

Multi Factor Authenticatie (MFA) instellen voor een school

Documentversie 1.3 datum: 10-10-2025

1. Extra beveiliging toegang schoolmedewerkers

Basispoort verwerkt (met toestemming van de school) een (zeer) beperkte set aan persoonsgegevens over leerlingen en medewerkers. Hoewel deze gegevens minimaal gevoelige informatie bevatten (slechts namen en groepstoewijzingen en voor medewerkers het emailadres), zijn met een medewerkerstoegang bij uitgeverijen leerresultaten in te zien. Voor extra veiligheid, is het steeds gebruikelijker om via 2 stappen in te loggen in applicaties. Dat gebeurt steeds vaker bij financiële dienstverleners en overheidsinstellingen.

Multi Factor Authenticatie (MFA) is een extra beveiligingsstap bij inloggen. MFA zorgt voor een betere bescherming van persoonsgegevens. Basispoort biedt scholen sinds 2023 de mogelijkheid (geen harde eis) om leerkrachten en beheerders (rol van 'ICT-Coördinator' bij Basispoort) veilig in te laten loggen via MFA.

Als verwerker van persoonsgegevens heeft Basispoort een eigen verantwoordelijkheid m.b.t. de privacywetgeving. En een zorgplicht. ICT-coördinatoren kunnen (anders dan de overige medewerkers) in Basispoort alle gegevens inzien - en ook wijzigen. Vanuit publiek-private ketensamenwerking zoals Edu-V, wordt aanbevolen MFA te verplichten voor beheerders.

Daarom staat verplicht inloggen via MFA vanaf 18 oktober 2025 standaard 'aan' voor ICT-coördinatoren.

Importeren Multi Factor Authenticatie IP-adressen Netwerkbeheerders Uitgeverijen

Multi Factor Authenticatie beheren

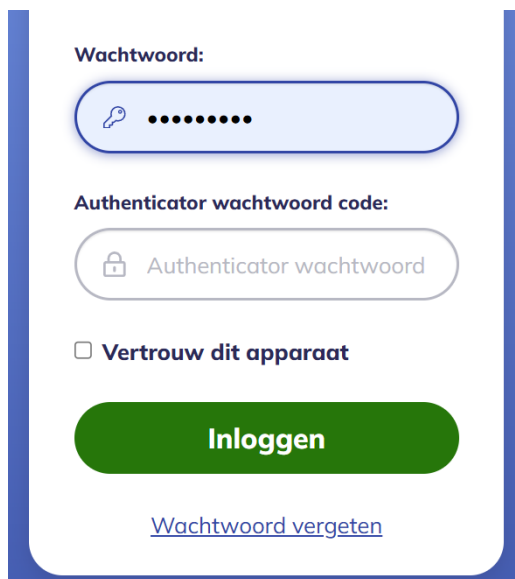
U kunt hieronder aangeven of Multi Factor Authenticatie verplicht is voor deze school.

Verplicht voor iedereen ☐

Verplicht voor ICT-Coördinatoren ☒

MFA zou eigenlijk óók verplicht moeten zijn voor leerkrachten en onderwijsmedewerkers. Dit omdat er via Basispoort bij aangesloten partners resultaat en voortgangsinformatie van leerlingen in te zien is. Zoals in omgevingen van de landelijke toets-aanbieders (Cito, Diataal en Bureau ICE). Om operationele (inlog)problemen voor leerkrachten te voorkomen, laat Basispoort deze keuze vooralsnog aan de school. MFA is met de optie 'verplicht voor iedereen' wel instelbaar voor alle medewerkers. De ICT-Coördinator kan dit in Basispoort instellen.

Het goede nieuws is dat als bij het inloggen met MFA, de optie 'Vertrouw dit apparaat' ervoor zorgt dat deze handeling de eerste 14 dagen niet herhaald hoeft te worden. Het gebruik van een authenticator hoeft dan dus niet ieder uur of iedere dag herhaald te worden.



Wachtwoord:

Authenticator wachtwoord code:

☐ Vertrouw dit apparaat

Inloggen

[Wachtwoord vergeten](#)

Indien de MFA niet wordt vastgehouden door de browser heeft dit te maken met settings die door de school beheerd worden. Helaas moet dan elke keer opnieuw de token ingevuld worden.

Basispoort neemt haar verantwoordelijkheid voor de veiligheid van vertrouwelijke gegevens van leerlingen en leerkrachten. Basispoort doet een beroep op iedere school om dat ook te doen!

Het instellen van MFA voor 'alle medewerkers' is een taak voor de schoolmedewerker(s) met in Basispoort de rol van 'ICT-coördinator'. Medewerkers hebben een mobiele telefoon nodig, met een "authenticator app" of een andere mogelijkheid om een code te genereren voor de 2e inlogstap.

Belangrijk!!!

2-staps/MFA verificatie geldt, eenmaal ingesteld voor een school, voor ALLE medewerkers van die school. Voordat MFA op schoolniveau wordt ingesteld, dienen ALLE medewerkers te beschikken over een mobiele telefoon met "authenticator app", of een andere methode om een code aan te maken voor de 2e inlogstap.

