

MITT KONTO > TVÅSTEGSINLOGGNING

Fältguide till tvåstegsinloggning

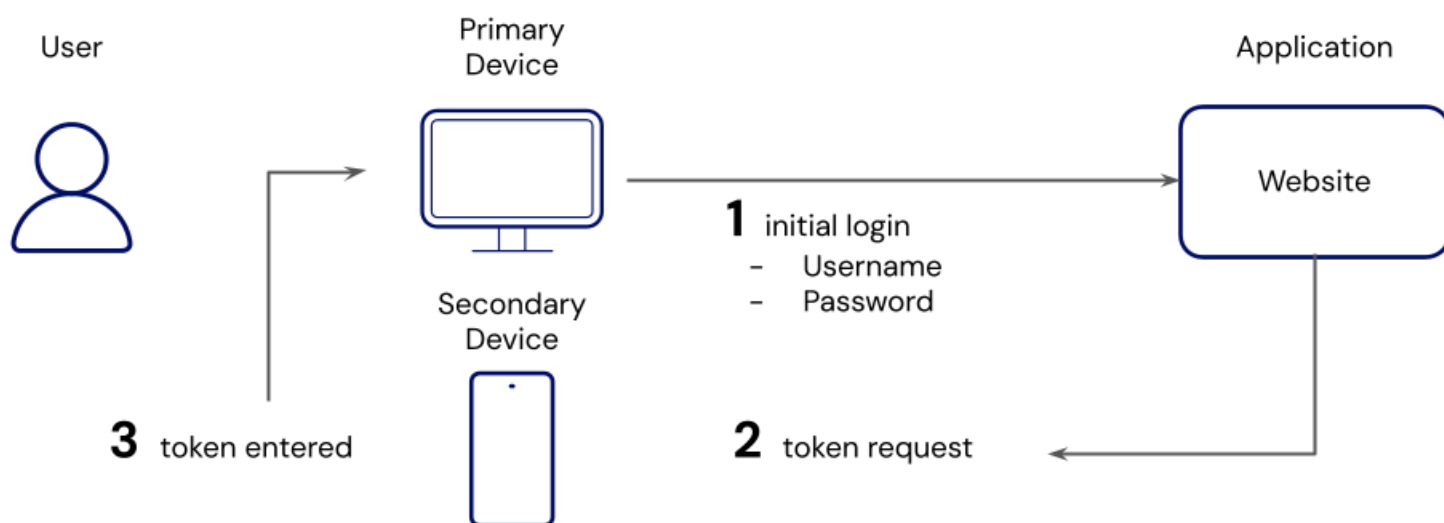
View in the help center:

<https://bitwarden.com/help/bitwarden-field-guide-two-step-login/>

Fältguide till tvåstegsinloggning

Tvåstegsinloggning (även kallad tvåfaktorsautentisering eller 2FA) är en vanlig säkerhetsteknik som används av webbplatser och appar för att skydda dina känsliga uppgifter. Webbplatser som använder tvåstegsinloggning kräver att du verifierar din identitet genom att ange en extra "token" (även kallad verifieringskod eller engångslösenord (OTP)) förutom användarnamn och lösenord, vanligtvis hämtade från en annan enhet.

Utan fysisk åtkomst till token från din sekundära enhet skulle en illvillig aktör inte kunna komma åt webbplatsen, även om de upptäcker ditt användarnamn och lösenord:



Basic Two-step Login flow

Vanligtvis kommer webbplatser eller appar med känslig data (till exempel ditt onlinebankkonto) att försöka verifiera din identitet utanför inloggningsskärmen genom att:

- Skicka en token i ett SMS/textmeddelande till den mobila enheten på fil.
- Be om en token som genereras av en Authenticator-app (till exempel [Bitwarden Authenticator](#)) på din mobila enhet.
- Letar efter en token från en fysisk säkerhetsnyckel (till exempel Yubikey).

Hur ska jag använda tvåstegsinloggning?

Säkerhet innebär ofta en avvägning mellan skydd och bekvämlighet, så i slutändan är det upp till dig! Generellt sett är de två mest kritiska sätten att använda tvåstegsinloggning:

1. För att säkra Bitwarden

Säkra all valvdata genom att kräva ett sekundärt steg varje gång du loggar in på Bitwarden, förutom att ange ditt huvudlösenord.

