Implementatie MFA

Versiebeheer:		
Versie 0.9	05-08-2021	Donny Langerak
Versie 1.0	16-09-2021	Sabrina Boetzkes – Hoop
Versie 2.0	02-11-2021	Sabrina Boetzkes - Hoop

Deze handleiding gaat uit van de standaard werking van de desbetreffende module en wordt jaarlijks herzien. Tussentijdse wijzigingen worden niet direct verwerkt, daarom kunnen er afwijkingen zijn in de beschrijving. Neem contact op met Livits support wanneer je hier vragen over hebt.

Inhoud

1. Inleiding

Dit document beschrijft de stappen voor het instellen en het gebruik van Multi-Factor Authentication (MFA). Om MFA in te stellen kun je diverse apps gebruiken.
Livits adviseert de Microsoft Authenticator app die op alle bekende mobiele platformen beschikbaar is. De beschreven stappen en voorbeelden in dit document zijn vanuit Microsoft Authenticator gemaakt. Het stappenplan kan anders verlopen als er voor een andere app gekozen wordt.

1.1. Downloaden van Microsoft Authenticator

Authenticator kan gedownload worden vanuit de Google Play store of App Store van Apple.

Android: Google Play Store
https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=nl&gl=US

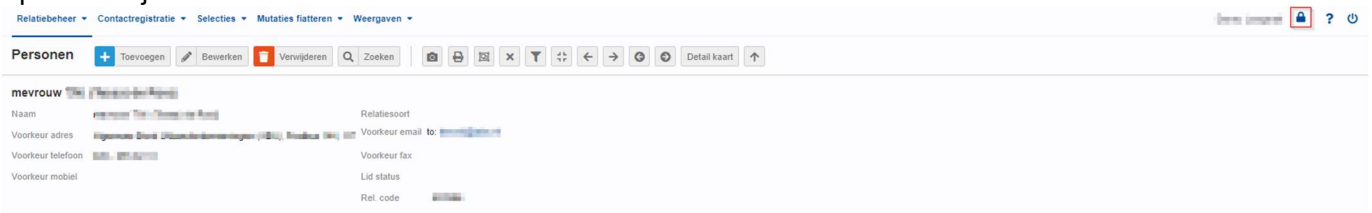
Apple/iOS: Apple Store
https://apps.apple.com/nl/app/microsoft-authenticator/id983156458

2. Instellen van MFA voor gebruikers

Voordat MFA ingesteld kan worden zal jouw functioneel consultant van Livits MFA instellen op de backoffice van Livits. Daarna kunnen de gebruikers Livits toevoegen aan hun eigen Authenticator App.

2.1. MFA instellen

Na het installeren van de Authenticator App (zie 1.1) open je Livits waarna je rechtsboven op het slotje klikt.



Nadat je op het slotje geklikt hebt wordt het onderstaande scherm getoond.

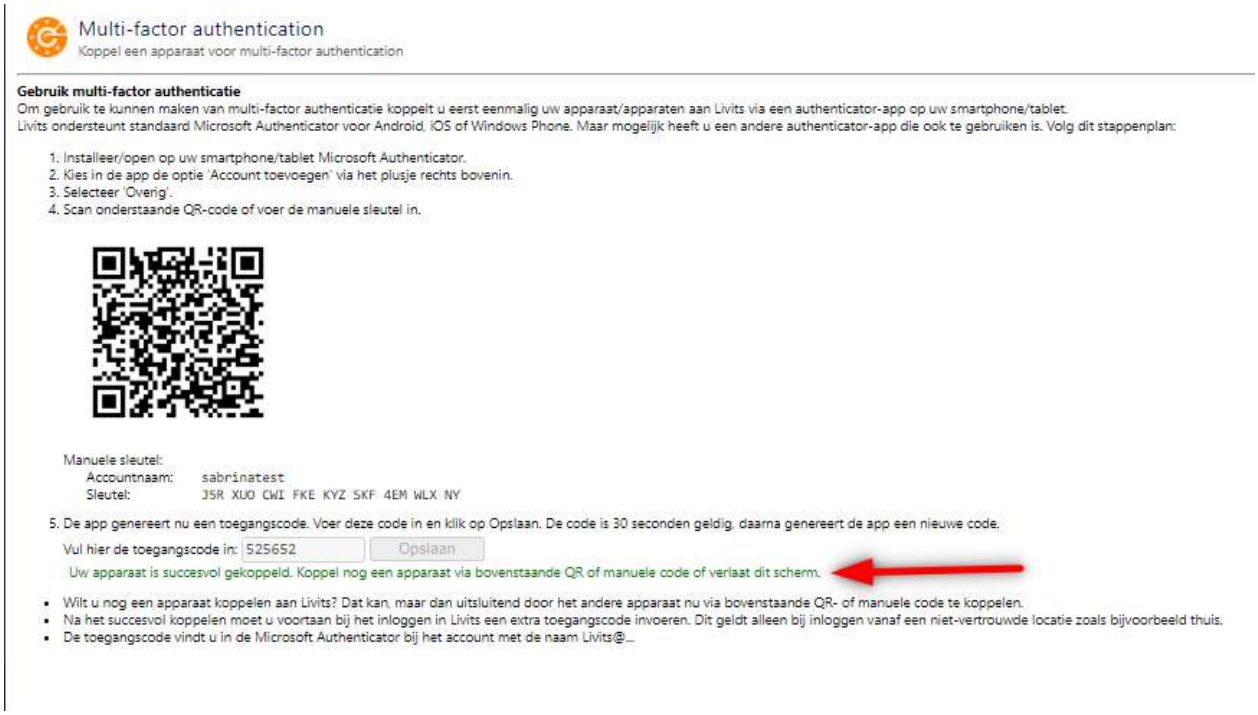
Daarna open je de Microsoft Authenticator app. Je klikt rechtsboven op het icoon '+' en kiest daarna voor de optie 'overig'.

