



# Kontrolpanel

Administrator guide til Uniqkeys kontrolpanel

# Indhold

## Administrator guide til Uniqkey funktioner

1. Inviter nye brugere
  - a. Tilføj administratorer
2. Opret grupper
  - a. Adgangskoder til grupper
3. Onboarding i Uniqkey
4. Offboarding af medarbejdere m. overførsel af login ejerskab
5. Overblik og Kontrol over medarbejder adgange til virksomhedskonti
  - a. Overblik over cloud services
6. E-mails
7. Aktivering af godkendt browser
8. Restriktionskontrol
  - a. Georestriktion
  - b. IP-restriktion
  - c. Tidsrestriktion
  - d. Kode synlighed
9. Audit logs

## 1 Inviter nye brugere

N.B Hvis i har integreret med AD og SCIM vil virksomhedens brugere automatisk blive placeret i inviterede brugere.

For at invitere medarbejdere, skal du inde i kontrolpanelet vælge brugere.

### Sådan inviterer du brugere:

- Klik på feltet brugere i menuen
- Klik "Inviter ny bruger" og skriv e-mailadressen på medarbejderen i input feltet
- Klik "send invitation"

Efterfølgende vil den pågældende medarbejder modtage en aktiveringsmail med en guide til at komme i gang med Uniqkey. Når brugeren er inviteret vil de blive placeret i Inviterede brugere



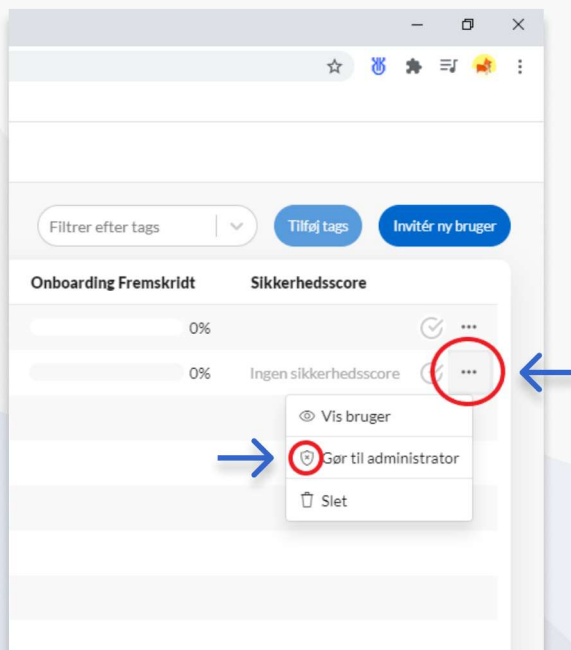
### 1.a Tilføj Administratorer

Administratorerne i virksomheden er de eneste som har adgang til virksomhedens data. Det er kun muligt at give brugere administratorrettigheder, når de er aktive i kontrolpanelet dvs. de har aktiveret deres Uniqkey bruger.

Det er vigtigt at udvælge flere ansatte til rollen som administrator, da Uniqkey under ingen omstændigheder kan genaktivere eller nulstille adgangen til kontrolpanelet for virksomheden.

#### Tilføj Administratorer:

- Klik på brugere under kontrolpanelet
- Ud fra den bruger du ønsker at gøre til administrator klikker du på de tre prikker
- Vælg "gør til administrator"



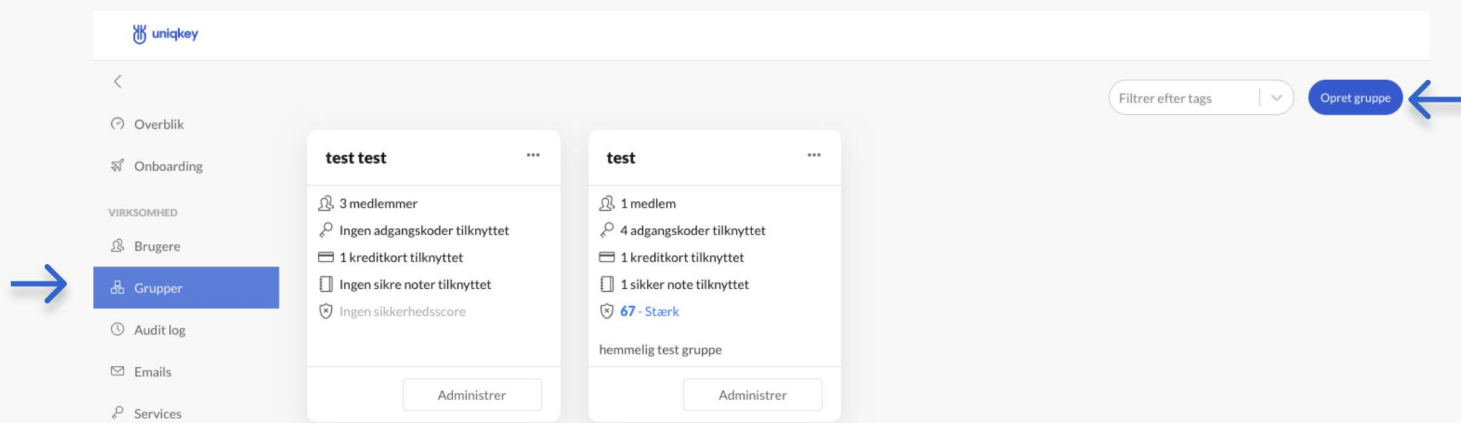
## 2 Opret grupper

Grupper er en funktion der gør det muligt at inddele medarbejdere i teams eller afdelinger og derved let og hurtigt give den samlede gruppen de nødvendige rettigheder, adgange og tilladelser.

