Logga in med lösenordsbeta

Logga in med lösenordsbeta

> **Note**
> Log in with passkeys is currently in beta.

Lösenord kan användas för att logga in på Bitwarden som ett alternativ till att använda ditt huvudlösenord och e-post. Lösenord som används för att logga in på Bitwarden kräver användarverifiering, vilket innebär att du måste använda något som en biometrisk faktor eller säkerhetsnyckel för att framgångsrikt etablera åtkomst till din lösenord.

För att lära dig mer om grunderna för lösenord, kolla in den här bloggen från Bitwarden.

Inloggning med en lösenordsnyckel kommer att kringgå Bitwardens tvåstegsinloggning, men endast PRF-kompatibla webbläsare (t.ex. Google Chrome) och autentiseringskombinationer (t.ex. YubiKey 5) kan användas för att ställa in inloggning med lösenord för valvdekryptering. Nyckelnycklar som inte använder PRF kommer att kräva att du anger ditt huvudlösenord efter att ha loggat in för att dekryptera ditt valv.

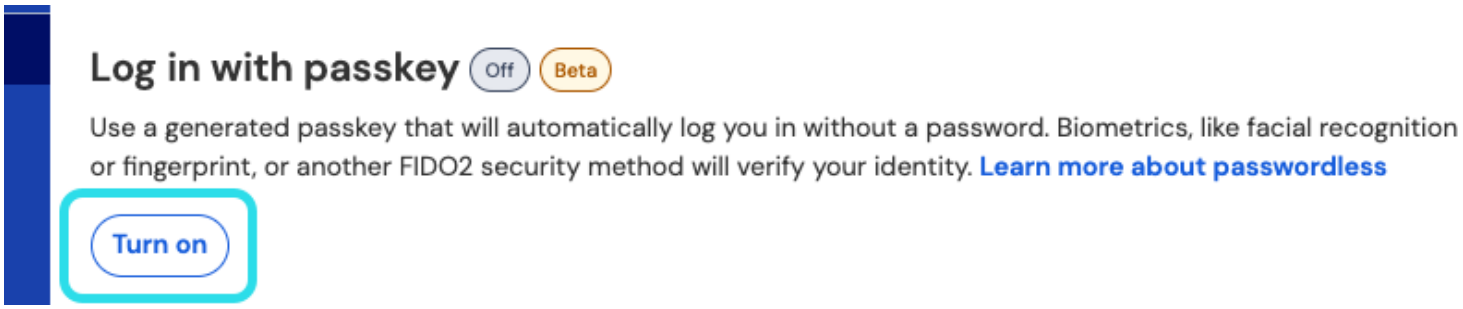
Nyckelnycklar kan för närvarande användas för att logga in på Bitwardens webbapp, och stöd för andra klientapplikationer planeras för en framtida version.

> **Note**
> Log in with passkeys can't be used by members of an organization that uses the Require single sign-on authentication policy, SSO with trusted devices, or Key Connector.

Skapa en lösenordsnyckel

Du kan ha upp till 5 lösenord att logga in med vid varje given tidpunkt. Så här skapar du en lösenordsnyckel för att logga in på Bitwarden:

1. I webbappen väljer du **Inställningar** → **Säkerhet** från navigeringen:
2. Välj **fliken** Huvudlösenord.
3. I avsnittet Logga in med lösenord väljer du **Aktivera** eller, om du redan har ställt in en lösenordsnyckel, **Ny lösenord**. Du kommer att bli ombedd att ange ditt huvudlösenord:



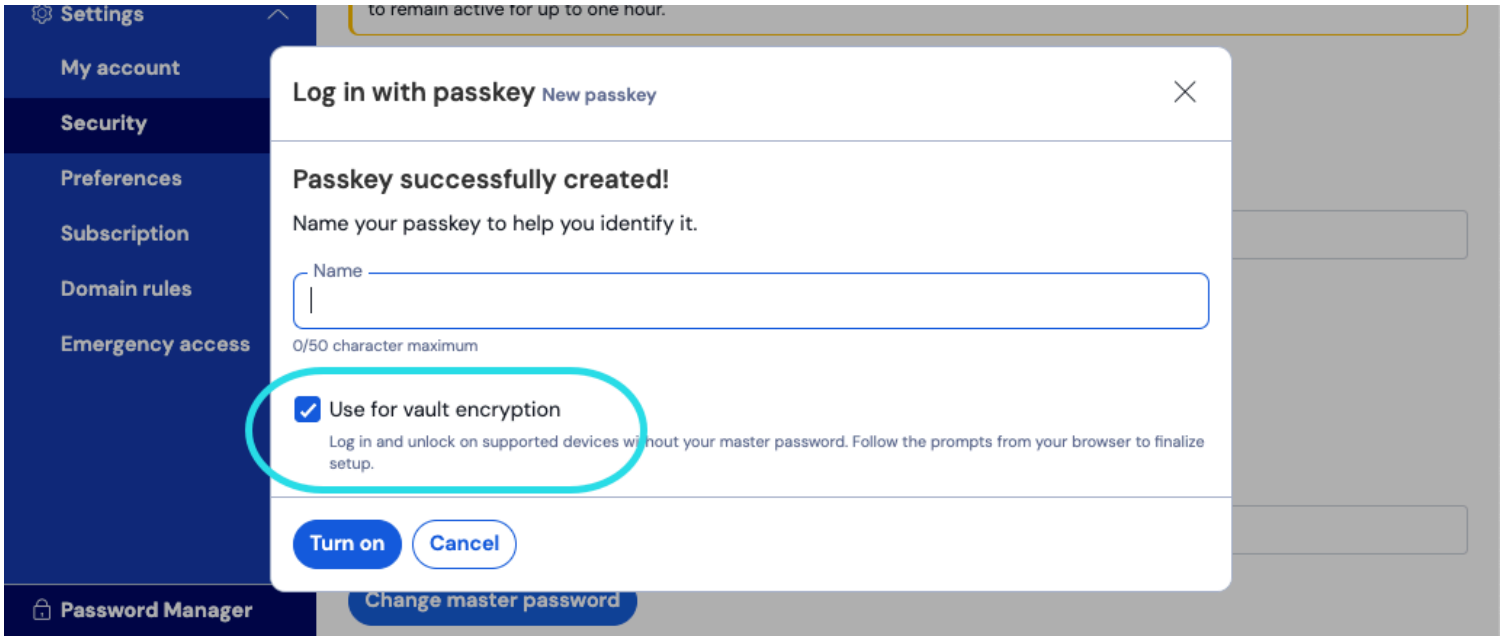
Turn on login with passkeys

4. Följ anvisningarna från din webbläsare för att skapa ett FIDO2-lösenord. Du kan slutföra användarverifiering med hjälp av en faktor som en biometrisk eller genom att skapa en PIN-kod.

Du kan under den här proceduren behöva avbryta en standardautentisering som din webbläsare vill att du ska använda, till exempel om du vill använda en hårdvarusäkerhetsnyckel på en macOS-enhet som kommer att prioritera Touch ID.

5. Ge ditt lösenord ett **namn**.

6. Om du inte vill använda din lösenordsnyckel för valvkryptering och dekryptering, avmarkera kryssrutan **Använd för valvkryptering**:



Use passkey for vault encryption

Det här alternativet kommer bara att visas om din webbläsare (t.ex. Google Chrome) och autentisering (t.ex. YubiKey 5) är PRF-kompatibla. Läs mer.

7. Välj **Slå på**.

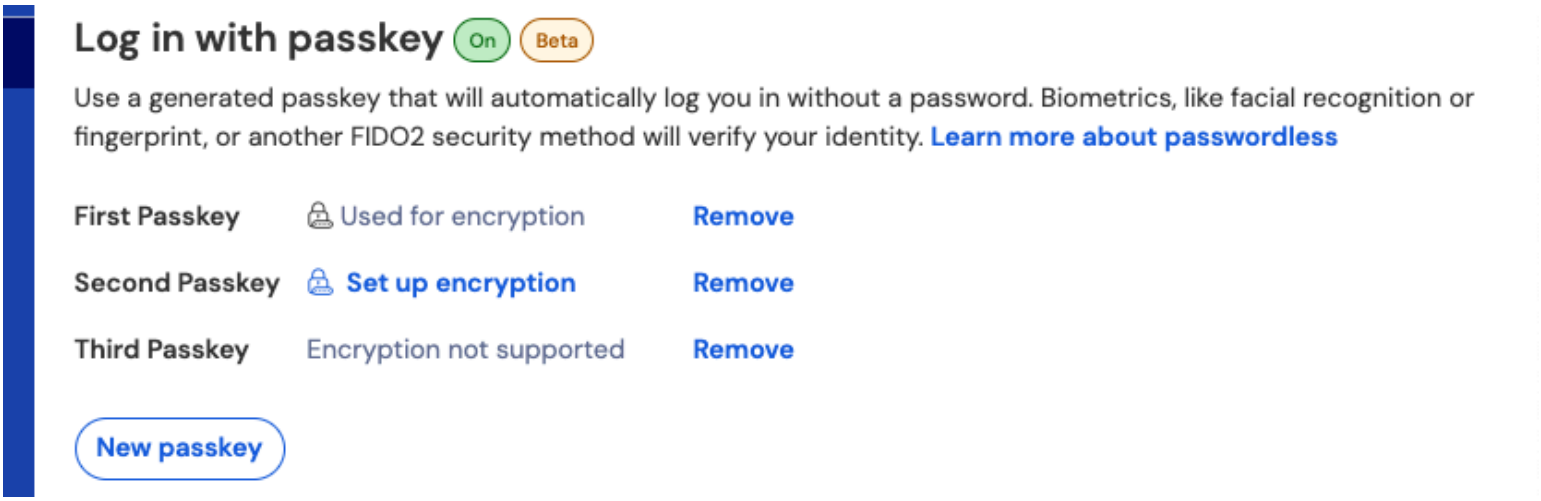
> **Tip**
> Bitwarden will not prompt or allow you to save a passkey for logging in to Bitwarden in your vault. This prevents a scenario where access to your vault is required to log in to Bitwarden.

