Click Here

Next: Make Chrome your default browser You can customise your browsing experience when you sign in to Chrome through your Google Account. Important: To sign in to Chrome, you must have a Google Account. On your iPhone or iPad, open Chrome . If you don't have Google Chrome, download it from the app store. Tap More Settings Sign in. Under 'Sign In to Chrome', select the account that you want to use. Tap Continue as. Post to the Help Community Get answers from community members Passkeys are a simple and secure alternative to passwords. With a passkey, you can sign in to your Google Account with your fingerprint, face scan, or phone screen lock, like a PIN. Important: If you add a passkey to your Google Account, it won't change or remove any authentication or recovery factors you currently have on your account. If your account has 2-Step Verification or is enrolled in the Advanced Protection Program, a passkey bypasses your second authentication step, since this verifies that you have possession of your device. Your biometric data, used for fingerprint or face unlock, stays on your device and is never shared with Google. Why should I use a passkey? Passkeys provide the strongest protection against threats like phishing. Once you create a passkey, you can use it to easily sign in to your Google Account, as well as some third-party apps or services, and to verify it's you when you make sensitive changes. Why are passkeys safer than passwords? Unlike passwords, passkeys can only exist on your devices. They can't be written down or accidentally given to a bad actor. When you use a passkey to sign in to your Google Account, it proves to Google that you have access to your device and are able to unlock it. Check what you need to create a passkey To create a passkey, you need one of these: A laptop or desktop that runs at least Windows 10, macOS Ventura, or ChromeOS 109. A phone that runs at least iOS 16 or Android 9. A hardware security key that supports the FIDO2 protocol. Tip: To create a passkey on a FIDO2 hardware security key added to your Google Account prior to May 2023, you may first need to remove this security key from your account. After it's removed, you'll be able to create a passkey on this security key. Your computer or mobile device also needs a supported browser like: Chrome 109 or up Safari 16 or up Edge 109 or up Firefox 122 or up To create and use a passkey, you must enable the following: Screen lock Bluetooth This applies if you want to use a passkey on a phone to sign in to another computer. For iOS or macOS: You must turn on iCloud Keychain. When you set up a passkey on your Apple device, it prompts you to turn on your iCloud Keychain if not set up already. For more info on how to set up iCloud Keychain, go here. Tip: To ensure the best passkeys experience, make sure your operating system and browser are up to date. Based on your operating system and browser, you may not be able to create or use passkeys while in Incognito mode. Passkeys for Google Workspace If you have a Google Workspace account through your school or employer, you may not be able to sign in to your account with just a passkey. You can still create passkeys on your devices, but they may only be used as a second factor in 2-Step Verification, in account recovery, and for some sensitive actions in your account that require Google to re-verify your identity. In the "Skip password when possible" account settings page, you can find whether your admin allows you to sign in with just a passkey. Workspace admins can learn more here. Set up passkeys Important: When you create a passkey, you opt in to a passkey-first, password-less sign-in experience. Create passkeys only on personal devices that you control. Even if you sign out of your Google Account, once you create a passkey on a device, anyone who can unlock the device can sign back into your Google Account with the passkey. To set up a passkey, you may need to sign in to your Google Account or verify it's really you. Tip: When you sign in to a site with a password saved in Google Password Manager, it may automatically create a passkey. Learn more about automatic passkey creation. Create a passkey To create a passkey on the phone or computer you're on: To create passkeys on multiple devices, repeat these steps from those devices. To create a passkey on an external FIDO2 capable USB security key: Tips: Once you create your first passkey, the next time you sign in on any device that supports passkeys, you'll be prompted to create a passkey on that device. If you don't want other users to access your account, do not create a passkey on a shared device. How do I use my passkey to sign in? On your device, open the Google sign-in page. Enter your username. Note: When you tap on the username field, you may see a list of passkeys. If so, tap the passkey you'd like to use. If you have previously created a passkey for your account on that device, Google will prompt you to verify your identity with that device's passkey. To unlock the device and verify your identity, follow the on-screen passkey instructions provided by your operating system and browser. Tips: When you sign out of an Android device: You can use your passkey to sign back in on this Android device for up to 6 hours post-sign out. After 6 hours, you need to use an alternate method to sign back in. When you sign back in, Android automatically generates a new passkey and the old passkey expires. When you sign out of a non-Android device: You can sign back in with your passkey