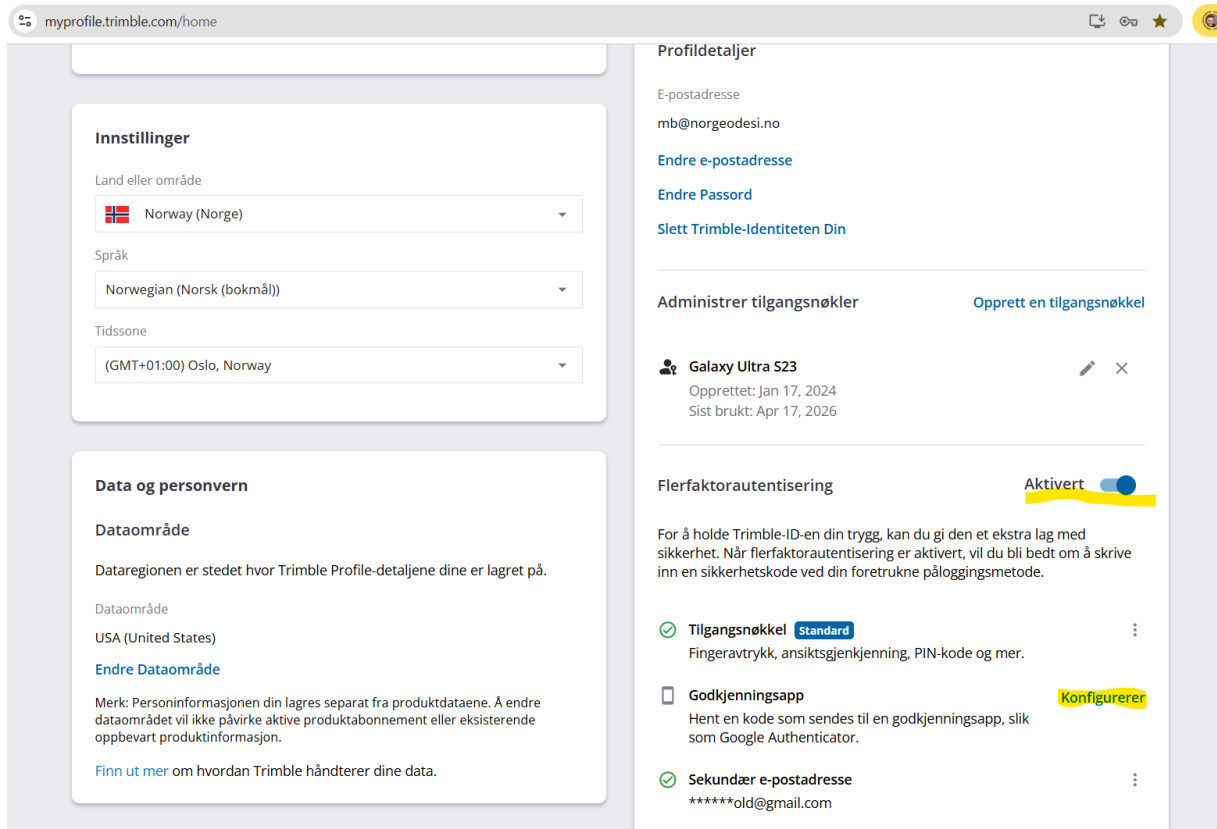


## Hvordan sette opp to-faktor med delt Trimble-ID (TID)

### Alternativ A: Authenticator-app

#### Gå til [myprofile.trimble.com](https://myprofile.trimble.com)



The screenshot shows the user profile page on myprofile.trimble.com. The page is divided into several sections:

- Innstillinger**: Settings for Land eller område (Norway (Norge)), Språk (Norwegian (Norsk (bokmål))), and Tidssone (GMT+01:00) Oslo, Norway).
- Data og personvern**: Dataområde (USA (United States)) and a note about data handling.
- Profildetaljer**: E-postadresse (mb@norgeodesi.no), Endre e-postadresse, Endre Passord, and Slett Trimble-Identiteten Din.
- Administrer tilgangsnøkler**: A section for managing access keys, with a button to create a new one.
- Flerfaktoraутентisering**: Multi-factor authentication settings, currently activated. It lists three methods: Tilgangsnøkkel (Standard), Godkjenningsapp (highlighted as Konfigurerer), and Sekundær e-postadresse.

Trykk konfigurere. Tast inn ditt eksisterende passord. (Bekreft evt. med alternativ to-faktor dersom du har andre metoder aktivert)

**VIKTIG:** Du får nå opp et bilde med en QR-kode. **Denne QR-koden må du lagre** (ta for eksempel et skjermbilde og lagre dette.) Alle som skal benytte seg av den delte TIDen skal benytte den samme QR-koden (den du nettopp lagret) for oppsett av to-faktor i autentiseringsapp.



