Sikkerhed

Lær hvordan du kan optimere sikkerheden på din hjemmeside

- Wordfence
  - Opsætning af 2FA

Wordfence

Opsætning af 2FA

> English version below

Opsætning af 2FA gennem Wordfence

Denne guide viser, hvordan du aktiverer **to-faktor-godkendelse (2FA)** på din WordPress-bruger via Wordfence. 2FA giver et ekstra sikkerhedslag ved login og beskytter din hjemmeside mod uautoriseret adgang.

Hvad er 2FA?

To-faktor-godkendelse (2FA) er en ekstra sikkerhedsforanstaltning, der beskytter din Wordpress bruger. Ud over dit almindelige login med brugernavn og adgangskode skal du også bekræfte din identitet med en ekstra kode. Denne kode genereres typisk i en autentificeringsapp på din telefon og ændrer sig løbende.

Hvorfor skal jeg tilføje 2FA?

Ved at aktivere 2FA gør du det langt sværere for uvedkommende at få adgang til din konto. Selv hvis nogen får fat i din adgangskode, kan de stadig ikke logge ind uden den ekstra kode fra din telefon. Det er derfor en effektiv måde at beskytte din hjemmeside og dine data mod uautoriseret adgang.

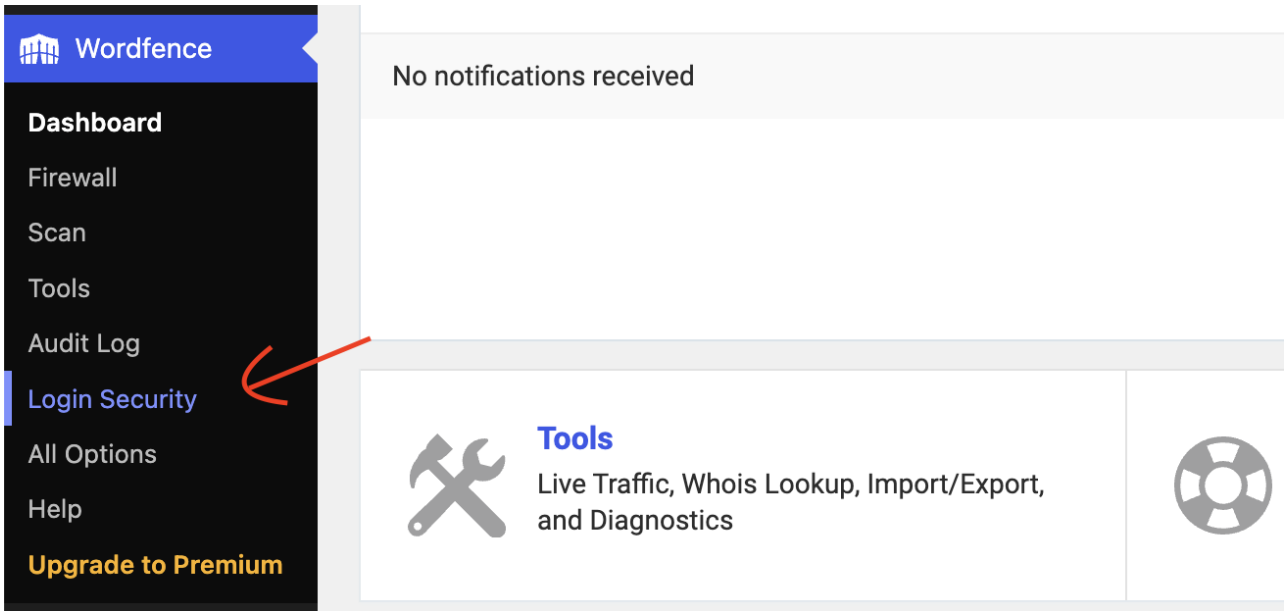
Før du går i gang

Før du aktiverer 2FA, skal du have adgang til din WordPress-administrator og en smartphone. Du skal også installere en autentificeringsapp på din telefon, fx **Google Authenticator** eller **Microsoft Authenticator**. Disse apps genererer de engangskoder, der bruges til at bekræfte dit login.

