Continue

To sign up for Gmail, create a Google Account. You can use the username and password to sign in to Gmail and other Google products like YouTube, Google Play, and Google Drive. Important: Before you set up a new Gmail account, make sure to sign out of your current Gmail account. Learn how to sign out of Gmail. From your device, go to the Google Account sign in page. Click Create account. In the drop down, select if the account is for your: Personal use Child Work or business To set up your account, follow the steps on the screen. Create an account Tip: To use Gmail for your business, a Google Workspace account might be better for you than a personal Google Account. With Google Workspace, you get increased storage, professional email addresses, and additional features. Learn about Google Workspace pricing and plans. Try Google Workspace The username I want is taken You cant create a Gmail address if the username you requested is: Already being used. Very similar to an existing username. For example, if example@gmail.com already exists, you can't use examp1e@gmail.com. The same as a username that someone used in the past and then deleted. Reserved by Google to prevent spam or abuse. Someone is impersonating me If you believe someone has created a Gmail address to try toimpersonate your identity, you can: Unfortunately, Gmail is unable to participate in mediations involving third parties regarding impersonation. Learn more about Gmail Terms of Use. Related resources How do I create a new Google Account? Sign in to Gmail Post to the help community Get answers from community members Pixel 7 & later phones and the Pixel Tablet have access to the optimized, built-in Virtual Private Network (VPN) by Google at no extra cost in countries where VPN is available. Add or use a VPN Add a saved network Get your VPN information from your administrator. You might need to install a VPN app and start set-up in that app. The app could come from the Google Play Store or from your administrator. Step 2: Enter VPN information Open your device's Settings app. Tap Network & internet VPN. At the top right, tap Add . Enter the information from your administrator. Tap Save. Connect Open your device's Settings app. Tap Network & internet VPN. Tap the VPN you want. Enter your username and password. Tap Connect. If you use a VPN app, the app opens. Tip:Whenyou're connected, you'll seeVPNon. Disconnect or forget a VPN Open your device's Settings app. Tap Network & internet VPN. Next to the VPN that you want to disconnect, tap Settings . To disconnect: Turn off that VPN. To forget the network: Tap Forget. Edit VPN settings Edit Open your device's Settings app. Tap Network & internet VPN. Next to the VPN you want to edit, tap Settings . If you use a VPN app, the app will open. Edit the VPN settings. If needed, tap Save. Stay connected all the time If you haven't already, add a VPN. Open your device's Settings app. Tap Network & internet VPN. Next to the VPN you want to change, tap Settings . Turn Always-on VPN on or off. If you've set up a VPN through an app, you won't have the always-on option. If needed, tap Save. Clear VPN notification Important: If your always-on VPN connection stops working, you'll get a notification that stays until you reconnect. To clear that notification, turn off always-on for that VPN. Open your device's Settings app. Tap Network & internet VPN. Next to the VPN you want to change, tap Settings . Turn Always-on VPN off. Work profile Related resources Add & remove certificates Set up a work profile Post to the help community Get answers from community members Shared drives are a great way for teams to collaborate and reference the same files in Google Drive. But it can be confusing trying to tell who can access a file or folder in a shared drive, what permissions they have for that item, and what to do if you want to change access.For a complete list of what each access level allows, review the following table: Access level Permission Manager Content manager Contributor Commenter Viewer Can view files and folders Can comment on files Can edit files Can create and add files, can create folders * Can add and remove people and groups onspecific files Can set limited access to folders Can restore files from the Trash (up to 30 days) Can move files from My Drive to a shared drive Can move files and folders to the Trash Can move files and folders within a shared drive Can add or remove people and groups onspecific folders in a shared drive ** Can move folders from My Drive to a shared drive Can move files from one shared drive to another shared drive Can add or remove members of a shared drive Can change member access levels Can permanently delete files in the Trash Can rename or change theme Can delete theshared drive * In Google Drive for desktop or files in the Chrome OS Files app, Contributor access gives only read access to files. To allow users to create, upload, and edit files in a shared drive in Google Drive for desktop and Chrome OS, give the user Content manager or Manager access. ** Administrators or Managers can prevent Content managers from sharing folders. You can use this feature only if your organization supports it. For help, contact youradministrator. Members with Manager access and Google Workspace admins can control access to the items in a shared drive. In addition to setting up members, they can set restrictions on sharing as follows: Prevent sharing files with people outside your organization Prevent sharing files with non-members Prevent specific members from accessing folders Prevent members with Content manageraccess from sharing folders Prevent members with Commenter or Viewer access from downloading, copying, or printing files These restrictions override file and folder sharing (described in the next section). If a shared drive Manager changes a shared drives restriction settings, access privileges for files in the shared drive are updated. For example, if a file in a shared drive is shared with an external person and then the shared drive settings are updated to prevent sharing with people outside your organization, that external user cant access the file anymore. However, their permission on the file stays in place. If the setting is changed to allow sharing with external users again, any external users who the file was already shared with regain access to it. Learn how to set sharing