Scan de QR-code die je in het Livits scherm ziet met de Authenticator app.

Zodra de QR-code is gescand of het account handmatig is gekoppeld verschijnt er een nieuwe registratie in de Authenticator App:

In de Authenticator App wordt een 6-cijferige code getoond met een timer. De code die je ziet is slechts 30 seconden geldig. Daarna verschijnt een nieuwe code met een nieuwe geldigheidsduur.

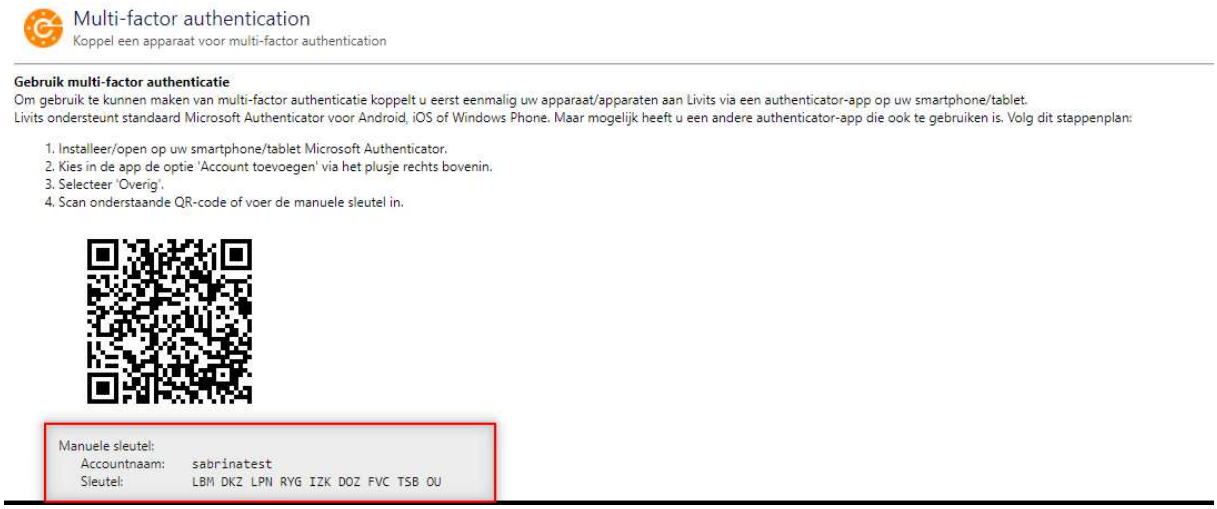
De code uit de app vul je in Livits in het juiste veld in. Daarna klik je op ‘opslaan’. De registratie is voltooid wanneer je in het groen de volgende melding ziet: ‘Uw apparaat is succesvol gekoppeld. Koppel nog een apparaat via bovenstaande QR of manuele code of verlaat dit scherm’.