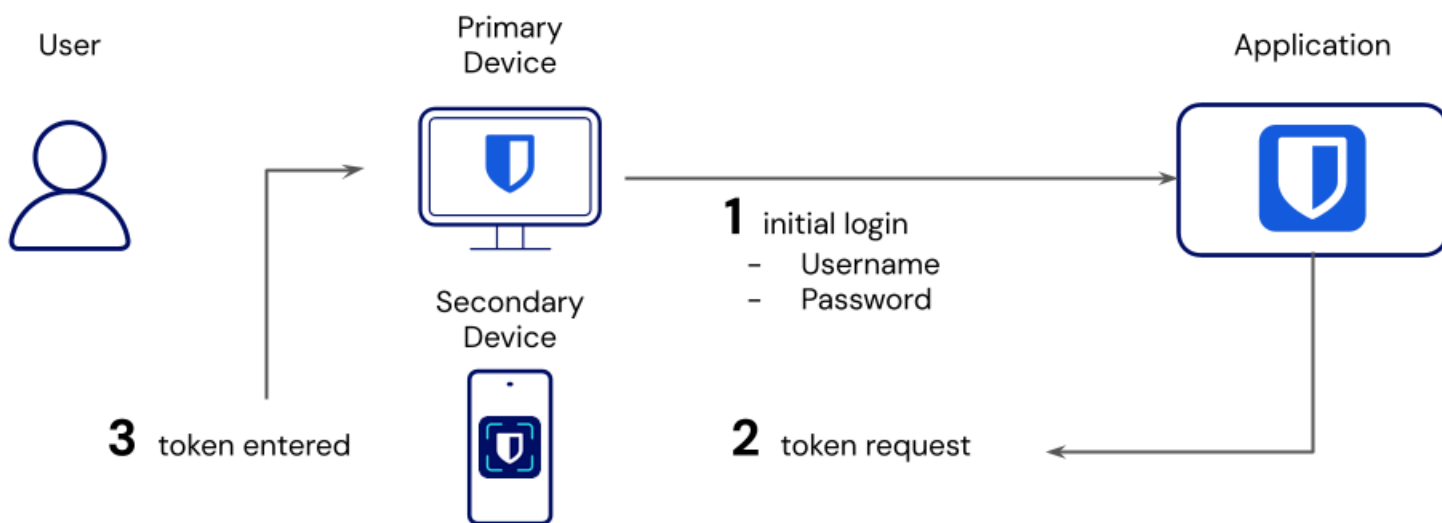
2. För att säkra viktiga webbplatser

Säkra en enskild webbplats genom att kräva ett tillfälligt engångslösenord (TOTP) när du loggar in. Du kan lagra och generera TOTP:er med Bitwarden.

Säkra Bitwarden

Eftersom din lösenordshanterare lagrar alla dina inloggningar rekommenderar vi starkt att du säkrar den med tvåstegsinloggning. Om du gör det skyddar du alla dina inloggningar genom att förhindra en illvillig aktör från att komma åt ditt valv, även om de upptäcker ditt huvudlösenord.

Om du aktiverar tvåstegsinloggning måste du slutföra ett sekundärt steg varje gång du loggar in, utöver din primära inloggningsmetod (huvudlösenord). Du behöver inte slutföra ditt sekundära steg för att låsa upp ditt valv, bara för att logga in.



Two-step login to access Bitwarden

Bitwarden erbjuder flera tvåstegsinloggningsmetoder gratis, inklusive:

- FIDO (valfri FIDO2 WebAuthn-certifierad nyckel)
- via en autentiseringsapp (till exempel [Bitwarden Authenticator](#))
- via e-post

För premiumanvändare erbjuder Bitwarden flera avancerade tvåstegsinloggningsmetoder:

- Duo Security med Duo Push, SMS, telefonsamtal och säkerhetsnycklar
- YubiKey (valfri enhet i 4/5-serien eller YubiKey NEO/NFC)

Läs mer om dina alternativ eller få hjälp med att ställa in valfri metod med hjälp av våra [installationsguider](#).