permissions Share files & folders in a shared drive Unless prohibited by the sharing settings for the shared drives (described in the previous section), members with Manager, Content manager, or Contributor privileges can share files with people and groups, the same as other files in My Drive. They can also share with people who don't have Google Accounts through visitor sharing (if allowed by their administrator). Members with Manager and Content manager access can share folders with people and groups. However, administrators and those with Manager access can prevent others from sharing folders. They can also restrict access to shared folders if they want to keep information private from specific people. Who gets access requests? When someone requests access to a shared drive or membership, the request is sent to those with Manageraccess. When someone requests access to a file or folder, the request is sent to the item's creator. If that person doesn't have permission to share the file or folder, the request goes to members with Manager access. How sharing a folder in a shared drive works If you have Manager or Content manager access to a shared drive, you can share a specific folder with other people and groups. However, administrators or Managers can prevent Content managers from sharing folders. Managers can control access to specific folders if they want to keep information private. Sharing folders instead of the entire shared drive can make sense when everyone needs view access, but only certain people need edit access. For example: For a marketing department, you can make a shared drive accessible by all internal employees, with a specific folder for advertising materials thats also shared with an external agency. For a shared drive used to prepare for a specific event, you can give all members view access to all files, while providing each specific team with edit access to the documents relevant to their part of the event. You cant make the access to folders more restrictive than the shared drive itself. A member with Commenter access cant have only Viewer access to a folder in that shared drive. If access to a file or folder is made more restricted, then access to the shared drive is also restricted to the same degree. When you share a folder in a shared drive with someone, they get a notification and can find the folder in the Shared with me section in Google Drive. They can organize shared folders in their My Drive using shortcuts. In Google Drive for desktop, shared drives and folders shared directly with you dont automatically appear unless you have Manageraccess. If you don't have Manager access, create shortcuts in your My Drive to the shared folders or shared drives. This way you can easily access them in Drive for desktop. Note: Limited-access folders are an exception to these rules, as they allow members with Manageraccess to restrict access to specific hierarchies. How link sharing in a shared drive works Unless prohibited by the sharing settings for the shared drives, you can share files and folders by link instead of directly with users and groups. However, link sharing cant be less restrictive for files and folders in a folder already shared with a link. If you share a folder in a shared drive with the option Anyone in this group with this link can view, you can't share any file or folder inside with the option Anyone with the link. To work around this limitation, try the following workarounds: First, share the item with the option Anyone with the link, then share the parent folder with the option Anyone in this group with this link can view. Ask your admin to use the Drive API to share the child folder after the parent. Learn more about sharing items in shared drives Move files or folders into a shared drive When a file or folder is moved into a shared drive, it keeps its sharing permissions, but access privileges may change if sharing settings for the shared drive are more restrictive. If access privileges on the file are more restrictive than the shared drive, they arent relaxed. For example, if a file owner sets their file to prevent downloading, copying, and printing, it stays like that after it's moved to a shared drive, even if those actions are allowed by the shared drive. Moving files into a shared drive does not affect sharing permissions or user roles, such as Editor or Viewer, set directly on the file. However, file permissions inherited from the folder the file was in arent copied. For example, if someone had a folder in My Drive shared with them, but not a file, if files from that folder are moved to a shared drive that person can lose access unless theyre a member of the shared drive. When you move a file you created into a shared drive, youre still the creator but no longer the owner. If the shared drive's access permissions change, its possible for you to lose access to a file you created. Moving folders into a shared drive can create broad changes to content access. Therefore, only users who have Manager access to the original and target locations can move folders into or between shared drives. If you move a folder to a shared drive: All members of the shared drive can view the contents of the folder, including previously hidden files. (Hidden files occur in My Drive when you share a folder with someone but remove access to a specific file in that folder). Some members cant view folders if the folders have limited access. Users who had a folder directly shared with them before the move can still access the folder. Users with Editor access to the folder before the move have Content manager access after. Users who had indirect access to a folder and its contents through access to a parent folder may lose access to the folder. Indirect file permissions inherited from parent folder permissions arent copied. Move Google Sites files into shared drives Moving sites into a shared drive doesnt change the visibility of a published site, but it can change who has access to the site file: If the original owner of the site is in the same organization as the shared drive, the Sites file associated with the site is still accessible to users who it was previously shared with. If the original owner of the site is in a different organization than the shared drive, the site file is not accessible to people who arent members of the shared drive, even if it was previously shared with them. Learn