Twee-factor-authenticatie (2FA) aanzetten voor je beheeromgeving

Algemeen Beheer · https://autorespond.nl/docs/twee-factor-authenticatie-2fa-aanzetten-voor-je-beheeromgeving/

Met twee-factor-authenticatie (2FA) beveilig je de toegang tot je Autorespond-dashboard met een extra stap: naast je wachtwoord vul je bij het inloggen ook een code in die je per e-mail ontvangt. Zo kan iemand die je wachtwoord in handen krijgt nog steeds niet bij je beheeromgeving. In dit artikel lees je hoe je 2FA aanzet, voor welke gebruikersrollen je het instelt en hoe het inloggen er daarna uitziet.

*Beveiliging en 2FA in Autorespond is gebaseerd op **FluentAuth**, inbegrepen in je pakket. Lees de Engelse documentatie*

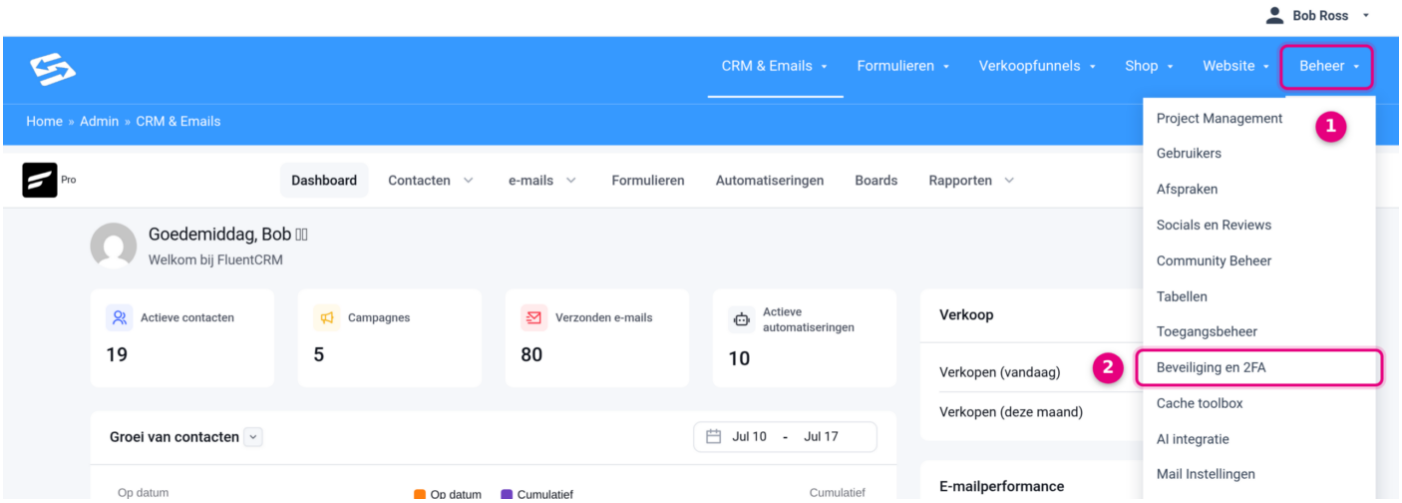
Welke 2FA-instellingen zijn de beste keuze?

Het korte antwoord: er valt weinig te kiezen, en dat is goed nieuws. Autorespond kent één 2FA-methode: een logincode via e-mail. Een authenticator-app (zoals Google Authenticator) is niet beschikbaar en ook niet nodig — je hoeft dus niets te installeren en geen QR-codes te scannen. Het enige dat je zelf kiest, is voor welke gebruikersrollen de extra controle verplicht is.

Ons advies: zet 2FA in elk geval aan voor de rol **ARadmin** (beheerder). Hebben ook redacteuren (**Editor**) of auteurs (**Author**) toegang tot je omgeving, voeg die rollen dan ook toe. Voor rollen zonder beheerrechten — zoals abonnees of cursisten die alleen in je academie inloggen — is 2FA meestal niet nodig.