Sådan tilføjer du brugere til grupper:

- Klik på "Grupper" i side panelet eller tryk på "Gå til grupper" på startsiden
- Find den gruppe du gerne vil tilføje en medarbejder til, og tryk på administrer
- Tryk på Invitér brugere
- Indtast brugerens e-mail, og tryk Invitér

Brugeren er nu inviteret



Som administrator kan du give en gruppe eller et team adgang til en specifikke services. Derved får hele gruppen adgang til kontoen på samme tid.

### 2.a Tilføj adgangskoder til grupper:

- Gå til "Adgangskoder" i gruppen
- Tryk på "Tilføj adgangskoder"
- Tilføj konto navn, web-adressen, brugernavn og adgangskode
- Herefter trykker du på "Tilføj adgangskode"
- Accepter notifikationen med din mobil app

Tilføj ny adgangskode til HR ×

Adgangskode navn

Hjemmeside

Brugernavn

Kodeord

Udfyld kodeord for at se styrken

Du har også mulighed for at dele en konto du allerede har oprettet i Uniqkey med en gruppe du er med i. Det kan gøres både fra appen og fra browser extension under den enkelte konto.

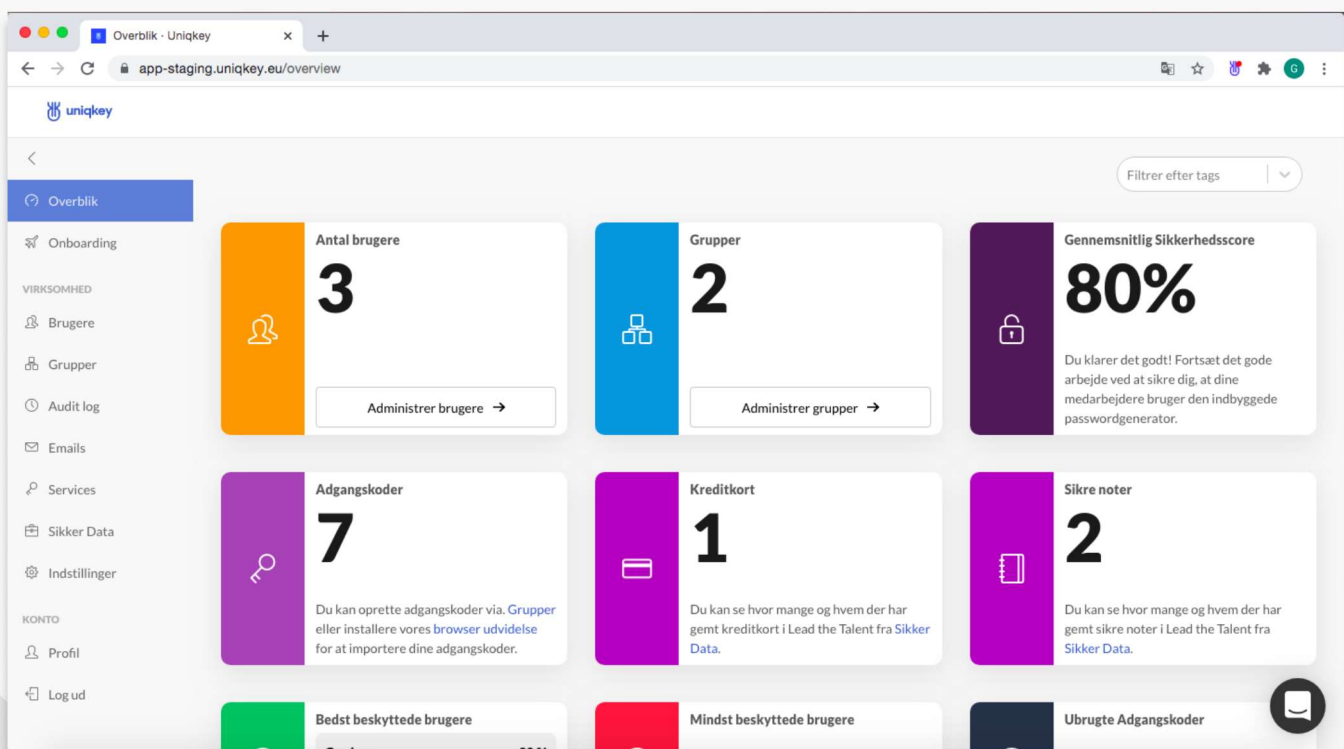
### 3 Onboarding i Uniqkey

I forbindelse med aktivering og onboarding af brugere i virksomheden, er der en række features I kan måle på.

