bitwarden | Help Center Article

ADMINISTRATÖRSKONSOL > RAPPORTERING

Företagspolicyer

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

Företagspolicyer

Vad är företagspolicyer?

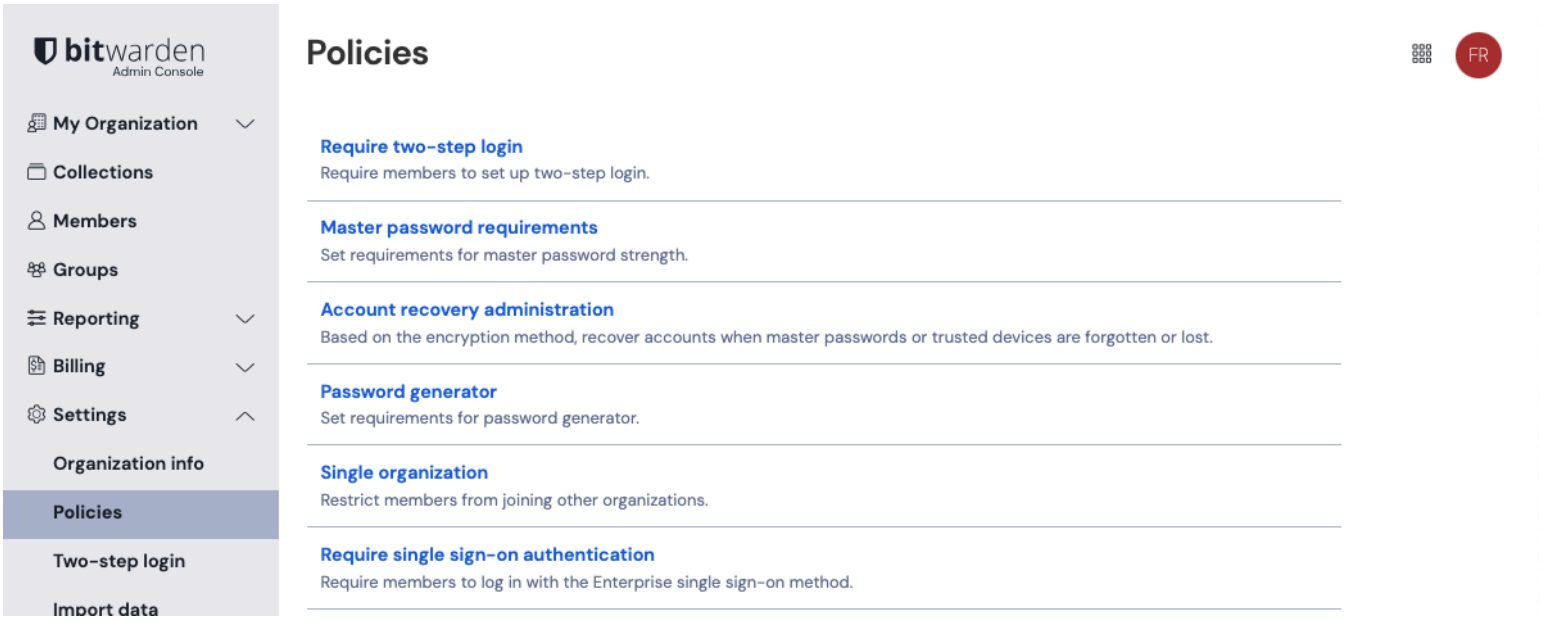
Företagspolicyer tillåter företagsorganisationer att upprätthålla säkerhetsregler för alla användare, till exempel tvingande användning av tvåstegsinloggning.

Företagspolicyer kan ställas in av organisationens administratörer eller ägare.

> **⚠ Warning**
>
> We recommend setting enterprise policies prior to inviting users to your organization. Some policies will revoke non-compliant users when turned on, and some are not retroactively enforceable.

