Bendik Gjøvikli og Dat-Danny Pham

Migrering til Azure

Migrering til Azure med hovedfokus på Co-Management

Bacheloroppgave i Informatikk, Drift av Datasystemer
Veileder: Stein Meisingseth og Lars Kristian Granlund
Mai 2019

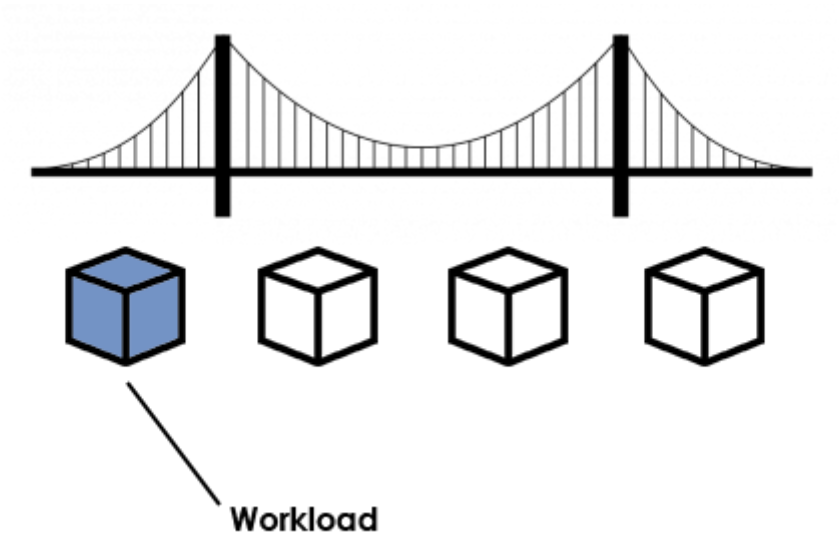
Bacheloroppgave

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

NTNU
Kunnskap for en bedre verden

Innholdsfortegnelse

«Migrering til Azure»



Forstudierapport

Bendik Gjøvikli og Dat-Danny Pham

Trondheim, 20.05.2019

Innholdsfortegnelse

Figurliste

Forkortelser og definisjoner

Forkortelse	Navn	Definisjon
AD	Active Directory	System for administrering av brukere, grupper, maskiner og mer.
AAD	Azure Active Directory	Tilsvarende system som Active Directory, men som finnes i Azure.
	Azure AD Connect	Prosess som utføres for å knytte lokal AD sammen med Azure AD.
	Co-Management	Trinnvis metode for migrering av jobber fra SCCM til Intune.
CM	Configuration Manager	Forkortelse for System Center Configuration Manager.
	Device Compliance Policy	Krav som settes til enheter for at de skal ha tilgang til ressurser i nettverket.
	Device Configuration Policy	Restriksjoner og mer som kan settes på enheter.
	Device enrollment	Innrulling av en enhet til domenet.
	Intune	Et verktøy for å administrere og drifte enheter i et nettverk, uavhengig om hvor enheter befinner seg.
	Windows Autopilot	Tar for seg OS-utrulling same klargjøring av maskiner, slik at de kan benyttes som bedriftsmaskiner.
	Hybrid Azure AD	En tilstand hvor lokal AD og Azure AD jobber sammen.
	Hyper-V	Verktøy for viirtualisering.
	On-premise	Systemer som er knyttet til bedriftens private nettverk.
	Powershell	Et verktøy for scripting.
	Sharepoint	Office programvare for samhandling og samling av dokumenter.

SCCM	System Center Configuration Manager	Et administreringsverktøy for å drifte maskiner, brukt for deployment av OS, Programvare, oppdateringer, monitorering og rapportering av hendelser
	Tenant/Azure tenant	Et område i Azure.
	Windows Update Policies	Retningslinjer som settes for oppdatering av enheter.

Tabell 1: Forkortelser og definisjoner

Revisjonshistorie

Dato	Versjon	Beskrivelse	Forfatter
10.01.19	0.1	Første utkast	Bendik Gjøvikli, Dat-Danny Pham
14.03.19	0.2	Gjorde endringer etter forslag fra referansegruppen	Bendik Gjøvikli, Dat-Danny Pham
05.05.19	1	Endelig versjon	Bendik Gjøvikli, Dat-Danny Pham

Tabell 2: Revisjonshistorie

Introduksjon

Hensikten med dokumentet er å sette rammeverket for det videre arbeidet med å få Alarmnett AS opp i skyen. Dokumentet skal være til hjelp slik at man har konkrete mål og krav, som vil gi en felles forståelse og enighet om resultatet som skal foreligge for både Alarmnett AS og prosjektgruppen.

Dokumentet beskriver bakgrunnen for prosjektet, hvor vi går inn på problemer og behov, samt kort om dagens systemer hos Alarmnett AS. Videre skal vi ta for oss prosjektmål, hvor vi ser på resultatmål, prosessmål, prosjektets omfang, og til slutt milepæler og de forskjellige hovedaktivitetene. Vi vil også foreta oss en interessentanalyse, og kartlegge rammebetingelser. Dokumentet vil også være til hjelp ved kartlegging av kritiske faktorer som man må ta stilling til, samt analyser av risikoelementer. Deretter vil vi ta for oss en kost/nytte-analyse, hvor vi setter tall på kostnader og diverse. Vi vil også ta for oss retningslinjer og standarder, hvor krav til dokumentasjon, kvalitetsgjennomganger, standarder og metoder vil beskrives. Til slutt dokumenteres prosjektorganisering og anbefalinger for videre arbeid.

Ved å legge inn et godt arbeid i forstudierapporten, vil vi kunne øke sjansene for et effektivt arbeid og ha tiltak klare dersom problemer skulle oppstå.

Bakgrunn for prosjektet

Vi lever i en verden hvor IT-systemer utvikler seg veldig raskt og endringer skjer hele tiden. Dette gjør at et behov for kunnskap om migrering av on-premise løsninger opp til skyen er meget relevant. I den sammenheng skal vi se på hvordan migrering av lokal AD, SCCM og andre systemer, kan gjennomføres ved å ta i bruk Co-Management. Prosjektet vil derfor være til nytte slik at vi i prosjektgruppen tilegner oss kunnskap om denne typen arbeid, samtidig som vi oppnår målet til Alarmnett AS, om å få migrert enkelte systemer opp i skyen.

Beskrivelse av problemer og behov

Alarmnett AS, har per i dag 40 ansatte, hvor noen jobber mye på kontorene mens andre jobber både av og på lokalene. Dette gjør at det har oppstått et behov hos de ansatte om å få tilgang til bedriftens resurser både i og utenfor kontorområdet. Dette gjør at vi må få på plass en løsning som tilfredsstiller de ansatte, slik at vi kan legge til rette for administrasjon av deres IT-systemer, selv om de befinner seg utenfor bedriftens lokaler.

Per i dag legges det ikke til rette for mobile enheter, og for å hente resurser eller vaktlister må de ansatte som jobber ute av kontoret få en ansatt på kontoret til å laste ned og sende filen over Facebook eller e-post. Det er derfor et behov for å få tilgang til bedriftens resurser fra mobile enheter, da dagens rutiner ikke har veldig høy sikkerhet og krever minst to personer for å utføres.

Behovet for å administrere mobile enheter har blitt større de siste 10 årene. Vi skal derfor se på hvordan Intune kan ta over arbeidet med enkelte oppgaver som tidligere har vært løst med SCCM og on-premise løsninger. Slik at Alarmnett AS, får mulighet til å administrere disse enhetene. Vi ønsker derfor å løse oppgaven gjennom denne problemstillingen:

«På hvilken måte kan kombinasjonen SCCM og Intune konkurrere mot en ren on-premise/skybasert løsning, når det gjelder å løse drifts-oppgaver innen deployment med tanke på tilgjengelighet, kompatibilitet og sikkerhet»

Kort om dagens systemer og rutiner

Systemet per i dag består av lokal AD og SCCM, som administrer de enhetene som har tilgang til bedriftens private nettverk. Ansatte som jobber utenfor bedriften bruker andre private og offentlige nett, som kan føre til sikkerhetsbrudd.

Brukerne av systemet er mer eller mindre todelt mellom de som er på kontoret og de som jobber utenfor kontoret. I tillegg har vi IT-avdelingen som trenger tilgang til litt kraftigere maskiner for å kunne utføre jobben sin.

Kontoransatte har per dags dato tilgang til enkeltprogrammene til Office på sin lokale maskin, som Word, Excel, PowerPoint og lignende, men det er kun snakk om engangskjøp. I tillegg er det bare opprettet fellesmapper i AD slik at de ansatte kan legge dokumenter de arbeider på når de jobber på samme prosjekt. Det er ikke lagt til rette for at de kan jobbe på dokumentene samtidig, og må dermed vente på hverandre når de skal skrive i samme dokument. De ansatte benytter seg av personlig mail-adresse også for jobbrelatert post.

Prosjektmål

Formålet med prosjektet er å flytte deler av dagens systemer til et tilsvarende system i skyen. Denne endringen skal i tillegg ikke skape for store endringer i hvordan de ansatte arbeider, slik at Alarmnett AS, ikke taper arbeidstid mens migreringen til skyen pågår. Med dette menes både nedetid i tilgangen til serveren og eventuell opplæring for å benytte det nye systemet. Optimalt sett ønsker vi at det bare oppleves som en endring i utseendet til arbeidsområdet fra de ansattes perspektiv. På den måten vil det ikke være behov for intensiv opplæring og Alarmnett AS, vil få muligheten til å dra nytte av funksjonene og godene som kommer med skyløsningen.

Mer spesifikt skal vi:

- Muliggjøre drift ved bruk av Azure for nye og gamle enheter
    - Migrere over brukere til Azure Active Directory.
    - Utføre Azure AD Connect, slik at vi oppnår et samspill mellom lokal AD og Azure AD (Hybrid Azure AD).
    - Trinnvis migrere over enkelte funksjoner fra SCCM 2016 til Intune ved bruk av Co-Management.
    - Ta i bruk funksjoner i Intune
        - Applikasjonsutrulling
        - Device Compliance policy
        - Device Configuration Policy
        - Device enrollment
            - Windows og Android
        - Windows Autopilot
            - OS-utrulling
            - Klargjøring av nye maskiner og gamle maskiner
        - Windows Update Policies
    - Drifte Intune med Powershell

Effektmål

Gjennom prosjektet ønsker vi å opprette et system som føles behagelig å bruke uten at det vil gå utover sikkerheten. Vi ønsker å øke sikkerhet og tilgjengelighet med tanke på mulighet for administrasjon av mobile-enheter. Få muligheten til å enkelt kunne skalere servere og annen infrastruktur. Gi drifts-ansvarlig bedre oversikt ved å avlaste arbeidsmengden. Mer detaljert ønsker vi å:

Effektmål
Legge til rette for muligheten om å migrere til en ren skyløsning, om det ønskes i fremtiden.
Effektivisere arbeid med 20%.
Minske nedetiden til serveren til mindre enn 1 time hvert år.
Oppnå økt produktivitet og samarbeid mellom de ansatte.
Gjøre hverdagen for ansatte som jobber utenfor bedriftens kontorer enklere (tilgjengelighet og mobilitet).

Tabell 3: Effektmål

Resultatmål

Ved endt prosjekt skal vi ha tilegnet oss kunnskap om migrering av on-premise løsninger til alternative løsninger i skyen, ved bruk av Co-Management metoden. Alarmnett AS, skal få et system som er tilrettelagt dagens standarder og som skal legge grunnlaget for en videre fremtid i skyen. Vi skal vise til et system hvor migreringsprosesser og opprettelse av skybaserte løsninger har blitt gjennomført, samt dokumentasjon av prosjektet.

Hva	Tid/fremdrift
Oppsett av on-premise systemer (AD, SCCM).	Innen 2 uker etter påbegynt arbeid.
Ta i bruk Azure AD Connect, samt oppsett av Hybrid Azure AD.	Innen 1 uke etter påbegynt arbeid.
Oppsett og testing av Co-management.	Ukjent
Oppsett og testing av funksjoner i Intune.	Ukjent
Lage et script for å kunne utføre oppgaver med Intune.	Innen 2 uker etter påbegynt arbeid.
God og forståelig dokumentasjon.	Underveis i prosjektet.

Tabell 4: Resultatmål

Prosessmål

Fra prosjektet vil vi tilegne oss erfaring i å samarbeide og samarbeidsrelatert arbeid. Vi ønsker også å tilegne oss nok kunnskap til å migrere workloads fra Configuration Manager opp mot skyen, for eventuelle fremtidige kunder. Videre ønsker vi å tilegne oss god kunnskap innen Intune, Azure AD og administrasjon av Intune gjennom Powershell. Vi vil møte opp til avtalte tider, slik at vi fullfører prosjektet til angitt tid. Vi forventer at alle deltakere gjør en god innsats i prosjektarbeidet.

Prosjektets omfang

Hovedmålene for prosjektet har blitt nevnt under punktet "Prosjektmål". Under dette punktet vil vi beskrive prosjektet omfang, ved å avgrense prosjektet ytterligere som et supplement til prosjektmålene. Vi vil gjøre dette ved å presisere hva prosjektet ikke skal gjøre:

Prosjektet skal ikke:

- Oppgradere eller håndtere det alarmsystemet som allerede er på plass hos bedriften.
- Endre på nettverkskablene i lokalene, som å legge til nye aksess punkter.
- Endre på lokal AD og Configuration Manager, utenom nødvendig konfigurasjon for å legge til rette for Azure AD Connect og Co-Management.
- Stille opp med lisenser, utenom de til Azure AD, Intune og programmene relatert til disse.
- Fysisk serverrelatert arbeid som å reparere skadet hardware.
- Løse dataproblemer for de ansatte som ikke er relatert til migreringen.
- Vi stiller ikke med opplæring av de nye systemene, bortsett fra dokumentasjon av arbeidet vi har utført.

Prosjektets milepæler og hovedaktiviteter

Prosjektets milepæler presenteres i vedlegg "Plan" (MS-Project dokumentet). Her listes prosjektets hovedaktiviteter og de mindre aktivitetene som inngår i hver hovedaktivitet. Oversikten viser også ressursdisponering for samtlige milepæler, og hvilke aktiviteter som avhenger av hverandre, samt hvem som er ansvarlig for hver aktivitet. Dokumentet vil komme til nytte når det gjelder disponering av ressurser og for å holde en oversikt over progresjonen, slik at vi ikke faller bak skjema.

Se vedlegg: «GANT-Diagram»

Interessenter og rammebetingelser

Interessentanalyse

Interessenter	Suksesskriterier	Bidrag til prosjektet
Ekstern (kunde):		
Oppdragsgiver	En ny og mer effektiv løsning, som kan føre til bedre inntjening	Beslutninger
IT-ansvarlig/drift-personell	Avlastning av arbeidsmengde og mer automatisering	Opplysning av problemområder
Administrasjon og ledelse	Tilgjengelighet	Ønsker og oppfølging
Økonomiansvarlig	Bedre metoder for dokumentering og kommunikasjon	Ønsker og oppfølging
Kontoransatte	Bedre metoder for dokumentering og kommunikasjon	Ønsker og oppfølging
Salgsmedarbeidere	Bedre metoder for dokumentering og kommunikasjon	Ønsker og oppfølging
Montør/servicearbeidere	Bedre tilgjengelighet. Forenkle prosessen med oppsett av nye maskiner og andre enheter.	Ønsker og oppfølging
Internt (leverandør)		
Prosjektgruppe	Innføre og dokumentere et system som opprettholder kravene vi, veiledere og Alarmnett AS, har satt for prosjektet	Ansvar
Veileder	Et godt gjennomført prosjekt som tilfredsstiller veileders krav.	Veiledning

Tabell 5: Interessentanalyse

Rammebetingelser

- Prosjektet starter 07.01.2019 og skal senest ferdigstilles 20.05.2019.
- Prosjektet skal ikke overgå 500 timer arbeidstid per prosjektdeltager ± 5%. (475-525 timer).
- Prosjektet skal ikke overgå kostnadsrammene som NTNU IDI stiller med, i forhold til utstyr og diverse som skal brukes under prosjektet.
- Prosjektet må godkjennes av Alarmnett AS, etter både planlegging og innføring av nye systemer.

Kritiske suksessfaktorer

Suksessfaktorer

Suksessfaktor	Beskrivelse
Et godt forarbeid og videre god kommunikasjon med kunden	Gjennom et godt forarbeid vil vi kartlegge kundens behov, oppfylle ønsker og legge til rette for systemer som de vil trenge. Ved å vedlikeholde god kommunikasjon gjennom prosjektet, vil vi kunne forbedre og tilpasse systemene ytterligere, etter hvert som nye innspill og behov avdekkes.
Innføring av nye systemer skal ikke sette den daglige driften ute av spill	Ved innføring av de nye systemene er det viktig at dette gjøres på slik måte at det ikke går ut over den daglige driften. Dette kan føre til store kostnader for Alarmnett AS. Vi må derfor unngå å jobbe med systemer som kan ha innvirkning på den daglige driften i arbeidstiden til Alarmnett AS.
Det må opplæres eller ansettes IT-ansvarlig med god nok forståelse for skyorienterte løsninger	Etter oppsett og migrering av workloads er det viktig at IT-ansvarlig forstår hva som er gjort og hva som endrer seg i forhold til deres arbeidshverdag. Det er særdeles viktig at sikkerhetsrutiner opprettholdes og dermed må IT-ansvarlige ha god innsikt i systemet.
Innfri rammebetingelser	Viktig at rammebetingelsene innfris, slik at det ikke medfører uønskede kostnader, eller andre uønskede hendelser.
Godt samarbeid og arbeidsvilje i prosjektgruppen	Det er et stort prosjekt som skal jobbes med over lang tid, som forutsetter at et godt samarbeid fra start til slutt opprettholdes. Viktig å vise god arbeidsvilje, slik at det smitter over til de andre prosjektdeltakerne, samtidig som at arbeidet fordeles og blir

	gjennomført av samtlige deltagere og ikke enkelte i prosjektgruppen.
God dokumentasjon	Det skal dannes gode vaner for dokumentasjon og dokumentering gjennom hele prosjektet. I tillegg skal det dokumenteres på en forståelig og ensformig måte slik at leseren skal lett forstå hva som menes.
Ikke overgå budsjettet	For å ikke skape uønskede utgifter ønskes det at vi holder oss innenfor de rammene som er gitt. Dette kan for eksempel være riktig antall lisenser.
Minimalt med arbeid-/sykefravær	For å sikre at prosjektet gjennomføres og kravene oppnås innen den avsatte tiden, gjelder det å holde fraværet minimalt.

Tabell 6: Suksessfaktorer

Informasjonsbehov

Til dette prosjektet benytter vi oss av en felles SharePoint for å dele dokumenter samt versjonshåndtering. Her vil det bli satt opp en MS Project med gant-diagram, med tidsfrister og milepæler som skal innfris gjennom hele prosjektet. Det er vesentlig for et vellykket prosjekt at både prosjektgruppen og Alarmnett AS, har en felles forståelse og enighet om hvordan det endelige produktet skal se ut. Derfor er det viktig at det føres en god dialog mellom partene, og at partene melder ifra om endringer som må gjennomføres. Viktige ting som må avklares på forhånd er for eksempel antall lisenser, hva vi skal kjøpe inn lisenser til, domenenavn, oversikt over brukere og eventuelt andre protokoller som bedriften ser på som viktige.

Underveis i prosjektet er det viktig at vi formidler informasjon om hvor langt i prosessen vi har kommet, for vår egen del, men også slik at Alarmnett AS, kan se fremgangen i prosjektet, og gjøre seg klar dersom endringer som kan påvirke den daglige driften inntreffer når man muligens kommer til et kritisk punkt i prosessen.

Risikoanalyse

Under risikoanalysen vil vi ta for oss problemer som kan oppstå under prosjektet. Her vil vi prøve å forutse problemene, se på sannsynlighet og konsekvens, samt planlegge tiltak slik at risikoen reduseres. Det er viktig at risikoanalysen er fyldig og tar for seg de mest sannsynlige hendelsene, som har stor betydning for prosjektets gjennomførelse. Vi velger å se bort ifra hendelser som kan løses med sunn fornuft.

Se vedlegg: «Risikoanalyse».

Kost/nytte-analyse

Kvantifiserbar og ikke-kvantifiserbar nytte

Kvantifiserbar nytte

Ved innføring av de nye systemene som er med på å øke tilgjengelighet, muliggjøre for samhandling, kalenderfunksjoner og kommunikasjon, redusere arbeid med å konfigurere og tilpasse maskiner til ansatte og mer, ser vi for oss at vi kan effektivisere arbeidet med 20% som nevnt i effektmålene. Vi ser også for oss at vi kan redusere nedetiden på servere til mindre enn 1 time hvert år, som er relativt lite i forhold til alle problemene som kan oppstå med et eget on-premise system.

Hvis vi tar utgangspunkt i effektivisering av arbeidet med 20%, vil dette bety at de ansatte får gjort mer arbeid i løpet av en dag. Hvis vi tenker at dette arbeidet vanligvis resulterer i at de ansatte kaster bort dyrbar tid, kan vi se på hvor mye kan man spare i året dersom dette hadde vært unngått.

Vi antar at de ansatte i gjennomsnitt har en timelønn på 170 kr. De er 40 ansatte som jobber i snitt 37 timer i uka og vi inkluderer ferielønn, vil de måtte jobbe 50 uker hver i året.

$$Timeslønn * antall\ timer\ i\ uka * antall\ uker * antall\ ansatte * arbeidsgiveravgift$$

$$= Totale\ lønnsutgifter\ per\ \text{år}$$

$$170\ kr * 37\ timer * 50\ uker * 40\ ansatte * 14{,}1\%\ arbeidsgiveravgift$$

$$= 12.757.378\ kr$$

20% av 37 timer, tilsvarer 7,4 timer. Dette er i gjennomsnitt 1 time hver dag som kunne blitt brukt til andre jobbrelaterte oppgaver som kunne ha gitt fortjeneste til bedriften. I året tilsvarer denne tiden totalt 2.551.475,6 kr i lønnsutgifter.

$$12.757.378\ kr * 20\% = 2.551.475{,}6\ kr$$

Ikke-kvantifiserbar nytte

Gjennom å innføre et felles system som skal gjelde for samtlige ansatte, vil vi kunne redusere frustrasjon og andre psykiske problemer som kunne oppstå. Til nå har de ansatte ikke hatt noen reell struktur i valg av hvilke programmer og systemer de skal ha tilgang til, som har gjort at det har vært vanskelig og frustrerende å jobbe sammen. Ved innføringen av vårt nye system vil vi definitivt kunne redusere dette problemet. Å skulle sette en kroneverdi på en slik nytte er ikke så lett, men det kan være lurt å ha det i bakhodet når man senere skal bestemme seg for om man skal gå videre med arbeidet eller ikke.

Bortfall av direkte kostnader

Alarmnett AS har allerede et on-premise system, med lokal AD og CM. Dette systemet skal de å fortsette med, men når det gjelder programvare vil de få vekk det systemet de bruker i dag og innføre et nytt og mer komplett system som skal dekke alle programvarebehov. Dette betyr at vi vil få bortfall av enkelte direkte kostnader. Det er da snakk om lisenser som de betaler for når det gjelder for eksempel Office programvare.

Estimerte kostnader

Programvare kostnader

Microsoft 365 Business – Kombinerer funksjoner fra flere Microsoft-produkter, en løsning som passer for små og mellomstore bedrifter. Office 365 pakken og Windows 10 er grunnlaget i Microsoft 365 pakken, men den tilbyr også funksjoner for enhetsadministrasjon (Windows autopilot etc.) og andre sikkerhetsaspekter. Under selve prosjektet vil vi benytte oss av andre tilsvarende lisenser som vi har tilgjengelig, men i realiteten ville vi tatt i bruk Microsoft 365 Business.

Pakken koster kroner 162,30 bruker/måned (sett bort i fra volumrabatter), og med 40 ansatte vil regnestykket se slik ut:

$$162{,}30\,\frac{kroner}{måned} * 40\ ansatte = 6.492\ kroner\ i\ måneden$$

$$6.492\,\frac{kroner}{måned} * 12\ måneder = 77.904\ kroner\ i\ året$$

Drift og forvaltningskostnader

Følgende kostnader er årlige kostnader:

Microsoft 365 Business lisenser: 77.904 kroner i året.

Totale lisenskostnader per år: 77.904 kroner

Utviklingskostnader

Følgende kostnader vil kun gjelde i første år, da det er snakk om kostnader i forhold til å betale prosjektgruppa under planlegning-, innføring- og oppfølgingsfasen.

Det er snakk om 500 timer per deltager, altså 1000 timer totalt. Prosjektstart er 7. januar 2019 og prosjektet skal avsluttes 1. mai 2019. Vi fakturerer 600 kroner i timelønn per deltaker.

$$1000\ timer * 600\,\frac{kroner}{time} = 600.000\ kroner$$

Sammenstilling kost/nytte

	År 1	År 2	År 3	År 4	År 5	SUM
Kvantifiserbare nytte	-	2,551,475.60	2,551,475.60	2,551,475.60	2,551,475.60	10,205,902.40
Bortfall kostnader	-	-	-	-	-	
Sum nytte	-	2,551,475.60	2,551,475.60	2,551,475.60	2,551,475.60	10,205,902.40
Utviklingskostnader	600,000.00	-	-	-	-	
Drifts og forv. Kostnader	-	77,904.00	77,904.00	77,904.00	77,904.00	311,616.00
Sum kostnader	600,000.00	77,904.00	77,904.00	77,904.00	77,904.00	911,616.00
Beregnet nytte (nytte - kostnader)	- 600,000.00	2,473,571.60	2,473,571.60	2,473,571.60	2,473,571.60	9,294,286.40

Figur 1: Sammenstilling kost/nytte

Ikke kvantifiserbar nytte

Ved å benytte seg av Office-pakken, vil gi de ansatte mulighet for bedret samskriving, som igjen vil føre til minsket frustrasjon ved samarbeid og versjonshåndtering relatert til dokumentasjon. Ved å gjøre det lettere å samarbeide vil de ansatte slippe å stoppe opp arbeidet for å se om noen andre jobber i samme dokument som en selv. I tillegg fører dette til mindre stress blant ansatte som igjen fører til mer effektivt arbeid.

Det har seg slik at kontoransatte generelt har gjort seg kjent med programmene i Office-pakken, så det nye systemet ikke vil kreve en altfor tung opplæring av de ansatte. Dette igjen vil gjøre at de ansatte ikke vil føle at de får for mye "hjemmelekser", mens de ansatte som ikke kan Office vil få en god innføring i å bruke Office-pakken. Ved å få tilgang til bedriftens ressurser mens man er ute av kontoret, vil gjøre arbeidet både lettere og mer komfortabelt for de ansatte som ikke er mye på kontoret. Det oppleves per dags dato mye stress rundt det å spørre om filer og å sende eller hente filer mens man er ute av kontoret, da minst to personer vil bli involvert og den ene på kontoret da må stoppe sitt arbeid for å hjelpe til. Dette vil da bortfalle ved at den ansatte som er ute av kontoret vil kunne hente og legge ifra seg filer så lenge de er koblet til internett.

Det vil også være mye lettere å få kontakt med personer utenfor kontoret slik at de også kan kort delta på møter når det trengs, da tenker vi på tekniske innspill, før de drar til neste kunde. Dette vil gjøre at de slipper å sette av dagen til å måtte dra inn til kontoret om de ikke ønsker det. For IT-ansatte vil innføringen av Intune gi mulighet for bedre oversikt og kontroll om noe skulle skje på deres lokaler, når det gjelder mobile enheter. De vil få muligheten til å faktisk gjøre noe om nettverket blir utsatt for et angrep gjennom en av de ansattes mobile enheter. Vi regner med at dette vil gi mindre stress når de nå kan sette opp mottiltak.

Retningslinjer og standarder

Krav til dokumentasjon

Nedenfor listes dokumentene som skal være med når prosjektet ferdigstilles.

Forstudierapport: 28.01.2019

- Dokument med vedlegg av risikoanalyse og Gantt-Diagram (plan over milepæler og hovedaktiviteter)
- Dokumentet skal godkjennes av Prosjektgruppen før 28.01.2019.

Designrapport: 12.02.2019

- Dokumentet viser til skisser og skriftlig dokumentasjon om hvordan de ulike systemene skal se ut og hvordan de fungerer sammen.
- Dokumentet skal godkjennes av Prosjektgruppen før 12.02.2019.

Driftsrapport: 26.04.2019

- Dokumentet inneholder dokumentasjon som beskriver hvert enkelt system som prosjektgruppen skal innføre hos Alarmnett AS.
- Dokumentet skal godkjennes av Prosjektgruppen før 26.04.2019.

Sluttrapport: 03.05.2019

- Et dokument som er med på å avslutte prosjektet. Rapporten skal gi en oppsummering og oversikt over prosjektet.
- Dokumentet skal godkjennes av Prosjektgruppen før 03.05.2019.

Samarbeidsrapport: 10.05.2019

- Et dokument som skal være med for å evaluere samarbeidet i prosjektet.
- Dokumentet skal godkjennes av Prosjektgruppen før 10.05.2019.

Krav til kvalitetsgjennomganger

For å sikre at systemene som skal innføres holder standarden og innfrir alle brukerkrav vil vi utføre pilottester. Ved slike tester vil velge ut enkelte fra bedriften som får være med på å teste de nye systemene før de innføres i bedriften og alle ansatte blir berørt av endringene. Her vil vi prøve å avdekke eventuelle problemer med systemene, før en endelig innføring. Ved å ha god kommunikasjon med testerne kan vi rette opp i eventuelle problemer som de gir tilbakemelding om. I prosjektet vil dette gjennomføres ved at vi kjører tester på enkelte brukere som vi har opprettet før vi kjører ut endringer til samtlige brukere.

Krav til standarder og metoder

Overordnet vil vi benytte oss av standard for gjennomføring av prosjekt med tanke på dokumentasjon som skal foreligge etter endt prosjekt. I den sammenheng kan vi referere til punkt "Krav til dokumentasjon" i forstudierapporten, som beskriver de forskjellige dokumentene.

For å enkelt kunne jobbe sammen på dokumenter og med tanke på deling av ressurser, maler, innkalling til møter, kalenderfunksjoner og diverse, bruker vi Sharepoint. Vi har opprettet vår egen Sharepoint hvor alt relatert til prosjektet ligger. Sammen med Office 365, vil samhandling med tanke på samskriving, kvalitetssikring og annen veiledning forenkles.

I og med at ikke alle som er involvert i prosjektet befinner seg under samme tak vil vi benytte Skype for Business til å holde møter, med mindre vi avtaler fysiske møter.

Som nevnt tidligere er dette et forskningsprosjekt som betyr at vi ikke skal implementere denne løsningen i virkeligheten. For å kunne simulere en implementasjon på en best mulig måte, vil vi derfor ta i bruk verktøy for virtualisering, slik at vi får satt opp et testmiljø. Her kan vi benytte oss av Hyper-V for virtualisering av lokal Active Directory og System Center Configuration Manager, samtidig som vi tar i bruk egen Azure tenant for å simulere et reelt Azure miljø.

Endringshåndtering

Dersom ønske om endringer eller nye behov avdekkes etter at dette dokumentet "ferdigstilles", vil vi ta i bruk fremgangsmåten listet nedenfor, for å håndtere endringsønsker:

1. Dokumentere endringenes innhold
2. Analysere konsekvensene for prosjektet
3. Beregne eventuelle kostnader/nytte
4. Godkjennelse og aksept
5. Logge endringer
6. Justere planene
7. Informere interessentene
8. Gjennomføre endringene

Prosjektorganisering

Vi vil nå gå inn på de forskjellige rollene i prosjektet, hvem som er involvert og hva de forskjellige rollene innebærer. Vi vil også se på arbeidsfordelingen og hvordan vi løser dette på en god måte.

