HYPR Info Brief

A User's Guide to Passkeys

What Are Passkeys?

Passkeys remove the need for passwords, making your login experience easier and more secure. Passkey authentication eliminates credential stuffing and other attacks that use stolen or cracked passwords. It also protects you against phishing sites as the passkey is linked to a specific website or application.

Passkey authentication requires either biometric authentication, such as a fingerprint or facial recognition, a PIN or a swipe pattern (on Android devices) for access. Passkeys are secret keys that stay on your personal devices that can be used for authenticating to applications and websites on your phone, tablet or laptop. They leverage the Web Authentication API security standard, which uses public key cryptography for access. Each key is unique and created with encrypted data for added security.

Types of Passkeys

There are two primary types of passkeys, which differ in their usage and functional purpose.

Multi-Device/Synced Passkeys

For the most part, this guide concerns the type of synced (multi-device) passkeys meant for consumer use. They have some limitations in security and functionality for enterprise environments (e.g., cannot be used for desktop login, do not meet regulatory requirements for an independent possession factor, and lack other critical enterprise capabilities).

Device-Bound Passkeys

A device-bound passkey, also called an Enterprise Passkey, is significantly more robust in terms of its functionality and ability to operate within a technology stack, covering the entire range of enterprise use cases. HYPR's fully FIDO Certified passwordless MFA solution provides this type of passkey. You can read more about the HYPR technology here.

Overview of How Passkeys Work

Passkeys work through an API called Web Authentication, commonly called WebAuthn. WebAuthn is a joint initiative of the World Wide Web Consortium (W3C) and the FIDO Alliance, an industry association that works to end our overreliance on passwords.

Instead of a password, WebAuth uses public and private keys – otherwise known as public-key cryptography – to verify that you are who you say you are. Public and private keys are mathematically linked to one another. You can think of them like interlocking puzzle pieces; they're designed to go together, and you need both pieces to authenticate successfully. Unlike a traditional password, the private key is never shared with the site you want to sign in to, or stored on their servers.

When you visit a website that supports passkeys, you can choose to secure your account with a passkey, rather than a traditional password. The website's server communicates information about the website, and asks you to confirm your authenticator. This could be your phone, tablet or PC. A passkey — which includes your public and private key pair — gets generated for that specific website. This happens locally, on your device. The public key is stored on the website's server, while the private key remains securely stored in your authenticator.

To sign in, the website sends an assertion challenge to your authenticator. You then must take the required action on the authenticator, such as entering a PIN or presenting a biometric. Your authenticator then signs the authentication assertion with your private key and sends it back to the website. The website verifies the signed authentication assertion using their copy of your trusted public key, and you gain access.

All of this happens behind the scenes. All you need to worry about is setting up the passkey and unlocking it with the required action.

Who Creates Passkeys?

Passkeys are created by you on your device and copied across your Google, Apple, and Microsoft accounts on your phones, tablets, and laptops.

- Apple announced support in iOS 16 in Sep 2022, and iPadOS 16 and macOS Ventura in October 2022.
- Google announced support in Android starting October 2022 and ChromeOS in December 2022.
- Microsoft Windows is set to deliver support in 2023.

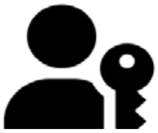
Many browsers already support sign-in with a passkey from a nearby device such as a mobile phone or security key. These include:

- Microsoft Edge and Google Chrome on Windows
- Edge, Safari and Google Chrome on macOS
- ChromeOS

How You Log In With Passkeys

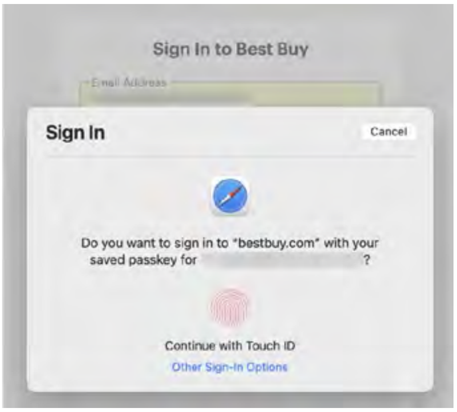
Passkeys are accessed using the same WebAuthn API that has been available across all the platforms and browsers since 2018. The cross-device sync of passkeys is managed transparently by the OS.

