Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

Kevin Nordnes, Matias Skjetne

M365 Compliance and Security

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Marius Andre Langseth-Nilsen
Medveileder: Stein Meisingseth
Mai 2021

NTNU
Kunnskap for en bedre verden

Kevin Nordnes, Matias Skjetne

M365 Compliance and Security

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Marius Andre Langseth-Nilsen
Medveileder: Stein Meisingseth
Mai 2021

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

NTNU

Kunnskap for en bedre verden

Abstract

In this thesis we design and implement an IT-system for a small business: Trondheim Knekk og Brekk AS. The project has a strong focus on Microsoft's systems for ensuring compliance and security and tries to implement a transparent system which is both secure and complies with the European General Data Protection Regulation (GDPR). Throughout this paper we discuss the design of such a system and the implementation and changes that must be made for such a system to comply to Microsoft's design philosophies. The finished system will, although complete in the scope of this paper, be an implementation which will require further development and maintenance.

Innhold

Forord

Det å skrive en bacheloroppgave har vært an lang og krevende prosess. Det skal likevel sies at det har vært en utrolig lærerik prosess som har krevd mye kompetansebygging fra prosjektdeltakerne. Men ikke bare det, oppgaven har også blitt formet med god hjelp fra veiledere, medstudenter og konsulenter hos Atea. Vi vil derfor takke noen av de som har hjulpet oss ekstra mye for at resultatet skulle bli slik som det ble. Vi vil takke Stein Meisingseth, vår veileder fra NTNU og studiet, som hele veien har kommet med konstruktive tilbakemeldinger, motivert oss til å yte vårt beste og hjulpet oss med alle spørsmål og utfordringer som vi har hatt. Vi vil takke Marius Andre Langseth-Nilsen, vår veileder hos Atea, som har vært den personen vi har jobbet mest og tettest med gjennom hele våren. Din evne til å tilrettelegge, følge opp og veilede har vært til stor betydning for oss – takk for et flott samarbeid! Atea, som er bedriften vi har skrevet hos, har også vært en stor ressurs for oss, spesielt fordi det finnes så mange kompetente ansatte som er svært villige til å lære bort. Spesielt vil vi trekke frem Jørgen Sundet som med sin tekniske kompetanse hjalp oss på lang vei med å løfte vår oppgave til et nytt nivå.

1 FORSTUDIERAPPORT

1.1 Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
21/januar/2021	0.1	Første utkast	Kevin Nordnes & Matias Skjetne
4/februar/2021	1.0	Utkast for godkjenning av veiledere	Kevin Nordnes & Matias Skjetne

1.2 Innledning

1.2.1 Dokumentets hensikt

Trondheim knekk og brekk AS ønsker å fornye systemene sine for å kunne følge dagens standard for sikkerhet og personvern. Dette er en forstudierapport som har som formål å gi samsvar mellom den oppfatningen oppdragsgiver og oppdragstaker har om det produktet som skal leveres. Dette dokumentet kan ses på som en kontrakt mellom de to partene; den skal si noe om hva dette prosjektet kommer til å handle om, hva som kommer til å skje, hvilke kostnader det kommer til å få og hvilke resultater partene ser for seg.

Dagens teknologi utvikler seg utrolig raskt og informasjon blir samlet og delt på en mye større skala enn noensinne før. Lagring av informasjon fører til mange nye muligheter samt nye problemer som bedrifter nå i dag står ovenfor. Datainnhentingen er med på å effektivisere hele behandlingsprosessen hos pasienter og gjort at en enklere kan finne nye løsninger på medisinske problemer. All denne datalagringen fører også til at store mengder personlig og sensitiv informasjon blir prosessert og delt rundt. Her kommer problemene som vi skal løse i dette prosjektet; Hvordan kan dette gjøres på en måte som holder informasjonen sikker fra uvedkommende og lett tilgjengelig for de som trenger den?

1.2.2 Avgrensninger

Dette dokumentet definere kun betingelsene for prosjektet, men går ikke inn på detaljer om implementering og teknologier. Mer spesifikt om hva prosjektet kommer til å inneholde vil bli forklart i designrapporten.

1.2.3 Definisjoner og forkortelser

WVD – Windows Virtual Desktop
GDPR – General Data Protection Regulation
ATP – Azure Threat Protection

1.2.4 Oversikt over innholdet

Punktet Bakgrunn for prosjektet (1.3) beskriver problemstillingen og begrunner prosjektets eksistens. Under Prosjektmål (1.4) bestemmes hvilke mål som settes til prosjektet for at det kan vurderes som en suksess. Interessenter og rammebetingelser (1.5) definerer hvem prosjektets interessenter er og hvilke betingelser og minimumskrav som settes til prosjektet. Under Kritiske suksessfaktorer (1.6) defineres hvilke krav som settes for at det skal være mulig å gjennomføre prosjektet. Risikoanalysen (1.7) skal sette søkelys mot eventuelle farer og hendelser som kan oppstå og forstyrre prosessen og resultatet. Punktet Kost/nytte-analyse (1.8) definerer hvilke kostnader og hvilken nytte bedriften skal/kan få ut av dette prosjektet. Retningslinjer og standarder (1.9) setter krav til rapporter, metoder og rutiner som skal brukes i prosjektet. Prosjektorganisering (1.10) gir en oversikt over prosjektets deltakere og interessenter. Helt til slutt er det en Anbefaling om videre arbeid (1.11) som understreker behovet for et slikt prosjekt før referansene (1.12) ligger i det siste punktet.

1.3 Bakgrunn for prosjektet

Bedriften Trondheim Knekk og Brekk AS har i dag en digital løsning som benytter seg av Office 365 E3. De ønsker å forbedre sikkerheten samt passe på at alle GDPR krav om sensitive personopplysninger overholdes. Derfor har de bedt oss (Atea) om å prosjektere en oppgradering.

1.3.1 Beskrivelse av problemer og behov

I bedriften Trondheim Knekk og Brekk skal det sendes personsensitive data over e-post, det skal kunne lagres på OneDrive og samhandles med over Teams. Problemet ligger i at GDPR må overholdes slik at ulike ansatte kun får tilgang til den informasjonen som de skal. Det er derfor behov for fokus på sikkerhet og personvern, noe som gjør det viktig med gode rutiner og sikre programmer. Dette skal være med på å gjøre det enkelt å overholde de kravene som blir satt for å kunne aksessere den ulike informasjonen – konfidensialitet, integritet og tilgjengelighet blir nøkkelord.

For at systemet i seg selv skal bli enkelt å lære seg for de ansatte og for at de ulike programmene skal kunne fungere godt sammen blir essensielt å bruke en løsning som klarer å dekke alle eller tilnærmet alle behov - Microsoft 365 er en slik totalløsning. M365 E5 inneholder programmer som ansatte i bedrifter ofte allerede er godt kjent med, som Windows 10, OneDrive og Office 365. Dette kan være helt nødvendig ettersom at prosjektets suksess avhenger av at alle ansatte følger de satte rutinene og programmene som løsningen skal inneholde.

Et (mulig) sikkerhetsproblem i dagens rutiner er at hver ansatt har et 1-1 forhold til sin datamaskin. Dette gjør bedriften i seg selv mye mindre fleksibel og gjør systemet mer sårbart, spesielt dersom det kan være ansatte som tar med seg sin maskin hjem. For å kunne sikre god konfidensialitet og tilgjengelighet blir det viktig med en sikrere og mer fleksibel løsning enn den de har i dag.

1.3.2 Kort om dagens systemer og rutiner

I dette punktet beskrives hvordan systemet fungerer den dag i dag hos TKoB og hvilke problemer og utfordringer det bringe. Det beskrives derfor også hvilken oppgradering som som bør implementeres for å svare på dette.

1.3.2.1 Dagens systemer

Dagens system har en brukerbase på ca. 80 ansatte fordelt over fire kontorer. Hver ansatt har en egen Windows 10 datamaskin og er satt opp i Office 365 E3 økosystemet. I tillegg til 80 klientdatamaskiner har man ett infosystem på hvert kontor. Systemet har ingen felles lagringsløsning og det meste av filutveksling skjer over e-post.

I dag brukes Office-produkter daglig av både leger og administrasjon for å utføre behandling og daglig drift. Dette medfører kommunikasjon på e-post mellom spesialister og administrasjon samt planlegging av timer i kalender. Mye av informasjonen som håndteres er ifølge GDPR klassifisert som sensitiv personinformasjon. Denne informasjonen blir ikke behandlet i henholdt til GDPR. Det finnes ingen oversikt over hvem som har aksessert informasjonen eller hvem som har tilgang. Dette må bedriften få orden i raskt for å unngå bøter fra myndighetene.

Det medfører et stort ansvar å håndtere slik informasjon, og glipper kan koste bedriften dyrt både i forma av store pengebeløp og tap av omdømme.

1.3.2.2 Oppgraderingen

Bedriften skal gjennom en omfattende oppgradering av systemene sine. De skal fortsette i et Office 365 økosystem, men vil ta i bruk flere sikkerhets elementer og skal ta i bruk Azure løsninger i større grad. Bedriften ønsker seg et system som gjør det enkelt å dele både normal og sensitiv data på en sikker måte. For å løfte ansvaret mest mulig av skuldrene til brukeren skal systemet benytte seg av automatiserte prosesser for å sikre at informasjon blir behandlet i henhold til GDPRs retningslinjer.

1.4 Prosjektmål

Ut ifra problemstillingen og dagens situasjon har vi formulert et sett med mål som skal være veiledende gjennom prosjektet. Disse målene skal sette kursen for prosjektet og skal brukes for å måle hva en fikk oppnådd og ikke av prosjektet. Vi deler disse inn i tre kategorier.

1.4.1 Effektmål

- Øke bedriftens digitale sikkerhet ved hjelp av Microsofts systemer og løsninger.
- Øke samsvar med GDPR gjennom sikring av sensitiv persondata og aksesslogger.
- Forenkle de ansattes hverdag gjennom automatisering av prosesser knyttet til GDPR krav.

1.4.2 Resultatmål

- Innføre et IT-system som automatisk tar seg av sikkerhetsrisikoer som oppdages samt beskytter brukere mot GDPR overtramp.
- En sky-basert løsning som tar i bruk Microsoft sine produkter og løsninger.
- En digital løsning som gjør det enklere for ansatte å dele sensitiv informasjon i henhold til GDPR.

1.4.3 Prosessmål

- Bygge kompetanse i Microsoft sitt økosystem med søkelys på sikkerhet.

1.4.4 Prosjektets omfang

- Prosjektet tar for seg designet av et nytt datasystem for bedriften.
- Prosjektet tar for seg implementeringen av nytt datasystem for bedriften.
- Prosjektet tar ikke for seg opplæring av ansatte.
- Prosjektet tar ikke for seg videre drift av systemet.

1.4.5 Prosjektets milepæler og hovedaktiviteter

Se vedlegg.

1.5 Interessenter og rammebetingelser

1.5.1 Interessentanalyse

Det er fire hovedinteressenter i dette prosjektet; oppdragsgiver (Trondheim Knekk og Brekk AS), oppdragstaker (Atea), pasienter hos Knekk og Brekk og sluttbruker (hovedsakelig de ansatte). Oppdragsgiver er initiativtaker av prosjektet og er den interessenten som vil sette de fleste krav og gjøre de største beslutningene. Oppdragstaker er interessenten som kommer til å gjennomføre selve prosjektet, implementere det nye systemet og være ansvarlig for den videre driften. Sluttbrukeren av systemet vil stort sett være de ansatte hos Trondheim Knekk og Brekk AS. Pasientene vil også bli sett på som en interessent ettersom de også kan komme til å ta nytte av fordelene av et slikt prosjekt.

Selv om det er oppdragsgiver som setter det meste av krav, vil det være helt kritisk at sluttbruker er fornøyd med resultatet av prosjektet. Ellers kan det føre til at de ansatte ikke bruker systemet slik det er ment eller begynner å bruke andre løsninger som kan stride imot formålet med prosjektet.

Hver av interessentene har sine forventninger og suksesskriterier til prosjektet. Oppdragsgiveren ønsker å se resultater av prosjektet gjennom økt fokus på sikkerhet og personvern, uten at det går ut over effektivitet i bedriften. Et ønsket resultat vil også være økt effektivitet gjennom bruk av et fullstendig system hvor ellers tungvinte rutiner rundt personvern, sensurering og adgangskontroll blir automatisert. Bedriftens pasienter vil ha interesse av at ens personlige data blir holdt konfidensiell. Dette er kanskje ikke noe pasientene kommer til å merke så veldig godt, men skulle det komme et dataangrep så vil nok pasientene sette pris på at informasjonen deres er sikker. Opplyste kunder/pasienter vil nok også foretrekke bedrifter som følger GDPR-krav (selv om dette uansett er pålagt).

Oppdragstakeren vil ha interesse i å levere et godt produkt for å tilfredsstille både kunden/oppdragsgiver og for å lette arbeidet til egne ansatte som skal drifte systemet videre. Alle interessentene, kanskje med unntak av pasientene, vil tilfredsstilles gjennom en rask og enkel overgang til det nye systemet. De ansatte vil også trenge god opplæring slik at systemet blir brukt som forventet og for at de ansatte skal kunne ta nytte av det på best måte.

Interessent	Suksesskriterier	Bidrag til prosjektet	Interessentens krav
Oppdragsgiver	Et sikrere system som overholder GDPR-krav Fornøyde ansatte og kunder Økt effektivitet gjennom automatisering	Beslutninger og krav Overordnet ansvar Godkjenning av rapporter og resultat	Frister blir overholdt Systemet sørger for at GDPR blir overholdt Systemet består kun av produkter fra Microsoft
Sluttbruker	Enklere arbeidshverdag	Ideer, ønsker og innspill Brukertester	Et brukervennlig system God opplæring
Oppdragstaker	Vellykket implementering av nye systemer Fornøyd oppdragsgiver	Ansvar for gjennomføring Implementering av nytt system	Realistiske krav og mål Godt samarbeid mellom de ulike interessentene
Kunder/pasienter	Kunden merker lite til selve overgangen Ingen negativ effekt på kundeopplevelsen	Ingen	Personlig sensitiv informasjon blir tatt vare på i henhold til GDPR

1.5.2 Rammebetingelser

I dette kapittelet setter vi noen absolutte krav som skal være med på å sette føringer for hvordan prosjektet vil utformes. Her vil vi sette absolutte minimumskrav til hva løsningen skal inneholde og for hvilke betingelser selve prosjektet skal ha. Med betingelser snakker vi om rammer for når prosjektet skal være ferdigstilt og for hvilket budsjett en får å operere med.

Prosjektet skal være ferdig og levert den 20. mai 2021. Systemet skal være lagt opp til å overholde GDPR-krav. Det skal være mulig å dele personsensitiv data over e-post, lagre det på OneDrive og samhandle på Teams.

Produkter som skal tas i bruk:

- Microsoft Intune
- Microsoft AutoPilot
- Microsoft 365 E5
- Microsoft Teams
- OneDrive
- MS Azure App Service
- Windows Defender
- O365 ATP
- Identity Protection
- Information Protection
- WVD

1.6 Kritiske suksessfaktorer

De kritiske suksessfaktorene er de forutsetningen som må oppfylles for at prosjektet skal kunne vurderes som vellykket. Disse punktene er satt sammen med oppdragsgiver slik at alle parter er enige om hva som skal dekkes. Dette vil være med på å hjelpe prosjektgruppen med å vite hva som skal jobbes mot og det vil hjelpe beslutningstakerne til å ta rette beslutninger. Prosjektet har også et behov for en viss kompetanse for å kunne utføres. Dokumenter og informasjon som blir nødvendig står beskrevet under «Informasjonsbehov».

1.6.1 Suksessfaktorer

- Enkel deling av filer mellom ansatte.
- Sikker deling av sensitiv informasjon med aksesslogger.
- God oversikt over hvordan sensitiv informasjon lagres og sikkerhetskopieres
- God beskyttelse mot e-post phising og andre angrepsvektorer.

1.6.2 Informasjonsbehov

Gjennom prosjektets gang vil det produseres en rekke dokumenter inkludert; forstudierapport, designrapport, driftsrapport og sluttrapport. Utkast til disse rapportene leveres hver onsdag, så sant det er nødvendig, til veileder fra NTNU og Atea. Ferdige rapporter blir å finne på Teams og vil også bli sendt til veiledere.

Det blir holdt veiledningsmøter hver andre uke og referat fra disse skal bli gjort tilgjengelig via Teams. Timeliste skal føres for hver uke og skal gjøres tilgjengelige i Teams. I slutten av uken skal det skrives en rapport om hva som ble gjort i uken som gikk, denne skal gjøres tilgjengelig på Teams.

1.7 Risikoanalyse

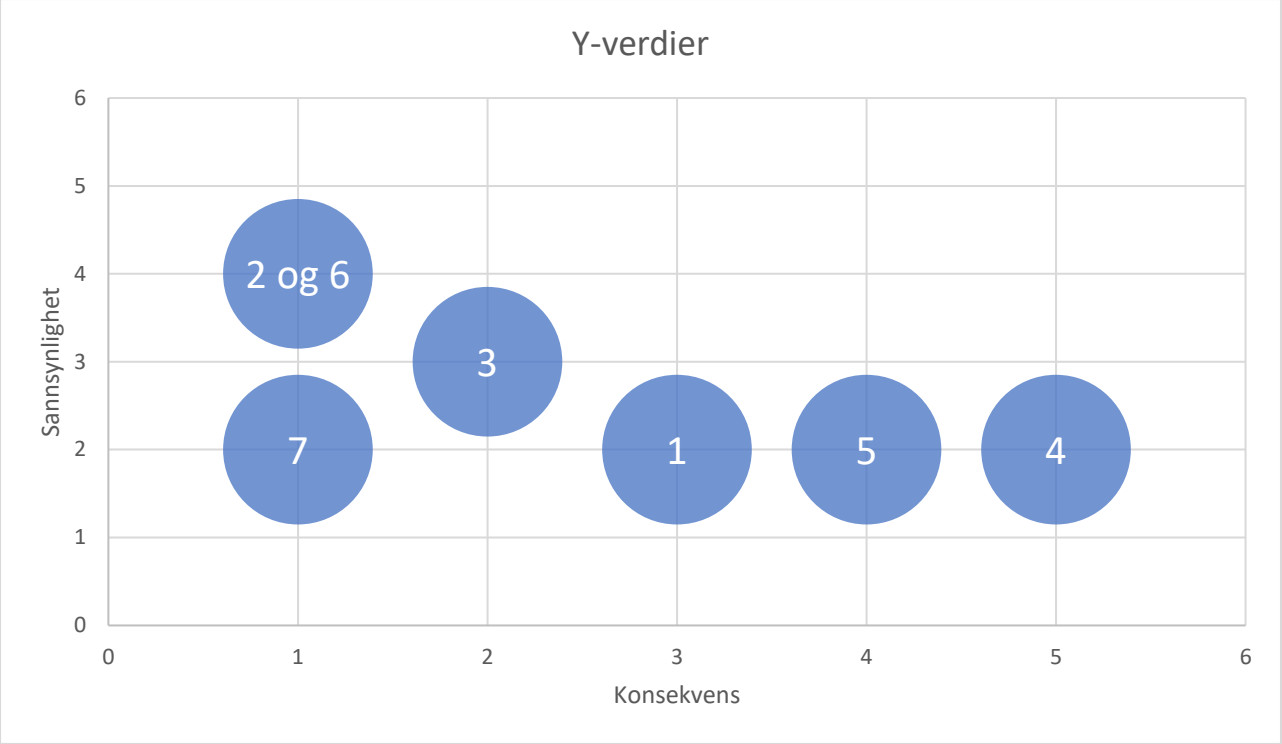
Risikoanalyse gjennomføres for å skaffe seg et overblikk over hva som kan gå galt i prosjektet. Den er ikke fullstendig da det ikke er mulig å forutse alle mulige uønskede hendelser. Det skal også foreslåes tiltak som enten skal forebygge eller reparere følgene av hendelsen. Hver hendelse blir rangert etter hvor alvorlig den er og hvor sannsynlig det er at den inntreffer. Ut ifra dette får man en rangering som man kan bruke til å prioritere tiltak.

Veldig alvorlig	5	10	15	20	25
Alvorlig	4	8	12	16	20
Moderat	3	6	9	12	15
Liten	2	4	6	8	10
Ubetydelig	1	2	3	4	5
	Veldig lav	Lav	Moderat	Høy	Veldig høy

Hendelse	Konsekvens	Tiltak	S	K	R	Kommentar
1. **Splid eller uenighet mellom prosjektdaltakere**	Dette kan føre til tap av tid og ressurser. Produktiviteten vil mest sannsynlig minke. Prosjektet blir kanskje ikke ferdig til avtalt tid og prosjektets resultat blir muligens ikke av avtalt kvalitet.	Veiledere skal kontaktes så raskt som mulig. Eventuelt kan aktuelle fagpersoner brukes for å prøve å løse problemet. Dette må vurderes ut ifra hvem det gjelder.	2	3	6	
2. **Sykdom eller fravær hos prosjektdeltakerne**	Arbeidet blir forsinket	Smittevernstiltak etter FHI sine retningslinjer. Ta i bruk digital arbeidsplass så mye som mulig for å unngå unødvendig utsettelse for smittefare.	4	1	4	Dette prosjektet er skrevet samtidig som det foregår en pandemi noe som gjør at dette punktet blir desto mer relevant.
3. **Tekniske problemer i f.eks. utviklingsmiljø eller andre produkter som skal tas i bruk**	Dette vil mest sannsynlig føre til stans i prosjektets framgang.		3	2	6	
4. **Mislykket implementasjon av nytt system**	En misfornøyd kunde. Dette kan føre til høyere kostnader dersom det fører til mer arbeid eller et nytt	Gode rutiner for sikkerhetskopiering slik at en kan rulle tilbake til en tidligere fungerende fase dersom dette er aktuelt.	2	4	8	

		«forsøk» på implementasjon.	Ta i bruk et større spekter av kompetanse ved å for eksempel ta inn ekstra konsulenter i prosjektgruppen.				
5.	**Nytt system oppfyller ikke kravene som har blitt satt**	Prosjektet blir ikke kvalifisert som en suksess dersom ikke alle kravene som skulle oppfylles blir det. Hvis systemet likevel implementeres kan dette føre til en dårlig brukeropplevelse eller at sikkerheten i systemet er for dårlig. Dette går både ut over de ansatte og det kan gå ut over kunden dersom informasjonen deres ikke oppbevares sikkert.	Dokumentere kravene godt på forhånd å bli enige med oppdragsgiver om kravene. God kommunikasjon med oppdragsgiver ved eventuelle endringer.	2	4	8	
6.	**Mangel på informasjon eller kompetanse**	Konsekvenser av dette vil først og fremst være at det vil bli brukt tid og ressurser på å tilegne seg den rette informasjonen. Dersom deltakerne ikke klarer å tilegne seg	Deltakerne får bruke læringsressurser som er blir gjort tilgjengelige av ATEA. ATEA har mange konsulenter med mye kompetanse og ulike eksperområder som kan bistå.	4	1	4	Konsekvensene avhenger av om det kun er deltakerne som mangler den nødvendige informasjonen eller om informasjonen ikke finnes og må skapes på egen hånd.

	informasjonen vil dette gå utover kvaliteten på sluttproduktet og kan gjøre at suksesskriteriene ikke blir oppfylt.	Dersom ingen av tiltakene over holder mål, kan prosjektgruppen ta direkte kontakt med Microsoft (eller annen aktuell leverandør) for å få hjelp med eventuelle problemer og spørsmål vi har.				
7. Ingen mulighet for fysisk oppmøte hos ATEA	Konsekvensen kan være at kvaliteten på prosjektet ikke vil bli lavere. Terskelen for å spørre konsulentene i firmaet øker.	Holde seg unna smittekilder og unngå å få Korona	2	1	2	Det er alltid enklere å kommunisere ansikt til ansikt og terskelen for å spørre andre om hjelp senkes når man kan møte fysisk med bedriften Dette punktet er det vanskelig å lage tiltak mot da en bare kan sørge for at en selv er frisk. Samfundet har man ikke kontroll over.


Y-verdier
Sannsynlighet
Konsekvens
0
1
2
3
4
5
6
2 og 6
3
7
1
5
4

1.8 Kost/nytte-analyse

For å lettere ta en beslutning om prosjektet bør gjennomføres utfører vi en kost- og nytteanalyse. Det vil her bli gjort anslag om hvor mye prosjektet kommer til å koste og hvilke goder/nytte det vil komme ut av prosjektet. Vi skal her sammenligne den planlagte Microsoft-løsningen mot 0-alternativet – altså å ikke gjøre noen ting. Ettersom prosjektet ikke vil føre til en direkte inntektskilde eller noe økt salg drøfter vi nytten i det ikke-økonomiske perspektivet. Kostnadene beregnes ut ifra Microsoft sin egen kalkulator for å sette sammen et system.

1.8.1 Kvantifiserbar og ikke-kvantifiserbar nytte

I dette prosjektet er effektmålene som følger:

- Øke bedriftens digitale sikkerhet ved hjelp av Microsofts systemer og løsninger.
- Øke samsvar med GDPR gjennom sikring av sensitiv persondata og aksesslogger.
- Forenkle de ansattes hverdag gjennom automatisering av prosesser knyttet til GDPR krav.

Kvantifiserbar nytte:

- Unngå GDPR bøter
- Redusere sjansen for kostbare løsepengevirus

Ikke-kvantifiserbar nytte:

- Redusert press for å feil håndtere sensitive pasientdata
- Enklere arbeidshverdag for de ansatte
- Økt trygghet blant kundene

1.8.2 Bortfall av potensielle direkte kostnader

1.8.2.1 Bøter ved brudd på GDPR

Ved brudd på GDPR vil det påføre bedriften store finansielle tap i form av bøter. Bøtene vil variere ut ifra størrelsen på overtrampet, og typen overtramp. Siden bedriften behandler og lagrer helsedata som under GDPR er regnet som sensitive personopplysninger, vil bøtene for feilaktig behandling variere fra 500 000 til flere millioner kroner. I en sak i helse sørøst ble ni institusjoner bøtelagt 800 000 kroner. (Ni helseforetak er varslet om gebyr, 2017)

1.8.2.2 Kostnader knyttet til løsepengevirus og tap av data

De siste årene har dataangrep som låser ned alle filene på systemet for å kreve løsepenger, økt i popularitet. Det har også oftere skjedd at aktørene går etter kritiske sektorer som helse. Selv små perioder med utilgjengelighet kan koste menneskeliv og det er derfor større sjanse for at offeret betaler raskt. Det varierer veldig hva som kreves av løsepenger, men en rapport gjort av Coveware viser at gjennomsnittlig kostnad i Q4 2019 var 725 720,88 kr (84 116 usd). (Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate, 2020). I tillegg til disse kostnadene kommer tap av inntekter, eventuelle tap av kritisk data og skade på omdømme.

1.8.3 Estimerte kostnader

1.8.3.1 Lisenskostnader

Lisens	Kostnad/bruker/mnd	Antall brukere/enheter	NOK/mnd
NÅVÆRENDE KOSTNADER			
Office 365 E3	187,50 kr	80 brukere	15 000 kr
Windows 10 Enterprise E3	60,37 kr	80 brukere	4 829,60 kr
SUM			**19 829,60 kr**
NYE KOSTNADER			
Microsoft 365 E5	515,70 kr	80 brukere	41 256 kr
App Service			1 382,50 kr
Virtual Machines		5 enheter	7 819,15 kr
Support			811,41 kr
SUM			**51 269,06 kr**
DIFFERANSE			**+31 439,46 kr**

1.8.3.2 Sammenstilling kost/nytte

Dette prosjektet har ingen kvantifiserbar nytte som kan realiseres, bare potensielle bortfall av kostnader. De potensielle kostnadene er dog mye høyere en prisen for å implementere og drifte det nye systemet så i lengden lønner det seg. De potensielle kostnadene er heller ikke begrenset til engangssummer og kan påløpe flere ganger. Dette styrker argumentet om at prosjektet, selv om det er en ren utgift, vil lønne seg i lengden

1.8.3.3 Ikke kvantifiserbar nytte

I tillegg til de finansielle fordelene til prosjektet har det også noen ikke kvantifiserbare fordeler. De ansatte som i dag har mye av ansvaret for at personopplysninger ikke havner på feil sted, vil ta i bruk verktøy som tar over mye av dette ansvaret. Dette betyr at en liten feil fra de ansatte ikke vil kunne føre til store problemer fra bedriften. En stor del av befolkningen har relativt enkel datakunnskap og gjør ofte feil når det bruker dataverktøy. Mange av de tungvinte arbeidsmåtene, som det å dele filer på e-post, vil i dag bli gjort enklere med det nye systemet. Dette betyr at de ansatte vil bruke mindre tid på frustrerende oppgaver og mer tid på pasienter og viktige arbeidsoppgaver.

En annen fordel er at bedriften vil kunne profilere seg som opptatt av å sikre personopplysningene til sine pasienter. Det å skape trygghet hos sine kunder er viktig i en tid hvor datainnbrudd får stadig større konsekvenser og den generelle befolkningen blir mer bevist på disse konsekvensene. Det at kundene vil kunne føle seg trygge på å dele sensitive personopplysninger vil være av stor verdi for bedriften.

1.9 Retningslinjer og standarder

1.9.1 Krav til dokumentasjon

Dokument	Innlevering	Form
Forstudierapport	29.01.2020	Digitalt
Designrapport	19.02.2020	Digitalt
Driftsrapport	14.05.2020	Digitalt
Sluttrapport	20.05.2020	Digitalt
Timeliste	Ukentlig	Digitalt
Ukesrapport	Ukentlig	Digitalt
Presentasjon	20.05.2021 (±2 uker)	Fysisk (dersom mulig) eller digitalt

1.9.2 Krav til kvalitetsgjennomganger

Annenhver uke vil det være møte med veiledere (Atea, NTNU) hvor det blir tatt en gjennomgang av fremgangen i prosjektet og fortløpende gjennomgang av dokumenter. Disse møtene vil hovedsakelig foregå digitalt (Teams) pga. pandemisituasjonen, men dette er noe som kan endre seg senere.

Alle dokumenter legges på Microsoft Teams slik at alle deltakere (prosjektmedlemmer og veiledere) kan se på de når som helst. Dokumenter godkjennes av bedriftskontaktperson i samarbeid med prosjektmedlemmer og med tilbakemelding fra veileder (NTNU). Etter at systemet er satt sammen vil det utføres brukertester sammen med veileder for å kvalitetssikre produktet.

1.9.3 Krav til standarder og metoder

- Referanser som brukes i dokumentene skal ta i bruk APA-standarden.
- Dokumenter skal skrives i Microsoft Word (.docx) og leveres som PDF
- Digitale møtes skal utføres gjennom Microsoft Teams
- Microsoft Azure skal brukes som plattform for systemløsningen
- Løsningen skal lages for å oppfylle kravene om informasjonssikkerhet i GDPR

1.9.4 Endringshåndtering

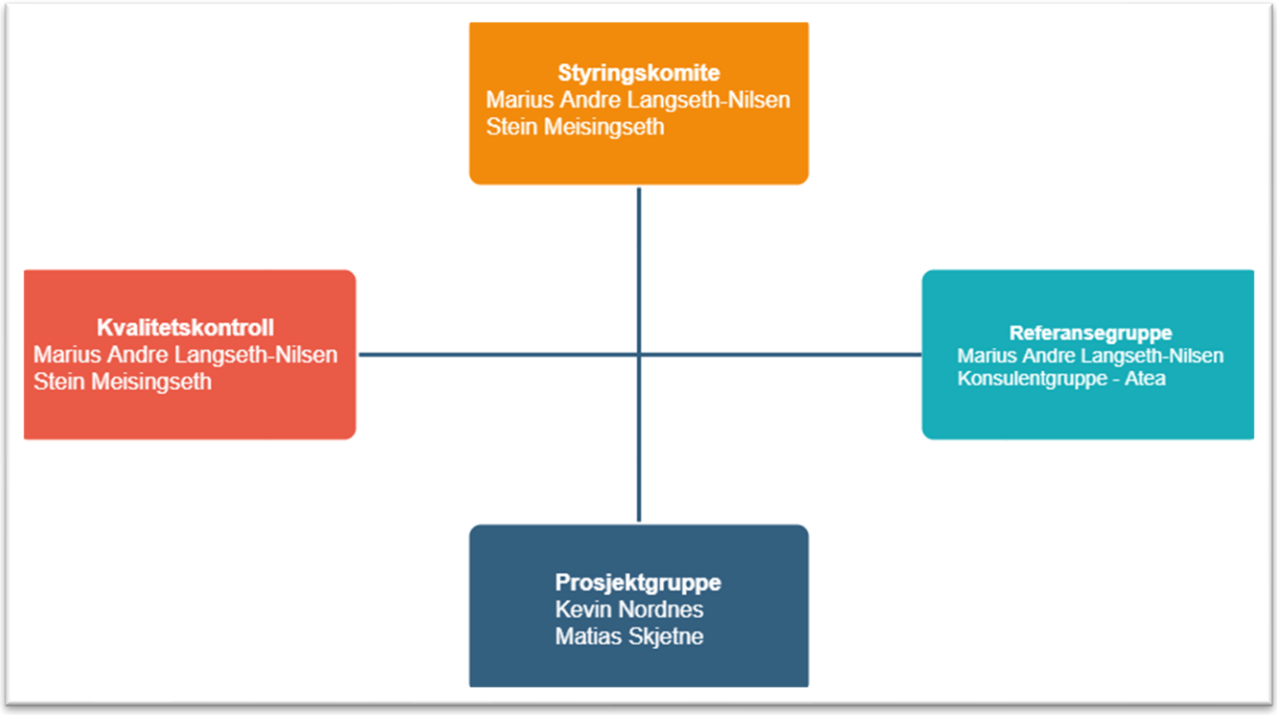
Underveis i prosjektet kan det oppstå endringsforespørsler fra prosjektleder/veileder, kunde (Trondheim Knekk og Brekk AS, prosjektmedlemmer eller de ansatte. Alle ønsker om endringer skal dokumenteres og gjennomføres i henhold til følgende mal:

1. Endringen skal beskrives og dokumenteres
2. Konsekvenser for prosjektet som kan komme av endringen skal analyseres
3. Det skal gjøres en kost/nytte analyse
4. Endringen skal godkjennes for utførelse
5. Endringen loggføres
6. Prosjektplanen skal justeres
7. Alle interessenter skal informeres
8. Endringen gjennomføres

1.10 Prosjektorganisering

Dette prosjektet vil bestå av en styringskomite hvor medlemmene er Marius Andre Langseth-Nilsen og Stein Meisingseth. Langseth-Nilsen er ansatt hos Atea og har rollen som oppdragsgiver og veileder. Meisingseth er ansatt hos NTNU og vil også være med som veileder i dette prosjektet. Disse vil se til at prosjektet går sin gang og vil være til hjelp ved eventuell konflikt mellom prosjektdeltakerne. De samme medlemmene vil også stå for kvalitetskontroll av prosjektet. Dette skal sikre at alt av dokumenter som blir levert er til ønsket standard og at implementeringen av systemet holder mål.

Selve prosjektgruppen består av Kevin Nordnes og Matias Skjetne. Det er valgt å ikke ha en leder i denne gruppen ettersom den kun består av to medlemmer og det ikke har blitt sett på som noe nødvendighet. Nordnes vil ha rolle som møteleder og vil ta seg av alle møteinnkallinger. Skjetne vil føre referat i disse møtene. Referansegruppen vil blir brukt til å gi tilbakemelding og komme med råd underveis. Denne vil bestå av Langseth-Nilsen og en konsulentgruppe fra Atea.



1.11 Anbefaling om videre arbeid

Ved å sette fokus på personvern og automatisering av sikkerhetstiltak vil dette gjøre hverdagen til de ansatte enklere og det gjør det lettere å kunne konsentrere seg om egne arbeidsoppgaver. Dette prosjektet er et investeringsprosjekt og det er derfor ikke å forvente at det vil føre til noe ny inntekt. Skal Trondheim Knekk og Brekk følge EUs krav om GDPR og kunne forsikre kunden sin om at deres lagrede data er sikker vil dette prosjektet bidra til dette.

Dataangrep blir bare mer og mer vanlig den dag i dag og skal dagens bedrifter kunne komme ut av et slikt angrep med ryktet sitt i behold, vil det å gjøre slike forebyggende tiltak være helt essensielt. Etter å ha utført denne forstudierapporten konkluderer vi med at vi sterkt vil anbefale å gå videre med prosjektet – ettersom vi ser på det som en viktig investering.

1.12 Referanser

Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate (Rep.). (2020, January 23). Retrieved January 18, 2021, from https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

Ni helseforetak er varslet om gebyr. (2017, October 27). Retrieved January 18, 2021, from https://www.datatilsynet.no/aktuelt/2017/ni-helseforetak-er-varslet-om-gebyr/

2 DESIGNRAPPORT

2.1 Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
27/januar/2021	0.1	Første utkast	Kevin Nordnes & Matias Skjetne
17/februar/2021	0.2	Utkast for tilbakemelding	Kevin Nordnes & Matias Skjetne
03/mars/2021	1.0	Til godkjenning	Kevin Nordnes & Matias Skjetne

2.2 Innledning

I denne rapporten vil vi presentere designet for systemet bestilt av Trondheim Knekk og Brekk AS. Det vil være en grundig gjennomgang av hvordan systemet skal settes opp og hvilke teknologier som skal dekke kundens behov. Design og teknologivalg blir forklart og begrunnet slik at kunden får en god oversikt over det nye systemet og nytten det bringer.

2.2.1 Dokumentets hensikt

Designrapporten er en fortsettelse på forstudierapporten. Her går vi mye mer detaljert inn i hvordan det nye systemet skal bli. Dette dokumentet skal være med på å kartlegge kundens behov slik at vi lettere kan se hvilke løsninger som kan passe til det nye systemet. Hvor forstudierapporten var en mer overordnet beskrivelse av prosjektet, vil designrapporten være en mer konkret og presis beskrivelse av nøyaktig hvilke produkter og tjenester som skal være med i den endelige løsningen.

Ut av dette dokumentet skal leseren få en forståelse av hvorfor de ulike valgene er tatt og hvordan de skal være med på å nå de målene som ble satt i forstudierapporten. Etter å ha lest dette dokumentet skal leseren få en forståelse av hvordan sluttproduktet kommer til å være utformet. Dokumentet er hovedsakelig rettet mot kunden og oppdragsgiver.

2.2.2 Avgrensning

Prosjektet omfatter de fleste av Trondheim Knekk og Brekks systemer, E-post, lagring og skrivebordsmiljø blant dem. Det inneholder ikke løsninger for regnskapsføring eller timebooking, da dette håndteres av tredjepartssystemer.

2.2.3 Definisjoner og forkortelser

WVD – Windows Virtual Desktop
AD – Active Directory

2.2.4 Oversikt over innholdet

I 2. Løsningsdesign starter vi med å beskrive kundens behov (2.3.1) før vi kommer med en kort forklaring på hvorfor vi valgte akkurat den teknologien vi gjorde (2.3.2). Vi dykker så litt dypere inn i hver av de ulike teknologiene og tjenestene, og snakker om hva de brukes til og hvordan de er relevante (2.3.3). Vi kommer så med en beskrivelse av dagens situasjon (2.3.4.1) for å så gi en oversikt over alle deloppgavene som må løses i dette prosjektet (2.3.4.2). I neste punkt (2.3.4.3) viser vi til en figur over alle tjenestene og hvordan disse fungerer sammen. Det vil så bli beskrevet hvilke forutsetninger som skal til for at prosjektet skal kunne gjennomføres (2.3.4.4). Videre ser vi på hvilke konsekvenser prosjektet kan ha for det organisatoriske og personellmessige (2.3.4.5). Det kommer så en kort forklaring på hvilke type programvare som skal brukes og hvilke systemkrav som er satt (2.3.4.6). Hvilke krav det er til dokumentasjon er forklart i det neste punktet (2.3.4.7). De neste tre punktene (2.3.4.8-10) beskriver piloten som skal gjennomføres før full implementasjon, og hvilke krav som er satt til den. Det kommer så en oversikt over deltagerne og deres roller i prosjektet (2.3.4.11). Helt til slutt er det vedlagt en aktivitetsplan for det videre arbeidet (2.3.4.12).

2.3 Løsningsdesign

2.3.1 Kort om kunden og behov

Trondheim Knekk og Brekk AS er en bedrift som driver med ortopedi og fysioterapi, noe som gjør at de må ta vare på mye persondata og helsedata. Bedriften har derfor behov for en løsning som gjør at deres kunders informasjon blir håndtert på en sikker måte og krav for GDPR må overholdes. For at informasjon skal kunne lagres, deles og arbeides med på en sikker og effektiv måte, har kunden behov for en komplett løsning hvor tilgangskontroll og sikker deling blir håndtert automatisk. Dette skal gjøre at det blir mye vanskeligere for de ansatte å gjøre feil som kan føre til mishandling av sensitiv kundedata.

2.3.2 Hvorfor valg av produkt-teknologi-løsning

Vår løsning er bygget på Microsofts skyplattform Azure og vil ta nytte av produkter som Office 365, Teams og diverse sikkerhetsprodukter som f.eks. Windows Defender, Microsoft Defender og Information Protection. Azure tilbyr en rekke produkter som garanterer god sikkerhet, samt tjenester for fjernstyring slik at de ansatte skal kunne jobbe fra hvor som helst. Slik det er i dag har hver ansatt en egen PC som tilhører seg selv, noe som ikke er heldig med tanke på sikkerhet dersom de ansatte tar med seg datamaskinen til og fra jobb. Ved å ta i bruk Windows Virtual Desktop (WVD) vil dette gi bedriften en mye større helhetlig fleksibilitet. De ansatte kan da i praksis jobbe sikkert, fra hvilken som helst datamaskin.

Dette prosjektet er først og fremst et investeringsprosjekt, noe som ikke vil føre til økte inntekter som følge av implementeringen. Det vil komme nye faste kostnader hver måned gjennom lisenser hos Microsoft. Hver bruker vil ha en egen M365 E5 lisens som vil være en stabil månedlig utgift dersom bedriften ikke velger å utvide og får behov for flere lisenser. Det samme gjelder de virtuelle maskinene som skal være tjenere for systemet. Disse vil mest sannsynlig ikke ha noe behov for å oppgraderes med det første, men det kan komme behov for å utvide lagringskapasiteten og eventuelt oppgradere dersom en ønsker raskere tjenester.

Fra forstudierapportens kost/nytte-analysen så vi at bedriften ikke vil få noen direkte inntekter eller overskudd som følge av dette prosjektet. Prosjektet vil føre til en økt kostnad på ca. 250% eller 31 439,46 kr mer enn de månedlige kostnadene fra i dag. Dette er derimot et investeringsprosjekt som kommer til sikre at bedriften opererer i henhold til GDPR, samt å beskytte den mot sikkerhetstrusler. Alt dette beskytter bedriften mot potensielt større kostnader i form av tapt inntekt og omdømme.

2.3.3 Tekniske løsninger

Dette kapittelet gir en kort beskrivelse av ulike programmer som skal tas i bruk og hvilken funksjon de tjener i systemet.

2.3.3.1 Brukertjenester

Office 365 E5

Office 365 E5 inneholder alle de essensielle programmene som de ansatte komme til å ta i bruk i arbeidshverdagen. Hver bruker vil få sin egen lisens som består av programmer som Word, Excel og PowerPoint. Dette er programmer som er kjent for de aller fleste og med Teams som knutepunkt blir det enklere å dele filer og jobbe sammen på dokumenter. Lisensen inneholder også Azure Information Protection, noe som er beskrevet under.

Microsoft Teams

MS Teams er et nyttig program som følger med i Office-pakken og vil gjøre samarbeid mellom de ulike gruppene lett og brukervennlig. Microsoft Teams gir en sentralisert løsning for fildeling og fungerer sømløst med de andre Office-programmene. Videokonferanser er også en av nøkkelfunksjonene som gir en enkel måte for de ansatte å kunne kommunisere med hverandre og holde møter. Teams støtter også mange programtillegg og kan skreddersys for å passe til brukernes arbeidsflyt

OneDrive

OneDrive er en skylagringstjeneste og gjør lagring og deling av filer enkelt. Dette vil gjøre at en i teorien kan aksessere filer fra hvor som helst og fra hvilken som helst maskin (så lenge det er gitt tilgang). OneDrive gir en sentralisert løsning for lagring av data, noe som vil effektivisere alt som har med fildeling å gjøre.

WVD

Windows Virtual Desktop er en tjeneste for å kunne levere Windows 10-skrivebord til hvilken som helst enhet på en enkel og sikker måte. WVD er en del av Microsoft 365 E5 lisensen som hver bruker vil bli tildelt. Ved å «hoste» datamaskinene i skyen kan bedriften spare penger på å ikke måtte kjøpe nytt maskinvare like ofte som før, og det vil gjøre bedriften mer fleksibel.

2.3.3.2 Administrative tjenester

Microsoft Intune

Microsoft Intune er en sky-basert tjeneste og brukes til å administrere mobile enheter (MDM) og mobile applikasjoner (MAM). Dette brukes til å kontrollere hva bedriftens enheter skal brukes til og det gjelder alt fra datamaskiner til mobiltelefoner. Intune brukes sammen med Azure Active Directory (Azure AD) for å kontrollere hvem som har tilgang og hva de har tilgang til.

Microsoft Autopilot

Microsoft Autopilot er en samling av teknologier som brukes til å forhånds konfigurere enheter. Dette vil være spesielt nyttig når det kommer nye ansatte som trenger å bli integrert i systemet eller en ansatt slutter og aktuelle enheter må resettes. Autopilot kan administrere Windows 10 enheter med blant annet Microsoft Intune og Windows Update for business.

Azure Active Directory

Azure AD er en tjeneste i Azure for å administrere brukere og tilgang, noe som brukes til å logge inn de ansatte til ulike resurser. Tjenesten gjør at man kan sette opp f.eks. to-faktor-autentisering når en skal ha tak i bedriftskritiske resurser.

2.3.3.3 Sikkerhetstjenester

MS Azure App Service

App Service er en tjeneste for bygging, implementering og skalering av webapplikasjoner. Tjenesten simplifiserer overvåking av applikasjoner og gir informasjon om ressursbruk og trafikk. App Service er en del av Azure og har innebygde funksjoner for å beskytte applikasjonene dine gjennom Azure Web Application Firewall og Azure Security Center.

Windows Defender

Windows Defender er et antivirusprogram som følger med Windows 10 og Windows Server 2019 som vi kommer til å ta i bruk i dette prosjektet. Tjenesten tar i bruk maskinlæring, big-data-analyse, trussel beskyttelse og Microsoft Cloud infrastruktur for å beskytte enheter i bedriften.

Microsoft Defender for Identity

MS Defender for Identity (før kalt Azure Advanced Threat Protection) er en sky-basert sikkerhetsløsning som bruker AD til å identifisere, oppdage og undersøke trusler, kompromitterte identiteter og farlige aktiviteter mot organisasjonen.

Microsoft Defender for Office

Microsoft Defender for Office er en sikkerhetsutvidelse for Officepakken med hoved fokus på e-post. Defender for Office tilbyr avansert e-post filtrering, skanning av vedlegg og behandling av lenker. Målet er å sikre en av de største angrepsflatene i dagens bedrifter.

Identity Protection

Identity Protection brukes til å automatisere deteksjon av uvanlig aktivitet relatert til autentisering. Tjenesten brukes med Azure AD for å sikre at forsøk på innlogginger av ondsinnede aktører blir plukket opp og sendt til videre analyse. Identity Protection følger blant annet med på om det er noen som bruke anonyme IP-adresser, om det er noen som prøver å logge inn fra en uvanlig lokasjon eller om innloggingsinformasjonen har blitt lekket.

Information Protection

Azure Information Protection er en helt essensiell tjeneste dersom bedriften skal holde sensitiv informasjon så beskyttet som mulig. Denne tjenesten gjør at de ansatte trygt kan samarbeide med hverandre og andre partnere uten at det er en fare for at klassifisert informasjon havner på avveie. Denne automatiseringen vil gjøre de ansattes arbeidsdag mye enklere med tanke på personvern og informasjonssikkerhet.

2.3.4 Detaljerte løsningsbeskrivelser

2.3.4.1 Dagens system

Dagens system har en brukerbase på ca. 80 ansatte fordelt over fire kontorer. Hver ansatt har en egen Windows 10 datamaskin og er satt opp i Office 365 E3 økosystemet. I tillegg til 80 klientdatamaskiner har man ett infosystem på hvert kontor. Systemet har ingen felles lagringsløsning og det meste av filutveksling skjer over e-post.

I dag brukes Office produkter daglig av både leger og administrasjon for å utføre behandling og daglig drift. Dette medfører kommunikasjon på e-post mellom spesialister og administrasjon samt planlegging av timer i kalender. Mye av informasjonen som håndteres er ifølge GDPR klassifisert som sensitiv personinformasjon. Denne informasjonen blir ikke behandlet i henholdt til GDPR. Det finnes ingen oversikt over hvem som har aksessert informasjonen eller hvem som har tilgang. Dette må bedriften få orden i raskt for å unngå bøter fra myndighetene.

Det medfører et stort ansvar å håndtere slik informasjon, og glipper kan koste bedriften dyrt både i form av store pengebeløp og tap av omdømme.

2.3.4.2 Deloppgaver som må løses

Oppsett av Azure AD

Azure Active Directory brukes for å administrere brukere i systemet. Dette kommer vi til å bruke til å gi brukerne tilgang til Microsoft 365 og for å gi god sikkerhet i systemet.

Oppretting av brukere

VI oppretter noen brukere for å simulere et arbeidsmiljø i Azure.

Oppsett av brukertjenester

Office 365-applikasjoner som Teams, OneDrive og Word må settes opp slik at brukerne lett kan ta i bruk disse.

Oppsett WVD

Microsoft 365 inneholder blant annet Windows 10 og Windows Virtual Desktop.

Oppsett Intune og Autopilot

Intune må settes opp slik at nye datamaskiner effektivt kan konfigureres og innmeldes i domenet. Autopilot må konfigureres for effektiv utrulling av programvare og sikkerhetsinnstillinger.

Utrulling av Office 365

Alle i bedriften må få egne områder i OneDrive samt tilgang til alle Office-produkter under bedriftens lisens.

Konfigurering av sikkerhetsprodukter

Dette prosjektet omfatter mange forskjellige sikkerhetsprodukter som må konfigureres for å oppnå optimal systemsikkerhet.

- Microsoft Defender for Office
- Microsoft Defender for Identity

Konfigurere policies og varslinger i Azure Identity Protection

Identity Protection brukes til å gi varsler om uvanlig hendelser som innlogging fra ukjente IP-adresser, lekkede passord og angrep som brute force. Dette skal være med på å sikre at det kun er autoriserte brukere som får logget inn i systemet.

Konfigurering av Azure Information Protection (AIP) scanner i Azure portalen

AIP on-premise scanner gjør at AIP kan scanne nettverket og delt data av den sensitive typen. AIP kan så legge til klassifisering og beskyttelsesetiketter slik som det blir konfigurert i policyene. Azure Information Protection legger man til i Azure-portalen. Det må her konfigureres et cluster og et nettverk som skal scannes.

Installering av Azure Information Protection (AIP) unified labeling scanner

Azure Information Protection unified labeling skanner er en tjeneste som må kjøres på en Windows Server.

Utrulling av Azure Information Protection unified labeling client til klienter

Information Protection må lastes ned og legges til i Microsoft Intune for å kunne administrere og rulle det ut til klienter. Det blir så en oppgave å konfigurere og beskytte applikasjonen gjennom betinget aksess og app protection policies.

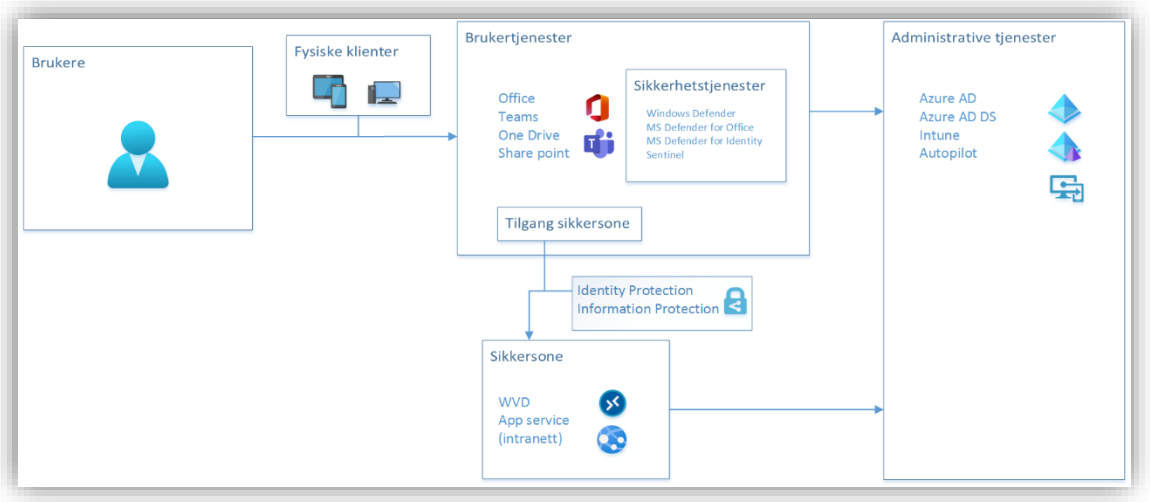
Oppsett av Azure Sentinel

Azure Sentinel samler opp data om enhetene, applikasjonene, brukerne og infrastrukturen i skyen. Tjenesten bruker denne dataen til å oppdage farer som kan finnes på systemet. Sentinel settes opp slik at den kan respondere på ulike scenarioer på en hensiktsmessig måte.

Oppsett av Azure App Service

Azure App Service er en plattform for å administrere, rulle ut, skalere og overvåke web applikasjoner. Vi kommer til å bruke dette til Knekk og Brekk sin interne web applikasjon som skal brukes av de ansatte.

2.3.4.3 Arkitekturdesign



Systemet bygger på et prinsipp om at sensitiv data skal separeres ut og bort fra brukerens fysiske datamaskin. Det skal aldri ligge sensitive opplysninger på en ansatts datamaskin. Derfor er systemet todelt, en usikker sone hvor man jobber til daglig, fysisk på sin egen datamaskin og en sikker sone som kun kan aksesseres gjennom en sikker applikasjon. Denne sikre sonen er virtuell og beskyttet med Identity Protection og Information Protection. Dette skal sikre at ansatte ikke kan kopiere informasjon eller skaffe seg tilgang uten at dette blir logget. All utveksling av denne informasjonen skjer også innenfor denne sikre sonen. Prøver de ansatte å dele informasjon, som personnummer eller journaler, utenfor sikker sone, blir det automatisk lastet opp til sikker sone og de ansatte får kun sendt en lenke til informasjonen. Dermed sikrer vi at feil oppstår hvor filer spres rundt og lagres der de ikke skal.

Brukerne vil ta i bruk sine fysiske klienter for å benytte seg av brukertjenestene. Brukertjenestene vil være alt som følger med i Office 365-pakken. På de fysiske klientene blir sikkerheten administrert av ulike tjenester gjennom Windows Defender, ATP og Sentinel. Dette økosystemet brukes primært til daglig kommunikasjon og arbeid.

Med en gang dokumenter som omhandler sensitive personopplysninger eller annen data som er underlagt spesielle GDPR krav skal behandles, må brukeren inn i sikkersone. Dette gjøres gjennom en applikasjon på brukerens fysiske datamaskin. Her må brukeren autentisere seg og får tilgang til et virtuelt miljø. Her ligger alt av konfidensiell materiell som ikke skal lagres fysisk på klienter. Man får også tilgang til intranett gjennom denne applikasjonen.

Gjennom Azure brukes Intune til å rulle ut applikasjoner til enhetene slik at en lett kan administrere mange enheter på en gang. Nye enheter blir raskt implementert gjennom tjenestene til Autopilot. Azure AD holder kontroll på alle brukerne og brukerinnlogging for sikker pålogging og autentisering.

2.3.4.4 Forutsetninger og avhengigheter

For å kunne utføre implementasjonen og fullføre prosjektet kreves det noen visse forutsetninger:

Tilgang til utviklingsmiljø

Det skal brukes Microsoft Azure som plattform for hele systemet. Det er derfor en nødvendighet at det er skaffet lisenser og tilgang til en MS Azure Tenant hvor systemet skal ligge.

Brukerlisenser

Systemet skal inneholde en komplett pakke hvor blant annet Office-pakken skal være inkludert. Det blir derfor nødvendig å skaffe tilstrekkelig med lisenser for hver bruker som skal ta i bruk denne programvaren. Microsoft 365 E5 pakken inneholder alt den vanlige Office 365-pakken inneholder, men det følger også med Windows 10 Pro og flere verktøy for økt sikkerhet.

Lisenser tilknyttet sikkerhet

Mye av hovedgrunnen til at det skal implementeres et nytt system er at det skal bli økt fokus på sikkerhet og personvern. Microsoft tilbyr en rekke tjenester som til sammen inneholder de egenskapene vi er ute etter til det nye systemet. Information Protection og Identity Protection er blant de programmene som blir nødvendige dersom en skal ha kontroll på hvem som får tilgang til hvilken informasjon.

Forankring hos ledelsen

For at prosjektet skal kunne vurderes som en suksess og ha langvarig effekt blir det helt nødvendig at hele bedriften er på samme lag. Det blir viktig å ha med seg alle de ansatte og for at det skal skje, må det hele starte hos ledelsen. Det nye systemet kan fungere helt optimalt, men dersom det ikke blir integrert godt gjennom god opplæring og videre drift, kan dette bli lite gunstig for bedriften.

2.3.4.5 Organisatoriske og personellmessige konsekvenser

Rent organisatorisk vil ikke det nye systemet ha noen direkte innvirkning på hvordan strukturen til bedriften er lagt opp. Forhåpentligvis vil det nye systemet inneholde mange elementer som de ansatte allerede er kjent med, som Office-pakken, men det vil også være nødvendig med ny opplæring på noen området - spesielt av de som skal drifte systemet. Forskjellen fra i dag og hvordan det blir etter implementeringen ligger stort sett i at selve integreringen av nye ansatte skal bli enklere og hverdagen til den enkelte ansatte skal også bli enklere.

2.3.4.6 Programvare og systemkrav

Ettersom bedriften er underlagt europeiske lover er det et krav at systemet overholder GDPR-krav. Et system med fokus på personvern er derfor nødvendig. For at det nye systemet skal kunne lykkes med dette er det viktig at det er et transparent system hvor muligheten for brukerfeil er så liten (eller ikke-eksisterende) som mulig.

For å gjøre sluttproduktet så intuitivt og velkjent som mulig for sluttbrukeren er det satt et krav i å kun bruke produkter som er utviklet av Microsoft. Dette er også for at alle de ulike tjenestene skal kunne fungere godt seg imellom og for at prosjektet skal kunne levere en komplett pakke som dekker alle behovene til Knekk og Brekk.

2.3.4.7 Krav til driftsdokumentasjon

Dokumentere endringer som oppstår

- Alle endringer som eventuelt skulle oppstå må gjennom en godkjenningsfase før disse kan iverksettes.
- Initiativtaker (oppdragsgiver eller oppdragstaker) må innkalle til møte med den andre parten. Det skal stå skriftlig hva endringen(e) er og hva resultatet av en slik endring er antatt å være.
- Oppdragstaker må gjøre en analyse av hvor nyttig en slik endring vil være. Det må vurderes om eventuell nytte er betydelig nok i forhold til hvor mye tid og ressurser som vil brukes.
- Oppdragstaker må vurdere om endringen er gjennomførbar i forhold til rammene som er satt av oppdragsgiver eller om disse også må endres. Viktig å vurdere alle ringvirkninger som kan oppstå.
- Når begge parter har blitt enige om å godkjenne en slik endring skal alle interessenter informeres om endringen(e).
- Dersom endringen(e) blir godkjent av alle parter kan oppgaven iverksettes.

Dokumentere fremgangsmåte

- Implementasjon og konfigurering av MS Azure skal dokumenteres slik at det senere kan bli brukt som et oppslagsverk.
- Systemstrukturen skal dokumenters i form av oversiktlige figurere og forklarende tekst.

2.3.4.8 Regler for pilot – hva må til for å gå videre

Etter at oppsettet av systemet er gjort skal det tas i bruk en testgruppe som består av en liten gruppe av de ansatte som får prøve ut systemet før full implementering. Hensikten er å finne eventuelle tekniske feil som gjør at deler av eller hele systemet ikke fungerer som det skal. Piloten er også med på å kartlegge informasjonshull hos de ansatte slik at en lettere kan sette sammen en opplæringsplan til når den fulle implementering skal foregå.

Regler for pilotkjøringen:

- Piloten vil foregå over et tidsrom på ca. 1 måned
- Piloten skal gjennomføres av en begrenset del av den aktuelle brukergruppen. Viktig at alle avdelinger er representert så godt som mulig i denne gruppen.
- Før testingen vil det gis en rask gjennomføring av systemet og hvilke funksjoner som en vil at sluttbruker skal teste og komme med tilbakemelding på
- Testbrukere oppfordres til å «leke» med systemet og prøve å finne feil som prosjektgruppen ikke klarer.
- Alle feil som oppdages skal dokumenteres
- Områder eller funksjoner hvor testbruker trengte mer informasjon for å ta i bruk systemet slik som var intensjonen må dokumenteres.

2.3.4.9 Overordnede godkjenningskriterier for pilot

Nivå	Kategori	Beskrivelse
1	Kritisk	Dette er feil som fører til de mest sentrale delene av systemet går ned. Hvis slike feil inntreffer, vil systemet være ubrukelig, og de ansatte vil ikke få utført arbeidet sitt.
2	Alvorlig	Feil i denne kategorien fører til at viktige funksjoner/deler av systemet går ned. Systemet vil fortsatt være oppe, men noen av de viktige funksjonene som for eksempel fildeling vil ikke være tilgjengelig.
3	Mindre alvorlig	Feil i nivå 3 vil ikke være like alvorlige som de i kategori 2 og 1, men likevel vil føre til nedsatt funksjonalitet. De ansatte vil likevel kunne utføre jobben sin i denne kategorien.
4	Andre feil	Feil i nivå 4 er småfeil som ikke vil påvirke arbeidet til brukeren, men som kan oppleves som "irriterende".

2.3.4.10 Ved ikke-godkjent test, hva skjer da

Dersom testen ikke godkjennes av Trondheim Knekk og Brekk, vil dette først og fremst gå ut over dato for prosjektslutt og full utrulling. Det vil da diskuteres en ny dato for utrulling. Dersom det er mindre kritiske feil, som ikke vil gå ut over sikkerhet, personvern eller bruk, så kan det vurderes å gjennomføre en delvis implementering.

Dersom utrulling blir utsatt, men testen heller ikke godkjennes på andre forsøk så må nye rammebetingelser og vilkår avtales. Eventuelle nye kostnader må evalueres og det må bestemmes hvem som skal ha ansvaret for disse kostnadene.

2.3.4.11 Deltagere

Deltakerne i prosjektet er Kevin Nordnes og Matias Skjetne som skal stå for implementeringen av systemet. Marias Andre Langseth-Nilsen vil sammen med konsulenter fra Atea stå for veiledning og hjelp til den tekniske delen av prosjektet. Stein Meisingseth er veileder fra NTNU og vil også være med for å se til prosjektets fremgang og komme med tilbakemeldinger underveis. Ledelsen i Trondheim Knekk og Brekk vil ha et overordnet ansvar for prosjektet i form av beslutninger og krav som settes.

2.3.4.12 Oppdatert Project-dokument

(Se vedlegg)

3 DRIFTSRAPPORT

3.1 Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
4/mars/2021	0.1	Første utkast	Kevin Nordnes & Matias Skjetne
29/april/2021	0.2	Andre utkast	Kevin Nordnes & Matias Skjetne
6/mai/2021	1.0	Endelig utkast	Kevin Nordnes & Matias Skjetne

3.2 Innledning

Denne rapporten er en grundig gjennomgang av hvordan systemet, som er bestilt av Trondheim Knekk og Brekk AS, implementeres. Implementeringen tar utgangspunkt i designrapporten, men kan avvike på visse punkter – dette beskrives i endringsmelding(er).

3.2.1 Dokumentets hensikt

Driftsrapporten er en guide til implementeringen som ble designet i *designrapporten*. Denne rapporten viser steg for steg hvordan systemet settes opp, men kan også brukes som en referanse til senere drift av systemet. Dokumentet gir innblikk i hvorfor de ulike valgene underveis er tatt og hver tjeneste eller teknologi beskrives. Dette er for å gi innsikt i hvorfor tjenesten eller teknologien er tatt med og hvilken rolle den har i det endelige systemet.

3.2.2 Avgrensninger

Implementeringen i dette dokumentet er en fullstendig forklaring til det sluttproduktet som ble beskrevet i designrapporten. Dokumentet beskriver selve implementeringen, men tar ikke for seg utvikling av applikasjonen som blir også er en del av oppgaven. Denne rapporten antar at leseren/brukeren har en fungerende applikasjon som kan distribueres og viser dermed kun selve utrullingen og sikkerhet rundt dette.

3.2.3 Definisjoner og forkortelser

AIP – Azure Information Protection
AD – Active Directory
AAD – Azure Active Directory
BYOD – Bring Your Own Device
M365 – Microsoft 365
MAM – Mobile Application Management
MDM – Mobile Device Management
MFA – Multi-Factor Autentication
OOBE – Out-Of-Box-Experience
VSC – Visual Studio Code

3.2.4 Oversikt over innholdet

I punkt 3.3 Oppsett av Azure Active Directory beskrives hvordan en setter på Azure AD, hvordan en legger til brukere, grupper og SharePoint sites. I punkt 3.4 blir det vist hvordan en setter opp M365 admin center og i punkt 3.4.1 blir det vist hvordan en gir ut Office lisenser. I punkt 3.5 forklares hvordan nye enheter skal automatisk bli lagt inn i grupper og satt opp klart til bruk. Punkt 3.6 viser hvordan enheter blir rullet inn i Intune, får Office-pakken og blir sjekket for «Compliance». Under punkt 3.7 er det en gjennomgang av Information Protection – hvordan sette opp sensitivity lables, label policyer og hvordan AIP Unified Labeling Client blir rullet ut til klienter. Punkt 3.8 har med Azure app service å gjøre og inneholder en gjennomgang av hvordan en ruller ut en applikasjon og setter opp konfigurering gjennom Azure AD. Punkt 3.9 handler om sikkerhet og går igjennom en rekke tjenester og teknologier som alt har med sikkerhet å gjøre. Dette er blant annet om innlogging, kryptering, overvåking, ulike policyer og oppsett av Microsoft Defender. Under punkt 3.11 ligger alle referanser som er brukt.

3.3 Azure Active Directory

Azure AD (AAD) er en skyløsning for å holde styr på identiteter og aksessrettigheter i en organisasjon. AAD brukes for å lage brukere til ansatte og å styre hvilke tjenester og ressurser hver bruker har tilgang til. En kan dele ut rettigheter på individuell basis eller basert på grupper.

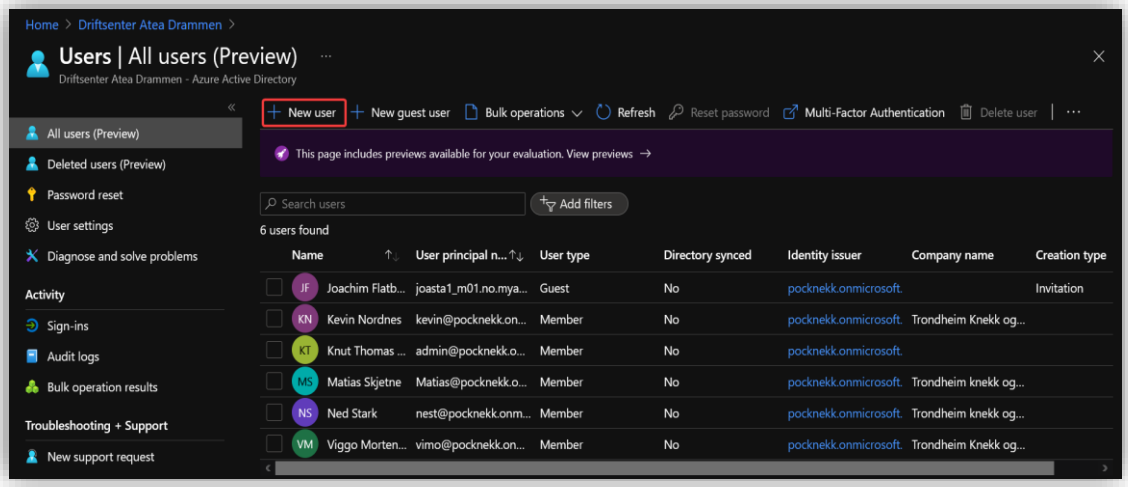
Azure AD skiller seg fra Microsofts tradisjonelle Active Directory, i at det er en ren skyløsning. Azure AD er rettet mot Software as a Service (SaaS) applikasjoner i skyen og støtter moderne autentisering som SAML og OAuth. Active Directory derimot retter seg mot on-premise applikasjoner og autentiserer med LDAP, Kerberos og NTLM.

Brukere og grupper er helt essensielt i denne implementasjonen og kommer til å være nødvendig for at tjenestene skal ha noen innvirkning på systemet.

3.3.1 Oppretting av brukere

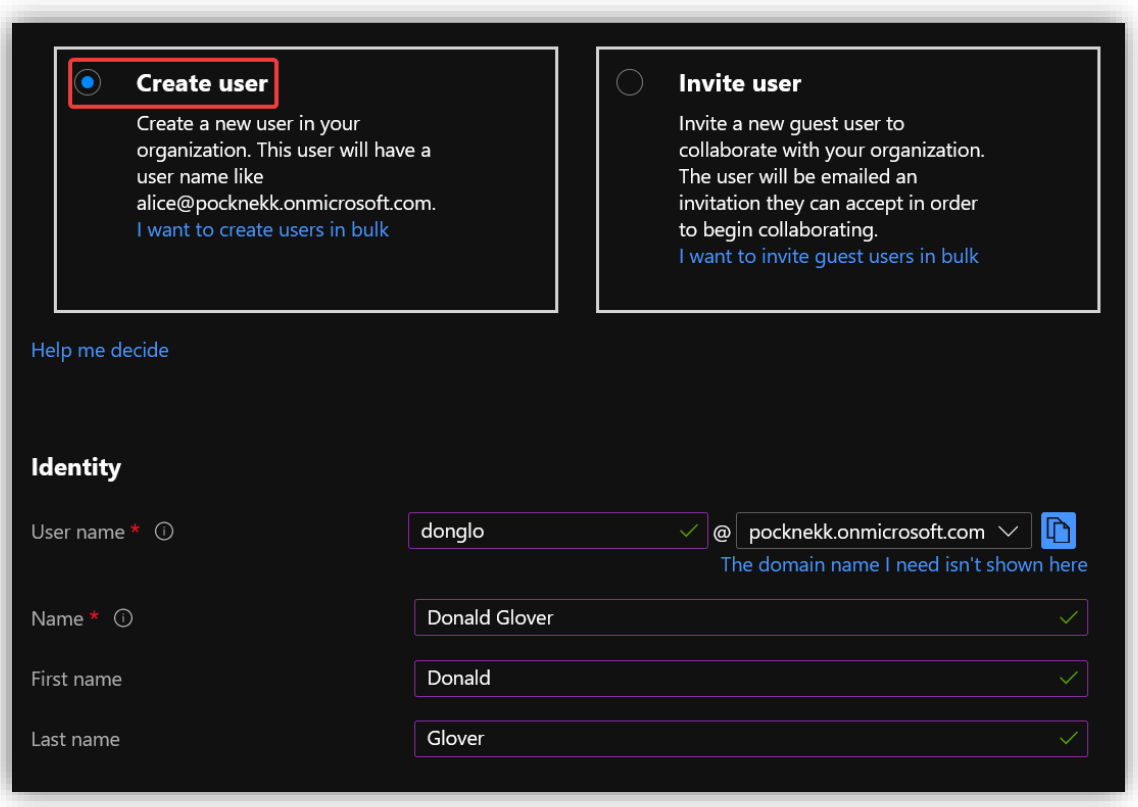
Når det kommer nye ansatte som skal ha maskinene sine registrert for bruk eller de skal ha tilgang til ressurser gjennom Microsoft, må de først legges til i Azure AD. Denne kontoen kommer til å bli brukt til å logge inn på alle skytjeneste, gi en maskin en eier, logge inn på intranettet og tildele rettigheter og lisenser. De neste stegene viser hvordan en setter opp en bruker.

I **Azure AD**[1], under **Azure Active Directory > Users > All users** velg **New user.**

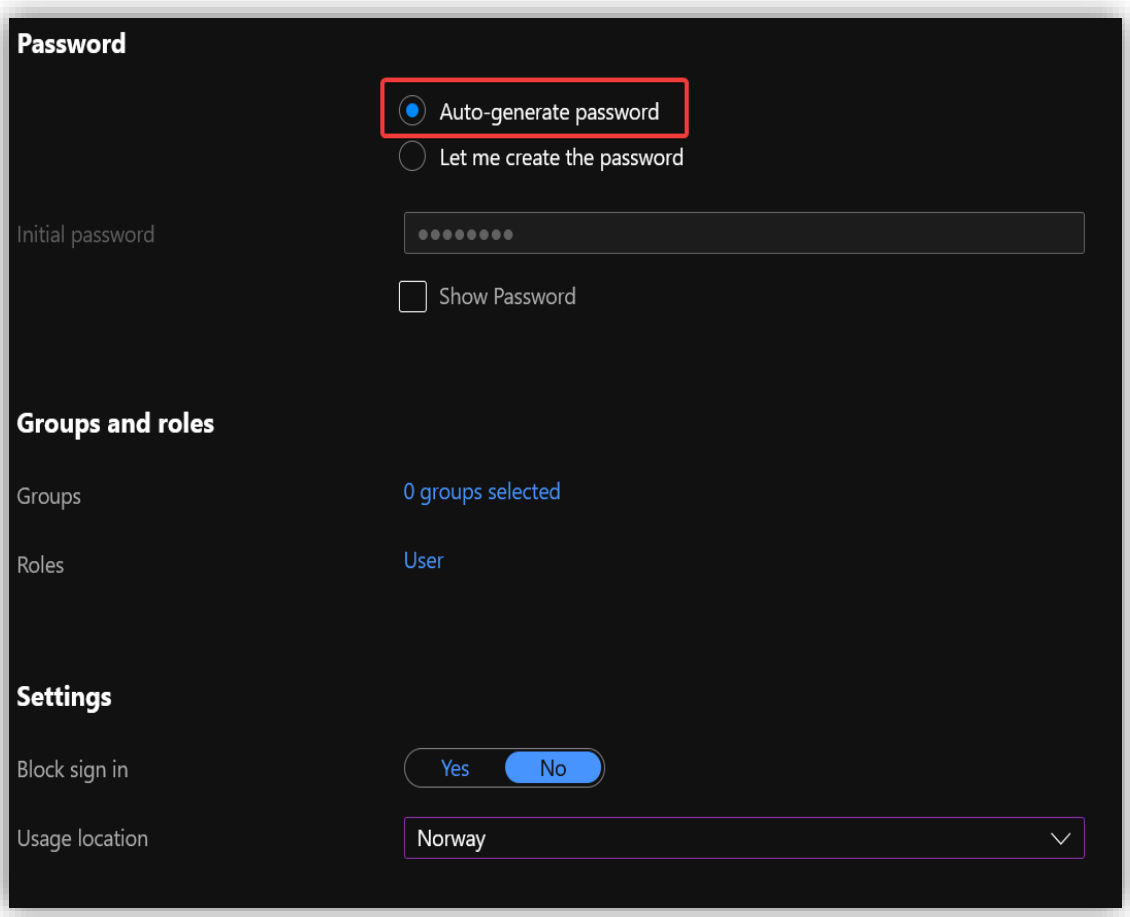


[1] https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

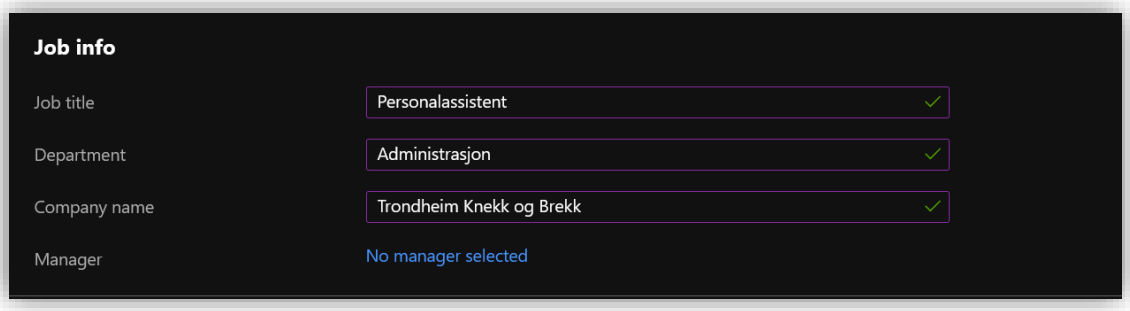
Velg **Create user** og fyll inn personalia.



Velg **Auto-generate password** og sett **Usage location** til **Norway.** Husk å kopiere passordet og distribuer det til den aktuelle brukeren.



Fyll inn informasjonen til brukeren.

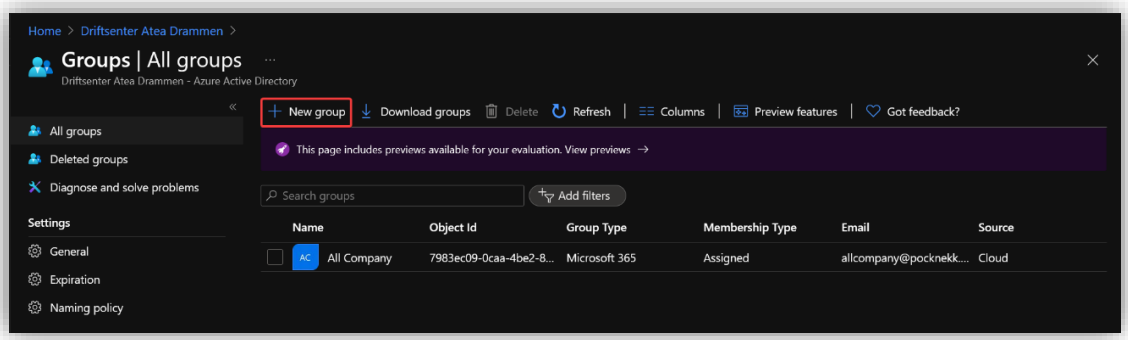


Trykk **Create** for å opprette brukeren.

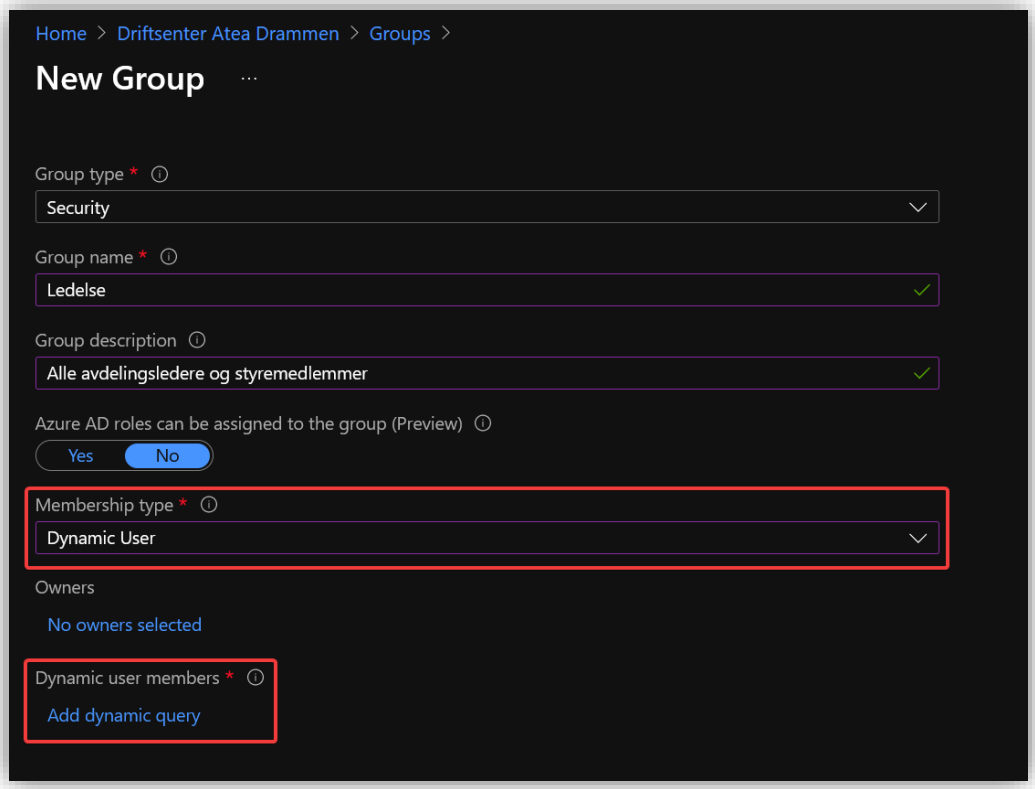
3.3.2 Oppretting av grupper

Grupper brukes for å gi flere brukere samme rettigheter til ulike ressurser i Azure. Gruppene bør settes opp slik at medlemmene meldes inn så automatisk som mulig, dette for å spare mye tid når det etter hvert blir mange ansatte. Lag grupper etter hva som gir mening i organisasjonen. For eksempel kan det være lurt å gi ulike avdelinger i bedriften egne sikkerhetspolicyer og rettigheter til ressurser.

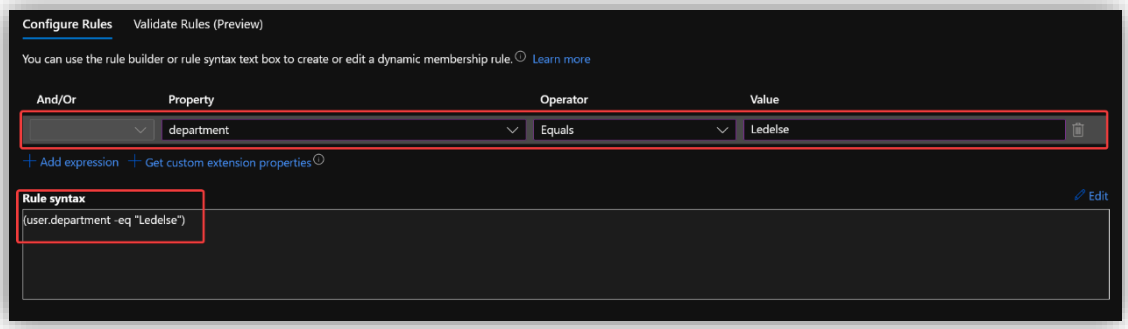
Under **Groups > All groups,** trykk på **New group**



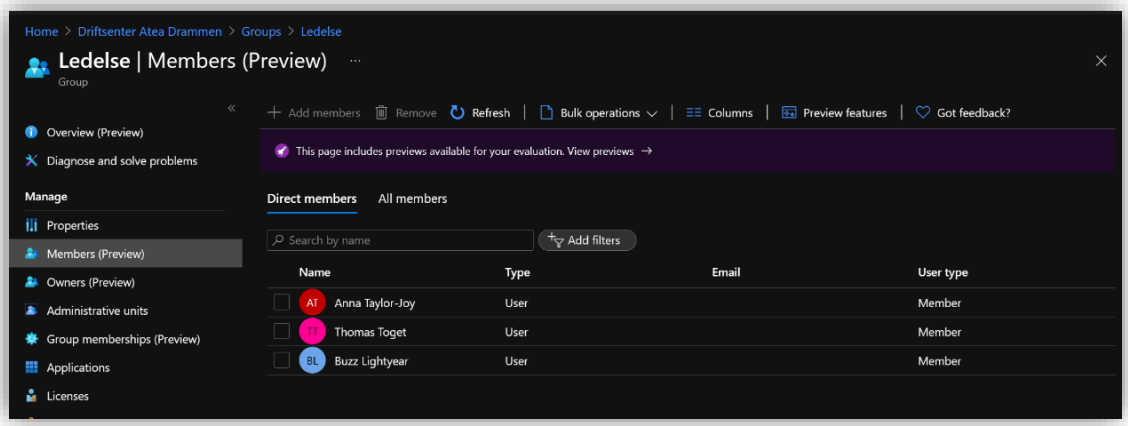
Lag en **Security group** og gi den et passende navn. **Membership type** satt til **Dynamic User** legger automatisk til brukere basert på en spørring. Trykk på **Add dynamic query** for å legge til en spørring.



Spørringen under sjekker om brukeren har «avdeling» feltet satt til «Ledelse». Dersom det er tilfellet, vil brukeren bli lagt til i Ledelses-gruppen.



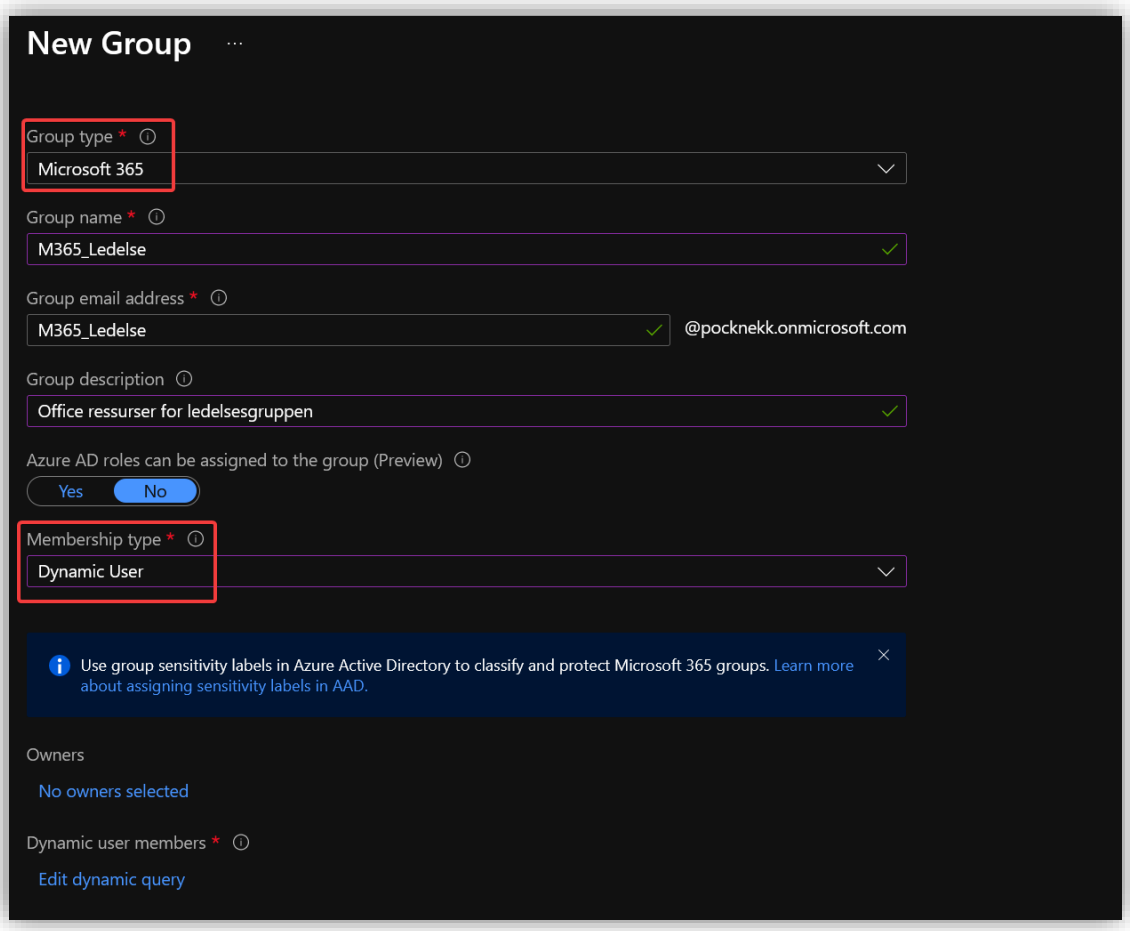
Etter noen minutter blir de aktuelle brukerne lagt til i gruppen “Ledelse”.



