

IndFak, RejsUd og Statens Digitale Indkøb

17. juni 2024
ØSY/DIBEN

Opsætningsguide til autentificator app

IndFak, RejsUd og Statens Digitale Indkøb understøtter nu to-faktor-autentifikation med en autentifikation-app-baseret løsning.

To-faktor-autentifikation er en sikkerhedsforanstaltning, som markant øger sikkerheden og beskytter mod phishing, adgangskodeangreb og sikrer logins mod angribere, der udnytter svage eller stjålne legitimationsoplysninger.

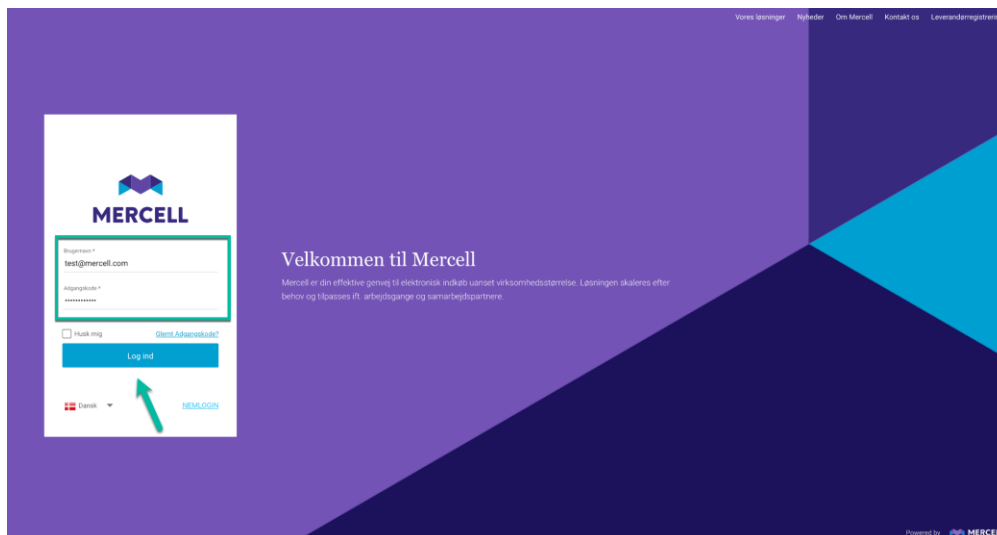
To-faktor-autentifikation er forbeholdt de brugere, der ikke anvender Single Sign On, men logger ind via "Brugernavn" og "Adgangskode".

Brugere, som normalt logger på via Single Sign On (SSO), skal fortsat anvende SSO. Vi anbefaler dog, at alle brugere downloader en autentificator app, som sikrer logon, selvom SSO skulle blive ramt af en driftsforstyrrelse.

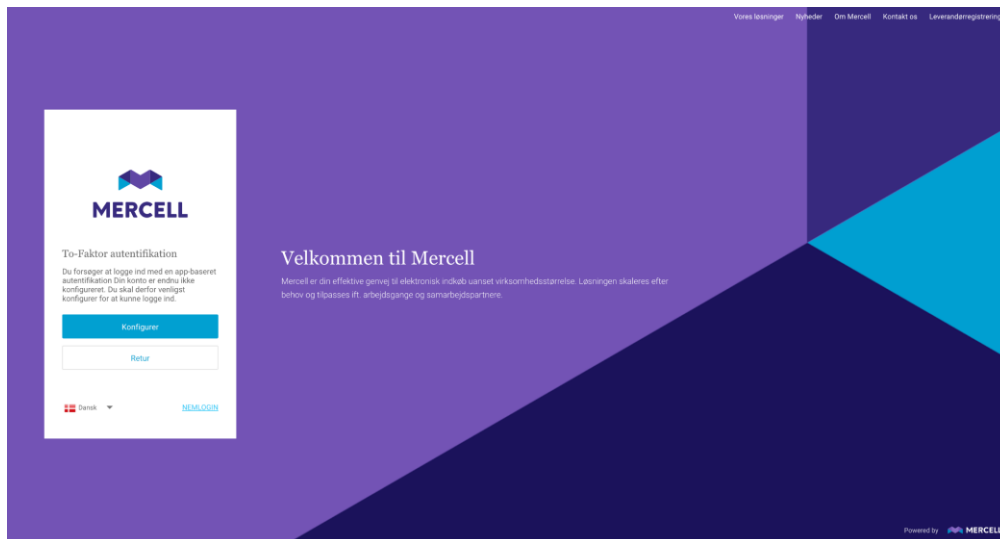
Opsætningen af to-faktor-autentifikation

Selve opsætningen af to-faktor-autentifikation foretages på login-siden.