Het scherm/tabblad kan hierna worden afgesloten.

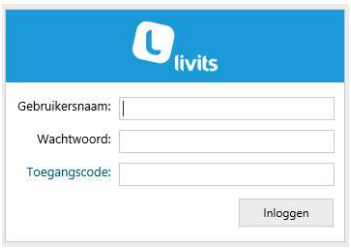
2.2. QR-code scannen werkt niet

Als het scannen van de QR-code niet lukt, kan het account handmatig worden gekoppeld door op ‘or enter code manually’, onderaan het scherm te klikken. Vervolgens kan de app worden gekoppeld door de accountnaam en bijbehorende sleutel handmatig in te voeren.

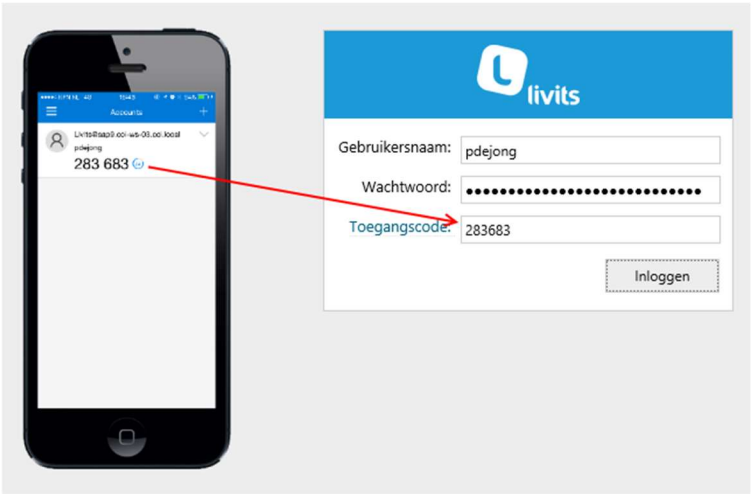


2.3. Gebruik van MFA bij het inloggen

Vanaf het moment dat MFA is ingeschakeld zal er bij het inloggen in de backoffice een toegangscode worden gevraagd. De toegangscode vind je in de Authenticator App.



Bij het inloggen vul je je gebruikersnaam en wachtwoord in zoals je gewend bent. Daarna open je de Authenticator App voor de toegangscode. De toegangscode vul je in het juiste veld in.



Let op! De code is 30 seconden geldig. Wanneer de 30seconden zijn verstreken wordt een nieuwe code aangemaakt.

Na het vullen van de juiste code klik je op 'Inloggen' waarna je in de backoffice terecht komt.

2.4. Inloggen zonder authenticator app

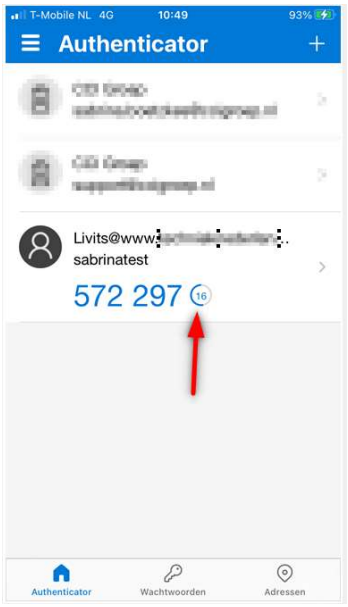
In sommige gevallen kan het voorkomen dat je geen toegang hebt tot de authenticator app. Dit kan voorkomen bij verlies van je telefoon of het vergeten ervan.

In dat geval kun je via een beheerder tijdelijk toegang krijgen tot Livits via de authenticator app van de beheerder. Dit proces is beschreven in hoofdstuk 4.

