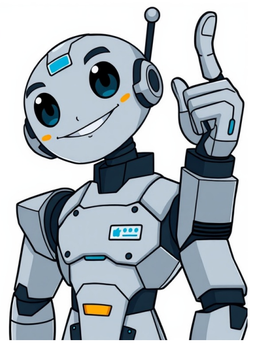
I'm not a robot



Calls and texts (SMS/RCS) aren't generally available from within the Work Profile because telephony works across the entire device and operates independently of the Work Profile. However, your IT admin may allow you to use other types of messaging apps (i.e., WhatsApp, Signal, etc.) and VoIP solutions in the Work Profile. If allowed by your IT admin, contacts saved in your work contacts app can be searched from your personal contacts and dialer apps on devices running Android 7 or later. These work contacts will also appear in the caller ID. Post to the help community Get answers from community members Managed Google Play allows organizations to deploy and manage apps on Android devices and enables end-users to access a curated Google Play Store for your organization. Organizations must register with Google to use managed Google Play and end-users need an account to access managed Google Play on Android. Organization registration process To begin the setup process, the IT admin logs into their 3rd party EMM provider and begins the “set up Android Enterprise” process (see the documentation for your EMM provider for specific steps). They will be redirected to the Android Enterprise registration process and prompted to specify the organization name, and the email address that the IT Admin will use to log in to manage the organization. From 2024, all new organizations completing this process will be provided with a managed Google domain. In certain error scenarios, the organization may be prompted to create a managed Google Play Accounts enterprise as a fall-back option. Managed Google domains Managed Google domains allow customers to use multiple Google products in their organization. The Google Admin console allows IT admins to manage these products. Google Workspace and Cloud Identity are two examples of products that use managed Google domains. From 2024, all new organizations using Android Enterprise will use managed Google domains to manage Android Enterprise alongside other Google products. End-users within organizations using managed Google domains can use managed Google accounts to access Google services, including managed Google Play. IT admins can bind multiple EMM instances to their managed Google domain, each will have a unique EMM binding ID (known as Enterprise ID). Once the managed Google domain is created, IT admins can utilize it to create and delete accounts for end users, and add these identities onto managed Android devices (via their EMM). Note: Managed Google domains support managed Google accounts (recommended) and managed Google Play accounts. Learn more about the types of Google accounts here. In order to provide a seamless experience, EMMs may integrate the managed Google Play iframe directly in their console, allowing IT admins to view and curate apps. IT admins can also use their admin account to log into play.google.com/work to perform these actions. However, access to play.google.com/work is restricted to customers who have a single EMM binding. Note: A number of Google services (e.g. Workspace Business Plus, Workspace Enterprise, Cloud Identity Premium) include advanced end-point management. Customers are advised to disable this feature, across their organization or per organizational unit, when using a third-party EMM to ensure a consistent experience when enrolling Android Enterprise devices and using managed Google Play. Role-based administration for managed Google domains Managed Google domains support extensive role based controls. IT admins can add additional admins to their managed Google domain and promote them to an admin role(s). For more information see Invite people to join your team and Change a team member’s role. Managed Google Play accounts enterprise For organizations that don’t use managed Google domains, A managed Google Play Accounts enterprise is a set of users, devices, and administrator accounts that are used to manage apps for your users. Your organization can have multiple managed Google Play Accounts enterprises. For more information see Organize managed Google Play accounts enterprise. The enterprise will have an Enterprise ID, which maps 1-1 to each EMM instance, and reflects that the EMM instance controls the enterprise and associated user accounts. Deleting the enterprise, or Removing the enterprise’s association with the EMM instance will result in the users losing access to Google Play, so take care to protect the Admin account. Once the managed Google Play Accounts enterprise is created, IT admins can utilize it to create and delete managed Google Play accounts for end users, and install these identities onto managed Android devices (via their EMM). Note: Managed Google accounts are not supported in managed Google Play accounts enterprises. Organizations using a Managed Google Play account enterprise can only use managed Google Play accounts. Learn more about the types of Google accounts here. IT admins can also use their admin account to log into play.google.com/work to view and curate apps that will be visible to their managed users. In order to provide a seamless experience, EMMs may also provide a portal directly in their console, where IT admins can view and curate apps instead of needing to navigate to play.google.com/work. Role-based