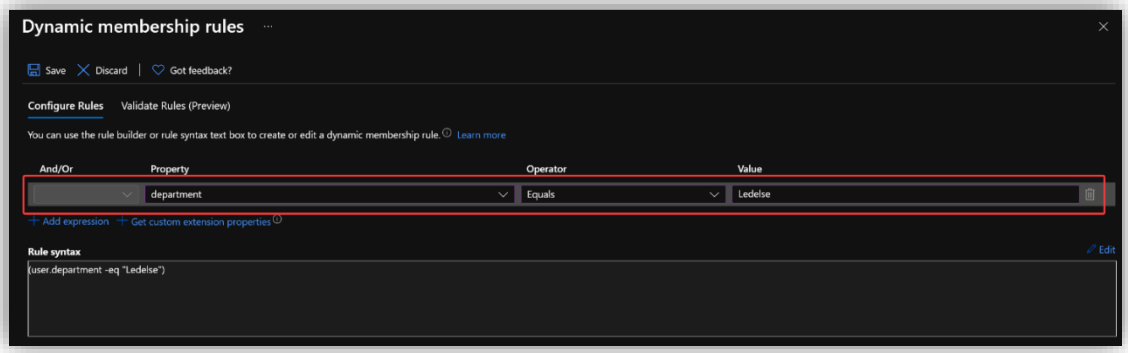
3.3.3 Sharepoint sites via Microsoft 365 grupper

SharePoint lar brukere enkelt dele informasjon samt samarbeide om arbeidsoppgaver. Hver avdeling kan ha sin egen Site hvor de enkelt kan dele informasjon og holde kontakten, med Teams integrasjon blir det enda enklere å holde møter digitalt og holde kontakten via chat.

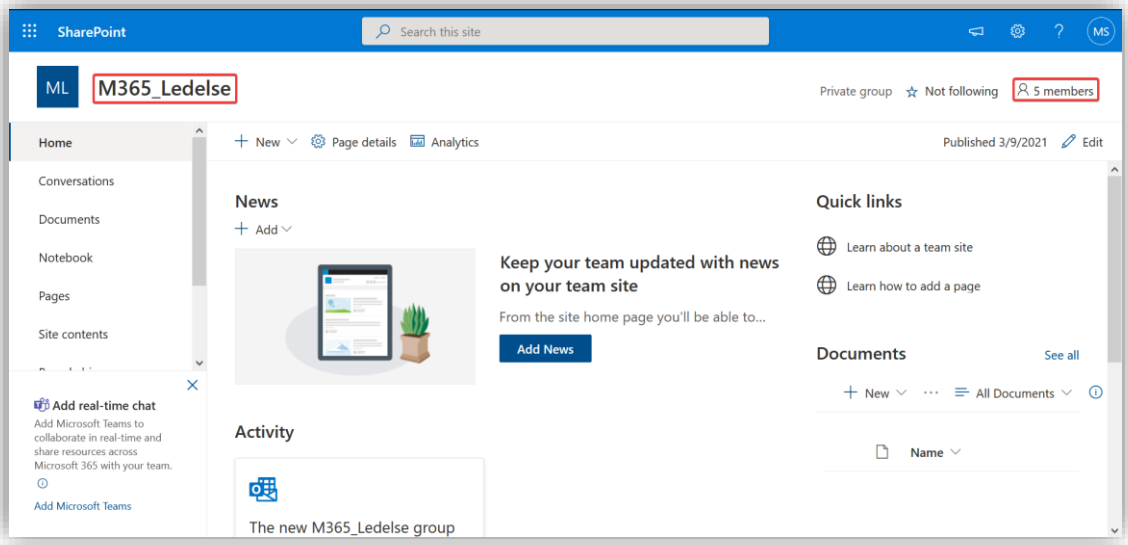
I Azure AD, opprett en **Microsoft 365** gruppe og gi den navn og beskrivelse. Velg **Dynamic user** som **Membership type**.



Lag en dynamisk regel som i dette tilfellet legger til alle i ledelsen.



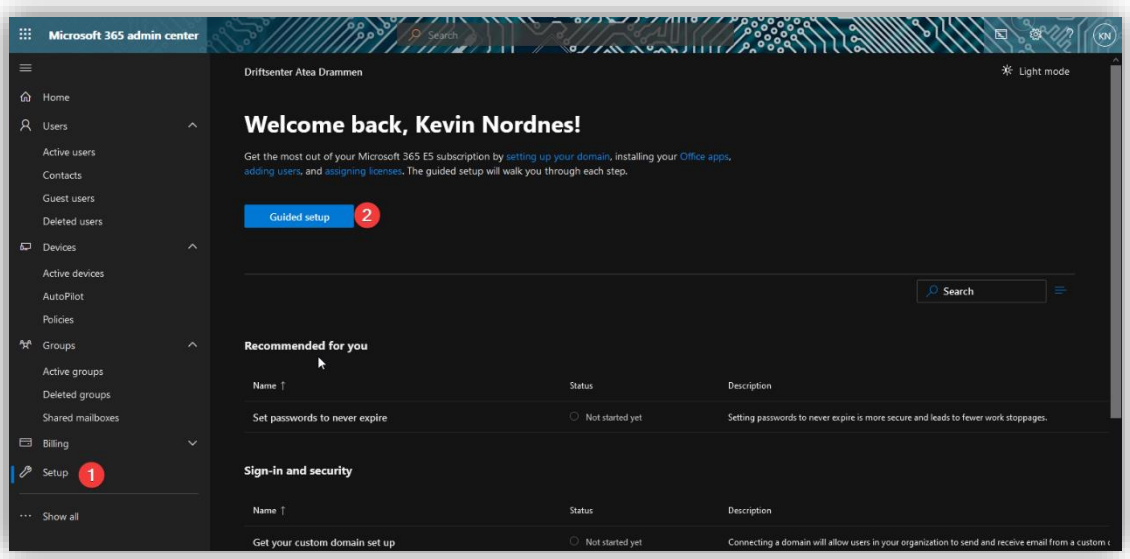
Slik ser ledelsen sin «site» ut. Legg merke til at den har 5 medlemer, alle fra Microsoft 365-gruppen.



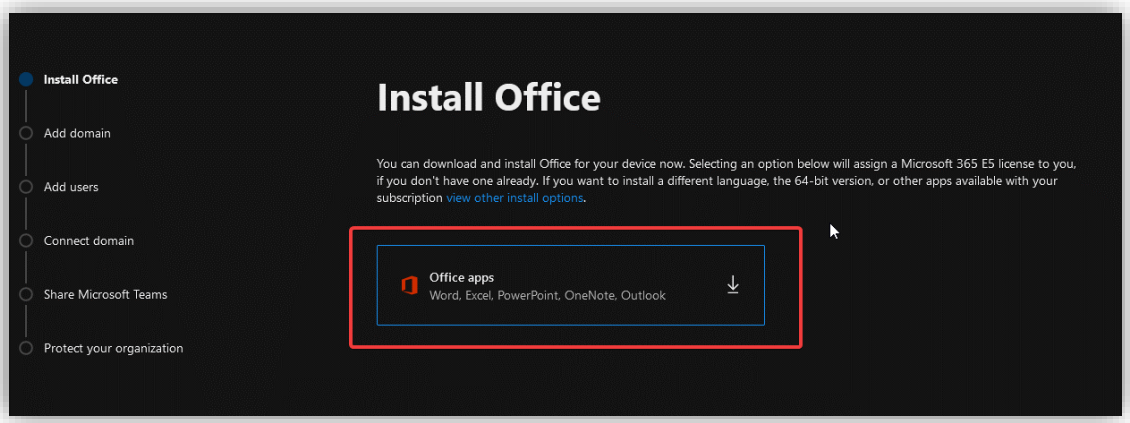
3.4 Microsoft 365 admin center

Microsoft 365 admin center[2] brukes for å administrere Microsoft 365 sine tjenester. Gjennom denne portalen kan en sette opp det meste av tjenestene Microsoft 365 tilbyr og konfigurere sikkerhetsinnstillinger for Exchange, SharePoint og Teams. En for også oversikt over fakturaer og tildeling av lisenser. En får også tilgang til **Security og Compliance** portalene hvor en kan konfigurere *Information Portection* og *Compliance policyer*, samt få rapporter over systemets helsetilstand.

Start med å gjennomgå det guidede oppsettet. Gå til **Setup** og trykk på **Guided setup.**

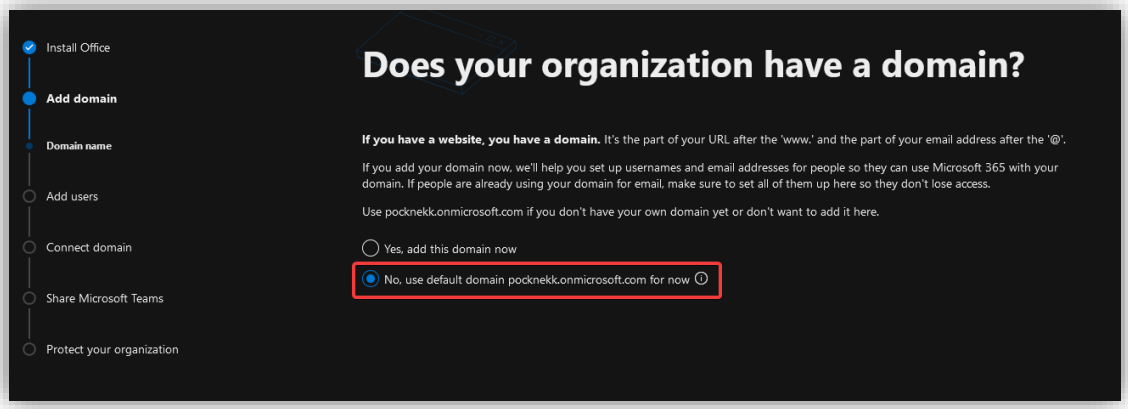


Dersom en ønsker kan en installere Office på sin egen enhet umiddelbart. Da vil en Microsoft 365 E5 lisens bli tildelt din bruker dersom du ikke allerede har en.

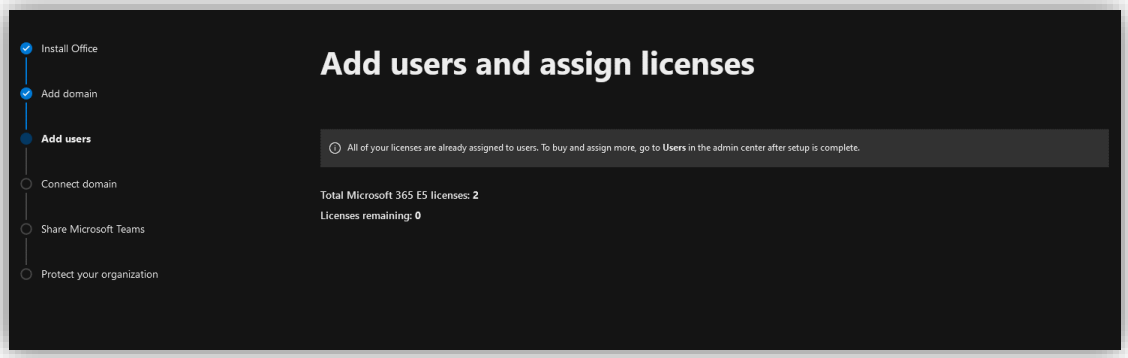


[2] https://admin.microsoft.com/#/homepage

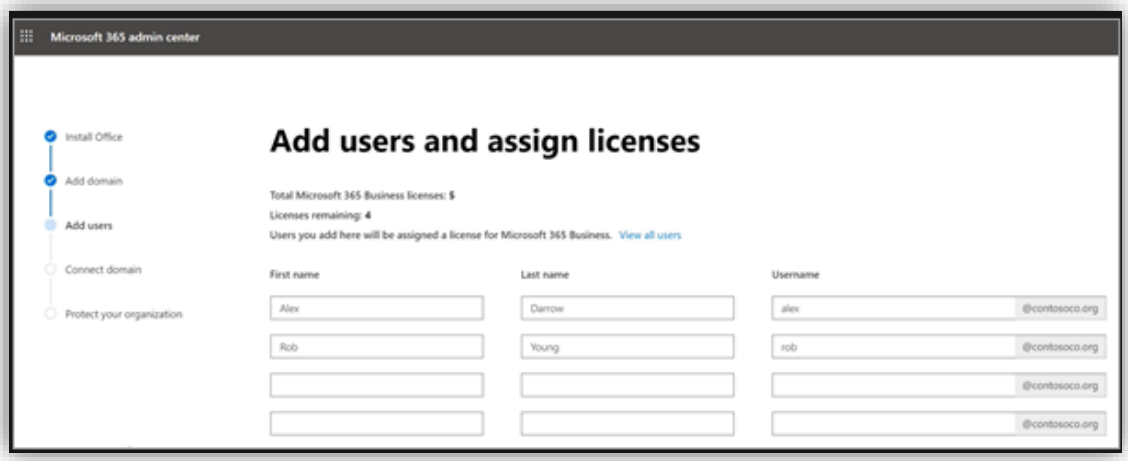
I et reelt miljø ville en her lagt til domenet til bedriften. I dette tilfellet brukes domenet som er gitt av Microsoft (pocknekk.onmicrosoft.com).



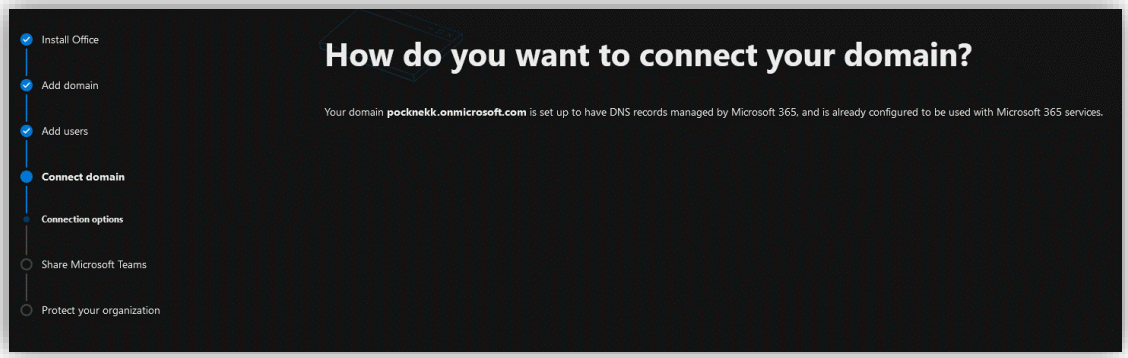
Under **Add users** kan en legge til brukere og tildele lisenser. Siden alle lisensene allerede er utdelt vil skjermen se slik ut:



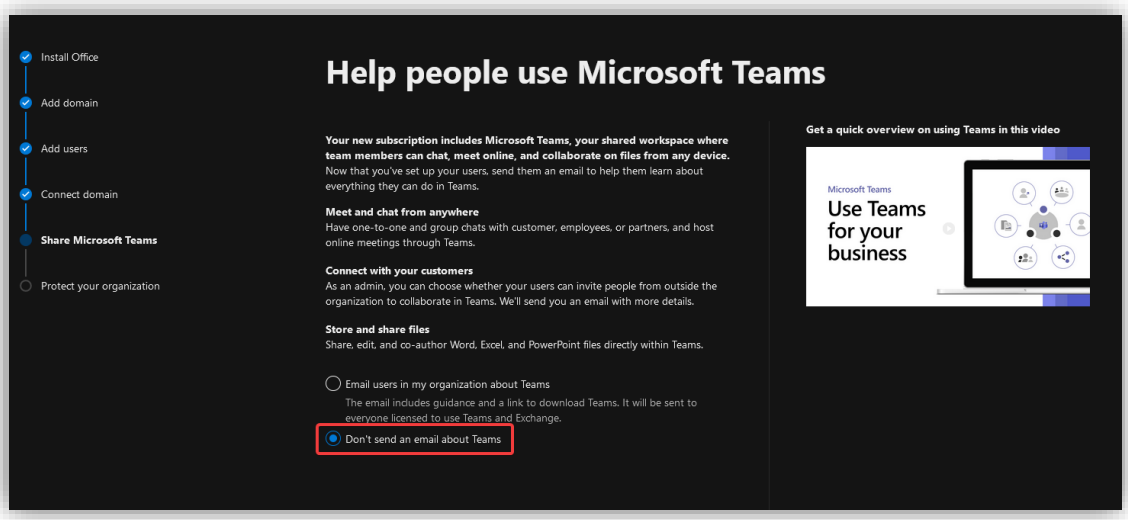
Sånn ser det ut dersom en har flere lisenser:



Under **Connect domain** kan en oppdatere DNS registeret. I dette tilfelle kommer det ikke opp ettersom det brukes et «.onmicrosoft»-domene. Dersom en ikke bruker et slikt domene vil det komme opp en guide som viser hvordan en skal oppdatere NS-postene.

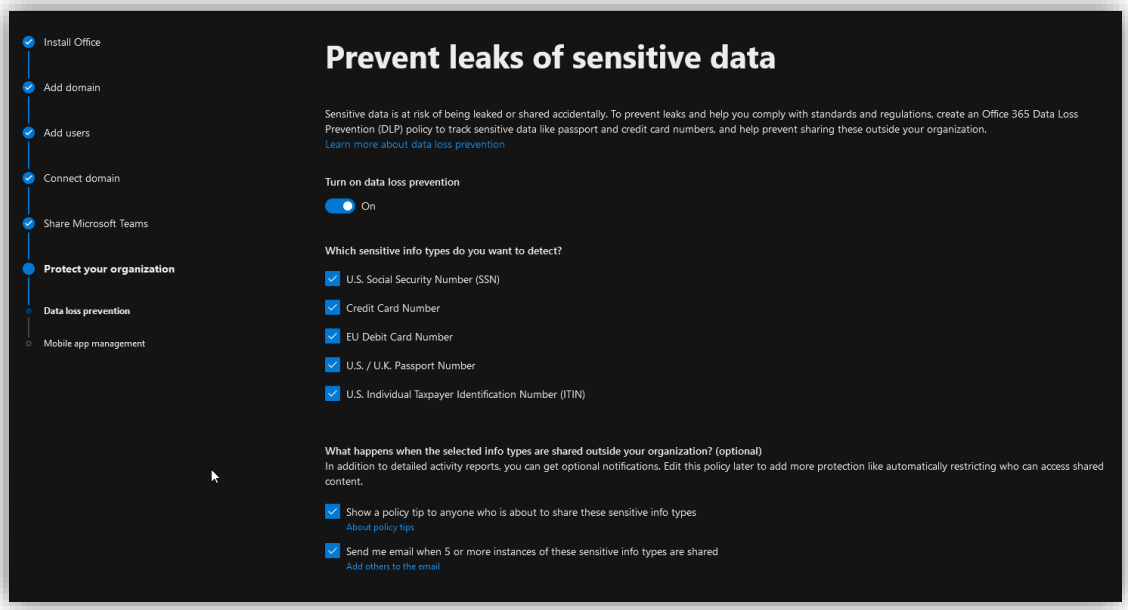


Under **Share Microsoft Teams** kan en velge å sende ut en e-post til alle brukeren med informasjon om Microsoft Teams. Dette kan være lurt dersom organisasjonen ikke har tatt i bruk Teams før. I dette tilfelle velges det å ikke sende ut noe e-post.

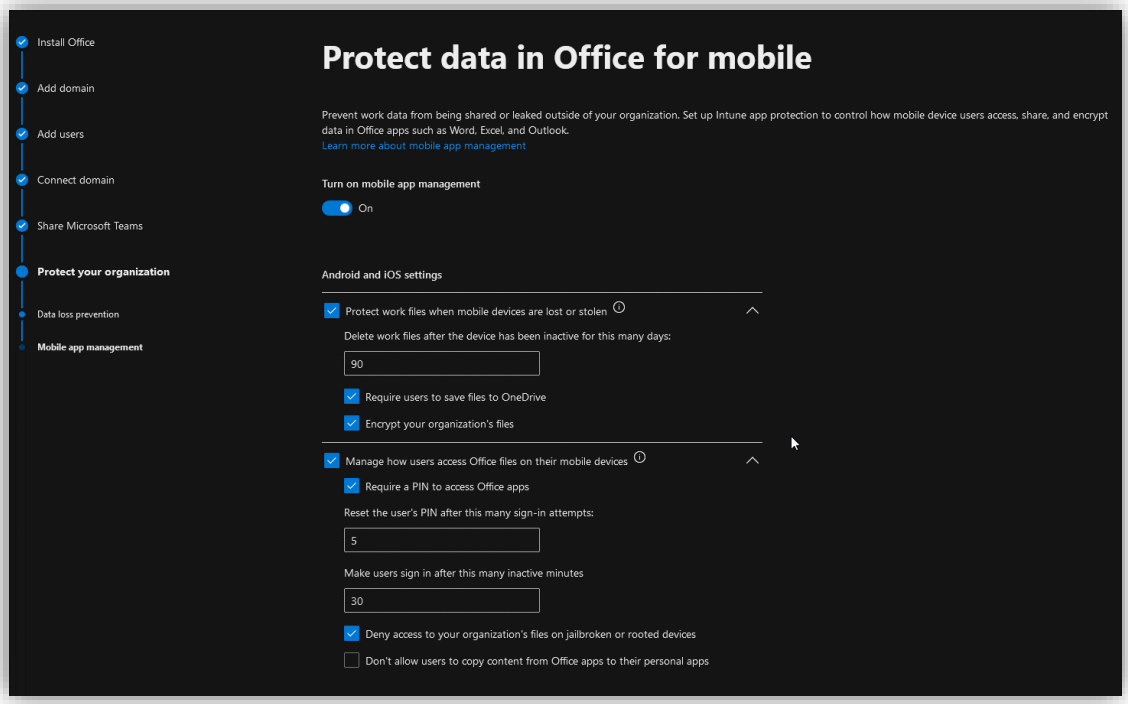


Under **Protect your organization > Data loss prevention** er det valgt en del standard regler for hvordan **Office 365 Data Loss Prevention** prøver å beskytte sensitiv informasjon slik at det ikke havner utenfor organisasjonen.

La alle valgene stå slik de er.



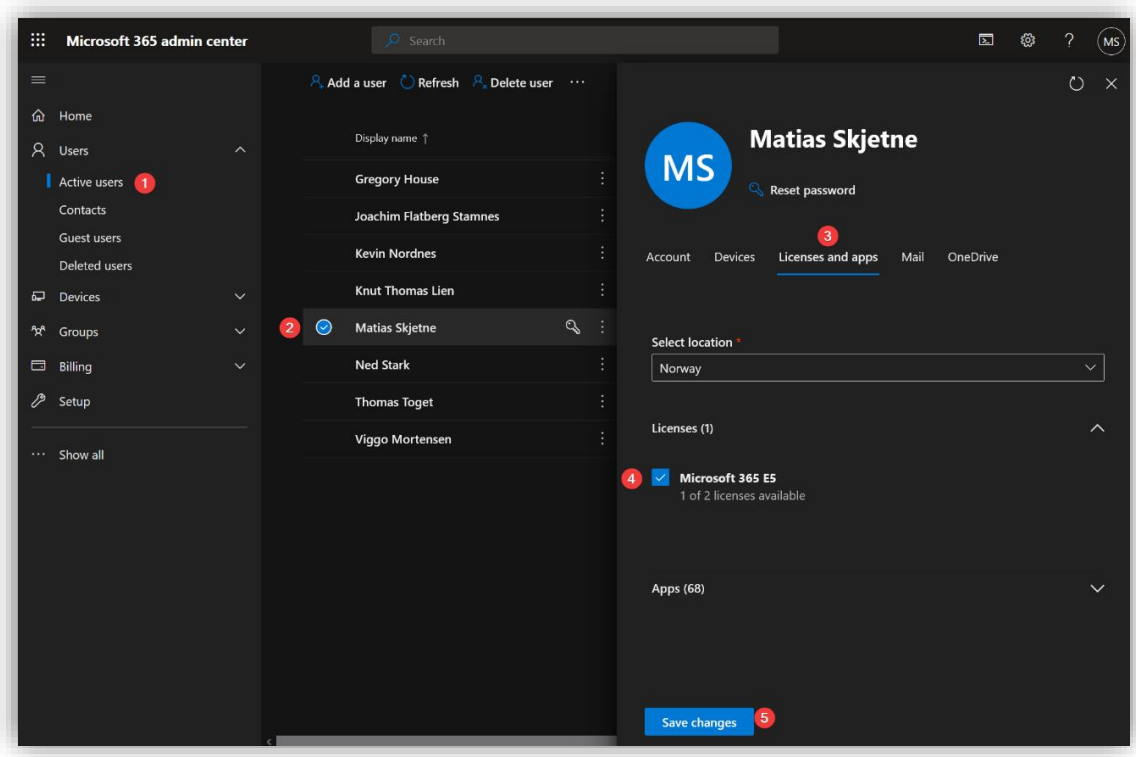
Under **Protect your organization > Mobile app management** kan en sette opp sikkerhet mot tap av data på mobile enheter. La alle valgene stå slik de er.



3.4.1 Utdeling av Office lisenser

Office lisenser brukes til å gå brukerne tilgang til Microsoft produkter som Teams, Word, Excel, SharePoint, samt sikkerhetstjenester som Information Protection som er unikt for E5-lisensen.

For å tildele en lisens til en bruker gå inn på **Microsoft 365 admin center**[3] **> Users > Active users**. Velg brukeren en ønsker å tildele en lisens, gå inn under **Licenses and apps** og huk av for lisensen som en ønsker å tildele – i dette tilfellet **Microsoft 365 E5**.



Trykk **Save Changes**. Brukeren er nå tildelt en Office-lisens.

[3] https://admin.microsoft.com/#/homepage

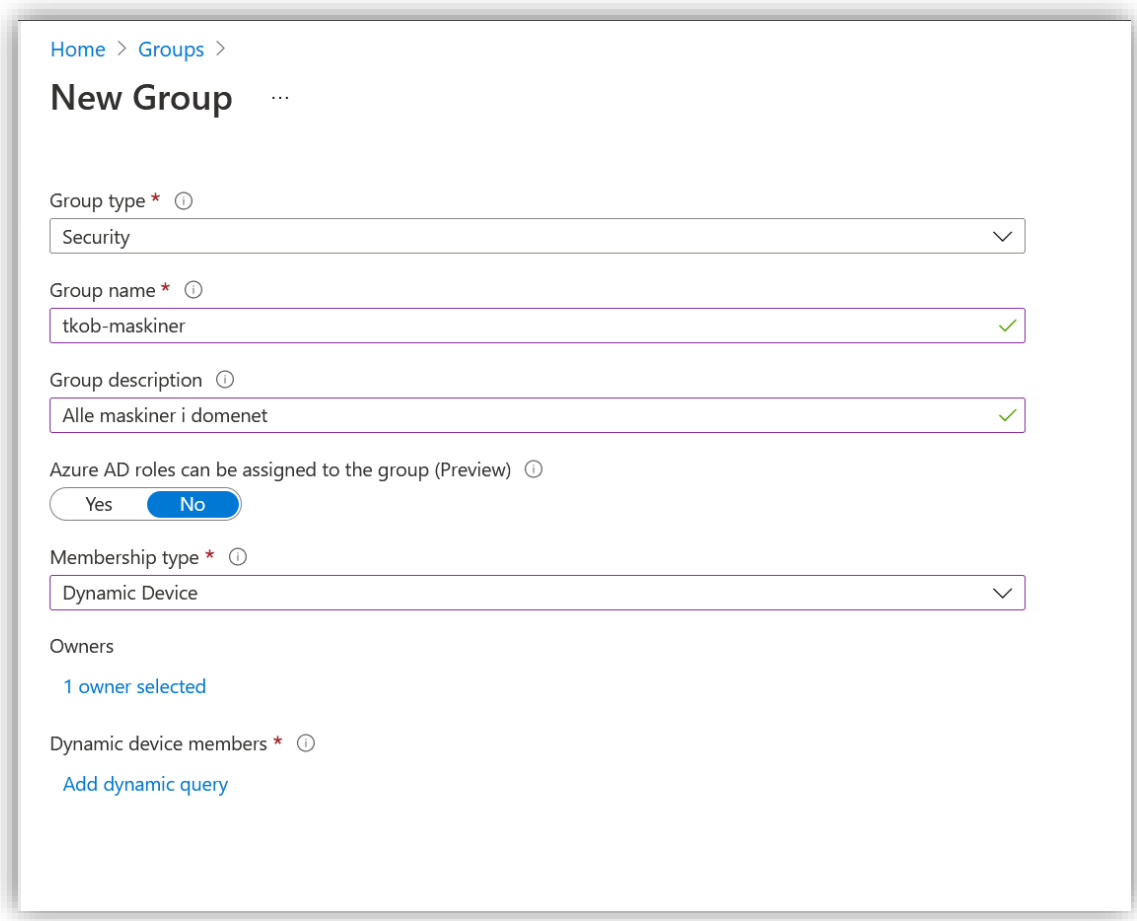
3.5 Autopilot

Autopilot er en tjeneste som setter opp og pre-konfigurerer (onboarder) maskiner for bruk i bedriften. Når maskinen skrus på for første gang tar Autopilot av seg installasjonen av Windows 10 og melder den inn i bedriftens domene. Dette gjør innkjøp og oppsett av nye maskiner mye enklere.

3.5.1 Lag en security group

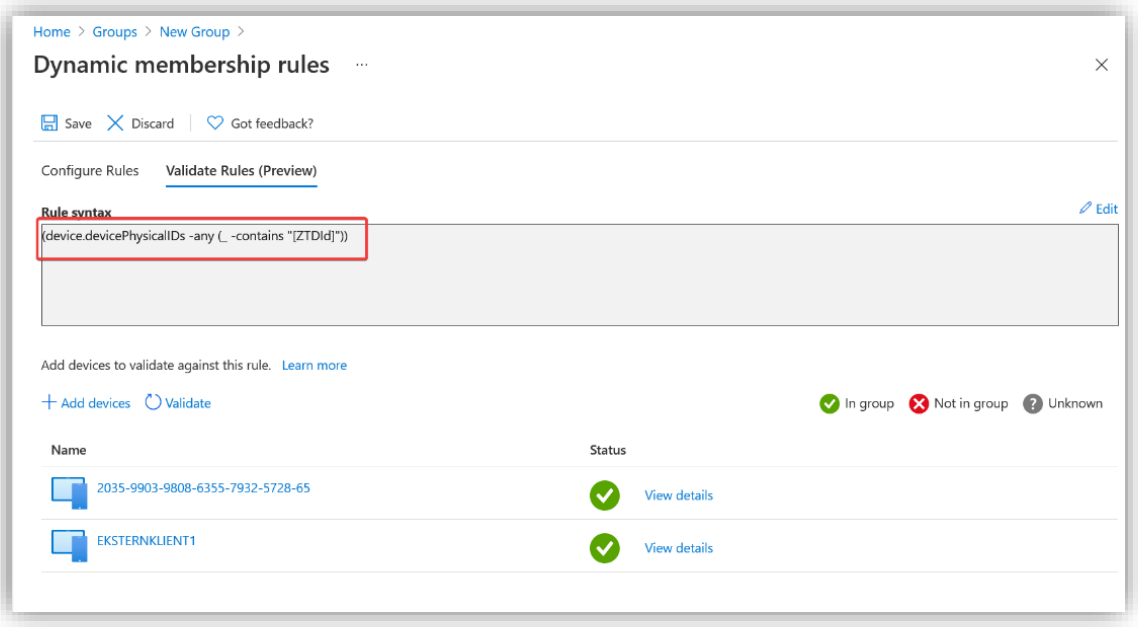
Inne i **Microsoft Endpoint Manager admin center**[4] (MEMac) kan en lage en ny **security group** som skal inneholde alle maskinene en ønsker å enrolle. I et ekte scenario vil man dele inn maskinene etter avdeling og funksjon slik at man senere kan tanke dem forskjellig etter behov, i dette eksempelet gjøres det enkelt og det lages én gruppe for alle.

Under **Groups > All groups** trykk på **New group.** Velg å lage en **Security group**, gi den et passende navn og beskrivelse.



[4] https://endpoint.microsoft.com/?ref=AdminCenter#home

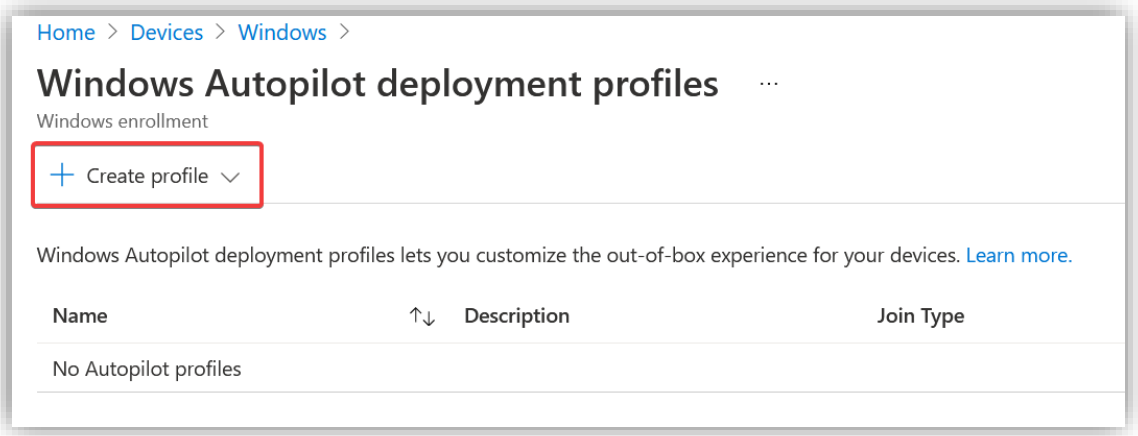
Sett gruppen til **Dynamic Device** og lag følgende medlemsregel (membership rule). Denne regelen legger til alle Autopilot enheter. På bildet under testes regelen på et par enheter som er i Autopilot.



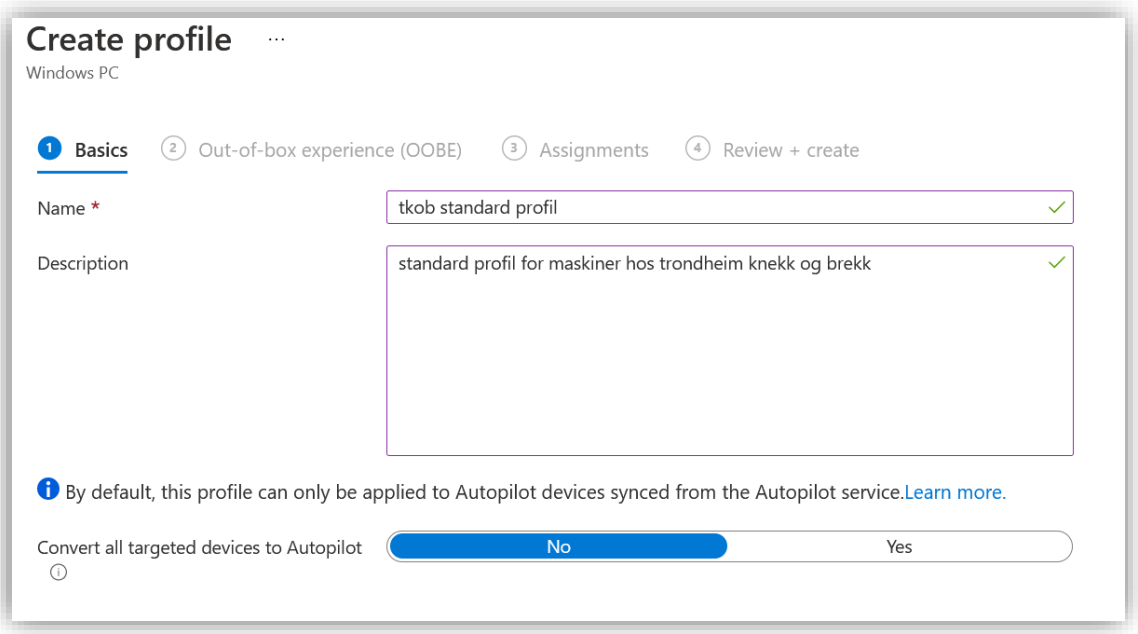
3.5.2 Lag en deployment profile

Neste steg er å lage en **Windows Autopilot deployment profile**. Denne profilen bestemmer hvordan maskinen blir satt opp ved førstegangs installasjon. Den gjør ting som å sette region og melde maskinen inn i domenet.

Gå inn **Devices > Windows.** Under **Create profile** velg **Windows PC.**

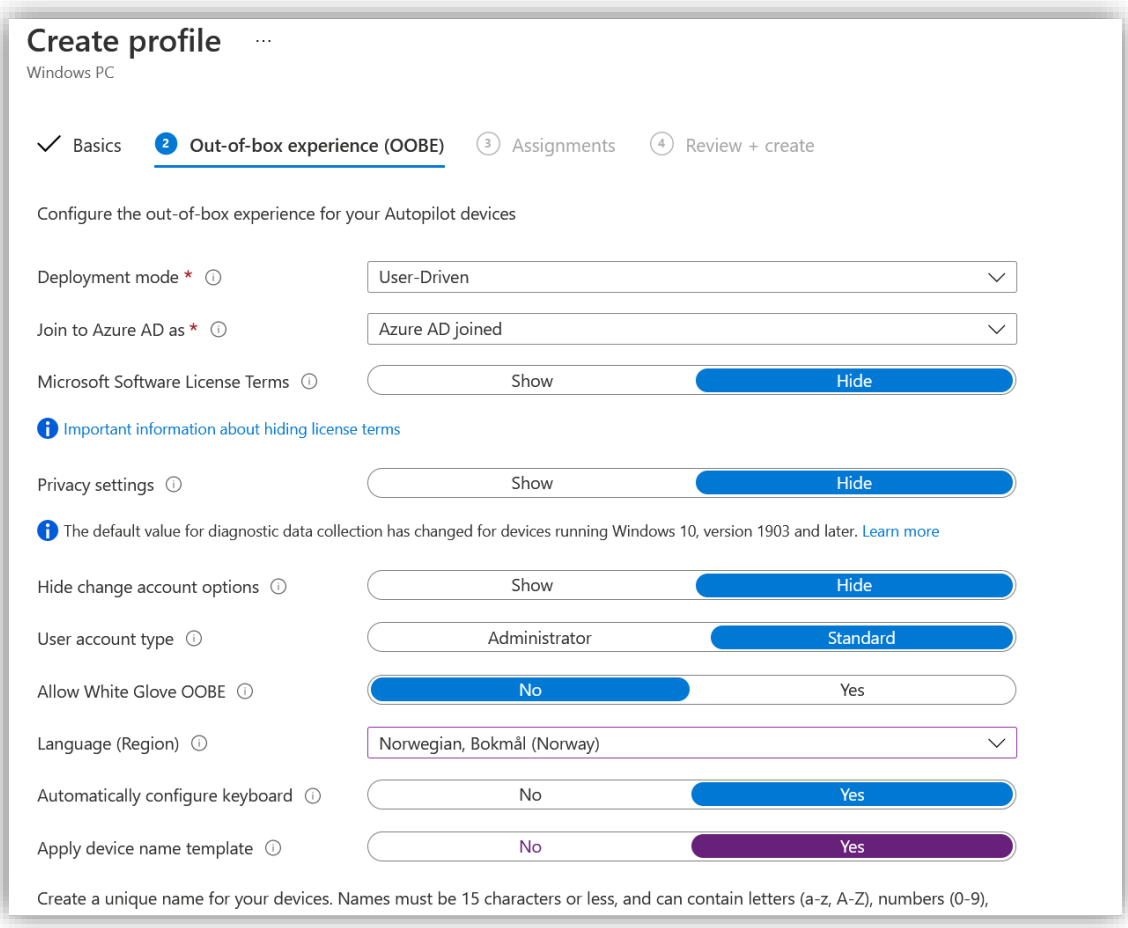


Gi profilen et passende navn og en beskrivelse. Velg å ikke konvertere alle enheter til Autopilot ettersom det ikke finnes andre enheter som ikke er Autopilot.

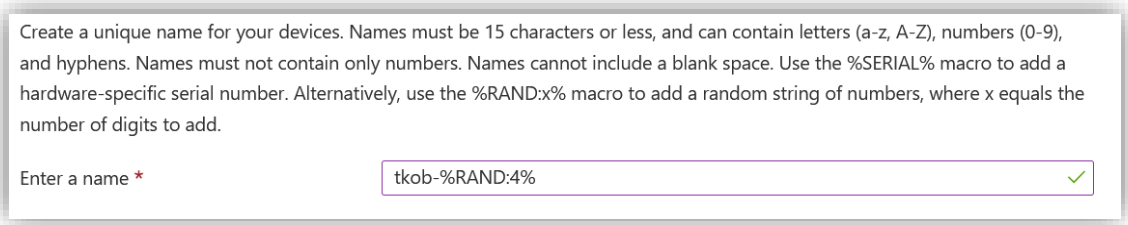


Videre må en velge innstillinger knyttet til OOBE. Mye av dette er standard, men noe er verdt å merke seg.

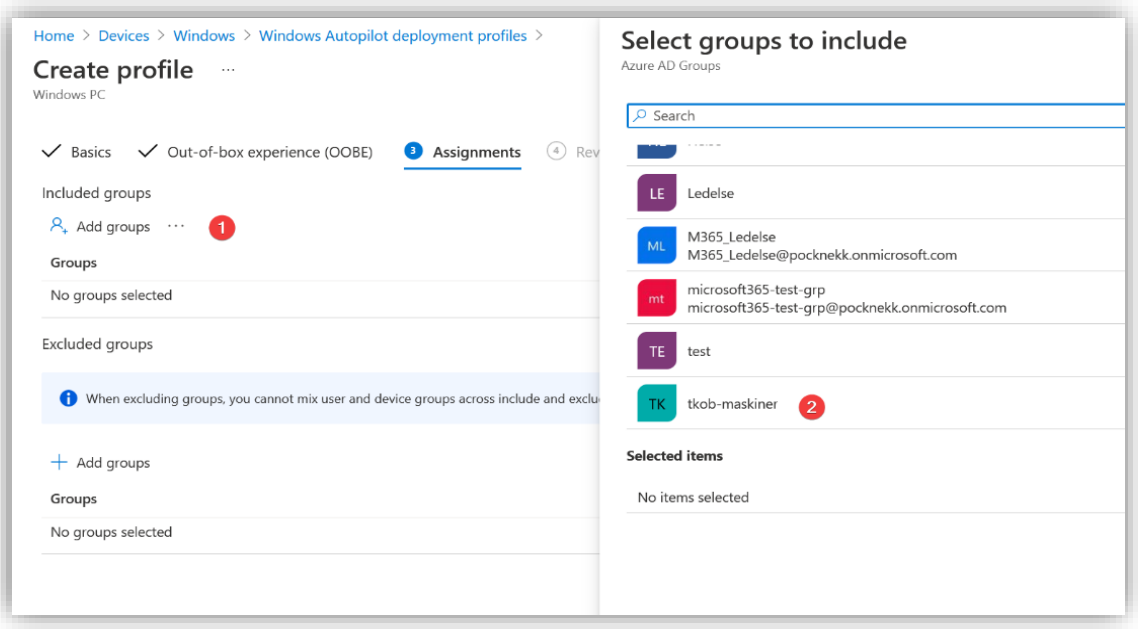
- Siden det er en full skyløsning, kan en kjøre **Azure AD joined**. Hadde det vært en hybridløsning med on-prem AD DC må en velge **Hybrid Azure AD joined**.
- **User Account** settes som Standard.



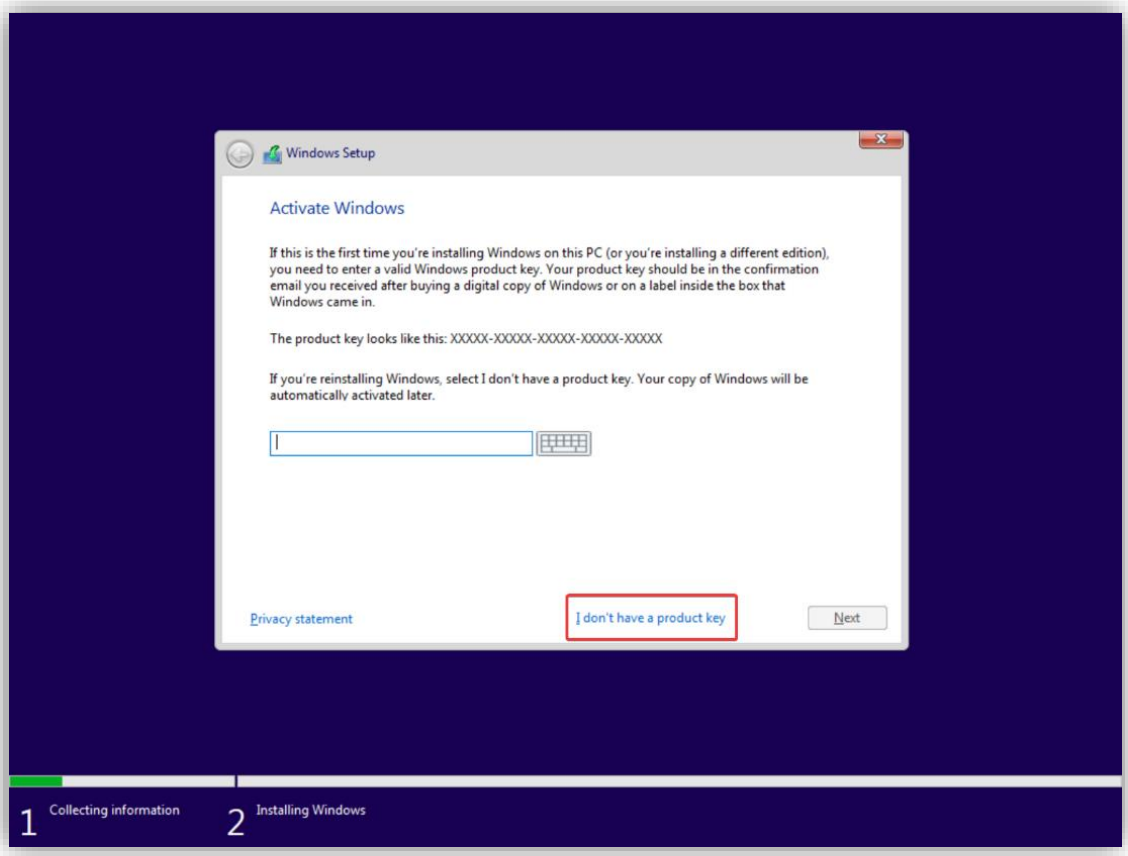
Sett opp et unikt navn på datamaskinene bestående av firmaakronym + en tilfeldig 4-sifferet kode



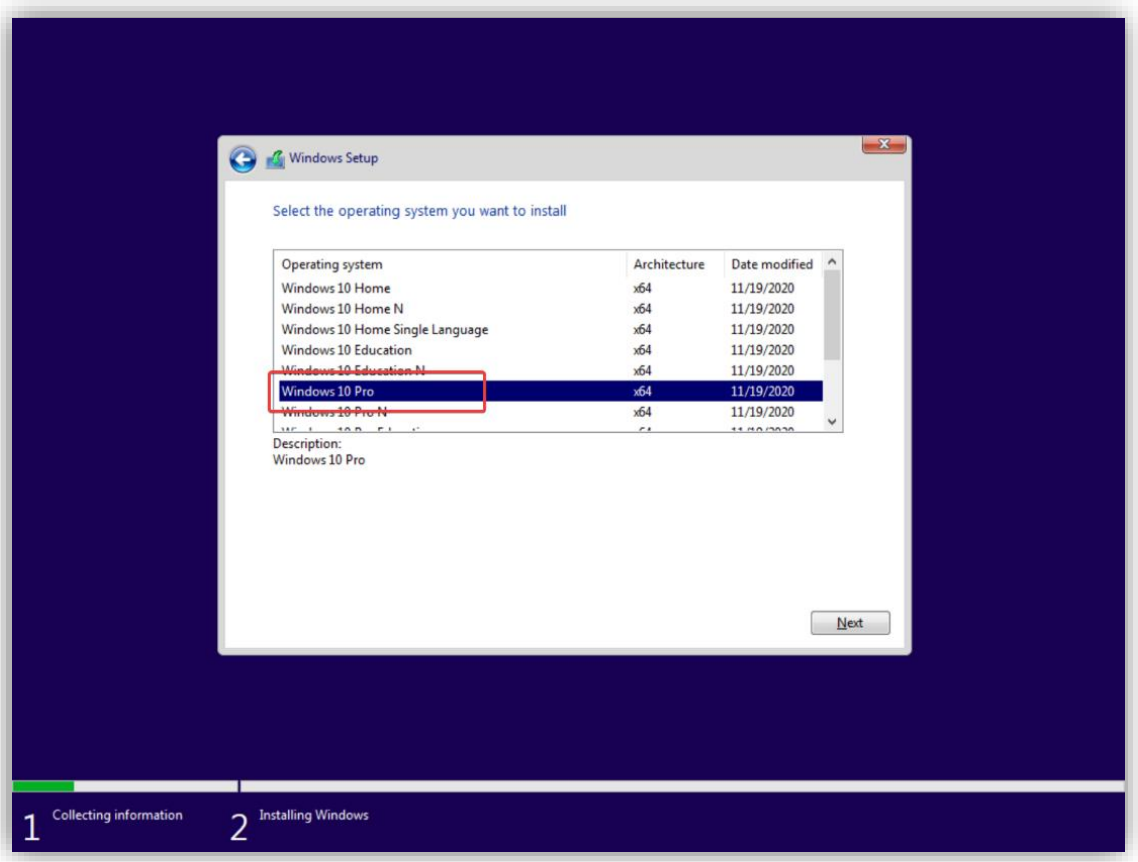
På neste side, velg gruppen denne profilen skal gjelde for. Velg da gruppen som ble lagd over.



På en nye Windows-enhet, gå gjennom installasjonen til du kommer til produktnøkkelvinduet. Her velger du **I don't have a product key** helt nederst



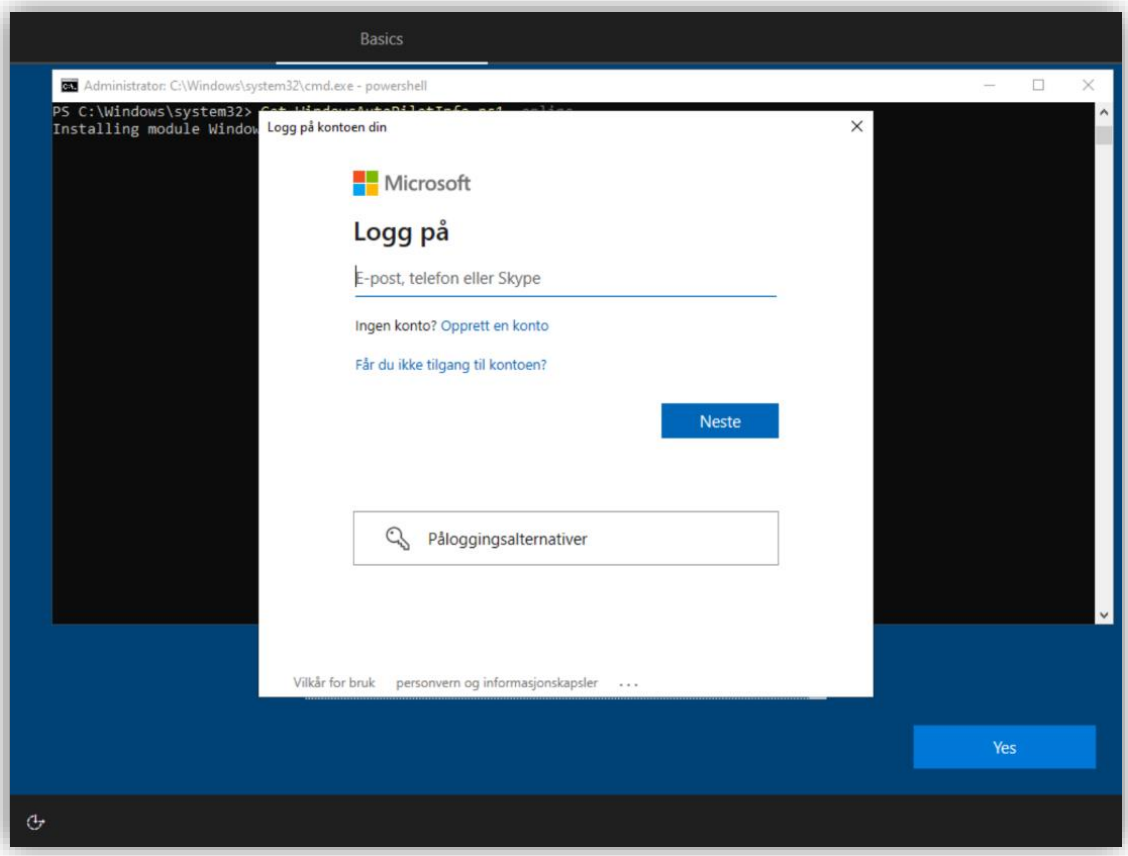
Deretter velg **Windows 10 pro**, aksepter EULA og velg **install Windows only**.



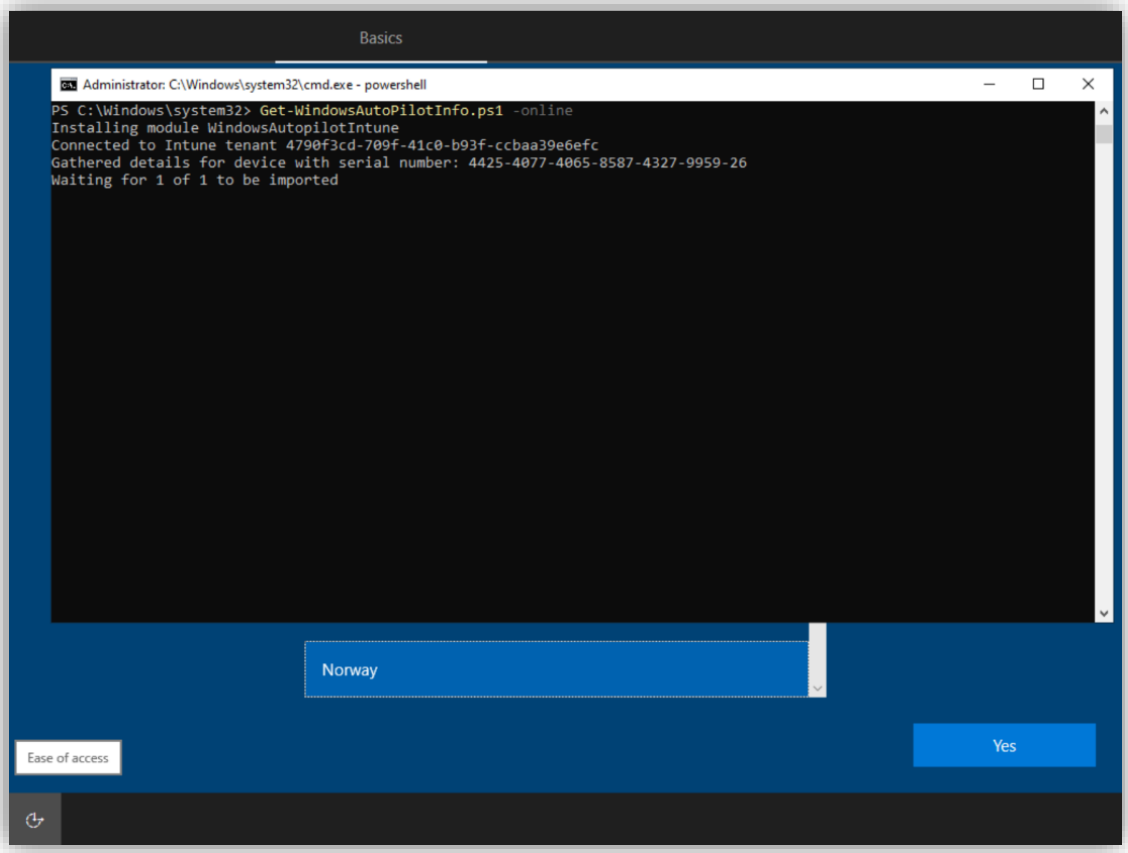
Når Windows er ferdig installert og du blir bedt om å velge region, trykk på **Shift + F10** for å åpne *Command Prompt*. Åpne så et PowerShell-skall og kjør følgende kommandoer:

1. **Set-ExecutionPolicy Unrestricted**
    - Denne kommandoen skrur av begrensninger slik at man kan kjøre alt av PowerShell skripts.
2. **Install-Script –name get-windowsautopilotinfo**
    - Installerer scriptet som brukes i neste steg.
3. **Get-WindowsAutoPilotInfo.ps1 -online**
    - Dette scriptet enroller maskinen med PowerShell ved å logge på en administratorbruker i bedriftens AD.
    - *-online*-flagget er viktig da det er det som prompter oss om å logge inn på AD.
    - Er *-online* ikke spesifiseres blir prosessen mye mer manuell.

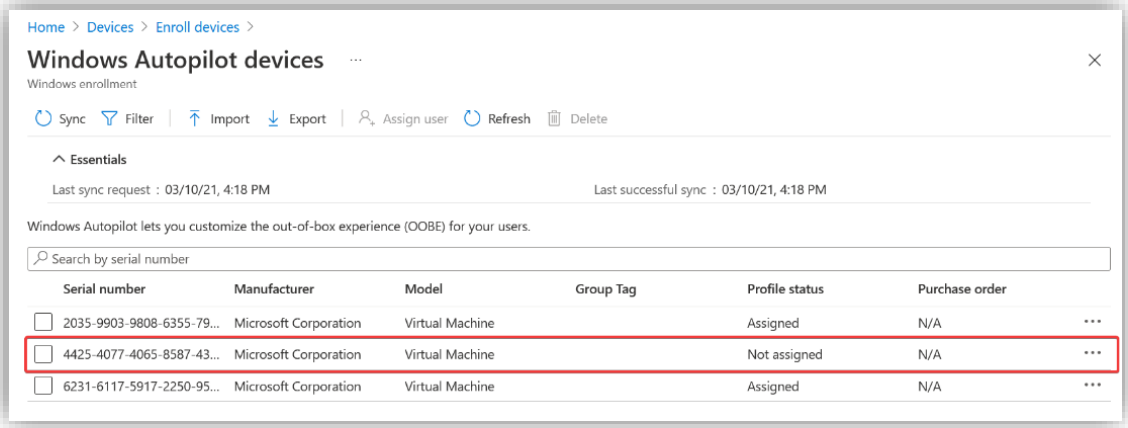
Etter den siste kommandoen er kjørt blir du bedt om å logge inn. Her bør en ha laget en egen bruker som kun har rettigheter til å gjøre dette - siden dette er en PoC så brukes en global administratorbruker for enkelthets skyld.



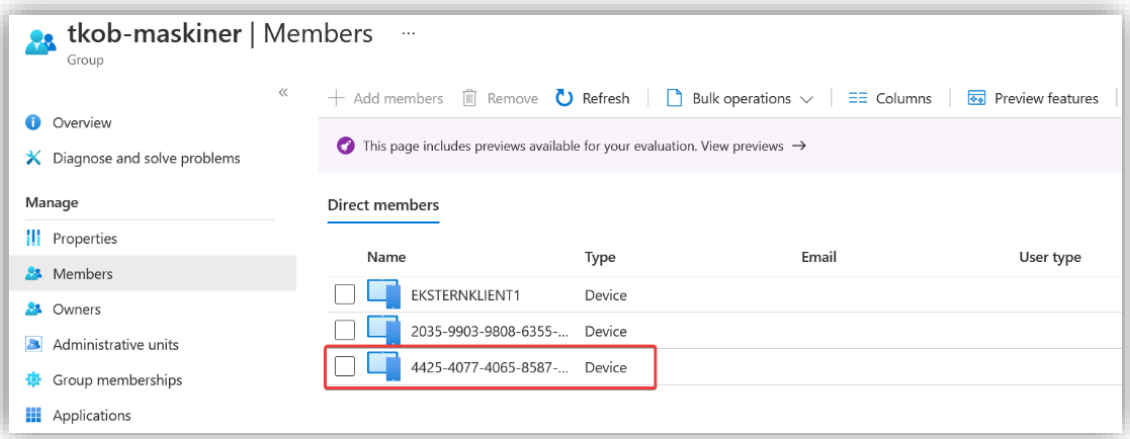
Neste steg syncher maskinen i Autopilot.



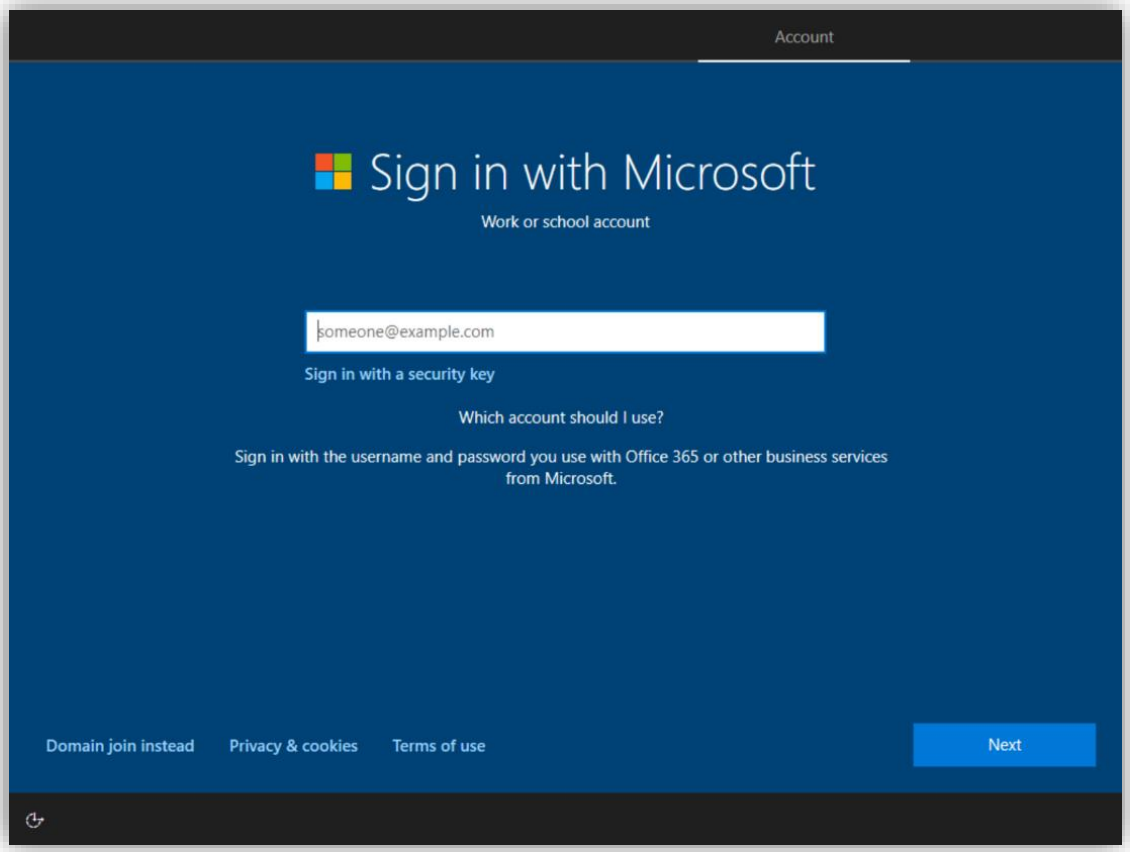
Når synchen er ferdig ser en at maskinen har dukket opp med et serienummer i **Windows Autopilot devices**



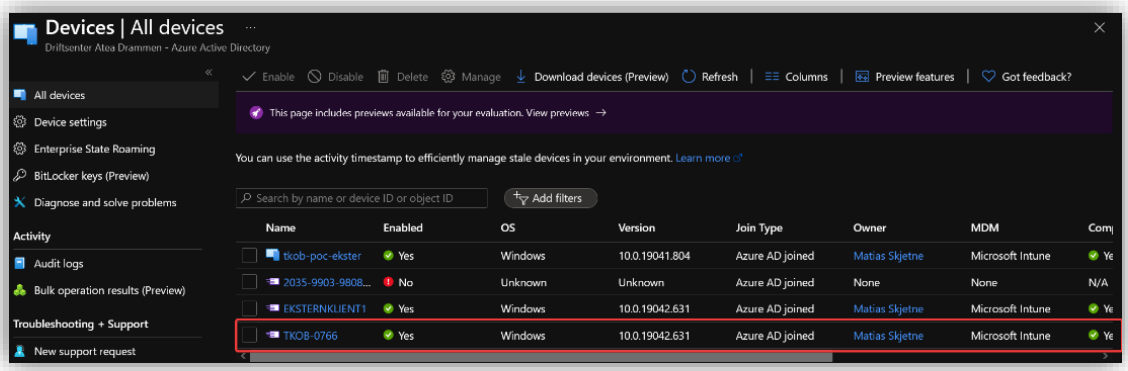
Her ser en også at den har dukket opp i gruppen «tkob-maskiner» takket være den dynamiske medlemsregelen. Du kan nå starte maskinen på nytt for at den skal settes opp og meldes inn i domenet.



Etter en rask omstart, kjører maskinen selv gjennom oppsettet og du må nå bare logge inn med brukeren som skal bruke maskinen.



Til slutt ser en at maskinene er lagt til i AD med riktig navn og eier.



3.6 Microsoft Intune

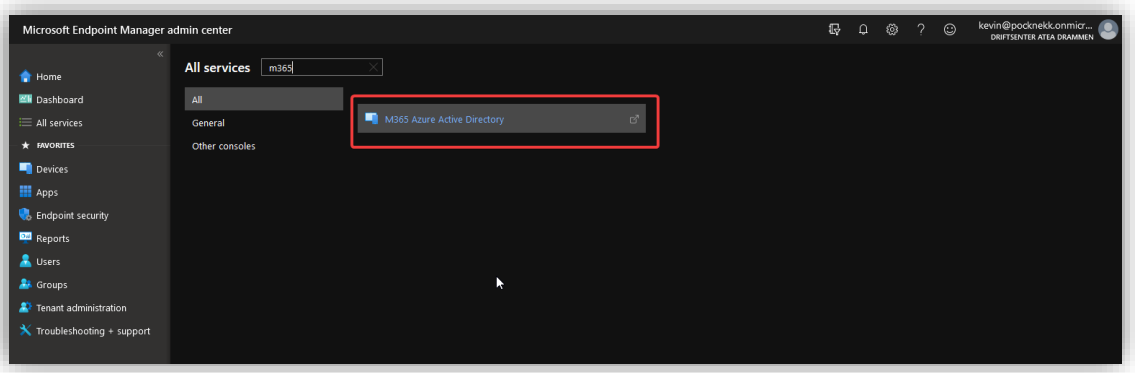
Microsoft Intune er Microsofts sky MDM og MAM. Løsningen administrerer alle enheter i bedriften og konfigurere disse etter satte profiler. Dette gjør det enkelt å overvåke maskiner å passe på at de er oppdatert, har riktig programvare og oppfyller alle krav til compliance satt av bedriften.

Intune støtter både «bring your own device» (BYOD) og firma-eide enheter. Dette gjør at man har stor fleksibilitet når det kommer til å sette opp sitt økosystem.

3.6.1 Oppsett av automatisk utrulling av Windows 10 maskiner

For å kunne administrere enheter (MDM) og applikasjoner (MAM) gjennom Intune, må en legge til de aktuelle enhetene i Intune. Dette gjør at en kan rulle ut ulike applikasjoner, som for eksempel Office-pakken, til de ulike enhetene og administrere hvordan enhetene kan brukes. For enheter i organisasjonen kan det være lurt å kunne administrere alt av innstillinger og sikkerhet.

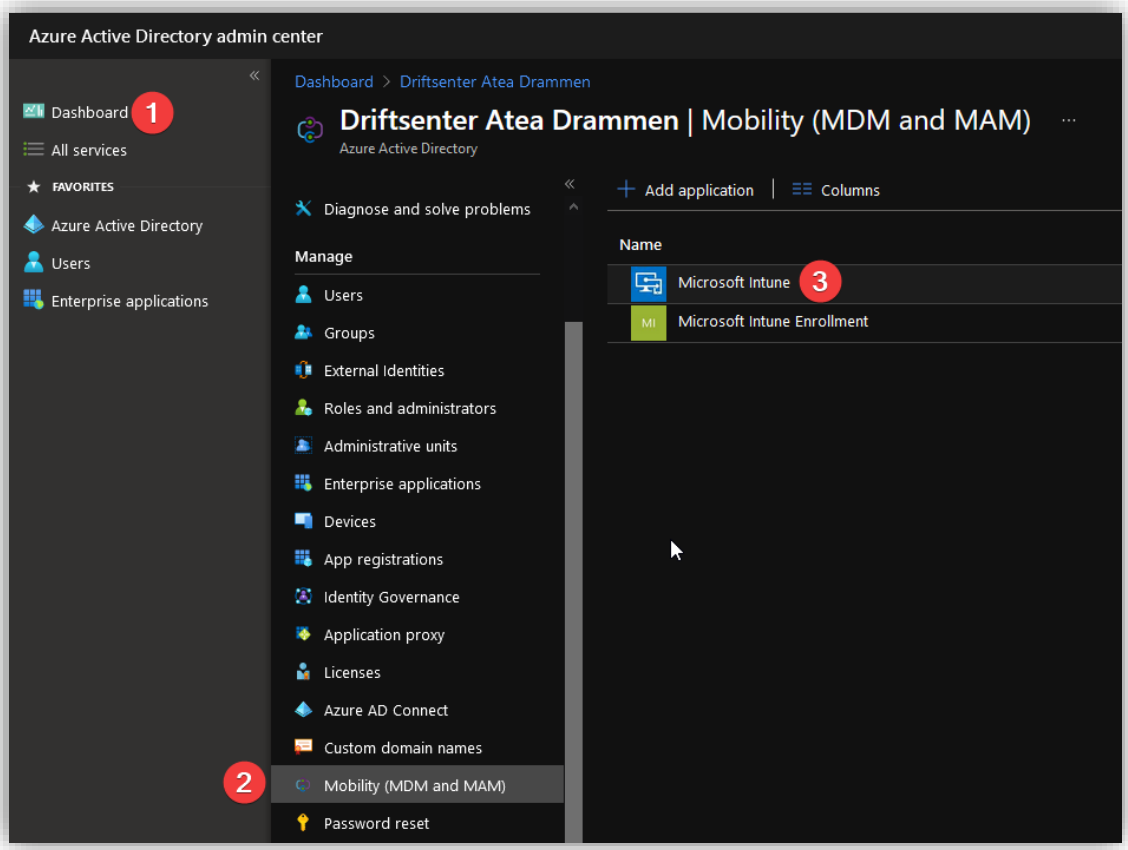
Inne i **Microsofit Endpoint Manager admin center**[5]**,** velg **All services > M365 Azure Active Directory.**



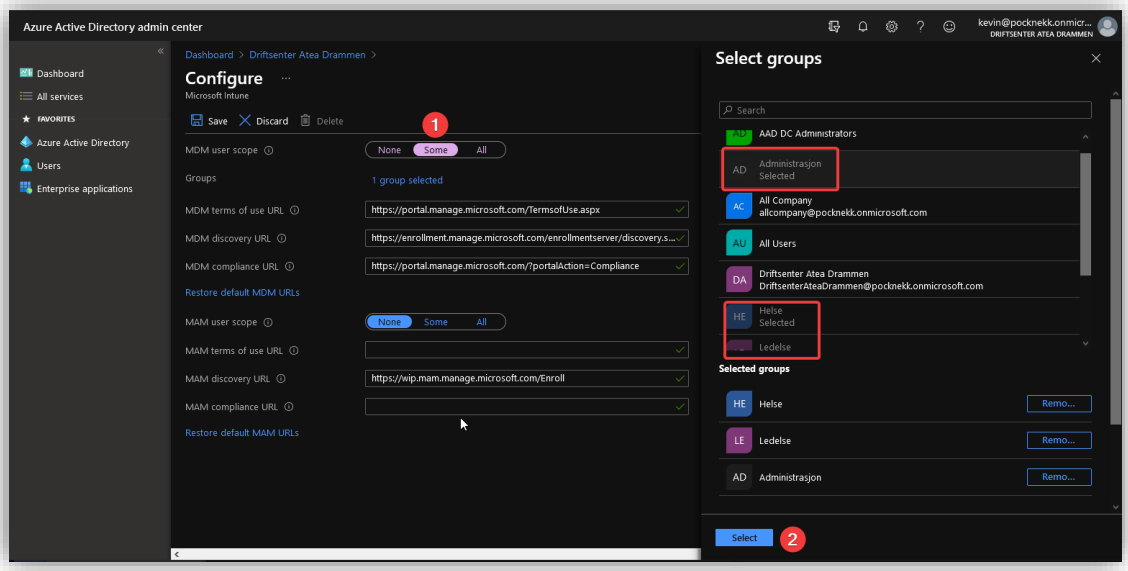
[5] https://endpoint.microsoft.com/?ref=AdminCenter#home

Dette vil åpne **Azuer Active Directory admin center**. Først må Microsoft Intune konfigureres.

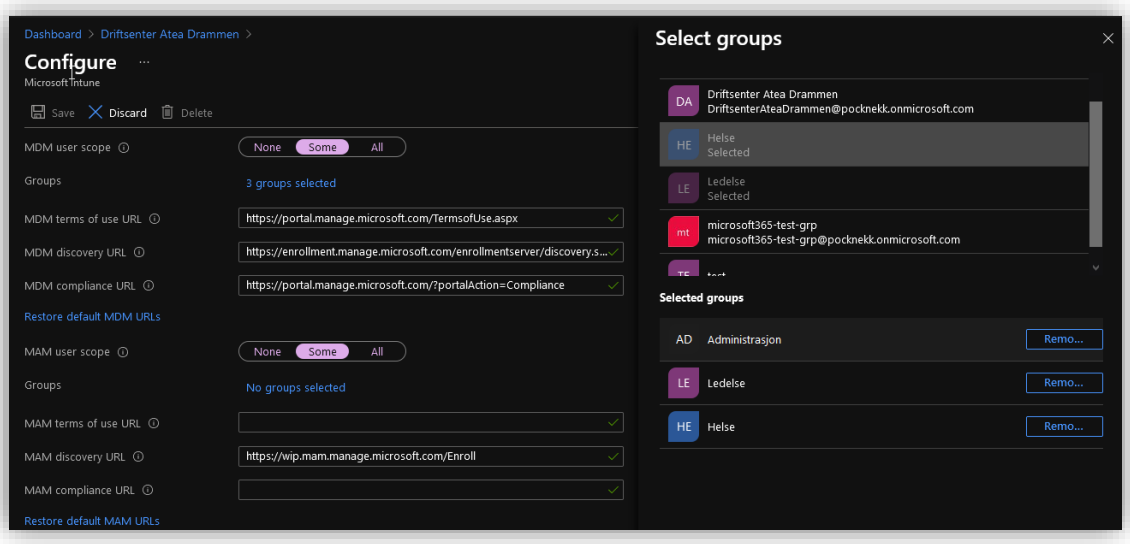
Gå inn på **Dashboard > Mobility (MDM and MAM)** og trykk på **Microsoft Intune**.



Legg til alle avdelingene slik at en kan kontrollere dataen på alle ansatte som kobler seg til.



Gjør det samme for **MAM user scope**.

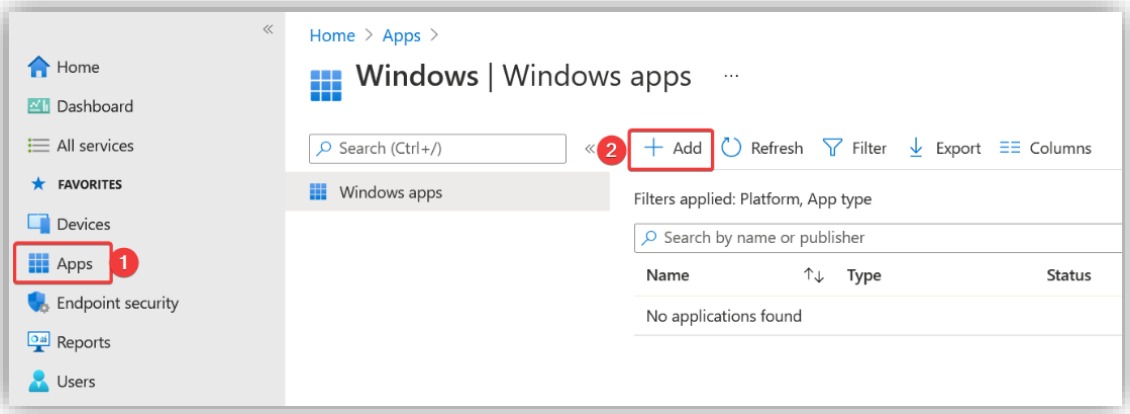


Trykk så på **Save.**

3.6.2 Utrulling av Office med Intune

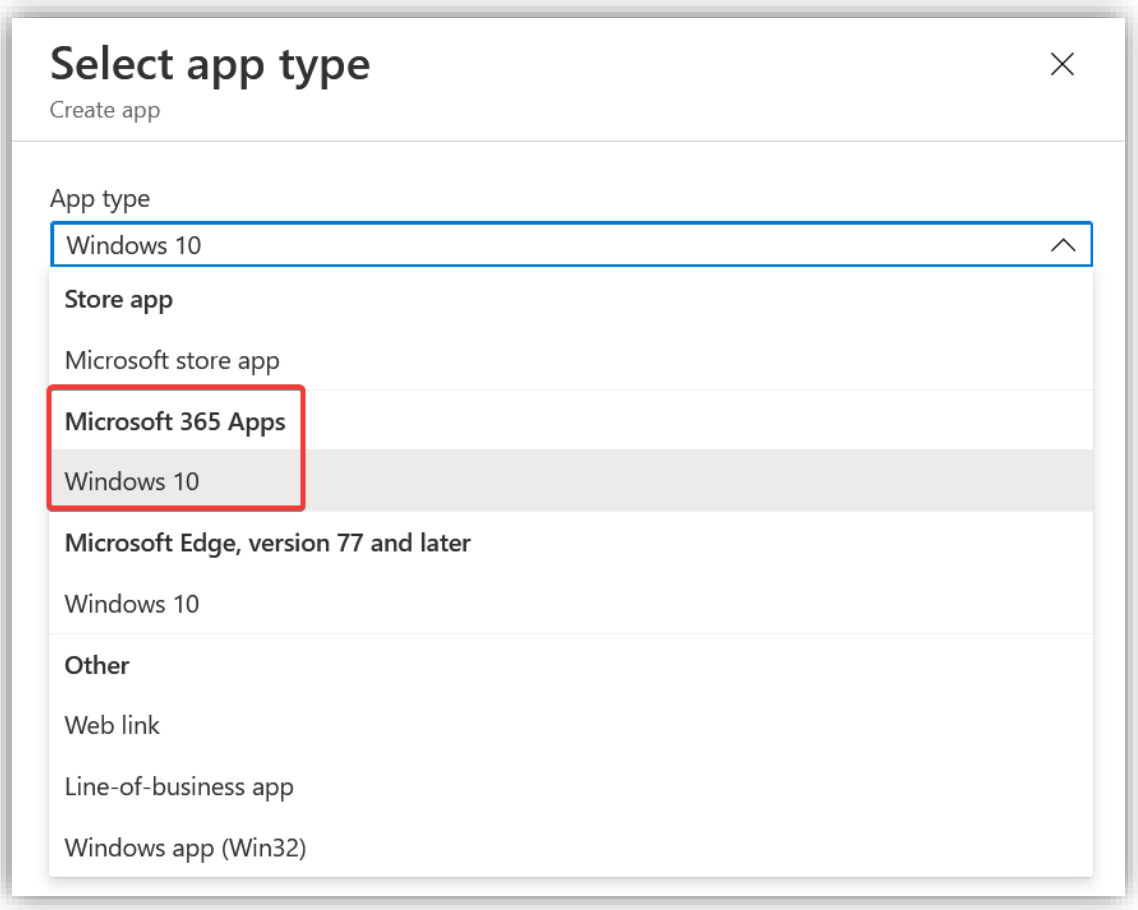
For å fullføre oppsettet av de ansattes maskiner, brukes Intune til å rulle ut applikasjoner. I dette eksemplet rulles Office pakken ut til de ansatte.

Legg til en ny applikasjon i adminfjeset[6] til Intune ved å trykke **Add** under **Apps > Windows apps.**

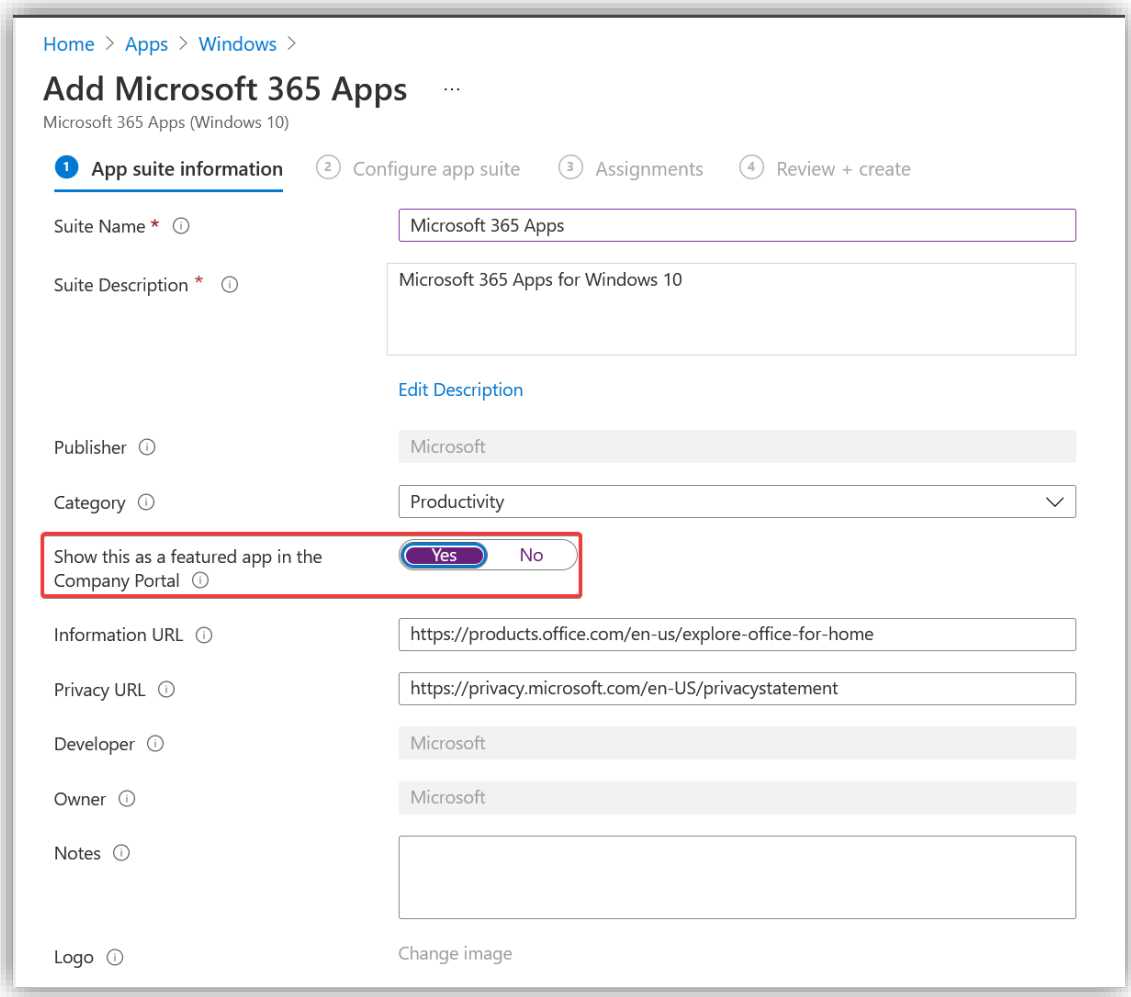


[6] https://endpoint.microsoft.com/?ref=AdminCenter#home

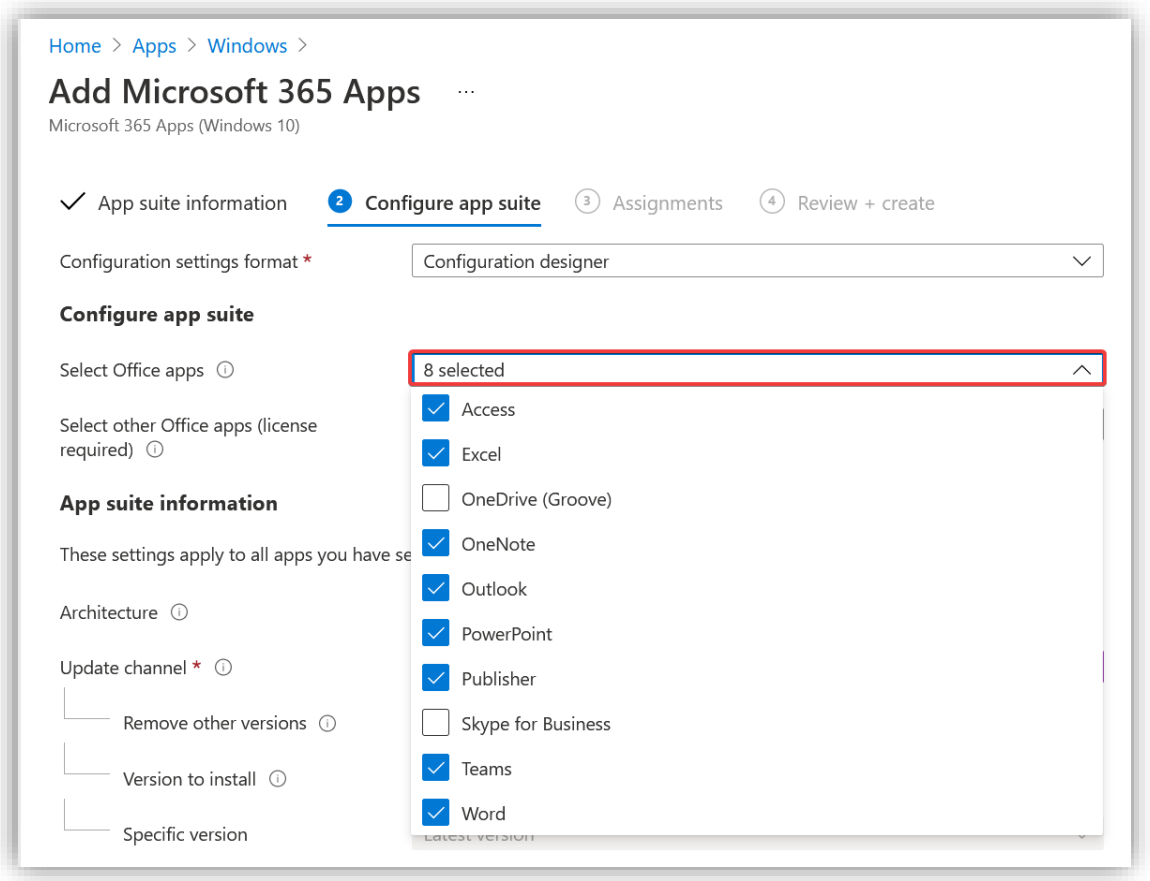
Velg **Windows 10** under **Microsoft 365 Apps** som **App type**.



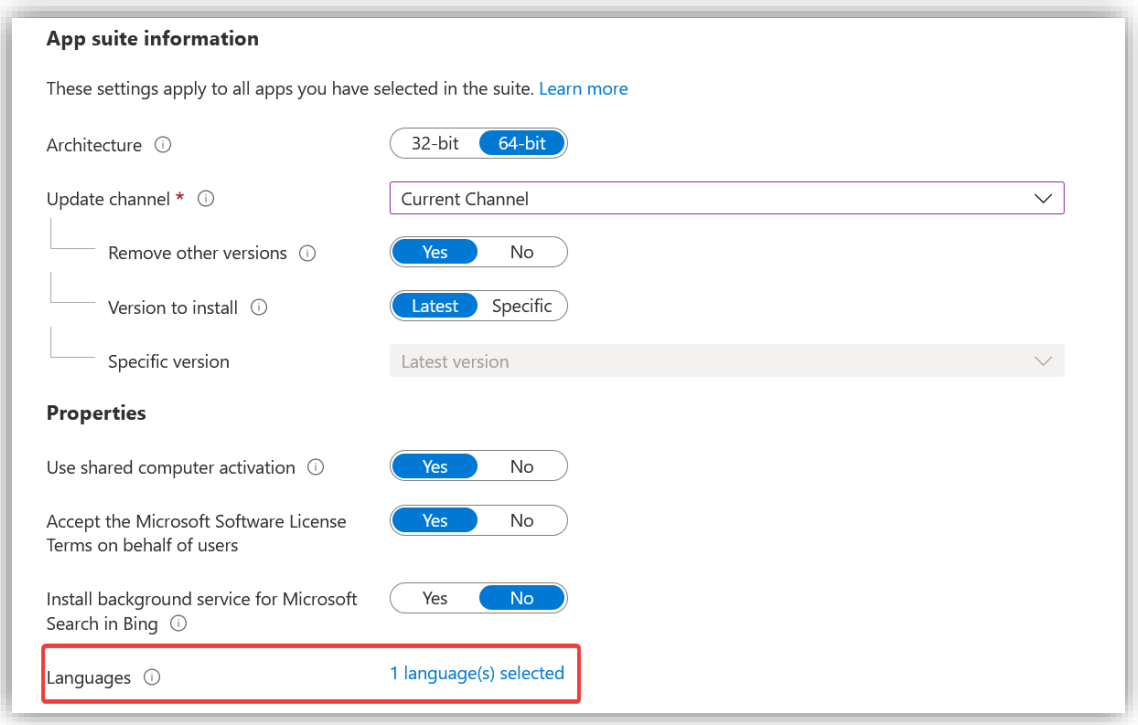
Applikasjonen må så konfigureres – mye av innstillingene kan stå som standard. Endre applikasjonen til å være en **featured app**. Dette gir den ekstra synlighet i en eventuell bedriftsportal. I dette tilfellet er det litt redundant siden man senere kommer til å velge at denne applikasjonen skal installeres automatisk for alle brukere.



