Säkerhet

- PasswordPusher
- Vaultwarden

PasswordPusher

Innehållsförteckning

Officiell dokumentation (EN)

1. Kontohantering

Inloggning och anonym användning

- **Med konto:** Genom att logga in med ditt Björknet-konto kan du hålla reda på dina aktiva länkar, se om de har blivit klickade samt radera dem manuellt i förtid.
- **Utan konto:** Tjänsten kan även användas anonymt för snabb delning. Skillnaden är att du då inte kan hantera eller radera länken efter att du har stängt webbläsarfönstret där länken genererades.

Ändra e-postadress och lösenord

1. Klicka på **Konto** > **Redigera inloggningsuppgifter**.
2. Ange uppgifter.
3. Klicka på **Uppdatera konto**.

Aktivera och hantera tvåfaktorsautentisering (2FA)

1. Klicka på **Konto** > **Redigera inloggningsuppgifter**.
2. Klicka på **Aktivera tvåfaktorsautentisering** och följ instruktionerna på skärmen för att skanna QR-koden med din autentiseringsapp (till exempel Bitwarden).

2. Säkerhetsinstruktioner vid delning

När du skapar en hemlig länk ska du alltid tillämpa principen om minsta möjliga exponering för att upprätthålla högsta säkerhet.

Konfigurera begränsningar

Innan du klickar på att generera länken ska standardvärdena justeras nedåt:

- **Minska antalet dagar:** Ställ ner giltighetstiden till så få dagar som möjligt (förslagsvis 1–2 dagar). Länken ska aldrig ligga aktiv på servern längre än absolut nödvändigt.
- **Minska antalet klick:** Sätt gränsen för maximalt antal visningar till ett lågt antal (rekommenderat är 1 eller 2 klick). Detta säkerställer att länken blir obrukbar omedelbart efter att mottagaren har hämtat informationen.

Hantering och radering

- **Uppmana till radering:** Informera mottagaren om att radera länken via gränssnittet så fort lösenordet har tagits emot och sparats på ett säkert ställe (exempelvis i Vaultwarden).
- **Permanent borttagning:** Genom att radera länken direkt efter hantering säkerställer ni att informationen rensas från serverns databas omedelbart och inte kan kommas åt i efterhand, även om kommunikationskanalen där länken skickades skulle bli kompromitterad.

3. Datahantering och arkivering

Kryptering och lagring

- All data krypteras på serversidan innan den sparas i databasen. Nyckeln som krävs för att dekryptera informationen finns endast i den unika URL-länk som du skickar till mottagaren.
- Administratörer eller obehöriga som har tillgång till databasen kan aldrig läsa innehållet i klartext utan den specifika länken.

Automatisk rensning

- När antingen tidsgränsen (dagarna) eller klickgränsen har uppnåtts, raderas texten helt och hållet från systemet automatiskt. Processen är irreversibel och datan kan inte återställas.

4. Radera konto

1. Klicka på **Konto** > **Redigera inloggningsuppgifter**.
2. Klicka på **Avsluta mitt konto**.

Vaultwarden

***Vaultwarden* är Björknets centrala och krypterade lösenordshanterare. Det är en resurssnål serverimplementation i Rust som är helt kompatibel med *Bitwardens API*. Detta innebär att du använder *Bitwardens* officiella appar och webbläsartillägg för att ansluta till Björknets Vaultwarden-server.**

Innehållsförteckning

Officiell dokumentation för Vaultwarden (EN)

Offciell dokumentation för Bitwarden (EN)

1. Kontohantering

Viktigt gällande säkerhet: En lösenordshanterare är en av de mest säkerhetskrävande tjänster du som privatperson hanterar. Här finns tillgången till det mesta av ditt digitala liv, och om du förlorar tillgången till detta konto kan det få stora konsekvenser.

Vaultwarden/Bitwarden erbjuder mycket hög säkerhet och ger dig verktygen att själv säkra tillgången till din data via flera olika metoder, såsom tvåfaktorsautentisering (2FA), nödkontakter samt export och import av data.

Björknets ansvariga frånskriver sig allt ansvar för förlorad data till följd av slarvig hantering av inloggningsuppgifter och inloggningsmetodor från användarens sida.

Ändra e-post (måste göras i webbgränssnittet)

1. Klicka på **Inställningar** > **Mitt konto**.

2. Ange uppgifter.
3. Klicka på **Fortsätt**.
4. E-post kommer med bekräftelseförfrågan.

Ändra huvudlösenord (måste göras i webbgränssnittet)

Björknet rekommenderar lösenord med minst 15 tecken bestående av slumpmässiga ord, varierade med versaler samt blandat med siffror och specialtecken. Detta lösenord bör memoreras och får inte finnas nedskrivet annat än på ett eget lagringsmedium eller fysiskt.

