# Account Recovery

This page details the strategies you can implement so that people can regain access to their passkey secured account if they lock themselves out.

This feature requires the latest V1 of the SDK to be installed

Why recovery is needed

Dynamic Embedded Wallets are protected by passkeys which are stored on a user's device through a password manager like iCloud, 1Password or Google Password Manager. One of two scenarios can result in a user losing access:

1. The user deletes the passkey manually.
2. The user loses access to their password manager (iCloud/Google Password manager)

For the second case, before continuing with the recovery flow in Dynamic, we recommend going through steps to recover access to the storage mechanism i.e. the Password manager:

For Apple and iCloud Go to iforgot.apple.com. Follow prompts to restore access to icloud. If a customer lost their device, they will need to complete additional steps to have their passkeys ported over to the new device. They must contact Apple Support for further verifications. For Google and Android Devices Passkeys created on Android are backed up and synced with google password manager. That means user's passkeys go with them when they replace their devices. Customers should follow google's password recovery flow to regain access to their account and assign ownership to their new device. Recovering a passkey from 1Password. Passkeys are gated in 1password through a combination of unique credentials and encryption. Passkeys are treated similar to existing passwords so that If a user forgets their 1password password, they can recover it using existing processes:https://support.1password.com/forgot-account-password

How to enable recovery

If your customer has deleted their passkey or is unable to see a passkey when signing, they can use recovery to generate a new one.

In Dashboard underembedded wallets , toggle Recovery On for all customers. That's it!

What it looks like for a user

Inside the Dynamic modal, your end user should see three dots to the right of their wallet address at the top

Upon clicking/tapping these three dots, the user should then see an option called "Wallet settings and should be able to click/tap on it.

On the wallet settings page the user should see an option called "Passkeys" and should be able to click/tap on it.

A new screen will open where the user will see both their existing passkeys and the option to initiate a request for a new passkey.

The user can then start the process to generate a new passkey for their device. They will be asked to enter their email address and a verification code will be sent to them.

Once they click this button and initiate a request, an email will be sent to the email address on file for them to copy and paste on the next page.

- The email will come from the domain turnkey.io
- It will contain containing a base58 encoded string
- The code will expire within 15 minutes
- The code is only valid on the browser and device they started the request on

When the code is validated they will be prompted to create a new passkey, which will be added to their passkey list, and they can then use this new passkey to gain access to their wallet.

Triggering recovery manually

If you want to open the recovery flow at any other point, you can. You can do this by calling theinitPasskeyRecoveryProcess method, which comes as part of the usePasskeyRecovery hook. It will open exactly the same flow as described above.

import { usePasskeyRecovery} from "@dynamic-labs/sdk-react-core" ; const { initPasskeyRecoveryProcess} = usePasskeyRecovery ( ) ; < button onClick = { ( ) => initPasskeyRecoveryProcess ( ) }

</ button

;

Risks & Considerations

If a customer’s email address is compromised, a malicious actor could initiate a request to generate a new passkey. It is your responsibility to decide whether you should have this feature enabled by default or only if a customer notifies you that they are locked out.

If you believe a customers email has been compromised, we can temporarily lock access to a specific Dynamic account and prevent access until your end-user regained access to their email address.

Was this page helpful?

Yes No Biconomy Smart Accounts Wallet Export twitter linkedin slack Powered by Mintlify