Rolle	Rolleinnehaver	Info
Prosjektledere	Bendik Gjøvikli og Dat-Danny Pham	Vi velger å ikke utnevne noen enkelt prosjektleder. Da vi kun er to personer i prosjektet, er det veldig enkelt å lede arbeidet oss imellom kontra hvis vi hadde vært en større gruppe.
Oppdragsgiver	Alarmnett AS	I og med at vi har laget oss et Case for dette forskningsprosjektet, vil oppdragsgiver være Alarmnett AS.
Kvalitetskontroll	Veiledere (Stein Meisingseth og Lars Kristian Granlund)	Stein Meisingseth og Lars Kristian Granlund vil fungere som veiledere, og ser derfor til at kvaliteten på arbeidet holder mål.
Arbeidsfordeling	Bendik Gjøvikli og Dat-Danny Pham	Vi har til enhver tid oversikt over hvilke deler av prosjektet som må ferdigstilles innen en tid. Vi velger å ikke tildele spesifikke oppgaver til hver enkelt prosjektdeltaker, men tar på oss ansvaret når det føles naturlig, med tanke på deltakers kompetanse, ekspertise og evne. Ved flere oppgaver vil vi måtte jobbe sammen, for å sikre god gjennomførelse, samtidig som vi begge opparbeider oss kompetanse på området.

Tabell 7: Prosjektorganisering

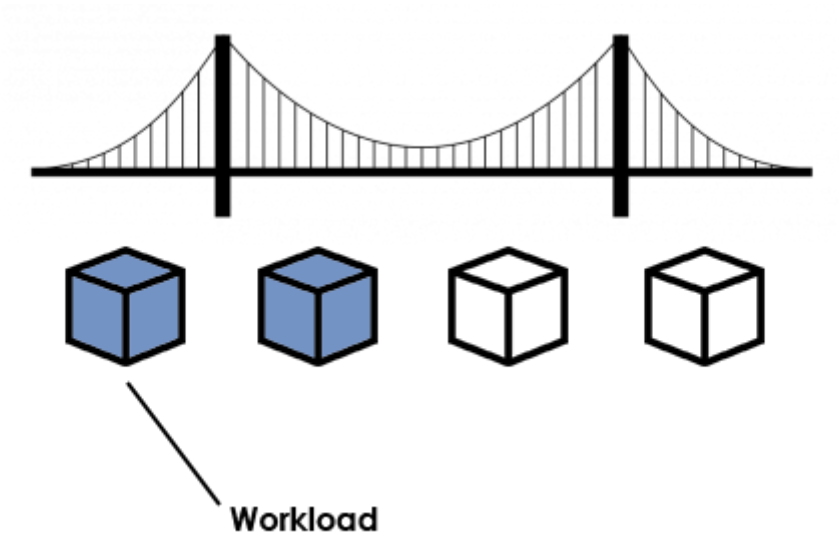
Anbefalinger for videre arbeid

Hvis våre estimater i forhold til økning i effektivisering stemmer, viser til resultatet for kost/nytte analysen av Alarmnett AS, kan spare i overkant av 9 millioner kroner i løpet av de neste 5 årene. Det skal sies at vi ser bort i fra eventuell nytte i form av nedetid på servere, samt ikke-kvalifiserbar nytte, da dette kommer utenom. Det nye systemet er tilpasset for fremtidige endringer, hvor det muligens kan være flere kroner å spare. Prosjektgruppen anbefaler videre at Alarmnett AS fortsetter prosjektet med innføring av nye IT-systemer.

Vedlegg

1. «GANT-Diagram» - Oversikt over planlagt tid til de forskjellige delene i prosjektet.
2. «Risikoanalyse» - Dokument for risikoanalyse.

«Migrering til Azure»



Designrapport

Bendik Gjøvikli og Dat-Danny Pham

Trondheim, 20.05.2019

Innholdsfortegnelse

Figurliste

Forkortelser og definisjonsliste

Forkortelse	Navn	Forklaring
AD/ADDC/DC	Active Directory / Active Directory Domain Controller	System for administrering av brukere, grupper, maskiner og autentisering.
	Azure	Azure er Microsoft sin skyplatform og infrastruktur.
AAD	Azure Active Directory	Tilsvarende system som Active Directory, men som finnes i Azure.
AADC	Azure AD Connect	Prosess som utføres for å knytte lokal AD sammen med Azure AD.
	Azure AD registered devices	Type join i Azure AD
	Azure AD joined devices	Type join i Azure AD
BYOD	Bring your own device	Ansatta benytter sine egne enheter i arbeid.
	Client apps	Type workload, samt et verktøy for utrulling av applikasjoner.
	CMTrace	Rapporterings verktøy
	Co-Management	Trinnvis metode for migrering av jobber fra SCCM til Intune.
	Company Branding	Tilpasser utseende på innlogging og mer.
	Company Portal	Applikasjonskatalog som brukes av Intune
	Compliance Policy	Krav som settes til enheter for at de skal ha tilgang til ressurser i nettverket.

	Compliant (Her i i forhold til devices i Intune)	Kompatibel i forhold til organisasjonens minstekrav til sikkerhet og mer.
DDoS	Distributed Denial of service	Type nett-angrep påvirker nettilgang til målene.
	Deployment profil	En mal man ønsker å bruke for å rulle ut OS til enheter.
	Device Compliance	Om en enhet tilfredsstiller kravene som er satt til å få tilgang til bedriftens ressurser.
	Device Configuration	Restriksjoner og mer som kan settes på enheter.
	Device Enrollment	Innrulling av en enhet til domenet.
	Device Restrictions	Restriksjoner man kan sette i policies.
	Domene kontroller	En server som håndterer autentisering av brukere og enheter.
	Endpoint protection	Et program for administrering av antivirus mot brukere i et domene.
	Enrollment Status Page	Innstillinger som kan settes for enheter under og etter innrulling.
EMS	Enterprise Mobility Suite	En pakke fra Microsoft som tilbyr forskjellige tjenester til mobile enheter som for eksempel Intune.

GP / GPM	Group Policy /Group Policy Management	Et verktøy i Server Manager, som benyttes til forskjellige formål.
	Hybrid Azure AD joined devices	Type join i Azure AD.
	Hyper-V	Verktøy for virtualisering.
IaaS	Infrastructure as a service	Et begrep innen skytjenester hvor en bedrift tilbyr deler av en server sine ressurser gjennom virtualisering. Eksempel når du leier en server som et virtuelt miljø.
	Intune	Et verktøy for å administrere og drifte enheter i et nettverk, uavhengig om hvor enheter befinner seg.
	IOS-enhet	En Apple-enhet som bruker operativsystemet iOS.
	Legacy systemer	Utdaterte systemer som fortsatt tas i bruk.
	Resource access policies	Retningslinjer for tilgang til ressurser.
	Software Center	Et program gitt av SCCM hvor brukerne får tilgang til å laste ned programmer.
SCCM/CM	System Center Configuration Manager / Configuration Manager	Et administreringsverktøy for å drifte maskiner, brukt for deployment av OS, Programvare, oppdateringer, monitorering og rapportering av hendelser.
	Man-in-the-middle-attacks	Type nettangrep

	Microsoft Enterprise Mobility Suit	En Microsoftlisens
	Microsoft Store for Business	En nettbutikk for Microsoft applikasjoner.
	Office 365 Enterprise E3 + e5	En Microsoftlisens
	Office Click-to-Run apps	Type workload
OS	Operating System	Operativsystem
OSD	Operating System Deployment	Utrulling av operativsystem.
	On-premise	Systemer som er knyttet til bedriftens private nettverk.
	Policy/policies	Retningslinjer/krav til enheter.
	Task Sequence	En liste med jobber som skal utføres.
	Tenant/Azure Tenant	Et område i Azure.
	Windows 10 Enterprise E3	Type lisens
	Windows Defender	Beskyttende program fra Microsoft.
	Windows Autopilot	Et verktøy for innrulling av nye og gamle maskiner, samt brukt til OSD.
	Wipe	Sletting av alt innhold på en enhet.
	Workload	En jobb som man kan velge å administrere med enten SCCM eller Intune

Tabell 1: Forkortelser og definisjonsliste

Introduksjon til løsningsdesign

Alarmnett AS, er en mellomstor bedrift som driver med salg, montering og service av alarmsystemer. Per dags dato har Alarmnett AS et kontor, som huser opp mot 40 ansatte, hvor 15 av disse ofte er ute av kontoret. De har et hovedkontor i Gjøvik. Bedriften har tidligere lagt mye arbeid og innvestering i Configuration Manager, men ønsker å bevege seg mot en mer skyorientert løsning, etter anbefalinger fra IT-Ansvarlig.

Montører/servicearbeidere, jobber ut mot kundene og befinner seg derfor mye utenfor bedriftens kontorer. Når montørene ikke er ute hos en kunde, vil de ha muligheten til å jobbe fra kontoret.

Salgsmedarbeidere er en gruppe ansatte som sitter halvt om halvt inne og ute av kontoret. Når de sitter på kontoret har de tilgang til nettverket via en bærbar maskin.

Resterende ansatte oppholder seg for det meste på hovedkontoret.

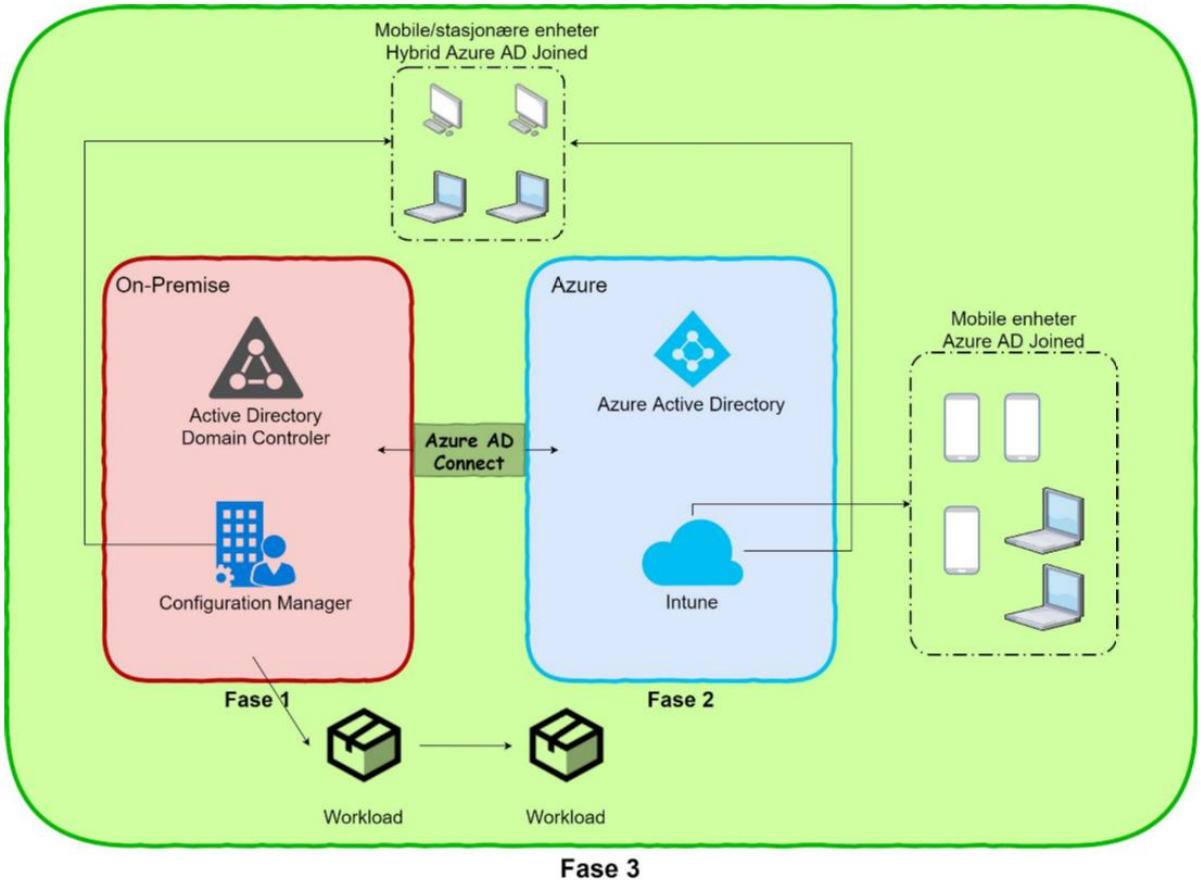
Krav til løsningsdesign:

- Ansatte ute av kontoret må ha tilgang til bedriftens ressurser digitalt.
- Bedriften skal fremdeles benytte seg av SCCM.
- De ansatte skal ikke trenge å logge på mer enn en gang per dag.

Vi skal nå se nærmere på hvilke produkter og løsninger prosjektet benytter seg av. Vi vil først beskrive de forskjellige verktøyene som vi kommer til å ta i bruk, og deretter gå enda dypere inn på hva disse verktøyene hjelper oss med.

Løsningsdesign

Løsningen vår baserer seg på et oppsett kalt Co-Management, hvor Configuration Manager jobber sammen med Intune i Azure AD for å sammen styre alle enheter i nettverket.



Figur 1: Løsningsdesign

Bildet over viser On-Premise miljøet som allerede eksisterer hos Alarmnett AS, koblet opp imot Azure miljøet som vi i hovedsak skal innføre.

På venstre side innenfor den røde samlingen, har vi domene kontroller og Configuration Manager. Her driftes i hovedsak de maskinene som befinner seg inne hos bedriften. På høyre side innenfor den blå samlingen, har vi Azure Active Directory og Intune. Her driftes i hovedsak mobile enheter. Disse to oppsettene er koblet sammen slik at vi oppnår en hybrid Azure AD løsning, som gjør at enkelte enheter som er co-managed kan administreres av både SCCM og Intune.

I fase én, vil vi sette opp de systemene som allerede eksisterer hos Alarmnett AS. Dette omfatter On-Premise systemer som domene kontroller og Configuration Manager. For å simulere at vi har et reelt on-premise miljø, setter vi dette opp på en egen tenant som er

adskilt fra Azure miljøet. Vi oppretter en virtuell maskin som benytter seg av Hyper-V, for å virtualisere on-premise miljøet, med domene kontroller, Configuration Manager og Windows 10 maskiner.

Når on-premise miljøet er satt opp, vil vi videre gjøre klart for fase to, oppsett av Azure miljøet. Her vil vi gjøre klart for å kunne koble disse to miljøene sammen, slik at vi kan begynne å jobbe med Co-Management. Vi vil også starte med konfigurasjon og oppsett av tjenester i Azure, samt tjenester under Intune, mer om dette i kapitelet "Produkt og begrunnelse".

Når begge miljøene er satt opp, vil vi i fase tre, opprette en kobling mellom on-premise og Azure (Azure AD Connect). På den måten kan Azure miljøet (Intune) være med å administrere maskiner og brukere fra on-premise miljøet. Vi vil her ta en beslutning om hvilke jobber (Workloads) som Intune skal ta over administrasjon for. Videre vil vi teste ut mulighetene i Intune, i og med at dette er et helt nytt system for oss, men i hovedsak vil vi ha fokuset på administrering av co-managed enheter.

Produkt og begrunnelse

Domain Controller

Active Directory brukes til administrasjon av brukere, grupper og AD-Objekter. Vår Active Directory er satt opp med en Windows Server 2016. Vi har også tilordnet den rollen Domain Controller, som gjør at vårt Active Directory i tillegg vil styre autentisering i domenet. Med autentisering menes passord og innloggingstjenesten, samt andre funksjoner som trenger verifiseringer av bruker og enheter. Dette gjør blant annet at vi kan logge inn på maskiner som er meldt inn i domenet med domenebrukerne. Domain Controller er et begrep på en Active Directory som kjører Active Directory Domain Services, og legger til ansvarsområdene til Active Directory med autentisering. Med tanke på at dette er et oppsett som kunden vår allerede har, trenger vi ikke gjøre noen andre endringer enn de som trengs for å koble den mot skytjenesten.

Active Directory Group Policy Management

Group Policy Management brukes til å sette regler for brukere og maskiner i et domene. For eksempel kan man lage et sett med regler for oppsatte grupper av maskiner eller brukere. Alt handler om å håndtere brukere og maskiner slik at sluttbrukeren har kun de tilgangene som er satt for brukeren spesifikt eller for en gruppe som brukeren er medlem av. Vi velger å benytte oss av denne funksjonen, da vi går ut ifra at kunden tar det i bruk i sitt on-premise miljø.

System Center Configuration Manager

System Center Configuration Manager er en opphøyet server rolle som tar seg av oppgaver som omhandler: innrulling av nye maskiner, håndtering og oppdatering av applikasjoner, beskyttelse av maskinene, oversikt og styring av software inventory, og støtter styring av maskiner med forskjellige operativsystemer.

System Center Configuration Manager, vil kunne rulle inn nye maskiner til domenet. Dette kan skje på flere måter men den mest hendige måten er å lage en Task Sequence, hvor den utrullingsansvarlige har satt forhåndsinnstillinger på hvordan den nye maskinen skal bli satt opp. Dette kan være å koble seg til domenet til en bestemt bruker, eller installere spesifikke programmer.

Task Sequence, er en forhåndsbestemt liste, som maskinen vil gå gjennom når den skal installeres eller OS skal rulles ut.

Håndtering av applikasjoner er mulig i Configuration Manager ved at maskinene og brukerne får tilgang til Software Center. Her vil brukerne få en liste over sine tilgjengelige applikasjoner samt oppdatering av programvarer. Det er også mulig for IT ansvarlige å bestemme om applikasjonene må være installert eller om brukerne selv skal få velge om de vil installere eller ikke. Det er i tillegg mulig for IT-ansvarlige å bestemme når de viktige applikasjonene eller oppdateringene skal installeres, for eksempel utenfor arbeidstid eller når brukerne logger på.

Man kan også håndtere diverse innstillinger i Endpoint Protection, som er styringsmekanismen til alle Windows defendere i domenet. Her kan man lage sine egne regler, som å konfigurere brannmur, blokkere programmer, oppdatere maskinene når Windows Defender har en ny oppdatering, og/eller gjøre manuelle ting som å scanne valgte maskiner etter virus, eller lese rapporter.

Man har ofte ekstra applikasjoner i en bedrift eller skole og man bør ha en måte for å holde oversikt over hvor mange applikasjoner man har og eventuelt hvem som skal ha tilgang til hvilke applikasjoner. Configuration Manager gir mulighet til å holde oversikt over applikasjonskatalogen til bedriften. Etter å ha registrert applikasjonen kan man senere distribuere den ut til brukerne som skal ha tilgang til den. Man sitter så igjen med en god oversikt over hvor mange brukere som har installert applikasjonen, hvor mange som har hatt

problemer med å installere og mange andre nyttige diagrammer som gir en fin oversikt over applikasjonene.

Det siste fine med Configuration Manager er at den støtter håndtering og styring av andre operativsystemer enn bare Windows 10. Den støtter ikke bare tidligere versjoner av Windows, som windows 7, 8.1 og Vista, men også populære operativsystemer som Linux, macOS.

Dette er et oppsett kunden har som de ønsker å fortsette å bruke.

Azure

Azure er Microsoft sin skyplatform og infrastruktur. Azure er designet til å levere applikasjoner og tjenester over internett. Den skal kunne gjøre alt det en on-premise Active directory kan gjøre og mer, i tillegg til at den skal være tilgjengelig i "skyen" altså over internett.

Azure tilbyr blant annet tjenester som å opprette virtuelle maskiner i et bedriftsmiljø, slik at man kan jobbe i Azure med bedriftsrelaterte saker. Dette har gitt ansatte over hele verden mer frihet i hvor og hvordan de jobber. Vi velger å benytte oss av Azure for å få tilgang til enkelte av disse funksjonene, samt legge opp til at Alarmnett AS, selv kan velge å benytte flere av funksjonene i fremtiden. Azure er et godt valg i og med at Alarmnett AS allerede tar i bruk et DC- og CM-oppsett, da disse systemene kan sys sammen med flere tjenester som ligger tilgjengelig i Azure. Å ta det første steget i retningen «skyen», vil være med å sikre at man er teknologisk med på de endringene som vil skje i fremtiden.

Azure sine tjenester er godt utbredt i verden med hele 54 regioner og tilgjengelighet i 140 land. Dette betyr at man kan sette opp en Azure server i 140 forskjellige land og ha tilgang til denne uansett hvor man er i verden.

Windows 10

Windows 10 er et operativsystem fra Microsoft. Man trenger operativsystemer for å kunne kjøre mer kompliserte koder, som applikasjoner, på en maskin. De fleste datamaskiner i hjemet kjører operativsystem fra Microsoft, hvor Windows 10 er det nyeste operativsystemet. Microsoft har fokusert mye på å integrere inn Windows 10 til tablets og mobiler slik at alle de forskjellige systemene kan bruke et operativsystem. Hovedtanken er "å føre maskinene sammen". Microsoft har i senere tid brukt mye energi og ressurser på å samle alle enheter under et operativsystem, og dette gjør det lettere for oss å rulle inn maskiner til domenet. Vi anbefaler derfor bedriften å benytte seg av enheter med Windows 10 for å gjøre det så lett som mulig for alle å rulle inn i domenet.

Azure Active Directory

Azure Active Directory er en standalone tjeneste som kan tilby mange tjenester som bruker- og gruppe-administrasjon, device management og mer. Azure Active directory er mer eller mindre en tilsvarene versjon av lokal Active Directory. Dette vil si at den håndterer ting som brukere og grupper, men det betyr ikke at den er en ren erstatning av lokal AD selv om den tilbyr mange av de samme funksjonene og mer. I tillegg vil den automatisk ha muligheten til å autentisere brukerne sine og vil fungere som en autentiseringsserver for sine brukere og enheter, lik en Domain controller. I tillegg til standard egenskapene til AD som å administrere brukere, grupper og enheter, har Azure AD også muligheten til å dele ut lisenser, registrere applikasjoner, sette opp conditional accsess og multifaktor autentisering. Ved å være i skyen vil man ha tilgang til kontrollpanelet fra hvor som helst i verden og kan styre bedriften og dens ressurser likedan. Vi trenger Azure AD da Intune krever dette. Sammen fungerer de utmerket som en utvidelse av DC og CM, som kunden allerede har.

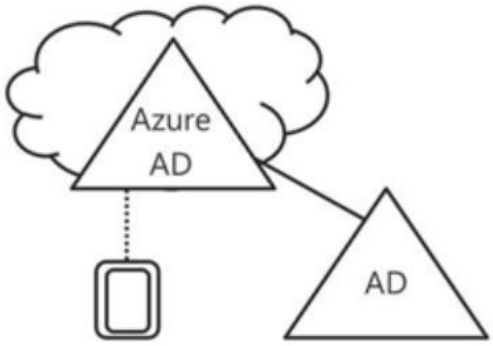
Azure AD Connect og ulike typer "Join"

Når en enhet kobler seg til Azure Active Directory, vil hver enhet få en «Join type». Vi skiller mellom tre typer:

- Azure AD registered devices
- Azure AD joined devices
- Hybrid Azure AD joined devices

Azure AD registered devices

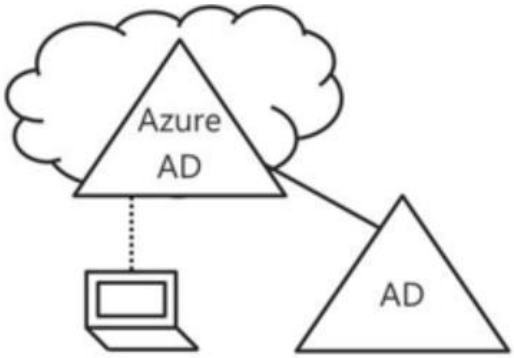
Denne typen «join» er tilpasset private enheter som ikke eies av organisasjonen. Ved å ta i bruk en slik type «join» kan man legge til rette for BYOD (Bring your own device) scenarioet. Enheten vil da få tilgang til organisasjonens ressurser. Dette gjøres ved at man oppretter en work-bruker på maskinen. Vi velger å ta i bruk denne typen join, for å legge til rette for at de ansatte kan ta med seg sine personlige mobile enheter til arbeid, og så filgang til enkelte ressurser.



Figur 2: Azure AD registered devices

Azure AD joined devices

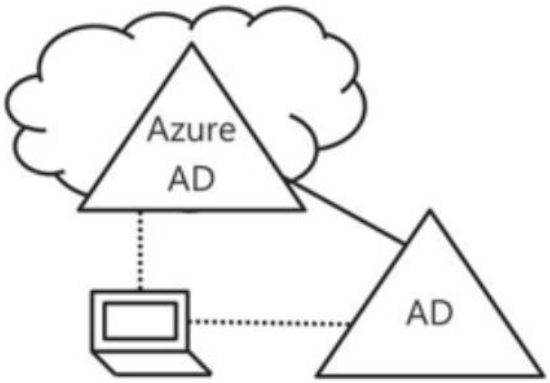
Denne typen «join» er tilpasset enheter som ikke er koblet til et on-premise miljø. Det er her snakk om enheter som kun skal administreres av Intune. Denne typen «join» legger til rette for at enheten kan benytte seg av organisasjonens applikasjoner og ressurser, samt at den kan få tildelt Policies og administreres av organisasjonen. Denne typen «join» blir satt enten ved innrulling gjennom Windows Autopilot, eller gjennom «Self-service experience» altså at man melder inn maskinen til Aure AD manuelt. I og med at vi skal benytte oss av Intune er det en selvfølge at vi benytter oss av Azure AD Join.



Figur 3: Azure AD joined devices

Hybrid Azure AD joined devices

Denne typen «join» er tilpasset enheter som er allerede administreres av Configuration Manager og som da tilhørere et on-premise miljø. Ved å ta i bruk Hybrid Azure AD join på slike enheter, vil man kunne administrere enhetene både ved bruk av lokal Active directory og Azure Active Directory. Hybrid Azure AD join, muliggjør også for at enheten kan bli co-managed av både SCCM og Intune. For å kunne benytte oss av Co-Management vil denne typen join også være rellevant, da den er et krav for å rulle inn enheter som skal være co-managed.



Figur 4: Hybrid Azure AD Joined devices

Azure AD Connect

Dette er et program som lastes ned fra Azure, og kjøres på Active Directory Domain Controller. Man kjører den for å konfigurere tilkoblingen opp til Azure miljøet. Her får man mulighet for å sette opp flere forskjellige tilkoblinger, som er nevnt ovenfor. Man må fullføre et av oppsettene for at domenene skal kunne se hverandre og eventuelt brukerne til hverandre. Vi velger derfor å benytte oss av Azure AD Connect slik at on-premise og Azure miljøet kan kommunisere med hverandre.

Intune

Intune er en sky-basert tjeneste i Azure som tilbyr administrering av mobile enheter. Dette er alt fra overvåkning, utrulling av applikasjoner og oppdateringer, til wiping (sletting av innhold) av enheter. Dette er en løsning som skal ta over for Configuration Manager og som blir endret og oppdatert kontinuerlig. Det største salgspunket til Intune er at den støtter administrering av mange forskjellige operativsystemer, den er lett skalerbar, den kan beskytte bedriftsdata mer effektivt og god brukerstøtte fra Microsoft. Altså den har muligheten til å administrere enheter på lik måte som Configuration Manager, men den største fordelen er tilgjengelighet. Intune gir muligheten til å administrere enheter uavhengig av om enhetene er tilkoblet organisasjonens on-premise nettverk. Dette betyr at Intune kan administrere enheter uansett hvor de er i verden, så lenge det eksisterer en internettforbindelse.

Intune kan på lik måte som Configuration Manager, drive administrasjon av sine enheter, men da i hovedsak mobile enheter. Alt fra Device Enrollment, Device compliance, Device configuration, utrulling av applikasjoner, programvare oppdateringer, bruker- og gruppe-administrasjon, altså funksjoner som er kjent fra Configuration Manager, kan nå driftes gjennom Azure portalen i nettleseren.

For å virkelig benytte oss av mulighetene i skyen og i Azure, er Intune en av hovedårsakene for at vi tar steget og beveger oss mot skyen. Intune vil være med på å dekke behov når det kommer til mye av administrasjonen av mobile enheter.

Device enrollment

Under Device Enrollment, finner man et sett med funksjoner for å administrere innrulling av iOS-, android- og Windows-enheter. Her har man mulighet til å aktivere automatisk innrulling, samt innstillinger knyttet til Windows autopilot:

- Opprette Deployment Profiler
- Håndtere Windows Autopilot enheter
- Aktivere Enrollment Status Page.

Vi tar i bruk Device enrollment, for å kunne rulle inn mobile enheter.

Windows Autopilot

I forhold til Device Enrollment i Intune, har vi nå med Intune fått mulighet til å ta i bruk Windows Autopilot. Dette gir mulighet for automatisk innrulling av enheter til domenet, når en mobil enhet blir sendt ut til brukeren. Denne funksjonen kan på mange måter sammenlignes med muligheten for OSD (Operating system deployment) og innmelding av enheter til domene ved bruk av Task Sequence, som vi er kjent med fra SCCM. Forskjellen her er at mye av jobben hos drifterne utgår, når maskinene er klar for innrulling med en gang de sendes ut fra leverandøren. Alt av Windows Autopilot konfigurasjon finner man under Device Enrollment. Vi velger å benytte oss av Windows autopilot for å forenkle og minke arbeidet med innrulling av mobile enheter.

Device compliance

Under Device Compliance har man mulighet til å sette opp et sett med krav som enheter og brukere må tilfredsstille for å bli "Compliant" (Kompatibel i forhold til organisasjonens krav). Altså ved å ta i bruk slike policies, vil administrator kunne blokkere brukere og enheter som ikke tilfredsstiller kravene som er satt. Type krav som kan stilles er OS versjoner, oppsett av passord, antivirus og lignende. Vi velger å benytte oss av Device compliance, for å forsikre at enheter oppfyller kravene som vi stiller til enheter som skal bli en del av organisasjonens nettverk.

Device configuration

Device configuration i Intune, kan sammenlignes med Group Policy Management i et on-premise miljø. Her har man mulighet til å opprette policies som kan sette restriksjoner eller tilpasse utseende og tildele disse til brukere eller enheter. Typer policies kan være i forhold til Device Restrictions, Endpoint Protection og mer. Vi velger å benytte oss av Device configuration for å kontrollere og lage regler slik at brukerne kan holde seg trygge.

Client apps

Under Client Apps i Intune, kan man på samme måte som i SCCM opprette applikasjoner og rulle ut disse til enheter eller brukere. Her er mulighetene mange, i forhold til typer applikasjoner, da alt fra Microsoft Store applikasjoner, Windows applikasjoner, Android, iOS, Windows Phone og mer, kan opprettes. Vi velger å benytte oss av Client apps for å kunne rulle ut applikasjoner til brukere og maskiner.

Company Branding

Ved å ta i bruk Company Branding har man mulighet til å tilpasse Innloggingssider, når brukeren skal logge seg inn i organisasjonens Microsoft relaterte applikasjoner både i nettleser og andre steder. Dette gir ikke noe mer funksjonalitet enn et kjennetegn for brukere, slik at de vet at de logger inn hos sin organisasjon. Vi velger å benytte oss av Company Branding for å vise brukerne at kunden er en formell bedrift og for å gi bedriftsressursene et personlig preg.