Når brugeren tilgår løsningen for første gang efter tildeling af den app-baserede autentifikation, skal autentifikationen konfigureres. Dette gøres ved, at brugeren indtaster et "Brugernavn og en Adgangskode" og klikker på knappen "Log ind".

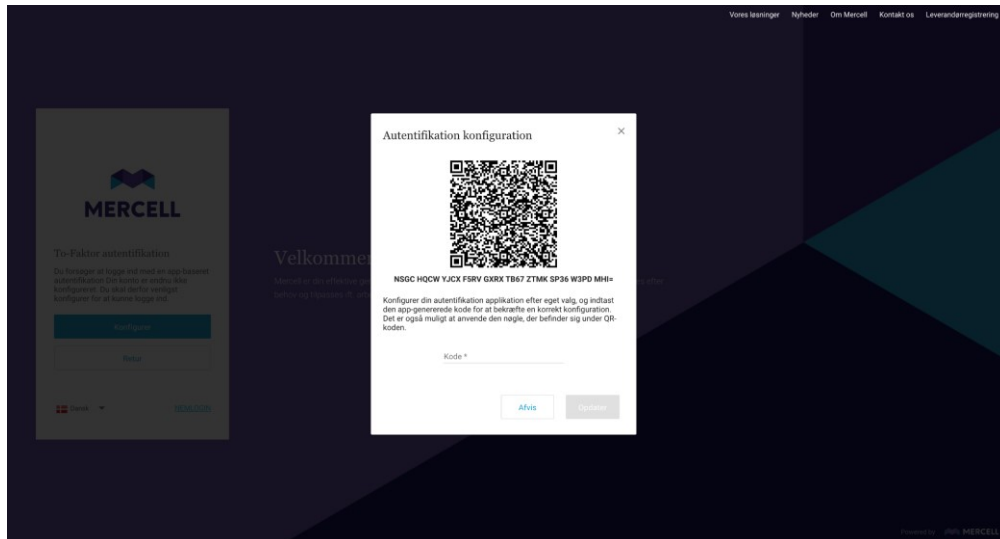


Man bliver derefter mødt af følgende side, hvor brugeren bliver gjort opmærksom på, at vedkommende har forsøgt at logge ind via den app-baseret autentifikation, men at kontoen endnu ikke er konfigureret.



Klikker man på "Retur", vender brugeren tilbage til sit udgangspunkt, hvor man kan tilføje brugernavn og adgangskode.

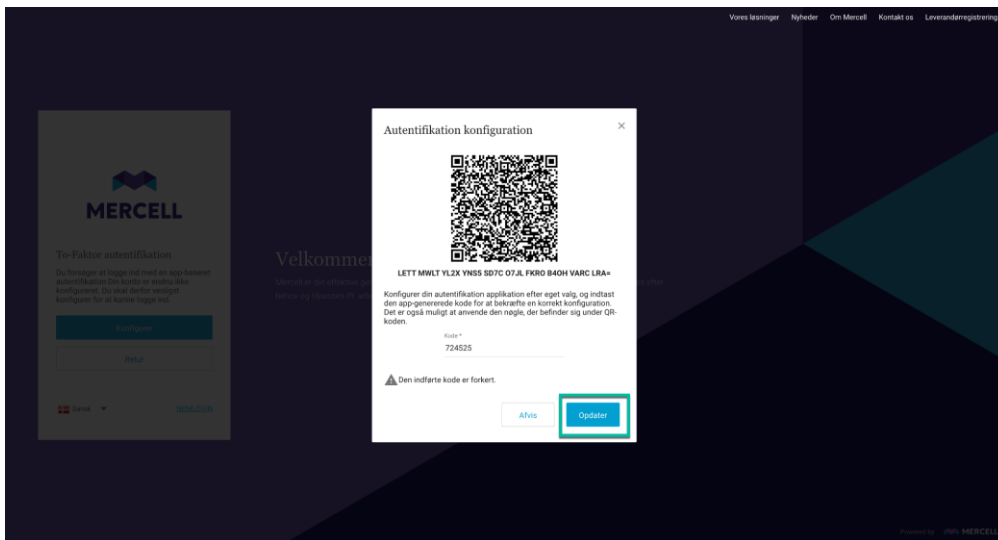
Klikker brugeren på den blå knap "Konfigurer", bliver vedkommende mødt af følgende pop op-besked:



Vælger man at klikke på "Afvis", sendes man tilbage til udgangspunktet, hvor man enten kan vælge at returnere til login-siden eller klikke på "Konfigurer"

Her får man at vide, at man kan konfigurere en autentifikationsapplikation efter eget valg og indtaste den genererede kode for at bekræfte, at konfigurationen er korrekt.

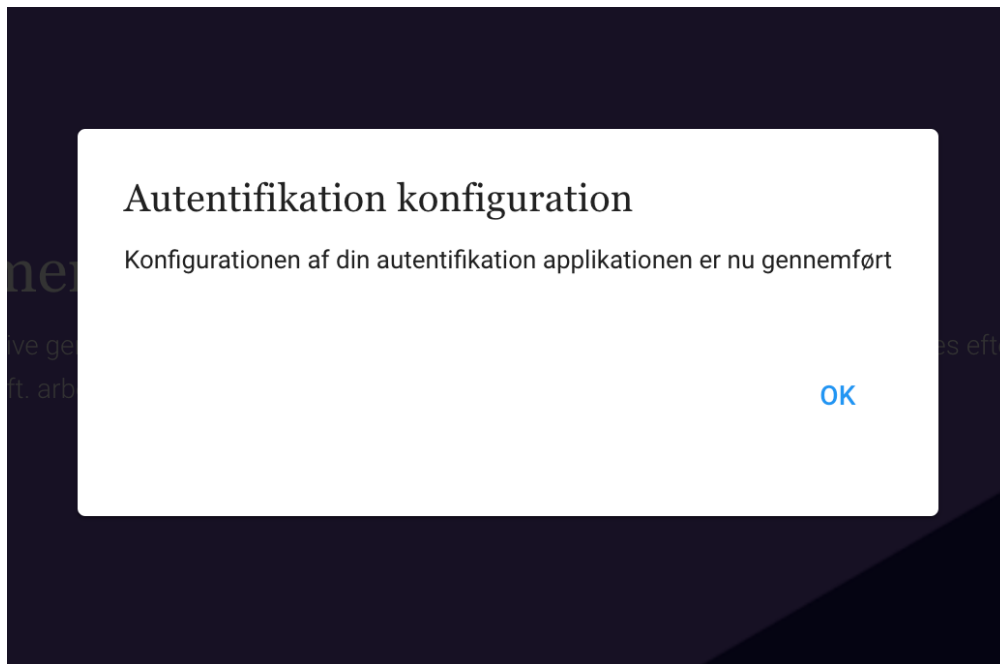
Ønsker man at fortsætte, scannes QR-koden fra den valgte autentifikation-app, og derefter indtastes den kode, man har modtaget i sin autentifikationsapplikation, og klikker på “Opdater”:



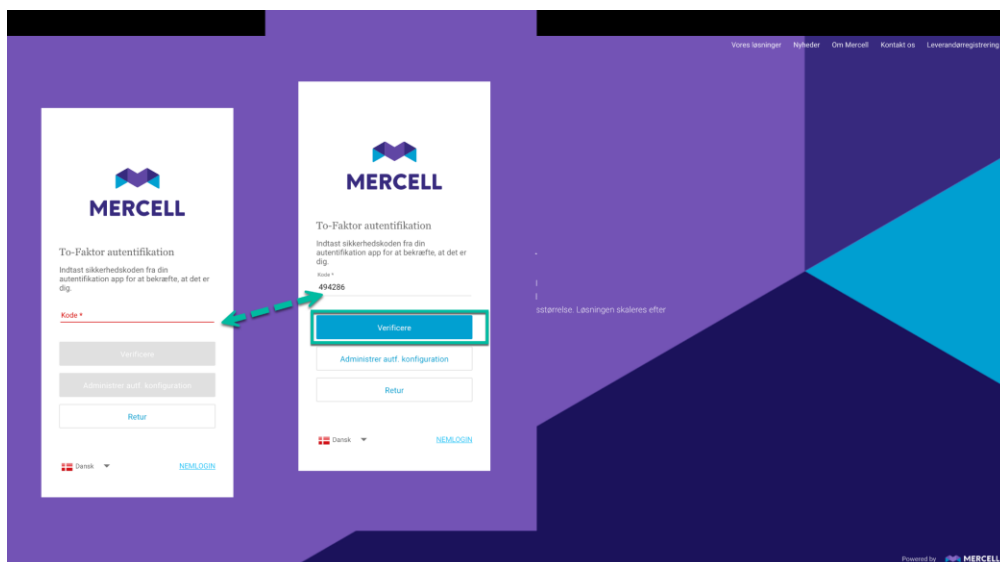
Man kan også vælge at indtaste nøglen, der står under QR-koden, i stedet for at scanne QR-koden.

LETT MWLT YL2X YNS5 SD7C O7JL FKRO B4OH VARC LRA=

Brugeren modtager derefter en pop op-besked, der informerer brugeren om, at konfigurationen af den app-baserede autentifikation er gennemført. Klik derefter på “OK”.



Den indledende autentifikationskonfiguration er nu på plads, og brugeren sendes tilbage til login-siden. Her bliver man nu bedt om at indtaste den kode, man modtager i sin autentifikationsapplikation. Klik derefter på “Verificere”, og brugeren bliver logget ind i løsningen.

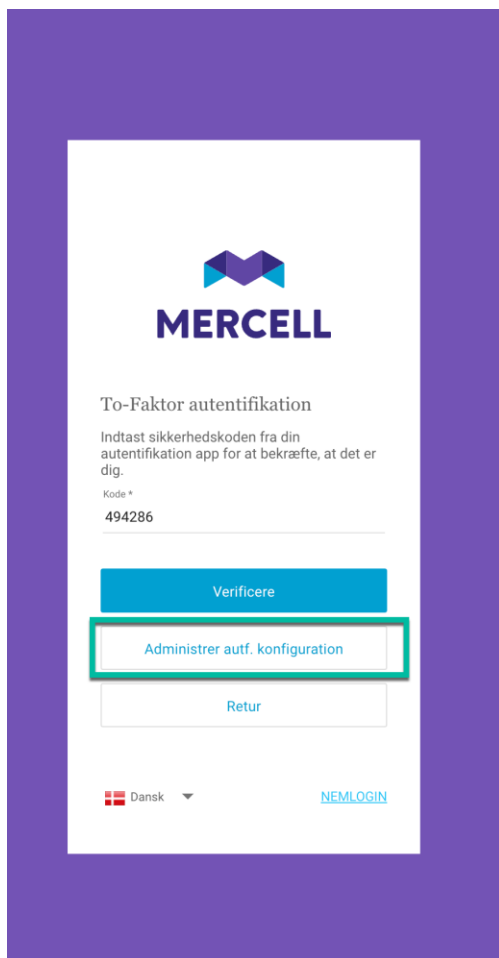


Næste gang brugeren har brug for at logge ind, indtaster brugeren først brugernavn og adgangskode, og dernæst den kode, der modtages i den valgte autentifikationsapplikation.

Administrering af den app-baserede autentifikation

En bruger kan til enhver tid opdatere eller slette autentifikationen. En opdatering kan skyldes, at man har brug for at skifte telefon. En sletning kan skyldes, at man enten er i gang med at skifte autentifikationsapplikationen, men det kan også skyldes, at man ønsker at skifte til den e-mailbaseret version (mere om dette senere).

Har man brug for at opdatere og skifte til en ny autentifikationsapplikation, indtaster man koden som vanligt og klikker derefter på "Administrer autf. konfiguration".



