



Rijksvastgoedbedrijf

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Google Authenticator instellen

In het kader van informatiebeveiliging is het van belang dat sommige webapplicaties extra beveiligd worden met 2FA, om goede bescherming te bieden tegen ongewenste toegang tot bijvoorbeeld gevoelige data.

Met 2FA voeg je een extra beveiligingslaag toe aan jouw account. Nadat je dit heb ingesteld, log je in twee stappen in op jouw account:

1. Iets dat je weet (jouw gebruikersnaam en wachtwoord);
2. Iets dat je hebt (zoals jouw telefoon / verificatiecode).

Twee weg authenticatie (Two Factor Authentication), kortweg aangeduid als 2FA, wordt binnen het Rijksvastgoedbedrijf ook gebruikt als extra beveiliging voor sommige webapplicaties.

Daarvoor gebruiken wij de app **Google Authenticator**. Hierop ontvang je tijdens het inlogproces een code die je als extra stap bij het inloggen moet invoeren.

In deze handleiding is beschreven hoe je de app tot jouw beschikking krijgt en hoe je deze in moet stellen en gebruiken.

Inhoudsopgave

1. Google Authenticator installeren.....	3
1.1 Download alvast de app op jouw telefoon.....	3
2. Instellen Google Authenticator app	4
2.1 Invoeren verificatiecode.....	4
2.2 Scan de QR-code	4
2.3 Gebruik de juiste en geldige 2FA code!	7
Colofon	7

1. Google Authenticator installeren

Voor Twee weg authenticatie (Two Factor Authentication), kortweg aangeduid als 2FA, gebruiken we de app Google Authenticator. Hierop ontvang je tijdens het inlogproces een code die je als extra stap bij het inloggen moet invoeren.

1.1 Download alvast de app op jouw telefoon

Dat mag eventueel ook op jouw eigen privé-telefoon als je dat makkelijker vindt. Je kunt er meerder websites in opslaan die 2FA authenticatie gebruiken.

Voor Samsung ga naar de Playstore;



Voor iPhone ga naar de Appstore



Zoek naar Google Authenticator en installeer deze;

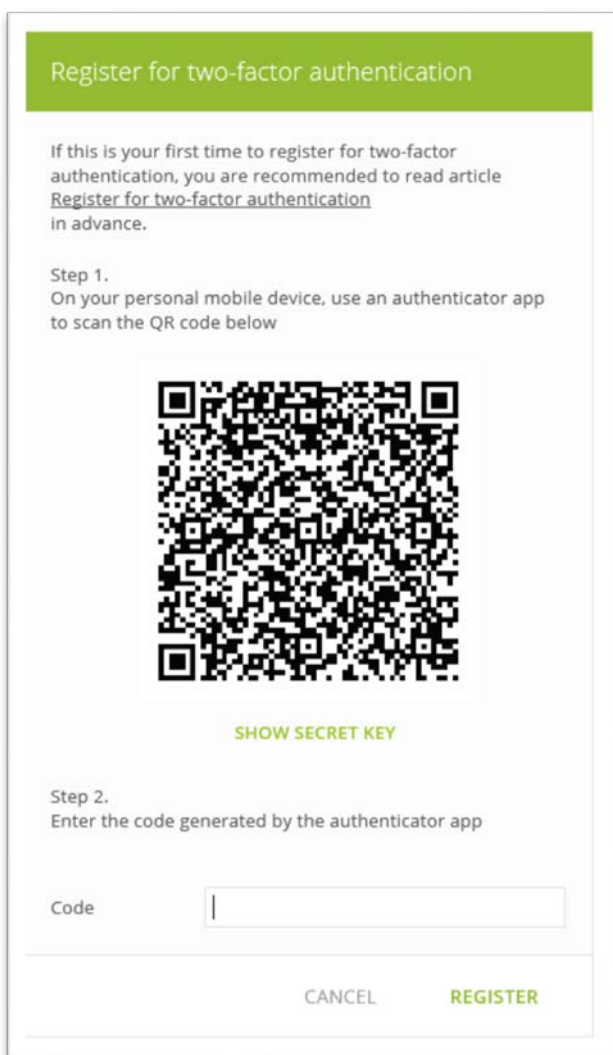


2. Instellen Google Authenticator app

2.1 Invoeren verificatiecode

Vanaf het moment dat in Relatics de 2FA wordt geactiveerd krijg je bij het inloggen eerst een inlogscherm waarbij je jouw gebruikersnaam en wachtwoord moet invoeren.

Daarna krijg je onderstaand scherm, waarbij je een verificatiecode moet gaan invoeren. Laat dit scherm open staan!



Register for two-factor authentication

If this is your first time to register for two-factor authentication, you are recommended to read article [Register for two-factor authentication](#) in advance.

