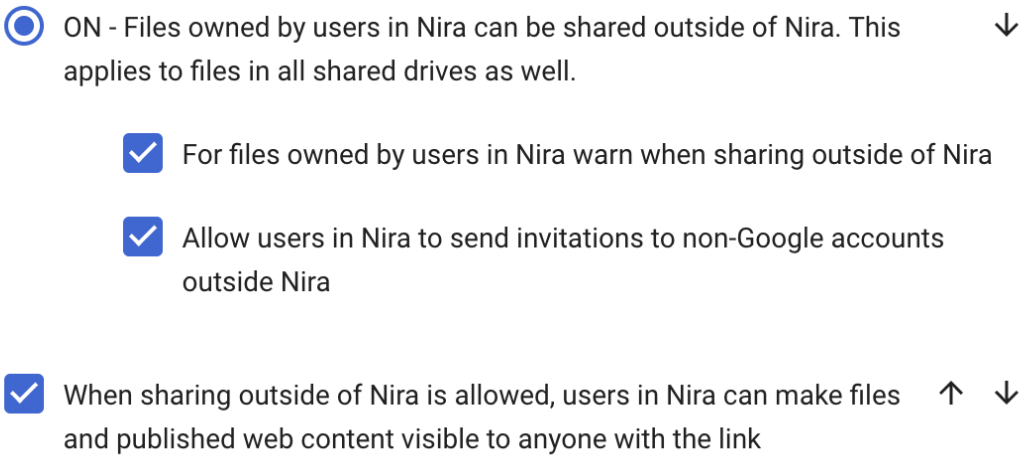
    - You can either apply the setting to everyone in the organization by leaving the top organizational unit selected. Or, you can choose a child organizational unit that allows you to apply different permissions to select users under an organizational unit or a configuration group.

2. You will then see "Sharing outside of your organization" and click "ON."
3. You now have several sharing options:

    - Warn when sharing outside of your organization
    - Send sharing invitations to people outside of your organization who aren't using a Google Account
    - Allow users to make files and published web content visible to anyone with the link

    Remember, if users want to edit or comment on files, they must sign in to a Google Account or a visitor account once visitor sharing is turned on.

4. Click "Save."



Restrict sharing to certain domains

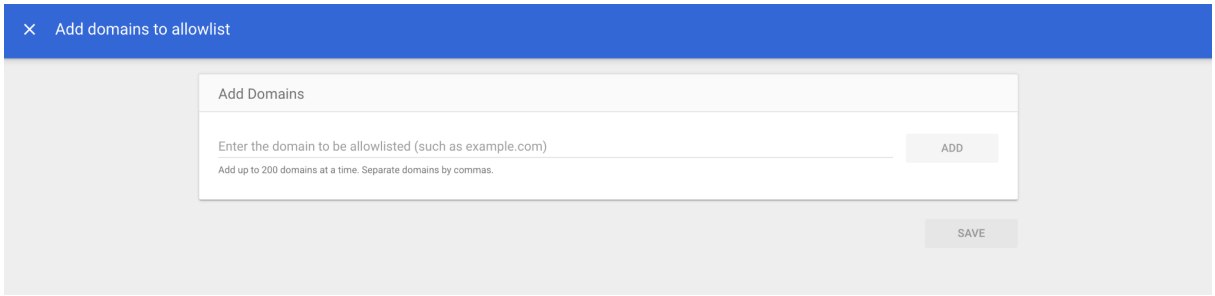
Note: *This admin permission only applies to companies with certain plans: Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; G Suite Business; Essentials.*

What is it?

Admins can use this permission to allow file sharing with only trusted domains. You can make an allowlist to restrict sharing, which you can create when you navigate to your Admin console home page.

Add a trusted domain to your Allowlist

1. In your Admin console, click on “Account.”
2. Go to “Domains,” then click “Overview.”
3. Click “Allowlisted domains.”
4. Click “Add new.”
5. Enter the domain, subdomain, or multiple domains separated by commas. You can add up to 200 domains at one time.
6. Click “Add.” Repeat to add more domains.
7. Click “Save.”



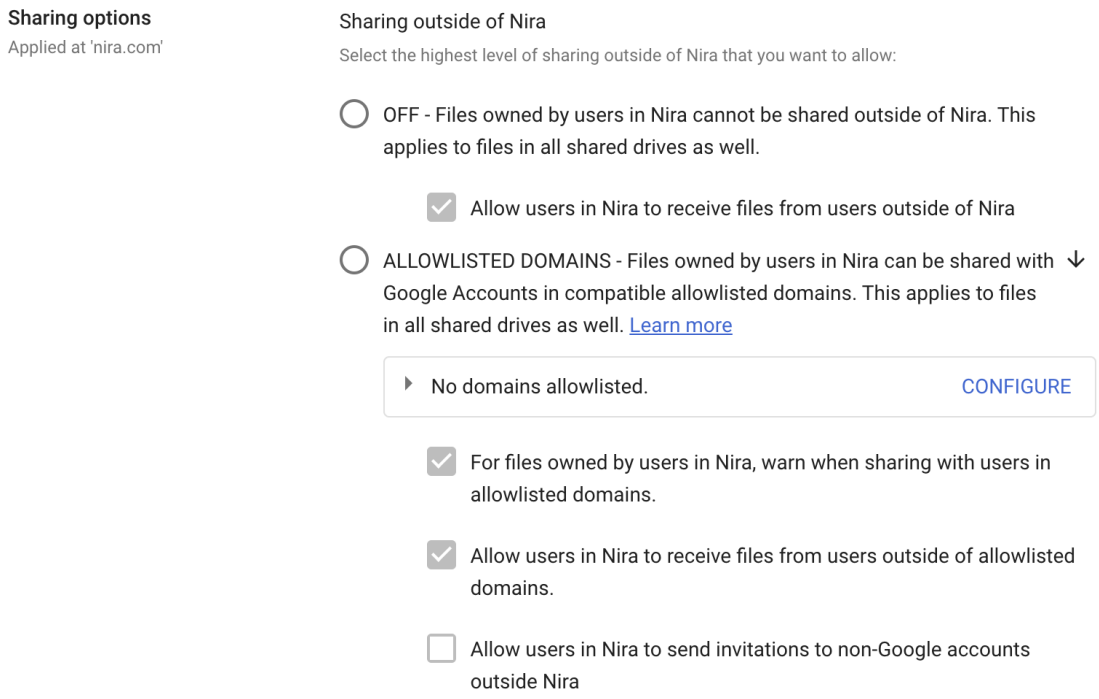
Why it matters

A variety of Access-Risk incidents stem from sharing with personal accounts and granting them access permissions. Being able to control this feature can help reduce the multitude of problems that come from sharing with domains you don’t trust, such as accidentally sharing with non-verified visitors. It’s a quick and safe way to keep certain documents more secure when sharing with external accounts, and actions like sending sharing invitations to visitors who are verified by a PIN number can help reduce risk.

How to do it

1. Go to “Apps” > “Google Workspace” > “Drive and Docs” > “Sharing settings” > “Sharing options”

2. For “Sharing outside of your organization,” click “Allowlisted Domains.”
3. You will then see several sharing options:
    - **Warn when sharing with users in allowlisted domains.**
    - **Allow users to receive files from users outside of allowlisted domains**—Users can open files from domains that aren’t on an allowlist and edit Docs, Sheets, and Slides stored on third-party storage systems.
    - **Allow users to send sharing invitations to people who are not using a Google Account**—Allows users to share with PIN-verified non-Google users in domains on your allowlist.
4. Click “Save.”



Restrict file sharing outside of your organization

Supported editions include *Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; G Suite Business; Essentials.*

What is it?

When you set this permission you can keep users from receiving or sharing things outside of your organization including:

- Invitations to collaborate or view externally-owned documents in Docs, Sheets, and Slides.
- Email attachments that users can send or receive that have been uploaded directly from devices and stored in Drive.

When you turn this off, users can't invite people outside the organization to view, comment on, or edit their files.

You also have the added option of keeping users from opening or editing files from outside of your organization or in third-party storage systems.

Why it matters
This method can be useful for keeping company data safe by regulating external sharing invitations and restricting inbound documents from external parties.

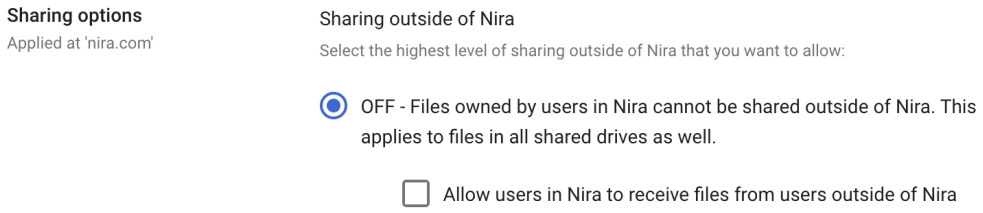
However, although it is possible to restrict external sharing outside of the organization, this method leads to risks of its own.

For example, as we saw with links, employees may still do workarounds to share invitations or email attachments, which can cause unintended negative consequences.

Be aware of the pitfalls of locking down employee permissions and educate your users about best practices.

How to do it

1. Go to “Apps” > “Google Workspace” > “Drive and Docs” > “Sharing settings” > “Sharing options”
    - You can either apply the setting to everyone in the organization by leaving the top organizational unit selected. Or you can choose a child organizational unit or a configuration group.
2. When you see “Sharing outside of your organization,” click “OFF.”
3. After you restrict file-sharing you also have the additional option to stop employees from receiving files from users outside of your organization. This means that users cannot open or edit files from outside of your organization or in third-party storage systems. Uncheck the “Allow users in your organization to receive files from users outside of your organization” box.
4. Click “Save.”



How Employees Can Set a Sharing Expiration Date

Many admins don't realize they can ask their employees to set an expiration date for specific files in My Drive, although this feature is not yet available for shared drives.

When the employee creates or shares a file, they can decide how long the accounts they're sharing with will have access to the file and what kind of access they can have.

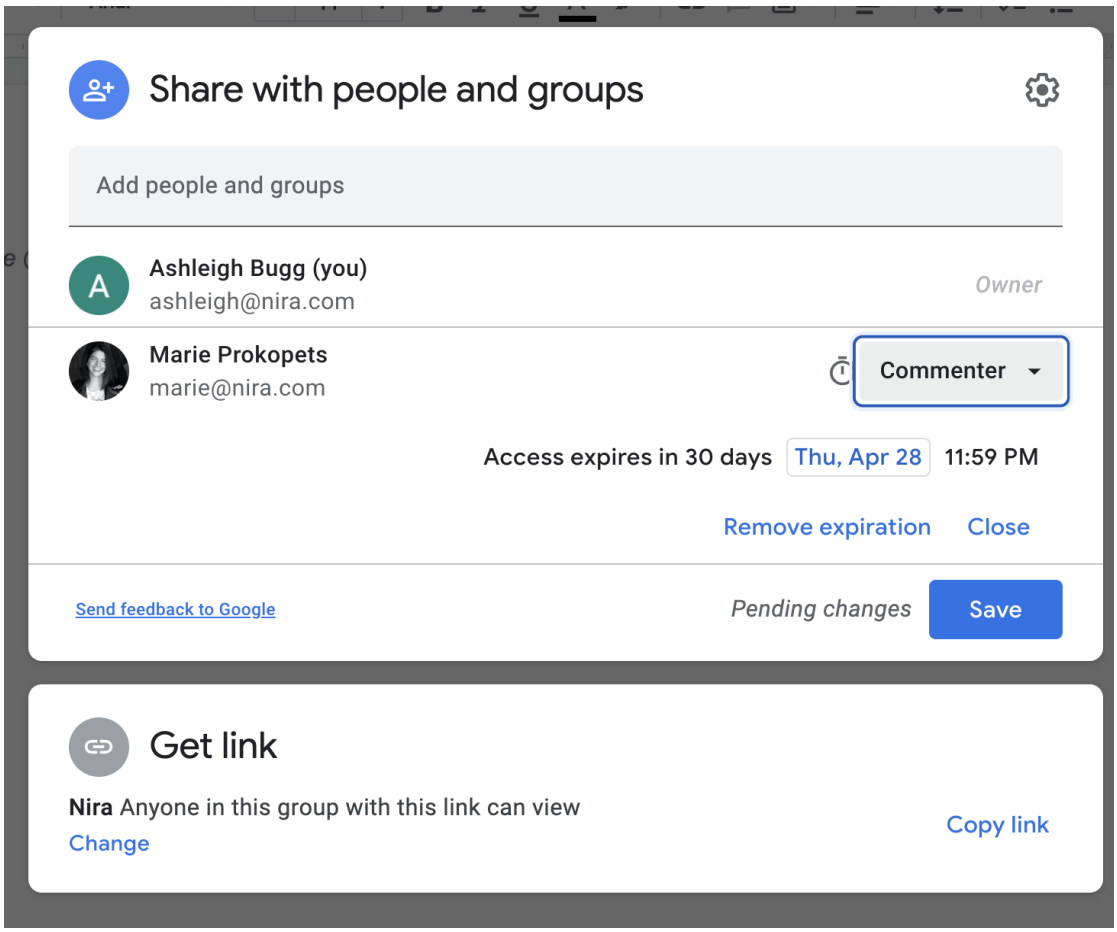
This comes in handy when working with vendors or customers who you know will end their contract by a certain time period. Employees can give them temporary access and then choose an expiration date within a year of the current date.