administration for managed Google Play accounts enterprises A managed Google Play Accounts enterprise has 2 levels of administrator–Admin and Owner. For more information about these roles, see Assign roles in managed Google Play Accounts. You can set up Google Workspace on an Android device so that you can access your work or school account on the go. You can use your own personal device or one from your company. If your company uses mobile management to keep data safe, you might need to install a Google device policy app on the device and create a work profile. Before you begin To get started, you need a Google Workspace account and an Android device. If you don’t have a Google Workspace account, sign up for a trial today. These instructions are for users with Pixel devices running Android 8.0 Oreo or later. If you have a different device, setup might vary. When you set up a personal device with a work profile or for work only, or when you set up a company-owned device, the backup tool in device settings is not available. Expand all | Collapse all Step 1: Add your Google Workspace account to the device I’m using my own personal device Choose an option: If you have a new or factory-reset device, start the device and follow the prompts to get to the Google sign-in screen. If your device isn’t new, tap SettingsAccountsAdd accountGoogle. If prompted, enter your device password. Enter your Google Workspace email address and tap Next. Your Google Workspace address is the email address that you use for work or school. Enter your password and tap Next. To accept the Terms of Service and Privacy Policy, tap I agree. If prompted, tap MoreNextNext and choose an option: Tap Use for work only. Tap Use for work & personal. What you see next depends on how your administrator wants to manage your device: If you’re asked to create a screen lock, tap Next and follow the steps. After the screen lock is created, you’re done. You can access your work apps and data on the device. If you’re asked to install a device policy app, go to Step 2. If you don’t see any prompts, you’re done. You can access your work apps and data on your device. For details about how your admin manages your device, see How your device is managed. I’m using a company-owned device If the device was already in use, do a factory reset. Tap SettingsBackup & resetFactory data resetfollow the prompts. On the home screen, tap Start. Connect to a mobile network or tap the Wi-Fi network that you want to use. Once connected, the device might check for updates. When prompted, choose an option: Copy your data from another device or the cloud. Set up the device as a new device. Sign in with your Google Workspace email address and tap Next. Your Google Workspace address is the email address that you use at your organization. Enter your password and tap Next. To accept the Terms of Service and Privacy Policy, tap I agree. When prompted, tap Accept & continue to set up your device for work. Note: If you get a prompt to install a device policy app, go to step 2 (below). Follow the prompts to set up security features. Use these steps if your device prompts you to install or update the Android Device Policy app, the Google Apps Device Policy app, or a work profile. Learn more about how your device is managed. Install the Android Device Policy app This app allows your administrator to manage your device and control some settings. For example, your administrator might want you to set a screen lock on your device. At the prompt, tap Install. Tap Install. Tap Accept & continue to create a work profile on the device. Tap Next and follow the prompts to set up your work profile. If prompted, tap Start and follow the steps to set a screen lock for your device. Tap InstallNext to install work apps. Tap Done. Create a work profile A work profile keeps your personal and work apps and data separate on a device. Creating a work profile is recommended so that your administrator doesn’t accidentally delete your personal apps or data from the device. To create a work profile: At the prompt, tap Accept & continue. Tap Next and follow the prompts to set up your work profile. If prompted to set a screen lock for your device, tap Start and follow the steps. Tap InstallNext to install work apps. Tap Done. If you didn’t create a work profile, you can open an app and sign in using your Google Workspace account to access your work or school data. If you already use an app, such as Gmail, with your personal account, you can switch to your work or school account. For details, see Switch accounts. If you created a work profile on your device, work apps are marked with a Briefcase . You might see work apps on your home screen. You can also access all work apps from your work profile. To access all apps, swipe up. Tap Work. (Optional) To find and install more work apps, go to managed Google Play . Note: Depending on your organization’s settings, you might not be able to install certain apps. For help, contact your administrator. How your device is managed Your administrator can set security policies on your device to protect data and make the device more secure. They can also erase work data from your device if you lose it. Depending on the level of device management that your administrator uses, you might need to install an