

Instellen 2-factor authenticatie door key-users van GemsTracker

Inleiding

In deze handleiding wordt het instellen van twee factor authenticatie (2FA) beschreven door key-users (account beheerders) voor 'gewone' gebruikers van GemsTracker.

Door het instellen van 2FA worden uw gebruikers geautoriseerd voor het koppelen van hun smartphone aan hun GemsTracker account en gaat hun smartphone als tweede factor werken voor het inloggen op een GemsTracker site. Hun inlog naam en wachtwoord blijft de eerste factor authenticatie die met deze procedure niet wijzigt. De standaard instelling in GemsTracker is dat na het aanzetten en aanmelden van deze 2FA, de 2FA alleen gevraagd zal worden buiten het locale netwerk. Binnen het locale netwerk fungeert het interne IP adres als 2FA.

Belangrijk:

Iemand kan een smartphone alleen koppelen als hij of zij op een PC ingelogd is in GemsTracker, binnen het locale netwerk. Ook via een VPN omgeving zoals "mijn werkplek" is de ervaring tot nu toe dat dit goed verloopt. Wijzigt de smartphone dan zal deze koppeling binnen het netwerk¹ opnieuw ingesteld moeten worden (zie de gebruiker handleiding).

2FA instellen voor eindgebruikers door key-users/administrators

1. Log in op de GemsTracker omgeving van uw project
 - Log in op een PC in het locale netwerk
 - Bezoek met uw webbrowser de link voor uw locale GemsTracker project en login met uw GemsTracker admin account.
2. Wijzig / controleer de gebruikersgroepen en rollen
 - Via het menu Beheer - toegang - groepen: controleer de rol van de groep die u wilt wijzigen. Voor groep staff is de rol staff ingesteld.
 - Via menu: Beheer - toegang - rollen - staff (Toon): controleer de privileges van de rol staff. Bijna onderaan, net voor het tonen van "Geërfde privileges", staat "Uw account → Twee factor instelling" (dit is goed).
 - Als dit privilege niet hier staat, dan staat deze nog onder "Niet toegestaan" (onderaan). In dit laatste geval kunt u bij de centraal beheerder het toevoegen van 2FA bij deze rol aanvragen.
3. Stel de gebruiker in staat 2FA in of uit te schakelen / wisselen van smartphone 2FA in te stellen.
 - Menu: Beheer - toegang - medewerkers: wijzig de medewerker die u 2FA toegang wilt laten instellen.
 - Vink de optie aan "Twee factor instelbaar" (laatste optie). U kunt hier later ook zien of iemand 2FA heeft ingesteld.
 - Uw GemsTracker medewerker account is nu gereed voor 2FA. Voor eindgebruikers is een aparte handleiding om 2FA in te stellen.

2FA herstellen / uitschakelen voor een eindgebruiker door key-users/administrators

1. Wat als iemand niet kan inloggen met 2FA
 - Gebruikt deze persoon misschien verschillende GemsTracker accounts? De 2FA is specifiek voor elk project.
 - Is de 2FA voor de productieserver ingesteld? Instellen voor de testserver kan ook, maar deze is alleen intern bereikbaar, ook voor 2FA
 - Is de code gescand of overgetypt? Bij overtypen kan een fout gemaakt zijn.
 - Is bij "Uw account" de 2FA optie niet zichtbaar? En indien ingelogd met hogere rechten, dan wel? Dan is punt 2 (het recht aan de juiste groep toekennen) niet goed afgerond.
2. Herstellen 2FA
 - Met behulp van de "Reset 2FA" knop kan kunt u bij een account de 2FA uitzetten, zodat iemand de 2FA opnieuw kan instellen. (vanaf versie 1.8.7, sept 2019).
 - Indien nodig kan de gebruiker via Citrix inloggen en de 2FA opnieuw instellen.
 - Indien dit niet mogelijk is zal de gebruiker alleen kunnen inloggen op het lokale netwerk¹ en daar opnieuw de 2FA activeren.

2FA configuratie instellingen door centraal beheerders

Toelichting: deze sectie kan door local administrators gecontroleerd worden, maar zij kunnen rollen niet aanpassen (groepen wel). Het is een taak voor centraal beheerders (superadministrators) om dit goed te configureren. Om te zorgen dat de 2FA goed instelbaar is voor key-users moet de configuratie van GemsTracker goed zijn ingesteld. Dit moet op 2 niveaus: ten eerste op rol-niveau om het recht op 2FA in te stellen, ten tweede op groep-niveau om de IP-adres toegang te configureren.

