

Wachtwoordsleutels (Passkeys) voor Microsoft 365

Handleiding



1. Inhoudsopgave

1.	Inhoudsopgave	2
2.	Inleiding.....	3
3.	Vorbereiding	3
4.	Wachtwoordsleutel toevoegen via beveiligingsgegevens (standaard gebruiker)	3
5.	Inloggen met je Android of Iphone (standaard Gebruiker)	7
6.	Wachtwoordsleutel aanmaken via Microsoft Authenticator (HighProfile Gebruikers).....	8
7.	Inloggen met je Android of Iphone (HighProfile Gebruiker)	13
8.	Microsoft 365-omgeving configureren voor passkeys.....	16
8.1	Authenticatiemigratie afronden	16
8.2	Passkey (FIDO2) inschakelen	17
8.3	Profielen.....	18
8.4	Default passkey profile.....	18
8.5	HighProfile profile	19
8.6	Admin Accounts profile	20
8.7	Profielen koppelen.....	21
9.	Passkeys afdwingen met Conditional Access	21
10.	Uitgebreide conclusie en advies per gebruikerstype.....	22
10.1	Standaardgebruikers.....	22
10.2	Gebruikers met verhoogd risico	22
10.3	Beheerders en zeer gevoelige accounts	22
10.4	Eindadvies.....	22



2. Inleiding

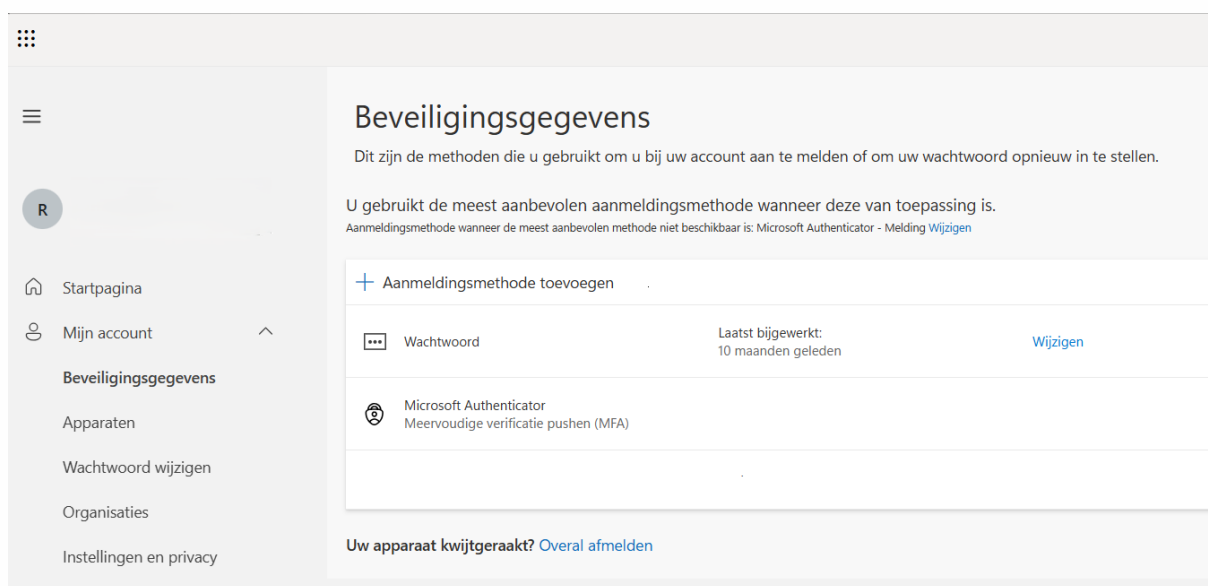
Deze handleiding beschrijft hoe gebruikers een wachtwoordsleutel, ook wel passkey genoemd, kunnen aanmaken en gebruiken voor Microsoft 365. Daarnaast bevat dit document beheerdersinstructies voor het inschakelen, configureren en afdwingen van passkeys binnen Microsoft Entra ID en Conditional Access. Passkeys zijn phishingbestendige aanmeldmethoden op basis van FIDO2. Ze vervangen zwakkere methoden, zoals wachtwoorden, sms-codes en telefonische verificatie, door een methode waarbij een priv sleutel veilig op of via een apparaat wordt opgeslagen. De gebruiker bevestigt de aanmelding lokaal met bijvoorbeeld biometrie of een pincode. Hierdoor kan de aanmeldmethode niet eenvoudig worden onderschept, hergebruikt of doorgestuurd naar een aanvaller.