MERCELL

To-Faktor autentifikation

Indtast sikkerhedskoden fra din autentifikation app for at bekræfte, at det er dig.

Kode *

494286

Verificere

Administrer autf. konfiguration


Retur

Dansk

NEMLOGIN

Man modtager derefter følgende pop op-besked, hvor man scanner QR-koden, tilføjer den tilsendte kode og klikker på "Opdater".

Autentifikation konfiguration ×



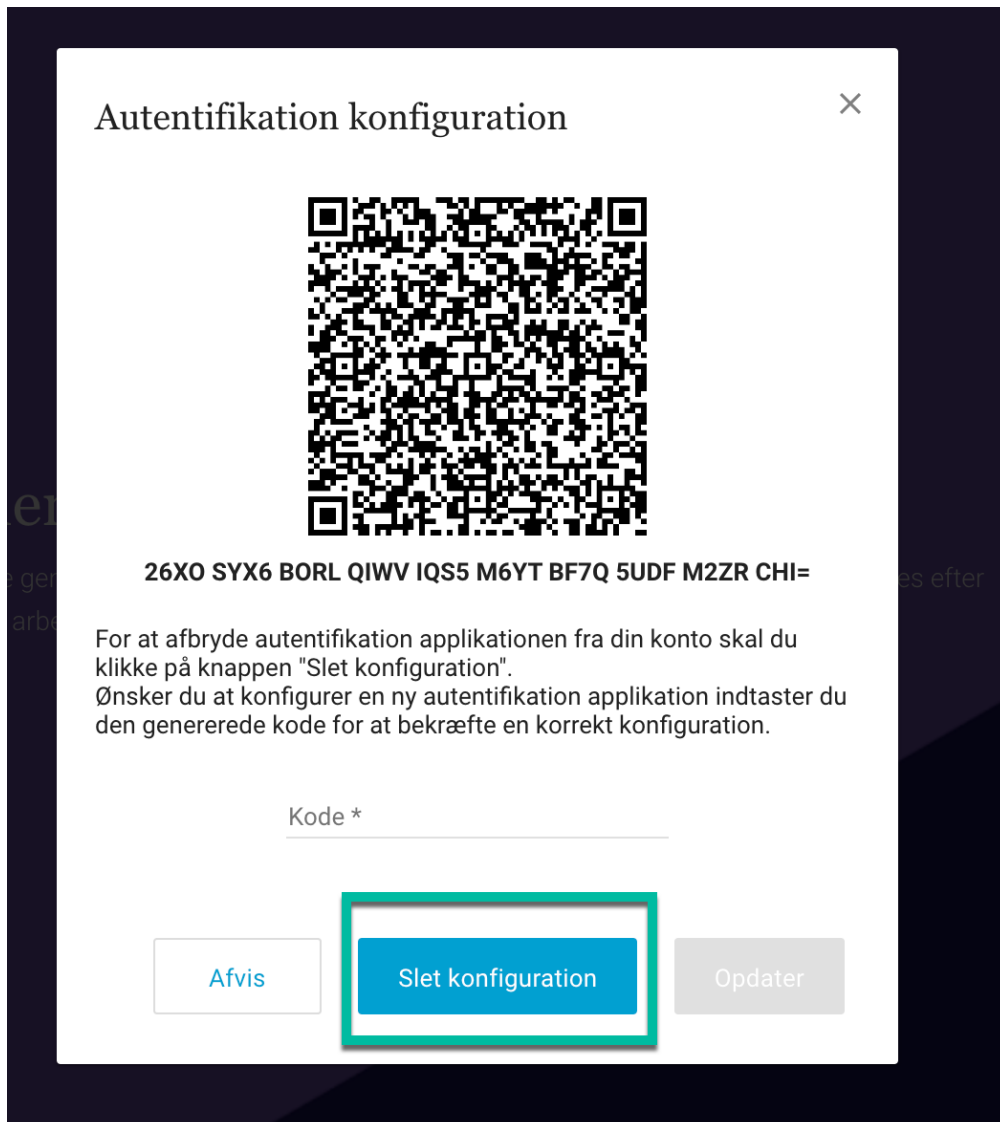
26XO SYX6 BORL QI WV IQS5 M6YT BF7Q 5UDF M2ZR CHI=

For at afbryde autentifikation applikationen fra din konto skal du klikke på knappen "Slet konfiguration".
Ønsker du at konfigurere en ny autentifikation applikation indtaster du den genererede kode for at bekræfte en korrekt konfiguration.