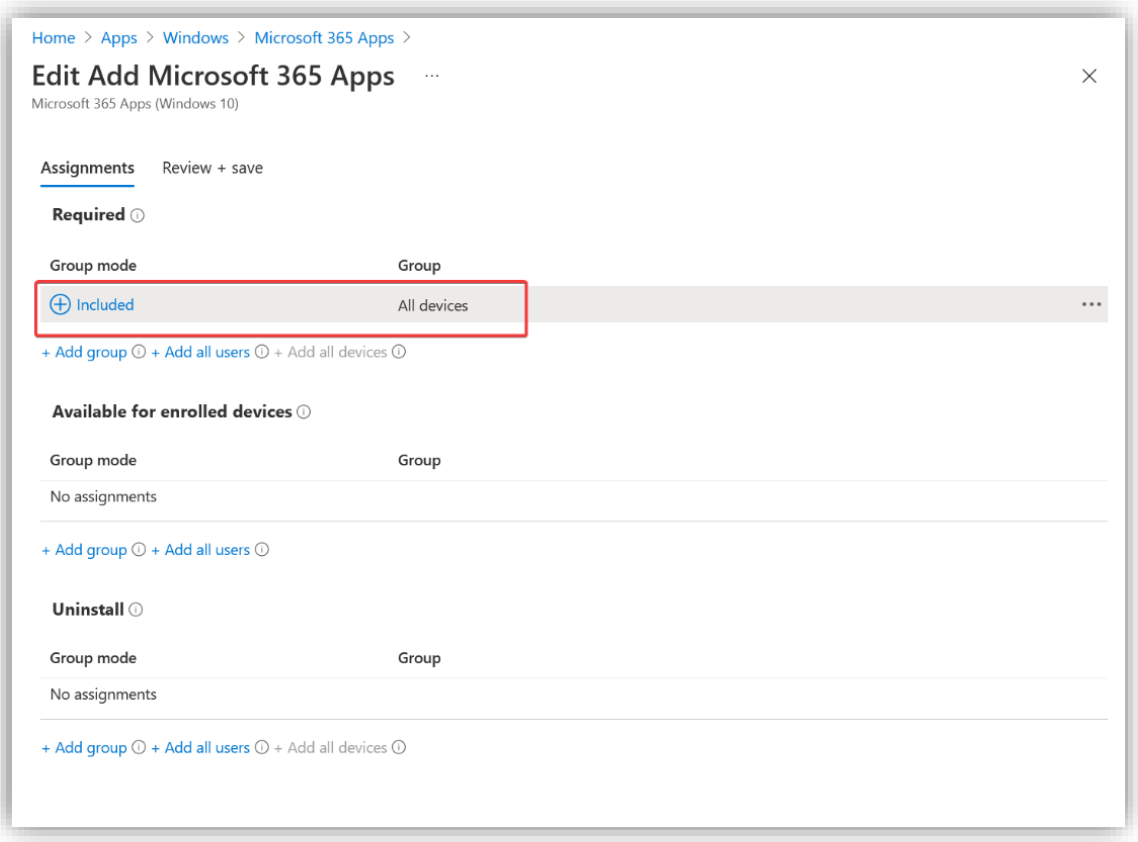
I den neste fanen, velg hvilke Office-applikasjoner som skal rulles ut, standard valg funker bra for dette oppsettet. Man kan også velge andre Office-applikasjoner som krever ekstra lisens, men i dette tilfellet er det ikke noe man har behov for.



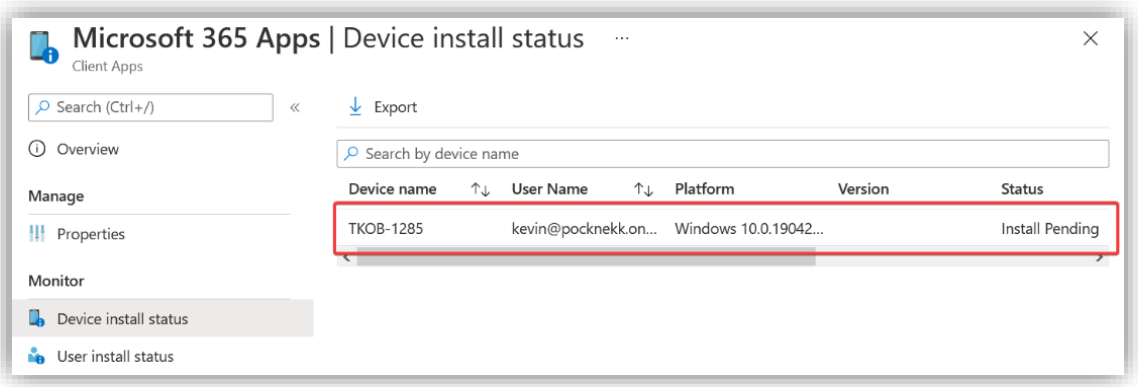
Videre kan det meste av innstillinger stå som standard, legg til norsk som språk nederst.



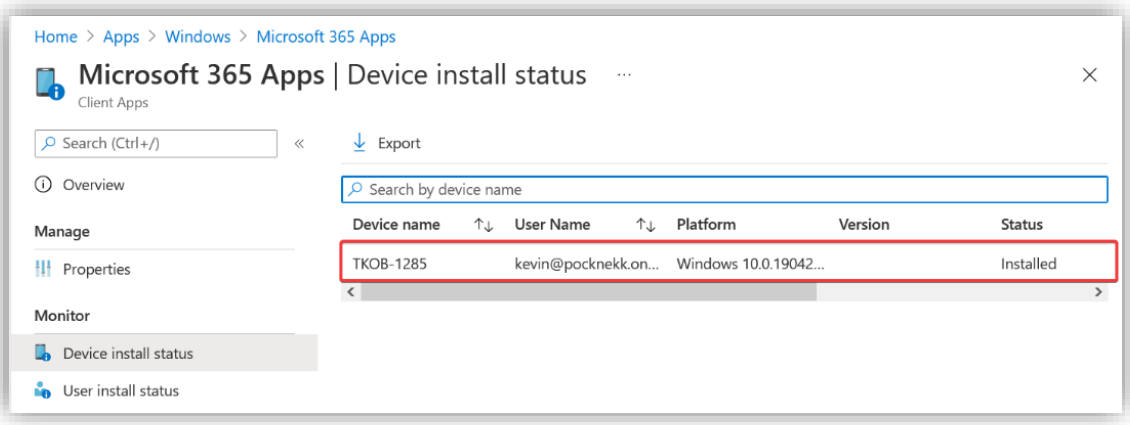
Velg at denne utrullingen skal gjelde for alle enheter. I produksjon vil man lage grupper med enheter slik at man har bedre kontroll på hvilke enheter som tankes med hvilken programvare.



Her kan man se maskinen at maskinen venter på installasjon



Og her er den etter at den har blitt tanket. Bildene er tatt med ca. 5 minutters mellomrom



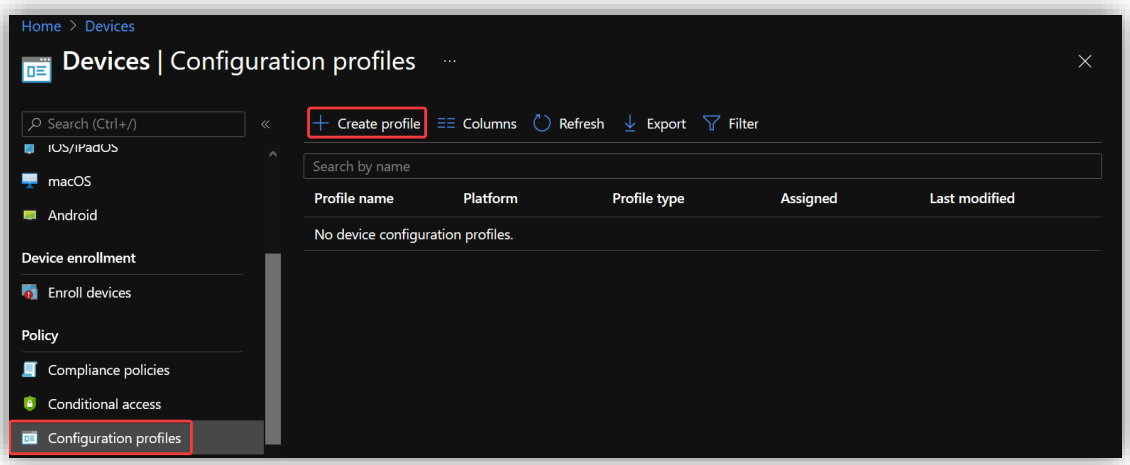
3.6.3 Device configuration

Configuration profiles brukes for å rulle ut innstillinger til maskiner i bedriften. Dette inkluderer sikkerhetsfunksjoner som brannmur, BitLocker, blokkering av applikasjoner og Microsoft Defender and encryption. Denne guiden viser hvordan en kan automatisere innlogging av Outlook og sette restriksjoner for hvilke innstillinger en bruker kan endre på.

3.6.3.1 Innlogging i Outlook

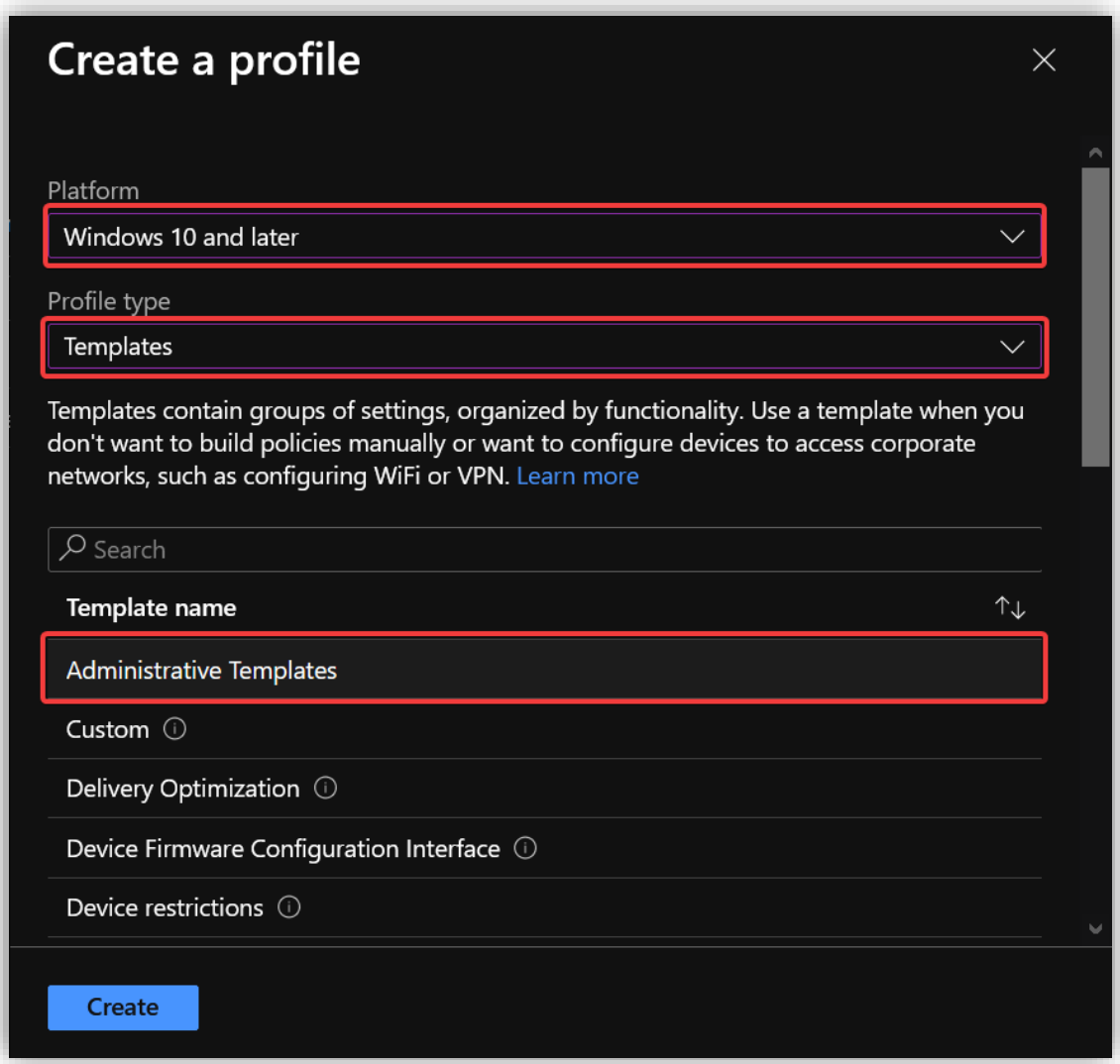
Denne konfigurasjonen automatiserer store deler av innloggingen av Outlook. Brukeren trenger kun å skrive inn e-postadressen og så vil Active Directory tas i bruk for å logge inn brukeren. En slipper altså å sette opp SMTP og lage en ny profil.

Lag en ny konfigurasjonsprofil inne på **Endpoint manager admin center**[7] under **Devices > Configuration profiles.**

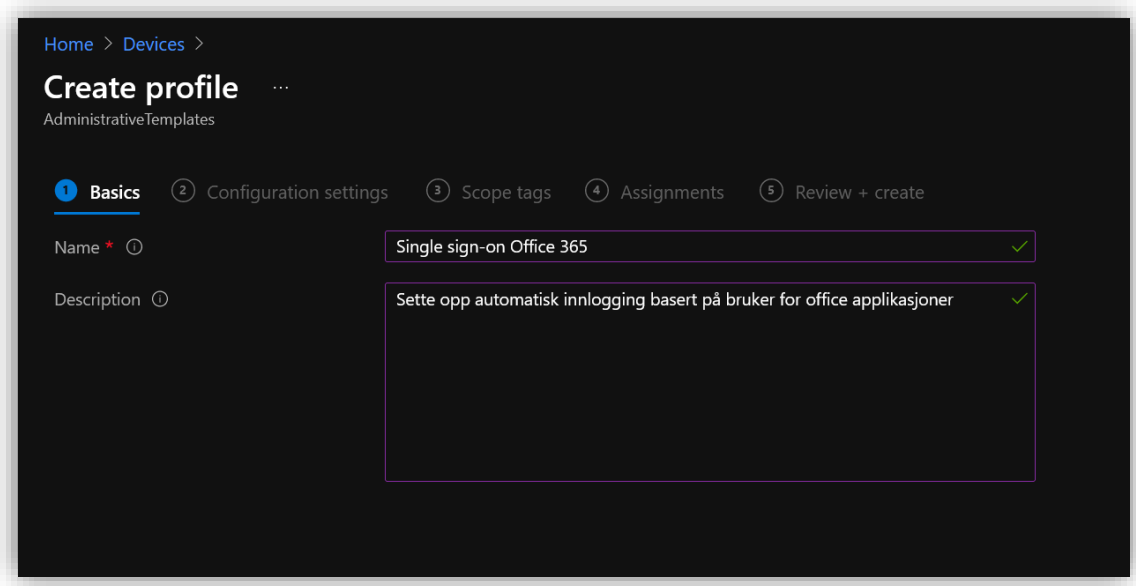


[7] https://endpoint.microsoft.com/?ref=AdminCenter#home

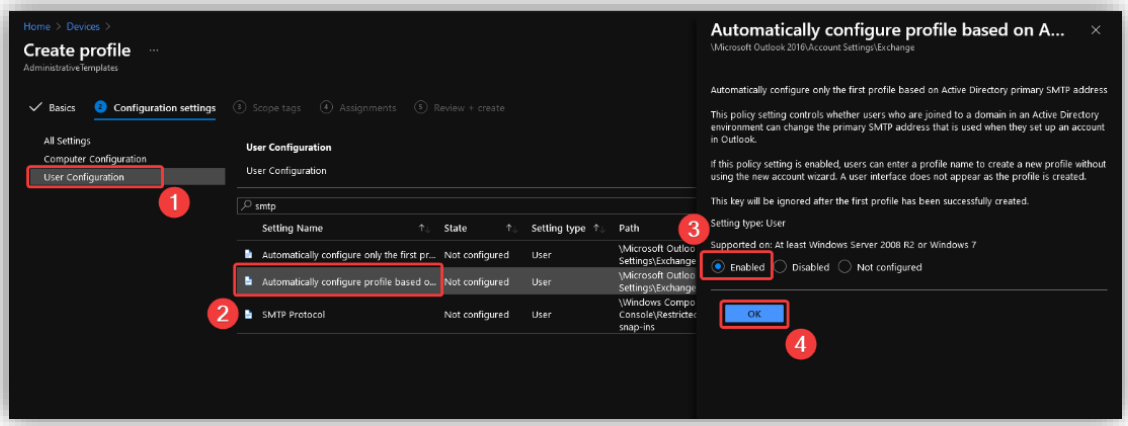
Sett plattform til **Windows 10 and later** og velg **Template** som profil type. Under template velg **Administrative Templates.**



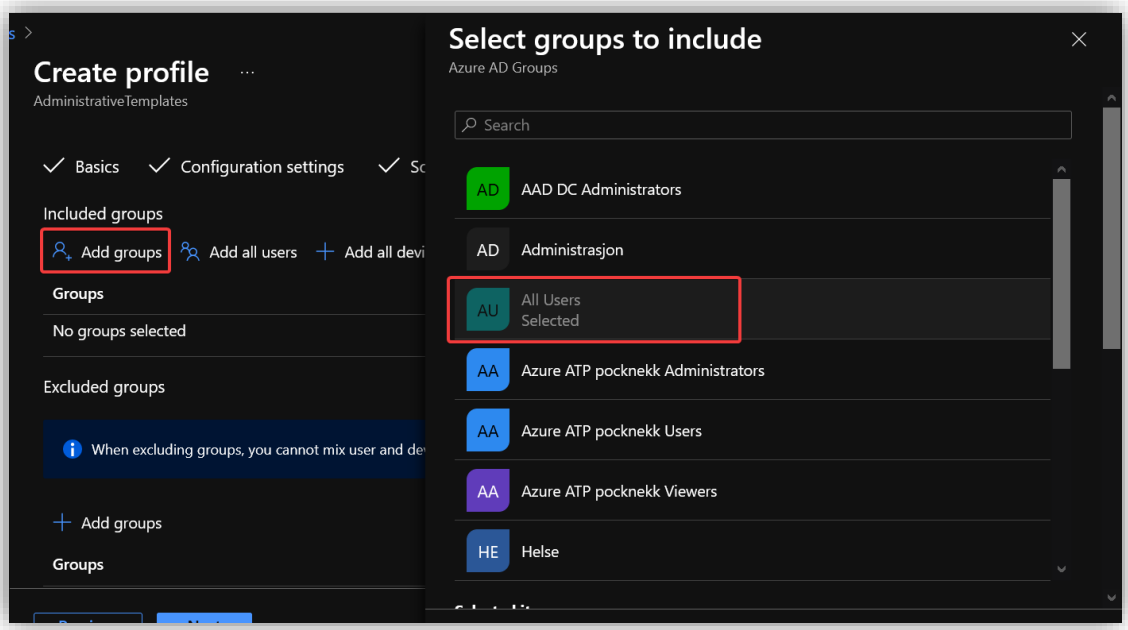
Gi profilen et passende navn og en beskrivelse.



Under **User Configuration** søk opp **SMTP** og velg alternativet **Automatically configure profile based on Active Directory Primary SMTP address**. Huk av for **Enabled** og trykk **ok.**



Velg hvilke brukere eller grupper profilen skal gjelde for. Denne profilen skal gjelde for alle.

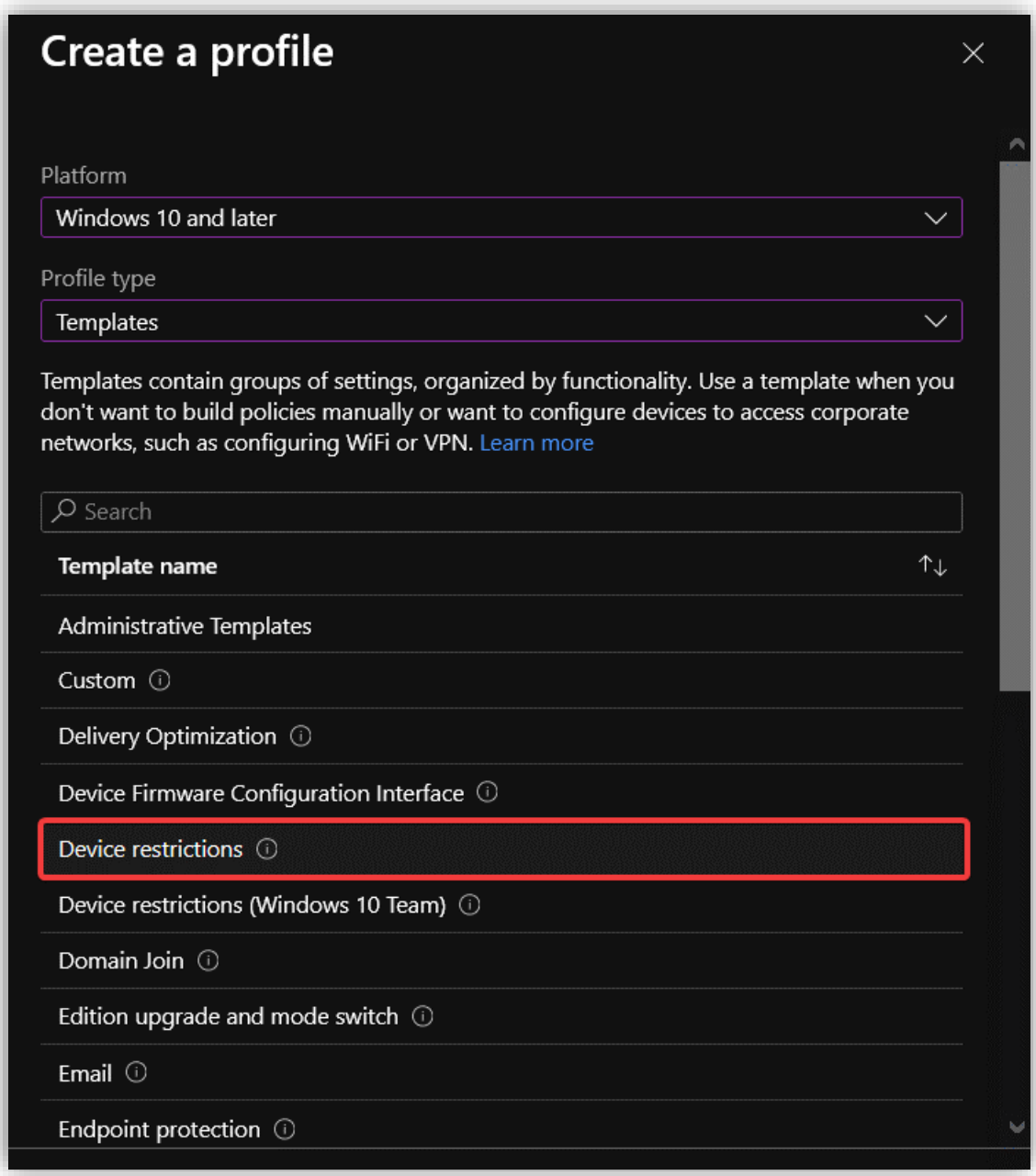


Til slutt trykk **create.**

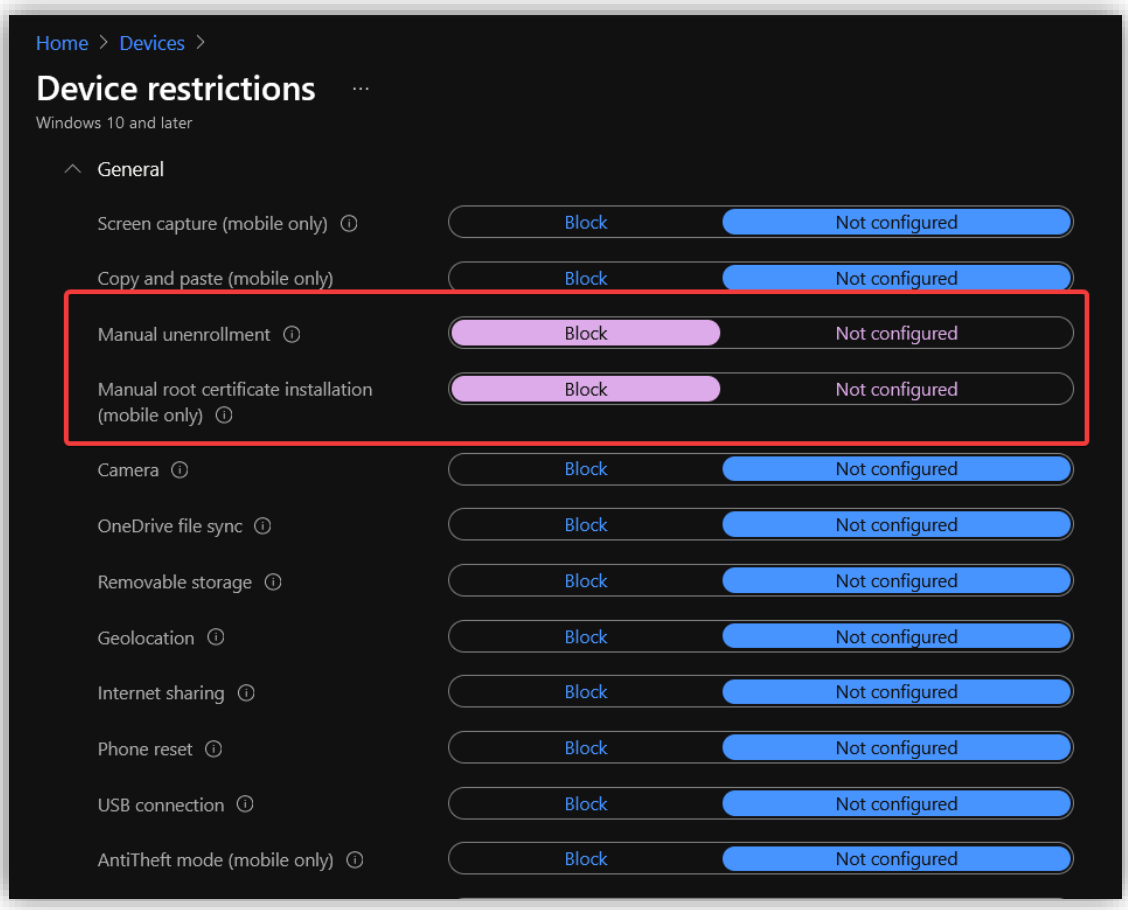
3.6.3.2 Enhetsrestriksjoner

For å hindre brukeren i å endre på visse innstillinger lager vi en **Configuration profile** som legger restriksjoner på brukerens muligheter.

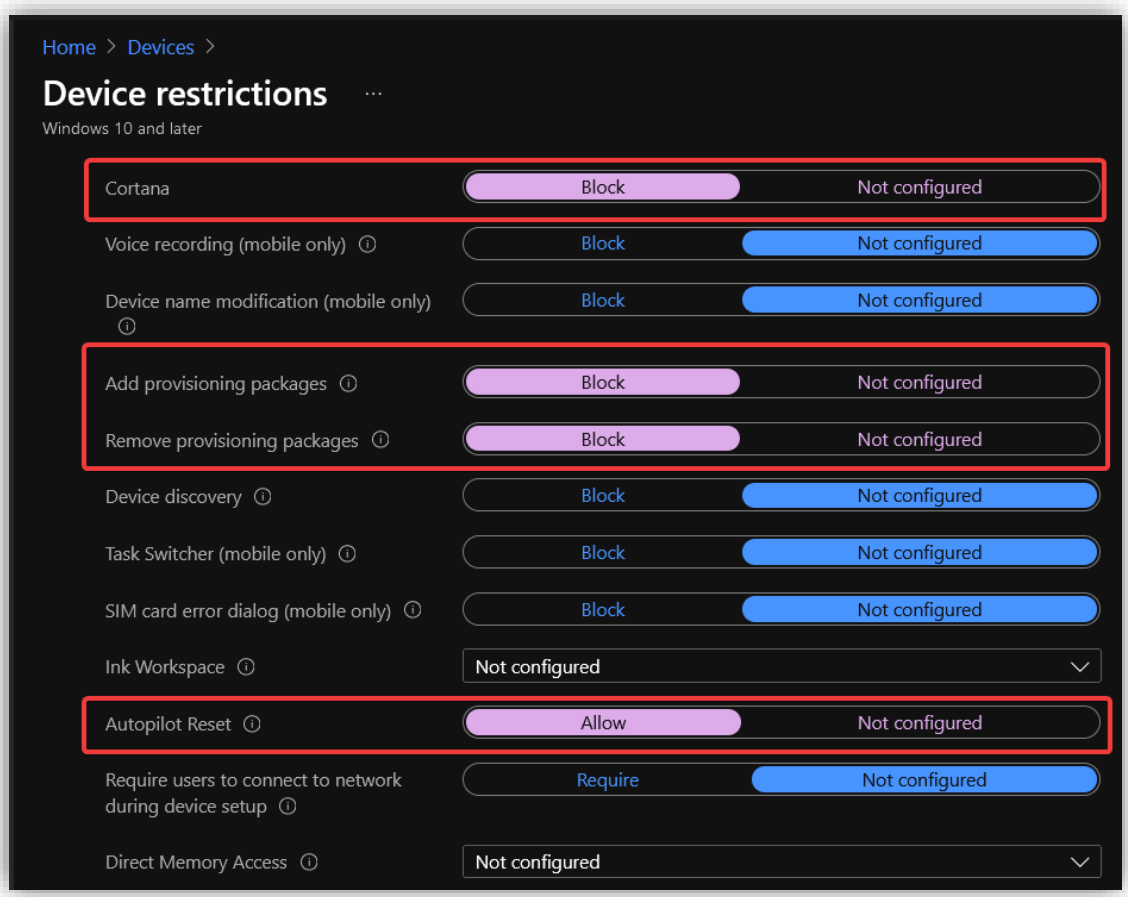
Lag en ny **Configuration Profile**, og velg **Device restrictions** som template.



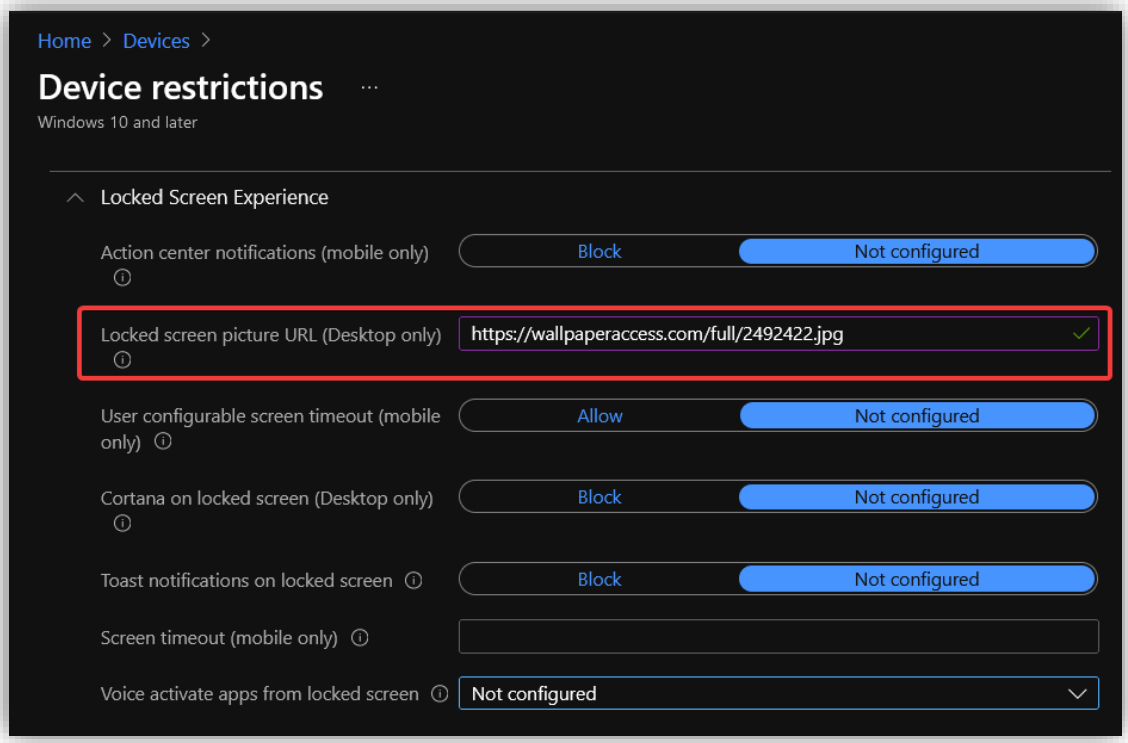
Under **General** blokker **Manual unenrollment** og **Manual root certificate installation.** Brukerne skal ikke få fjerne maskinen sin fra Intune da dette kan medføre at de mister viktig konfigurasjon. De skal heller ikke få styre med sertifikater selv, da det er viktig at bedriften selv har kontroll på dette.



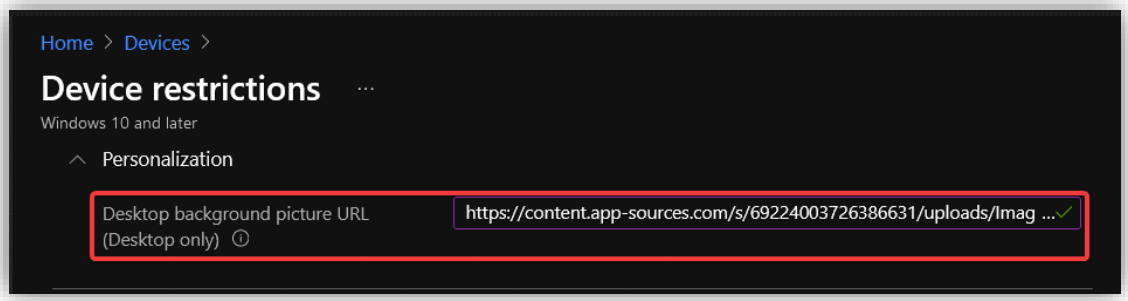
Cortana skrus av på grunn av personværnshensyn. Begge alternativene knyttet til **provisioning packages** blokkeres også. En provisioning package (.ppkg fil) er en måte å automatisk sette et sett med instillinger på en enhet. Dette gjøres manuelt og er brukes sjeldent i bedrifter.



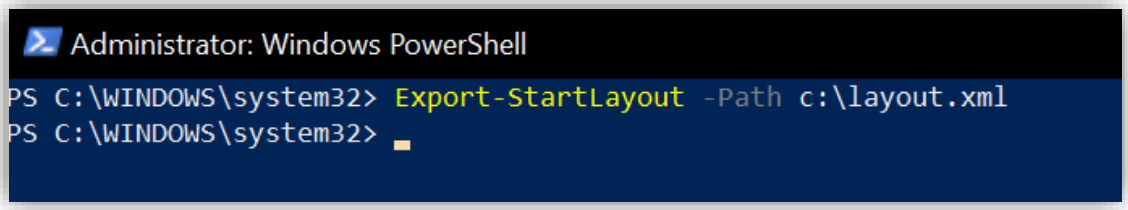
Under **Locked Screen Experience** legg in en URL for et bakgrunnsbilde.



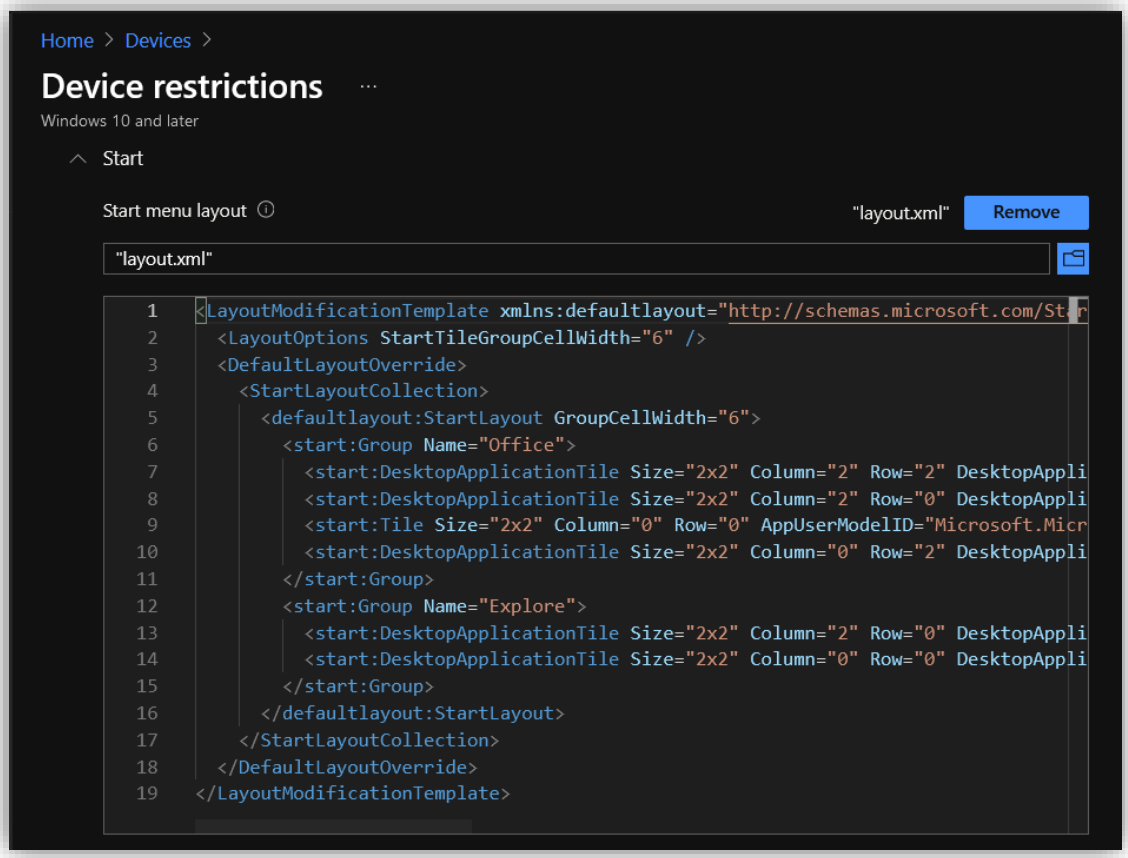
Under **Personalization** legg inn en URL for et bakgrunnsbilde.



For å generere et layout til startmenyen, sett opp menyen slik man ønsker på din egen maskin. Kjør deretter dette PowerShell-scriptet i administratormodus.



Velg filen som ble generert i det forrige steget og last den opp under **Start > Start menu layout.**



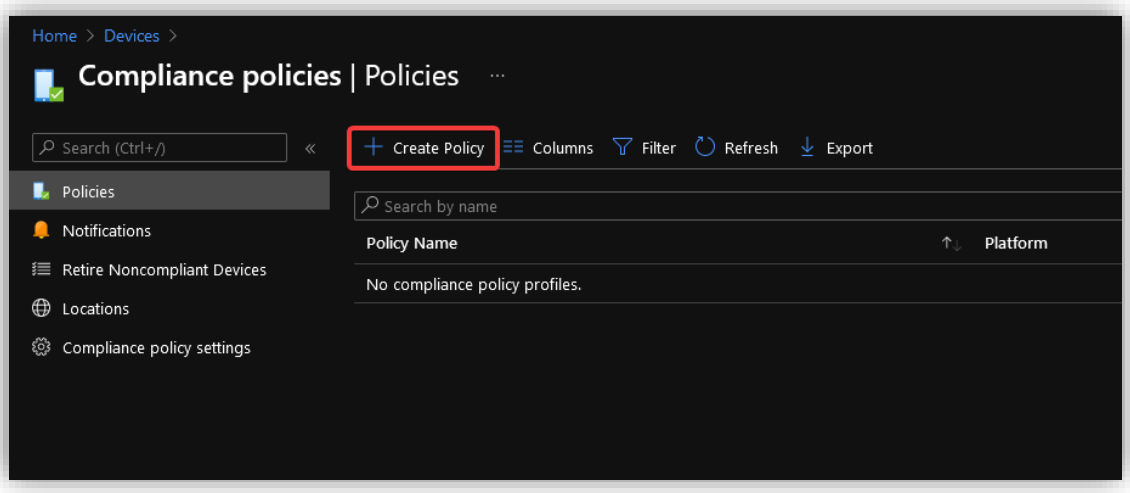
Brukeren vil nå ikke kunne endre bakgrunnsbilde eller layout i startmenyen.

Gå videre og velg **Create Policy.**

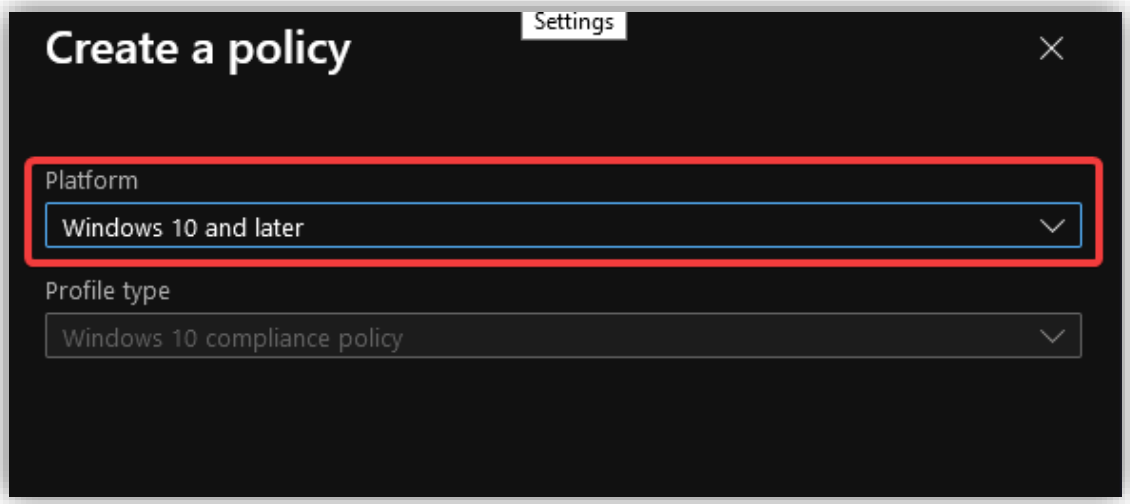
3.6.4 Lage compliance policy

For å sikre bedriftens data kan en lage compliance policyer som setter krav til brukere og enheter må møte. Her kan en også bestemme hva som skal skje dersom kravene ikke blir møtt. Ettersom bedriften håndterer personsensitiv data så kommer dette eksempelet til å sette relativt strenge policyer.

I **Microsoft Endpoint Manager**[8] gå inn under **Devices > Compliance policies** og velg **Create Policy**

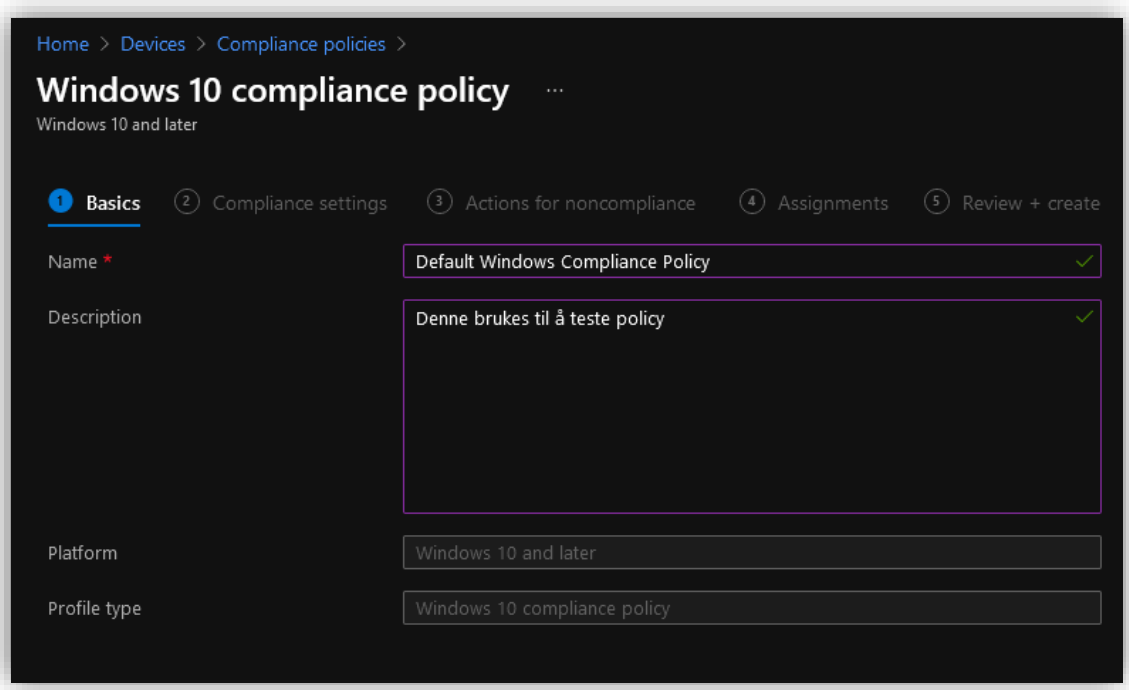


Velg **Windows 10 and later** og trykker på **Create.**



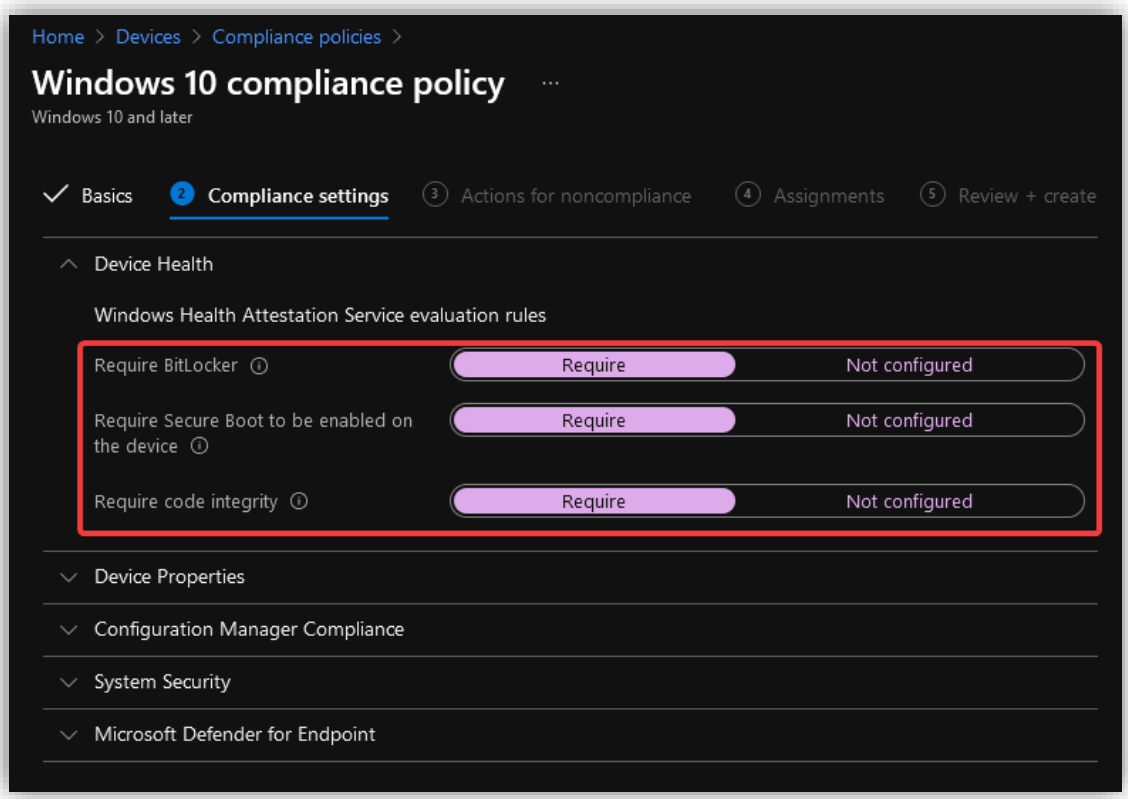
[8] https://endpoint.microsoft.com/?ref=AdminCenter#home

Gir den et passende navn og beskrivelse.

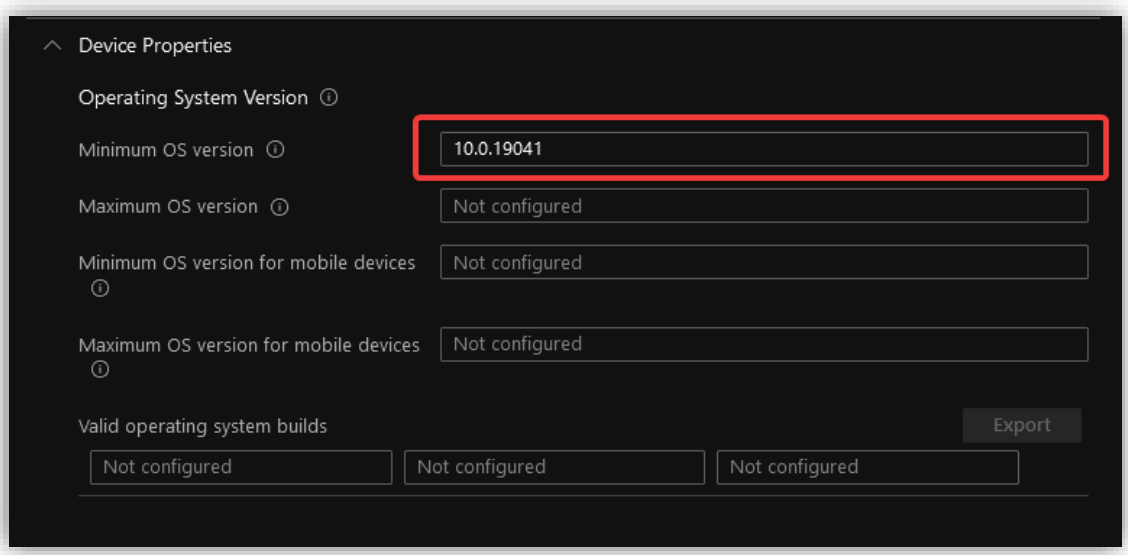


På denne siden er det en rekke innstillinger en kan sette som setter krav til enhetene og brukerne. Under **Device Health** velg å kreve **BitLocker, Secure Boot** og **code integrity**.

Ved å kreve BitLocker kan en sikre at alle enhetene er krypterte for å være compliant. Skulle en ansatt miste sin datamaskin vil det ikke være mulig å hente ut noe informasjon uten å ha nøkkelen. **Secure Boot** passer på at komponentene som starter maskinen har de rette kryptografiske signaturene før den lar maskinene starte. **Require code integrity** passer på at det ikke er noen systemfiler som er endret på av malware eller en administratorbruker.

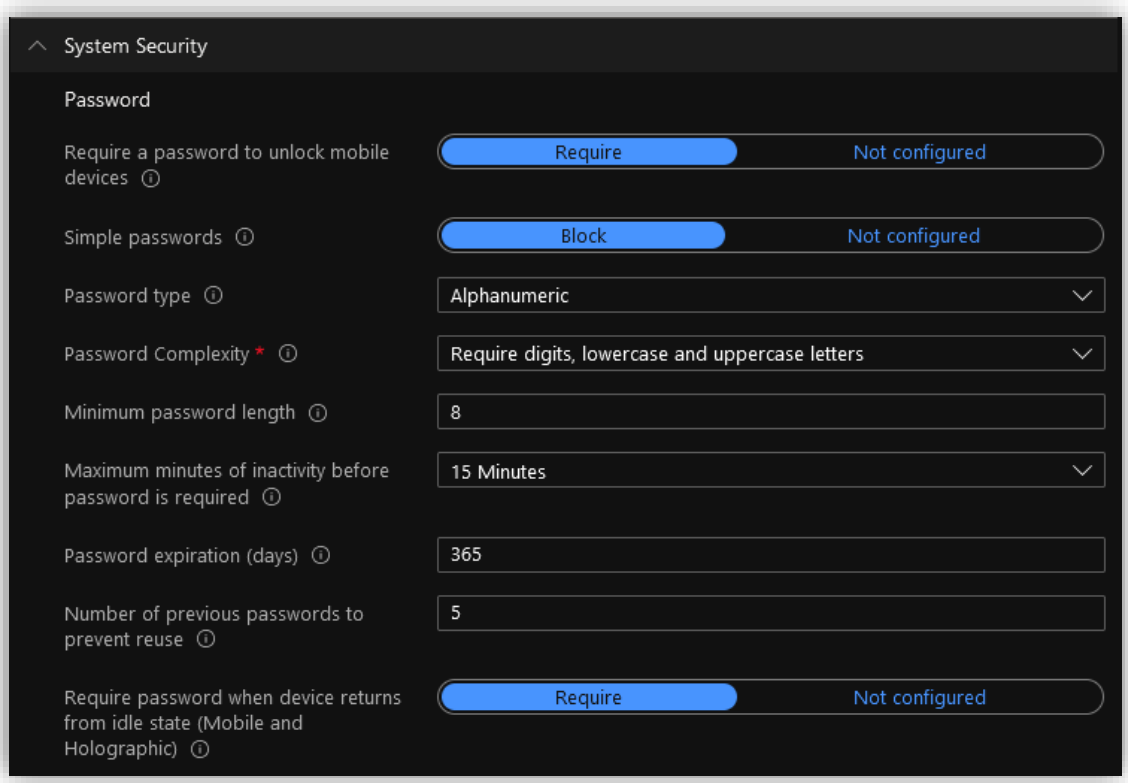


Under **Device Properties** skriv inn en minimum-OS versjon. Versjonen som er skrevet inn under er den nest nyeste versjonen av Windows 10 per dags dato (16.04.2021).

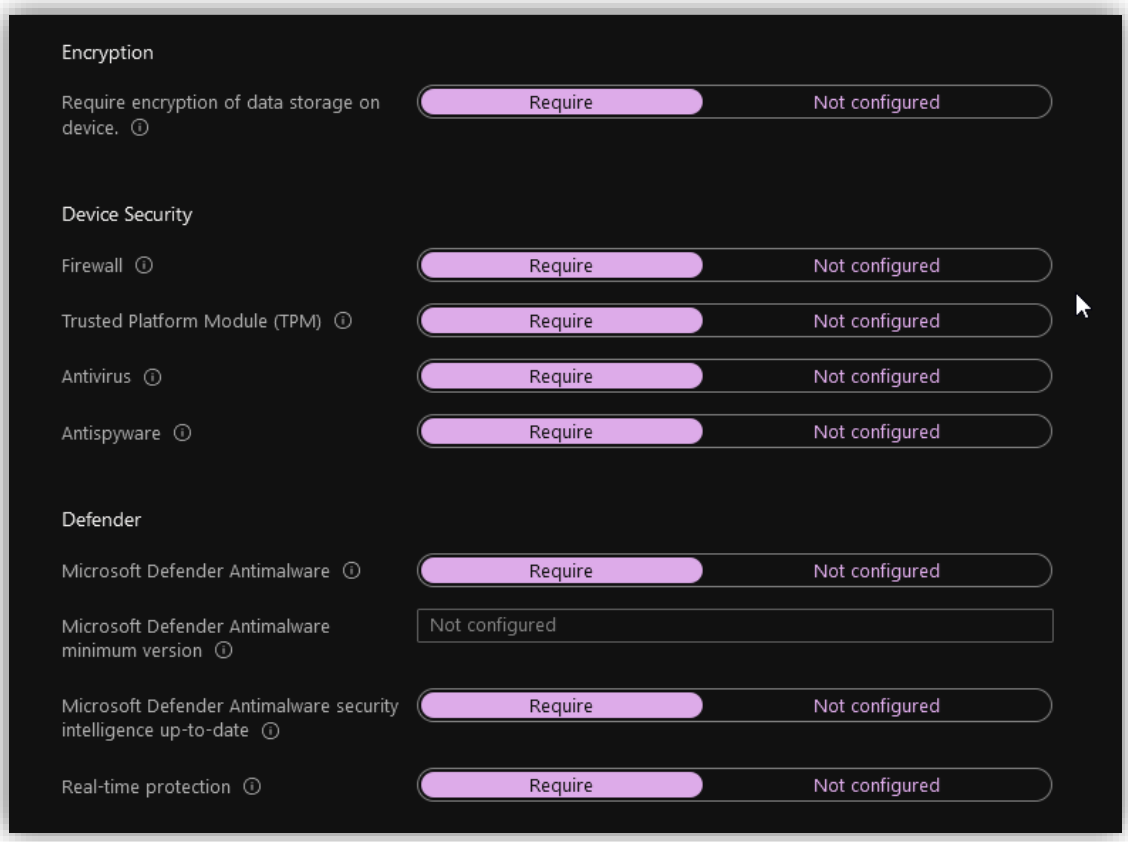


Under **System Security** sett først passord-policy.

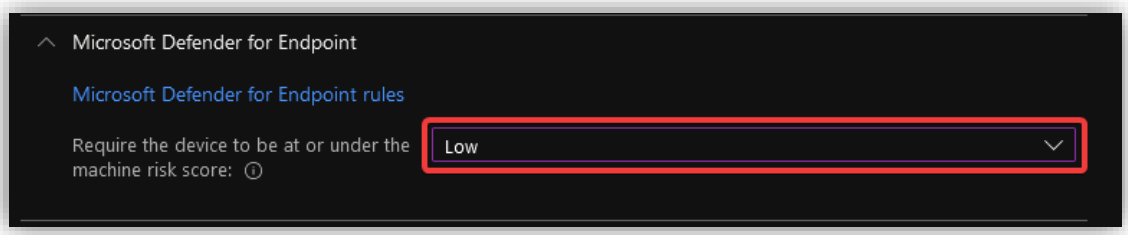
- Krev at alle enheter må ha et passord – det blir sett på som et absolutt minimum.
- Velg så at brukerne ikke kan ha et simpelt passord (f.eks. 1234 og 1111). Setter så krav for hva passordet må inneholde. Ved å kreve tall og store og små bokstaver sikres en viss kompleksitet i passordene – det anbefales også å sette en minimumslengde på 8.
- Sett at skjermen skal låses etter 15 minutter dersom den ikke er i bruk.
- Velger å sette en utløpsdato på passordene til 1 år.
- Sett at en ikke kan gjenbruke noen av de 5 siste passordene som har vært i bruk.



Velg å kreve kryptering gjennom BitLocker – dette er et godt tiltak mot evt. Stjeling av data dersom enheten skulle bli borte. Under **Device Security,** velg **Require** på alt ettersom dette gir den høyeste sikkerheten. Under **Defender,** sett også **Require** på alt slik at alle enhetene tar i bruk Windows Defender og at den alltid er oppdatert.

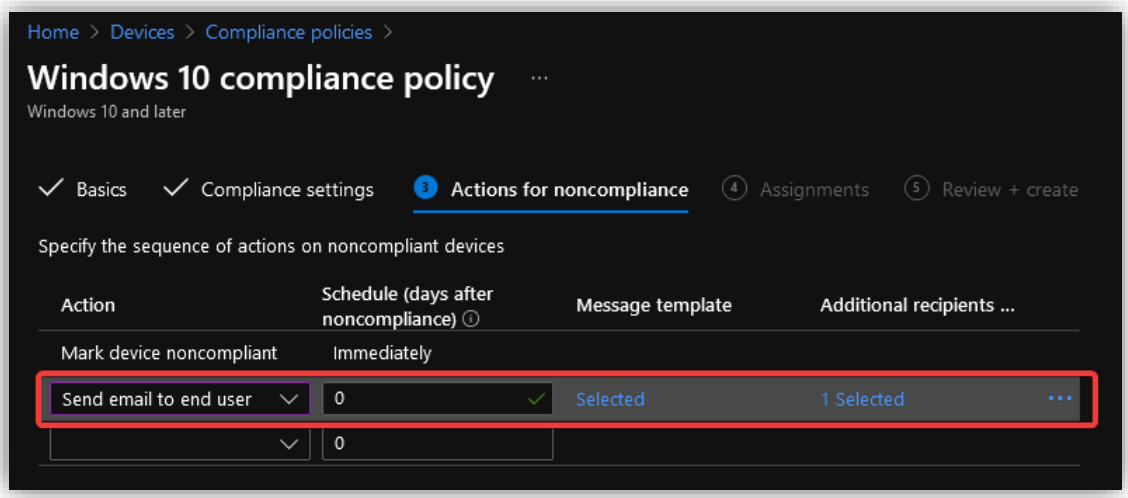


Under **Microsoft Defender for Endpoint,** sett kravet til sikkerhets-score til å være **Low**. Dette er for å gi brukeren en liten slingring dersom det skulle være noe som ikke er satt opp riktig med en gang. Denne kan også settes til **Clean** dersom en vil ha best sikkerhet og ingen mulige farer på enhetene i bedriften.

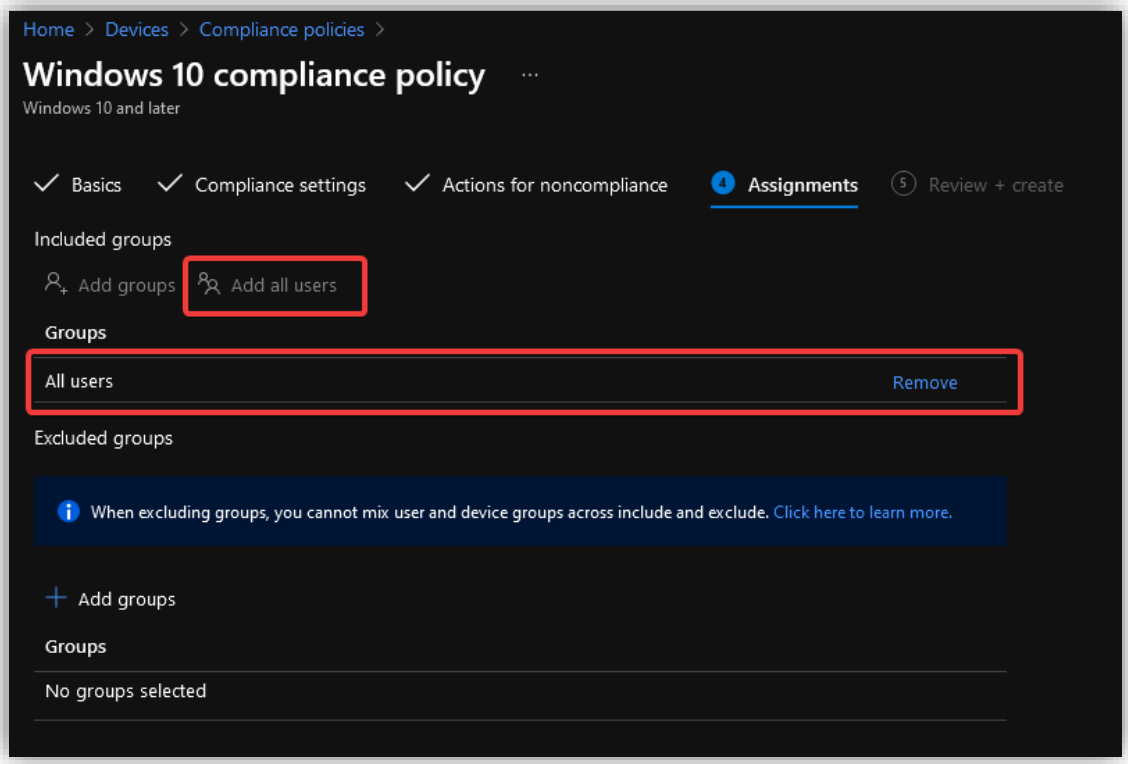


En kan bestemme hva som skal skje dersom en enhet ikke er “compliant”. For å gi brukerne en beskjed dersom enheten dens ikke følger kravene, kan en konfigurere at det skal sendes ut en e-post til brukeren.

Under **Message tamplate,** velg en passende template. Dersom du ikke har noen template, kan du gå til neste punkt for å se hvordan en setter opp dette. Legg også til IT-avdelingen under **Additional recipients** slik at de kan bli varslet om eventuelle overtredelser.



Velg så at alle brukere må følge denne policyen.

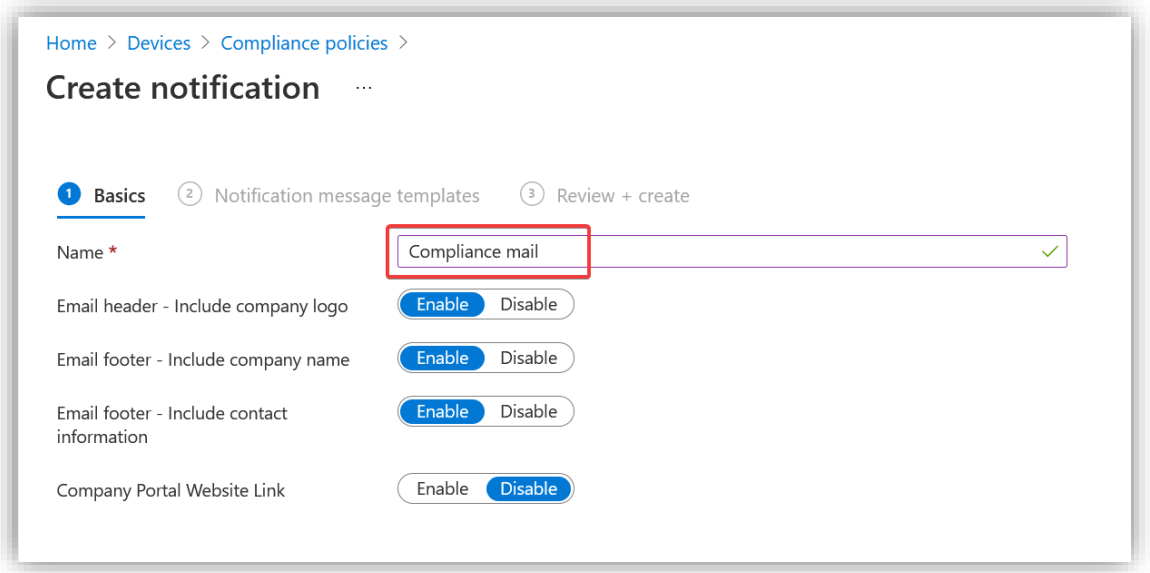


Trykk så på **Review + create** for å fullføre opprettelsen av policyen

3.6.4.1 Lag en compliance e-post

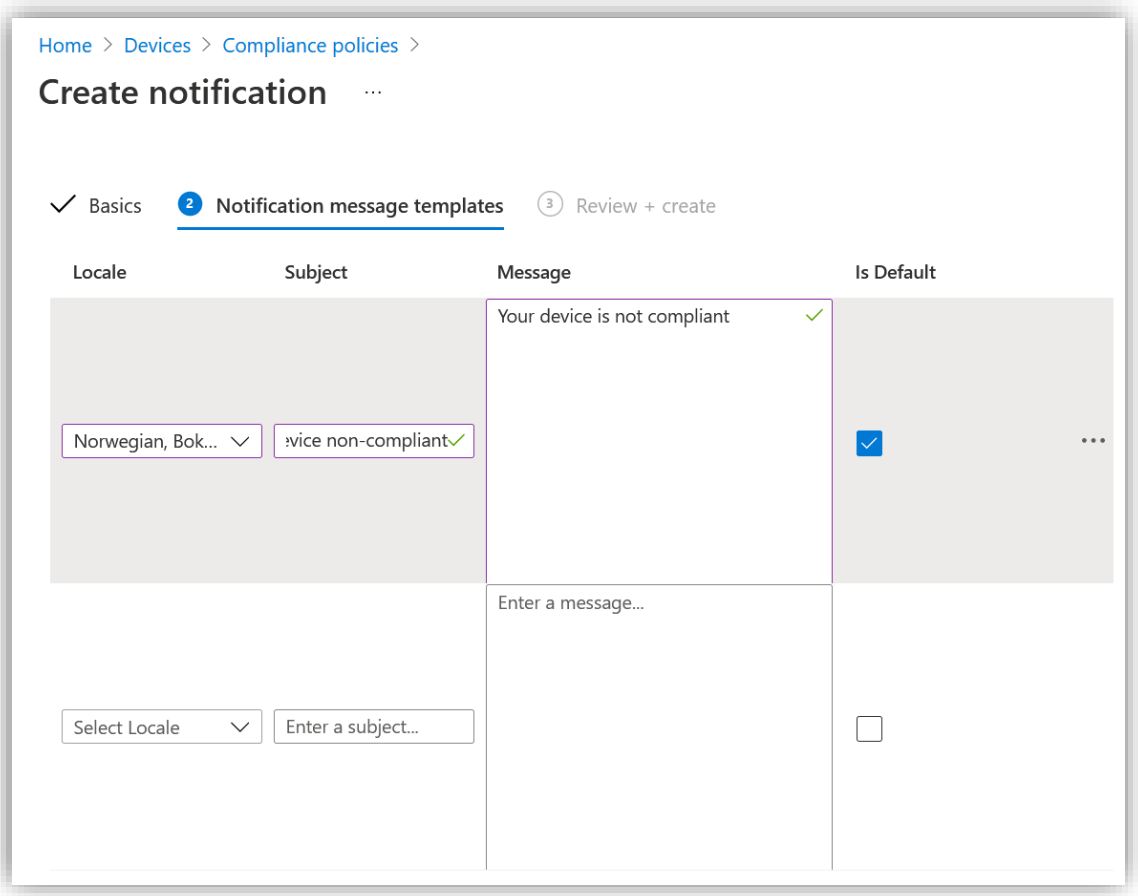
En compliance e-post er en e-post som blir sendt dersom en enhet ikke er compliant – enheten tilfredsstiller altså ikke de kravene som er satt i compliance policyen.

I **endpoint manager admin center**[9] Under **Home > Devices > Compliance policies > Notifications,** trykk på **Create notification**. I dette eksempelet er ikke en slik e-post særlig nyttig da brukeren selv ikke har mye kontroll over enheten. Man kan dog sende e-posten til andre parter som raskt trenger å vite om en enhet ikke er compliant.



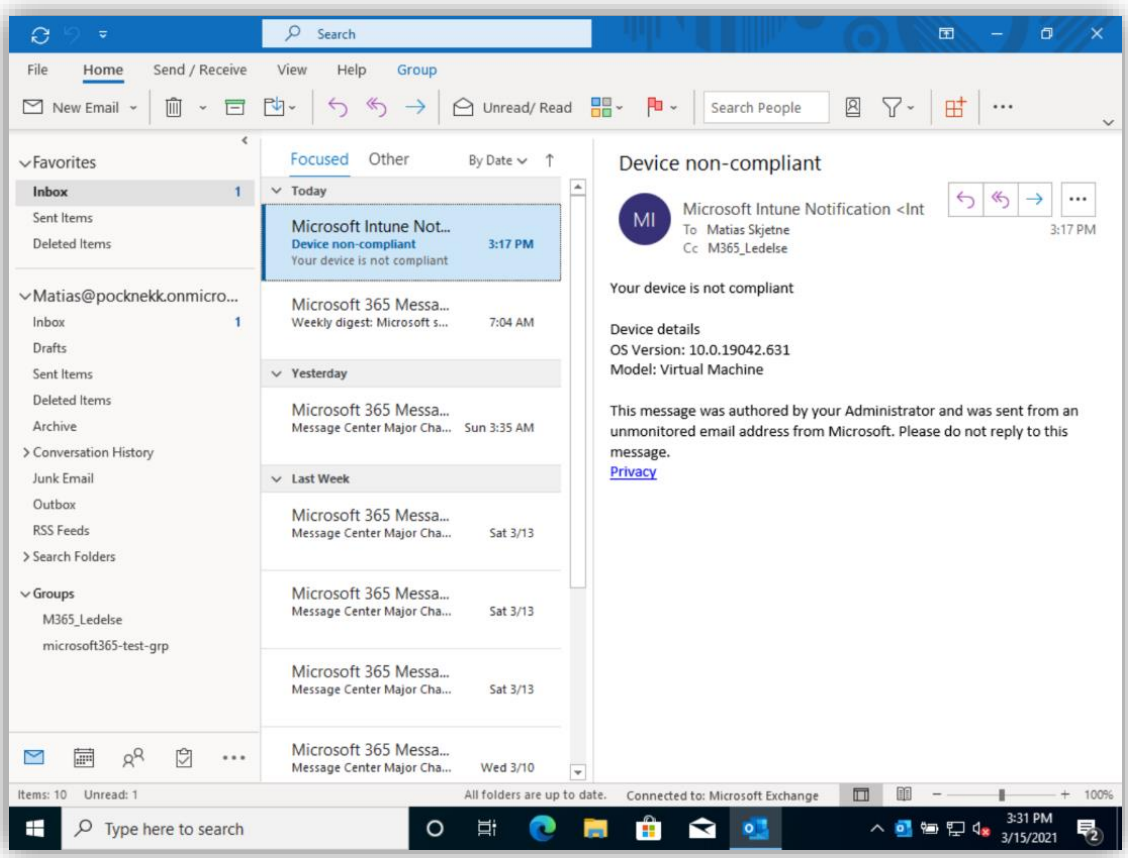
[9] https://endpoint.microsoft.com/?ref=AdminCenter#home

Lag e-posten som sendes til brukeren.



Fullfør ved å gå til **Review + create** og trykk på **Create.**

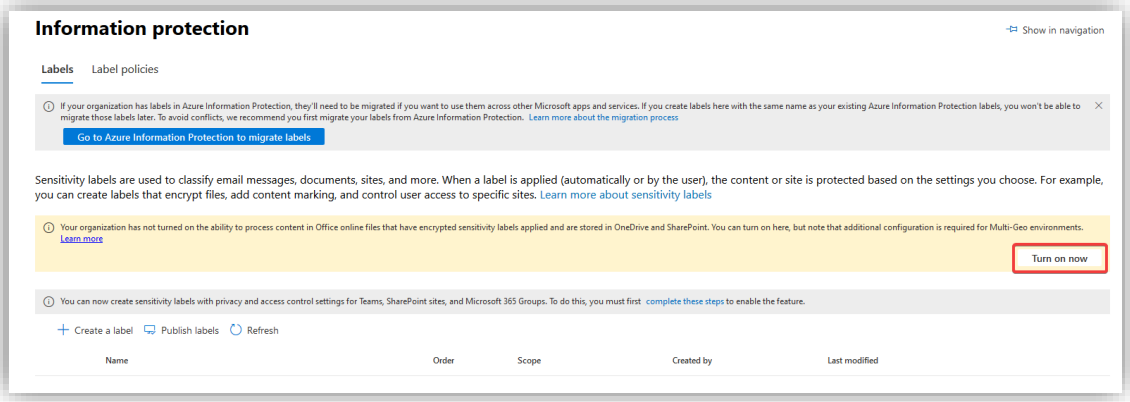
Her har brukeren fått e-posten.



3.7 Information Protection

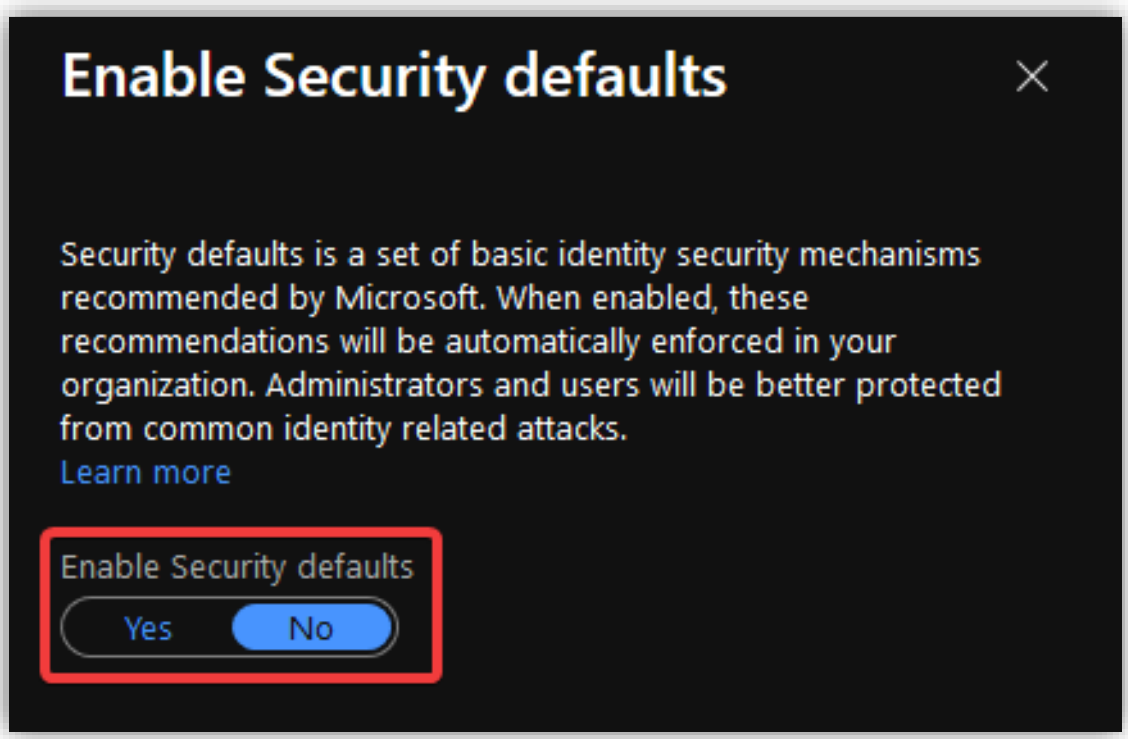
For å kunne ha bedre kontroll på all informasjon i bedriften tas **Azure Information Protection** i bruk. Dette lar oss merke dokumenter med en sensitivitets grad (sensitivity label). Graden bestemmer hvor et dokument kan sendes og hvem som kan se det. Generelle dokumenter kan ses, åpnes og redigeres av alle, mens konfidensielle dokumenter kun kan åpnes av bestemte grupper. Man kan også lage grader som kun er tilgjengelige for spesifikke avdelinger i bedriften. Administrasjonen kan ha egne grader for lønnsdokumenter, for så å gi tilgang til den personen som skal motta lønnslippen. Konfidensialiteten bevares ved å kryptere dokumentene slik at kun de med rett nøkkel kan aksessere den.

For å effektivt bruke Information Protection må man aktivere muligheten for å prosessere filer i **Office Online** og sette labels i **SharePoint** og **OneDrive**. Detter gjøres under **Information Protection** menyen i **Compliance**-portalen[10]



[10] https://compliance.microsoft.com/informationprotection?viewid=sensitivitylabels

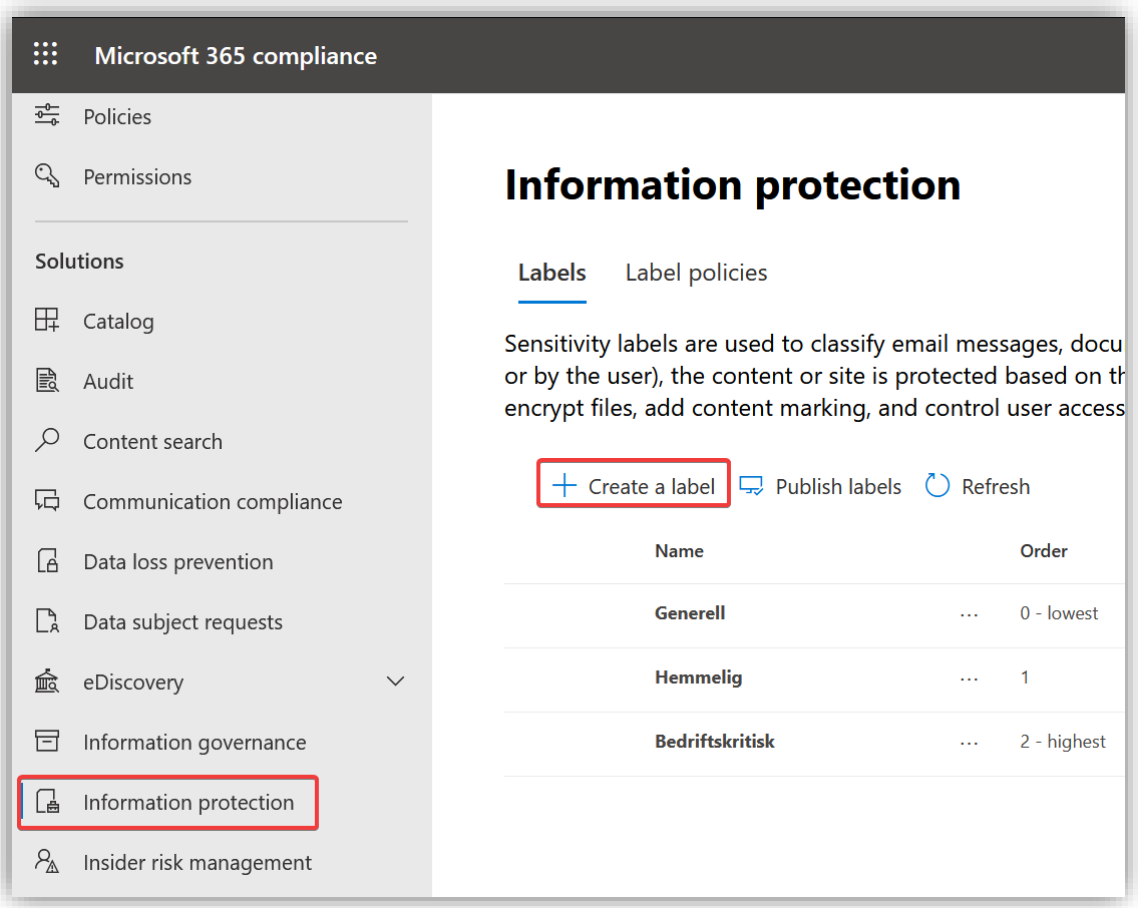
Skru av **Security Defaults**.



3.7.1 Opprette sensitivity lables

For å styre hvem som kan aksessere dokumenter og hvor de kan ta veien gjennom systemet, brukes **sensitivity lables**. Dette er lables som brukerne selv setter på dokumentene for å klassifisere de og evt. aktivere kryptering dersom dokumentet ikke skal være offentlig.

Inne på **Compliance** portalen gå til **Information Protection** menyen[11] og velg **Create Label.**



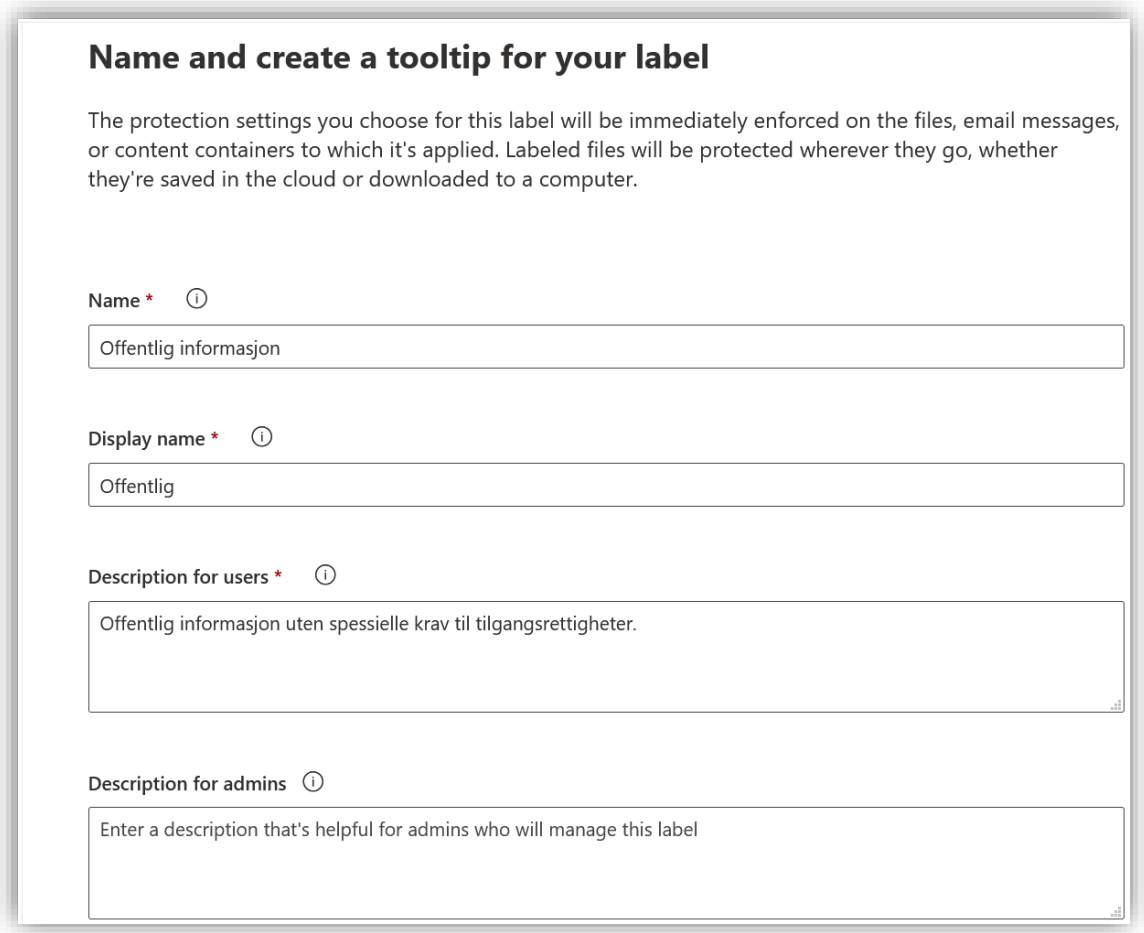
I dette eksemplet opprettes seks labels: Offentlig, Privat, konfidensiell, Strengt Konfidensiell, Ledelse, Helsepersonell.

[11] https://compliance.microsoft.com/informationprotection?viewid=sensitivitylabels

3.7.1.1 Offentlig

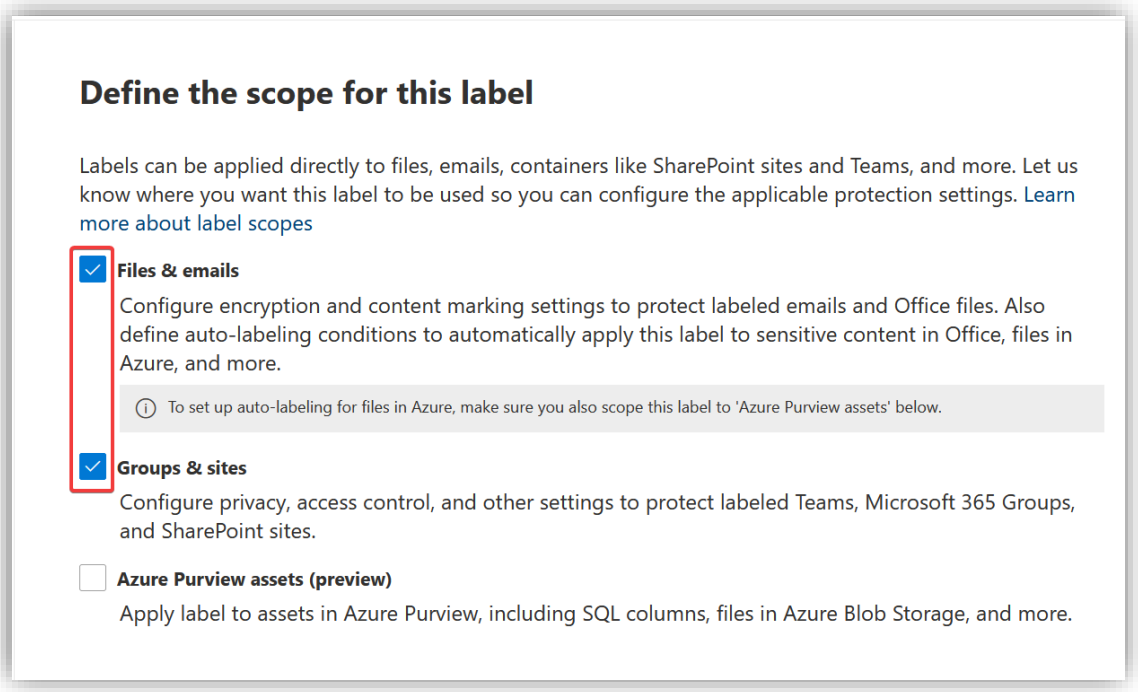
Den offentlige labelen er for dokumenter som ikke trenger noen adgangsstyring eller begrensning på deling og lagring. Dette er dokumenter som ikke medfører konsekvenser om de forsvinner ut av bedriften.