How to do it

1. Open a file in Drive, Docs, Sheets, or Slides.
2. Click "Share" > find the user you'd like to give temporary permissions to.

   Note if you haven't shared the file with that person yet, add the user's email and click "Send" or "Share." At the top right of the document, click "Share" again.

3. Next to the person's name, click the Down arrow > "Give temporary access."
4. Next to "Access expires," click a date to set as the expiration date. Choose a date within one year of the current date.
5. Click "Save."



What Security Risks Come from Sharing with Collaborators?

- **Risks with personal accounts:** Quite a few risks come with sharing files with and from personal email domains.

  For example, these types of accounts rarely have two-factor authentication set up.

  People are also less likely to change their passwords on personal accounts or they may use the same password for many years and across different sites and channels. These passwords may have been compromised but never changed.

  Additionally, if employees accidentally or purposely share files with their personal accounts and then leave the company, they'll still have access to company information and can do things like add more collaborators, copy the documents, or make changes. These practices make personal accounts more vulnerable.

- **Risks with outside accounts:** Sharing with external partners, customers, vendors, and companies also has risks. An organization may have certain compliance and security standards and processes that outside parties do not.

  Outside accounts may never be fully off-boarded, and it's rare for admins to have full visibility into how third parties are handling their company's documents and data. Additionally, outside accounts can often add their own personal accounts or make copies of documents that they should no longer have access to.

Here's What Employees Should Know

- It's best to add collaborators to documents instead of using Public or Company links.
- Grant collaborators the least amount of access needed. For example, it's good to give collaborators Commenter access rather than Editor access. They can still chime in with their ideas but will have fewer permissions overall.
- Set an expiration date for shared documents where the accounts you're sharing with don't need access in perpetuity, especially with third-party collaborators and vendors.
- Make sure you are reviewing old files and removing unnecessary access as you go.
- Do not share sensitive information with those who do not need access.

Now that we've looked at sharing via links and collaborators, we'll go over something our customers repeatedly ask about: shared drives and folders.

Chapter 3: Shared Drives and Folders

What are Shared Drives?

We often hear the most questions from our customers about shared drives in Google Workspace. That's why we devoted a seperate section to answer questions like:

What are shared drives? How do they work? Are permissions inherited? What do you need to know to keep documents safe when using them?

Shared drives vs. My Drive

In Google Workspace, documents and folders either live within a particular user's My Drive, or they reside in shared drives. Shared drives enable multiple people/accounts in an organization to create, manage, and organize documents and folders in a shared space.

However, this ease of collaboration also can lead to some pretty serious security issues.

What Security Risks Come from Using Shared Drives?

The biggest risk related to shared drives is permissions. That's because permissions on shared drives are inherited by all documents and folders within them. If an account that shouldn't have access gets added at the shared drive level, they'll have access to all documents and folders in that shared drive. If this happens with confidential information, like a folder full of salary information or a secret project, it can have more consequences than if someone were added to a single document.

Another challenge with shared drives is when members are never fully removed once a project is finished. After you complete a project in a shared drive, it's usually a good idea to remove members' access or downgrade them from a Manager, Content manager, or Contributor so that they have fewer permissions. (More on these permission types below)

It's also vital to make sure that users are not uploading anything to a company shared drive that shouldn't be there. For example, one admin shared that an employee once uploaded their tax forms to a shared drive, causing a multitude of headaches for the admin as they tried to find and remove access to these sensitive personal files.

Departments often have their own shared drives, and they need to be extra careful with who has access.

As we've noted before, if you have a department that regularly deals with sensitive customer or employee information such as HR and Finance, they will want to make sure their shared drives are not easily accessed by any external third parties, anyone in the organization that shouldn't be added as a collaborator, and that they do not have Company links.

Set Permissions on Shared Drives

In shared drives, users have different access levels or roles: Managers, Content managers, Contributors, Commenters, and Viewers.

Within a shared drive, permissions can vary at the folder or document level, where there can be additional Managers, Editors, Commenters, and Viewers. Permissions are also inherited from the folder level as well. So just because a top-level shared drive is secure, it doesn't automatically mean that the folders within the drive and the documents in those folders are secure.

We'll go over what each of these roles can do and how to change permissions in your organization.

Shared drive access levels

A **Manager** has the highest level of permissions in the shared drive.

They can perform any task including viewing and commenting on files; making and rejecting edits in documents; creating, removing, or restoring files in the shared drive; as well as adding people and groups to specific files or folders.

When an account creates a new shared drive, they are automatically a Manager. However, when new members are added to the drive, they are not Managers by default, but automatically become Content managers unless the default permissions are changed. There can be multiple Managers for a single shared drive.

Content managers have almost as many permissions as Managers, but they are unable to add people and groups to the drive or folders within it. They also can't move files and folders from a shared drive to another shared drive or to their My Drive. And they can't permanently delete files and folders in the trash.

On an overarching level, they are unable to add or remove people to or from shared drives/folders or delete a shared drive. Only Managers have this permission. There can be multiple Content managers for a single shared drive.

Contributors are also known as Editors at the individual file level. They have a good amount of privileges. For example, they can add people to specific files in the drive, but they are restricted from doing other tasks, like adding people to specific folders.

In the files themselves, contributors can make or approve edits. They are also able to create and upload files and create folders in the shared drive. However, they won't be able to move shared drive files or folders anywhere: not to My Drive, not to another shared drive, and not within the shared drive itself.

They are also unable to move any files or folders to the Trash or permanently delete them once they're in there. However, they do have the privilege of being able to restore files and folders from trash for up to 30 days.

Commenters only have two actions they can take in shared drives: they can view the shared drives, files, and folders, and they can add their comments to the files.

Viewers are only allowed to view the shared drive, folders, and files. They can offer no further input to the drive or its individual documents.

Permission level	**Collaborator type**				
	Manager	Content Manager	Contributor	Commenter	Viewer
Can view shared drives, folders, and files	✅	✅	✅	✅	✅
Can comment on files in shared drives	✅	✅	✅	✅	❌
Can make edits, approve edits, and reject edits in files	✅	✅	✅	❌	❌
Can create and upload files, and create folders within shared drives	✅	✅	✅	❌	❌
Can add accounts and groups to specific files in shared drives	✅	✅	✅	❌	❌

Can add accounts and groups to specific folders in shared drives	✅	❌	❌	❌	❌
Can move files and folders from a shared drive to their My Drive	✅	❌	❌	❌	❌
Can move folders and files within a shared drive	✅	✅	❌	❌	❌
Can move folders and files from one shared drive to another shared drive	✅	❌	❌	❌	❌
Can move shared drive folders and files into the Trash	✅	✅	❌	❌	❌
Can permanently delete folders and files that are in the Trash	✅	❌	❌	❌	❌
Can restore folders and files from trash (for up to 30 days)	✅	✅	✅	❌	❌

Source: Google

For all of these permission types, access to the shared drive or the folders within the shared drive grants the same level of access to all folders and documents within it.

What Admin Privileges Should You Be Aware Of?

Supported editions for this feature: Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; Nonprofits; G Suite Business; Essentials.

Admins with the “Drive and Docs” settings privilege have lots of control in shared drives.

Remember that when users create shared drives, the new drives automatically inherit Google Drive sharing settings from the top-level organizational unit, which overrides an individual user’s organizational unit settings.

For example, let’s say an employee is in a child organizational unit that has external sharing restrictions turned off. However, your company’s parent organizational unit has external sharing turned on.

When the employee is added to a shared drive, they will be able to share documents in the shared drive with external people outside of your organization, unless you restrict them.

Let’s dig deeper into admins’ privileges in shared drives:

Turn shared drive creation on or off for your organization

What is it?
As an admin, you can allow people to create shared drives for specific organizational units. For example, someone wants to create a shared drive for just the Sales team.
You can also turn this feature off for child organizational units. However, let’s say you have a child organizational unit for Engineering that has shared drive creation turned off, but someone in the Engineering unit needs to be added to a shared drive that’s owned by the Product team. People outside of the Engineering organization may still add the Engineering employee to the Product shared drive. And the same is true even if it’s a shared drive that’s outside of your company.

Why it matters
Shared drives aid with ease of collaboration and the ability to quickly find the right documents. Rather than having a lot of individual files floating around that are owned by one account and stored in their My Drive, a shared drive keeps all of a group of people’s or a departments’ documents in one centralized place. That’s why it’s so important to make sure that the right accounts have the proper permissions in their shared drives.

How to do it

1. In your Admin console, go to “Apps” > “Google Workspace” >”Drive and Docs.”
2. Double-check that Drive is turned on for your organization.
3. Click “Sharing settings.”

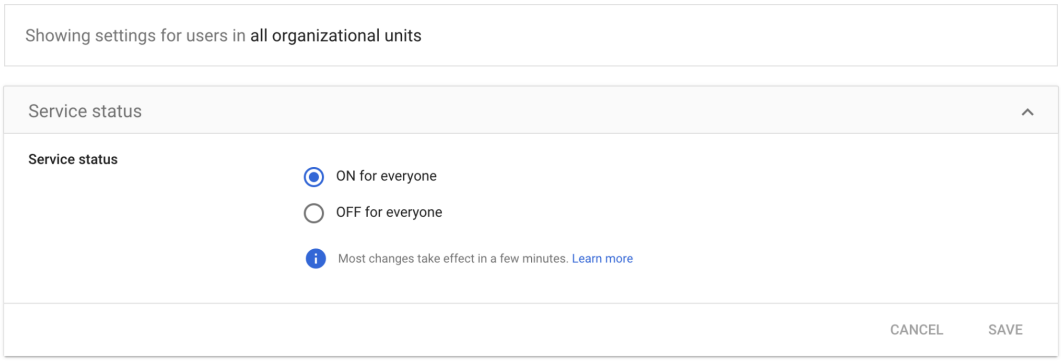
4. To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select a child organizational unit.
5. Click “Shared drive creation.”
6. Check or uncheck the “Prevent users in your organization from creating new shared drives” box.
7. Click “Save.”

Manage shared drives users

What is it?
You have several options when managing shared drives. You can manage the members of the shared drive by removing members or changing their access levels. You can also add new members to shared drives and then set their access levels.

Why it matters
Being able to easily manage members and having visibility into who is sharing what and when is one of the best tools when combatting Access-Risk. You’ll be able to quickly remove a member who no longer needs access or change the access-level permissions of current members. For example, if an employee transfers departments within the company and should no longer be able to access the shared drive for their old department.