Websites that support passkeys use the passkey icon shown below:



For any website or application that you have set up passkey authentication, you will be asked if you want to sign in using your saved passkey. You then authorize using the same biometric or PIN that you use to unlock your device and you'll be signed into your account.

The login experience might look like this:



Sign In to Best Buy

Email Address

Sign In

Cancel

Do you want to sign in to "bestbuy.com" with your saved passkey for [redacted] ?

Continue with Touch ID

Other Sign-In Options

Can You Lose a Passkey?

For shareable passkeys (typical of individual passkeys) it is possible to lose a passkey if it hasn't been copied to your other devices automatically or if you lose all your devices that are tied to your Apple or Google accounts.

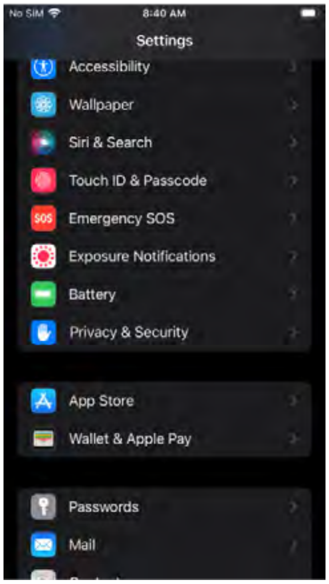
For enterprise passkeys, FIDO specifies they should be available only from a single device from which they cannot be copied. Such passkeys are sometimes referred to as "device-bound passkeys". In such a case retrieval difficulties vary depending on how the instance is configured. See more about individual vs. enterprise passkeys below.

How to View Your Passkeys

On iOS Devices (Apple iPhone or iPad)

Passkeys are located In Settings > Passwords , You can view listing of the sites with corresponding passkeys.

Settings:

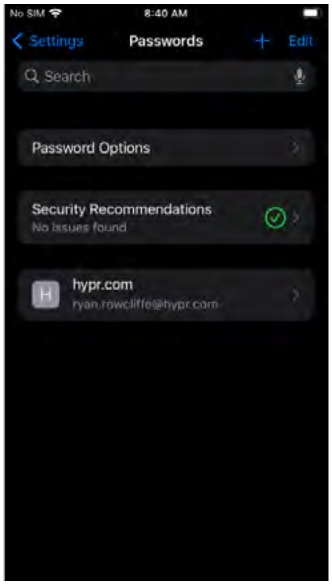


No SIM 8:40 AM

Settings

- Accessibility
- Wallpaper
- Siri & Search
- Touch ID & Passcode
- Emergency SOS
- Exposure Notifications
- Battery
- Privacy & Security
- App Store
- Wallet & Apple Pay
- Passwords
- Mail

Passwords:



No SIM 8:40 AM

Settings Passwords + Edit

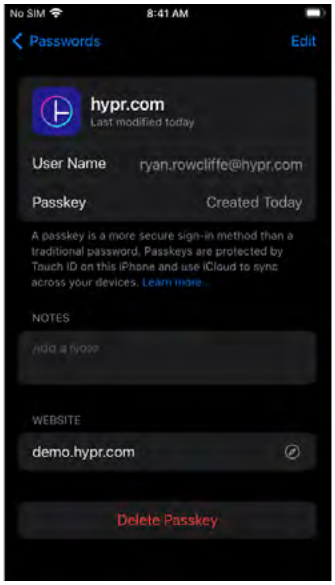
Search

Password Options

Security Recommendations
No Issues found

hypr.com
ryan.rowcliffe@hypr.com

Passkey:



No SIM 8:41 AM

Passwords Edit

hypr.com
Last modified today

User Name ryan.rowcliffe@hypr.com

Passkey Created Today

A passkey is a more secure sign-in method than a traditional password. Passkeys are protected by Touch ID on this iPhone and use iCloud to sync across your devices. Learn more

