bitwarden | Help Center Article

MITT KONTO > LOGGA IN OCH LÅS UPP >

Lås upp med Biometrics

View in the help center:
https://bitwarden.com/help/biometrics/

Lås upp med Biometrics

Bitwarden kan konfigureras för att acceptera biometri som en metod för att låsa upp ditt valv.

Biometri 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 Biometrics är inte en funktion utformad för att vara en lösenordslös inloggning, om du inte är säker på skillnaden, se Förstå upplåsning vs. logga in.

> **Tip**
>
> Biometriska funktioner är en del av den inbyggda säkerheten i din enhet och/eller operativsystem. Bitwarden utnyttjar inbyggda API:er för att utföra denna validering, och därför får **Bitwarden ingen biometrisk information** från enheten.

Aktivera upplåsning med biometri

Lås upp med biometri kan aktiveras för Bitwarden på mobil-, dator- och webbläsartillägg:

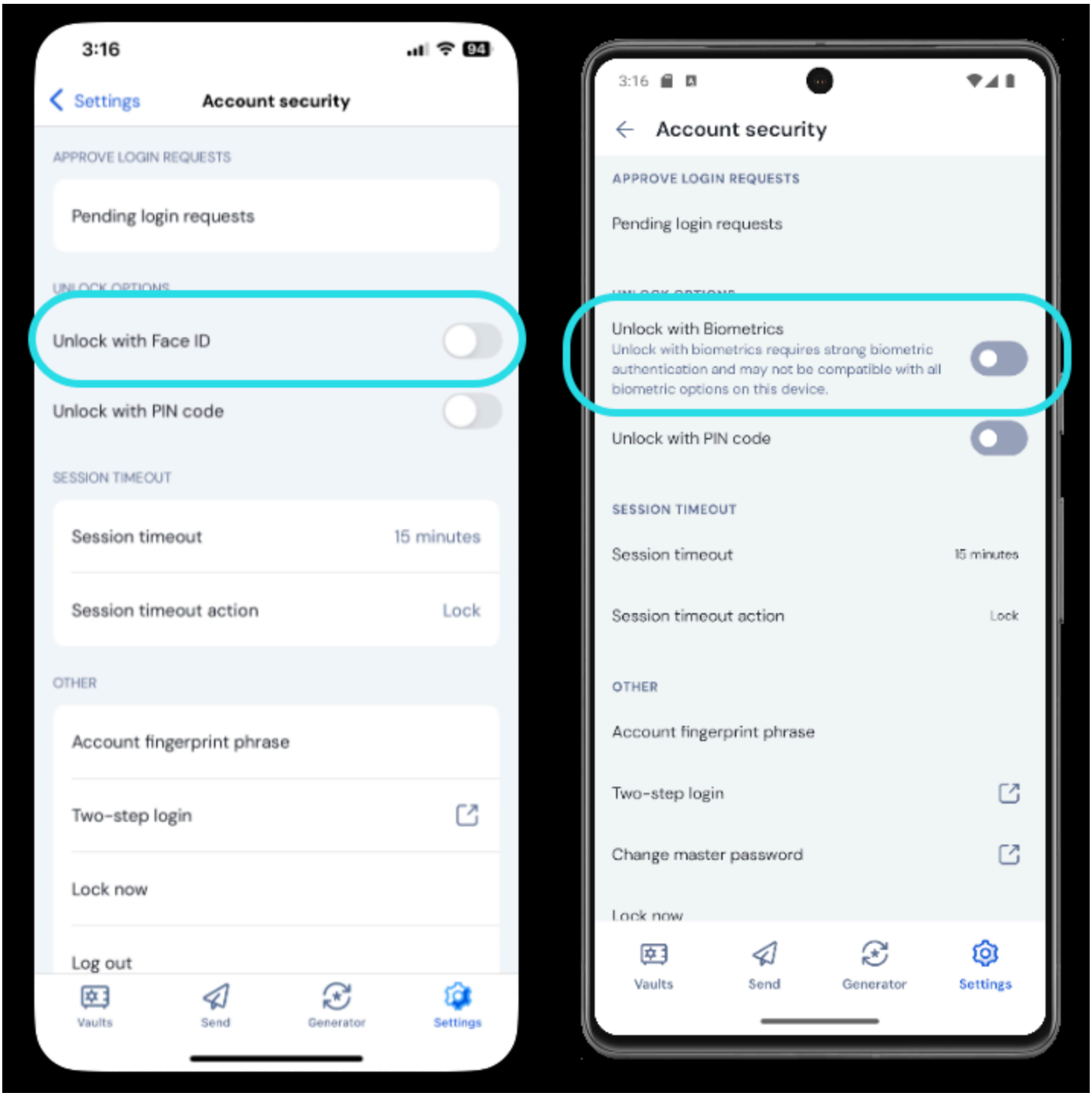
⇒Mobil

Aktivera för mobil

Upplåsning med biometri stöds för Android (Google Play eller FDroid) via fingeravtrycksupplåsning eller ansiktsupplåsning, och för iOS via Touch ID och Face ID.

Så här aktiverar du upplåsning med biometri för din mobila enhet:

1. Se till att din biometriska metod är aktiverad i enhetens ursprungliga inställningar (t.ex. iOS **Settings**-appen).
2. Öppna fliken **Inställningar** i din Bitwarden-app.
3. Öppna avsnittet Kontosäkerhet och tryck på det biometriska alternativet du vill aktivera. Vad som är tillgängligt på den här skärmen bestäms av din enhets hårdvarukapacitet och vad du har aktiverat (**steg ett**), till exempel:



Biometrisk upplåsning på mobil

Om du trycker på alternativet kommer du att uppmanas att ange din biometriska (till exempel ansikte eller tumavtryck). Växeln kommer att fyllas i när upplåsning med biometri har aktiverats.

Inaktiverad i väntan på verifiering av huvudlösenord

Om du får ett meddelande som rapporterar att biometrisk upplåsning är inaktiverad för autofyll i väntan på verifiering av ditt huvudlösenord:

1. Stäng tillfälligt av autofyll i Bitwarden.
2. Återaktivera biometri i Bitwarden.
3. Aktivera autofyll igen i Bitwarden.

