Lås upp med PIN

Lås upp med PIN

Du kan ställa in en PIN-kod som en metod för att låsa upp ditt valv. PIN-koder kan endast användas för att låsa upp ditt valv, du kommer fortfarande att behöva använda ditt huvudlösenord eller logga in med enheten, och alla aktiverade tvåstegsinloggningsmetoder när du loggar in.

Lås upp med PIN är inte en lösenordslös metod för att komma åt ditt Bitwarden-konto, om du inte är säker på skillnaden, se Förstå upplåsning vs. logga in.

Efter **fem** misslyckade PIN-försök loggar appen automatiskt ut från ditt konto.

> **Note**
>
> If you are a member of an Enterprise organization, a policy may prohibit you from setting up unlock with PIN.

Aktivera upplåsning med PIN

Lås upp med PIN kan aktiveras för Bitwarden webbläsartillägg, mobilapp och stationär app. PIN-koder ställs in per Bitwarden-app, inte per konto:

> **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.
   >
   > Browser extensions now require at least 4 characters, and this will be implemented in other clients in a future release. If you were using a PIN of less than 4 characters before this change was introduced, you will not be forced to change your PIN however using a stronger PIN is recommended.

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.

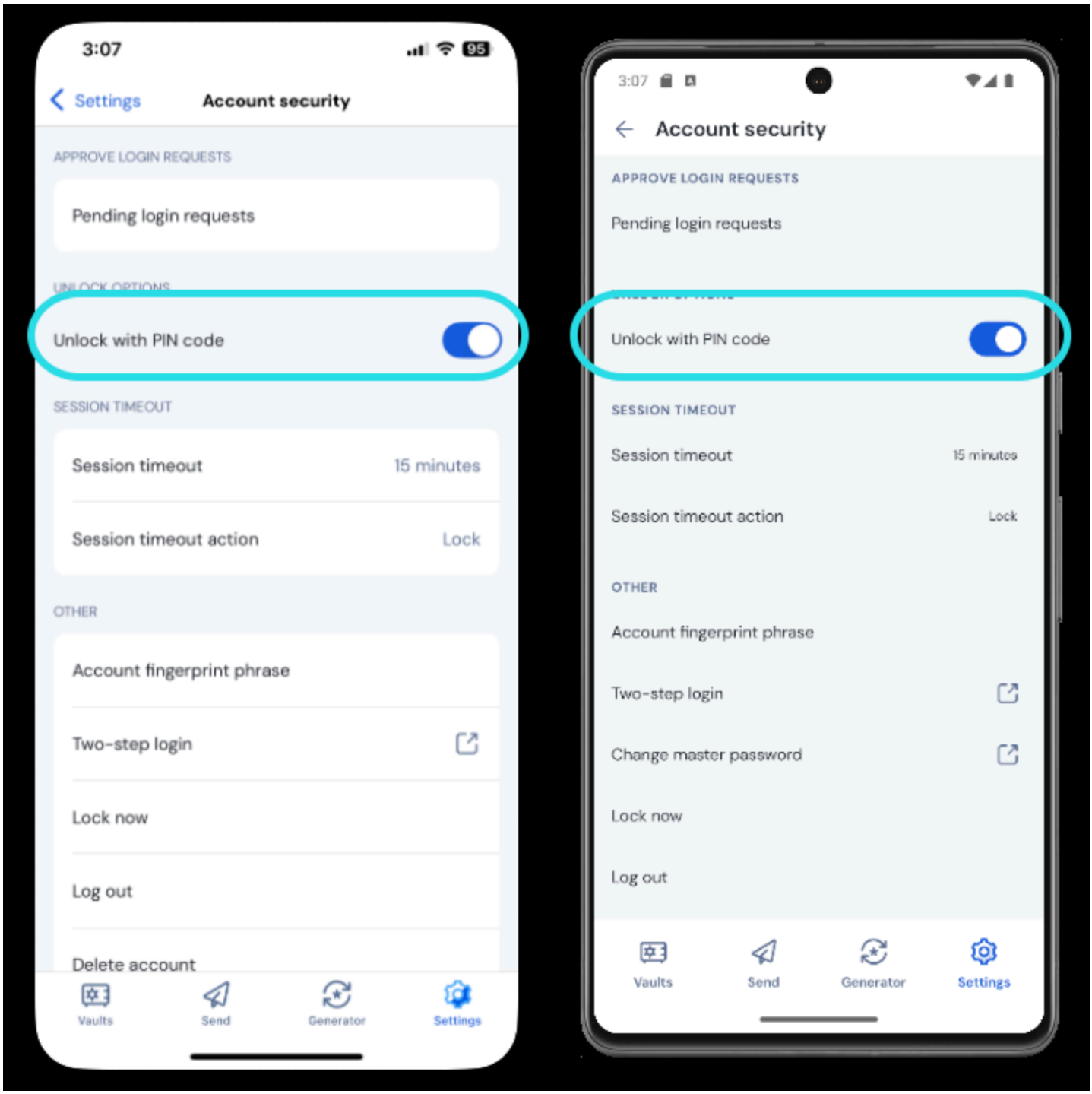
Once set, you can change your PIN by disabling and re-enabling unlock with PIN.

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:



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.
>
> Browser extensions now require at least 4 characters, and this will be implemented in other clients in a future release. If you were using a PIN of less than 4 characters before this change was introduced, you will not be forced to change your PIN however using a stronger PIN is recommended.

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.
>
> Browser extensions now require at least 4 characters, and this will be implemented in other clients in a future release. If you were using a PIN of less than 4 characters before this change was introduced, you will not be forced to change your PIN however using a stronger PIN is recommended.

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.

Förstå upplåsning vs. logga in

För att förstå varför upplåsning och inloggning inte är samma sak är det viktigt att komma ihåg att Bitwarden aldrig lagrar okrypterad data på sina servrar. **När ditt valv varken är upplåst eller inloggat**, finns dina valvdata bara på servern i sin krypterade form.

Loggar in

Att logga in på Bitwarden hämtar krypterad valvdata och dekrypterar valvdata lokalt på din enhet. I praktiken betyder det två saker:

1. Om du loggar in måste du alltid använda ditt huvudlösenord eller logga in med enheten för att få tillgång till kontokrypteringsnyckeln som kommer att behövas för att dekryptera valvdata.

   Detta steg är också där alla aktiverade tvåstegsinloggningsmetoder kommer att krävas.

2. Inloggning kräver alltid att du är ansluten till internet (eller, om du är självvärd, ansluten till servern) för att ladda ner det krypterade valvet till disken, som sedan kommer att dekrypteras i din enhets minne.

Låser upp

Upplåsning kan endast göras när du redan är inloggad. Detta betyder, enligt avsnittet ovan, har din enhet **krypterad** valvdata lagrad på disken. I praktiken betyder det två saker:

1. Du behöver inte specifikt ditt huvudlösenord. Medan ditt huvudlösenord kan användas för att låsa upp ditt valv, så kan andra metoder som PIN-koder och biometri.

   > **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. Du behöver inte vara ansluten till internet (eller, om du är självvärd, ansluten till servern).