

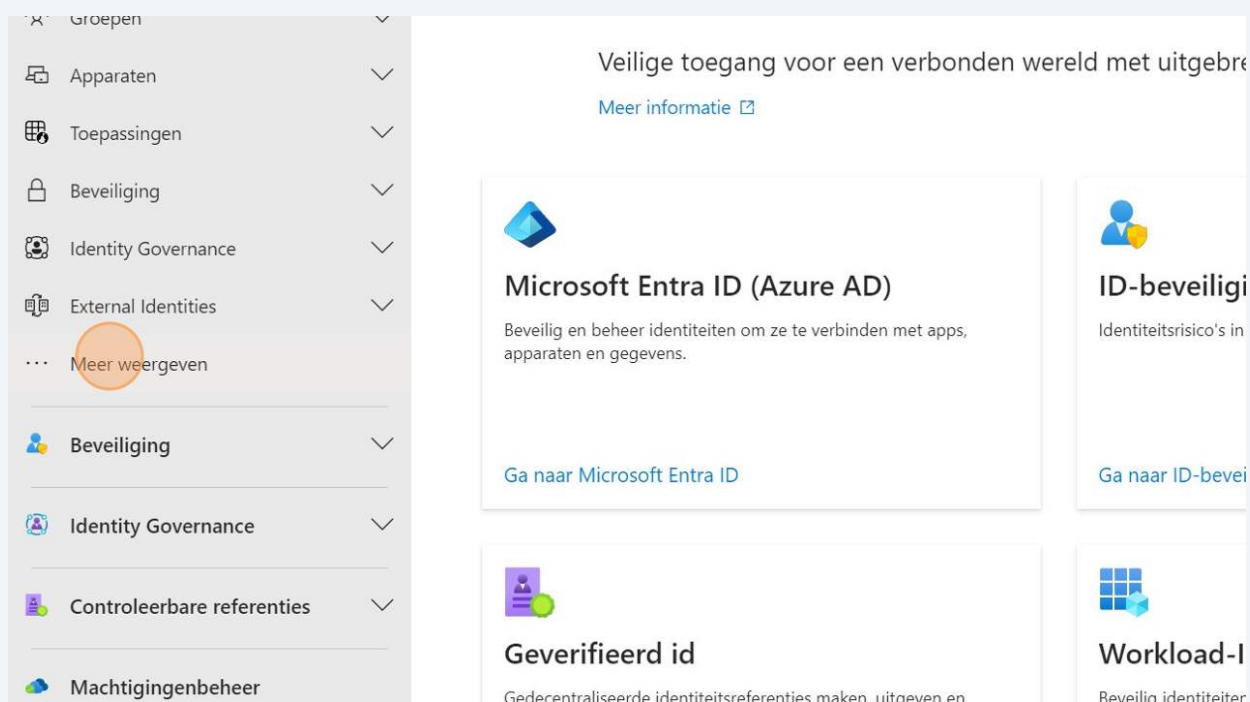
Stel Multi-Factor Authenticatie in met Voorwaardelijke toegang (M365 A3+)



