Solid Partners

Wachtwoordsleutels (Passkeys) voor Microsoft 365

Handleiding

solidpartners.nl

1. Inhoudsopgave

2. Inleiding

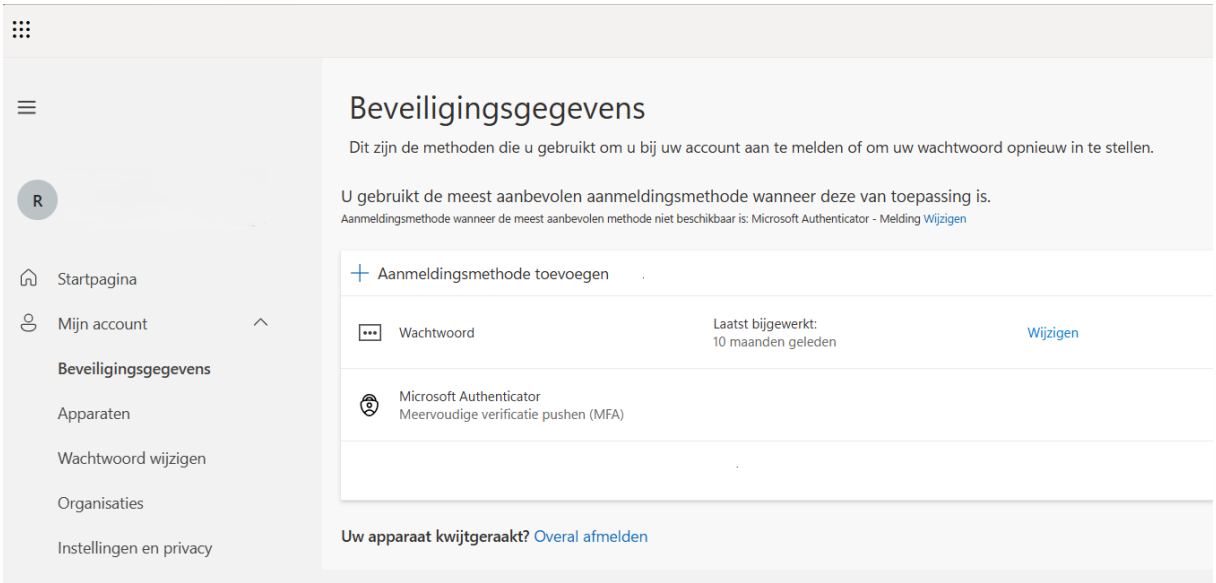
Deze handleiding beschrijft hoe gebruikers een wachtwoordsleutel, ook wel passkey genoemd, kunnen aanmaken en gebruiken voor Microsoft 365. Daarnaast bevat dit document beheerdersinstructies voor het inschakelen, configureren en afdwingen van passkeys binnen Microsoft Entra ID en Conditional Access.
Passkeys zijn phishingbestendige aanmeldmethoden op basis van FIDO2. Ze vervangen zwakkere methoden, zoals wachtwoorden, sms-codes en telefonische verificatie, door een methode waarbij een privésleutel 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

