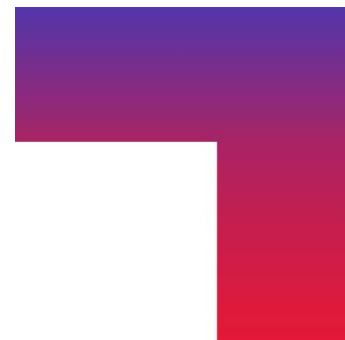




Guide: Sätt upp flerfaktorsautentisering (MFA) för ditt NordicHub Identity konto

NordicHub Identity tjänsten används av applikationer såsom **Unified Portal** för att ha ett säkert sätt att logga in. En del av *NordicHub Identity* är *MFA-konfiguratorn* som används för att sätta upp flerfaktorsautentisering för användarkonton.

Använd den här guiden för att sätta upp flerfaktorsautentisering för ditt användarkonto.



Contents

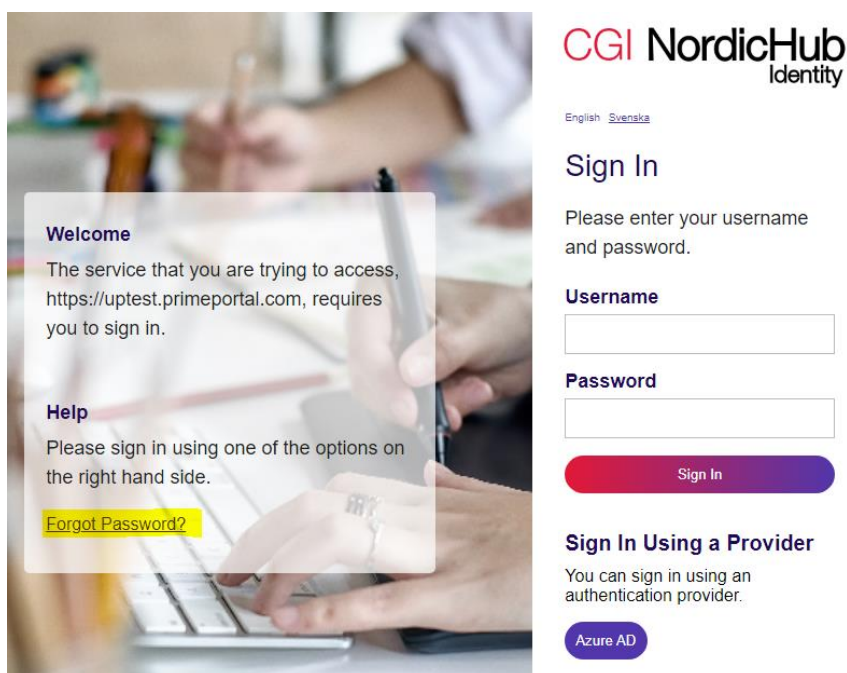
Guide: Sätt upp flerfaktorsautentisering (MFA) för ditt NordicHub Identity konto	1
Kom igång med MFA	2
Hur du sätter ett nytt lösenord:	2
Att aktivera tvåfaktorsautentisering	3
Hur man aktiverar SMS som andra faktor:	3
Hur man aktiverar en Authenticator app som andra faktor (google authenticator, Microsoft authenticator, Accman...)	4

Kom igång med MFA

Börja med att surfa till tjänsten som du vill logga in mot i din webbläsare. T.ex. Unified Portal:

<https://up.primeportal.com>.

Efter att du har surfat mot din tjänst kommer du hamna på en inloggningssida (se figur 1). Sedan flerfaktorsautentisering blivit ett krav måste alla nya och gamla användare sätta ett nytt lösenord vid första inloggning. Följ stegen i sektionen nedanför för att sätta ett nytt lösenord. **Ditt gamla lösenord kommer inte fungera.**



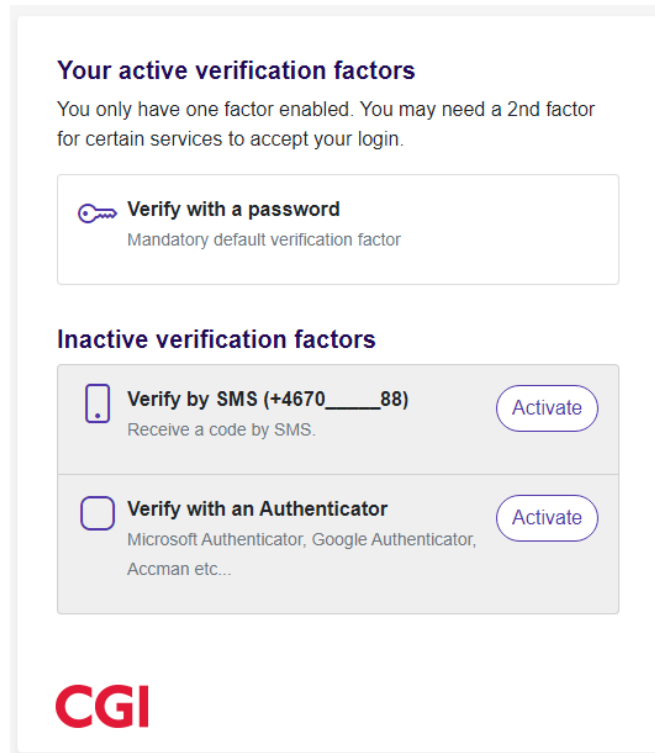
Figur 1: En bild av den nya inloggningssidan

