bitwarden | Help Center Article

MITT KONTO > LOGGA IN OCH LÅS UPP

Nytt skydd för enhetsinloggning

View in the help center:
https://bitwarden.com/help/new-device-verification/

Nytt skydd för enhetsinloggning

> **Note**
>
> Från och med den 4 **mars 2025** kommer inloggningar från nya enheter att uppmanas för denna nya verifiering. Denna ändring kommer initialt att finnas i webbappen och sedan utökas till andra Bitwarden-appar när användare uppdaterar till den senaste versionen.

För att hålla ditt konto säkert och säkert kräver Bitwarden ytterligare verifiering **för användare som inte använder tvåstegsinloggning**. Efter att ha angett ditt Bitwarden-huvudlösenord kommer du att bli ombedd att ange en engångsverifieringskod som skickas till ditt kontos e-post för att slutföra inloggningsprocessen **när du loggar in från en enhet som du inte har loggat in på tidigare**. Om du till exempel loggar in på en mobilapp eller ett webbläsartillägg som du har använt tidigare kommer du inte att få denna prompt.

De flesta användare kommer inte att uppleva denna prompt om de inte ofta loggar in på nya enheter. Denna verifiering behövs endast för nya enheter eller efter att webbläsarcookies har rensats.

Om du regelbundet kommer åt din e-post bör det vara enkelt att hämta verifieringskoden. Om du föredrar att inte lita på ditt Bitwarden-kontos e-post för verifiering kan du ställa in tvåstegsinloggning via en Authenticator-app, en hårdvarunyckel eller tvåstegsinloggning via en annan e-post.

Vanliga frågor

När kommer detta att hända?

Från och med den 4 **mars 2025** kommer inloggningar från nya enheter att uppmanas för denna nya verifiering. Denna ändring kommer initialt att finnas i webbappen och sedan utökas till andra Bitwarden-appar när användare uppdaterar till de senaste versionerna.

Varför implementerade Bitwarden detta?

Bitwarden implementerade denna förändring för att förbättra säkerheten för användare som inte har tvåstegsinloggning aktiverad. Om någon får åtkomst till ditt lösenord kommer de fortfarande inte att kunna logga in på ditt konto utan sekundär verifiering (koden som skickas till din e-post). Detta extra lager hjälper till att skydda din data från hackare som ofta riktar sig mot svaga eller utsatta lösenord för att få obehörig åtkomst.

När blir jag tillfrågad om denna verifiering?

Du kommer bara att bli tillfrågad om denna verifiering när du loggar in från nya enheter. Om du loggar in på en enhet som du har använt tidigare kommer du inte att bli tillfrågad.

Vad anses vara en ny enhet?

En ny enhet är vilken enhet som helst som inte tidigare har använts för att logga in på ditt Bitwarden-konto. Detta kan inkludera en ny telefon, surfplatta, dator eller webbläsartillägg som du aldrig har loggat in från tidigare. När du loggar in från en ny enhet blir du ombedd att verifiera din identitet via en engångskod som skickas till din e-post.

Andra scenarier som kommer att initiera en ny enhet är:

- Om du avinstallerar och installerar om mobilappen, skrivbordsappen eller webbläsartillägget initieras en ny enhet.
- Rensa webbläsarcookies kommer att initiera en ny enhet för webbappen, men inte för webbläsartillägg.
- Använda webbläsartillägget i Virtual Desktop Infrastructure (VDI) som återställer användarprofillagring efter varje session. I detta scenario kvarstår inte lokal lagring.

Mina e-postuppgifter sparas i Bitwarden. Kommer jag att låsas ute från Bitwarden?

E-postverifieringskoder kommer endast att krävas på nya enheter för användare som inte har tvåstegsinloggning aktiverad. Du kommer inte att se denna prompt på tidigare inloggade enheter och du kommer att logga in som vanligt med din e-postadress för ditt konto och ditt huvudlösenord.

Om du loggar in på en ny enhet kommer ditt Bitwarden-konto att få en engångsverifieringskod. Om du har tillgång till din e-post, det vill säga ett beständigt inloggat e-postmeddelande på din mobiltelefon, kommer du att kunna hämta engångsverifieringskoden för att logga in. När du väl har loggat in på den nya enheten kommer du inte att uppmanas att ange verifieringskoden igen.

Om du regelbundet loggar in på din e-post med inloggningsuppgifter sparade i Bitwarden eller inte vill lita på din e-post för verifiering, bör du ställa in tvåstegsinloggning som kommer att vara oberoende av Bitwarden-kontots e-postadress. Detta inkluderar en autentiseringsapp som Bitwarden Authenticator-mobilappen, säkerhetsnyckel eller e-postbaserad tvåstegsinloggning med en annan e-postadress. Om någon 2FA-metod är aktiv kommer användaren att välja bort den e-postbaserade verifieringen av nya enheter. Användare med 2FA aktiv bör också spara sin Bitwarden-återställningskod på ett säkert ställe.

Vem är utesluten från den här kontots e-postbaserade verifiering av nya enheter?