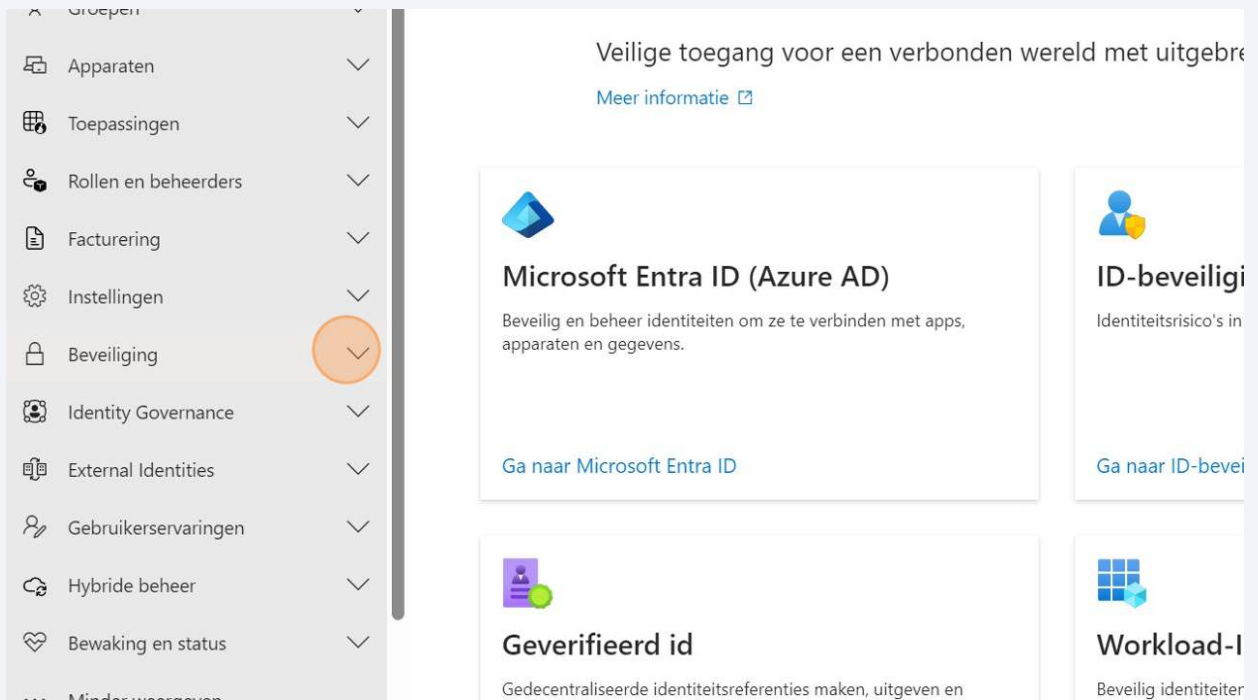
Deze handleiding bevat stapsgewijze instructies voor het instellen van Multi-Factor Authenticatie met voorwaardelijke toegang. We gebruiken de nieuwe Verificatiemethode interface alsook de Voorwaardelijke toegang. Er zijn nog veel meer instellingen mogelijk, maar we beperken ons in deze handleiding tot de basis om dit beleid te activeren voor leerkrachten.

1 Surf naar entra.microsoft.com

Klik in de grijze menubalk op "Meer weergeven"



2 Open het menu Beveiliging



The screenshot shows the Microsoft Entra ID dashboard. On the left, a navigation menu is open, with 'Beveiliging' (Security) highlighted by an orange circle. The main content area displays a header with the text 'Veilige toegang voor een verbonden wereld met uitgebreide' and a link 'Meer informatie'. Below the header, there are four tiles: 'Microsoft Entra ID (Azure AD)', 'ID-beveiliging', 'Geverifieerd id', and 'Workload-Id'. Each tile has a brief description and a link to go to the respective page.

Veilige toegang voor een verbonden wereld met uitgebreide

[Meer informatie](#)

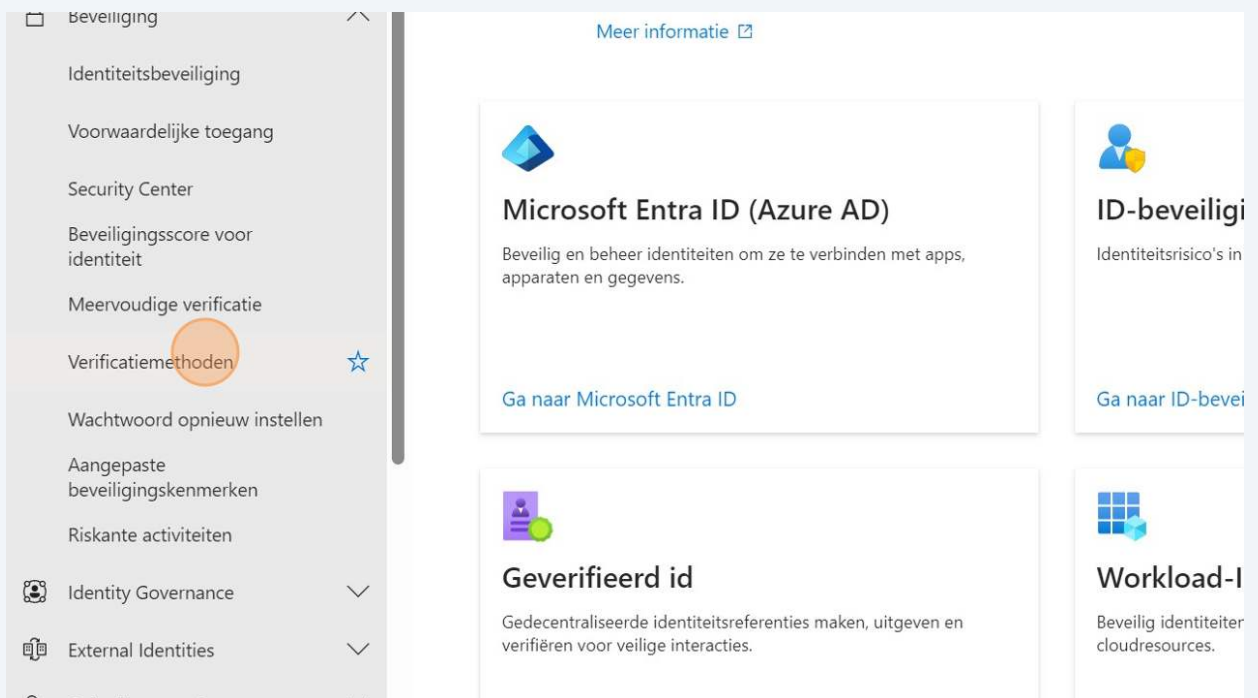
Microsoft Entra ID (Azure AD)
Beveilig en beheer identiteiten om ze te verbinden met apps, apparaten en gegevens.
[Ga naar Microsoft Entra ID](#)