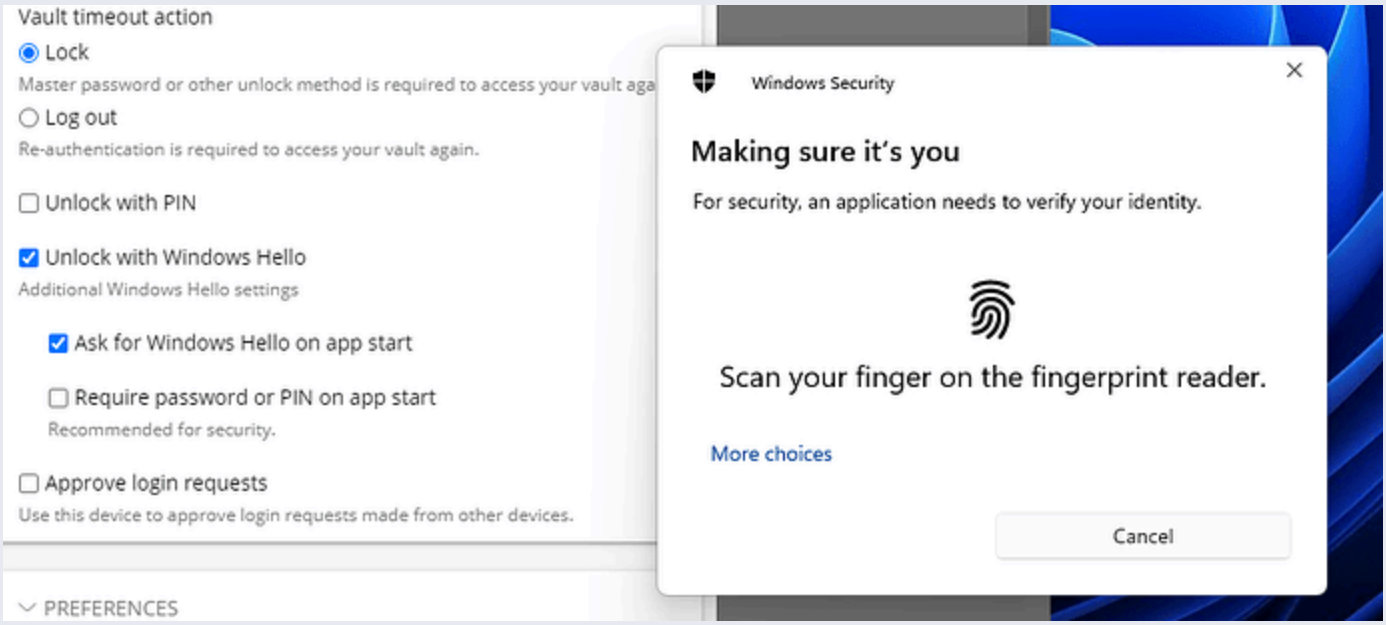
⇒Skrivbord

Aktivera för skrivbordet

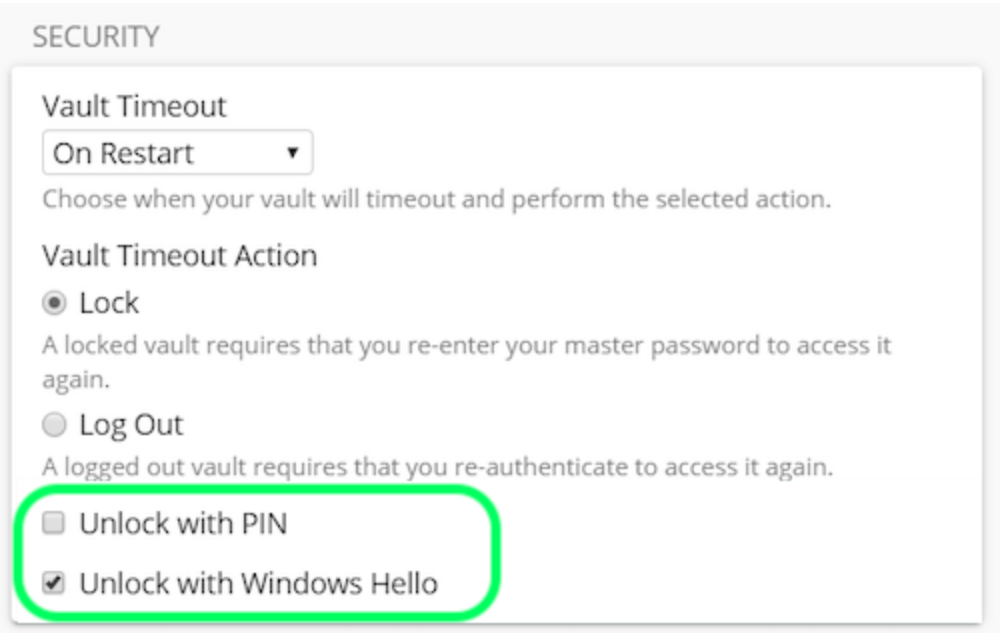
Lås upp med biometri stöds för Windows via Windows Hello med PIN, ansiktsigenkänning eller annan hårdvara som uppfyller Windows Hello biometriska krav och för macOS via Touch ID och för Linux med systemautentisering.

Lås upp med biometri ställs in separat för varje konto som är inloggat på skrivbordsappen. Så här aktiverar du upplåsning med biometri:

1. Se till att din biometriska metod är aktiverad i enhetens ursprungliga inställningar (till exempel appen macOS⚙ **System Preferences**).