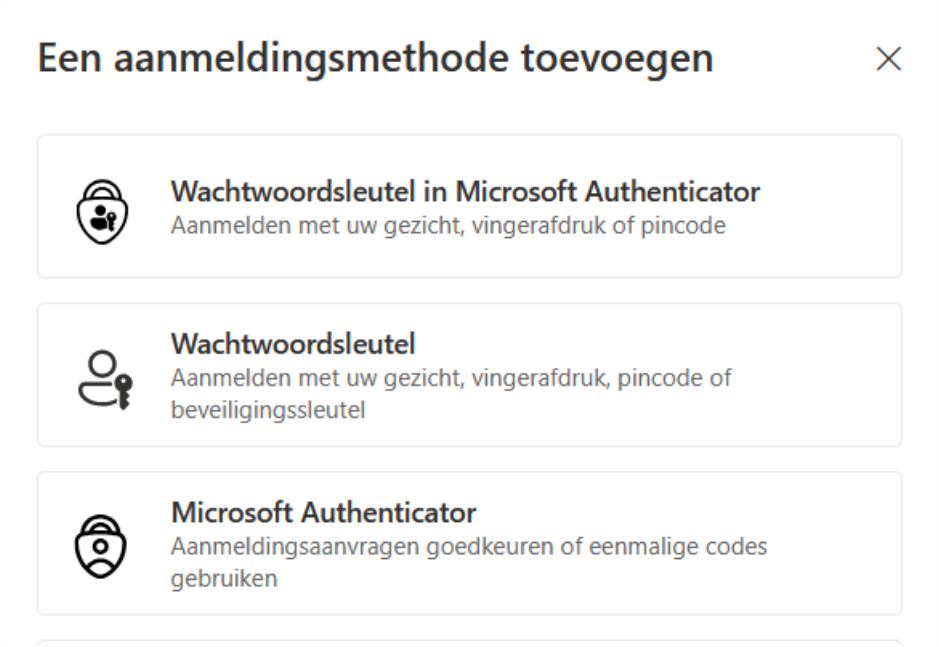
Benodigdheden

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

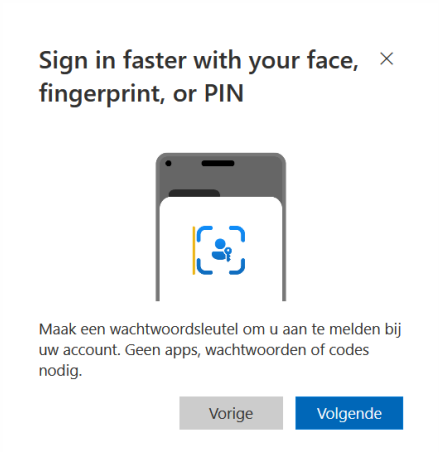
4. Wachtwoordsleutel toevoegen via beveiligingsgegevens (standaard gebruiker)



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.



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.



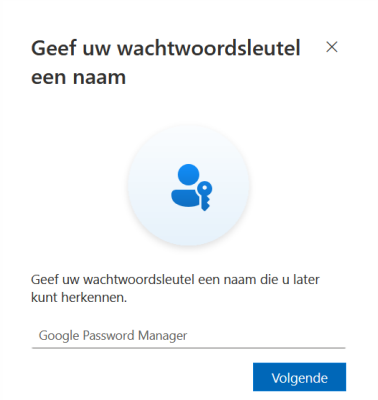
Klik bij de opslaglocatie op Wijzigen.

Selecteer iPhone-, iPad- of Android-apparaat

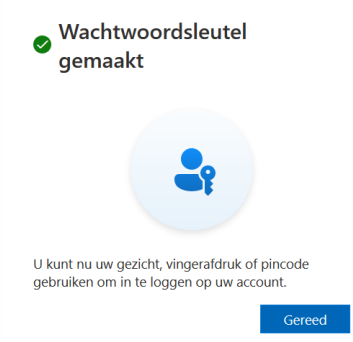
Er verschijnt een QR-code op het scherm. Scan deze QR-code met de camera-app van de telefoon en open de koppeling die wordt weergegeven.

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)

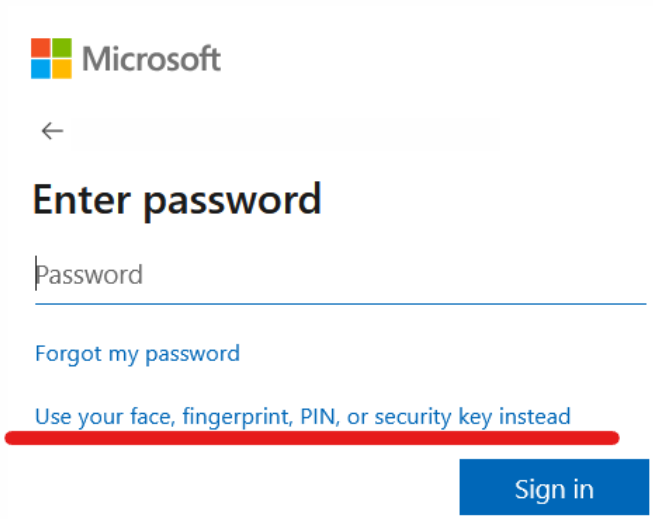


Na afronding verschijnt een bevestiging dat de wachtwoordsleutel is aangemaakt.



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 sequirity key instead".