app that enforces security policies on your device. For details, see About Android Device Policy. Related topics You can lock your work profile on devices with Android 7.0 Nougat or later. If you try to open a work app, you’ll be prompted to enter your passcode. Some administrators require a lock. If so, you’ll be prompted to set it when you set up your Android device. If your current screen lock meets the work profile lock requirements, you can use the same passcode for both. That way, you can open your work apps without having to enter another passcode. For devices with Android 9.0 Pie or later, your administrator can require you to use two different passcodes for your lock screen and work profile. Your administrator might set security restrictions, such as passcode complexity. They can also set a limit on the number of invalid passcode attempts. If you exceed the limit, your work profile and associated data is removed from your device. Some of this information might not be the same on every device. Set up or change your work profile lock On your device, go to Settings Security and privacy More security settings Work profile security. Tap the lock type you’d like to use and follow the instructions. (See options below.) (Optional) If you’re changing your work profile lock, enter the pattern, PIN, or password when prompted. If necessary, choose how you want your work notifications to show on your device when it’s locked. Note: You can change your work notification settings at anytime. Tap Done. Work profile lock options None Pattern Draw a simple pattern with your finger to unlock your work profile. PIN Use 4 or more numbers to unlock your work profile. Longer PINs are usually more secure. Password Use 4 or more letters or numbers to unlock your work profile. This is the most secure option, as long as you create a strong password. Fingerprint If your device has biometric sensors, you can use your fingerprint or face recognition to unlock your work profile. First though, you need to set up a pattern, PIN, or password for additional security. If you restart your device, you’ll be prompted to enter the additional lock to open your work profile. You also need to register at least one fingerprint or face on your device. Even with face or fingerprint lock active, you may still be required to provide your device pattern, pin, or password from time to time for additional security. This can occur when rebooting your device, conducting sensitive operations or after some time using only fingerprint lock. Note: Android Smart Lock is only supported as a device screen lock, not as a work profile lock. Post to the help community Get answers from community members A Work Profile is a self contained profile on an Android device for storing work apps and data. Work Profile allows separation of work apps and data, giving organizations full control of the data, apps, and security policies within a Work Profile. Simultaneously, users retain privacy over their personal apps, data, and usage. On devices designated as company-owned during setup, organizations can enforce some policies that apply to a device’s personal profile and overall device behavior. Apps installed in the Work Profile are marked with the briefcase icon, so as to be easily distinguishable from personal apps. For more information on how to use a Work Profile device, see What is a Work Profile. Feature support for devices with Work Profile All EMM providers offering Work Profiles support the following standard features: Device setup Device security Feature Description Set lock screen restrictions Set and enforce the type of passcode (e.g. PIN/pattern/password) required to unlock a device. Set Work Profile lock screen restrictions Set and enforce the type of passcode (e.g. PIN/pattern/password) required to unlock a Work Profile. Wipe and lock work data Remotely lock and wipe the Work Profile on a device. Automatic compliance enforcement Automatically restrict access to data and apps in Work Profiles on devices that aren't in compliance with security policies. Configure Smart Lock settings Enable or disable specific Smart Lock methods, such as trusted bluetooth devices, face recognition, or voice recognition. App management EMM providers support Android app management through an enterprise version of Google Play, called managed Google Play. With an EMM, you can create Managed Google Play accounts* for your users. These accounts enable app distribution to their Work Profiles. Feature Description View and manage your app catalog View a list of purchased apps, approved apps, and private apps. Distribute apps silently Silently install apps on a device without any user interaction. Download apps from the managed Play app Users can install and update apps approved for them through the managed Google Play app on their device. Set managed configurations Configure work apps for individual users or devices. Customize users' managed Play app Customize the app store layout displayed in the managed Google Play app on a device. Support Google-hosted private apps Publish Google-hosted private apps from the EMM's console and distribute them to Work Profiles. Support externally hosted private apps Publish externally hosted private apps from the EMM's console and distribute them to Work Profiles. Disable app installs from