Step 1.
On your personal mobile device, use an authenticator app to scan the QR code below



[SHOW SECRET KEY](#)

Step 2.
Enter the code generated by the authenticator app

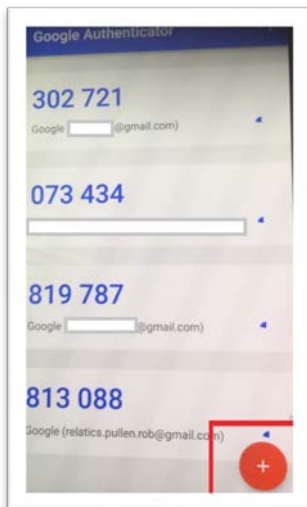
Code

[CANCEL](#) [REGISTER](#)

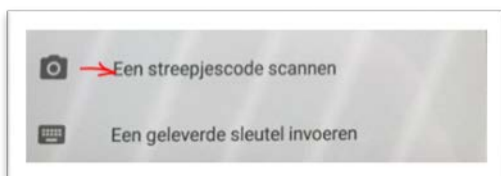
2.2 Scan de QR-code

Open nu de Google Authenticator app op jouw telefoon;

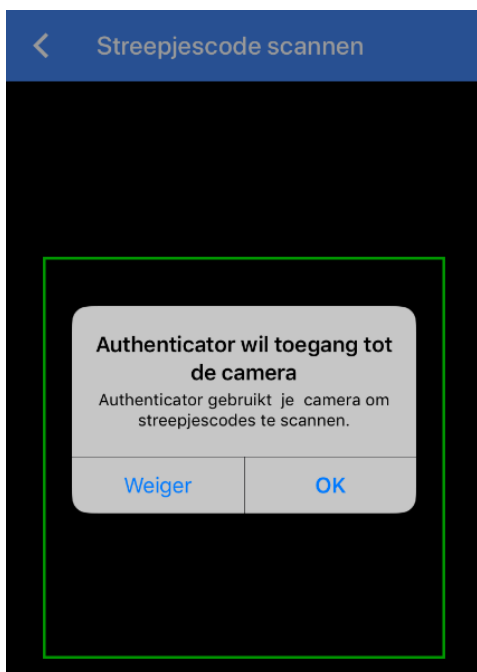
Als je op meerdere websites 2FA gebruikt, heb je voor elke site apart al hier een code generator staan. Tussen haakjes wordt weergegeven voor welke site een van de codes is.



Druk op het plusteken (+) en kies voor “Een streepjescode scannen”.



Er opent een kader en mogelijk wordt gevraagd of de Authenticator toegang mag tot de camera op jouw telefoon.



Klik hier op OK, om toegang tot de camera te verlenen (nodig om zo de QR-code te kunnen scannen;

Houdt nu jouw telefoon voor de QR-code op het beeldscherm en richt zodanig dat de code binnen het groene kader past.

Druk op Volgende als je dat gedaan hebt

Er verschijnt een code in de app op jouw telefoon. Voer deze code in

Register for two-factor authentication.

If this is your first time to register for two-factor authentication, you are recommended to read article [Register for two-factor authentication](#) in advance.

Step 1.
On your personal mobile device, use an authenticator app to scan the QR code below



[SHOW SECRET KEY](#)

Step 2.
Enter the code generated by the authenticator app

Code 

[CANCEL](#) [REGISTER](#)

Als je er te lang over doet om de QR-code met jouw telefoon te scannen, dan is de zgn. 'Secret Key' verlopen en krijg je onderstaande melding.

Klik op Close en voer je gebruikersnaam en wachtwoord opnieuw in. Je krijgt dan een volgende poging om de QR-code te scannen.

Secret key expired

Secret key has expired. No problem. Two-factor authentication might be new to you and obviously it takes you some time to prepare and read for example article [Register for two-factor authentication](#)

However, a QR code is valid for only three minutes.

To provide you with a fresh QR code, you are requested to enter your username and password once again.

[CLOSE](#)

Daarna zal de registratie wel lukken, en krijg je een bevestigingsscherm en tevens een mail toegestuurd.

Registration complete

You have successfully registered for two-factor authentication.

You are about to access Relatics now.

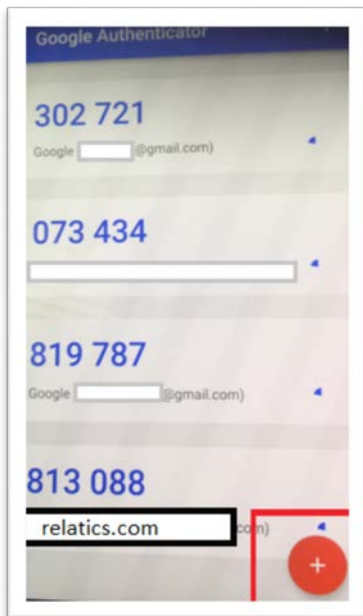
[CLOSE](#)

2.3 Gebruik de juiste en geldige 2FA code!

Elke volgende keer dat je nu met jouw account en wachtwoord inlogt in Relatics, krijg je een tweede scherm krijgen waarin je een verificatiecode kunt invoeren.

In de Google Authenticator zie je (indien je deze ook voor andere websites met 2FA gebruikt) meerdere codes onder elkaar staan. Tussen haakjes staat er onder voor welke site de betreffende code is.

Gebruik dus de juiste code waar relatics.com bij staat! De andere werken daar niet!



Geldigheid code

Deze code wordt elke 30 seconden opnieuw gegenereerd. Het blauwe schijfje achter de code wordt steeds kleiner. Op het moment dat deze geheel verdwijnt, is de code niet meer geldig. Daarna wordt er een nieuwe code weergegeven, die dan geldig is.

Colofon

Functioneel beheer

Afdeling Proces- en Informatiemanagement

Directie Portefeuillestrategie & Portefeuillemanagement

Rijksvastgoedbedrijf

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Korte Voorhout 7 | 2511 CW | Den Haag

Postbus 16700 | 2500 BB | Den Haag

Postbus.rvb.functioneelbeheer@rijksoverheid.nl