

Tweestapsverificatie via Authenticator-app instellen

Tweestapsverificatie (2FA) is een methode om accounts beter te beveiligen. Inloggen met alleen een wachtwoord is dan niet meer voldoende. De gebruiker moet ook een code gebruiken om in te loggen.

Uitgangspunten vanaf 17 juni 2024:

- 2FA staat aan voor **alle gebruikers met een medewerkersaccount**.
- Het is niet verplicht voor extranetgebruikers.
- Medewerkers kunnen dan alleen inloggen via 2FA met een (Google) Authenticator-app.
- Het beheer van apparaten en accounts ligt bij je organisatie en niet bij Zilliz support. Het resetten van apparaten kan dus niet door support worden uitgevoerd. Het is de verantwoordelijkheid van de organisatie dat er meerdere Zilliz beheerders zijn met toegang tot de module P&O, zodat altijd een beheerder beschikbaar is om gebruikers toegang tot Zilliz te geven of te deblokken.

Al eerder zelf instellen

Een beheerder met recht op module P&O kan de tweestapsverificatie via de Authenticator-app al eerder aanzetten dan de verplichte invoerdatum. Ga hiervoor naar **module P&O > Instellen > Modulegebruik**.

Tweestapsverificatie

medewerkers	<input checked="" type="radio"/> ja <input type="radio"/> nee
standaard methode	Authenticatie app
aanpasbaar voor gebruiker?	<input type="radio"/> ja <input checked="" type="radio"/> nee
extranetters	<input type="radio"/> ja <input checked="" type="radio"/> nee
standaard methode	E-mail
aanpasbaar voor gebruiker?	<input type="radio"/> ja <input checked="" type="radio"/> nee
geldigheid authenticator (uren)	5
geldigheid mail (dagen)	0

De geldigheidsduur van de code van de Authenticator-app kan door een beheerder worden ingesteld in **module P&O > Instellen > Modulegebruik >**. De geldigheidsduur kan maximaal op 24 uur worden ingesteld. Als de geldigheidsduur op 0 uur staat moet je elke keer als je inlogt in Zilliz een nieuwe code invoeren. Als de geldigheidsduur op 24 uur staat moet je eens in de 24 uur bij het inloggen in Zilliz een nieuwe code invoeren.

Authenticator-app

Zilliz werkt in ieder geval met de Google Authenticator-app. Deze kun je downloaden via Google Play of de App Store. Andere Authenticator-apps werken ook. Zilliz geeft geen ondersteuning op de werking van Authenticator-apps, daarvoor verwijzen we je naar de makers van die apps.

- Bij de eerste keer inloggen met 2FA moet de app gekoppeld worden aan Zilliz. De uitleg over het koppelen van je mobiele telefoon is te vinden via: <https://zilliz.nl/inloghulp/>. Deze uitleg is ook voor je medewerkers te lezen voordat ze in Zilliz zijn ingelogd. Scan de QR-code met je app op je telefoon en voer de code in Zilliz in. Het is ook mogelijk om in plaats van de QR-code de getoonde instelsleutel te kopiëren in de Authenticator-app. Als je een QR code scant of instelsleutel overneemt, maar vervolgens géén code invoert in Zilliz, is de koppeling NIET “afgerond” en zal er bij een volgende keer inloggen weer een QR code weergegeven worden. Zilliz is dan mogelijk al wél toegevoegd aan de Authenticator-app, maar de

gegenereerde codes zijn NIET geldig omdat het koppelproces niet afgerond was.
Je ziet dit:



Het koppelen moet in dit geval opnieuw:

- Verwijder de oude regel uit de app
- Scan de QR code of neem de instelsleutel over
- Vul de gegenereerde code in om in te loggen en de koppeling te voltooien
- Als een gebruiker een “onjuiste” code gebruikt, zal het volgende scherm getoond worden:



- Elke 30 seconden genereert de Authenticator-app een nieuwe code. Een gebruiker kan de code voorsnog onbeperkt fout invoeren.
- Gebruik je Zilliz op je telefoon? Je kunt de code op de telefoon kopiëren en plakken door de code op de Authenticator-app lang ingedrukt te houden. Er komt dan een melding dat de code naar het klembord gekopieerd is. Deze kan vervolgens in de mobiele browser ingevoerd worden met de “plakken” functie.

Overige info voor beheerders;

- Medewerkers apparaten kunnen enkel door beheerders gereset worden, net als wachtwoorden.
- Het beheer vindt plaats in module **P&O > P&O Beheer > Medewerker >** op het **tabblad Account** van het betreffende medewerkersdossier.