more about moving files Move files out of shared drives If you have Manager access to a shared drive, you can move files and folders out of shared drive to My Drive or another shared drive. To move files from a shared drive to another, you need Contributor, Content manager, or Manager access in the destination shared drive. To move folders from one shared drive to another, you need Manager access in the destination shared drive. Just like moving files into shared drives, access privileges on files and folders are reassessed when theyre moved out of a shared drive. If a file or folder is moved out of a shared drive to My Drive within the same organization: The shared drives sharing settings no longer apply and the files original sharing settings take effect. Some users might gain or lose access. For example, you have a file in the Sales team shared drive, and all members of the Sales team have Viewer access to the shared drive and the file. The document was also directly shared with five Sales team members to give them Editor access. If the file is moved out of the Sales team shared drive, most of the Sales team loses their access, but the five people it was directly shared with still have Editor access. File-level restrictions stay in place unless specifically changed or removed from the file. For example, if a file owner sets their file to prevent downloading, copying, and printing, it stays like that after it's moved out of a shared drive, even if those actions are allowed by the new location. Remove access to files & folders in shared drives Just like in My Drive, you can remove someones access to a file or folder in a shared drive thats directly shared with them. (For details, go to Unshare files or folders.) All members of the shared drive can still at least view the file or folder, unless that folder has limited access. To remove access for shared drive members, you need to move the file or folder out of the shared drive, which requires Manager access. Note: When you remove a member from a shared drive, they also lose access to any files and folders in the shared drive that were directly shared with them. Back to top Supported editions for this feature: Frontline Starter, Frontline Standard, and Frontline Plus; Business Starter, Business Standard, and Business Plus; Enterprise Standard and Enterprise Plus; Education Fundamentals, Education Standard, Teaching and Learning Upgrade, Education Plus, and Endpoint Education Upgrade; Essentials, Enterprise Essentials, and Enterprise Essentials Plus; GSuite Basic and GSuite Business; Cloud Identity Free and Cloud Identity Premium. Compareyouredition You can host Android apps specifically for your organization in the managed Google Play store and control who can download them. With managed Google Play, you also get security checks, such as user authentication and malware detection. You can publish private apps to the Play store from the Google Admin console or the Google Play Console. After you add a private app to the apps list, users can download it from the managed Play Store on their Android device. It can take a few hours for the app to be available to users. Before you begin Read the following sections to decide how to publish your app and important considerations. Expandsection|CollapseallManaging private apps in Admin console versus Google Play Console You might want to use Google Play Console ifthe following is true: You have existing private apps in Play Console. You can't manage existing private apps in the Admin console. You might want to use Admin console if any of the following are true: You don't plan on making your private apps public. You don't want to pay a one-time $25 USD registration fee. You want your apps list to include all managed appspublic mobile apps, SAML apps, and private apps. You want to make the app available to only select organizational units and groups. Important information about app publishing Apps can't be published as a private app and in the public Google Play store at the same time. If an app with the same app ID was published by another organization (publicly or privately), you cant publish the app until the developer changes the application ID for your variant. However, you can add public apps to your app list to make them available to your users as managed apps. This setup allows your users to easily find all work-related apps in one place. If you publish an app to the public Google Play store, you can change it to a private app but you won't be able to manage it in your Admin console. Private apps don't support billing features. Publishers can't charge for private apps. In Play Console, you can't publish the app for a specific group of users. You can publish an app intended for a specific country or specific device models. If you want to beta test your app with specific groups, or Play Store users, you can set up alpha/beta testing. The app must be less than the download size limit. Option 1: Publish private apps from the Admin console To upload and publish private apps in the Admin console, you need an Android App Bundle (AAB), or application package (APK), and a title. When you publish a private app for the first time, a Play Console account is created on behalf of your organization. Private apps are automatically approved for your organization and are typically ready for distribution within 10 minutes. You can upload up to 15 private apps per day. Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. ClickAdd appAdd private Android app. At the bottom, click Create. Enter a title. Click Upload App. Select an ABB or APKand click Open. If you select an AAB, agree to the Play apps signing terms of service. When creating new private apps using AAB in the Admin console, and Google generates and manages the signing key for the app. If you want to use your own signing key, you can: Click Select. Set who can find and download the app. To let all users in your organization install the app, select Entire organization. To allow only certain users to install the app, clickSelect groups or Select organizational units. You can add both groups and organizational units. Supported editions for this feature:Frontline Starter, Frontline Standard, and Frontline Plus; Business Plus; Enterprise Standard and Enterprise Plus; Education Standard, Education Plus, and Endpoint Education Upgrade; Enterprise Essentials and Enterprise Essentials