3. Voorbereiding

Benodigheden

Voordat een gebruiker een passkey kan aanmaken, moet de Microsoft Authenticator-app op de telefoon zijn ge nstalleerd. De app is beschikbaar voor Android en iPhone. Daarnaast moet de gebruiker toegang hebben tot de beveiligingsgegevens van het eigen Microsoft 365-account.

4. Wachtwoordsleutel toevoegen via beveiligingsgegevens (standaard gebruiker)



Ga in Microsoft 365 naar de beveiligingsgegevens van het eigen account. De rechtstreekse pagina hiervoor is: <https://mysignins.microsoft.com/security-info>
Als Microsoft Authenticator nog niet is ingesteld, configureer deze dan eerst voordat je een passkey toevoegt.



Een aanmeldingsmethode toevoegen



Wachtwoordsleutel in Microsoft Authenticator

Aanmelden met uw gezicht, vingerafdruk of pincode



Wachtwoordsleutel

Aanmelden met uw gezicht, vingerafdruk, pincode of beveiligingssleutel



Microsoft Authenticator

Aanmeldingsaanvragen goedkeuren of eenmalige codes gebruiken

Klik op de optie om een nieuwe aanmeldingsmethode toe te voegen. Kies vervolgens voor Wachtwoordsleutel. Microsoft toont daarna de beschikbare opties voor het opslaan en gebruiken van de passkey. Een telefoon gebruikt de beveiliging van het besturingssysteem, zoals vingerafdruk, gezichtsherkenning of pincode. Kies tijdens de wizard voor iPhone-, iPad- of Android-apparaat wanneer de passkey op de telefoon moet worden opgeslagen.

Sign in faster with your face,  fingerprint, or PIN



Maak een wachtwoordsleutel om u aan te melden bij uw account. Geen apps, wachtwoorden of codes nodig.

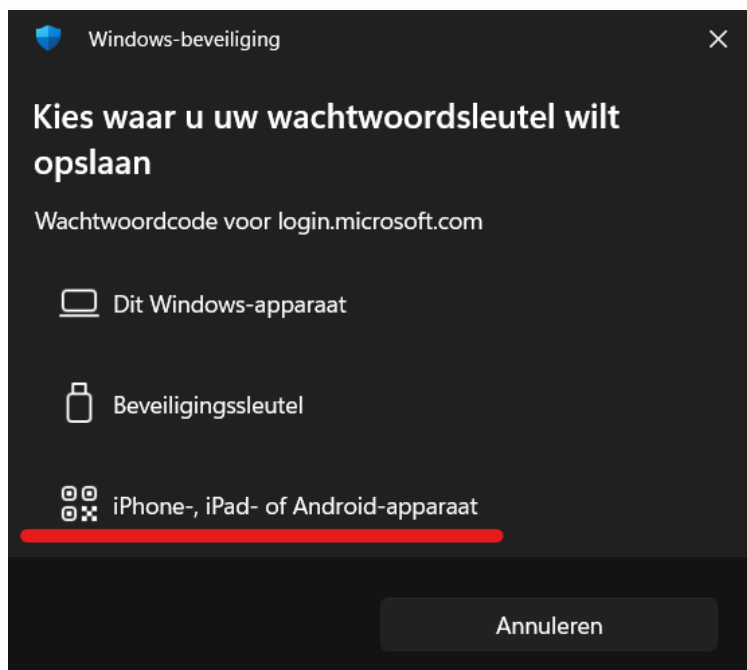
Vorige

Volgende

Klik bij de opslaglocatie op Wijzigen.