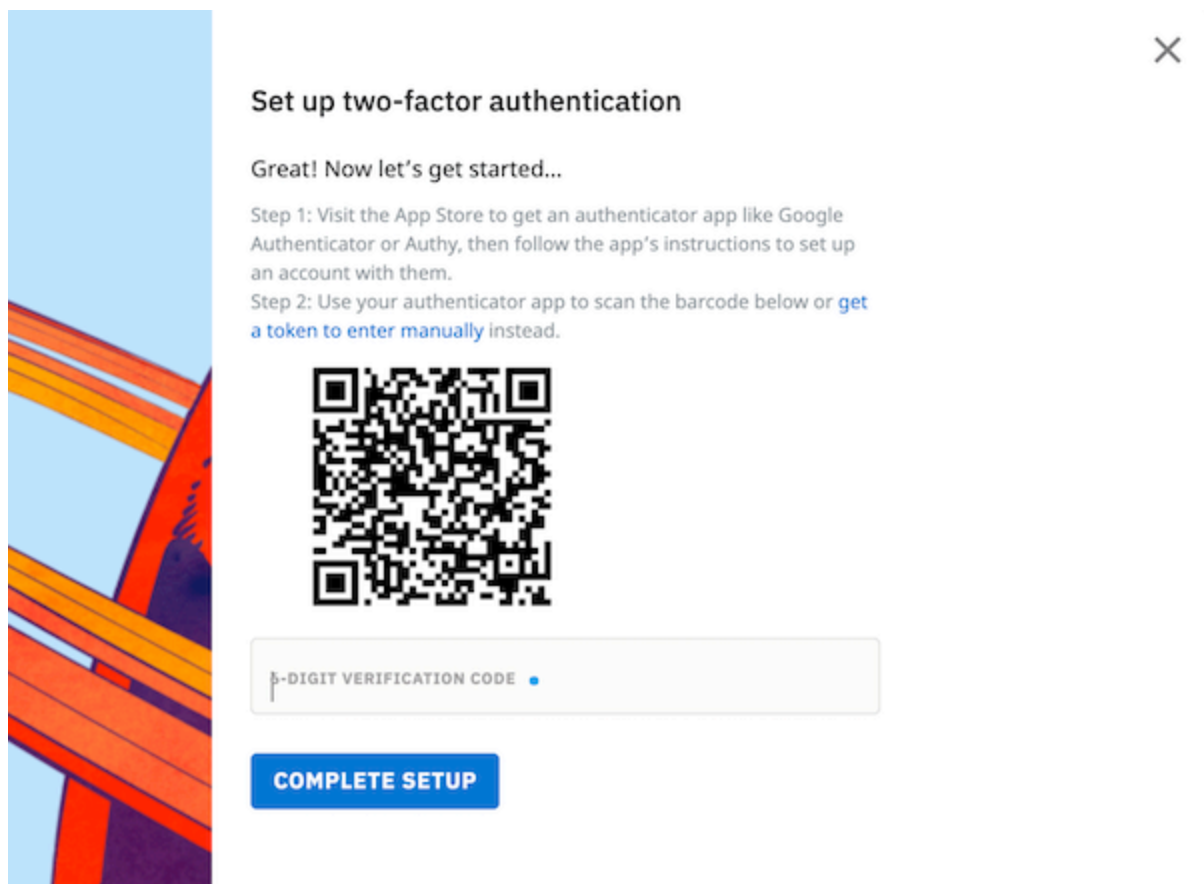
📘 Note

Bitwarden does not support SMS 2FA due to vulnerabilities, including SIM hijacking. We do not recommend SMS 2FA for other accounts unless it is the only available method. Any second factor is recommended over having none, but most alternatives are safer than SMS 2FA.

Säkra viktiga webbplatser

Många andra webbplatser och appar har tvåstegsinloggningsalternativ, detta är särskilt vanligt för webbplatser som lagrar känslig information (till exempel kreditkorts- eller bankkontonummer). De flesta webbplatserns tvåstegsinloggningsalternativ kommer att finnas i menyerna **Inställningar**, **Säkerhet** eller **Sekretess**.