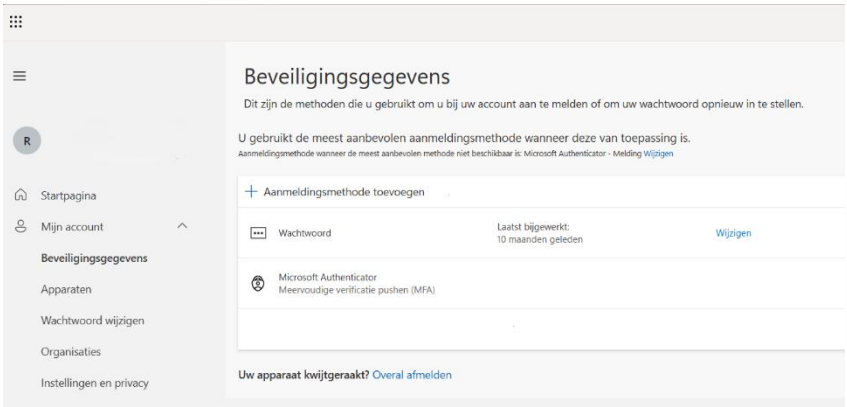
Kies vervolgwens voor iPhone-, iPad,- of Android-apparaat.

Er wordt nu een QR code getoond op het scherm:

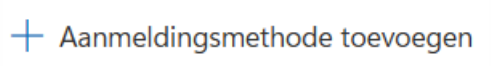
Scan de QR code met je camera.
Klik op de link om vervolgens in te loggen bij Microsoft 365.

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

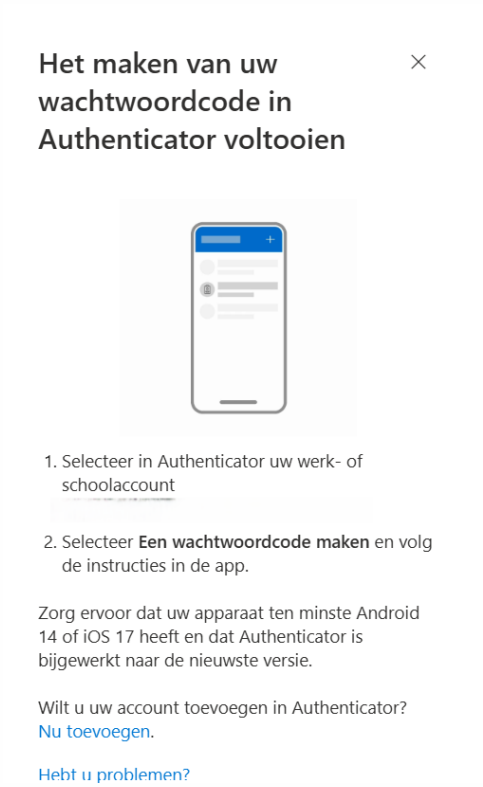


De volgende stap is om een extra aanmeldingsmethode toe te voegen.
Dit doe je door op het plus je te klikken:



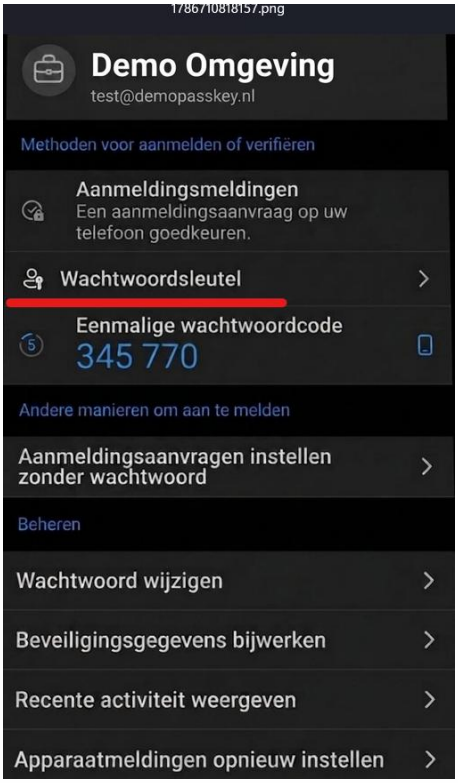
Je krijgt nu een menu met allerlei verschillende aanmeldingsmethodes.
We selecteren de bovenste optie : “Wachtwoordsleutel in Microsoft Authenticator”.