NOTES

Add a Note

WEBSITE

demo.hypr.com

Delete Passkey

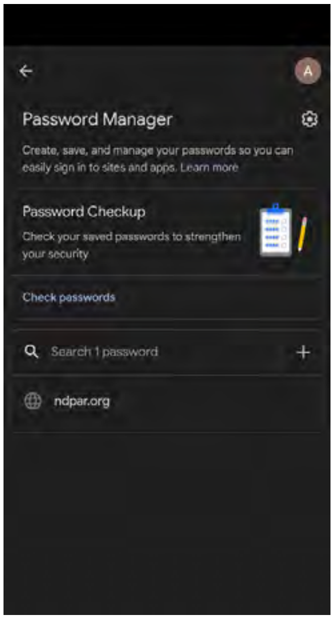
On Android Devices

Passkeys from Google Password Manager are available to all Android apps, including Chrome and other browsers. Passkeys are stored on an Android device when the user creates a passkey. The passkeys are encrypted end-to-end and then synced with the user's other Android devices. This makes passkeys available to the user across all Android devices that use Google Password Manager, as long as they are signed in with the same Google account.

1. On your Android phone or tablet, open your device's **Settings** app
2. Tap **Passwords & accounts**
3. Tap **Google** in Passwords section
4. Passkeys will be shown at the bottom of the list

On Samsung

Settings > Privacy > Autofill service from Google > Password
OR Settings > General Management > Passwords and autofill > Google > Password Manager



Password Manager

Create, save, and manage your passwords so you can easily sign in to sites and apps. Learn more

Password Checkup

Check your saved passwords to strengthen your security

Check passwords

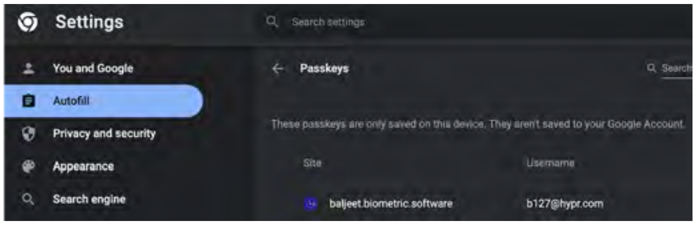
Search 1 password

ndpar.org

On Your Mac Computer

In the Chrome Browser

In the chrome browser, navigate to chrome://settings/passkeys:



These passkeys are only saved on this device. They aren't saved to your Google Account.

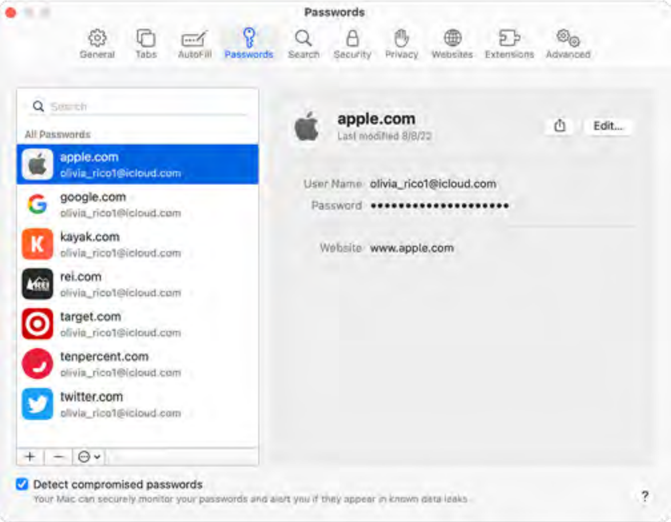
Site	Username
baljeet.biometric.software	b127@hypr.com

NOTE: Apple keeps passwords and passkeys in the same location and are indistinguishable until you select the website.