Plus; GSuite Basic and GSuite Business; Cloud Identity Premium. Compareyouredition Groups settings are applied at the top organizational unit level and override organizational unit settings. If a user belongs to multiple groups with conflicting configurations, the settings are applied in order of group precedence, which you can set after you add the app. Set app options. Access methodChoose how users get the app. To apply a managed configuration before you force install an app, select Available, complete app setup, apply the managed configuration, then edit the app settings to force install the app. AvailableLet users install the app themselves. Users who dont need the app dont have to download it. Force installAutomatically install the app on all managed devices with no option to opt out. Optionally, you can prevent users from uninstalling a force-installed app. Force install is also supported for basic mobile management with Business Plus, Enterprise, G Suite Business, and Cloud Identity Premium editions. Allow users to add widgets to home screenLet users create a home screen shortcut when a widget is available. Use as the always-on VPN appWhen turned on, app traffic from a work profile or managed device must pass through this app. Requires Android7.0 or later. This setting creates a more secure network connection for work profile traffic. App auto-update timingChoose when app updates should be installed: DefaultUpdate the app automatically when the device is connected to a Wi-Fi network, is charging, is not actively in use, and the app is not running in the foreground. High priorityUpdate the app as soon as the developer publishes a new version and Google Play reviews it. If the device is offline at that time, the app immediately updates the next time the device connects to the internet. PostponePostpone app updates for 90 days after the update first becomes available. After 90 days, automatically install the latest available version of the app. For details, see Support app updates. Supported editions for this feature: Frontline Starter, Frontline Standard, and Frontline Plus; Business Plus; Enterprise Standard and Enterprise Plus; Education Standard, Education Plus, and Endpoint Education Upgrade; Enterprise Essentials and Enterprise Essentials Plus; Cloud Identity Premium.Compareyouredition Testing tracks (optional)Select prerelease test versions of the app that you want to make available to users. Selecting multiple tracks makes the highest version code available. To learn how to make an app available to organizations, see Closed test: manage testers by organization. Supported editions for this feature: Frontline Starter, Frontline Standard, and Frontline Plus; Business Plus; Enterprise Standard and Enterprise Plus; Education Standard, Education Plus, and Endpoint Education Upgrade; Enterprise Essentials and Enterprise Essentials Plus; Cloud Identity Premium.Compareyouredition Edit and unpublish private apps from the Admin console Expandsection|Collapse all & go to topEdit the title or APK of a private app Edit advanced private app details To add a description, screenshots, and other advanced app details: Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. ClickAdd appAdd private Android app. Select the private app you want to edit. Click Make advanced edits. Go to GrowStore presenceMain store listing. Make any edits and click Save. Unpublish a private app If you unpublish a private app, the app isn't available for new users to find and download in managed Google Play. However, existing users can still use your app. To unpublish an app: Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. ClickAdd appAdd private Android app. Select the private app you want to unpublish. Click Make advanced edits. Using a Google Account, sign in to the Play Console. You can use this account in the future to sign into the Play Console. Go to ReleaseSetupAdvanced settings. In the App Availability section, select Unpublish. Option 2: Publish private apps from the Play Console For instructions, see Publish private apps from the Play Console. Note: To avoid the registration fee, follow the instructions in this article to publish private apps from the Admin console. Set who can publish and access private apps If you aren't the one who publishes private apps, you can allow other users or third-party developers to publish private apps. If your organization uses managed Play without an EMM (formerly called Google Play Private Channel) to grant access to private apps, you must explicitly allow users to access and download private apps. For instructions, see the following sections. Expandsection|Collapse all & go to topAllow other users to publish private apps Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. (Optional) To apply the setting to a department or team, at the side, select an organizational unit. Show me how Turn on the Google Play Console for users in the selected organizational unit. On the left of the Admin console, go toDevicesMobile & endpointsAndroid settings. Click Apps and data sharingGoogle Play private apps. (Optional) To apply the setting to a department or team, at the side, select an organizational unit. Show me how To allow users in the selected organizational unit to publish private apps, check theAllow users to publish and update Google Play Private appsbox. Click Save. Or, you might click Override for an organizational unit.To later restore the inherited value, click Inherit. Allow third-party developers to publish apps For instructions, see Publish private apps from the Play Console.No EMM: Allow users to access private apps Sign in with an administrator account to the GoogleAdminconsole.If you arent using an administrator account, you cant access the Admin console. Click Apps and data sharingGoogle Play private apps. (Optional) To apply the setting to a department or team, at the side, select an organizational unit. Show me how Check theAllow users to access Google Play private appsbox. Click Save. Or, you might click Override for an organizational unit.To later restore the inherited value, click Inherit. Related topic Manage private apps (Managed Google Play)

Private internet access vpn free download for pc. Is private internet access vpn good. Private internet access vpn download. What is private internet access vpn. Private internet access vpn tutorial. Private internet acces. Internet access vpn.