Co-Management

I IT-verden i dag går man bort fra lokale servere, og mot skyløsninger. Der mange bedrifter har benyttet seg av Configuration Manager, er det i dag et ønske om å gå over til skybaserte løsninger som intune. For å sette i gang denne prosessen, har Microsoft lagt til rette for at Intune gradvis skal kunne ta over workloads (jobber) som Configuration Manager tidligere har hatt ansvar for. Dette gjelder enheter som i hovedsak driftes av Configuration Manager og prosessen kalles for Co-Management. Vi har valgt å benytte oss av Co-Management da vi føler det er den beste måten å gjøre bedriften stegvis klar for en migrering over til skyen.

Antallet workloads ser ut til å øke med tiden, og om ikke alt for lenge vil Intune kunne erstatte behovet for Configuration Manager. Etter utgivelsen av SCCM versjon 1806, har Intune til nå fått mulighet til å ta over adminsitrasjon av:

- Compliance policies
- Device Configuration (Endpoint Protection og Resource access policies)
- Office Click-to-Run apps
- Client apps (pre-release).
- Windows Update Policies

For å få tilgang til denne funksjonaliteten i Intune, forutsetter dette at man konfigurere Co-Management i SCCM og switcher over workloads til Intune. Enheter som er Hybrid Azure AD joined, vil da kunne rulles inn til Intune enten automatisk ved bruk av Group Policy eller manuelt. Enhetene vil da bli co-managed, altså at de kan administreres av både Configuration Manager og Intune.

Remote assistanse ved hjelp av TeamViewer

Ved å ta i bruk Remote assistanse ved hjelp av TeamViewer, kan vi enkelt og greit få tilgang til de ansattes maskiner og løse problemer som krever at vi fysisk jobber på deres maskiner.

Drift av Intune med Powershell

Intune og dets mange funksjoner kan på lik måte som Active Directory og Exchange driftes gjennom Powershell. Dette gjør det mulig for automatisering, samt enkel tilgang til de mange funksjonene som vi finner i Intune.

Lisenser

Microsoft Enterprise Mobility Suit

Inneholder et sett med verktøy, som for eksempel Intune, man kan bruke til å drifte og beskytte tjenestene til bedriften. Fokuspunktet til EMS er mobilitet og at man kan jobbe fra hvor som helst uten at det vil påvirke sikkerheten for mye. Den benytter seg av Single Sign-On som vil si at man bare trenger å logge på en gang før man får tilgang til applikasjonene og tjenestene, og den vil huske identiteten til den innloggede brukeren slik at man slipper å bruke mye tid på å koble seg på igjen.

EMS skal gi deg muligheten til å drifte tjenestene og administrere enhetene fra en enkelt konsoll. Dette skal også gi en høyere sikkerhet over bedriftens filer, og gi mulighet til å administrere dem på enheter, hvor som helt i verden. Vi har valgt å benytte oss av EMS, for å lettere kunne administrere mobile enheter som er koblet til Azure, ved hjelp av Intune, og for å få tjenester som Azure AD ikke kan tilby.

Office 365 Enterprise E3 + E5

Office 365 er en pakke med applikasjoner til kontorarbeid, som tekstredigering, presentasjonsverktøy, noteringsverktøy og mer. De mest kjente verktøyene er Word, PowerPoint, One note, Outlook og Excel. I tillegg vil man kunne få tilgang til tjenestene over nett, muligheten for å redigere dokumenter samtidig som andre og backup av filene i skyen. Office 365 Enterprise E3 tilbyr i tillegg mer skreddersydd tilrettelegging mot bedrifter og registrering av produktene mot flere enheter som 5 datamaskiner, 5 tablets og 5 mobiler. Man vil også få tilgang til det som er i Enterprise E1 pakken som inkluderer tjenestene: SharePoint, Exchange (e-post server), Teams, Yammer og Stream. Forskjellen mellom E3 og E5, er at E5 er bedre lagt til rette for de skal drifte miljøet, ved at den gir mye mer detaljerte rapporter, i tillegg til mer avansert antivirus som skal være bedre utrustet til å håndtere zero day angrep. For å kunne gi bedriftens ansatte muligheten til å ta i bruk disse verktøyene, velger vi å benytte oss av denne lisensen.

Windows 10 Enterprise E3

Windows 10 Enterprise E3 er et operativsystem som alle andre versjoner av Windows 10. Enterprise E3 har derimot mange flere funksjoner rettet mot skyen og tjenester i skyen til motsetning fra den vanlige pro versjonen. Den er ikke like tilgjengelig for den vanlige brukeren, derimot må man på Cloud Solution Provider (CSP) via Partner Center for å kunne kjøpe denne lisensen. Disse lisensene vil da bli tildelt til din Azure Active Directory hvor nettverksadministratoren kan tilordne lisensene til brukerne. E3 gjør det lettere for administrator å flytte rundt på lisensene, så om en bruker slutter eller ikke skal ha lisensen sin lenger kan lisensen flyttes over til noen andre som ikke har fått lisensen enda og den vil fungere umiddelbart. Det kreves ingen restart av maskinen for å få tilordnet lisensene og det hele skal gjennomføres uten noen problemer for sluttbrukeren. Windows 10 Enterprise E3 gir brukeren muligheten til å installere lisensen på opptil fem forskjellige enheter. Vi har valgt å benytte oss av Windows 10 Enterprise E3, da den gir oss flere funksjoner og tjenester rettet mot skytjenester. Den vil dermed gjøre det lettere for oss å administrere hver mobil enhet fra Intune og gir oss mulighet for å utføre ting fra Intune som vi ellers ikke hadde hat mulighet til med den vanlige pro versjonen.

Hvordan vi ivaretar behov

Samhandlingsverktøy

Ved å ta i bruk Office 365, dekker vi behovet for Samhandlingsverktøy, samt utviklingsverktøy for dokumenter, e-post og kalender-løsninger. Vi legger spesielt vekt på at de ansatte skal benytte seg av SharePoint for dokument og fildeling.

Tilgjengelighet

Intune vil ivareta behovet vi har for tilgjengelighet, når det gjelder administrering og drifting av de ansattes mobile-enheter, spesielt når de befinner seg utenfor bedriftens kontorer. Oppsettet av Intune og overgangen til skyen fra et on-premise system vil også legge til rette for en videre skyorientert drift, dersom Alarmnett AS ønsker å migrere flere av sine systemer opp i skyen.

Legacy systemer

Mange av de ansatte er avhengige av programmer som ikke er tilgjengelige på Azure. Dette kan være fordi programmene ikke har kommet til Azure enda eller fordi det er veldig gamle programmer. Vi tilfredsstiller behovene til de ansatte ved å tilby administrering av de gamle programmene via SCCM samtidig som de er koblet til Azure og deres tjenester. På den måten kan IT-ansatte gradvis bytte ut programmene når de finner lignende tjenester i Azure.

Automatikk

Systemet vi skal sette opp vil gi mye rom for automatikk. Mange av hovedfunksjonene kan utføres automatisk slik at de krever mindre av tiden til en driftsansvarlig. Hovedfunksjoner omfatter blant annet innrulling av maskiner, utrulling av operativsystem, utrulling av oppdateringer og sette opp policies for restriksjoner og sikkerhet. I tillegg til dette vil vi lage et script som automatiserer prosessen med Windows Autopilot. Vi vil også gjøre det lettere for de ansatte å benytte seg av tjenestene ved å automatisk installere applikasjoner og tjenester slik at de er klare når de ansatte starter maskinen.

Programvare

Ved å benytte oss av Company Portal og Software Center, kan vi distribuere applikasjoner til de ansatte uten at de trenger å gjøre noe mer spesielt enn å logge på maskinen sin. Det vil også være mulig å legge til nye applikasjoner ved å kjøpe eller legge til direkte fra Microsoft store for business, som tilbyr en rekke applikasjoner ment for bedrifter. Man kan ellers legge dem til på den vanlige måten som krever en installasjonsfil, som skal brukes når programvaren skal installeres på de ansatte sine maskiner.

Programvare oppdateringer

Ved å holde alle applikasjonene på et fast sted, eller to, som Company Portal og Software Center, kan vi lettere administrere applikasjonene i ettertid. Det er mulig å få de ansatte til å oppdatere applikasjonsversjonen til de nyeste når man måtte ønske, om en oppdatering er tilgjengelig. I tillegg er det mulig å lage automatiske regler slik at de ansatte alltid skal oppdatere antivirus og lignende programmer om man finner en ny oppdatering for de programmene.

Gradvis migrering til skyen

I og med at IT-verdenen går mer og mer mot en sky-orientert fremtid, er det et sterkt behov og ønske hos Alarmnett AS å gradvis bevege seg over til skyen. For å dekke dette behovet vil vi først og fremst begynne å ta i bruk skyløsninger spesielt for å administrere nye enheter, men også eksisterende enheter. Det er her snakk om å ta i bruk tjenester i Azure og da spesielt Intune. Intune vil i hovedsak kunne ta over administrasjon av nye enheter og utføre administrative oppgaver. Men i og med at vi ønsker en gradvis overgang, vil vi ikke gå bort i fra on-premise løsningen som Alarmnett AS allerede har investert mye tid og ressurser i. Derfor vil vi benytte oss av Co-Management prosessen, som legger til rette for at et on-premise miljøet kan jobbe sammen med Azure miljøet, og vi oppnår en best mulig utnytting av ressursene som allerede eksisterer og nye som innføres. Vi vil her ha fokus på Workloads og kartlegge når tiden er inne for å la Intune ta over deler av arbeidet hos SCCM.

Redusere driftskostnader og arbeid

Ved å automatisere mye av det som tidligere var manuelt arbeid, vil vi spare driftsansvarlige for mye tid og arbeid. Et on-premise system koster mye å sette opp med tanke på servere og hardware. Ved å bevege seg bort fra en on-premise løsning og over til skyen, vil Alarmnett AS kunne spare mye penger i og med at skyen er veldig skalerbar. I tillegg vil de oppleve raskere respons på innrullinger og arbeid generelt da skyløsningene er raskere enn on-premise løsningene.

Sikkerhet

Microsoft tilbyr økt sikkerhet på sine skytjenester. Ved å samle tilgangen til Azure på en portal vil de slippe å håndtere hver sin separate servers innloggingstjeneste. På den måten kan de forene innloggingene med økte ressurser og sikkerhet. Behovet for fysisk sikkerhet blir mindre da flere av tjenestene vil ligge hos Microsoft. I tillegg vil Microsoft kunne stille med bedre sikkerhet og et større drifts-team for fysisk vedlikehold. Utenom dette vil man ikke trenge å bry seg om nettverk og hardware til maskinene da det vil være Microsoft sin oppgave å vedlikeholde dette. Dette er typisk for en IaaS, da vi bare kjøper deler av serveren, for eksempel infrastrukturen, som en tjeneste og Microsoft vil holde styr på resten. I tillegg vil serverne ha økt beskyttelse mot DDos angrep og man-in-the-middle-attacks. Intune gir også sikkerhet til mobile enheter og muligheten til kontrollere disse, noe Configuration Manager ikke hadde muligheten til alene. Dette vil naturlig gi høyere sikkerhet da man får kontroll over noe man ikke tidligere hadde kontroll over. I tillegg kan man utføre en rekke handlinger for å beskytte bedriften mot at filene deres havner på villspor om en mobil enhet blir kompromittert. Da har man muligheten til å wipe enheten og eventuelt skru den av. Man kan også legge til restriksjoner på enhetene slik at man ikke kan kopiere eller endre viktige dokumenter, som ikke skal tukles med. Dette kan gjøres ved hjelp av Policies. Man kan også sette opp regler for å få lov til å bli med i domenet, som også kan settes opp ved hjelp av Policies.

Oversikt og kontroll

Systemet vi setter opp skal gi bedriften god oversikt over applikasjoner, enheter, brukere, policies og mer, ved å tilby to forskjellige administrasjonsplattformer. Intune gir oss en lett måte å holde oversikt over systemet. Ved å inkludere Configuration Manager vil vi tilby mer kompliserte verktøy som ikke støttes av Intune, samt støtte for legacy systemer. Configuration manager gir dessuten mer detaljerte og grundige rapporter og benytter seg gjerne av andre verktøy som skal hjelpe driftsansvarlige for å lettere søke gjennom rapportene. Disse verktøyene kan for eksempel være verktøy som CMTrace og andre rapporterings verktøy. Intune derimot gir oss en god og veldig oversiktlig måte å styre enhetene og brukerne på. Ved å navigere deg inn på en bruker eller enhet kan du fjernstyre enheten, som for eksempel å wipe enhten. Ved å benytte oss av de sterke sidene fra hvert system vil vi dekke samtlige behov.

Lave krav til IT-kunnskaper

Office-pakken tilbyr mange hendige programmer med veldig lav terskel på både tilgang og bruk. Det er i tillegg veldig stor sjanse for at de ansatte har benyttet seg av tidligere versjoner av programmene, og da er det veldig lett å venne seg til de nye versjonene. Microsoft tilbyr i tillegg god brukerstøtte til sine kunder om det skulle være problemer med programvaren. Company Portal og Software Center skal også gjøre det veldig lett å få applikasjoner som bedriften har, ved å tilby et enkelt system for å installere applikasjonene. Samtidig vil man få en katalog hvor man kan se alle de tilgjengelige produktene man har tilgang til via bedriften. Det vil i tillegg bli enda lettere for de ansatte når Office365 kan huske brukeren din slik at de bare trenger å logge seg på deres tjenester ved et tastetrykk. Dette vil si at man i teorien bare trenger å logge seg på med passord, via deres tjenester, en eneste gang. Ved å holde lav terskel på bruk av produktene vil man spare tid og penger på opplæring og man vil sjeldnere støte på problemer.

Driftsrutiner

Per dags dato har Alarmnett AS fem IT-ansatte og vi legger opp til at det er rundt fem som vil drifte systemet videre. Det vil være mulighet for å utvide antall ansatte i fremtiden om arbeidsoppgavene skulle bli noe større enn det de fem ansatte kan håndtere. Dette er derimot noe Alarmnett AS må avgjøre selv.

Alle endringer skal dokumenteres og avklares med IT-ansvarlig før eventuell gjennomføring. Dette er for å få oversikt over mulig skadeomfang og hvilke ansatte som vil bli påvirket av endringen. Ansatte som blir berørt av endringen skal så bli varslet god tid i forveien, som igjen bør være på en fast tidsramme. Vi anbefaler minst en uke i forveien, men tidligere er bedre.

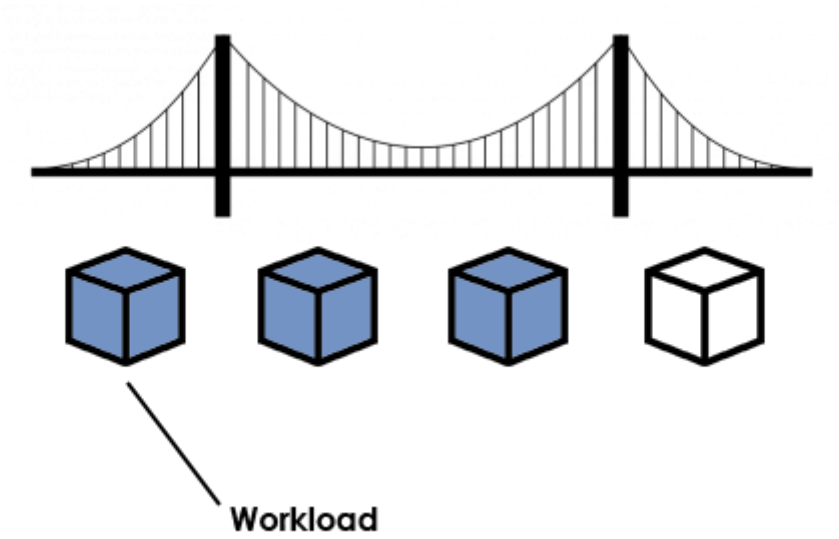
Etter å ha integrert Intune og Azure i systemet vil det bli mindre å ta back-up av da man vil ha back-up av on-premise løsningen i skyen. Det er mulig å fortsette back-up-løsningen Alarmnett AS har i dag, men denne bør kanskje kopieres en gang iblant i tilfelle Azure går ned. Optimalt sett vil man spare mye på å bare ha back-up i Azure, i tillegg til at det er veldig usannsynlig at Azure går ned.

Vi anbefaler ellers å oppdatere programvarene så jevnlig som mulig for å opprettholde et høyt sikkerhetsnivå på systemet. I tillegg anbefaler vi å bytte ut tjenester eller programmer med tilsvarende tjenester og programmer som Azure tilbyr. Dette er for å øke sikkerheten slik at man får mer oppdaterte og sikre produkter. Dette er nødvendigvis ikke noe som må gjøres med en gang, men heller noe bedriften kan gjøre over tid.

Kilder

1. Hybrid Azure AD Joined. *Microsoft Docs*. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/active-directory/devices/overview (hentet: 05.02.2019)
2. Azure AD Connect. *Microsoft Docs*. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect (hentet: 05.02.2019)
3. Intune. *Microsoft Docs*. Tilgjengelig fra: https://docs.microsoft.com/en-us/intune/what-is-intune (hentet: 05.02.2019)
4. Enterprise Mobility Suite. *Bloggpost fra Sadasystems*. Tilgjengelig fra: https://sadasystems.com/cloud-solutions/one-microsoft-solution/enterprise-mobility-suite (hentet: 05.02.2019)
   What is Microsoft Enterprise Mobility Suite? Tilgjengelig fra: https://www.petri.com/what-is-microsoft-enterprise-mobility-suite (hentet: 05.02.2019)
5. Azure AD. *Microsoft Docs*. Tilgjengelig fra: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis (hentet: 05.02.2019)

«Migrering til Azure»



Driftsrapport

Bendik Gjøvikli og Dat-Danny Pham

Trondheim, 20.05.2019

Innholdsfortegnelse

Figurliste

Forkortelser og definisjoner

Forkortelse	Navn	Definisjon
AD/ADDC/DC	Active Directory / Active Directory Domain Controller	System for administrering av brukere, grupper, maskiner og autentisering
	Active Directory Domains and Trust	Et verktøy i Server Manager, som gjør det mulig å sette opp trust mellom domener
	Active Directory Schema	En del av Active Directory, som inneholder regler for opprettelse av objekter i en forest
	Autogrowth	Autogrowth bestemmer hvor mye lagring databasen skal utvide seg med dersom den blir full
	Azure	Azure er Microsoft sin skyplatform og infrastruktur
	Azure Active Directory	Tilsvarende system som Active Directory, men som finnes i Azure
	Azure AD Connect	Prosess som utføres for å knytte lokal AD sammen med Azure AD
	Boot diagnostics	Informasjon som brukes for å avklare oppstartsproblemer
	Boundary group	Nettverkslokasjon for enheter
	Client Apps	Type workload, samt et verktøy for utrulling av applikasjoner
	Client /SCCM client	En pakke med innstillinger som sendes ut til klienter. Ofte referert som clienten for å få tilgang til Software Center.
	Co-Management	Trinnvis metode for migrering av jobber fra SCCM til Intune

	Compliant (Her i forhold til devices i Intune)	Kompatibel i forhold til organisasjonens minstekrav til sikkerhet og mer
	Company Branding	Tilpasser utseende på innlogging og mer
	Compliance policies	Krav som settes til enheter for at de skal ha tilgang til ressurser i nettverket
	Cumulative Updates	Tidligere utgitte oppdateringer fra Windows Updates
	Device Configuration	Restriksjoner og mer som kan settes på enheter.
DC	Domain Controller	En server som håndterer autentisering av brukere og enheter.
DHCP	Dynamic Host Configuration Protocol	DHCP gjør det mulig å tildele IP-adresser og andre nettverksparametre til maskiner og enheter automatisk
DNS	Domain Name Server	En server som oversetter forståelig domene navn som vg.no til IP-adresser som maskinen forstår. Gjør internettopplevelsen mer behagelig.
	Hyper-V	Verktøy for virtualisering
	Hybrid Azure AD join	Type join i Azure AD
EMS	Microsoft Enterprise Mobility	En pakke fra Microsoft som tilbyr forskjellige tjenester til mobile enheter som for eksempel Intune
	Endpoint Protection policies	Et program for administrering av antivirus mot brukere i et domene
	Intune	Et verktøy i Azure for å administrere og drifte enheter i et

		nettverk, uavhengig om hvor enheter befinner seg
	Intune managed enheter	Enheter som administreres av Intune
	Lease duration	Hvor lenge en klient kan ta i bruk en IP-adresse
	Non-Compliant	Ikke kompatibel i forhold til organisasjonens minstekrav til sikkerhet og mer
	PowerShell	Et verktøy for scripting
	Private Memory Limit	Et maksimalt antall minne som en prosess kan bruke før "application poolet" resirkuleres
	Office Click-to-Run Apps	Workload, som gjør det mulig å rulle ut Office-pakken til co-managed enheter ved bruk av Intune
	Queue Length	Et maksimalt antall forespørsler, som setter som en maksverdi, for å hindre at serveren ikke henger alt for langt etter
SCCM/ CM	System Center Configuration Manager	Et administreringsverktøy for å drifte maskiner, brukt for deployment av OS, Programvare, oppdateringer, monitorering og rapportering av hendelser
	Resource access policies	Retningslinjer for tilgang til ressurser
SPN	Service Principal Name	Navnet til en tjeneste i et "epost-format"
SQL	Structured Query Language	I vårt tilfelle en type database som benytter SQL, som spørrespråk

	Tenant/Azure tenant	Et område i Azure
UPN	User Principal Name	Navnet til en bruker i et e-post-format
VM	Virtuell Machine	En virtuell maskin. Altså ikke en fysisk maskin, ofte opprettet inni en annen fysisk maskin eller server. Brukes ofte for fjernstyring.
	Windows ADK	En samling verktøy og teknologier produsert av Microsoft, som er utformet for å hjelpe med å distribuere Windows-operativsystemer til datamaskiner
	Windows Autopilot	Et verktøy for innrulling av nye og gamle maskiner, samt brukt til OSD
WSUS	Windows Server Update Services	En oppdateringstjeneste fra SCCM som vil oppdatere Windows for maskinene i domenet, hvor man kan bestemme tidspunkt og slikt selv. Gjør at ting føles automatisk for sluttbrukeren.
	Windows Update policies	En workload som lar Intune ta på seg arbeid med diverse oppdateringer.
WMI	Windows Imaging Format	Denne filtypen er den Microsoft bruker for blant annet utrulling av programvare i Intune
	Workload	En arbeidsoppgave som finnes i SCCM, men som kan flyttes over til Intune

Tabell 1: Forkortelser og definisjoner

Faser i implementasjon

Nedenfor vil vi beskrive de forskjellige fasene i implementasjonen. Vi har valgt å dele opp fasene slik:

- **Fase 1**: Oppsett av DC og SCCM
- **Fase 2**: Post-konfigurasjon av SCCM
- **Fase 3**: Veien til Co-Management
- **Fase 4**: Demonstrasjon av funksjoner i Intune
- **Fase 5**: Microsoft Intune API

Beskrivelse av faser

Fase 1 – Oppsett av ADDC og SCCM

I fase 1, vil vi først se på hvordan man oppretter en VM i Azure. Denne virtuelle maskinen, vil kunne ses på som vårt on-premise system. Vi vil deretter sette opp en VM for domenekontroller og SCCM, samt Windows 10 maskiner som skal brukes til testing. Videre vil gå gjennom oppsett og konfigurasjon av domenekontroller. Deretter vil vi gjøre klart for å installere SCCM, samt gå gjennom installasjon av SCCM.
Fasen er svært omfattende og legger grunnlaget for det videre arbeidet i oppgaven vår. Mye av det vi gjør i denne fasen er å sette opp systemer som allerede skal ligge til rette og være i bruk hos vår fiktive bedrift Alarmnett. I fase 2, vil vi fortsette der vi slapp i fase 1, men vi velger å dele opp disse to delene i hver sin fase, da arbeidet er omfattende og tar en del tid.

Fase 2 – Post-konfigurasjon av SCCM

Når fase 1, er gjennomført og SCCM er installert, kan vi begynne å se på post-konfigurasjon av SCCM. Her vil vi gå gjennom de innstilligene som vi velger å konfigurere for at SCCM skal fungere som det skal for vårt formål. Det skal sies at ikke all konfigurasjon på SCCM gjennomføres i denne fasen, da vi vil gå tilbake og gjøre ytterligere konfigurasjon i de senere fasene. Målet i denne fasen er å få konfigurert det vi trenger til nå, før vi går videre og legger til flere funksjoner, som vil kreve mer konfigurasjon.

Fase 3 – Co-Management

Etter fase 2, kan vi endelig starte arbeidet med å sette opp nye systemer hos vår fiktive bedrift Alarmnett. Grunnlaget for det videre arbeidet er gjort og vi skal nå se på hvordan vi kan få lokalt Active Directory til å koble seg sammen med Azure Active Directory. Selv om vi velger å kalle denne fasen «Co-Management», vil vi først se på Azure AD Connect og komme tilbake til Co-Management, når dette er gjort. Vi demonstrerer oppsett av Azure AD Connect, for å legge til rette for Hybrid Azure AD Join. Når det er gjort ser vi på hvordan man tildeler lisenser til brukere i Azure.
Når Azure AD Connect, er satt opp, ser vi på hvordan vi kan konfigurere Co-management. Vi vil først og fremst fokusere på konfigurasjon av Co-Management, men vi vil også ta for oss oppsett som legger til rette for automatisk innrulling, som demonstreres i fase 4. Videre vil vi også beskrive mulighetene med workloads, samt demonstrere hvordan Intune kan administrere co-managed enheter ved å flytte workloads til Intune.

Workloads som vi skal se på er:

- Compliance policies
- Windows Update policies
- Device Configuration (Endpoint Protection og Resource access polices)
- Office Click-to-Run Apps
- Client Apps

Fase 4 – Funksjoner i Azure AD og Intune

Når vi endelig har fått koblet on-premise miljøet med Azure, kan vi se på hvilke funksjoner Intune har å tilby. Vi vil først se på enkle funksjoner i Azure AD, som opprettelse av brukere, grupper og tilordning av lisenser. Videre vil vi se hvordan man kan laste opp eller opprette applikasjoner i Intune og hvordan disse kan rulles ut til brukere/grupper, før vi går over til å rulle ut operativsystem med Windows Autopilot. Når dette er gjort, vil vi videre se på Innrulling av maskiner til Intune, hvor vi tar for oss samtlige former for innrulling av både Intune managed enheter og co-managed enheter. Vi vil også se på automatisk innrulling.

Fase 5 – Administrasjon av Intune ved hjelp av PowerShell

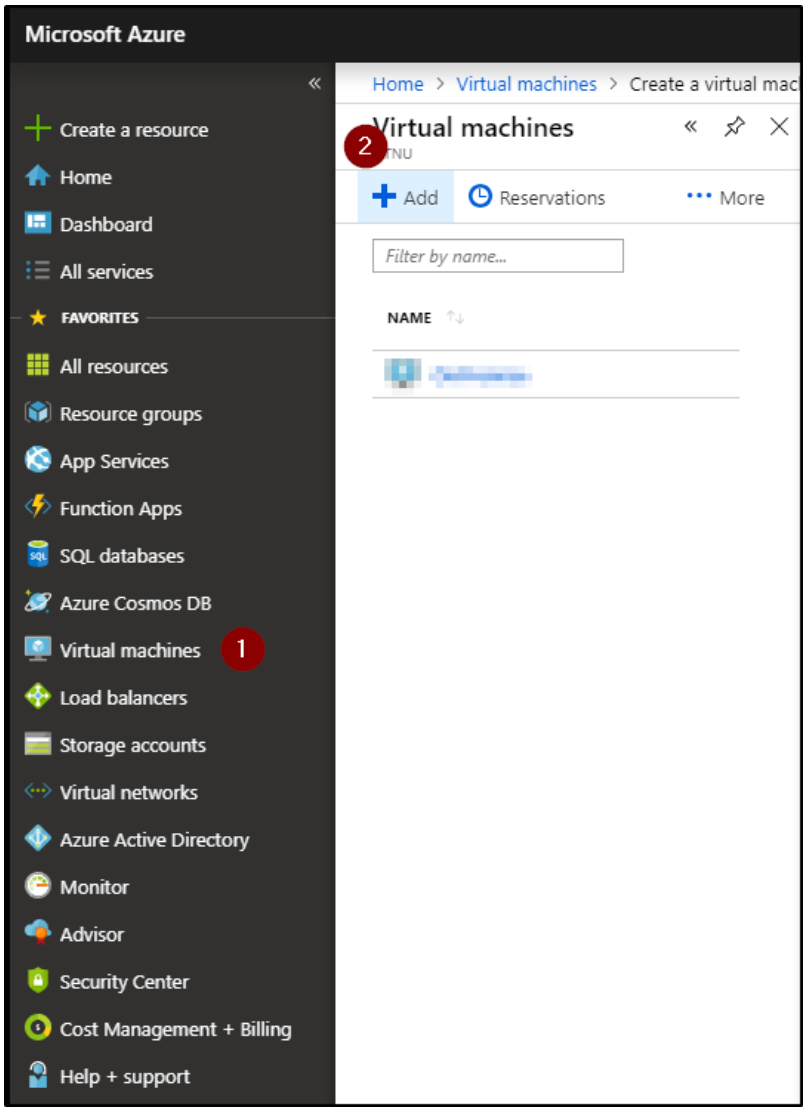
Når vi har vært gjennomført fase 4, vil vi nå se på hvordan man kan drifte Intune med PowerShell. Vi vil her vise til eksempler på kode, på funksjoner som støttes i PowerShell. Til slutt vil vi også opprette et script som vil inneholde flere av disse funksjonene, og som kan brukes til å utføre like operasjoner, men som er tilpasset behov og de funksjonene som vi kjenner til best. Vi velger bevist å ta for oss oppgaven med dette scriptet i fase 5, slik at vi sitter med mer kunnskap om hva Intune og Azure hare å tilby av funksjonalitet.

