

[← Main Menu](#)

Authenticate


ADD LOGIN


[Login](#) >[Single Sign-On](#) >[Passwordless](#) >

PROVISION USERS

[Identity Providers](#) >[Database Connections](#) ✓[Auth0 User Store](#)[Your User Store](#) >[Passkeys](#) ✓[Configure Passkey Policy](#)[Monitor Passkey Events in Tenant Logs](#)[Password Options in Auth0 Database Connections](#)[Password Strength in Auth0 Database Connections](#)[Change Users' Passwords](#)[Adding Username for Database Connections](#)[Login Script for IBM DB2](#)[Activate and Configure Attributes for Flexible Identif...](#)[Flexible Identifiers and Attributes](#)[Docs](#) > [Authenticate](#) > [Database Connections](#) > [Passkeys](#)

Passkeys

Passkeys are a phishing-resistant alternative to traditional authentication factors (such as username/password) that offer an easier and more secure login experience to users. Passkeys are modeled from FIDO® W3C Web Authentication (WebAuthn) and Client to Authenticator Protocol (CTAP) [specifications](#) .

Passkeys reduce the friction experienced with single-device authentication methods by allowing credentials to sync across devices. Cross-device authentication eliminates the need for users to re-enroll on each of their devices. It also supports a more reliable recovery method as the stored credentials can survive the loss of an originating device. To learn more about passkeys, review the FIDO® Alliance [Passkey FAQs](#) .

Auth0 supports passkeys as an authentication method for [database connections](#).

User experience flows

Similar to traditional authentication factors, passkeys can support several user experience flows such as signup, login, and account recovery.



Auth0 Universal Login currently supports the signup and login user experience flows for passkeys.

Signup flow

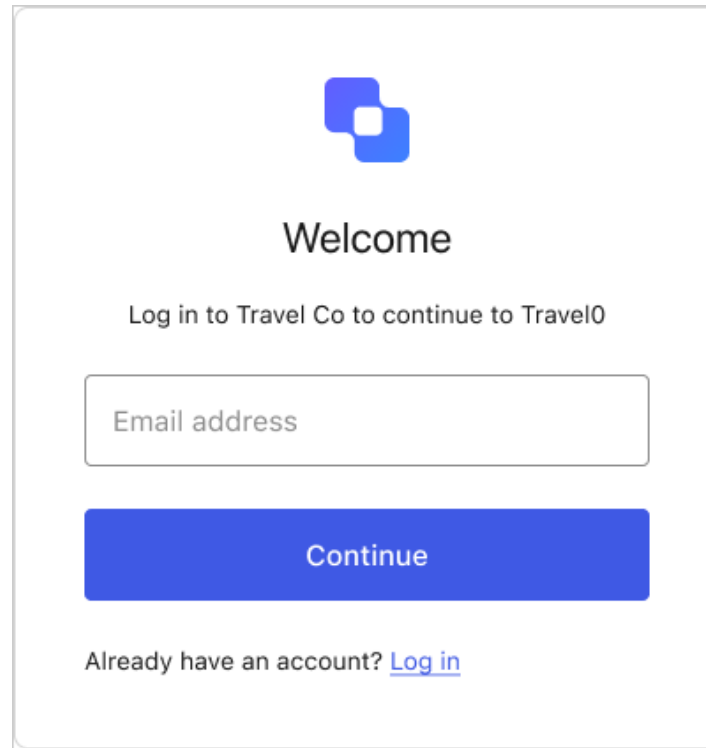
Is this article helpful?

✓ Yes

✗ No


The signup flow requires the user to provide an email address, and then create a passkey on either their current device or another device through cross-device authentication.

1. Prompts the user to enter their email address.



The image shows a login screen for 'Travel Co'. At the top is a blue logo consisting of two overlapping squares. Below the logo is the word 'Welcome' in a large, bold, black font. Underneath 'Welcome' is the text 'Log in to Travel Co to continue to Travel0' in a smaller, regular black font. Below this text is a white input field with a thin gray border and the placeholder text 'Email address' in a light gray font. Below the input field is a solid blue button with the word 'Continue' in white text. At the bottom of the screen is the text 'Already have an account?' followed by a blue, underlined link that says 'Log in'.

2. User enters their email address.



Welcome

Log in to Travel Co to continue to Travel0

Email Address

[Continue](#)

Already have an account? [Log in](#)

3. Prompts the user to create a passkey.



Create a passkey for Travel0 on this device?



No need to remember a password

With passkeys, you can use your fingerprint or face to login.



Works on all your devices

Passkeys will automatically be available across your synced devices.