Selecteer iPhone-, iPad- of Android-apparaat



Er verschijnt een QR-code op het scherm. Scan deze QR-code met de camera-app van de telefoon en open de koppeling die wordt weergegeven.



Op Android wordt gevraagd om een toegangssleutel aan te maken voor login.microsoft.com. Bevestig dit met de beveiliging van de telefoon, bijvoorbeeld met vingerafdruk of gezichtsherkenning..

Geef de wachtwoordsleutel daarna op de Windows-desktop een herkenbare naam. (Je kan ook de standaard naam laten staan)

Geef uw wachtwoordsleutel
een naam



Geef uw wachtwoordsleutel een naam die u later kunt herkennen.

Google Password Manager

Volgende

Na afronding verschijnt een bevestiging dat de wachtwoordsleutel is aangemaakt.

✓ Wachtwoordsleutel
gemaakt



U kunt nu uw gezicht, vingerafdruk of pincode gebruiken om in te loggen op uw account.

Gereed



5. Inloggen met je Android of Iphone (standaard Gebruiker)

Na het invullen van je naam kies je onder je wachtwoord voor de optie "User your face, fingerprint, PIN or security key instead".



Enter password

[Forgot my password](#)

[Use your face, fingerprint, PIN, or security key instead](#)

Sign in

Kies vervolgens voor iPhone-, iPad-, of Android-apparaat.





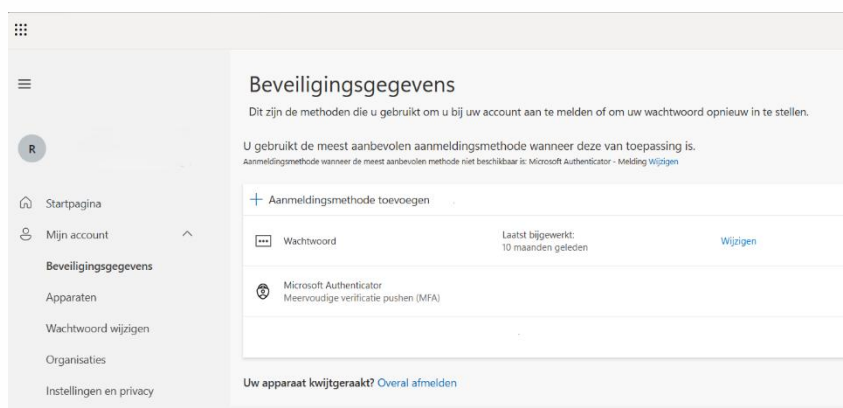
Er wordt nu een QR code getoond op het scherm:



Scan de QR code met je camera.
Klik op de link om vervolgens in te loggen bij Microsoft 365.

6. Wachtwoordsleutel aanmaken via Microsoft Authenticator (HighProfile Gebruikers)

In de Office 365 omgeving ga je naar je beveiligingsgegevens onder je eigen account.
De rechtstreekse link hiervoor is : <https://mysignins.microsoft.com/security-info>



De volgende stap is om een extra aanmeldingsmethode toe te voegen.
Dit doe je door op het plus te klikken:



+ Aanmeldingsmethode toevoegen

Je krijgt nu een menu met allerlei verschillende aanmeldingsmethodes.

We selecteren de bovenste optie : "Wachtwoordsleutel in Microsoft Authenticator".

Een aanmeldingsmethode toevoegen



Wachtwoordsleutel in Microsoft Authenticator

Aanmelden met uw gezicht, vingerafdruk of pincode



Wachtwoordsleutel

Aanmelden met uw gezicht, vingerafdruk, pincode of beveiligingssleutel



Microsoft Authenticator

Aanmeldingsaanvragen goedkeuren of eenmalige codes gebruiken

De gebruiker krijgt nu een venster te zien om verder te gaan op de telefoon.