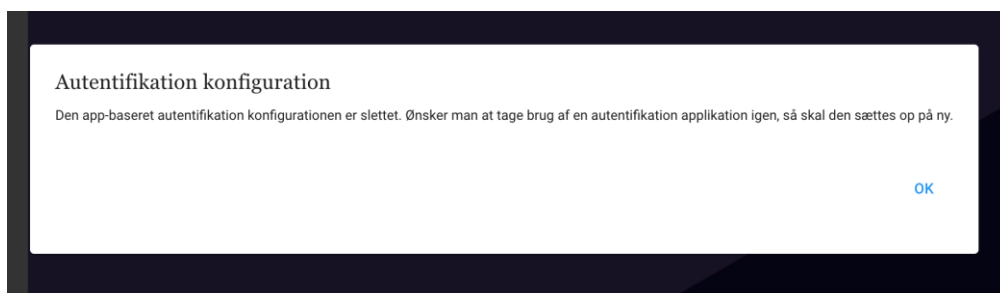
Kode *

760312

Ønsker man at slette sin konfiguration, klikker man på 'Slet konfiguration'.

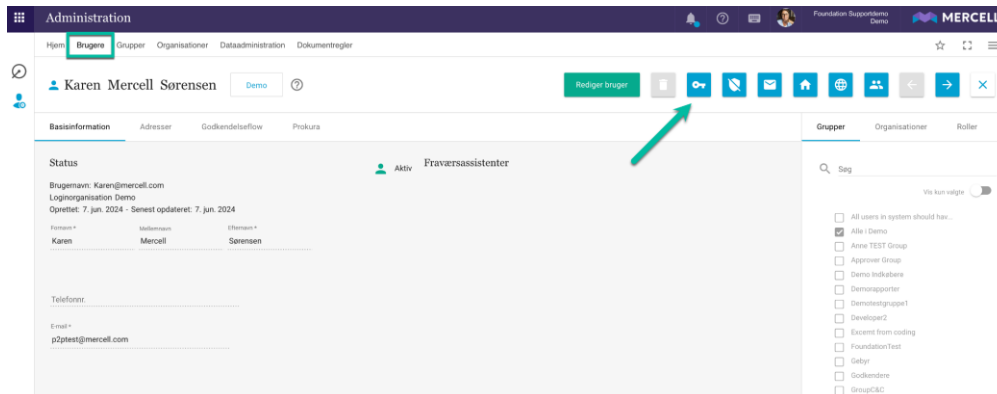


Brugeren modtager derefter en pop op-besked, der informerer brugeren om, at konfigurationen nu er slettet.