Aktivering av tvåstegsinloggning öppnar vanligtvis en QR-kod, som det här exemplet från Reddit:



2FA QR Code

Genom att skanna den här koden med en autentiseringsapp kommer appen att kunna generera roterande sexsiffriga tokens som du kan använda för att verifiera din identitet, som den här som genereras av [Bitwarden Authenticator](#):



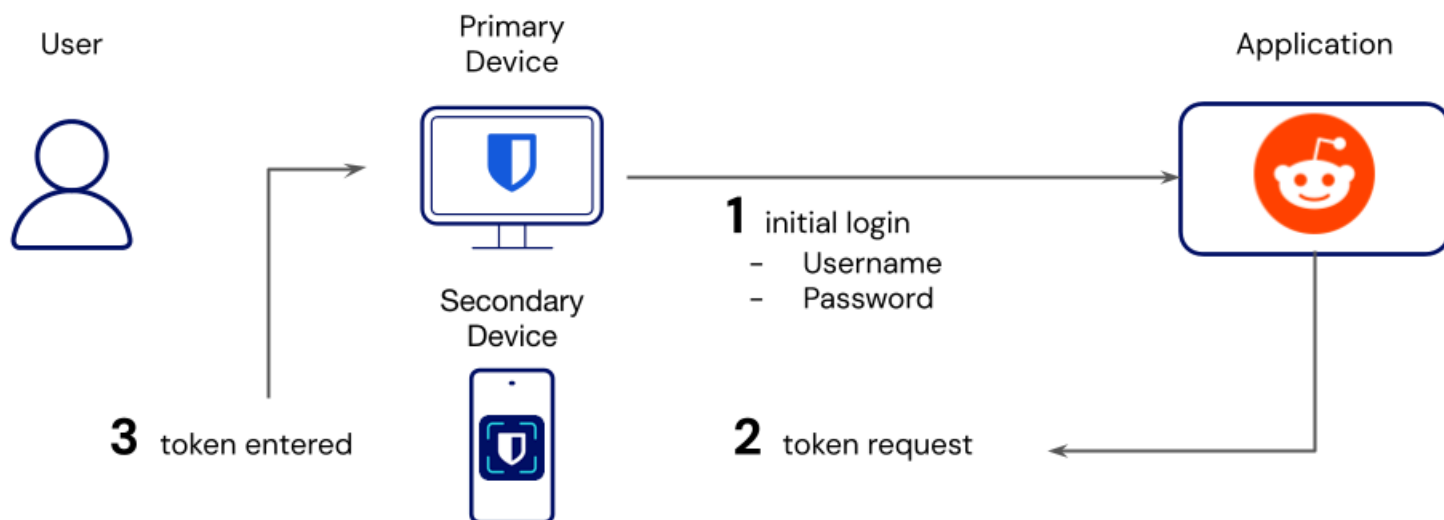
Reddit

18 153 974

TOTP token

Använd Bitwarden Authenticator

Bitwarden Authenticator är en mobil autentiseringsapp som du kan använda för att verifiera din identitet för webbplatser och appar som använder tvåfaktorsautentisering (2FA). Bitwarden Authenticator kan laddas ner från iOS App Store och Google Play Store.

