

Two Factor Authenticatie (TFA) op de server

Het is op onze servers nu mogelijk om naast de bestaande “gebruikersnaam + wachtwoord” inlog (factor 1: iets dat je weet), ook te werken met een 2^e factor, namelijk iets dat je hebt, een mobiel apparaat (smartphone of tablet).

Bij het inloggen op onze server verschijnt de volgende keer het onderstaande scherm. Er zijn twee opties, of inloggen zonder TFA, of de TFA voor de gehele praktijk inschakelen. Let op, het kan dus niet voor 1 persoon binnen de praktijk ingeschakeld worden, wanneer het ingeschakeld wordt, geldt het voor iedereen van de praktijk.

Je kan besluiten om zonder TFA te blijven inloggen, dan heb je dus altijd alleen maar een gebruikersnaam en wachtwoord nodig. Dit scherm blijft wel altijd verschijnen, kies dan voortaan altijd voor “Log in zonder Two Factor Authenticatie”.

Wanneer je voor de gehele praktijk besluit om de inlog op de server te voorzien van de TFA, druk je op de knop om het in te schakelen.



Wat gebeurt er daarna?

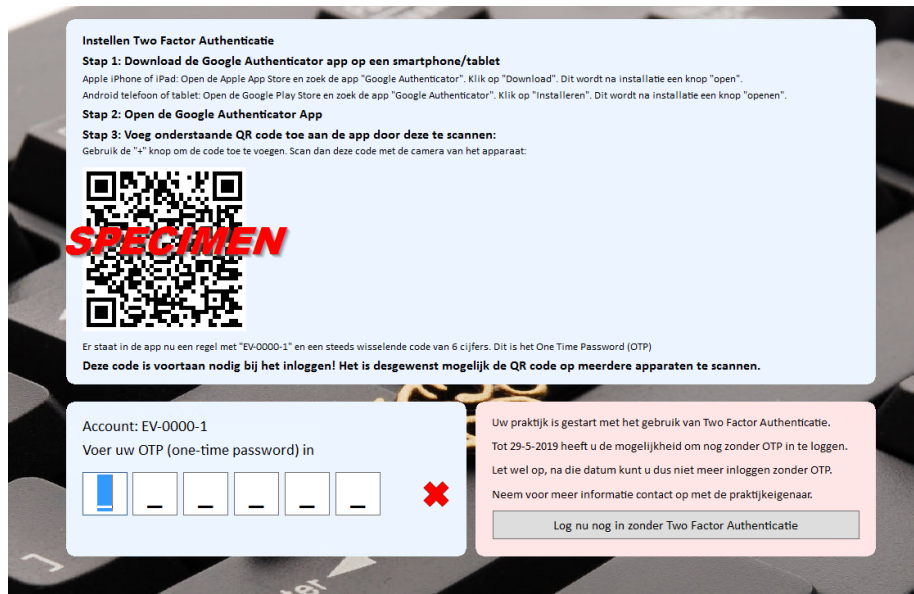
De eerstvolgende keer dat iemand van jullie praktijk inlogt met één van jullie accounts, verschijnt een scherm met een QR code, die gescand kan worden.

Het is handig om iedereen van de praktijk vooraf op de hoogte te brengen van de veranderingen, en iedereen alvast de **Google Authenticator** te laten installeren op hun smartphone/tablet. Die hebben ze nodig om deze QR code te scannen.

Let op: alleen de eerste keer dat er ingelogd wordt, zie je direct de QR code. Daarna kan je die altijd nog wel vinden, in de “Two Factor RDP beheertool” op de server.