> **Tip**
>
> Windows-användare kan behöva installera Microsoft Visual C++ Redistributable innan Windows Hello kan slås på i skrivbordsinställningarna. Observera att första gången du aktiverar Windows Hello på din maskin kan en obligatorisk "Se till att det är du"-prompt visas i bakgrunden eller timeout om den inte bekräftas:
>
> 
>
>
> Windows Hello-prompt

2. Öppna dina inställningar i din Bitwarden-app (på Windows eller Linux, **Arkiv → Inställningar**) (på macOS, **Bitwarden → Inställningar**).
3. I säkerhetsavsnittet väljer du det biometriska alternativ du vill aktivera. Vad som är tillgängligt på den här skärmen bestäms av din enhets maskinvarukapacitet och vad du har aktiverat (**steg 1**). På Linux kommer detta alltid att vara **Lås upp med systemautentisering**. Exempel:

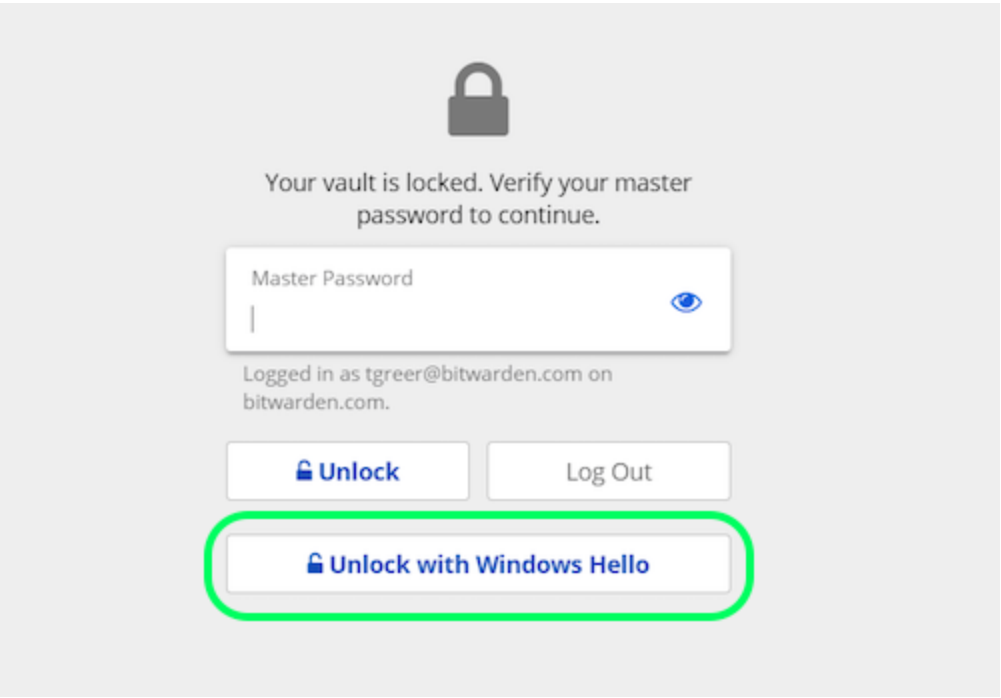


Lås upp med Windows Hello

4. Om du vill kan du välja antingenalternativet **Kräv lösenord (eller PIN-kod) vid appstart** eller **Be om biometrisk vid appstartför** att ställa in hur din stationära app ska bete sig när du startar appen.

> **Tip**
>
> Om du använder Windows rekommenderar Bitwarden att du använder **Kräv lösenord (eller PIN-kod) vid första inloggning efter start** för att maximera säkerheten.

Om du inte väljer något av alternativen kan du helt enkelt välja **Lås upp med** biometrisk-knappen på inloggningsskärmen för att fråga efter ditt biometriska alternativ:



Lås upp med Windows Hello

⇒Webbläsartillägg

Om Biometri i webbläsartillägg

Lås upp med biometri stöds för tillägg genom en integration med Bitwardens skrivbordsapp. Rent praktiskt betyder detta:

1. **För alla webbläsartillägg** måste du aktivera upplåsning med biometri på skrivbordet innan du fortsätter. **För alla utom Safari** måste Bitwarden-skrivbordsappen vara inloggad och köra för att kunna använda upplåsning med biometri för ett webbläsartillägg.

2. Webbläsartillägg stöder samma biometriska alternativ som skrivbordet; för Windows via Windows Hello med PIN, ansiktsigenkänning eller annan hårdvara som uppfyller Windows Hello biometriska krav, för macOS via Touch ID och för Linux (endast Chromium-baserade webbläsare) med systemautentisering.