In the Safari Browser

To View saved passkeys in Safari:

1. Open Safari
2. From the Safari menu, choose Settings (or Preferences), then click Passwords
3. Sign in with Touch ID, or enter your user account password
4. Select a website



apple.com
olivia_rico1@icloud.com
google.com
olivia_rico1@icloud.com
kayak.com
olivia_rico1@icloud.com
rei.com
olivia_rico1@icloud.com
target.com
olivia_rico1@icloud.com
tenpercent.com
olivia_rico1@icloud.com
twitter.com
olivia_rico1@icloud.com

apple.com
Last modified 8/8/22

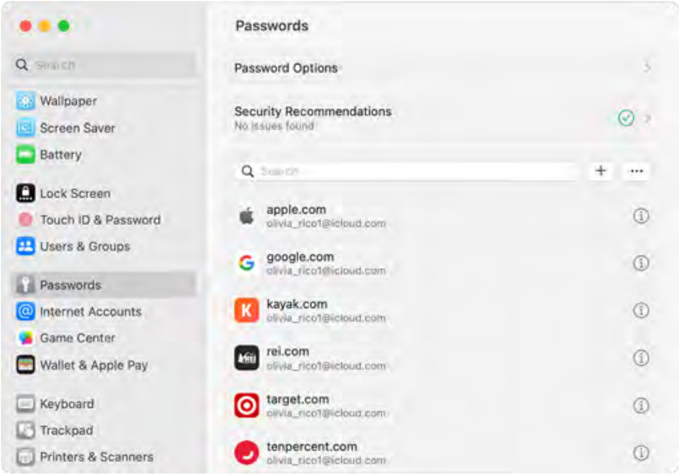
User Name olivia_rico1@icloud.com
Password ••••••••••••••••••••
Website www.apple.com

☑ Detect compromised passwords
Your Mac can securely monitor your passwords and alert you if they appear in known data leaks

In System Settings

To view saved passwords and passkeys in System Settings:

1. Choose Apple menu > System Settings.
2. Click Passwords
3. Sign in with Touch ID, or enter your user account password
4. Select a website, then click the Show Details button



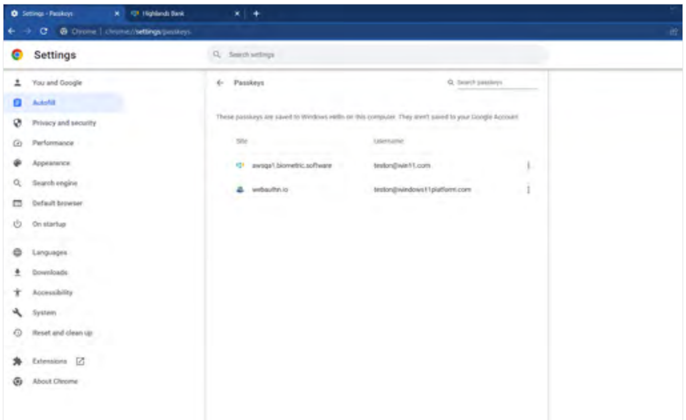
Security Recommendations
No issues found

apple.com
olivia_rico1@icloud.com
google.com
olivia_rico1@icloud.com
kayak.com
olivia_rico1@icloud.com
rei.com
olivia_rico1@icloud.com
target.com
olivia_rico1@icloud.com
tenpercent.com
olivia_rico1@icloud.com

On Your Windows PC

You cannot view synced passkeys in any current version of Windows. You can view local device-bound passkeys in Chrome on Windows 11 only (not Windows 10). To view device-bound passkeys on Windows 11, open Chrome and enter chrome://settings/passkeys in the URL bar.