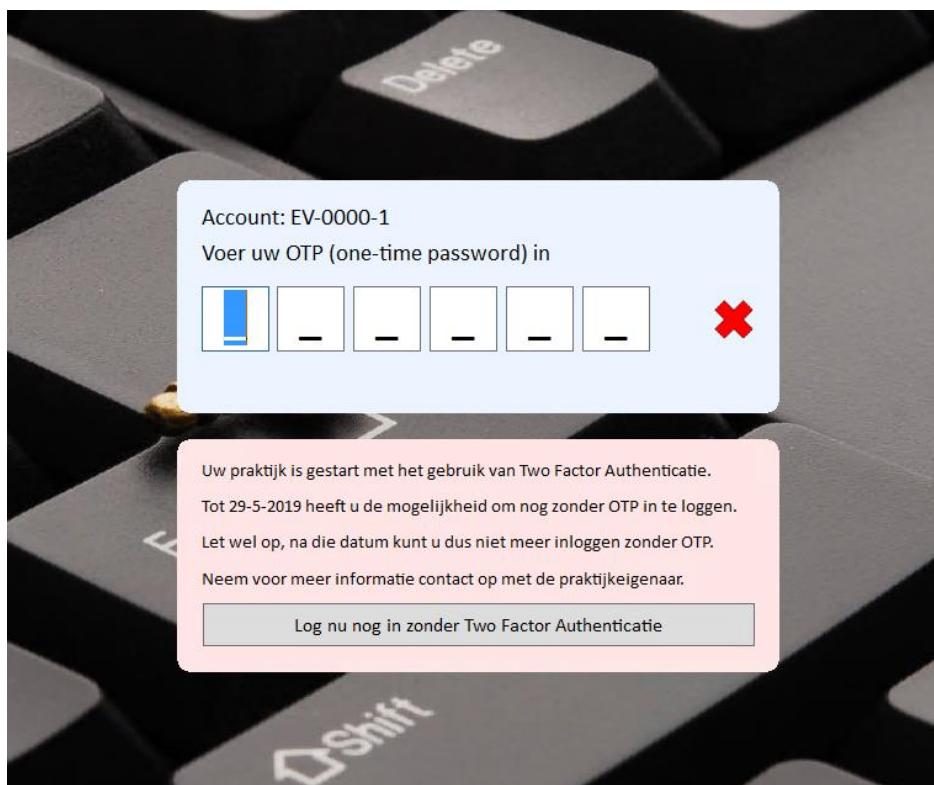
De eerste 14 dagen na het inschakelen is een overgangperiode. Daarin kan je altijd nog zonder TFA inloggen, zie de knop in het rode vak hieronder (Log nu nog in zonder Two Factor Authenticatie). In die periode moet er voor gezorgd worden dat alle medewerkers de juiste QR codes hebben gescand.

Schakel de TFA dus pas in wanneer je weet dat het in de komende 14 dagen voor iedereen mogelijk is om minimaal 1 keer in te loggen en de QR code te scannen.



Als er eenmaal met een account is ingelogd, zie je geen QR code meer, maar alleen onderstaande vakken. Wanneer de QR code eerder al gescand is, kan die OTP hier ingevoerd worden, dan wordt er gewoon ingelogd.

Wanneer die code om welke reden dan ook nog niet gescand is, kan er nu nog ingelogd worden zonder TFA. Het is dan wel belangrijk om zo snel mogelijk alsnog de QR code te scannen, dat kan via de "Two Factor RDP beheertool", waarvoor een snelkoppeling op het bureaublad van de server staat.



Na die overgangperiode is het alleen nog maar mogelijk om met je OTP in te loggen, er is dan dus geen omweg meer mogelijk.



De “Two Factor RDP beheertool”

Op het bureaublad van de server staat een snelkoppeling naar de “Two Factor RDP beheertool”.



Wanneer dat opgestart wordt als TFA nog niet ingeschakeld is, verschijnt dit scherm:



Als TFA wel is ingeschakeld, kunnen in deze tool allerlei zaken worden geregeld.



Wat kan je in de beheertool?

- Hier kan je van elk account (dat ingelogd heeft sinds de TFA is ingeschakeld) de QR code vinden.
- Hier kan je die QR code ook scannen, om voortaan het OTP van het account op je apparaat hebt.
- Hier kan je desgewenst ook alle QR codes scannen, zodat je van elk account het OTP hebt.
- Hier kan je van elk account het OTP zien, handig wanneer een collega zijn/haar apparaat vergeten is en de code nodig heeft om in te loggen.
- Hier kan je een QR code resetten, handig wanneer een medewerker uit dienst gaat. Dan verschijnt bij de eerstvolgende inlog van dat account weer een nieuwe QR code, die daarna dan ook weer hier in de tool zichtbaar wordt.
- Je kan de code in je klembord zetten zodat je de code(s) ook kunt gebruiken via www.evry.nl/otp zonder gebruik van een mobiele telefoon.