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



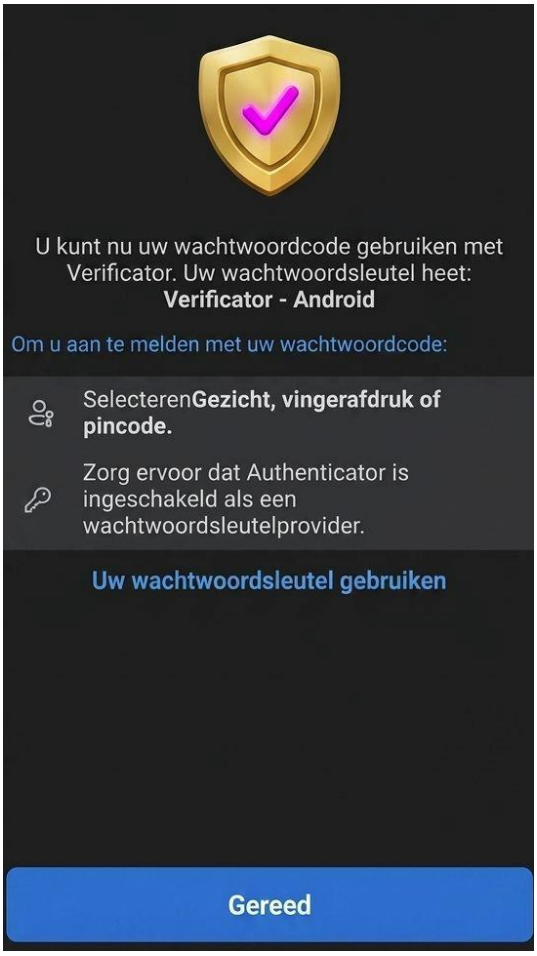
Op de telefoon zie onder de Microsoft Authenticator je account terug van de Microsoft omgeving.
Door hierop te klikken ga je naar de informatie hiervan.

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.

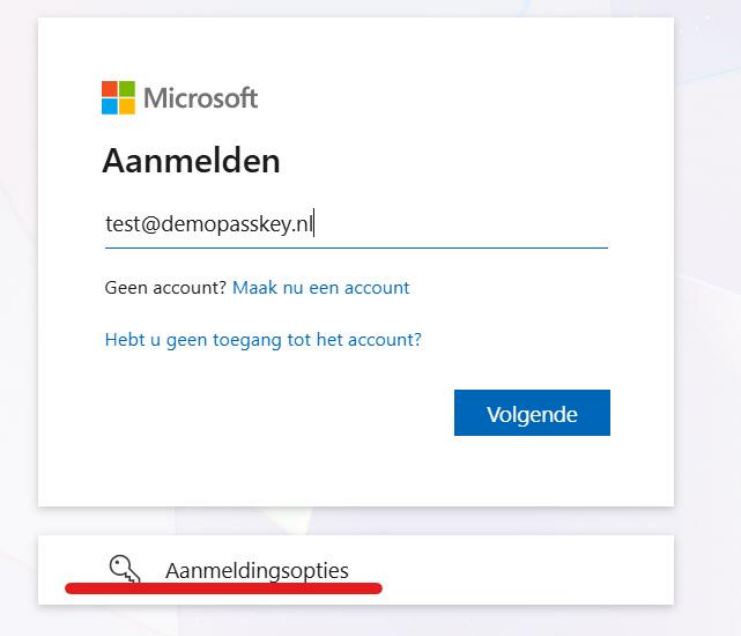
Je wachtwoord sleutel is nu aangemaakt op je telefoon.
Als je op gereed klikt, is dit proces afgerond.



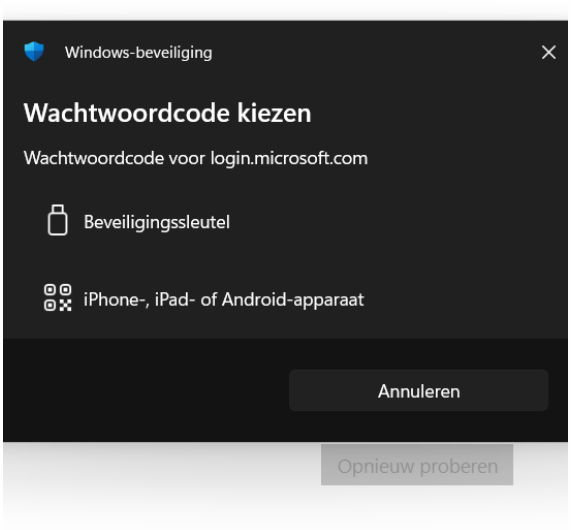
In Windows krijg je als je nu verder gaat een melding dat er een wachtwoordsleutel is aangemaakt.