Windows 11 example:



These passkeys are saved to Windows Hello on this computer. They aren't saved to your Google Account

Site	Username
awsqa1.biometric.software	teston@win11.com
webauthn.io	teston@windows11platform.com

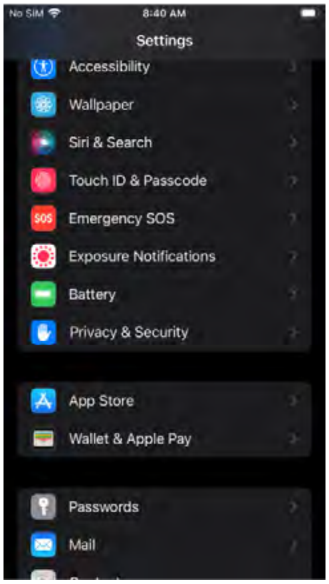
How To Revoke Passkeys

On iOS Devices (Apple iPhone or iPad)

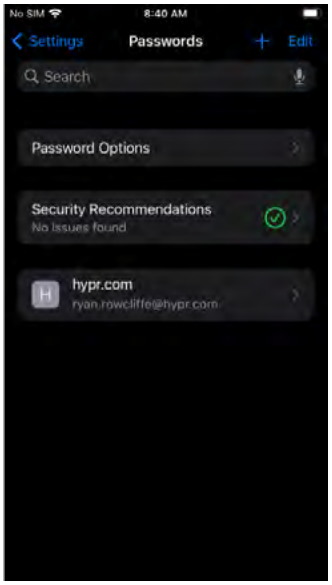
Passkeys are located In Settings > Passwords , You can view listing of the sites with corresponding passkeys.

Use the “Delete Passkey” button to revoke the passkey.

Settings:

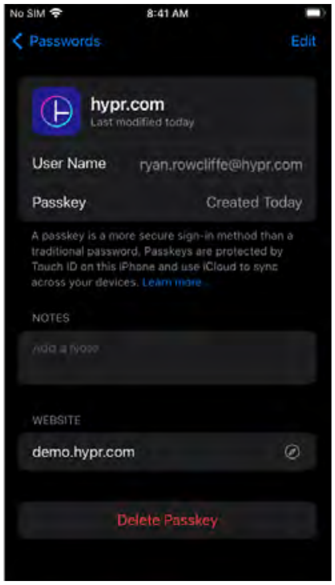


Passwords:



hypr.com
ryan.rowcliffe@hypr.com

Passkey:



hypr.com
Last modified today

User Name: ryan.rowcliffe@hypr.com

Passkey: Created Today

A passkey is a more secure sign-in method than a traditional password. Passkeys are protected by Touch ID on this iPhone and use iCloud to sync across your devices. Learn more

NOTES

Add a Note

WEBSITE

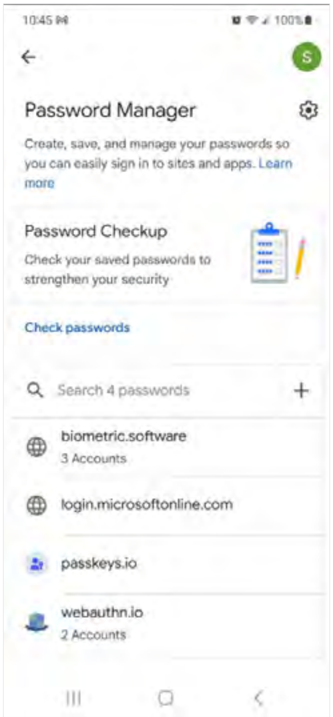
demo.hypr.com

On Android Devices

Passkeys are revoked by navigating to: Settings > General Management > Passwords and autofill > Google

If there are multiple accounts on the device, select the account in which the passkeys were created. Google Password Manager opens and displays a list of stored passkeys. Select the specific domain which the passkeys were registered to and hit "Delete."