at any time after sign out. To sign in to your account on a computer, you can use a passkey created on a phone: If you have a passkey on an Android or iOS device or on a hardware security key, you can use it to sign in on a different device that supports passkeys. On the Google sign-in page on your computer, enter your username. Below the password field, click the Try another way link. Click Use your passkey. On your screen, find the QR code. If you want to use a passkey that was created on a hardware security key, you'll have an option to select "USB security key" or equivalent. To scan the QR code, use your phone's built-in QR code scanner app. For iOS: You can use the built-in camera app. For Google Pixel phones: You can use the built-in QR code scanner. For other Android devices: If you can't scan the QR code with the native camera app or the system QR code scanner, you can use Google Lens. On your phone, tap Use passkey. To verify your identity on your phone, you'll be prompted for your fingerprint, face unlock, or phone PIN. The next time you sign in with this computer and phone combination, you'll automatically get a notification on your phone to complete the identity verification process. Tip: After you sign in, you may be asked to create a passkey on the computer. If you don't want other users to access your account, do not create a passkey on a shared device. Use your passkey to sign in By default, when you create a passkey you opt in to a passkey-first, password-less sign-in experience. However, you'll still have the option to use your password to sign in to your account. If you would like to always use your password first, you can change this default preference in your account settings. Go to your Google Account. Select Security. Under "How you sign in to Google," turn off Skip password when possible. When this option is turned off and you sign in, you'll be prompted for your password. If you're enrolled in 2-Step Verification, you'll have the option to use any of your passkeys as the second step. Check your passkeys If your account already has passkeys, they're listed here. Tip: If you have an Android phone signed in with this account, you may have passkeys registered automatically for you. Remove or opt out of passkeys If you lose a device where you created a passkey, or created a passkey on a shared device by mistake, you should invalidate the passkey for use with your Google Account. Remove a passkey that you created Go to your Google Account. Select Security. Under "How you sign in to Google," tap Passkeys and security keys. Select the passkey you want to remove. Tap Remove . Remove a passkey automatically created by Android To remove a passkey that was automatically created on your Android phone, you need to remove the device from your Google Account. Go to your Google Account. On the left navigation panel, select Security. On the Your devices panel, select Manage all devices. Select the device Sign out. If multiple sessions appear with the same device name, they could all come from the same device or multiple devices. If you want to make sure there's no account access from a device, sign out of all the sessions with this device name. Tips: You can check google.com/devices to review all devices with access to your account. If you removed a passkey from your Google Account, but you're still prompted to use it at sign-in, check any third-party credential manager that you use to see if the passkey is there. If so, remove the passkey from the credential manager. For instructions on how to remove the passkey, go to your credential manager's support documentation. Fix a problem about a lost or missing passkey Lost or stolen device On a device you're able to access, sign in to your Google Account. Remove the passkey associated with the lost or stolen device. Learn how to remove a passkey. Missing or unavailable passkey If you have passkeys on your account but aren't offered a passkey during sign-in, make sure that: The device with the passkey has the screen lock enabled. If your device's screen lock is disabled, you will not be able to use the passkey on that device until you enable the screen lock again. The "Skip password when possible" toggle is on in your security settings at myaccount.google.com/security. To sign in to your Google Account without a passkey, tap Try another way to skip the passkey challenge and go back to your earlier sign-in choices. Tip: If you choose "Try another way" often, Google will offer the passkey challenge less frequently in the future to reflect your implied preferences. You can change this by repeatedly signing in with passkeys. Related resources Post to the help community Get answers from community members Important: To use Sign in with Google, you need a Google Account. Your Google Account is the same account you use for Gmail, Drive, and other Google apps. Sign in with Google helps you easily and securely sign in to third-party apps or services with your Google Account. When you use Sign in with Google, you don't have to enter a username and password repeatedly across different services. Tips: Sign in with Google | Faster, safer access Different ways to sign in You can use your Google Account to sign into third-party apps or services in 3 ways. These are all methods to use your Google Account to sign in: Sign in with Google button Google sign-in prompt Automatic Sign-in Sign in with Google button If you've never used Sign in with Google to sign into the third-party app: The app displays a non-personalized Sign in with