Fase 1 – Oppsett av ADDC og SCCM

Oppsett av VM i Azure

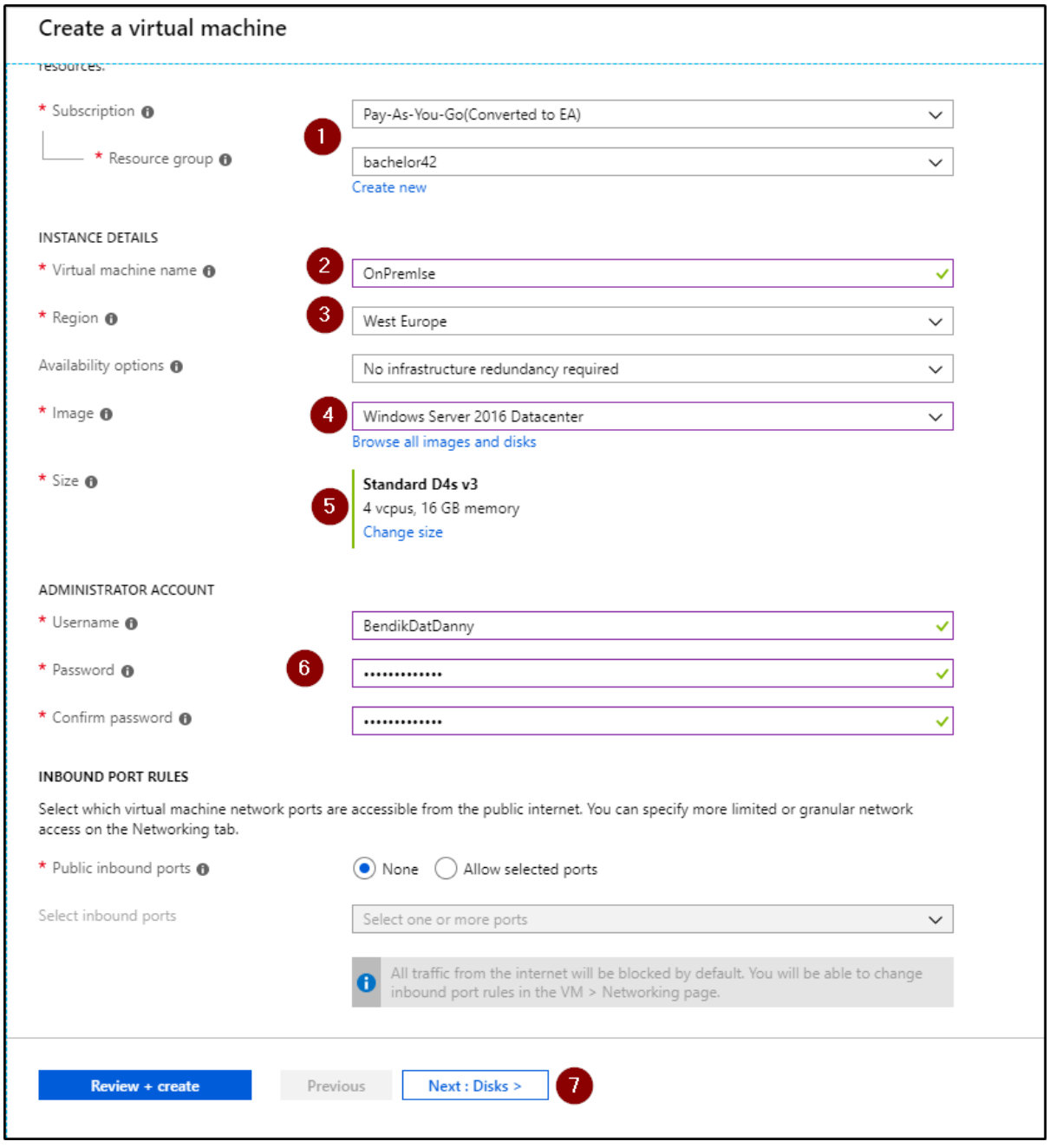
Vi oppretter en VM på NTNU sin egen tenant. På denne virtuelle maskinen skal vårt on-premise miljø, hvor vi setter opp DC og SCCM, samt Windows 10 maskiner ligge. I en reel situasjon ville vi hatt en fysisk server, men siden vi ikke har tilgang på en benytter vi oss av en virtuell en. Vi passer også på at serverne, on-premise og Azure, ikke kan kommunisere med hverandre på forhånd.

Velger **Virtual Machine** og trykker på **Add**.



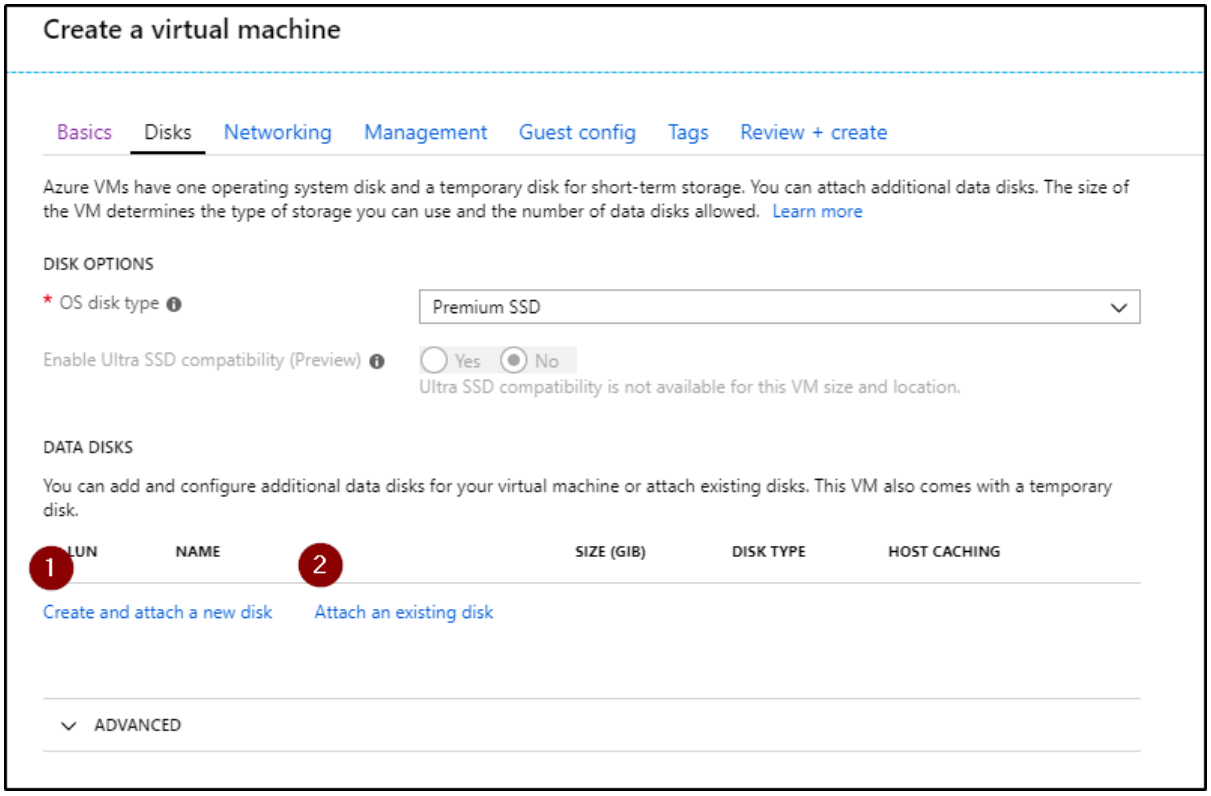
Figur 1: Oppsett av VM i Azure

Ved punkt (5), er det viktig at man velger en VM som har hardware som støtter virtualisering. Dersom man velger en VM, hvor hardware ikke har støtte for virtualisering, kan man enkelt gå inn å oppgradere den virtuelle maskinen på et senere tidspunkt.



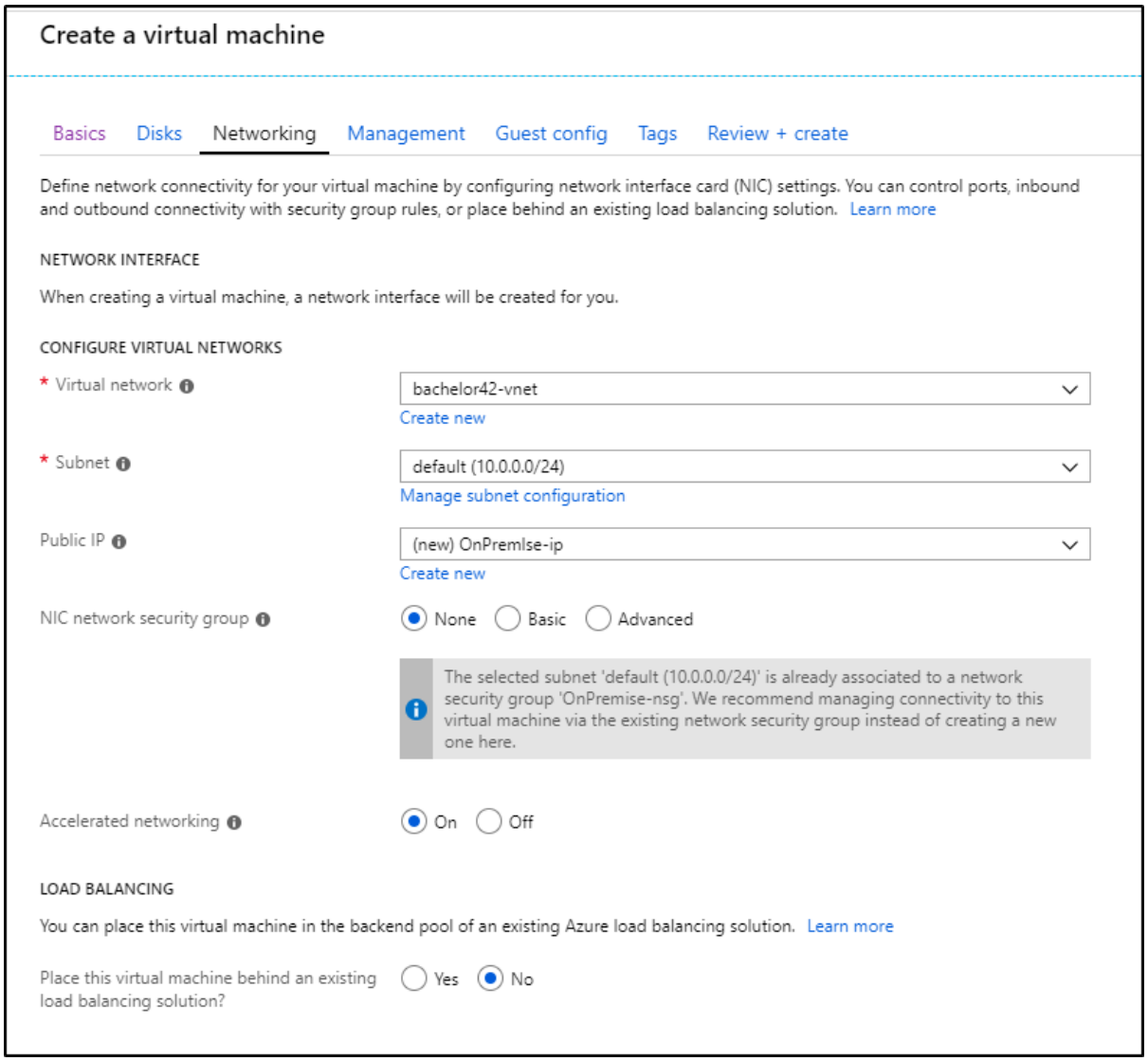
Figur 2: Oppsett av VM i Azure

Under ***Disks*** har man mulighet til å lage en ekstern disk, eller legge til en allerede eksisterende disk.



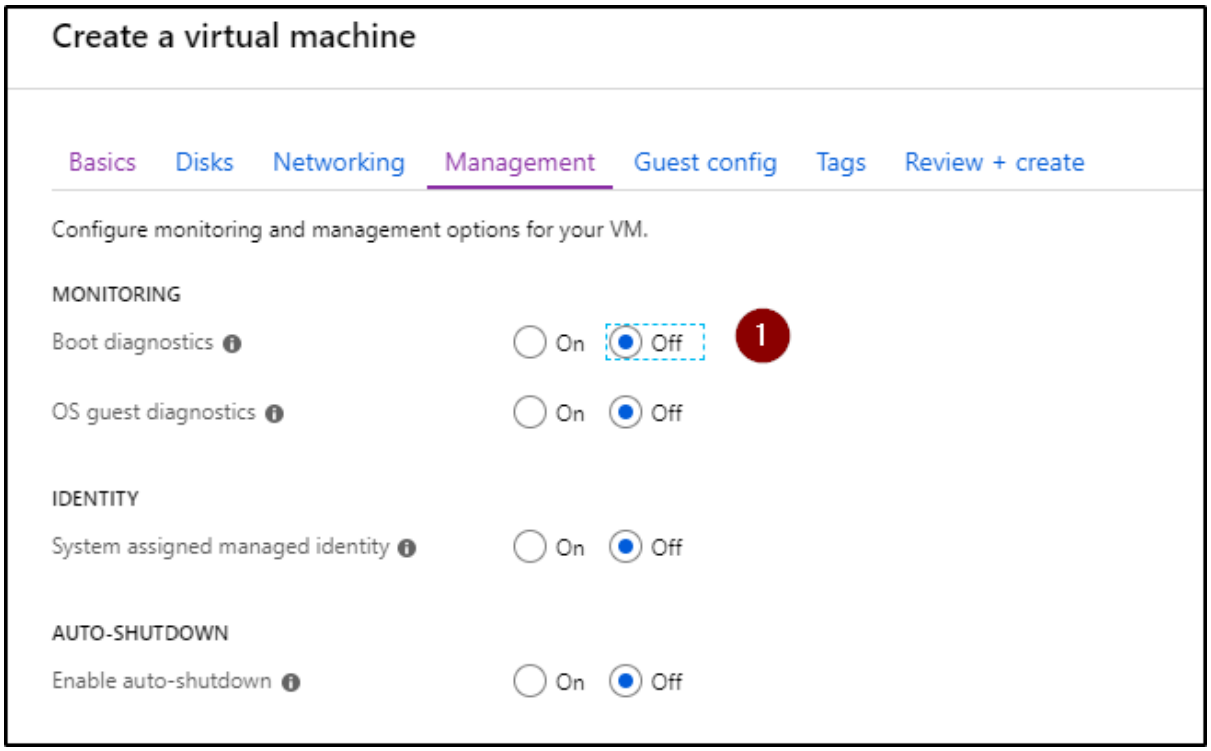
Figur 3: Oppsett av VM I Azure

Ser til at alt stemmer i forhold til valg av nettverk.



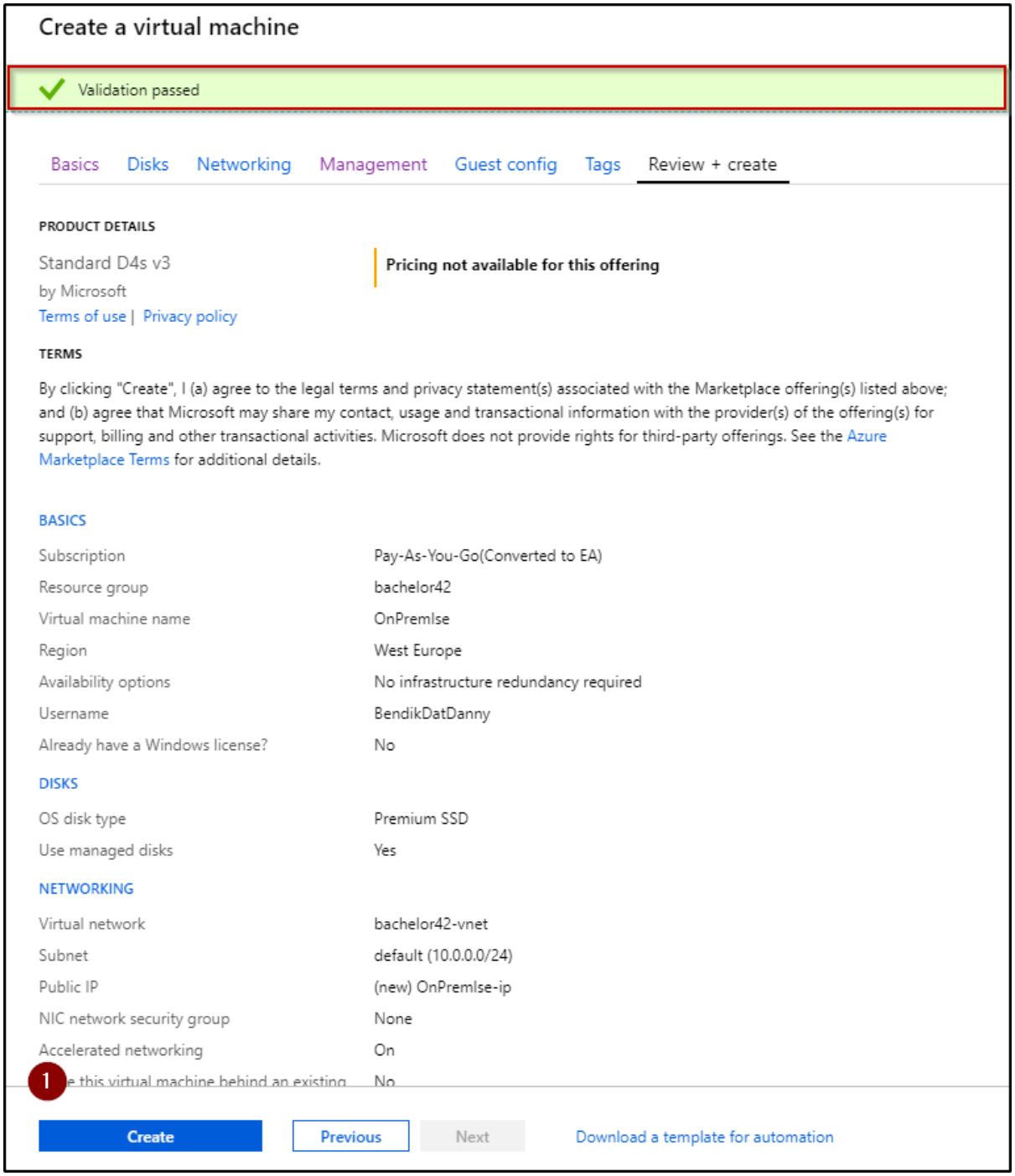
Figur 4: Oppsett av VM I Azure

Her velger vi å slå av Boot diagnostics, da denne ikke støttes av premium storage account. Dersom Boot diagnostics står på kan det hende at vi får en feilmelding av typen «StorageAccountTypeNotSupported». Vi beholder resterende standard innstillinger**.**



Figur 5: Oppsett av VM I Azure

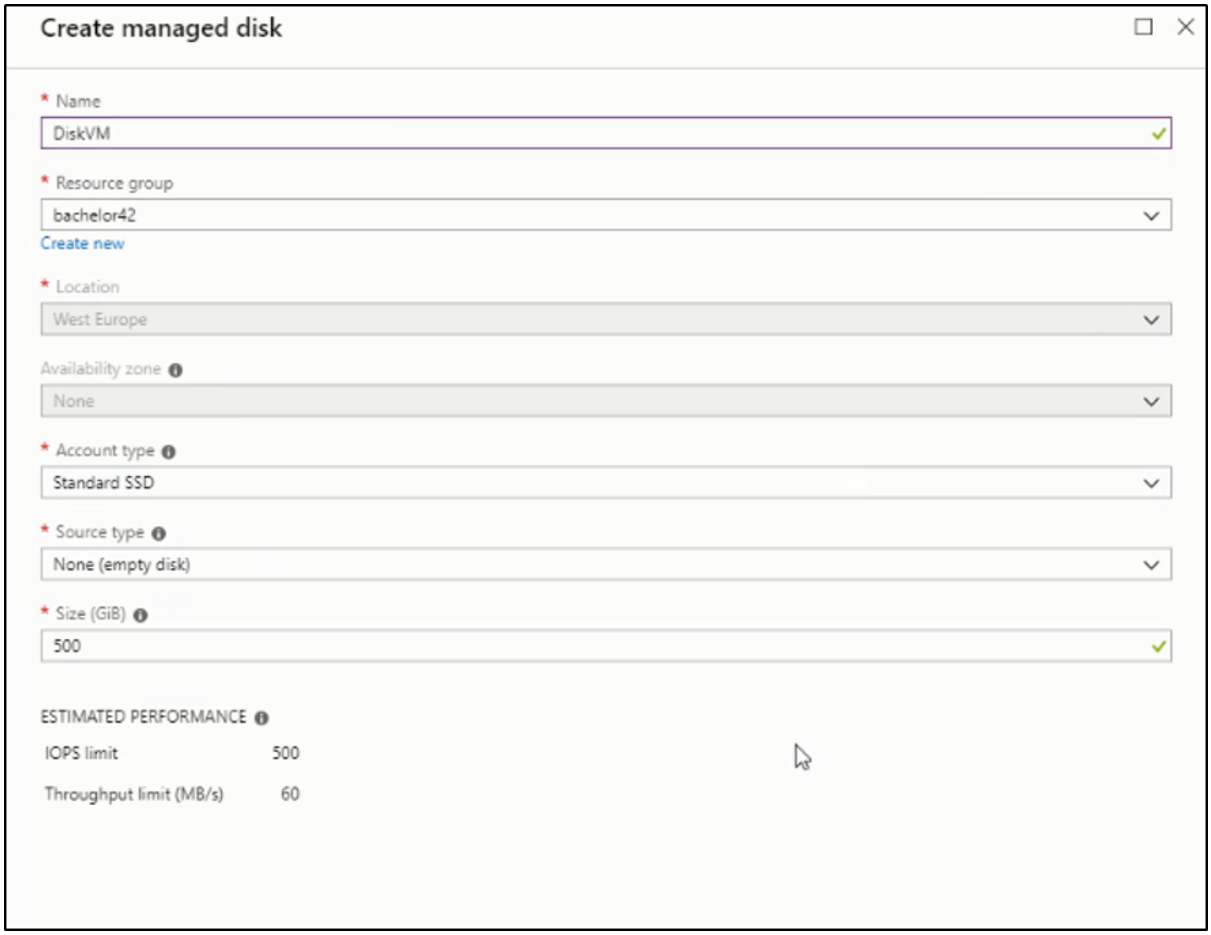
Til slutt kan vi gå direkte til ***Review + create*** og se til at Validation er satt til «passed», altså at VM-en er klar til å opprettes. Vi velger deretter **Create** for å starte opprettelse av VM.



Figur 6: Oppsett av VM I Azure

Oppsett av Disk i Azure

For å få plass til VM-er i vårt Hyper-V miljø, trenger vi mer diskplass. Eventuelt kan man bruke dette til å opprette mer diskplass om det skulle være et behov senere. Disker kan opprettes og kobles til VM-en når som helst.

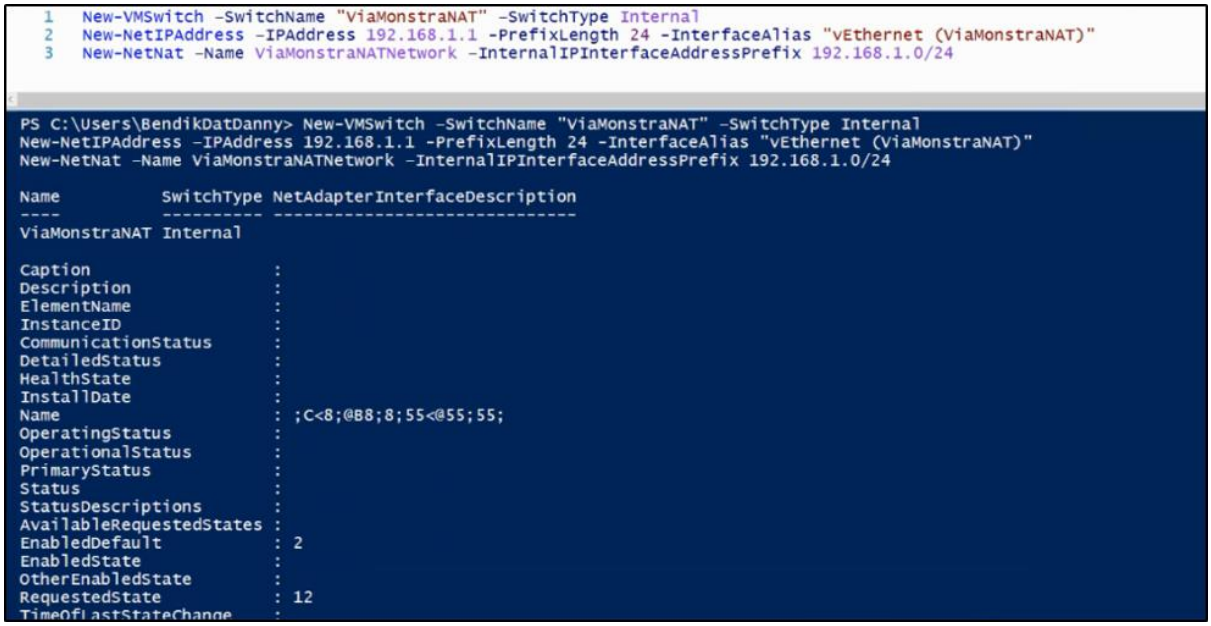


Figur 7: Oppsett av Disk i Azure

Oppsett av Virtuell Switch

For å kunne få Hyper-V VM-ene på nett, må vi opprette en virtuell switch som er koblet til den "fysiske" maskinen, altså i vårt tilfelle On-Premise maskinen som vi har laget i vårt Azure miljø.

I skjermbildet nedenfor kjører vi et script i PowerShell som opprettet en virtuell switch for oss.

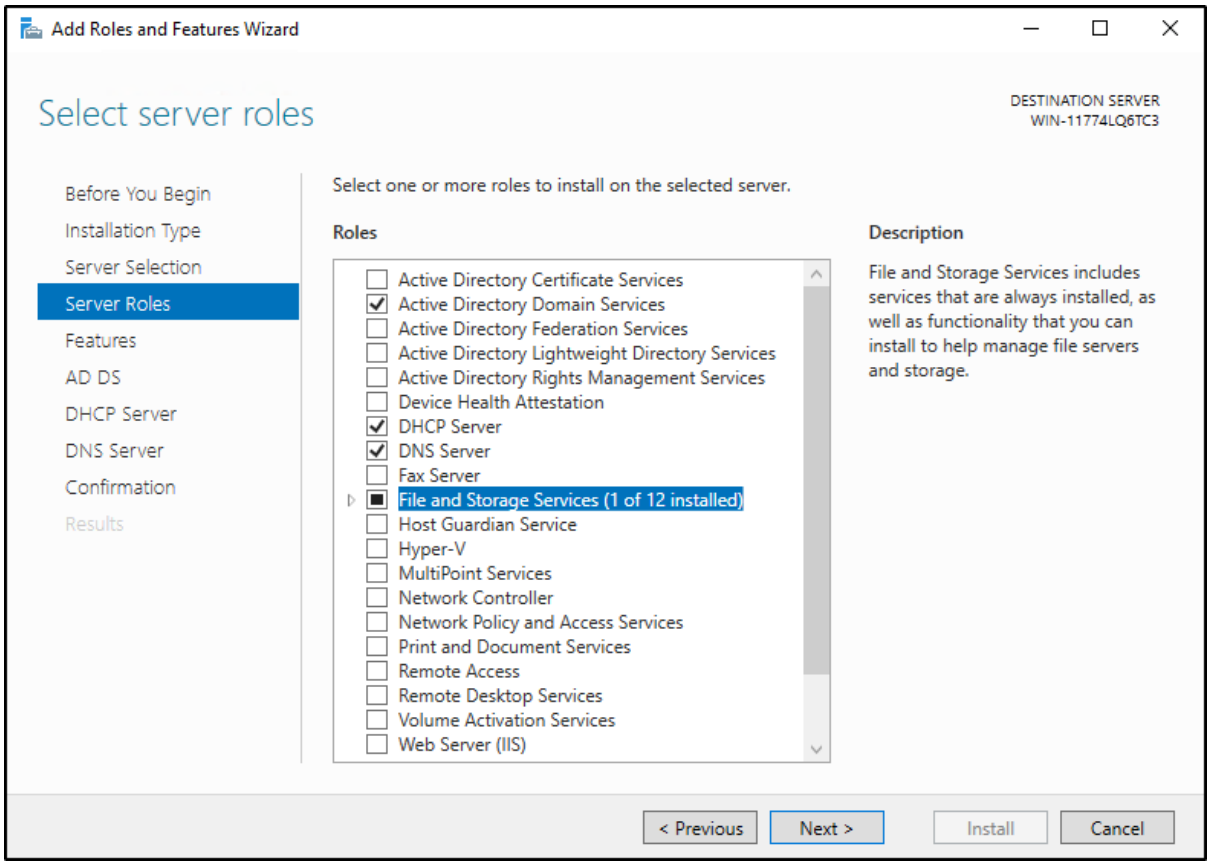


Figur 8: Oppsett av Virtuell Swtich

Installasjon av ADDC, DNS og DHCP rollen

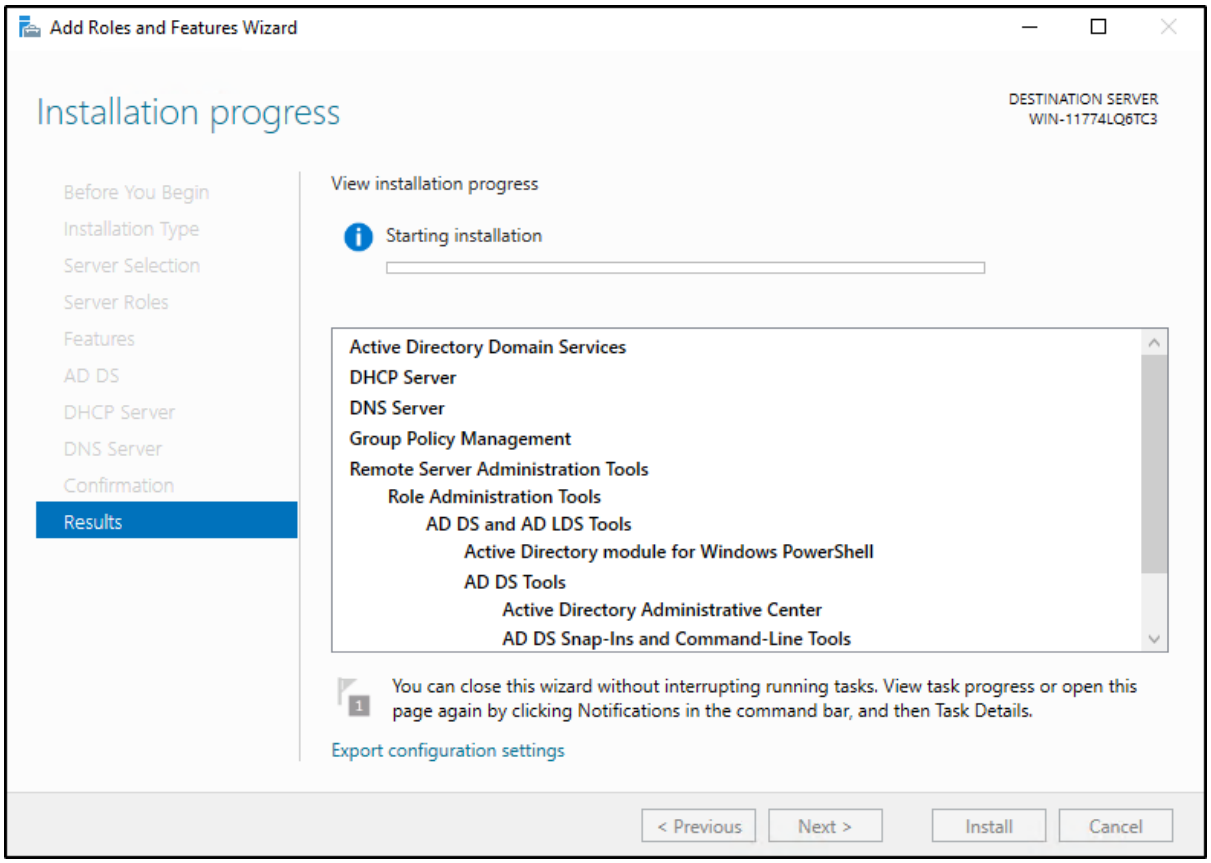
Under dette kapittelet og underkapitlene, skal vi nå se på hvordan vi kan installere rollene ADDC, DNS og DHCP. Disse rollene vil sammen utgjøre vår DC.

Velger rollene som vi ønsker å installere. Nedenfor kan vi se at vi velger rollene «*Active Directory Domain Services*», «*DHCP Server*» og «*DNS Server*».