For at komme bedst muligt fra start anbefaler Uniqkey at I kun opsætter nogle enkelte onboarding kriterier for jeres brugere. Grunden til denne anbefaling er for at give jer som administrators og jeres brugere bedre mulighed for at blive bekendt og føle sig tryk ved systemet.

I takt med at flere brugere bliver trygge med at bruge systemet, kan I opsætte flere trin og måle på hvilke funktioner der bliver brugt f.eks. 2FA på Microsoft logins el.lign.

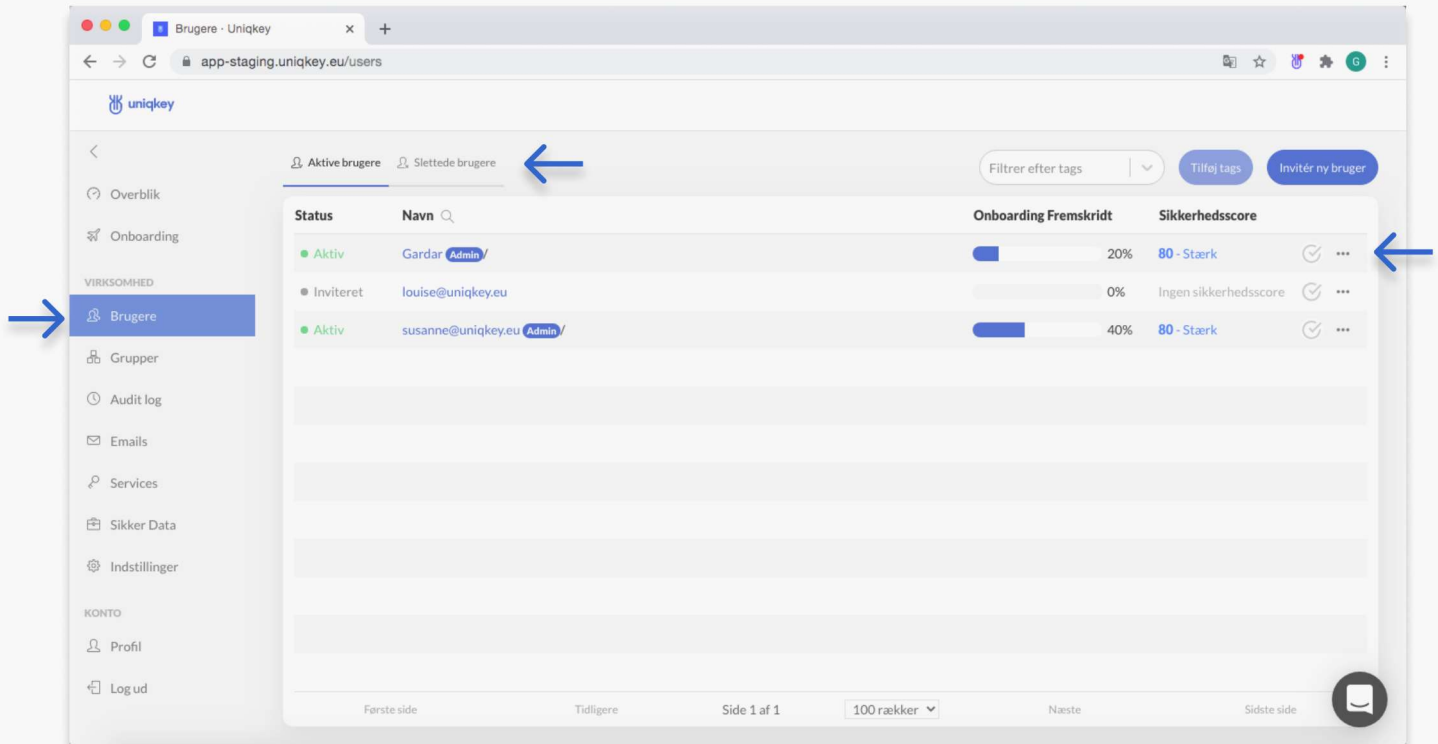
I vil kunne måle hvor succesfuld jeres onboarding er både på individuelle brugere og på gruppe niveau.



## 4 Offboarding af medarbejdere

Når en medarbejder stopper, bliver det lettere som virksomhed at få overblik og kontrol over medarbejderens forskellige logins til diverse cloud services.

Efter fratrædelse skal medarbejderens bruger slettes, derved fratages de adgangen til deres virksomhedslogins. Hvis virksomheden får brug for adgangskoder fra den tidligere medarbejder, kan administrator tilgå i kontrolpanel og derefter slettede konti.