Att sätta företagspolicyer

Policyer kan ställas in från administratörskonsolen genom att navigera till **Inställningar → Policyer**:



Ange policyer

Tillgängliga policyer

Kräv inloggning i två steg

Om du aktiverar policyn **Kräv tvåstegsinloggning** måste medlemmarna använda valfri tvåstegsinloggningsmetod för att komma åt sina valv. Om du använder en SSO eller identitetsleverantörs 2FA-funktionalitet behöver du inte aktivera denna policy. Denna policy tillämpas även för användare som bara har accepterat inbjudan till din organisation.

> **⚠ Warning**
>
> **Organization members who are not owners or admins and do not comply with this policy will have access revoked when you activate this policy.** Users who have access revoked as a result of this policy will be notified via email, and must take steps to become compliant before their access can be restored.

Krav på huvudlösenord

Om du aktiverar principen för krav **för** huvudlösenord kommer en konfigurerbar uppsättning minimikrav för användarnas huvudlösenordsstyrka att tillämpas. Organisationer kan genomdriva:

- Lägsta huvudlösenordskomplexitet
- Minsta huvudlösenordslängd
- Typer av tecken som krävs

Lösenordets komplexitet beräknas på en skala från 0 (svag) till 4 (stark). Bitwarden beräknar lösenordskomplexiteten med hjälp av zxcvbn-biblioteket.

Använd **alternativet** Kräv befintliga medlemmar att ändra sina lösenord för att kräva att befintliga, icke-kompatibla organisationsmedlemmar, oavsett roll, uppdaterar sitt huvudlösenord vid nästa inloggning. Användare som skapar ett nytt konto från organisationsinbjudan kommer att uppmanas att skapa ett huvudlösenord som uppfyller dina krav.

Ta bort Lås upp med PIN

Om du aktiverar policyn **Ta bort Lås upp med PIN-kod** förbjuds medlemmar från att konfigurera eller använda upplåsning med PIN-kod på webbappar, webbläsartillägg och skrivbordsappar. Denna policy gäller för alla organisationsmedlemmar när den är aktiverad, inklusive administratörer och ägare.

> **ⓘ Note**
>
> Support for enforcing this policy on mobile apps is planned for a future release.

Medlemmar som använder upplåsning med PIN före policyn kommer att få det genomdrivet vid nästa inloggning, vilket innebär att om de har en redan inloggad session kommer de fortfarande att se alternativet i användargränssnittet och kunna låsa upp med PIN **tills** de loggar ut **eller** stänger av alternativet för upplåsning med PIN i klienten.

Administration av kontoåterställning

Om du aktiverar administrationspolicyn **för** kontoåterställning kan ägare och administratörer använda lösenordsåterställning för att återställa huvudlösenordet för registrerade användare. Som standard kommer användare att behöva registrera sig för lösenordsåterställning, men alternativet för automatisk registrering kan användas för att tvinga fram automatisk registrering av inbjudna användare.

Administrationspolicyn för kontoåterställning krävs för att din organisation ska kunna använda SSO med betrodda enheter.

> **Note**
>
> The **Single organization** policy must be enabled before activating this policy.
>
> As a result, you must turn off the **Account recovery administration** policy before you can turn off the **Single organization** policy.

Automatisk registrering

Om du aktiverar alternativet för **automatisk registrering** registreras automatiskt alla nya medlemmar, oavsett roll, i lösenordsåterställning när deras inbjudan till organisationen accepteras och hindrar dem från att dra sig ur.

> **Note**
>
> Users already in the organization will not be retroactively enrolled in password reset, and will be required to self-enroll.

Lösenordsgenerator

Om du aktiverar policyn för **lösenordsgenerering** kommer en konfigurerbar uppsättning minimikrav att tillämpas för alla användargenererade lösenord för alla medlemmar, oavsett roll. Organisationer kan genomdriva:

- Lösenord, lösenordsfras eller användarpreferens

För lösenord:

- Minsta lösenordslängd
- Minsta antal (0-9) räknas
- Minsta antal specialtecken (!@#$%^&*).
- Typer av tecken som krävs

För lösenordsfraser:

- Minsta antal ord
- Om man ska kapitalisera
- Om siffror ska inkluderas

> **⚠ Warning**
>
> Existing non-compliant passwords **will not** be changed when this policy is turned on, nor will the items be removed from the organization. When changing or generating a password after this policy is turn on, configured policy rules will be enforced.
>
> A banner is displayed to users on the password generator screen to indicate that a policy is affecting their generator settings.