Figur 9: Installasjon av roller til DC

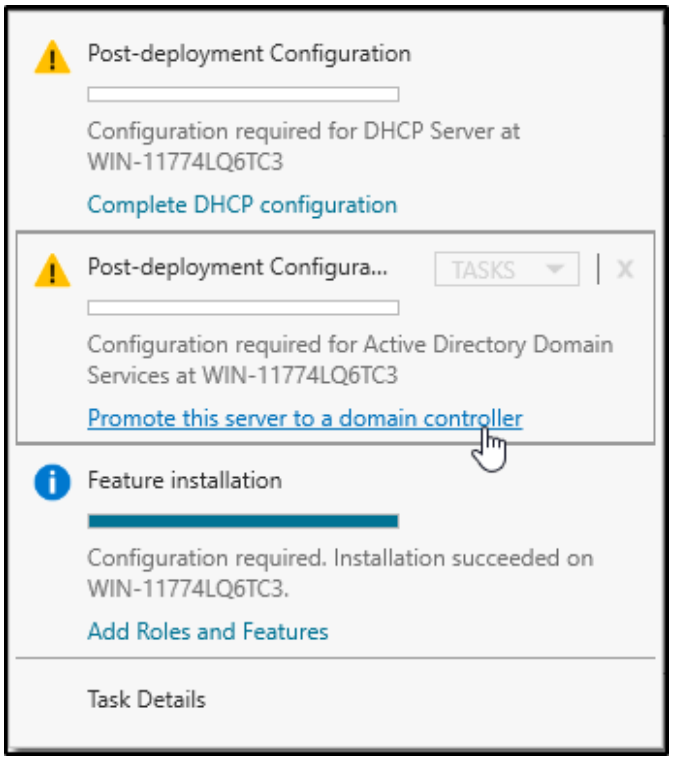
Fortsetter ned til ***Results*** og velger **Install**.



Figur 10: Installasjon av roller til DC

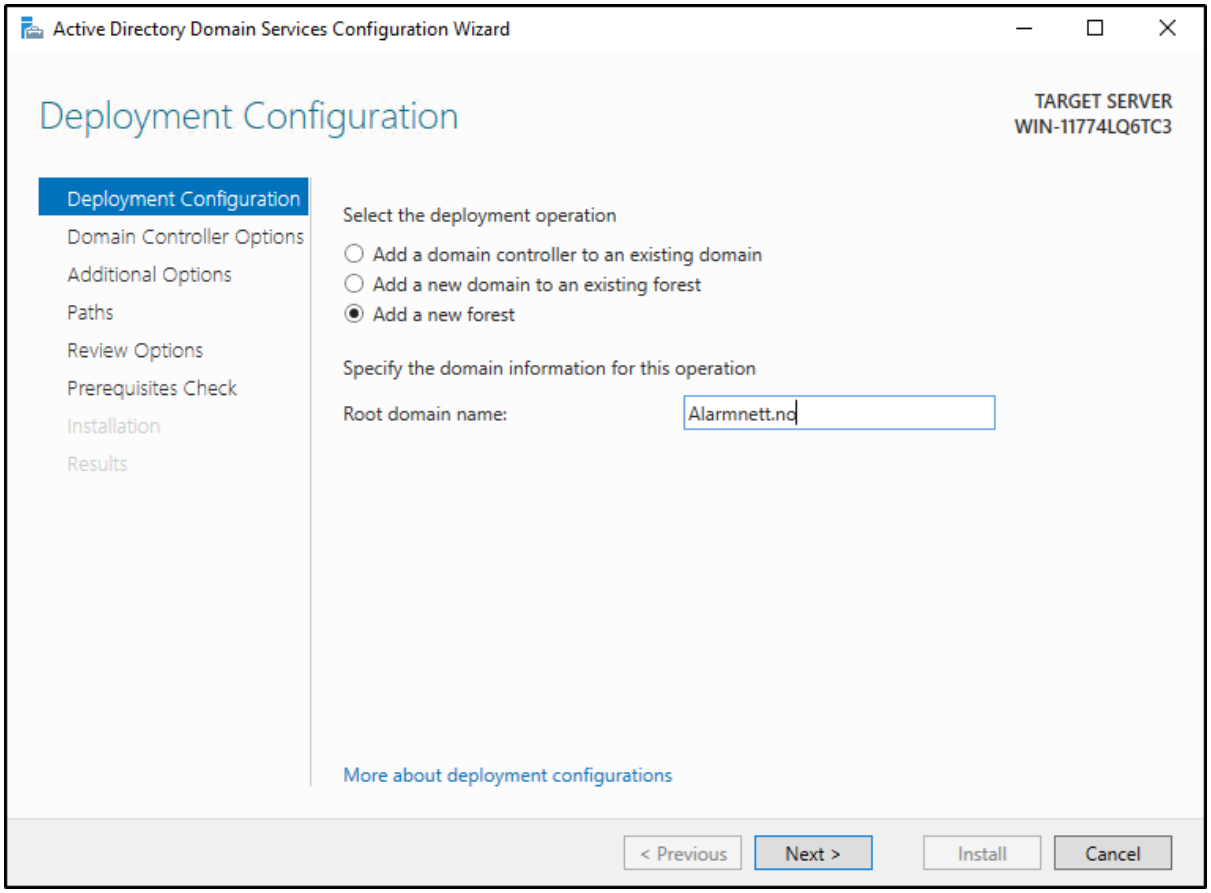
Promotering av Domenekontroller

Etter å ha installert rollene kan vi promotere serveren til en domenekontroller. Dette gjøres via Server Manager, ved å velge «**Promote this server to a domain controller**».



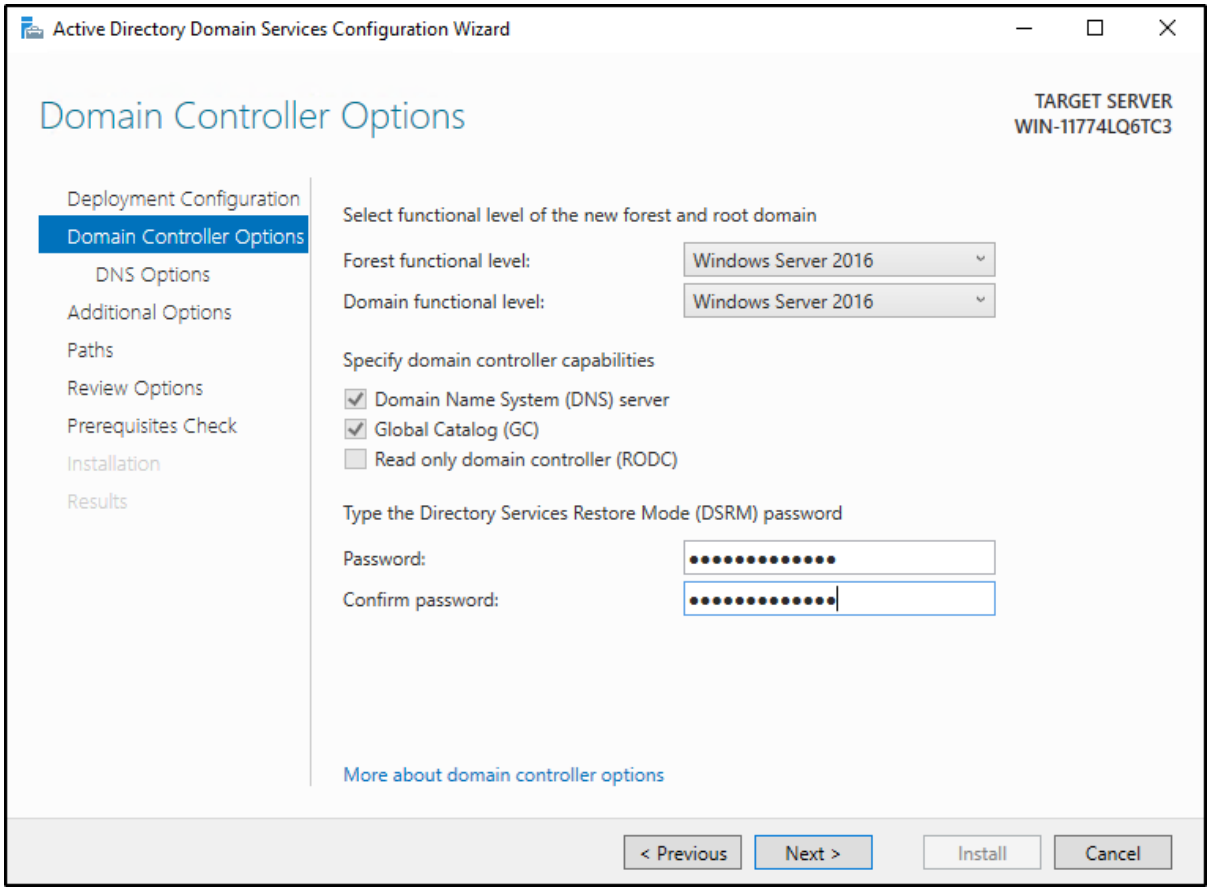
Figur 11: Domenekontroller - Promotering

Under ***Deployment Configuration***, velger man **Add a new forest** og skriver inn et *Root domain name*. I vårt tilfelle velger vi navnet til bedriften i casen.



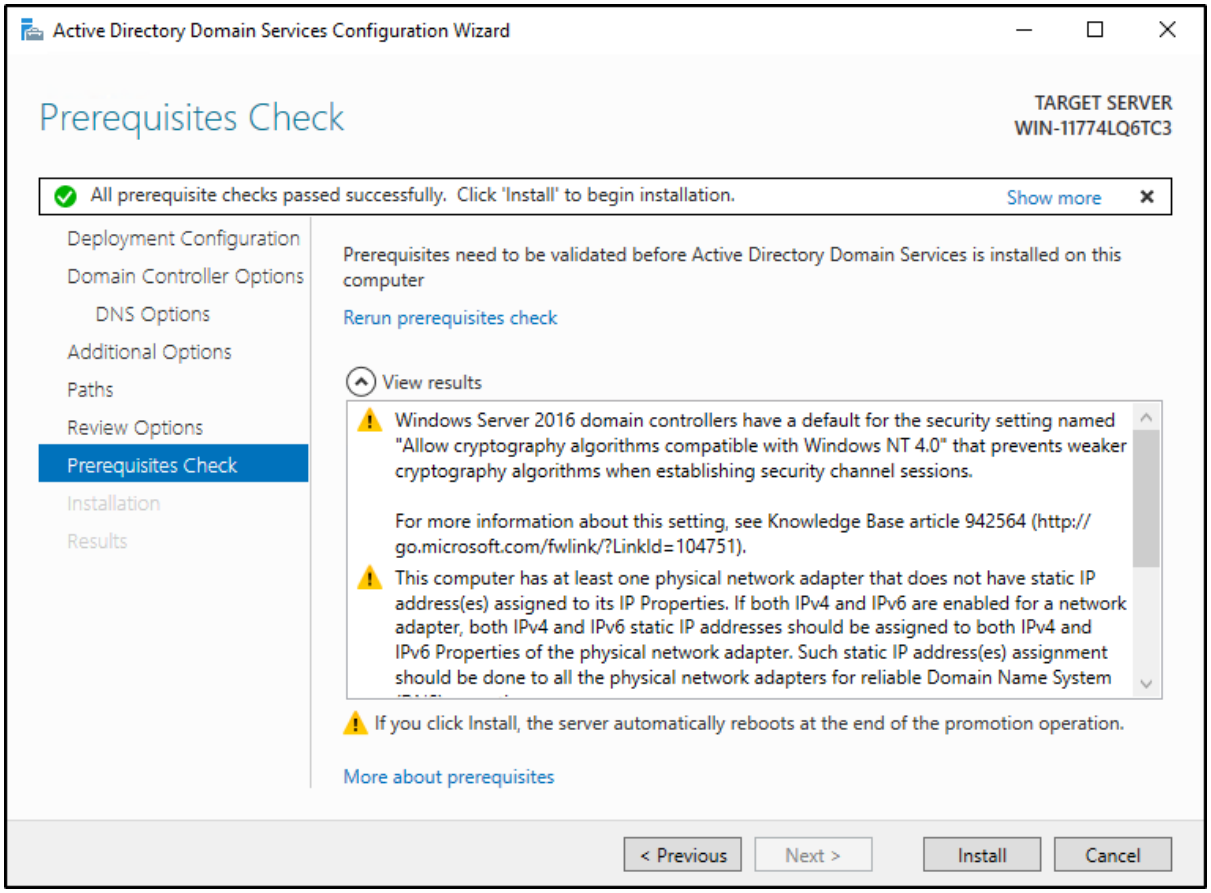
Figur 12: Domenekontroller - Promotering

Under ***Domain Controller Options*** ser vi til at vi setter **Windows Server 2016** på både *forest-* og *Domain functional level.* Deretter setter man et passord.



Figur 13: Domenekontroller – Promotering

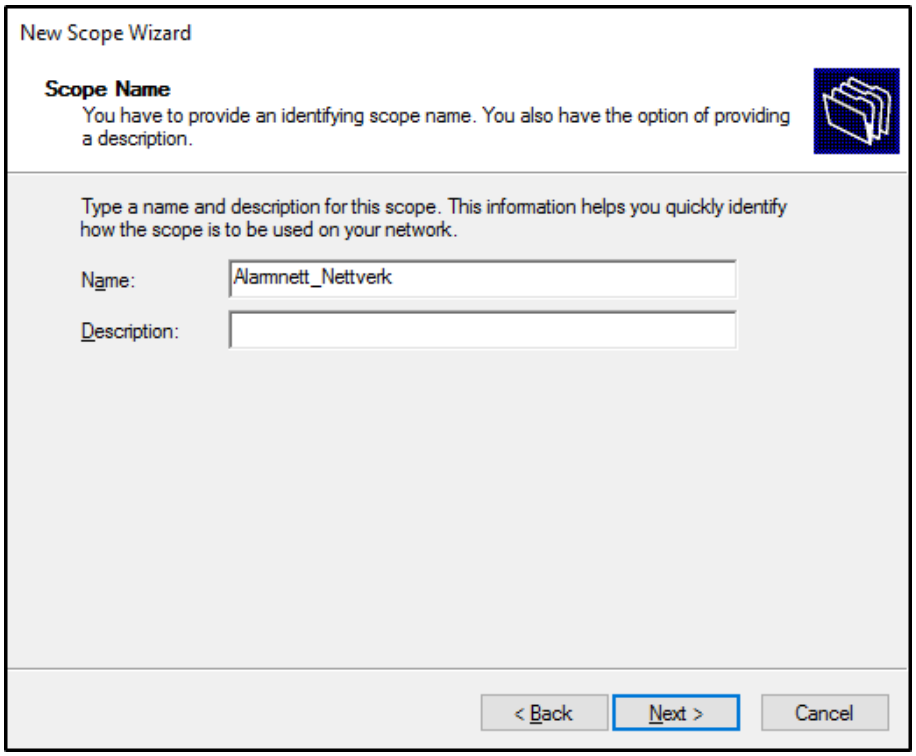
Beholder standard innstillinger på resten av stegene til promotering av domenekontroller er gjennomført og velger **install**.



Figur 14: Domenekontroller - Promotering

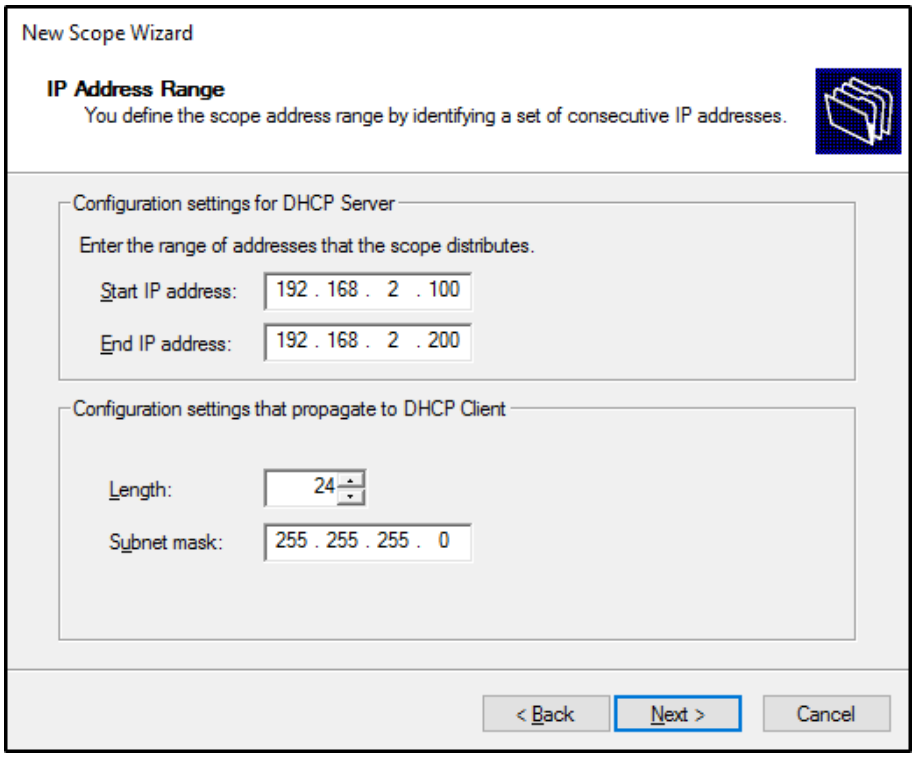
Konfigurasjon av DHCP og DNS

Vi skal nå gjennomgå hvordan vi setter opp en DHCP server. Under ***Scope Name***, setter vi først et navn på DHCP serveren. I vårt tilfelle velger vi å sette denne til «Alarmnett_Nettverk».



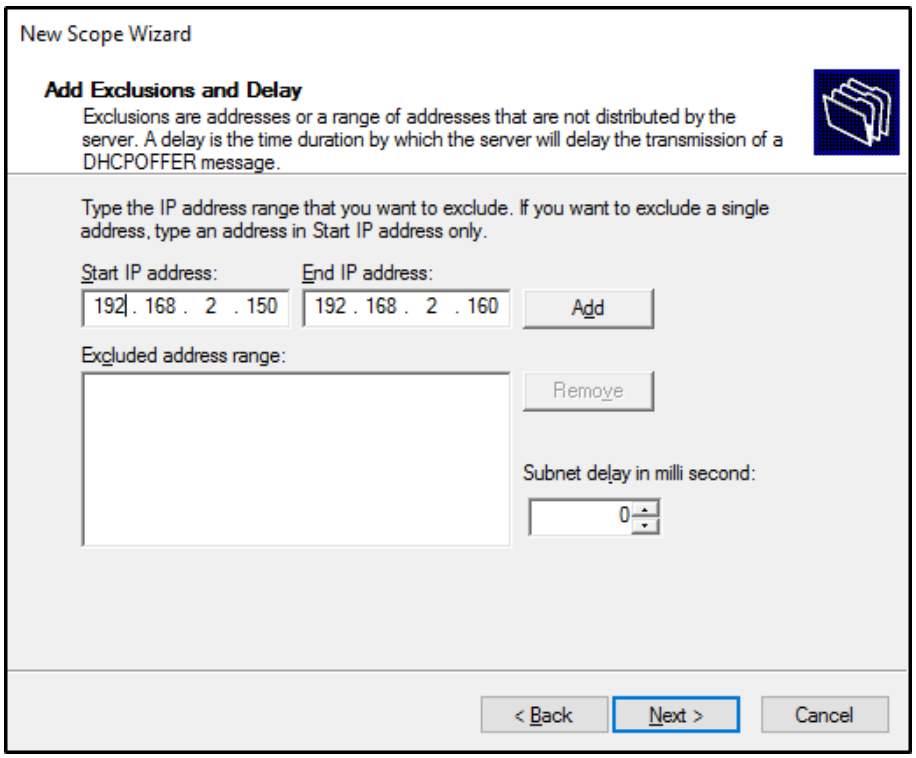
Figur 15: DHCP og DNS - Konfigurasjon

Videre under ***IP Address Range,*** setter vi *Start IP address*, *End IP address* og *Subnet mask*.



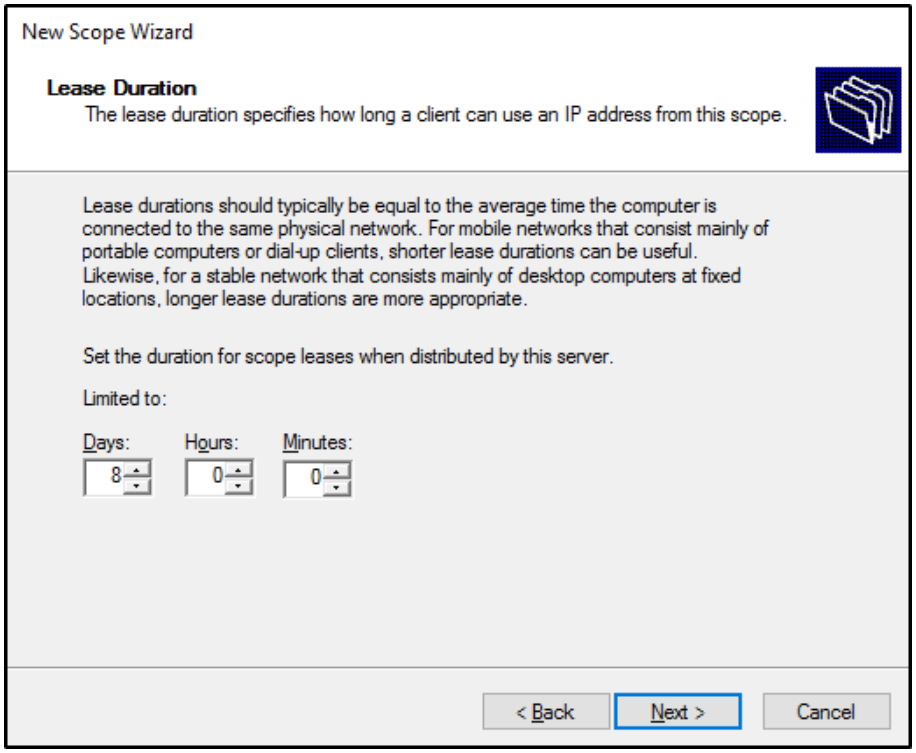
Figur 16: DHCP og DNS - Konfigurasjon

Deretter under ***Add Exclusions and Delay,*** setter vi vi *Start IP address* og *End IP address*, for de IP-adressene vi ønsker å ekskludere.



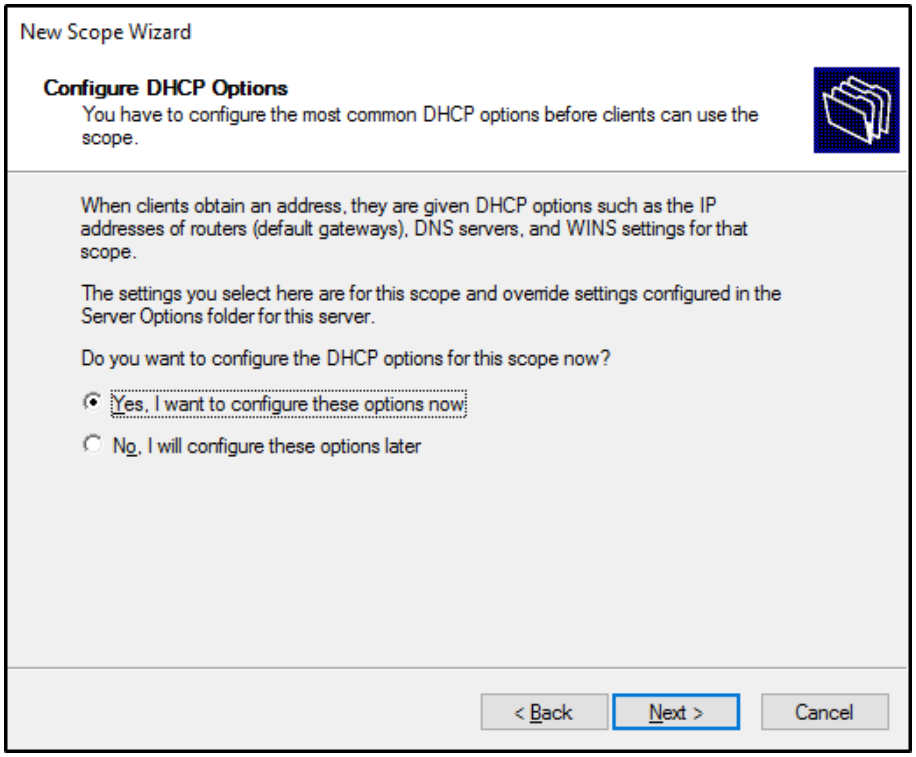
Figur 17: DHCP og DNS - Konfigurasjon

Under ***Lease Duration***, spesifiserer vi hvor lenge en IP-adresse skal være satt av til en bruker dersom brukeren ikke logger på nettet på en stund.



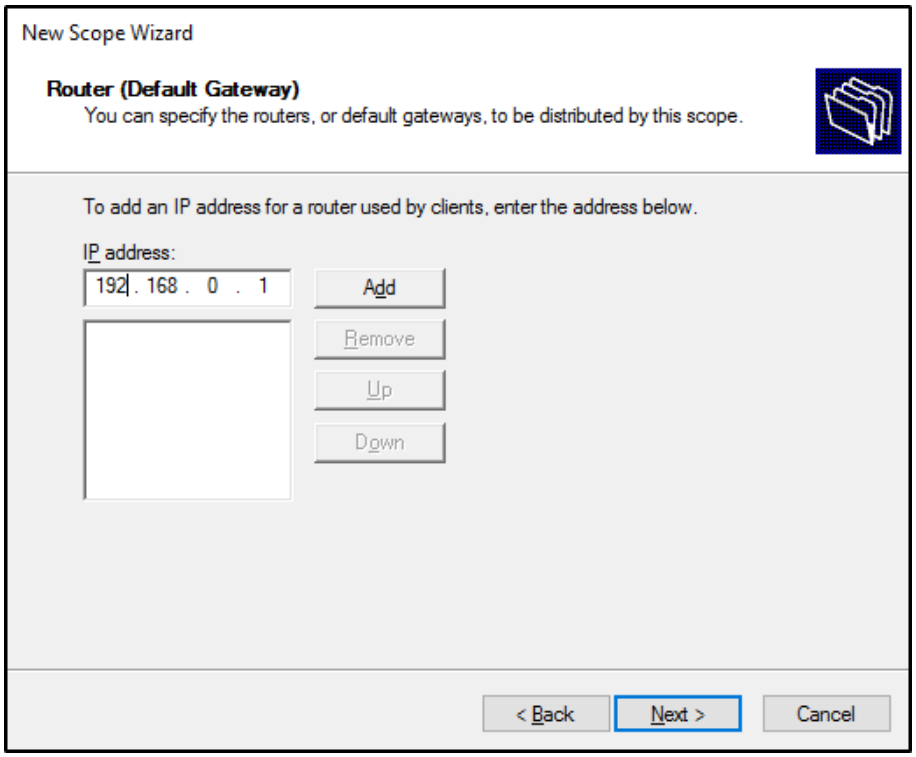
Figur 18: DHCP og DNS - Konfigurasjon

Under ***Configure DHCP Options***, velger vi første valg: «yes, I want to configure these options now».



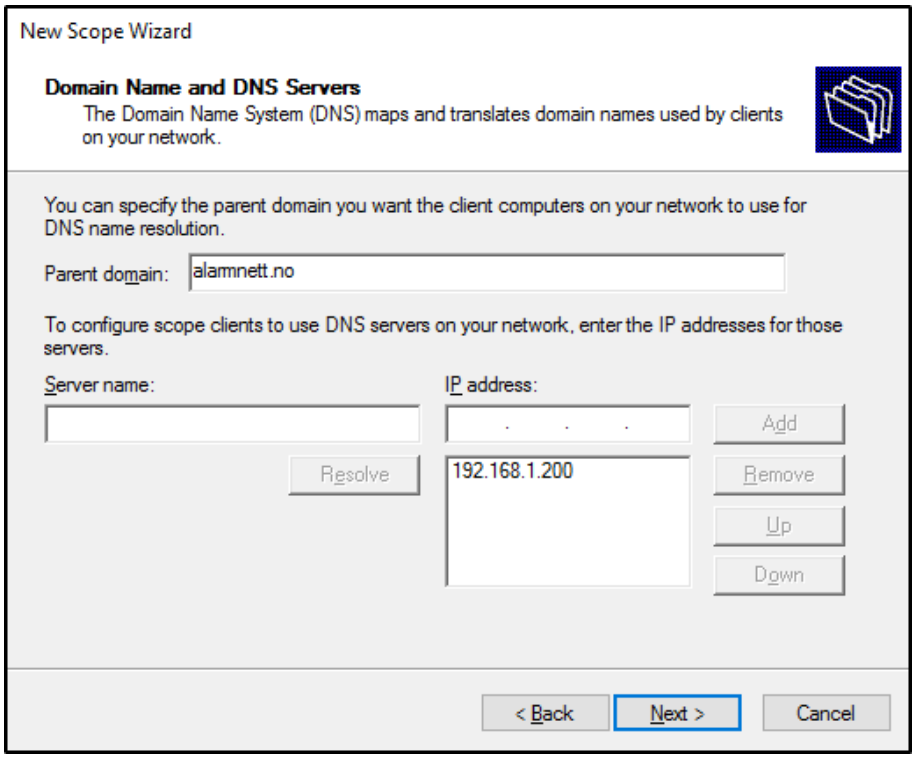
Figur 19: DHCP og DNS - Konfigurasjon

Under ***Router (Default Gateway),*** setter vi IP-adresse til Default Gateway.



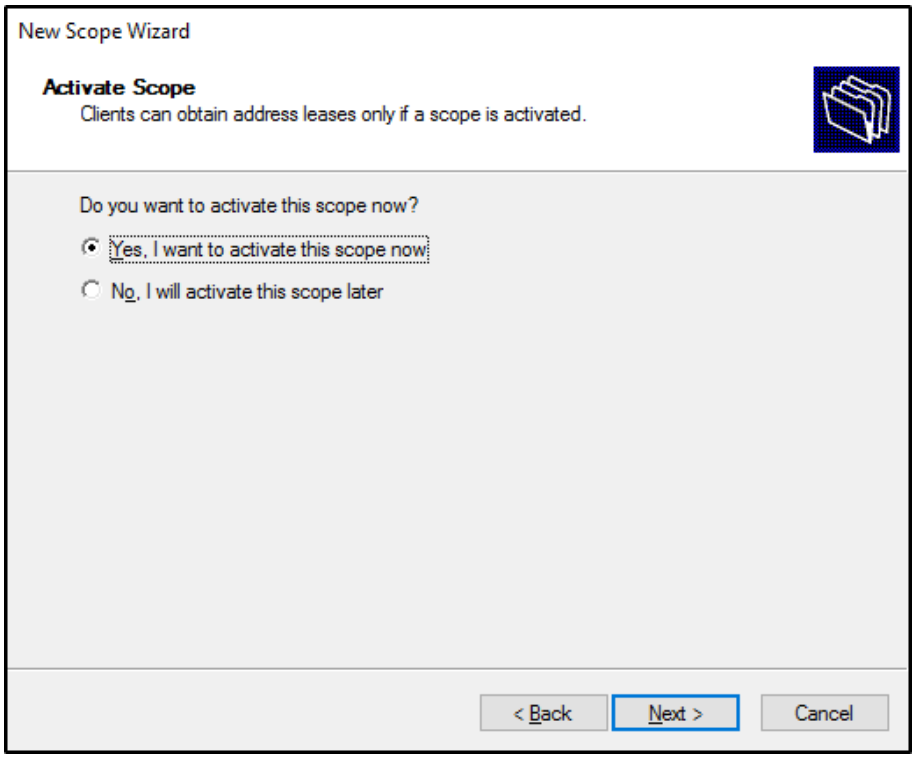
Figur 20: DHCP og DNS - Konfigurasjon

Under **Domain name and DNS Servers,** skriver vi inn *Parent domain* og trykker **Next**.



