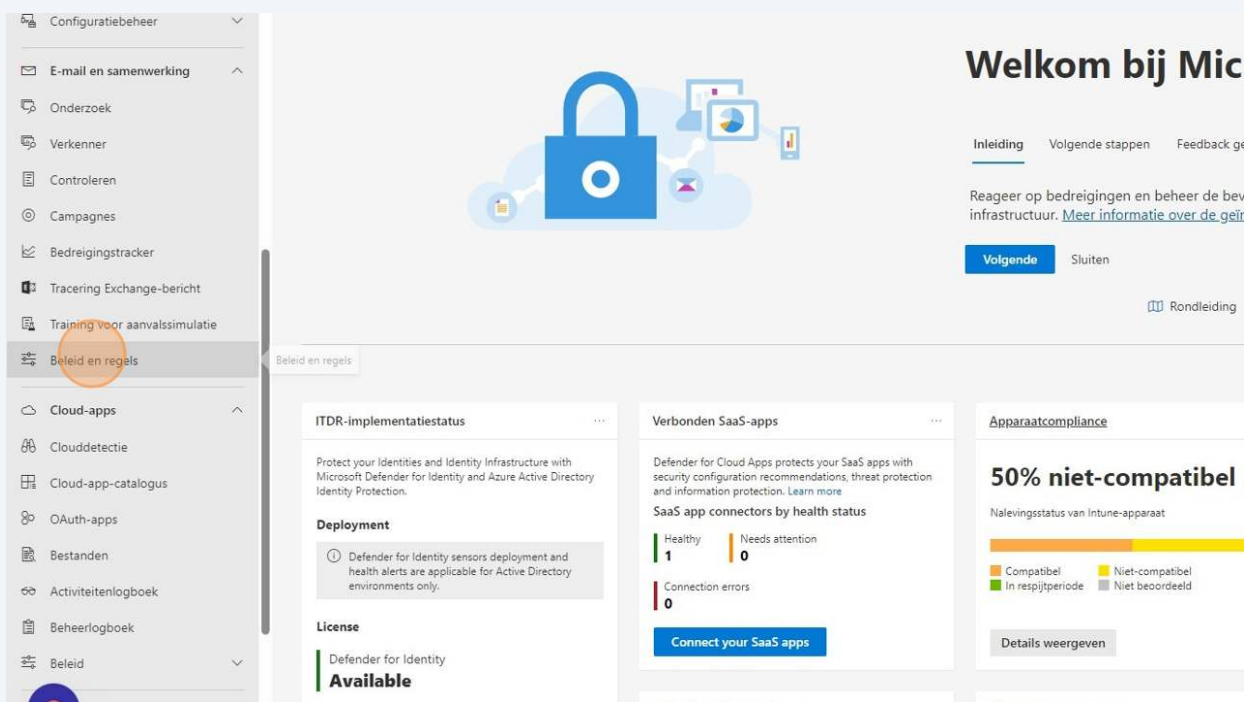


# Verhoog email beveiliging met Microsoft Defender E-mail security (A5 Security)

Deze handleiding biedt stapsgewijze instructies voor het verbeteren van e-mailbeveiliging met behulp van Microsoft Defender E-mail Security (A5 Security). Door deze stappen te volgen, kunnen beheerders hun beveiligingsbeleid en -instellingen aanpassen. Zo zorgen ze ervoor dat gevoelige e-mails grondig worden gecontroleerd en beschermd. Het implementeren van deze maatregelen kan de algehele beveiliging van de e-mailcommunicatie op school sterk verbeteren.

- 1 Surf naar [security.microsoft.com](https://security.microsoft.com) en meld aan met een beheerdersaccount

- 2 Klik onder "e-mail en samenwerking" op "Beleid en regels"



The screenshot displays the Microsoft Defender E-mail security console. On the left, a navigation pane shows the 'Policy and rules' section selected under 'Email and collaboration'. The main content area is titled 'Welkom bij Microsoft Defender E-mail security' and includes a 'Volgende' button. Below the welcome message, there are three panels: 'ITDR-implementatiestatus' showing deployment and license status, 'Verbonden SaaS-apps' showing the health status of connected SaaS applications, and 'Apparaatcompliance' showing a 50% non-compliance rate for Intune devices. The 'Policy and rules' section is highlighted in the navigation pane.

### 3 Klik op "Bedreigingsbeleid"

**Beleid en regels**

Stel beleidsregels in om apparaten te beheren en te protect against threats, en om waars

- Bedreigingsbeleid
- Bedreigingsbeleid
- Waarschuwingsbeleid
- Geavanceerde waarschuwingen beheren
- Activiteitsmeldingen

### 4 Je kan onder "Beleid" alles zelf instellen. Wij verkiezen "Vooraf ingesteld beveiligingsbeleid".

**Bedreigingsbeleid**

① Door de gebruiker gemelde instellingen zijn verplaatst van deze pagina naar Instellingen. [Ga naar Instellingen](#)

**Sjabloonbeleidsregels**

- [Vooraf ingesteld beveiligingsbeleid](#) Eenvoudig
- Configuratieanalysehulpmiddel Probleem

**Beleid**

- Antiphishing Beveilig
- Anti-spam Beveilig

5

De ingebouwde beveiliging is altijd actief.

Kies om het standaardbeleid te bewerken voor de leerkrachten.

Kies om het Stricte beleid te bewerken voor Administratieve medewerkers en directie.

Klik telkens op "Beveiligingsinstellingen beheren"

De ingebouwde beveiliging van Microsoft Office 365 wordt toegepast op alle gebruikers in uw organisatie om te beschermen tegen schadelijke koppelingen en bijlagen.