Status	Navn	Onboarding Fremskridt	Sikkerhedsscore
Aktiv	Gardar Admin	20%	80 - Stærk
Inviteret	louise@uniqkey.eu	0%	Ingen sikkerhedsscore
Aktiv	susanne@uniqkey.eu Admin	40%	80 - Stærk

### Sådan offboarder du medarbejdere:

- Du skal være logget ind i administrator kontrolpanelet
- Tryk på "Brugere" i side panelet eller tryk på "Gå til brugere" på startside
- Find den medarbejder du gerne vil fjerne, og tryk på de tre prikker til højre fra deres navn
- Tryk på fjern bruger, og tryk Slet
- Medarbejderen vil nu være arkiveret under Slettede konti i kontrol panelet

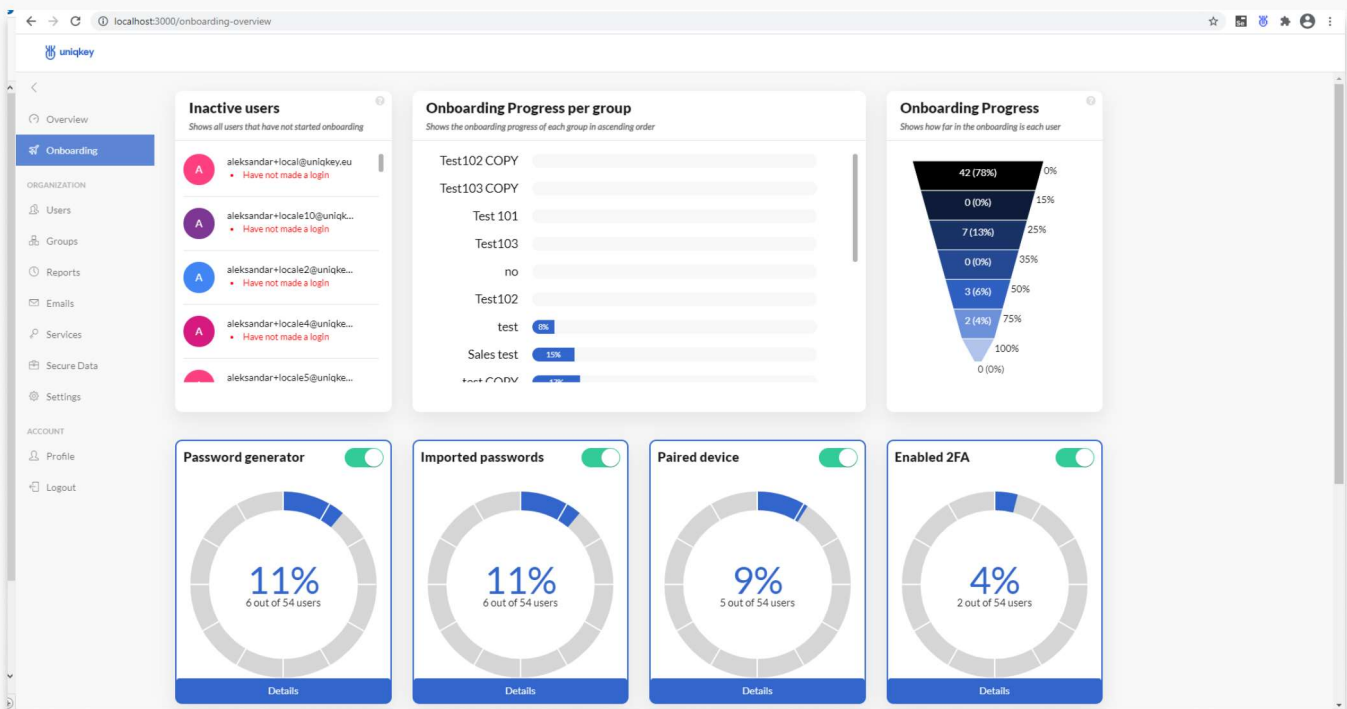
### Slettede brugere:

I slettede konti kan administrator hente den tidligere medarbejders virksomhedsadgangskoder og derefter flytte disse koder til en anden bruger eller gruppe. Derved sikre I at logins til diverse cloud services ikke går tabt og at virksomheden kan logge på dennes service, annullere licenser og ændre 2FA opsætninger.

## 5 Centraliseret overblik og kontrol over medarbejder adgange til virksomhedskonti

Ved hjælp af Uniqkey bliver det lettere at styre, hvilke medarbejdere der har adgang til de forskellige systemer og virksomhedslogins. Det bliver også lettere at holde styr på adgangskontrol til forretningskritiske systemer.

Derved sikre du som administrator, at de mest kritiske systemer er beskyttet og kun er tilgængelige for relevant personale.