Figur 21: DHCP og DNS - Konfigurasjon

Under ***Active Scope***, velger vi «Yes, I want to activate this scope now». Trykker **Next.**



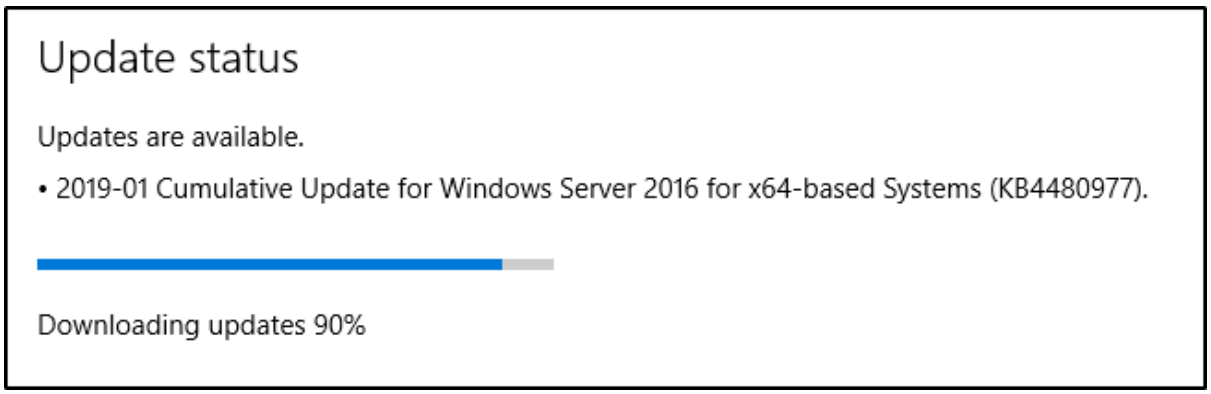
Figur 22: DHCP og DNS - Konfigurasjon

SCCM Forberedelser

Før vi kan starte med installasjonen av SCCM, må vi se til at serveren har det den trenger av nødvendige forutsetninger for å kunne fungere. Det vil si at det som gjøres videre fremover til SCCM blir installert skal gjøres på samme server som SCCM skal installeres på, med mindre noe annet blir sagt.

Windows Updates

Før vi begynner å installere noe som helst på serveren, velger vi å installere Windows oppdateringer, slik at vi unngår eventuelle problemer som kan oppstå på grunn av nyere oppdateringer.

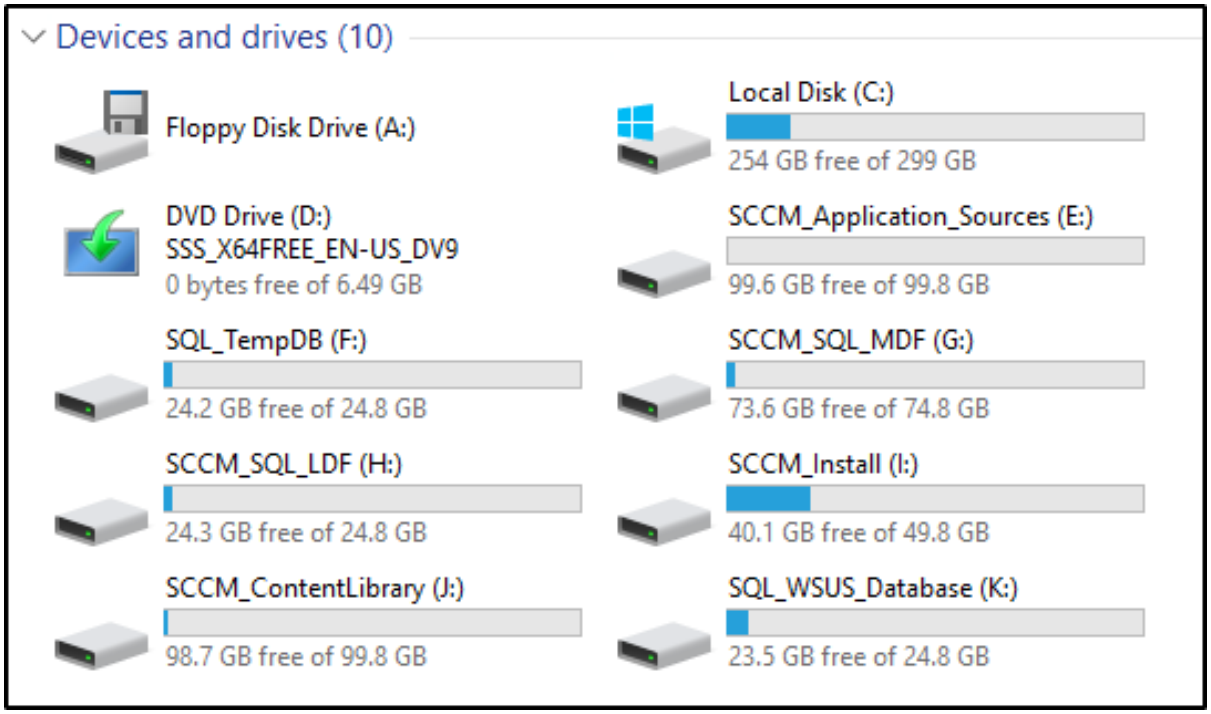


Figur 23: Installasjon av Windows Updates

Disk Oppsett

Vi velger å dele opp disken vår i flere mindre disker, både for å holde god oversikt, samtidig som vi oppnår bedre ytelse. Dette er for så vidt ikke en forutsetning, men heller en god arbeidsvane.

Nedenfor kan vi se hvordan vi har valgt å dele opp diskene.



Figur 24: Oversikt over disker

Script for installasjon av Windows Features

Vi kjører et script for å installere IIS, BITS og RDC som er nødvendig for SCCM. Vi benyttet PowerShell for å gjøre dette.

```
INSTALL-WINDOWSFEATURE WEB-STATIC-CONTENT,WEB-DEFAULT-DOC,WEB-DIR-
BROWSING,WEB-HTTP-ERRORS,WEB-HTTP-REDIRECT,WEB-NET-EXT,WEB-ISAPI-EXT,WEB-
HTTP-LOGGING,WEB-LOG-LIBRARIES,WEB-REQUEST-MONITOR,WEB-HTTP-TRACING,WEB-
WINDOWS-AUTH,WEB-FILTERING,WEB-STAT-COMPRESSION,WEB-MGMT-TOOLS,WEB-MGMT-
COMPAT,WEB-METABASE,WEB-WMI,BITS,RDC
```

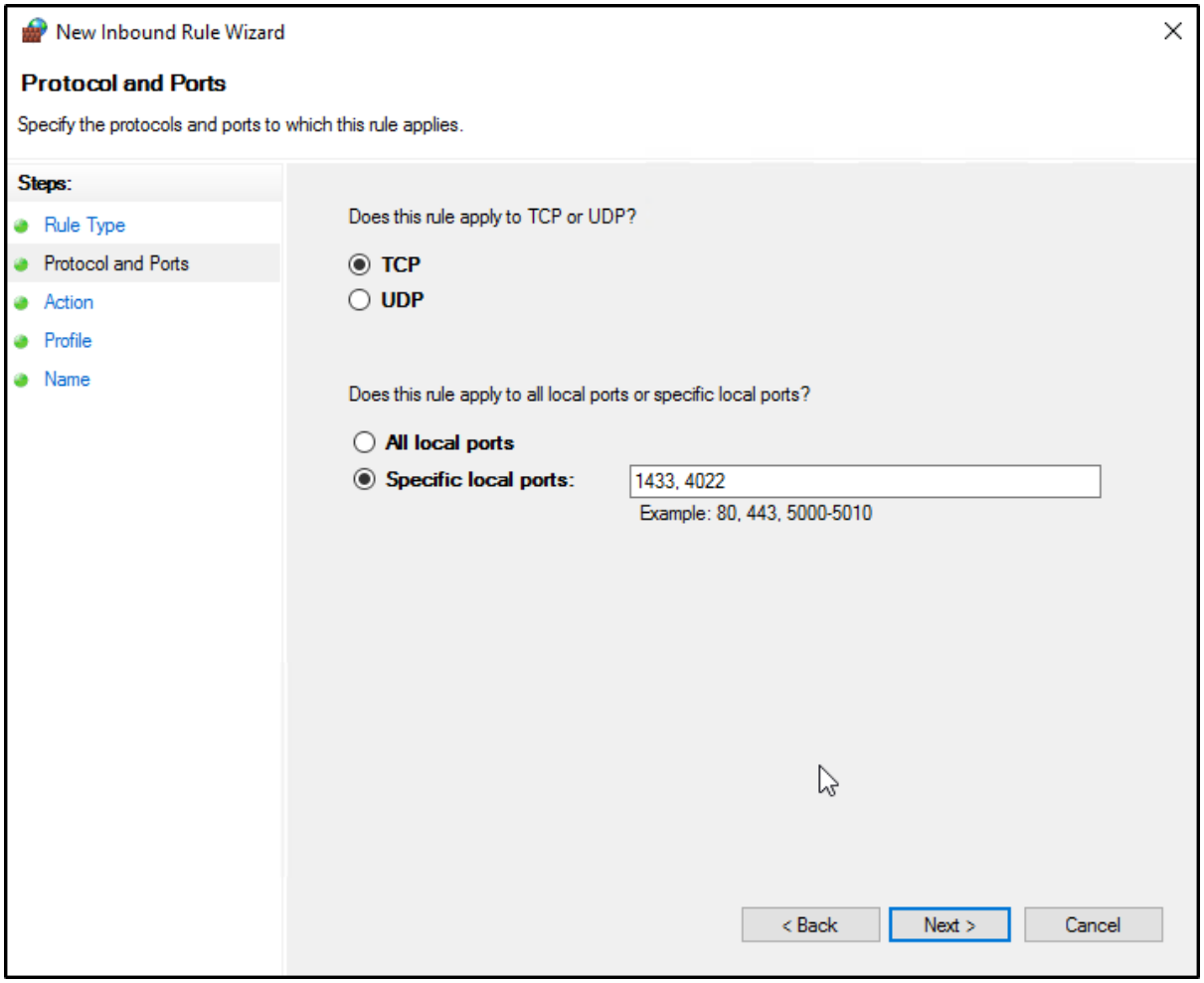
Vi ønsker å kjøre SQL-tjenesten under en domenebruker. Vi skal derfor lage oss et SPN (Service Principal Name) i Active Directory, for service-brukeren som vi skal kjøre SQL-tjenesten under. Vi benyttet CMD for å utføre denne operasjonen. Nedenfor ser vi to kommandoer som begge lager en slik SPN.

```
SETSPN -A MSSQLSVC/SCCM3:1433 CONTOSO\SCCM_SQL
SETSPN -A MSSQLSVC/SCCM3.ALARMNETT.NO:1433 CONTOSO\SCCM_SQL
```

Setter brannmurinnstillinger

Vi skal nå se på hvordan vi setter brannmurinnstillingene. Vi setter disse slik at portene til SQL-serveren er åpne.

På bildet nedenfor under ***Protocol and Ports,*** kan vi se at vi setter en ny *inbound rule* for port 1433 og 4022.



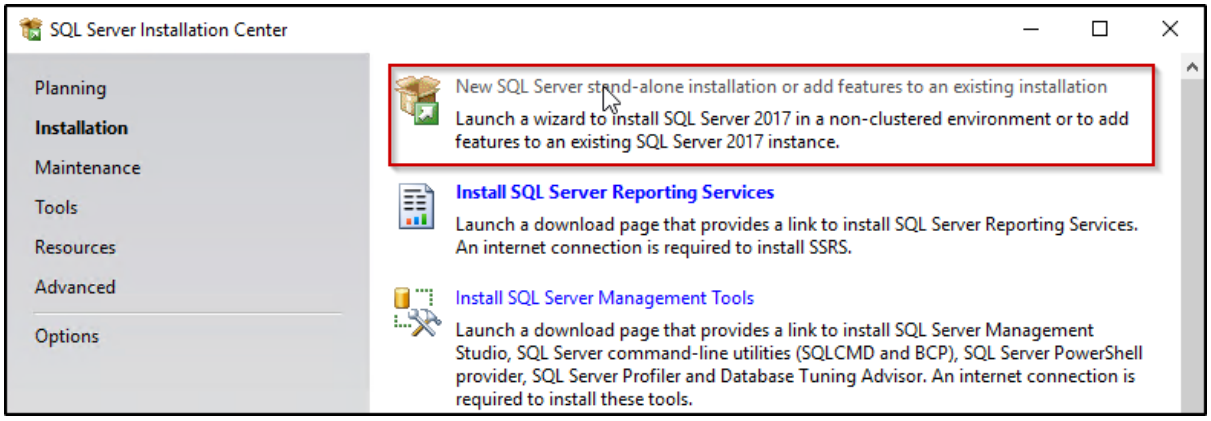
Figur 25: Setter brannmurinnstillinger

Installasjon av SQL Server 2017

Vi starter nå installasjonen av SQL Server 2017. Som også er en annen viktig forutsetning for å installere SCCM.

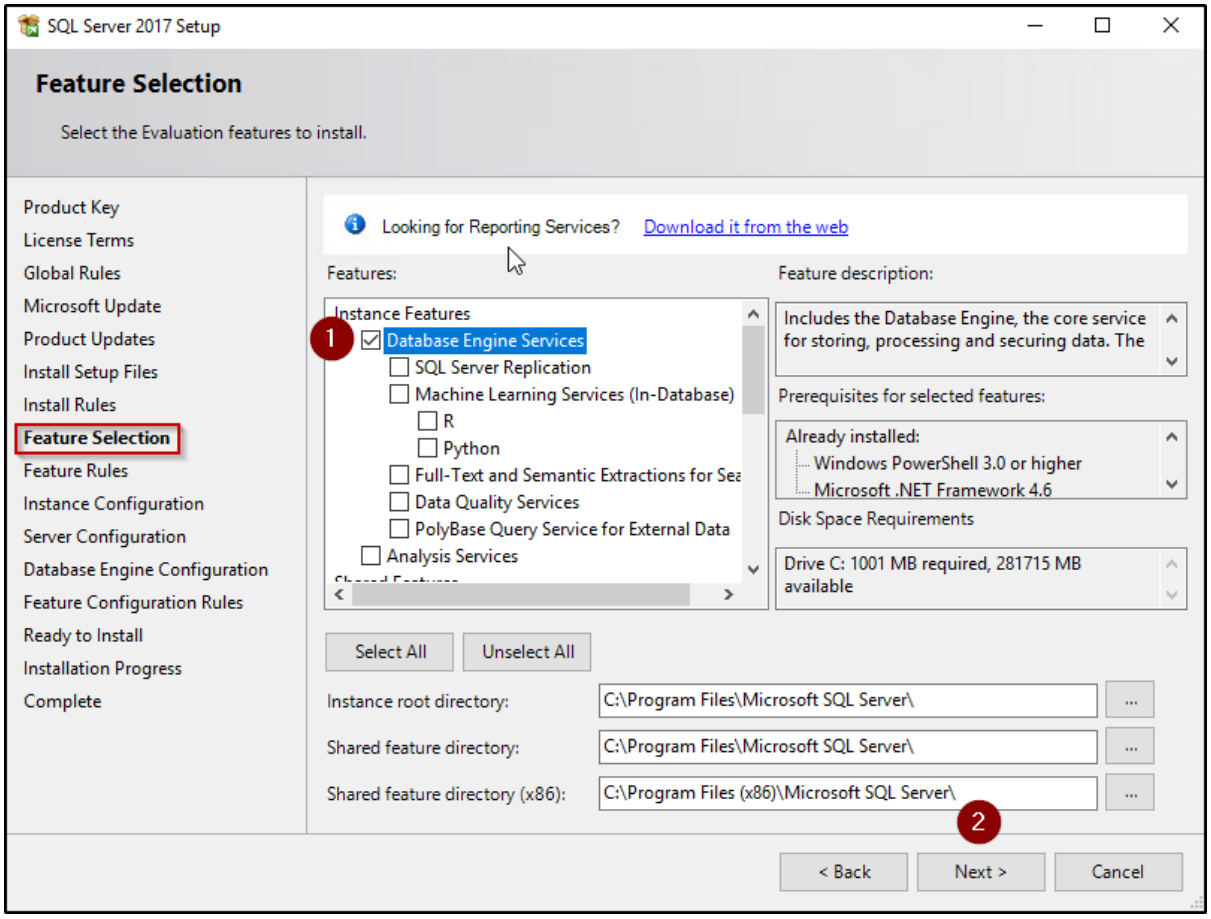
NB: Om man i ettertid finner ut at man har installert SQL feil er det lettere å bare installere hele programmet på nytt i motsetning til å feilsøke og rette opp problemet.

Vi starter opp installasjonsfilen og navigerer oss til ***Installation***, her velger vi å opprette en ny stand-alone SQL Server.



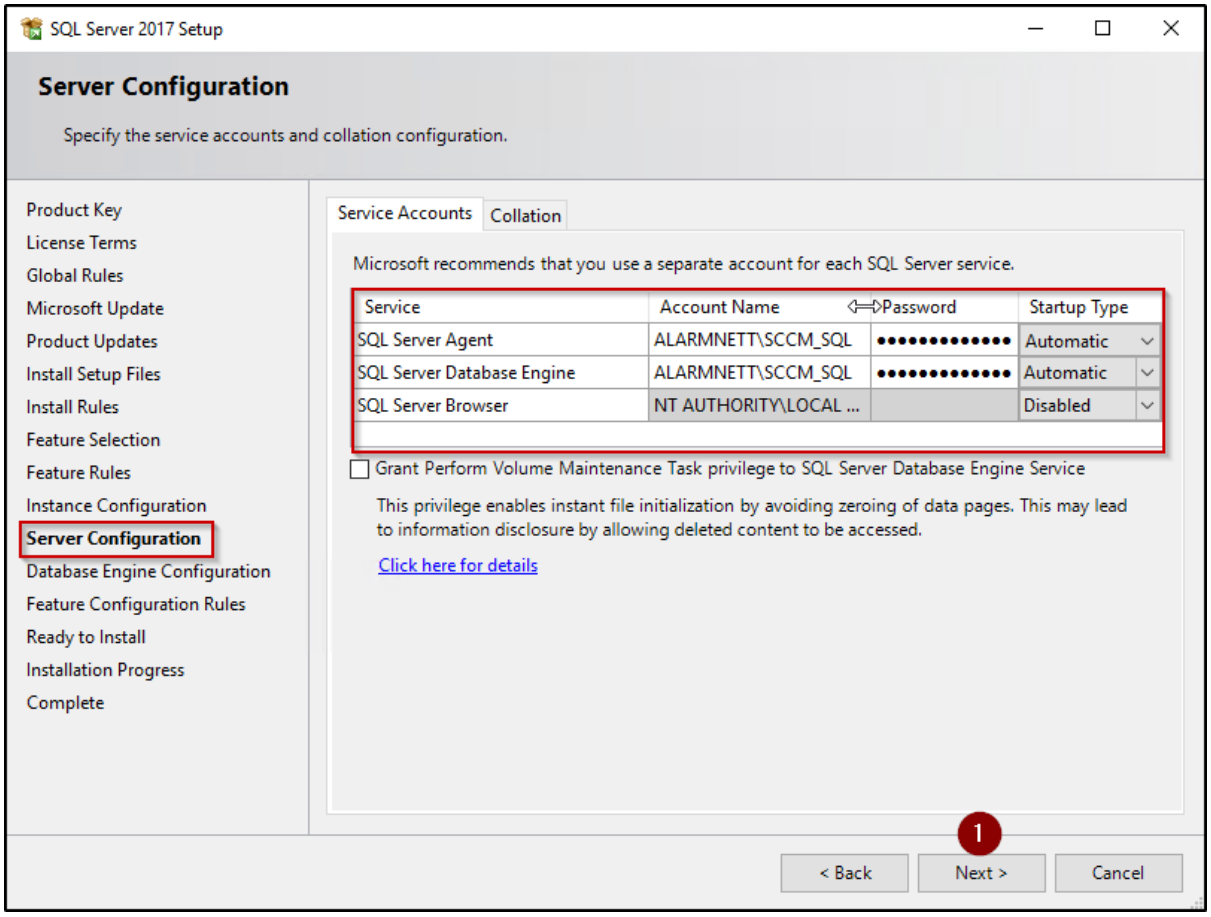
Figur 26: SQL Server 2017 - Installasjon

Under ***Feature Selection***, ville vi vanligvis valgt flere funksjoner som skal installeres, men på grunn av at vi kjører SQL Server 2017, så kommer ikke alle disse tjenestene med i denne installasjonspakken. Vi velger derfor kun **Database Engine Services**, og kommer tilbake de andre tjenestene senere.



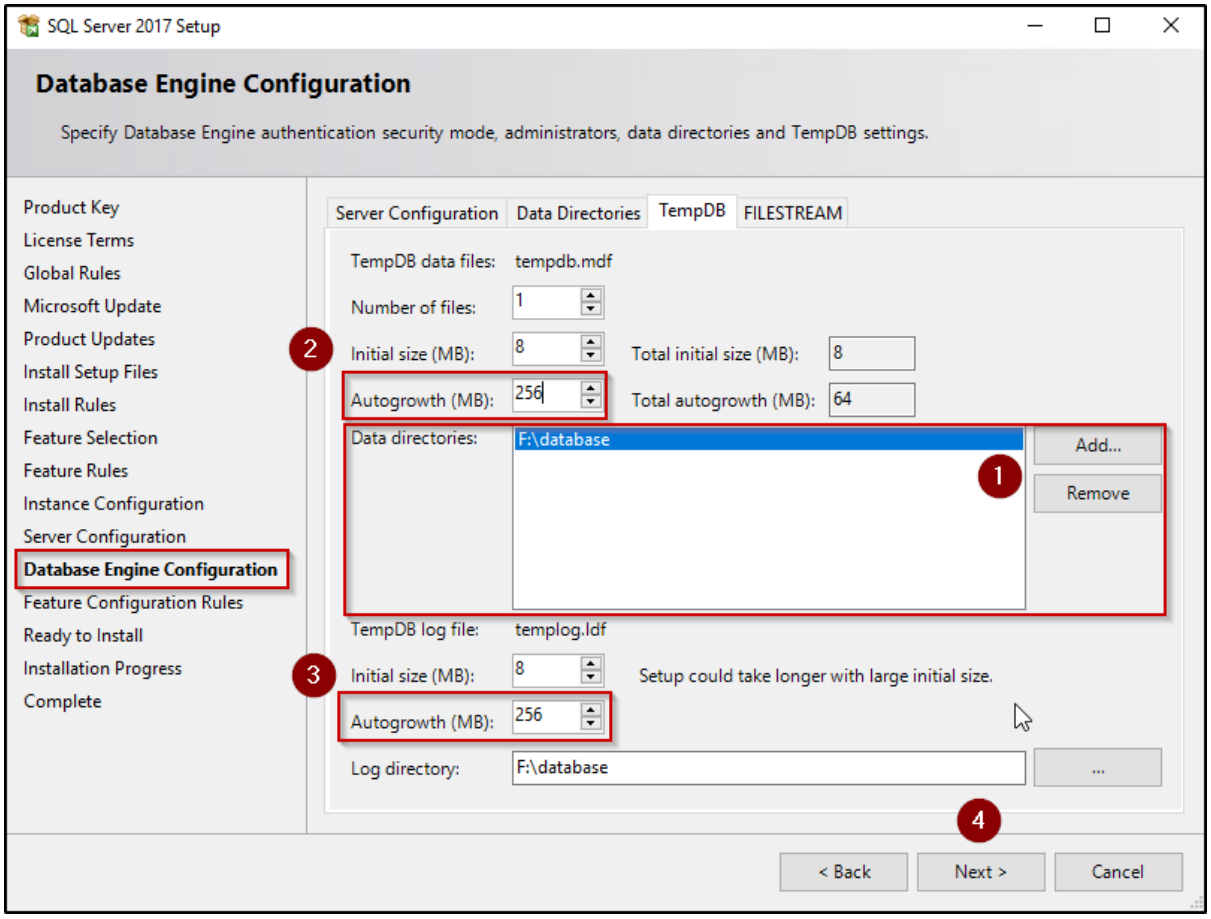
Figur 27: SQL Server 2017 - Installasjon

Under ***Server Configuration***, setter vi våre service-accounts. Det er her snakk om SPN-ene som vi opprettet med CMD tidligere.



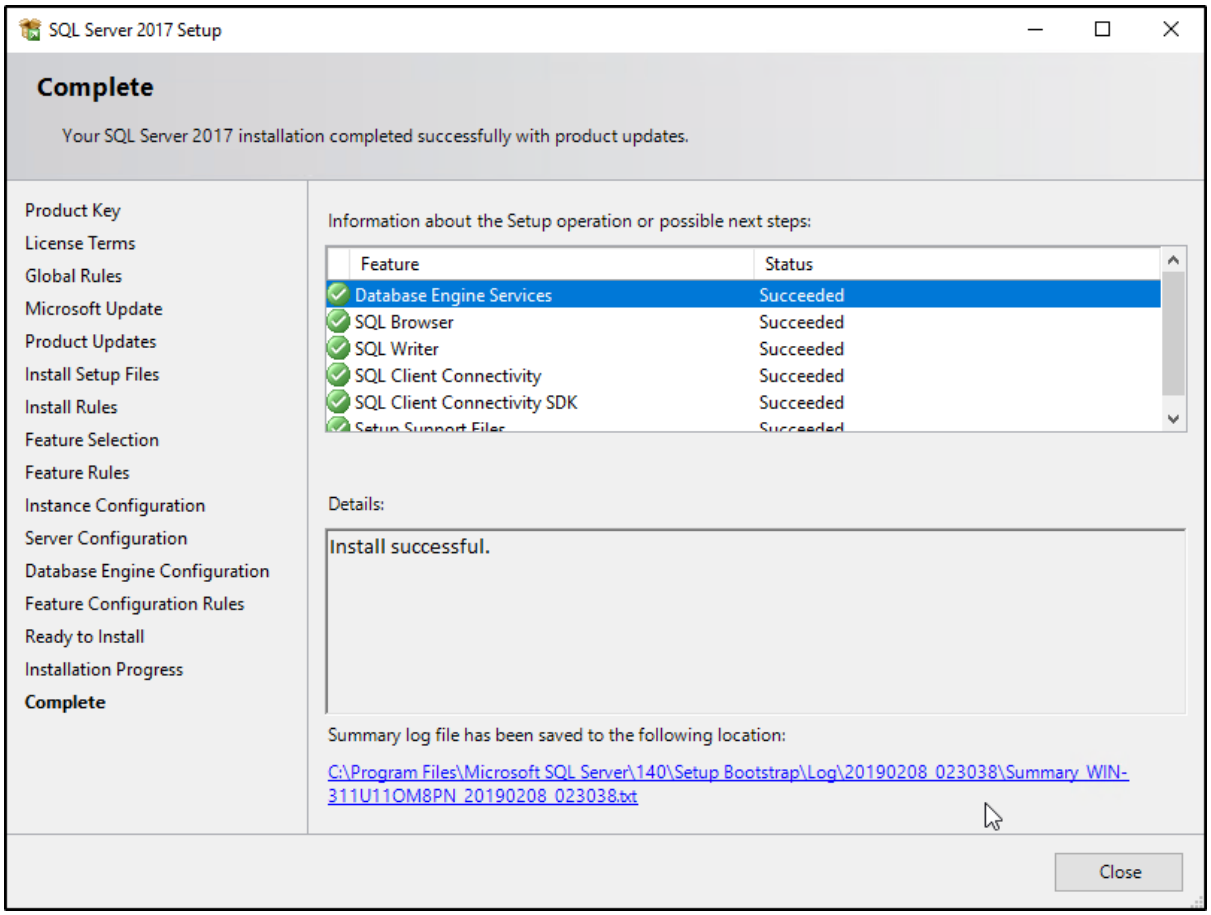
Figur 28: SQL Server 2017 - Installasjon

Under ***Database Engine Configuration***, vil vi nå se at vi benytter oss av at vi har opprettet flere disker til forskjellige gjøremål. Vi velger derfor å ta i bruk F-disken til dette gjøremålet. Vi setter også *autogrowth* til passende størrelse. (Autogrowth bestemmer hvor mye lagring databasen skal utvide seg med dersom den blir full).



Figur 29: SQL Server 2017 - Installasjon

Installasjonen av SQL Server 2017 er gjennomført.



Figur 30: SQL Server 2017 - Installasjon

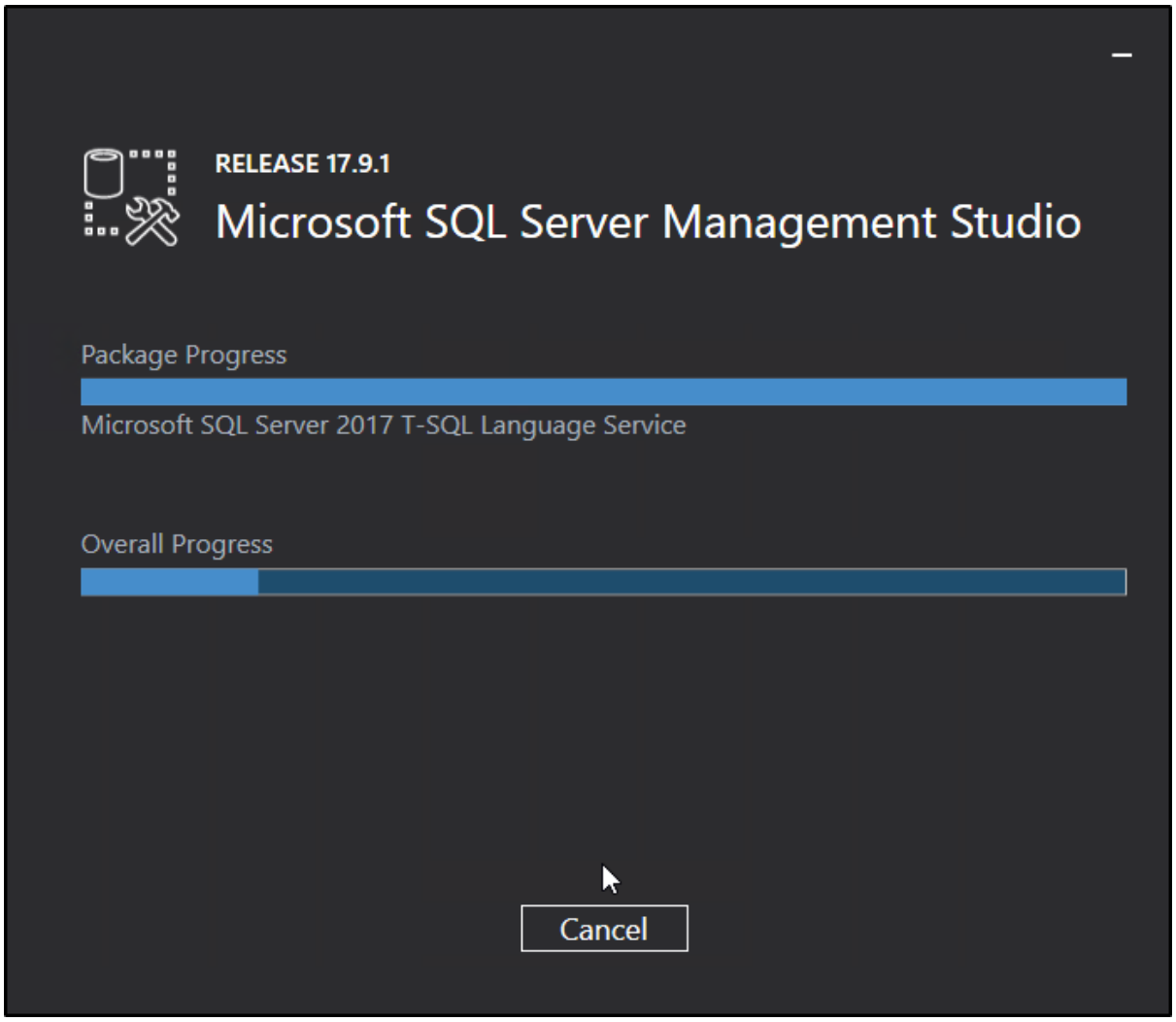
Installasjon av SQL Server 2017 Reporting Services

Tidligere ble det nevnt at vi skulle legge til noen tilleggstjenester som ikke kom med i den nyere installasjonspakken av SQL Server 2017. MS SQL Server 2017 Reporting Services, er en av disse. Denne installeres som vist nedenfor. Samme vil gjelde for SQL Server Management Studio, som følger etter denne installasjonen. Når installasjonen av SQL Server 2017 Reporting Services er fullført, går vi inn i programmet og setter min/max memory usage. Vi setter vår til 8gb.

Figur 31: SQL Server 2017 Reporting Services - Installasjon

Installasjon av SQL Server Management Studio

Vi bruker Management studio, om vi i etterkant av installasjonen skal endre på databasen eller SQL server-innstillingene.

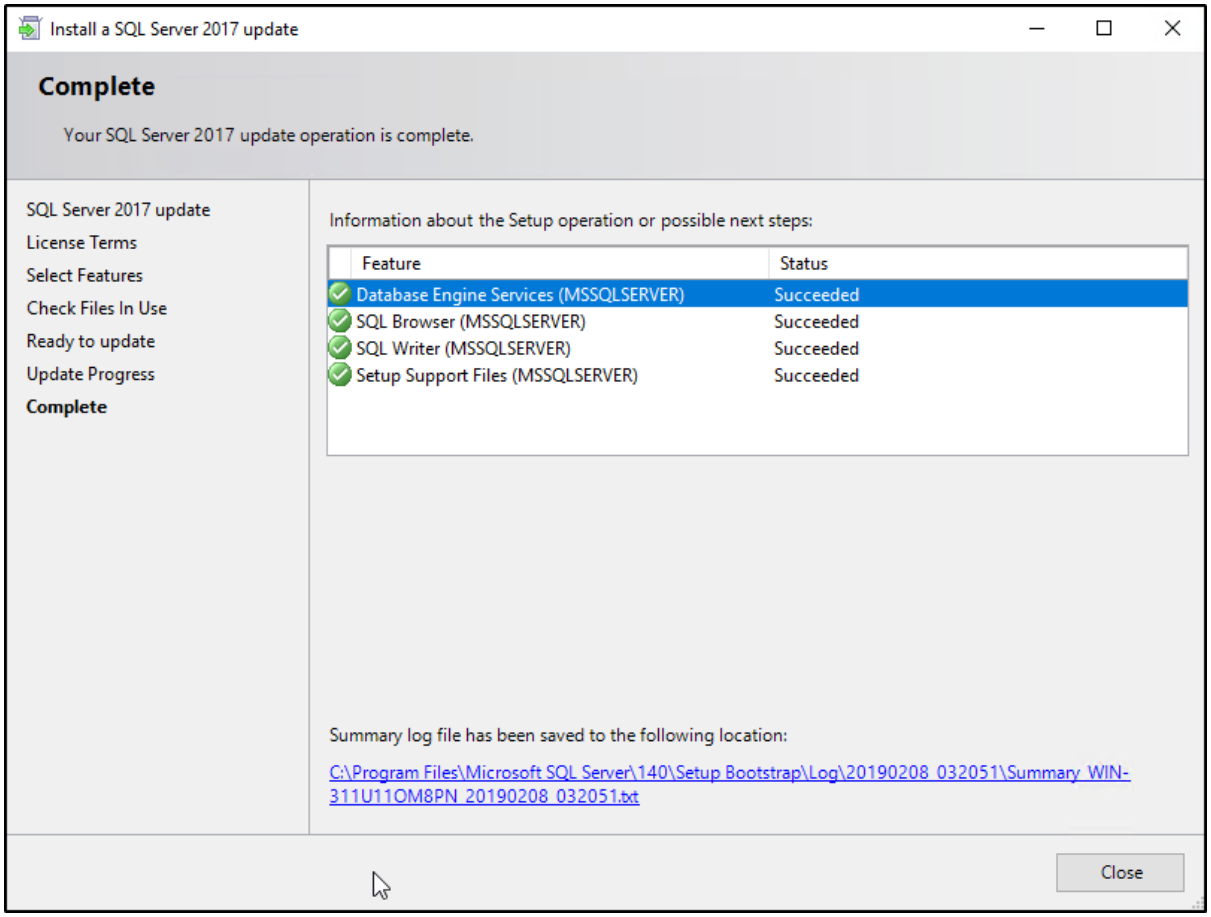


Figur 32: SQL Server Management Studio – Installasjon

Installasjon av Cumulative Updates for SQL Server 2017

Vi utfører Cumulative Updates på vår SQL Server, som inneholder tidligere utgitte oppdateringer fra Windows Updates. Disse oppdateringene vil sammen sikre at vi har en stabil og sikker SQL Server.

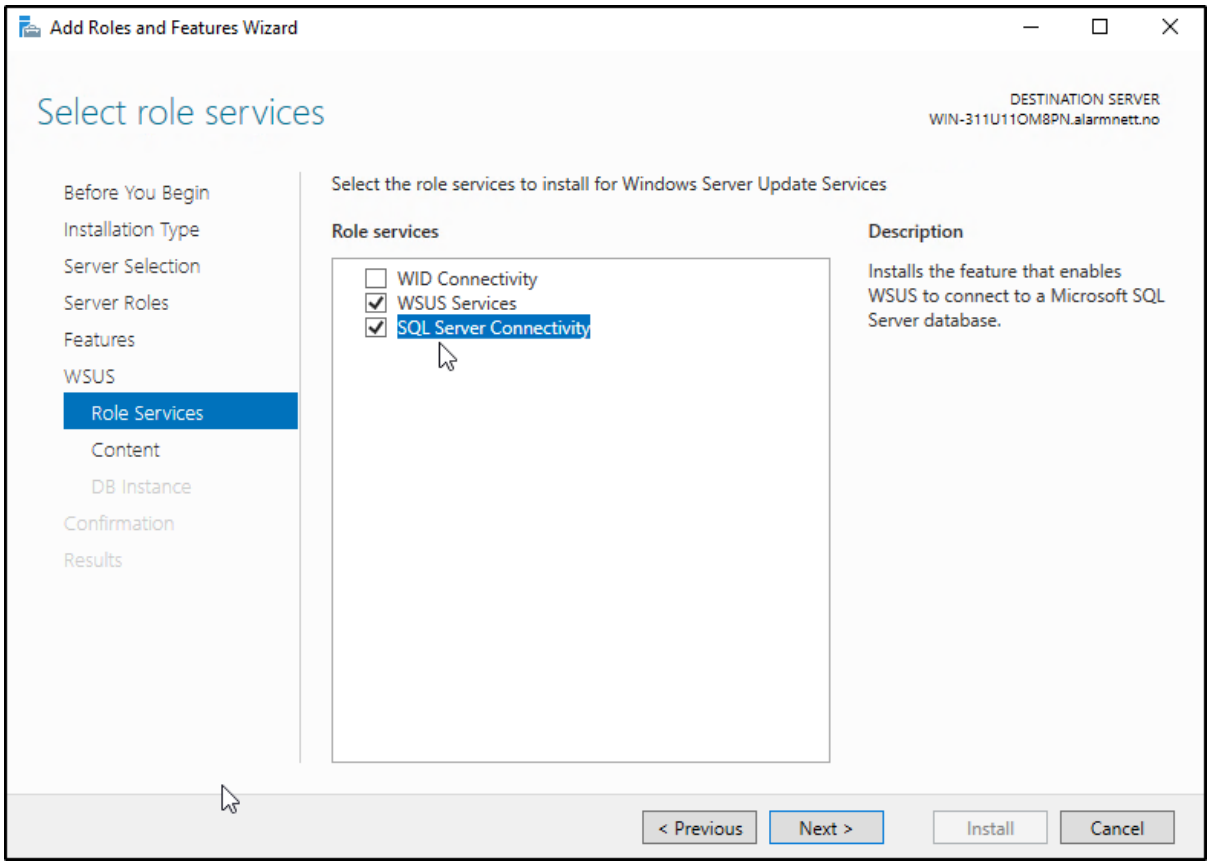
Installerer Cumulative Updates og restarter serveren.



Figur 33: Installasjon av Cumulative Updates for SQL Server 2017

Installasjon av WSUS (Windows Server Update Services)

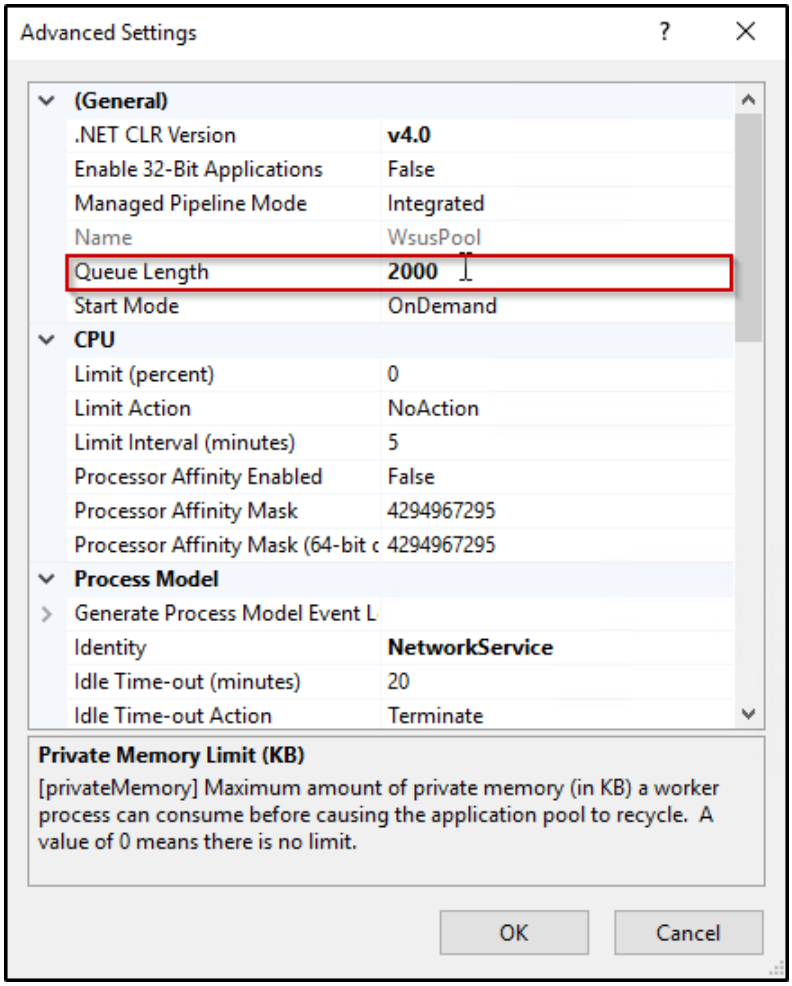
Installerer WSUS slik at vi kan benytte software updates i Configuration Manager. Etter installasjonen, kjøres Post-installation Task, som faktisk installerer databasen og det vi trenger for å ta den i bruk.



Figur 34: Legge til rollen WSUS

Sette «Kø-lengde» Queue Length i IIS (Internet Information Services)

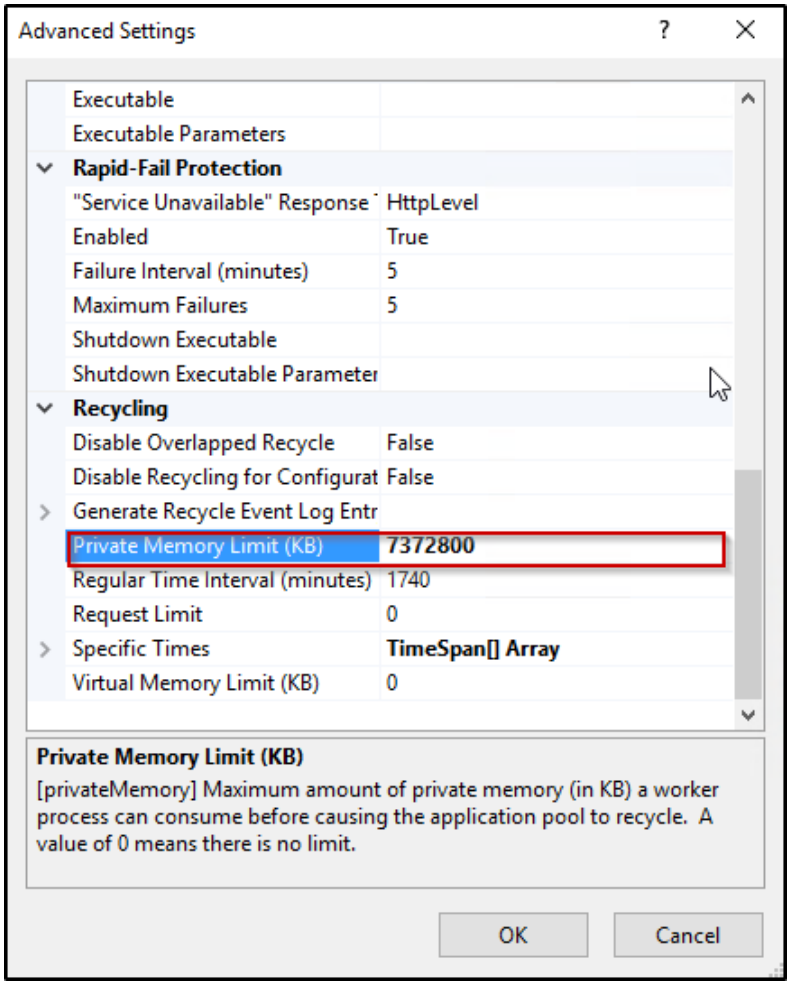
Vi setter vår Queue Length til 2000.



Figur 35: Queue Length

Sette minnegrense i IIS (Internet Information Services)

Videre setter vi minnegrensen i IIS til 7372800.

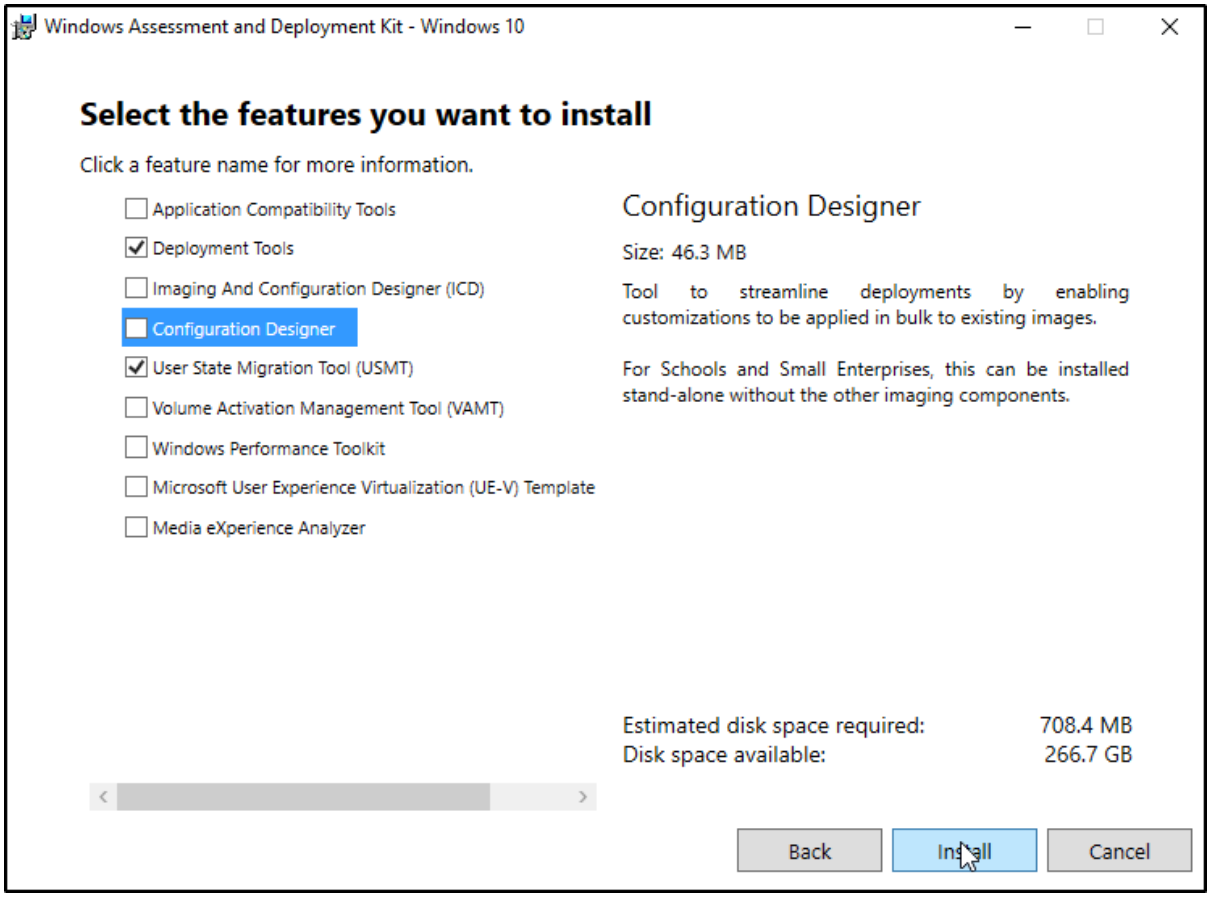


Figur 36: Memory Limit

Installasjon av Windows ADK (Assessment and Deployment Kit)

Windows ADK, er en samling verktøy og teknologier produsert av Microsoft, som er utformet for å hjelpe med å distribuere Windows-operativsystemer til datamaskiner.

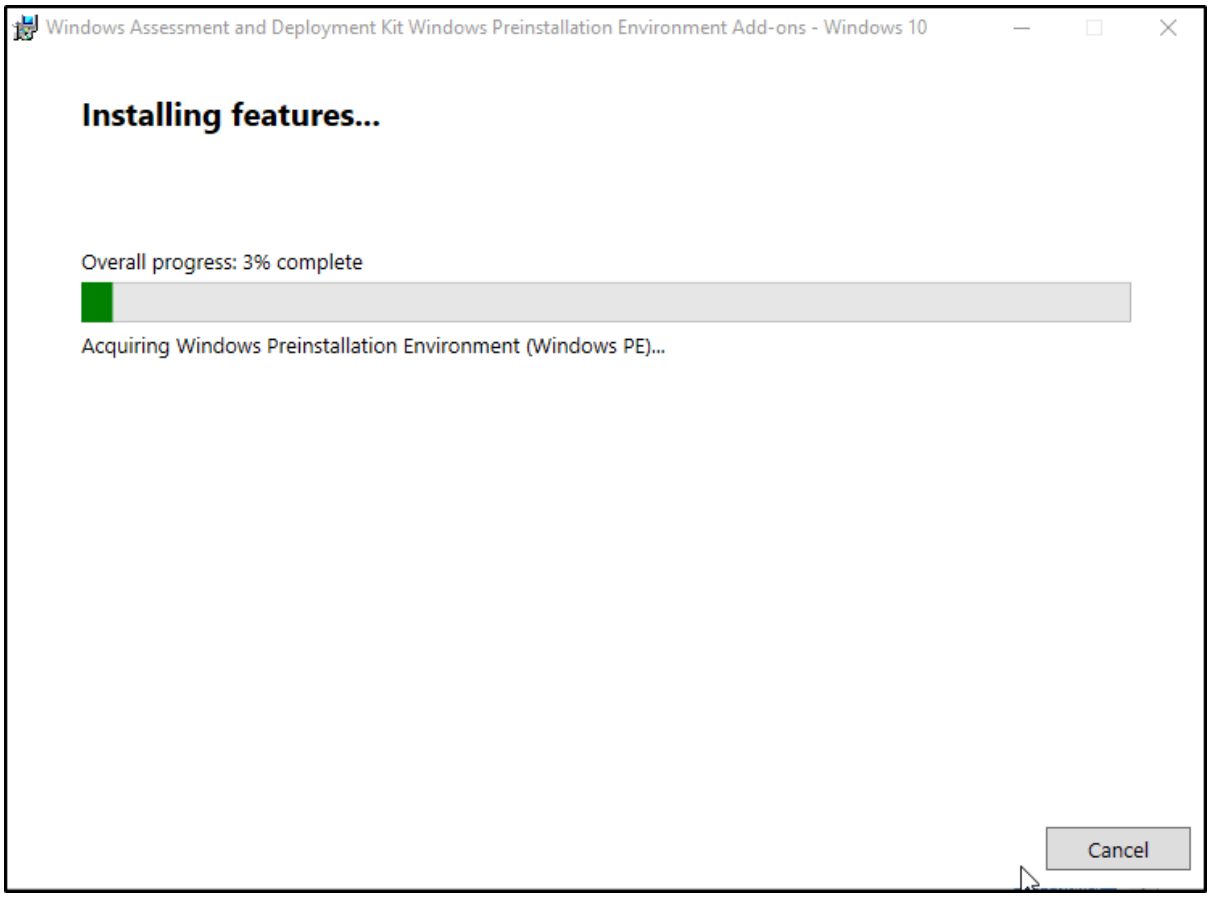
Vi velger **Deployment Tools** og **User State Migration Tool (USMT)**. Deretter trykker vi **Install**.



Figur 37: Windows Assessment and Deployment Kit – Installasjon

Installasjon av Windows ADK Environment Add-ons

Viktig at vi også installerer **«***Windows preinstallation Environment (Windows PE)***».** Denne lastes ned og installeres separat, hvis man bruker en nyeste versjonen av Windows ADK.

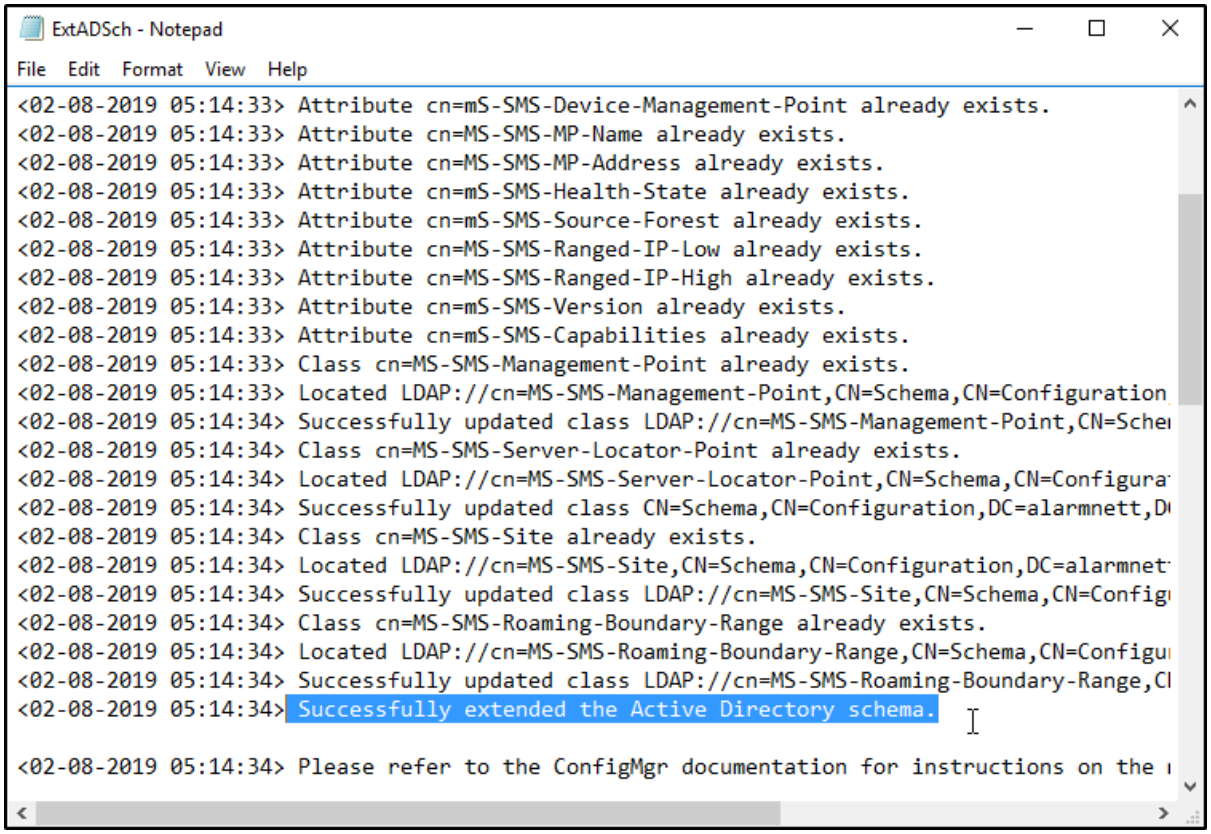


Figur 38: Windows Assessment and Deployment kit Environment Add-ons - Installasjon

Utvidelse av Active Directory Schema

Kjører extadsch.exe, ligger vanligvis under SCCM-setup-files, for å utvide Active Directory Schema.

Vi ser så i loggfilen extadsch.log om Active Directory Schema er utvidet.

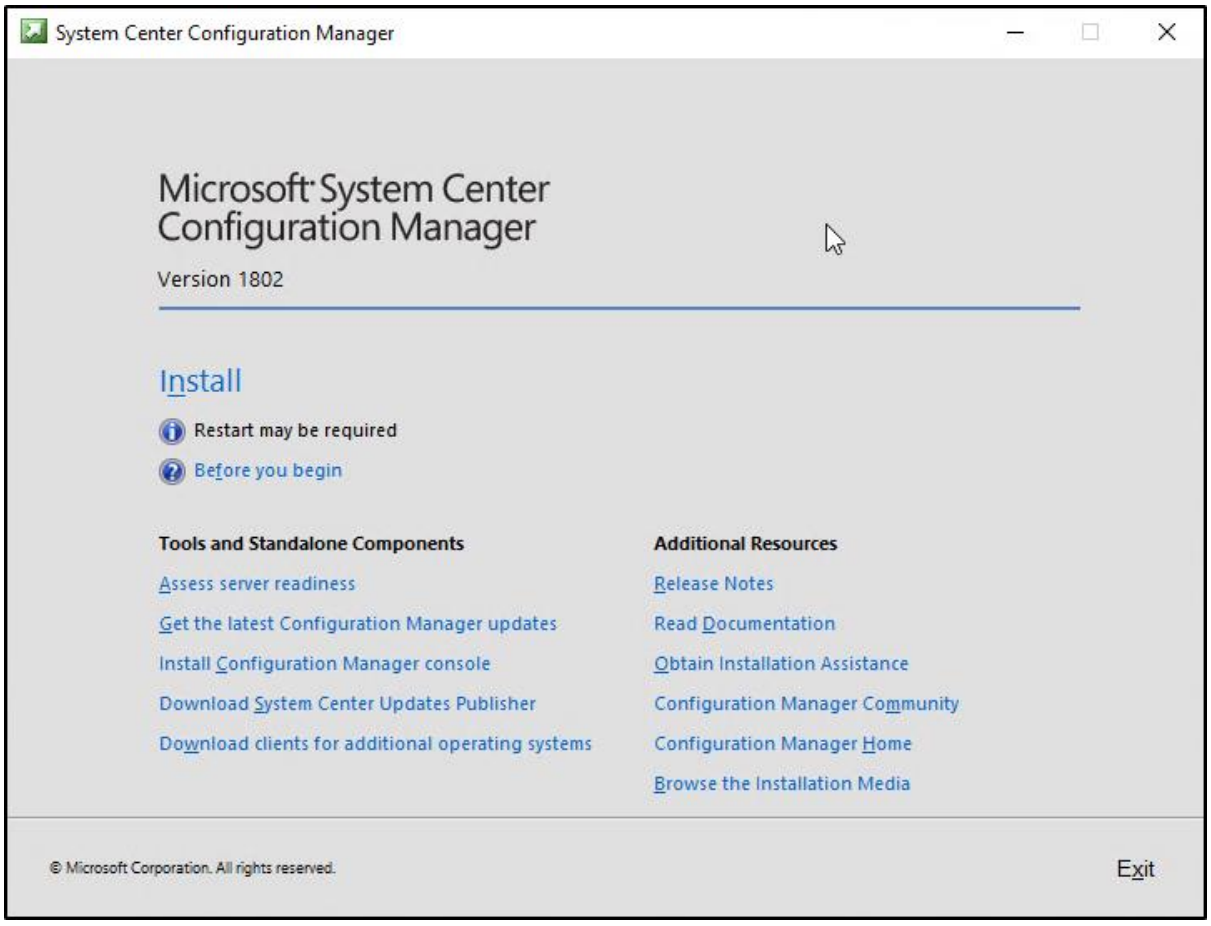


Figur 39: Utvidelse av Active Directory Schema

SCCM Installasjon

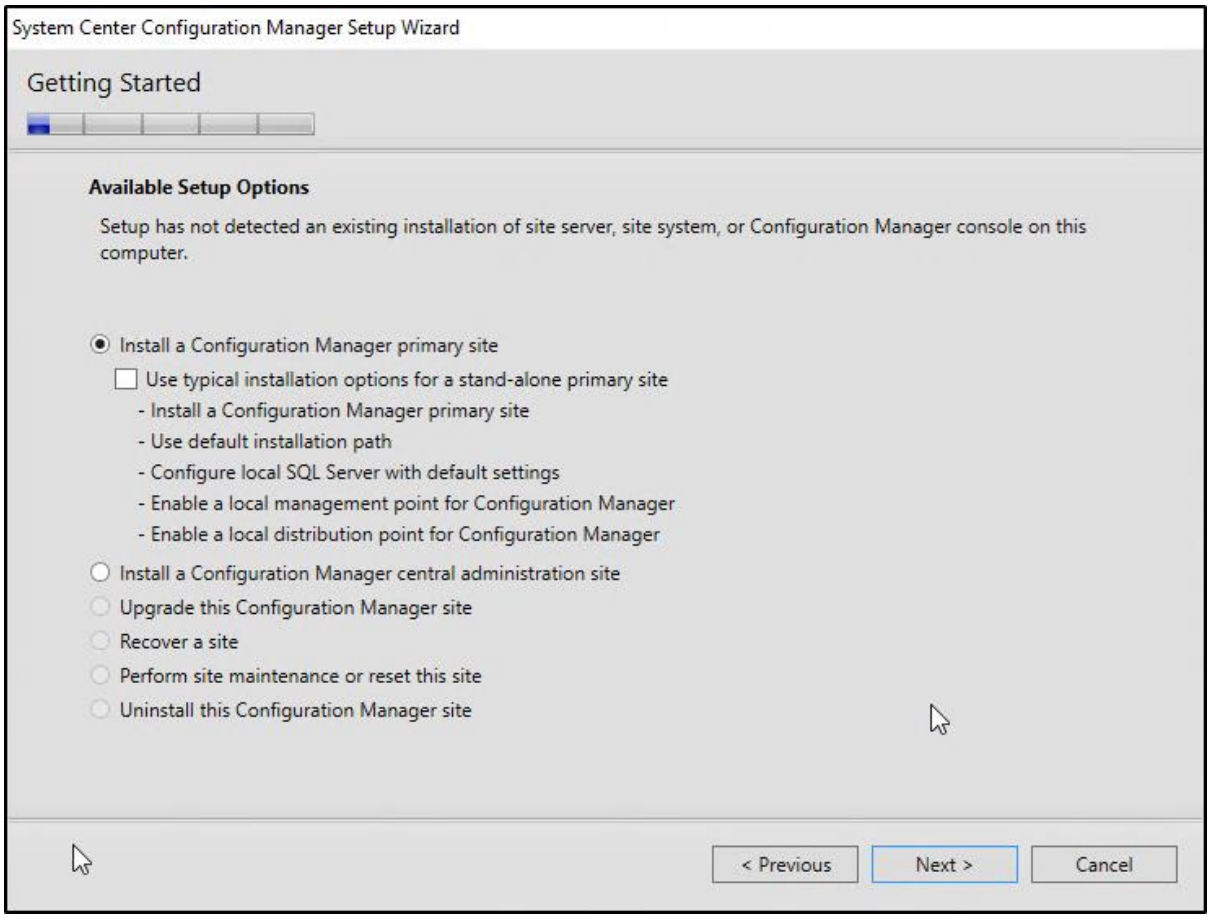
Nå som samtlige forutsetninger er unnagjort, kan vi endelig starte installasjonen av SCCM. Ved å ta i bruk SCCM får man mulighet til å blant annet ta i bruk tjenester for Windows 10 management, In-Console Updates, Application Delivery, Device Management, Endpoint Protection, Software Update Management, Operating System Deployment, Inventory, og mer.