*Werkt een medewerker op meerdere scholen en is MFA is ingesteld op 1 van die scholen?
Dan zal deze medewerker voor ALLE scholen via MFA moeten inloggen.*

Het instellen van MFA op schoolniveau, als ook ondersteuning in het gebruik van de "authenticator app" hoort bij de rol van ICT-coördinator. De Basispoort helpdesk kan hierin slechts beperkt ondersteunen.

2. Uitleg over Multi Factor Authenticatie (MFA)

Multi Factor Authenticatie (MFA) of “2-staps verificatie” is een manier om met een extra code, niet in 1 maar in 2 stappen, in te loggen. Eerst logt een gebruiker in met ‘gebruikersnaam’ en ‘wachtwoord’. Daarna verschijnt het verzoek om een extra code in te voeren. Deze code wordt aangemaakt met een zogenaamde ‘authenticator’. Er bestaan verschillende soorten ‘authenticators’, die alle werken vanuit hetzelfde principe. Er zijn 3 werkwijzen:

- De extra code wordt gestuurd via een SMS bericht naar een telefoonnummer;
- De extra code wordt gestuurd naar een e-mailadres;
- De extra code wordt gegenereerd via een ‘authenticator-app’ op de mobiele telefoon.

2.1. Niet via telefoon nummer

Veel ‘authenticators’ werken met een oplossing waarbij een mobiel nummer opgegeven moet worden, die dan de authenticator start op die telefoon. Aangezien Basispoort dan privacygevoelige mobiele nummers van schoolmedewerkers zou moeten gaan opslaan, heeft Basispoort afgezien van het gebruiken van die techniek. Basispoort heeft als stelregel zo min mogelijk persoonsgegevens te verwerken. Basispoort heeft gekozen voor de variant ‘authenticator-app’. Leerkrachten en onderwijsondersteunende medewerkers van een school dienen op hun mobiele telefoon daarom een ‘authenticator-app’ te installeren. Daarvan zijn er meerdere varianten gratis te downloaden via Google Play of de Apple Appstore. Veelgebruikte ‘authenticator-apps’ zijn: Microsoft Authenticator, Google Authenticator en ‘iPhone-Authenticator’.

2.2. Gebaseerd op de tijd

Een TOTP-code (Time-based One-Time Password) is een tijdelijke, numerieke code die wordt gebruikt voor extra beveiliging bij het inloggen, vaak als onderdeel van multifactor authenticatie (MFA). De code wordt elke 30 seconden opnieuw gegenereerd door een app op je telefoon of een ander apparaat, die de huidige tijd en een gedeelte geheime sleutel als input gebruikt.

De MFA-token is gebaseerd op de tijd. Het gebruikt de tijd van de telefoon.

Het is van belang dat de telefoon dus de juiste tijd aangeeft.

Zorg er bij problemen voor dat de tijd van de telefoon gesynchroniseerd wordt met de internet tijd.

3. MFA Activering met een Authenticator

De eerste keer dat een medewerker inlogt nadat de MFA voor een school is aangezet zal onderstaand scherm getoond worden. De medewerker opent dan de 'authenticator-app' en scant dan de QR code.



Mocht het inscannen niet lukken gebruik dan de volgende code in uw authenticator:.

JUUS2BSKAZLGRDLI

De alias van dit token:

Basispoort MFA

Na het koppelen verschijnt er een code, vul deze in.

Authenticator wachtwoord code verifiëren:

Authenticator wachtwoord code...

Code verifiëren

3.1. MFA via de Microsoft Authenticator

Als de Microsoft Authenticator is geïnstalleerd op de mobiele telefoon, kan een nieuwe code aangemaakt worden. Dit kan door in de authenticator de + (Plus) aan te klikken. Daarna zijn er 3 opties, waarbij gekozen moet worden voor de optie 'Ander account'. Dan wil de app toegang tot de camera om de QR code te scannen. Na het scannen moet die code ingevoerd worden in Basispoort om te bevestigen dat het activeren van de authenticator is gelukt.

3.2. MFA via de Google Authenticator

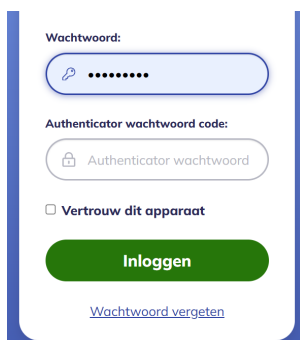
Als de Google Authenticator is geïnstalleerd op de mobiele telefoon, kan een nieuwe code aangemaakt worden. Dit kan door in de authenticator de + (Plus) aan te klikken. Dan wil de app toegang tot de camera om de QR code te scannen. Na het scannen, wordt een code getoond en moet die code ingevoerd worden in Basispoort om te bevestigen dat het activeren van de authenticator is gelukt.

3.3. MFA via de iPhone Authenticator

Nieuwere iPhones hebben een ingebouwde authenticator. Deze werkt min of meer zoals de Microsoft- en Google authenticators. Deze zit bij *Instellingen > Wachtwoorden*. Bij het aanmaken van een nieuw account moet de QR code gescand worden. Na het scannen moet die code ingevoerd worden in Basispoort om te bevestigen dat het activeren van de authenticator is gelukt.

