MFA via Salesforce

STAFFING
MANAGEMENT
SERVICES
Part of HeadFirst Group

Inhoudsopgave

Deze handleiding betreft een generieke handleiding. Het kan zijn dat de werkwijze in jouw Inhuurdesk portaal afwijkt.

Multi Factor Authentication via Salesforce

Multi-factor authenticatie (MFA)

Multi-factor authenticatie (hierna, MFA) is een extra beveiligingslaag voor een account. Naast iets dat je weet (je wachtwoord) vereist het systeem ook iets dat je hebt (je smartphone) om toegang te krijgen tot je account. Als - in het ergste geval – je wachtwoord is uitgelekt, blijft je account beschermd door deze verbinding met je smartphone.

Dit document helpt je bij het instellen van MFA voor je aanmelding bij Nétive VMS.

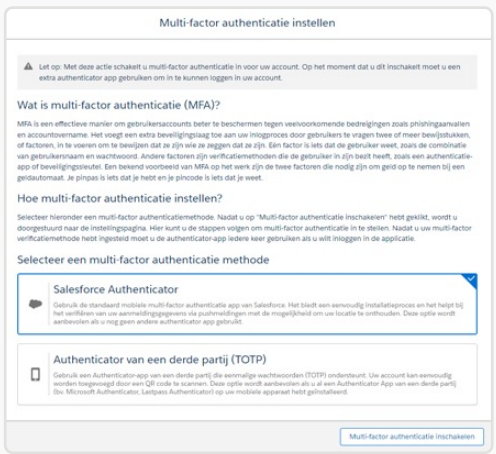
Instellen MFA

Om gebruik te maken van MFA moet je een Authenticator-app downloaden op je smartphone. We beperken het gebruik van MFA niet tot een specifieke app, er zijn er meerdere beschikbaar. We maken onderscheid tussen: Salesforce Authenticator en Third Party Authenticators (Google Authenticator, Microsoft Authenticator, Authy, LastPass Authenticator, etc.). Met behulp van deze apps kun je je VMS-account koppelen aan je smartphone. Inloggen kan daarna alleen met diezelfde smartphone.

Hoe stelt u MFA in?

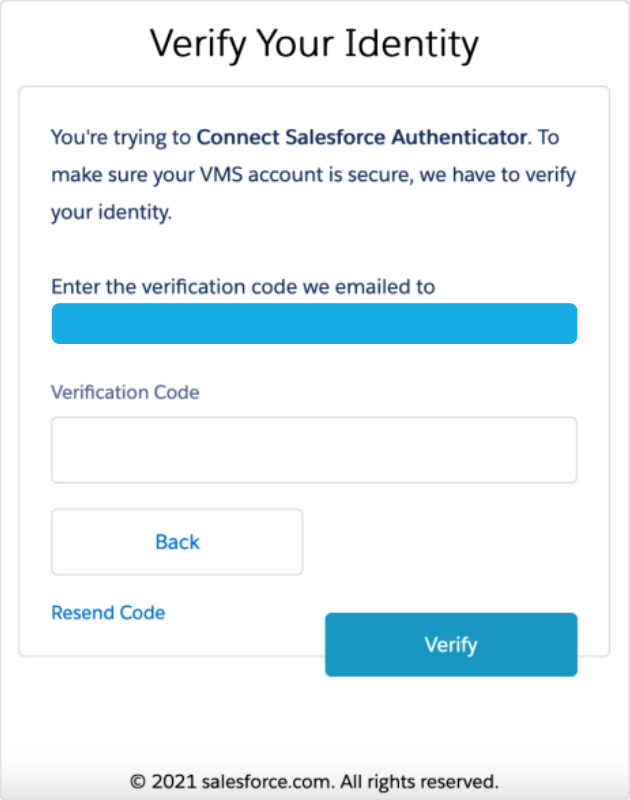
MFA is verplicht voor opdrachtgevers, die niet werken met Single Sign On (SSO). Als MFA voor jou verplicht is, zul je de volgende keer dat je inlogt een melding krijgen over de MFA-instelling.