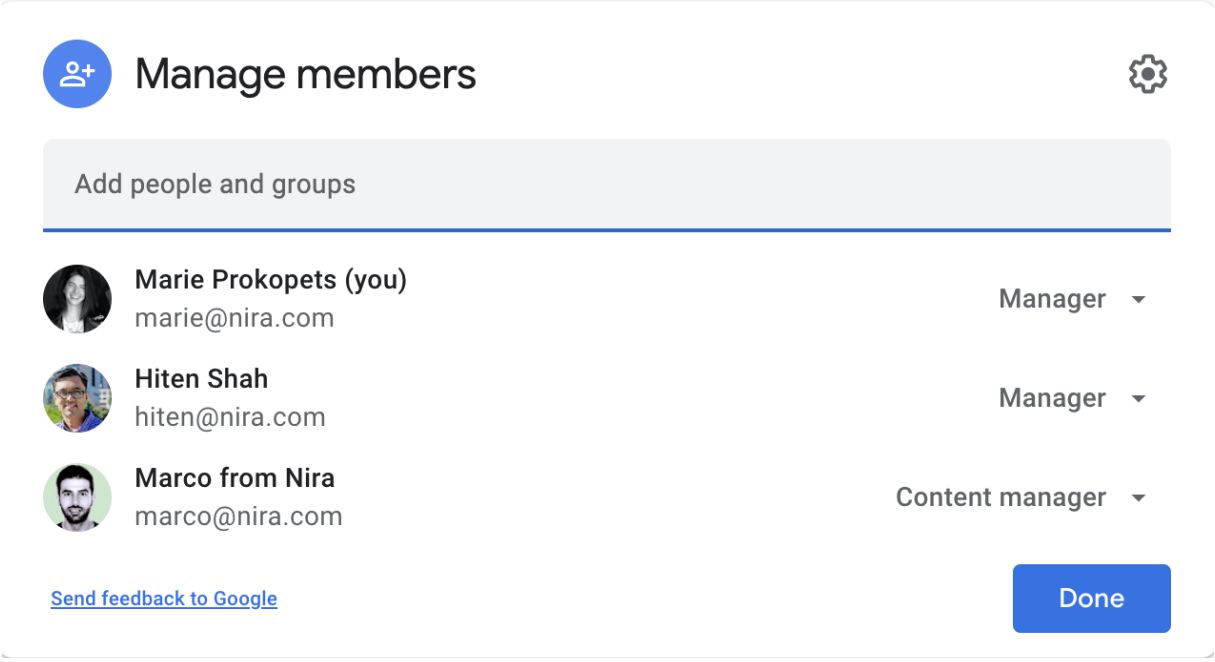
How to do it
1. “Apps” > “Google Workspace” > “Drive and Docs.”
2. Go to “Service status” and double-check that Drive is turned on. The status should read “ON for everyone.”



3. Click “Manage shared drives.”
4. Choose a shared drive and click “Manage members.”

Here's where you have several options:

- You can remove a member from the shared drive or change their access levels, by clicking the down arrow and choosing an option.



- You can also add new members to the shared drive:
    - Click "Add people and groups" and enter the names or email addresses of the people or groups you want to add. If you want to add more members than your limits will allow, it's a good idea to add Groups rather than every individual email account.
    - Set access levels by clicking the "Down arrow" and choosing an access setting. Remember by default, shared drive members can upload, edit, and delete files and invite other members.
    - In the Message field, you can enter a custom message for the email notification. Or you can uncheck the "Notify people" box to forgo the welcome message with a link to the shared drive.
    - Click "Send."

Control default sharing of shared drives content

What is it?

You have several options when you define the default sharing restrictions for shared drives. These are the default restrictions when you first create a shared drive, but can easily be changed or overridden if needed.

As an admin, you can keep employees from creating new shared drives or making changes to existing shared drive settings. You can also keep external users, as well as people in your company who are not members of the shared drive, from accessing shared drive files.
If you move a file into a shared drive, the file will retain its original sharing permissions and user roles. For example, if the document was able to be edited by anyone in the company, then it still will be.

However, the shared drive's restrictions do come into play. For example, if a shared drive restricts people outside the organization from accessing the shared drive's content, external users will be removed from files in that shared drive in the future.

Why it matters
The ability to control who has access to your files in shared drives, as well as the shared drive settings themselves, gives admins an added tool to boost their company's document security. Something as simple as changing the default sharing restrictions can help employees from accidentally giving access to sensitive information.

For example, someone may be a full-access member in your shared drive, but you still wouldn't want them to be able to change the shared drive settings or allow them to override any of the default restrictions for individual shared drives.

It's important to be aware of what happens to files when shared drive restrictions are set or changed, and what user permissions might still remain unchanged.

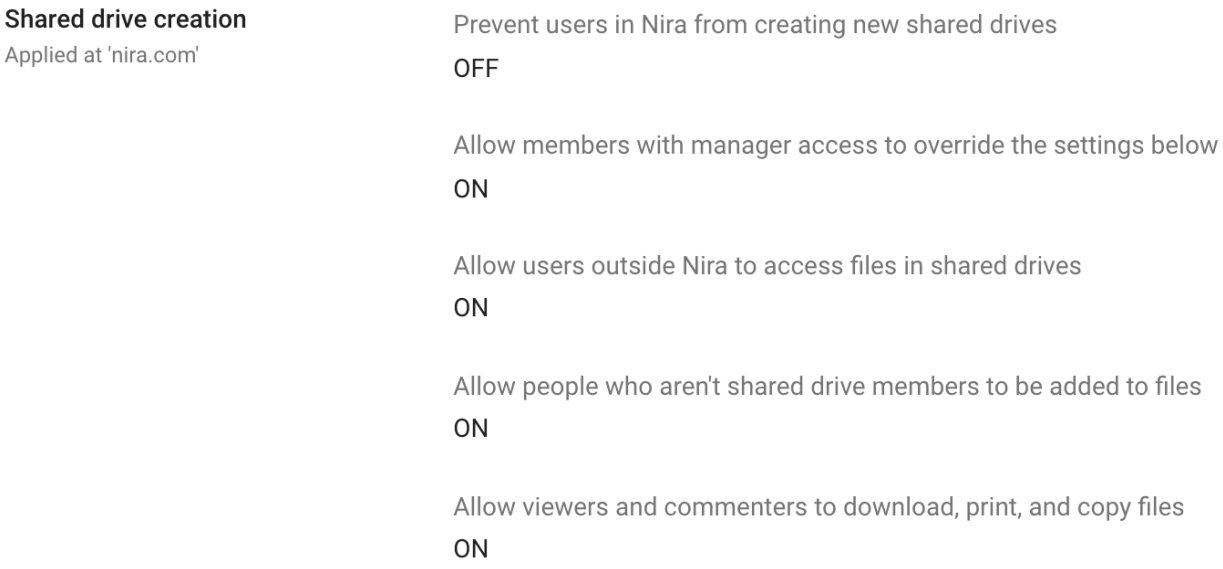
How to do it

1. In your Admin console, go to "Apps" > "Google Workspace" > "Drive and Docs."

2. Select "Sharing settings."

    - To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select a child organizational unit or a configuration group.
3. Next to Shared drive creation, select the default restrictions for all new shared drives:
    - Prevent users in your organization from creating new shared drives
    - Prevent full-access members from modifying the shared drive's settings
    - Prevent people outside your organization from accessing files in the shared drive
    - Prevent non-members of the shared drive from accessing files in the shared drive

- Prevent commenters and viewers from downloading, copying, and printing files in the shared drive



Manage access for an existing shared drive

What is it?
As an administrator, you have certain shared drive settings you can manage. You can:

- Allow shared drive members with Manager permissions to modify shared drive settings.
- Decide if outside people who are not members of the shared drive can be added to files.
- Control if viewers and commenters can download, print, or copy files.

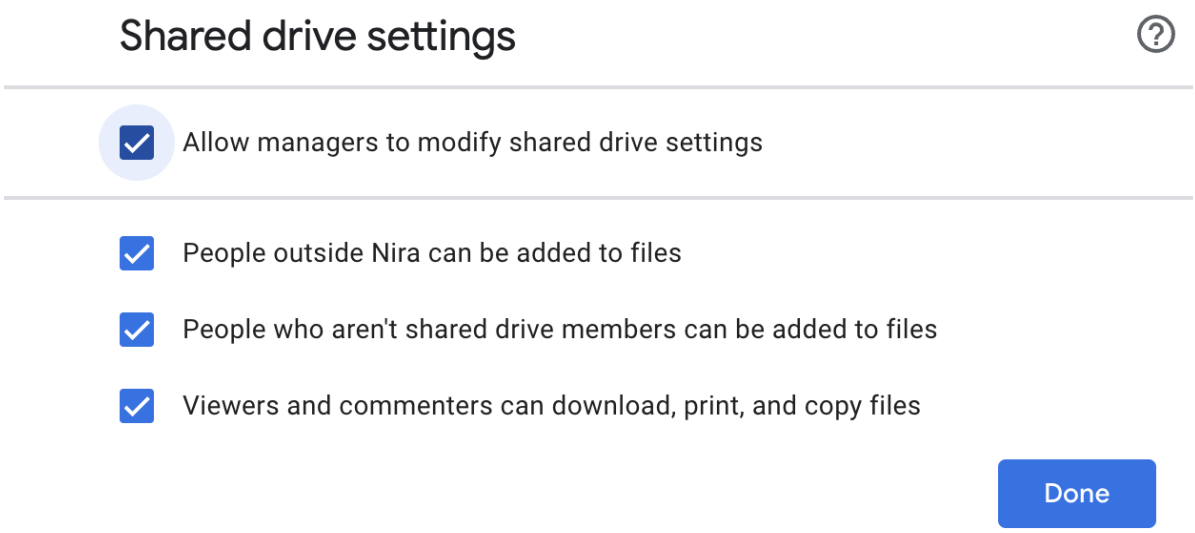
Why it matters
You've set up all your shared drive settings just the way you want them for best security practices. You're feeling confident that your sensitive files are safe and protected from negligent or unauthorized access.

And then you realize that Managers of shared drives can modify your settings without your knowledge, or people who are outside of your organization can be added to files by other members.

This may be necessary to keep workflows running smoothly and efficiently. However, depending on your policies and the level of security needed, you might want to turn off some of these settings for better control over who can change access permissions or be added to files.

How to do it

1. Go to “Apps”> “Google Workspace”> “Settings for Drive and Docs”>”Manage Drives and Docs”
2. Hover over the shared drive, and click “Settings.”



3. Admins can now choose whether to allow managers to modify shared drive settings:

- **Allow managers to modify shared drive settings:** This prevents full-access members from modifying shared drive settings. It keeps people from overriding the default settings for the shared drive.

  If admins select this option, they can go further and control the following:

  - **People outside the company can be added to files:** Allow or prevent external people from accessing files in the shared drive.
  - **People who aren’t shared drive members can be added to files:** Allow or prevent shared drive members from giving non-members access to files in the shared drive.
  - **Viewers and commentators can download, print, and copy files:** Allow or prevent commenters and viewers from downloading, copying, and printing files in the shared drive.

Allow users to move content to a shared drive

Please note only these editions are supported for this feature: *Business Standard and Plus; Enterprise; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; Nonprofits; G Suite Business; Essentials.*

What is it?
Admins can allow users in their organization with Editor access to move content. They may be able to move content from their My Drive to a shared drive. Or from one shared drive to another shared drive.

There are several points to consider before allowing users to move content to and from shared drives. First is the concept of Ownership. When a user creates a file, they are automatically the owner of that file.
But when they move that file to a shared drive, they lose this ownership. Now, your organization "owns" the file.
When the file is moved, access levels may also change, as we went over in the section on Shared drive access levels. Who is able to move content and where they can move it depends heavily on these access levels.

If you want to allow users to move files from My Drive to a shared drive:

- The user must have Edit access to the file they are trying to move. They must also be a Contributor, Content manager, or Manager in the shared drive they want to move the file to.
- The owner of the file must be a member of the shared drive where they are moving it.
- Please note that this may conflict with sharing permissions you set up to control how content is shared outside your organization.

If users want to move files from one shared drive to another:

- They must have Manager access in the shared drive they're moving content from, and Contributor, Content manager, or Manager access in the shared drive they're moving content to.

It's also vital to be aware of who has access to the file that was moved. When a file is moved, everyone in the shared drive now has access as well as the people it was directly shared with before the file was moved.

Let's say the original owner of the file is not in the shared drive. They would lose ownership of the file but still be able to access and edit the file as its creator.

What about if you're dealing with users outside of your organization?

Admins cannot move files owned by external users to a shared drive even if that user is a member of the destination shared drive. Meanwhile, external users can move individual files to shared drives in your organization if they have the necessary permissions.

Why it matters

Moving content around at any time has its risks. However, moving content to shared drives where users may not be thinking about who already has access, or who could have access in the future, can open the organization to all sorts of security issues.

It's important to be aware of who can share content in your organization's shared drives, and what permissions they need. For example, users will need Edit access for any files they want to move.

Also, to move files from one shared drive to another shared drive, users need to have Manager access in the shared drive they're moving content from, and Contributor, Content manager, or Manager access in the shared drive they're moving content to.