Gi labelen et navn og en beskrivelse.

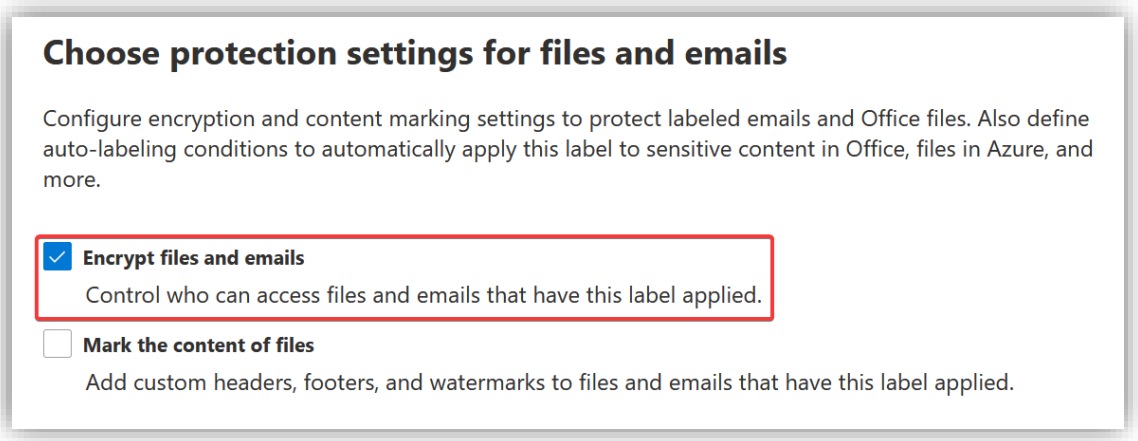


1 Dette steget er likt for alle labels og vises kun én gang

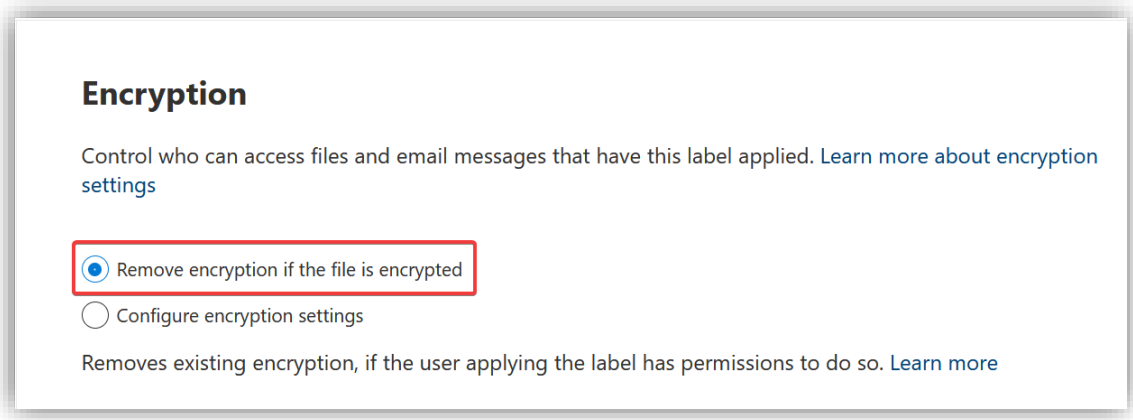
Velg at labelen skal gjelde for **Files & emails** og **Groups & sites.**



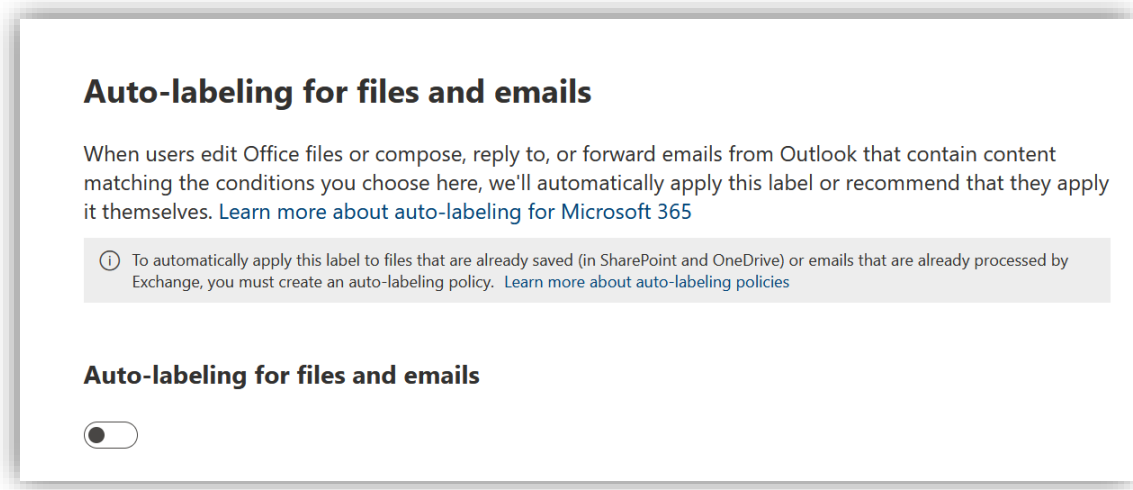
Velg **Encrypt files and emails**.



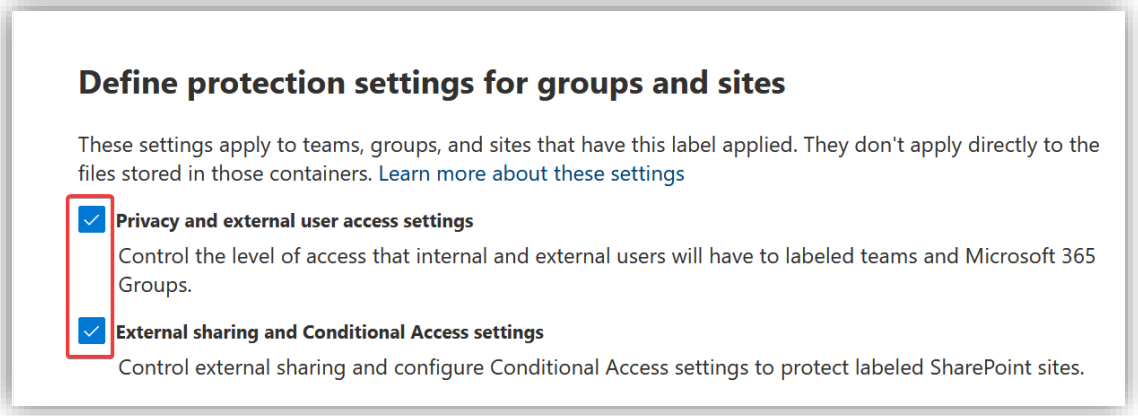
Offentlige filer trenger ikke kryptering, derfor velges det at dette skal fjernes om filen allerede er kryptert. Brukeren må ha rettigheten **Full Controll** for å kunne fjerne kryptering på en fil slik at en bruker som mottar en kryptert fil ikke uten videre kan fjerne krypteringen.



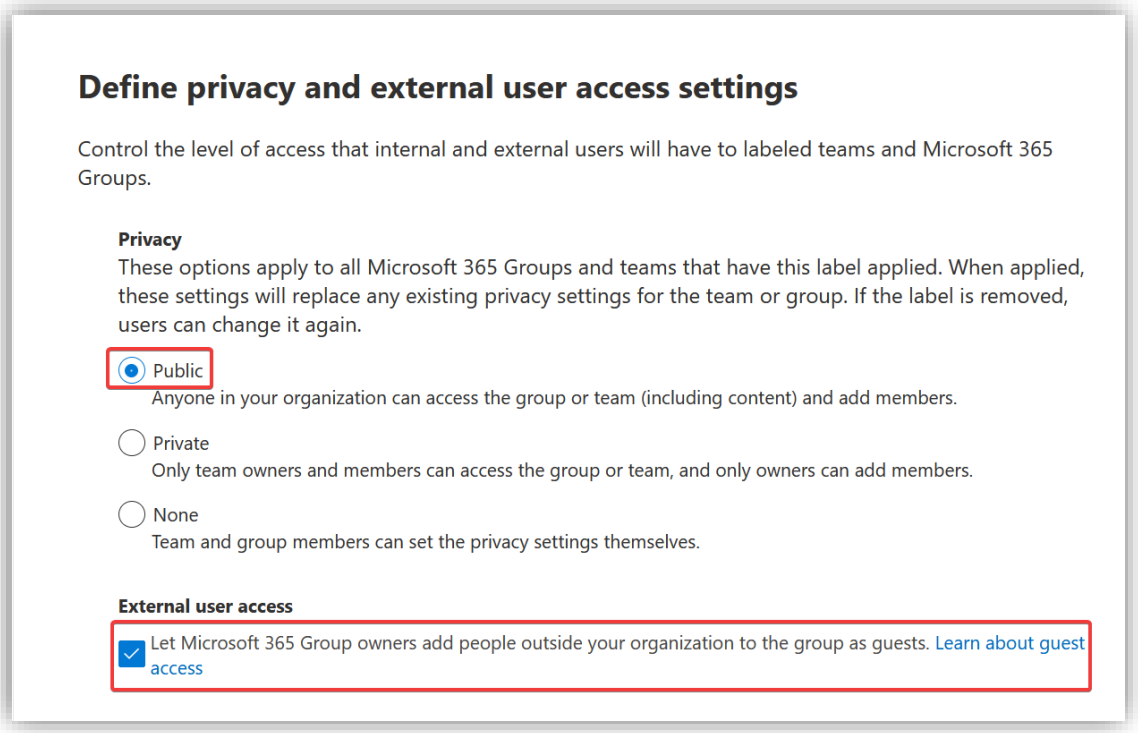
Auto-labeling skal være av.



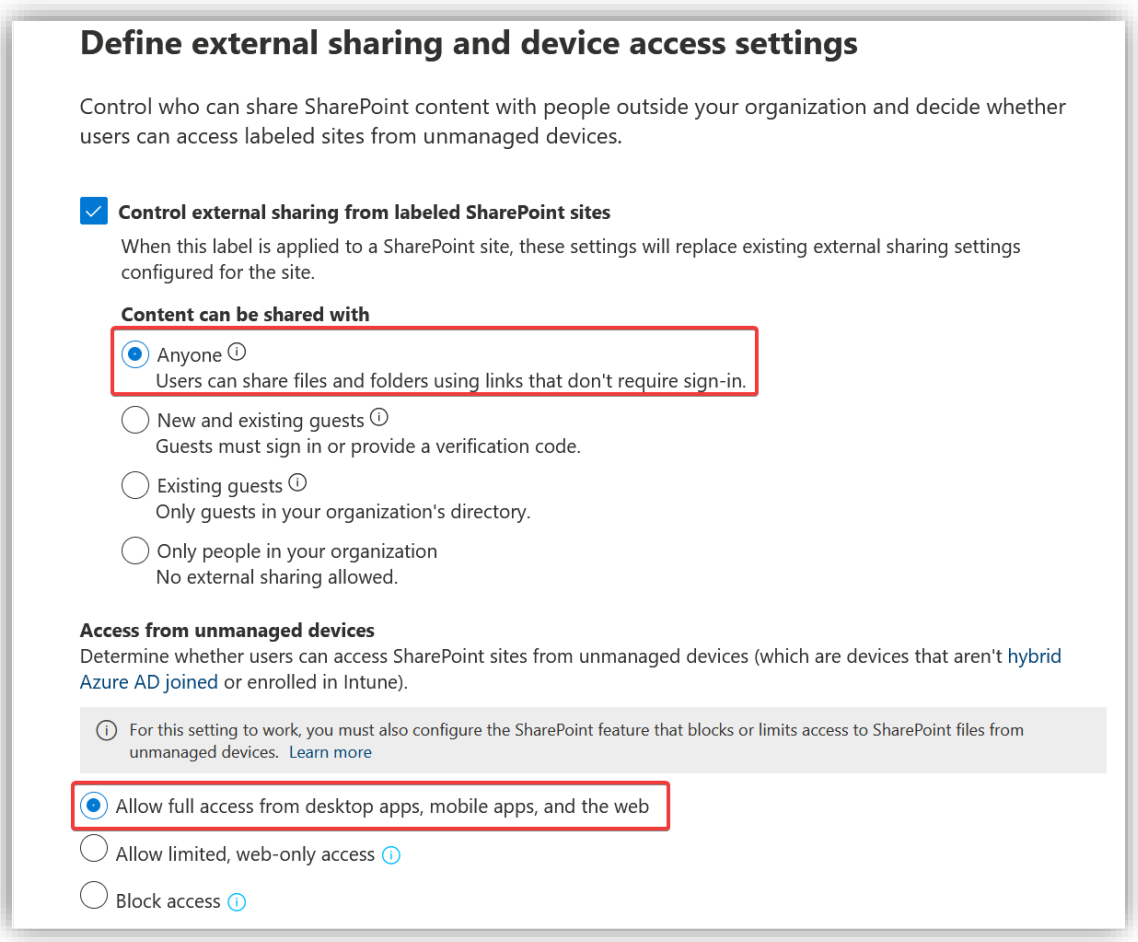
Skru på kontroll for både **Privacy and external user access settings** og **External sharing and conditional Access settings.**



SharePoint sites med denne labelen skal være **public** og eierne av siten skal kunne invitere personer utenfor bedriften som gjester.



Velg at hvem som helst som får tilsendt en link til offentlige SharePoint sites kan se innholdet. Velg også at det ikke settes restriksjoner på hvilke enheter man kan se innholdet fra.

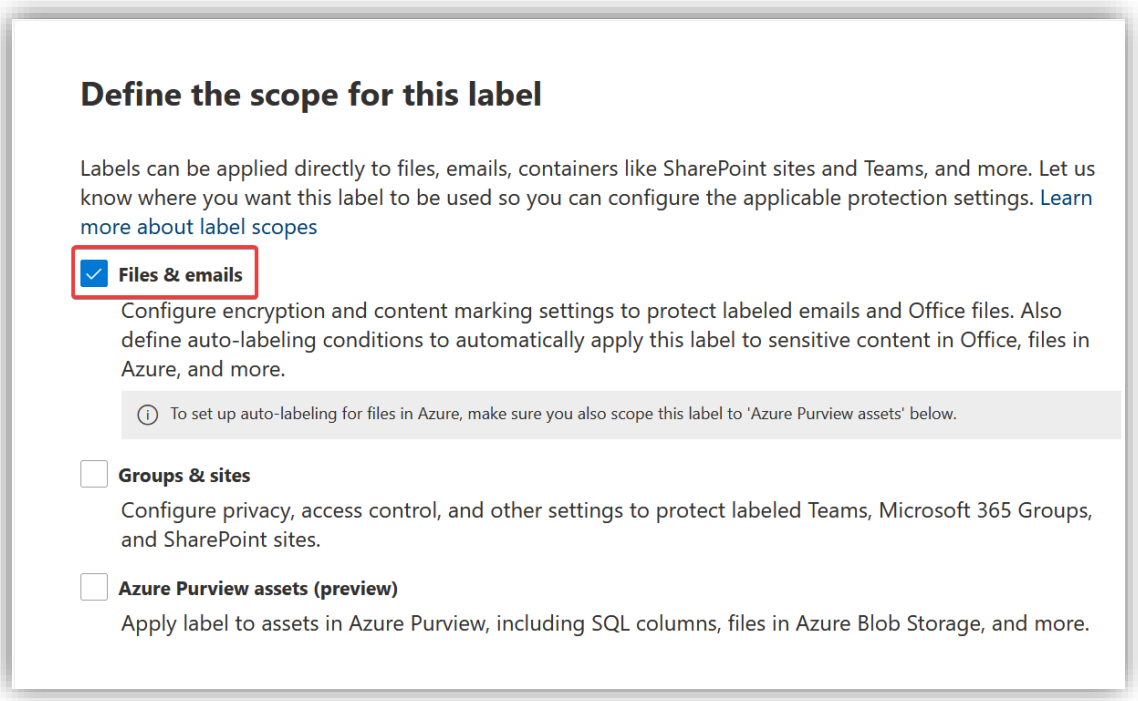


3.7.1.2 Privat

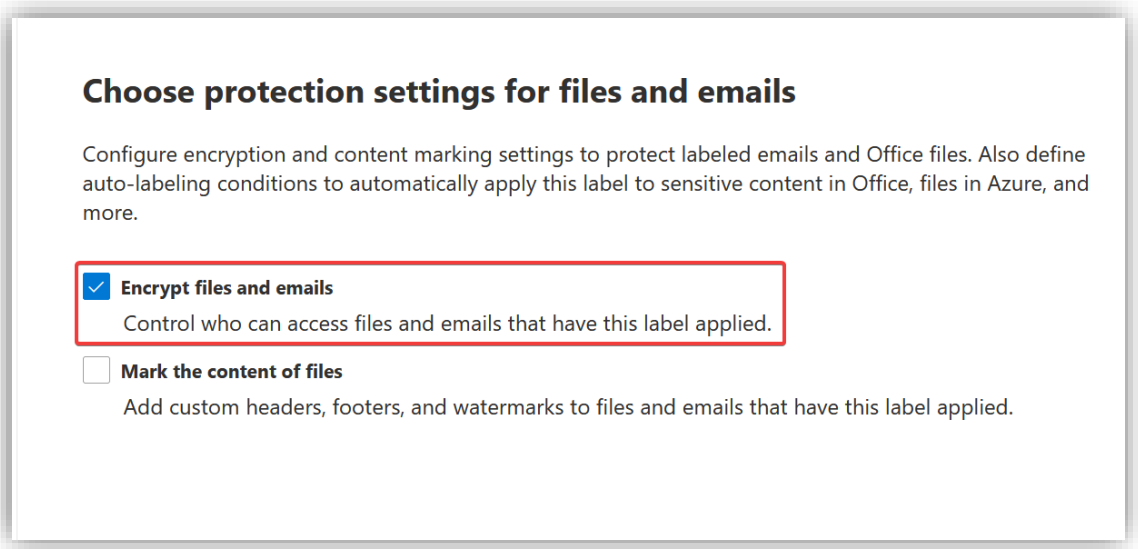
Lag en ny label.

Dette skal være en privat label som de ansatte kan bruke på egne filer og er ikke knyttet til bedriftens drift. Bare eieren av filen kan åpne filen og se innholdet.

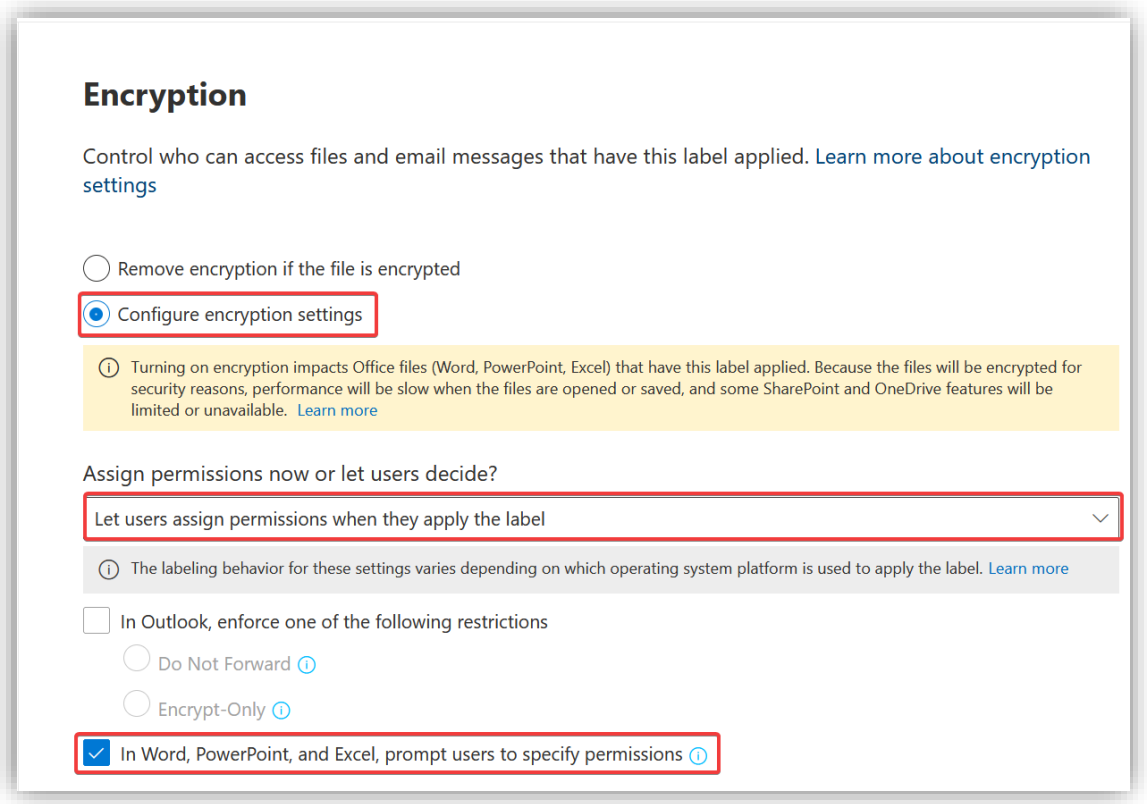
Denne labelen gjelder bare for filer og kan ikke settes på SharePoint sites.



Skru på kryptering og tilgangskontroll.



Velg **Configure ecryption settings** og skru på at brukeren selv kan velge hvilke tilganger hen har lyst til å gi andre personer. Dette gir brukeren frihet til å dele private filer med andre i bedriften.



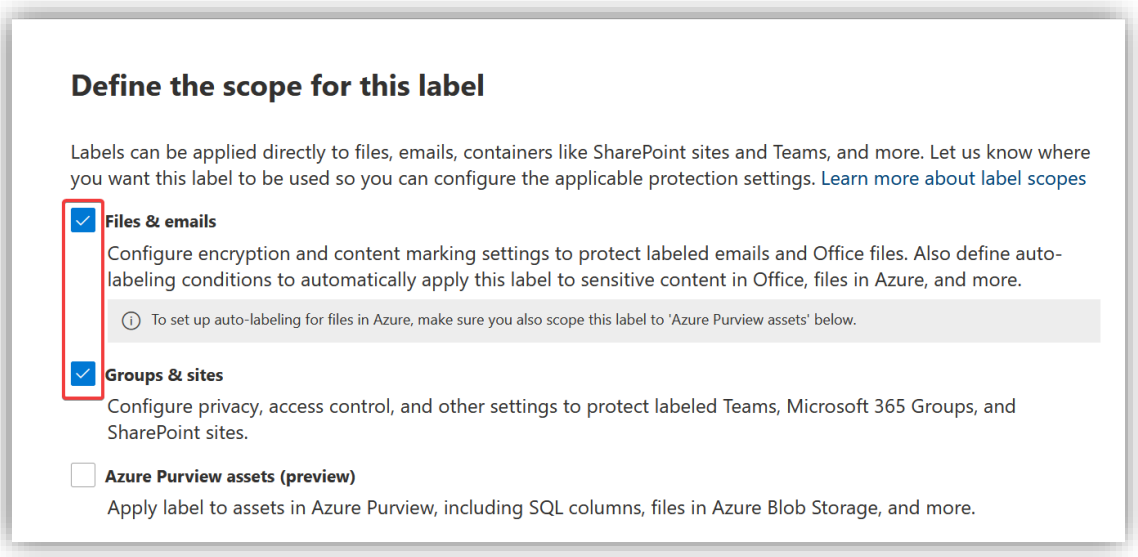
Auto-labeling skal ikke være på for denne labelen. Etter man har gått videre er det bare å se over valgene og lage labelen.

3.7.1.3 Konfidensiell

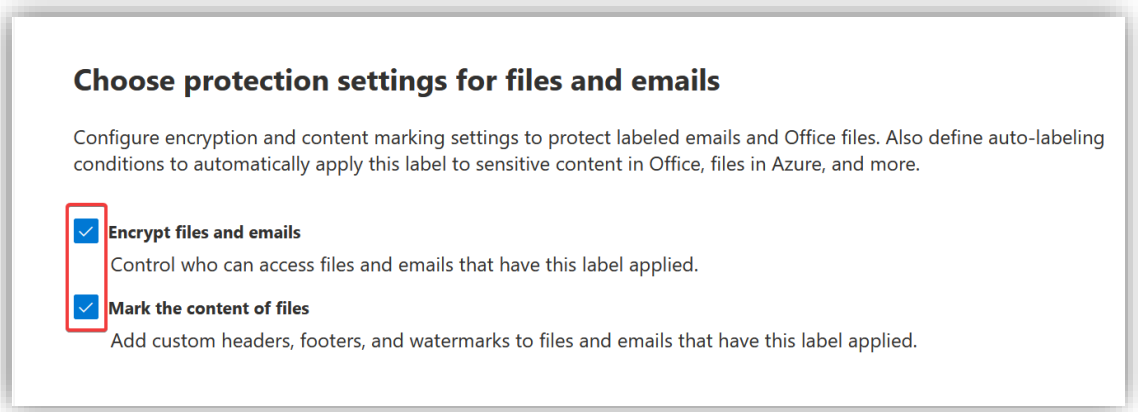
Lag en ny label.

Konfidensielle filer krever ekstra sikkerhet for at uvedkommende ikke skal få tilgang. Denne brukes til deling av filer innad i bedriften – filer det er viktig at ikke havner hos utenforstående.

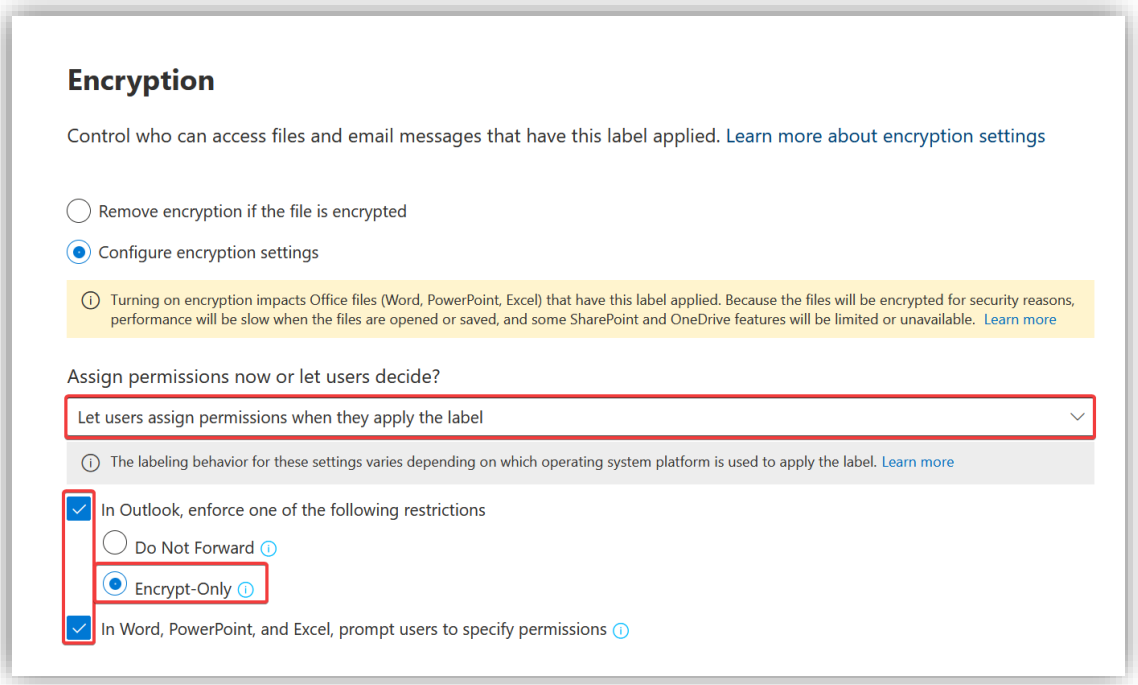
Denne labelen skal kunne settes på filer og sites.



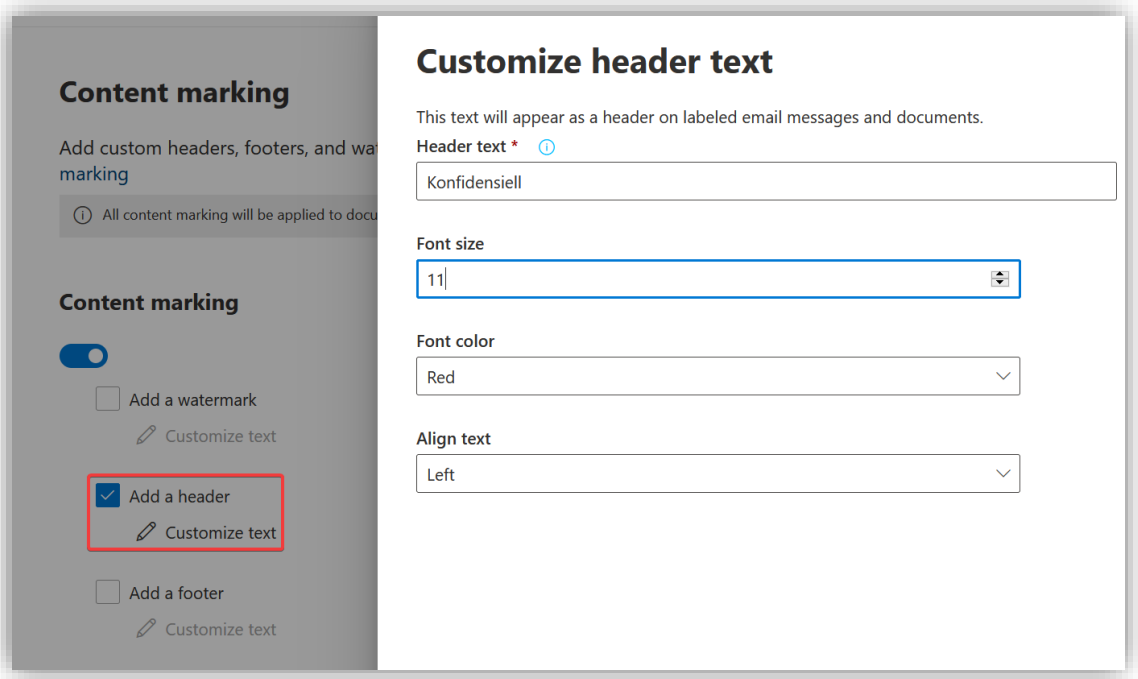
Skru på kryptering og markering av filer.



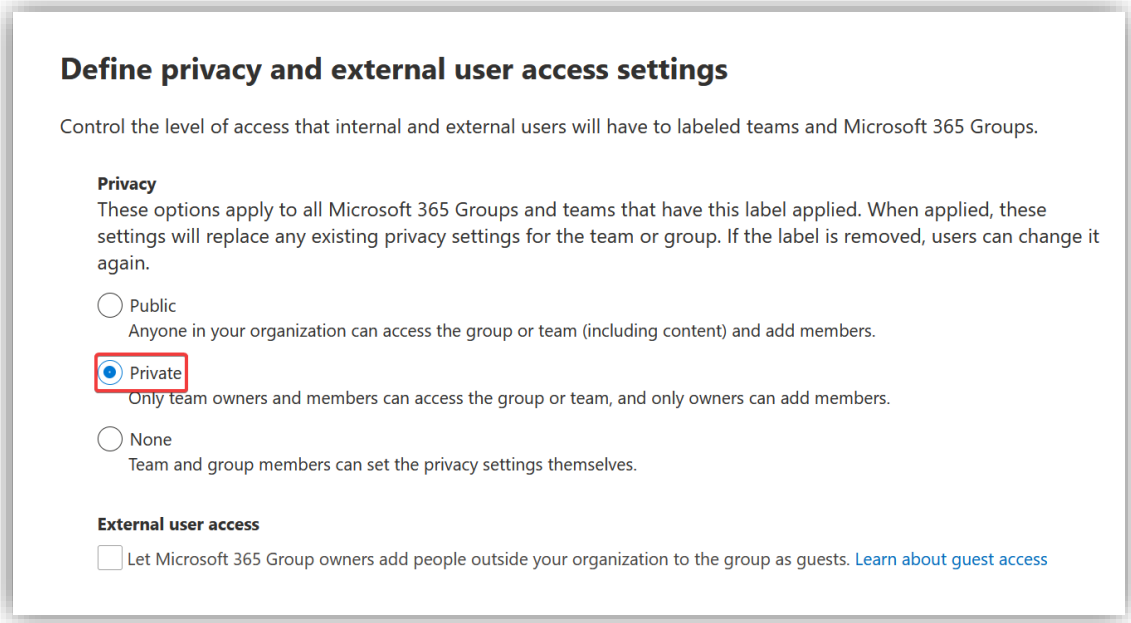
Konfidensielle filer skal fortsatt kunne deles og brukeren må selv velge hvem som skal få tilgang til materialet. Filene blir kryptert og kun de med tilgang kan åpne filen.



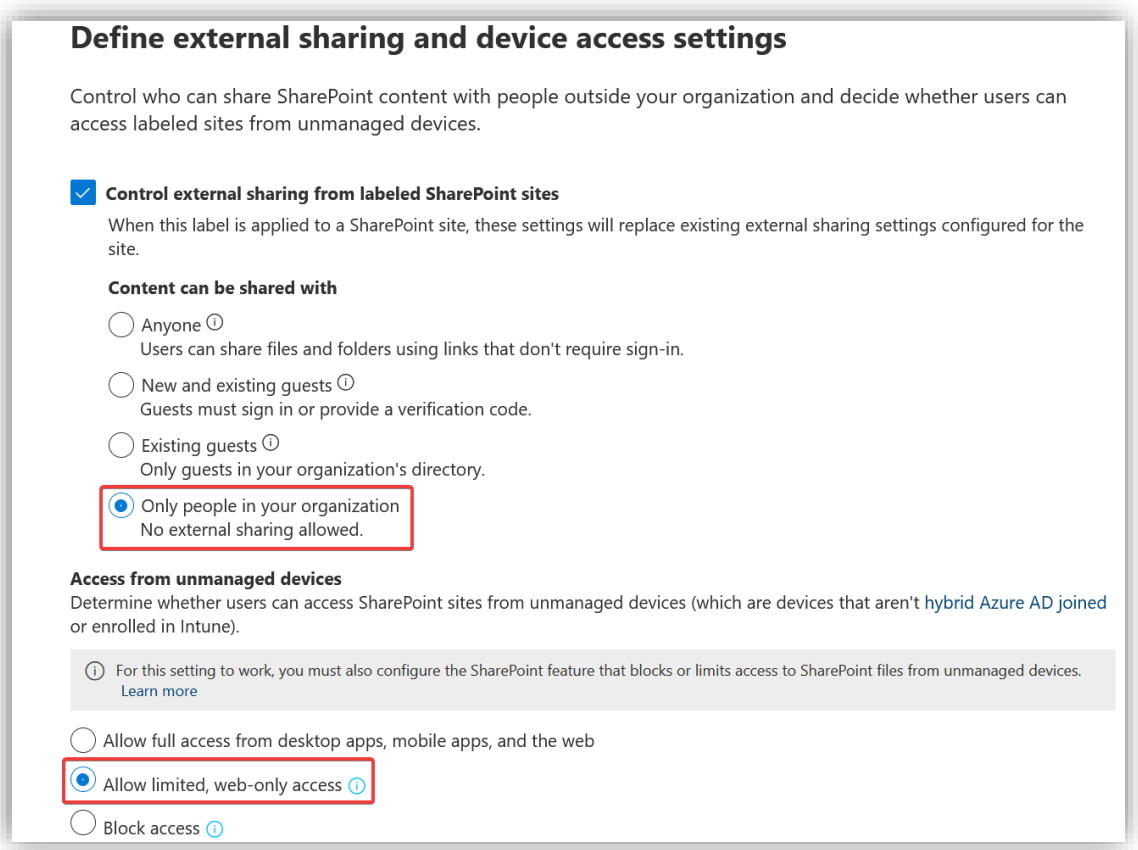
Skru på merking av innhold og velg **Add a header**. Fyll ut skjema for merking og trykk **Save.** Innholdet får nå en klar merknad om at det er konfidensiell informasjon.



Velg at Sites med denne labelen skal være privat, slik at ingen som ikke er invitert kan bli med. Gjester skal ikke kunne legges til.



Deling skal kun finne sted med medlemmer i organisasjonen og enheter som ikke er compliant kan kun nå Siten fra web.



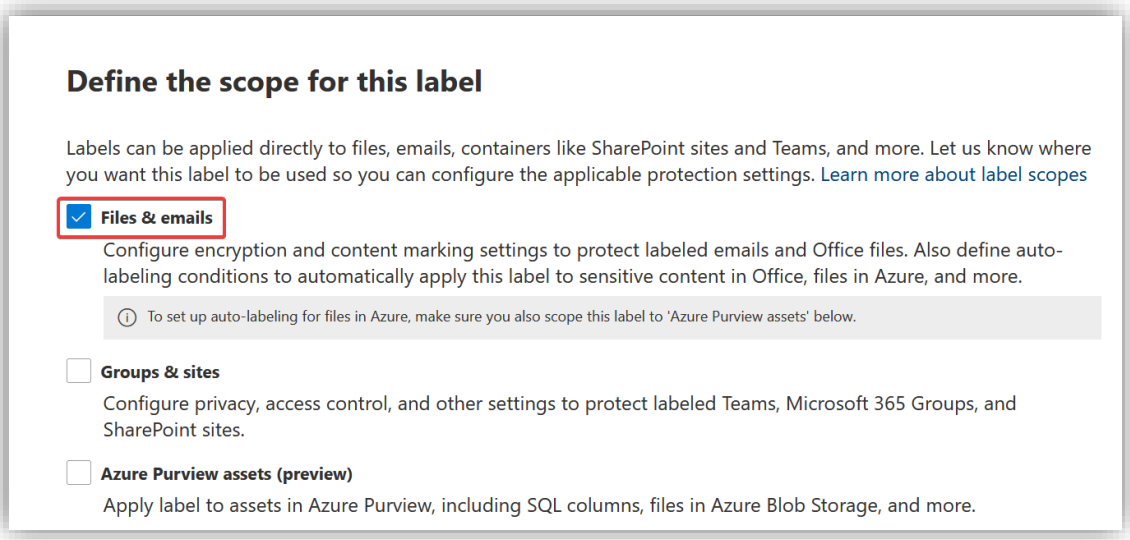
Tilslutt, se over og trykk **Create label.**

3.7.1.4 Administrasjon

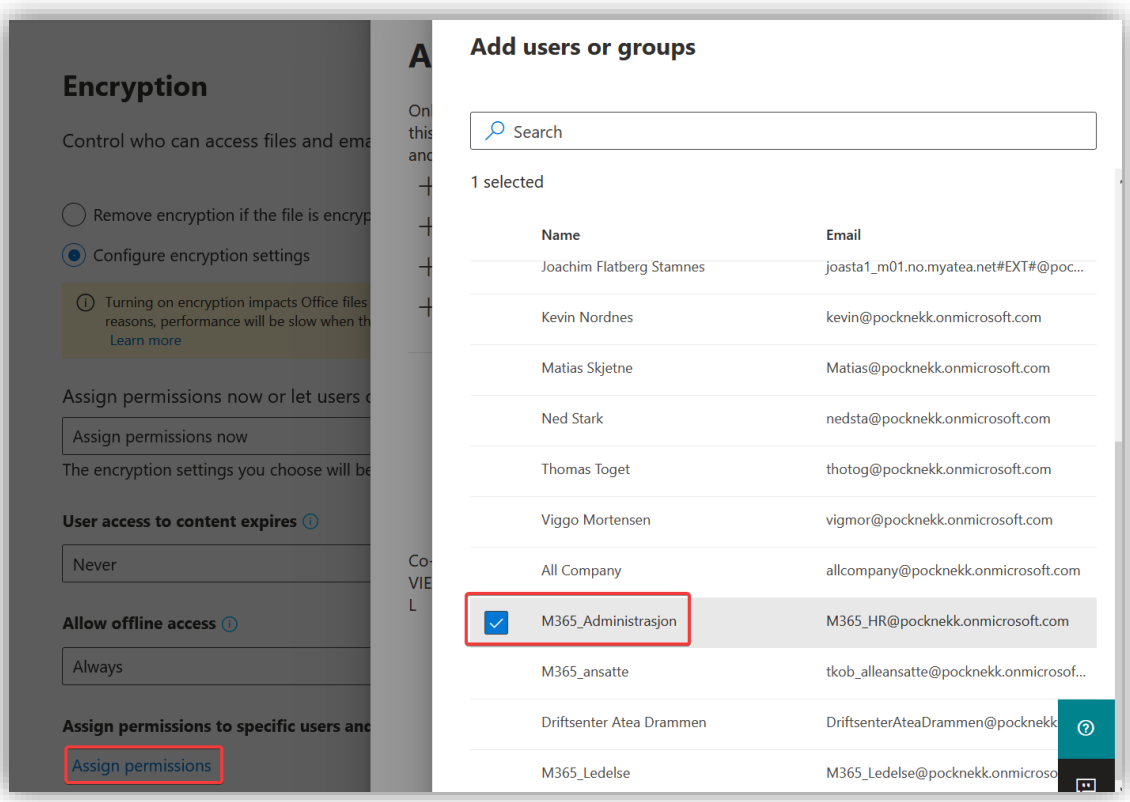
Lag en ny label.

Denne labelen settes for generelle filer og dokumenter som kun administrasjonen skal ha tilgang til. Spesielle typer filer som administrasjonen lager som f.eks. lønnslipper og avviksrapporter har sine egne sublables.

Labelen skal kun påvirke filer og e-poster.



Under **Encryption** velg **Assign permissions now** og velg **Assign permission.** Velg så **Users and Groups** og finn administrasjonsgruppen. Når man nå setter labelen på et dokument eller e-post vil hele administrasjonsgruppen få tilgang.

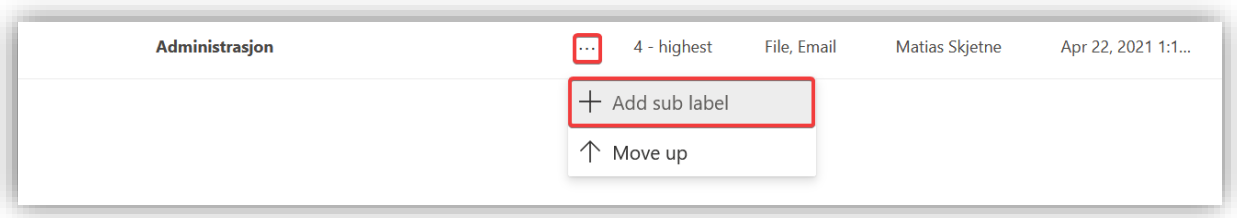


Se over til slutt og trykk **Create.**

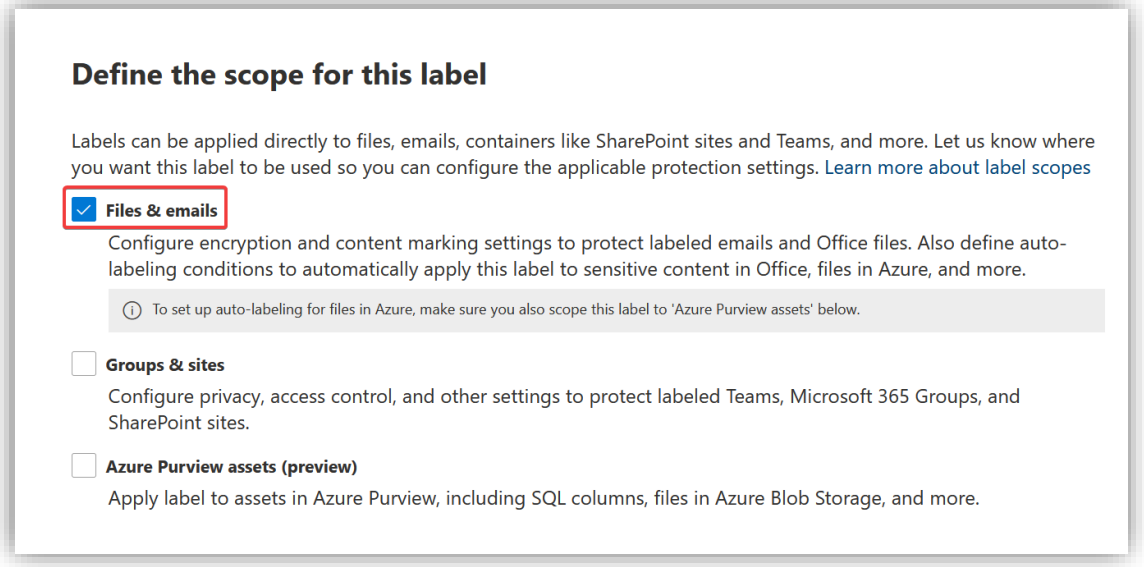
3.7.1.4.1 Lønnsslipp

Lønnslipper er spesielle administrasjons dokumenter som krever egen tilgangskontroll. Denne labelen blir opprettet som sublable av administrasjons labelen.

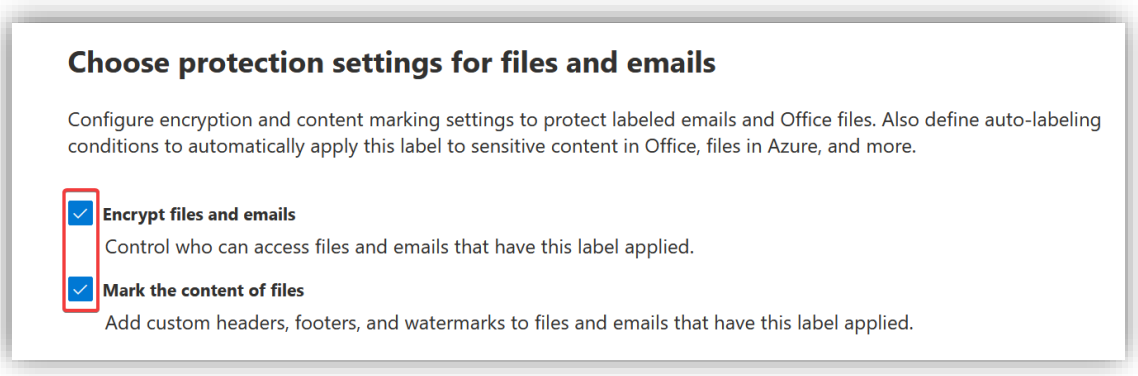
Opprett en sublable under Administrasjon, og fyll ut navn og beskrivelse.



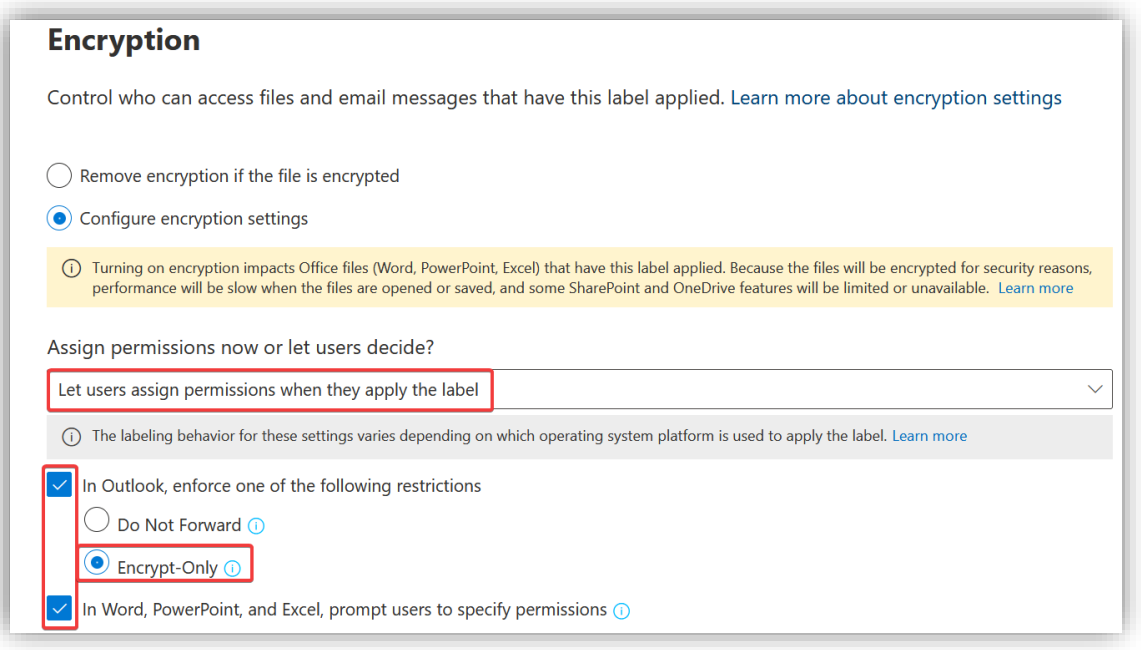
Scopet til labelen skal væer **Files & emails.**



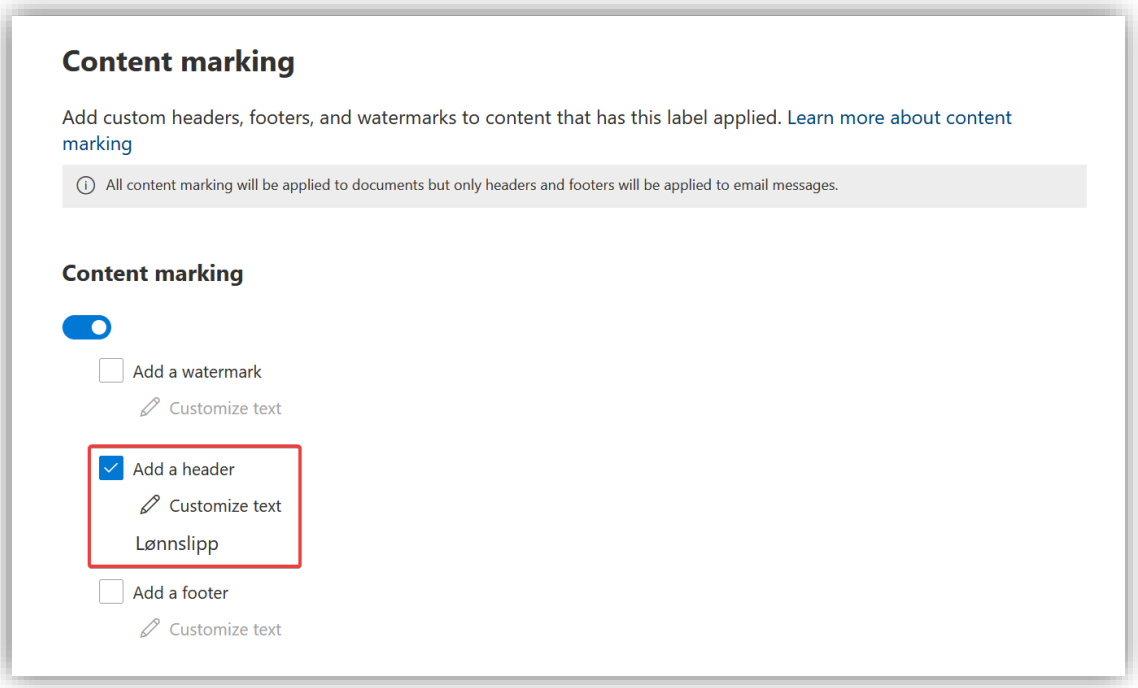
Filene skal markeres som lønnslipper og krypteres.



Tilganger må settes manuelt basert på hvem som skal motta lønnslippen, og innholdet krypteres. Selv om en lønnslipp blir sendt til feil ansatt vil personen ikke kunne åpne den.



Slippen skal markeres med en header som sier «lønnslipp».

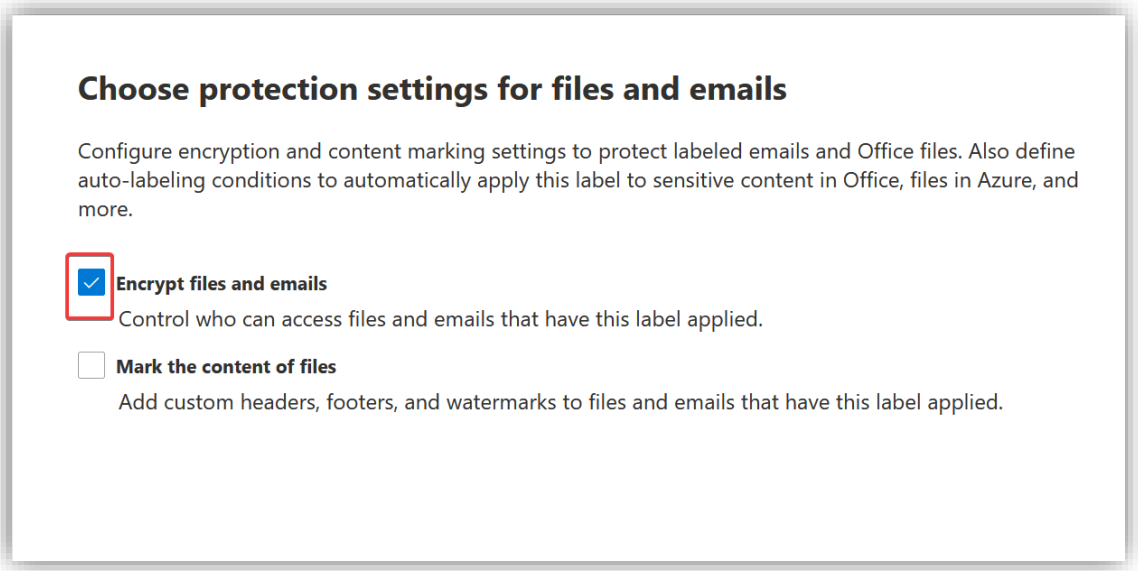


Tilslutt trykk **Create label**

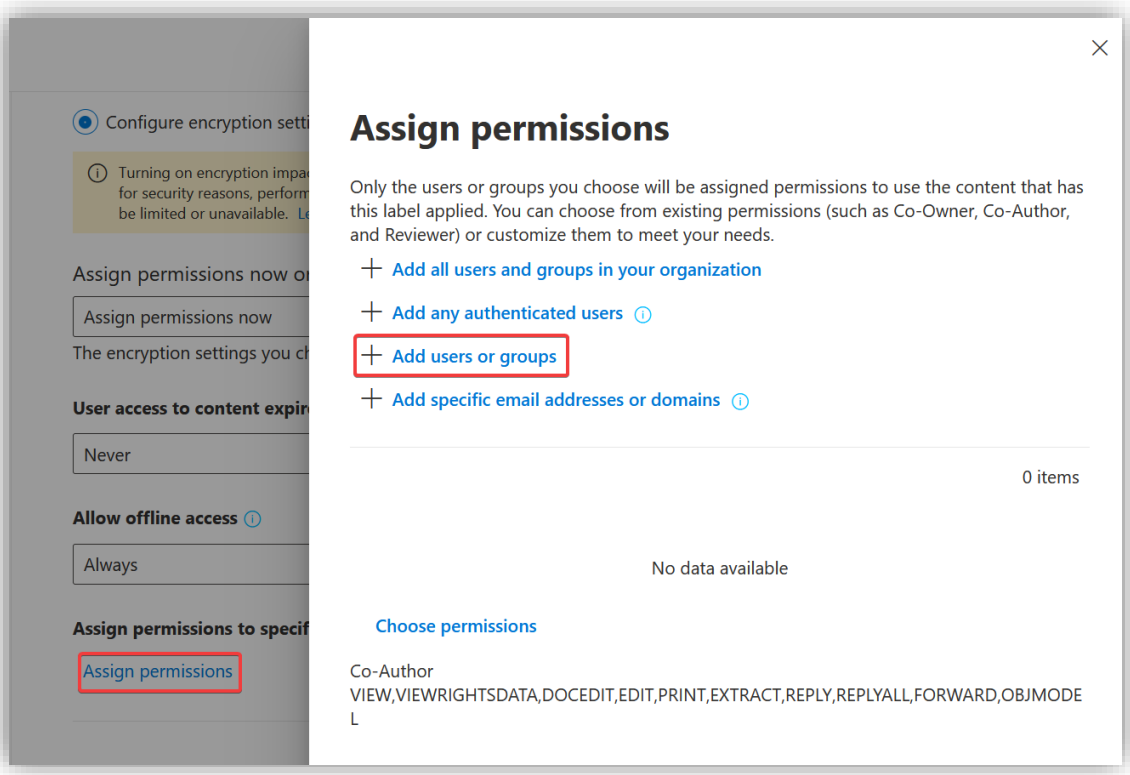
3.7.1.5 Ledelse

Lag en ny label.

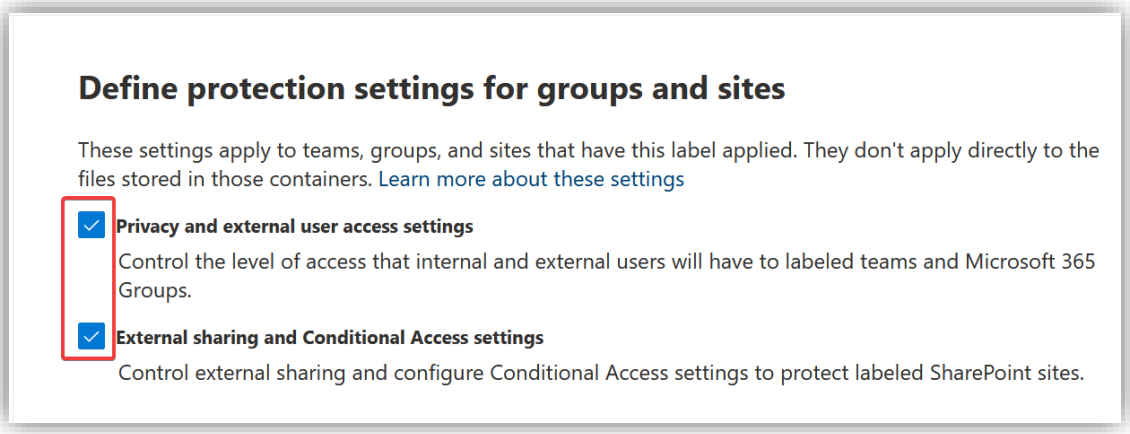
Ledelsens filer skal krypteres og skal ikke kunne lagres hvor som helst. Velg **Encrypt files and emails**



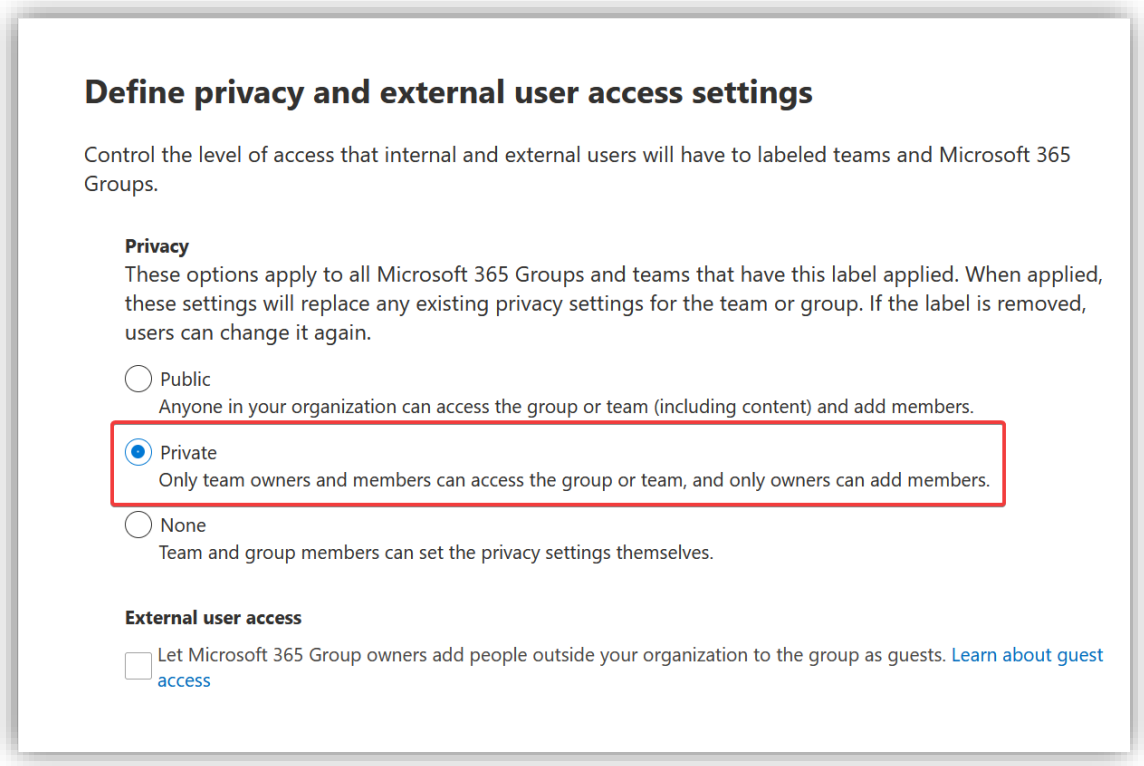
Velg **Assign permissions**, **Add users and groups** og til siste velg ledelse gruppen fra menyen. **Permission** skal stå som **Co-Author**.



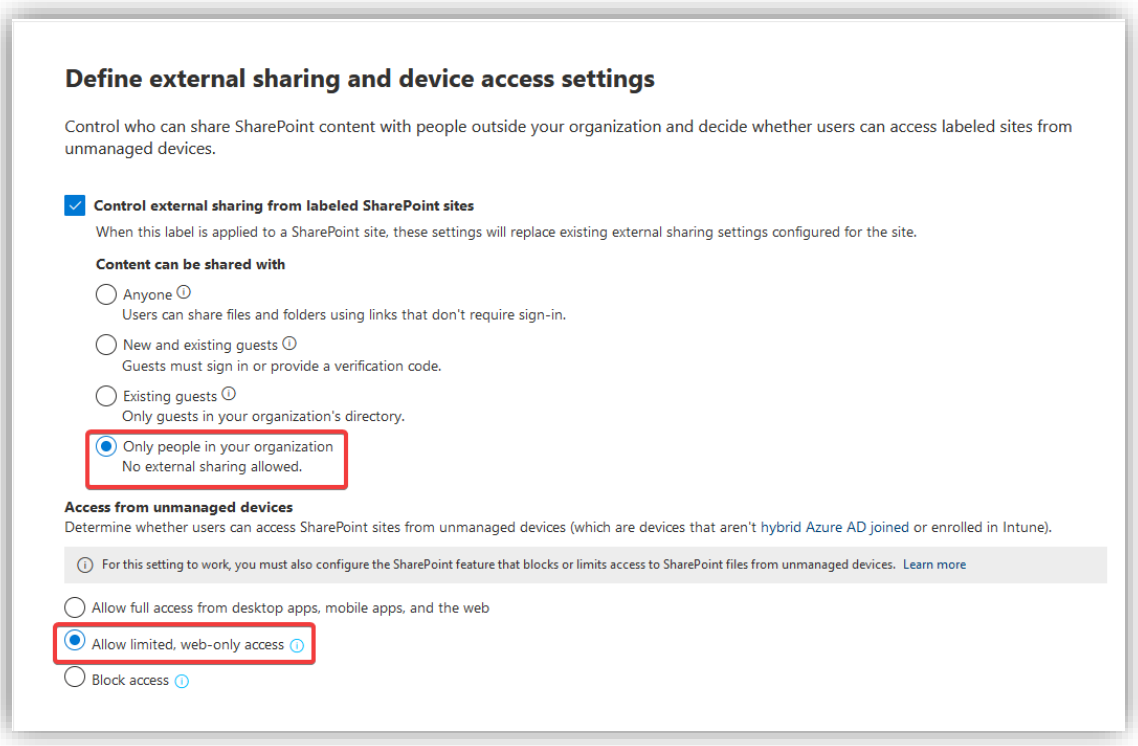
Hopp over **Auto-labeling** steget og velg begge alternativene på neste steg.



Sett **Privacy** til **Private**, slik at det er kun ledelsen som kan aksessere Teams og SharePoint sites som har denne labelen.



Velg **Only peple in your organization** og **Allow limited web-only access.** Ledelsen ønsker ikke å dele sine interne dokumenter med omverdenen, men de trenger kanskje å aksessere dokumenter fra maskiner som ikke er i Intune, dette får de kun lov til gjennom en nettleser.

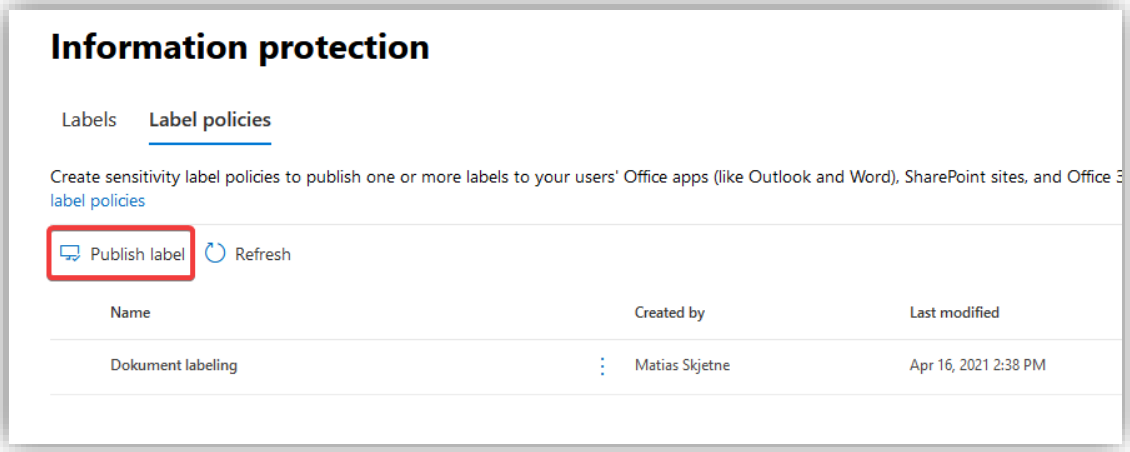


Se over valgene på siste side og trykk **Create label.**

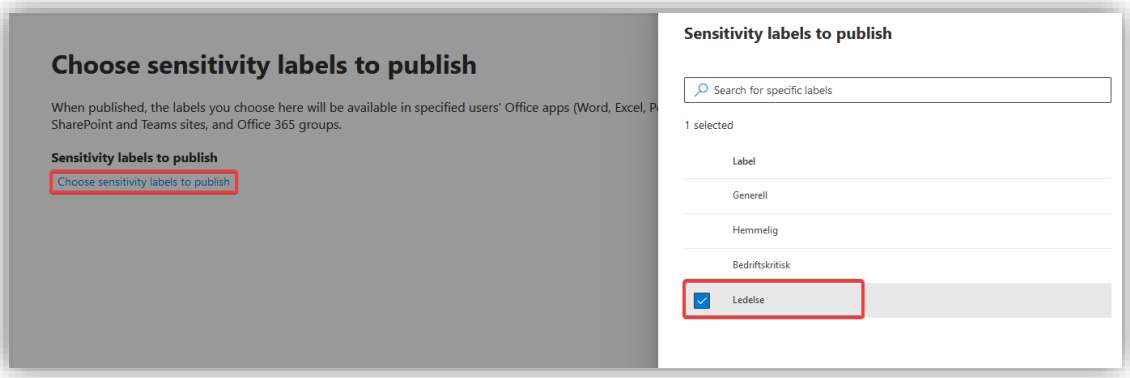
3.7.2 Label policies

Label policies brukes for å publisere labels slik at brukere kan sette dem på dokumenter. Policyene bestemmer hvem som skal få bruke et sett med lables, og flere alternativer knyttet til bruk. For eksempel kan man kreve at man må oppgi en grunn om man vil fjerne en lable fra et dokument.

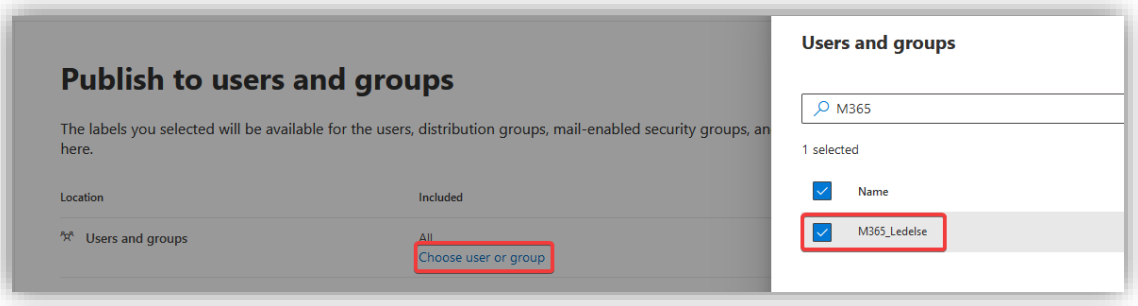
Velg **Publish label** under **Label Policies.**



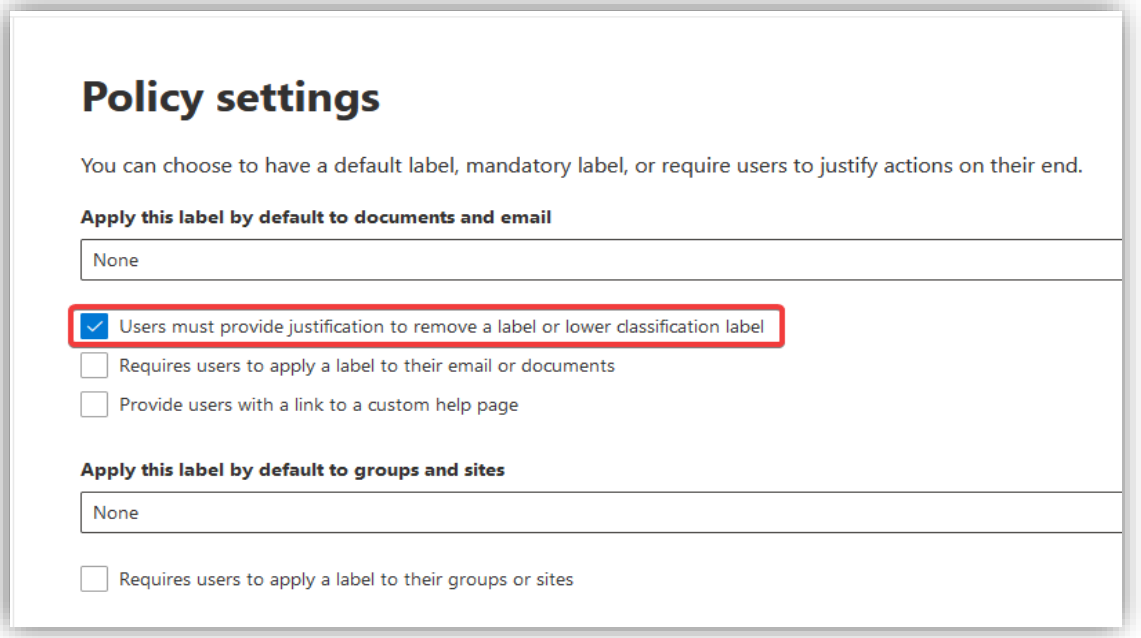
Trykk på **Choose sensitivity labels to publish** og velg **Ledelse** fra menyen.



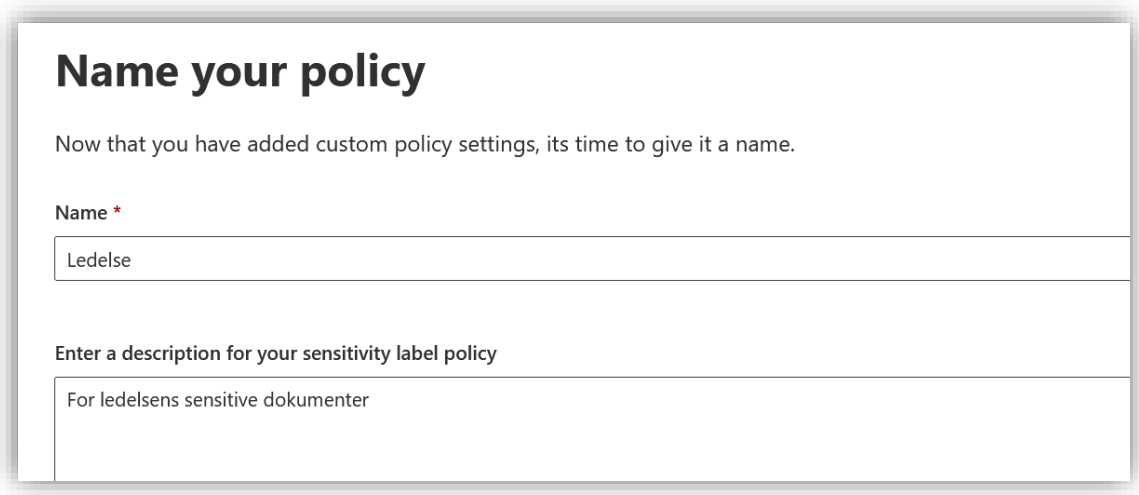
Trykk på **Choose users or group** og deretter velg brukerne som skal få bruke labelen.



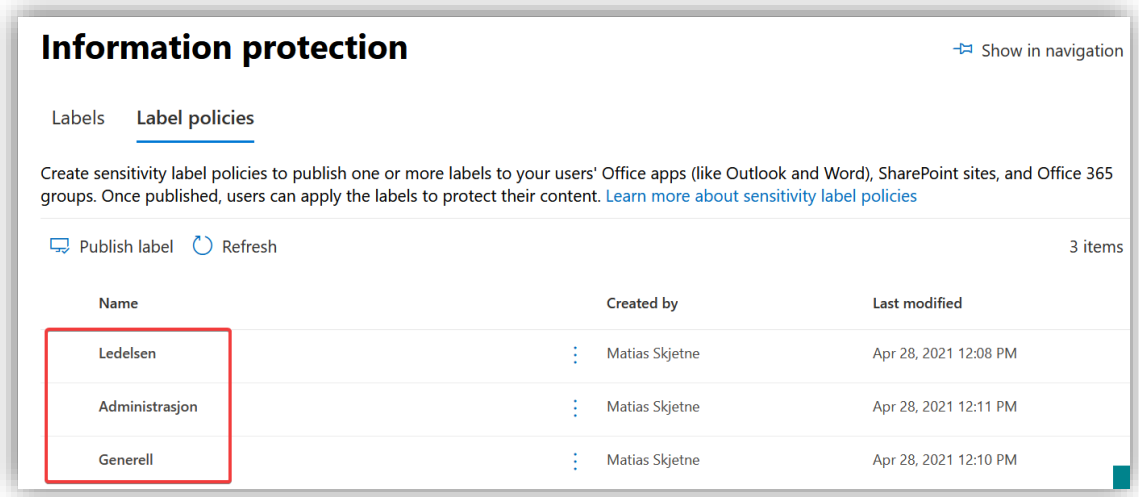
Skru på at brukerne må forklare seg om de ønsker å fjerne labelen.



Til slutt, gi policyen et navn og en beskrivelse og se over før man trykker **create.**



På samme måte lag en policy for administrasjonen og de generelle lablene. Administrasjons lablene skal kun være tilgjengelig for adminiastrasjonen mens de generelle skal være tilgjengelig for alle.

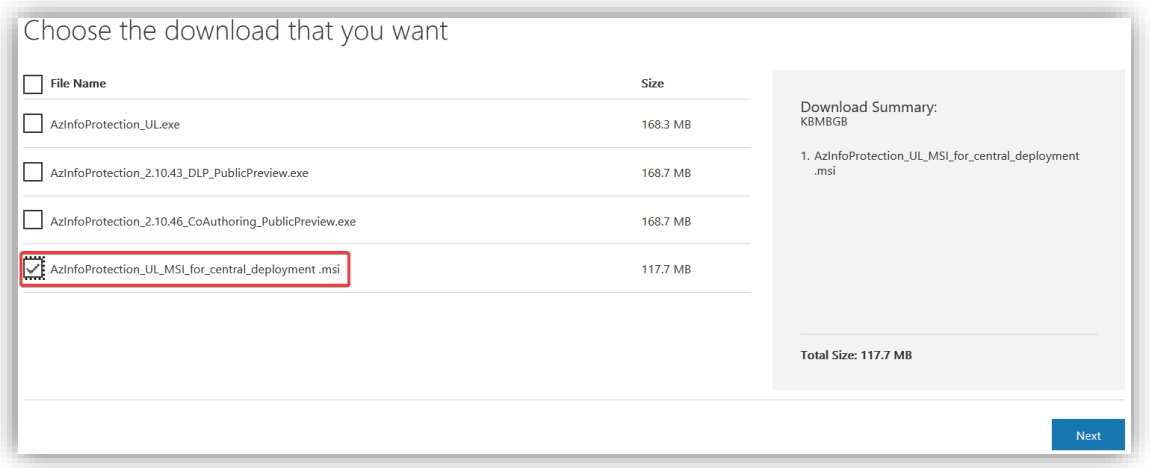


3.7.3 AIP Unified Labeling Client utrulling med Microsoft Intune

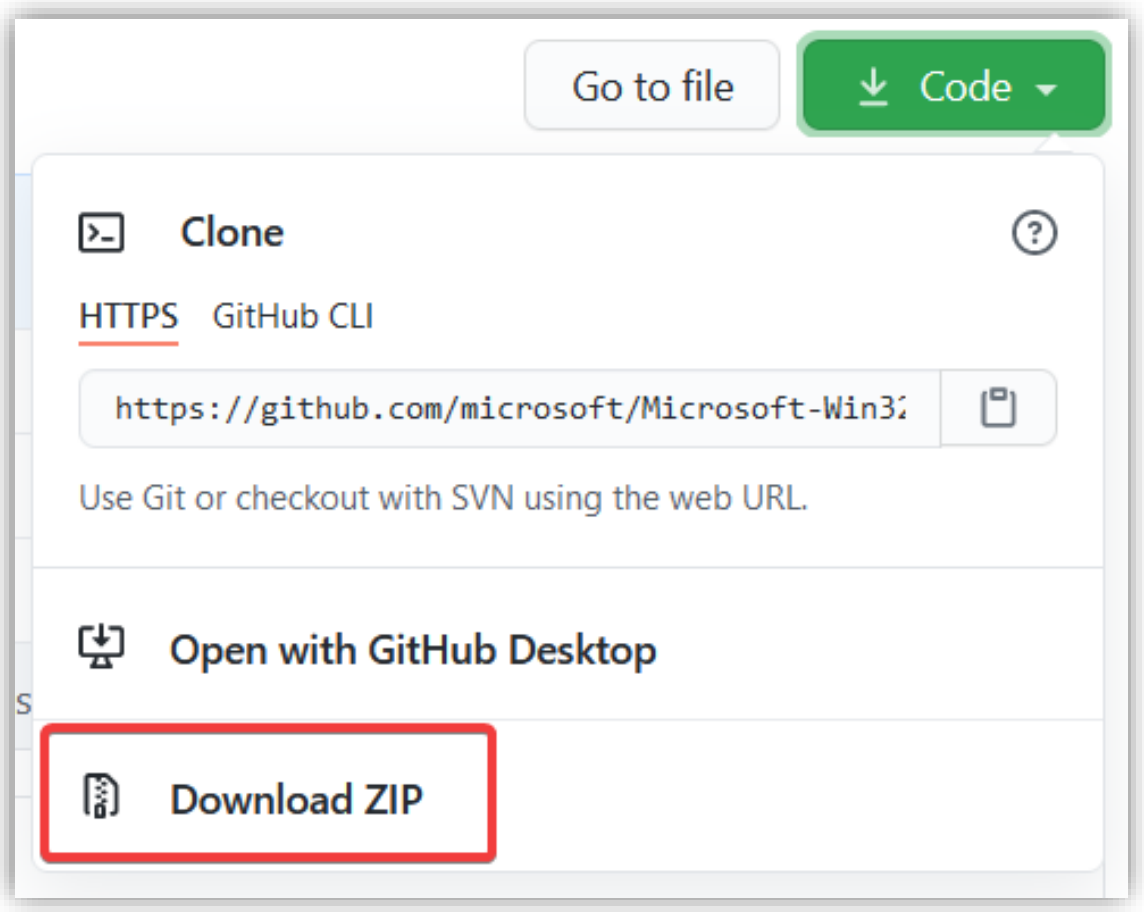
AIP unified labeling client gjør at brukerne av enheten kan sette labels på alt av dokumenter, inkludert de som ligger i File Explorer. Denne er også nødvendig dersom en ønsker å åpne dokumenter som er klassifisert som for eksempel “konfidensielle”. Det er krav om at det i minimum kjøres en versjon av Windows 8 eller høyere.

For å gjøre utrullingen av denne klienten så transparent som kan en ta i bruk Microsoft Intune. Da slipper hver bruker å måtte laste ned programmet selv.

Gå til denne nettsiden https://www.microsoft.com/en-gb/download/details.aspx?id=53018 for å laste ned .msi filen til **unified labeling client for central deployment**.



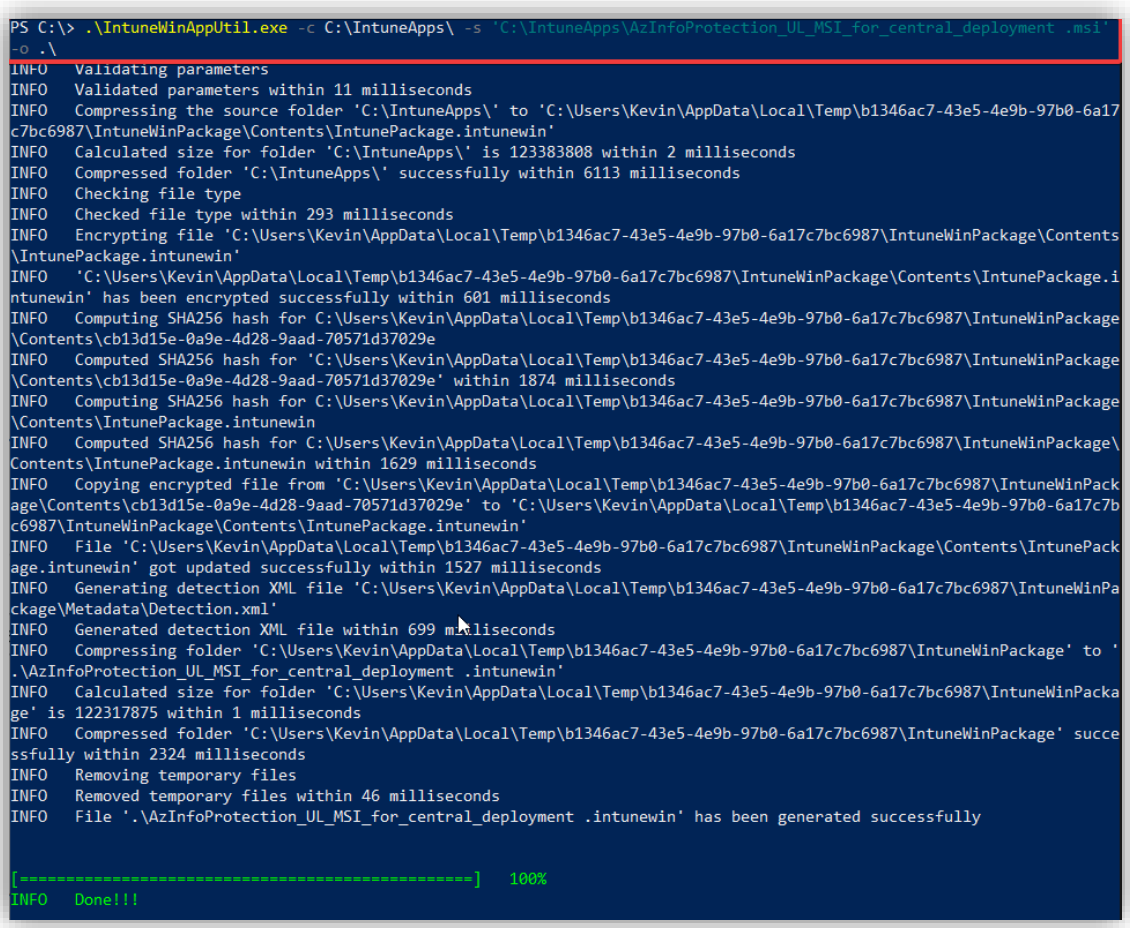
For å kunne rulle ut klienten trenger filen å være av «.intunewin»-filtype. Last derfor ned **Microsoft Win32 Content Prep Tool,** denne gjør denne konverteringen for oss. Gå til denne nettsiden https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool og last ned ZIP-filen.



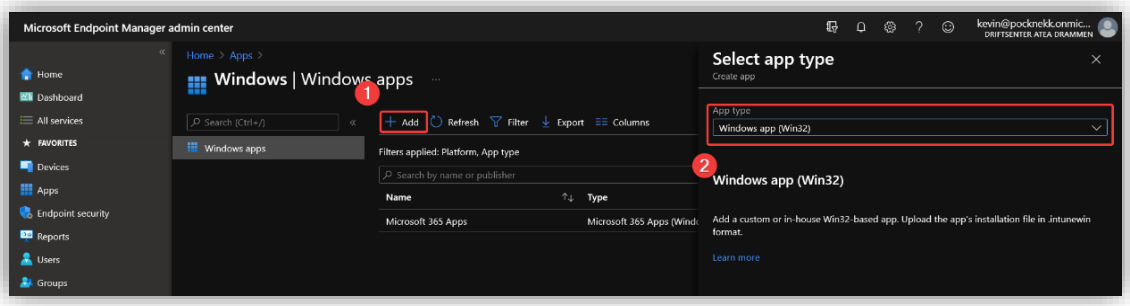
Legg .msi-filen i en egen mappe og “extract” ZIP-filen til prep tool. Kjør deretter denne kommandoen i PowerShell:

.\IntuneWinAppUtil.exe -c C:\IntuneApps\ -s AzInfoProtection_UL_MSI_for_central_deployment .msi -o C:\IntuneApps

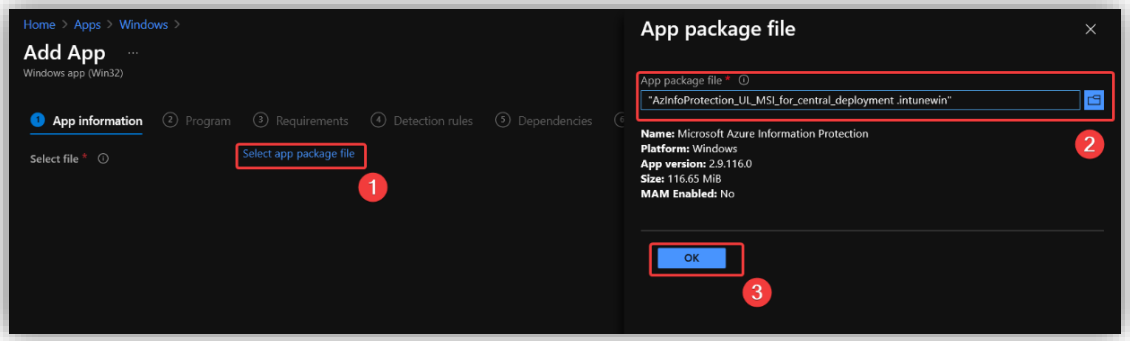
Gjør om kommandoen slik at –c er stien til mappen hvor .msi-filen ligger, -s er .msi-filen og –o er stien til hvor intunewin-filen skal legges. Se under for referanse.



Gå inn i **Microsoft Endpoint Manager admin center**[12] **> Apps > Windows** og trykk på **Add**. Under **Select app type** velg **Windows app (Win32)**. Trykk så på **Select**.