Enskild organisation

Om du aktiverar policyn för **singelorganisation** kommer det att begränsa icke-ägande/icke-administratörsmedlemmar i din organisation från att kunna gå med i andra organisationer eller från att skapa andra organisationer. Denna policy tillämpas även för användare som bara har accepterat inbjudan till din organisation, men denna policy tillämpas inte för ägare och administratörer.

> **⚠ Warning**
>
> **Organization members who are not owners or admins and do not comply with this policy will have access revoked when you activate this policy.** Users who have access revoked as a result of this policy will be notified via email, and must take steps to become compliant before their access can be restored.

Kräv enkel inloggningsautentisering

Om du aktiverar policyn **Kräv enkel inloggning-autentisering** måste användare som inte är ägare eller administratörer logga in med SSO. Om du är självvärd kan du tillämpa denna policy för ägare och administratörer med hjälp av en miljövariabel. För mer information, se Använda inloggning med SSO. Denna policy tillämpas inte för ägare och administratörer.

Medlemmar i organisationer som använder denna policy kommer inte att kunna logga in med lösenord.

> **ⓘ Note**
>
> The **Single organization** policy must be on before activating this policy.
>
> As a result, you must turn off the **Require single sign-on authentication** policy before you can turn off the **Single organization** policy.

Ta bort individuellt valv

Om du aktiverar policyn **Ta bort individuella valv** måste användare som inte äger/inte är administratörer spara valvobjekt till en organisation genom att förhindra ägande av valvobjekt för organisationsmedlemmar.

En banner visas för användarna på skärmen **Lägg till objekt** som indikerar att en policy påverkar deras ägandealternativ.

Denna policy tillämpas även för användare som bara har accepterat inbjudan till din organisation, men denna policy tillämpas inte för ägare och administratörer.

> **Note**
> Vault items that were created prior to the implementation of this policy or prior to joining the organization will remain in the user's individual vault.

Ta bort Skicka

Om du aktiverar policyn för att **ta bort sändning** förhindras medlemmar som inte är ägare eller administratörer från att skapa eller redigera en sändning med Bitwarden Send. Medlemmar som omfattas av denna policy kommer fortfarande att kunna ta bort befintliga sändningar som ännu inte har nått raderingsdatumet. Denna policy tillämpas inte för ägare och administratörer.

En banner visas för användare i Skicka-vyn och när alla befintliga Skicka öppnas för att indikera att en policy begränsar dem till att bara ta bort Sends.

Skicka alternativ

Om du aktiverar policyn för **sändningsalternativ** kan ägare och administratörer ange alternativ för att skapa och redigera sändningar. Denna policy tillämpas inte för ägare och administratörer. Alternativen inkluderar:

Alternativ	Beskrivning
Tillåt inte användare att dölja sin e-postadress	Om du aktiverar det här alternativet tas alternativet dölj e-post bort, vilket innebär att alla mottagna sändningar kommer att inkludera vem de skickas från.

Vault timeout

Genom att ställa in timeoutpolicyn **för** Arkiv kan du:

- Implementera en maximal tidsgräns för valvet för alla medlemmar i din organisation **utom ägare**. Det här alternativet tillämpar tidsgränsen på alla klientapplikationer (mobil, stationär, webbläsartillägg och mer).
- Ställ in en tidsgräns för valvet för alla medlemmar i din organisation **utom ägare**. Det här alternativet kan ställas in på **Användarpreferens**, **Lås** eller **Logga ut** när en valv-timeout inträffar.

  Alternativet Logga ut kan till exempel användas för att uppmana användare att använda 2FA varje gång de kommer åt sina valv och för att förhindra offlineanvändning genom att regelbundet rensa lokal data från användarnas maskiner.

