

2.53 Handleiding Twee-factor authenticatie (met software-token)

In Magister is veel persoonlijke informatie opgeslagen, dus aandacht voor Informatiebeveiliging en Privacy (IBP) is van groot belang. Een eenvoudige manier om het beveiligingsniveau van Magister te verhogen is twee-factor-authenticatie (2FA). Bij 2FA is naast het invoeren van een wachtwoord nog een tweede handeling nodig om in te loggen. Dat is minder omslachtig dan men denkt. Dankzij deze dubbele beveiliging voorkom je dat onbevoegde personen de gegevens in Magister kunnen raadplegen (of erger nog: wijzigen). Zelfs als iemand je inloggegevens heeft afgekeken of op een andere manier bemachtigd, heeft hij nog altijd geen toegang tot Magister.

Twee-factor-authenticatie met software-token instellen (voor M5 (.RDP) en M6)

Met twee-factor-authenticatie met software-token kan alleen worden ingelogd via een app op de smartphone.

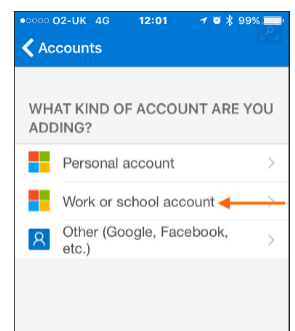
Ga naar de Play Store, de Apple Store of de Windows store en zoek de app met de zoekterm Microsoft Authenticator of Google Authenticator en installeer de app op de smartphone.



Microsoft Authenticator
Microsoft Corporation
#30 in Productiviteit
★★★★★ 4,4, 27 beoordelingen
Gratis

In de AuthenticatorApp moet vervolgens geklikt worden op 'Account toevoegen' (drie puntjes in de App rechts boven in het telefoonscherm) en vervolgens kiezen voor 'Werk- of schoolaccount'.

De App opent vervolgens de QR-scanner op de smartphone. Deze scanner richt je op de QR-code (zwart-witte bokjes) die in het Magisterscherm staat in



Na het inscannen geeft de App een code die overgetypt moet worden in het getoonde Magisterscherm M5 of M6

NB. Moet er ingelogd worden in meerdere databases, dan per database bovenstaande acties herhalen (toevoegen werk- of schoolaccount) in dezelfde App.

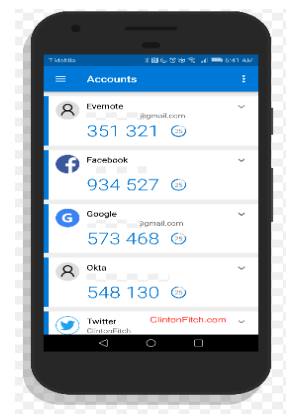
Twee-factor-authenticatie in Magister5 met software-token:

Het team Administratieve Controle en Onderwijsinrichting zal voor alle 2FA gebruikers in Magister.rdp aangeven dat de gebruiker in gaat loggen via twee-weg-authenticatie met software-token.

Bij de eerstvolgende inlog voert de gebruiker de gebruikersnaam en het wachtwoord in. De gebruiker waarvoor de software token is ingesteld krijgt hierna de volgende melding:



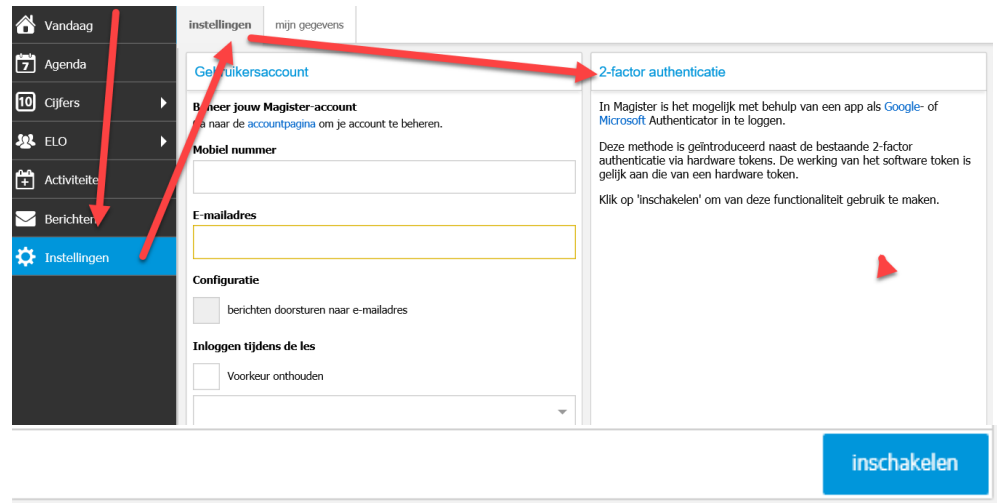
Na het intypen van de 'koppelingscode' is de app klaar voor gebruik en produceert het om de 30 seconde een numerieke code. Deze code is vanaf nu nodig om in te kunnen loggen in Magister.



Twee-factor-authenticatie in Magister6 met software-token:

In Magister 6 kunnen docenten, mentoren, teamleiders zelf bij instellingen de twee-factor-authenticatie activeren. Na het inloggen in Magister kan worden geklikt op instellingen en kan een vinkje worden gezet bij twee-factor-authenticatie:

Om in Magister 6 2-factor authenticatie te activeren, log je eerst in, in Magister6 en kies je vervolgens voor 'Instellingen'. In het Instellingenschermb kan je vervolgens klikken op 'Inschakelen' in het menu 2-factor authenticatie.



Hierna vraagt M6 opnieuw om je wachtwoord en word je vervolgens verzocht om de Authenticatie-app op je telefoon te openen en de QR-code in te scannen. Het nummer die verschijnt in de App moet vervolgens worden ingevoerd bij Verificatietoken in M6. Klik vervolgens op Koppelen.



Vanaf nu moet je, wanneer je Magister6 opnieuw opstart, inloggen met je gebruikersnaam en wachtwoord gevolgd door de code die de App heeft gegenereerd voor betreffende school (database).