The screenshot shows the 'Account' management page for a user. At the top, there is a navigation bar with tabs: Medewerker, Adres, Account (highlighted), Cliënten, Beschikbaarheid, Contract, Dossier, Attenderingsservice, and Reminders. Below the tabs, there are several form fields:

- gebruikersnaam ***: A text input field with a green border.
- wachtwoord**: A text input field with a 'reset wachtwoord' link below it.
- locatiemanager ***: Radio buttons for 'ja' and 'nee' (selected).
- beheerder ***: Radio buttons for 'ja' and 'nee' (selected). Below it, a note says: 'Een beheerder kan instellingen wijzigen. Overige gebruikers niet.'
- IP adres**: A text input field with a note: 'Niets ingevuld? Dan geen beperking op IP adres. Meerdere IP adressen scheiden met komma.'

 On the right side, there is a 'modules' section with a list of checkboxes:

- admini
- alle mc
- contrac
- p&o + r
- relaties
- zorg
- zorg + r

 At the bottom, there is a row of buttons: 'opslaan' (green), 'mail activatie' (grey), 'blokkeer' (green), 'annuleer' (dark grey), and 'reset tweestapsverificatie' (green, highlighted with a red box).

Op deze plek kun je een apparaat ontkoppelen, bijvoorbeeld indien de medewerker een nieuwe telefoon heeft. Dat doe je met de knop [reset tweestapsverificatie].

Veelgestelde vragen met antwoorden

Waarom is de tweestapsverificatie verplicht?

De Wet digitale overheid (Wdo) schrijft voor dat er zo zorgvuldig mogelijk wordt omgegaan met zorgdata. Op dit moment is de veiligste manier van inloggen via de tweestapsverificatie, waarbij in de tweede stap een Authenticator-app wordt gebruikt. De tweestapsverificatie maakt het gebruik van Zilliz veiliger. Wij vinden het belangrijk dat onze klanten op een veilige manier in Zilliz werken.

Kan de code voor tweestapsverificatie nog per e-mail binnenkomen?

Vanaf 17 juni 2024 wordt tweestapsverificatie via de Authenticator-app verplicht in Zilliz. De code per e-mail komt dan te vervallen. We adviseren je om eerder dan 17 juni de overstap van e-mail naar de Authenticator-app te maken.

Welke Authenticator-app kan ik gebruiken? Kan ik alleen de Google Authenticator gebruiken?

Er zijn verschillende Authenticator-apps. Wij hebben de Google Authenticator-app getest met Zilliz. We weten zeker dat deze app werkt. Je kunt ook andere Authenticator-apps gebruiken. Op de site van [de consumentenbond](#) staat dat de meest gebruikte apps de Google Authenticator ([Android](#), [Apple](#)), Microsoft Authenticator ([Android](#), [Apple](#)) en Twilio Authy ([Android](#), [Apple](#)) zijn. We doen verder geen aanbevelingen.

Wordt de tweestapsverificatie ook verplicht voor extranetgebruikers?

Op 17 juni 2024 zetten wij de tweestapsverificatie via de Authenticator-app aan voor medewerkers. Voor extranetgebruikers zetten we deze functie niet aan. Je kunt deze functie wel zelf aanzetten voor extranetgebruikers. Dit doe je in: module P&O > Instellen > Modulegebruik. Onder Tweestapsverificatie zet je deze functie bij extranetgebruikers op: ja en selecteer je Authenticator-app.

Kan ik de tweestapsverificatie aanzetten voor enkele medewerkers?

Nee. Je kunt in de **module P&O > Instellen > Modulegebruik > onder Tweestapsverificatie** de tweestapsverificatie aanzetten, dit geldt meteen voor alle medewerkers. Tot 17 juni 2024 is het mogelijk om te kiezen voor e-mail of Authenticator-app. Na 17 juni moet tweestapsverificatie altijd via de Authenticator-app, we raden dus aan om meteen die optie te kiezen.

Hoe vaak moet ik de code invoeren?

Je kunt zelf instellen hoe vaak om een code gevraagd wordt. In de **module P&O > Instellen > Modulegebruik > onder Tweestapsverificatie > geldigheid authenticator (uren)** kun je aangeven hoeveel uren het duurt voordat Zilliz weer om een verificatiecode vraagt, met een minimum van 0 (dus bij elke inlog) en een maximum van 24 uren.

Wat moet ik doen als de code niet werkt?