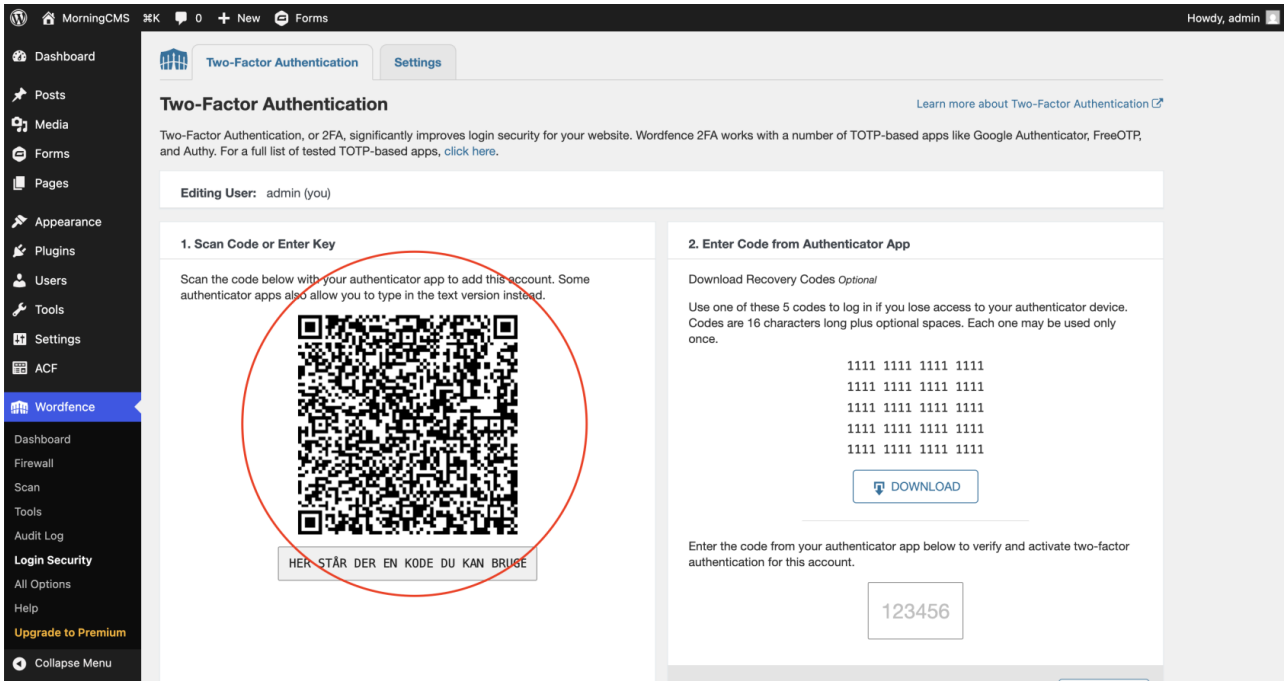
Sådan aktiverer du 2FA

1. Log ind på din hjemmeside med din administrator bruger.

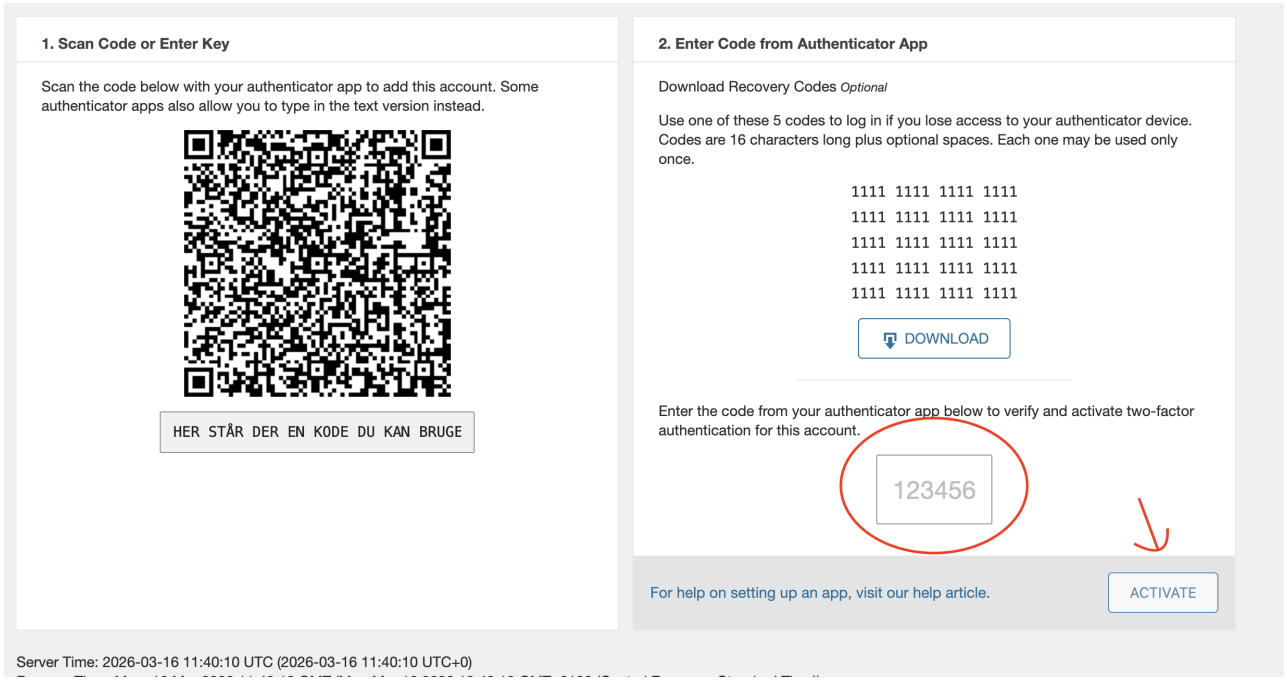
2. Gå til **Wordfence → Login Security** i menuen, og åbn fanen **Two-Factor Authentication**