ID-beveiliging
Identiteitsrisico's in
[Ga naar ID-beveiliging](#)

Geverifieerd id
Gedecentraliseerde identiteitsreferenties maken, uitgeven en
[Ga naar Geverifieerd id](#)

Workload-Id
Beveilig identiteiter
[Ga naar Workload-Id](#)

3 Klik op "Verificatiemethoden" om de verificatiemethoden te activeren



The screenshot shows the Microsoft Entra ID dashboard with the 'Beveiliging' (Security) menu expanded. The 'Verificatiemethoden' (Authentication methods) option is highlighted by an orange circle. The main content area is the same as in the previous screenshot, showing the header and the four tiles for Microsoft Entra ID, ID-beveiliging, Geverifieerd id, and Workload-Id.

Beveiliging

- Identiteitsbeveiliging
- Voorwaardelijke toegang
- Security Center
- Beveiligingsscore voor identiteit
- Meervoudige verificatie
- Verificatiemethoden** [★](#)
- Wachtwoord opnieuw instellen
- Aangepaste beveiligingskenmerken
- Risikante activiteiten
- Identity Governance
- External Identities

Meer informatie

Microsoft Entra ID (Azure AD)
Beveilig en beheer identiteiten om ze te verbinden met apps, apparaten en gegevens.
[Ga naar Microsoft Entra ID](#)

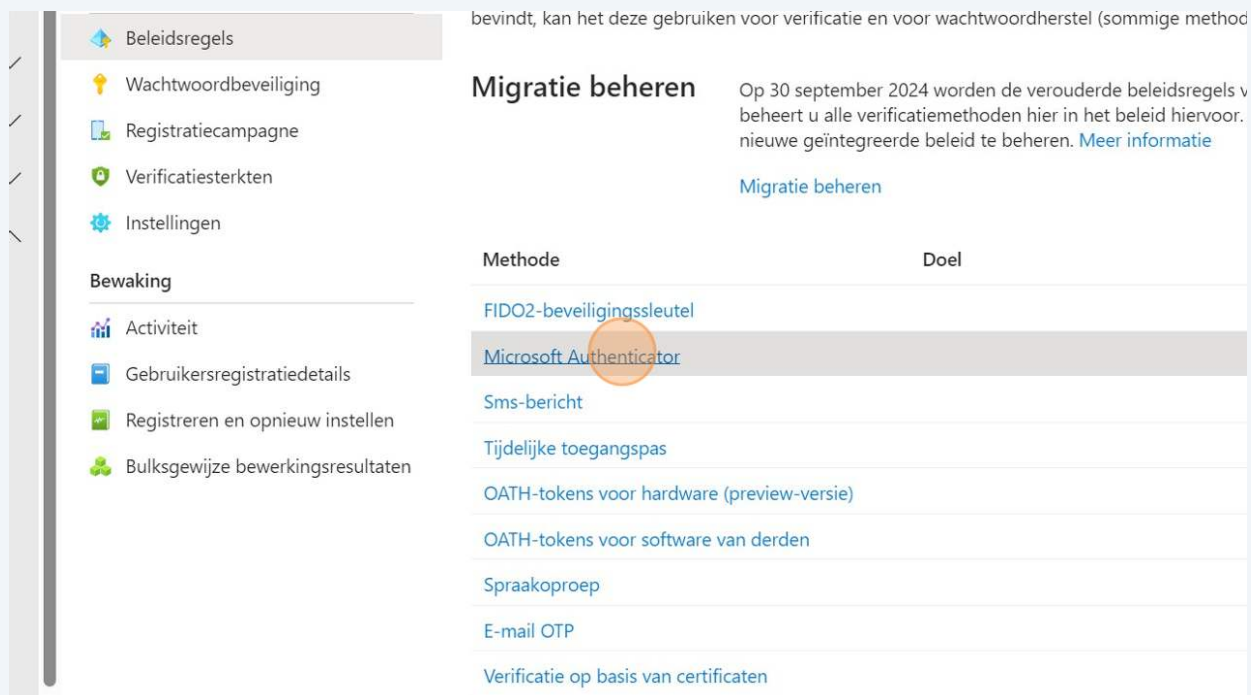
ID-beveiliging
Identiteitsrisico's in
[Ga naar ID-beveiliging](#)