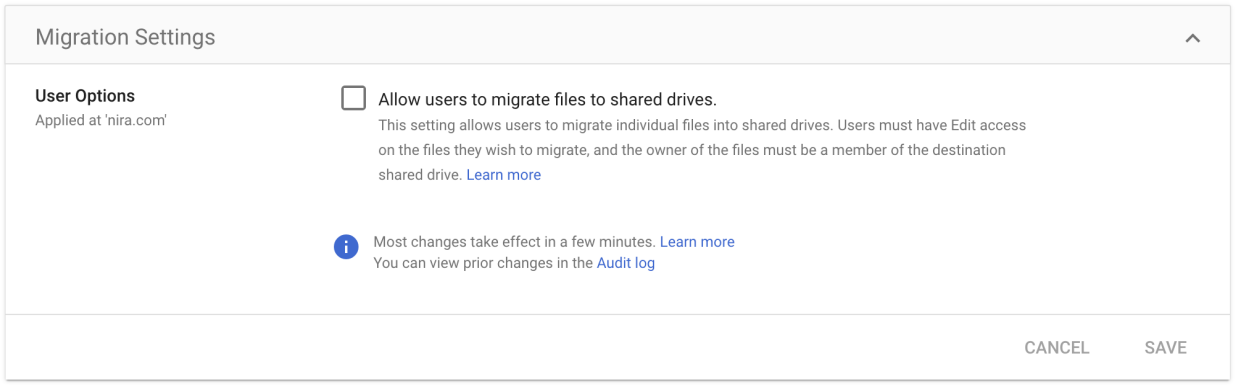
How to do it

1. In your Admin console, go to "Apps" > "Google Workspace" > "Drive and Docs."

2. Click "Migration settings."
    - To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select a child organizational unit or a configuration group.
3. Next to "User options," select "Allow users to migrate files to shared drives."

    Remember users who are moving files from My Drive to a shared drive must have Edit access on the files they are moving, and they must have Contributor, Content manager, or Manager access in the shared drive they are moving the files to. Finally, the owner of the file must be a member of the destination shared drive.

4. Click "Save."



Shared Drives FAQs

At Nira, we've received a lot of questions surrounding shared drives. Here are answers to the most frequently asked ones:

- **Can users add Public links or Company links to shared drives?**
  Shared drives do not have Public or Company links, they can only be Restricted, meaning only collaborators can access shared drives using a link. However, documents and folders within shared drives can have Public or Company links. As we've gone over before, we don't recommend using Public and Company links for sensitive information.

- **How much visibility do users have in shared drives?**
  People with access to the shared drive can view everything in that shared drive unless they are removed as a collaborator on the drive or folder.

- **What kinds of accounts can be added to shared drives?**
  Any account types can be added to shared drives. If you add an external user to a shared drive, they must have a Google account and be signed in to Drive to access the shared drive.

- **What happens when you suddenly stop sharing a shared drive with external parties?**
  When you add an external account to a shared drive, they receive access to all the documents and folders within the shared drive. If you later remove that external account from the shared drive, they will be removed from all the documents and folders in the shared drive as well. It's not possible to remove the external account from individual documents within the shared drive. Their access must be removed at the overarching shared drive or folder level. The only way to keep them from having access to the documents and folders is to remove them from the shared drive.

- **Can I remove a collaborator on a shared drive from the documents within the shared drive?**

  Since permissions are inherited from shared drives to all items within them, the accounts will need to be removed from the shared drive itself. They cannot be removed from individual items within the shared drive. They must be removed at the top-drive level.

- **How do you deal with multiple members in shared drives?**

  It's important to be aware of the various roles that are available in shared drives. For example, there can be multiple Managers, Content managers, Contributors, etc. for one drive. Knowing who is a member of the shared drive and what level of access permissions they have is key to keeping company documents secure.

- **Can shared drives be owned across multiple domains?**

  Multiple domains can be Managers on the same shared drive. Either domain can remove the other from the shared drive and all of its folders and documents, no matter who originally first created the shared drive. This is why it's so important to manage shared drive permissions and ensure that Manager-level access is only given when absolutely necessary and is revoked when access is no longer needed.

Folders in Shared Drives

Before we move on, let's examine folders. Remember you can create folders in your My Drive as well as in specific shared drives. You can also move files to folders from various locations.

Here are some things to remember when it comes to folders in shared drives:

- Your employees can't move folders from My Drive into a shared drive even if they have Manager-level permissions.

- But, employees are able to create new folders in a shared drive if they have required permissions to do so.

- Admins can only move folders that they or users in their organization own.

- When a folder is moved from one shared drive to another shared drive, the users with access to the shared drive can access the files within it (even if they previously didn't have access.)

- To move folders from one shared drive to another shared drive, users must have Manager access in both shared drives.

- If a previously shared folder is moved to a shared drive, users who had access to that shared folder don't automatically retain access. To gain access, they must be added as members to the shared drive.

- When an admin moves a folder to a shared drive, all of its files will be visible to all members of the shared drive, including hidden files.

When it comes to external users and folders in shared drives, please remember:

- External users (including users with personal Google Accounts) can't move folders to shared drives in your organization even if they have Manager access.
- Admins can't move folders owned by external users even if the external user is a member of the destination shared drive.
- Admins can't move internally owned subfolders that are part of an externally owned folder.
- When an admin moves a folder to a shared drive, everyone with access to that shared drive now has access to the files within that folder, including external accounts with access.

Move Drive folders to a shared drive as an admin

Please remember that admins can only move folders that users in their organizations own.

1. To move existing folders, ask employees to grant your admin account Viewer access or higher to the folder/s you want to move.

    - *Note: If you're using a real-time access control system, you can make this change there instead. For more information about access control systems see Chapter 8.*
2. Next, ask the employees to add you as a Manager of the destination shared drive.
3. Open drive.google.com and sign in with your Admin account.
4. Open "Shared with me" to view the folders you want to move and expand the "Shared drives" folders to which you're moving them.
5. Drag the "Shared with me" folders to the "Shared drives" folders.
6. Accept the confirmation request to begin the moving process.

Restrict users from moving shared drive content outside your organization

What is it?
When moving content, admins have several options when sharing from a shared drive in the organization. Admins can control sharing to:

- A shared drive in another organization
- An individual's My Drive in another organization

Admins can also control if someone in the organization can share a file from their My Drive to an external organization's shared drive.

Why it matters
Sharing files to external shared drives or My Drive comes with risk. It's important to be aware of the various restrictions that can be set for employees, as well as the ways they may try to get around them to more easily do their jobs. This comes into play when deciding user roles in shared drives. For example, admins can choose who will have Manager access or who will only be able to view or comment.

Remember, admins can lock all external shared drive sharing down, however, this may cause employees to take riskier actions like recreating a document in their personal Google account and sharing it that way instead.

How to do it
1. Go to "Apps" > "Google Workspace" > "Drive and Docs."

2. Select “Sharing settings” > “Sharing options.”
3. Select the right organizational unit or group.
4. Go to “Distributing content outside of your organization.”

   You now have three options:
   - Anyone
   - Only users in your organization
   - No one

   For “**Anyone**,” admins can control if:
   - Shared drive Managers can move files from that shared drive to a Drive location in a different organization.
   - Members of the selected organizational unit or group can move content from their My Drive to a shared drive owned by a different organization.

   For “**Only users in your organization**,” you have the same two options, but it doesn’t apply to external users outside your organization:
   - Shared drive Managers can move files from that shared drive to a Drive location in a different organization.
   - Members of the selected organizational unit or group can move content from their My Drive to a shared drive owned by a different organization.

   For “**No one**,” you can completely lock shared drive movement down:
   - Files on a shared drive cannot be moved to a Drive location in a different organization.
   - No one in the selected organizational unit or group can move content from My Drive to a shared drive owned by a different organization.
   - No one in the selected organizational unit or group can create files on a shared drive owned by another organization.

5. “Click Save.”

Here’s What Employees Should Know

- Be extra careful about who you add to shared drives as collaborators, since permissions on shared drives are inherited by all items within the drive.
- Shared drives let you assign Manager, Content manager, Contributor (aka Editor), Commenter, and Viewer permissions. Be careful when giving someone Manager permissions because it will let them have the highest level of permissions to make changes to the drive.
- **Always grant collaborators the least amount of access needed**. Opt for Commenter or Viewer access over Editor access where possible.
- Make sure to review older shared drives and remove unnecessary access as you go.
- Do not drop sensitive information into shared drives unless everyone in that shared drive should have access to that information.
- Be mindful that other people or accounts could be added without your knowledge to a shared drive in the future and could gain access to all the information in that drive.
- Shared drives cannot have Public or Company links. However, folders within shared drives can have Public or Company links, so be careful when adding those links to folders that reside in shared drives.

Now that we've gone over using shared drives and the various admin permissions available to your company, we'll briefly look at document retention.

Chapter 4: Document Retention

Document Retention and Policies

What is it?
Document retention allows companies to create policies for how to handle their files and documents after a certain period of time.

Companies set retention policies to stay compliant within legal frameworks, mitigate Access-Risk incidents, and keep organized and up-to-date with the most relevant information.

These retention policies dictate that companies will take actions like automatically deleting files after a certain number of years have passed, or moving documents to a new directory or system to archive them.

Why it matters
One of the biggest reasons companies implement a document retention policy is to stay compliant. A multitude of U.S. federal laws and regulations pertain to document retention, including HIPAA, the Fair Labor Standards Act, and the Employee Retirement and Income Security Act.

You'll want to keep certain documents for as long as relevant laws and compliance frameworks require. On the flip side, once that time period is up, it's important to purge documents and files that are no longer necessary to your business needs, to mitigate risk and stay compliant.

Document retention policies can also keep you better organized and even save your organization time and money, particularly if the process of retention policy enforcement is automated or delegated to employees.

How to do it
In Google Workspace, document retention is really only possible through an extra paid service called Google Vault.

Document Retention through Google Vault

For Vault to search and retain a user's data, employees need a Google Workspace license and a Vault license. These plans have Vault's licenses included: *Business Plus, Enterprise, Enterprise Essentials (domain-verified only), Education Fundamentals and Plus, and G Suite Business*. You can also buy Vault add-on licenses for the *Frontline and G Suite Basic* plans.

Google's default settings require that data stays in Workspace until an admin or user deletes it.

In Google's updated Data Retention Policy, end-users' Drive files in the Trash will be deleted after 30 days. However, in Workspace, admins will be able to restore items deleted from a user's trash for up to 25 days.

How Vault retention works

Admins can keep data for as long as is needed or remove it when keeping the data is no longer necessary. Admins can change the settings to retain files even after they are deleted by employees or employees empty their Trash.

Admins can also set retention rules to automatically delete data after a certain period of time and remove it from all user accounts and Google systems.

However, admins should be extremely careful when configuring retention rules, as important information could be immediately and permanently deleted.

Retain files in Drive in Vault

In Vault, you can set two types of retention rules: custom and default.

Custom data retention rules allow data to be kept for a set amount of time. In Drive, custom rules can be set by the dates the documents were created, trashed, or last modified.

Choosing dates based on when documents were last modified addresses the issue of stale documents. Meanwhile, setting custom rules by when documents were created helps with compliance requirements.

A default retention rule is used when organizations need to keep all company data for all licensed accounts for a set period of time. This means that you can't apply default retention rules to only specific accounts or time periods.

Remember, you can have only one default retention rule per service, and it only applies to files in Drive that aren't covered by a custom rule or hold.

How to set a custom retention rule

1. Visit vault.google.com
2. Go to "Retention"> "Custom Rules"> "Create"

3. Click “Drive” and “Continue.”
4. Choose from an organizational unit, all shared drives, or specific shared drives:

    - You can choose from an **organizational unit** such as Sales, Marketing, etc., and then you have the additional option of including shared drives by selecting “Include results from shared drives.”
    - You can choose to include **all shared drives** in your organization.
    - You can select **shared drives from specific accounts**. Enter the names of one or more accounts and click “Find.” Select one or more shared drives and click “Add.”

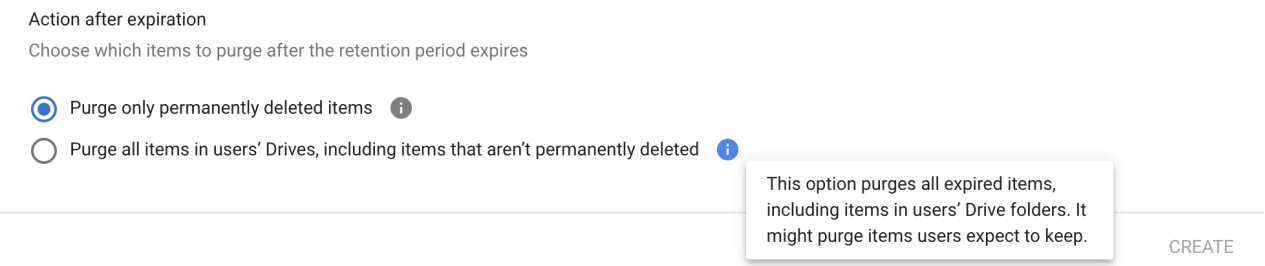
5. Click “Continue”
6. Choose how long to keep your files:

    - If you select “Indefinitely,” you will permanently retain documents under this rule.
    - If you select “Retention period,” you can choose a number of days to retain your documents and select the reference time for the start of the period.