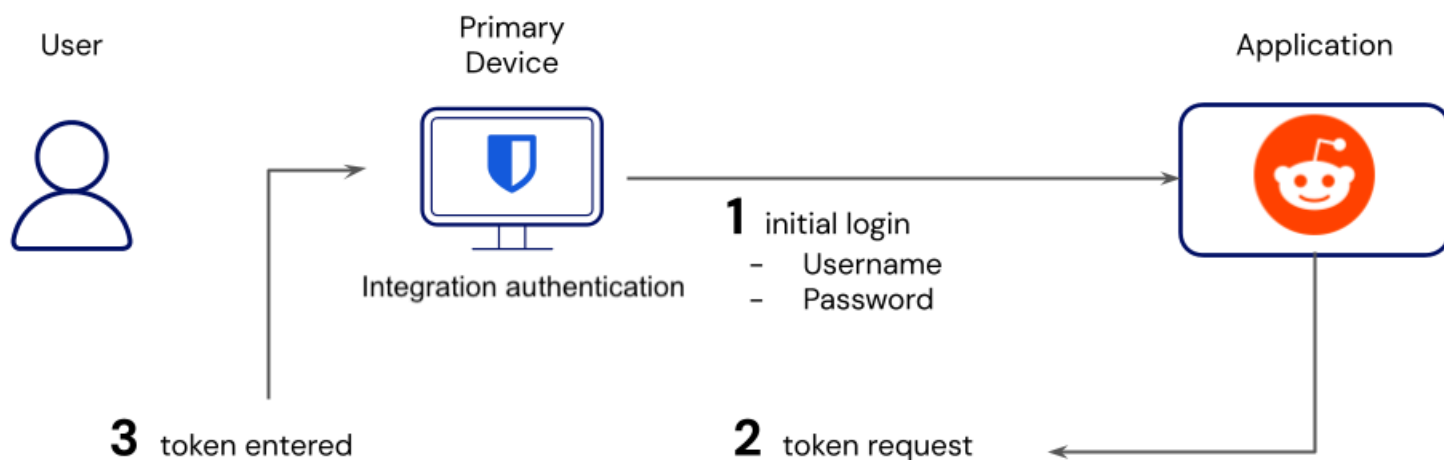


Two-step login using Bitwarden Authenticator

För hjälp med att använda Bitwarden Authenticator, se den [här artikeln](#).

Använd integrerad autentisering

Som ett alternativ erbjuder Bitwarden Password Manager en inbyggd autentisering för premiumanvändare, inklusive medlemmar av betalda organisationer (familjer, team eller företag).



Two-step Login using Bitwarden

För hjälp med att använda integrationsautentisering, se den [här artikeln](#).

När ska jag använda den fristående appen i motsats till den integrerade autentiseringsenheten?

Endast den fristående appen låter dig ställa in 2FA för ditt Bitwarden-konto, men du kan använda båda apparna för att lagra och generera verifieringskoder för alla dina andra konton. Endast den integrerade autentiseringen låter dig för närvarande dela tokengenereringen mellan teammedlemmar. De kan användas tillsammans eller separat, beroende på dina säkerhetsinställningar.

2FA säkerhetsnycklar och lösenord

FIDO2-säkerhetsnycklar är ett populärt och säkert alternativ för att lägga till 2FA till ditt Bitwarden-konto. Om du inte är bekant med FIDO2-säkerhetsnycklar, se [FIDO Alliances webbplats](#) för ytterligare information om FIDO2.

En YubiKey-enhet är en säkerhetsnyckel som fungerar med FIDO-autentiseringsprotokoll och kan ha flera användningsfall. Två användningsområden är som 2FA-säkerhetsnycklar eller [lösenord](#).

- **2FA-säkerhetsnyckel:** Att använda en YubiKey som en 2FA-säkerhetsnyckel kommer att fungera som en extra enhet i autentiseringsprocessen. Detta kommer att åtföljas av en annan primär metod för autentisering (som huvudlösenord). YubiKey-säkerhetsnyckeln måste vara fysiskt ansluten för att ge autentiseringsuppgifterna.
- **Nyckel:** En lösenordsnyckel är ett par eller offentlig-privata kryptografiska nycklar som används för att autentisera en inloggning. Istället för att skapa ett användarnamn, lösenord och lägga till 2FA till ett konto, används den enda lösenordsnyckeln. Under skapandet av lösenordsnyckeln kan YubiKey fungera som lösenordsgenerator för att skapa de offentliga och privata nycklar som krävs för inloggning med lösenord. Läs mer om att använda en YubiKey som lösenord [här](#).

Med Bitwarden är den primära användningen av en säkerhetsnyckel som en YubiKey-enhet att tillhandahålla 2FA-autentisering.

Nästa steg

Nu när du är en tvåstegs inloggningsexpert rekommenderar vi:

- [Ställ in tvåstegsinloggning](#)
- [Få premium för tillgång till avancerade tvåstegsinloggningsmetoder](#)
- [Ställ in Bitwarden-autentiseringsverktyget](#)
- [Ställ in tvåstegsinloggning för team och företag](#)