Google button. This button prompts you to sign in. When you do so, you grant consent to share the name, email, and profile picture on your Google Account with the third-party. If you've previously used Sign in with Google with the third-party app: The app displays a personalized button. This button helps you remember how you last signed into this app. Once you click the button, you can confirm the account you want to use to sign in. It then signs you into the app. Google sign-in prompt You can sign up for or sign in to third-party accounts easily with the Google sign-in prompt. When you visit a site or app that supports the Google sign-in prompt, a notification pops up. This notification prompts you to sign up or sign in. After you tap this, you're signed in to the third-party app. Automatic Sign-in Important: To use Automatic Sign-in, you must already be signed in to your Google Account and have previously granted consent to share your profile with the third party for the purpose of signing in. If you haven't granted consent to the third party, the Google sign-in prompt appears. To provide a seamless experience, Automatic Sign-in removes the manual steps to sign in when you return to an app or service. A dialog box shows the process of the sign in as it occurs. Why use Sign in with Google Sign in with Google makes it easy for you to sign in and sign up to websites and apps across the internet with the trusted security of your Google Account. It eliminates your dependency on passwords, which reduces the frustrations and security risks associated with them. Improved security When you use Sign in with Google, you create a secure, passwordless account with the third party service. This means you don't have to use unique usernames and passwords for each third-party service. When you use Sign in with Google, you reduce the number of apps and services where passwords need to be stored. Sign in with Google also ensures the secure transfer of authentication information. Since you can use Google Account to log in to multiple apps and services, we work to ensure the safety of your experiences with your favorite apps and websites. For example, we enforce the use of HTTPS to encrypt your data. This makes browsing safer and prevents insecure sign-in experiences. Our secure technology, Cross-Account Protection, also helps detect suspicious events on your account. It shares security notifications with participating third-party apps and services you connect to your Google Account. That way, third-party apps and services can use Google's suspicious event detection to help keep you safer online. Easy to use Sign in with Google allows for easy sign-in experiences. It lets you sign in with one or two clicks. In some cases, after you use Sign in with Google on a site or app on one platform, you can then sign in automatically and consistently across all platforms. When you browse a new website or try out a new app, you can use Sign in with Google to create a new third-party account. The account uses your Google Account profile information, which includes your name, email, and profile picture. Preserve your privacy Important: We never share your Google Account password with a third party. Your privacy is important, so it's easy for you to control what information is shared and with whom. When you consent to share information with the third party to sign in, the information we share includes your name, email address, and profile picture. Google doesn't use data from Sign-in with Google for ads or other non-security purposes. To learn more, review How Sign in with Google helps you share data safely. If you have concerns about a third party's privacy or data sharing policies, you can stop using Sign in with Google with their app or site. Once you consent to share your data, it is controlled by the third party and becomes their responsibility to manage. For more information, check the third party's privacy policy. Sign In Everywhere When you use the Sign in with Google option, you are able to sign in across different platforms and browsers and can expect a consistent sign-in flow. While the sign-in experience across platforms like Android and iOS may differ slightly from the experience on the web, we try to make the process consistent. How Sign in with Google works Sign in with Google offers an easier way to log into different sites across the internet. If you have questions on what Sign in with Google offers, learn more below. Can I use Sign in with Google if I don't have a Google Account? In order to use Sign in with Google, you need a Google Account. What if I'm logged out of my Google Account when I want to use Sign in with Google? To use Sign in with Google, you must first log into your Google Account. If I have more than one Google Account, how does Sign in with Google work? If you have more than one Google Account, Sign in with Google prompts you to choose which account you want to use. If the Google Account you want to use isn't one of the choices, select Add another account. Does it matter if I already have an account on the third-party app? If you have an account with a third-party app or service, you can use Sign in with Google to log in. If you don't have an existing account with the third party, one may be automatically created for you when you use Sign in with Google. What happens if I delete my Google Account? Your Sign in with Google data is also deleted, which includes your sign-in credentials for the third-party site. That means you can no longer use the Sign in with Google