

Set default authentication method

Login Preferences

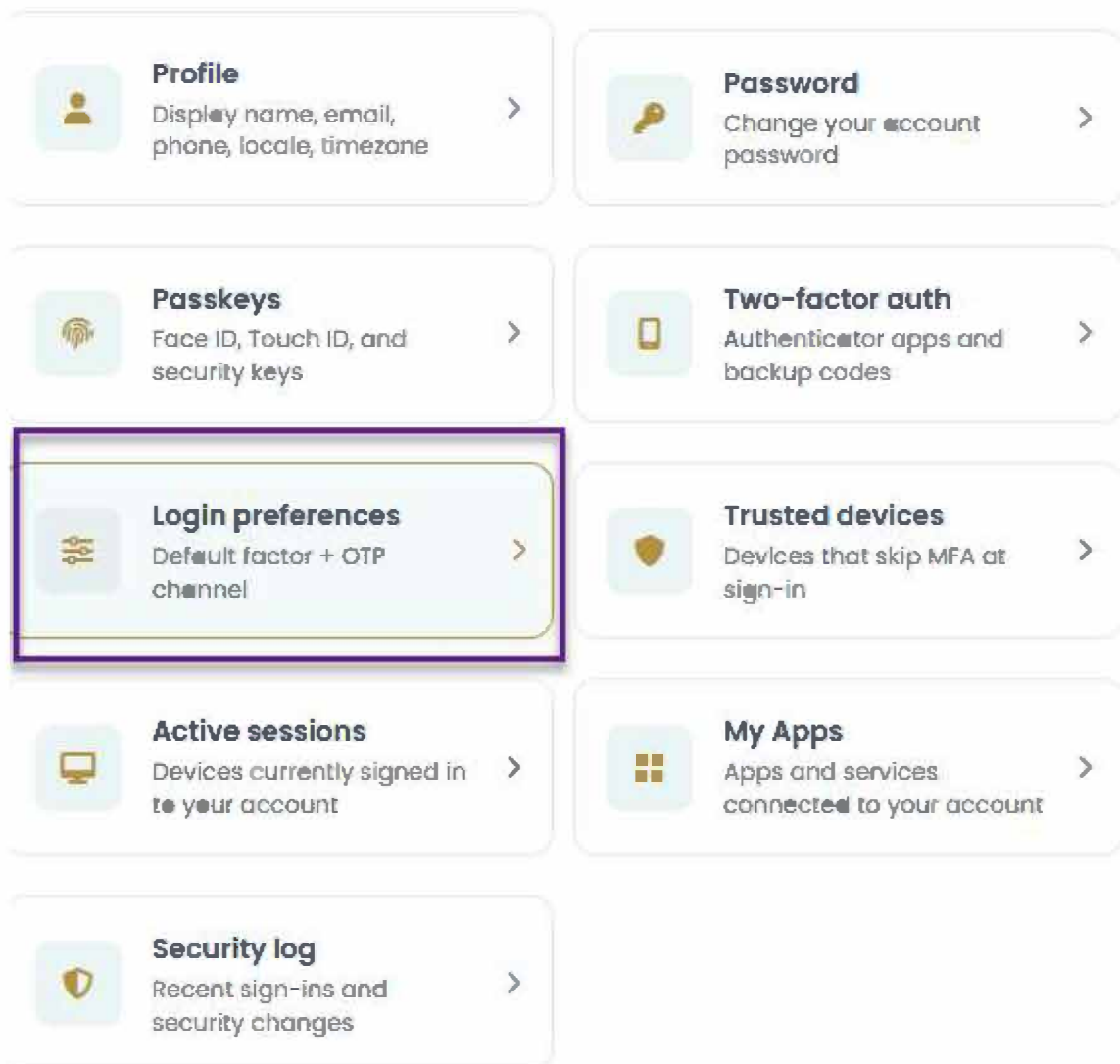
The Login Preferences section in your Account settings allows you to manage how you authenticate when signing in to your account.

After you login

1. Hover over your name in the top-right corner of the page.
2. Select Manage Account.

Your Account

Manage your profile, sign-in methods, active sessions, and security activity.



From this section, you can:

- choose your preferred default secondary authentication method
- and enable or disable passwordless sign-in.

These settings help you customize the security and convenience of your login.

Selecting a Default Secondary Authentication Method

If you have multiple two-factor authentication methods configured, you can choose which method should be used by default during sign-in. The available options depend on which authentication methods you have already set up on your account.

For example, if you have configured:

- a passkey,
- and an authenticator app,

you will be able to choose between:

- passkey authentication,
- authenticator app verification,
- or Email/SMS one-time passcode (OTP).

Login preferences

How you want to sign in. These apply the next time you authenticate.

Preferred second factor

When two-factor is required at sign-in, this is the method we prompt you for first. You can always pick a different method at the prompt.



Passkey

Use Face ID, Touch ID, Windows Hello, or a hardware security key.



Authenticator app

Use an app like 1Password, Authy, or Google Authenticator.



Email or SMS code

We send a one-time code. Less secure than passkeys or authenticator apps — use only if you can't use the others.

Passwordless sign-in

Skip the password step entirely. Sign in with your passkey, or get a one-time code by email or text.



Default Fallback Authentication Method

If passkey or authenticator app authentication has not been configured, the default secondary authentication method will fall back to "Email or SMS one-time passcode (OTP)".

This ensures that you can still securely verify your identity during login even if more advanced authentication methods are not yet set up.

Preferred second factor

When two-factor is required at sign-in, this is the method we prompt you for first. You can always pick a different method at the prompt.



Passkey

Use Face ID, Touch ID, Windows Hello or a hardware security key if a passkey is enrolled.



Authenticator app

Use an app like 1Password Auth or Google Authenticator. No authenticator enrolled.



Email or SMS code

We send a one-time code. Less secure than passkeys or authenticator apps. Use only if you can't use the others.

Changing Your Preferred Authentication Method

You can update your preferred secondary authentication method at any time from the Login Preferences settings. Changing your preference only affects the default method presented during sign-in. Other configured authentication methods will still be available as alternative options when logging in.

Passwordless Sign-In

The Login Preferences section also includes the option to enable or disable passwordless sign-in. When passwordless sign-in is enabled, you may be able to sign in without entering your password by using:

- a passkey,
- or a one-time verification code sent to your email address or mobile phone.

This can provide:

- faster login,
- improved convenience,
- and reduced reliance on traditional passwords.