HANDLEIDING

Verplichte tweefactorauthenticatie Nmbrs

Belangrijke **UPDATE** vanaf 1 juli 2026

Voor alle gebruikers van Nmbrs

SALARISZAKEN
digitaal op voorsprong

Bij Salariszaken doen we er alles aan om de gegevens van onze klanten optimaal te beschermen. In het licht van de ontwikkelingen op het gebied van cyber-veiligheid hebben we eerder al proactief de beveiliging van ons systeem versterkt middels een verplichte tweefactorauthenticatie op alle accounts.

UPDATE: Nmbrs had een eigen 2FA-systeem. Dat komt te vervallen per 1 juli 2026. Nmbrs is onderdeel van Visma en dat betekent dat we kunnen bouwen op de beveiligingsinfrastructuur van een van de grootste softwarebedrijven van Europa. Visma Connect is de inlogomgeving die Visma breed inzet en continu verder ontwikkelt. Dit betekent meer keuze in verificatiemethode (app, sms, face ID), betere ondersteuning en na de eerste instelling log je voortaan in met één tik of je vingerafdruk.

We stappen dus over op Visma Connect. De 2FA in Nmbrs wordt gedeactiveerd. Je dient de 2FA daarom opnieuw in te stellen via Visma Connect, dit wordt uitgelegd in hoofdstuk 2 van dit document.

Heb je vragen of opmerkingen na het lezen van deze handleiding?
Neem dan contact met ons op per email via info@salariszaken.nl.
We helpen je graag verder.

Inhoud

1. De werking van tweefactorauthenticatie

Wachtwoorden zijn al tientallen jaren in gebruik en zijn nog steeds de meest gebruikte vorm van authenticatie. Door te authenticeren verifieert het systeem of de gebruiker de daadwerkelijke eigenaar van het account is en autoriseert het systeem de gebruiker.
Bij veel systemen wordt gebruik gemaakt van een tweede stap in de authenticatie, bijvoorbeeld door controle van een extra code die een gebruiker moet invoeren.

De zescijferige verificatiecode wordt gegenereerd door een authenticatie-app en is slechts 30 seconden geldig voordat er een nieuwe code verschijnt. Dit verkleint aanzienlijk de kans dat kwaadwillenden toegang krijgen tot je account.

Er zijn verschillende authenticatie-apps beschikbaar voor iOS- en Android-gebruikers. De meest gebruikte zijn *Google Authenticator, Microsoft Authenticator en Authy*.
Deze apps zijn gratis te downloaden en volledig Nederlandstalig, maar ook in andere talen beschikbaar.

LET OP: Hoewel tweefactorauthenticatie een extra beveiligingslaag toevoegt, is de combinatie met een uniek, lang wachtwoord of een passphrase nog veiliger. Een passphrase is een reeks woorden of een zin die makkelijk te onthouden is, zoals 'Mijnafspraakisom10:30indekoffiebar'. Vermijd voorspelbare patronen en kies een zin of reeks woorden die niet eenvoudig te raden is. Overweeg daarnaast het gebruik van een wachtwoordmanager, waarmee je veilige wachtwoorden en passphrases kunt genereren en beheren. Salariszaken heeft kundig personeel op dit gebied en kan gericht adviseren om jouw beveiliging verder te versterken.

2. Wat moet ik doen?

Ga naar home.visma.com en probeer in te loggen met het e-mailadres en wachtwoord waarmee je altijd al inlogt bij Nmbrs. **Je hoeft geen nieuw account aan te maken**. Lukt het inloggen zonder problemen? Dan zit je goed. Kom je vast te zitten omdat je een 2FA-code moet invoeren die je niet meer weet? Lees dan verder.

2.1 Hoe stel ik 2FA in?

1. Ga naar home.visma.com en log in met je bestaande e-mailadres en wachtwoord.
2. Je wordt gevraagd een verificatiemethode te kiezen: een authenticator-app (Google, Microsoft, Authy of Visma authenticator), sms, of face ID. Kies wat voor jou het makkelijkst werkt.
3. **Sla aan het einde de herstelcode op.** Als je ooit je telefoon kwijt bent, is dat de enige manier om toch in te kunnen loggen.

Zien hoe het werkt? Bekijk het in deze klikbare demo.

LET OP: Je ontvangt tijdens de installatie een mail van Visma (*do.not.reply@mail.connect.visma.com*). Dat klopt, vanuit daar wordt communicatie verzonden. Check ook je spamfolder.

2.2 Dagelijks gebruik

Wanneer je de applicatie Nmbrs start, moet je jouw gebruikersnaam, wachtwoord én een door de authenticator gegenereerde code in te voeren. Wanneer je dit hebt ingevoerd, wordt je doorverwezen naar de online omgeving van Nmbrs.

3. Faq

Ik gebruik al 2FA van Nmbrs. Moet ik iets doen?

Ja. We stappen over op Visma Connect. De 2FA in Nmbrs wordt gedeactiveerd. Je dient de 2FA opnieuw in te stellen via Visma Connect, dit wordt uitgelegd in 2.1 Hoe stel je 2FA in?

Ik gebruik al 2FA via Visma Connect maar heb geen toegang tot mijn authenticator. Wat nu?

Je kunt een herstelcode aanvragen via dit formulier. Support van Visma stuurt je dan een backupcode waarmee je opnieuw kunt inloggen en 2FA opnieuw kunt instellen.

Moet ik gebruik maken van de Visma Authenticator?

Nee, je kan ook gebruik maken van Google Authenticator, Microsoft Authenticator of Authy.

Kan een tweefactor authenticator gehackt worden?

Hoewel het mogelijk is om tweefactor authenticator te hacken, is de kans erg klein.
De tweefactorauthenticatie is een sterk hulpmiddel om accounts en systemen veilig te houden. Een manier waarop tweefactorauthenticatie gehackt kan worden, is via de SMS-methode. Dit is een methode waar een eenmalige code wordt verzonden naar het telefoonnummer van een gebruiker. Hackers kunnen de mobiele telefoonaanbieders misleiden om het telefoonnummer van iemand anders over te zetten naar hun eigen telefoon. De hackers nemen contact op met de providers die zich voordoen als klant en vragen om een nieuwe simkaart met het nummer van het slachtoffer. Ze hebben dan toegang tot elke authenticatiecode die aan dat telefoonnummer is verbonden. Dit komt echter zelden voor, maar blijf altijd alert.

Vragen?

Heb je nog vragen of opmerkingen na het lezen van deze handleiding?
Neem dan contact met ons op via info@salariszaken.nl. We helpen je graag verder.

SALARISZAKEN
digitaal op voorsprong

Salariszaken BV
Zuiderplein 43
8911 AP Leeuwarden

info@salariszaken.nl
salariszaken.nl