Het maken van uw wachtwoordcode in Authenticator voltooien



1. Selecteer in Authenticator uw werk- of schoolaccount

2. Selecteer **Een wachtwoordcode maken** en volg de instructies in de app.

Zorg ervoor dat uw apparaat ten minste Android 14 of iOS 17 heeft en dat Authenticator is bijgewerkt naar de nieuwste versie.

Wilt u uw account toevoegen in Authenticator?
[Nu toevoegen.](#)

[Hebt u problemen?](#)



Op de telefoon zie onder de Microsoft Authenticator je account terug van de Microsoft omgeving. Door hierop te klikken ga je naar de informatie hiervan.



Hier zie je de optie voor wachtwoordsleutel staan. Deze klik je aan.





Nu doorloop je de wizard voor het aanmaken van de wachtwoordsleutel.
Er zal worden gevraagd om je aan te melden met je account.

Laten we uw wachtwoordsleutel maken

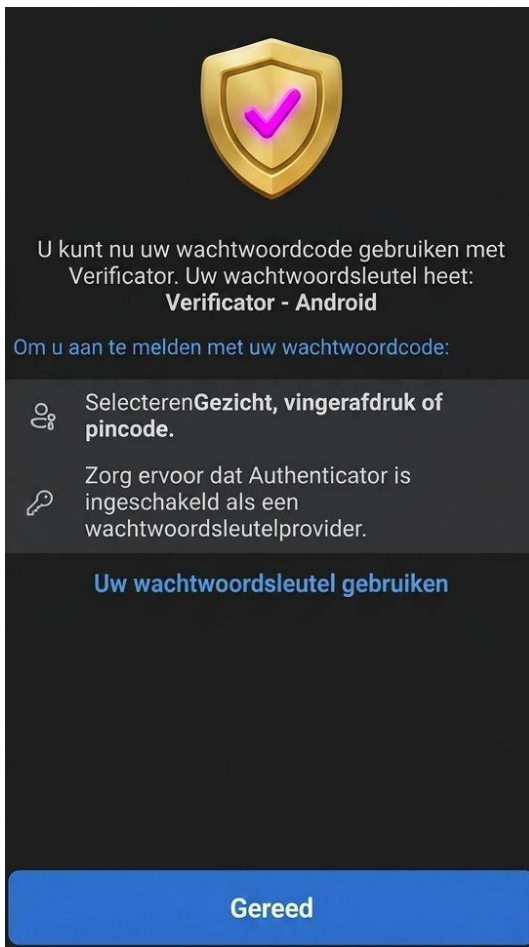


Wachtwoordsleutels zijn een snelle en veilige manier om u aan te melden met uw gezicht, vingerafdruk of pincode. We helpen u bij het maken van uw wachtwoordsleutel. Meld u eerst aan met uw Tester@wereldlichtjesdagommen.nl-account om uw identiteit te verifiëren.

Aanmelden



Je wachtwoord sleutel is nu aangemaakt op je telefoon.
Als je op gereed klikt, is dit proces afgerond.



In Windows krijg je als je nu verder gaat een melding dat er een wachtwoordsleutel is aangemaakt.

✓ Wachtwoordsleutel
gemaakt



U kunt nu uw gezicht, vingerafdruk of pincode
gebruiken om in te loggen op uw account.

[Uw wachtwoordcode gebruiken om u aan te melden](#)

Gereed



7. Inloggen met je Android of Iphone (HighProfile Gebruiker)

Wanneer je inlogt pas je, je aanmeldingsopties aan bij het aanmeldt scherm.

Microsoft

Aanmelden

test@demopasskey.nl

Geen account? [Maak nu een account](#)

[Hebt u geen toegang tot het account?](#)

Volgende

Aanmeldingsopties

Bij een volgende aanmelding bij Microsoft 365 kan de gebruiker kiezen voor Aanmeldingsopties. Selecteer vervolgens de optie Gezicht, vingerafdruk, pincode of beveiligingssleutel.