Hur du sätter ett nytt lösenord:

1. Surfa till din tjänsts URL med din webbläsare (t.ex. [Unified Portal](#)).
2. Använd "[Glömt lösenord](#)"-länken och begär ett nytt lösenord.
 - a. Följ instruktionerna på "glömt lösenord"-sidan och sätt ett nytt personligt lösenord.
3. Efter att ha satt ett nytt lösenord har du redan kommit igång med en första autentiseringsfaktor (ditt lösenord). För att kunna nå din tjänst behöver du sen sätta upp en andra faktor. Följ instruktionerna i "Att aktivera tvåfaktorsautentisering"-sektionen nedan för att aktivera en andra faktor.

Att aktivera tvåfaktorsautentisering

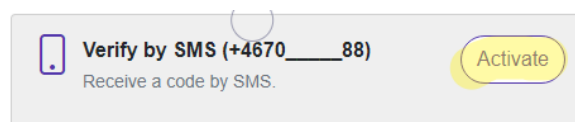
Efter att ha följt guiden fram tills nu borde du ha ett nytt lösenord satt. Det är då dags för dig att sätta upp en andra faktor med [MFA-konfiguratorn](#). Första gången du kommer in i MFA-konfiguratorn bör det se ut likt figur 2 nedan. Du kan välja mellan att aktivera en andra faktor i form av SMS eller en Authenticator app på din PC eller mobil. Du behöver bara sätta upp ett av alternativen. Se respektive guide nedan:



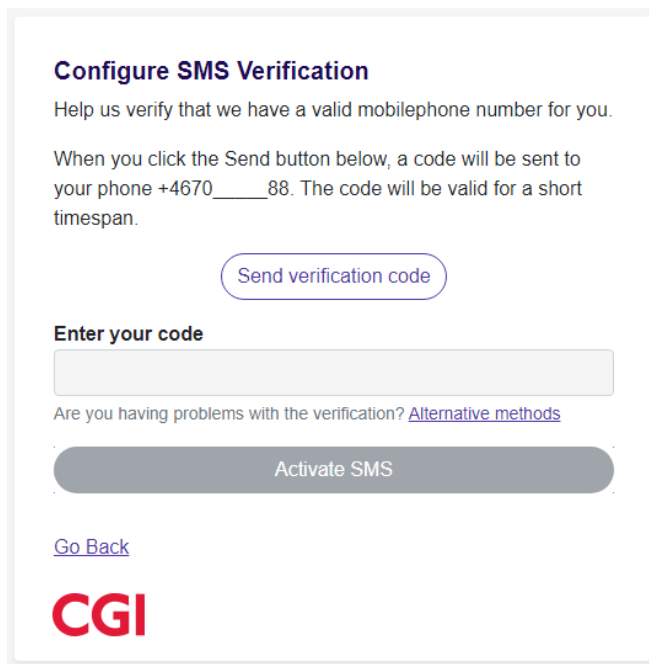
Figur 2: En bild av MFA-konfiguratorns landningssida innan en andra faktor aktiverats

Hur man aktiverar SMS som andra faktor:

1. Surfa till [MFA-konfiguratorns hemsida](#) i din webbläsare.
2. Kontrollera att ditt mobilnummer stämmer i "verify by SMS"-alternativet.
 - a. Om ditt nummer är felaktigt eller inte stämmer kan du använda [självbetjäningssidan](#) och sätta det mobilnummer du vill använda.
3. Klicka på "activate"-knappen (se bilden nedan) för "Verify by SMS"-alternativet.



4. Klicka på "Send Verification Code"-knappen (se figur 3 nedan) för att få en första verifieringskod skickad till ditt mobilnummer.