Ställ in kryptering

Både din webbläsare (t.ex. Google Chrome) och autentisering (t.ex. YubiKey 5) måste vara PRF-kompatibla för att stödja användning av lösenordet för valvkryptering och dekryptering.

> **Tip**
> While Google Chrome is PRF-capable, Chrome profiles are not PRF-capable authenticators. As a counter example, the YubiKey 5 is a PRF-capable authenticator. Additionally, Windows 10 is known to have issues with PRF-capable passkeys.
>
> The equipment you have at your disposal and in your environment will determine your ability to use passkeys for encryption.

Din lösenordslista kommer att visa om varje lösenord används för kryptering, stöds men inte aktiverat eller inte:



Passkeys list

Om du inte markerade **kryssrutan** Använd för valvkryptering när du först konfigurerade lösenordet, eller om till exempel webbläsaren du använde vid den tidpunkten inte var PRF-kompatibel, navigera till den här menyn och välj knappen **Konfigurera kryptering**.

Ta bort ett lösenord

Du kan ta bort en befintlig lösenordsnyckel från Bitwarden genom att använda **knappen** Ta bort på samma skärm. Att ta bort en lösenordsnyckel från Bitwarden kommer inte att radera den privata nyckeln som är lagrad i din FIDO2-autentisering, men du kommer inte längre att kunna använda den för att logga in på Bitwarden.

Logga in med ditt lösenord

När ditt lösenord har skapats kan du använda det för att logga in på Bitwardens webbapp:

1. På Bitwardens inloggningsskärm, välj **Logga in med lösenord** där du vanligtvis skulle ange din e-postadress.
2. Följ anvisningarna från din webbläsare för att läsa lösenordet, detta kommer att autentisera dig med Bitwarden.
3. Om din lösenordsnyckel är inställd för valvkryptering är du klar! Annars anger du ditt huvudlösenord och väljer **Lås upp** för att dekryptera dina valvdata.

Hur det fungerar

Följande beskriver mekaniken för att logga in med lösenord. Vilken flik som är relevant för dig beror på om dina lösenord har konfigurerats med kryptering.

⇒Passkeys with encryption turned on

Create a passkey

When a passkey is registered for log in to Bitwarden:

- A **passkey public and private key pair** is generated by the authenticator via the WebAuthn API. This key pair, by definition, is what constitutes your passkey.
- A **PRF symmetric key** is generated by the authenticator via the WebAuthn API's PRF extension. This key is derived from an **internal secret** unique to your passkey and a **salt** provided by Bitwarden.

- A **PRF public and private key pair** is generated by the Bitwarden client. The PRF public key encrypts your **account encryption key**, which your client will have access to by virtue of being logged in and unlocked, and the resulting **PRF-encrypted account encryption key** is sent to the server.
- The **PRF private key** is encrypted with the **PRF symmetric key** (see Step 2) and the resulting **PRF-encrypted private key** is sent to the server.
- Your client sends data to Bitwarden servers to create a new passkey credential record for your account. If your passkey is registered with support for vault encryption and decryption, this record includes:
  - The passkey name
  - The passkey public key
  - The PRF public key
  - The PRF-encrypted account encryption key
  - The PRF-encrypted private key

Your passkey private key, which is required to accomplish authentication, only ever leaves the client in an encrypted format.

Log in with your passkey

When a passkey is used to log in and, specifically, to decrypt your vault data:

- Using WebAuthn API public key cryptography, your authentication request is asserted and affirmed.
- Your **PRF-encrypted account encryption key** and **PRF-encrypted private key** are sent from the server to your client.
- Using the same **salt** provided by Bitwarden and the **internal secret** unique to your passkey, the **PRF symmetric key** is re-created locally.
- The **PRF symmetric key** is used to decrypt your **PRF-encrypted private key**, resulting in your **PRF private key**.
- The **PRF private key** is used to decrypt your **PRF-encrypted account encryption key**, resulting in your **account encryption key**. Your account encryption key is used to decrypt your vault data.

⇒Passkeys with encryption turned off

Create a passkey

When a passkey is registered for log in to Bitwarden:

1. A **passkey public and private key pair** is created. This key pair, by definition, is what constitutes your passkey.
2. Your client sends data to Bitwarden servers to create a new passkey credential record for your account. If your passkey is not registered with support for vault encryption and decryption, this record includes:
   - The passkey's name
   - The passkey's public key

Your passkey's private key, which is required to accomplish authentication, only ever leaves the client in an encrypted format.

Log in with your passkey

When a passkey is used to log in, your authentication request is asserted and affirmed using WebAuthn API public key cryptography. You will then be required to decrypt your vault using your master password.