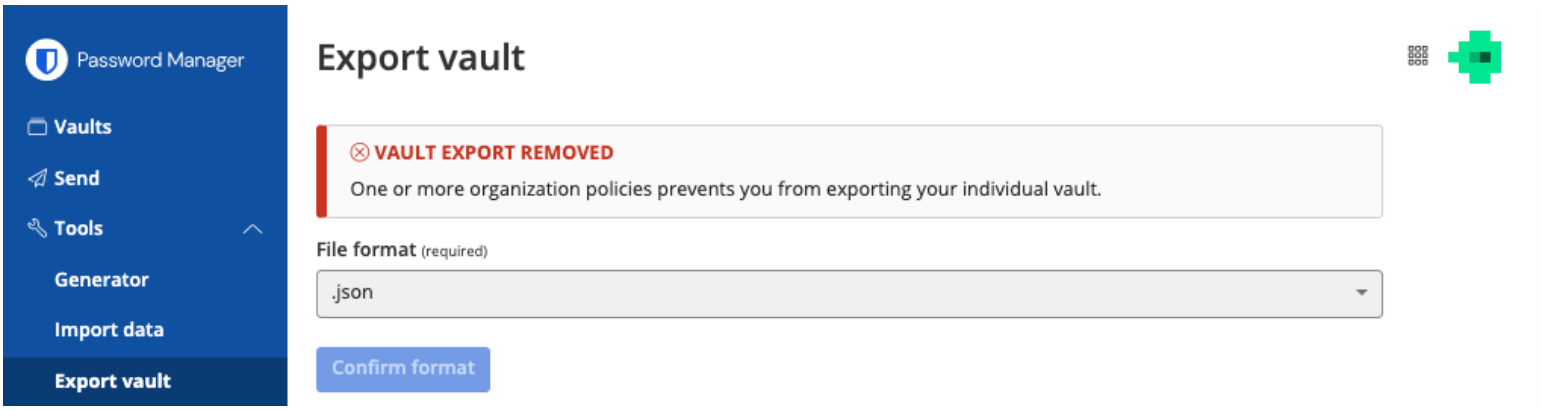
En banner visas för användarna under valvets timeoutkonfiguration som indikerar att en policy påverkar deras alternativ. Vissa tidsgränsalternativ för valv, som **Vid omstart av webbläsare** eller **Aldrig,** kommer inte att vara tillgängliga för användare när denna policy är aktiverad. Denna policy tillämpas inte för ägare och administratörer.

> **Note**
>
> The **Single organization** policy must be enabled before activating this policy.
>
> As a result, you must turn off the **Vault timeout** policy before you can turn off the **Single organization** policy.

Ta bort individuell valvexport

Om du aktiverar **exportpolicyn för Ta** bort individuella valv förbjuds medlemmar som inte är ägare eller administratörer i din organisation från att exportera sina individuella valvdata. Denna policy tillämpas inte för ägare och administratörer.

I webbappen och CLI visas ett meddelande för användarna som indikerar att en policy påverkar deras alternativ. I andra klienter kommer alternativet helt enkelt att inaktiveras:



Vault export removed

Ta bort gratis Bitwarden Families-sponsring

Om du aktiverar **sponsringspolicyn för** Ta bort gratis Bitwarden Families förhindras medlemmar i din organisation från att ha möjlighet att lösa in en gratis familjeplan via din organisation.

Användare som har löst in en sponsrad familjeorganisation innan policyn aktiveras kommer att fortsätta att ha sin organisation sponsrad till slutet av den aktuella faktureringsperioden. Deras lagrade betalningsmetod kommer att debiteras för organisationen när nästa faktureringscykel börjar.