Google Password Manager:



10:45

Password Manager

Create, save, and manage your passwords so you can easily sign in to sites and apps. Learn more

Password Checkup

Check your saved passwords to strengthen your security

Check passwords

Search 4 passwords

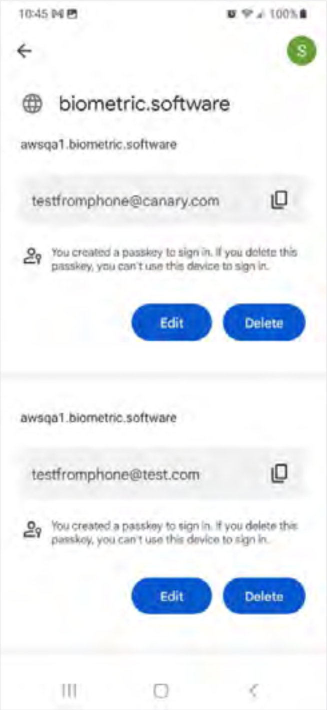
biometric.software
3 Accounts

login.microsoftonline.com

passkeys.io

webauthn.io
2 Accounts

Example:



10:45

biometric.software

awsqa1.biometric.software

testfromphone@canary.com

You created a passkey to sign in. If you delete this passkey, you can't use this device to sign in.

Edit Delete

awsqa1.biometric.software

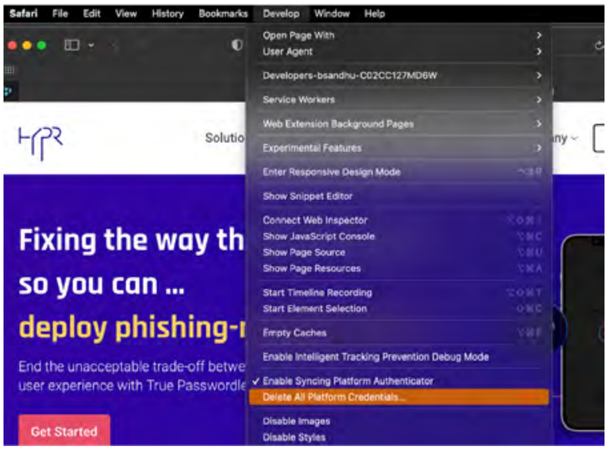
testfromphone@test.com

You created a passkey to sign in. If you delete this passkey, you can't use this device to sign in.

Edit Delete

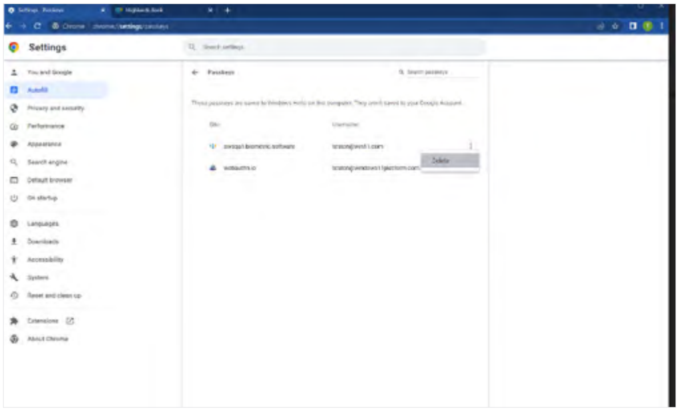
On Your Mac Computer

Via Safari, navigate to "Develop", and then select "delete platform credentials."


Safari File Edit View History Bookmarks Develop Window Help
Open Page With
User Agent
Developers-bsandhu-C02CC127MD6W
Service Workers
Web Extension Background Pages
Experimental Features
Enter Responsive Design Mode
Show Snippet Editor
Connect Web Inspector
Show JavaScript Console
Show Page Source
Show Page Resources
Start Timeline Recording
Start Element Selection
Empty Caches
Enable Intelligent Tracking Prevention Debug Mode
✓ Enable Syncing Platform Authenticator
Delete All Platform Credentials...
Disable Images
Disable Styles
HYPR
Solutio
Fixing the way th
so you can ...
deploy phishing-r
End the unacceptable trade-off betwe
user experience with True Passwordle
Get Started

On Your Windows PC

Managing passkeys on Windows is only supported on Windows 11. The user has the option to delete the passkeys that are local to the Windows host. This is performed by opening Chrome and entering chrome://settings/passkeys as the URL. Chrome will display the local passkeys. Select the menu next to the one you want to delete and select the delete option (the only option available). See image below:



Copying Passkeys to a New Device

New iOS Device (Apple iPhone or iPad)

Passkeys are stored in iCloud Keychain, so they're automatically available for use as soon as you enable iCloud Keychain on your new iOS device.