Stap 1 — Open Beveiliging en 2FA

1. Log in op je Autorespond-dashboard.
2. Klik rechtsboven op het menu **Beheer**.
3. Kies in het uitklapmenu voor **Beveiliging en 2FA**.



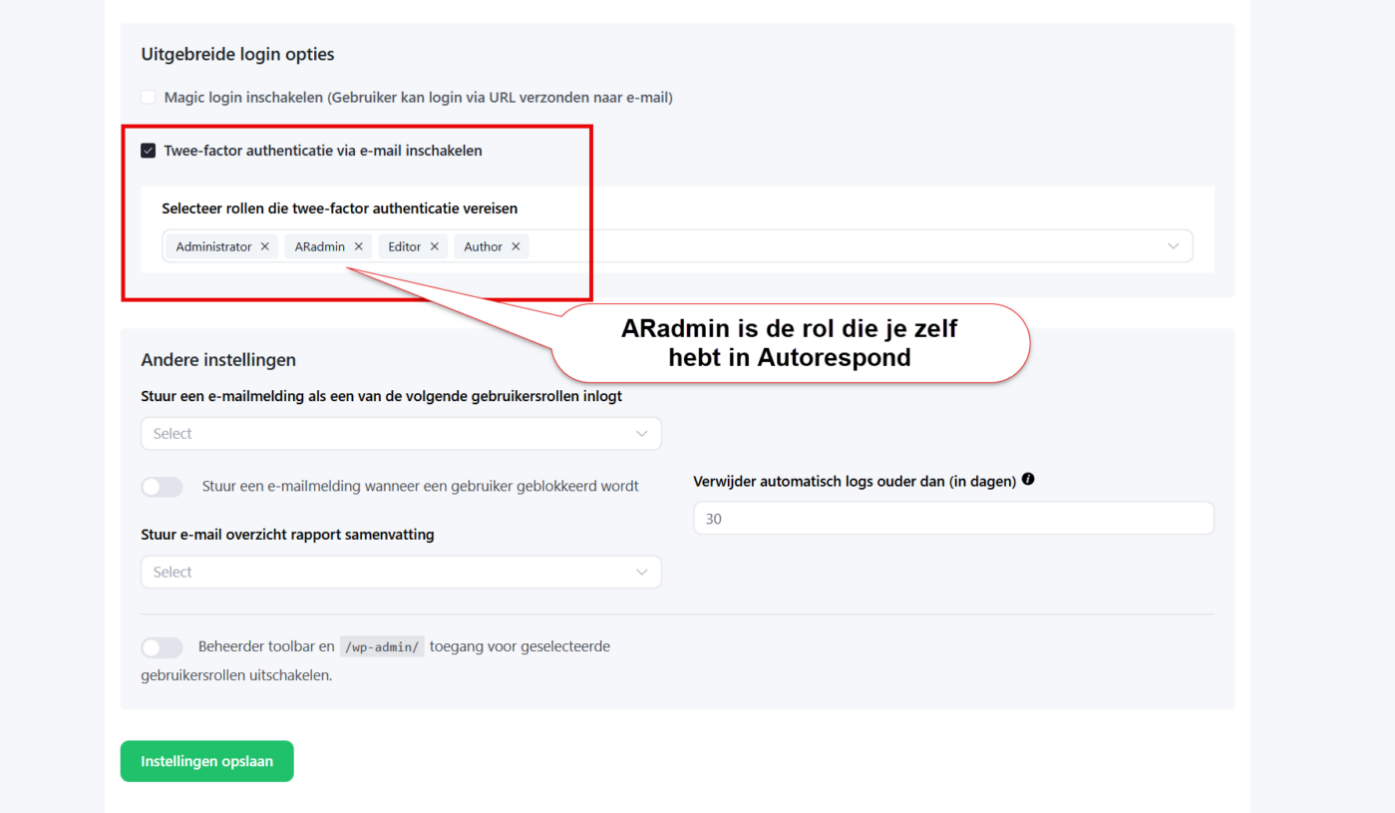
Via het menu Beheer open je Beveiliging en 2FA

1. **Beheer** — het menu rechtsboven in je dashboard met alle beheeronderdelen van je omgeving, zoals Gebruikers, Toegangsbeheer en Mail Instellingen.
2. **Beveiliging en 2FA** — opent de beveiligingsinstellingen van je omgeving, waaronder twee-factor-authenticatie en de beveiliging van het loginformulier.