Als MFA voor jou optioneel is, kun je in de Inhuurdesk rechtsboven navigeren naar Mijn instellingen en daarna naar Mijn persoonlijke gegevens om de sectie Multi-factor authenticatie te vinden. Achter de status vind je een link: Koppelen. Wanneer je op deze link klikt, kun je MFA instellen.



Uw identiteit verifiëren

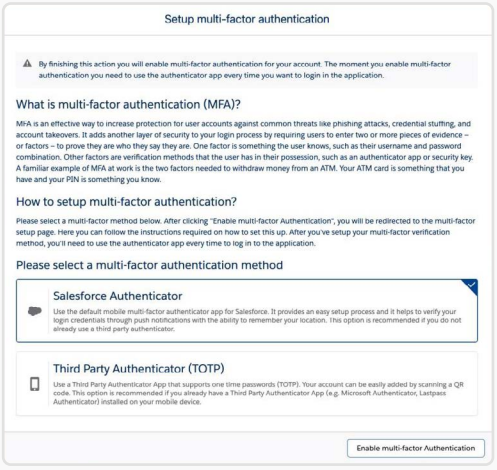
Deze stap is alleen relevant wanneer je MFA aansluit via Mijn instellingen.
Jouw identiteit moet worden geverifieerd voordat je een telefoon kunt aansluiten. Dit gebeurt via een code die wordt gestuurd naar jouw e-mailadres dat in het systeem bekend is. Zorg ervoor dat je de code uit de e-mail kopieert naar het formulier in de applicatie.



Kies een authenticator app

Je kunt kiezen uit de Salesforce Authenticator en Authenticators van derden (Google Authenticator, Microsoft Authenticator, Authy, LastPass Authenticator, enz.). Als je de Salesforce Authenticator gebruikt, krijg je een pushmelding op je telefoon telkens wanneer je inlogt. Met een Third Party Authenticator moet je een code uit de app kopiëren in de applicatie.

- Als MFA voor jou optioneel is, krijg je een pop-up om een van de methoden te kiezen zoals hierboven beschreven.



- Als MFA voor jou verplicht is, krijg je direct de optie om de Salesforce Authenticator te gebruiken wanneer je inlogt. Door op de link Een andere verificatiemethode gebruiken onder aan de pagina te klikken, kun een authenticator van een derde partij gebruiken.

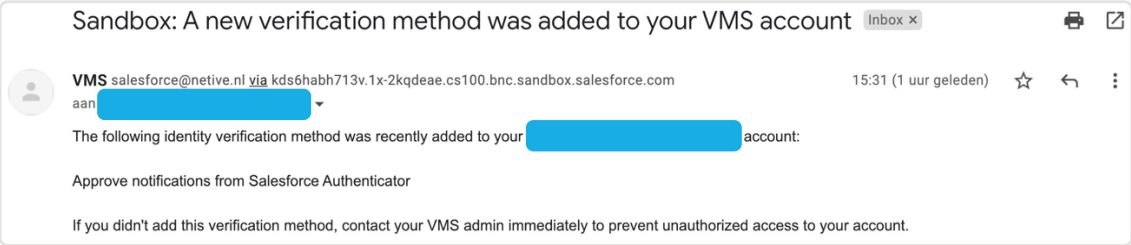
Uw telefoon koppelen

Als je de Salesforce Authenticator hebt gekozen als verificatiemethode (in stap b), wordt in de app een zinnetje van twee woorden weergegeven dat je moet invoeren op het formulier in de applicatie. Als je niet onmiddellijk een zinsdeel van twee woorden ziet, moet je op de knop Een account toevoegen in de app klikken.

Na het invoeren van het twee-woord zinnetje, klik je op Connect in de applicatie en Connect in de app en de telefoon zal verbonden worden met je account. Je ontvangt een e-mail als bevestiging. Het verbindingsproces kan een minuutje duren.

Heb je besloten om gebruik te maken van een Third Party Authenticator (in stap b)? Dan moet je met behulp van je app een QR-code scannen. Vervolgens zal de app een zescijferige code voor je genereren. Wanneer je de code invoert in het formulier in de applicatie en op Connect klikt, wordt de app verbonden met je account. Je ontvangt een e-mail als bevestiging. Het verbindingsproces kan een minuutje duren.

Nadat je MFA hebt ingesteld, ontvang je een bevestigingsmail:



Inloggen als MFA is ingesteld

Als je al een MFA-verbinding tussen je account en je smartphone hebt ingesteld, kun je zoals gebruikelijk inloggen met gebruikersnaam en wachtwoord. Na het invoeren van de juiste inloggegevens word je gevraagd om je identiteit te verifiëren met behulp van de Authenticator-app.

- Als je de Salesforce Authenticator hebt gekozen als verificatiemethode (zie paragraaf Instellen stap 2), ontvang je een pushmelding op je smartphone. Heb je geen pushmelding ontvangen of kun je niet op de pushmelding klikken? Open dan de Salesforce Authenticator-app. Na het openen van de app kunt je je poging om in te loggen bevestigen.

- Heb je besloten om gebruik te maken van een Third Party Authenticator? Bij het inloggen word je gevraagd een verificatiecode van zes cijfers in te voeren. Deze code wordt geproduceerd door de Authenticator-app van jouw keuze (dat is de app die je hebt gebruikt om je telefoon te verbinden zoals in de vorige paragraaf beschreven).

Inloggen als MFA nog niet is ingesteld

Als je MFA nog niet hebt ingesteld, zijn er twee mogelijkheden:

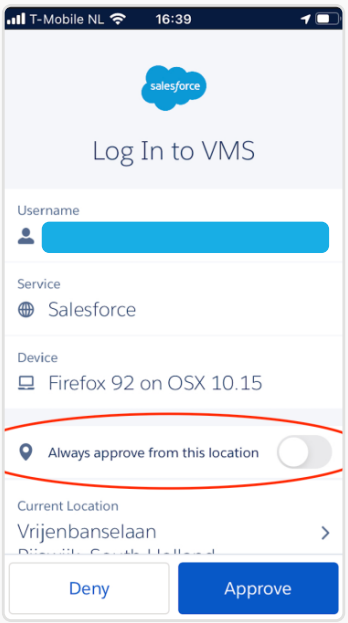
1. MFA is optioneel gemaakt voor jouw type account. In dit geval lees je paragraaf 2 Instellen, als je MFA wilt configureren. Dit is echter geen must. Je kan ook gewoon doorgaan zonder dit in te stellen.
2. Als MFA verplicht is voor jouw type account, dan word je onmiddellijk gevraagd om een verificatiemethode in te stellen. Zie Stap b in Paragraaf 2 Instellen hoe dat eruitziet.

Onthoud apparaat

Een gebruikerssessie in het VMS is beperkt tot een maximale tijd van inactiviteit (standaard is 2 uur). Daarna word je automatisch uitgelogd en dien je met gebruikersnaam, wachtwoord en MFA opnieuw in te loggen.

- Wanneer je de Salesforce Authenticator-app gebruikt, kun je gebruikmaken van een 'onthoud mij'-functie op basis van de GPS-locatie van je apparaat. Je kan dit doen door de knop net achter Altijd goedkeuren vanaf deze locatie aan te vinken. Als je dit doet, controleert de Salesforce Authenticator-app de volgende keer dat je inlogt jouw GPS-locatie. Als je je binnen een goedgekeurd gebied bevindt, dan wordt de stap van de MFA automatisch overgeslagen.

- Wanneer je gebruikmaakt van een Authenticator-app van een derde partij, is het niet mogelijk om de multifactor authenticatiestap over te slaan wanneer je inlogt.



Smartphone defect of vervangen?

Is je mobiele telefoon defect, zoekgeraakt of vervangen door een nieuwe telefoon waardoor je niet meer inloggen op de VMS? Geen probleem! Neem dan contact met ons op.

Taurusavenue 18, 2132 LS Hoofddorp
+31 (0)10 76 00 900
www.staffingms.com

STAFFING
MANAGEMENT
SERVICES
Part of HeadFirst Group