To turn on iCloud Keychain on your new iOS device:

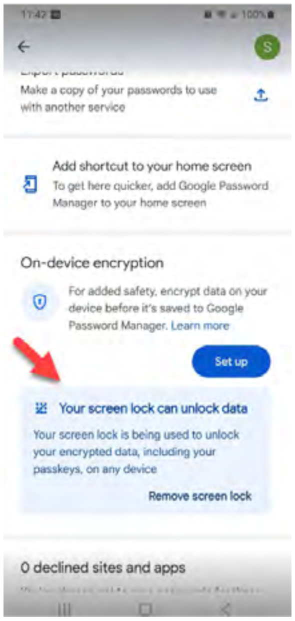
1. Tap Settings, tap [your name], then choose iCloud.
2. Tap Passwords and Keychain.
3. Turn on iCloud Keychain. You might be asked for your passcode or Apple ID password.

New Android Device

Passkeys will automatically be copied between Android devices provided that:

- The same Google email account is logged on for each Android device
- The Google email account in question has "Sync" enabled
- All of the Android devices need to have the Screen Lock explicitly enabled because this feature is used to encrypt the passkeys. Without all devices having the Screen Lock enabled, the "other devices" will not be able to leverage them. This is different from having your phone protected by PIN or Biometric. It needs to be explicitly set. See: https://support.google.com/android/answer/9079129?hl=en

- This is accomplished on Android by going to Password Manager and clicking the “gear” next to it.Note: This is different from “On-device encryption."



17:42 100%

S

Make a copy of your passwords to use with another service

Add shortcut to your home screen
To get here quicker, add Google Password Manager to your home screen

On-device encryption

For added safety, encrypt data on your device before it's saved to Google Password Manager. Learn more

Set up

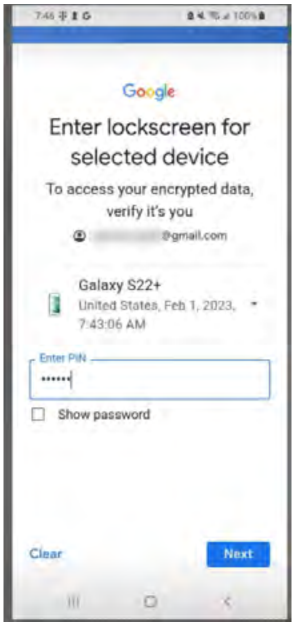
Your screen lock can unlock data

Your screen lock is being used to unlock your encrypted data, including your passkeys, on any device

Remove screen lock

0 declined sites and apps

- Upon first attempt to leverage a passkey from another device, you will be prompted for that device's Screen Lock.



7:46 100%

Google

Enter lockscreen for selected device

To access your encrypted data, verify it's you

[redacted]@gmail.com

Galaxy S22+
United States, Feb 1, 2023, 7:43:06 AM

Enter PIN
••••••

□ Show password

Clear

Next

New Mac Computer

Passkeys are stored in iCloud Keychain, so they’re automatically available for use as soon as you enable iCloud Keychain on your new Mac.

To turn on iCloud Keychain on your new Mac Computer:

1. Choose Apple menu > System Settings (or System Preferences)
2. Click your name, then click iCloud. In earlier versions of macOS, click Apple ID, then click iCloud in the sidebar
3. Turn on Password & Keychain

New Windows PC

You can use both synced passkeys and device-bound passkeys for Chrome/Edge on both Windows 10 or 11. Log into Chrome/Edge and have Sync set up.

For example, a passkey exists on your phone for https://awsq1.biometric.software. On a Chrome browser on the Windows workstation, you navigate to https://awsq1.biometric.software. You are logged into Chrome with the same account for which the passkey was generated. Upon login, select "Passkey" or "Use Platform Authenticator." The browser will present an option to scan a QR Code or send a notification to known devices associated with that Google account.