Stap 2 — Zet twee-factor-authenticatie via e-mail aan

Je komt binnen op het tabblad **Instellingen**. Scrol naar het kopje **Uitgebreide login opties**.

1. Vink **Twee-factor authenticatie via e-mail inschakelen** aan.
2. Kies bij **Selecteer rollen die twee-factor authenticatie vereisen** de rollen waarvoor de logincode verplicht wordt. Kies in elk geval **administrator**.
3. Klik onderaan op **Instellingen opslaan**. De instelling geldt direct: bij de eerstvolgende login krijgen de geselecteerde rollen het codescherm te zien.



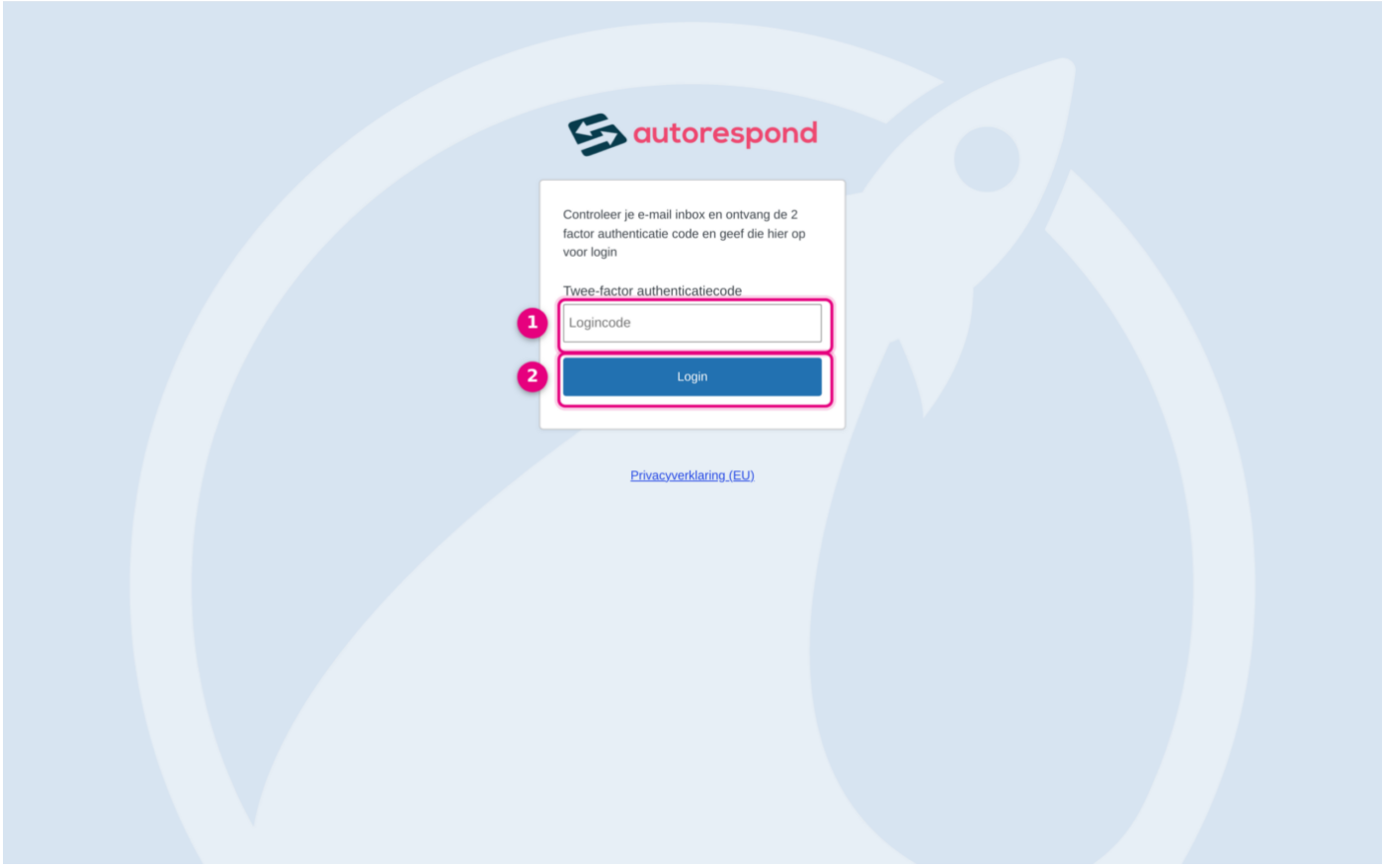
1. **Twee-factor authenticatie via e-mail inschakelen** — de hoofdschakelaar. Aangevinkt betekent: bij het inloggen is naast het wachtwoord ook de logincode uit de e-mail verplicht.
2. **Selecteer rollen die twee-factor authenticatie vereisen** — alleen gebruikers met een rol in dit veld krijgen het codescherm. In het voorbeeld staan administrator, Editor en Author ingesteld; met het kruisje achter een rol haal je hem weg, via het pijltje rechts voeg je rollen toe.
3. **Instellingen opslaan** — vergeet deze knop niet: pas na het opslaan is 2FA actief.

