MY ACCOUNT > LOG IN & UNLOCK

Unlock with PIN

Weergeven in het Helpcentrum:
https://bitwarden.com/help/unlock-with-pin/

Unlock with PIN

You can set a PIN code as a method for unlocking your vault. PINs can only be used to unlock your vault, you will still be required to use your master password or login with device, and any enabled two-step login method when you log in.

Unlock with PIN is not a passwordless method of accessing your Bitwarden account, if you are not sure of the difference, see Understanding unlock vs. log in.

> ⓘ **Note**
>
> After **five** failed PIN attempts, the app will automatically log out of your account.

Enable unlock with PIN

Unlock with PIN can be enabled for the Bitwarden browser extension, mobile app, and desktop app:

> ⚠ **Warning**
>
> Using a PIN can weaken the level of encryption that protects your application's local vault database. If you are worried about attack vectors that involve your device's local data being compromised, you may want to reconsider the convenience of using a PIN.

⇒Browser extension

To enable unlock with PIN for your browser extension:

1. Open the ⚙ **Settings** tab.

2. Select **Account security** and check the **Unlock with PIN** checkbox.

3. Enter the desired PIN code in the input box. Your PIN can be any combination of characters (a-z, 0-9, $, #, etc.).

   > **Tip**
   >
   > If you share your device, it's important to create a strong PIN by avoiding easily guessable digits like date of birth or by using a PIN that's more than four digits.

4. The pre-checked option **Lock with master password on browser restart** will require you to enter your master password instead of the PIN when your browser restarts. If you want the ability to unlock with a PIN even when the browser restarts, uncheck the option.

   > ⓘ **Note**
   >
   > If you turn off the **Lock with master password on restart** option, the Bitwarden application may not fully purge sensitive data from application memory when entering a locked state. If you are concerned about your device's local memory being compromised, you should keep the **Lock with master password on restart** option turned on.

Once set, you can change your PIN by disabling and re-enabling unlock with PIN.

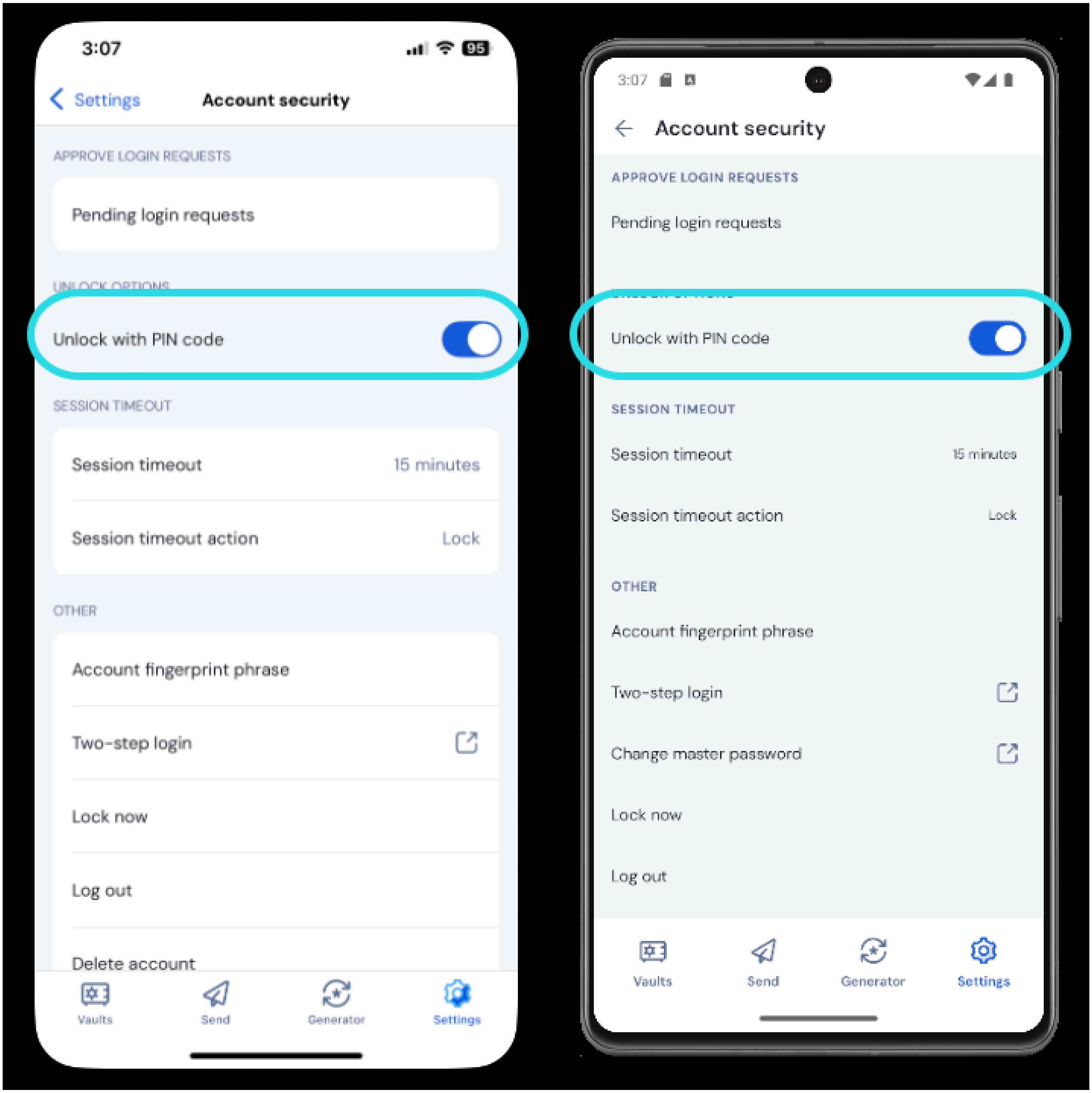
When you **log out** of your browser extension, your unlock with PIN settings will be wiped and you will need to re-enable unlock with PIN.