Works alongside passwords

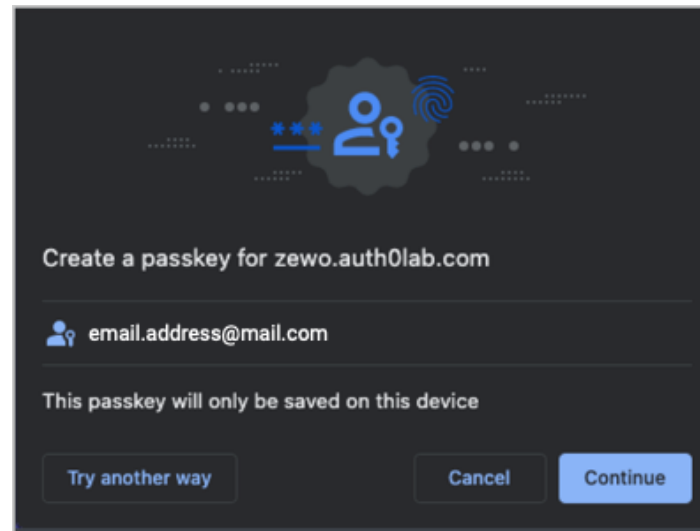
Passkeys offer state of the art phishing resistance.

Create a new passkey

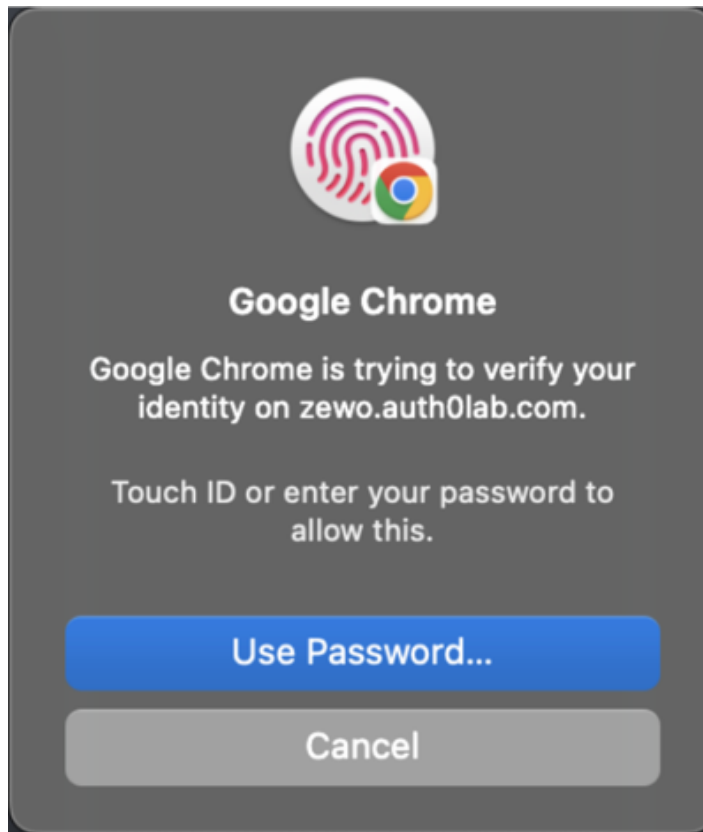
[Continue without a passkey](#)

[Go back](#)

4. If the user selects **Create a passkey**, it triggers the browser (or operating system) flow to create a passkey.



- If the user selects **Continue**, it prompts them to authenticate with their device's credentials.




- If the user selects **Try another way**, it prompts them to create a passkey on another device.



Login flow

The login flow detects if the user has a passkey registered to the current device and then automatically selects it using autofill. If the user has multiple passkeys registered to the device, they can manually select one with a button.

1. Prompts the user for an email address or a passkey.



Welcome


Log in to Travel Co to continue to Travel0

[Forgot password?](#)

Continue

Don't have an account? [Sign up](#)

OR

 Continue with a passkey

2. User can use autofill or select **Continue with a passkey**.



Welcome

Log in to Travel Co to continue to Travel0

Email Address

email.address@mail.com

[Forgot password?](#)