4. Normaal gebruik

Als voor een schoolaccount in Basispoort door de ICT-coördinator, MFA is ingesteld, krijgt de medewerker na het ingeven van gebruikersnaam en wachtwoord het extra invoerveld '**Authenticator wachtwoordcode**'. Daar wordt de via de authenticator gegenereerde 2e code ingevoerd om in te loggen.

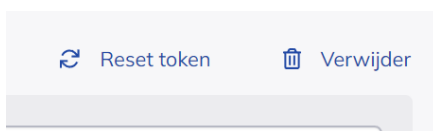


The screenshot shows a login form with the following elements:

- A label "Wachtwoord:" above a password input field with a masked password "*****".
- A label "Authenticator wachtwoord code:" above an input field containing the text "Authenticator wachtwoord".
- A checkbox labeled "Vertrouw dit apparaat" which is currently unchecked.
- A green "Inloggen" button.
- A link "Wachtwoord vergeten" at the bottom.

5. Bij problemen, bijvoorbeeld andere telefoon

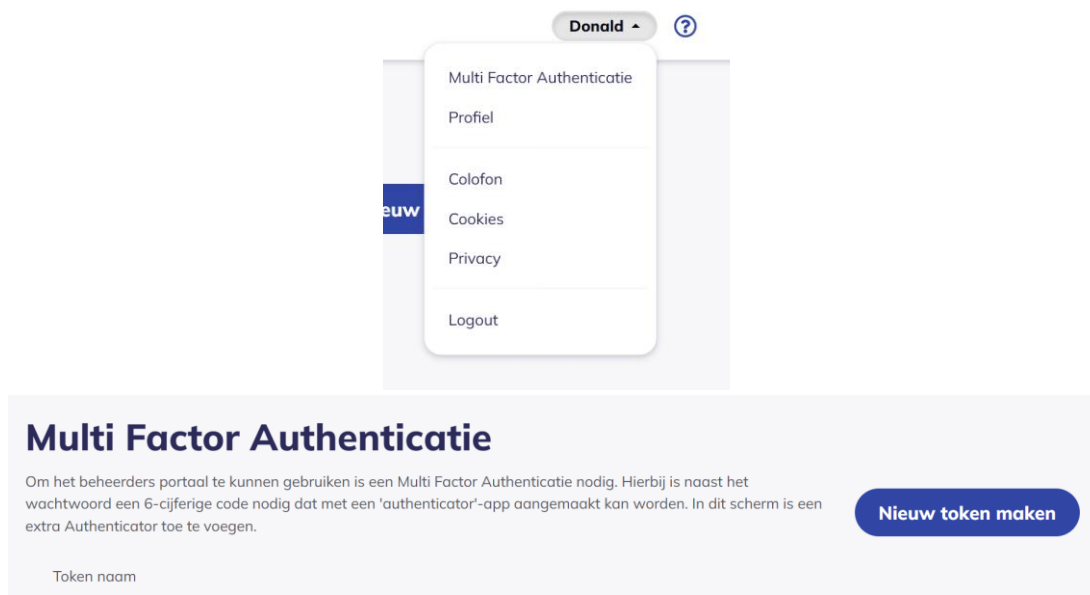
Indien een medewerker problemen heeft kan een ICT-coördinator de code bij de medewerker weghalen via de '**reset token**'. Dit is te vinden in het medewerkers overzicht scherm bij de betreffende medewerker.



Let op dat het opgeslagen 'Basispoort MFA account' ook uit de authenticator app verwijderd wordt. Bij een QR code, moet ALTIJD een NIEUW 'Basispoort MFA account' aangemaakt worden. Als er al een Basispoort account bestaat in de authenticator, verwijder die eerst!

6. Extra telefoon, extra token

Een medewerker heeft ook de mogelijkheid een extra token aan te maken. Bijvoorbeeld als deze een 2^e telefoon wil gebruiken of een andere authenticator app fijner vindt in gebruik. Deze optie staat in de menuopties van de medewerker.



Na het aanklikken van de optie “Nieuw Token maken”, krijgt de medewerker een pop-up met een QR code zoals dat ook bij het aanmaken van de eerste code het geval is.

7. Medewerker kan zelf ook met MFA starten

Een medewerker heeft ook de mogelijkheid zelf met MFA te gaan werken, om de eigen inlog beter te beveiligen. Dit werkt op dezelfde wijze als in de vorige paragraaf beschreven.

8. Wat te doen bij problemen

Bij problemen vraag een collega ICT coördinator waar het instellen wel gelukt is. De MFA verplichting kan door de collega ICT coördinator uitgezet worden, echter wordt dit streng afgeraden. **Ook de Basispoort helpdesk heeft die mogelijkheid (pas na 18 oktober), echter kan dit alleen schriftelijk, dus via een mail aanvraag ingediend worden door een ICT coördinator van die school. Er wordt dus gecontroleerd of die medewerker aan de school verbonden is.**