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

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



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



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

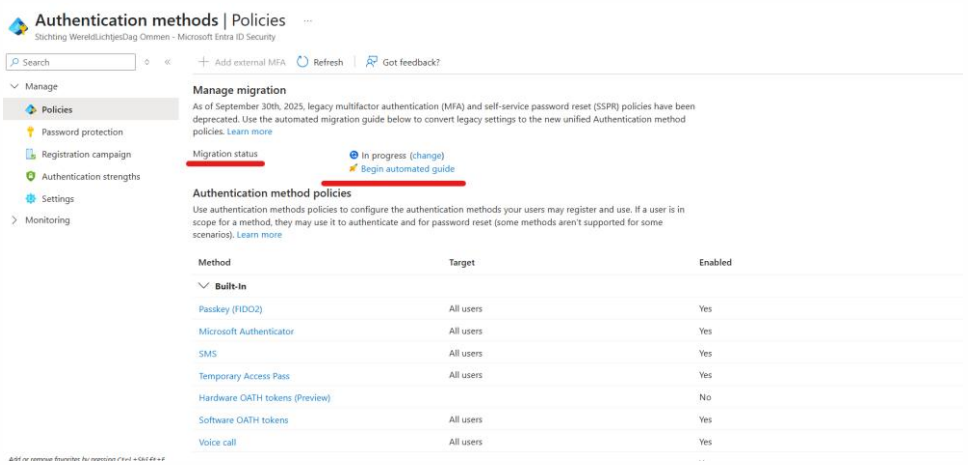
8.1 Authenticatiemigratie afronden

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.

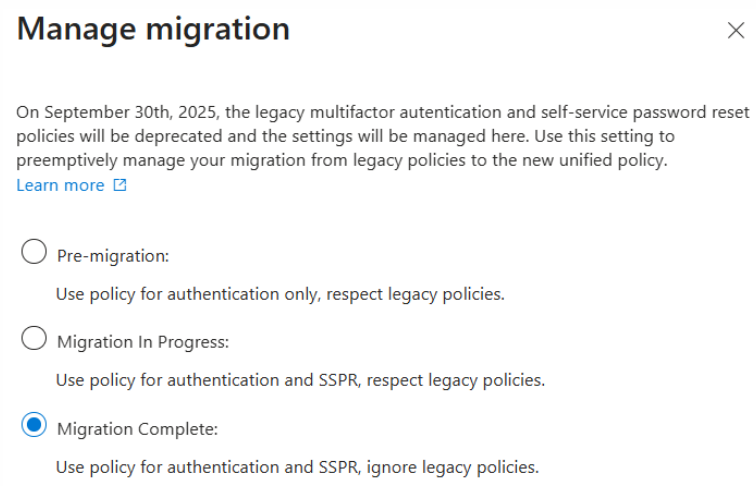
Je vindt dit onder :
https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/AdminAuthMethods

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.