locations other than Google Play App installations from locations other than Google Play and OEM-approved sources are disabled by default. Restrict default apps Configure default apps for various supported types and prevent users from changing them. Supported Types: BROWSER CALL_REDIRECTION CALL_SCREENING DIALER SMS WALLET *For organizations with Google Workspace or Cloud Identity, users can access managed Google Play with their Google Workspace or Cloud Identity account. Device management Feature Description Set default runtime permission policies Set the default response (prompt, allow, or deny) to all runtime permission requests from apps. Set specific runtime permission policies Set the default response (prompt, allow, or deny) to specific runtime permission requests from apps. Manage certificates Deploy identity certificates and certificate authorities to a device to enable access to corporate resources. Control access to input methods Configure the input methods (e.g. keyboards) that a user can configure on their device. Control access to accessibility services Configure the accessibility services that can be enabled on a device. Set location sharing preferences Configure device location sharing settings (e.g. high accuracy, battery-saving, sensors only, off) for apps. Block users from uninstalling apps Prevent users from uninstalling apps or modifying apps through Settings. Disable screen captures and Circle to Search Prevent users from taking screenshots and using Circle to Search when using apps in a Work Profile. Retrieve network statistics Retrieve network usage statistics for a device. Device usability Feature Description Customize Work Profile setup UI Set the color, logo, and terms and conditions displayed during Work Profile setup. Customize Work Profile UI Customize Work Profiles with corporate branding. Set contact info sharing policies Control what contact information can be shared from a device's Work Profile to its personal profile. Set default apps for specific activities Set the default app for specific activities. For example, choose the default browser for opening web links. In addition to the standard features above, all Android Enterprise Recommended EMM providers offering Work Profiles support the following advanced features: Device security Feature Description Set advanced lock screen restrictions Set and enforce the quality, length, and complexity of the passcode required to unlock a device. Device integrity verification Validate device integrity to help detect if a device has been tampered with or modified. Set up automated rules (e.g. wipe and lock) if validation fails. Google Play Protect enforcement Google Play Protect's Verify Apps feature is enabled by default and scans apps for malware before and after installation. Block external data transfers Lock down bluetooth and hardware elements (e.g. Quickshare, NFC beam, external media, USB storage) to prevent users from sharing or transferring work data. App management Feature Description Managed Google Play in EMM's console Access Managed Google Play directly through the EMM's console to search for, approve, and manage work apps. Device management Feature Description Configure Wi-Fi settings Remotely deploy Wi-Fi login settings (SSID, password) to a device. Configure certificate-authenticated Wi-Fi Remotely deploy Wi-Fi settings to a device that include identity, certificates for client authorization, and CA certificates. Manage eSIMs Remotely add, remove and provision eSIMs. For Work Profile on employee-owned devices, users are responsible for activating eSIMs and can delete eSIMs at any time. Restrict access to authorized accounts Ensure that only authorized corporate accounts can interact with Work Profiles data by preventing users from adding or modifying accounts. Manage advanced certificate details Select certificates for specific work apps, remove CAs and identity certs from an active device, and prevent users from modifying credentials in the managed keystore. Manage 3rd party certificates Distribute a 3rd-party certificate management app to a Work Profile and grant the app privileged access to install certificates in the managed keystore. Enable Always On VPN Enable Always On VPN for specified apps in a Work Profile to ensure they always go through a configured VPN. Enforce approved credential managers Prevent backing up work credentials and passwords to an unapproved credential manager. Use of credential managers is blocked if no approved credential manager is set. Which Android devices are supported? Work Profile is supported on devices with 2GB or more of RAM, personally-owned devices running Android 5.0 or later, and company-owned devices running Android 8.0 or later. Learn more about the difference between personally and company-owned devices. Which EMM providers support Work Profiles? EMM providers that support Work Profiles are listed in the Android Enterprise Solutions Directory. Post to the help community Get answers from community members 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 can’t 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 to impersonate 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 Android 11.0 or later devices only You may have some core apps on your device that are installed in both your work profile and your