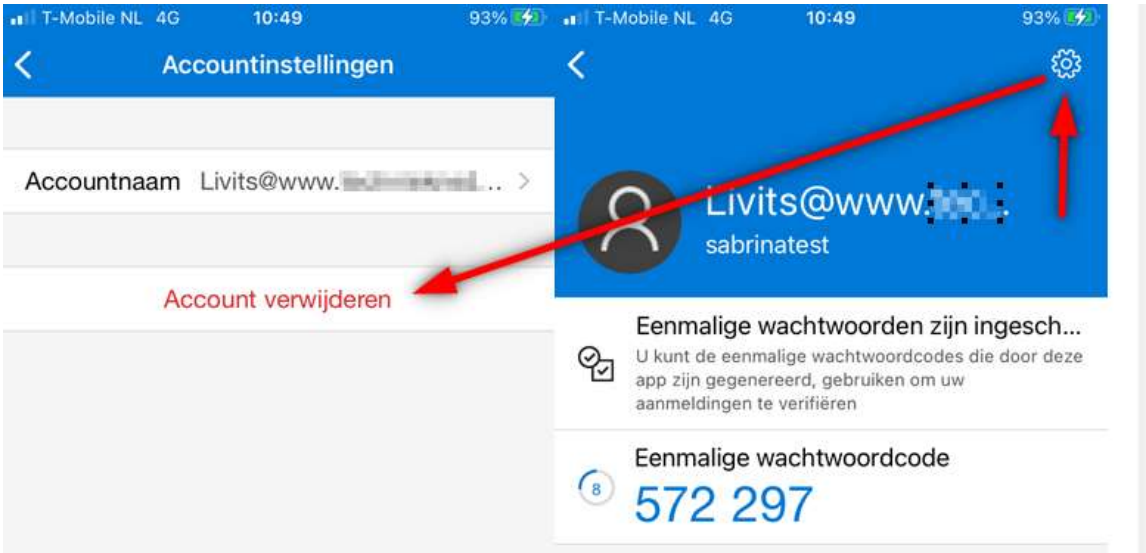
2.5. Inloggen na toegang via beheerder

Wanneer je tijdelijke toegang hebt gehad tot Livits dan log je de eerstvolgende keer weer in via de beheerder. Zodra dit gedaan is moet de beheerder de gekoppelde code loskoppelen zodat je je eigen Authenticator App weer kunt koppelen.

Nadat de code van de beheerder is verwijderd ga je naar de authenticator app om je oude code te verwijderen. Je doet dit door in de app op de oude code te klikken.



Daarna klik je op het tandwiel en vervolgens op ‘account verwijderen’ om je oude code te verwijderen.



Na het verwijderen volg je de stappen beschreven bij 2.1 om je code opnieuw te koppelen en daarna zonder beheerder te kunnen inloggen.

3. Informatie voor MFA-beheerders

3.1. Livegang van MFA

Voordat MFA live gaat moeten alle gebruikers hun account hebben gekoppeld. Het verloop hiervan kun je via Livits backoffice monitoren. Via het menu selecties > Rapporten > rechtenstructuur is er een rapport beschikbaar waarin de voortgang te volgen is.

Hieronder een voorbeeld van de inhoud van het rapport:

Informele_naam	Sorteer_naam	MFA_aangemaakt	MFA_gewijzigd
Pieter Willemsen	Willemsen,	22-5-2017 13:59	24-5-2017 16:54
John Jacobs	Jacobs,		
Rob de Wit	De Wit,	29-5-2017 09:40	
Ricardo de Vries	Vries,		
Astrid de Jong	Jong,	30-5-2017 11:51	

De personen 'Pieter Willemsen', 'Rob de Wit' en 'Astrid de Jong' hebben hun MFA gekoppeld. De gebruikers 'John Jacobs en 'Ricardo de Vries' hebben nog geen MFA-koppeling. Dit is te zien in de lege kolom MFA_aangemaakt.

De livegang kan plaatsvinden voordat alle personen zijn gekoppeld (bijvoorbeeld door verlof of ziekte van één of meerdere medewerkers). De overige personen kunnen dan op een later moment gekoppeld worden.

Vergeet niet dat de personen die hun MFA nog niet hebben gekoppeld vanaf dat moment geen toegang meer hebben tot de backoffice. Deze gebruikers moeten eerst gekoppeld worden aan een MFA. In paragraaf 2.5 kun je nalezen hoe gebruikers achteraf gekoppeld worden.