Geverifieerd id
Gedecentraliseerde identiteitsreferenties maken, uitgeven en verifiëren voor veilige interacties.
[Ga naar Geverifieerd id](#)

Workload-Id
Beveilig identiteiter cloudresources.
[Ga naar Workload-Id](#)

4

Klik op de authenticatiemethode (vb: Microsoft Authenticator) om deze te activeren.



bevindt, kan het deze gebruiken voor verificatie en voor wachtwoordherstel (sommige methoden)

Migratie beheren

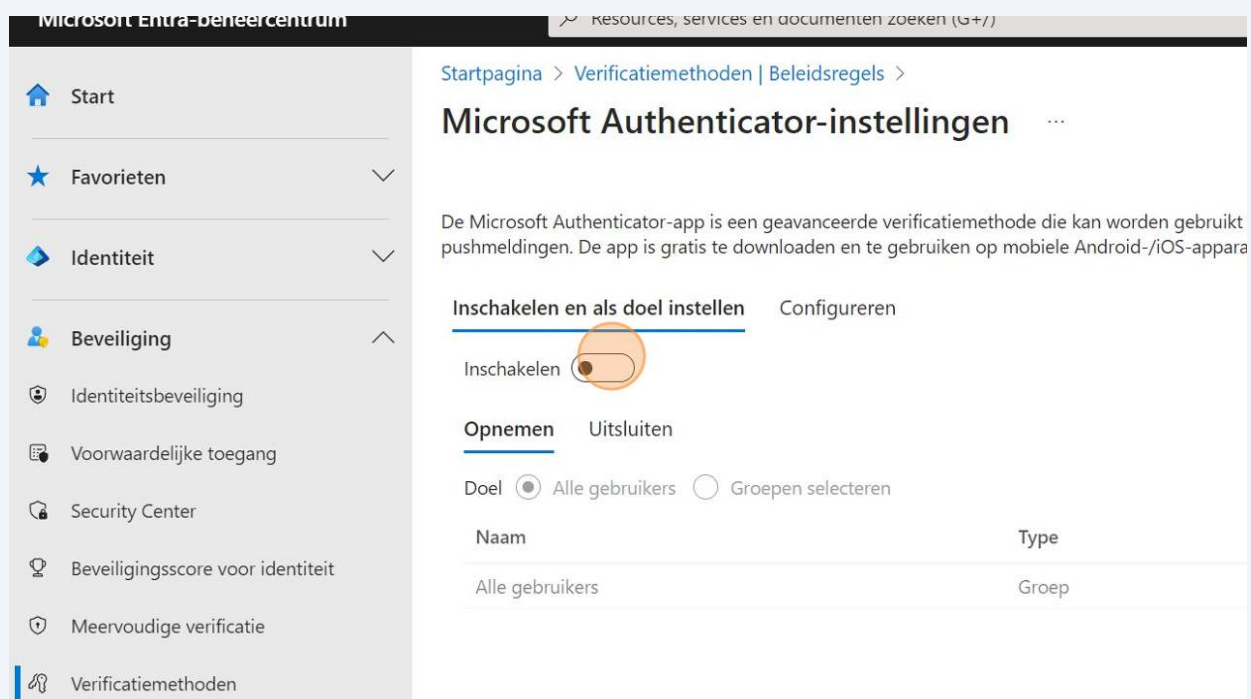
Op 30 september 2024 worden de verouderde beleidsregels voor verificatiemethoden beheert u alle verificatiemethoden hier in het beleid hiervoor. [Meer informatie](#)

[Migratie beheren](#)

Methode	Doel
FIDO2-beveiligingssleutel	
Microsoft Authenticator	
Sms-bericht	
Tijdelijke toegangspas	
OATH-tokens voor hardware (preview-versie)	
OATH-tokens voor software van derden	
Sprakoproep	
E-mail OTP	
Verificatie op basis van certificaten	

5

Schakel de methode in en kies welke groep gebruikers deze mag gebruiken.