Als de code van jouw Authenticator-app niet werkt, kun je de volgende stappen doorlopen. Kijk daarnaast ook in de helpfunctie van jouw app voor mogelijke oplossingen.

- Controleer of je de meest recente code gebruikt. Elke 30 seconde krijg je een nieuwe code.
- Controleer of de ingevoerde code hoort bij het Zilliz-account waarop je probeert in te loggen.
- Controleer de tijd op je telefoon en computer. Als de tijd van beide apparaten niet gelijk loopt klopt de code niet. Je kunt de tijdzone en klok van je telefoon op automatisch zetten, waardoor dit meestal goed gaat. In de Google Authenticator-app kun je daarnaast ook bij instellingen een tijdscorrectie voor codes uitvoeren.
- Controleer of jouw apparaat goed gekoppeld is. Krijg je op de inlogpagina opnieuw de QR code te zien? Dan is de Authenticator-app niet juist gekoppeld. Zilliz is al toegevoegd aan de Authenticator-app, maar de gegenereerde code is niet geldig omdat het koppelproces op dat moment niet goed was afgerond. Het koppelen van de Authenticator-app moet dan opnieuw. Zie hiervoor inloghulp 2FA voor medewerkers(link: <https://zilliz.nl/inloghulp/>)

Als bovenstaande stappen niet werken, laat dan de tweestapsverificatie resetten.

- Een beheerder met recht op **module P&O** reset de tweestapsverificatie bij **module P&O > P&O beheer > Medewerkers** > selecteer de medewerker > **tabblad Account** en klik op **[reset tweestapsverificatie]**.
- Je krijgt als medewerker bij het inloggen opnieuw de QR-code te zien en kan Zilliz opnieuw koppelen. Verwijder wel eerst het oude Zilliz account uit de Authenticator-app en koppel opnieuw je account, je krijgt een nieuwe code.

Werkt het nog niet, dan zijn er twee opties. Voor beide opties laat je de tweestapsverificatie (opnieuw) resetten:

- Gebruik dezelfde Authenticator-app op een ander apparaat, bijvoorbeeld met een extensie in de browser. Koppel de Authenticator-app en genereer hiermee de code.
- Gebruik een andere Authenticator-app op hetzelfde apparaat. Koppel deze Authenticator app en genereer hiermee de code.

Wat te doen bij een nieuwe telefoon of ander mobiel apparaat?

Als je wilt wisselen van telefoon en je op je oude telefoon in de Google Authenticator-app bent ingelogd in je Google account, dan hoef je de nieuwe telefoon niet opnieuw te koppelen aan Zilliz. Op je nieuwe telefoon installeer je de Google Authenticator-app en daarin log in op jouw Google account. De koppeling met Zilliz blijft dan behouden en je kunt de codes uit de Authenticator-app blijven gebruiken zoals je gewend was

Mocht dit toch niet goed gaan, dan kan een beheerder met recht op module P&O de tweestapsverificatie resetten. In de **module P&O > P&O beheer > Medewerkers** > selecteer je de medewerker > **op het tabblad Account** klik je op de knop **[reset tweestapsverificatie]**. De medewerker krijgt dan opnieuw de QR-code te zien bij het inloggen en kan de telefoon opnieuw koppelen.

Kan ik meerdere telefoons gebruiken om dezelfde code te genereren?

Als je meerdere gedeelde werktelefoons hebt, die afwisselend door medewerkers gebruikt worden, kan het zijn dat je al die telefoons dezelfde code wilt laten genereren, zodat het niet uitmaakt welke telefoon de medewerker bij zich heeft.

Dat kan, maar vraagt wel een goede afstemming. Om meerdere telefoons of apps te koppelen aan hetzelfde account moet je namelijk met alle telefoons tegelijk, op precies hetzelfde moment, de QR-code scannen. Daarna geven alle telefoons dezelfde verificatiecode. Omdat de code elke 30 seconde verandert, is het belangrijk dat je dit echt tegelijk doet. Het is niet nodig dat hiervoor dezelfde Authenticator-app gebruikt wordt. Je zou bijvoorbeeld een wachtwoordmanager en een telefoon tegelijk kunnen koppelen.

Als je bij de Authenticator-app inlogt met een algemeen e-mailadres en op meerdere telefoons bij de Authenticator-app inlogt met dat e-mailadres, dan krijg je op alle telefoons dezelfde codes.

Als je de telefoons niet deelt, maar alleen persoonlijk gebruikt, kun je ook gebruik maken van de tweestapsverificatie via een wachtwoordmanager en die wachtwoordmanager op meerdere apparaten instellen. Je krijgt dan via de wachtwoordmanager de code om in te loggen. Deze is op alle apparaten gelijk.