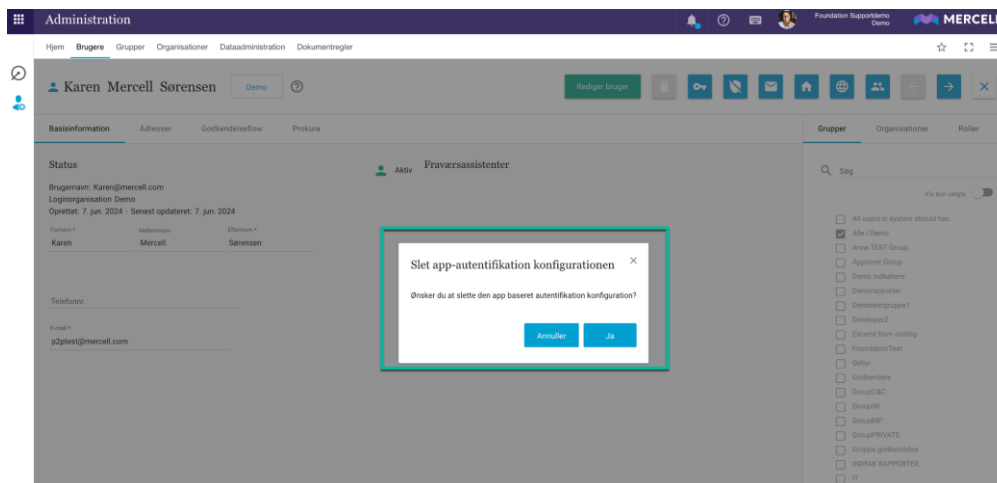


Specielt for den lokale systemadministrator

Hvis brugeren ikke har adgang til sin telefon, har en administrator også mulighed for at slette konfigurationen i administrationsmodul. Dette gør administratoren ved at tilgå brugerfanen i administrationsmodul. Brugere, der anvender den app-baserede autentifikation, har følgende ikon tilføjet på basisinformation:

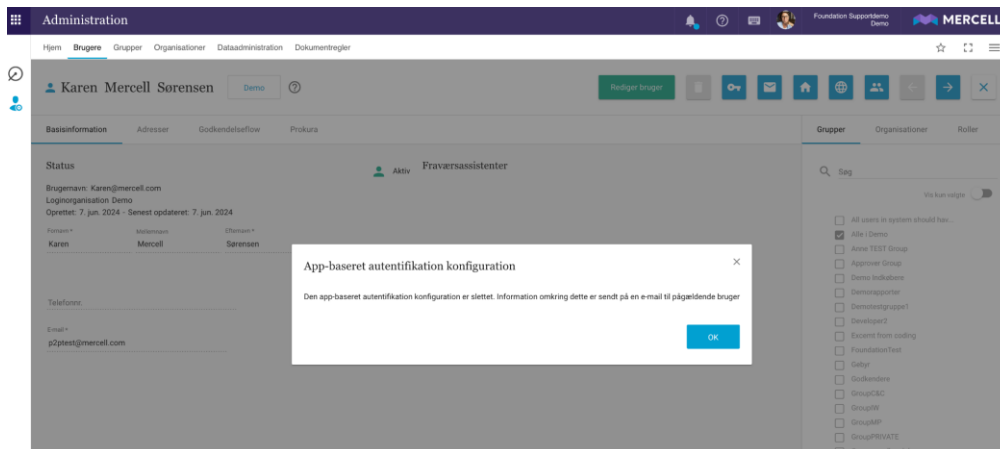


For at slette konfigurationen klikker man på ikonet, hvor administratoren bliver mødt af en pop op-besked, der spørger, om man ønsker at slette:



Administratoren kan vælge at klikke på "Annuller", hvis man fortryder sletningen.

Klikker administrator på 'Ja', så slettes konfigurationen, og man bliver mødt med følgende besked:

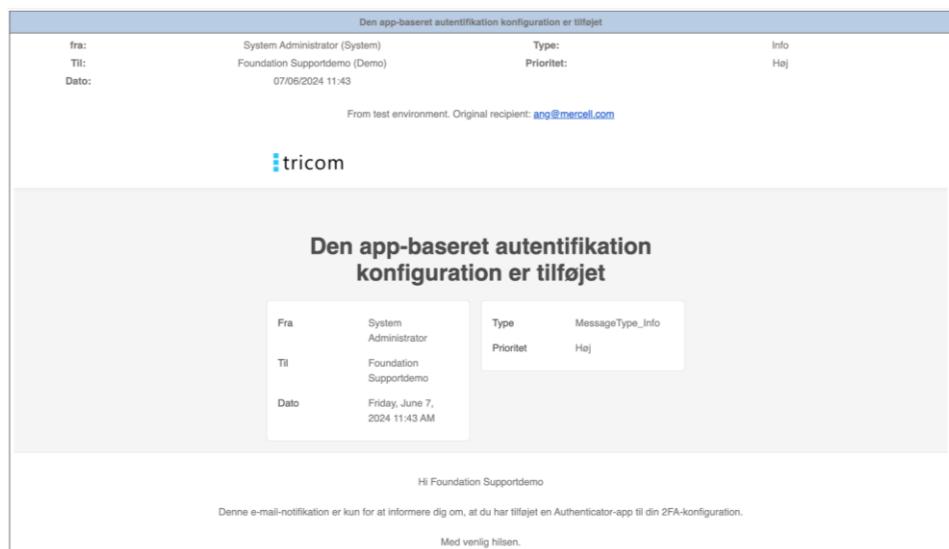


Næste gang brugeren forsøger at logge ind, skal en app-baseret konfiguration opsættes på ny.