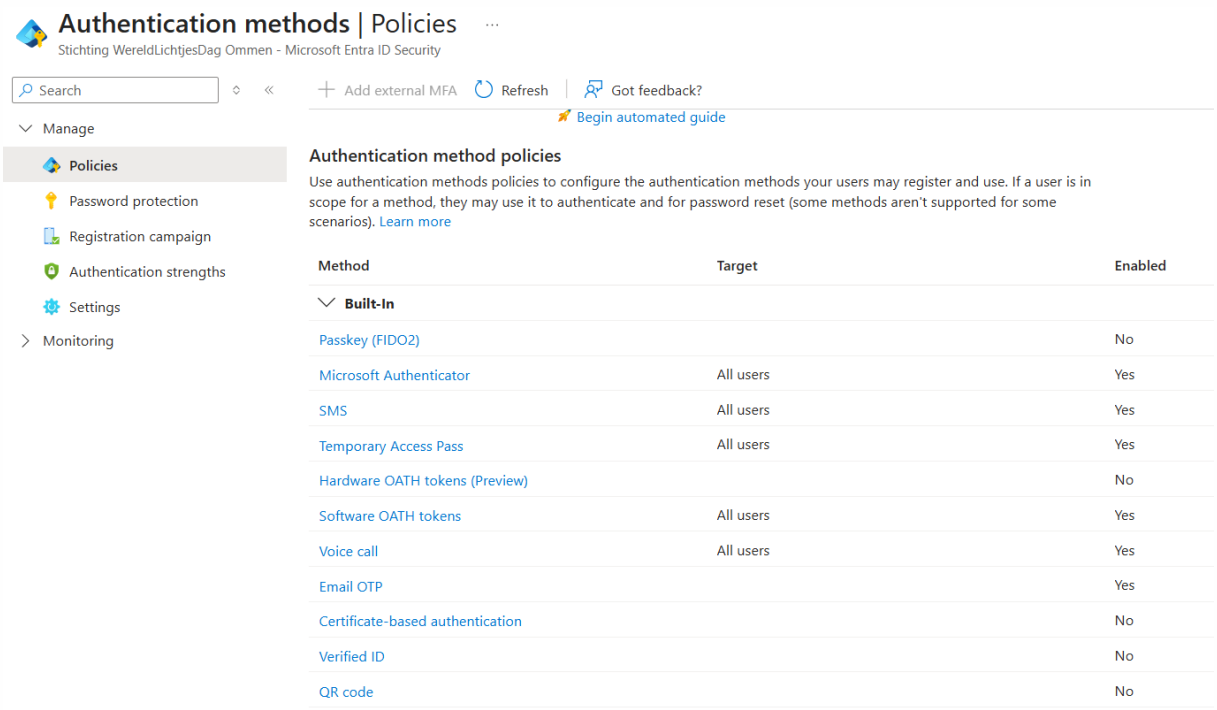


Bij de migratie klik je op Migration Complete om de migratie af te ronden.