1. Log in op de GemsTracker omgeving van uw project
 - Log in op een PC in het lokale netwerk
 - Bezoek met uw webbrowser de link voor uw lokale GemsTracker project en login met uw GemsTracker superadmin account.
2. Wijzig / controleer de gebruikersgroepen en rollen
 - Via het menu Beheer - toegang - groepen: controleer de rol van de groep die u wilt wijzigen. Voor groep staff is de rol staff ingesteld.
 - Via menu: Beheer - toegang - rollen - staff (Toon): controleer de privileges van de rol staff. Bijna onderaan, net voor het tonen van "Geërfde privileges", staat "Uw account → Twee factor instelling". Als dit zo is bent u klaar met instelling van de rol.
 - Als dit privilege niet hier staat, dan staat deze nog onder "Niet toegestaan" (onderaan), en kunt u het beste een rol toevoegen met 2FA rechten.
 1. * Maak een nieuwe rol "2FAtoegang", beschrijving "2FA toegang toestaan", met alleen een vinkje bij "Uw account → Twee factor instelling" (bijna onderaan), sla dit op.
 2. * wijzig de rol staff: zet onder "Afgeleid van" een vinkje bij "2FAtoegang, sla dit op"
 - Via menu: Beheer - toegang - groepen - staff (Toon): U kunt nu deze IP beperkingen controleren:

Toegang toestaan voor IP adres reeksen

Twee factor optionele IP adres reeksen 10.0.0.0-10.255.255.255
 Login als twee factor ingesteld Verplicht - behalve in optionele IP adres reeksen
 Login als twee factor niet ingesteld Toegang alleen in optionele IP adres reeksen

Pas dit aan indien dit niet precies zo is ingesteld. U gebruikt dus alleen de optionele IP adres reeksen. Instellen van een lokale IP reeks bij de eerste regel overruled de optionele instellingen, waardoor men toch niet buiten de toegestane IP reeks kan inloggen met 2FA.

¹ Dit is ook op te lossen door een extra rol en groep (bijv. AccountValidation) te maken met minimale privileges: alleen voor het wijzigen van het eigen account, en met open toegang. Na instellen van de 2FA door de gebruiker zelf kan de gebruiker aan de administrator vragen in de juiste groep geplaatst te worden.

account	role	group	privacysettings in group
account not validated	Showing role Name Account_validation Description Start or restart account settings - no privileges Parents Privileges <ul style="list-style-type: none"> Contact->About GemsTracker Contact->Reporting bugs Contact->Support Your account->Change password Your account->Two factor setup Your account + Your account->Activity overview + Your account->Activity overview->Show Inherited privileges No privileges found. Not allowed <ul style="list-style-type: none"> Calendar Calendar->Event 	Showing group Name EXTACCOUNTVALIDATION Description New accounts for Extern Role Account_validation May set these groups Default group n/a Staff Yes Patients No Login allowed from IP Ranges Two factor Optional IP Ranges *.*.* Login with two factor set Always required - even in optional IP Range Login without two factor set Allowed in "allowed from" IP Range Active Yes	Privacy settings Mask patient name Mask Mask gender Mask Mask birthday Mask completely Mask address Mask everything Mask phones Mask Mask health data Mask
account validated (e.g. staff)		Showing group Name EXTSTAFF Description Staff workers at Extern Role Staff May set these groups EXTSTAFF Default group EXTSTAFF Staff Yes Patients No Login allowed from IP Ranges Two factor Optional IP Ranges 10.* Login with two factor set Always required - even in optional IP Range Login without two factor set Allowed only in optional IP Range Active Yes	Privacy settings Mask patient name Show Mask gender Show Mask birthday Show completely Mask address Show Mask phones Show Mask health data Show

Naam Rol	Omschrijving	Mag deze groepen instellen	Standaard groep Actief	Medewerkers Patiënten
super Administrators super	super administrators with access to the whole site	EXTACCOUNTVALIDATION, EXTSTAFF, Local Admins, Monitors, Secretariaat, Staff, super Administrators	Staff Ja	Ja Nee

And don't forget this:

From: <https://gemstracker.org/wiki/> - **GemsTracker**

Permanent link: <https://gemstracker.org/wiki/doku.php?id=userzone:security:2fa>

Last update: **2020/10/19 16:33**