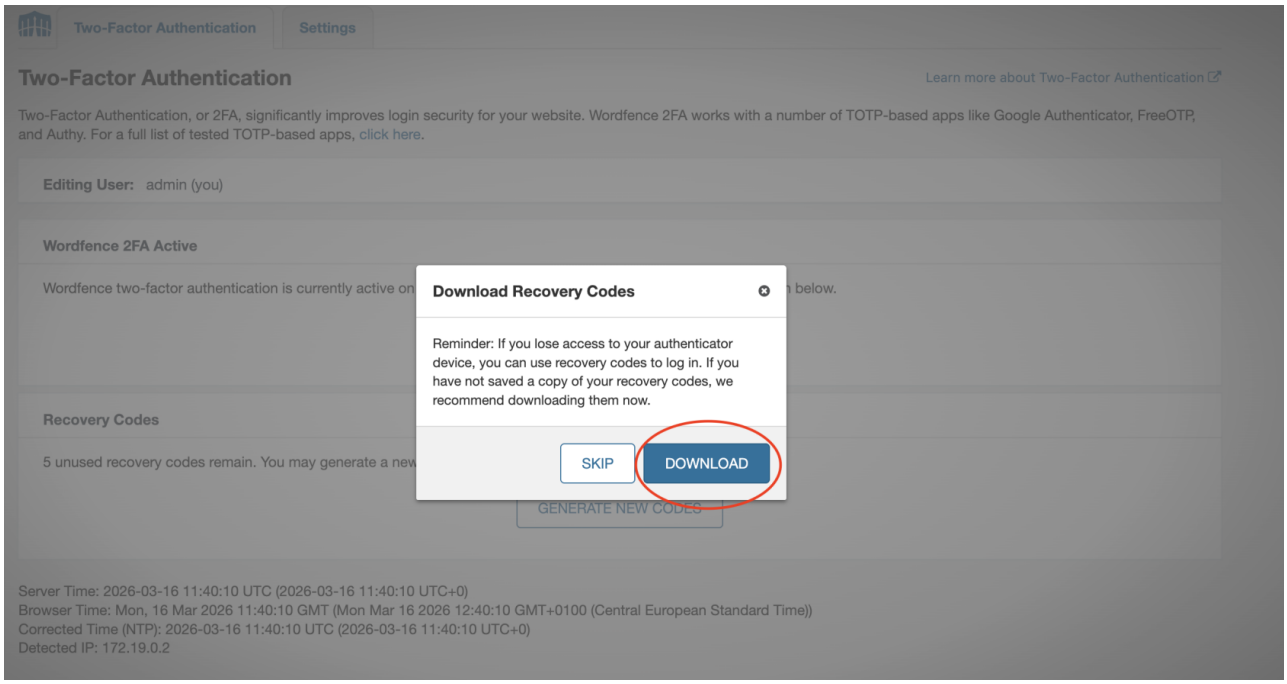
3. Scan QR-koden med din autentificeringsapp på telefonen.



4. Indtast den kode, som appen genererer, for at bekræfte opsætningen.



5. Gem dine **backupkoder**, så du stadig kan logge ind, hvis du mister din telefon.



Hvad hvis jeg mister min telefon?