button to sign in with the deleted account. Even if your Google Account is deleted, you may still be able to access your separate third-party account in another way. Try to sign in to the app or service with a username and password, or contact the developer directly. You can also try to create new sign-in credentials on the third-party site. What happens if I delete my third party account? If you delete your third-party account, your Google Account is unaffected, because third-party accounts and Google Accounts are independent of each other. The third party doesn't notify Google even if you used Sign in with Google to create that account. Your Google Account might still show the app or service is linked to your account. To understand how the third party handles your data, review their Terms of Service. Some third parties simply disable your account. Others delete your data from their service. If your data is deleted, you need to create a new account on the app or service. You can still use Sign in with Google to do this, but you may need to use a different Google Account. How do I keep track of where I use Sign in with Google? How do I stop using Sign in with Google? If you no longer want to use your Google Account to sign in to a third-party app or service, you can remove its connection. Make sure you're signed into your Google Account. View the apps and services that use Sign in with Google. Select the third-party app or service whose connection you want to remove. Select See details Stop using Sign in with Google Confirm. Tip: If you have more than one connection type, your Sign in with Google connection will appear under "How Google helps you sign into {App name}." What happens when I use Sign in with Google? Sign in with Google uses a securely transmitted code that's based on your Google Account. It allows apps to authenticate you and create an account based on the information it shares from your Google Account, like name, email, and profile picture. To learn more, review how Sign in with Google helps you share data safely. Post to the help community Get answers from community members SearchClear searchClose searchGoogle appsMain menu It doesn't look like you have an account yet. You can sign up on your own below or get free, personalized support with a Google Ads Expert. Start Now This article shows you how to sign in to your Google Ads account. You can also learn more about additional sign-in options and other relevant information for signing in to Google Ads. Your Google account allows access to most Google products, so we recommend you don't share your password with anyone. Enable 2-step verification in your Google Account for additional security. This verification process requires your username, password, and validation using your phone or verification codes when you sign into your account. Adding a current recovery phone number is an easy way to help recover access to your account. Learn more about how to Set up a recovery phone number or email address. Before you begin, make sure you're using the most up-to-date version of your browser. Google Ads is compatible with the latest versions of Firefox, Internet Explorer, Safari, and Chrome. Learn more about how to Fix an issue with your browser. Sign in to Google Ads using your Google account Go to the Google Ads homepage. Click the Sign in link at the top right of the page. Enter your Google account email address, an alternate email address, or your Gmail username in the "Email" field. Enter your password in the "Password" field. Click Next. Additional sign-in options Access multiple Google Ads accounts from the same Google account If you're an agency or manage multiple Google Ads accounts, a manager account could save you time by letting you view and easily manage all of your Google Ads accounts from one account. Learn more About Google Ads manager accounts. If you already have a manager account, you can use the same email address for your manager account and your Google Ads accounts. If you have multiple Google Ads accounts, you can associate them with your Google account and access them all from one place. This allows you to manage multiple businesses with separate Google Ads accounts without needing to create a new Google account or email address for each of them. Switch to another Google Ads account without signing out Click your profile image on the top right of your Google Ads account. This will show a list of the Google Ads accounts associated with your current Google account. From the list of associated accounts, select the account you want to access. If your Google Ads accounts are linked to different Google accounts, you can also access these different Google accounts, and associated Google Ads accounts without having to sign out and back in again. Sign in to multiple Google accounts Click your profile image on the top right of your Google account. Click Switch account. Enter the email address for the account, and click Next. Enter the password for the account, and click Next. Note that signing into multiple accounts doesn't merge your account data or give these accounts access to one another. After you've logged into multiple accounts in the same browser, you can click your profile image and select a different account from the list at any time.If you sign in to a Google account that isn't yet associated with a Google Ads account, you'll be directed to the Google Ads sign-up page. Sign in with an alternate email address for your Google account If you've added an alternate email address to your