### 5.a Overblik over cloud-services

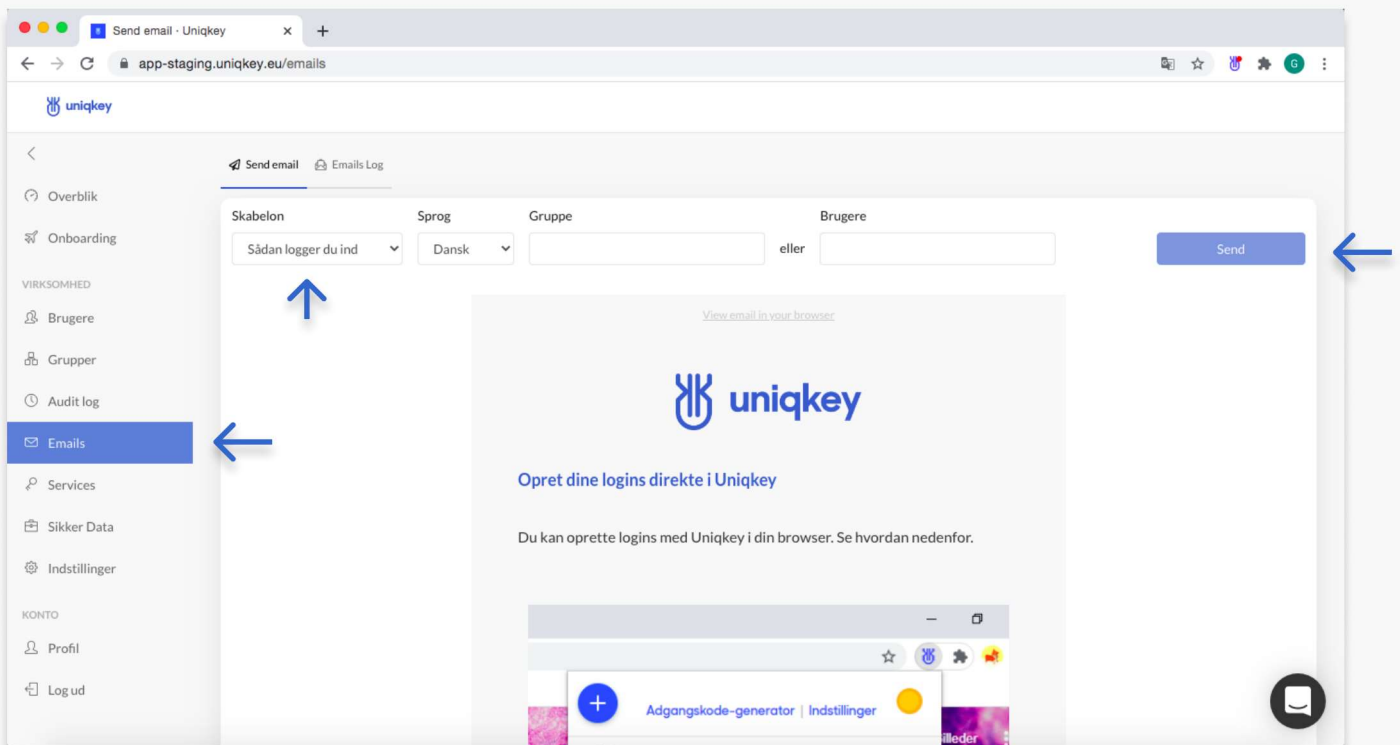
Som administrator har du mulighed for at få et overblik over de cloud services der bliver anvendt i virksomheden. Det er også muligt at se aktive licenser og inviterede licenser.

The screenshot shows the 'Serviceoversigt' (Service Overview) section of the Uniqkey dashboard. It features a table listing cloud services used by the organization. The table has columns for 'Service', 'Brugere' (Users), 'Sikkerhedsscore' (Security Score), and 'Seneste aktivitet' (Last Activity). A search bar and a 'Filtrer efter tags' (Filter by tags) dropdown are visible at the top of the table. A 'Opret adgangskode' (Create access code) button is also present.

Service	Brugere	Sikkerhedsscore	Seneste aktivitet
canva.com	1	80 - Stærk	10 dage siden
figma.com	1	60 - God	10 dage siden
gmail.com	1	100 - Meget stærk	11 dage siden
linkedin.com	1	100 - Meget stærk	11 dage siden

## 6 E-mails i kontrolpanelet

Du kan som administrator sende e-mails ud til brugere direkte fra kontrolpanelet. Det kan for eksempel være feature mails. Feature e-mails er blevet lavet til at hjælpe med at informere brugere om, hvordan de kan øge deres sikkerhed gennem f.eks. 2FA, adgangskodegenerator osv. Alle feature e-mails findes både på dansk og engelsk i dit kontrolpanel.



### Sådan sender du E-mails:

- Klik på "E-mails" i menuen
- Vælg mail type
- Vælg "Sprog"
- Vælg hvilken gruppe/bruger skal modtage denne mail
- Tryk "Send"