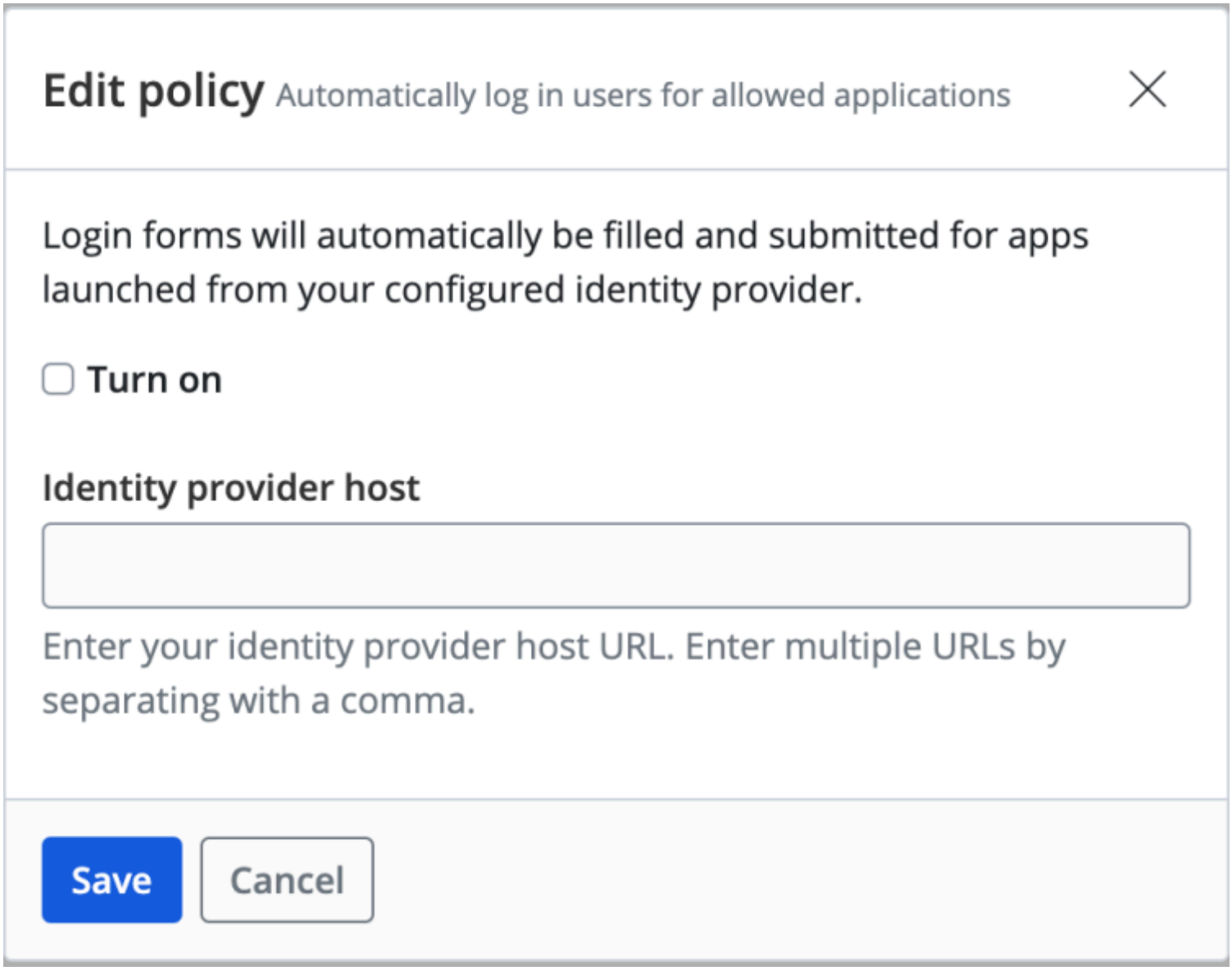
Aktivera autofyll

Om du aktiverar **policyn för** Aktivera autofyll aktiveras automatiskt funktionen autofyll vid sidladdning i webbläsartillägget för alla befintliga och nya medlemmar i organisationen. Om den är aktiverad kommer medlemmar inte att ha möjlighet att inaktivera autofyll vid sidladdning.