Hvis du mister din telefon, kan du stadig få adgang til din konto ved hjælp af de **backupkoder**, som blev genereret under opsætningen af 2FA. Det er derfor vigtigt at gemme disse et sikkert sted. Hvis du ikke længere har adgang til dine backupkoder, kan en administrator på hjemmesiden hjælpe med at nulstille din 2FA.

Anbefaling

Det anbefales at aktivere 2FA for alle brugere med administrator- eller redaktørrettigheder. På den måde mindsker man risikoen for, at uvedkommende får adgang til hjemmesiden.

Setting up 2FA

Setting up 2FA through Wordfence

This guide shows you how to enable two-factor authentication (2FA) for your WordPress user through Wordfence. 2FA adds an extra layer of security when logging in and protects your website from unauthorized access.

What is 2FA?

Two-factor authentication (2FA) is an additional security measure that protects your WordPress user account. In addition to your regular login with username and password, you must also verify your identity with an additional code. This code is typically generated in an authentication app on your phone and changes continuously.

Why should I add 2FA?

By enabling 2FA, you make it much harder for unauthorized users to access your account. Even if someone obtains your password, they still cannot log in without the additional code from your phone. It is therefore an effective way to protect your website and your data from unauthorized access.

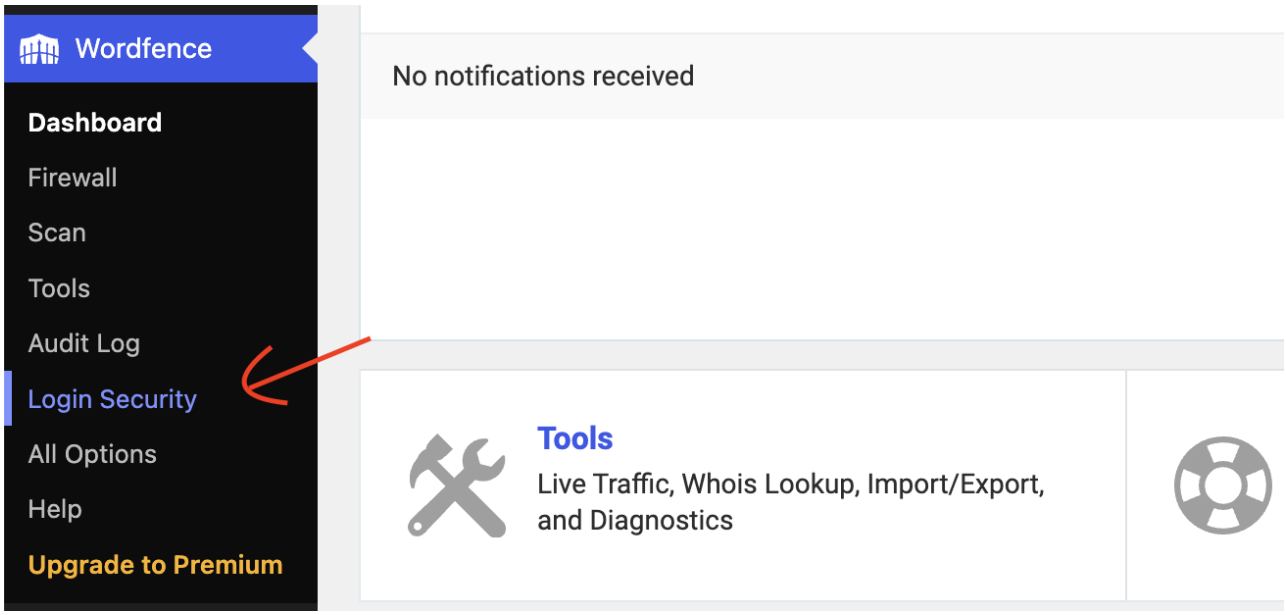
Before you get started

Before enabling 2FA, you need access to your WordPress administrator account and a smartphone. You also need to install an authentication app on your phone, such as Google Authenticator or Microsoft Authenticator. These apps generate the one-time codes used to verify your login.