### Uniqkey anbefaler

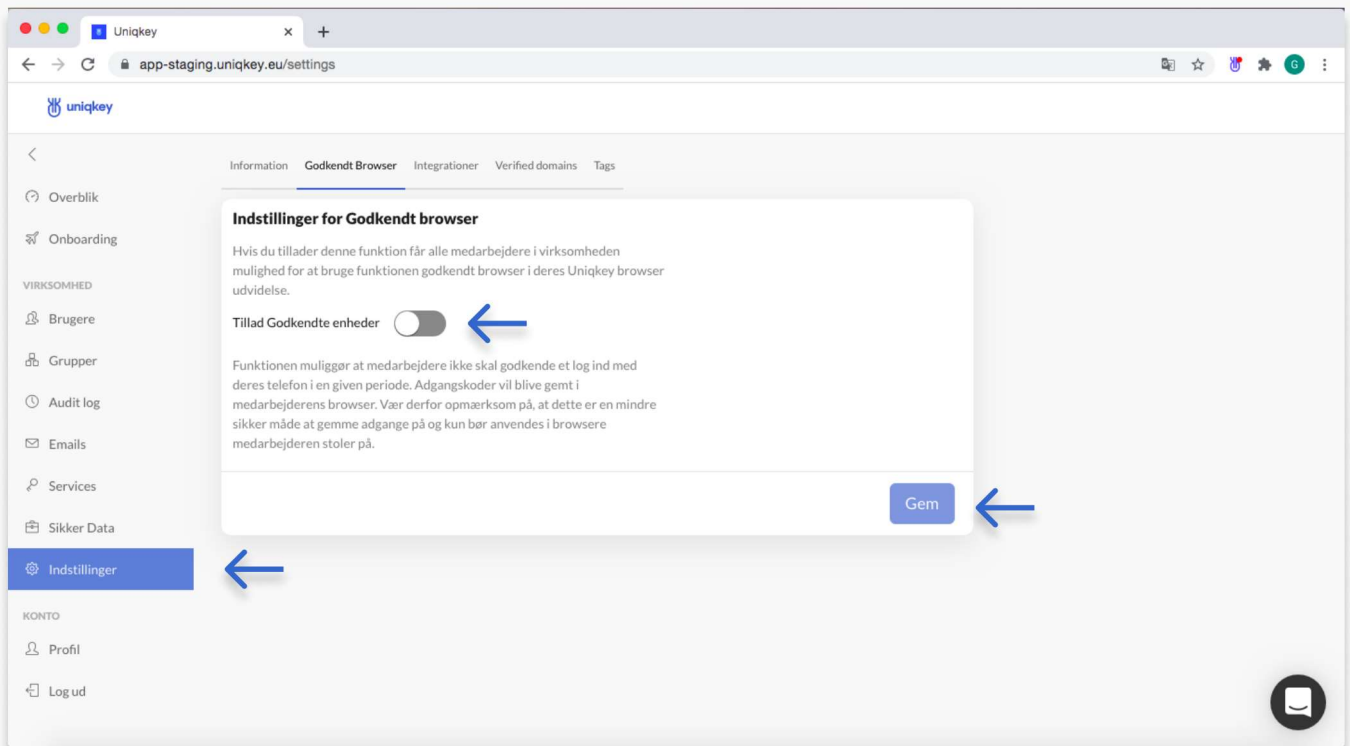
Hvis en bruger har en lav sikkerhedsscore, anbefaler Uniqkey at disse feature e-mails sendes ud for at opfordre brugeren til at øge sikkerheden omkring denne brugers logins. Du kan sende mails til specifikke grupper eller til den enkelte brugere



## 7 Aktivering af godkendt browser

Det kan forekomme, at brugerne vil blive generet af at skulle godkende hvert eneste login med deres smartphone. Derfor har vi udviklet funktionen godkendt browser: Det er en funktion der gør at brugeren ikke er nødsaget til at godkende logins fra deres smartphone i et givent tidsrum fx 08.00-16.00. I dette tidsrum vil adgangskoderne være gemt lokalt i brugerens browser.

Uniqkey anbefaler af sikkerhedsmæssige årsager ikke at man anvender denne funktion. Efter stor efterspørgsel er det dog en mulighed at aktivere denne funktion.



## 8 Restriktionskontrol

Restriktionskontrol er en feature der kan sikre virksomheden via Georestriktion, IP-og tidrestriktioner. Du kan for eksempel bestemme, om medarbejdere kun må tilgå diverse virksomhedskonti fra arbejdspladsen.

Disse restriktioner kan opsættes for grupper i virksomheden. Med grupperestriktioner kan du som it-administrator bestemme hvor og hvornår specifikke konti må tilgås.

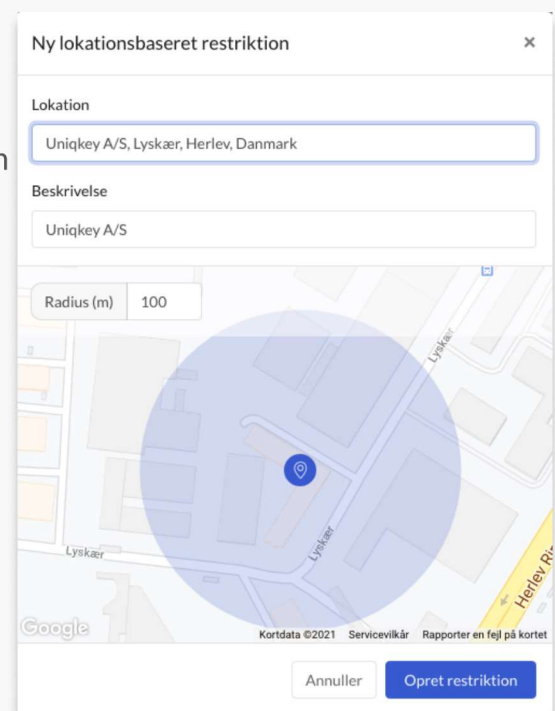
N.B. Hvis du tilføjer mere end en af den samme type restriktion til en gruppe, er det kun en af de to restriktioner af samme type der behøver at være opfyldt. Dvs. Hvis I har sat to Geo restriktioner på fx for jeres kontor i både Århus og København, er det naturligvis kun nødvendigt at opfylde det ene lokationskrav.

### 8.a Georestriktion

Med georestriktion kan du sætte en radius ud fra en adresse hvor gruppens konti må tilgås. Georestriktion kræver at brugeren har aktiveret Beliggenhed (Location Services) i appen.