Microsoft

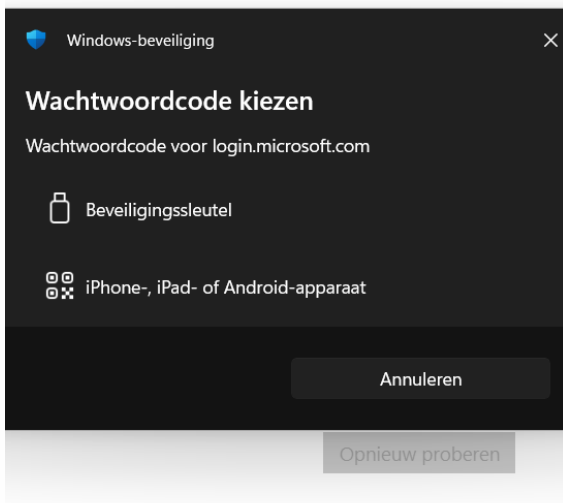
Een methode voor aanmelden kiezen

Gezicht, vingerafdruk, pincode of beveiligingssleutel

Een aanvraag in de Microsoft Authenticator-app goedkeuren

Mijn wachtwoord gebruiken

Vorige



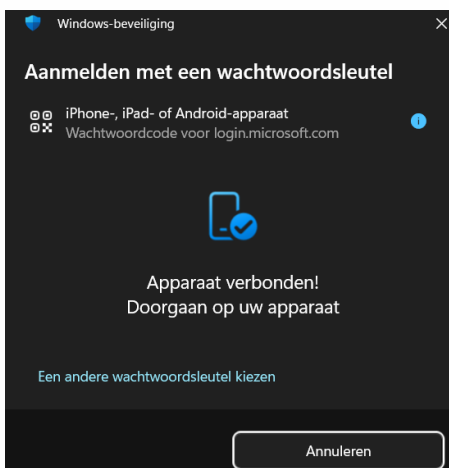
Kies voor iPhone-, iPad- of Android-apparaat.



Er verschijnt een QR-code die met de telefoon kan worden gescand.



Vanuit de Microsoft Authenticator kan je de QR code scannen vanuit het blauwe bolletje. .
In Windows komt er een melding met het verzoek, om de aanmelding op je telefoon goed te keuren.



Je krijgt een bevestiging om de wachtwoordsleutel te gebruiken, op de telefoon.



Je bent nu als gebruiker ingelogd zonder je wachtwoord te gebruiken.



8. Microsoft 365-omgeving configureren voor passkeys

8.1 Authenticatiemigratie afronden

Voordat passkeys gebruikt kunnen worden, moet de migratie van authenticatiemethoden in Entra ID zijn afgerond. Controleer eerst of bestaande methoden, zoals Microsoft Authenticator, correct zijn ingeschakeld. Rond daarna de migratie af met Migration Complete.

Je vindt dit onder :

https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_AdminAuthMethods

Als de migratie nog niet is afgerond, rond deze dan eerst af. Anders kan het voorkomen dat gebruikers zich niet met passkeys kunnen aanmelden.

Controleer vooraf of de gebruikte authenticatiemethoden, zoals Microsoft Authenticator, correct zijn ingeschakeld. Doe dit voordat je wijzigingen doorvoert, zodat je jezelf of andere beheerders niet onbedoeld buitensluit.

Method	Target	Enabled
Built-in		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens	All users	Yes
Voice call	All users	Yes

Bij de migratie klik je op Migration Complete om de migratie af te ronden.

Manage migration



On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and the settings will be managed here. Use this setting to preemptively manage your migration from legacy policies to the new unified policy. [Learn more](#)

- ☐ Pre-migration:
Use policy for authentication only, respect legacy policies.
- ☐ Migration In Progress:
Use policy for authentication and SSPR, respect legacy policies.
- ☒ Migration Complete:
Use policy for authentication and SSPR, ignore legacy policies.