7. Decide what to do with files after the retention period:

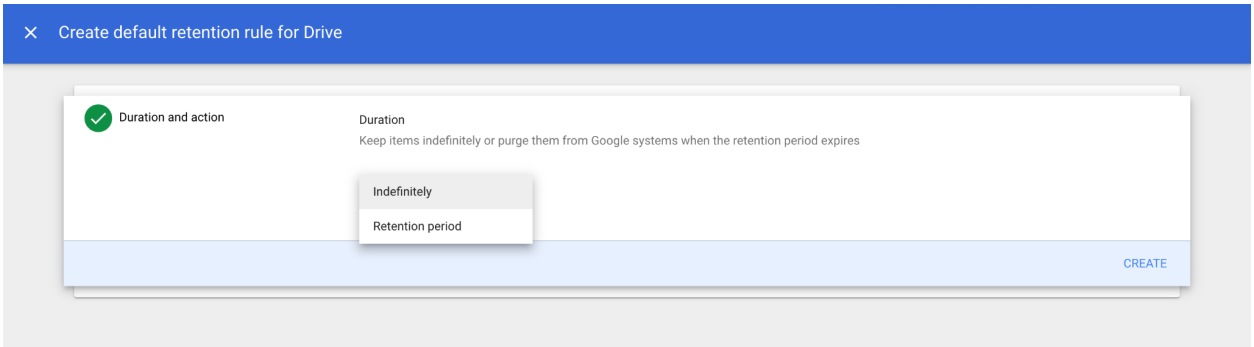
    - Choose option one in the modal to remove only the files that are already emptied from the users' Trash folder.
    - Choose option two in the modal to remove all files, including files that aren't deleted.

8. Click “Create.”
9. For accounts with a retention period, you must confirm that you understand the rule’s effects. Check the boxes and click “Accept” to create the retention rule.



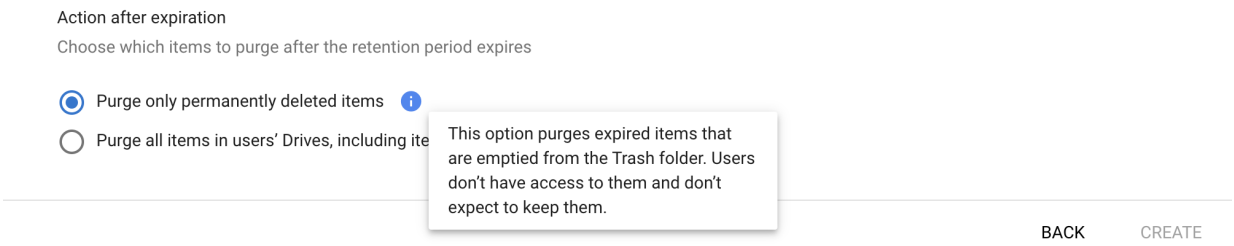
How to set a default retention rule

1. Visit vault.google.com.
2. Click "Retention."
3. Click "Drive."
4. Choose how long to keep files:
    - If you select "Indefinitely," you will permanently retain documents under this rule.
    - If you select "Retention period," you can choose a number of days to retain your documents and select the time for the start of the period.



5. Decide what to do with files after retention period
    - Choose option one in the modal to remove only the files that are already emptied from the users' Trash folder.
    - Choose option two in the modal to remove all files, including files that aren't deleted.

6. Click "Save." You must then confirm that you understand the rule's effects. Check the boxes and click "Accept," to save the retention rule.



Having document retention rules and policies in place can help greatly with the Access-Risk issues that stem from having stale documents or not properly following compliance protocol.

Here's What Employees Should Know

- Documents get stale when their contents haven't been changed in months or even years.
- There are lots of risks associated with older documents, including:
    - Stale information that's no longer relevant.
    - Access that's no longer needed—whether it's from internal accounts, personal accounts, or other domains.
    - Public or Company links that should be set to restricted, because no one is using the documents anymore.
- If your company has a document retention policy that applies to you, make sure to follow it by deleting old documents or using the mechanisms laid out in the retention policy (like archiving documents or transferring ownership).
- If you are exempt from the policy because of the nature of your work (e.g. you are a part of a legal hold because of a special project), or you need to keep information and not delete it, please make sure to follow those guidelines.

Next, we'll go over transferring ownership.

Chapter 5: Transferring Ownership

How Employees Can Transfer Ownership

What is it?
We talked before about the concept of “owners” of documents. Employees are able to transfer ownership of their files and folders to anyone else in their organization, and the new owner doesn’t even have to consent for the transfer to happen.

Remember, even if a user transfers ownership of a folder, they still own the individual files inside. If they want to fully transfer folder ownership, they’ll need to transfer ownership of all the individual files inside the folder.

Once they transfer ownership of a file, they can’t transfer ownership again, even back to themselves, and they’ll no longer be able to permanently delete that file from Google Drive.

Why it matters
It’s important to be careful when transferring ownership because owners have more control over access permissions in documents than other users with lower permission types. For example, if an employee accidentally transfers ownership of a document with sensitive information to the wrong employee, they can’t transfer ownership again, but they’ll be able to share and set access permissions.

It’s also important to be aware of ownership when employees are about to leave the company or the organization is about to end a contract with an external third party. You may want to retain the former employee's work, so you’ll need to transfer ownership of their documents to someone else in your organization.

How users can transfer ownership

1. Open Google Drive and click the file or folder that will be transferred.
2. Click “Share.”
3. To the right of a person the file has been shared with, click the “Down arrow.”
4. Click “Transfer ownership.”
5. Select “Yes.”

After a user makes someone else the file’s owner, they can still edit the document unless the new owner changes their permissions.

How to Transfer Drive Files to a New Owner as an Admin

Transfer one file

Admins have two options for transferring individual files: the original owner can transfer ownership, or you as an admin can do it. Please note that as an admin, you can only transfer an individual file using Google Drive APIs.

Admins can transfer file ownership from one Google Workspace account to another in the same organization. To transfer ownership of a file in My Drive, users are advised to “create or update the file’s permission with the ‘owner’ role and set the ‘transferOwnership’ query parameter to ‘true.’ When a file is transferred, the previous owner’s role is downgraded to ‘writer.’”

Admins can also use Google Drive APIs to transfer file ownership from one consumer account to another consumer account. However, in this case, the new owner must consent to the transfer before it can take place.

Transfer all of a user’s files

Admins can also transfer ownership of all of a user’s files. This comes in handy if an employee leaves the company and policy dictates that all their files are transferred to someone new before their account is deleted. However, be aware that the original Owner can still edit the document until you delete their account or the new owner changes their permissions.

1. Go to your Admin console.
2. Go to “Apps”> “Google Workspace” >”Drive and Docs.”
3. Click “Transfer ownership.”
4. In the “From user” field, write the current owner’s email address and select the user.
5. In the “To user” field, enter the new owner’s email address address and select the user.
6. Click “Transfer Files.”

After the transfer is complete, even if the last owners' accounts are deleted, you can still find the document's ownership history in the version history or the Drive Audit Log, which is found under Reports in your Admin console: “Reporting” > “Audit” > “Drive.”

Here’s What Employees Should Know

- Transferring ownership is the process of taking documents owned by your account and giving another account ownership of those documents.
- Remember, once you’ve transferred ownership of a file, you can’t transfer it again, not even to yourself. You also won’t be able to permanently delete that file in Google Drive.
- When you transfer ownership from yourself, you will still be able to edit the file you used to own, unless the new owner changes your permissions.
- If you transfer ownership of a folder, after the ownership transfer is complete, you will still own all the individual files inside the folder. You must also transfer ownership of all the individual files if you want their ownership to change.

Next, we’ll go over creating and managing labels.

Chapter 6: Managing Labels

Labels are metadata that admins can define to help their employees better find and organize documents. They can also be used by admins to apply certain policies in Drive, as well as classify content and find files more quickly.

Using labels helps with things like reporting and auditing but can lead to Access-Risk issues if label names that anyone in the organization can view contain confidential information.

Labels related to classification of sensitive data help admins understand what types of audiences documents should have. For example, if a document is classified as Confidential using a label created by an admin, then access to that document should be limited. They also work with Google’s DLP capabilities and will eventually work with Vault retention rules, too.

Labels related to a company’s data classification policy are essentially a way for employees to help admins know how sensitive files are. Admins can then put more focus on the sensitive files with the highest risk.

Labels can also be used to help classify files based on the departments that own them or based on the project the files are related to. These labels make finding those documents easier for employees, since they show up for employees when they search for documents within Drive.

They also help organize and group files without needing to put them all into the same place, like a specific folder or shared drive.

We'll go over how to turn labels on and off, how to create them, how employees can use them, and how to manage label permissions.

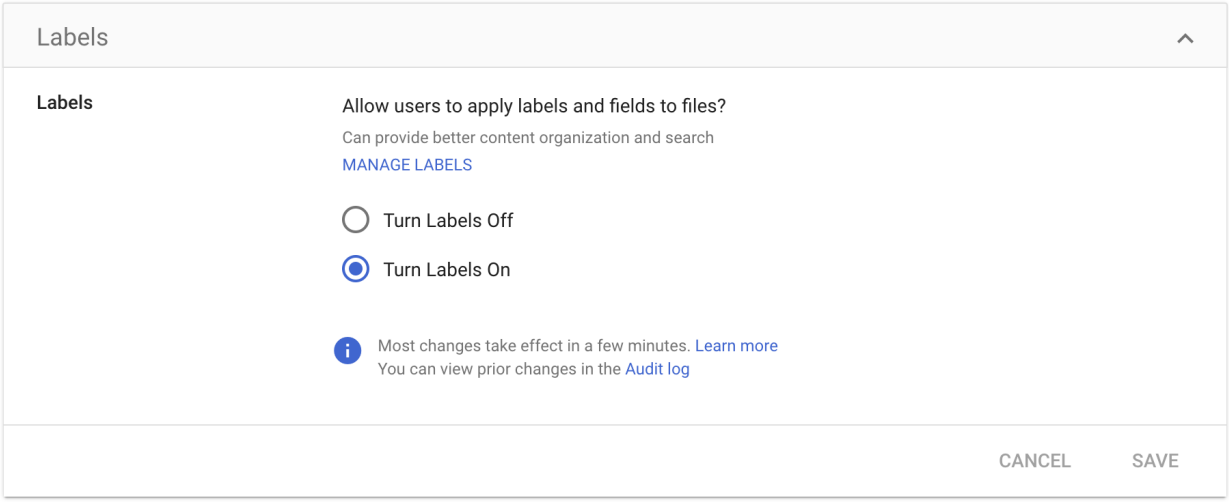
Turn Labels On or Off for Your Organization

What is it?
As an admin, you have the power to turn labels on and off for your employees. If labels are on, admins can create labels, and employees can add them to their documents. For example, any admin can create new labels and manage the label taxonomy. When labels are on, users with Edit access can edit labels, apply published labels, and even edit the fields for those labels. People with Viewer access can't edit, but they are able to view labels applied to files. Both users with View and Edit permissions can search for specific labels or fields to find content in Drive.

Why it matters
Turning labels off could help combat Access-Risk issues like accidentally writing confidential information in a field name, but it also keeps users and admins from being able to easily organize and find files in Drive. It's better to be aware of best practices like making sure labels are properly named and ensuring the right employees have editing or viewing permissions.

How to do it

1. From the Admin console, go to "Apps" > "Google Workspace" > "Drive and Docs."
2. Click "Labels."
3. Turn labels on or off.
4. Click "Save."



Note: You can let certain people manage metadata without any other admin privileges, by creating a custom administrator role for only the Manage Labels privilege.