Vær opmærksom på, at kun administratorer med adgang til at redigere brugerprofiler har mulighed for at fjerne den app-baserede konfiguration.

E-mail-notifikation

For at forbedre sikkerheden omkring den app-baserede autentifikation samt brugervenligheden, modtager brugeren en e-mail-notifikation, hvis en administrator sletter brugerens autentifikationskonfiguration. Det samme gælder, når en bruger enten konfigurerer autentifikationsapplikationen eller sletter den.



Her ses et eksempel på en at den app-baseret autentifikation nu er tilføjet en bruger

Handlings Log

Administratører har mulighed for at tilgå en 2FA-rapport kaldet "Opdatering på brugerautentifikation". Her kan man se, hvilke af følgende handlinger der er foretaget:

- Opdatering af autentifikation
- Sletning af autentifikation
- Ændring af autentifikation til e-mail

	Bruger	Login organisation	Handling	Oprettet	Aktiv bruger	Session bruger
1	99Release@ww.ww	99 Staging Test	Oprettede	05/06/2024 14:35	99Release@ww.ww	99Release@ww.ww
2	Passtest1	98 Staging Test	Oprettede	05/06/2024 14:44	Passtest1	Passtest1
3	2fa@test.com	99 Staging Test	Oprettede	05/06/2024 14:53	2fa@test.com	2fa@test.com
4	Ruben2FATest	99 Staging Test	Oprettede	05/06/2024 15:06	Ruben2FATest	Ruben2FATest
5	Passtest1	98 Staging Test	Slettet	05/06/2024 15:37	maria.pronichkina@external.m...	maria.pronichkina@external.m...
6	Passtest1	98 Staging Test	Oprettede	05/06/2024 15:37	Passtest1	Passtest1
7	99Release@ww.ww	99 Staging Test	Slettet	05/06/2024 15:43	STGFD	STGFD
8	99Release@ww.ww	99 Staging Test	Oprettede	05/06/2024 15:45	99Release@ww.ww	99Release@ww.ww
9	99Release@ww.ww	99 Staging Test	Slettet	05/06/2024 15:50	99Release@ww.ww	99Release@ww.ww
10	99Release@ww.ww	99 Staging Test	Oprettede	05/06/2024 15:51	99Release@ww.ww	99Release@ww.ww
11	99Release@ww.ww	99 Staging Test	Slettet	05/06/2024 15:58	STGFD	STGFD
12	Passtest1	98 Staging Test	Opdateret	05/06/2024 16:21	Passtest1	Passtest1
13	Passtest1	98 Staging Test	Slettet	06/06/2024 12:00	Passtest1	Passtest1
14	ang@mercell.com	Demo	Oprettede	07/06/2024 11:43	ang@mercell.com	ang@mercell.com
15	ang@mercell.com	Demo	Slettet	07/06/2024 12:06	ang@mercell.com	ang@mercell.com
16	ang@mercell.com	Demo	Oprettede	07/06/2024 12:16	ang@mercell.com	ang@mercell.com
17	Karen@mercell.com	Demo	Oprettede	07/06/2024 12:27	Karen@mercell.com	Karen@mercell.com

Rapporten indeholder en organisationsvælger samt dato og tidsinterval og mulighed for filtrering i søgningen. Derudover indeholder den følgende kolonner:

- Bruger: Dette felt indikerer navnet på brugeren, der anvender den app-baserede konfiguration.
- Loginorganisation: Dette felt viser den tildelte loginorganisation for den førnævnte bruger.
- Handling: Dette felt angiver typen af handling, der er foretaget, såsom sletning, oprettelse eller opdatering af konfigurationen.
- Oprettet: Felt angiver dato og klokkeslæt for oprettelsen af den nævnte handling.
- Aktiv bruger: Dette felt indikerer, hvilken bruger der er aktiv.
- Sessionsbruger: Dette felt angiver navnet på den bruger, der udførte handlingen.