8.2 Passkey (FIDO2) inschakelen

Ga in Entra ID naar Authentication Methods en open Passkey (FIDO2). Zet deze methode op Enabled. Open daarna het default passkey profile of maak een nieuw profiel aan wanneer er nog geen profiel bestaat.

Authentication methods | Policies ...
Stichting WereldLichtjesDag Ommen - Microsoft Entra ID Security

Search + Add external MFA Refresh Got feedback? Begin automated guide

Manage

- Policies**
- Password protection
- Registration campaign
- Authentication strengths
- Settings
- Monitoring

Authentication method policies

Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). [Learn more](#)

Method	Target	Enabled
Built-In		
Passkey (FIDO2)		No
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens	All users	Yes
Voice call	All users	Yes
Email OTP		Yes
Certificate-based authentication		No
Verified ID		No
QR code		No

Zet deze optie op Enabled

Passkey (FIDO2) No

Passkey (FIDO2) settings ...
Passkeys (FIDO2) Authentication Methods

Passkey profiles are now available. Your previous passkey settings have been moved into the default passkey profile. Up to 10 passkey profiles are supported at a time.

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey profiles.

Enable and target Configure

Enable ☒ On

Include Exclude

+ Add target

Name	Type	Passkey profiles
All users	Group	Default passkey profile



8.3 Profielen

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods

Passkey profiles are now available. Your previous passkey settings have been moved into the default passkey profile. Up to 10 passkey profiles are supported at this time. [Learn more](#)

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. [Learn more](#)

Enable and target **Configure**

General

Allow self-service set-up ☒

Passkey profiles

At least one passkey profile must be applied to each target in this policy. The default passkey profile cannot be deleted or renamed. Up to 10 passkey profiles are supported. [Learn more](#)

+ Add profile

Name	Enforce attestation	Passkey types	Key restrictions	
Default passkey profile	No	Device-bound, Synced	No	
Highprofile Profile	No	Device-bound	Yes	
Admin Accounts	Yes	Device-bound	Yes	

Het is verstandig om meerdere passkey-profielen te gebruiken. Hiermee kan per gebruikerstype worden bepaald welke passkey is toegestaan. Een praktische indeling is: Default passkey profile voor standaardgebruikers, High Profile passkey profile voor gebruikers met verhoogd risico of toegang tot gevoelige data, en Admin Accounts profile voor beheerdersaccounts.

8.4 Default passkey profile

Dit profiel is bedoeld voor standaardgebruikers met reguliere rechten in de Microsoft 365-omgeving. Voor deze groep is een gesynchroniseerde passkey via Apple iCloud Keychain of Google Password Manager meestal de meest gebruiksvriendelijke keuze. De passkey wordt versleuteld opgeslagen en via de passkey-provider beschikbaar gemaakt op vertrouwde apparaten van de gebruiker. Dit verlaagt de beheerlast en voorkomt dat gebruikers voor ieder apparaat afzonderlijk een nieuwe passkey moeten registreren.

Voor dit profiel is het meestal verstandig om Enforce attestation uitgeschakeld te laten. Gesynchroniseerde passkeys ondersteunen attestation doorgaans niet. Als attestation wordt afgedwongen, kunnen gebruikers mogelijk geen passkey registreren via Apple iCloud Keychain, Google Password Manager of vergelijkbare providers.

- Microsoft Authenticator
- Apple iCloud Keychain
- Google Password Manager
- sommige Windows Hello for Business scenario's

Als je attestation afdwingt kan het gebeuren dat gebruikers hun passkey niet meer kunnen registreren.



Het passkey profiel stel je als volgt in:

Edit passkey profile



Certain combinations of these settings could target passkeys that may not exist. This can prevent your users from registering and signing in with a passkey.