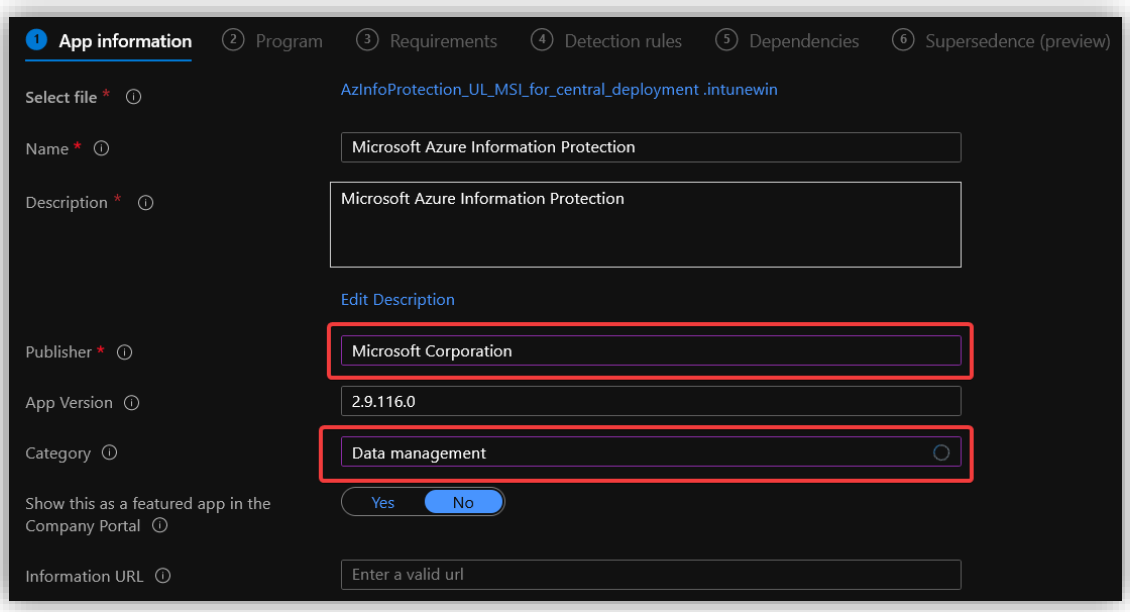


For å legge inn filen som ble gjort klar. Velg **Select app package file** og legg inn «.intunewin»-filen. Trykk så på **OK.**



[12] https://endpoint.microsoft.com/?ref=AdminCenter#home

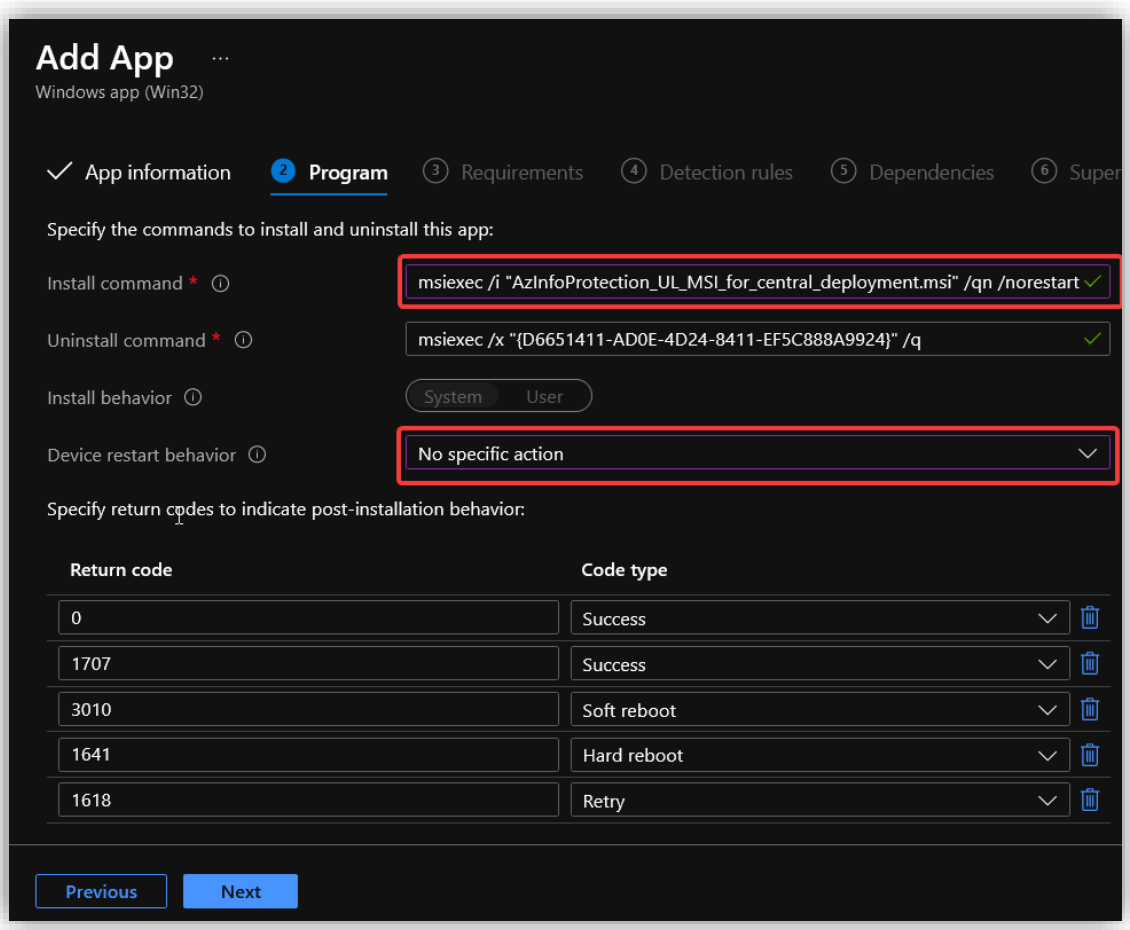
Det fylles så inn litt informasjon på egenhånd. Legg inn **publisher** som “Microsoft Corporation” og kategori til “Data management”. Kategorien er til slik at en lettere kan finne applikasjonen I katalogen på klientsiden. Trykk så på **Next**.



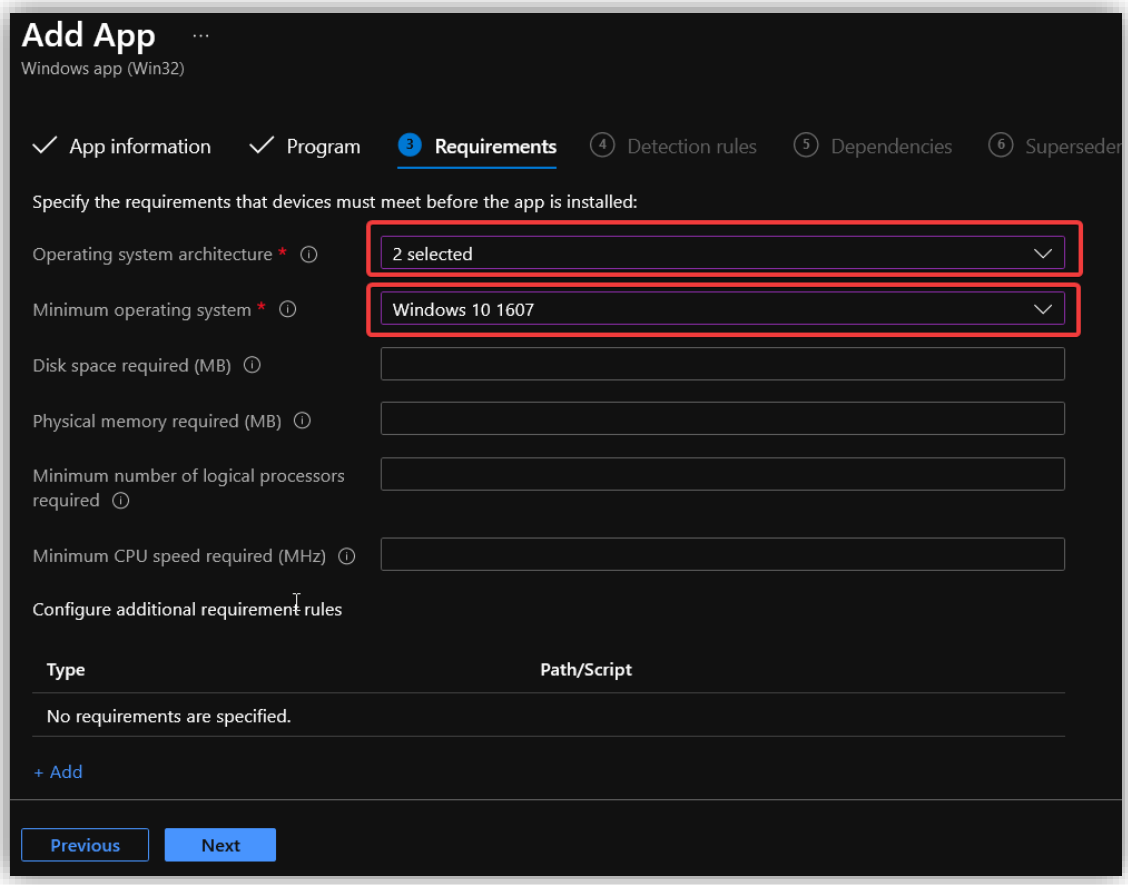
Sett installasjons-scriptet til det som står under:

msiexec /i "AzInfoProtection_UL_MSI_for_central_deployment.msi" /qn /norestart

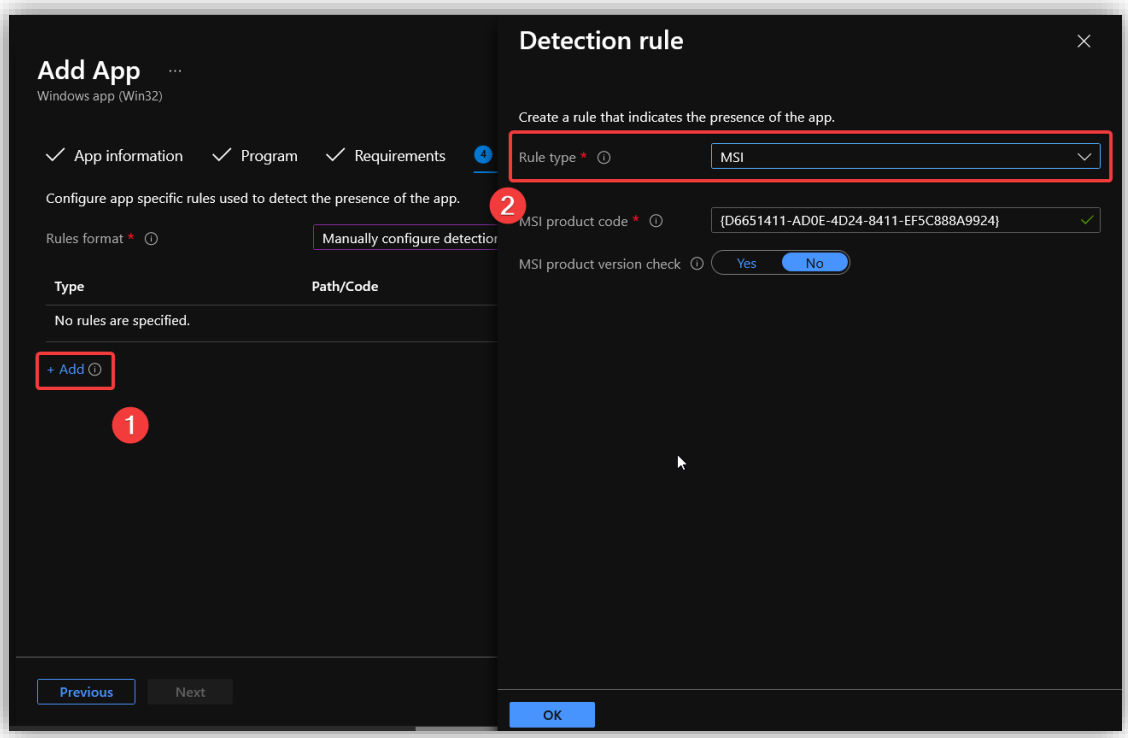
/qn for at det ikke skal kjøres noe UI og /norestart for at maskinen ikke skal restartes. Sett derfor også **Device restart behavior** til “No specific action”.



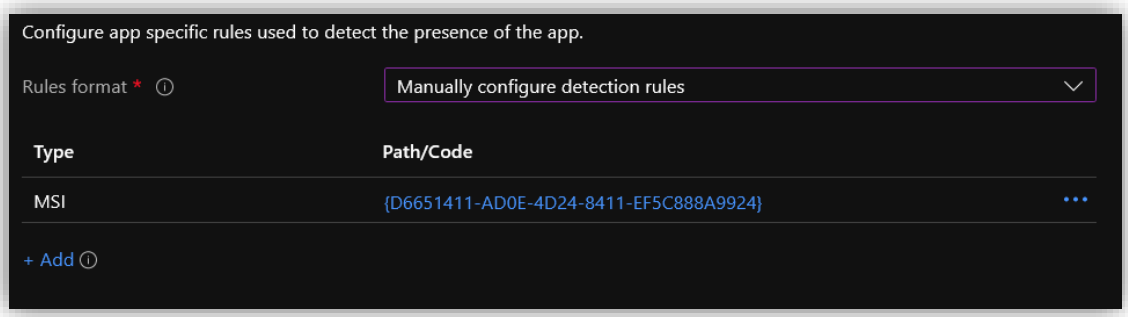
Under **Requirements** legg til både 64- og 32-bit system arkitektur. Sett også minimumskravet for OS til den tidligste av OS-ene.



For at **Intune** skal kunne detektere hvilke enheter som programmet skal installeres på, må den først sjekke om klienten allerede er installert på enheten først. Velg å sette regelen manuelt og trykk på **Add**. Under **Rule type** velg "MSI" og du vil da se at "MSI product code" blir lagt til automatisk. Trykk så på **OK.**

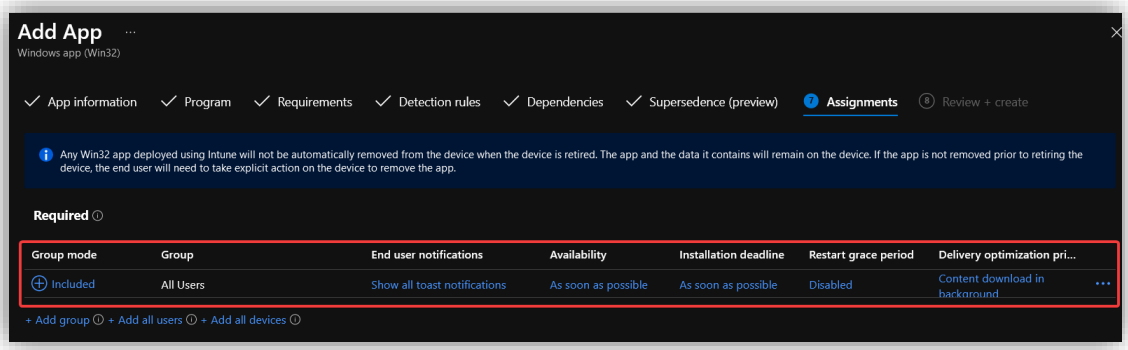


Slik skal det se ut.

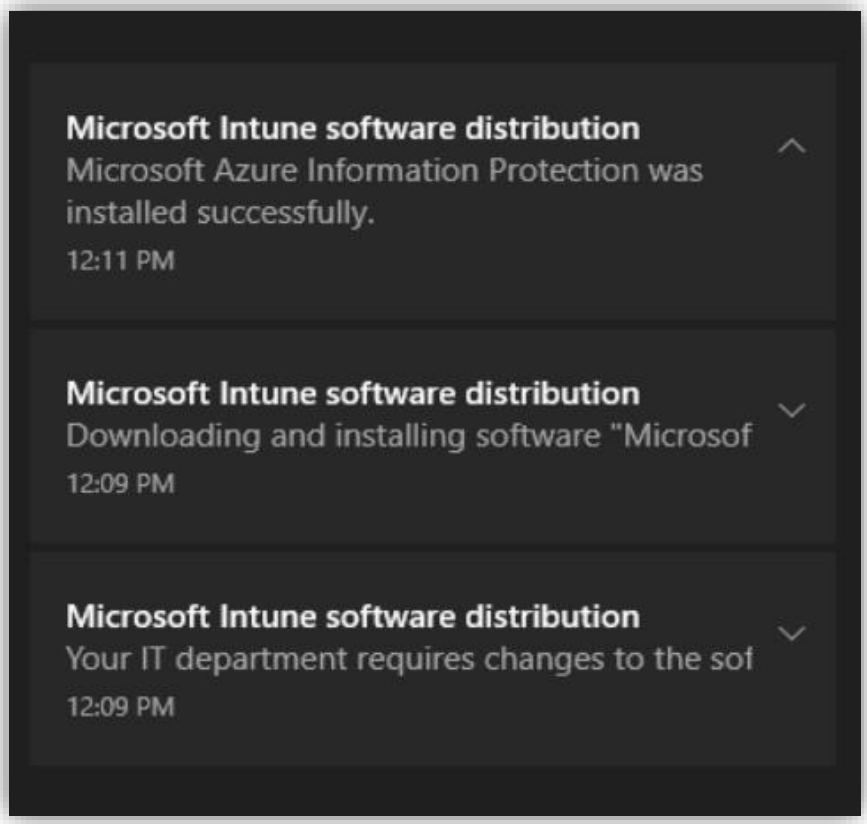


Trykk så på **Next** fram til **Assignments**-fanen.

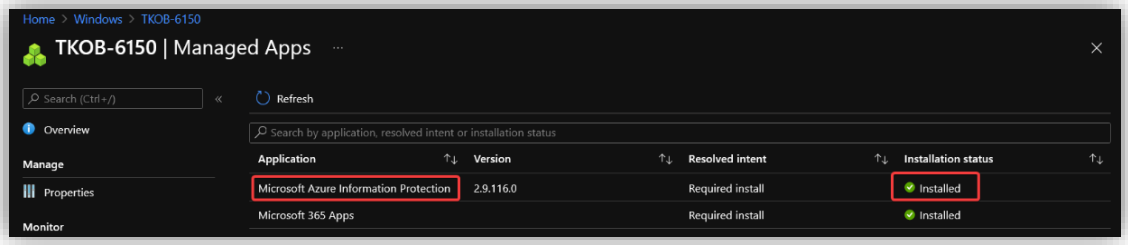
Trykk på “Add all devices” under **Required**.



Etter en liten stund vil det på klientsiden komme varsler om installasjonen. Det vil også dukke opp et program som heter **Azure Information Protection Viewer**. Brukeren kan nå høyreklikke på dokumenter i File Explorer og trykke **Classify and protect** for å styre labeling og adgangstilgang til dokumentet.



I **Endpoint Manager** kan du gå inn på enheten og trykke på **Managed Apps**. Her ser du at applikasjonen er installert suksessfullt.

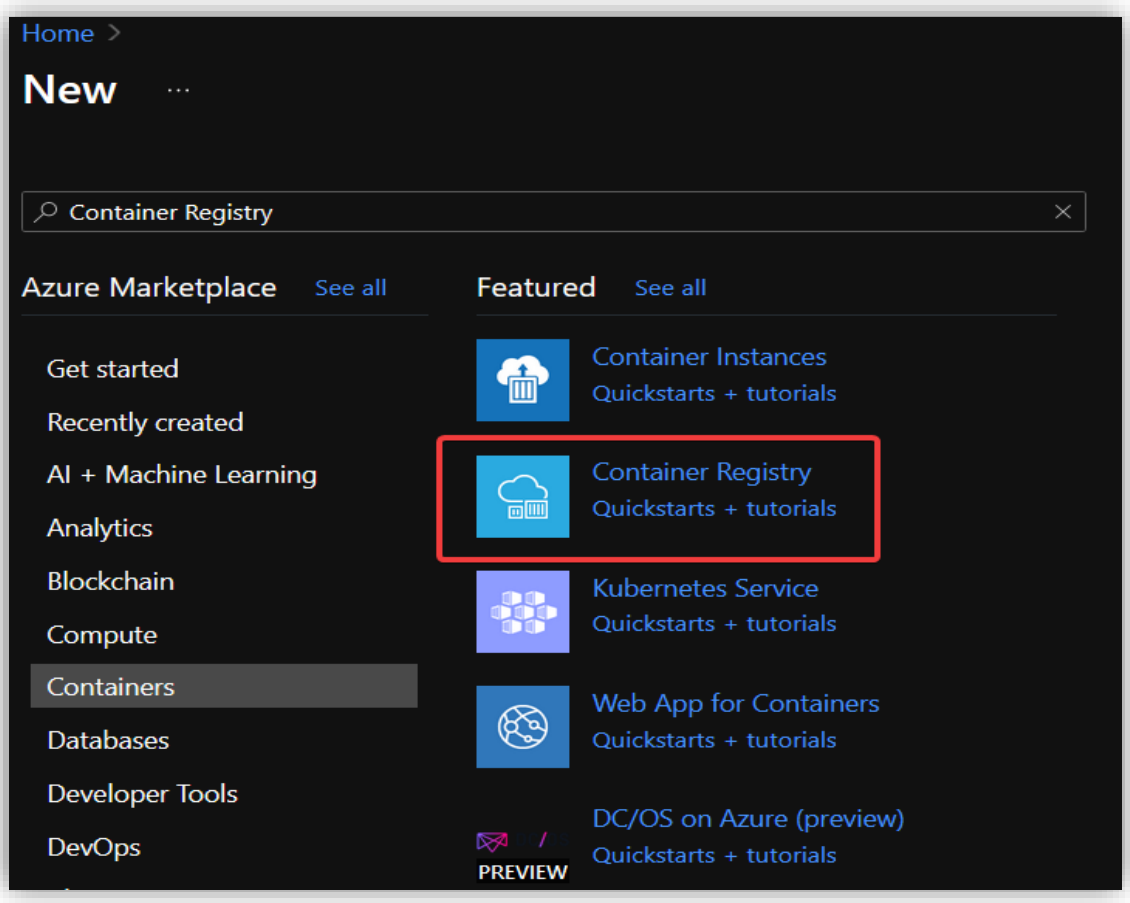


3.8 Azure app service

Azure app service[13] kan brukes til å publisere en nettside som skal være til bruk for de ansatte. App service gjør at en kan bruke Azure Active Directory til å autentisere brukere. **Azure Container Registry** gjør at en kan ta i bruk Docker images til å lage applikasjoner. I denne utrullingen antas det at du har en applikasjon som er klar til å publiseres. I eksempelet publiseres en enkel node.js applikasjon i en Docker container.

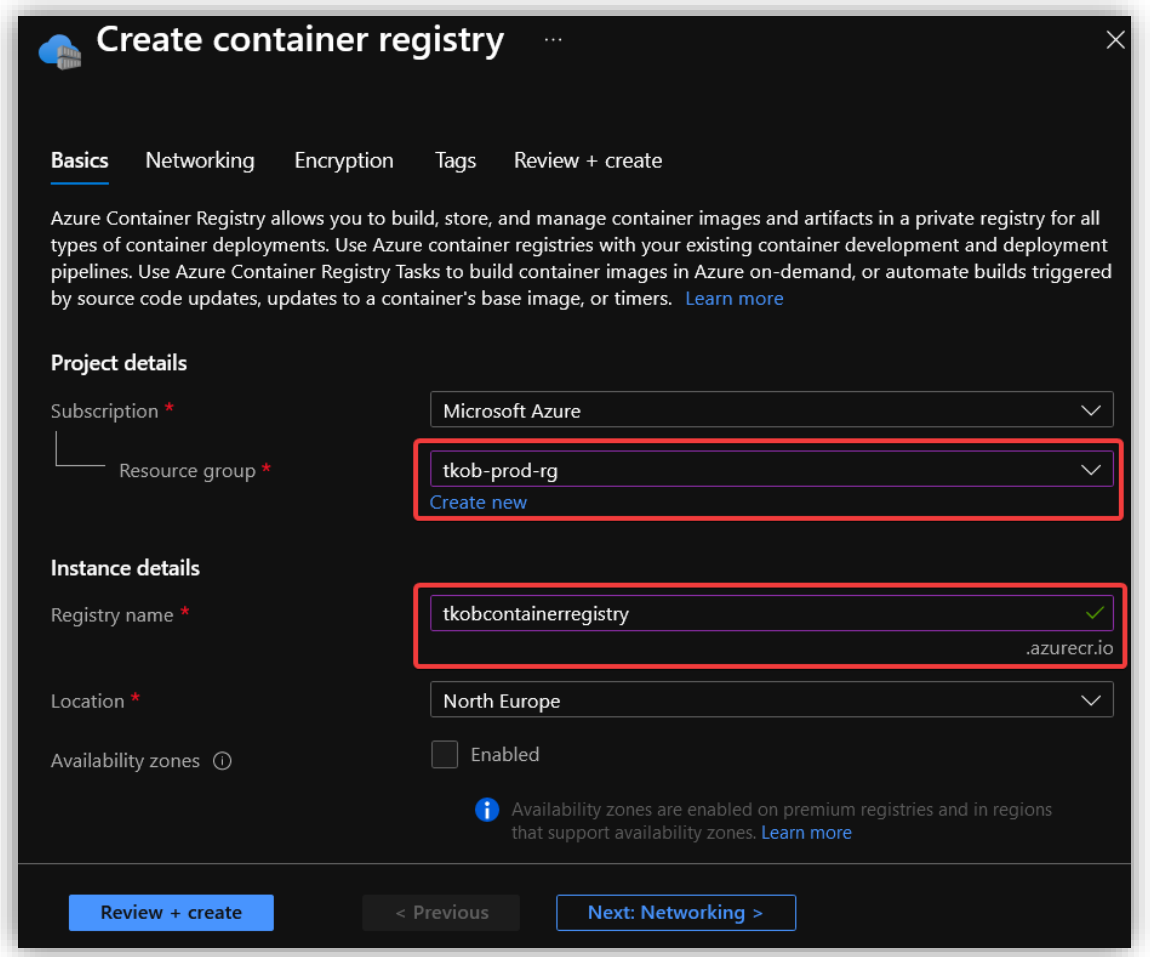
3.8.1 Lag et Container registry

Først må en lage et **Container Registry**. Dette gjøres ved å gå inn på **Create a resource > Containers > Container Registry**.

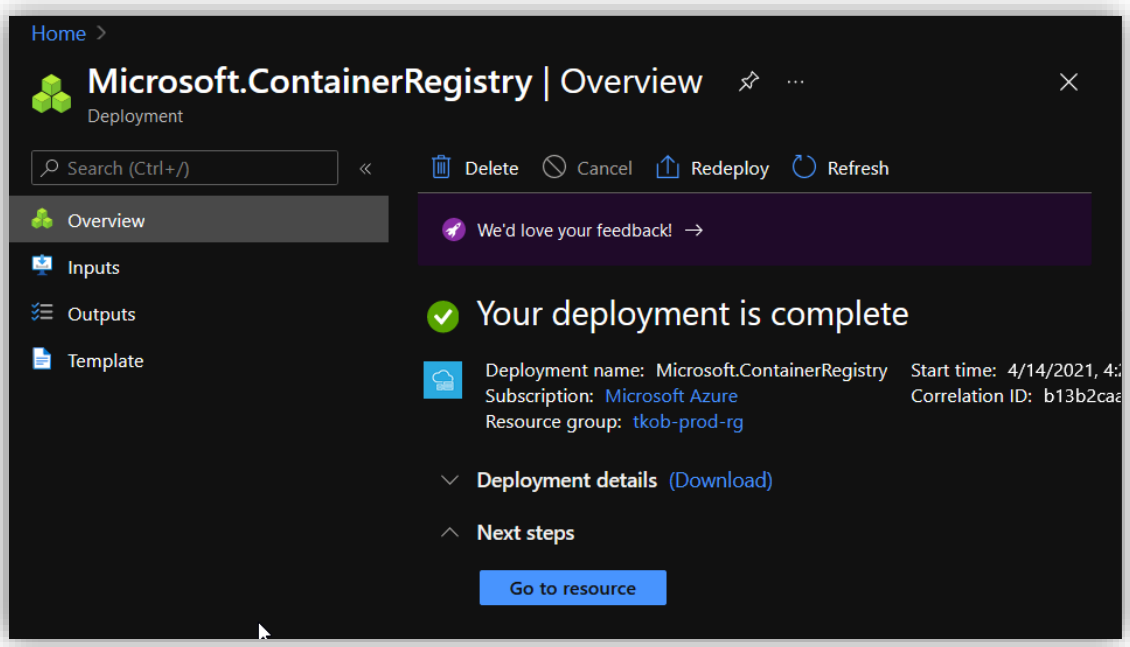


[13] https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Web%2Fsites

Du må så lage registre hvor du skal legge containeren til applikasjonen. Velg aktuell **Resource group** og gi den et passende navn.



Gå så videre til **Review + Create**, se over og trykk **Create**.

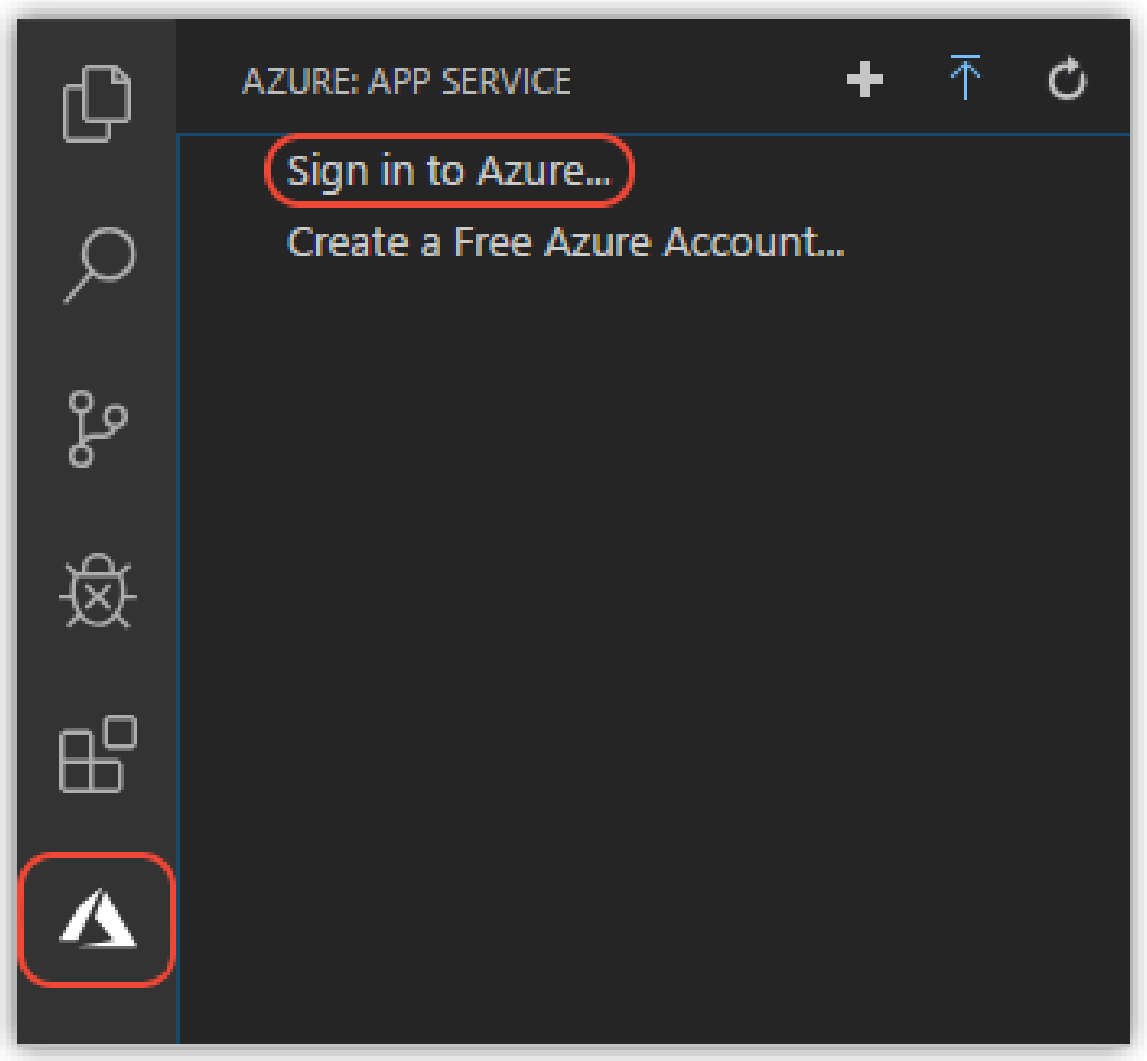


3.8.2 Laste opp Node.js app til Azure App Service

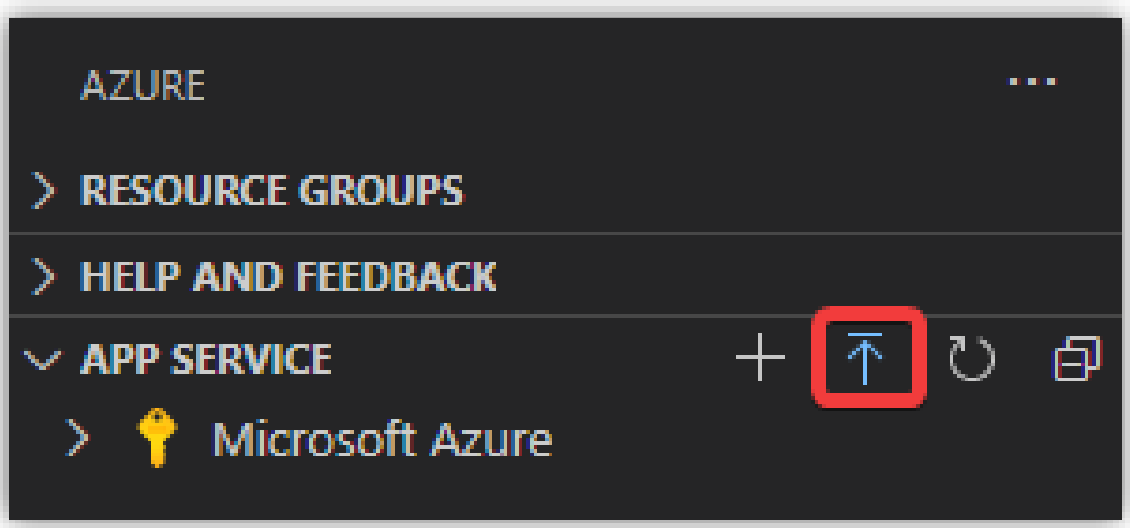
For å gjøre denne prosessen enkel brukes et tilleggsprogram til Visual Studio Code. Dette gjør at en kan logge inn i Azure fra VSC og på en enkel måte laste opp applikasjonen til Azure App Service.

Last ned **Azure App Service extension** (https://marketplace.visualstudio.com/items?itemName=ms-azuretools.vscode-azureappservice) til **Visual Studio Code.**

Logg inn inn ved å trykke på **Sign in to Azure...**

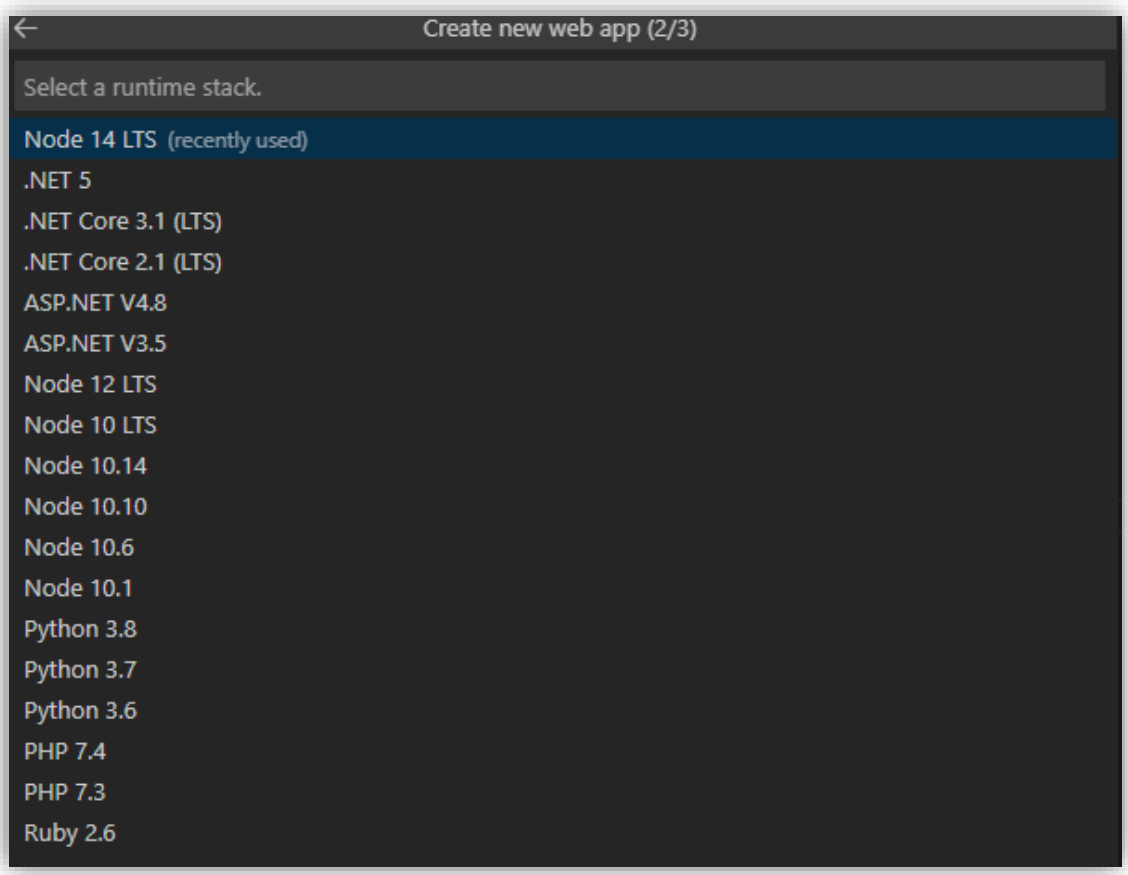


For å laste opp en applikasjon til Azure, trykk på **den blå pilen.**

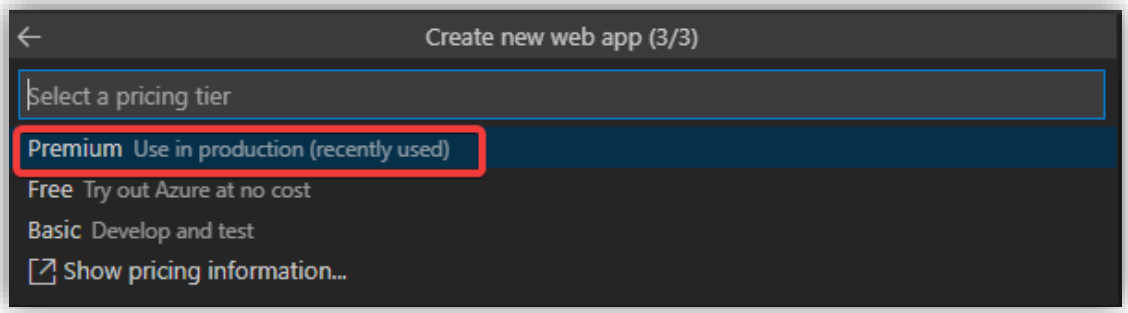


Det vil så dukke opp en rekke valg:

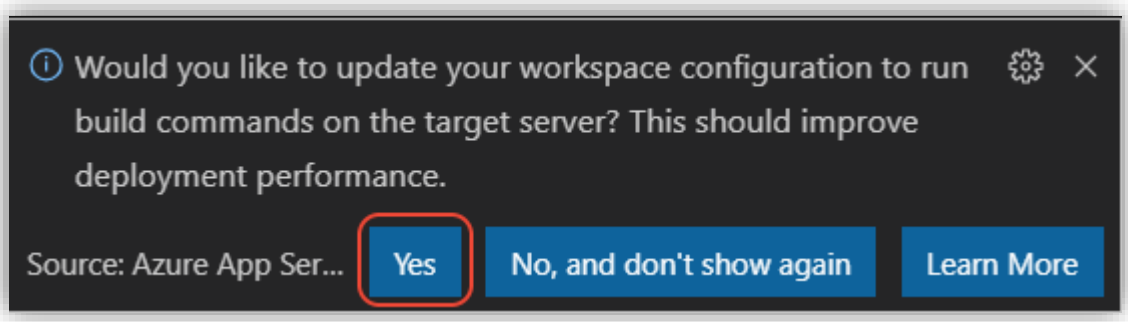
- Velg først rotmappen til applikasjonen.
- Velg så **Create new Web App.**
  - Velg denne ettersom man vil rulle ut applikasjonen til et Linux-basert operativsystem.
  - **Create new Web App... Advanced** er til Windows-basert OS.
- Gi applikasjonen et globalt unikt navn.
- Velg så en passende runtime stack.
  - I dette eksemplet har man en enkel Node.js applikasjon og velger derfor **Node 14 LTS.**
  - LTS versjonene er anbefalt.



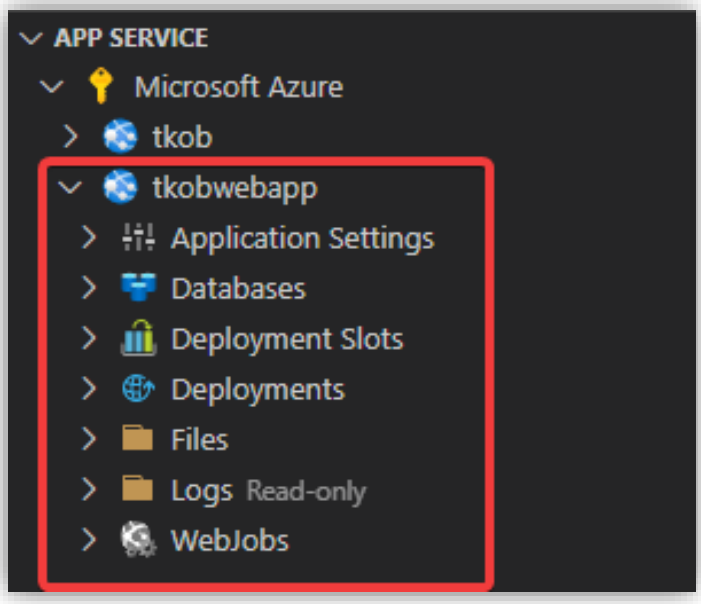
Velg **Premium** under **Select pricing tier** ettersom dette er en applikasjon som skal ut i produksjon.



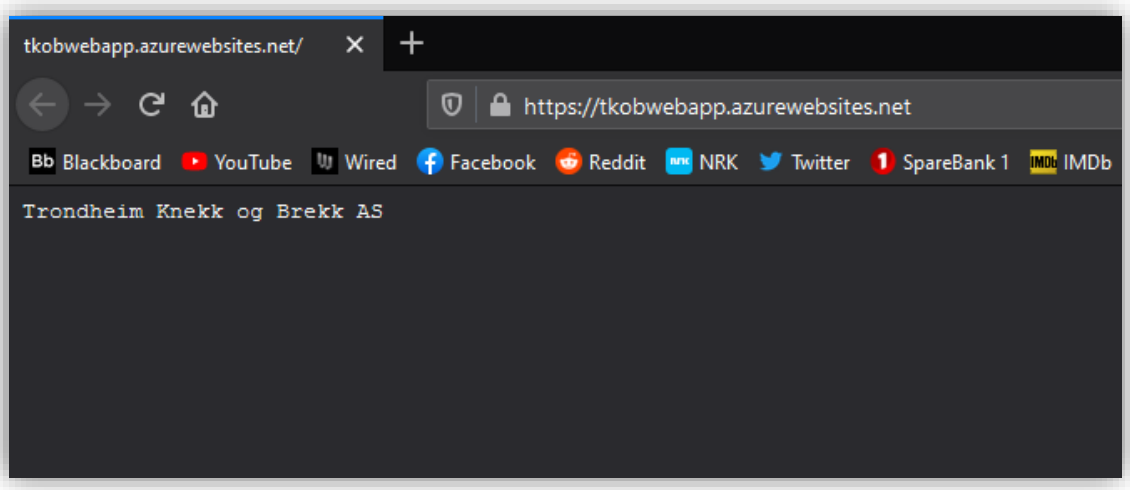
Det vil så dukke opp et vindu som spør om en ønsker å oppdatere konfigurasjonen for å kjøre **npm install** på den aktuelle Linux-serveren. Trykk på **Yes** ettersom dette vil forbedre ytelsen.



Etter at utrullingen er fullført, kan en se applikasjonen og tilhørende data i VSC



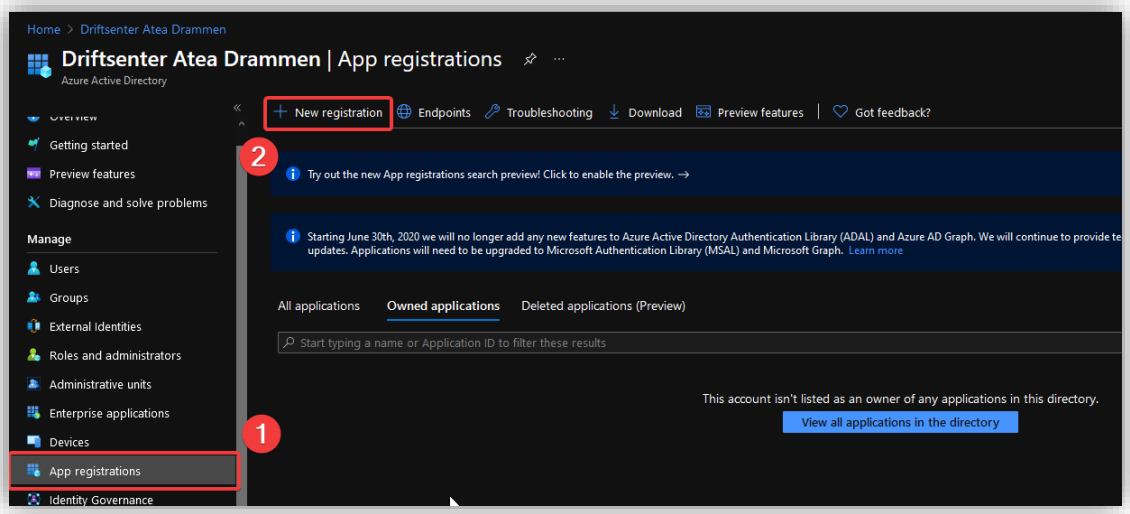
Høyretrykk på applikasjonen og trykk **Browse Website** for å se nettsiden som er lastet opp.



3.8.3 Konfigurer autentisering i app

For å sikre applikasjonen, kan en konfigurere App Service slik at en bruker må logge seg inn med sin Microsoft-bruker for å kunne komme seg inn på nettsiden.

Gå inn i **Azure Active Directory**[14] **> App registration** og trykk på **New registration**.



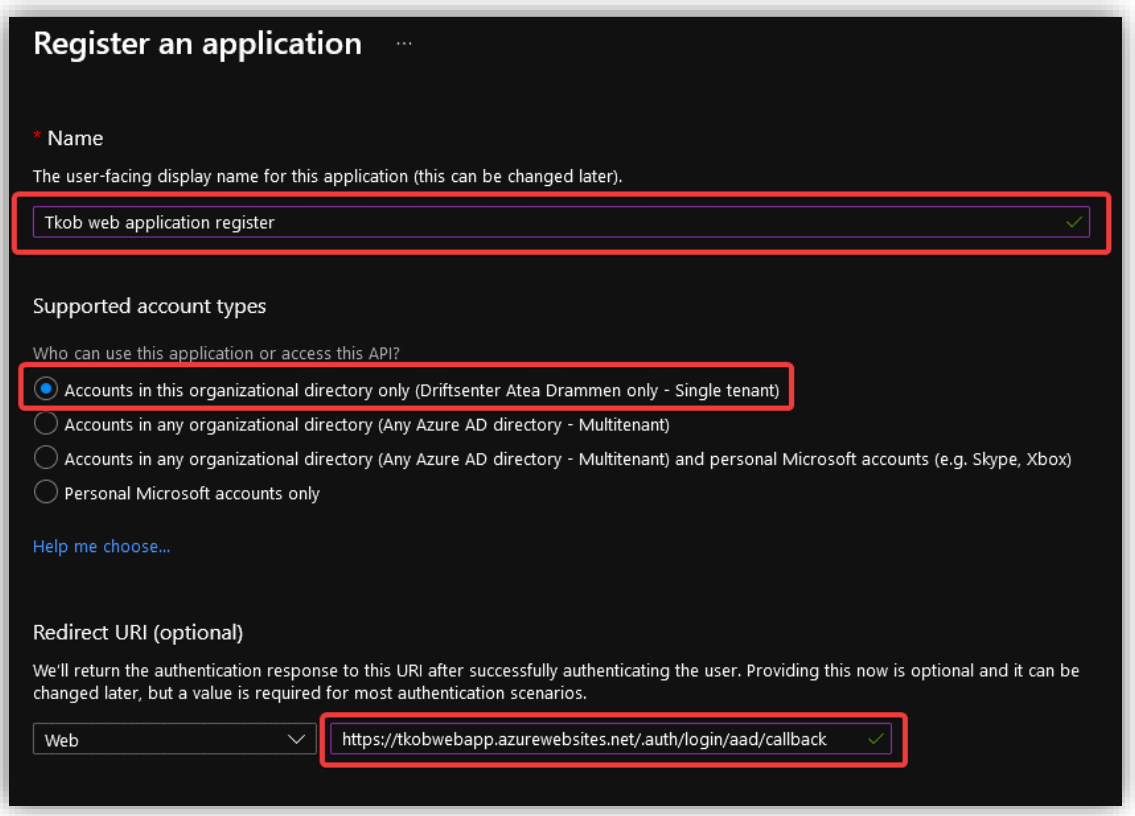
[14] https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

Skriv inn et passende navn, velg **Single tenant**. Under **Redirect URI¸** velg **Web** og skriv inn følgende:

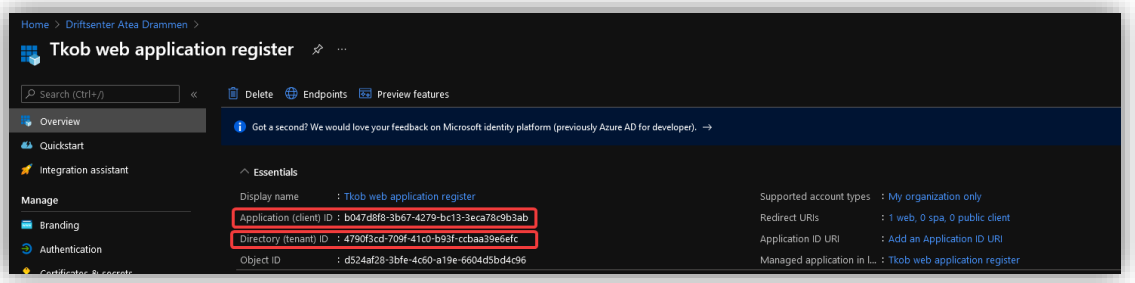
<app-url>/.auth/login/aad/callback

I dette eksempelet blir det:

https://tkobwebapp.azurewebsites.net/.auth/login/aad/callback

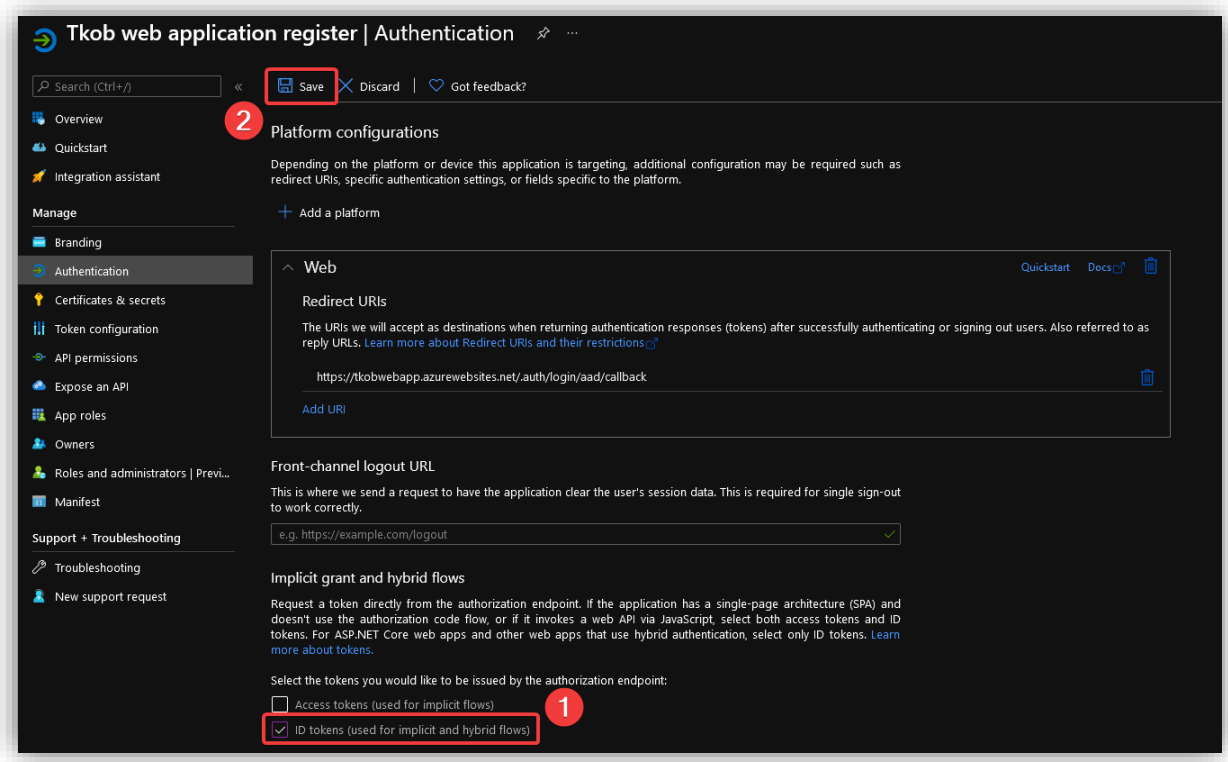


Når registreringen er ferdig, vil du komme til denne skjermen:

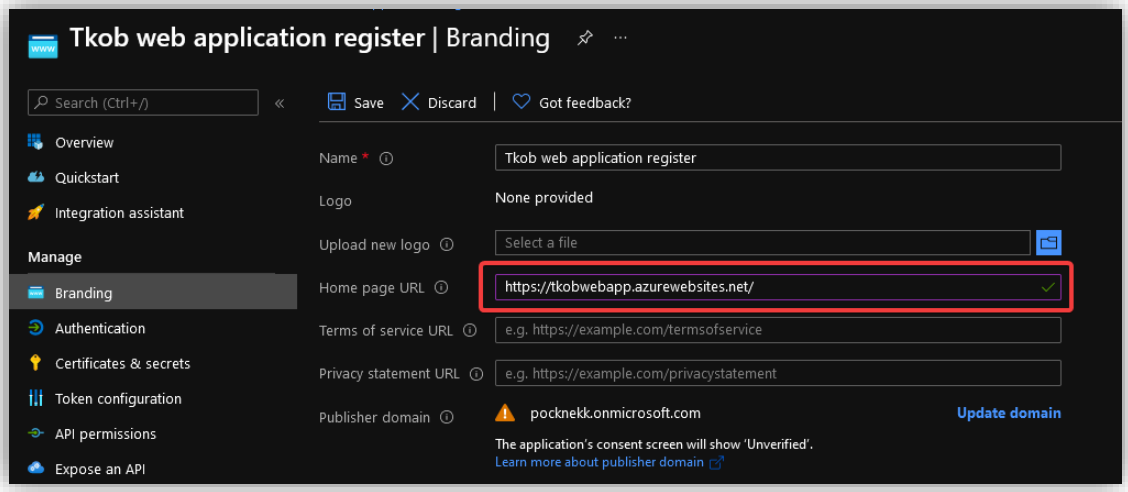


Kopier **Application (client) ID** og **Directory (tenant) ID** slik at disse er lett tilgjengelige til senere steg.

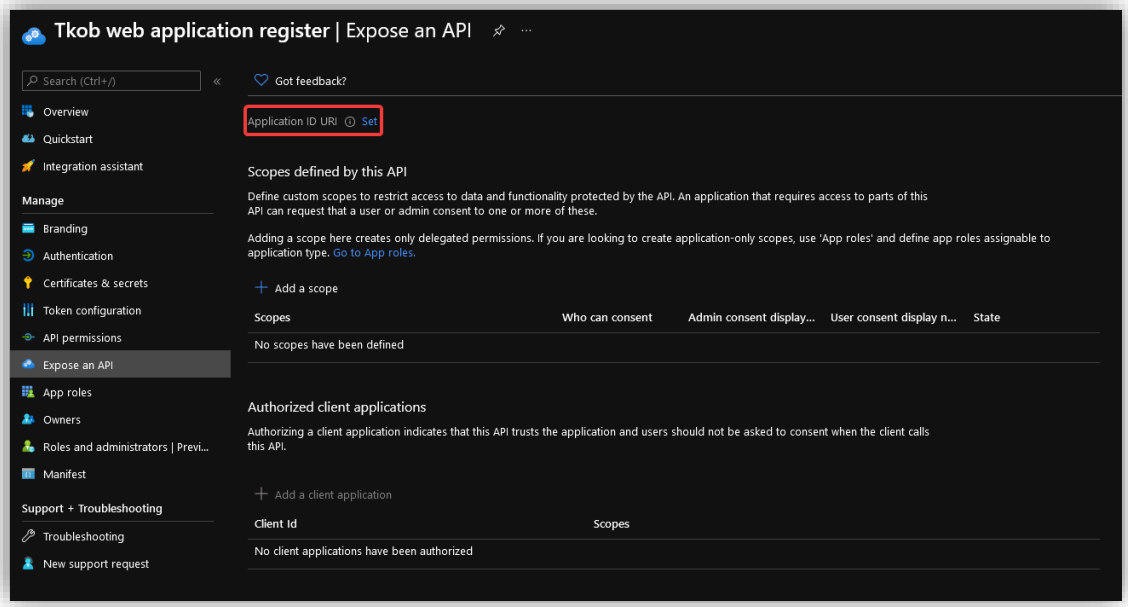
Under **Authentication**-fanen, huk av for **ID tokens** og trykk på **Save.** Dette gjør at en kan bruke OpenID Connect bruker-innlogging fra App Service.



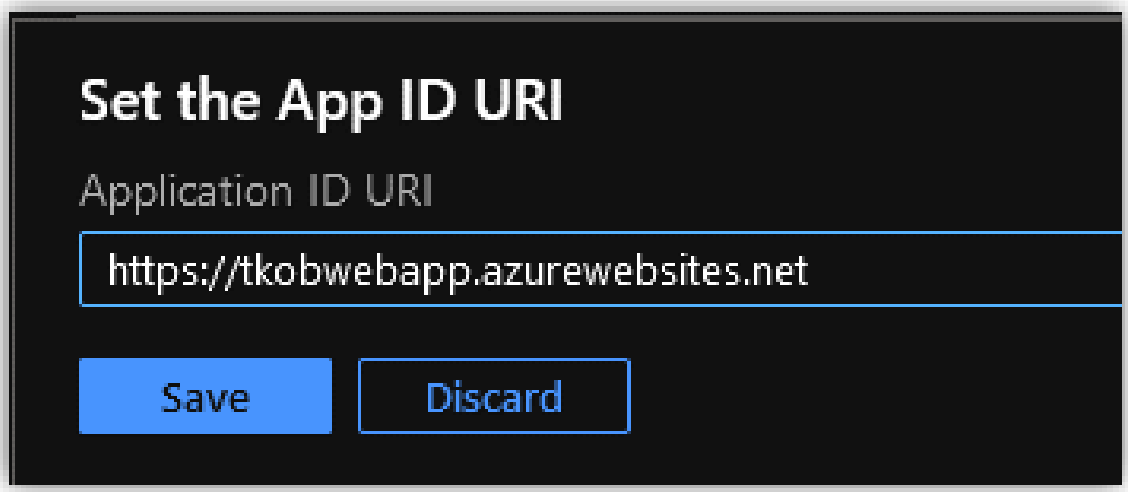
Under **Branding** legg inn URLen til applikasjonen under **Home page URL.**



Under **Expose an API** trykk på **Set** bak **Application ID Url** og legg inn URLen til applikasjonen.

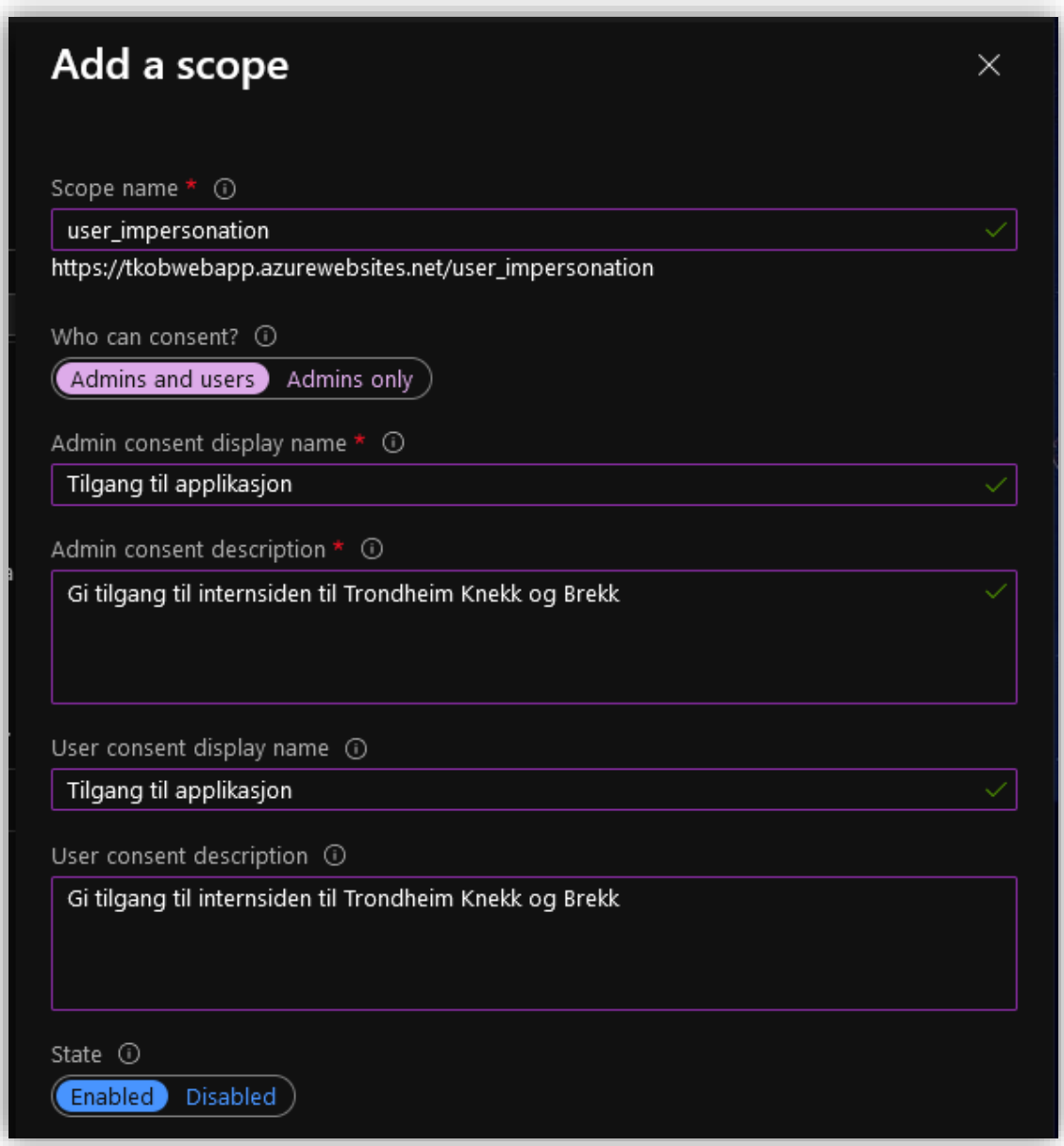


I dette tilfellet:

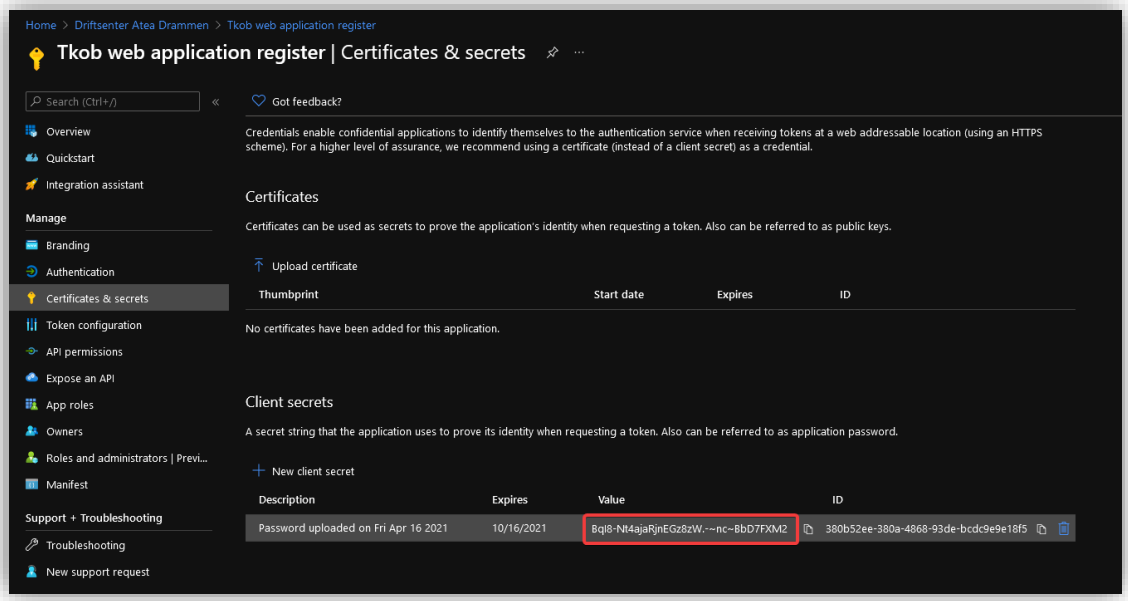


Trykk på **Add a scope.**

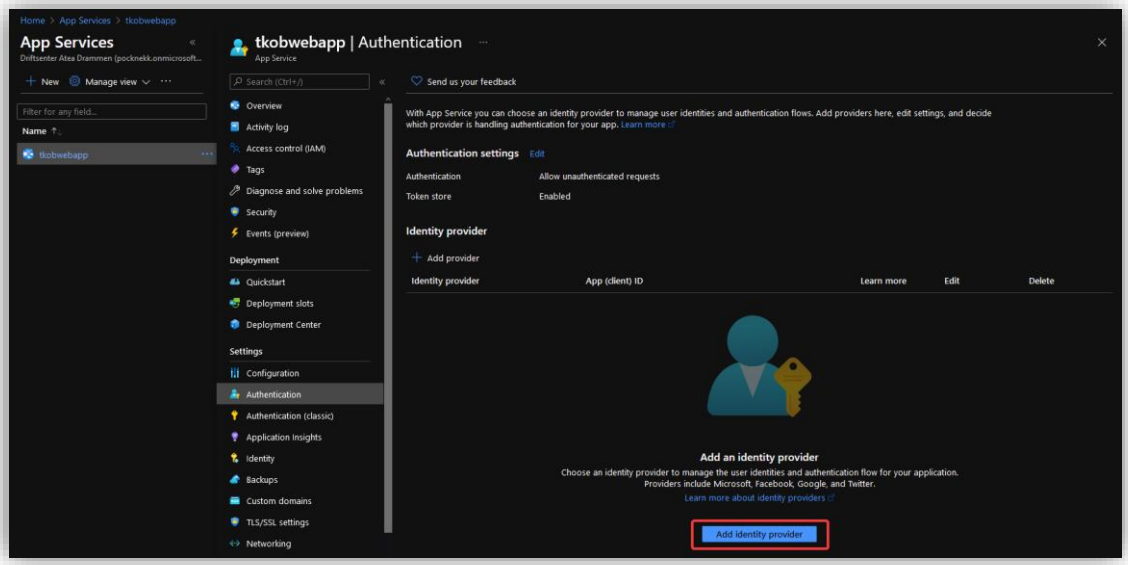
- Gi scopet et passende navn.
- Velg at både administratorbrukere og vanlige brukere skal kunne logge inn.
- Gi et passende navn og beskrivelse som skal vises på samtykkesiden.



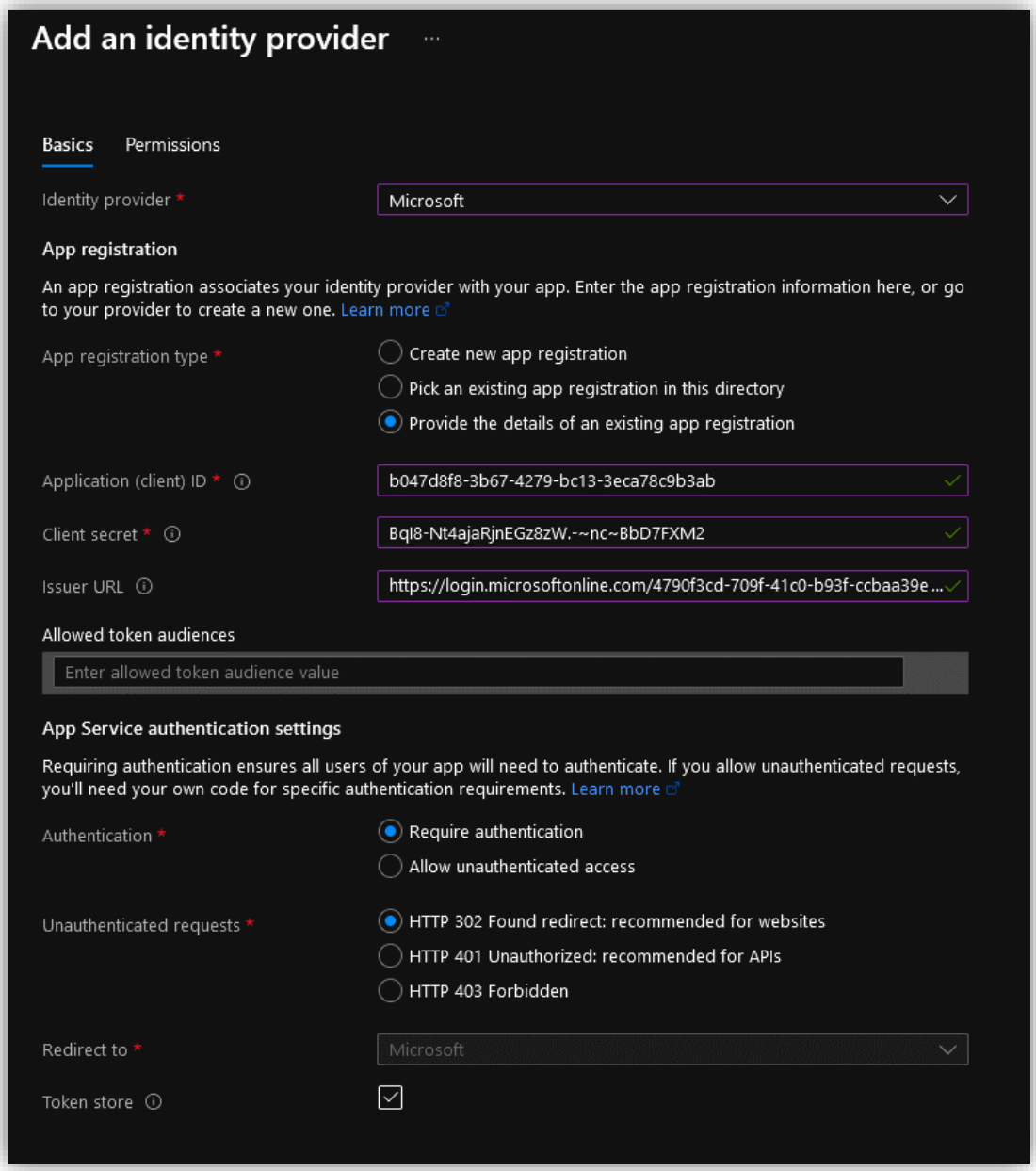
Under **Certificates & secrets**, trykk på **New client secret**, og trykk **Add.** Kopier verdien til hemmeligheten.



Naviger tilbake til applikasjonen i **App Services**, gå til **Authentication**-fanen og trykk på **Add identity provider.**

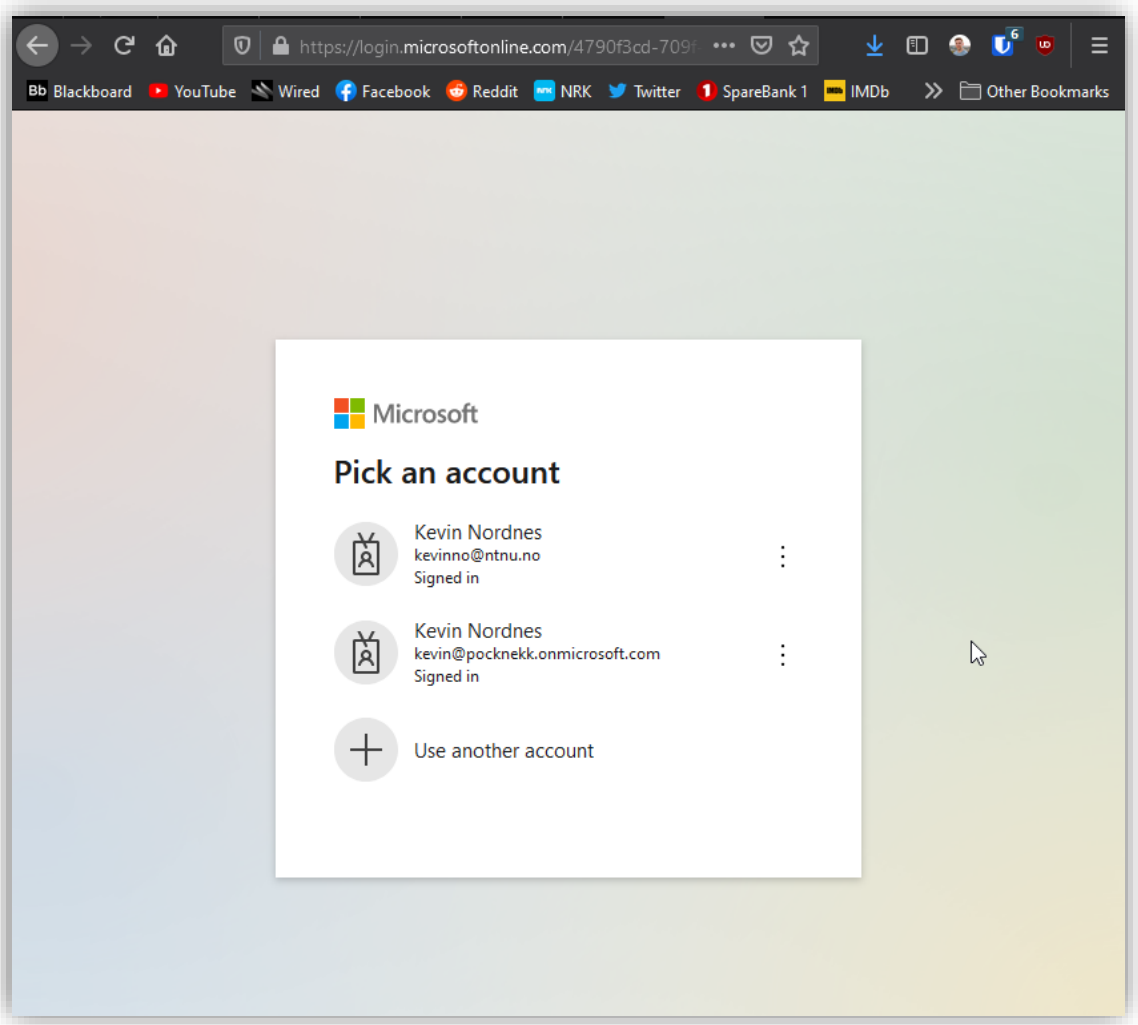


- Velg **Microsoft** som provider.
- Velg **Provide the details of an existing app registration.**
- Under **Application (client) ID**, lim inn Application IDen til app registration fra tidligere.
- Under **Client secret** legges verdien som ble kopiert i forrige punkt.
- Under **Issuer URL** skriv inn følgende: *<authentication-endpoint>/<tenant-id>/v2.0*
    - Authentication endpoint er *https://login.microsoftonline.com*
    - Tenant id er **Directory (tenant) ID** som applikasjonsregisteret genererte.
    - I dette tilfelle blir dette: *https://login.microsoftonline.com/4790f3cd-709f-41c0-b93f-ccbaa39e6efc/v2.0*
- Resten av innstillingene kan stå som standard.



Trykk så på **Add.**

Prøver du nå å gå inn på nettsiden blir du videresendt til Microsoft sin innloggingsside og må logge inn med en bruker som ligger i AD i valgt tenant.

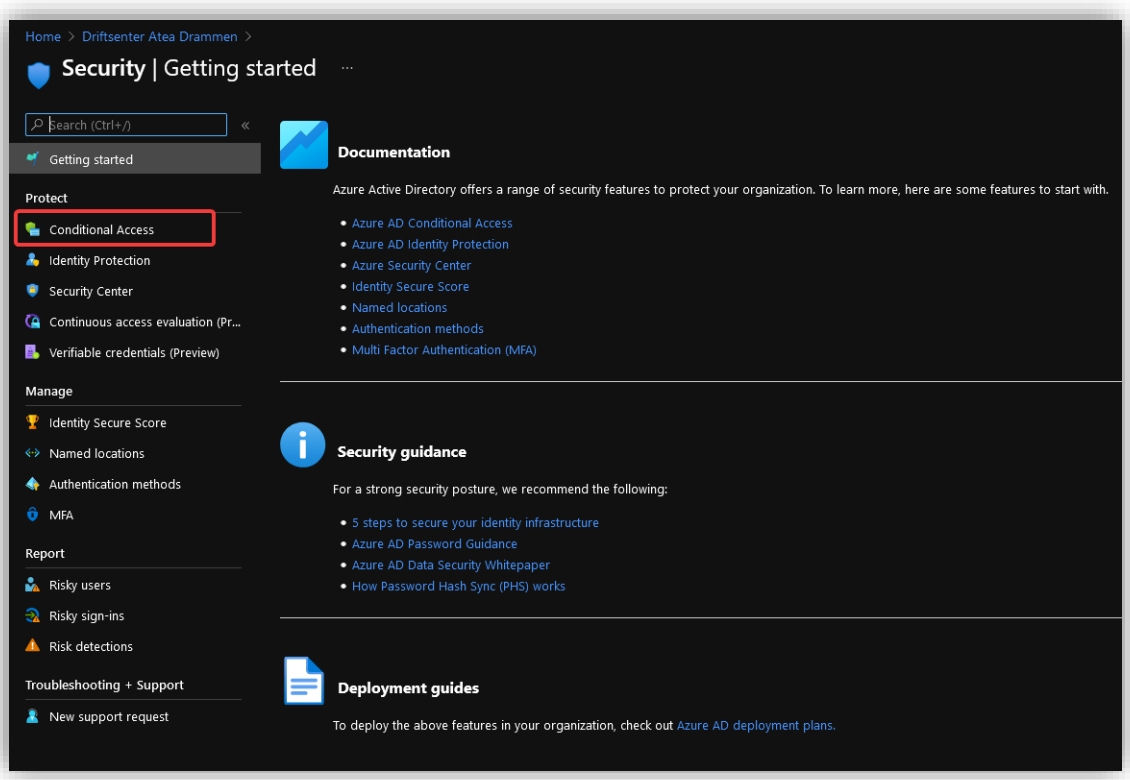


3.9 Sikkerhet

3.9.1 Azure AD Multi-Factor Authentication

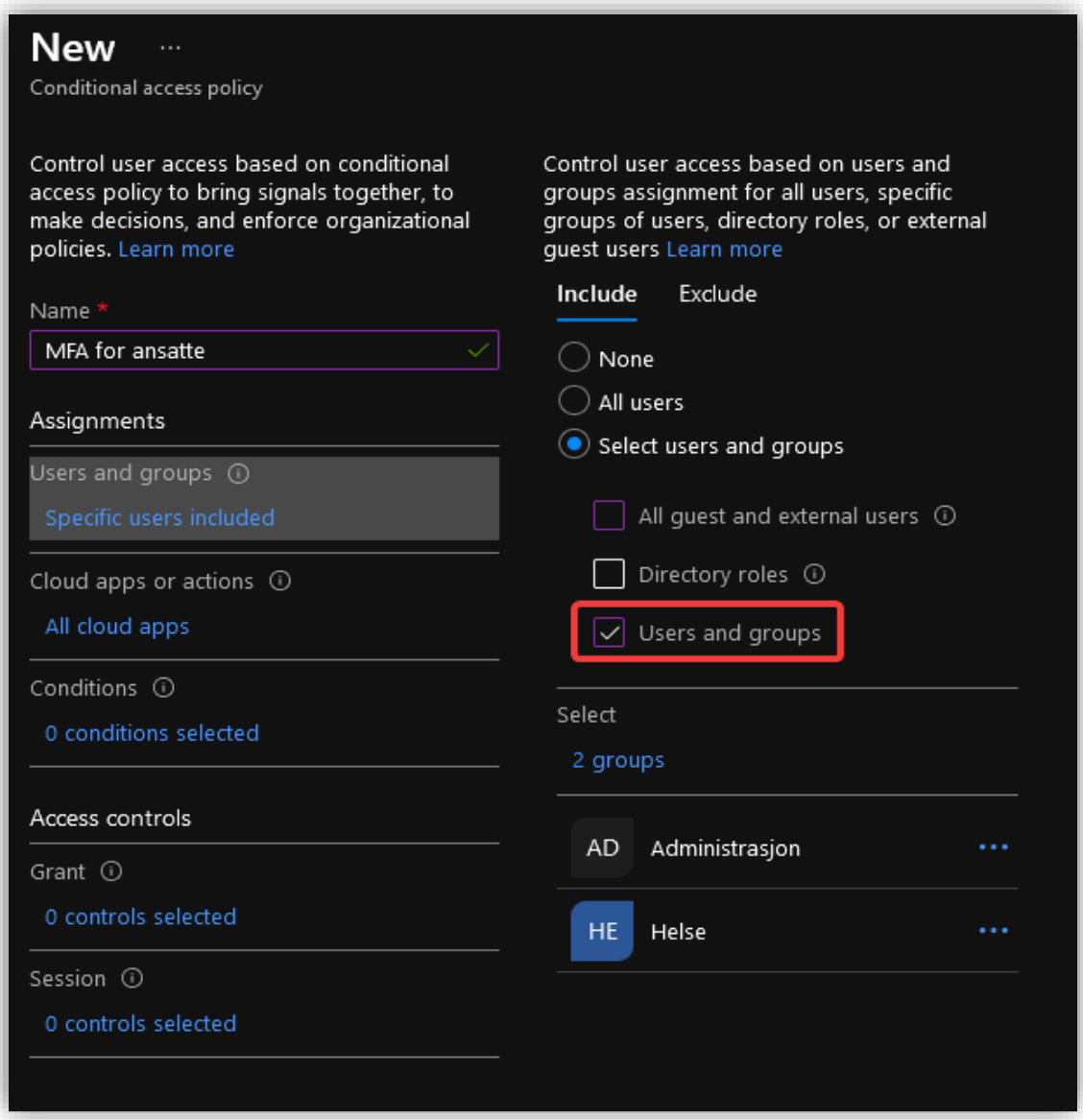
For å legge til et ekstra lag med sikkerhet kan en aktivere MFA ved innlogging til ulike sky-tjenester. Dette gjør at brukerne trenger et ekstra steg, utenom passord og brukernavn, for å verifisere seg når en prøver å logge inn et sted. Dette kan for eksempel være en kode brukeren får oppgitt på SMS eller i en app.

Gå inn i **Azure Active Directory**[15] **> Security** og trykk på **Conditional Access.**

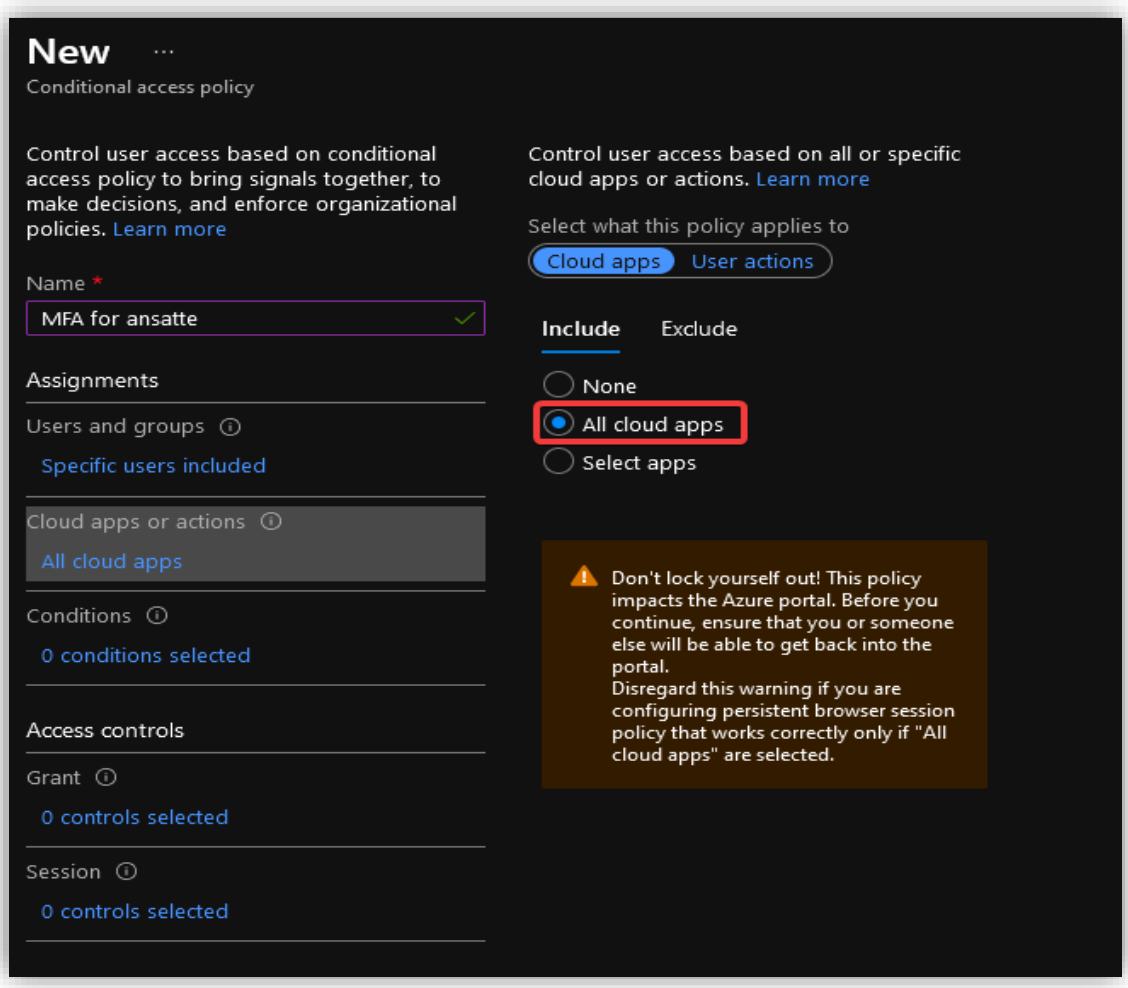


[15] https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

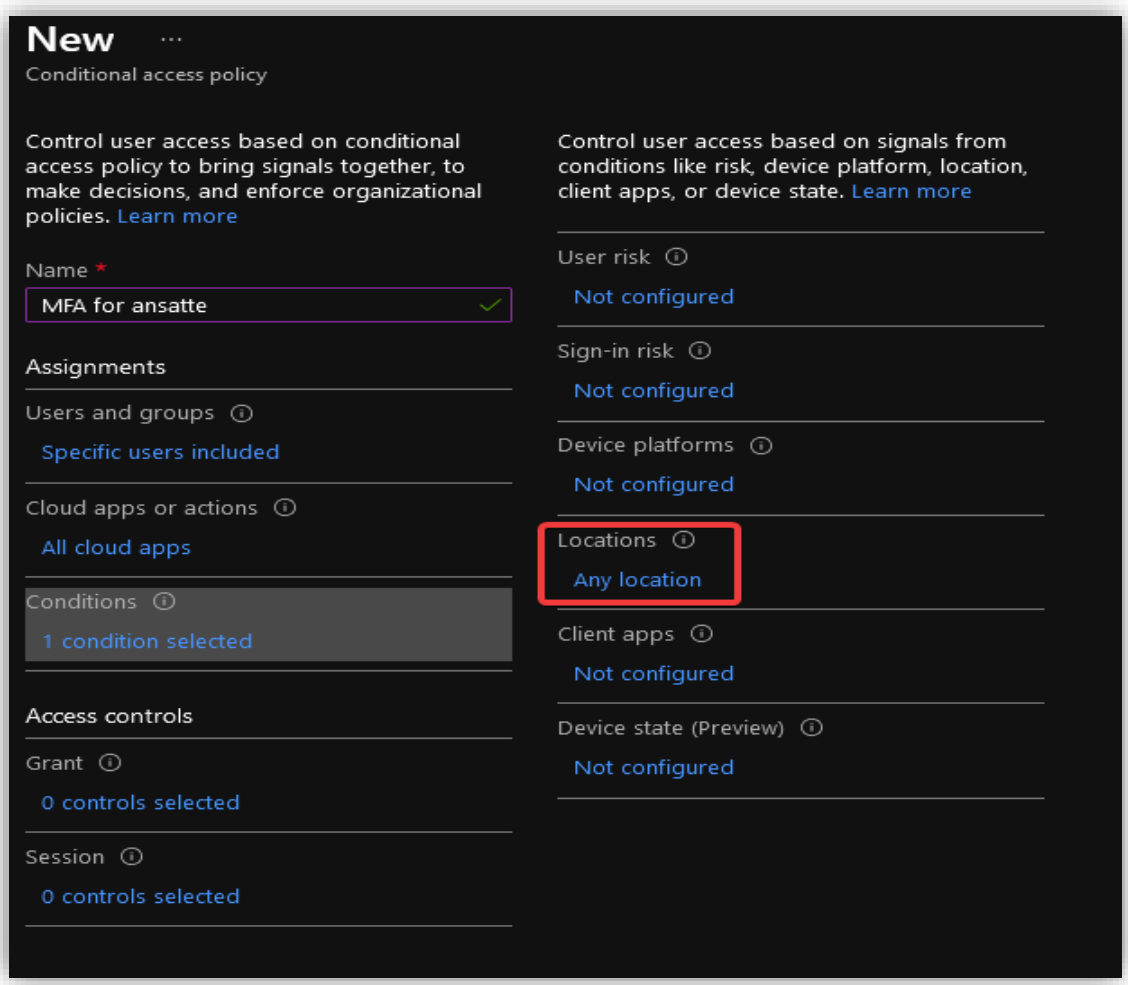
Under **Policies** trykk på **New policy**. Velg så en gruppe/grupper som skal ha MFA aktivert ved å velge **Users and groups.** Det er lurt å ikke legge til alle brukere i tilfelle en skulle klare å låse seg selv ute. Test heller på en begrenset gruppe før en setter en policy for alle.