personal profile (e.g. the Calendar app). If your organization allows it, you can enable some of these apps to share data and connect with themselves across your work and personal profiles. Note: Enabled connected apps may share your personal data with your employer or other work apps. Connecting an app across profiles can enhance the way you use your device. For example, by connecting your calendar app you could view your work and personal events together. Some apps (for example, Google Search) may be connected on your device by default. To view your connected apps at any time, go to Settings > Apps > Special app access > Connected work & personal apps. Connect apps Open and use any app in your work profile. If the app can be connected across profiles, you will be prompted to connect them. Follow the prompt to open Settings. Toggle the Connect these apps switch. Review the permissions screen to learn how your data will be shared between connected apps. Only connect apps that you trust with your personal data. To connect the apps, click Allow. If the app is only installed in your work profile, you’ll be prompted to install it in your personal profile. If you see Action Not Allowed or a similar warning message, then your organization has not permitted you to connect this app. Contact your administrator for more information. Disconnect apps If you have connected apps, you can disconnect them at any time. Go to Apps > Special app access > Connected work & personal apps. Tap the app you want to disconnect. Toggle Connect these apps to disable communication between your work app and personal app. Post to the help community Get answers from community members Android 5 or later devices only Android Work Profile can be set up on an Android device to separate work apps and data from personal apps and data. With a Work Profile you can securely and privately use the same device for work and personal purposes—your organization manages your work apps and data while your personal apps, data, and usage remain private. Note: Work Profile apps can't access SMS or MMS data from the personal profile on Android 11+. If your organization supports enrolling devices to use a Work Profile, your IT admin should provide instructions on how to add one to your device. Does my device have a Work Profile? Go to Settings Passwords and accounts. If you have a Work Profile, you will see a work tab with Work Profile settings listed underneath. Work Profile settings are also searchable in your device’s main Settings on Android 14 or later. How do I access my work apps? Work apps are marked with a briefcase icon so you can distinguish them from personal apps. To access your work apps: Swipe up from the bottom of your screen to the top. Tap the "Work" tab. Tap the app that you want to open. If your work app icons are gray, your work profile may be paused. Learn how to pause or turn on your Work Profile. How do I delete my Work Profile? You can only delete your Work Profile if you personally own your device or your organization relinquishes ownership of a company-owned device to you. To delete your Work Profile: Go to Settings Passwords and accounts Tap the Work tab Remove Work Profile. Tap Delete to confirm the removal of all apps and data within your Work Profile. Ensure that the policy app ("Device Policy") is uninstalled and not present on your device. After the Work Profile is deleted, all local data on the device within that profile is deleted. You can also remove all apps and data (both personal and work) by factory-resetting your device. Related articles Post to the help community Get answers from community members If you have an Android Work Profile your work or school manages, you can show your personal calendars in the Google Calendar app for Android. Learn how personal calendars work To show personal calendars in your work account, your administrator must allow it. If you can’t find an option to add your personal calendars, you might not have access to the feature. Your work and personal calendars are stored separately. Personal account details aren’t shared with your work account. Unless you share your personal calendars directly with your work account, coworkers and administrators can’t find your personal calendars. Learn more about an Android Work Profile. Set up personal calendars On your Android phone or tablet, open the Google Calendar app . Tap Menu Settings Personal calendars. Tap Turn on in Settings. Turn on Connect these apps. Tap Allow. Tips: To maintain a clear separation between your personal and work calendar data, in your work Calendar app, turn on the “Personal calendars” setting. To make your personal calendars available on all Calendar surfaces, such as computers and mobile devices, share your personal calendars directly with your work account. Remove duplicate personal events If you share your personal calendars with your work account, you can find copies of personal events in the "Personal calendars" section of your work Calendar app. You can remove these duplicate events from your work account. On your Android phone or tablet, open the Google Calendar app . Tap Menu Settings Personal calendars Connected. Related resources What is an Android Work Profile? Connect your work and personal apps Post to the help community Get answers from community members