Both options allow you to leverage their mobile device's passkey to authenticate to the website.

Note: Even after this type of passkey authentication, the passkeys will not be shown in Chrome. You can only see/manage device-bound passkeys on Windows 11.

Passkeys FAQs

Can I use my passkey from my iOS device on my Android device?

At the time of this writing, cross platform or cross ecosystem is not supported.

Can I use my passkey from my Android device on my iOS device?

At the time of this writing, cross platform or cross ecosystem is not supported.

Can I use my passkey from my iOS device on my Windows Computer?

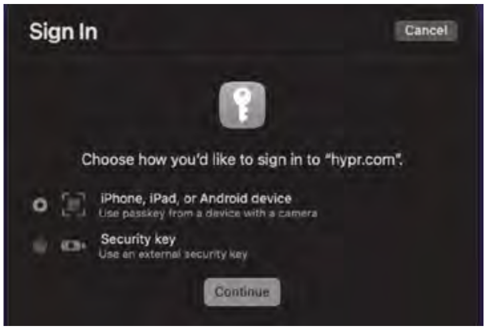
If you have installed iCloud for Windows and have keychain sync enabled, your passkeys will be available on the Windows device.

Can I use my passkey from my Android device on my Windows Computer?

Android and Chrome leverage the Google password manager. Your passkeys will be made available to you through the use of the Chrome web browser.

Can I use the passkey on my phone to get into a website on my computer?

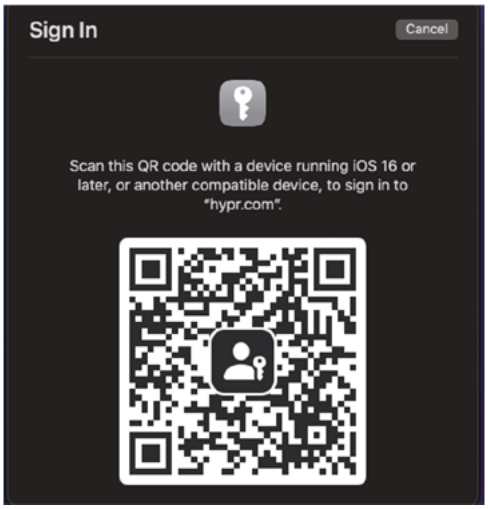
Yes. as long as the Service Provider “Relying Party” enables the support for it. You will see a dialog presented like the following:



Choose how you'd like to sign in to “hypr.com”.

● iPhone, iPad, or Android device
Use passkey from a device with a camera

○ Security key
Use an external security key



Scan this QR code with a device running iOS 16 or later, or another compatible device, to sign in to “hypr.com”.

Can I use the passkey on my computer to get into an app or website on my phone?

When leveraging passkeys which have been synced. The passkey will be available on any devices leveraging either iCloud Keychain or the Google Password Manager.

Can I use passkeys on a shared computer, for example at a library?

Passkeys are synced by the underlying platform such as Mac/Win/Android. To do so:

- You must be logged into your Apple/Google/MS account
- iCloud keychain or Google password manager must be enabled
- In instances where you are not logged into your personal account, such as a public computer, passkeys won’t work. Personal account logins on public computers are not recommended. You can, however, use the passkey on your phone to log into the shared computer.

Can I share my passkey with my spouse, kids, friends, etc.?

With Apple generated passkeys it is possible to airdrop your passkey to any mutual contacts. This is useful for backup only with someone you trust. Anything less can pose a significant security risk. As long as both individuals have each other within the contacts app in iOS and are within AirDrop range of each other, it is possible to share your passkey.

Can I use a passkey on my Apple Watch?

Passkeys require either Face ID or Touch ID. Apple Watch is not supported.

HYPR

THE IDENTITY ASSURANCE COMPANY

LEARN MORE: WWW.HYPR.COM

HYPR creates trust in the identity lifecycle. HYPR Identity Assurance provides the strongest end-to-end identity security for your workforce and customers, combining phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience.