Toelichting Youforce

Twee-factor authenti-catie

Versie 2015 -12

4 december 2015

Inleiding

Om uw vertrouwelijke gegevens doeltreffend af te schermen en te beveiligen, wordt toegang tot Youforce verleend op basis van een uitgebreid beveiligingssysteem. Centraal daarbij staat de legitimatie bij aanmelding. Alle Youforce-gebruikers melden zich aan met een persoonlijke gebruikersidentificatie en een wachtwoord. Daarnaast hebben Youforce beheerders, HR-professionals en Payroll-professionals nog een gebruikerscertificaat nodig voor toegang tot het professionele portaal van Youforce.

Extra beveiliging noodzakelijk?

Als het beveiligingsbeleid van uw organisatie dit noodzakelijk maakt, is het beveiligingsniveau van Youforce verder te verhogen door het inlogproces uit te breiden met tweefactor-authenticatie. Gebruikers melden zich aan met een wachtwoord **en een additionele toegangscode**. Dit betreft een éénmalig te gebruiken code van 6 cijfers, die Raet tijdens het aanmelden per SMS verzendt. De verzending van deze toegangscodes wordt geregistreerd in het Logboek Youforce, zodat een audit op dit proces achteraf mogelijk is.

Configuratie

U kunt nauwkeurig instellen voor welke gebruikers van Youforce deze extra beveiliging geldt: voor bepaalde rollen en/of voor individuele gebruikers. Standaard ontvangen gebruikers hun toegangscode door middel van een SMS-bericht naar hun mobiele telefoonnummer. Om dat mogelijk te maken, moet dat nummer in Youforce bekend zijn. U kunt er ook voor kiezen de codes op verzoek van de gebruiker tevens per e-mail te laten verzenden. Heeft een gebruiker tijdelijk niet de beschikking over de mobiele telefoon, dan is voor één dag aanmelding zonder toegangscode in te stellen.

Authenticatie per rol, per groep en/of per individuele gebruiker

Bij gebruik van twee-factor authenticatie kunt u als volgt instellen voor welke Youforce gebruikers deze extra beveiliging moet gelden:

- Is de authenticatie van toepassing voor bepaalde rollen − bijvoorbeeld wel voor 'managers', maar niet voor 'medewerkers' − dan legt u dit vast via de beheeroptie *Gebruikersinstellingen* | *Autorisatieprofielen beheren*; kies hier module: **twee-factor authenticatie**.
- Voor individuele gebruikers kunt u de authenticatie instellen in *Gebruikersbeheer* |*Toegangsbeheer*; ook hier kiest u de module: **twee-factor authenticatie**
- Als u een gebruiker wilt autoriseren om andere gebruikers één dag toegang te verlenen zonder SMS-code zet u de optie **twee-factor authenticatie beheerder** aan. Deze gebruiker moet ook over beheerdersrechten hebben in Youforce.

Authenticatie uitsluiten voor groepen gebruikers

Tijdens het log in proces wordt als standaard voor alle gebruikers altijd om een code gevraagd. Er zijn echter een aantal situaties denkbaar waarbij het niet gewenst is om

van twee-factor authenticatie gebruik te maken, bijvoorbeeld voor gebruikers die met een certificaat inloggen of gebruikers die via Single Sign-on inloggen. Zo nodig kunt u deze gebruikers uitsluiten van het gebruik van deze dienst.

Bovenstaande opties kunt u als beheerder instellen in *Youforce beheer* | *Gebruikersinstellingen* | *Twee factor authenticatie.*

Authenticatiecode ontvangen via SMS en/of e-mail

Standaard ontvangen gebruikers hun toegangscode door middel van een SMS-bericht, dat naar het mobiele telefoonnummer van de gebruiker wordt gestuurd (maximaal 50 toegangscodes per dag). Op de *beheerpagina Beperken toegangscode tot SMS' in Youforce beheer* | *Gebruikersinstellingen* | *Twee factor authenticatie* geeft u dan aan of toegangscodes uitsluitend via SMS worden toegestuurd. Vinkt u deze optie uit, dan ontvangen de gebruiker de codes, op verzoek, ook *per e-mail* (maximaal éénmaal per sessie).