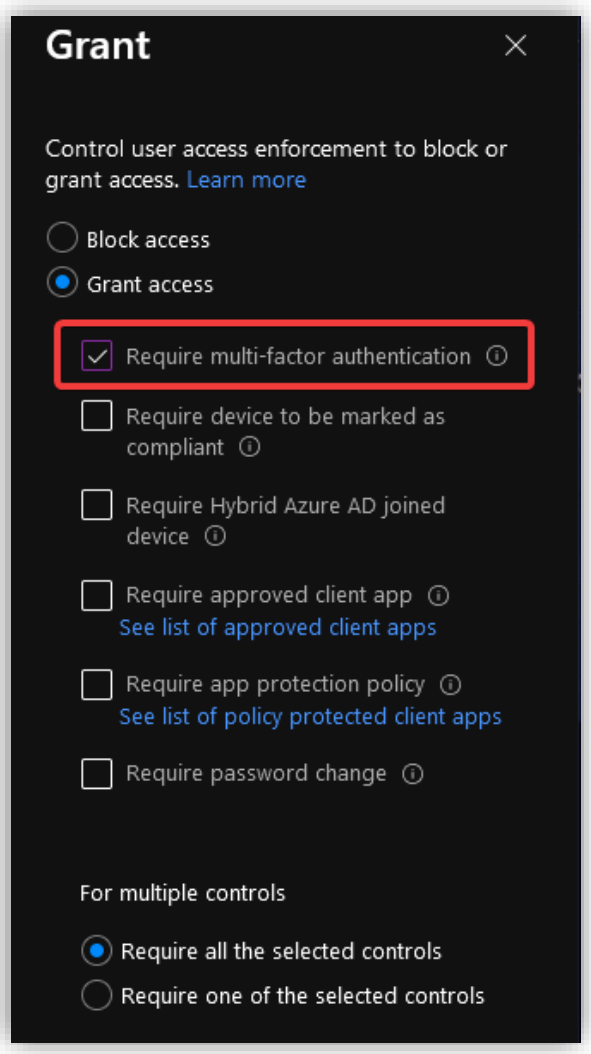
Under **Cloud apps or actions**, velg **All cloud apps.**



Under **Conditions**, legg til **Any location** slik at policyen vil gjelde uansett hvor en logger seg inn fra i verden.



Under **Grant**, pass på å velge **Require multi-factor authentication**. Det er denne som styrer at brukerne må bruke MFA for å logge seg inn i applikasjoner.



Aktiver policyen ved å sette **Enable policy** til **On**, og trykk på **Create.**

3.9.2 Azure AD Identity Protection

Azure AD Identity Protection lar oss automatisk oppdage, rette opp og undersøke identitetsbaserte risikoer i bedriften. Kompromitterte identiteter kan la uønskede aktører få tilgang til sensitiv informasjon. Ved å ta i bruk **Identity Protection** forebygges slike uønskede hendelser. Microsoft kategoriserer inn i to typer risiko:

- **Innloggingsrisikoer**

Dette er risikoer som har med selve innloggingen av en bruker å gjøre. Dette kan f.eks. være at det er en forespørsel om innlogging fra en lokasjon som det ikke vanligvis logges inn fra. Det kan også være kjente IP-addresser som har med malware å gjøre eller anonyme IP-adresser (f.eks. Gjennom Tor Browser).

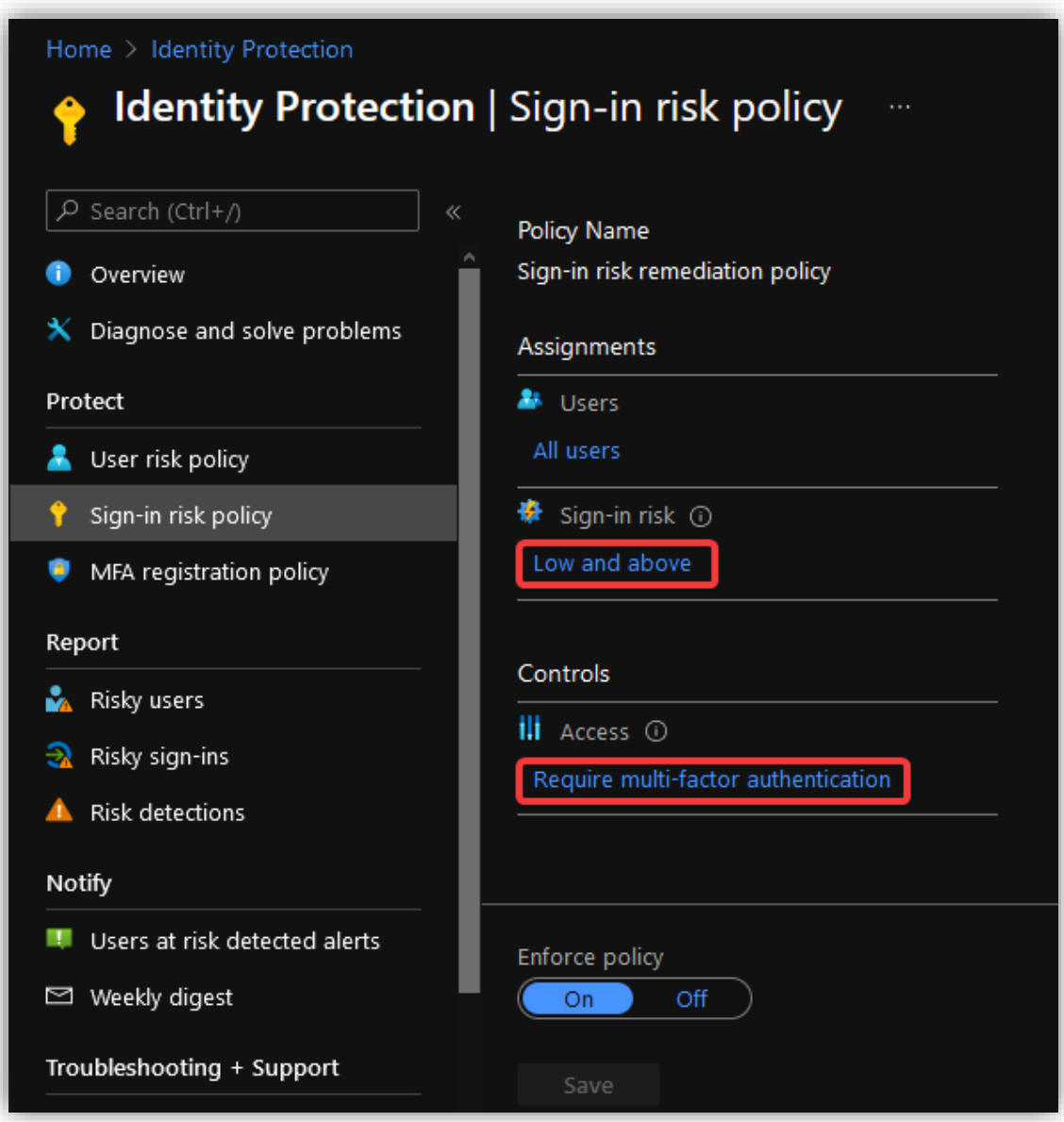
- **Brukerrisikoer**

Dette er risikoer som forekommer dersom en bruker er kompromittert eller brukeridentiteten er lekket. Microsoft kan oppdage slike risikoer ved å se uvanlige mønstre i en brukers aktivitet eller det kan være funnet en liste av lekket legitimasjon på nettet.

Gå inn i **Azure AD Identity Protection**[16] **> Sign-in risk policy**

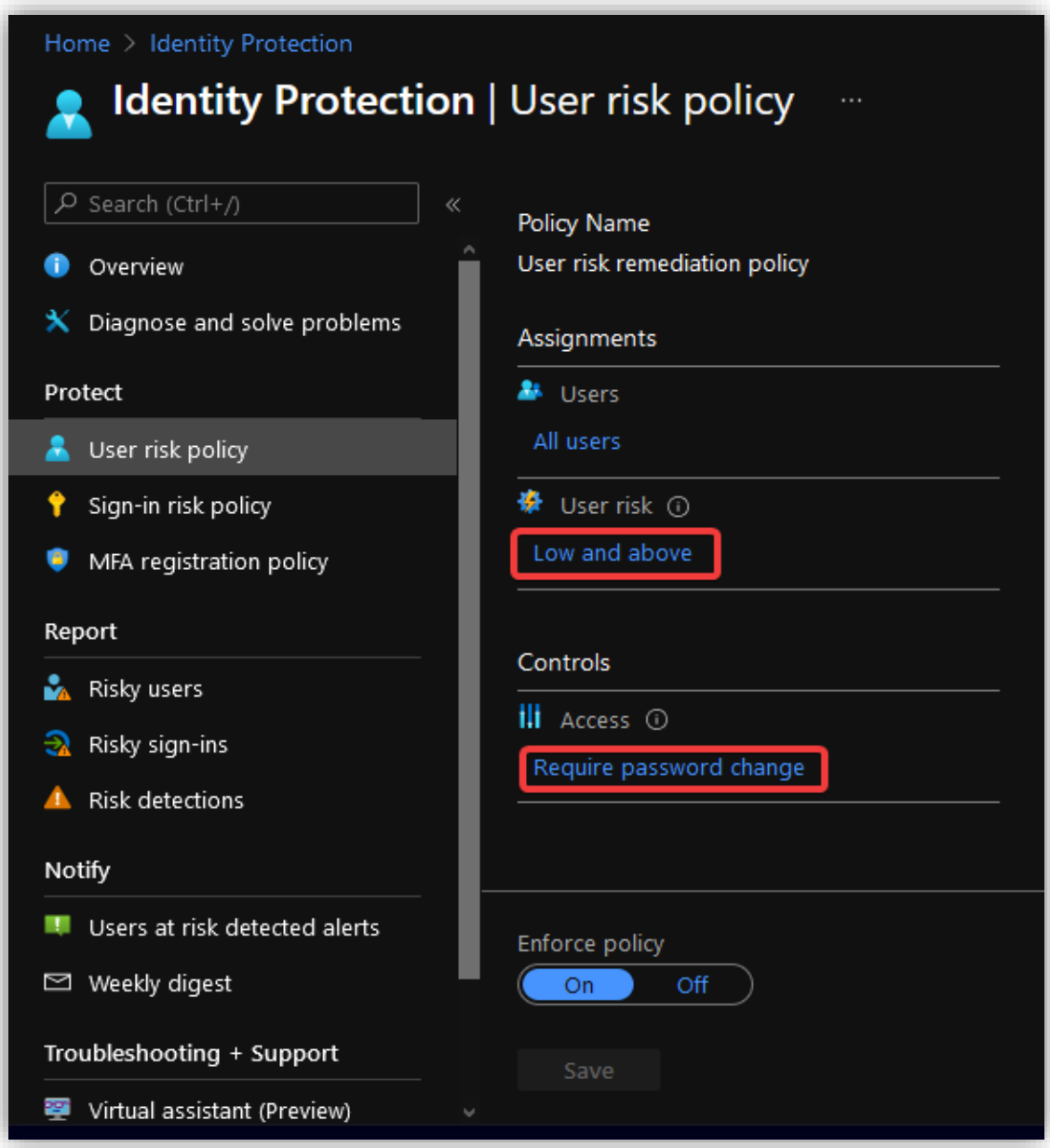
Ved å sette **Sign-in risk** til **Low and above** vil dette gjøre at policyen inntreffer dersom Microsoft vurderer at det finnes en risiko i denne innloggingen. Ved å sette på **Require multi-factor authentication** vil brukerne måtte logge inn med MFA dersom det finnes noe risiko i innloggingen.

Husk å sette **Enforce policy** til **On.**

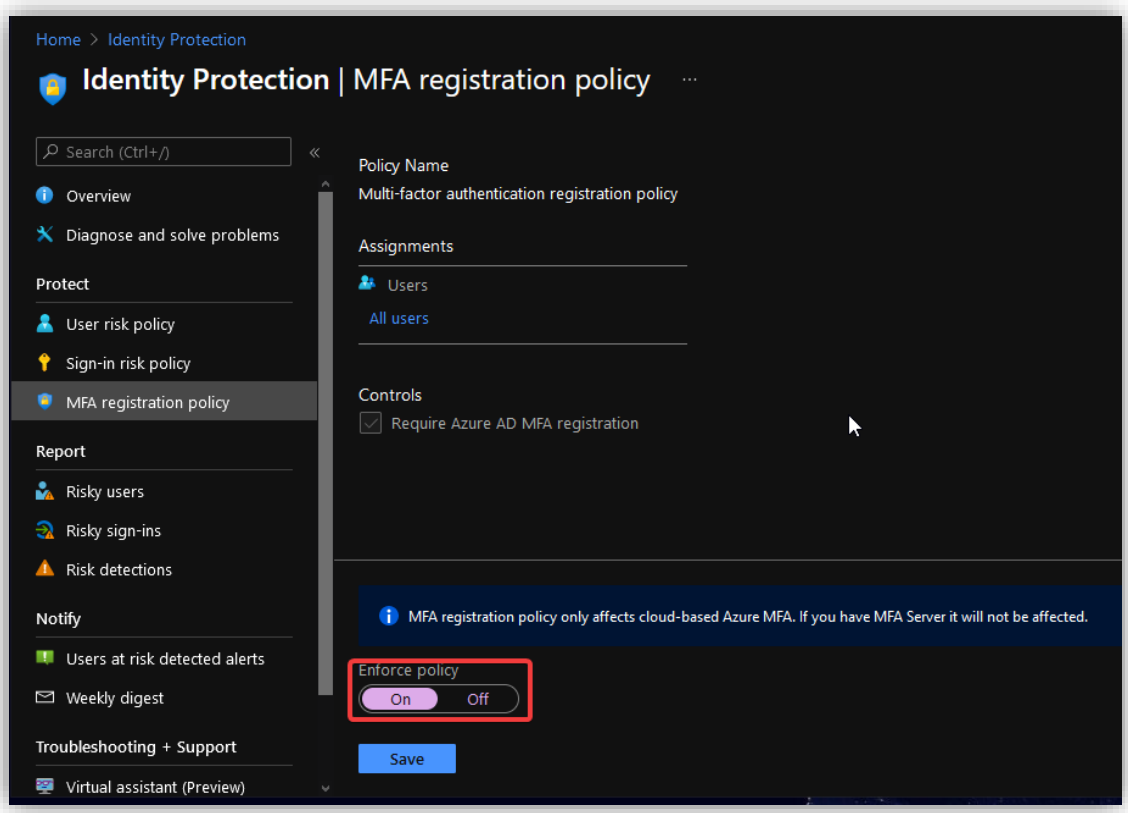


[16] https://portal.azure.com/#blade/Microsoft_AAD_IAM/IdentityProtectionMenuBlade/Overview

Sett de samme innstillingene under **User risk policy**. Dersom Microsoft vurderer det til å være en risiko for at brukeren er kompromittert, vil dette tvinge fram at passordet må resettes.



Under **MFA registration policy,** sett **Enforce policy** til **On**. Dette sørger for at alle brukere må registrere for MFA første gang de logger inn.



3.9.3 Azure Sentinel

Azure Sentinel[17] er et verktøy som brukes til å hente inn, analysere og utføre sikkerhets prosedyrer på datasystemet til en organisasjon. Dette kan brukes til (blant annet) å loggføre data, sende beskjeder dersom det er skjedd en hendelse og å visualisere loggført data for å få en bedre oversikt. Azure Sentinel behøver ingen servere for å overvåke Azure-miljøet og ressursene, skalering skjer altså automatisk.

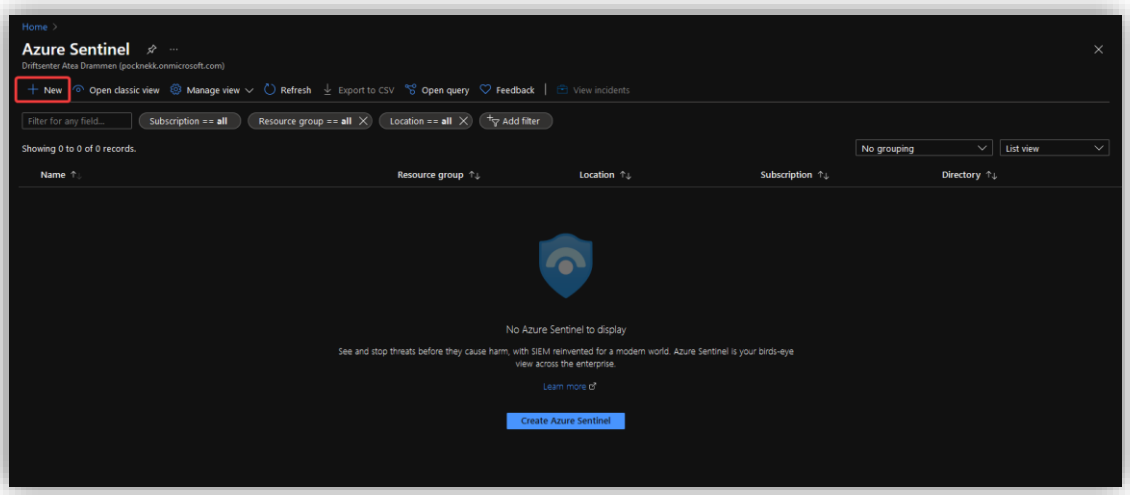
Azure Sentinel har tre alternative implementeringer:

1. Single-Tenant with a single Azure Sentinel Workspace
2. Single-Tenant with regional Azure Sentinel Workspace
3. Multi-Tenant

For oss vil det være det første valget som er mest aktuelt. I dette tilfellet er det en enkelt tenant og det brukes en enkelt *resource group* og *workspace*. Man skal da altså kun hente inn data fra et arbeidsområde og lagre dette på et og samme sted. Dette valget krever også minst konfigurasjon. Dersom data kommer til å bevege seg over flere regioner og dette strider med datastyringen vil det være lurt å velge alternativ nummer 2. Da kan en holde dataen i de regionene som kreves.

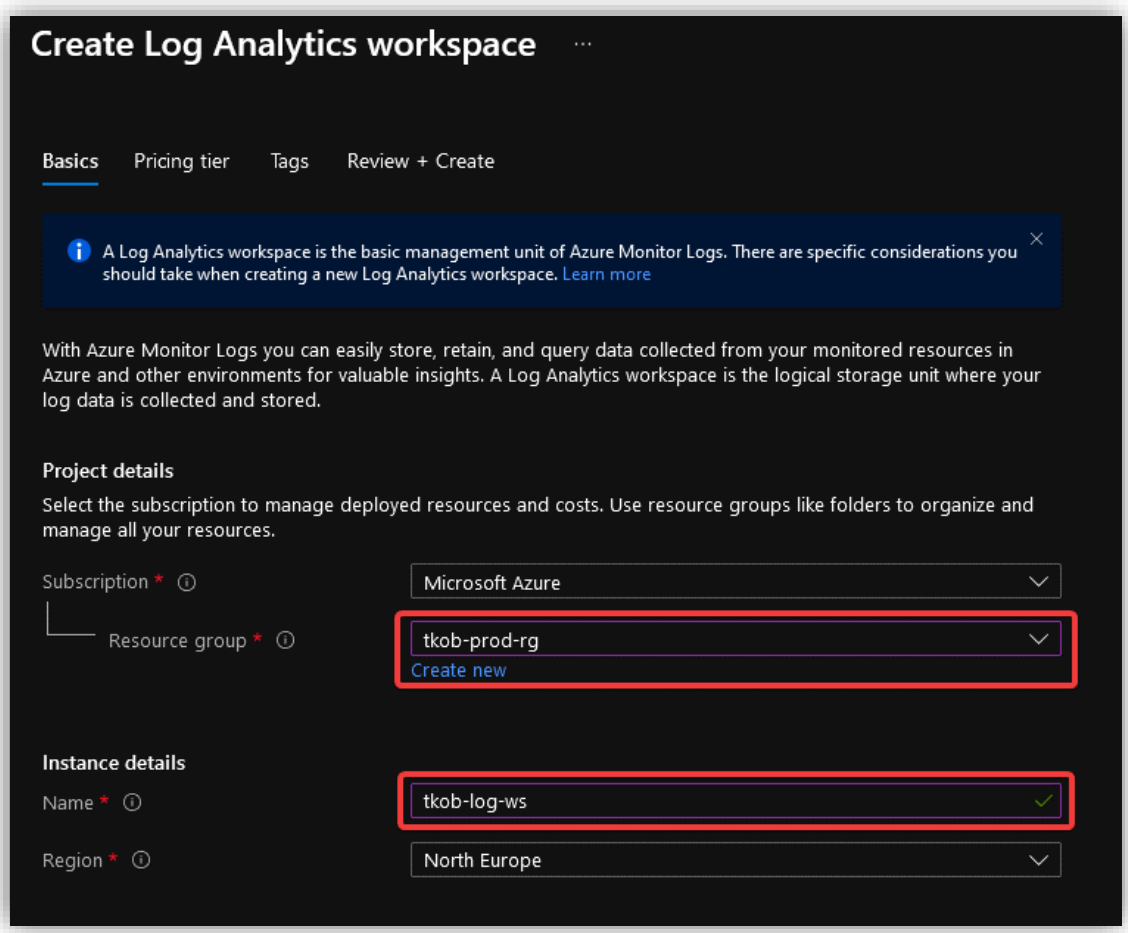
3.9.3.1 Utrulling av Azure Sentinel

I **Azure portalen**, gå inn i **Azure Sentinel** og trykk på **New.**

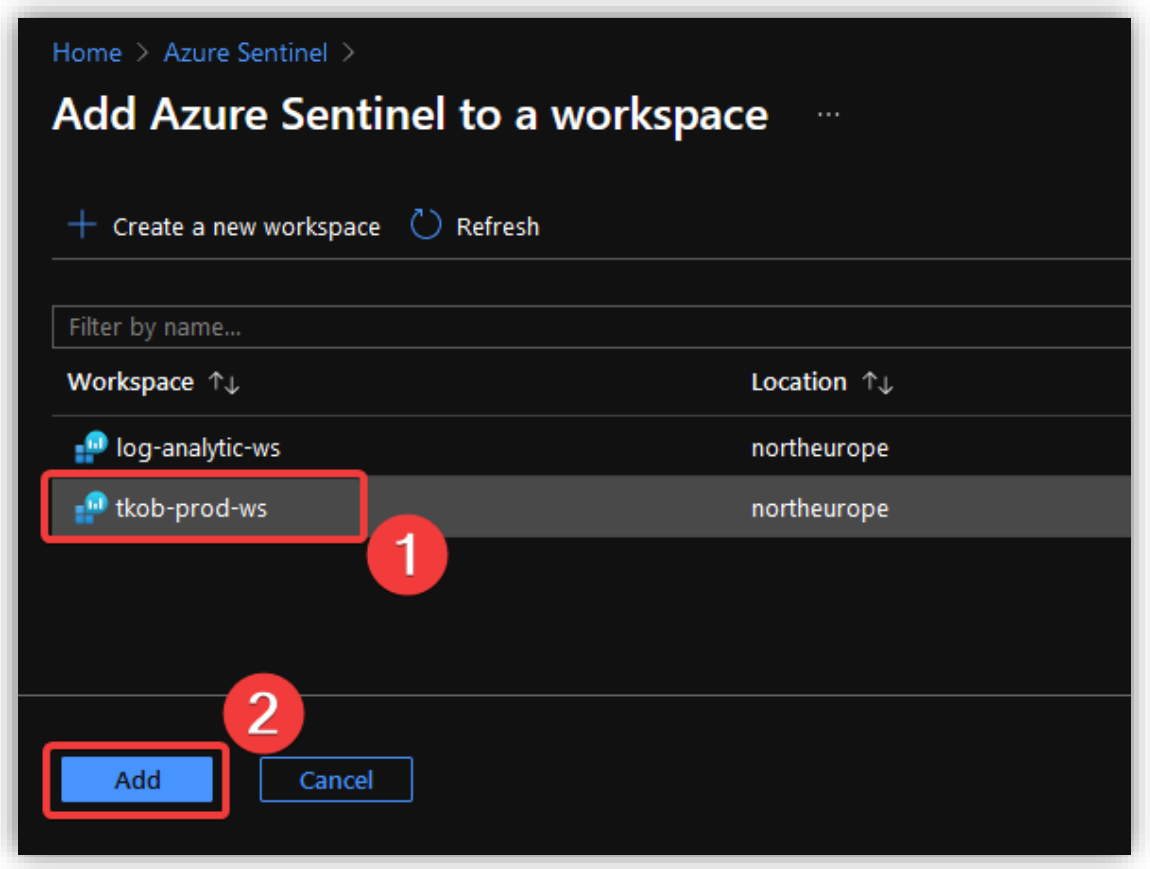


17 https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Trykk så på **Create a new workspace**, velg **Resource group** og gi et passende navn. Trykk så på **Review + Create** og så **Create.**



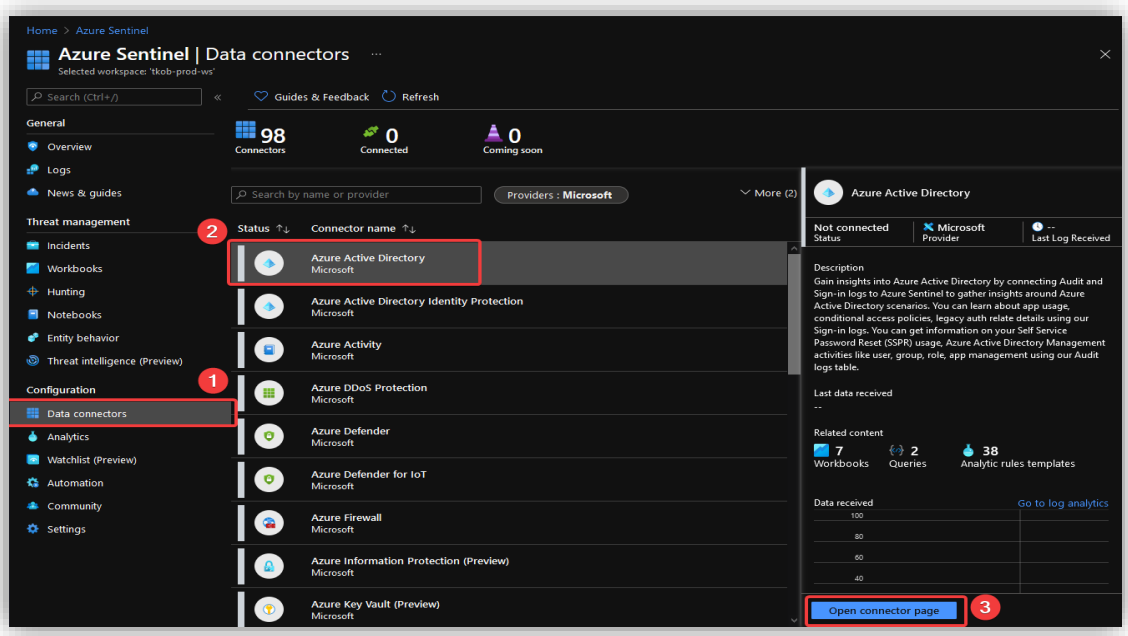
Legg så det nye Workspace-et til i Sentinel ved å velge det og trykke **Add.**



3.9.3.2 *Koble Sentinel til datakilder*

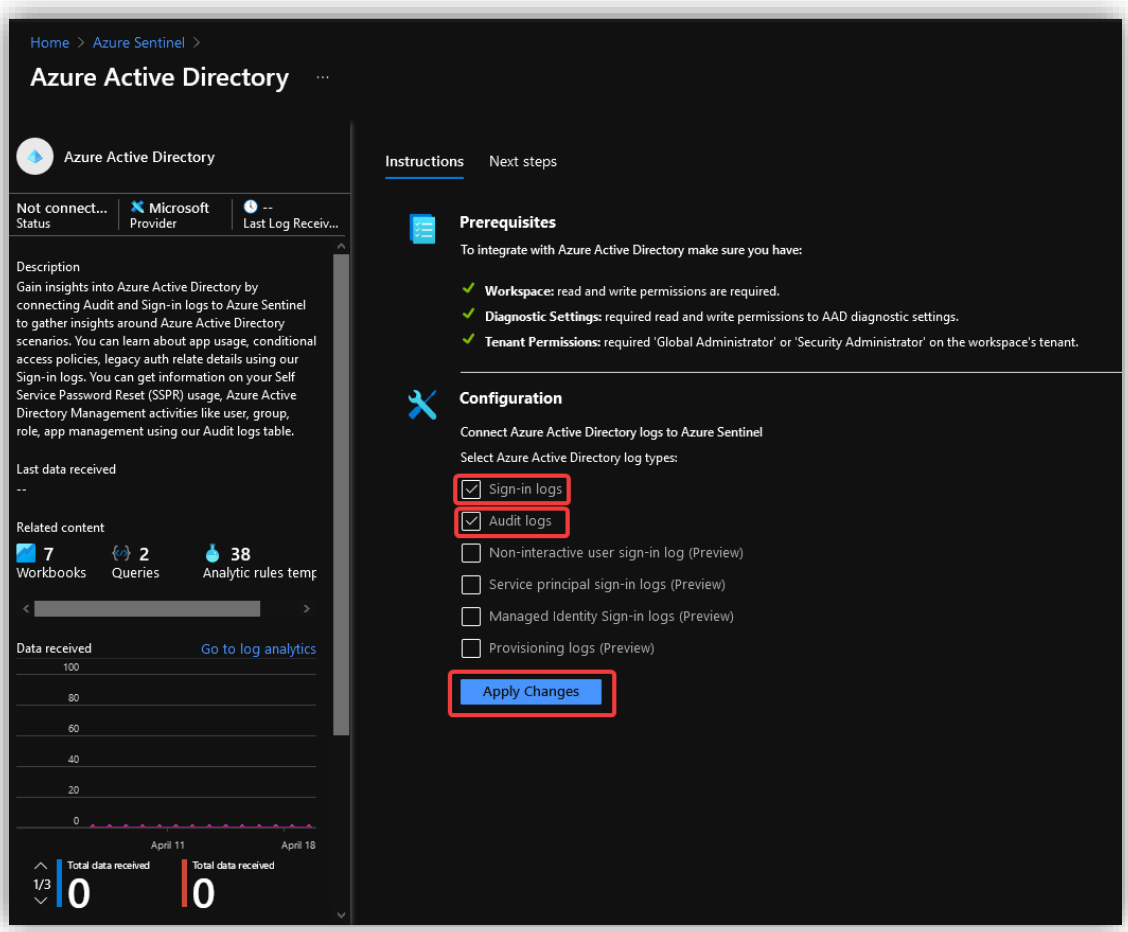
Etter at Sentinel er satt opp og koblet til et *workspace,* er det neste steget å koble datakilder til *workspacet*. Dette gjør at all data blir sendt til et og samme sted og overvåking av disse ressursene blir sentralisert.

For å koble Azure AD til Sentinel, gå inn i **Azure Sentinel > [Aktuelt WS] > Data connectors.** Trykk så på **Azure Active Directory** og **Open connector page.**



Huk av for **Sign-in logs** og **Audit logs**. Trykk så på **Apply Changes**.

- **Sign-in logs:** Gir informasjon om bruken av administrerte applikasjoner og innloggingsaktiviteter.
- **Audit logs:** Gir systemaktivitetsinformasjon om bruker- og gruppeadministrasjon, administrerte applikasjoner, og katalog aktiviteter.



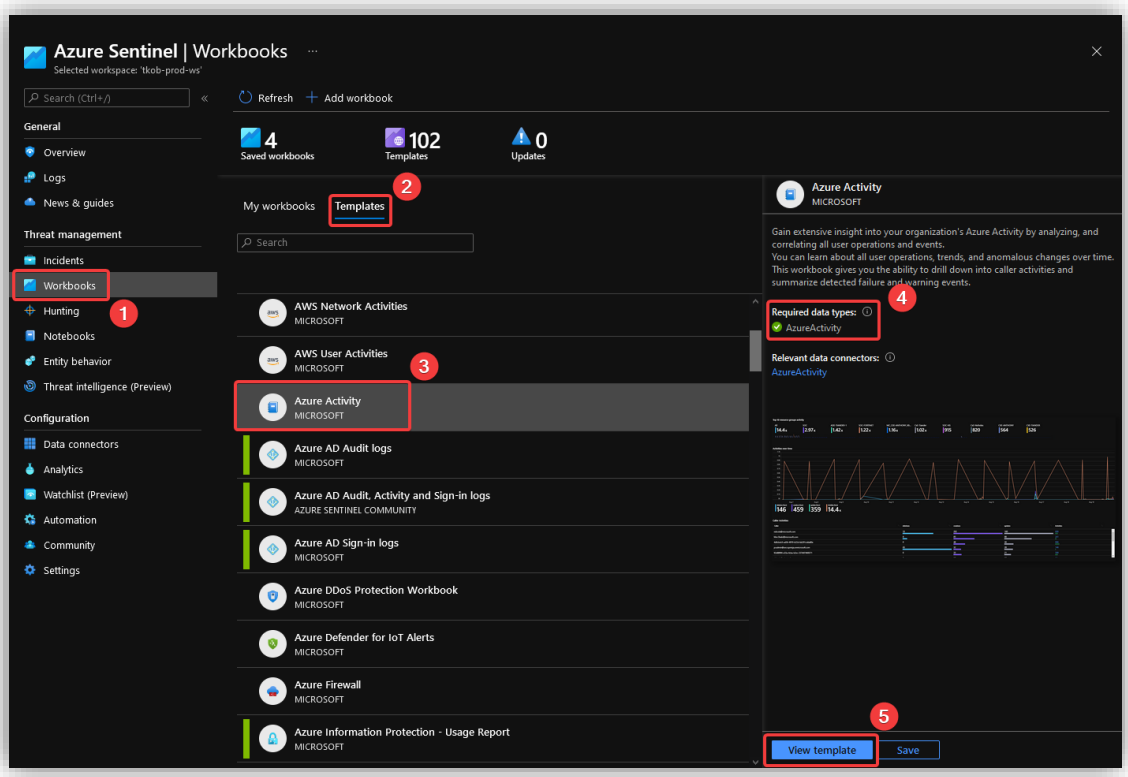
Det vil variere litt hvordan en kobler til de ulike datakildene, men det er som regel relativt intuitivt. Koble til følgende datakilder:

- Azure Active Directory
- Azure Active Directory Identity Protection
- Azure Activity
- Azure Defender
- Azure Information Protection
- Microsoft 365 Defender
- Microsoft Cloud App Security
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Office 365

3.9.3.3 *Overvåking av datakilder*

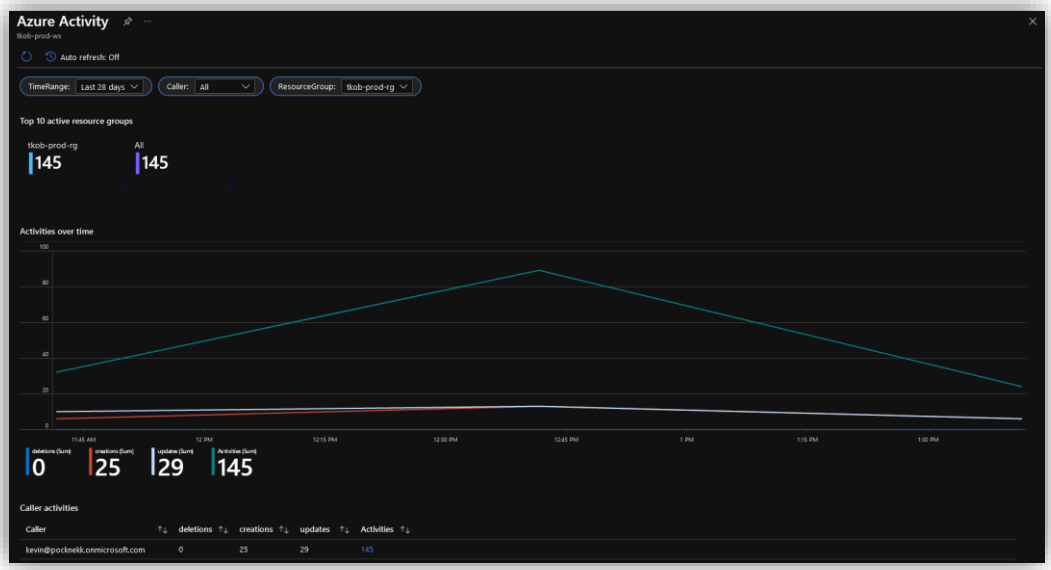
Etter å ha koblet til ulike datakilder (Data connectors), er det på tide å overvåke de ulike tjenestene. Ved å ta i bruk ulike **workbooks** vil Sentinel visualisere data fra de ulike kildene for oss. En kan lage egne workbooks eller en kan bruke de innebygde – i dette tilfellet tas de innebygde i bruk.

Gå inn i **Azure Sentinel**[18] **> Workbooks > Templates** og trykk på templaten som heter **Azure Activity.** I panelet på høyre side, sjekk først at du oppfyller alle krav. Trykk så på **View template** for å se oversikten over dataen denne templaten vil vise.

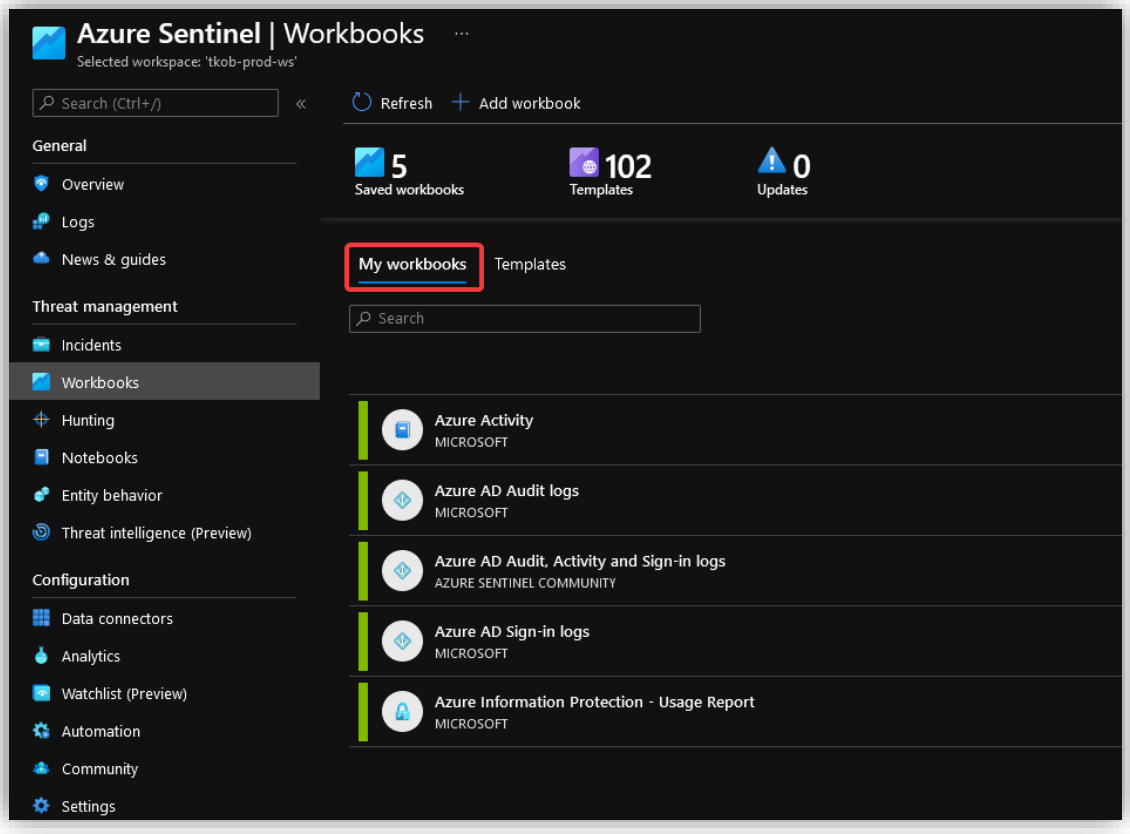


18 https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Denne templaten gir en oversikt over aktivitet i Azure over tid.



Trykk på krysset øverst i høyre hjørne for å gå tilbake. Trykk så på **Save** for å lagre templaten. Du vil så bli spurt om hvilken lokasjon dataen skal lagres. Velg **North Europe** ettersom dette er lokasjonen nærmest hvor bedriften holder til. Lagrede workbooks finner du under **My wokbooks.**



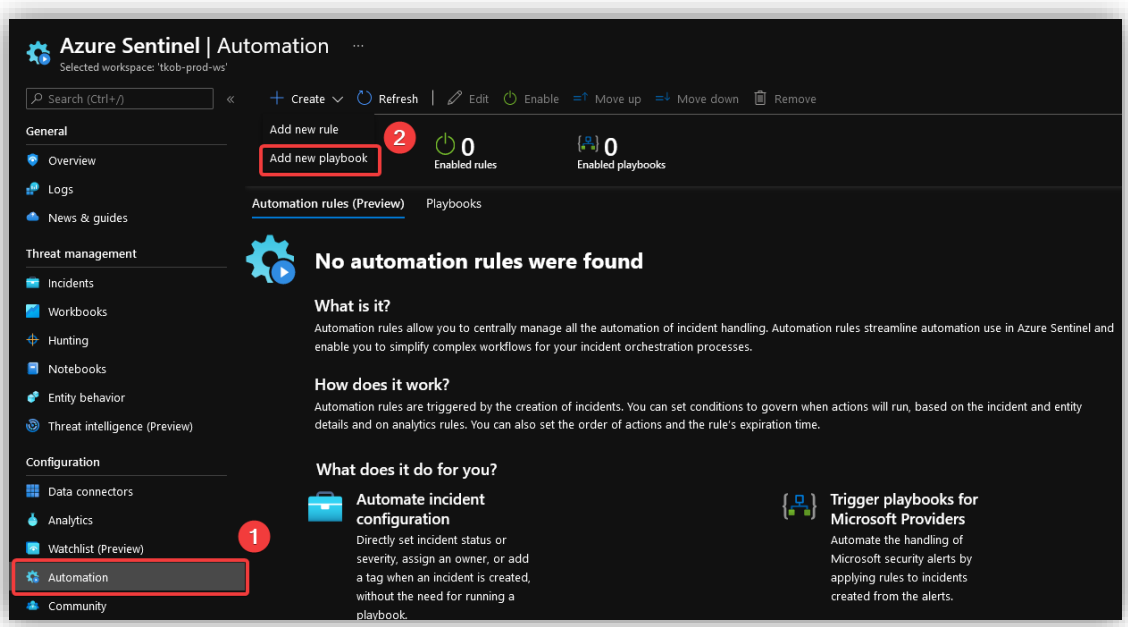
3.9.3.4 Automatiser trusselhåndtering

Automatiseringsregler kan brukes til å tildele hendelsen til riktig personell, lukke uviktige hendelser eller kjente falske positiver, endre alvorlighetsgrad, eller legge til en tag. Med **Automation** er det også mekanismer som lar en bruke **playbooks** til å respondere på hendelser. **Playbooks** er en samling med prosedyrer som kan kjøres fra Azure Sentinel for å håndtere et varsel eller en hendelse. Playbooks er basert på *workflows* i **Azure Logic Apps**, dette kan påføre ekstra kostnader.

3.9.3.4.1 Lag playbook

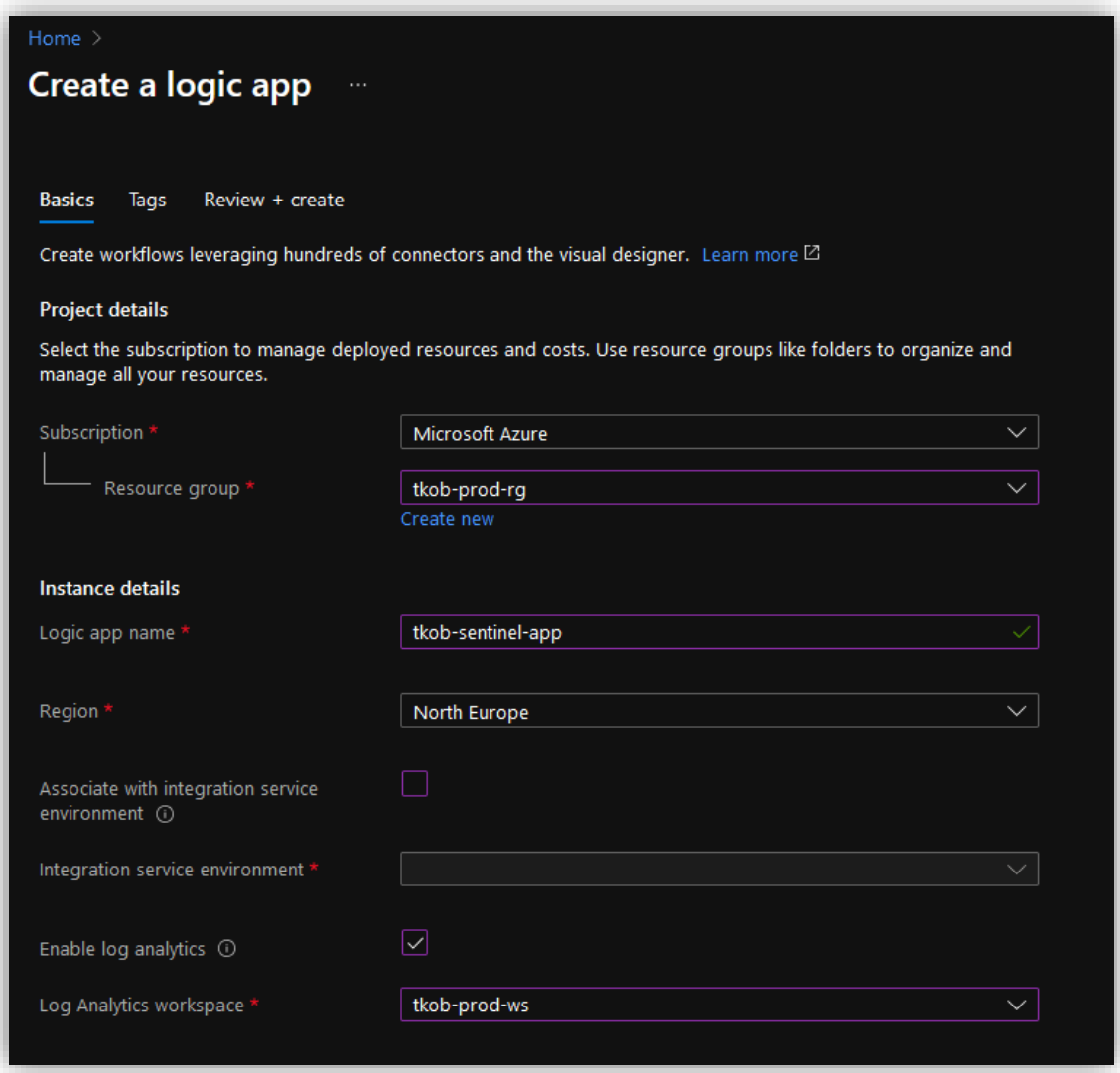
Følg disse stegene for å lage en ny playbook for å sende en melding til IT-avdelingen gjennom Slack når det dukker opp en hendelse.

I **Azure Portalen,** gå til **Azure Sentinel**[19] **> Automation** og trykk på **Create > Add new playbook.**

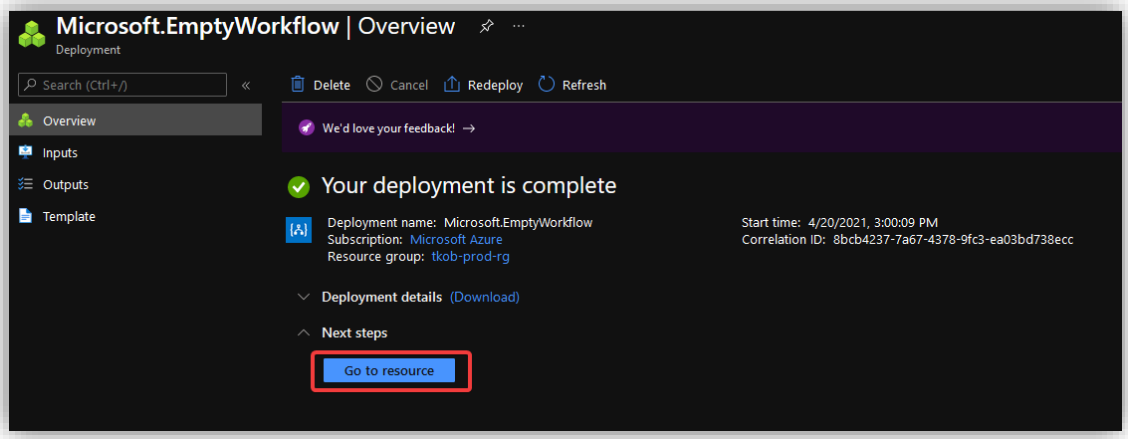


19 https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

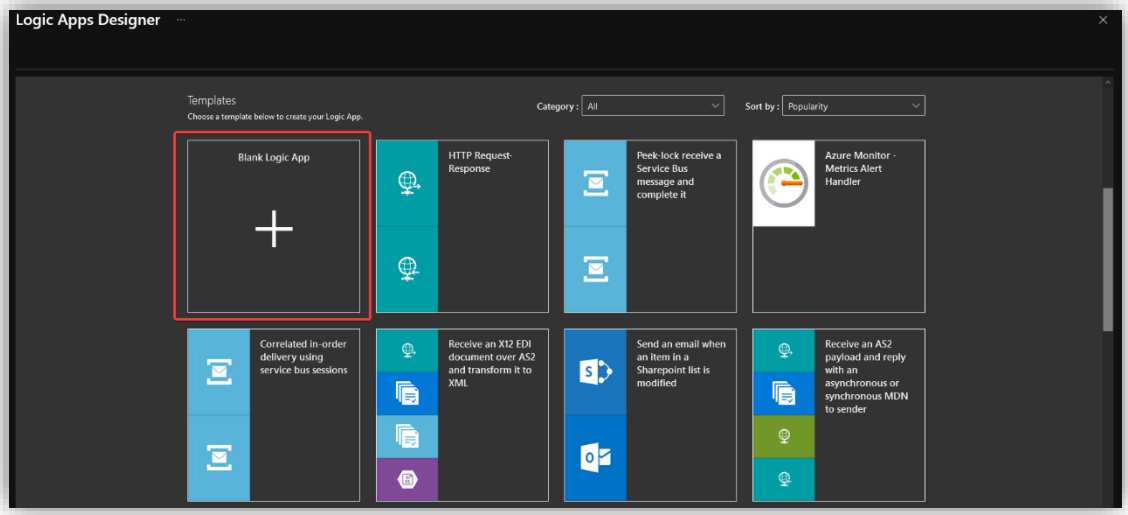
Velg aktuell **Resource group**, gi et passende navn, huk av for **Enable Log Analytics** og velg aktuelt **workspace.** Dette gjør at en kan overvåke hendelsene i applikasjonen gjennom valgt workspace.



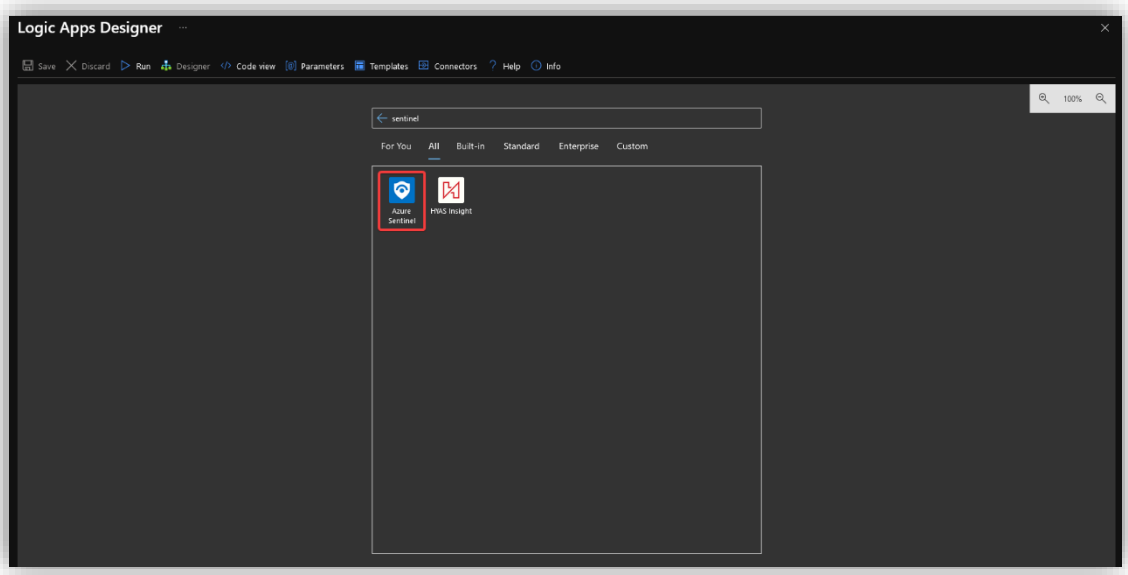
Trykk på **Review + create** og så **Create.** Når applikasjonen er ferdig utrullet, trykk på **Go to resource.**



Trykk på **Blank Logic App.**

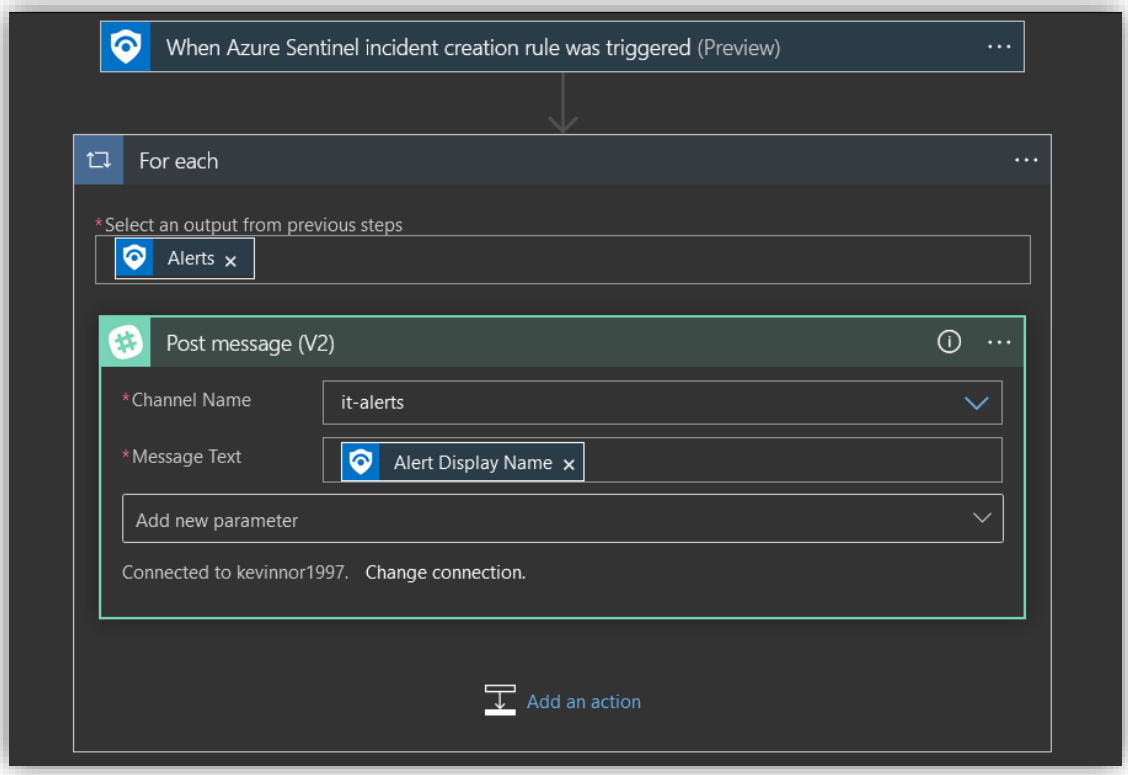


Velg så **Azure Sentinel**, ettersom det er der input kommet fra i dette tilfellet.



Velg så **When Azure Sentinel incident creation rule was triggered**. Dette gjør at en kan bruke **automation rules** for å automatisk utløse denne **playbooken.** Dette blir utløseren av de neste stegene.

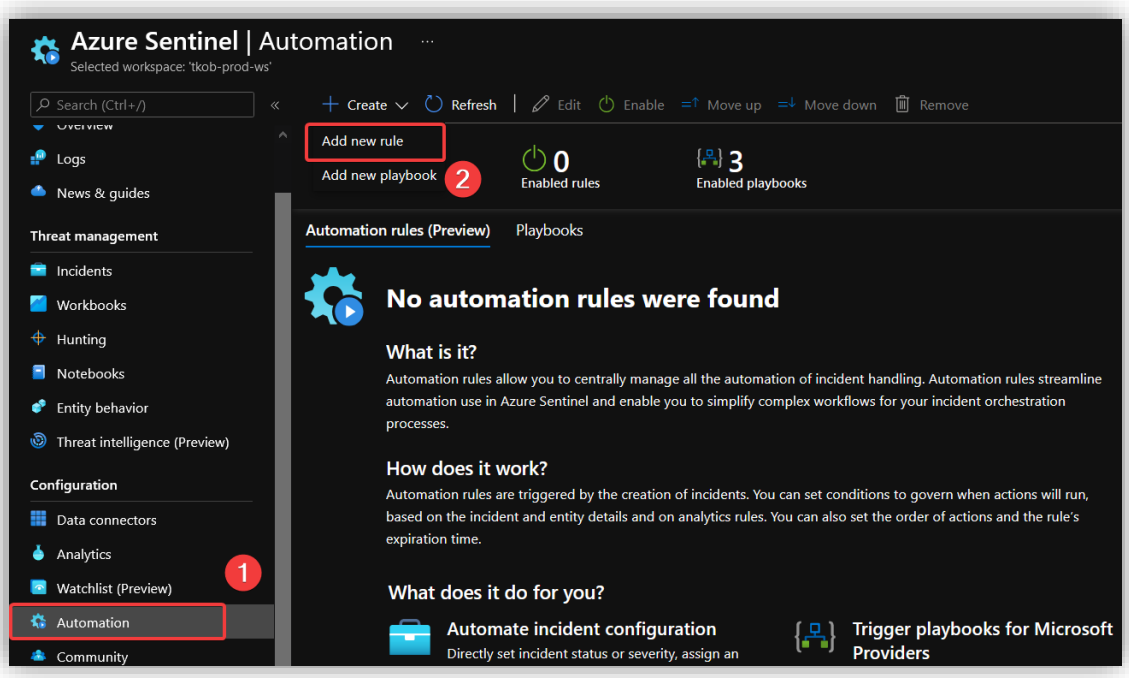
Lag et enkelt varselssystem ved å koble til Slack og sende en beskjed i “it-alerts”-kanalen. Ved å legge inn en **For each**-løkke, vil det bli sendt en melding til Slack for hver **Alert.**



3.9.3.4.2 Lag automation rule

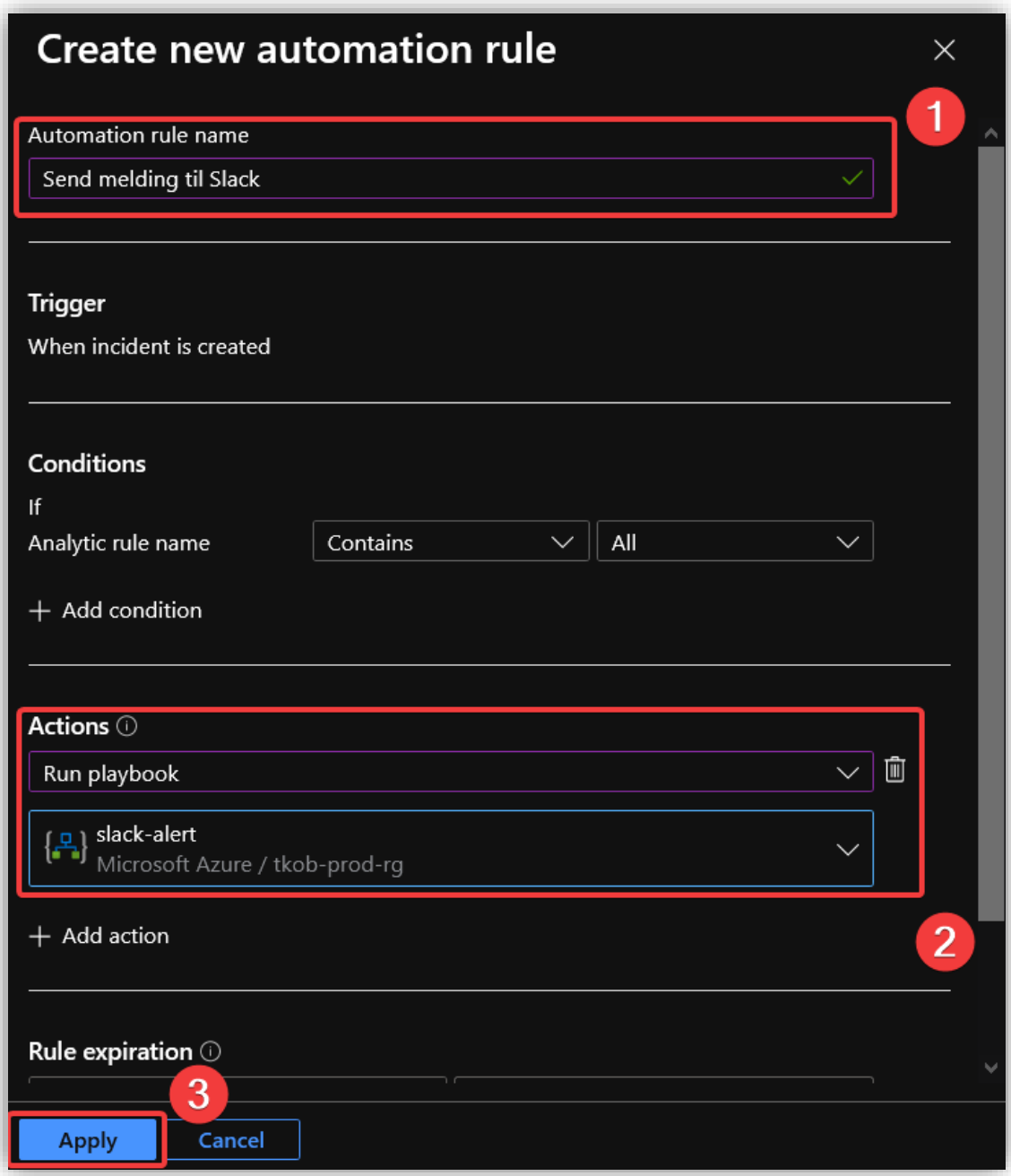
Etter å ha lagd en **playbook,** må denne på en eller annen måte bli utløst. Hva som skal utløse en playbook defineres i en **automation rule** - man kan også utløse andre hendelser enn playbooks, for eksempel å gi hendelsen en eier eller endre risikonivå.

Under **Azure Sentinel**[20] **> Automation,** trykk på **Add new rule.**

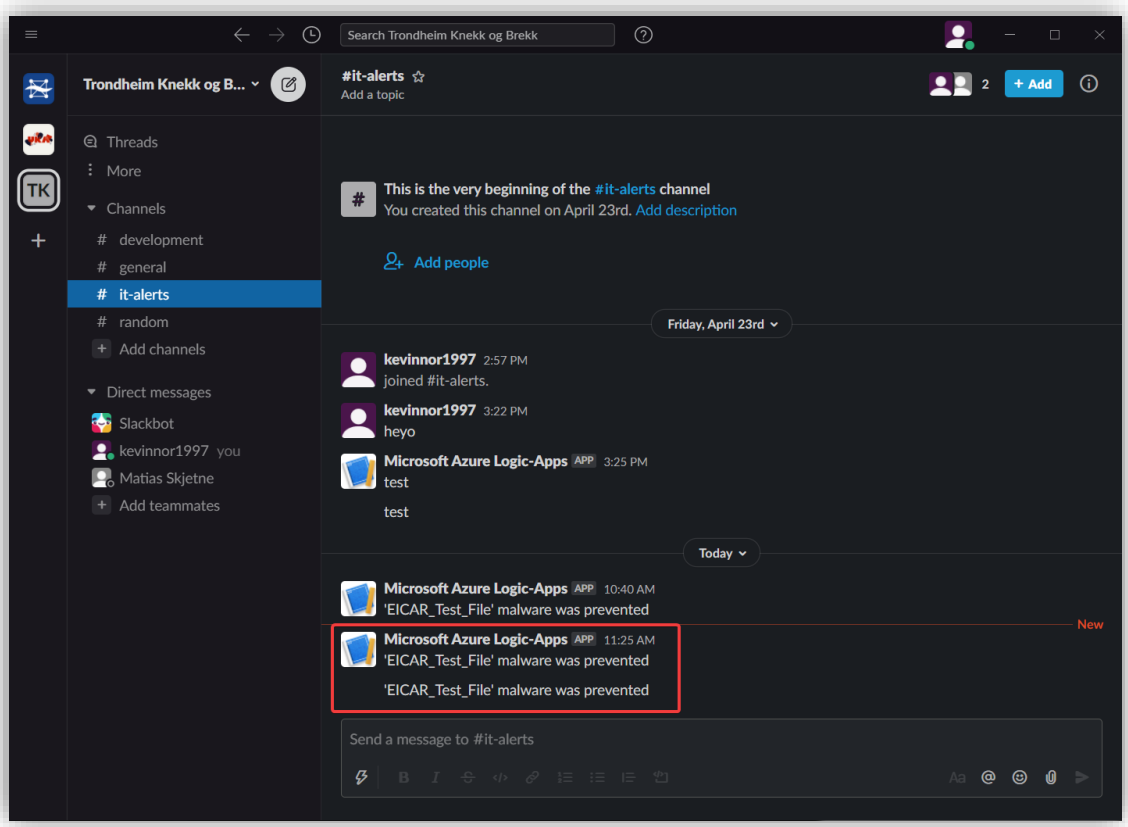


20 https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Gi regelen et passende navn og la **Condition** stå på **All** slik at regelen inntreffer ved alle hendelser. Under **Actions**, velg **Run playbook** og velg den aktuelle playbooken som skal utløsesn. Trykk så på **Apply.**



En kan teste regelen ved å kjøre EICAR-testfil i en AAD Joined enhet. Her har en melding blitt sendt til Slack etter at Windows Defender oppdaget filen og markerte det som en trussel.



3.9.4 Microsoft Defender for Endpoint

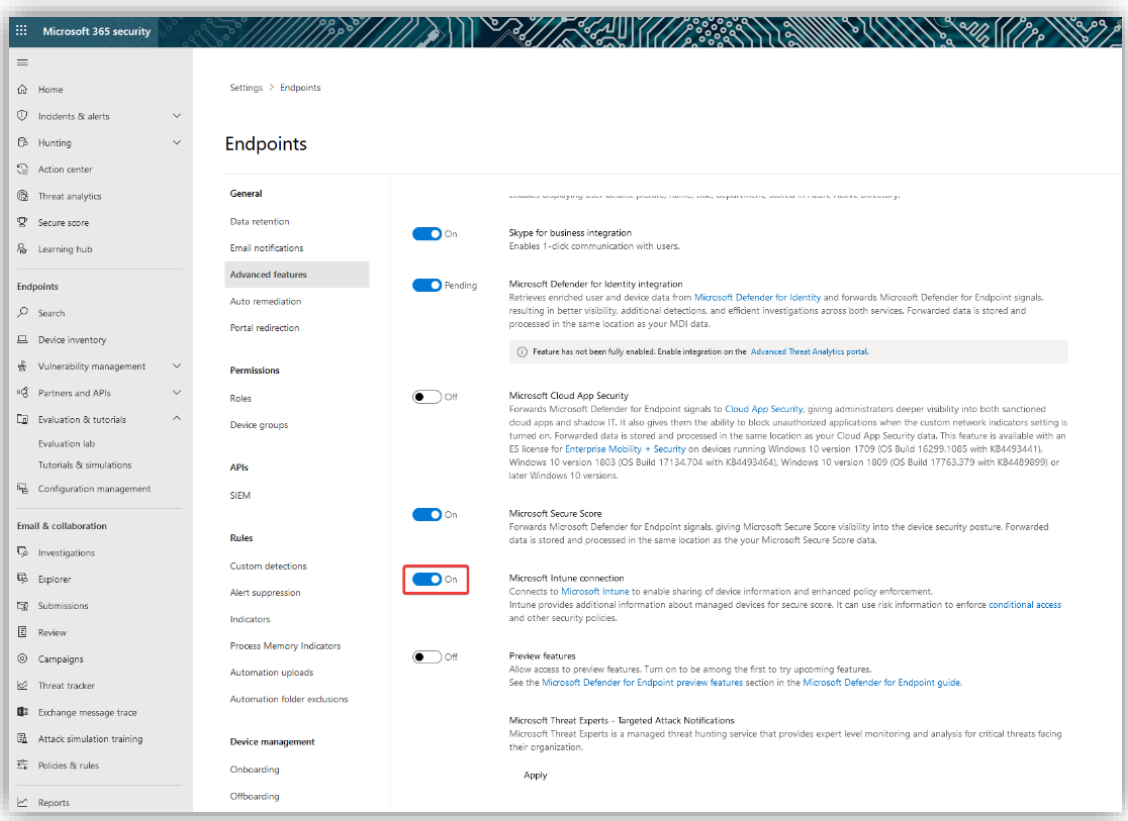
Ved hjelp av Microsoft Intune kan man integrere Microsoft Defender for Endpoint Protection som en Mobile Threat Defense-løsning. Dette kan hjelpe mot å forhindre innbrudd og begrense skadeomfanget av et eventuelt innbrudd.

Microsoft Defender for Endpoint fungerer for enheter som kjører:

- Android
- IOS/iPadOS
- Windows 10 eller senere

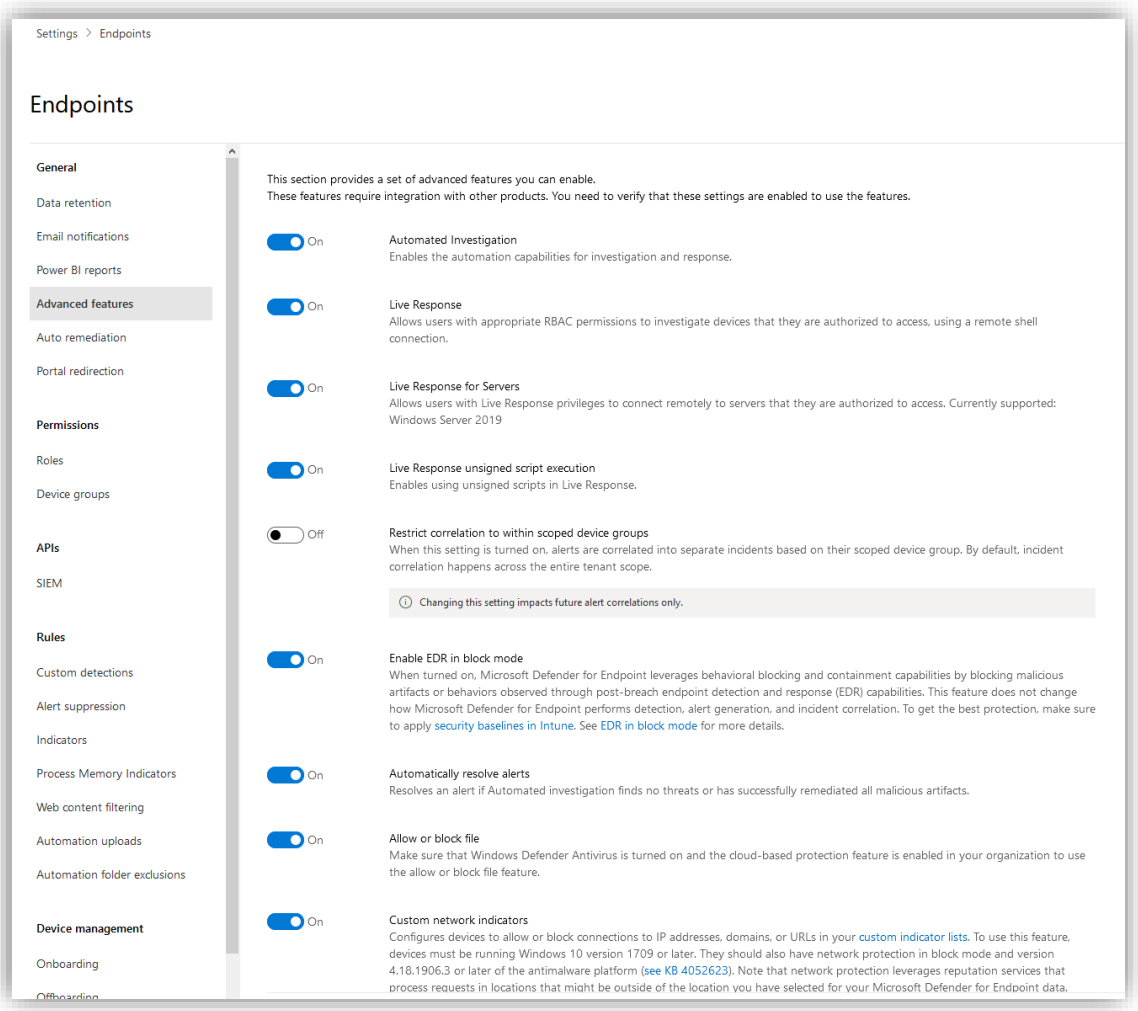
3.9.4.1 Aktiver Microsoft Defender for Endpoint

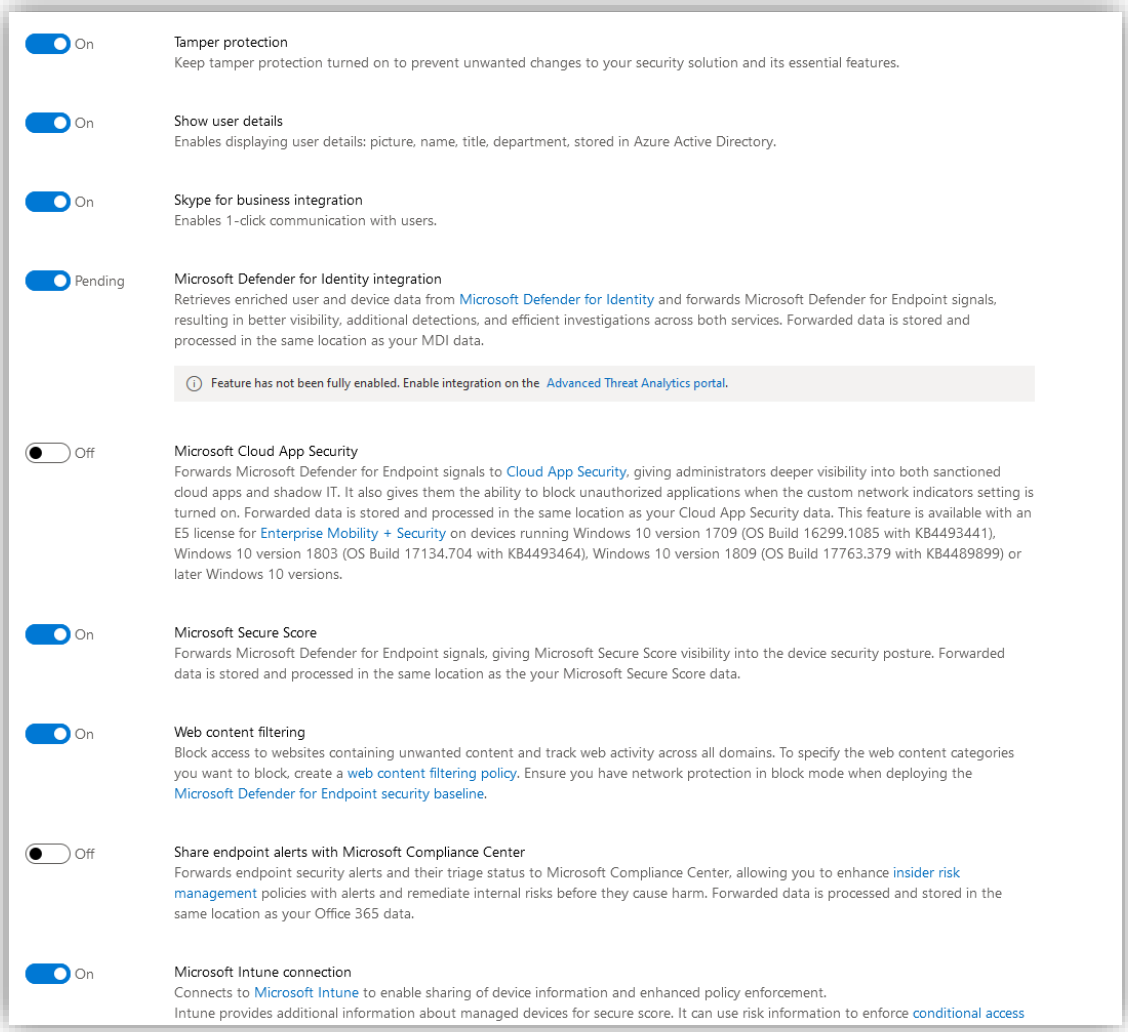
Logg inn i **Microsoft 365 Security**[21], gå til **Settings > Endpoints > Advanced features** og huk av for **Microsoft Intune connection**. Dette aktiverer service-to-service-tilkobling mellom Intune og Microsoft Defender for Endpoint. Dette gjør at en kan hente ut risikodata på enhetene som er koblet til Intune.

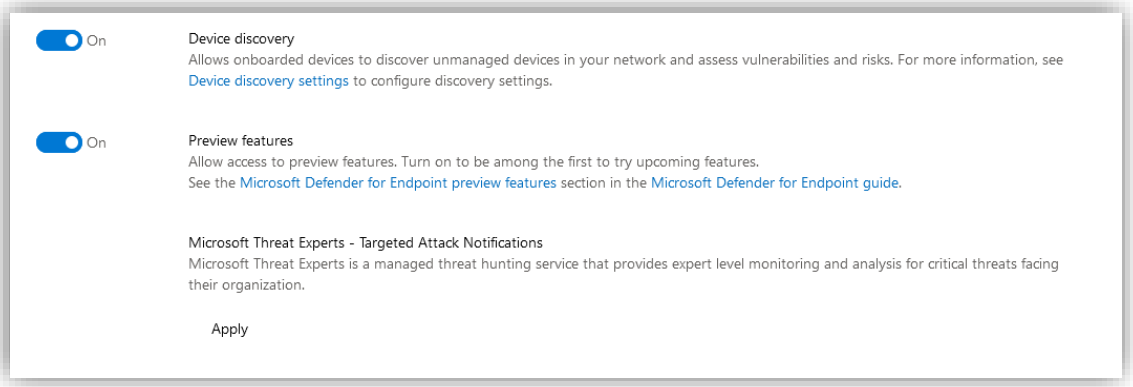


[21] https://security.microsoft.com/?rfr=AdminCenter

På bildene under er en rekke andre sikkerhetsfunksjoner også skrudd på. Skru på disse. Dette gir ulike administrative muligheter. Det blokkerer også muligheten for en admin-bruker til å endre innstillinger i Windows Defender.





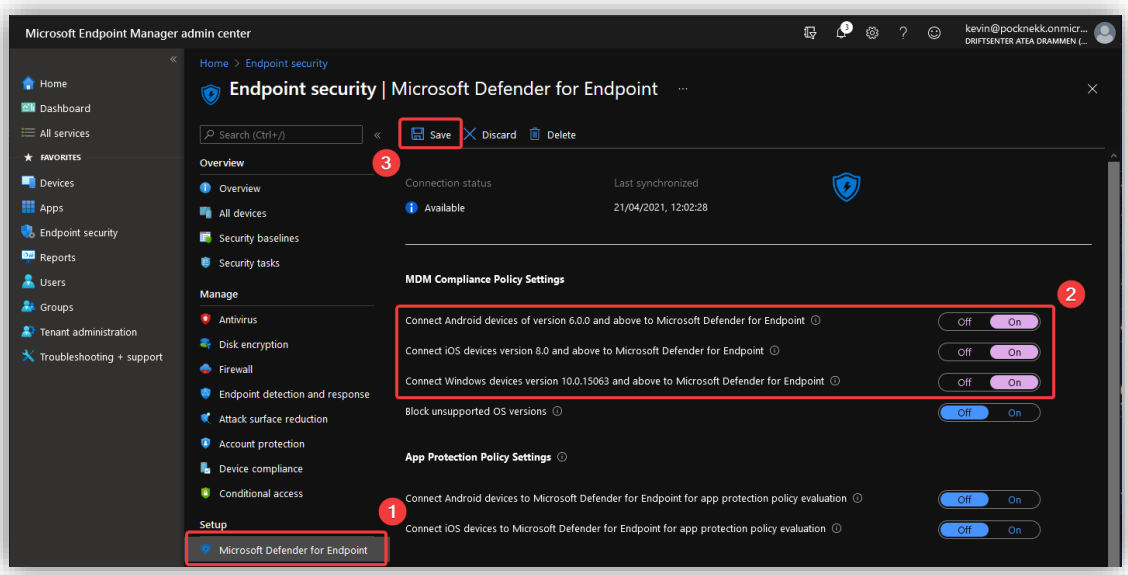


Gå så til **Microsoft Endpoint manager admin center[22] > Endpoint security > Microsoft Defender for Endpoint**.

[22] https://endpoint.microsoft.com/?ref=AdminCenter#home

Under **MDM Compliance Policy Settings** kan en huke av for hvilke typer enheter en ønsker å ta i bruk Microsoft Defender for Endpoint på.

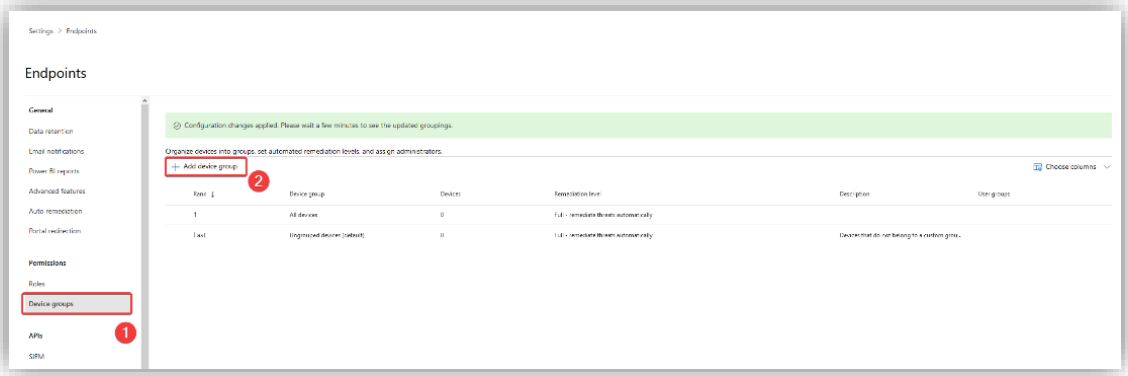
Huk av for **Android, iOS** og **Windows**, trykk så på **Save.**



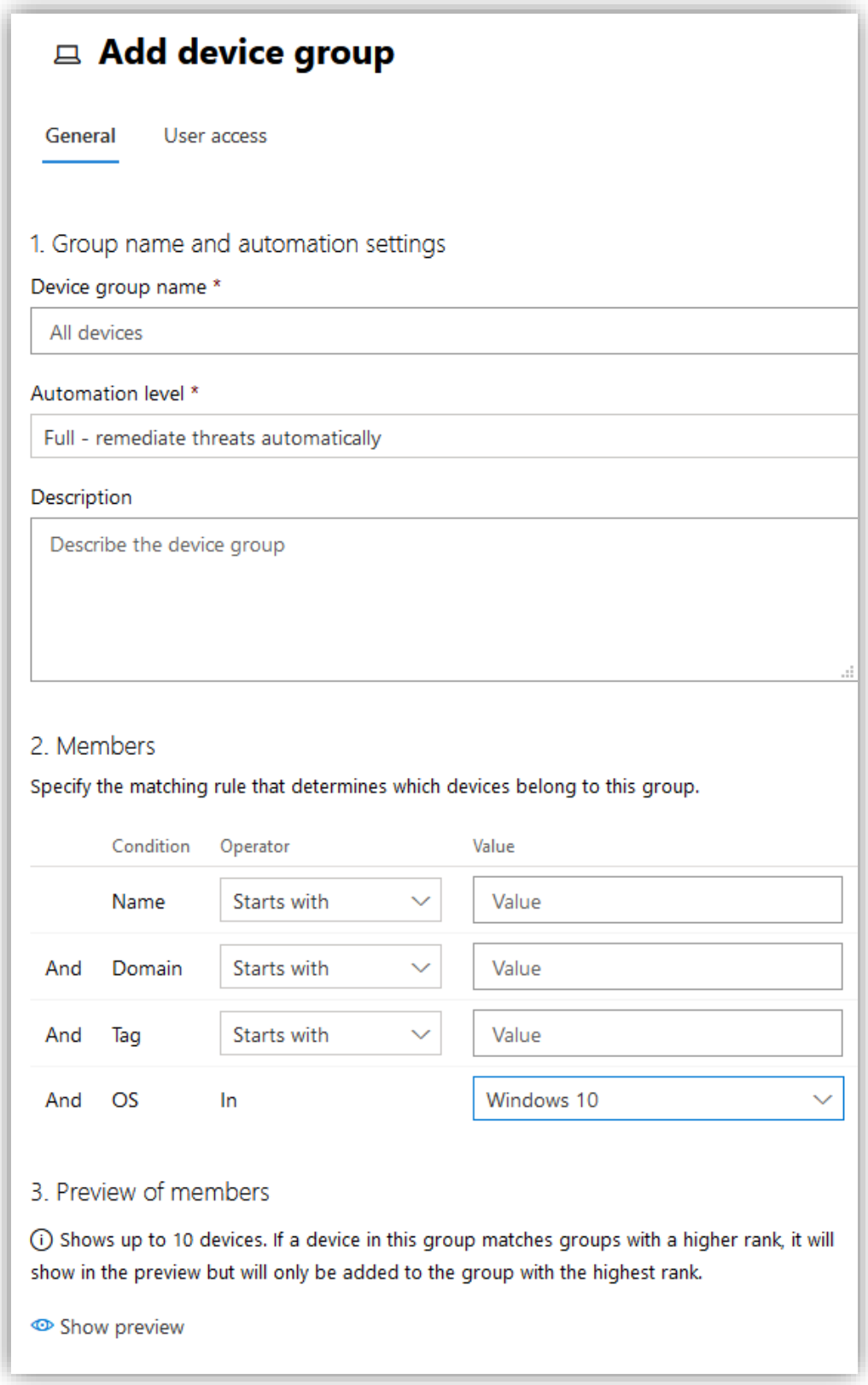
3.9.4.2 Lag en device group

For at policyer og regler skal gjeldene for alle enheter må en lage en **device group** og definere hvilke saneringsnivå som skal tillegges.