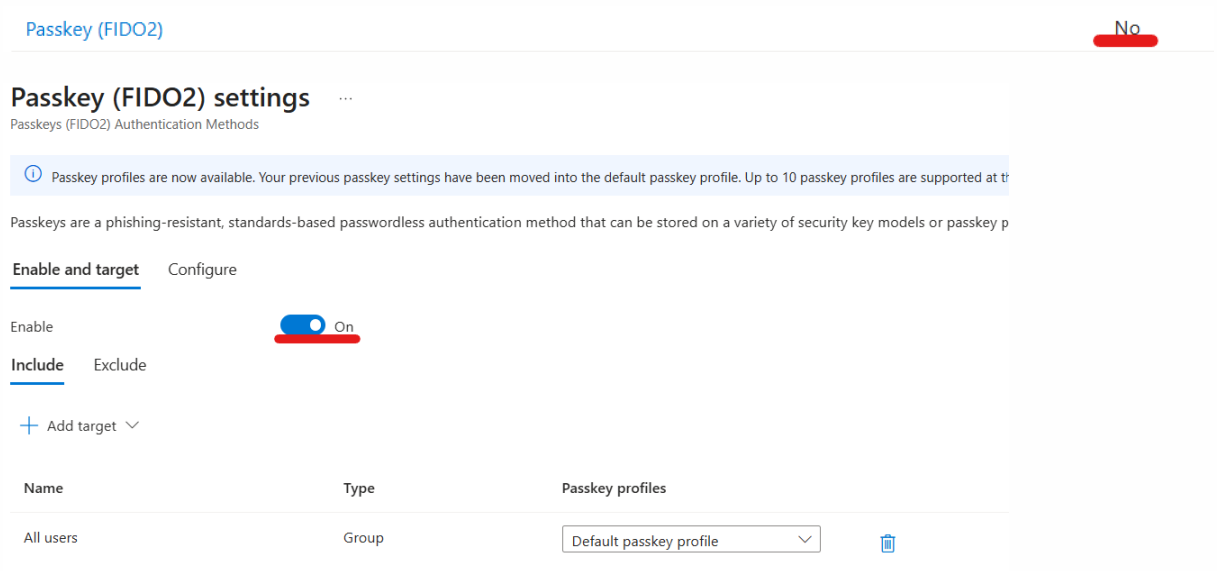


8.2 Passkey (FIDO2) inschakelen

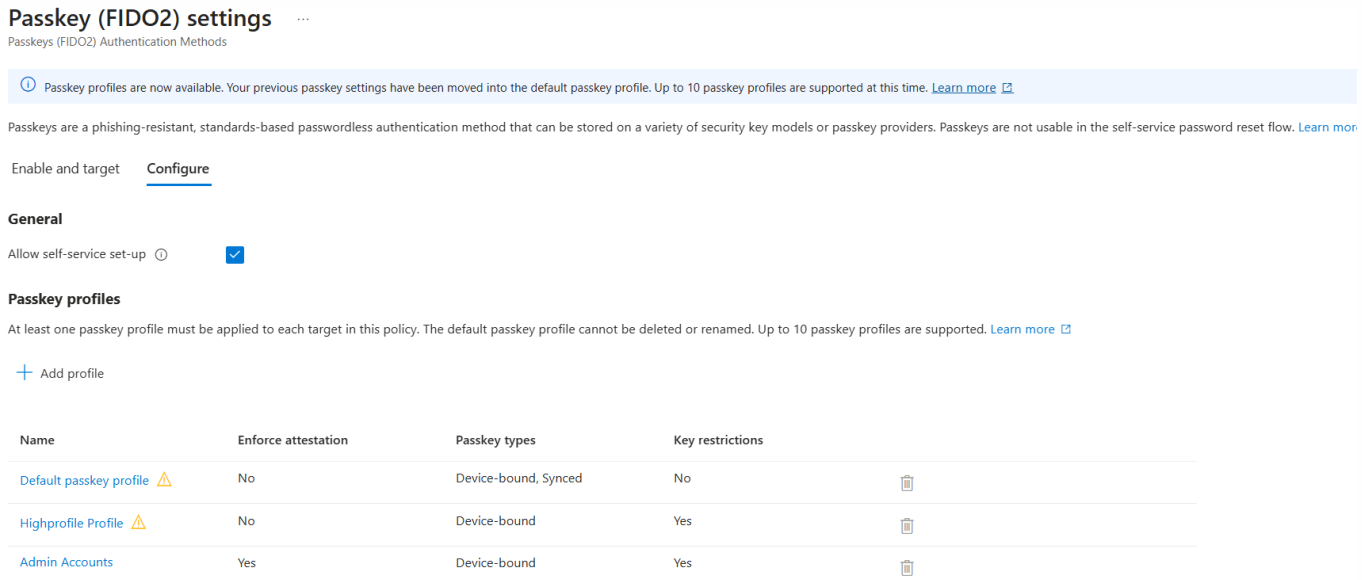
Ga in Entra ID naar Authentication Methods en open Passkey (FIDO2). Zet deze methode op Enabled. Open daarna het default passkey profile of maak een nieuw profiel aan wanneer er nog geen profiel bestaat.



Zet deze optie op Enabled



8.3 Profielen



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

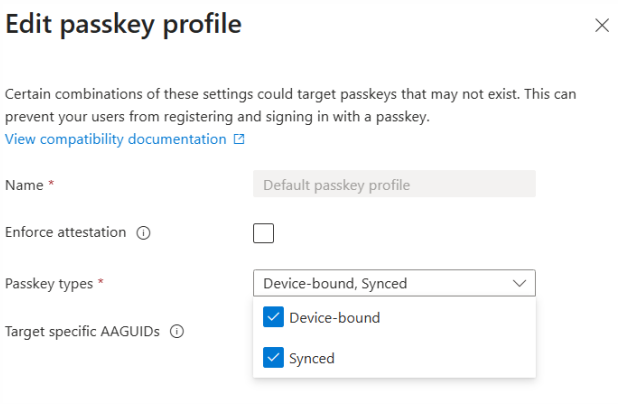
Dit profiel is bedoeld voor standaardgebruikers met reguliere rechten in de Microsoft 365-omgeving. Voor deze groep is een gesynchroniseerde passkey via Apple iCloud Keychain of Google Password Manager meestal de meest gebruiksvriendelijke keuze. De passkey wordt versleuteld opgeslagen en via de passkey-provider 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

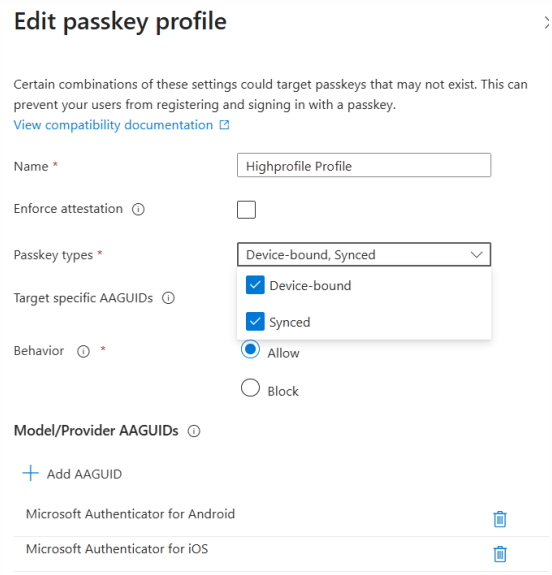
Als je attestation afdwingt kan het gebeuren dat gebruikers hun passkey niet meer kunnen registreren.