Create Labels

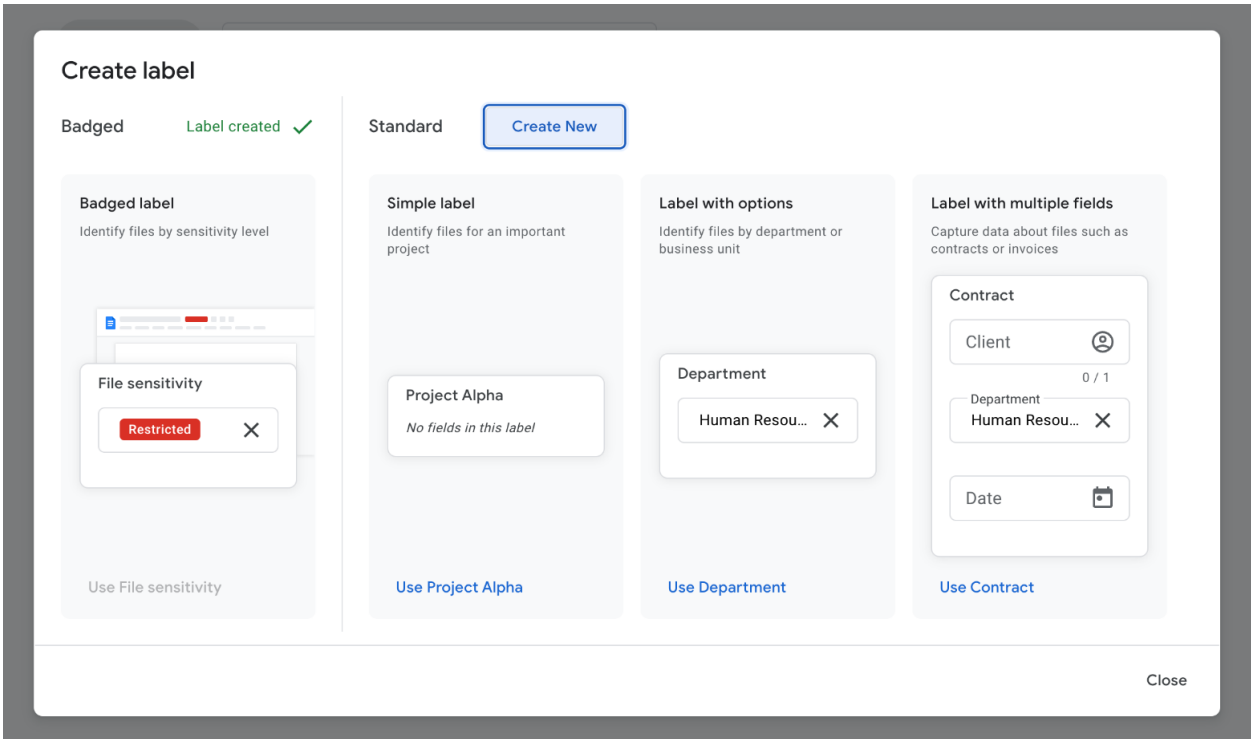
What is it?
When creating labels, admins can choose to either create Badged labels or Standard labels. Badged labels relate to classifying files based on their confidentiality level. Standard labels relate to projects, departments, or those with multiple fields.

Why it matters
Labels help organizations classify their information so they can then add rules using DLP functionality. Creating labels for your organization will also help employees find and organize information faster.

How to do it

1. Once labels have been turned on for the organization, labels can be created by visiting https://drive.google.com/labels and clicking on “New Label.”

2. From there, you’ll need to select the type of label you’d like to create. You can either create a Badged label or a Standard label.

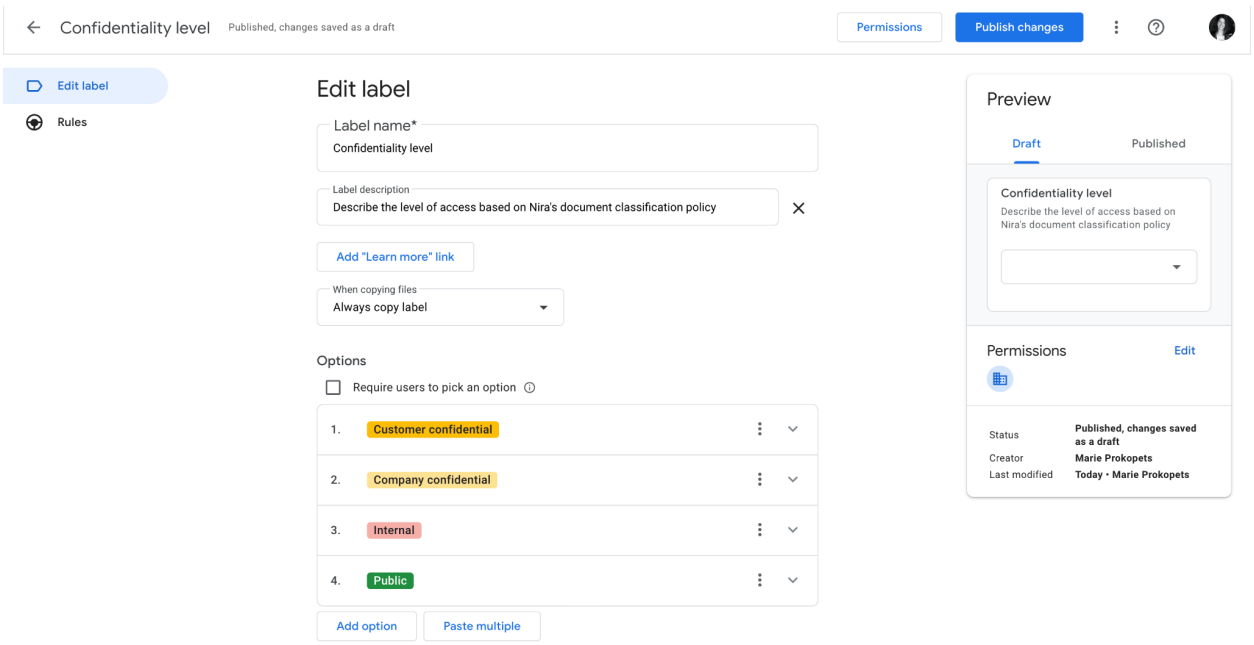


Create Badged labels

Organizations can only have one Badged label. These labels are related to data classification policies as they explain how sensitive or confidential a file is.

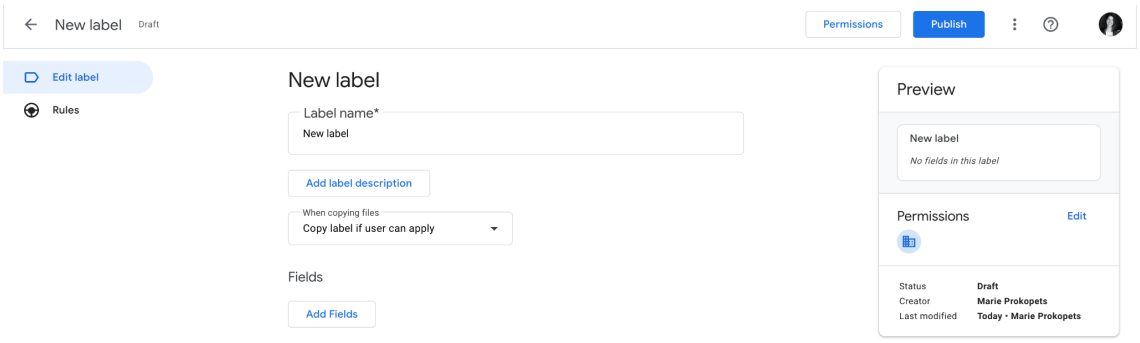
1. Click “New label” and choose “Badged label.”
2. Choose to start from the example provided by Google or to start from scratch.
3. Update the label’s title. You can also optionally add a description or a URL to share internal documentation about the label. For example, your data classification policy.
4. Choose whether employees will be required to fill out the label.
5. Customize the options and colors.
6. Click “Publish.”

Here’s a sample Badged label:



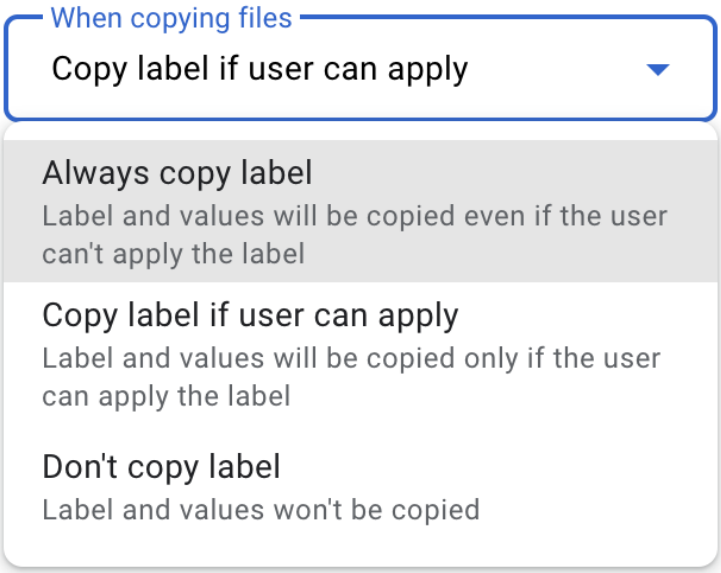
Create Standard labels

1. If you'd like to create a Standard label, click new label from drive.google.com/labels
2. Click on "Create New" next to "Standard." You can "Create New" or use one of the label templates such as "Use Contract."
3. You'll be taken to a screen to edit the New label.

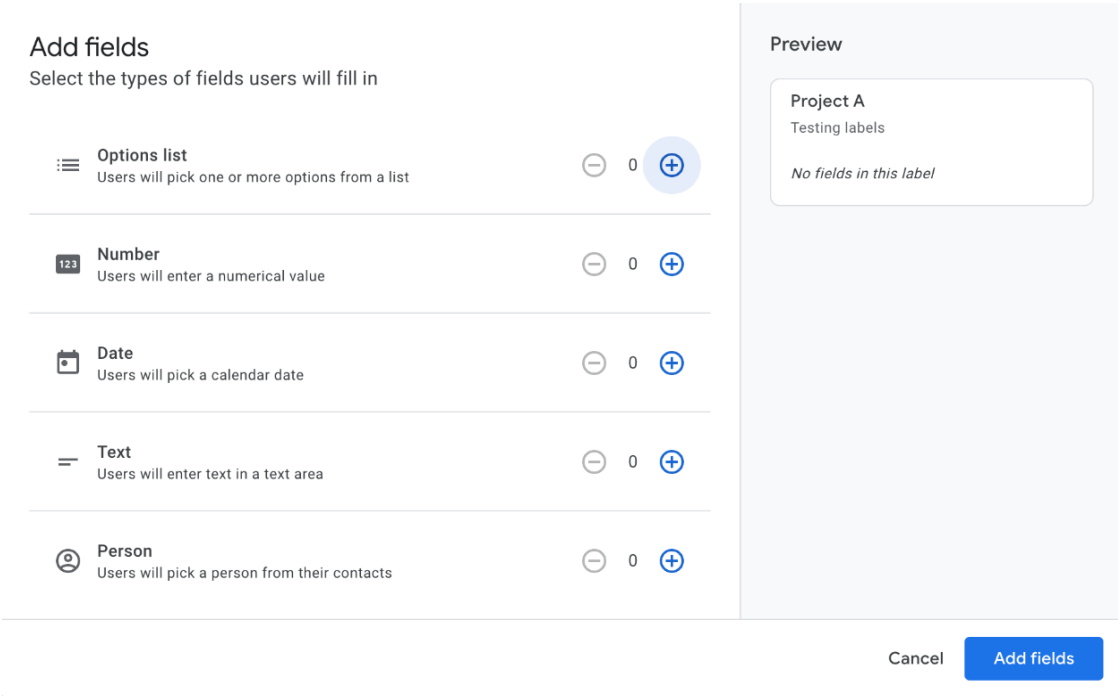


4. Add a label name and add an optional label description (this is what people with permissions to add the label will see).

5. Next, select what happens when files are copied. You'll be able to select from three options:
    - Always copy label
    - Copy label if user can apply
    - Don't copy label



6. You'll then be able to add optional fields for employees to fill out when they add the label to documents. These fields include: Options, Number, Date, Text, or Person. Labels can have a maximum of 10 fields.



7. Once you've finished customizing the label and setting permissions (see Managing Label Permissions below), click "Publish."

    - Note that if you added any fields, the field types cannot be edited once you publish the label.

    - If you'd like to edit the labels you created at any time, click on the label you'd like to edit from drive.google.com/labels.

    - To delete a label, first you must disable it by clicking the three dots on the right side of the labels and selecting disable. Once the label is disabled, you can either enable it or delete the label.