Under **Settings > Endpoints > Device groups**, trykk på **Add device group.**



Kall gruppen “All devices”. Sett **Automation level** til **Full – remediate threats automatically** og legg til at alle enheter som bruker Windows som OS skal legges til i gruppen.

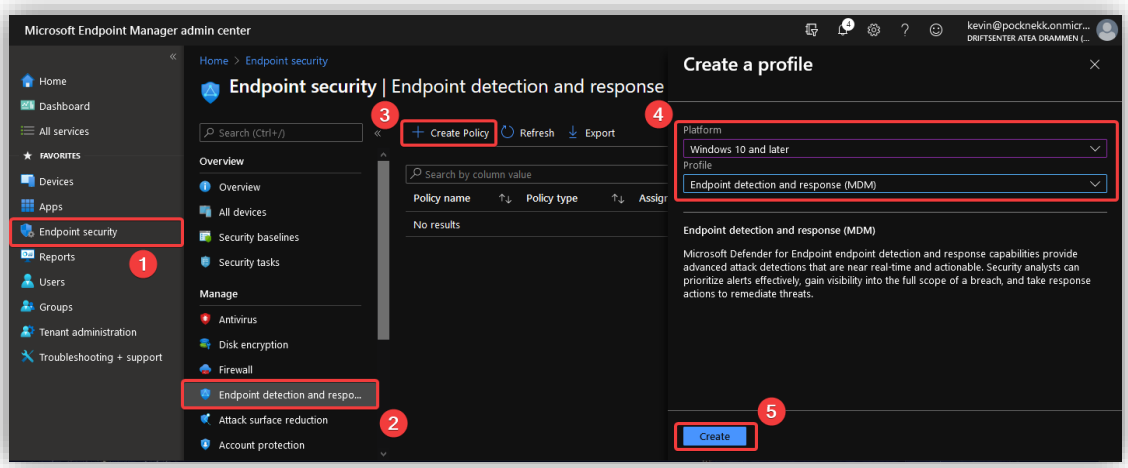


Trykk så på **Done** for å fullføre.

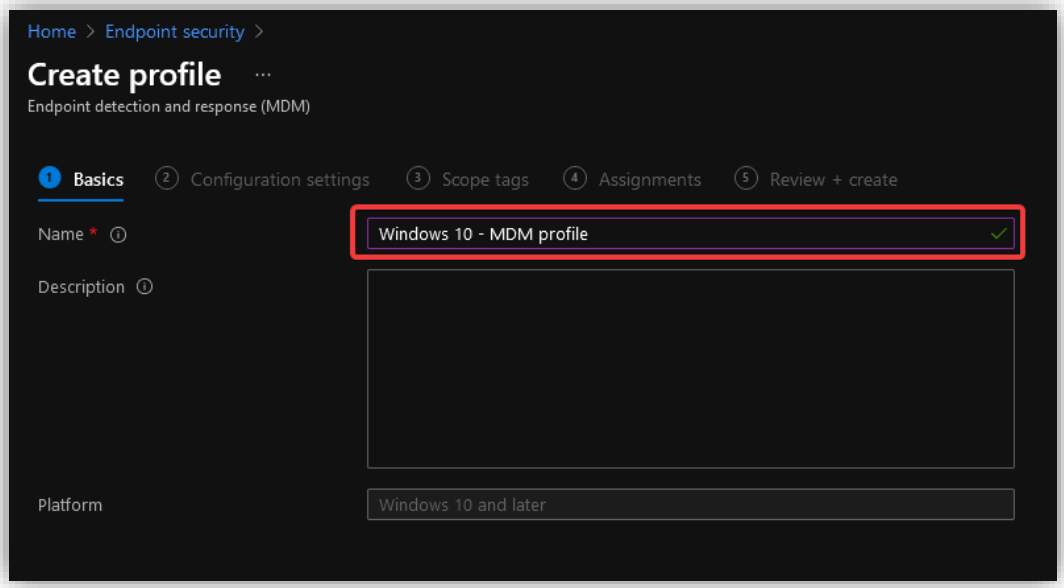
3.9.4.3 Lag enhetskonfigurasjonsfil for Windows-enheter

Etter å ha koblet sammen Intune og Microsoft Defender for Endpoint, mottar Intune en konfigurasjonspakke fra Microsoft Defender for Endpoint. En bruker så en konfigurasjonsprofil for Microsoft Defender for Endpoint for å rulle ut pakken til Windows-enhetene. Denne konfigurasjonspakken konfigurerer enhetene til å kommunisere med Microsoft Defender for Endpoint sevices for å scanne filer og oppdage trusler. Enheten rapporterer også risikonivået basert på dine compliance policyer.

I **Microsoft Endpoint Manager admin center**[23], gå til **Enpoint security > Endpoint detection and response** og trykk på **Create Policy.** Velg **Windows 10 and later** som plattform og **Endpoint detection and response (MDM)** som profil. Trykk så på **Create.**

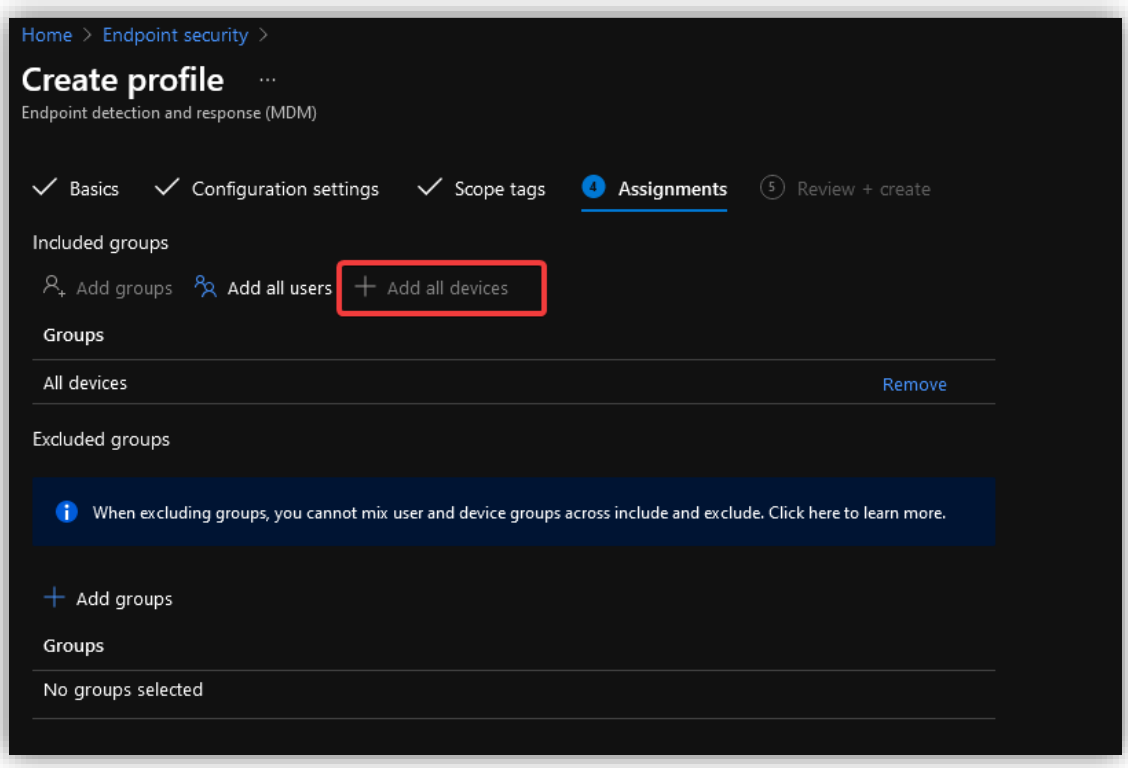


I **Basics**-tabben, skriv inn et passende navn.



[23] https://endpoint.microsoft.com/?ref=AdminCenter#home

Under **Assignments**, legg til **All devices** under **Included groups.**

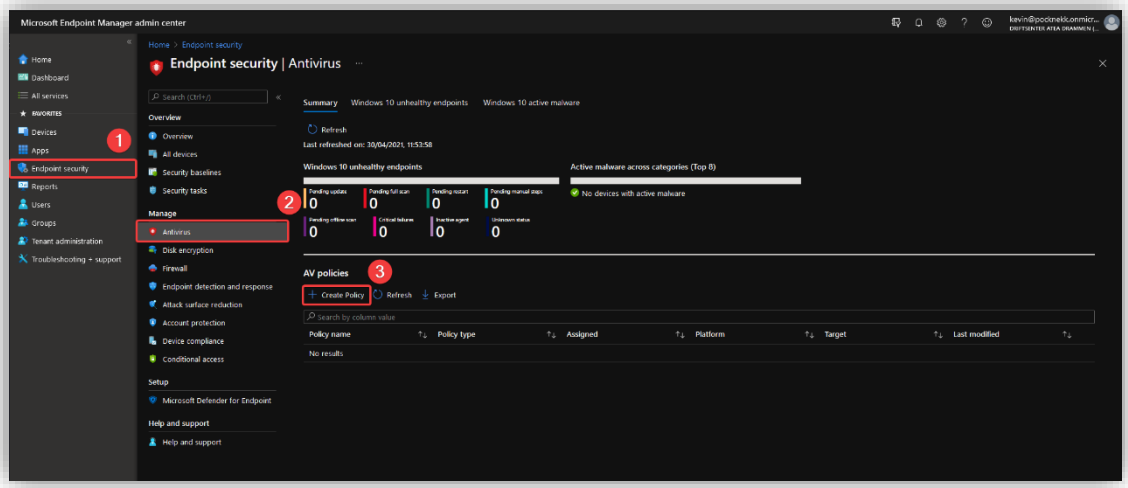


Naviger videre til **Review + create** og trykk **Create.** Den nye profilen vil nå legge seg i listen over konfigurasjonsprofiler.

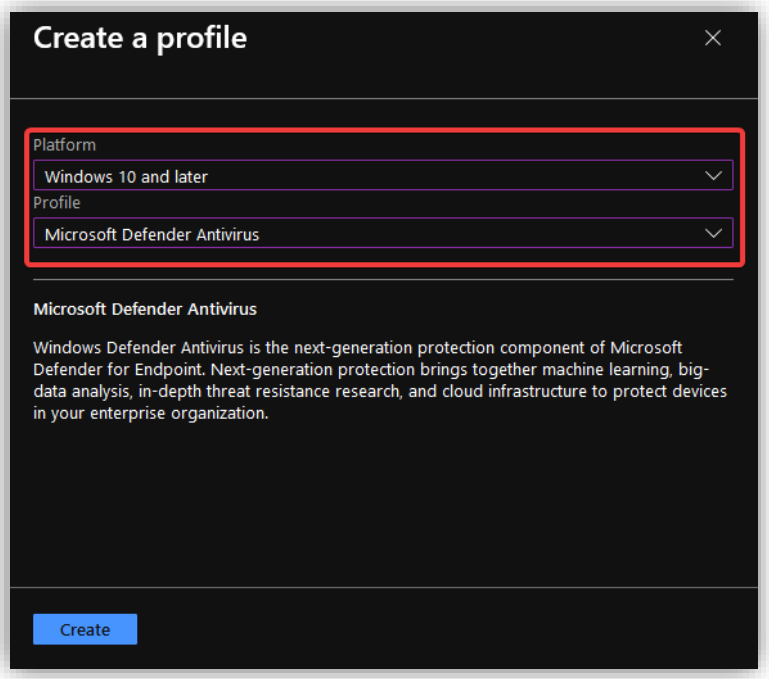
3.9.4.4 Lag antivirus policy

Ved å ta i bruk **antivirus policy** kan en administrere Windows Defender for alle enhetene for å øke sikkerheten. Dette gjør at brukere selv ikke kan skru av antivirus-funksjoner som kan la skadevare komme inn på enheten. Konfigureringen vist under vil være av den strenge typen, dette er for å følge "zero trust"-modellen. Dersom det viser seg å være for strenge tiltak, kan en heller lette på noe av konfigureringen.

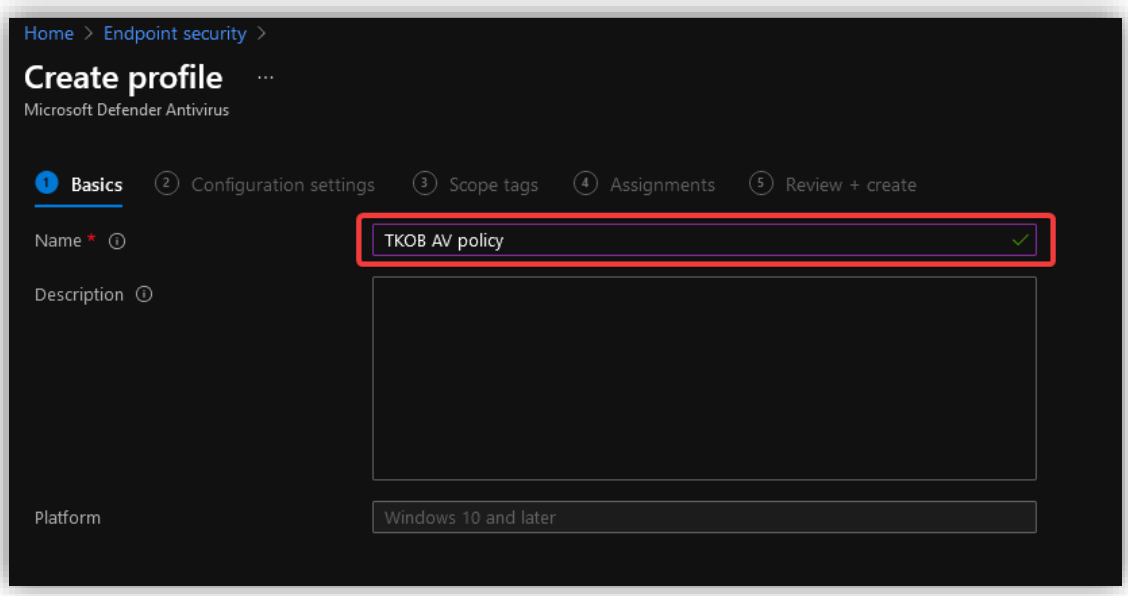
For å lage en policy, gå under **Endpoint security > Antivirus** og trykk på **Create Policy**.



Under **Create a profile**, velg **Windows 10 and later** som plattform og **Microsoft Defender Antivirus** som profil. Trykk så på **Create.**



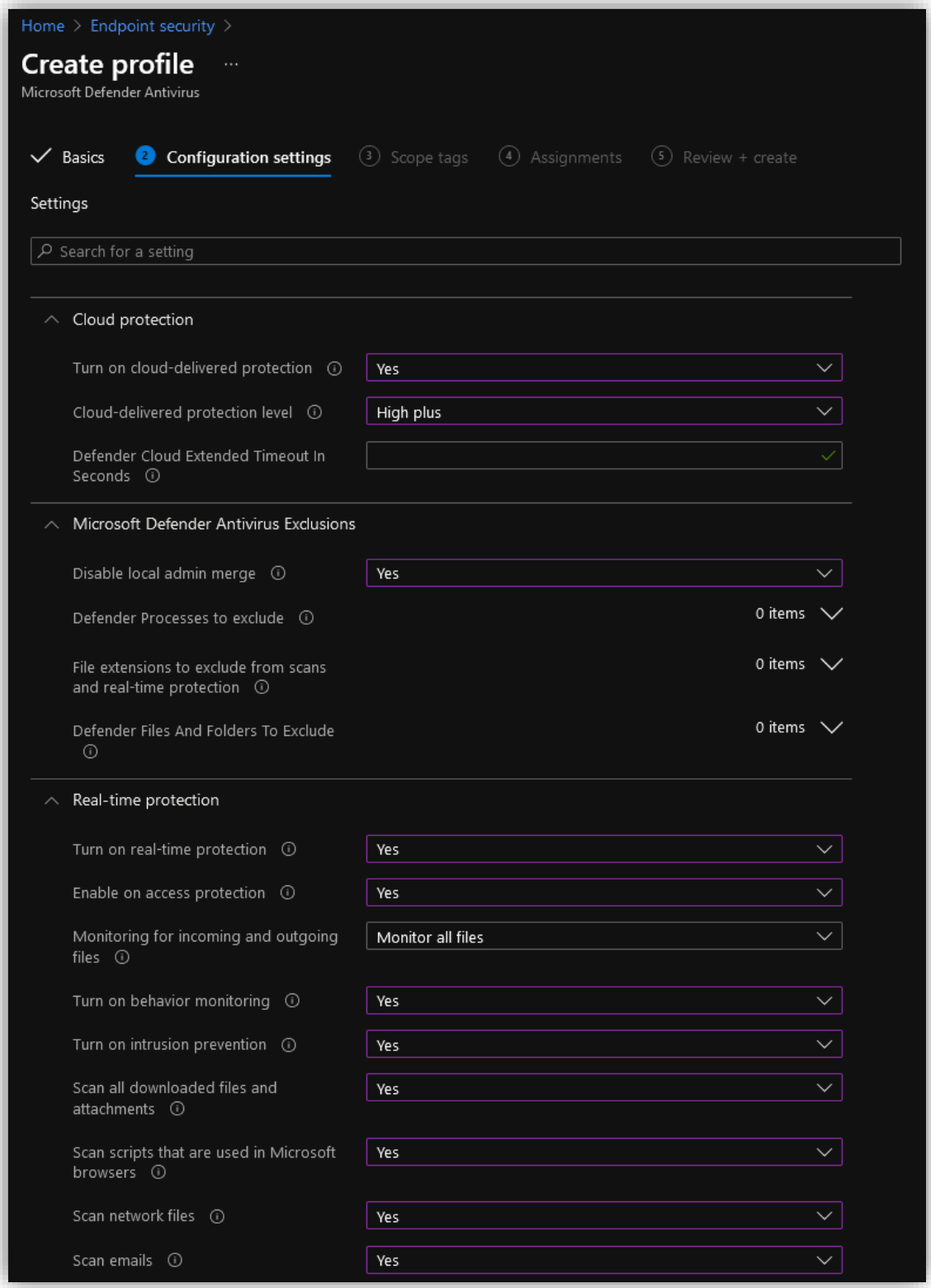
Gi et passende navn til policyen.

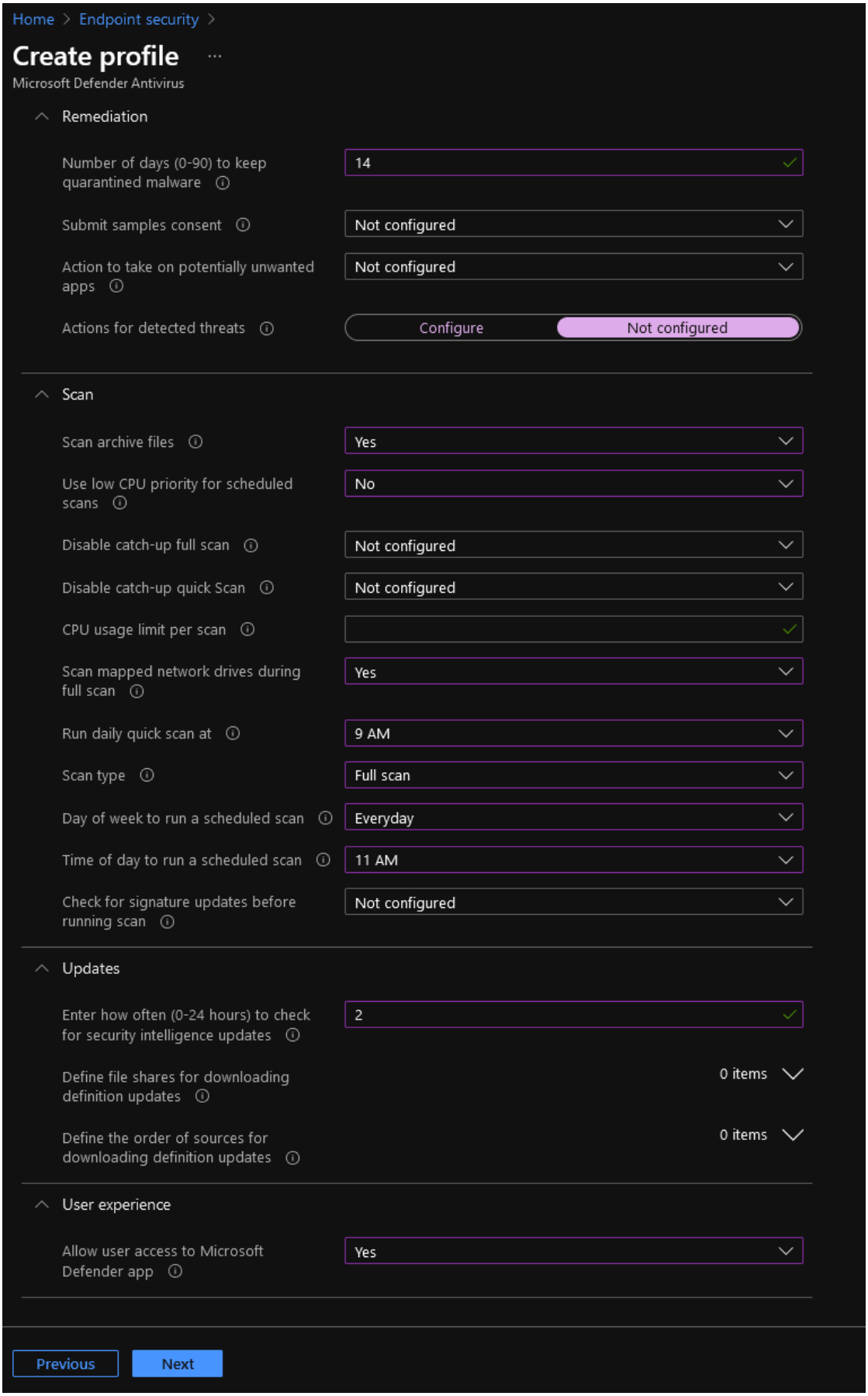


Under **Configuration settings,** skru på "alt". Dette er for å sørge for et så sikkert system som mulig på alle enhetene.

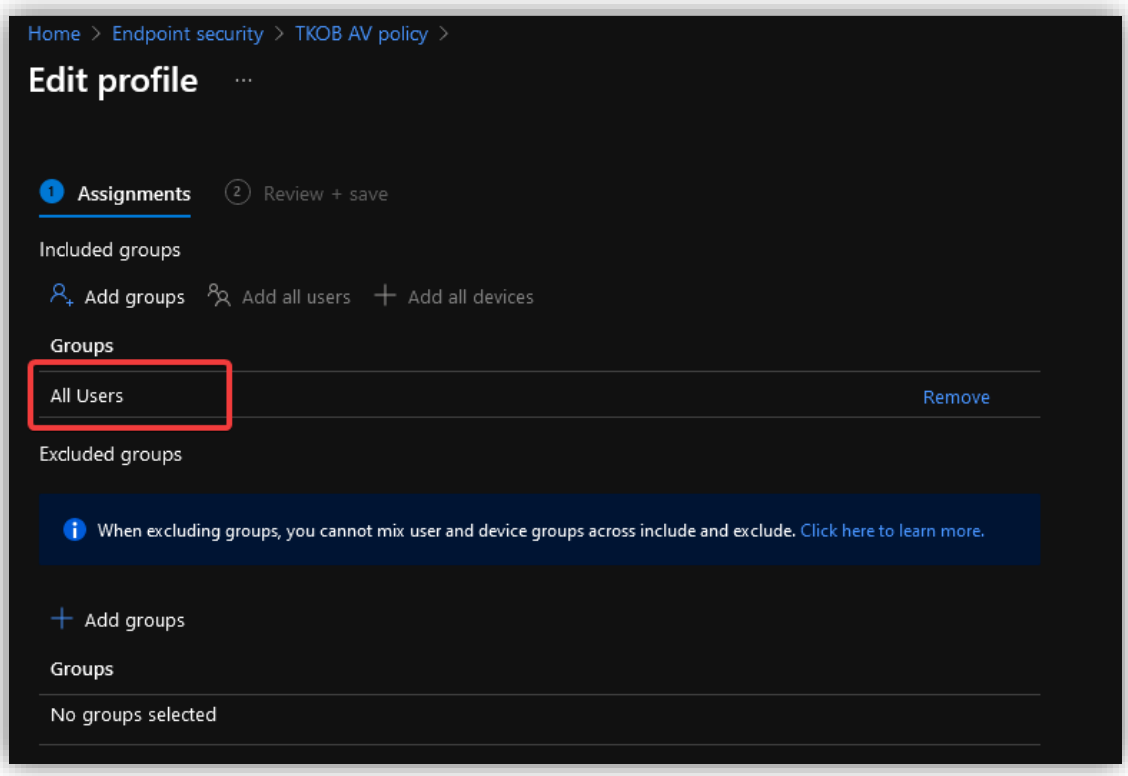
Verdt å merke seg:

- **Cloud delivered protection level** settes ikke til **Zero tolerance** ettersom dette kan føre til en dårlig brukeropplevelse. Dette kan gjøre at det blir vanskelig å ta i bruk programmer uten at de blir skrudd av pga. en mindre risiko.
- Skadevare i karantene blir fjernet etter 14 dager, dette kan justeres etter ønske. Dersom en ikke setter en verdi, vil ikke skadevaren bli fjernet.
- Det blir kjørt en **quick scan** hver morgen og en **full scan** rundt lunsjtider hver dag.
- Brukeren får tilgang til å se innstillingene i Windows Defender.


Home > Endpoint security >
Create profile
Microsoft Defender Antivirus
Basics
2 Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Settings
Search for a setting
Cloud protection
Turn on cloud-delivered protection
Yes
Cloud-delivered protection level
High plus
Defender Cloud Extended Timeout In Seconds
Microsoft Defender Antivirus Exclusions
Disable local admin merge
Yes
Defender Processes to exclude
0 items
File extensions to exclude from scans and real-time protection
0 items
Defender Files And Folders To Exclude
0 items
Real-time protection
Turn on real-time protection
Yes
Enable on access protection
Yes
Monitoring for incoming and outgoing files
Monitor all files
Turn on behavior monitoring
Yes
Turn on intrusion prevention
Yes
Scan all downloaded files and attachments
Yes
Scan scripts that are used in Microsoft browsers
Yes
Scan network files
Yes
Scan emails
Yes


Home > Endpoint security >
Create profile
Microsoft Defender Antivirus
Remediation
Number of days (0-90) to keep quarantined malware
14
Submit samples consent
Not configured
Action to take on potentially unwanted apps
Not configured
Actions for detected threats
Configure
Not configured
Scan
Scan archive files
Yes
Use low CPU priority for scheduled scans
No
Disable catch-up full scan
Not configured
Disable catch-up quick Scan
Not configured
CPU usage limit per scan
Scan mapped network drives during full scan
Yes
Run daily quick scan at
9 AM
Scan type
Full scan
Day of week to run a scheduled scan
Everyday
Time of day to run a scheduled scan
11 AM
Check for signature updates before running scan
Not configured
Updates
Enter how often (0-24 hours) to check for security intelligence updates
2
Define file shares for downloading definition updates
0 items
Define the order of sources for downloading definition updates
0 items
User experience
Allow user access to Microsoft Defender app
Yes
Previous
Next

Legg til **All users** slik at alle brukere blir tildelt denne policyen.

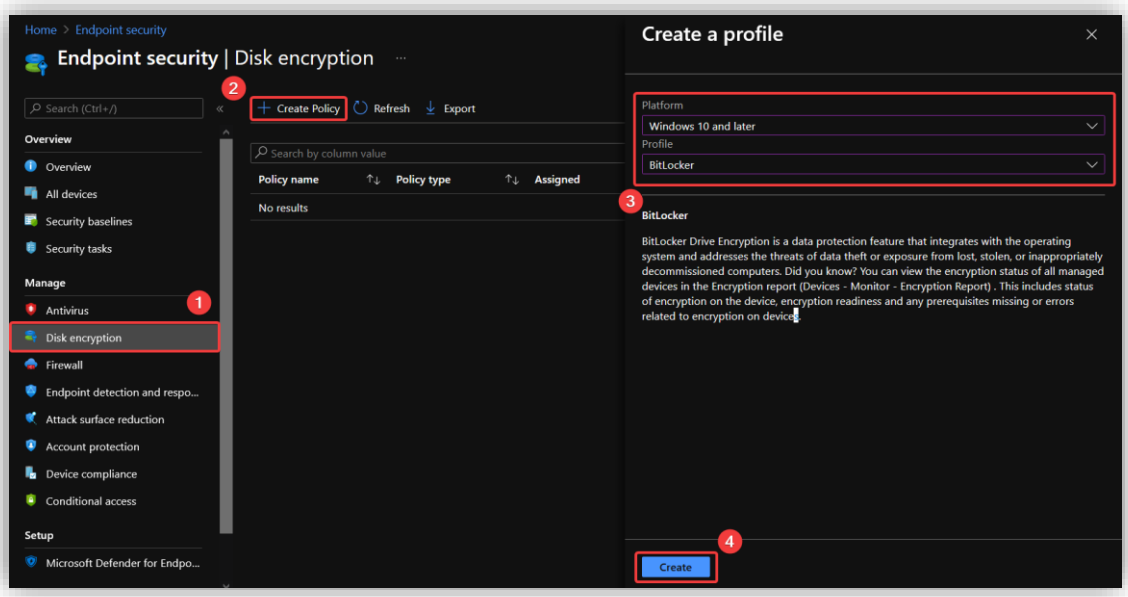


Fullfør ved å gå til **Review + create** og trykk **Create.**

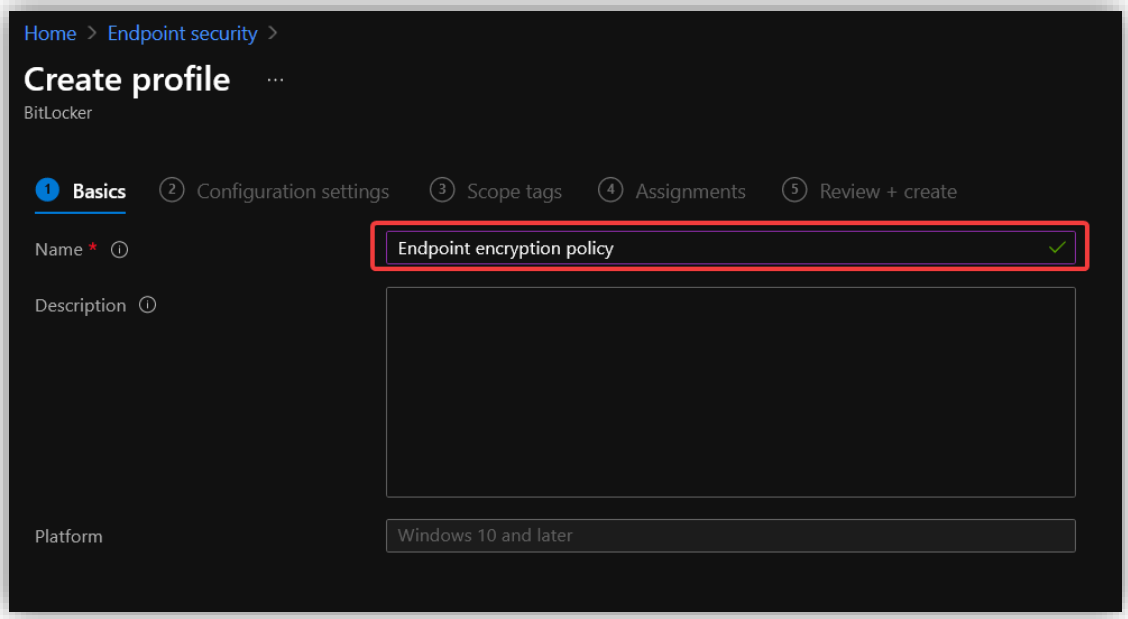
3.9.4.5 Lag en krypterings policy

For at enhetene skal være compliant må de være krypterte, ettersom dette ble satt som et krav i compliant policy. Ved å automatisere denne operasjonen med Endpoint Security, slipper hver enkelt bruker å kryptere enheten selv. Dette gjøres ved å lage en *disk encryption policy.*

I **Microsoft Endpoint Manager admin center**[24], gå til **Endpoint security > Disk encryption** og trykk på **Create Policy.** I Vinduet på høyre side, velg **Windows 10 and later** som plattform og **BitLocker** som profil.



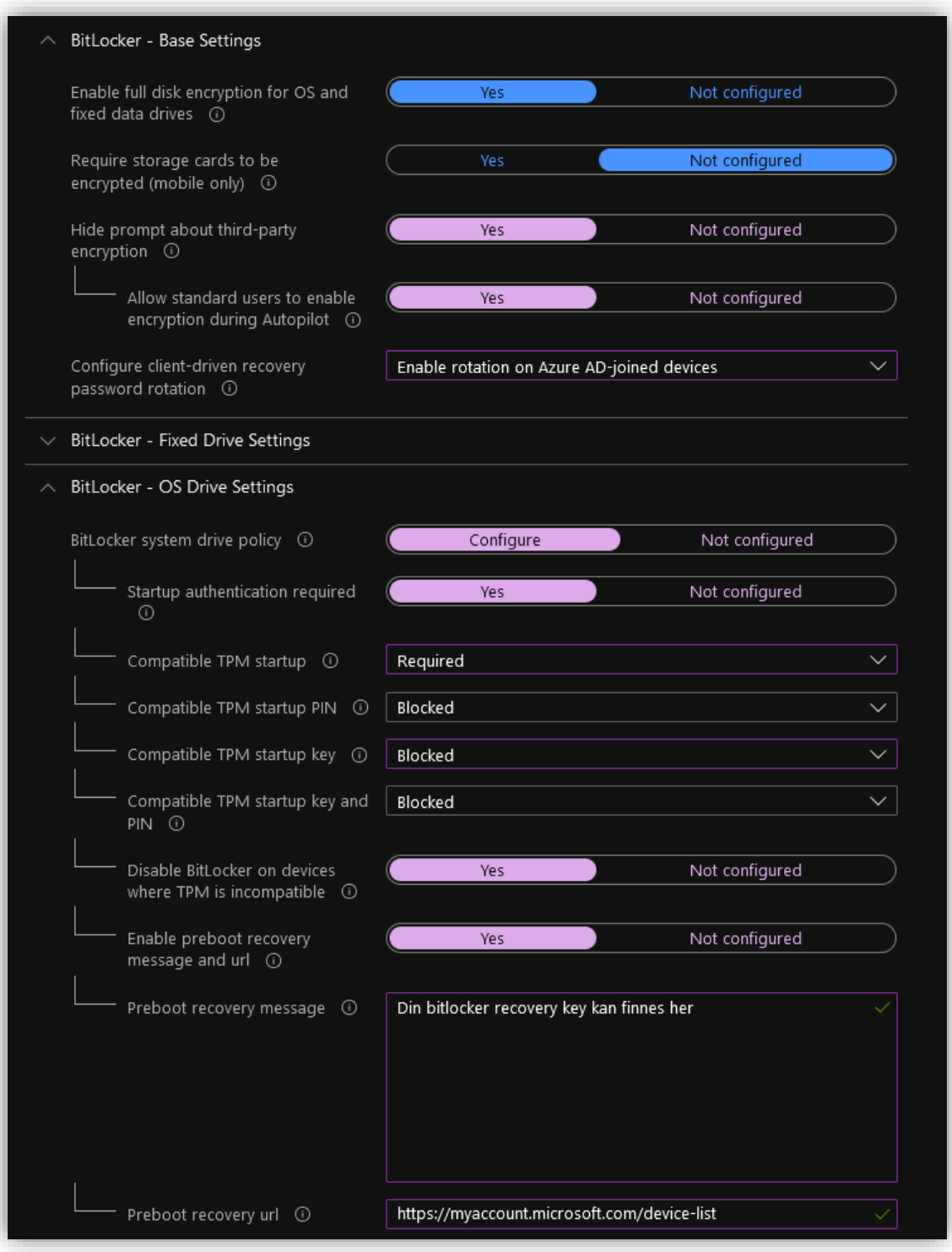
I **Basics**-tabben, gi policyen et passende navn.

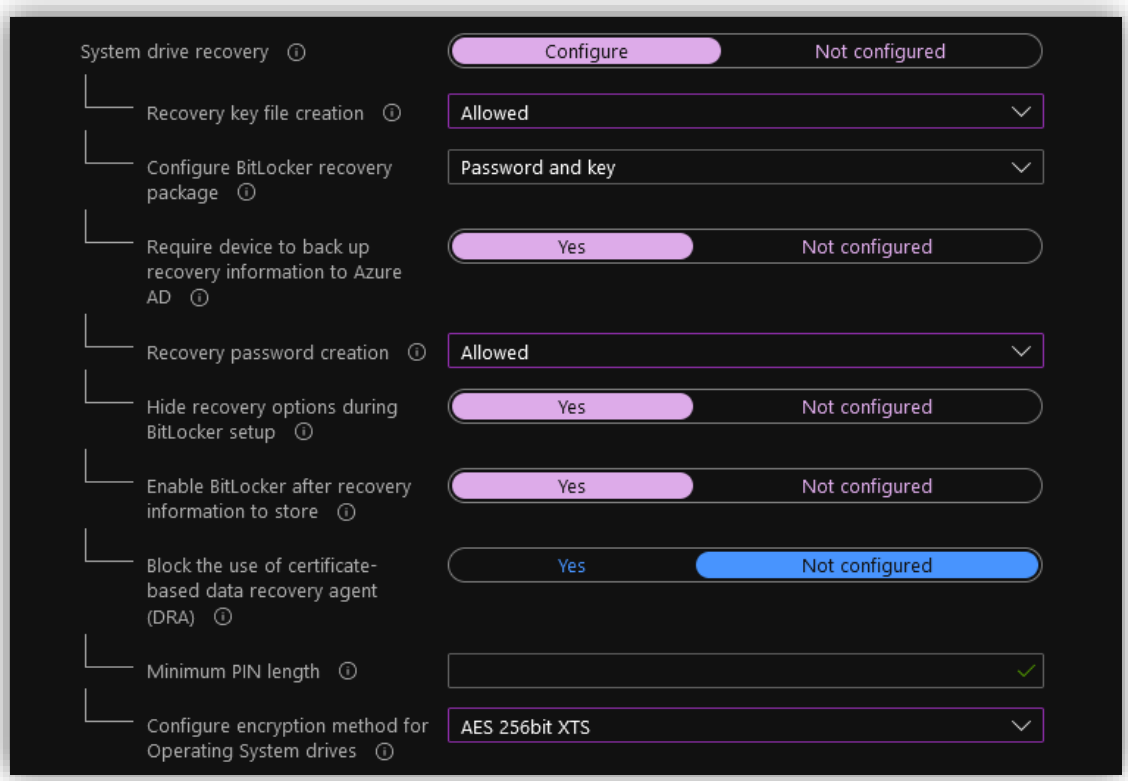


[24] https://endpoint.microsoft.com/#home

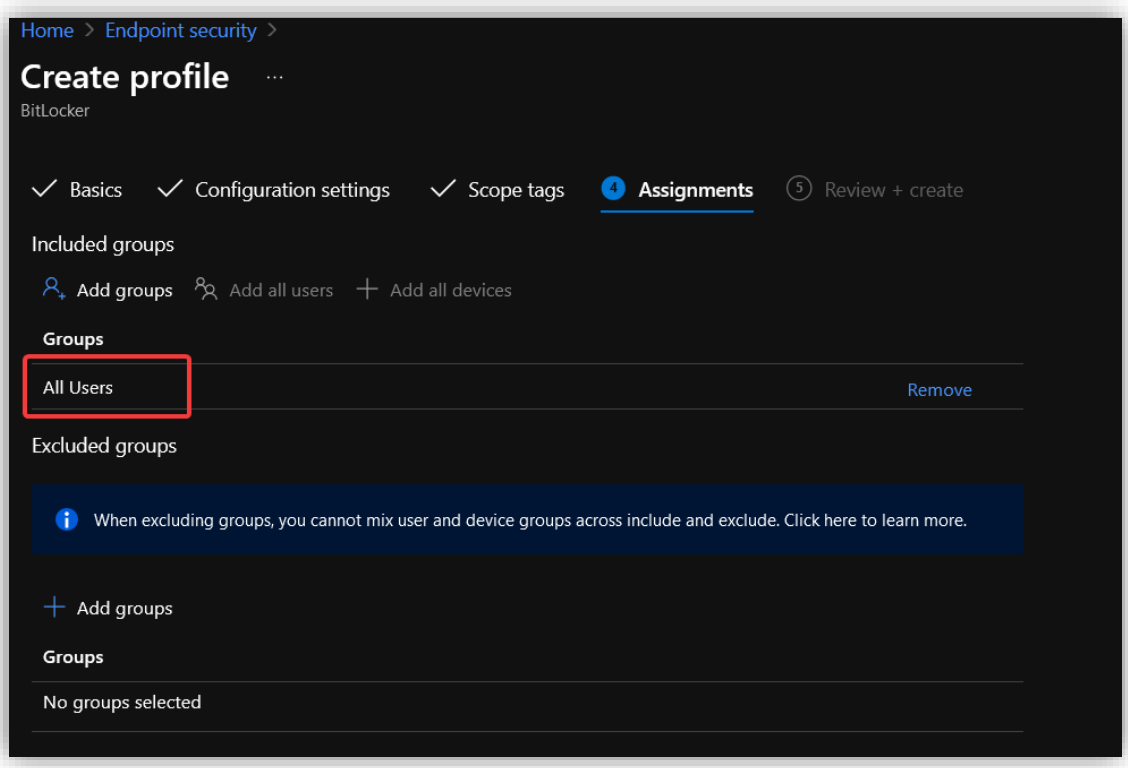
I **Configuration settings**-tabben, åpne **BitLocker – Base Settings** og sett **Enable full disk encryption** til **Yes.** Dette gjør at enhetene som tar i bruk denne policyen blir kryptert.

Konfigurer enheten slik som vist på bildene under. Kort sagt gjør dette at enheter blir kryptert stille – brukeren får ikke opp noen varsel eller prompt. For å gjøre brukeropplevelsen så god som mulig, velg at det ikke skal brukes noe PIN eller nøkkel. Dersom brukeren trenger gjenopprettingsnøkkel, blir brukeren vist til nettsiden hvor en kan finne denne.




System drive recovery
Configure
Not configured
Recovery key file creation
Allowed
Configure BitLocker recovery package
Password and key
Require device to back up recovery information to Azure AD
Yes
Not configured
Recovery password creation
Allowed
Hide recovery options during BitLocker setup
Yes
Not configured
Enable BitLocker after recovery information to store
Yes
Not configured
Block the use of certificate-based data recovery agent (DRA)
Yes
Not configured
Minimum PIN length
Configure encryption method for Operating System drives
AES 256bit XTS

I **Assignments**-tabben, legg til gruppen **All Users** inn under **Included groups.**

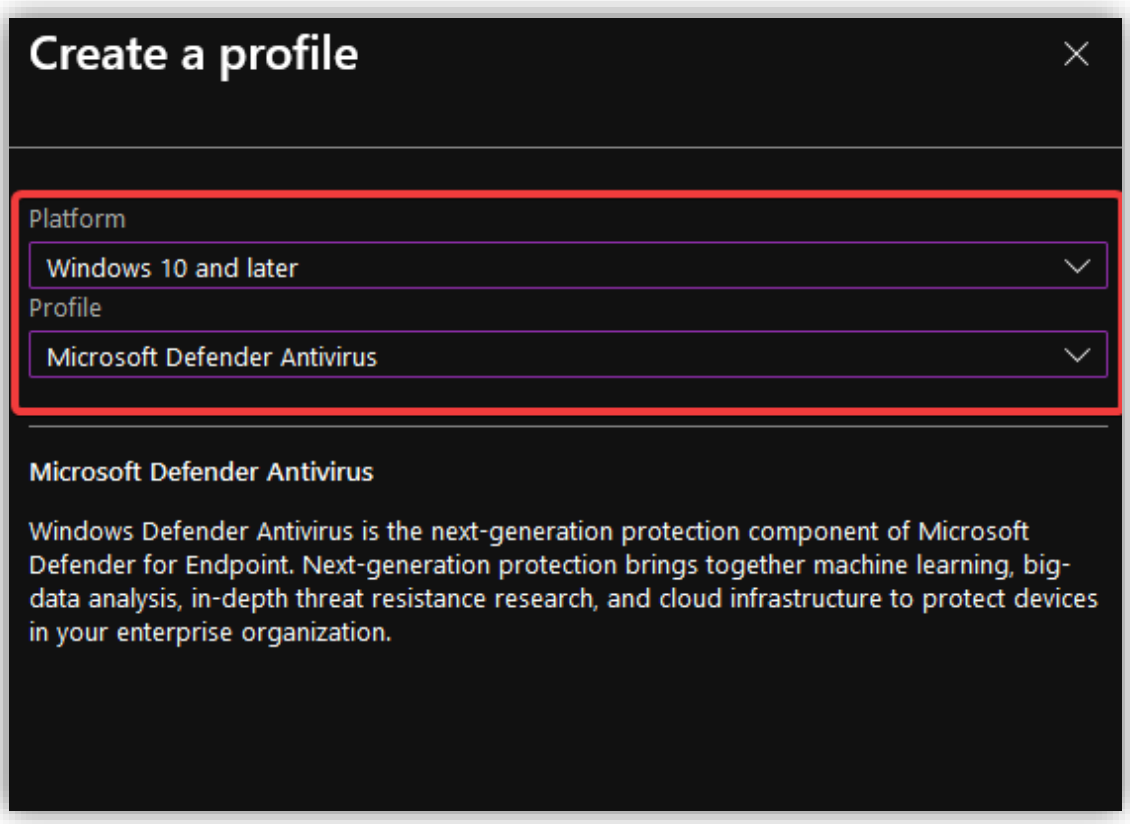


Fullfør ved å gå til **Review + create** og trykk på **Create.**

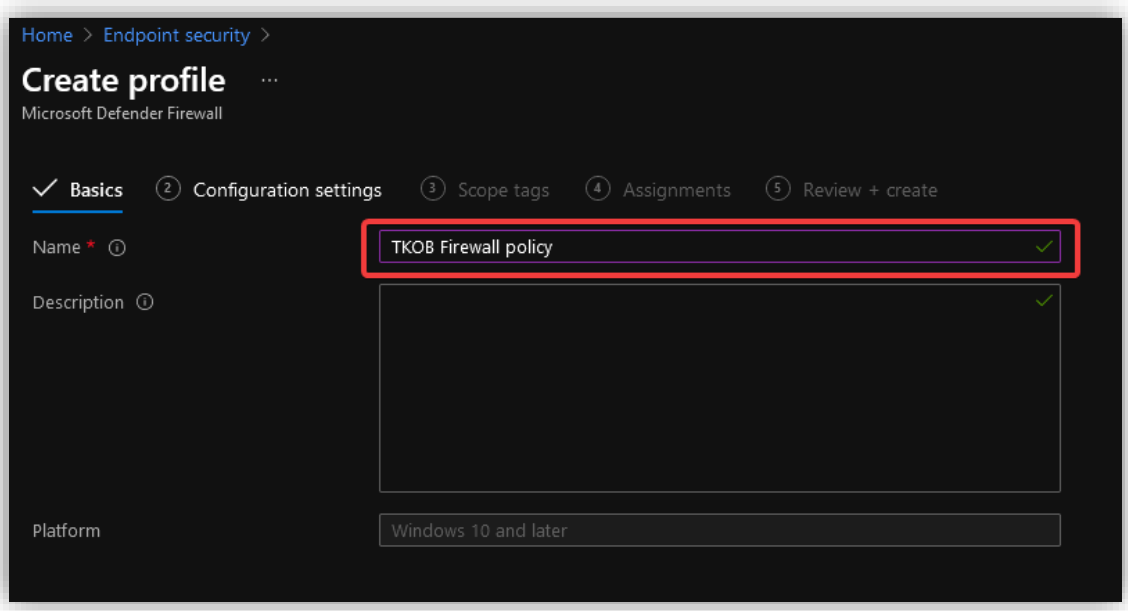
3.9.4.6 Lag brannmur policy

For å sikre at alle enheter bruker en brannmur lager man en policy for dette. Brannmuren hjelper med å sikre at porter som ikke bør være åpne er lukket og fungerer som enda et lag med sikkerhet på enhetene.

Under **Endpoint Security > Antivirus**, trykk på **Create policy.** Velg **Windows 10 and later** som plattform og **Microsoft Defender Antivirus** som profil. Trykk så på **Create.**

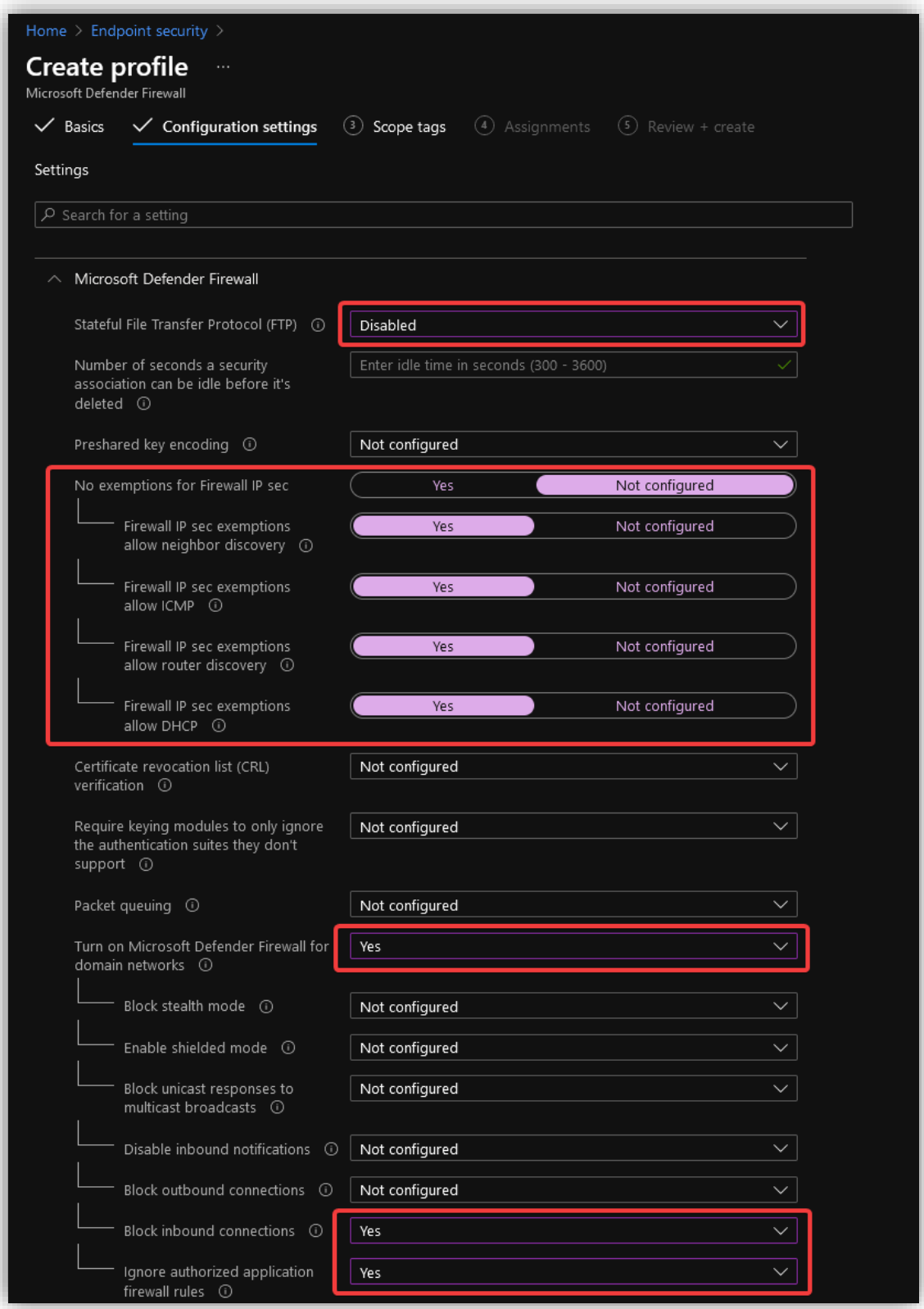


Gi policyen et passende navn.

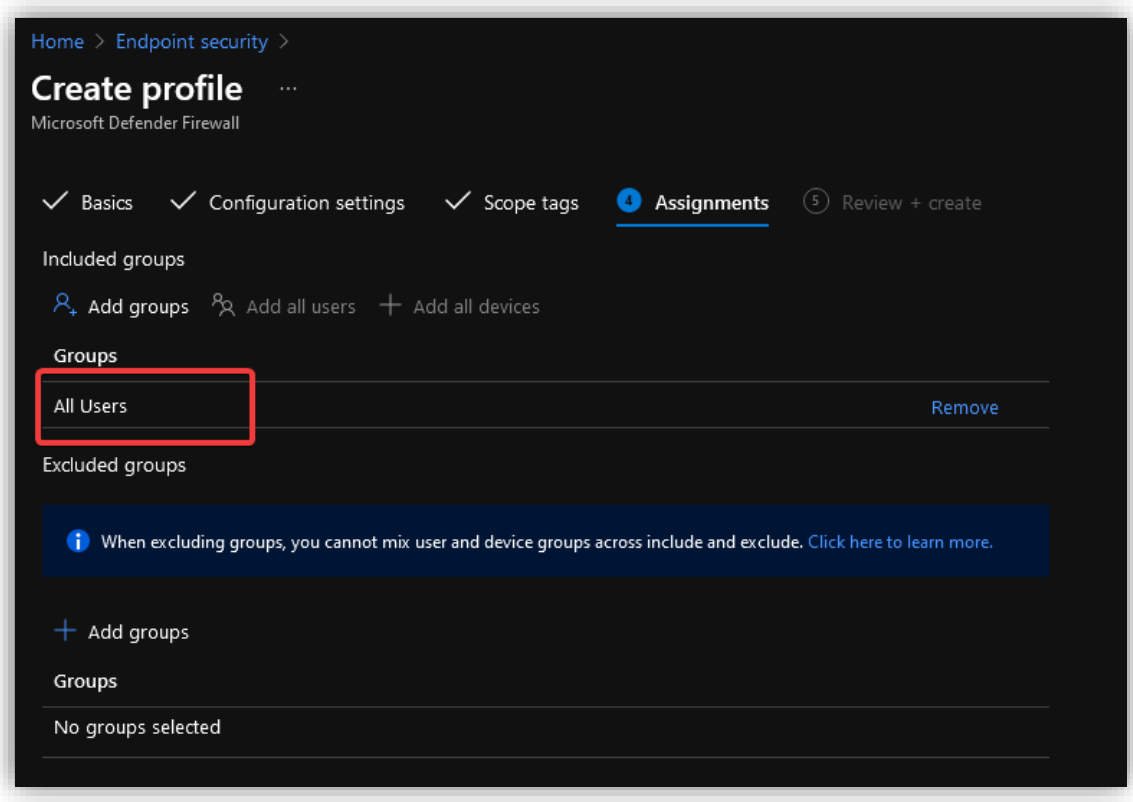


Under **Configuration settings** gjør følgende konfigurasjoner:

- Skru av FTP ettersom dette er en lite sikker protokoll.
- De *neighbor discovery, ICMP, router discovery* og *dhcp* settes til **Yes** for at enhetene skal fungerer riktig.
- For domene-, private- og offentlige nettverk sett de samme reglene:
    - Skru på brannmuren
    - Blokker inngående trafikk – det er kun trafikken som sluttbruker initierer som bør komme igjennom
    - Blokker autoriserte applikasjoners brannmur regler – ikke la applikasjoner kunne endre reglene og kjøre programmer utenfor en selv.


Home > Endpoint security >
Create profile
Microsoft Defender Firewall
Basics
Configuration settings
3 Scope tags
4 Assignments
5 Review + create
Settings
Search for a setting
Microsoft Defender Firewall
Stateful File Transfer Protocol (FTP)
Disabled
Number of seconds a security association can be idle before it's deleted
Enter idle time in seconds (300 - 3600)
Preshared key encoding
Not configured
No exemptions for Firewall IP sec
Yes
Not configured
Firewall IP sec exemptions allow neighbor discovery
Yes
Not configured
Firewall IP sec exemptions allow ICMP
Yes
Not configured
Firewall IP sec exemptions allow router discovery
Yes
Not configured
Firewall IP sec exemptions allow DHCP
Yes
Not configured
Certificate revocation list (CRL) verification
Not configured
Require keying modules to only ignore the authentication suites they don't support
Not configured
Packet queuing
Not configured
Turn on Microsoft Defender Firewall for domain networks
Yes
Block stealth mode
Not configured
Enable shielded mode
Not configured
Block unicast responses to multicast broadcasts
Not configured
Disable inbound notifications
Not configured
Block outbound connections
Not configured
Block inbound connections
Yes
Ignore authorized application firewall rules
Yes

Legg til **All Users**.



Fullfør ved å gå til **Review + create** og trykk på **Create.**

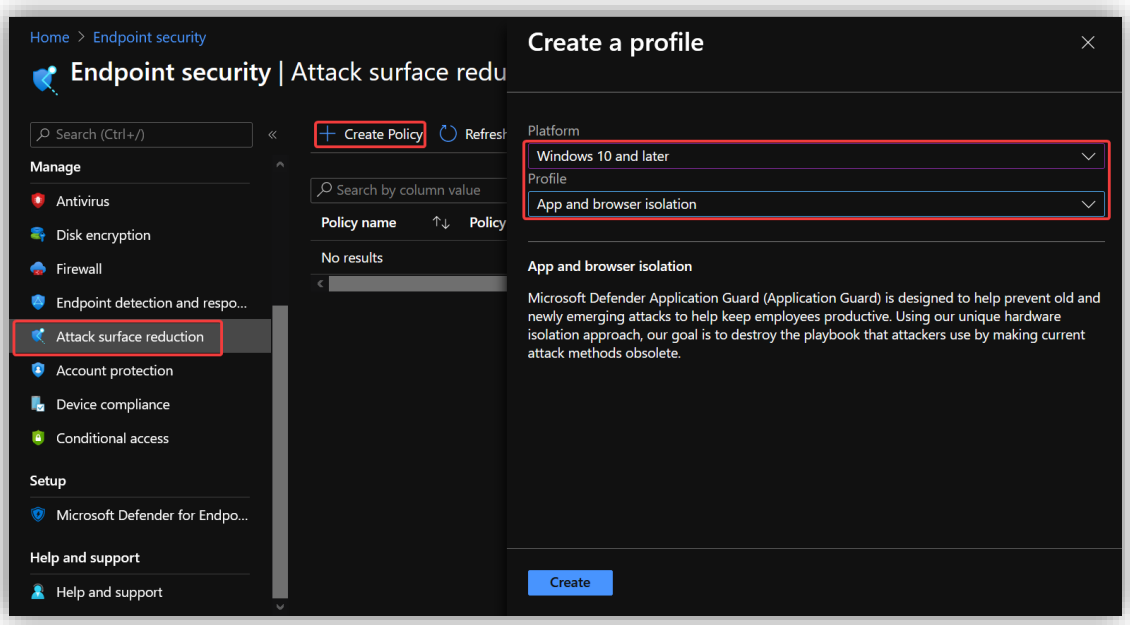
3.9.4.7 Attack surface reduction

Attack Surface Reduction inneholder en rekke innstillinger beregnet på å fjerne angrepsvektorer inn i systemet. De fleste av disse innstillingene er noe man bare skrur på uten noen ytterligere konfigurasjoner.

3.9.4.7.1 App and browser isolation

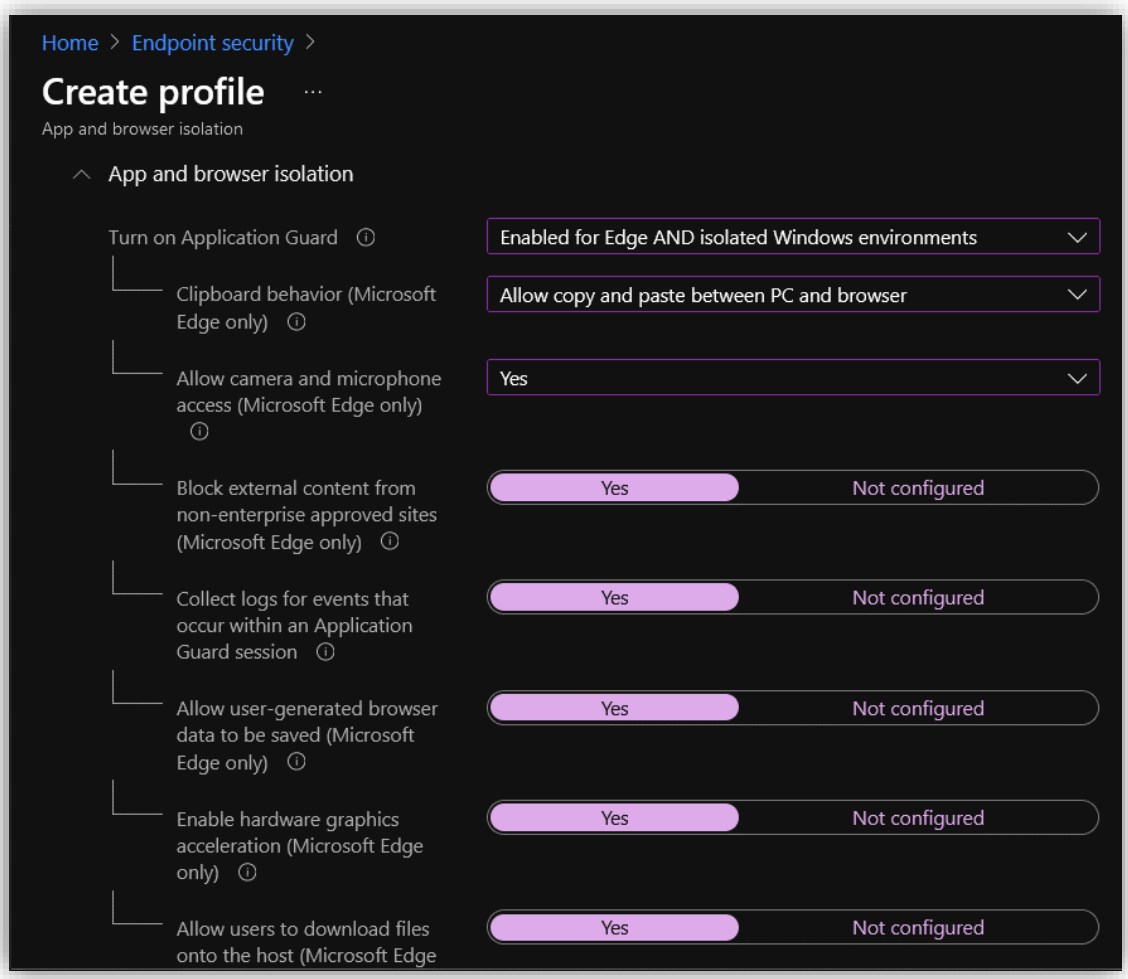
App and browser isolation bruker **Application Guard** for å åpne usikre nettsider i en virtuell maskin. Den kan også åpne dokumenter som maskinen ikke stoler på. Om nettsiden eller filen som åpnes oppfører seg merkelig eller det blir oppdaget skadevare, vil det ikke nå maskinen til brukeren.

Trykk **Create Policy,** velg **Windows 10** og **App and browser isolation.**

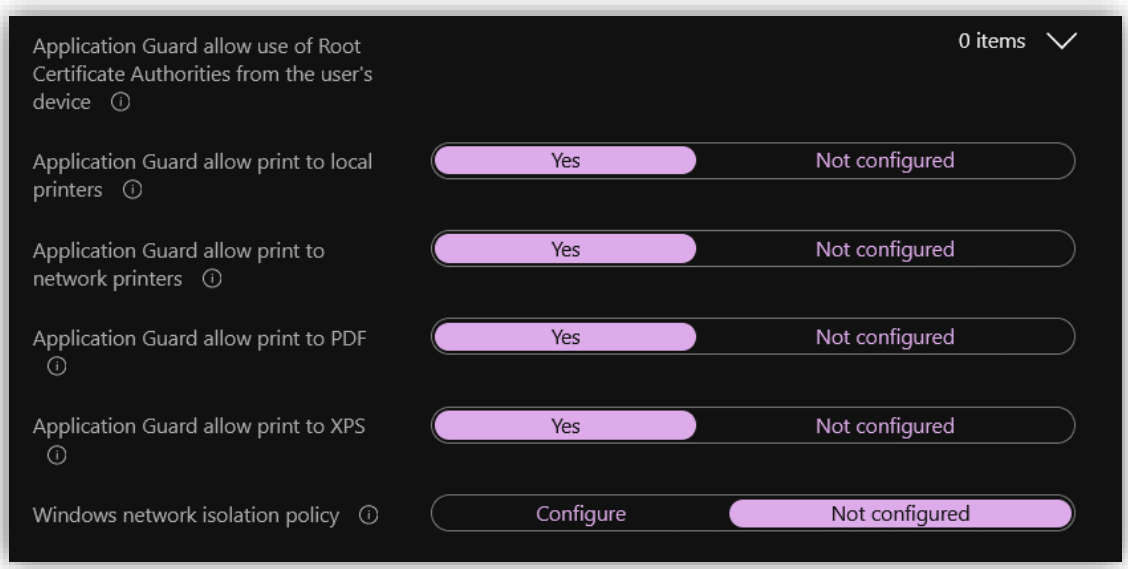


2 Dette steget er likt for alle policyer og vises bare en gang.

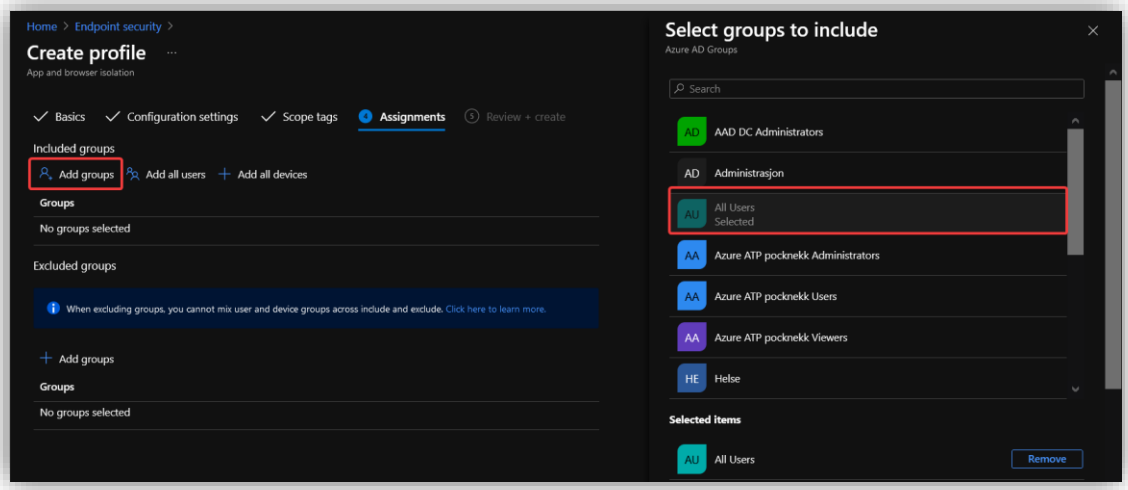
Skru på alt under **App and browser isolation**. Det første punktet skrur på **Application Guard,** resten passer på at brukeropplevelsen ikke blir dårligere av alle begrensningene. Man skal fortsatt kunne skrive ut dokumenter eller kopiere tekst ut fra det sikre miljøet.



Som i punktet over, skru på alt. Det eneste som ikke skal være på er **Windows network isolation policy.**



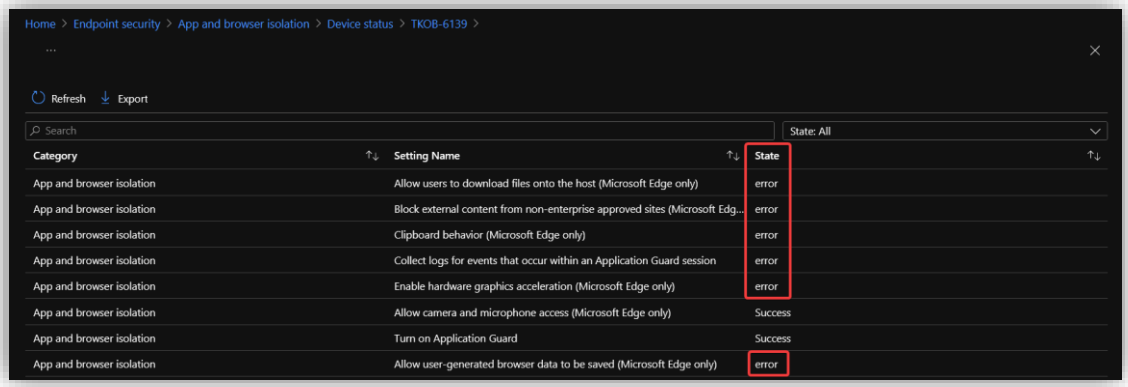
Velg **Add group** og deretter **All Users**.



Dette steget er likt for alle policyer og vises bare en gang.

Trykk deretter **Create Policy**.

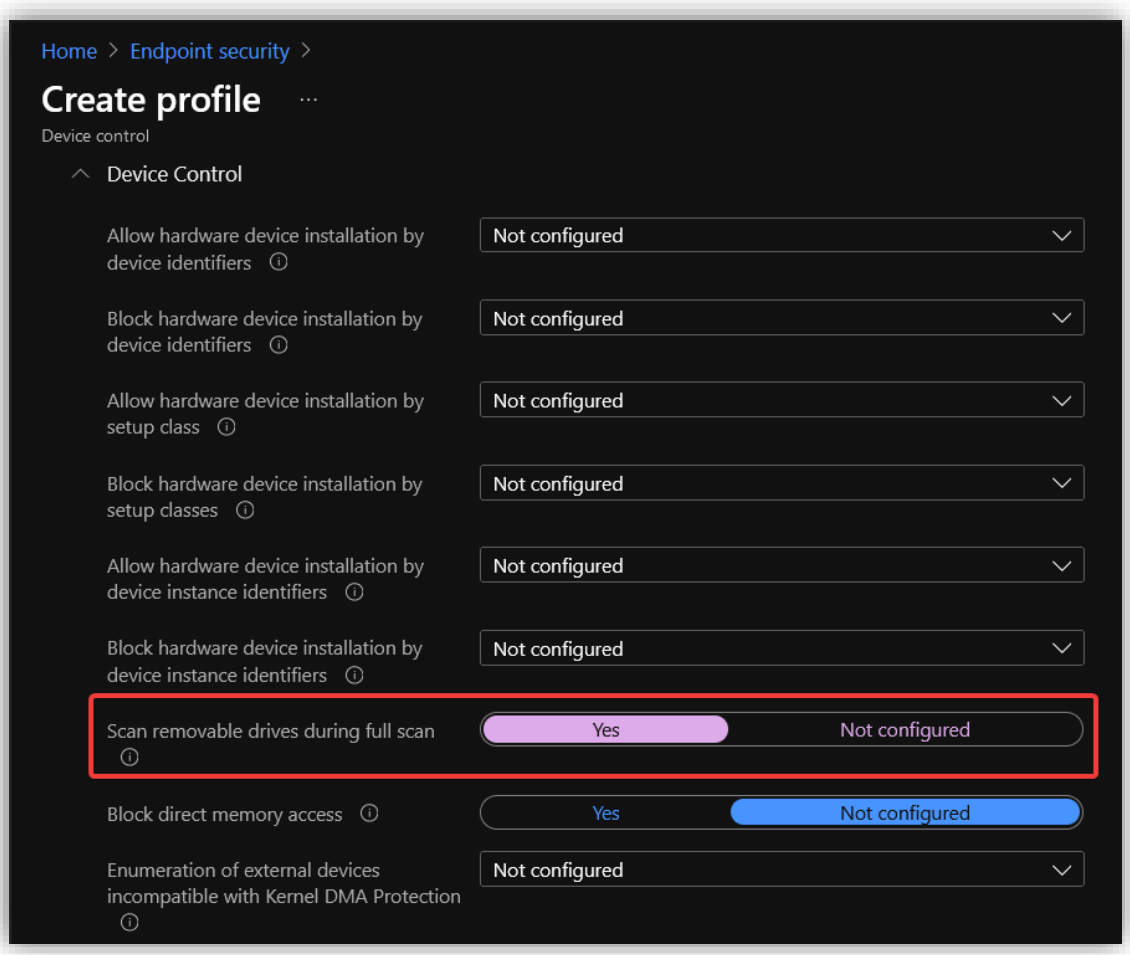
En kjent feil med denne policyen er at det står error på de fleste av reglene etter utrulling. Dette kan ses bort ifra da det er en feil i måten klienten rapporterer tilbake til MDM.



3.9.4.7.2 Device Control

Lag en ny policy og velg **Device Control**.

La alt stå som standard, men velg **Scan removable drives during full scan.**



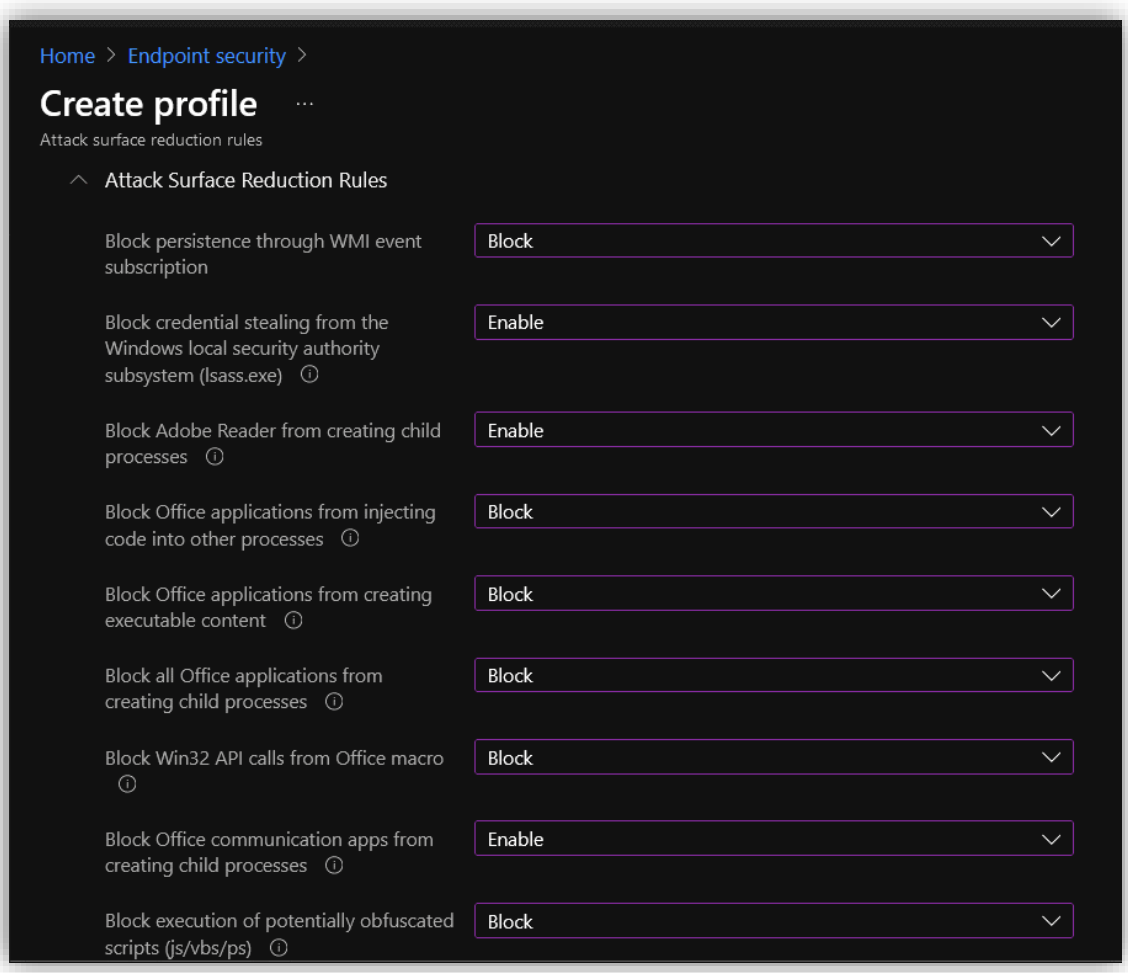
Gå deretter gjennom resten av stegene og klikk **Create policy**.

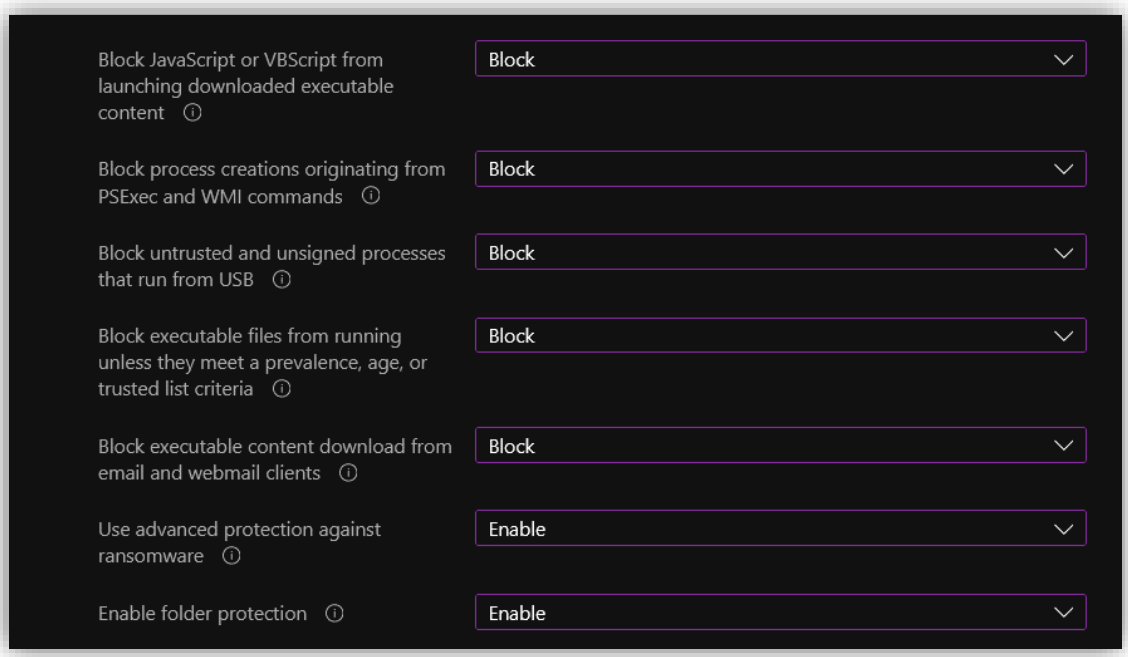
3.9.4.7.3 Attack Surface Reduction Rules

Denne policyen sikter seg inn på å redusere antall angrepsvektorer som skadevare kan benytter seg av i et angrep. Alle alternativene i denne policyen skal skrus på og hvert alternativ tar seg av en spesifikk angrepsvektor.

Lag en ny policy som i stegene over, velg **Attack surface reduction rules** fra menyen.

Under **Attack Sruface Reduction Rules** skal alt enten stå som **Block** eller **Enable.** Hva de forskjellige alternativene gjør er beskrevet under.





- **Block persistence through WMI event subscription**
  Windows Management Instrumentiation (WMI) er et styringsverktøy for Windows. Ondsinnede aktører kan bruke dette verktøyet til å gjemme skadevare. Denne regelen hindrer dette.
- **Block credential stealing from the Windows local security authority subsystem (lsass.exe)**
  Lsass.exe er prosessen som autentiserer brukere som forsøker å logge inn på Windows. Lsass er en vanlig vektor for å stjele brukernavn og passord som igjen brukes til å eskalere tilgangene til aktøren. Denne regelen låser ned prosessen slik at det blir vanskeligere å skaffe seg uautorisert tilgang til informasjonen.
- **Block Adobe Reader from creating child processes**
  Gjennom spesiallagde filer kan ondsinnede aktører gjennom Reader kjøre skadevare utenfor Reader miljøet. Denne regelen stopper Reader fra å lage underprosesser slik at skadevaren ikke kan kjøre.
- **Block Office applications from injecting code into other processes**
  Spesiallagde Office filer kan dytte ondsinnet kode inn i andre prosesser som kjører på systemet. Det finnes ingen formål for dette i legitim virksomhet, derfor har det liten innvirkning å blokkere dette. Dette gjelder også for de tre andre vektorene knyttet til Office.
- **Block Office applications from creating executable content**
  Denne regelen stopper Office om den prøver å skrive ondsinnet kode til disk via virus. Dette stopper ondsinnet kode fra å gjemme seg på systemet.
- **Block all Office applications from creating child processes**
  Stopper Office VBA makroer fra å kunne lage underprosesser. Dette er en vanlig angrepsvektor mot office, og bruker underprosessene til å laste ned hoved viruset.
- **Block Win32 API calls from Office macro**
  VBA skript i Office kan kalle Win32 api for å kjøre shell kode, dermed kan en ondsinnet aktør få tilgang til maskinen uten å lagre noe på disken. Denne funksjonaliteten er ikke mye brukt, derfor blokkeres den.
- **Block Office communication apps from creating child processes**

Denne regelen stopper Outlook fra å lage underprosesser slik at ondsinnede aktører ikke kan misbruke svakheter i programvaren via e-poster med vedlegg.

- **Block execution of potentially obfuscated scripts (js/vbs/ps)**
  Obfuscated kode brukes for å gjøre kode vanskeligere å lese, dette for å beskytte åndsverk, men også for å gjemme ondsinnet kode. Denne regelen ser gjennom slik kode og stopper den om den virker ondsinnet.
- **Block JavaScript or VBScript from launching downloaded executable content**
  Stopper skripts fra å laste ned kjørbar kode fra nettet. Dette er en vanlig måte å få lastet ned en ondsinnet nyttelast på maskiner.
- **Block process creations originating from PSExec and WMI commands**
  PSExec og WMI brukes ofte for å fjernstyre maskiner. Denne regelen lar ikke disse programmene lage nye prosesser på fjernstyrte maskiner, dermed blir det vanskeligere for ondsinnede aktører med stjålne passord å infisere andre maskiner i nettet.
- **Block untrusted and unsigned processes that run from USB**
  Denne regelen stopper en ondsinnet aktør fra å sette en USB-minnepinne i en maskin å kjøre virus derfra. Kun godkjent programvare kan kjøre fra minnepinner.
- **Block executable files from running unless they meet a prevalence, age, or trusted list criteria**
  Stopper kjørbare filer (.exe .dll .scr) fra å kjøre om de ikke møter krav til alder og utbredelse i systemet. Dermed kan man ikke kjøre slike filer om de er veldig nye eller ikke har blitt sett av systemet før. Filer kan legges inn i en liste over godkjent programvare.
- **Block executable content download from email and webmail clients**
  Blokkerer kjørbare filer fra å åpne fra e-poster gjennom Outlook og andre e-post klienter.
- **Use advanced protection against ransomware**
  Bruker forskjellige metoder for å finne ut om et program er et kryptovirus. Skytjenester hos Microsoft bruker innsamlet data fra hele verden og sammenligner filen mot dette. Om filsignaturen ser ut som et kryptovirus blir den blokkert, og resultatene brukt til fremtidige sjekker.
- **Enable folder protection**
  Stopper ukjente programmer fra å slette eller modifisere filer i beskyttede mapper.

3.9.5 Microsoft Defender for Office 365

Microsoft Defender for Office 365 beskytter organisasjonen mot skadelige trusler gjennom e-post, lenker og samarbeidsverktøy. Dette inkluderer:

- **Threat protection policies:** Definerer hvilke policyer som skal brukes for at din organisasjon skal ha et passende nivå av beskyttelse.
- **Reports:** Real-time rapporter som overvåker ytelsen til Defender for Office 365.
- **Threat investigation and response capabilities:** Verktøy som etterforsker, simulerer og motvirker trusler.
- **Automated investigation and response capabilities:** Spar tid ved å automatisere.

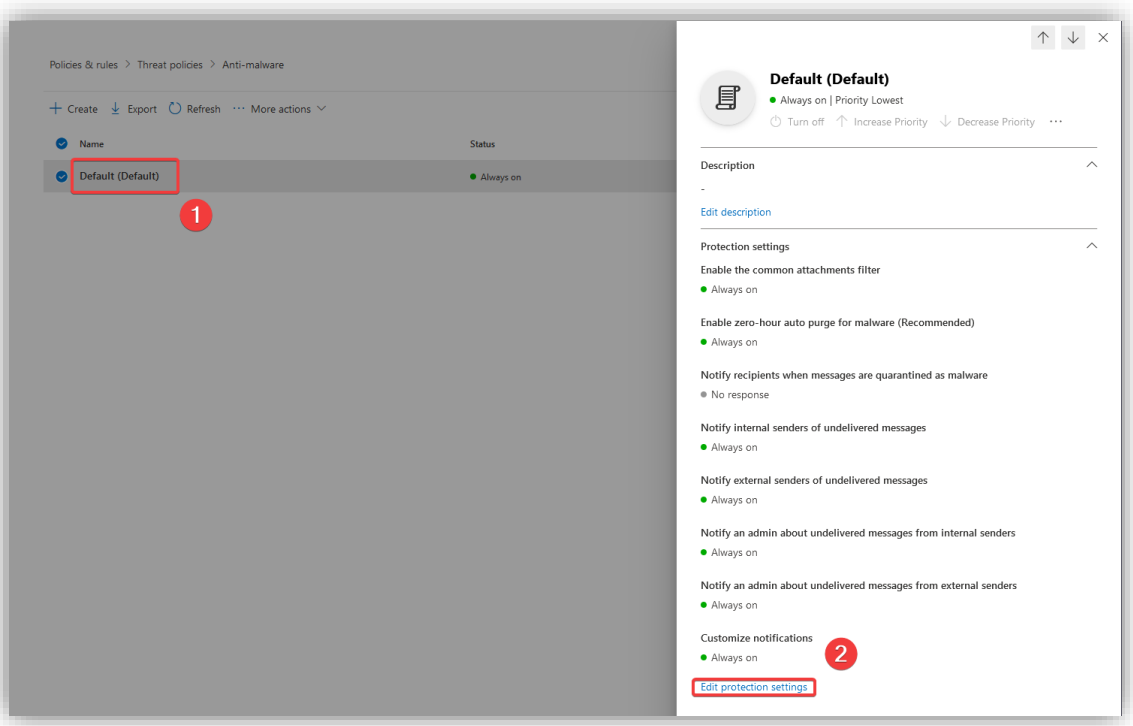
All konfigurering foregår i **Microsoft 365 Security**[25]-portalen.

3.9.5.1 Konfigurering av Anti-malware

Anti-malware brukes for å detektere farlig innhold i en e-post. Dette er med på å forhindre at virus havner på en enhet eller i systemet.

Under **Email & collabortaion**, gå til **Policies & rules > Threat policies > Anti-malware.** Her ligger det en **Default** fra før av, for et enkelt oppsett holder med å redigere denne.

