

## Veiligheid zonder wachtwoorden: het kan

### Eenvoudige aanmelding bij de LastPass-kluis



### Op naar een wachtwoordloze toekomst: minder wachtwoorden = minder gedoe.

LastPass werkt al 15 jaar aan een sterkere beveiliging voor bedrijven door beter wachtwoordbeheer. Door wachtwoorden veilig op te slaan in één kluis, zorgt LastPass ervoor dat gebruikers minder wachtwoorden gebruiken, zodat bedrijven minder afhankelijk zijn van menselijk gedrag.

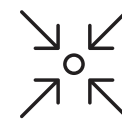
De technologie voor verificatie wordt steeds beter, en we blijven eraan werken om bedrijven minder afhankelijk te maken van wachtwoorden. Sterker nog, we werken aan een toekomst zonder wachtwoorden, met optimaal gemak voor gebruikers. En veiligheid kan ook zonder extra drempels: met wachtwoordloze aanmelding bij de LastPass-kluis op het bureaublad.

### Zet hoofdwachtwoorden op de automatische piloot

Gebruikers kunnen de wachtwoordloze toegang tot hun LastPass-kluis op hun bureaublad inschakelen als ze hun account aanmaken of via de instellingen van hun account. Hiervoor kiezen ze één van drie veilige mechanismen om hun identiteit te verifiëren: met de LastPass Authenticator, of met hardware sleutels of biometrische technologie die compatibel zijn met FIDO2. Als ze de begeleide configuratie hebben voltooid, hoeven ze op vertrouwde apparaten hun wachtwoord niet meer in te voeren.

### Nog geen afscheid van het hoofdwachtwoord

De technologie voor wachtwoordloze toegang ontwikkelt zich razendsnel. Het doel is om helemaal zonder hoofdwachtwoord te kunnen werken, maar dat is een proces van meerdere stappen. Voorlopig blijft het hoofdwachtwoord nog bestaan om wijzigingen in de beveiligingsinstellingen van het account te bevestigen, en voor mislukte verificatiepogingen. Gebruikers hebben hun wachtwoord minder vaak nodig, dus zorg ervoor dat ze hun opties voor accountherstel zo configureren dat ze altijd nog een back-up hebben om bij hun kluis te komen.



**Vereenvoudigde gebruikerservaring**



**Minder wachtwoordfrustraties**



**Hogere productiviteit voor IT-beheerders**



**Veilige verificatie**

[Probeer wachtwoordloze aanmeldingen](#)

# Het is tijd om te denken over een wereld zonder wachtwoorden

## Vereenvoudigde gebruikerservaring

Met wachtwoordloze aanmelding kunnen medewerkers hun kluis openen en belangrijke aanmeldingsgegevens beheren, zonder dat ze hiervoor hun hoofdwachtwoord nodig hebben. Geef direct probleemloos toegang en voorkom frustraties en vertragingen door wachtwoorden. Werk met een wachtwoordbeheerder om de digitale assets van uw bedrijf te beveiligen, en versoepel de toegang met aanmeldingen zonder wachtwoorden.

## Sterkere beveiligingsstandaarden

Uw medewerkers kunnen een nog sterker hoofdwachtwoord instellen – tenslotte hoeven ze het niet te onthouden! En u kunt dit simpel afdwingen met een strengere beleidsregel. Met twee beveiligingsmechanismen die compatibel zijn met FIDO2, kunt u erop vertrouwen dat uw aanmelding verloopt volgens met nieuwste beveiligingsprotocol.

En als uw medewerkers hun hoofdwachtwoord minder vaak invoeren en gebruiken, dalen de risico's voor u en uw bedrijf.

## Minder gedoe betekent meer gebruik

Als aanmelden nog makkelijker wordt, gebruiken mensen hun LastPass-kluis vaker. Dit verbetert de aanname voor uw hele organisatie. Een betere aanname zorgt voor betere algehele wachtwoordgewoontes en verlaagt uw digitale risico's aanzienlijk.

## Verhoog de productiviteit

Als er geen wachtwoorden meer nodig zijn voor aanmeldingen, gaat er geen kostbare werktijd meer verloren aan wachtwoordherstel of vertragingen als mensen accounts niet kunnen gebruiken. En ook uw IT-afdeling kan zich bezighouden met nuttigere zaken. Iedereen kan zich weer richten op echte toegevoegde waarde, in plaats van gedoe rondom wachtwoorden.

Werk zonder wachtwoorden met LastPass Business