Hieronder zie je een rode pijl, in die keuzelijst staan alle accounts van je praktijk, daar kan je dus wisselen van account en dus ook de QR code + OTP (zie blauwe pijl) zien van dat account.

Via de knop bij de groene pijl kan je een QR code resetten, let op, iedereen die de QR code al gescand heeft, kan dan niet meer inloggen met hun OTP. Zij zullen dan dus allemaal opnieuw de QR code moeten scannen. Dit gebruik je vermoedelijk alleen wanneer een medewerker uit dienst gaat. Maar het kan ook handig zijn wanneer een medewerker een nieuwe mobiele telefoon heeft (bij de eerstvolgende inlog verschijnt er dan een nieuwe QR code namelijk, die makkelijk gescand kan worden). Let wel op, dan moet het account wel alleen door die persoon gebruikt worden.



Gebruik maken van “Two Factor Authenticatie” zonder gebruik te maken van een mobiele telefoon

Om gebruik te maken van de “Two Factor Authenticatie” zonder mobiele telefoon, kun je op het bureaublad van Evry-Online de “Two factor beheertool” openen. Selecteer vervolgens het account en klik de QR-code met de rechtermuisknop aan. Onderstaande verschijnt:



- Gebruik je een eigen applicatie voor de “Two Factor Authenticatie” en heb je alleen de “Secret” nodig, klik dan bij A op “Zet secret in klembord” en plak deze in je programma.
- Wil je alleen van dit account de code kunnen zien via de website www.evry.nl/otp klik dan bij B op “Zet OTP Auth string in klembord” en open daarna de website www.evry.nl/otp.



Klik daar op de knop instellen. Plak dan de gegevens in dit scherm en klik op “OK”. Daarna verschijnt hier voortaan de code. Als je de volgende keer weer naar www.evry.nl/otp toe gaat zie je meteen de code weer. Deze wordt lokaal opgeslagen op de computer. Let op: als je de cookies op de computer verwijderd, dan zal de code opnieuw ingesteld moeten worden.

Veel gestelde vragen

Moet ik "Two Factor Authenticatie" inschakelen?

Nee, voorlopig maken wij het alleen mogelijk op onze servers. Je kunt al je medewerkers opdracht geven om altijd te kiezen voor "Log in zonder Two Factor Authenticatie". Mogelijk moeten we het in de toekomst wel verplicht stellen, maar voorlopig is dat niet aan de orde.

Wat kan ik doen als ik mijn apparaat met het OTP vergeten ben?

Bel een collega en laat hem/haar op de server de "Two Factor RDP beheertool" opstarten, daarin kunnen ze jouw account selecteren en het OTP zien dat jij nodig hebt.

Wat ook mogelijk is, is dat alle medewerkers via de beheer tool sowieso alle QR codes scannen, zodat ze van alle accounts de OTP in hun apparaat zien. Op het moment dat je er zelf niet kan, kan je een collega bellen voor jouw OTP code. Die hoeven dan dus niet de beheertool op de server te starten, maar zien jouw OTP direct in hun apparaat.

Ik heb een nieuwe telefoon, hoe krijg ik daar de code in?

Log in via de code op je oude apparaat, start de "Two Factor RDP beheertool" en scan met je nieuwe telefoon de QR code van jouw account. Heb je je oude apparaat niet meer, zie dan het antwoord op de vraag "Wat kan ik doen als ik mijn apparaat met het OTP vergeten ben?".

Ben je de enige die het account op de server gebruikt? Dan kan je (of een collega) via de "Two Factor RDP beheertool" jouw QR code resetten. Bij de eerstvolgende inlog krijg je dan een nieuwe QR code in beeld die je kan scannen op je nieuwe telefoon. **Let wel op:** op alle andere apparaten (van je collega's bijvoorbeeld) werkt hun OTP voor dit account dan niet meer, die moeten dan ook de nieuwe QR code scannen.

Wij delen Online accounts, kan je dan wel met Two Factor Authenticatie werken?

Ja hoor, dat is geen probleem, meerdere mensen kunnen dezelfde QR code scannen. De eerste die inlogt met een bepaald account ziet de QR code automatisch, de anderen kunnen de eerste 14 dagen nog inloggen zonder OTP en via de beheertool ook de QR code vinden en die scannen.