How Employees Can Use Labels

What is it?
Employees have the ability to apply or remove labels that were created by admins in Google Drive. Employees can do this in several places including in the side panel and context menu in Drive, and the Labels panel in Docs, Sheets, and Slides. They can also search for files with labels that they have access to from their Google Drive.

Why it matters
Trying to find documents can take up a lot of time. If an employee can't find a document, they often end up asking others where the document is, wasting even more time. Labels cut that time by allowing employees to group information and find it more quickly. Labels are also helpful for data classification policy compliance, where employees can add a label (either as an option or required) to define how confidential the document is. Although labels can be useful, admins should make sure that employees don't have permissions to labels they shouldn't, such as labels related to an acquisition or a confidential project.

How to do it
There are several ways that your employees can apply, remove, view, and search for labels in Google Workspace:

Apply labels

Using the side panel in Drive:

1. Go to drive.google.com.
2. Single click the file, then click the “Info” icon (view details) in the top right corner above the list of files. A Details panel will open.
3. In the “Labels” section of the Details panel, click the “Apply label” button
4. Select a label from the drop down menu.
5. If the chosen label contains one or more fields, optionally choose or enter values.
    - *Note: Employees may remove a label from a file by clicking the “Remove” trash icon.*

Using the context menu in Drive

1. Go to drive.google.com.
2. Right click on a file, and choose “Labels” and then “Apply a label” from the menu. You can also choose from suggested labels.
3. Use the dialog to choose a label by searching, and select or enter in field values to apply to the file.
    - *Note: Employees can also bulk apply labels by selecting multiple files at once and following the steps above.*

View and apply labels

Use the Labels panel in Docs, Sheets, Slides

1. When viewing or editing a file in Docs, Sheets, or Slides, click the “File” menu and choose “Labels.”
2. View existing labels and apply new labels in the side panel.
3. To apply a new label, click “Apply label.”
4. Search for the label or select a suggested label.

Use the Labels panel in Drive Preview

1. Go to drive.google.com.
2. Single click on an item.
3. Click the preview icon (eye icon) at the top of the screen right above the list of files.
4. Once in preview, click the three dots at the top right corner of the screen (“More actions”) and choose “View labels.”
5. View existing labels and apply new labels in the side panel.

Notes: You can add multiple labels to each file. Labels can only be applied to files. They cannot be applied to folders or Shared drives.

Search for files with labels

1. Go to drive.google.com.
2. At the top of the screen, next to “Search in Drive,” select the “Search options” icon on the right. A detailed search dropdown will appear.
3. Next to "Labels," select a label from the drop-down menu or search for a label.
4. Below the label, you can optionally select a field from the drop down menu if the label has any fields, and specify a value.
5. Click “Search.”

Manage Label Permissions

What is it?
Admins can decide which users have what permissions: regulating who can view, apply, edit field values, and search for labels.

By default, everyone in the organization has the ability to view and apply labels. Admins can also allow people outside the organization to have these label permissions, as well as groups who may have outside members.

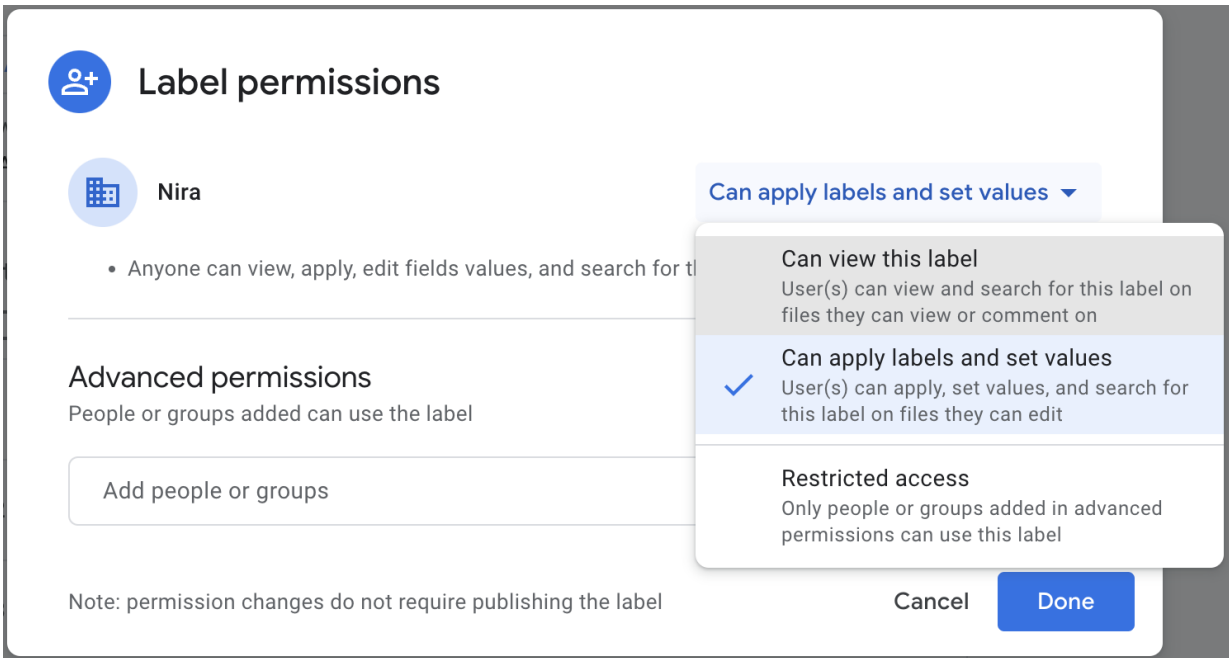
Why it matters
Labels can be tricky because most people don’t immediately think of them when they think about document security. But in reality, labels can help organizations comply with their document classification policies, which dictate how different types of documents should be labeled and what level of permissions they should have. However, when working with labels, you should always avoid writing confidential information in label names, field names, and selection options, as they may become visible to everyone in your organization. For example, if there’s a secret acquisition in the works, a code name should be used for the label, and not the word “acquisition.”

Remember that any other admin with “Manage Label” permissions could edit these labels, even if they didn’t create them.

Remember to be cautious when changing labels that have been published as it will affect all the other files previously using the label.

How to do it

1. Go to the labels manager at drive.google.com/labels
2. Click on the label you want to manage.
3. In editing mode, click the “Permissions” button in the header.
4. In the Label Permission dialog, use the selection drop down to choose the right permission level for your organization.
5. To restrict access to specific people or groups, select “Restricted” access next to your organization name. Then specify the individual users or groups and their permission levels.



Here’s What Employees Should Know

- You can apply, remove, or search for labels which can save you time and help you organize information. Adding labels to your documents will help you find them faster.
- Adding labels related to how confidential your documents are will help your IT and Security teams better protect company information.
- You can check with your administrator to make sure you have the right label permissions.

- If you'd like labels created, check with your administrator.

Chapter 7: Other Access Controls

As an admin, you have various options for securing and controlling access to your documents. We'll go over the access controls that deal with restricting file permissions, sharing content with Groups, viewing activity on all documents, as well as briefly go over inbound documents. We'll explore why these controls matter and how to implement them.

Restrict File Access

Prevent Editors from re-sharing and changing access permissions

What is it?
If a user has a file that they own in Drive that has sensitive content, they can prevent Editors from sharing it again and changing its access permissions. You can set it so that only the owner can share or set permissions.

Why it matters
Under normal circumstances, if a user is sharing with someone who has Editor access, they can easily change the sharing permissions for that file. As we've seen, this leads to Access-Risk, and Owners now have limited control over who is sharing their documents or setting their permissions. Preventing editors from having re-sharing and access permission change controls is a best practice if users are sharing documents with extremely sensitive content but is less applicable to other types of files.

How to do it

1. Open the homescreen for Drive, Docs, Sheets, or Slides.
2. Select one or more files to limit.
3. Click "Share" or "Share  ."
4. At the top, click "Settings  ."
5. Uncheck "Editors can change permissions and share."
6. Click "Done."

Prevent a file from being copied, printed, or downloaded

What is it?
Users can prevent those with Commenter and Viewer access from downloading, printing, or copying files. Whenever a Commenter or Viewer tries this with a shared file, those options are grayed out and unavailable to them.

Why it matters
We understand there are plenty of workarounds for this method, however, it helps prevent accidental downloading and copying of files that do not need to be saved to people's company or personal computers. It adds another layer of protection to sensitive files and prevents human error but wouldn't do much to deter someone with serious malicious intent.

How to do it in My Drive

1. Open the homescreen for Drive, Docs, Sheets, or Slides.
2. Select one or more files to limit.
3. Click "Share" or "Share ."
4. At the top, click "Settings ."
5. Uncheck "Viewers and commenters can see the option to download, print, and copy."
6. Click "Save" > "Done."

How to do it in shared drives
Please note users must have Manager access for the shared drive to apply this rule.

1. Click the file.
2. At the top, click "Share ."
3. At the bottom, click "Who Has Access."
4. Click "More" and check the "Restrict download, print, & copy actions on this file for commenters and viewers" box.
5. Click "Done."

Share Content with Groups

Google Groups allow users to share with multiple people using one email address. We'll go over how to share a document with a group and ways admins and employees can manage sharing outside the organization.

Share a document with a group

What is it?
Users can share a single file with a Google group through the group's email address. Sharing with a group saves employees time and energy as they no longer have to add everyone's individual email addresses to documents.

Why it matters
Sharing with a group allows users to quickly change access permissions for everyone at once. Furthermore, if someone leaves the team—say they transfer to a new role internally—you can simply remove them from the group, and they will lose access to all documents that were previously shared via the group's email address.

However, there's also risk with groups. For example, teams may never clean up group permissions, they might add personal accounts or outside domains to groups, and users might share documents with groups that they shouldn't share them with.

How to do it

1. Create a file in Google Drive or open an existing document.
2. In the file, click "Share."
3. In the "Invite people" field, enter the group's email address.
4. Select the level of access you want to provide the group: "Can edit," "Can comment," or "Can view."
5. Click "Done."

Share outside the organization

What is it?
As an admin, you can stop the sharing of content with group members outside your organization. You are able to set organization-wide policies in your Admin console and determine if your groups should be private (accessible by accounts in the company only) or accessible by the public. You can also decide if group members can add external members or receive emails from outside the organization. Remember that as an admin, you automatically have ownership privileges for all groups at your company, even the ones you didn't create.

Why it matters
Google Groups are defaulted to private and usually designed for employees in your organization to quickly and efficiently collaborate. However, room for error exists as sensitive data could be accidentally shared if your Google Group privacy settings are misconfigured. It's important to

know what privacy options you have in your Admin console so sharing capabilities and safety features can stay in equilibrium.

How to do it

1. In the Admin console, go to “Apps” > “Google Workspace”> “Groups for Business.” (Please note that Groups for Business is available for all editions of Google Workspace.)

2. Click “Sharing settings.”

3. Now you are able to apply various settings. Admins have control over the following:

- **Accessing groups from outside this organization:** You may set this to “Private” and only people in the organization can access your organization's groups in Google Groups. External members may be allowed to access your groups by email only.

  Note that if you change this setting, the change will affect new and existing groups. If you change from public to private and existing groups have external members, those members will be unable to access their groups in Google Groups, regardless of the settings for the individual group. However, they can still send and receive emails from their groups, depending on the group settings.

- **Creating groups:** You can decide if all admins, all users in your organization, or even anyone on the internet can create groups for your organization.

- **Can external users participate in groups:** You can control if group owners can invite or add external members to groups. You can also decide if group owners can allow their groups to receive incoming emails from outside your organization. Please note that if you change these settings, they do not automatically affect existing external group members or messages.

- **Default for permission to view conversations:** Please note that this setting is unavailable for groups created in the Admin console or Google Cloud Console. Admins can set the default for who can view conversations in their organization’s groups as well as decide who can post and who can view members.

- **Can a group be hidden from non-members:** You can hide new groups from your directory by default. Group admins will still be able to see all groups, and group members will still be able to see all the groups they belong to in the directory. You also have the option to make these settings public, but we don’t recommend allowing just anyone on the internet visibility into your groups.

View All Activity on Documents

Please note that the supported editions for this feature are *Frontline; Business Standard and Business Plus; one or more Enterprise editions; Education Fundamentals, Standard, Teaching and Learning Upgrade, and Plus; G Suite Business; Essentials.*

What is it?
In your Drive Audit Log, you can see the actions employees perform on individual files as well as review when a setting or membership changes for a shared drive. Event names that you can filter for include when users view, rename, create, edit, preview, update, delete, upload, download, or share a Drive file.