[View compatibility documentation](#)

Name *

Enforce attestation ☐

Passkey types *

Target specific AAGUIDs

☒ Device-bound

☒ Synced

8.5 HighProfile profile

Dit profiel is bedoeld voor gebruikers met een verhoogd risicoprofiel, bijvoorbeeld gebruikers die toegang hebben tot gevoelige bedrijfsdata, financiële informatie of kritieke applicaties. Voor deze groep is een device-bound passkey in Microsoft Authenticator een goede keuze. De passkey blijft gekoppeld aan het toestel waarop deze is aangemaakt en wordt niet gesynchroniseerd via een persoonlijk Apple- of Google-account. Dit biedt meer controle dan een algemene gesynchroniseerde passkey, maar vraagt wel iets meer begeleiding bij de inrichting.

Edit passkey profile



Certain combinations of these settings could target passkeys that may not exist. This can prevent your users from registering and signing in with a passkey.

[View compatibility documentation](#)

Name *

Enforce attestation ☐

Passkey types *

Target specific AAGUIDs

Behavior *

☒ Allow

☐ Block

Model/Provider AAGUIDs

Add AAGUID

Microsoft Authenticator for Android

Microsoft Authenticator for iOS



8.6 Admin Accounts profile

Dit profiel is bedoeld voor accounts met beheerrollen binnen Microsoft 365 of Microsoft Entra ID. Voor deze groep is een device-bound FIDO2-beveiligingssleutel, zoals een YubiKey, de meest geschikte keuze. Door Enforce attestation in te schakelen en alleen goedgekeurde AAGUIDs toe te staan, kan worden afgedwongen dat uitsluitend vooraf goedgekeurde hardwaretokens worden geregistreerd.

Een goede plek om de AAGUID te vinden is via:

<https://passkeydeveloper.github.io/passkey-authenticator-aaguids/explorer/>

<https://support.yubico.com/s/article/YubiKey-hardware-FIDO2-AAGUIDs>

Wanneer Enforce attestation is ingeschakeld, controleert Microsoft Entra ID of de authenticator een geldige attestation-verklaring levert en of de authenticator voldoet aan de ingestelde beperkingen. Dit verhoogt de zekerheid over het gebruikte type beveiligingssleutel, maar maakt de inrichting minder flexibel. Gebruik deze instelling daarom vooral voor beheerdersaccounts en andere zeer gevoelige accounts.

Dan krijg je een strenger beleid:

- ✓ Alleen authenticators die een geldig attestation certificaat leveren mogen registreren.

Maar mogelijk:

- ✗ Sommige Microsoft Authenticator-passkeys registreren niet meer.
- ✗ Toekomstige wijzigingen in Android/iOS privacygedrag kunnen problemen geven.

Dit profiel is bedoeld voor accounts met beheer rollen binnen de Microsoft 365 / Entra omgeving.

Edit passkey profile



Certain combinations of these settings could target passkeys that may not exist. This can prevent your users from registering and signing in with a passkey.

[View compatibility documentation](#)

Name *

Enforce attestation ⓘ ☒

Passkey types *

Target specific AAGUIDs ⓘ ☒

Behavior ⓘ * ☒ Allow
☐ Block

Model/Provider AAGUIDs ⓘ

+ Add AAGUID

2fc0579f-8113-47ea-b116-bb5a8db9202a





8.7 Profielen koppelen

Onder de Passkey settings kan je de profielen koppelen aan security groepen. In dit geval zijn er 2 groepen aangemaakt SG-Passkey-HighProfile en SG-Passkey-Admin. Die zijn respectievelijk toegewezen aan het juiste Passkey profiel.