Microsoft Entra-beheercentrum Resources, services en documenten zoeken (G+/)

Startpagina > Verificatiemethoden | Beleidsregels >

Microsoft Authenticator-instellingen

De Microsoft Authenticator-app is een geavanceerde verificatiemethode die kan worden gebruikt voor pushmeldingen. De app is gratis te downloaden en te gebruiken op mobiele Android-/iOS-apparaten.

Inschakelen en als doel instellen Configureren

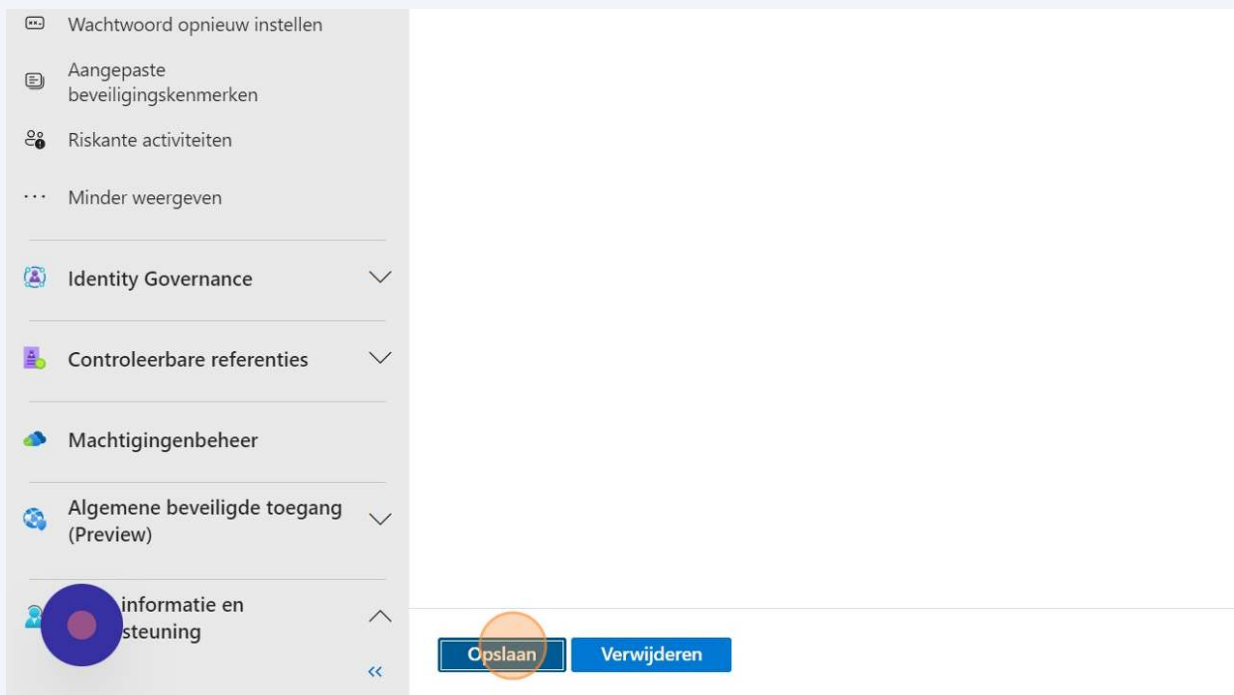
Inschakelen ☒

Opnemen Uitsluiten

Doel ☒ Alle gebruikers ☐ Groepen selecteren

Naam	Type
Alle gebruikers	Groep

6 Bevestig deze configuratie door te klikken op "Opslaan"



Wachtwoord opnieuw instellen

Aangepaste beveiligingskenmerken

Riskante activiteiten

Minder weergeven

Identity Governance