Det finnes flere autentiseringsapper å velge mellom. Google authenticator og Microsoft Authenticator to anbefalte apper.

[< Avbryt](#)



## Konfigurer autentiseringsapp

mb@norgeodesi.no

- 1 Last ned en godkjenningsapp på telefonen din, slik som Google Authenticator.
- 2 Åpne godkjenningsappen på telefonen din. Bruk appen til å skanne QR-koden:

[Åpne i appen](#)



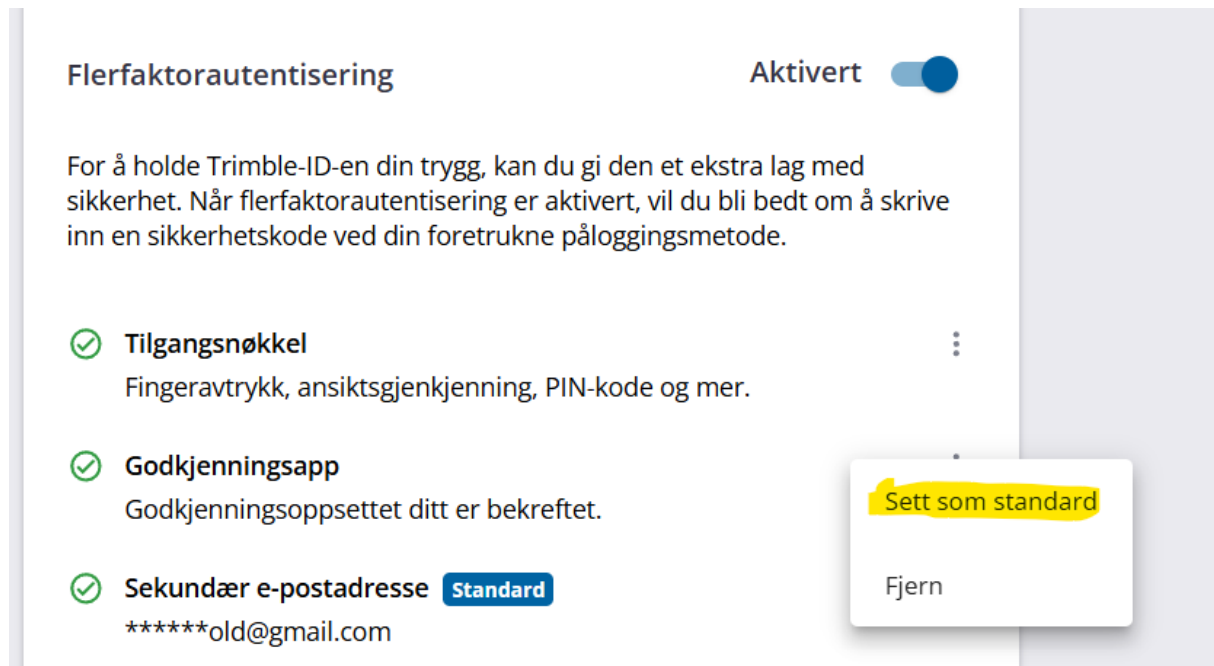
[Kan du ikke skanne den?](#)

- 3 Skriv inn koden som vises på skjermen.

Bekreftelseskode

### I [myprofile.trimble.com](https://myprofile.trimble.com):

Trykk de tre prikkene og velg *Sett som standard*



**Flerfaktoraautentisering** Aktivert

For å holde Trimble-ID-en din trygg, kan du gi den et ekstra lag med sikkerhet. Når flerfaktoraautentisering er aktivert, vil du bli bedt om å skrive inn en sikkerhetskode ved din foretrukne påloggingsmetode.

- ✓ **Tilgangsnøkkel** ⋮  
Fingeravtrykk, ansiktsgjenkjenning, PIN-kode og mer.
- ✓ **Godkjenningssapp**  
Godkjenningssoppsettet ditt er bekreftet.
- ✓ **Sekundær e-postadresse** **Standard**  
\*\*\*\*\*old@gmail.com

Sett som standard  
Fjern

### Alternativ 2:

Sørg for at alle som skal bruke enheten har tilgang til eposten som brukes til innlogging. Fjern alle andre autentiseringsmetoder. Da vil den som standard sende en engangskode til eposten som brukes til innlogging. Dersom denne eposten er tilgjengelig på selve måleboken (eller brukens egen mobile enhet), kan denne metoden brukes.

### Alternativ 3: sekundær epost.

Samme som over, bare med en annen epostadresse enn den som blir brukt til innlogging.