3.2. Nieuwe gebruikers toevoegen na livegang

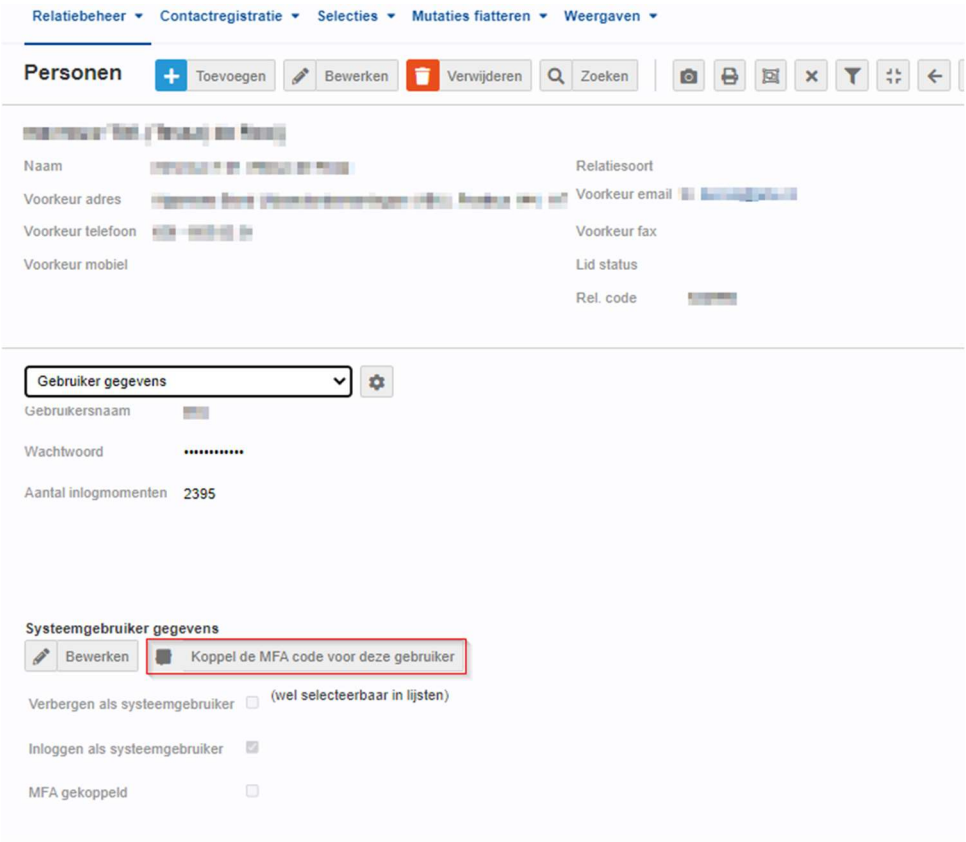
Nieuwe gebruikers van Livits kunnen niet meteen inloggen in de backoffice van Livits. Dit kan de eerste keer alleen met behulp van een beheerder die toegang heeft tot de knoppen 'MFA koppelen' en 'MFA ontkoppelen' in het tabblad gebruikersgegevens van het CRM.

4. Toegang verstrekken via beheerder

Het kan voorkomen dat iemand via een beheerder tijdelijke toegang tot de backoffice nodig heeft. Dit komt voor bij personen die na livegang een account krijgen en personen die hun telefoon verliezen of vergeten.

In dat geval kan de beheerder helpen om in te loggen in Livits.

De beheerder heeft toegang nodig tot het CRM, het tabblad persoonsgegevens en daarbij de knoppen MFA koppelen en ontkoppelen.



4.1. Code ontkoppelen

Voordat je een persoon tijdelijke toegang kunt geven via jouw beheerdersapp moet de huidige code van deze persoon ontkoppeld worden. Dit doe je door naar de tab gebruikersgegevens te gaan en te kiezen voor de optie ‘ontkoppel de huidige MFA-code voor deze gebruiker’.

4.2. Persoonlijke QR-code ophalen

Na het ontkoppelen van de code wordt de knop 'Koppel de MFA-code voor deze gebruiker' zichtbaar. Klik op deze knop om de persoonlijke QR-code van deze persoon op te halen.

Volg nu de stappen zoals beschreven bij 2.1.
Nadat de MFA-code gekoppeld is kan de gebruiker inloggen met behulp van de beheerdersapp.

De gebruiker logt in met zijn normale gegevens en vult de code uit de beheerdersapp om via MFA-toegang te krijgen.

4.3. Ontkoppelen na tijdelijke toegang

Wanneer iemand toegang via de beheerder heeft gehad dan moet er de eerstvolgende keer weer ingelogd worden de beheerder.

Daarna moet de persoon zijn eigen toegang herstellen, maar dit kan alleen wanneer de MFA-code ontkoppeld is.
Dit doe je weer via de knop 'Ontkoppel de MFA-code voor deze gebruiker'.

Daarna kan de gebruiker zijn oude code in de Authenticator app verwijderen en stap 2.1 opnieuw volgen om zijn eigen app te koppelen.