Controleerbare referenties

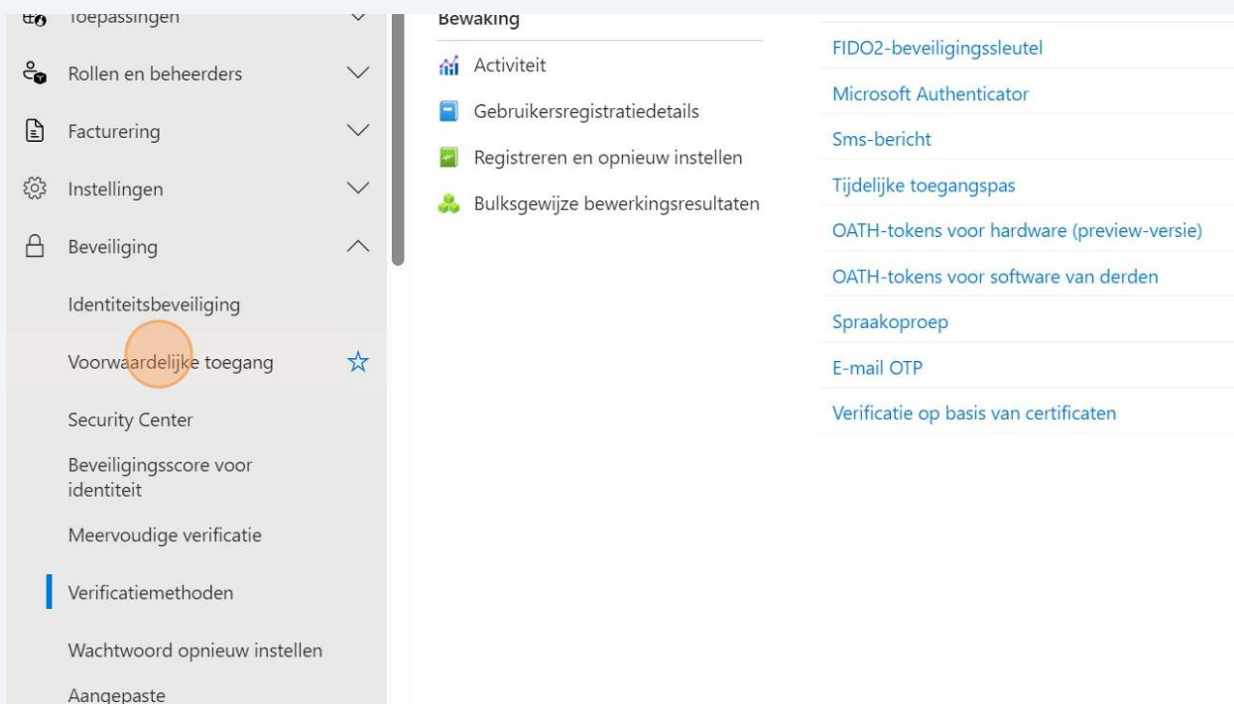
Machtigingenbeheer

Algemene beveiligde toegang (Preview)

Informatie en steuning

Opslaan Verwijderen

7 Klik in het grijze menu, onder Beveiliging op "Voorwaardelijke toegang"



Toepassingen

Rollen en beheerders

Facturering

Instellingen

Beveiliging

Identiteitsbeveiliging

Voorwaardelijke toegang

Security Center

Beveiligingsscore voor identiteit

Meervoudige verificatie

Verificatiemethoden

Wachtwoord opnieuw instellen

Aangepaste

Bewaking

Activiteit

Gebruikersregistratiedetails

Registreren en opnieuw instellen

Bulkgewijze bewerkingsresultaten

FIDO2-beveiligingssleutel

Microsoft Authenticator

Sms-bericht

Tijdelijke toegangspas

OATH-tokens voor hardware (preview-versie)