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods

Passkey profiles are now available. Your previous passkey settings have been moved into the default passkey profile. Up to 10 passkey profiles are supported at th

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey pr

Enable and target Configure

Enable ☒ On

Include Exclude

+ Add target

Name	Type	Passkey profiles	
All users	Group	Default passkey profile	
SG-Passkey-HighProfile	Group	Highprofile Profile	
SG-Passkey-Admin	Group	Admin Accounts	

9. Passkeys afdwingen met Conditional Access

Wanneer passkeys correct zijn ingericht en gebruikers succesvol kunnen aanmelden, kan Conditional Access worden gebruikt om phishing-resistent MFA af te dwingen. Gebruik hiervoor Authentication Strengths en kies bijvoorbeeld de ingebouwde sterkte Phishing-resistant MFA strength of een custom authentication strength. Activeer dit beleid pas nadat de betreffende gebruikers een werkende passkey of FIDO2-beveiligingssleutel hebben geregistreerd. Sluit daarnaast break-glass accounts uit om tenant-lockout te voorkomen.



10. Uitgebreide conclusie en advies per gebruikerstype

Microsoft adviseert om phishingbestendige, wachtwoordloze authenticatie gefaseerd in te voeren op basis van gebruikersprofielen. Niet iedere gebruiker heeft hetzelfde risico, dezelfde technische vaardigheid of dezelfde beheerlast. Daarom is één generiek passkey-beleid voor de volledige organisatie meestal niet ideaal. Een inrichting met meerdere passkey-profielen sluit beter aan op de standaardaanpak van Microsoft, waarbij gebruikers worden ingedeeld in persona's en waarbij passkey-profielen per groep kunnen worden toegepast.

10.1 Standaardgebruikers

Voor standaardgebruikers is een gesynchroniseerde passkey meestal de beste keuze. Denk hierbij aan gebruikers zonder beheerrollen en zonder structurele toegang tot zeer gevoelige systemen. Een passkey via Apple iCloud Keychain of Google Password Manager is gebruiksvriendelijk, snel te registreren en eenvoudig te herstellen wanneer een gebruiker een nieuw toestel krijgt. Dit verlaagt de servicedeskbelasting en versnelt de adoptie. Omdat gesynchroniseerde passkeys doorgaans geen attestatie ondersteunen, moet Enforce attestatie voor deze groep uitgeschakeld blijven.

10.2 Gebruikers met verhoogd risico

Voor gebruikers met toegang tot gevoelige data, financiële processen, HR-informatie, klantgegevens of bedrijfskritische applicaties is een device-bound passkey in Microsoft Authenticator aan te raden. Deze passkey blijft gekoppeld aan het toestel waarop deze is aangemaakt en wordt niet breed gesynchroniseerd via een persoonlijk cloudaccount. Dit biedt een betere balans tussen veiligheid en gebruiksgemak. Voor deze groep kan het profiel worden beperkt tot de AAGUIDs van Microsoft Authenticator, zodat gebruikers niet willekeurig andere passkey-providers kunnen registreren.

10.3 Beheerders en zeer gevoelige accounts

Voor beheerdersaccounts, privileged roles en andere zeer gevoelige accounts is een hardwarematige FIDO2-beveiligingssleutel de meest passende keuze. Hierbij kan Enforce attestatie worden ingeschakeld en kunnen alleen goedgekeurde AAGUIDs worden toegestaan. Dit geeft de organisatie meer zekerheid over het gebruikte type authenticator. Deze aanpak is strenger en minder flexibel, maar past bij accounts waarbij misbruik direct grote impact kan hebben op de omgeving.

10.4 Eindadvies

De aanbevolen inrichting is daarom: gesynchroniseerde passkeys voor standaardgebruikers, Microsoft Authenticator-passkeys voor gebruikers met verhoogd risico en hardwarematige FIDO2-beveiligingssleutels voor beheerdersaccounts. Dwing phishing-resistent MFA pas af met Conditional Access nadat de registratie succesvol is getest en alle betrokken gebruikers beschikken over een werkende methode. Houd altijd minimaal één of meer break-glass accounts buiten dit beleid om te voorkomen dat de organisatie zichzelf buitensluit.