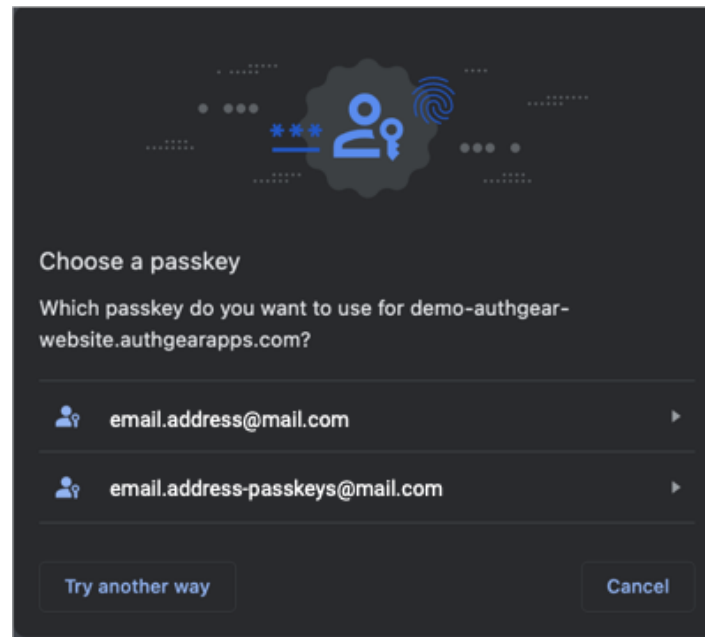
Continue

Don't have an account? [Sign up](#)

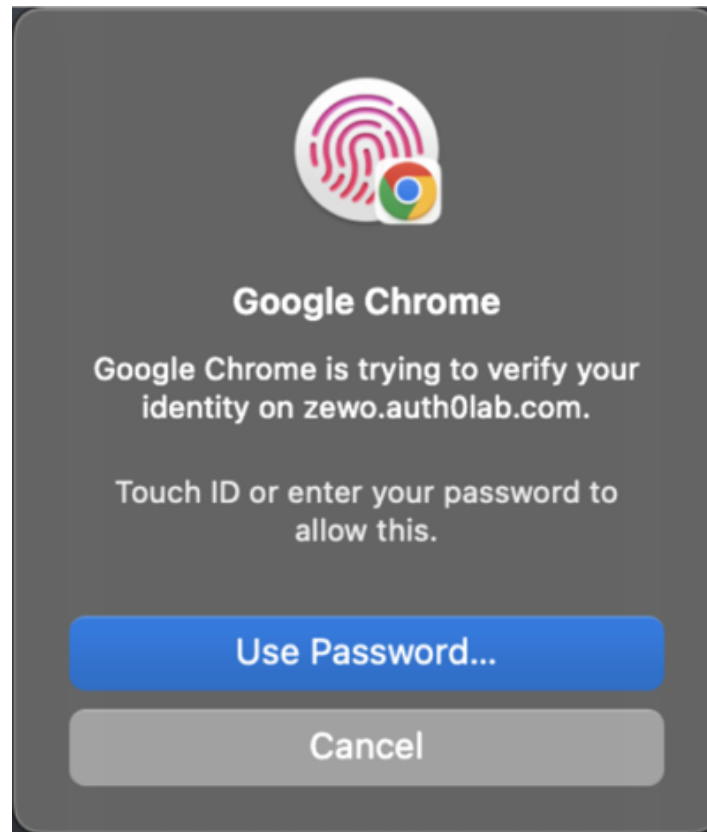
OR



Continue with a passkey



3. Prompts the user to authenticate with the device's credentials.



Passkeys with MFA enabled

If MFA is enabled, the user may be prompted to complete an MFA challenge after authenticating with a passkey based on settings and risk assessment.

The default behavior is to require the completion of an MFA challenge regardless if the authentication method used was a password or a passkey. Given the high level of security passkeys provide, you may skip MFA for users that have authenticated with a passkey in order to reduce friction. This can be achieved by using a post-login Action.

To learn more, read [Reduce friction with passkeys](#) and [Multi-Factor Authentication](#).



FIDO® is a trademark (registered in numerous countries) of [FIDO Alliance, Inc](#).

Was this article helpful?

✓ Yes

✗ No

DEVELOPERS

Developer Hub

Code Samples and Guides

Blog posts

Videos

Identity Unlocked - Podcasts

Zero Index Newsletter

DOCUMENTATION

Articles

Quickstarts

APIs

SDK Libraries

Blog

Reports

Webinars

GET INVOLVED

Forum

Events

Ambassador Program

Auth0 Research Program

COMPANY

Our Customers

Compliance - Ensuring privacy and security

Partners

Careers [We're hiring!](#)

Okta + Auth0

SUPPORT CENTER

Community

Support

Help

FAQs

Auth0 Marketplace

LEARNING

Learn

Intro to IAM (CIAM)

Blog

PLATFORM

Access Management

Extensibility

Security

User Management

Authentication

FEATURES

Universal Login

Single Sign On

Multifactor Authentication

Actions

Machine to Machine

Passwordless

Breached Passwords