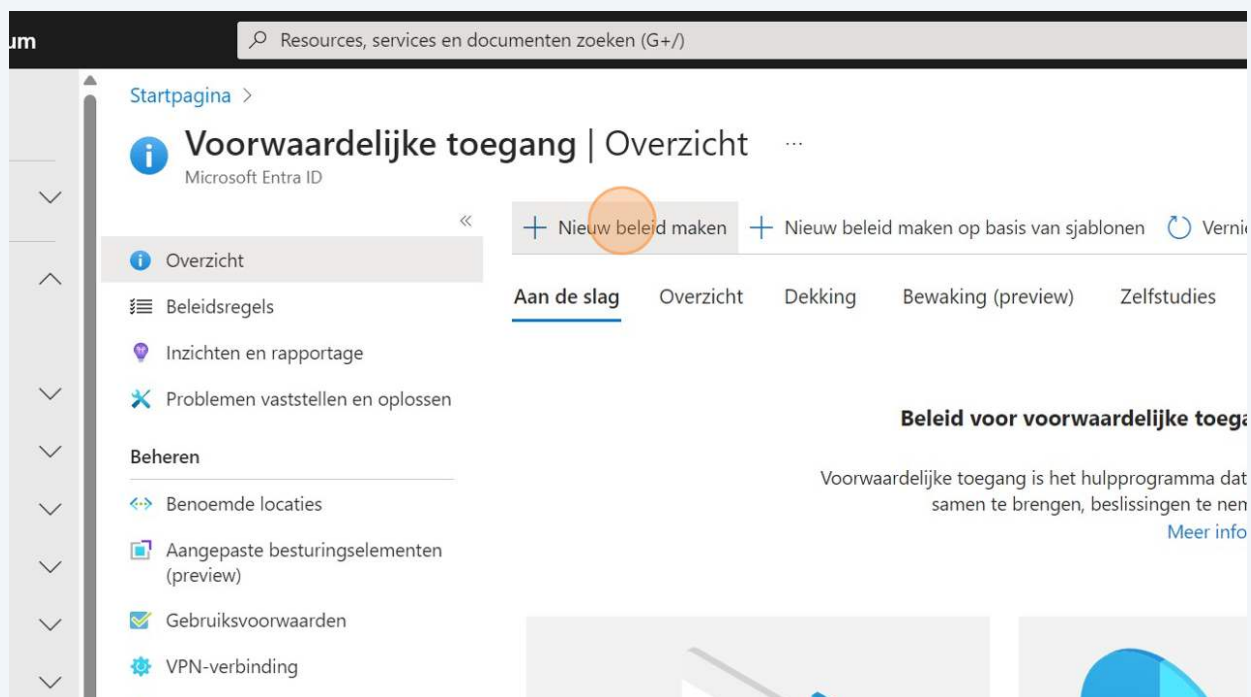
OATH-tokens voor software van derden

Spraakoproep

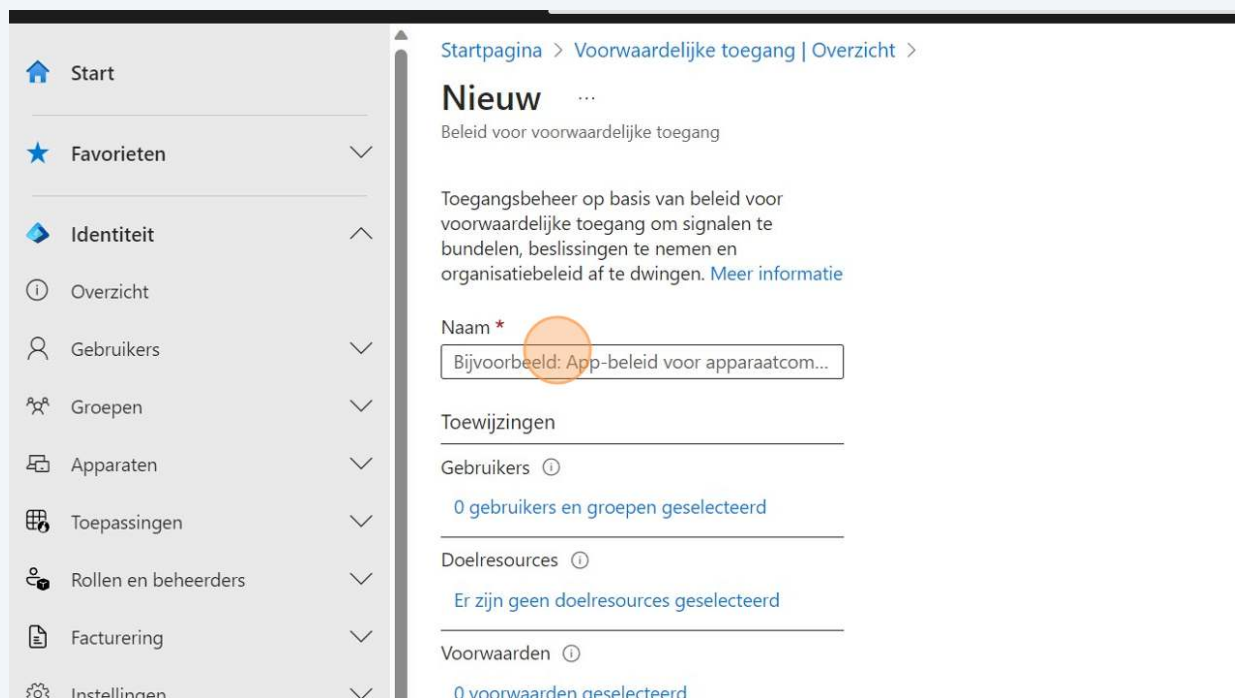
E-mail OTP

Verificatie op basis van certificaten

8 Klik op "Nieuw beleid maken"



9 Geef een naam op voor het beleid (vb: Multi-Factor leerkrachten).



10

Klik op de blauwe tekst onder gebruikers om de groep gebruikers te kiezen waarop dit beleid wordt toegepast.