Två saker att tänka på innan du aktiverar integrationen är **behörigheter** och **stödbarhet**, som dokumenteras nedan:

Behörigheter

För att underlätta denna integrering kommer webbläsartillägg **förutom Safari** att be dig att acceptera ett nytt tillstånd för Bitwarden att `kommunicera med samarbetande inbyggda applikationer`. Denna behörighet är säker, men **valfri**, och kommer att möjliggöra den integration som krävs för att aktivera upplåsning med biometri.

Om du tackar nej till denna behörighet kan du använda webbläsartillägget som vanligt, utan upplåsning med biometrisk funktionalitet.

Stödbarhet

Lås upp med biometri stöds för tillägg på **Chromium-baserade** webbläsare (Chrome, Edge, Opera, Brave och mer), Firefox 87+ och Safari 14+. Lås upp med biometri stöds för **närvarande inte för**:

- Firefox ESR (Firefox v87+ kommer att fungera).

- Microsoft App Store-skrivbordsappar (en sidoladdad Windows-skrivbordsapp, tillgänglig på bitwarden.com/download fungerar bra).

- Sidoladdade MacOS-skrivbordsappar (en App Store-skrivbordsapp fungerar bra).

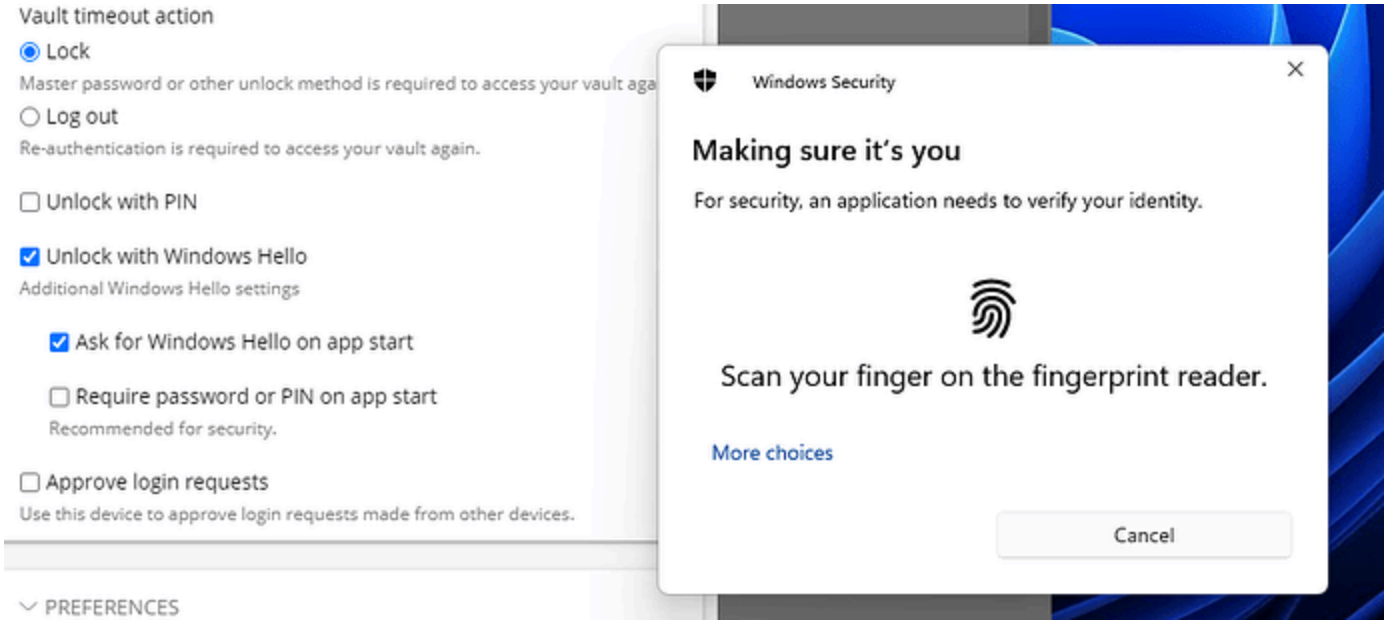
Aktivera för webbläsartillägg

Så här aktiverar du upplåsning med biometri för ditt webbläsartillägg:

Tip

Biometri (Windows Hello eller Touch Id) måste vara aktiverat i din skrivbordsapp innan du fortsätter. Om du inte ser alternativet Windows Hello i din skrivbordsapp kan du behöva installera Microsoft Visual C++ Redistributable. Dessutom, **om du använder Safari** kan du hoppa direkt till **steg 4**.