- ✓ Aanvullende machine learning-modellen
- ✓ Evaluatie van agressievere deactivering
- ✓ Visuele indicatie in de ervaring

**Notitie:** Ingebouwde beveiliging is alleen ingeschakeld voor betaalde Microsoft Defender voor Office 365-tenants.

Uitsluitingen toevoegen (niet aanbevolen)

Een basislijnbeveiligingsprofiel dat bescherming biedt tegen spam-, phishing- en malwarebedreigingen.

- ✓ Gebalanceerde maatregelen tegen schadelijke inhoud
- ✓ Gebalanceerde verwerking van bulkinhoud
- ✓ Beveiliging van bijlagen en koppelingen met Veilige koppelingen en Veilige bijlagen

☐ Standaardbeveiliging is uitgeschakeld

[Beveiligingsinstellingen beheren](#)

Een agressievere beveiligingsprofiel voor geselecteerde gebruikers, zoals waardevolle doelwitten of gebruikers met prioriteit.

- ✓ Agressievere maatregelen tegen schadelijke e-mail
- ✓ Betere controle over bulkzenders
- ✓ Agressievere machine learning

☒ Strikte beveiliging is uitgeschakeld

[Beveiligingsinstellingen beheren](#)

6

Kies op welke groep gebruikers of welke domeinnaam binnen deze instellingsgroep valt (standaard of strikt).

Er mag GEEN overlap zijn.

Gebruikers

En

Groepen

En

Domeinen

veggivino.be x veggivino.com x vinonovo.be x

☒ Geen

☐ Deze geadresseerden uitsluiten

7

Kies "gevoelige" externe contactpersonen waarvan e-mails extra moeten gecontroleerd worden.

Denk aan Financieel afgevaardigden, externe leden van raad van bestuur, verificateur, CLB, ...

## erming toepassen

### Voeg e-mailadressen toe om te markeren bij imitatie door aanvallers

Voeg interne of externe adressen toe van personen die mogelijk worden geïmiteerd door aanvallers, zoals lopmanag bestuursleden en andere personen in sleutelposities. Gedecteerde berichten van geïmiteerde afzenders worden in quarantaine geplaatst. [Meer informatie over imitatie-instellingen](#)

Toevo

0 items

Weergavenaam

E-mailadres van afzender

Geen gegevens beschikbaar

8

Je kan ook domeinnamen toevoegen i.p.v. personen als gevoelige afzenders. Het gaat hier om externe personen.

## toepassen

### Voeg domeinen toe om deze te markeren wanneer ze worden geïmiteerd door aanvallers

Deze domeinen kunnen van u zijn of domeinen die toebehoren aan uw belangrijkste leveranciers en partners. Berichten die worden gedetecteerd met geïmiteerde afzenderdomeinen, worden in quarantaine geplaatst. [Meer informatie over imitatie-instellingen](#)

Toevoegen

Naam

Verwijderen

9

Klik op "Bevestigen"

De afzender voor Office 365 is van toepassing op

Als het domein van de geadresseerde is:

veggivino.be;  
veggivino.com;  
vinonovo.be;

**Imitatiebeveiliging is van toepassing op e-mailberichten van**

E-mailadres van afzender

Afzenderdomeinen

Met uitzondering van de volgende vertrouwde afzenders en domeinen

Terug

Bevestigen

10

Schakel het beleid in dat je hebt geconfigureerd.

herhaal deze stappen voor het andere beleid.

De ingebouwde beveiliging van Microsoft Office 365 wordt toegepast op alle gebruikers in uw organisatie om te beschermen tegen schadelijke koppelingen en bijlagen.

- ✓ Aanvullende machine learning-modellen
- ✓ Evaluatie van agressievere deactivering
- ✓ Visuele indicatie in de ervaring

**Notitie:** Ingebouwde beveiliging is alleen ingeschakeld voor betaalde Microsoft Defender voor Office 365-tenants.

[Uitsluitingen toevoegen \(niet aanbevolen\)](#)

Een basislijnbeveiligingsprofiel dat bescherming biedt tegen spam-, phishing- en malwarebedreigingen.

- ✓ Gebalanceerde maatregelen tegen schadelijke inhoud
- ✓ Gebalanceerde verwerking van bulkinhoud
- ✓ Beveiliging van bijlagen en koppelingen met Veilige koppelingen en Veilige bijlagen



Standaardbeveiliging is uitgeschakeld

[Beveiligingsinstellingen beheren](#)

Een agressievere geselecteerde doelwitten

- ✓ Agressievere mail
- ✓ Betere controle over bulkzenders
- ✓ Agressievere machine learning



Strikte beveiliging is uitgeschakeld

[Beveiligingsinstellingen beheren](#)

11

Click "Beveiligingsinstellingen beheren"

geen spam-, phishing- en malwarebedreigingen.

Gebalanceerde maatregelen tegen schadelijke inhoud

Gebalanceerde verwerking van bulkinhoud

Beveiliging van bijlagen en koppelingen met Veilige koppelingen en Veilige bijlagen

Standaardbeveiliging is ingeschakeld

[Beveiligingsinstellingen beheren](#)

geen spam-, phishing- en malwarebedreigingen, maar bescherming van doelwitten of gebruikers met prioriteit.

✓ Agressievere maatregelen tegen schadelijke e-mail

✓ Betere controle over bulkzenders

✓ Agressievere machine learning



Strikte beveiliging is uitgeschakeld

[Beveiligingsinstellingen beheren](#)