Google Account, you can use that alternate email address to sign in to Google Ads. Your password will be the same as the password for your primary email address. Fix a problem with signing in How to Sign into Google Ads Troubleshoot issues with signing in Use the sign-in issues troubleshooter to help resolve login issues in your Google Ads account. This troubleshooter can help you learn more about issues such as lost usernames or passwords, common browser issues, and account recovery. Update your credentials You can change the information you use to sign in to your Google Ads account in several ways. The method you choose affects how you sign in to your other Google products. Learn more about how to Change your Google Ads sign-in information. Recover a lost account If you can't access your account because the original account manager has left your organization, submit the lost account form. In case contacting an Admin is not feasible, like in cases where there are no active admins in the account, you can request access using the form. You'll need to provide proof of account ownership, which will be validated by the support team that grants access to the account. Related links This article is for people who manage Google services or devices for a company, school, or group. If you're using a personal (@gmail.com) account, go instead to the Google Account Help Center. If you have access to an administrator (or admin) account, you can sign in to the Google Admin console. The Admin console, at admin.google.com, is where admins manage Google services for people in an organization. In any web browser, go to admin.google.com. Starting from the sign-in page, enter the email address and password for your admin account (it does not end in @gmail.com). If you forgot your password, go to Reset your administrator password. An admin account has privileges to manage services for other people in your organization. The Admin console is only available when you're signed in to an admin account. If you don't have access to an admin account, get help from someone else who does. For details, go to Who is my administrator?. If you find a list of Google Accounts on the sign-in page, be sure to choose your admin account (it does not end in @gmail.com). Tip: You can switch between accounts on the same computer without signing in each time. For details, learn how to sign in to multiple accounts at once. Get help signing in If you forgot your password, go to Reset your administrator password. If you're still having trouble signing in, go to Can't sign in to the Admin console. Questions Expand all | Collapse all Why did I have to sign in twice? If your company is using a single sign-on (SSO) service with your Google account, then signing in to your account from admin.google.com sends you to a second sign-in page. From here, you sign in to your Admin console and other programs or services your company has set up with SSO at the same time. Just enter the sign-in name and password your admin gave you. Learn how to sign in with SSO. Can Chrome's password manager store my Google login details? With Chrome Browser, you can manage your website passwords so that Chrome automatically completes the sign-in fields for you when you visit these websites. The two-step sign-in flow for all Google accounts does not impact the behavior of the password manager. Why do I sometimes need to sign in again while using the Admin console? To keep your organization's Google services secure, you need to sign in to the Admin console after each hour of use. How does enabling single sign-on (SSO) affect sign-in if I'm an administrator? If you're a super administrator and you sign in to admin.google.com with your full admin address (name@example.com) and password, you're redirected to the Admin console. Google does not redirect you to the SSO server. If you're not a super administrator and sign in at admin.google.com, you are redirected to the SSO sign-in page. For more details, go to Signing in with SSO I'm a reseller. Can I access my customer's Admin console? It is possible for a reseller to access their customer's Admin console. Go to admin.google.com/customer_domain. Sign in with either your own reseller account name and password, or use an admin account at the customer's domain. For more details, go to Access a customer's Admin console To connect to any Outlook account, Microsoft now requires non-Microsoft email clients to use modern authentication methods. If you try to sync your Outlook account with Gmail, you might experience sync failures and get error messages. Learn what happens when you try to add an Outlook account In Gmail on your computer, you can no longer add an Outlook account. To add an Outlook account, use the Gmail app . If you use the Gmail app for iPhone and iPad, your Outlook account continues to sync with your Gmail account. Fix sync issues with Outlook in the Gmail app If the sync fails, follow these steps to remove your account and add it again. Remove an account from your Android device On your Android phone or tablet, open the Gmail app . At the top right, tap your Profile picture Manage accounts on this device. Tap your Microsoft account Remove account. When you remove the account, any unsent emails are also deleted. Add an account to your Android device On your Android phone or tablet, open the Gmail app . At the top right, tap your Profile picture Add another account Outlook, Hotmail, and Live. Sign in with your Microsoft account. Post to the help community Get answers from community members