⇒Mobile

To enable unlock with PIN for your mobile app:

1. Open the ⚙ **Settings** tab.

2. Scroll down to the security section and tap the **Unlock with PIN Code** option:



3:07

‹ Settings — Account security

APPROVE LOGIN REQUESTS

Pending login requests

UNLOCK OPTIONS

Unlock with PIN code — on

SESSION TIMEOUT

Session timeout — 15 minutes

Session timeout action — Lock

OTHER

Account fingerprint phrase

Two-step login

Lock now

Log out

Delete account

3:07

← Account security

APPROVE LOGIN REQUESTS

Pending login requests

UNLOCK OPTIONS

Unlock with PIN code — on

SESSION TIMEOUT

Session timeout — 15 minutes

Session timeout action — Lock

OTHER

Account fingerprint phrase

Two-step login

Change master password

Lock now

Log out

Unlock with PIN on mobile

3. Enter the the desired PIN code in the input box. Your PIN can be any combination of numbers (0-9).

> **Tip**
>
> If you share your device, it's important to create a strong PIN by avoiding easily guessable digits like date of birth or by using a PIN that's more than four digits.

4. A dialog box will appear asking whether you want to require unlocking with your master password when the application is restarted. Tap **Yes** to require your master password instead of PIN when the app restarts. Tap **No** for the ability to unlock with the PIN when the app restarts.

Once set, you can change your PIN by disabling and re-enabling Unlock with PIN.

When you **log out** of your mobile app, your unlock with PIN settings will be wiped and you will need to re-enable Unlock with PIN.

⇒Desktop

Unlock with PIN is set separately for each account logged in to the desktop app. To enable unlock with PIN:

1. Open your **Settings** (on Windows, **File** → **Settings**) (on macOS, **Bitwarden** → **Settings**).

2. In the Security section, check the **Unlock with PIN** checkbox.

3. Enter the desired PIN code in the input box. Your PIN can be any combination of characters (a-z, 0-9, $, #, etc.).

> **Tip**
>
> If you share your device, it's important to create a strong PIN by avoiding easily guessable digits like date of birth or by using a PIN that's more than four digits.

4. The pre-checked option **Lock with master password on restart** will require you to enter your master password instead of the PIN when the app restarts. If you want the ability to unlock with a PIN when the app restarts, uncheck this option.

> **Note**
>
> If you turn off the **Lock with master password on restart** option, the Bitwarden application may not fully purge sensitive data from application memory when entering a locked state. If you are concerned about your device's local memory being compromised, you should keep the **Lock with master password on restart** option turned on.

Once set, you can change your PIN by disabling and re-enabling unlock with PIN.

When you **log out** of your desktop app, your unlock with PIN settings will be wiped and you will need to re-enable unlock with PIN.

Understanding unlock vs. log in

In order to understand why unlocking and logging in are not the same, it's important to remember that Bitwarden never stores unencrypted data on its servers. **When your vault is neither unlocked nor logged in**, your vault data only exists on the server in its encrypted form.

Logging in

Logging in to Bitwarden retrieves the encrypted vault data and decrypts the vault data locally on your device. In practice, that means two things:

1. Logging in will always require you to use your master password or login with device to gain access to the account encryption key that will be needed to decrypt vault data.

   This stage is also where any enabled two-step login methods will be required.

2. Logging in will always require you to be connected to the internet (or, if you are self-hosting, connected to the server) to download the encrypted vault to disk, which will subsequently be decrypted in your device's memory.

Unlocking

Unlocking can only be done when you are already logged in. This means, according to the above section, your device has **encrypted** vault data stored on disk. In practice, this means two things:

1. You don't specifically need your master password. While your master password *can* be used to unlock your vault, so can other methods like PIN codes and biometrics.

   > ⓘ **Note**
   >
   > When you setup a PIN or biometrics, a new encryption key derived from the PIN or biometric factor is used to encrypt the account encryption key, which you will have access to by virtue of being logged in, and stored on disk[a].
   >
   > **Unlocking** your vault causes the PIN or biometric key to decrypt the account encryption key in memory. The decrypted account encryption key is then used to decrypt all vault data in memory.
   >
   > **Locking** your vault causes all decrypted vault data, including the decrypted account encryption key, to be deleted.
   >
   > [a] - If you use the **Lock with master password on restart** option, this key is only stored in memory rather than on disk.

2. You don't need to be connected to the internet (or, if you are self-hosting, connected to the server).