Trykk på **Default** og velg **Edit protection settings.**



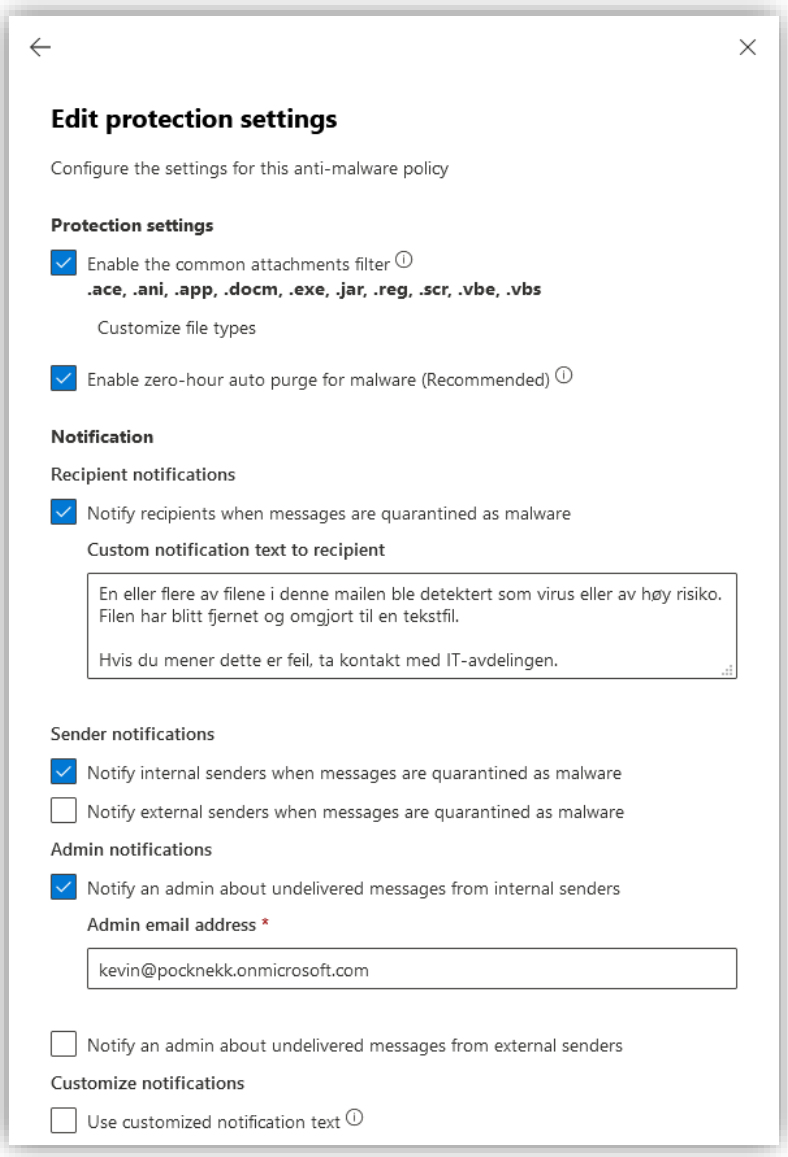
[25] https://security.microsoft.com/

Under **Protection settings:**

- Skru på **Enable the common attachments filter** for å automatisk identifisere de følgende filtypene som skadevare. Dette er kjørbare filtyper som kan inneholde virus og kan være lurt å ikke la sendes over e-post.
- Skru på **Enable zero-hour auto purge for malware** for at meldinger som allerede har kommet til Exchange e-postboksen kan bli satt i karantene dersom det er oppdaget at de inneholder skadevare.

Under **Notification:**

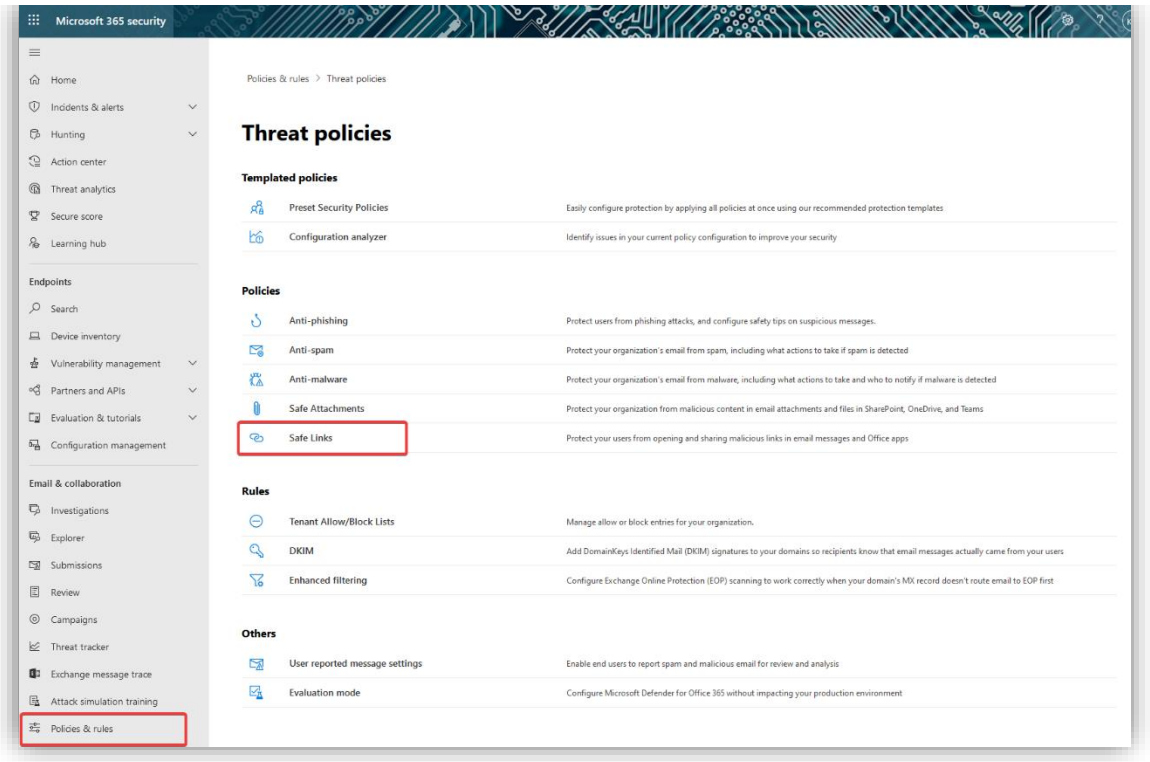
- Sett at mottakere skal få beskjed dersom en mottatt melding inneholdt skadevare.
- Sett at interne sendere skal få beskjed dersom meldingen inneholdt potensiell skadevare.
- Det kan være lurt å varsle en IT-ansvarlig dersom meldinger ikke kommer frem pga. Skadevare.
- Velg å ikke få varsle når eksterne e-post blir satt i karantene. Det kan bli veldig mye e-post å gå igjennom dersom eksterne e-post også skal varsles om.



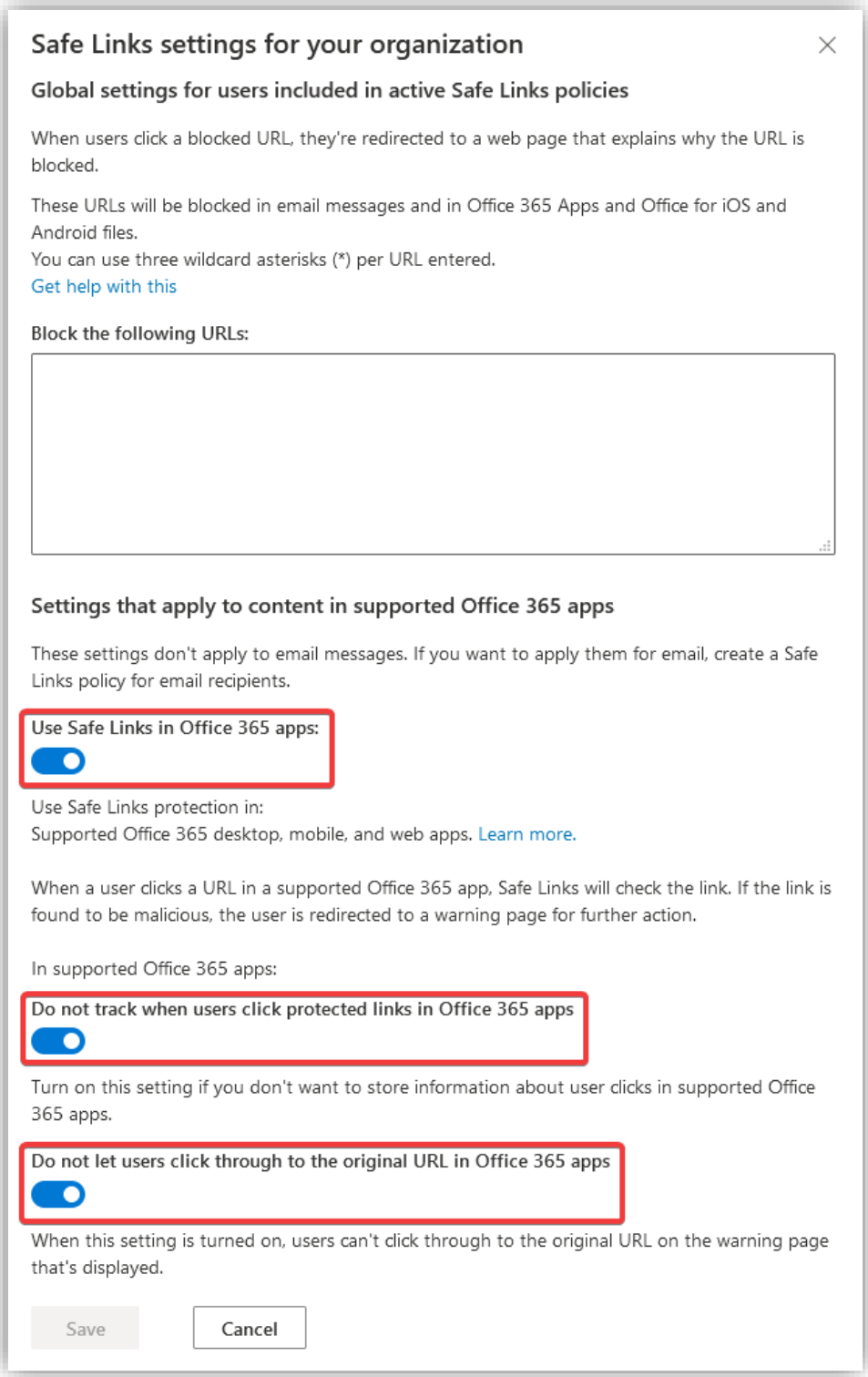
3.9.5.2 Konfigurering av Safe Links

Safe Links gjør at URL-lenker i e-post og dokumenter som kommer til organisasjonen kan bli gjenkjent som farlige lenker og kan forhindre brukerne i å trykke seg inn på disse.

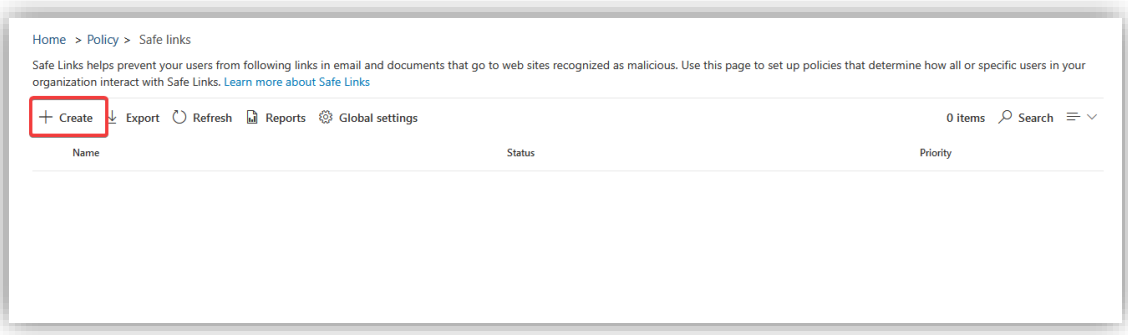
Gå til **Policies and rules > Safe Links.**



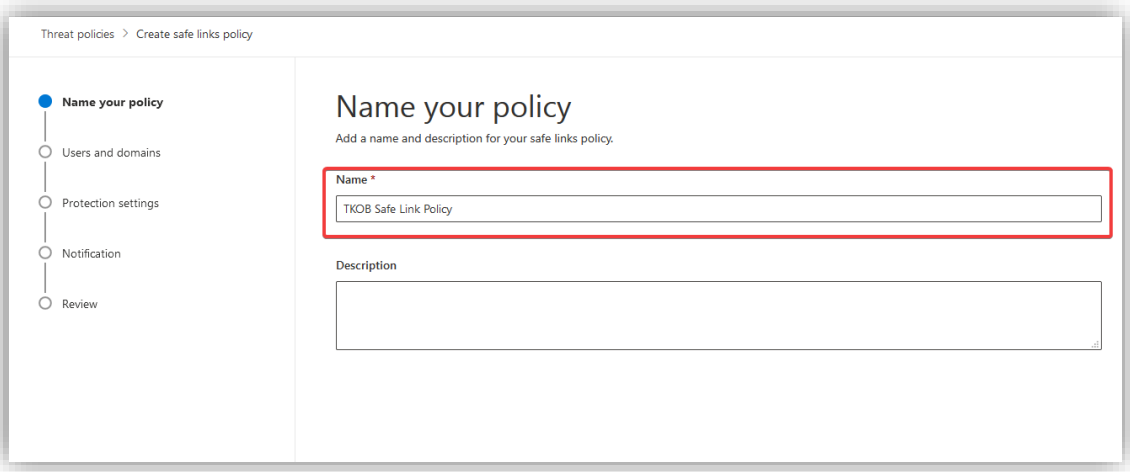
Sett først de globale innstillingene for **Safe Links** ved å trykke på **Global Settings**. Disse innstillingene gjelder for Office 365-applikasjoner, altså ikke for e-post. Skru på **Use Safe Links in Office 365 app**. Dersom en bruker trykker på en lenke som blir identifisert som farlig, vil brukeren isteden bli sendt til er advarselsside. Ved å huke av de to nederste valgene, vil ikke informasjon om hvor brukeren trykker bli lagret – verken når det er en beskyttet lenke eller den originale lenken.



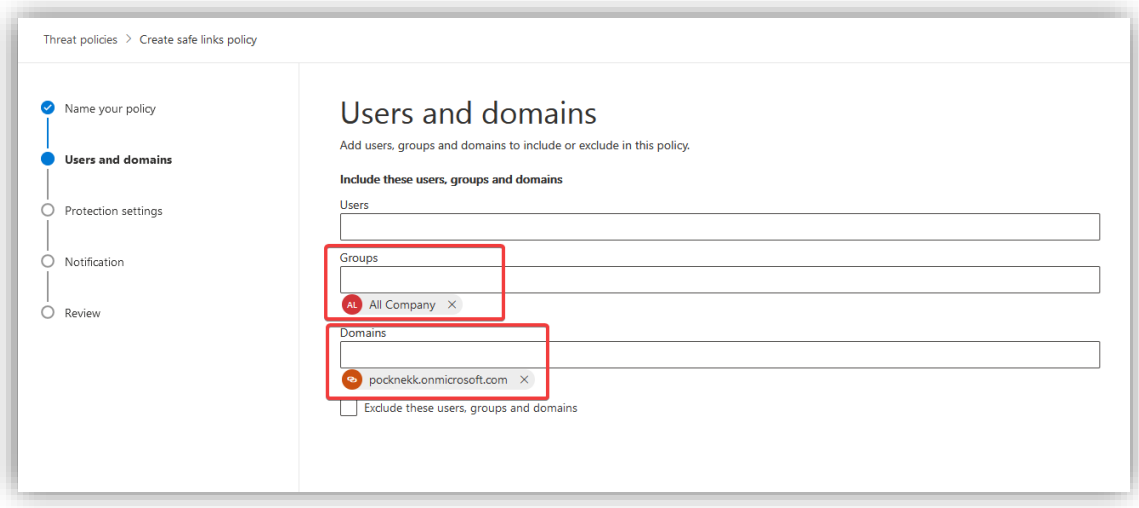
For at **Safe Links** skal fungere for e-post lager man **Safe Link policies**. Under **Policy > Safe links**, trykk på **Create**.



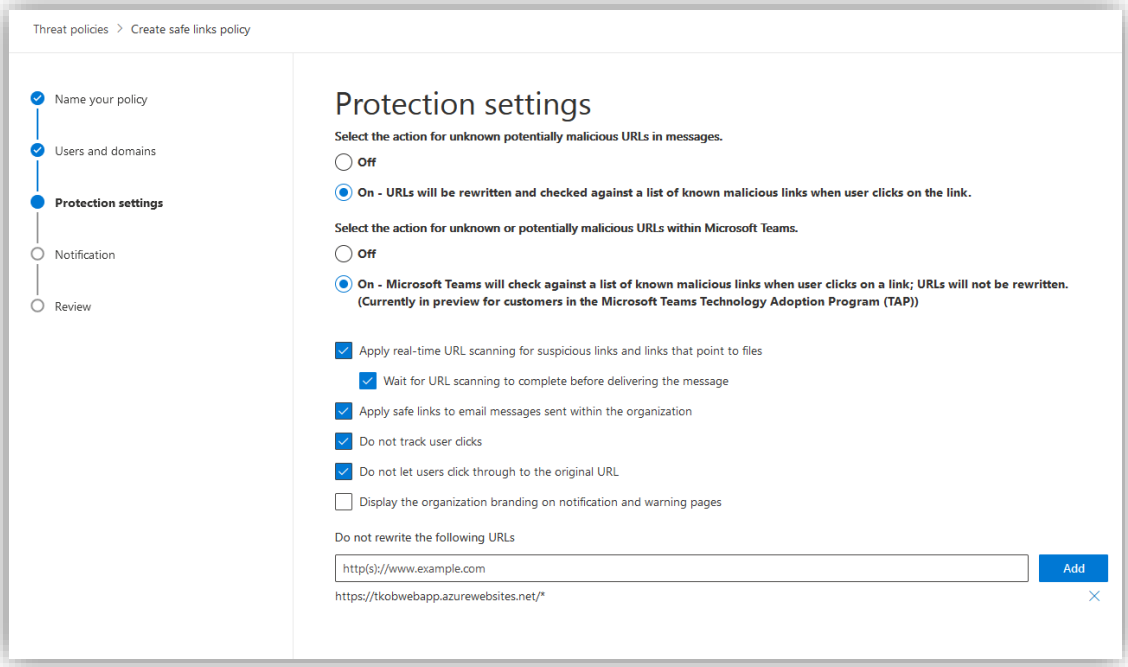
Skriv inn et passende navn for policyen.



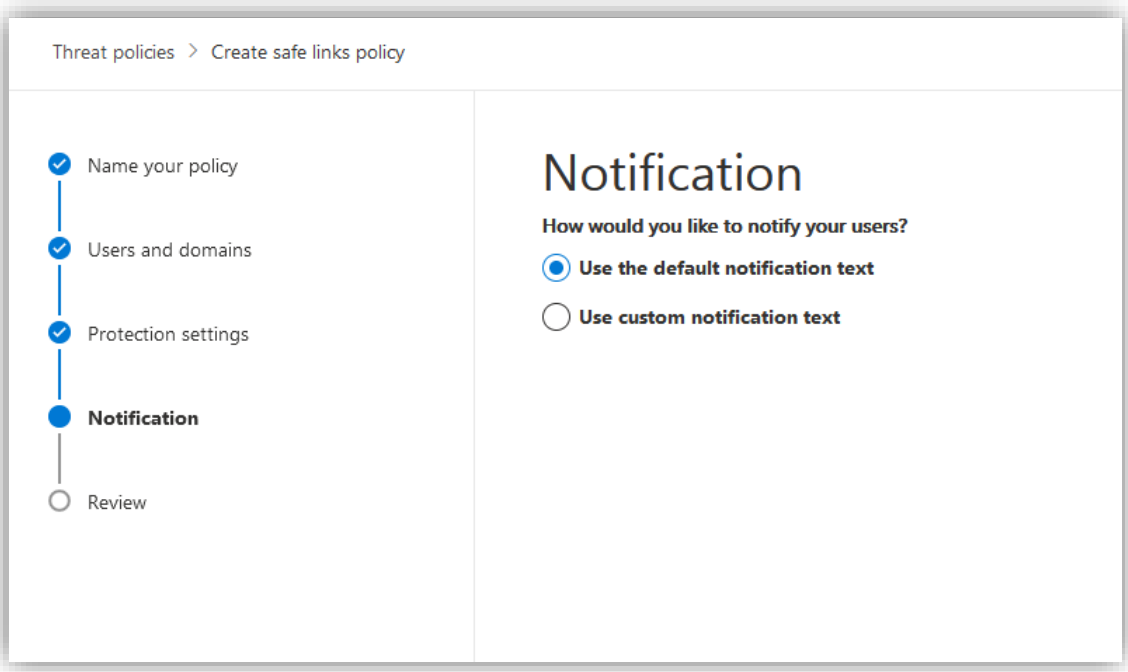
Under **Users and domains**, legg til alle brukere og det aktuelle domenet. Dette definerer hvem policyen gjelder for.



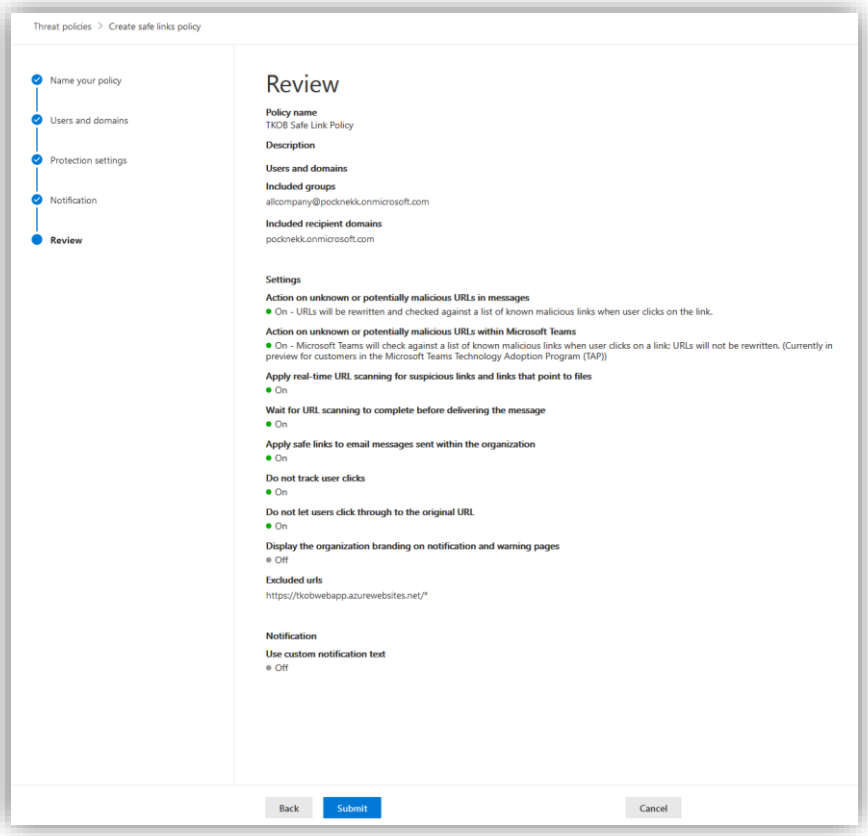
Under **Protection settings**, skru på at URL-er skal bli omskrevet og sjekket opp mot en liste med farlige lenker. Gjør det samme for lenker i MS Teams. Huk av for at det skal kjøres kontinuerlig skanning av lenker som peker til filer, og for at disse filene ikke skal kunne åpnes før skanningen er ferdig. Huk av for at Safe links skal brukes på e-post innad i organisasjonen. Skru også av loggføring av brukerklikk. Nederst kan en legge til URL-er som ikke trenger å omskrives. Her kan en for eksempel legge til URL-er fra intranettet.



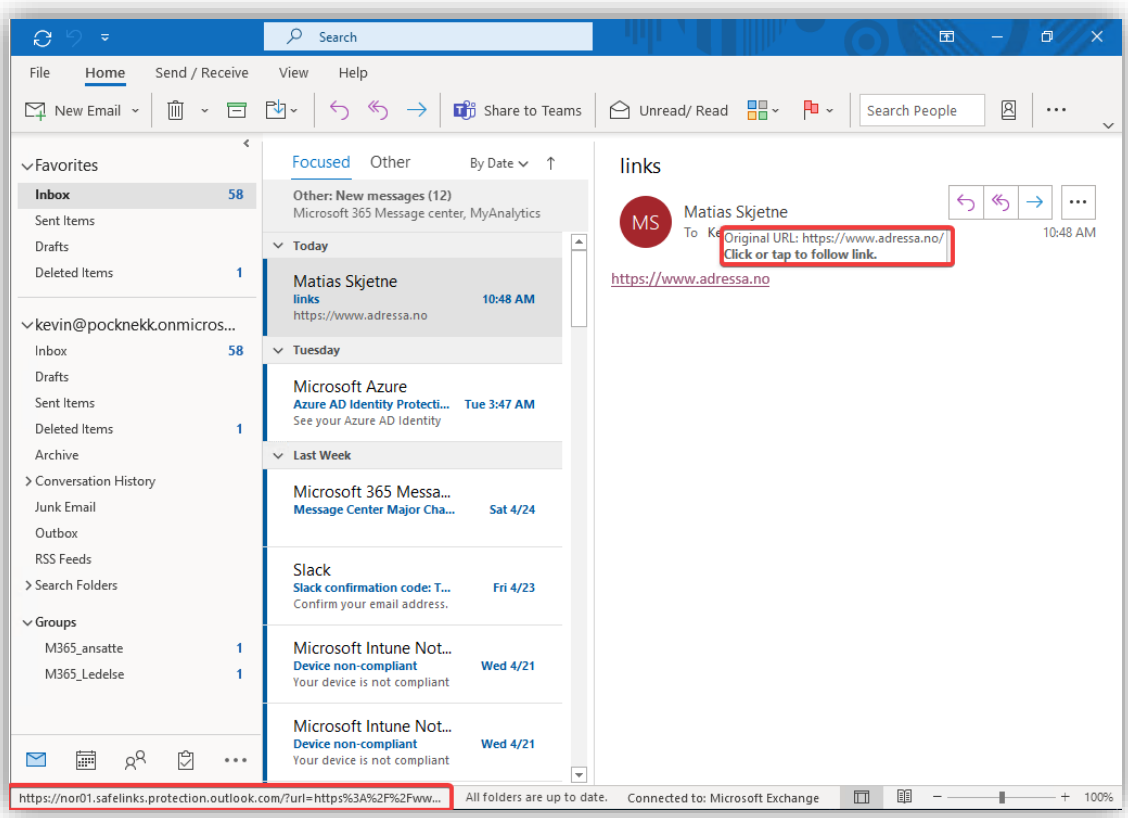
Under **Notification**, velg å bruk standard melding.



Se over policyen og trykk **Submit**. Policyen er nå aktivert.



Dersom en ansatt nå sender en e-post med en lenke i, vil denne lenken bli omgjort til en **Safe link**. Slik ser det ut når en lenke blir sendt over e-post. Nederst i venstre hjørne ser du den omgjort lenken som en blir videreført til om en trykker på denne.



3.9.5.3 Konfigurere Safe Attachments

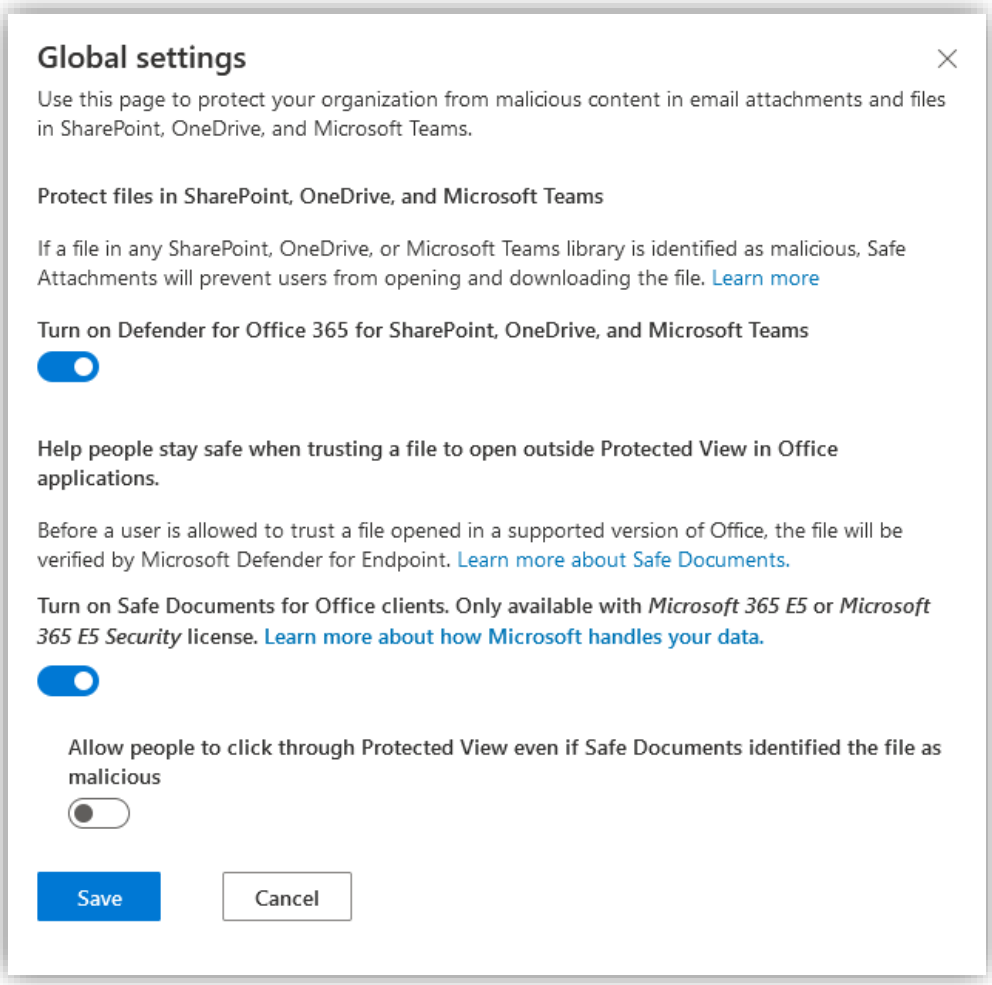
Safe Attachments gjør at vedlegg blir testet i et sikkert miljø - en *sandbox* - før den blir sendt til sluttbrukeren. I denne sandoksen blir adferden til filen analysert for å sjekke om den kommer til å gjøre noe mistenkelig. Dette er til kontrast til anti-malware, som sjekker etter signaturen til filen, mens Safe Attachments ser på hvordan filen eller programmet oppfører seg. Ettersom denne prosessen tar litt tid, mellom 2 til 15 minuttet ifølge Microsoft, kan man konfigurere dette etter behov.

Under **Email & collaboration**, gå til **Policies & rules > Threat policies > Safe attachments.**

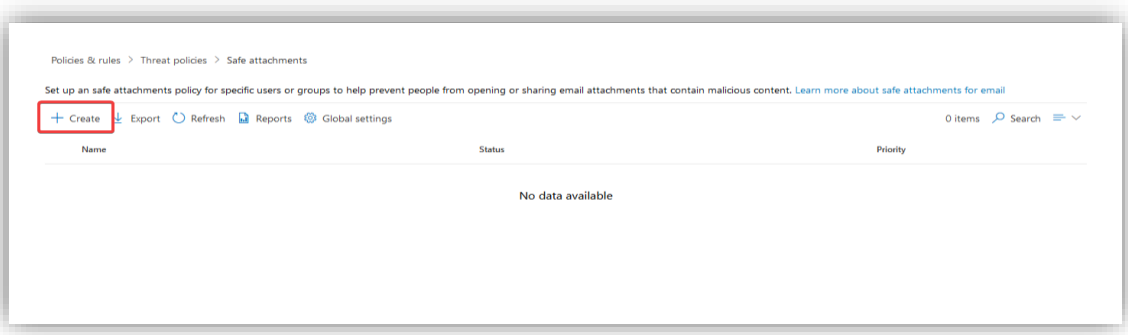
Trykk på **Global settings** for å sette de globale innstillingene for Safe Attachements.

- Skru på **Defender for Office 365** for SharePoint, OneDrive og MS Teams. Dette forhindrer brukere i å åpne filer som er identifisert som skadelige.
- Skru på **Safe Documents for office clients**. Dette gjør at filer blir sendt til Microsoft Defender for Endpoint for å analyseres før brukeren kan åpne filen.
- Ikke la brukerne trykke seg igjennom i Protected View, ettersom dette er anbefalt av Microsoft.

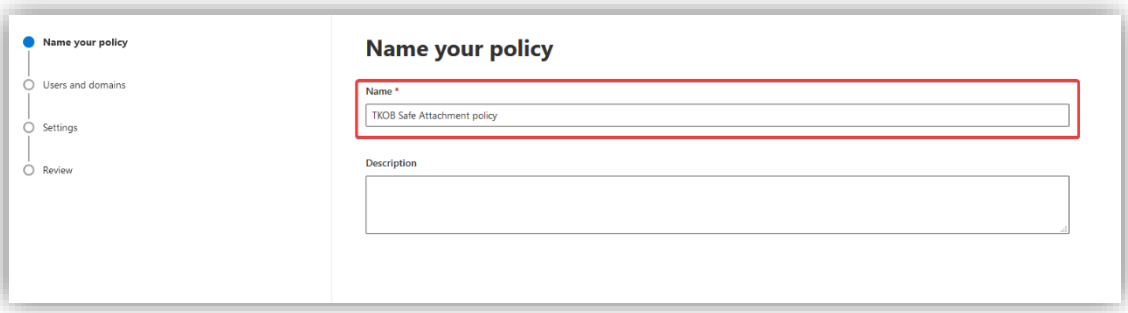
Trykk så på **Save.**



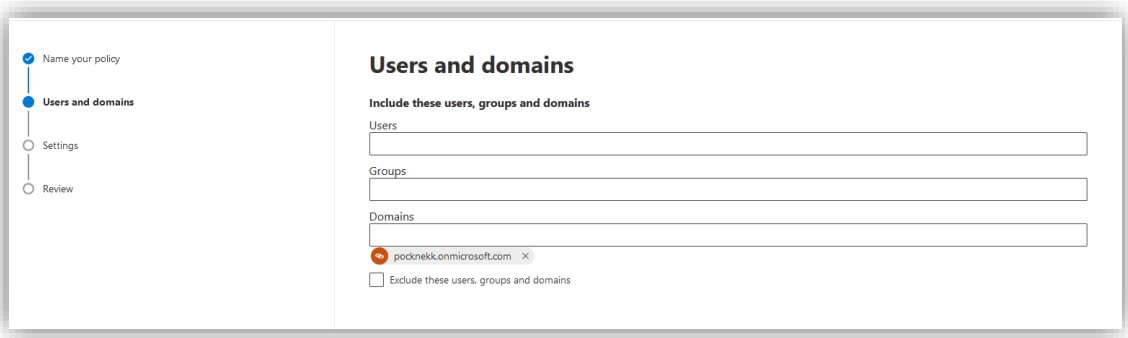
Trykk på **Create** for å lage en policy for vedlegg.



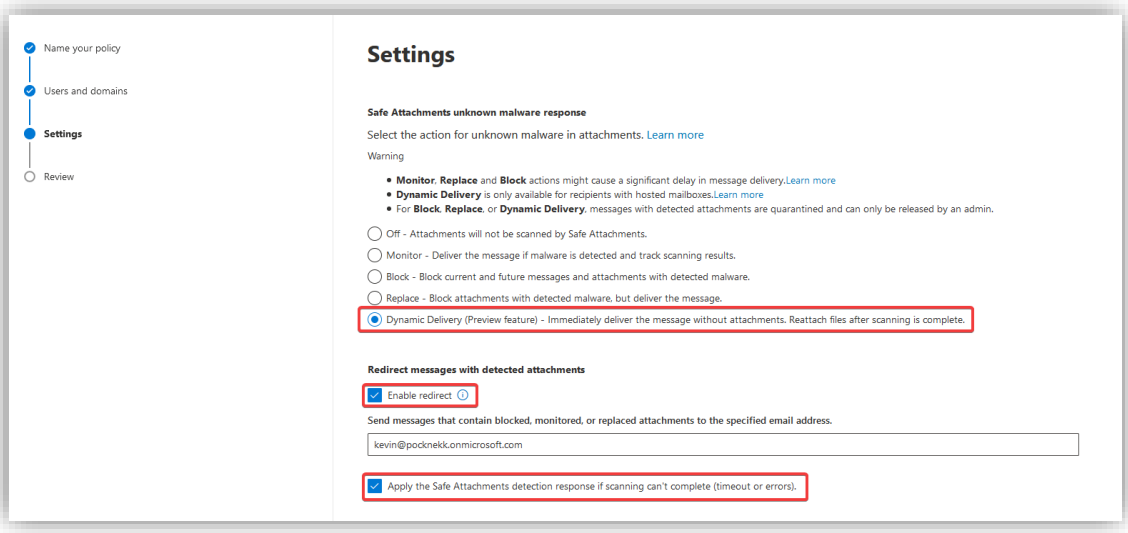
Gi policyen et passende navn.



Under **Users and domains** legg til domenet til bedriften.

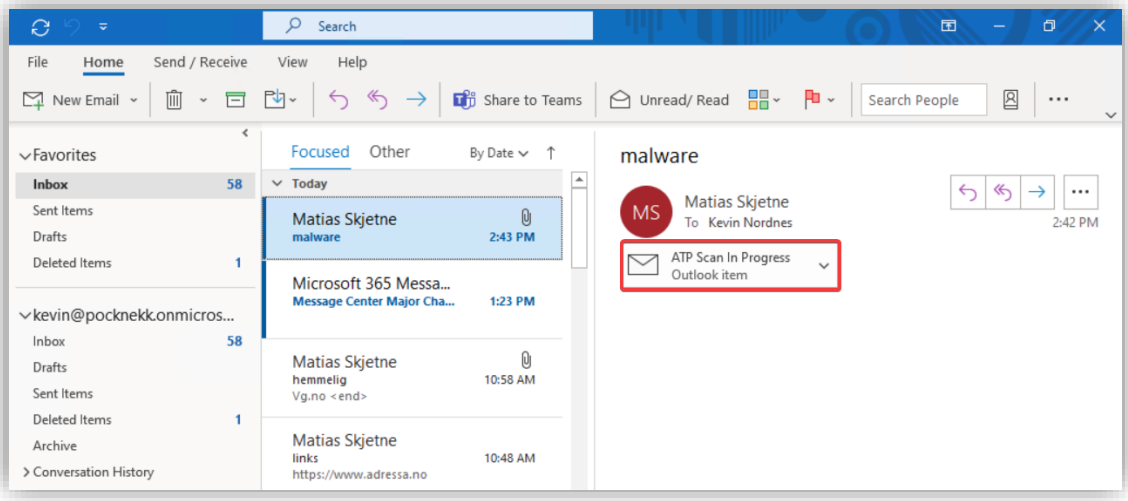


Under **Settings**, velg **Dynamic delivery**. Dette gjør at meldinger blir levert umiddelbart, men vedlegg må skannes før de sendes til mottakeren. Mottakeren vil se en boks med en forklaring på at filen blir sjekket før den blir sendt videre. Mottakeren vil også kunne se en forhåndsvisning av Word og PDF dokumenter. Skru på videresending og at brukere skal varsles dersom skanningen ikke klarer å fullføre – på grunn av en feil eller tidsbruk.



Fullfør ved å trykke **Submit** på den neste fanen.

Når filer blir sendt vil mottakeren se en slik melding før den kan åpnes. Word og PDF-filer kan ses i en forhåndsvisningsmodus får dokumentet er ferdig skannet.



3.10 Avslutning

Etter å ha fulgt denne guiden skal man ende opp med et system som er brukervennlig og sikkert. Mye fokus har blitt lagt på å gjøre sikkerheten så transparent for brukeren som mulig, slik at de får en enkel brukeropplevelse. Sikkerheten støttes opp av mange bak omliggende systemer som beskytter mot vanlige angrepsvektorer bedrifter i dag må forholde seg til og overvåkningsverktøy sørger for at angrep blir oppdaget raskt og håndtert. Systemet er ikke komplett og det er flere teknologier som kan utforskes for å gjøre det enda bedre, videre arbeid diskuteres i sluttrapporten.

3.11 Referanser

Her er en oversikt over referanser vi har brukt i denne rapporten

3.11.1 Azure AD

John Savill. (2020, February 10). *Managing Microsoft Azure Active Directory* [Video]. Pluralsight. https://www.pluralsight.com/courses/microsoft-azure-managing-active-directory

Compare Active Directory to Azure Active Directory. (2020, February 26). Microsoft Docs. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad

3.11.2 Microsoft 365 Admin Center

Set up Microsoft 365 Business Premium - Microsoft 365 Business. (2021, January 5). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/business/set-up?view=o365-worldwide

3.11.3 Autopilot

Overview of Windows Autopilot. (2020, December 16). Microsoft Docs. https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot

Create device groups for Windows Autopilot - Microsoft Intune - Microsoft Intune. (2021, March 16). Microsoft Docs. https://docs.microsoft.com/en-us/mem/autopilot/enrollment-autopilot

Configure Autopilot profiles. (2020, December 16). Microsoft Docs. https://docs.microsoft.com/en-us/mem/autopilot/profiles

Windows Autopilot Enrollment Status Page. (2020, December 16). Microsoft Docs. https://docs.microsoft.com/en-us/mem/autopilot/enrollment-status

3.11.4 Intune

What is Microsoft Intune - Azure. (2020, June 23). Microsoft Docs. https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Tutorial: Walkthrough Intune in Microsoft Endpoint Manager. (2021, April 12). Microsoft Docs. https://docs.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager

Device features and settings in Microsoft Intune - Azure. (2021, April 15). Microsoft Docs. https://docs.microsoft.com/en-us/mem/intune/configuration/device-profiles

Greg Shields. (2020, April 28). *Enroll Devices into Microsoft Intune* [Video]. Pluralsight. https://www.pluralsight.com/courses/enroll-devices-microsoft-intune

Greg Shields. (2020b, April 28). *Introduce Microsoft Endpoint Manager and Prepare Microsoft Intune* [Video]. Pluralsight. https://www.pluralsight.com/courses/introduce-microsoft-endpoint-manager-prepare-microsoft-intune

Create device profiles in Microsoft Intune - Azure. (2021, February 17). Microsoft Docs. https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

Provisioning packages (Windows 10) - Configure Windows. (2017, July 27). Microsoft Docs. https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

3.11.5 Information Protection

Robert McMillen. (2021, March 23). *Microsoft 365 Security: Information Protection Implementation and Management* [Video]. Pluralsight. https://www.pluralsight.com/courses/msft-365-security-information-protection-implementation-management

Microsoft Information Protection in Microsoft 365 - Microsoft 365 Compliance. (2021, March 26). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

Learn about sensitivity labels - Microsoft 365 Compliance. (2021, April 20). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Get started with sensitivity labels - Microsoft 365 Compliance. (2021, April 23). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

Create and publish sensitivity labels - Microsoft 365 Compliance. (2021, April 23). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide

Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance. (2021, April 29). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide

Automatically apply a sensitivity label to content in Microsoft 365 - Microsoft 365 Compliance. (2021, April 22). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

Use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and SharePoint sites - Microsoft 365 Compliance. (2021, April 16). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

Enable sensitivity labels for Office files in SharePoint and OneDrive - Microsoft 365 Compliance. (2021, April 2). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide

Encryption in Microsoft 365 - Microsoft 365 Compliance. (2019, August 15). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption?view=o365-worldwide

Email encryption in Microsoft 365 - Microsoft 365 Compliance. (2019, August 28). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption?view=o365-worldwide

3.11.6 App service

Quickstart: Create a Node.js web app - Azure App Service. (2020, January 8). Microsoft Docs. https://docs.microsoft.com/en-us/azure/app-service/quickstart-nodejs?pivots=platform-linux

Deploy and run a containerized web app with Azure App Service - Learn. (n.d.). Microsoft Docs. Retrieved May 4, 2021, from https://docs.microsoft.com/en-us/learn/modules/deploy-run-container-app-service/

Explore Azure compute services (AZ-900) - Learn. (n.d.). Microsoft Docs. Retrieved May 4, 2021, from https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/

3.11.7 Sikkerhet

3.11.7.1 Sentinel

Introduction to Azure Sentinel - Learn. (n.d.). Microsoft Docs. Retrieved May 4, 2021, from https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-sentinel/

Query logs in Azure Sentinel - Learn. (n.d.). Microsoft Docs. Retrieved May 4, 2021, from https://docs.microsoft.com/en-us/learn/modules/query-logs-azure-sentinel/

Create and manage Azure Sentinel workspaces - Learn. (n.d.). Microsoft Docs. Retrieved May 4, 2021, from https://docs.microsoft.com/en-us/learn/modules/create-manage-azure-sentinel-workspaces/

What is Azure Sentinel? (2020, September 16). Microsoft Docs. https://docs.microsoft.com/en-us/azure/sentinel/overview

3.11.7.2 Microsoft Defender for endpoint

Use attack surface reduction rules to prevent malware infection. (2021, April 26). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide#rule-block-credential-stealing-from-the-windows-local-security-authority-subsystem-lsassexe

Overview of Microsoft Defender Security Center. (2021, April 3). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/use?view=o365-worldwide

3.11.7.3 Microsoft Defender for Office 365

Paul Cunningham. (2018, May 8). *Configuring and Managing Office 365 Security* [Video]. Pluralsight. https://www.pluralsight.com/courses/configuring-managing-office-365-security

Office 365 Security, Microsoft Defender for Office 365, EOP, MSDO - Office 365. (2020, August 13). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/overview?view=o365-worldwide

Microsoft Defender for Office 365 - Office 365. (2021, April 9). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/defender-for-office-365?view=o365-worldwide

Step-by-step threat protection stack in Microsoft Defender for Office 365 - Office 365. (2021, April 5). Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide

4 SLUTTRAPPORT

4.1 Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
13/mai/2021	0.1	Første utkast	Kevin Nordnes & Matias Skjetne
19/mai/2021	1.0	Endelig utkast	Kevin Nordnes & Matias Skjetne

4.2 Innledning

I denne rapporten skal vi ta for oss arbeidet som ble utført, diskutere løsningene vi prøvde ut og læringsutbyttet vi sitter igjen med. Vi diskuterer hvordan samarbeidet i gruppen fungerte og løsningen vi til slutt satt igjen med. Vi kommer også med anbefalinger til veien videre hvor vi går inn på hvordan systemet kan videreutvikles og bygges videre på.

4.2.1 Dokumentets hensikt

Sluttrapporten kan ses på som en egenvurdering av prosjektet og løsningen. Rapporten skal gi en oversikt over hvordan resultatet ble i forhold til målene som ble satt i forstudierapporten, samt hvordan systemet ble i forhold til designet i designrapporten. Prosjektet som en bacheloroppgave og prosjektet som en implementering av et system blir vurdert. Dette skal være med på å vurdere prosjektets suksess, med hensyn til «kunden» og produktet, men også med hensyn til prosjektdeltakernes kompetansebygging.

4.2.2 Avgrensninger

Vurderingen som tas i denne rapporten blir kun gjort av oss (prosjektdeltakerne), og er derfor ikke nødvendigvis den samme vurdering «kunden» eller veiledere ville kommet med. Vurderingen begrenser seg derfor til vår egen selvinnsikt til hvordan gjennomføringen har gått og til vår egen kompetanse til å vurdere om prosjektet nådde de målene som er satt – da spesielt knyttet til den tekniske delen. Mange av valgene som har blitt tatt underveis har blitt beskrevet i driftsrapporten og vil derfor ikke bli tatt med i diksjonsdelen av denne rapporten. Større valg som ble gjort og ikke kom med i selve implementeringen vil derimot bli diskutert her.

4.2.3 Definisjoner og forkortelse

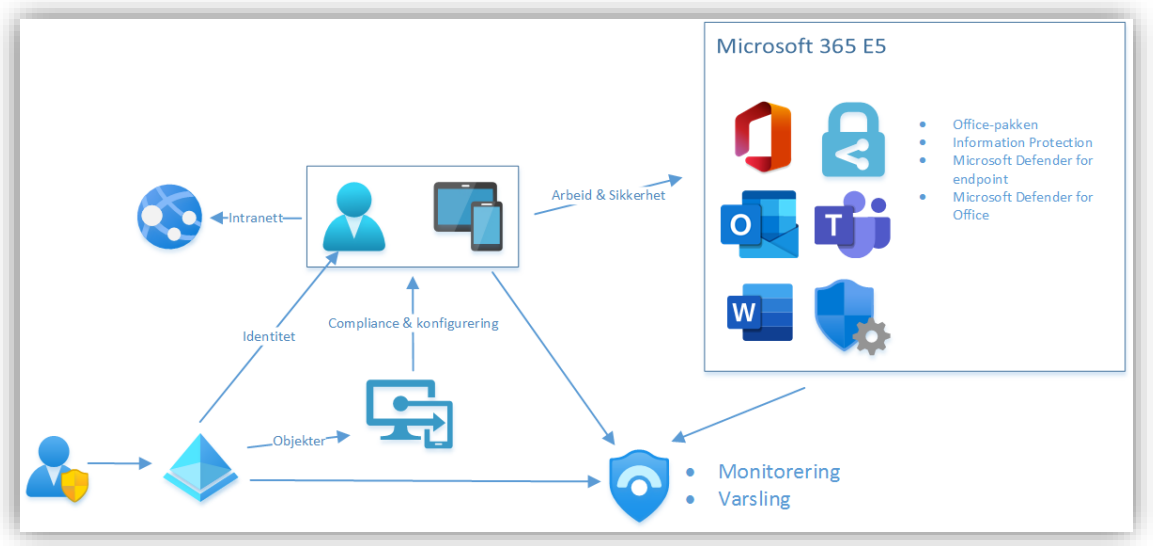
AIP – Azure Information Protection
Prosjektdeltakere – Matias Skjetne og Kevin Nordnes
TKoB – Trondheim Knekk og Brekk AS

4.2.4 Oversikt over innholdet

Under Løsningen (4.3) beskrives systemet, ulike valg som ble gjort og en vurdering om oppgaven ble svart på. Punktet Utfordringer (4.4) inneholder drøfting av de mest sentrale utfordringene om oppstod under prosjektet. En mer grundig gjennomgang av prosjektforløpet ligger under punktet Prosessen (4.5) hvor samarbeidet og læringsutbyttet også diskuteres. Helt til slutt gis anbefalinger om videre arbeid, under punktet Veien videre (4.6), før prosjektet konkluderes (4.7).

4.3 Løsningen

Løsningen som er beskrevet i designrapporten avviker fra løsningen som til slutt ble levert. Da vi så at løsningen slik den originalt var tiltenkt viste seg å gi det ønskede resultatet, endret vi designet. Dette ble gjort gjennom en endringsmelding som er vedlagt vår oppgave. Under beskriver vi endringene fra det originale designet til det endelige designet og alle løsningene som ble utprøvd.



Ut ifra tegningen over kan man se endringene i systemet fra designrapporten, det meste av systemet er fortsatt den samme bortsett fra at det ikke lenger finnes en sikker sone. Systemet baserer seg på identiteter og Azure AD står sentralt i behandlingen av disse. Intune brukes for å administrere maskiner og sørge for at disse er følger sikkerhetsstandarder i bedriften. Sentinel overvåker systemet og varlser om hendelser. Microsoft 365 gir de ansatte produktivitetsverktøy som Word og Powerpoint og sørger for sikkerheten i systemet gjennom et bredt utvalg av sikkerhetstjenester. App Service har blitt flyttet ut av den sikre sonen og tilbyr intranett tjenester back to faktor autentisering.

4.3.1 Sikker sone

Det originale designet besto av to deler, en sone hvor de ansatte skulle gjøre vanlig arbeid, som å sende e-post og annet administrativt arbeid som ikke omfavner opplysninger sensitive for bedriften, og en sikker sone hvor strengere regler gjelder. I denne sonen skulle man f.eks. ikke kunne kopiere data ut eller dele data med hvem som helst.

Da vi planla implementeringen, så vi for oss å sette opp den usikre sonen først og bygge den sikre etterpå. Dette fordi den usikre sonen er veldig enkel og består for det meste bare av Office-produkter. Vi tenkte også at den sikre sonen skulle bygge på den usikre og bruke mye av de samme teknologiene bare med strengere regler og policyer. Det eneste vi visste var at sikre sone skulle basere seg på at brukeren måtte nå inn i sonen med Windows Virtual Desktop (WVD).
Hvordan sonen i seg selv skulle bygges opp viste vi ikke. Oppsettet av WVD gikk fint, men da vi skulle starte oppbyggingen av sikker sone fikk vi problemer. Løsningen hadde noen konkrete kriterier som måtte oppfylles:

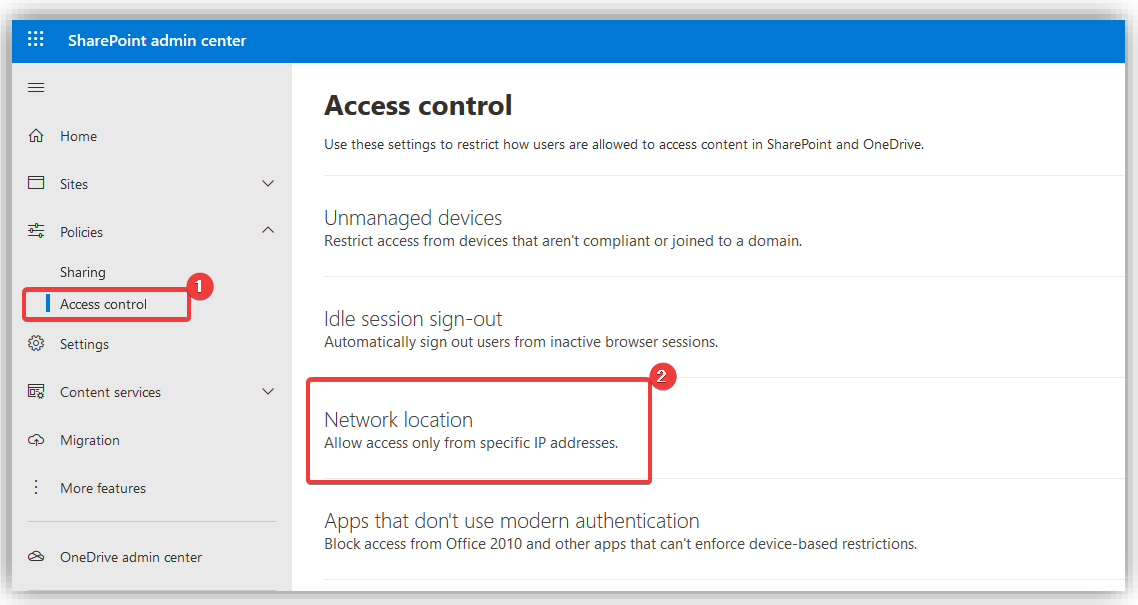
- Data skal ikke kunne kopieres ut av sikker sone.

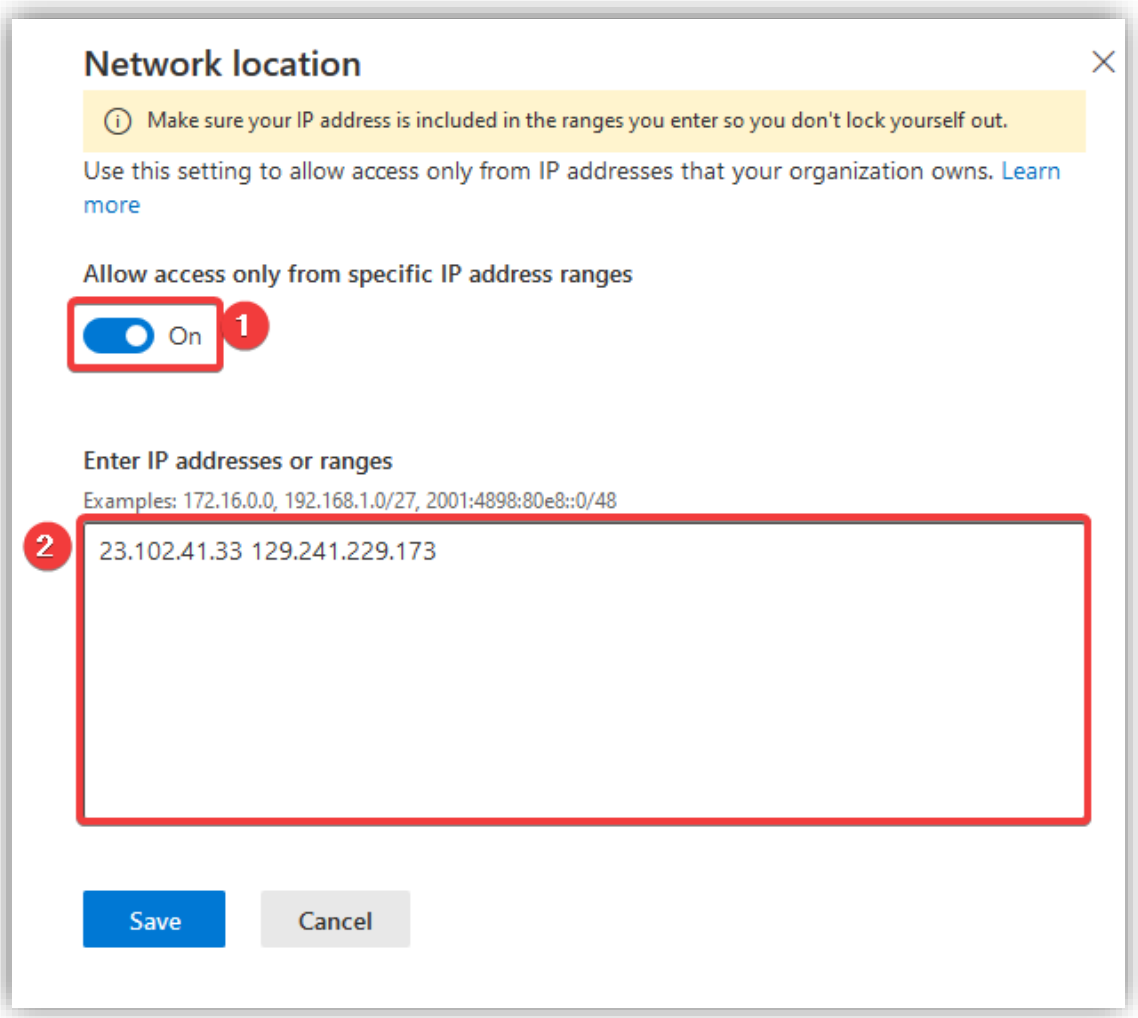
- Man skal ikke kunne dele data med personer utenfor sikker sone
- Data som hører hjemme i sikker sone skal automatisk legges der når den opprettes/blir forsøkt delt utenfor sikker sone.

De første to punktene hadde vi en viss aning om hvordan vi ville oppnå. Vi så for oss et lagringssystem separert bort fra den vanlige sonen, som benytter seg av SharePoint og OneDrive, og vi prøvde ut tre forskjellige løsninger på dette problemet. To i SharePoint og en i Azure files.

SharePoint – Access Control

Her så vi for oss en enkel løsning hvor man begrenset IP området som kunne nå SharePoint. Tanken var at man kun skulle nå visse sites fra IP-området til det interne Azure nettverket som Wvd ligger i. Dette konfigurerte vi fra administratorpanelet i SharePoint:





Dette fungerte på sett og vis, og nå kunne man bare nå SharePoint fra min pc og alle WVD instansene. Problemet var at man ikke kunne gjøre dette på en per site basis. Dette betydde at normal bruk av SharePoint ikke var mulig, alt måtte gjøres gjennom WVD. Dette gikk utover brukervennligheten av systemet og var ikke en ideell løsning dermed måtte vi finne på noe annet.

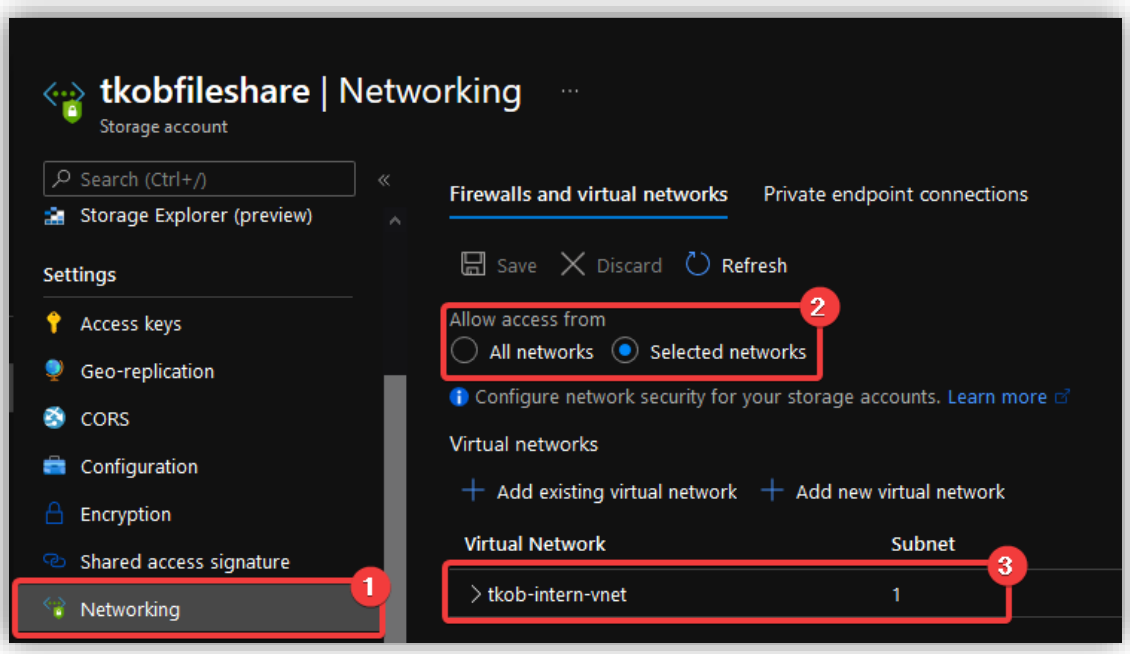
4.3.1.1 SharePoint Server – lokal instans

Siden vi ikke kunne delegere tilgang på sites i SharePoint basert på maskiner eller lokasjoner, tenkte vi at vi kunne sette opp en ny SharePoint instans kjørende på VM-er i Azure. Dette var ikke en like vedlikeholdsfri løsning siden serverne måtte vedlikeholdes av oss og ikke av Microsoft. Dette gjorde det til en lite ideell løsning, men vi tenkte det var verdt å prøve det uansett.

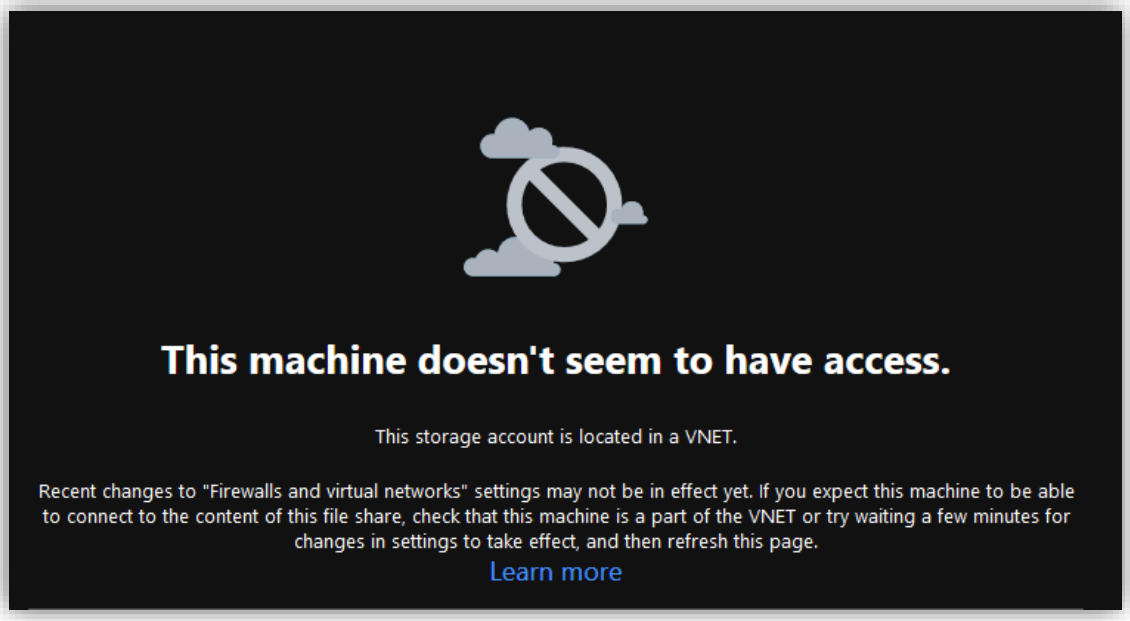
Vi kom dog ikke veldig langt med denne implementasjonen, det viste seg at SharePoint Server krever en del for å settes opp og trives dårlig i et miljø uten fysisk domenekontroller. Vårt system bygger på en ren skyløsning med både AD (Azure AD) og domenekontroller (Azure ADDS) i Azure. Vi hadde også trengt flere servere med databaser for å få systemet til å fungere. Derfor bestemte vi oss for å skrinlegge denne løsningen og heller se etter enklere alternativer.

4.3.1.2 *Azure files*

Tanken bak Azure Files var at vi skulle ha fileshares som kun kunne monteres på WVD-maskinene. De ansatte skulle kunne dele filer mellom seg slik man gjorde det på gamle on-prem-systemer før man tok i bruk skydeling som OneDrive og SharePoint. Dette var i praksis veldig enkelt å sette opp.



Her har vi valgt hvilket nettverk som man kan nå filsharen fra.



Dette er meldingen som møter en om man ikke befinner seg i det interne v-nettet.

Vi fikk montert diskene inne i WVD-miljøet og alt virket vell. Problemet med denne løsningen er at den ikke er veldig fleksibel. Man har i grunn egentlig bare mapper som man enten har tilgang til, eller ikke, og det finnes ingen dynamisk måte å bestemme hvem som har tilgang til mappene. Det er veldig enkelt å sette opp mapper som er delt med f.eks. hele avdelinger, men med en gang man vil gjøre mer komplekse ting som tidsbegrenset deling mellom to spesifikke ansatte blir det vanskelig.

Om ansatt A vil dele et regneark med ansatt B uten at hele avdelingen trenger å se det, finnes det ingen god måte å gjøre dette på. Man måtte i så fall opprettet en ny mappe som kun disse to har tilgang til. Dette er ikke noe brukeren selv kan gjøre og det er ikke realistisk at en administrator skal gjøre det hver gang noe skal deles. På grunn av disse begrensningene i brukervennlighet valgte vi å skrinlegge denne løsningen.

4.3.2 Information Protection

Etter mye frem og tilbake, og diskusjoner med både veileder og konsulenter i Atea, kom vi frem til at den beste løsningen lå i Information Protection. Dette var noe vi uansett skulle ta i bruk og når vi så nærmere på løsningen, så vi at det var mulig å begrense tilgang til SharePoint sites basert på sensitivitets merkinger (sensitivity lables). Dermed kunne vi styre hvem som hadde tilgang til sensitiv informasjon og hvor denne kunne lagres. Vi kom også frem til at det var best å skrinlegge den sikre sonen. Information Protection lot oss styre hvor data kan ta veien gjennom systemet og en sikker sone bak WVD vil ikke føre til noen ekstra sikkerhet. Vi kunne isteden bruke Intune og Information Protection til å bestemme at sensitiv informasjon kun kan lagres på maskiner som oppfyller sikkerhetskravene (compliance) vi stiller.

Ved å gå bort fra WVD gjorde vi brukeropplevelsen bedre for de ansatte; de slipper å forholde seg til et ekstra sett med applikasjoner som ligger i en sikker sone. Microsofts filosofi virker å være at man skal kun styre tilganger etter identitet og kryptere innhold slik at om man sender noe til feil sted vil det ikke få store konsekvenser. Denne måten å tenke på gjør at systemet kan bygges enklere og man slipper å tenke mye på hvor informasjon kan befinne seg til enhver tid. Gjennom Azure AD har man god kontroll på identiteter i sin bedrift og da gir det mening å bygge systemet sitt rundt dette faktumet. Det tok tid før vi forstod dette konseptet og derfor gikk det med mye tid på å prøve å lage noe som gikk imot Microsofts tankegang. Da vi endelig forsto at identitet står i sentrum ble det mye lettere å forme teknologien til et fungerende system.

4.3.3 Klarte vi å svare på problemstillingen?

Trondheim Knekk og Brekk AS skulle oppgradere sine systemer ved å ta i bruk Microsoft sine løsninger og ha er fokus på å ta vare på sikkerheten til dataen som ble lagret i bedriften. Hovedutfordringen var at TKoB lagrer mye personsensitiv data som må kunne sendes mellom de ansatte uten at data kommer på avveie. Samtidig skal ikke sikkerhet gå ut over brukeropplevelsen til da ansatte og effektiviteten i bedriften – løsningen skulle være så transparent for brukeren som mulig.

Slik systemet fungerer vil de ansatte bli tildelt en Microsoft 365 E5 lisensen som inneholder Office-pakken som de allerede skal være kjent med. Alt av data blir lagret i skyen i SharePoint hvor de ansatte kan samhandle og dele filer mellom seg. På denne måten har ikke det nye systemet gått ut over brukeropplevelsen til de ansatte i form av at de må lære seg et helt nytt system. Alle programmene som fantes i Office 365 E3-lisensen de tidligere brukte, finnes også i Microsoft 365 E5-lisensen (med mer).

Selv om deling av dokumenter og samskriving vil gjøre at arbeidet til de ansatte kan fungere på en enkel og effektiv måte, svarer ikke dette på hvordan informasjon skal kunne sikres og tas vare på innad i bedriften. For å løse dette benytter vi av oss Azure Information Protection (AIP) for at brukere kan merke (lable) ulike filer for å begrense tilgangen og sette rettigheter. AIP kan kryptere filer slik at du kun kan aksesseres av brukere med de rette nøklene. Dette gjør at det ikke skal «ha noe å si» hvor disse dokumentene ligger, f.eks. om de skulle komme på avveie, ettersom det er kun de ansatte eller rette brukerne som har muligheten til å åpne, redigere og sette rettigheter på dokumentene. Dette gjør at brukerne ikke trenger å tenke på at filer skal havne på avveie, men det forutsetter at de ansatte faktisk husker å sette riktig label på dokumentene de oppretter.

AIP tar seg av hovedparten av det som har med personvern og datasensitivitet å gjøre, men alt dette vil ikke ha noe å se dersom ikke bedriften sikrer sine brukere og enheter. Microsoft Intune brukes til å rulle ut applikasjoner (MAM), samt konfigurere enhetene slik at de følger de krav som settes til compliance (MDM). Microsoft Defender for endpoint (MDE) gjør at en kan sette en rekke policyer som sikrer enhetene, blant annet kryptering, antivirus og brannmur. Med Intune kan enhetene «onboardes» med MDE og sikres ved hjelp igjennom Microsoft Endpoint Manager admin center. Her har vi satt universelle policyer som gjør at alle enheter i domenet vil få de samme sikkerhetspolicyene. Dersom en enhet skulle komme på avveie kan bedriften være sikker på at all dataen er kryptert og at angrep fra nettet blir stoppet av brannmur og antivirus.

Microsoft Defender for Office 365 (MDO) fungerer også som et ekstra lag med sikkerhet på bruk av e-post. Gjennom tjenestene Safe Links, Safe Attachements og Anti-malware, passer MDO på at det ikke blir sendt og åpnet filer som kan skade enheten eller systemet. Dette igjen fungerer helt automatisk og er ikke noe brukeren selv trenger å tenke på, med unntak av at det blir en liten forsinkelse i sendingen. Denne forsinkelsen er så liten at vi er sikre på at dette ikke vil gå utover effektiviteten til den enkelte ansatte.

Gjennom disse tjenestene kan TKoB arbeide uten noen bekymring for at deres data skal kunne havne i feil hender. Den menneskelige faktoren til å gjøre feil er gjort så minimal som mulig. Det skal derimot poengteres, som det tidligere også ble nevnt, at dokumenter og filer må klassifiseres av brukerne selv. Gjøres ikke dette, er dataen åpen for alle som har fått tak i den. Auto labeling ville delvis løst dette problemet ved at dokumenter automatisk ble klassifisert dersom det ble oppdaget å inneholde sensitiv informasjon. En begrensning til tilgangen til denne funksjonen gjør derimot at dette ikke er en del av den endelige løsningen.

Om dataen blir holdt konfidensiell er en ting, en annen faktor er brukerne som må sikres for identitetstyveri og innbrudd. Azure AD Identity Protection sørger for at all mistenkelig pålogging og identitetsbasert aktivitet, blir loggført og stanset dersom hendelsen er identifisert som høy risiko.

Alle sikkerhetstjenestene som er nevnt over samler inn data om hendelser og aktivitet som kan være trusler mot bedriften. Med Azure Sentinel sentraliseres all denne dataen på et sted ved å koble den aktuelle datakilden (f.eks. Azure AD Identity Protection) til Sentinel. Denne tjenesten analyserer så denne dataen. Dersom det skulle oppstå en hendelse (f.eks. et innbrudd eller skadevare på en enhet blir oppdaget) vil Sentinel automatisk rapportere dette til IT-avdelingen.

Sammen mener vi at alle disse tjenestene, både med tanke på sikkerhetstjenester og brukertjenester, gir en løsning som svarer til de krav som oppgaven krever og spør etter. I sin helhet er dette et system som vi mener oppfyller kravene om at det skal være brukervennlig, sikkert og transparent for sluttbrukeren og bedriften i sin helhet. Systemet er en totalløsning som skal inneholde alt av funksjonalitet som TKoB har behov for å fullføre sine elementære administrative oppgaver.

4.4 Utfordringer

Her diskuterer vi utfordringer vi møtte på i løpet av prosjektet.

4.4.1 Designfasen

Den første utfordringen vi støtte på var ved selve utformingen og designet av systemet. Denne delen kommer i en veldig tidlig del av et prosjekt og er med på å bestemme hvilke aktiviteter prosjektet skal inneholde og hvordan oppgaven skal løses. Poenget med en bacheloroppgave er å skaffe seg en viss kompetanse som kan brukes ute i arbeidslivet, men samtidig krever oppgaven enn viss kompetanse for å utføres. Det å designe et system med tjenester og teknologier som vi aldri har vært borti før viste seg å være en krevende oppgave og førte til mye usikkerhet og synsing.

Det å få oppgaven, tjenestene og teknologien forklart er en ting, og det hjalp oss en god del på veien, men det var først når vi fikk prøve oss selv på Microsoft sine tjenester at vi begynte å se en helhet i det vi drev med. Det å skulle skissere ut et system så tidlig i fasen var derfor en stor utfordring, men vi følte vi lærte mye av det. Det er en god del avvik fra det det systemet vi så for oss og det endelige systemet hvis man ser stort på det – tjenestene som ble beskrevet i designfasen er likevel fortsatt med (med unntak av WVD). Det er kanskje nettopp dette som viser kompetansen som vi tilegnet oss underveis i prosessen.

4.4.2 Auto-labling

I vår implementasjon er det noen mangler ved Information Protection - vanligvis ville man tatt i bruk Auto Labeling funksjonaliteten for å automatisk sette opp regler for markering av filer og dokumenter. Dette ville tillatt oss å finne dokumenter i systemet som inneholder sensitiv informasjon, f.eks. personnummer, lønnslipper eller bedriftshemmeligheter og markert disse med riktig tilgangskontroll. Dette er en stor del av Information Protection og vår løsning er mindre dekkende på grunn av dette.

Denne delen av Information Protection var ikke tilgjengelig for oss da dette er ny funksjonalitet og ikke tilgjengelig i alle Regioner. Vår Tenant i Azure ligger i Norge og er dermed en del av gruppen med regioner hvor dette ikke er tilgjengelig. Mye tid ble brukt på å forsøke å løse dette problemet, blant annet ble det tatt kontakt med Microsoft support som tok flere uker å få avklart. Til slutt måtte vi innse at vi ikke fikk tatt i bruk denne funksjonaliteten.

På tross av problemene var det en veldig lærerik opplevelse. Det å jobbe med Microsoft support er en vanlig del av hverdagen for en IT-konsulent og en nyttig erfaring å ta med seg videre. Det er viktig å ta med i vurderinger og tidsberegninger at om man støter på et problem som dette så kan det ta tid å få hjelp og løse.

4.4.3 Fravær av en reel kunde

Underveis i implementering blir det gjort en god del valg, som f.eks. hvor streng en passordpolicy skal være, noe som i en ekte situasjon er noe som hadde blitt gjort i dialog med sluttbrukeren og bedriften. Denne aktiviteten ble dermed preget av mye diskusjon mellom oss prosjektdeltakerne, samt dialog med konsulenter i Atea. I kontrast til utfordringene med å designe et system, hvor en kan lese seg opp og skaffe kompetanse på nettet, så står det ikke noe sted hva som passer en spesifikk bedrift når en skal konfigurere ulike policyer og spesifikasjoner.

Mye av utfordringen lå dermed i å se for seg behovene til en bedrift og en sluttbruker som ikke faktisk finnes. En viktig del av oppgaven er å lage et brukervennlig system som samtidig innehar tilstrekkelig med sikkerhet. Det er en fin balanse som må vurderes og prøves ut før en finner ut av hva som er den optimale løsningen for nettopp denne bedriften. Vi måtte dermed fungerer som våre egne testbrukere og ta avgjørelser mye basert på egen intuisjon og vurdering. Dette fungerte til en viss grad som et beslutningsgrunnlag, men vi fant fort ut at vårt begrensede testmiljø og mangel på erfaring fra arbeidslivet (i en slik setting) gjorde at det falt litt kort. Gode tilbakemeldinger fra veiledere og god veiledning fra konsulenter som kunne referere til reelle caser ble til stor hjelp. Sluttproduktet legger sikkerhetsnivået høyt, uten at det skal gå ut over en sluttbrukers arbeidsdag på noe betydelig måte. Det vil også komme fram i videre anbefalinger at disse konfigurasjonen ikke er endelige og bør justeres dersom en ser behovet.

4.5 Prosessen

Her diskutere vi prosessen og hvordan gjennomføringen av prosjektet gikk.

4.5.1 Gjennomføring

Prosjektet startet smått i starten av januar med noen møter, kontraktskriving og mye selvstendig research. I begynnelsen var arbeidet mye preget av usikkerhet, mye fordi den nødvendige kompetansen for å utføre prosjektet ikke var til stede hos oss som skulle gjennomføre prosjektet. Det ble derfor brukt mye tid på å få oversikt over alle teknologiene og tjenestene som kunne være med i en endelig løsning.

Samtidig som vi tilegnet oss den nødvendige grunnleggende kunnskapen, skrev vi forstudierapporten. Dette gikk i seg selv veldig greit, mye av oppgaven ble å definere prosjektet, mål, krav og rammebetingelser. Gjennom god diskusjon med veiledere, samt få krav til kompetanse knyttet til teknologiene, gikk denne delen av prosessen veldig bra.

Prosessen, spesielt den første måneden, ble preget av hjemmekontor og mye selvstendig arbeid. Vi følte oss mindre motivert av mye jobbing fra egen husstand. Fra uke 6 ble det derimot åpnet for å kunne jobbe på kontorene til Atea og vi merket begge at både effektivitet og motivasjon økte fra dette tidspunktet. Det å kunne jobbe på samme plass, samtidig som veileder og andre konsulenter var til stede, gjorde arbeidet mye mer gjennomførbart med tanke på samarbeidsevnen og tilgangen til veiledning, kompetanse og informasjon.

Ved designing av selve systemet (designrapporten) ble arbeidet en god del preget av mye informasjonshenting. Det ble brukt mye tid på å se gjennom Microsoft sin dokumentasjon, å se videoer på Pluralsight og generelt bruk av forum på nett for å finne en mulig løsning på oppgaven. Det ble tidlig bestemt at designet ikke skulle inneholde en fullstendig oversikt over systemet, da spesielt nettverket, ettersom dette krevde god kompetanse og innsikt – noe vi ikke hadde på denne tiden. Prosjektet i seg selv skulle gi oss denne kompetansen underveis, dette ble derfor et element som skulle være en del av sluttrapporten.

Implementeringen var den mest interessante, lærerike, men også den mest frustrerende delen av hele prosjektet. Selv om vi hadde et design å gå ut ifra, var det mye som manglet for at vi skulle kunne implementere systemet og gi brukeren en god brukeropplevelse. Store deler av implementeringen gikk ut på å prøve og teste ulike løsninger og se hvordan brukeropplevelsen ble. Det å prøve selv og se hva som skjer følte vi var minst like lærerikt som researchen som ble gjort på forhånd og underveis. Samtidig fikk vi god hjelp fra konsulentene til Atea, som var veldig hjelpvillige når vi hadde spørsmål eller satt fast.

4.5.2 Samarbeid

Som sagt så var mye av den innledende delen av prosjektet preget av mye arbeid fra hjemmekontor. For å holde samarbeidet oppe og passe på at vi jobbet uten misforståelse, satt vi i et møte i Teams fra hele arbeidsdagen mens vi jobbet. Dette gjorde at vi kunne diskutere hva som var målene for dagen og hva vi skulle jobbe med. Mye av arbeidet i starten bestod av å diskutere ulike retninger vi kunne gå i prosjektet og å ta valg for hvordan vi kunne løse oppgaven. Vi følte derfor at dette var den beste måten for å holde arbeidet i prosjektet i gang ettersom dette var perioden med mest usikkerhet, noe som gjorde det lite egnet for selvstendig arbeid.

Samarbeidet har i seg selv fungerte på en veldig god måte. Mye av dette kommer nok av at ambisjonsnivå og arbeidsnivået stort sett var sammenfallende. Vi har begge lagt oss på et nivå hvor vi ønsker å få det best mulige resultatet, samtidig ser vi begge et behov for muligheten til fleksibilitet i arbeidet. Vi hadde f.eks. enighet i at vi jobber mandag til fredag, og var med svært få unntak på kontoret lenger enn til klokken 17:00. Dette ga mye tid til frihet, både på kvelder og hverdager, noe som også åpnet for å jobbe selvstendig om man følte for det.

Som tidligere nevnt, har det vært mye diskusjon i det innledende arbeidet før implementasjonen, men det var nok minst like mye diskusjon under selve implementeringen av systemet. Det har oppstått mindre uenigheter, men aldri noe som har ført til noen nevneverdig konflikt. Samarbeidet har vært preget av mye dialog og det at vi har jobbet tett oppå hverandre. Dette har nok vært noe av grunnen til at vi har klart å jobbe så godt sammen som vi føler vi har.

4.5.3 Læringsutbytte

Dette har vært en oppgave som har krevd mye informasjonshenting og kompetansebygging av oss prosjektdeltakerne. Helt elementært føler vi at vi har fått mye utbytte av selve prosessen i å måte finne all informasjon selv, uten å ha en mal eller oppskrift å gå ut ifra. Dette har testet vår evne til å lære og stort sett vært det området som har måtte utvikle seg mest hos oss. Ettersom vi bare er en gruppe på to personer, har dette også krevd mer av begge deltakerne – gjennom studie er vi mest vant til gruppearbeid i grupper på 4-5 stykk. Mer spesifikt har dette ført til et sterkt behov for god kommunikasjon mellom prosjektdeltakerne, god utnytelse av tilgjengelige ressurser (kurs på nett, veiledere og konsulenter) og tiltro til egne beslutninger og evner. Spesielt det siste har vært en utfordring og kilde til usikkerhet, men kanskje vært det som har gjort at vi har vokst mest som personer.

Systemet er et rent Microsoft system. Det vil si alle tjenester, funksjoner, teknologier og lisenser tilhører Microsoft. Dette har åpenbart satt er behov for stor kompetansebygging på dette området, og det er også dette vi, prosjektdeltakerne, sitter mest igjen med. Mange av tjenestene (f.eks. Intune, Information Protection og Sentinel) kunne i seg selv vært sett på som et eget fagområde ettersom det ligger et hav av muligheter til å gå mye dypere i hver av tjenesten enn det det vi har gjort i denne oppgaven. Kompetansen vi har bygd på denne oppgaven er derfor i mye større grad en breddekompetanse, hvor vi har lært oss hvordan en kan bruke disse ulike teknologiene til å sette opp et fungerende system. Fordelen med denne kompetansen er at vi i stor grad føler vi klarer å se et mye større bilde av hvordan et slikt system fungerer i sin helhet. I begynnelsen leste vi oss mye opp på hver at tjenestene og begynte å forstå hva hver av disse gjorde, men det er først nå vi kan se hvordan alle disse fungerer sammen og hvorfor hver av deres roller er viktige i et fullstendig system.

For å konkretisere enda mer, ramser vi opp de mest sentrale punktene om læringsutbytte vi har tilegnet oss i dette prosjektet:

- Bruk av Microsoft 365 E5-lisensen i en bedrift.
- Bruk av Azure Information Protection til å ta vare på konfidensialiteten til data innad i en bedrift.
- Bruk av Microsoft Intune og Autopilot til enhets- og applikasjonsadministrasjon.
- Sikring av et system med bruk av Azure Sentinel og Microsoft Defender for endpoint og Office.
- Oppsett av et system med fokus på både sikkerhet, personvern og brukervennlighet.

4.6 Veien videre

Utvikling og drift av IT-systemer er en kontinuerlig prosess og jobben vi har gjort i dette prosjektet representerer bare de første fasene i denne prosessen. Vi har designet et system som skal settes i drift og stoppet der. Videre arbeid må fokusere på utbedring av sikkerhet og brukervennlighet etter en periode med bruk. Tilbakemelding fra brukerne av systemet vil være viktig i prosessen og kontinuerlig testing av systemet er en forutsetning for forbedring.

Det er flere aspekter ved teknologien som er brukt i prosjektet som ikke er utforsket. Både Information Protection, Intune og Defender for endpoint/Office har utrolig mye dybde og man kunne skrevet en bachelor oppgave på hver av dem.

Til videre arbeid vil vi anbefale å få så mye tilbakemeldinger fra de ansatte som mulig. Det er disse som kommer til å bruke systemet fra dag til dag, det blir derfor viktig å høre på disse for å så gjøre endringer som kan gjøre systemet enda mer brukervennlig. Det er også muligheter til å spesifisere policyer og rette de mer mot enkelte grupper mennesker. De fleste av policyene som er lagd i denne implementeringer er generelle policyer som skal gjelde alle som bruker systemet. Det kan derimot være at det er noen ansatte som trenger flere tillatelser eller enheter hvor sikkerhet blir ekstra viktig. Det kan derfor være lurt å se på muligheten til å lage egne policyer – f.eks. strengere passordpolicy - til disse gruppene.

Azure Sentinel er en teknologi som en kan dykke mye dypere i enn det vi har gjort i denne oppgaven. Det å fortsette å utvikle egnendefinerte trusselhåndteringer vil være veldig fordelaktig for bedriften. Dette vil på lengre sikt avlaste de ansvarlige for IT-sikkerhet og gjøre at hendelser kan håndteres mye raskere og sørge for bedre sikkerhet totalt sett. Skulle bedriften få tilgang til auto-labling-funksjonen til Information Protection, vil dette også være anbefalt sterkt å implementere for å gjøre dokumenthåndteringen automatisert til mye større grad.

4.7 Konklusjon

Denne bacheloroppgaven hadde et stort omfang. Sikkerhet og GDPR er to brede områder innenfor IT og Microsoft har mange løsninger som man kan dykke dypt ned i. Til tross for dette sitter vi igjen med et fungerende system som vi mener svarer på oppgaven på en tilfredsstillende måte. En stor del av oppgaven var selve læringsprosessen og hvordan vi har måtte tilegne oss kunnskap. Gjennom hele prosessen har vi blitt utfordret på det vi kan og ikke kan. Vi har måttet tilegne oss kunnskap om mange forskjellige teknologier og knytte disse sammen til et fungerende system som er brukervennlig og sikkert.

Systemet vi står igjen med nå er ikke det samme systemet som ble beskrevet i designrapporten. En bratt læringskurve og mye kompetansebygging har gjort at vi føler det vi står igjen med svarer mye bedre på oppgaven enn det systemet vi først så for oss. Dette gjelder spesielt hvordan denne løsningen svarer på oppgavens krav til sikkerhet og brukervennlighet. Bare dette i seg selv mener vi viser til hvilken utvikling vi selv har hatt underveis og hvordan vi nå står igjen med mye mer erfaring og kunnskap enn det vi startet med.

Til tross for noen mangler grunnet tekniske begrensninger, samt endringer i design, mener vi at vi har løst oppgaven på en god måte og sitter igjen med et system vi er fornøyde med.

Kevin Nordnes, Matias Skjetne

M365 Compliance and Security

NTNU
Kunnskap for en bedre verden