Du kan opsætte restriktioner:

- I menuen til venstre vælg "Grupper"
- Vælg "Administrer grupper"
- Vælg en restriktionen du ønsker
- Vælg lokation og beskrivelse
- Tryk "Opret"



Ny lokationsbaseret restriktion

Lokation  
Uniqkey A/S, Lyskær, Herlev, Danmark

Beskrivelse  
Uniqkey A/S

Radius (m) 100

Google Kortdata ©2021 Servicevilkår Rapporter en fejl på kortet

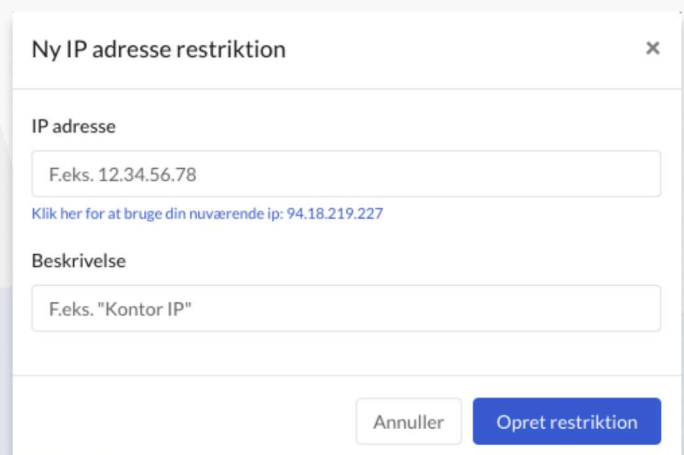
Annuller Opret restriktion

### 8.b IP-restriktion

Med IP-restriktion kan du bestemme, hvilke IP-adresser der må tilgå en gruppes konti. IP-adressen der skal indtastes skal være en CIDR adresse.

Du kan opsætte restriktioner:

- I menuen til venstre vælg "Grupper"
- Vælg "Administrer grupper"
- Vælg en restriktionen du ønsker
- Udfyld IP adresse og beskrivelse
- Tryk "Opret"



Ny IP adresse restriktion

IP adresse  
F.eks. 12.34.56.78  
[Klik her for at bruge din nuværende ip: 94.18.219.227](#)

Beskrivelse  
F.eks. "Kontor IP"

Annuller Opret restriktion

## 8.c Tidsrestriktion

Med tidsrestriktioner kan du bestemme hvilke dage, og i hvilke tidsrum en gruppes konti må tilgås.

Du kan opsætte restriktioner:

- I menuen til venstre vælg "Grupper"
- Vælg "Administrer grupper"
- Vælg en restriktionen du ønsker
- Vælg dage, tidsinterval, og den pågældende tidszone
- Tryk "Opret"

### Ny tidsbaseret restriktion

Vælg dage

M	T	O	T	F	L	S
---	---	---	---	---	---	---

Vælg tidsinterval

0:00 8:00 16:30 24:00

Select a timezone

(GMT+01:00) Central European Time - Copenhagen

Annuller Opret restriktion

## 8.d Kodesynlighed

I fanen indstillinger er det muligt at opsætte restriktioner for synligheden på virksomhedslogins. Dvs. at administrator kan beskytte logins, ved ikke at gøre selve koderne synlige for medarbejderne.

Sådan opsætter du kodesynlighed:

- Under "Grupper" gå til "Indstillinger"
- Vælg "Kopier og rediger"
- Vælg "Kopiering tilladt"
- Tryk "Opdater"

← Grupper / test test

Info Adgangskoder Kreditkort Sikre noter Ubrugte adgangskoder Medlemmer Restriktioner **Indstillinger**

Information Godkendt Browser **Kopier og rediger**

Redigering tilladt

Når denne indstilling er slået til, vil alle medarbejdere i denne gruppe kunne redigere adgangskoder, kreditkort og sikre noter i denne gruppe. Det vil også gøre det muligt for medarbejdere at se og kopiere adgangskoder, kreditkort og sikre noter. Vi anbefaler at denne indstilling er slået til.