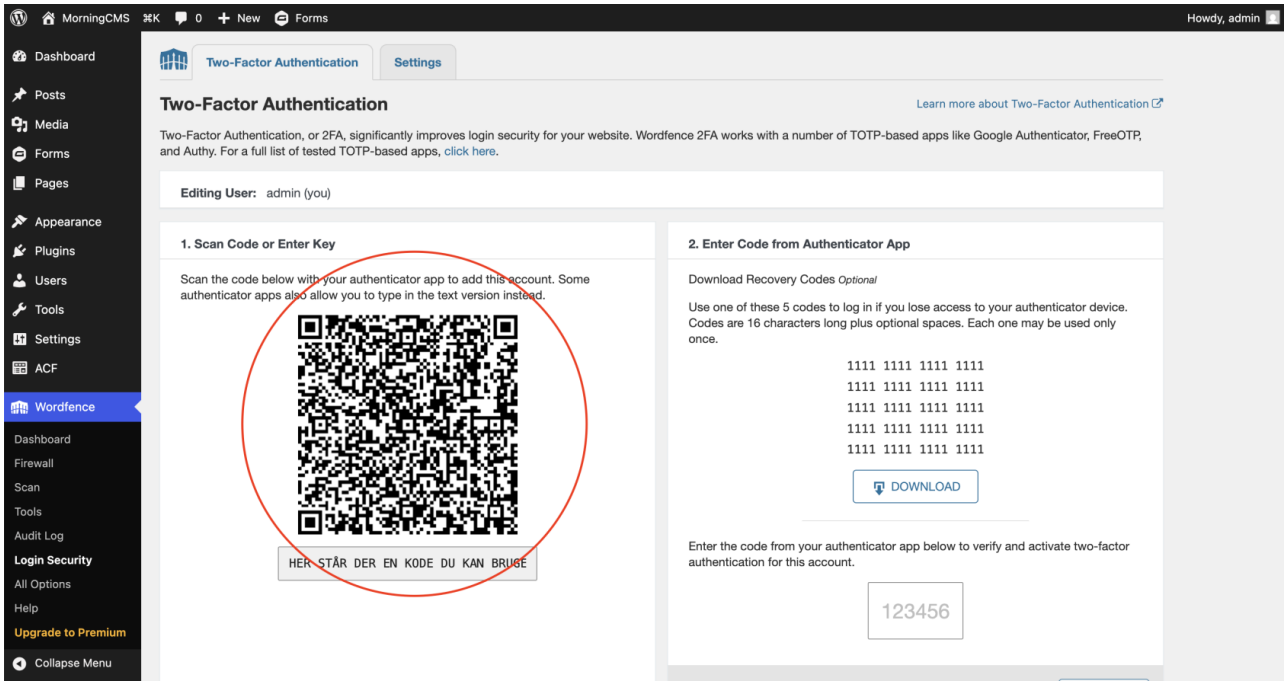
How to enable 2FA

1. Log in to your website with your administrator user.

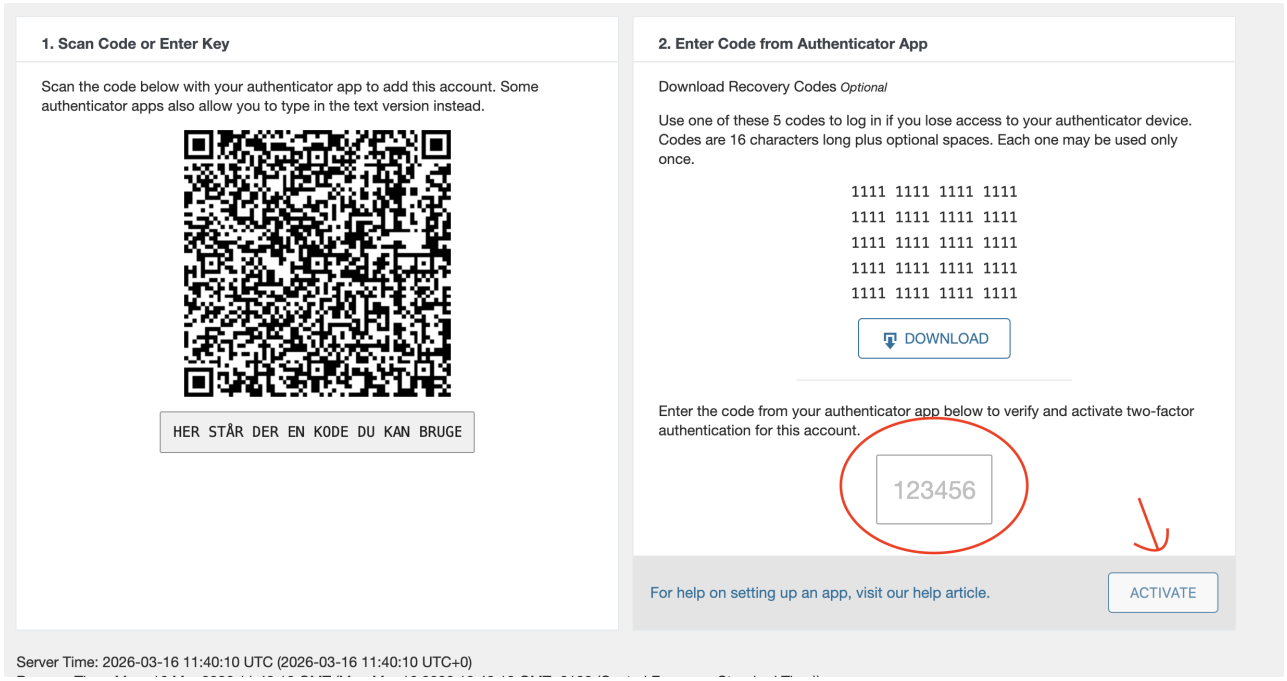
2. Go to **Wordfence → Login Security** in the menu, and open the **Two-Factor Authentication** tab.