Op dit scherm zie je nog meer opties die voor 2FA niet nodig zijn: **Magic login inschakelen** (inloggen via een link in je e-mail, staat standaard uit) en onder **Andere instellingen** kun je een e-mailmelding instellen wanneer iemand met een bepaalde rol inlogt of geblokkeerd wordt, oude logboeken automatisch laten opschonen en de beheerder-toolbar voor bepaalde rollen uitschakelen. Die kun je gewoon laten staan zoals ze staan.

Stap 3 — Zo ziet inloggen er voortaan uit

Vanaf nu verandert het inloggen voor de rollen die je hebt geselecteerd. Na het invullen van je gebruikersnaam en wachtwoord verschijnt een extra scherm dat om een logincode vraagt. Die code wordt op dat moment automatisch gemaild naar het e-mailadres van het account waarmee je inlogt.

1. Log in met je gebruikersnaam en wachtwoord, zoals je gewend bent.
2. Open de e-mail met je logincode. Zie je hem niet meteen, kijk dan ook even in je spammap.
3. Vul de code in bij **Twee-factor authenticatiecode** en klik op **Login**.



Na je wachtwoord vraagt het loginscherm om de code uit je e-mail

1. **Twee-factor authenticatiecode** — vul hier de cijfercode in die je zojuist per e-mail hebt ontvangen. De code is tijdelijk geldig en werkt maar één keer.
2. **Login** — bevestigt de code en logt je in op je dashboard.

Goed om te weten

- 2FA geldt per gebruikersrol, niet per persoon. Alle gebruikers met een geselecteerde rol krijgen bij hun eerstvolgende login het codescherm — kondig het dus even aan bij collega’s die ook inloggen.
- Test het direct na het aanzetten: log in een privé-/incognitovenster opnieuw in met je eigen account. Je huidige sessie blijft gewoon open terwijl je controleert of de code-e-mail aankomt.
- Je wachtwoord blijft de eerste sleutel. Gebruik een sterk, uniek wachtwoord; hoe je dat aanpast lees je in het artikel WordPress gebruikersaccount wijzigen (zoals het wachtwoord).

Gerelateerde artikelen

- WordPress gebruikersaccount wijzigen (zoals het wachtwoord)

Alles voor je e-maillijst, academie en verkoop in één beveiligde omgeving — dat is Autorespond.

Ontdek Autorespond →