Kan ik gebruik maken van de Authenticator-app zonder een smartphone?

We raden aan om de Authenticator-app op je telefoon te gebruiken, maar je hebt niet per se een smartphone nodig om gebruik te kunnen maken van de tweestapsverificatie. Je kunt ook gebruik maken van een wachtwoordmanager op jouw computer om een code te genereren. We gebruiken bij ZilliZ zelf 1Password maar je kunt ook andere wachtwoordmanagers gebruiken.

Een andere oplossing is een browserextensie of desktop app gebruiken. Je kunt in de browser zoeken naar extensies. Een extensie die je kunt gebruiken is bijvoorbeeld: authenticator.cc van mymindstorm. Andere extensies werken waarschijnlijk ook.

Kan ik meerdere ZilliZ-accounts koppelen aan dezelfde Authenticator-app?

Je kunt in de gangbare Authenticator-apps meerdere accounts koppelen aan dezelfde site. Je kunt dus verschillende ZilliZ-accounts koppelen aan dezelfde Authenticator-app.

Kan ik gebruik maken van de Authenticator-app in een internetbrowser en op de smartphone tegelijk?

Wij weten niet van het bestaan van een gratis Authenticator-app die tegelijk werkt op een internetbrowser en de smartphone. Je kunt wel gebruik maken van een wachtwoordmanager en deze installeren op verschillende apparaten, zoals een desktop en een smartphone.

Hoe werkt de Google Authenticator-app?

ZilliZ support ondersteunt bij het gebruik van ZilliZ. We kunnen je niet ondersteunen bij het gebruik van de Authenticator-app. Meer informatie over het gebruik van de Authenticator app van Google

lees je in de support van Google:

<https://support.google.com/accounts/answer/1066447?hl=nl&co=GENIE.Platform%3DAndroid>

Krijg je de melding dat de code niet klopt, scroll dan naar Veelvoorkomende problemen > Een onjuiste code verhelpen.

Moet mijn telefoon internet hebben om de Authenticator-app te gebruiken?

Nee, de code die je bij het inloggen nodig hebt wordt ook gegenereerd zonder internetverbinding.

Waarom krijg ik opnieuw de QR-code te zien terwijl ik Zilliz al een keer gekoppeld heb?

Bij de eerste keer inloggen met tweestapsverificatie moet de Authenticator-app gekoppeld worden aan Zilliz. De uitleg over het koppelen van je mobiele telefoon is te vinden via:

<https://zilliz.nl/inloghulp/>.

Als je een QR-code scant maar vervolgens géén code invoert in Zilliz, is de koppeling niet afgerond. Bij een volgende keer inloggen wordt weer een QR-code weergegeven. Je Zilliz account is dan mogelijk al wél toegevoegd aan de Authenticator-app, maar de gegenereerde code is NIET geldig omdat het koppelproces eerder niet afgerond is. Het koppelen moet in dit geval opnieuw:.

- Verwijder de oude regel uit de Authenticator app
- Scan de QR-code
- Vul de gegenereerde code in om in te loggen en de koppeling te voltooien

Ik gebruik één mobiel apparaat met daarop Zilliz en de Authenticator-app. Hoe kan ik de Authenticator-app koppelen?

Als de Authenticator-app gekoppeld moet worden aan je account, verschijnt bij het inloggen tegelijk met de QR-code een instelsleutel. Je kunt de instelsleutel kopiëren middels het kopieericoontje. Deze sleutel kan vervolgens in de Authenticator-app ingevoerd worden met de “plakken”-functie.

Ik werk in Zilliz op mijn mobiel, kan ik dan ook de Authenticator-app gebruiken?

Je kunt in Zilliz werken op je mobiel en tegelijk de Authenticator-app gebruiken. Je kunt de code op de telefoon kopiëren en plakken door de code op de Authenticator-app lang ingedrukt te houden. Er komt dan een melding dat de code naar het klembord gekopieerd is. Deze code kan vervolgens in de browser ingevoerd worden met de “plakken”-functie.

Welke tweestapsverificatie-methode bevelen jullie aan?

Wij adviseren het gebruik van een Authenticator app. Je kunt zelf een keuze maken welke app je hiervoor gebruikt. Voor Zilliz hebben we de Google Authenticator-app getest, en weten we dat alles goed werkt. Voor meer informatie over tweestapsverificatie kun je kijken op de site van de Consumentenbond. <https://www.consumentenbond.nl/veilig-internetten>