Observera att första gången du aktiverar Windows Hello på din maskin kan en obligatorisk "Se till att det är du"-prompt visas i bakgrunden eller timeout om den inte bekräftas:



Windows Hello-prompt

1. I din Bitwarden-skrivbordsapp navigerar du till inställningar (på Windows, **Arkiv → Inställningar**) (på macOS, **Bitwarden → Inställningar**).

2. Rulla ned till alternativsektionen och markera rutan **Tillåt webbläsarintegration**.

Note

På macOS kan du stöta på ett fel om din användarnamnskatalog (t.ex. /`Användare/ditt_användarnamn/Bibliotek`/...) är längre än 104 tecken. Om du stöter på detta. fel, förkorta ditt användarnamn (t.ex. `ditt_användarnamn`).

Note

Om du vill kan du markera alternativet **Kräv verifiering för webbläsarintegration** för att kräva ett unikt fingeravtrycksverifieringssteg när du aktiverar integrationen.

3. I din webbläsare navigerar du till tilläggshanteraren (t.ex. `chrome://extensions` eller `brave://extensions`), öppnar Bitwarden och växlar alternativet **Tillåt åtkomst till filwebbadresser**.

   Inte alla webbläsare kommer att kräva att detta aktiveras, så hoppa gärna över det här steget och ring tillbaka till det endast om den återstående proceduren inte fungerar.

4. Öppna fliken **Inställningar** i ditt webbläsartillägg.

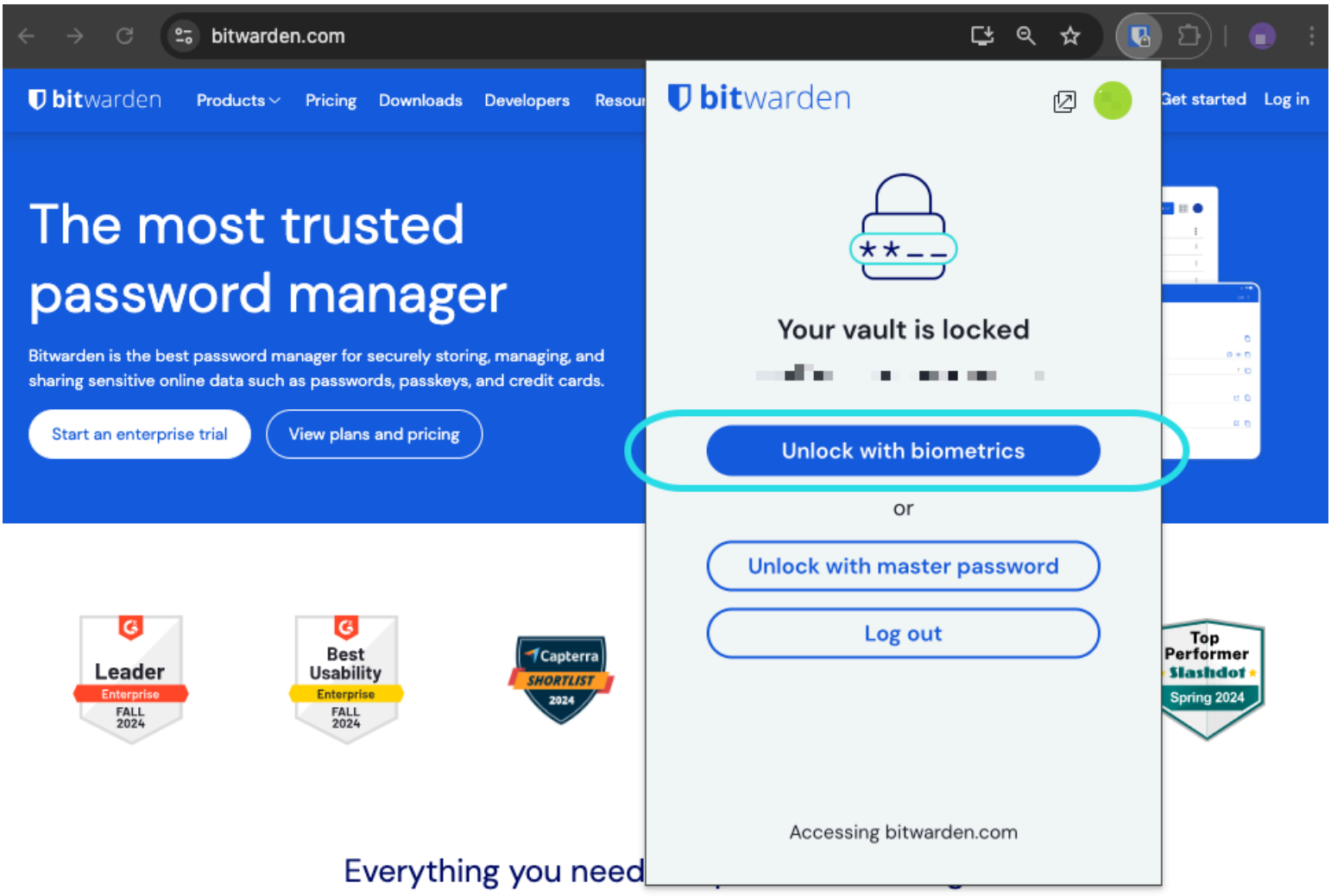
5. Välj **Kontosäkerhet** och markera rutan **Lås upp med biometri**.