Följande kategorier av inloggningar är exkluderade:

- Användare som har konfigurerat tvåstegsinloggning är uteslutna.
- Användare som loggar in med SSO, med en lösenordsnyckel eller med en API-nyckel exkluderas.
- Användare med egen värd är exkluderade.
- Användare som loggar in från en enhet där de tidigare har loggat in exkluderas.
- Användare vars konton är mindre än 24 timmar gamla.
- Användare som väljer bort sina **Inställningar → Mitt konto-skärmen** exkluderas (rekommenderas inte).

Min organisation använder SSO, måste mina användare slutföra ny enhetsverifiering?

Nej. Användare som loggar in med SSO är undantagna och ombeds inte att verifiera inloggningen på en ny enhet. Men om en användare, utan tvåstegsinloggning aktiverad, loggar in med ett användarnamn och lösenord utan att gå igenom SSO, uppmanas de att verifiera den nya enheten.

Jag vill inte dela min riktiga e-post med Bitwarden, hur kan jag konfigurera mitt konto?

Användare som vill vara anonyma har flera alternativ tillgängliga:

- Använd ett tvåstegsinloggningsalternativ som inte kräver ett e-postmeddelande, inklusive en autentiseringsapp, säkerhetsnyckel eller e-postbaserad tvåstegsinloggning med en annan e-postadress.
- Använd en tjänst för vidarebefordran av e-postalias.
- Självvärd Bitwarden.

Bitwarden uppmuntrar användare att ha en aktiv e-post, eftersom Bitwarden skickar viktiga säkerhetsvarningar som misslyckade inloggningsförsök.

Om jag använder 2FA-återställningskoden på en ny enhet eftersom jag har förlorat min 2FA-åtkomst, kommer jag fortfarande att bli föremål för denna nya enhetsverifiering?

Bitwarden kommer att uppdatera återställningskodflödet så att när du skickar in ditt lösenord och återställningskod loggas du in på webbappen och förs till dina 2FA-inställningar. Om du är orolig för att bli utelåst bör du **undvika** att gå igenom det här flödet i en inkognitowebbläsare eller på en enhet med opålitlig internetanslutning för att se till att du kan slutföra alla nödvändiga installationssteg i den här inloggade sessionen.

Jag vill välja bort! Finns det ett alternativ?

Detta är extra säkerhet för användare som inte har tvåstegsinloggning aktiverad. Användare som inte har aktiverat tvåstegsinloggning är mer sårbara för obehörig åtkomst av angripare eftersom lösenord kan äventyras på flera sätt, även om de är starka och unika. Vanliga metoder inkluderar till exempel:

- **Nätfiskeattacker:** Cyberbrottslingar använder vilseledande e-postmeddelanden eller webbplatser för att lura dig att avslöja ditt lösenord.
- **Social ingenjörskonst**: Angripare kan försöka manipulera eller lura dig till att avslöja ditt lösenord genom telefonsamtal, sms eller på annat sätt.
- **Lösenordsknäckning via brute-force-attacker**: Angripare kommer att använda automatiserade verktyg för att upprepade gånger försöka gissa lösenordet.
- **Tangentloggning eller skadlig programvara:** Om din enhet är infekterad med skadlig programvara eller en keylogger, kan angripare registrera varje tangenttryckning du gör – inklusive ditt lösenord – utan din vetskap.

Med ny enhetsverifiering, även om ditt lösenord komprometteras genom någon av metoderna ovan, skulle angriparen fortfarande behöva hämta den andra verifieringen, som är engångskoden i din e-post. Detta minskar avsevärt sannolikheten för obehörig åtkomst.

Ny enhetsverifiering är utformad för att vara mindre påträngande än traditionell tvåstegsinloggning. Det gäller bara när du loggar in från en enhet eller klient som du inte har använt tidigare, så de flesta användare kommer inte att uppleva detta extra steg, eftersom de regelbundet loggar in på sina vardagliga enheter. Verifieringsprocessen använder din e-post, vilket är något som många håller öppet på en telefon eller dator, så det går snabbt och enkelt att hämta koden.

Användare som kan uppleva vissa utmaningar är de som gör följande:

- Ha inte tvåstegsinloggning aktiverad.
- Lagra deras e-postlösenord i Bitwarden.
- Avinstallera och installera om Bitwarden ständigt.
- Logga ut från deras e-post överallt.

Endast användare som gör alla dessa saker och matchar villkoren ovan kommer att uppleva friktion med den här säkerhetsuppdateringen. Om användare blir utelåsta från sitt konto kan de kontakta Customer Success på Bitwarden.

Om användare inte vill ha ny enhetsverifiering rekommenderas det starkt att aktivera en alternativ tvåstegsinloggningsmetod (antingen via en autentiseringsapp, hårdvarunyckel eller en annan e-post) för att skydda ditt konto.

Om användare inte vill ha ny enhetsverifiering, inte vill ställa in en alternativ tvåstegsinloggningsmetod och **inte vill ha någon ytterligare säkerhet på sitt konto,** finns det ett alternativ att välja bort det genom att navigera till skärmen **Inställningar → Mitt konto** och rulla till

avsnittet Riskzon. Vi måste betona att detta **starkt inte rekommenderas**, eftersom det gör ditt konto sårbart för olika attacker.