Logga in användare automatiskt för tillåtna applikationer

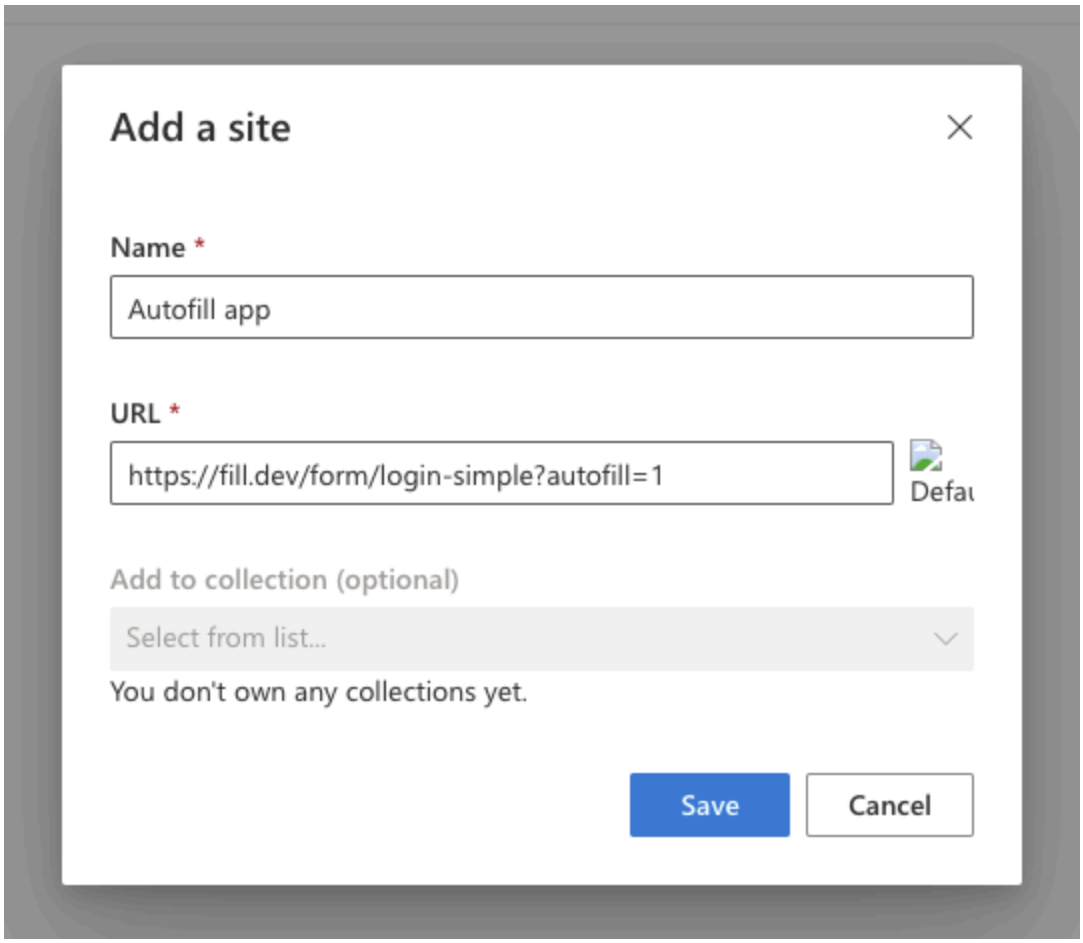
Om du aktiverar policyn Logga in användare **automatiskt för tillåtna applikationer** kan inloggningsformulär fyllas i och skickas automatiskt när du får åtkomst till appar som inte är SSO från din identitetsleverantör. För att aktivera denna inställning:

1. För att aktivera policyn Logga in användare **automatiskt för tillåtna applikationer**, markera rutan **Slå på** och ange din **identitetsleverantörs** värd-URL(er). URL:en ska innehålla `protocol://domän`.



Automatically log in users for allowed applications

2. Som administratör på din IdP, lägg till en applikation eller appgenväg till din slutanvändarinstrumentpanel som innehåller måladressen med den tillagda parametern `?autofill=1`. Om du till exempel använder Microsoft Azure:



Microsoft app example

3. När applikationen har sparats kan användare välja applikationen från IdP-instrumentpanelen och Bitwarden kommer att autofylla och logga in på applikationen

> **Note**
> Automatically log in users will autofill data based on the users current active account on the Bitwarden browser extension. Additionally, the data autofilled will be the most recent credential that user used associated with the target application's URL.