Het passkey profiel stel je als volgt in:



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.



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/

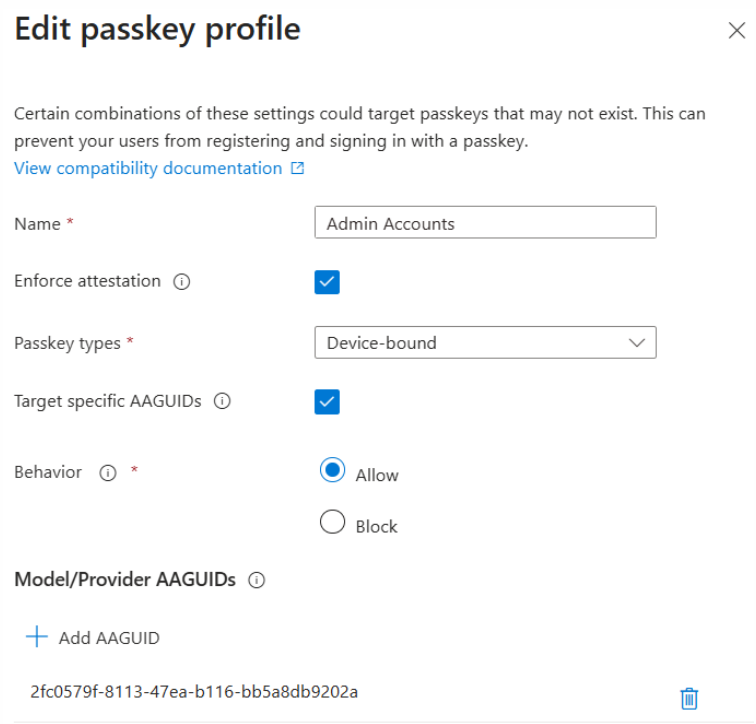
https://support.yubico.com/s/article/YubiKey-hardware-FIDO2-AAGUIDs

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.

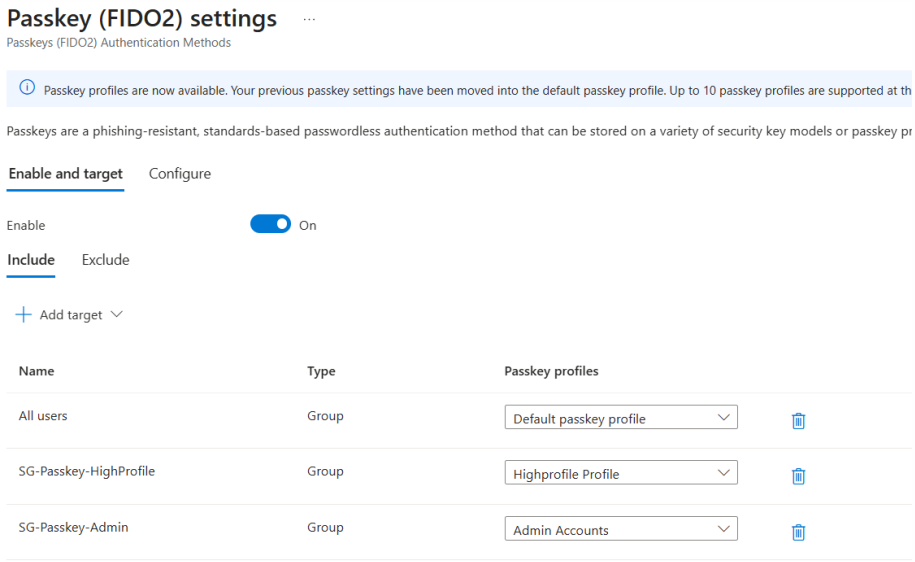
Maar mogelijk:
❌ Sommige Microsoft Authenticator-passkeys registreren niet meer.
❌ Toekomstige wijzigingen in Android/iOS privacygedrag kunnen problemen geven.

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



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.



9. Passkeys afdwingen met Conditional Access

Wanneer passkeys correct zijn ingericht en gebruikers succesvol kunnen aanmelden, kan Conditional Access worden gebruikt om phishing-resistant 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 attestation ondersteunen, moet Enforce attestation 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 attestation 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-resistant 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.