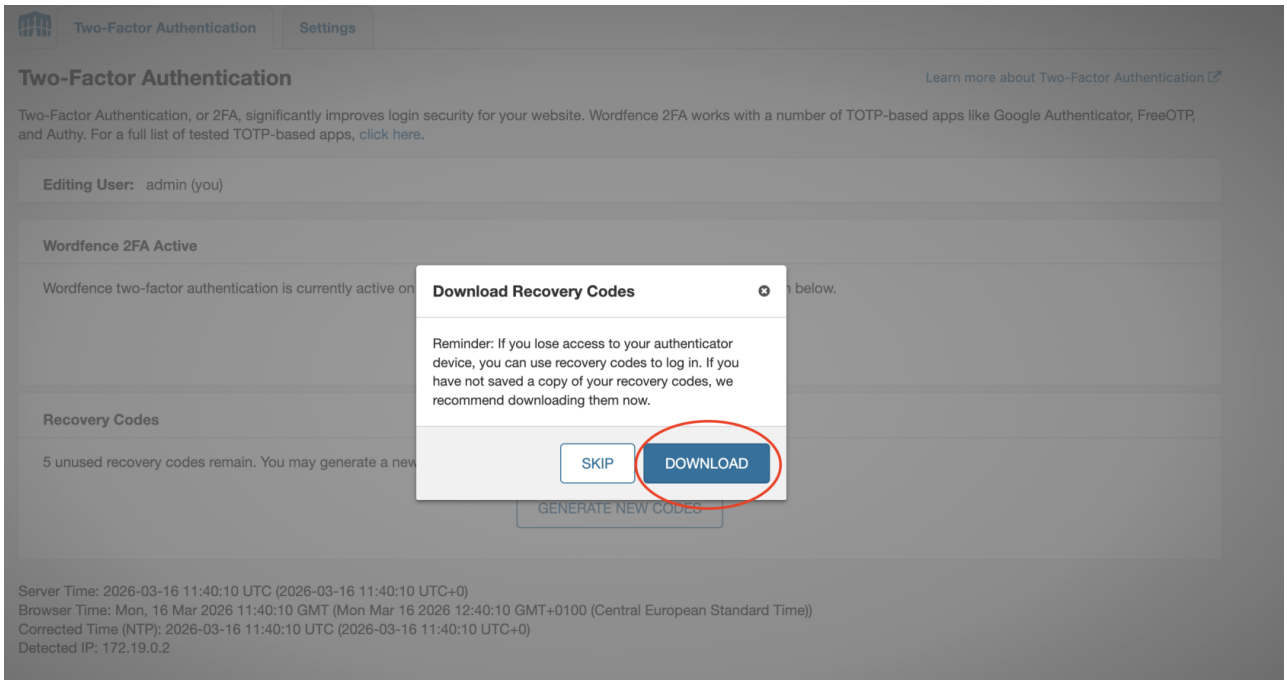
3. Scan the QR code with the authentication app on your phone.



4. Enter the code generated by the app to confirm the setup.



5. Save your backup codes so you can still log in if you lose your phone.



What if I lose my phone?

If you lose your phone, you can still access your account using the backup codes that were generated during the 2FA setup. It is therefore important to store them in a safe place. If you no longer have access to your backup codes, an administrator on the website can help reset your 2FA.

Recommendation

It is recommended to enable 2FA for all users with administrator or editor permissions. This reduces the risk of unauthorized users gaining access to the website.