favorieten

Identiteit

Overzicht

Gebruikers

Groepen

Apparaten

Toepassingen

Rollen en beheerders

Facturering

Instellingen

Beveiliging

Identiteitsbeveiliging

Toegangsbeheer op basis van beleid voor voorwaardelijke toegang om signalen te bundelen, beslissingen te nemen en organisatiebeleid af te dwingen. [Meer informatie](#)

Naam *

MFA Leerkrachten

Toewijzingen

Gebruikers ①

0 gebruikers en groepen geselecteerd

Doelresources ①

Er zijn geen doelresources geselecteerd

Voorwaarden ①

0 voorwaarden geselecteerd

Besturingselementen voor toegang

Verlenen ①

11

Je kan groepen "opnemen" maar ook gebruikers binnen deze groepen vrijstellen via "uitsluiten". Zo kan je tijdelijk één groep gebruikers vrijstellen van dit beleid bij problemen.

achten

gebruikers opgenomen

doelresources geselecteerd

den geselecteerd

ementen voor toegang

selementen geselecteerd

selementen geselecteerd

Opnemen Uitsluiten

☐ Geen

☐ Alle gebruikers

☒ Gebruikers en groepen selecteren

☐ Gasten of externe gebruikers ①

☐ Directory-rollen ①

☒ Gebruikers en groepen

Selecteren

1 groep

LE Leerkrachten

12 Selecteer onder "Doelresources" Alle cloud-apps.

Toegangsbeheer op basis van beleid voor voorwaardelijke toegang om signalen te bundelen, beslissingen te nemen en organisatiebeleid af te dwingen. [Meer informatie](#)

Naam *
MFA Leerkrachten ✓

Toewijzingen

Gebruikers ⓘ
[Specifieke gebruikers opgenomen](#)

Doelresources ⓘ
Er zijn geen doelresources geselecteerd

Voorwaarden ⓘ
[0 voorwaarden geselecteerd](#)

Besturingselementen voor toegang

Verlenen ⓘ

Toegang beheren op basis van alle of specifiek netwerktoegangsverkeer, cloud-apps of acties. [Meer informatie](#)

Selecteren waarop dit beleid van toepassing is
Cloud-apps

Opnemen Uitsluiten

☐ Geen
☒ Alle cloud-apps
☐ Apps selecteren

13 Klik op de blauwe tekst onder "Verlenen".

Specifieke gebruikers opgenomen

Doelresources ⓘ
[Alle cloud-apps](#)

Voorwaarden ⓘ
[0 voorwaarden geselecteerd](#)

Besturingselementen voor toegang

Verlenen ⓘ
[0 besturingselementen geselecteerd](#)

Sessie ⓘ
[0 besturingselementen geselecteerd](#)

Client-apps ⓘ
[Niet geconfigureerd](#)

Filteren op apparaten ⓘ
[Niet geconfigureerd](#)

Toepassingen

Rollen en beheerders

Facturering

Instellingen

Beveiliging

Identiteitsbeveiliging

Voorwaardelijke toegang

Security Center

Beveiligingsscore voor identiteit

Meervoudige verificatie

Verificatiemethoden

Wachtwoord opnieuw instellen

14

Kies om "Toegang te verlenen" maar door "Meervoudige verificatie" te verplichten.

Je kan de Microsoft AI dit ook zelf laten bepalen a.d.h.v. geavanceerde patronen via "Verificatiesterkte vereisen".

Verlenen ×

Het afdwingen van toegang beheren om toegang te blokkeren of te verlenen.
[Meer informatie](#)

☐ Toegang blokkeren
☒ Toegang verlenen

☒ Meervoudige verificatie vereisen ⓘ
☐ Verificatiesterkte vereisen ⓘ
☐ Vereisen dat het apparaat moet worden gemarkeerd als compatibel ⓘ
☐ Vereisen dat een conform met of aan hybride Microsoft Entra gekoppeld apparaat wordt gebruikt ⓘ
☐ Goedgekeurde client-apps ⓘ

15

Schakel het beleid in en bevestig met "Maken".

Beveiliging ^

Identiteitsbeveiliging

Voorwaardelijke toegang

Security Center

Beveiligingsscore voor identiteit

Meervoudige verificatie

Verificatiemethoden

Wachtwoord opnieuw instellen

Aangepaste beveiligingskenmerken

Beveiligingsinformatie en steuning ^

Besturingselementen voor toegang

Verlenen ⓘ

1 besturingselement geselecteerd

Sessie ⓘ

0 besturingselementen geselecteerd

Beleid inschakelen

Alleen rapporteren Aan Uit

Maken