Why it matters
Being able to have a record and get some sort of visibility into what employees are doing to individual documents, as well as who has access to your shared drives, can be crucial when finding, remediating and investigating unauthorized access issues. Unfortunately, Google Workspace does not offer complete visibility, however, you can use your Drive Audit Log to understand some of the Access-Risks your company faces.

How to do it

1. In your Admin console, go to “Reporting.”
2. On the left, click “Audit” > “Drive.”
3. (Optional) To customize your data, on the right, click “Manage columns” gearbox icon.
4. Select the columns that you want to see or hide and click “Save.”

Understand Inbound Documents

What is it?
Inbound documents are documents that are owned externally and shared with accounts at your company.

Companies are constantly collaborating with vendors who create materials for their clients, like documents created by lawyers, marketing vendors, or auditors. Freelancers who don’t have a company email account or mistakenly use their personal accounts also create and share documents with the company. Another common use case is employees who accidentally create documents on their personal email accounts and share those documents with people at the company.

Admins don't have visibility into inbound documents using Google Workspace. However, these documents can have all of the Access-Risk issues we've mentioned before, including Public and Company links or personal accounts.

Why it matters
Working with third parties can lead to all manner of access risks, as externally-owned documents could be shared with accounts who should have never had access. And if your sensitive information does fall into the wrong hands, it can result in legal and compliance issues, reputational damage, HR problems, and loss of customer business.

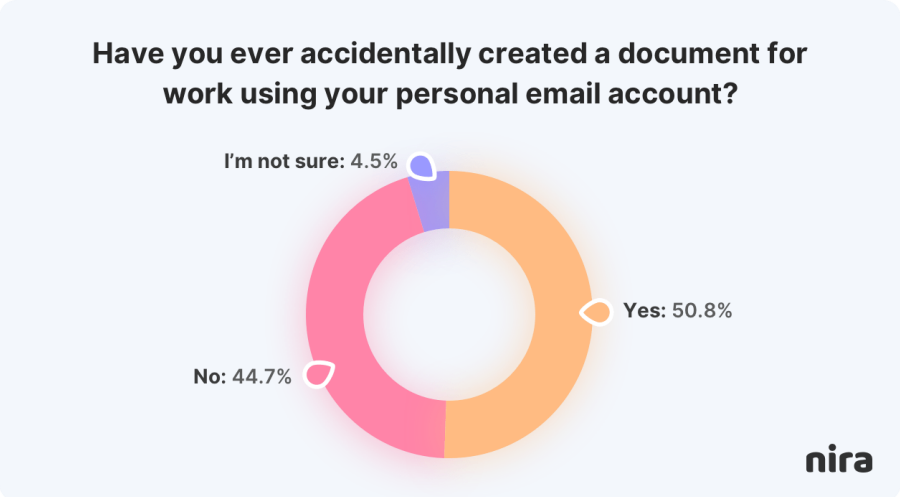
The most common situations we see are:

- Vendors who create and share confidential information with the company (for example, accounting, legal, audit, and consulting firms) are not securing that information for their customers. They will have Public links, Company links and personal accounts on documents that should all be Restricted with access only from required accounts.

- Vendors where the relationship has ended, and they were supposed to delete all documents and remove access per contractual requirements, but the access and documents still persist months and even years later.

- Employees who accidentally create documents using their personal accounts.

  They then leave the company, and the documents remain tied to their personal account, unsecured and with the potential that the employee can look back at them later. This is a real concern, since over 45% of employees admit to taking documents from former employers.



How to do it

As we mentioned, in Google Workspace, it's currently not possible to get comprehensive visibility into these types of issues. We recommend finding a solution that provides visibility over inbound documents shared with your company that are owned by external domains or personal accounts. That way, you can alleviate data leakage risk that is caused by mistakes related to current and past vendors, other partners, and former employees.

Here's What Employees Should Know

- Do not work on or share your work documents with your personal Google Workspace accounts. If this happens, remove access from the personal account as soon as possible.
- Double-check to make sure you are not using a personal account to create and share work files, as people often accidentally switch back and forth between their accounts and don't realize they are using the wrong account.
- Do not create documents from your personal Google Workspace account. If you notice that you've done this by accident, make a new copy of the document using your work account and delete the document you made using your personal account.
- Be careful when receiving inbound documents from freelancers, contractors, and third-party vendors. Do not put highly sensitive information in these documents unless absolutely necessary. Be aware that these documents are owned by outside parties who can change permissions and add members to the documents at any time.

Chapter 8: Real-time Access Control Systems

Real-time Access Control System

What is it?
A real-time access control system provides complete visibility and management capabilities over who has access to company information—like documents, code repositories, and channels in tools like Slack and Microsoft Teams.

When security professionals use the term “real-time,” they can mean anything from several minutes to mere milliseconds. The faster that companies can detect, investigate, and remediate issues, the more effective their security response will be.

Despite this knowledge, companies are rarely able to respond so quickly. For example, an IBM report showed that the average time to identify and contain a data breach was 287 days in 2021.

Real-time monitoring and the ability to act swiftly on that monitoring is what sets access control systems apart. Companies need to have full visibility into their various risks, threats, and vulnerabilities, along with the capability to actually do something with this information before a negative event occurs.

Why it matters
As IT and security professionals know, we can never fully eliminate risk. Anyone who claims otherwise is selling you something. However, what we can do is mitigate it, and the goal of any real-time access control system is to do so as quickly and efficiently as possible.

A good access control system will be proactive and help you prevent most negative events before they happen. However, when a data breach or an Access-Risk incident does occur, they should aid the appropriate security response to effectively handle the situation.

How to do it
Although there’s a lot you can do in Google Workspace to keep your data safe, it still has a bevy of limitations. At the moment, Google Workspace does not have the capabilities to monitor document access changes for every account in real time. Furthermore, it doesn’t give full visibility and control of external sharing and document ownership.

It also relies on lots of work from IT and security teams, as end-users are unable to review and remediate access control on their documents without going through document by document in their Google Workspace. Instead of being allies in document security, employees are left without the tools they need to aid administrators and reduce administrative burden.

To complement your security response in Google Workspace, we recommend implementing a real-time access control system to speed up investigations and automate alerting and policy enforcement.

Conclusion

Being able to share with anyone, anywhere, across any device has allowed for a major increase in collaboration and distributed/remote work. However, this also leads to Access-Risks incidents that can cost companies millions of dollars and put employees' and customers' personal information at stake.

Keeping your company and customer documents safe in Google Workspace is quintessential to any security plan. As admins, you want to stay compliant and secure, without taking up a lot of valuable time and resources.

We've gone over best practices for sharing documents in Google Workspace, what capabilities you have as an admin to allow and restrict access, and the benefits of employee education and real-time access control.

We hope this guide will help you empower your teams and make data security more collaborative and easier for everyone.

About Nira

Nira is a real-time access control system that provides complete visibility and management over who has access to your company documents in Google Workspace and more. Nira provides a single, comprehensive view of who has access to valuable cloud-based company data. It allows you to easily find and identify risks, quickly control access and fix issues, and efficiently automate the process through policy enforcement and remediation delegation. Nira also enables employees to manage and control who has access to their information, without needing tons of technical expertise.

Glossary

Access-Risk incident: Data breaches stemming from unauthorized access.

Allowlist: A list of trusted domains for your organization. In Google Workspace, administrators can create one allowlist for Drive, Sites, Data Studio, and Classroom settings. If your organization has a Google Workspace Business Standard or Business Plus plan, then users can only share externally with trusted domains. If your organization has Google Workspace Enterprise, Education, Nonprofits, G Suite Business, or Essentials plans, you can turn the allowlist on or off for a group or organizational unit.

Child organizational unit: Child organizational units are nested below a top-level (parent) organizational unit and used to apply different settings to a set of users or to Chrome devices. These units inherit the settings from the parent but can be changed to apply unique settings that fit the needs of the child organizational unit.

Configuration group: A group of users that administrators can apply service settings for. Configuration groups can include users from any organizational unit in your account. A user can belong to multiple configuration groups, unlike organizational units. You set the priority of configuration groups, and the user gets the setting of the highest priority group they belong to. Please note that admins can only set up configuration groups through their Admin console, not APIs, and that a user's group settings always override their organizational unit's settings.

Data classification policy: A comprehensive plan used to categorize a company's stored data based on its sensitivity level, to ensure that the data is handled properly and to lower organizational risk. Organizations can create categories such as Public, Internal, Company Confidential, and Customer Confidential, and then define who should have access to the types of data in each category.

Documents: Your organization's assets in Google Workspace. These include items like Sheets, Slides, Docs, PDFs, PPTs, Word Files, video files, images, shared drives, and folders.

Document retention policy: How an organization deals with documents from creation to destruction. This policy can be used to satisfy compliance, legal, and regulatory requirements as well as maintain financial records. Policies can be stand-alone documents or integrated into an employee handbook.

My Drive: In Google Drive, My Drive is where a user's personal files are stored. Files and folders created in My Drive are owned by the account, and the account is the only person who can have ownership. To learn about collaborating within a team in Google Drive, see "shared drives."

Organizational unit: An organizational unit is a group that an administrator can create in the Google Admin console to apply settings to a specific set of users. By default, all users are placed in the top-level (parent) organizational unit. Child organizational units can then be created below the parent unit and unique settings applied. See “child organizational unit” for more.

Primary target audience: In the Admin console, admins have the ability to create up to five target audiences. The primary target audience is the default audience and it appears first in a user's list of sharing recommendations. See “target audience.”

Real-time access control system: A real-time access control system provides complete visibility and management capabilities over who has access to company information—like documents, code repositories, and channels in tools like Slack and Microsoft Teams.

Shared drive: In Google Drive, shared drives are used for collaboration. Shared drives can be used to store, search, and access files with a team. Shared drive files belong to the team instead of an individual account. Even if members leave, the files stay in place so the team can keep sharing information and work together anywhere, from any device.

Target audience: Target audiences are groups of people—such as departments or teams—that admins can recommend for users to share their items with. Administrators can add them to users' sharing settings in a Google service, such as Google Drive, to encourage users to share items with a more specific or limited audience rather than their entire organization. Note that target audiences are currently available only for Google Drive and Docs.

Vault: Vault is Google’s information governance and eDiscovery tool for Google Workspace. With Vault, organizations can retain, hold, search, and export users’ Google Workspace data. For Vault to search and retain a user’s data, users must have a Google Workspace license and a Vault license. These plans have Vault’s licenses included: *Business Plus, Enterprise, Enterprise Essentials (domain-verified only), Education Fundamentals and Plus, and G Suite Business*. Vault add-on licenses are also available for *Frontline and G Suite Basic*.

Visitor sharing: With visitor sharing, users can invite non-Google users to collaborate on files as visitors and use a PIN to verify their identity. You can also see who has access to your organization's files and folders if you allow visitor sharing. Once visitor sharing has been turned on for your organization, you can share documents with non-Google accounts like normal. Visitors can edit, comment on, or view your document for seven days after they verify their email address. If they need to collaborate longer, they can use the link from the original sharing email to verify their identity again.

Shared Drive Terms

Manager: In Shared Drives, Managers have the highest level of access permission and can complete various tasks. These include:

- View shared drives, files, and folders.
- Comment on files in shared drives.
- Make, approve, and reject edits in files.
- Create and upload files and create folders in shared drives.
- Add people and groups to specific files in shared drives.
- Add people and groups to specific folders in shared drives
- Move files and folders from a shared drive to My Drive.
- Move files and folders within a shared drive.
- Move files and folders from one shared drive to another shared drive.
- Move shared drive files and folders into the trash.
- Permanently delete files and folders in the trash.
- Restore files and folders from trash (up to 30 days).

Content Manager
When a user is added to a shared drive, they automatically become a Content manager.

Content managers can:

- View shared drives, files, and folders.
- Comment on files in shared drives.
- Make, approve, and reject edits in files.
- Create and upload files, and create folders in shared drives.
- Add people and groups to specific files in shared drives.
- Move files and folders within a shared drive.
- Move shared drive files and folders into the trash.
- Restore files and folders from trash (up to 30 days).

Contributor
Contributors are also known as editors at the individual file level. They have fewer permissions than Managers and Content managers, but they can still:

- View shared drives, files, and folders.
- Comment on files in shared drives.
- Make, approve, and reject edits in files.
- Create and upload files and create folders in shared drives.
- Add people and groups to specific files in shared drives.
- Restore files and folders from trash (up to 30 days)

Commenter

- View shared drives, files, and folders.
- Comment on files in shared drives.

Viewer

- View shared drives, files, and folders.