Verzending uitsluitend via SMS is veiliger, omdat e-mailberichten en mailboxen minder goed te beveiligen zijn dan mobiele devices. Wel hebben de gebruikers dan waarschijnlijk vaker assistentie nodig, bijvoorbeeld als zij geen mobiele telefoon bij zich hebben.

Eénmalig aanmelden zonder authenticatiecode

Youforce-gebruikers met authenticatieverplichting die tijdelijk geen beschikking hebben over hun mobiele telefoon, kunt u voor één dag toestemming geven om zich zonder toegangscode aan te melden. Daartoe vinkt u voor deze gebruiker in *Individueel gebruikersbeheer* het veld aan **Vandaag toestaan om zonder toegangscode in te loggen**. Deze indicatie vervalt automatisch om middernacht (het vinkje in Individueel gebruikersbeheer wordt overigens niet automatisch weggehaald). U kunt deze toestemming als beheerder ook eerder uitvinken.

Mobiele nummer opgeven

Is het mobiele nummer van een Youforce-gebruiker niet bekend, dan moet men dit de eerste keer dat men zich aanmeldt direct opgeven. Daarbij moet het ingevoerde nummer voldoen aan de eisen voor een mobiel telefoonnummer en wordt de internationale notatie toegepast:

Eerst het plusteken (+) van de internationale toegangscode. Daarna het nummer van het land waarin het abonnement is geregistreerd, gevolgd door het GSM-nummer (voor Nederlandse nummers: zonder het cijfer nul). Een voorbeeld van een Nederlands nummer: **+31612345678**, bestaande uit **+** (internationale toegangscode), **31** (landnummer), **6** (kengetal mobiel nummer) en **12345678** (GSM-nummer).

Is later nodig het geregistreerde nummer te veranderen, dan kan de gebruiker dit zelf doen bij Mijn instellingen | Profiel aanpassen. Ook een Youforce-beheerder kan dat doen. In *Gebruikersbeheer* | *Individueel gebruikersbeheer* zijn hiervoor de velden e-mailadres privé en Mobiel nummer aanwezig.

N.B.: Aan de inhoud van de rapportages *Overzichten Aanmaken* en *Gebruikersoverzicht downloaden* is het veld 'mobiel nummer' toegevoegd, zodat u kunt controleren of de mobiele nummers van gebruikers met authenticatieverplichting bekend zijn in Youforce.

Registratie in het Logboek gebruik Youforce

Per SMS kan elke Youforce-gebruiker maximaal 50 toegangscodes per dag ontvangen. Voor e-mail geldt dat éénmaal per sessie e-mail verzonden wordt. Al deze verzendingen worden opgenomen in het Logboek gebruik Youforce. In het menu *Berichtenoverzicht* is optie *Toegangscodehistorie* aanwezig met de lijst van alle verzendingen, onder vermelding van

- het mobiele nummer en/of het e-mailadres waarnaar de code is verzonden
- het tijdstip van verzending en de eventuele bevestigingsberichten
- of de code juist is teruggekoppeld en
- hoe vaak er een onjuiste code is ingevoerd.

Blokkeren en deblokkeren

Zodra een gebruiker meer dan 5 keer een onjuiste toegangscode heeft ingevoerd, wordt de verzonden toegangscode ongeldig gemaakt en ontvangt de gebruiker de melding ‘Te veel onjuiste toegangscodes ingevoerd’. Deze gebruiker ontvangt dan geen nieuwe toegangscodes meer en wordt in het gebruikersoverzicht in Individueel gebruikersbeheer aangemerkt als ‘geblokkeerd’ (evenals gebruikers die te vaak een onjuist wachtwoord hebben ingevoerd).

Een geblokkeerde gebruiker kunt u in *Individueel gebruikersbeheer* weer deblokkeren door het veld Blokkeren weer uit te vinken en/of de gebruiker een nieuw wachtwoord toe te kennen. De teller voor het aantal onjuiste toegangscodes wordt dan voor die gebruiker weer op nul gezet.

Meer informatie?

Deze optioneel af te nemen dienst is beschikbaar voor een eenmalig bedrag en een bedrag per verzonden SMS-bericht. Voor meer informatie kunt u contact opnemen met uw accountmanager.