T.ex. ¤T()CkH=lM-h?r@lD~357
Ord som jag utgått från Stockholm Harald.

Viktigt gällande säkerhet: Du ansvarar själv för hanteringen av ditt lösenord. Det går inte att få någon återställningslänk om du glömmer bort det. Du kan däremot lägga in en lösenordsledtråd som skickas till den e-postadress som är kopplad till kontot. Se därför alltid till att ha en fungerande e-postadress angiven. Om du förlorar tillgång till både ditt huvudlösenord kan **INGEN** återställa kontot eller hjälpa dig att logga in.

1. Klicka på **Säkerhet** > **Huvudlösenord**.
2. Ange uppgifter.
3. Klicka på **Fortsätt**.
4. E-postlänk kommer med bekräftelseförfrågan.

Aktivera och hantera tvåfaktorsautentisering (2FA) i Autentiseringsapp (måste göras i webbgränssnittet)

Det är rekommenderat att använda minst 2 metoder för 2FA och ha återställningsnycklar.

Viktigt gällande säkerhet: Använd en separat autentiseringsapp (lagra inte 2FA-koden för detta konto inuti själva valvet). Om du förlorar tillgång till din primära 2FA-enhet måste du använda dina återställningskoder för att logga in. Om du förlorar både tvåfaktorsautentiseringen och dina återställningskoder kan **INGEN** återställa kontot eller hjälpa dig att logga in.

1. Klicka på **Säkerhet** > **Tvåfaktorsautentisering**.
2. Klicka på **Aktivera tvåfaktorsautentisering** och följ instruktionerna på skärmen för att skanna QR-koden med din autentiseringsapp.
3. Klicka på **Hämta återställningskoder** och dem som genereras på ett säkert ställe. Dessa krävs om du förlorar tillgång till din app.

Aktivera biometrisk upplåsning (kan göras i webbläsartillägg eller app)

1. Klicka på **Inställningar** > **Kontosäkerhet**.
2. Ange uppgifter.
3. Klicka på **Fortsätt**.
4. E-post kommer med bekräftelseförfrågan.

Konfigurera Nödåtkomst (måste göras i webbgränssnittet)

Du kan utse betrodda personer som får tillgång till eller kan ta över ditt konto om du blir inaktiv under en längre tid (1-90dagar).

1. Klicka på **Inställningar** > **Mitt konto**.
2. Klicka **Lägg till nödkontakt**.
3. Ange uppgifter.
4. Klicka på **Spara**.
5. E-post kommer med bekräftelseförfrågan.

2. Datahantering

Exportera data

1. Klicka på **Verktyg** > **Export**.
2. Välj valv i **Exportera från**.
3. Välj önskat format:
   - **JSON (okrypterad):** Standardformat i klartext, lämpligt för import till andra lösenordshanterare. *Hantera filen med extrem försiktighet.*
   - **CSV (okrypterad):** Textformat uppdelat i kolumner för kalkylprogram.
   - **Krypterad JSON**: Krypterad JSON: Säkert format för backup, men kräver samma konto/lösenord för att kunna importeras igen.

Importera data

1. Klicka på **Verktyg** > **Import**.
2. Välj valv i **Valv**.
3. Välj var lösenorden skall sparas i **Mapp**.
4. Välj format i **Filformat**.
5. Välj importfil eller kopiera och klistra in innehållet från filen.

Synkronisering av data (gäller webbläsartillägg eller app)

Hanterar du data mellan flera enheter kan det hända att appen/webbläsartillägget inte hinna synkronisera

1. Klicka på **Säkerhet** > **Huvudlösenord**.
2. Klicka på **Synkronisera nu.**

3. Administratörers datatillgång

- Administratörer kan se/administrera delade lösenord i de organisationer som de har blivit tilldelade åtkomst till, men de kan aldrig få åtkomst till lösenord i ditt eget personliga valv.
- En administratör kan inte se vilka användarkonton som finns i systemet, förutom de medlemmar som ingår i den organisation som administratören har ansvar över.
- En organisationsadministratör kan endast ta bort en användare från själva organisationen, inte radera eller ändra användarens personliga konto.
- Endast du har full tillgång och exklusiv kontroll över ditt eget konto.

4. Radera konto

BookStack hanterar inte självständiga kontoraderingar direkt från användarprofilen för att förhindra att dokumentation som ägs av gemenskapen raderas av misstag.

1. Klicka på din profilbild eller ditt namn i det övre högra hörnet och välj **Visa profil**.
2. Klicka på **Mitt konto**.
3. Klicka på **Radera konto**.