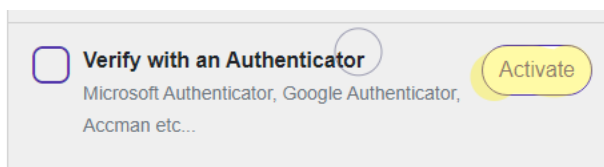
Figur 3: En bild över aktiveringssidan för SMS som andra faktor

5. Skriv in koden som du fick på din mobil i "Enter your code"-fältet.
6. Klicka på "Activate SMS"-knappen för att slutligen aktivera SMS som en andra faktor.
 - a. Obs: Om koden du fått på mobilen inte godkänns kan du använda "send verification code"-knappen igen för att få en ny.
7. Ditt konto ska nu vara säkrat med flerfaktorsautentisering. Surfa till din tjänst (t.ex. [Unified Portal](#)) och logga in på högersidan (se figur 1).

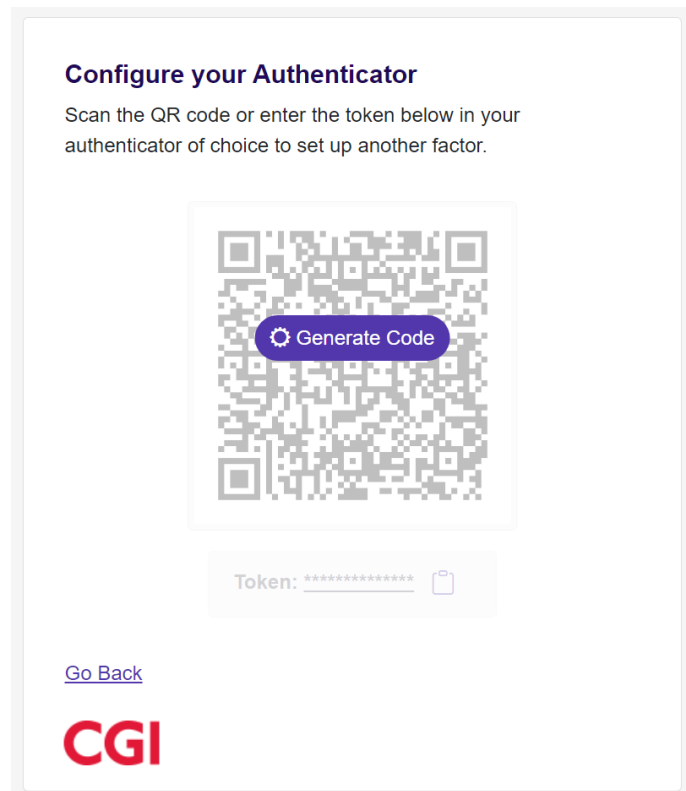
Hur man aktiverar en Authenticator app som andra faktor

(google authenticator, Microsoft authenticator, Accman...)

1. Ladda ner valfri authenticator app till din PC eller mobil.
 - a. [Windows Authenticator](#), [Google Authenticator](#), [Accman](#) eller andra...
2. Surfa till [MFA-konfiguratorns hemsida](#).
3. Klicka på "activate"-knappen för "Verify with an Authenticator"-alternativet (se figur nedan).

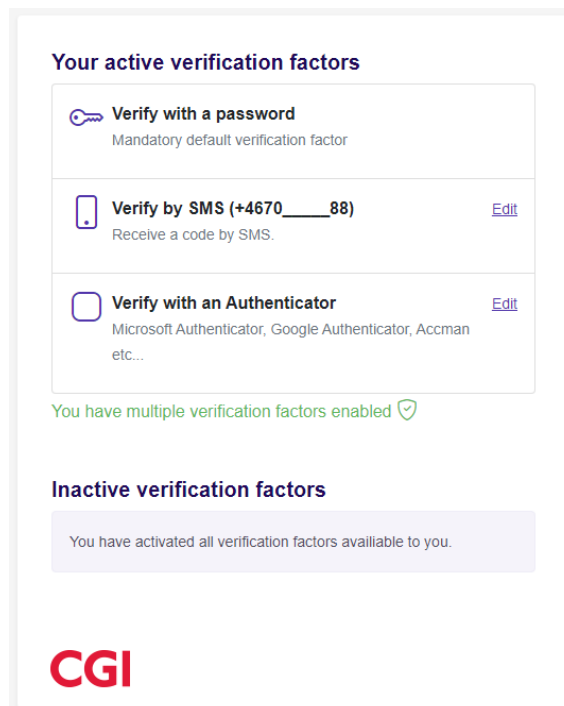


4. Klicka på "Generate code"-knappen (se figur 4 nedan).



Figur 4: En bild över aktiveringen av en authenticator som andra faktor

5. Skanna den genererade QR-koden eller skriv in koden manuellt i din authenticator app.



Figur 5: En bild av ett konto med både SMS och en authenticator app aktiverade som faktorer

6. Om du nu klickar på "go back"-knappen ska du kunna se att din andra faktor aktiverats.
7. Du kan nu surfa mot din tjänst igen och logga in med ditt lösenord och din nya faktor.
 - a. OBS: Du kan behöva logga ut och in för att dina ändringar ska slå.