   > **Tip**
   >
   > Du kan i detta skede bli ombedd att tillåta Bitwarden att `kommunicera med samarbetande inbyggda applikationer`. Denna behörighet är säker, men **valfri** och gör det endast möjligt för webbläsartillägget att kommunicera med skrivbordet enligt beskrivningen ovan.

   Du kommer att uppmanas av din stationära app att mata in din biometriska. Om du gör det slutförs den första installationsproceduren. Om du har valt att kräva verifiering (**steg två**) måste du godkänna en kontroll av fingeravtrycksvalidering.

6. Om du vill att webbläsartillägget automatiskt ska fråga efter din biometriska inmatning när det startas, se till att alternativet **Fråga efter biometri vid start** är aktiverat.

Webbläsartillägget kommer automatiskt att fråga efter din biometriska när du öppnar den. Om du stänger av promptalternativet (**steg sex**), använd knappen **Lås upp med biometri** på upplåsningsskärmen:



Lås upp webbläsartillägg med biometri

> **Tip**
> Din stationära app måste vara inloggad och upplåst för att kunna låsa upp ett webbläsartillägg med biometri.

Inaktiverad i väntan på verifiering av huvudlösenord

Om du får ett meddelande som rapporterar att biometrisk upplåsning är inaktiverad för autofyll i väntan på verifiering av ditt huvudlösenord:

1. Stäng tillfälligt av autofyll i Bitwarden.
2. Återaktivera biometri i Bitwarden.
3. Aktivera autofyll igen i Bitwarden.

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**
   >
   > När du ställer in en PIN-kod eller biometri används en ny krypteringsnyckel härledd från PIN-koden eller den biometriska faktorn för att kryptera kontons krypteringsnyckel, som du kommer att ha tillgång till genom att vara inloggad och lagrad på disk[a].
   >
   > **Upplåsning av** ditt valv gör att PIN-koden eller den biometriska nyckeln dekrypterar kontokrypteringsnyckeln i minnet. Den dekrypterade kontokrypteringsnyckeln används sedan för att dekryptera alla valvdata i minnet.
   >
   > **Att låsa** ditt valv gör att all dekrypterad valvdata, inklusive den dekrypterade kontokrypteringsnyckeln, raderas.
   >
   > [a] - Om du använder alternativet **Lås med huvudlösenord vid omstart**, lagras denna nyckel bara i minnet istället för på disken.

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