Kopiering tilladt  ←

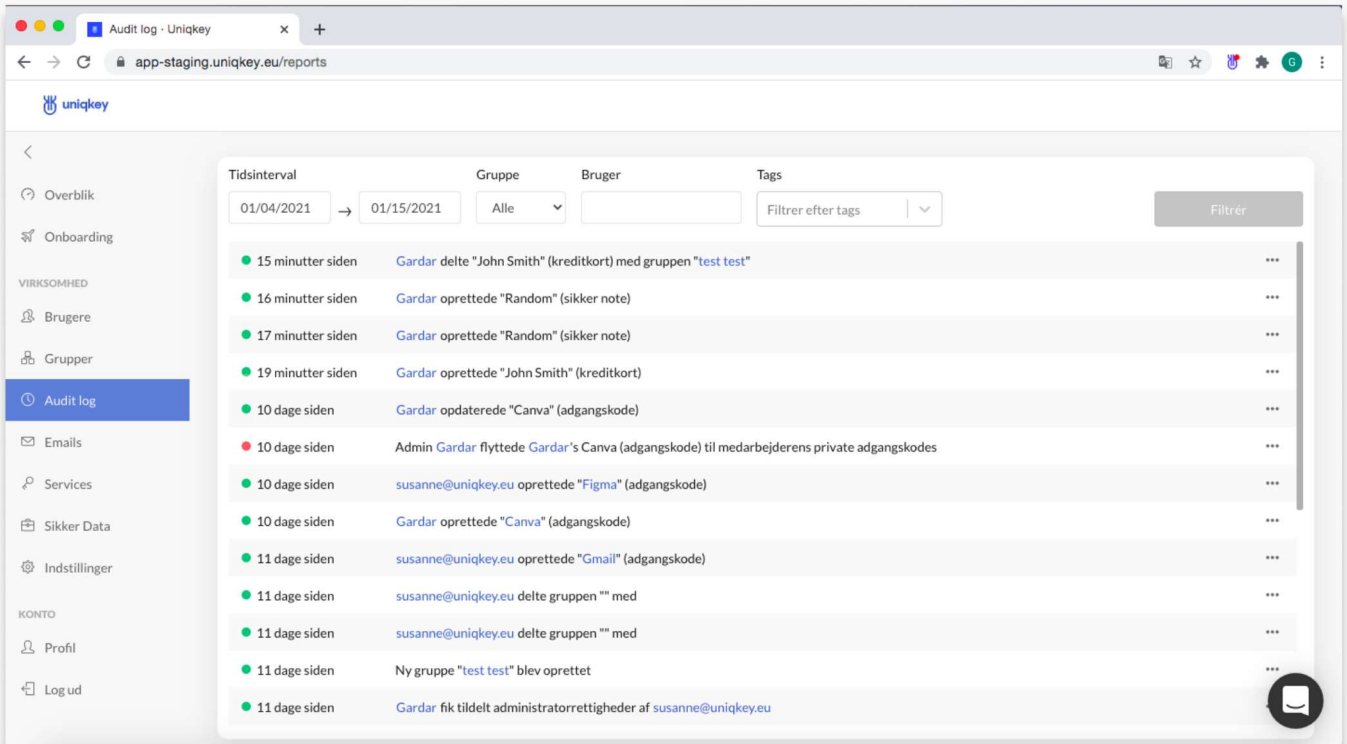
Når denne indstilling er slået til, vil alle medarbejdere i denne gruppe kunne kopiere adgangskoder, kreditkort og sikre noter. Hvis redigering er tilladt vil kopiering også være tilladt (da medarbejderen kan redigere og kopiere). Vi anbefaler at denne indstilling er slået til.

→ Opdater

## 9 Auditlog

Audit loggen viser en oversigt over logins og aktiviteter i Uniqkey - loggen viser både brugeres og administratorers aktiviteter.

Du kan se audit logs på enten gruppeniveau eller på de enkelte brugere, du kan filtrere tidsintervallet for auditloggen til den ønskede tidsramme.



The screenshot shows the Uniqkey Audit Log interface. The top navigation bar includes 'Audit log - Uniqkey' and the URL 'app-staging.uniqkey.eu/reports'. The left sidebar contains various menu items: 'Overblik', 'Onboarding', 'VIRKSOMHED', 'Brugere', 'Grupper', 'Audit log' (highlighted), 'Emails', 'Services', 'Sikker Data', 'Indstillinger', 'KONTO', 'Profil', and 'Log ud'. The main content area displays a list of activities with the following columns: 'Tidsinterval', 'Gruppe', 'Bruger', and 'Tags'. The activities are as follows:

Tidsinterval	Gruppe	Bruger	Tags
15 minutter siden		Gardar	delte "John Smith" (kreditkort) med gruppen "test test"
16 minutter siden		Gardar	oprettede "Random" (sikker note)
17 minutter siden		Gardar	oprettede "Random" (sikker note)
19 minutter siden		Gardar	oprettede "John Smith" (kreditkort)
10 dage siden		Gardar	opdaterede "Canva" (adgangskode)
10 dage siden		Admin Gardar	flyttede Gardar's Canva (adgangskode) til medarbejderens private adgangskodes
10 dage siden		susanne@uniqkey.eu	oprettede "Figma" (adgangskode)
10 dage siden		Gardar	oprettede "Canva" (adgangskode)
11 dage siden		susanne@uniqkey.eu	oprettede "Gmail" (adgangskode)
11 dage siden		susanne@uniqkey.eu	delte gruppen "" med
11 dage siden		susanne@uniqkey.eu	delte gruppen "" med
11 dage siden			Ny gruppe "test test" blev oprettet
11 dage siden		Gardar	fik tildelt administratorrettigheder af susanne@uniqkey.eu

### Overhold GDPR med Uniqkey

Efter GDPR trådte i kraft d.25/5-2018 er det et lovkrav at alle virksomheder skal kunne levere en komplet Audit-Log inden for 72 timer, hvis man bliver hacket eller på anden måde er involveret i et data-læk. Audit loggen kan også bruges internt til sikkerhedskontrol og den skal, af sikkerhedsmæssige årsager, altid kunne fremvises i tilfælde af databrud.