Velger **Install**.



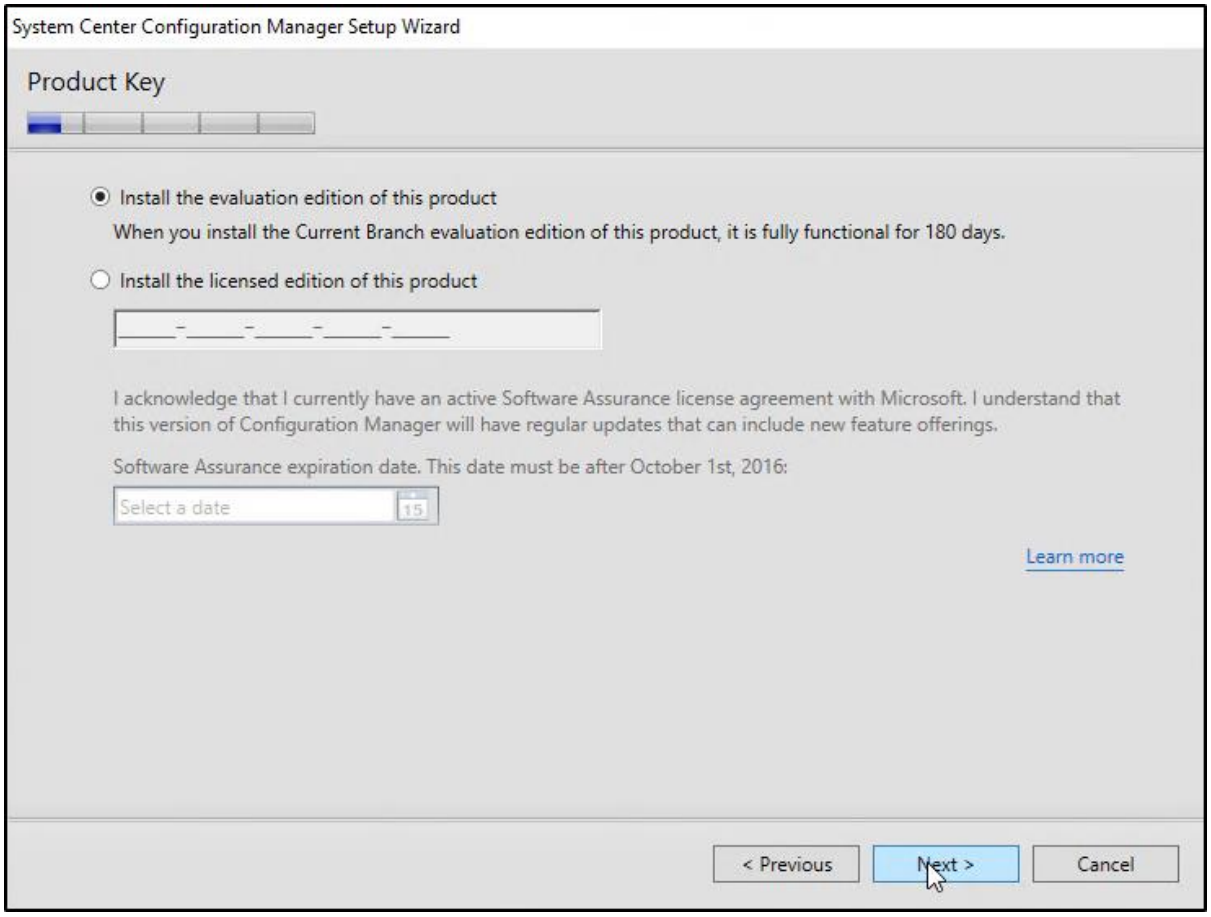
Figur 40: System Center Configuration Manager – Installasjon

Velger her å installere en **Configuration Manager primary site**.



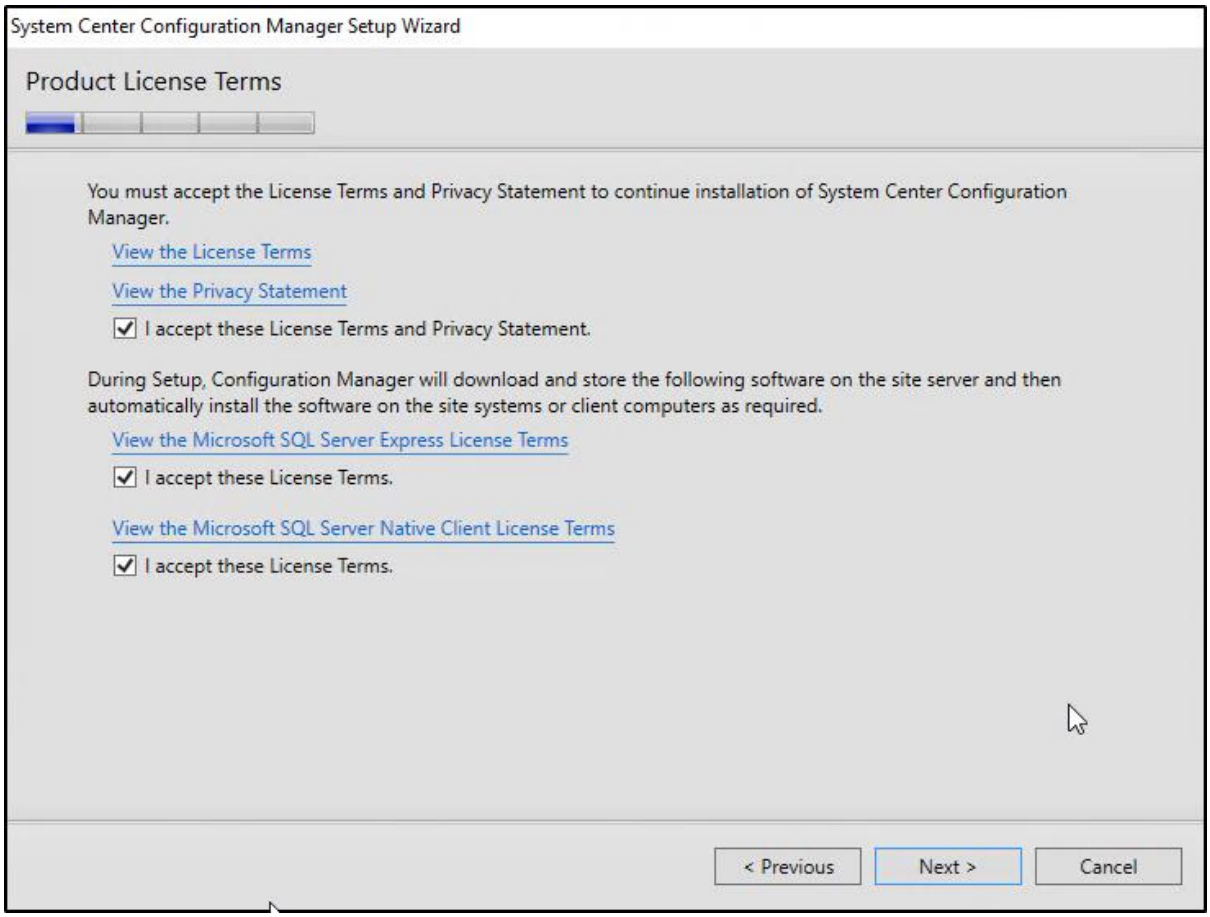
Figur 41: System Center Configuration Manager – Installasjon

Velger her: **Install the evaluation edition of this product**, siden vi ikke har noen product key for SCCM. Deretter trykker vi **Next**.



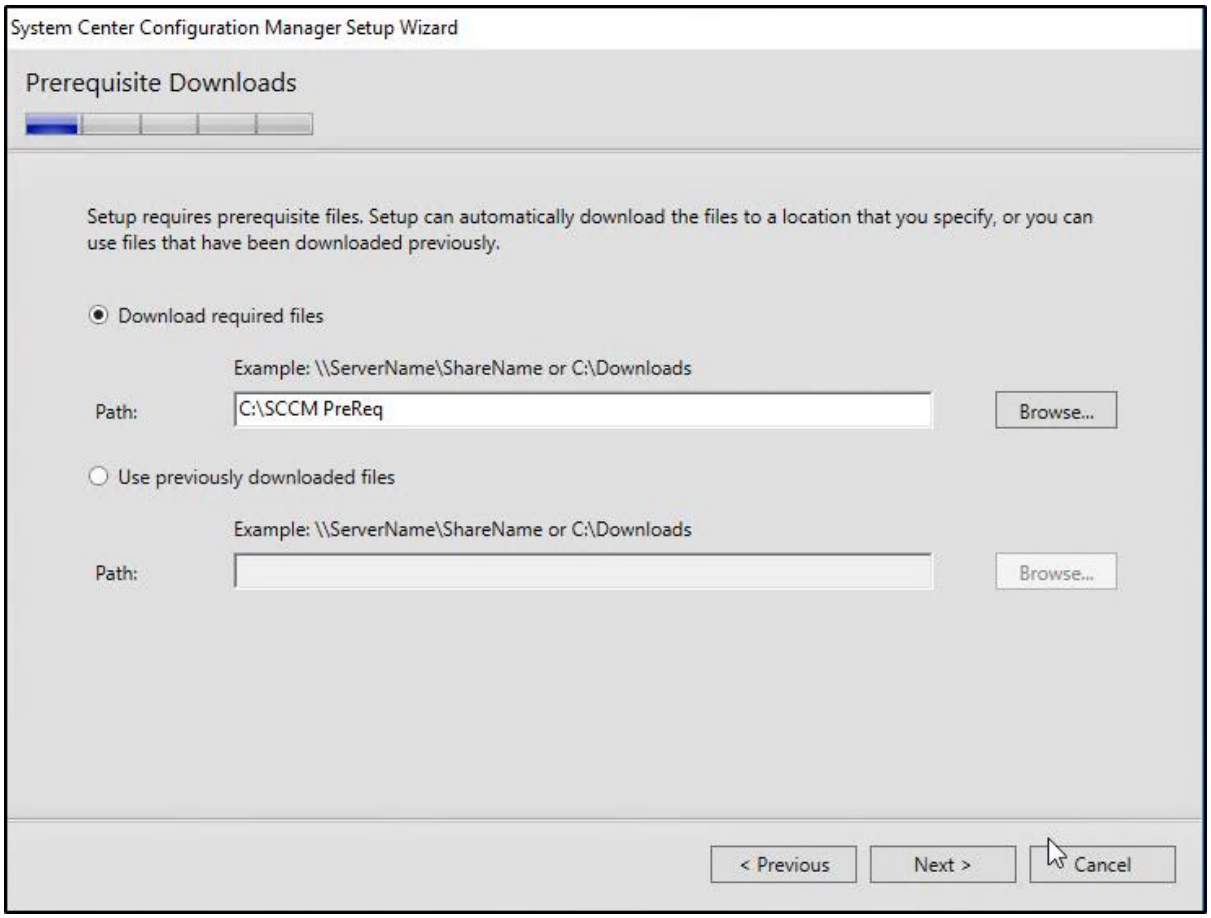
Figur 42: System Center Configuration Manager – Installasjon

Aksepterer vilkårene og trykker **Next.**



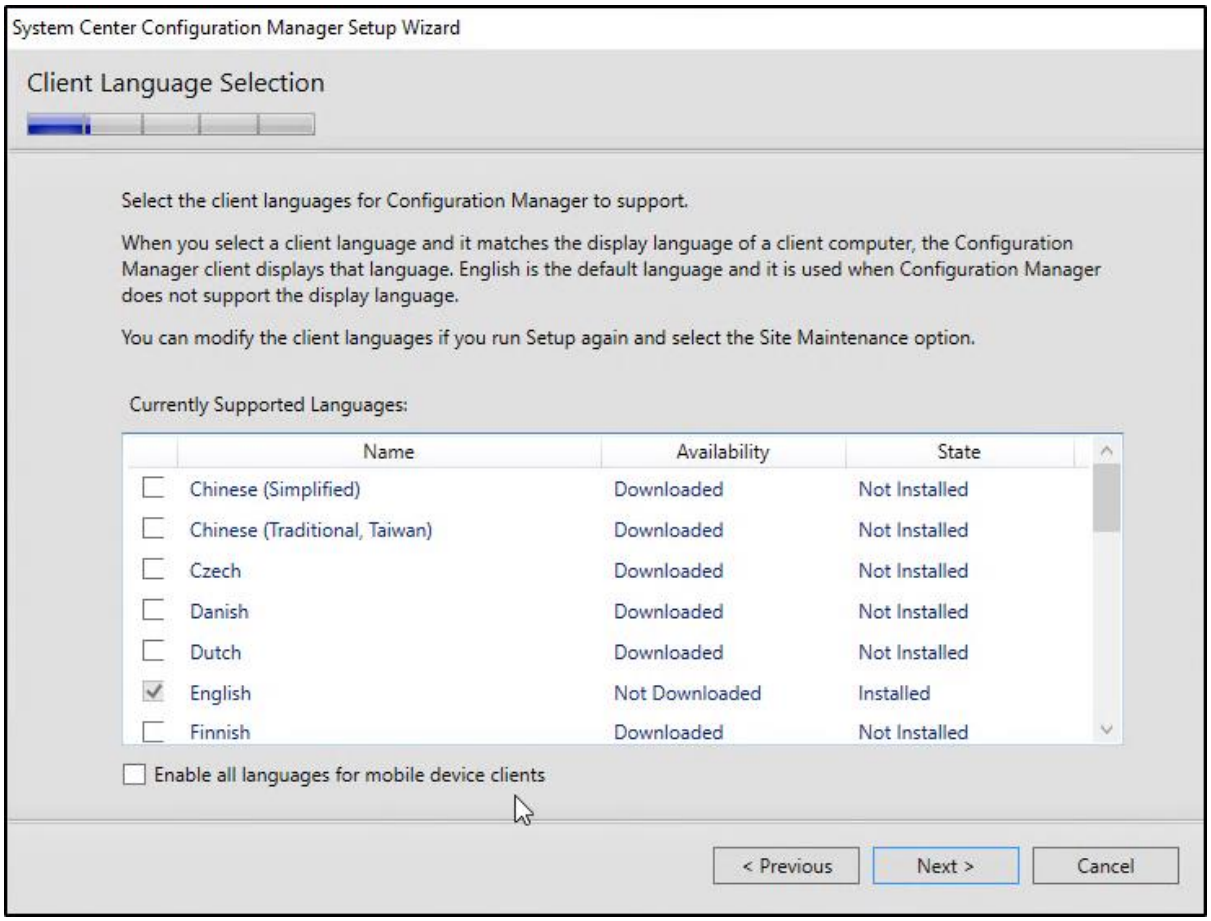
Figur 43: System Center Configuration Manager – Installasjon

Velger å laste ned SCCM PreReq filene til en bestemt path. Trykker deretter **Next.**



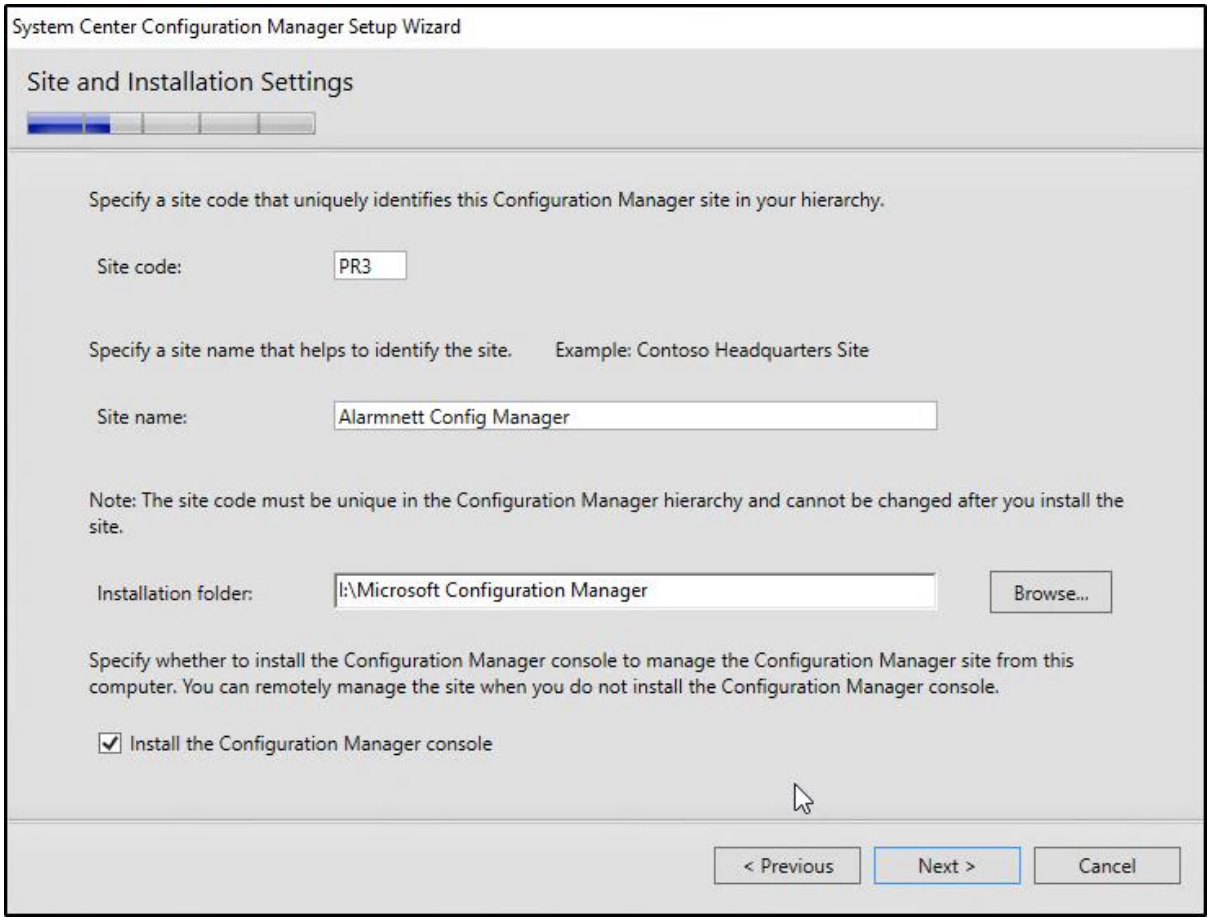
Figur 44: System Center Configuration Manager – Installasjon

Setter språk-innstillinger og trykker **Next.**



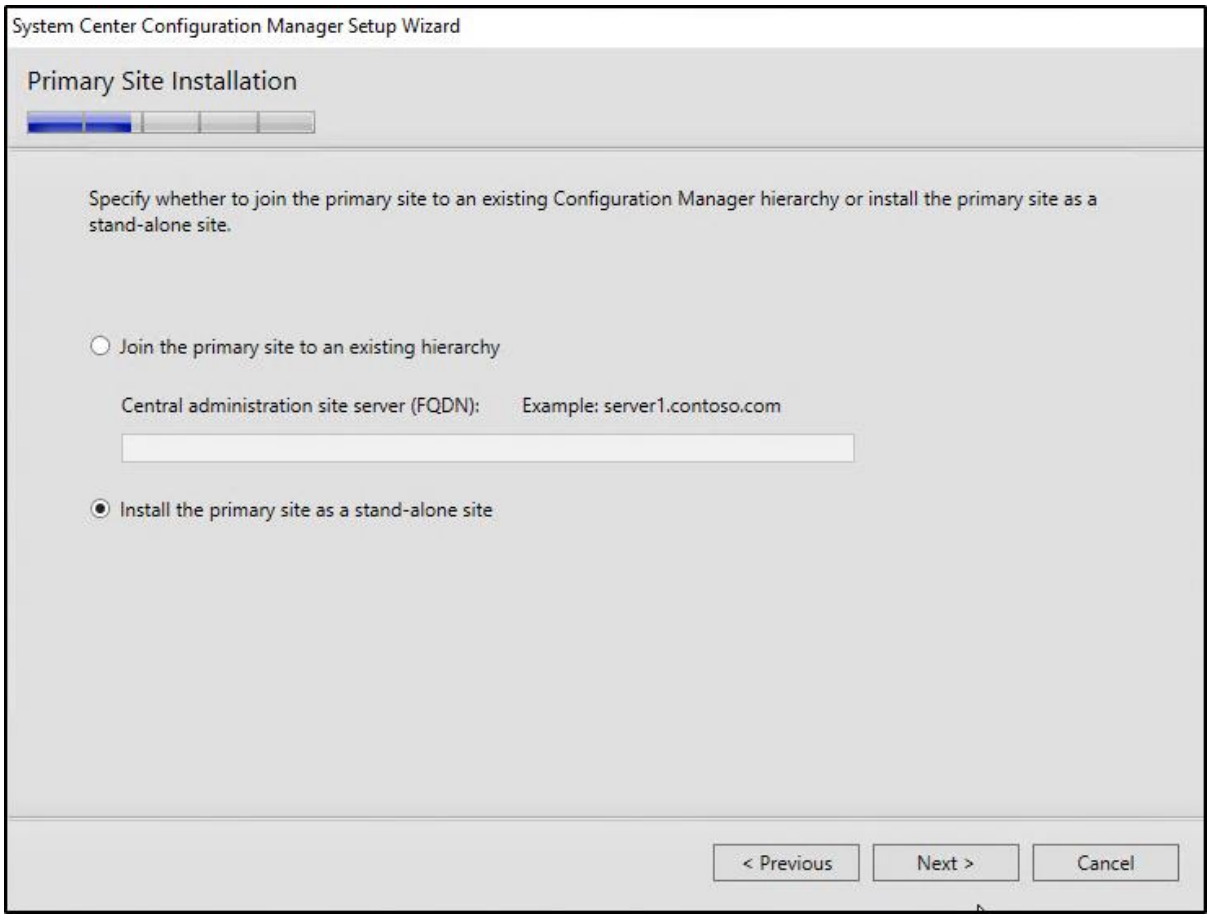
Figur 45: System Center Configuration Manager – Installasjon

Setter vår *site code*, samt gir et *site navn*, en *installasjons path* og velger at vi ønsker å installere Configuration Manager konsollen. Trykker deretter **Next**.



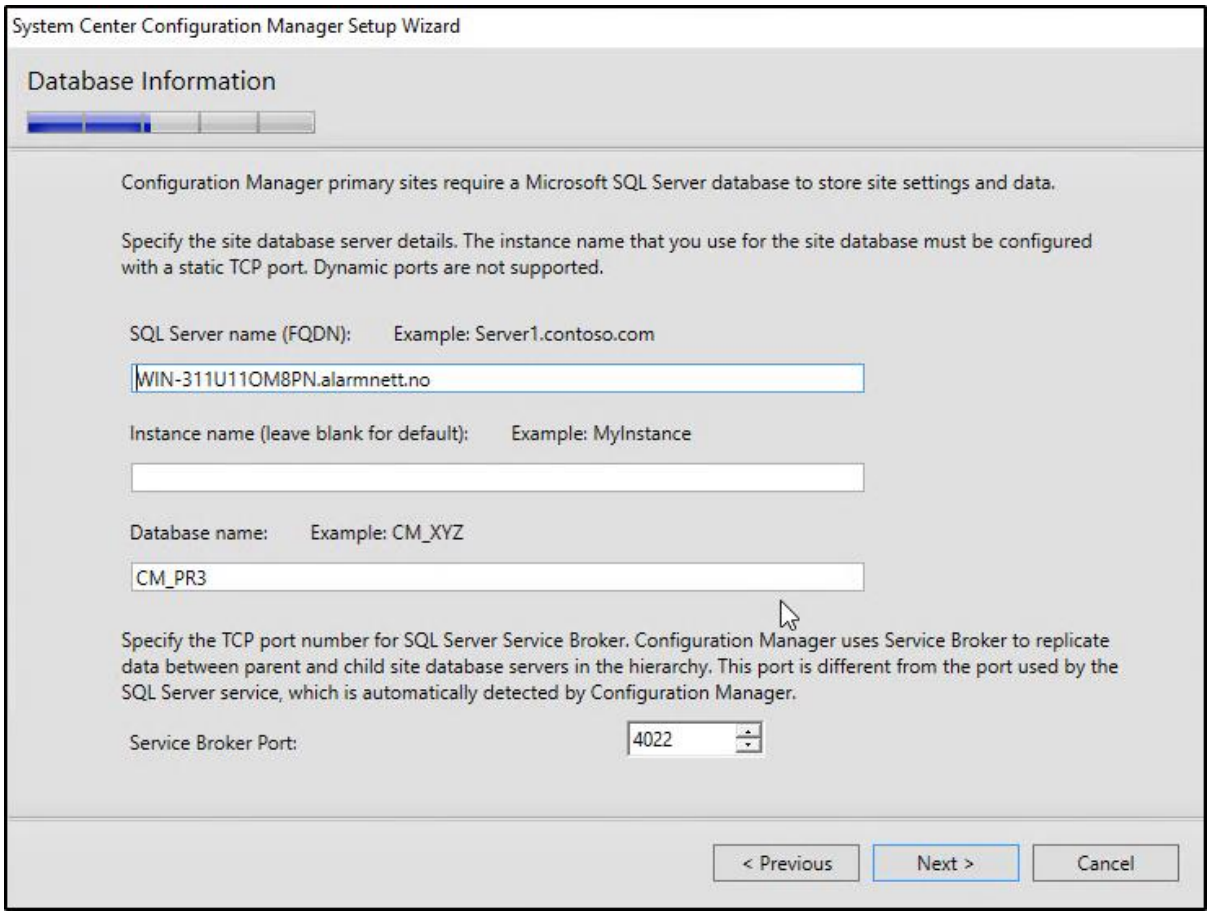
Figur 46: System Center Configuration Manager – Installasjon

Velger at vi ønsker å installere primary site stand-alone site. Trykker **Next**.



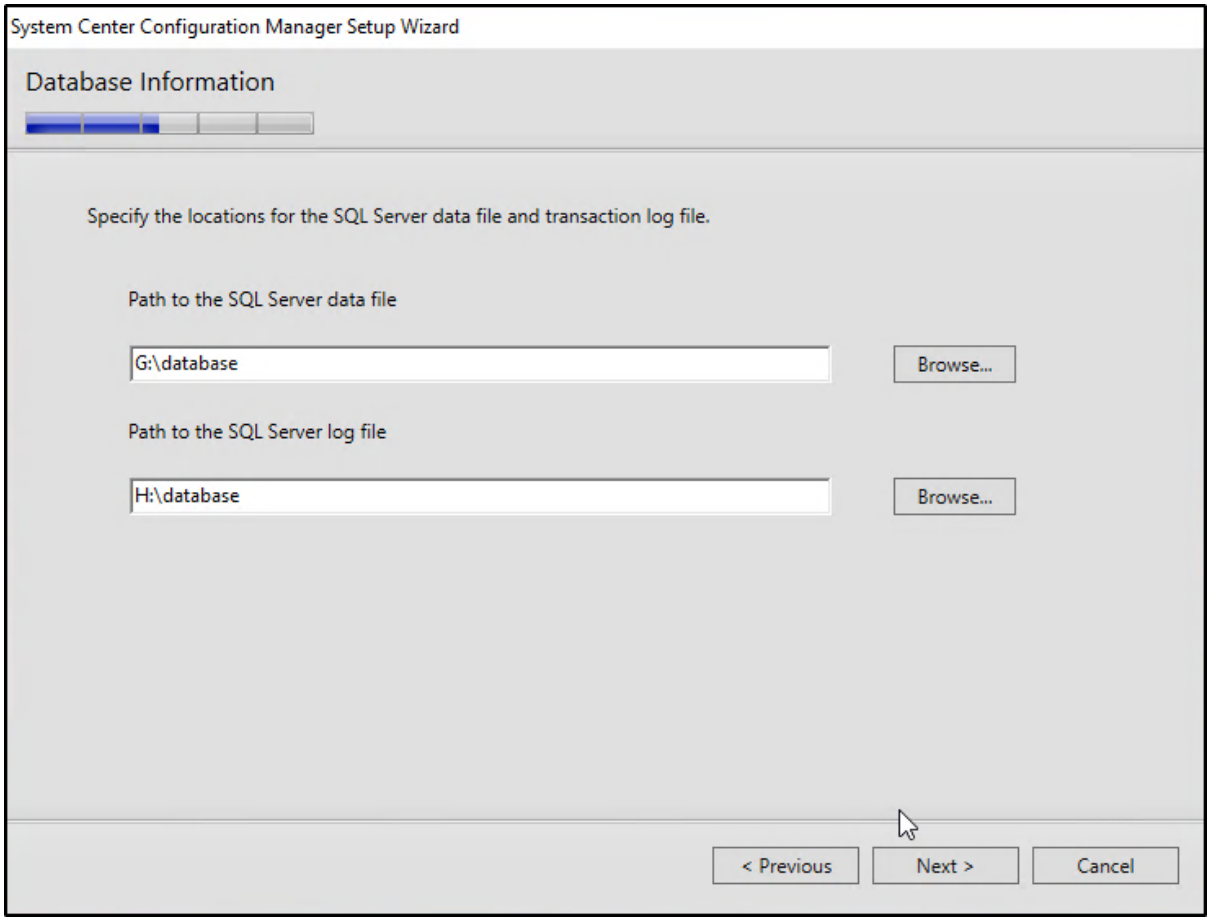
Figur 47: System Center Configuration Manager – Installasjon

Beholder standardinnstillinger og trykker **Next.**



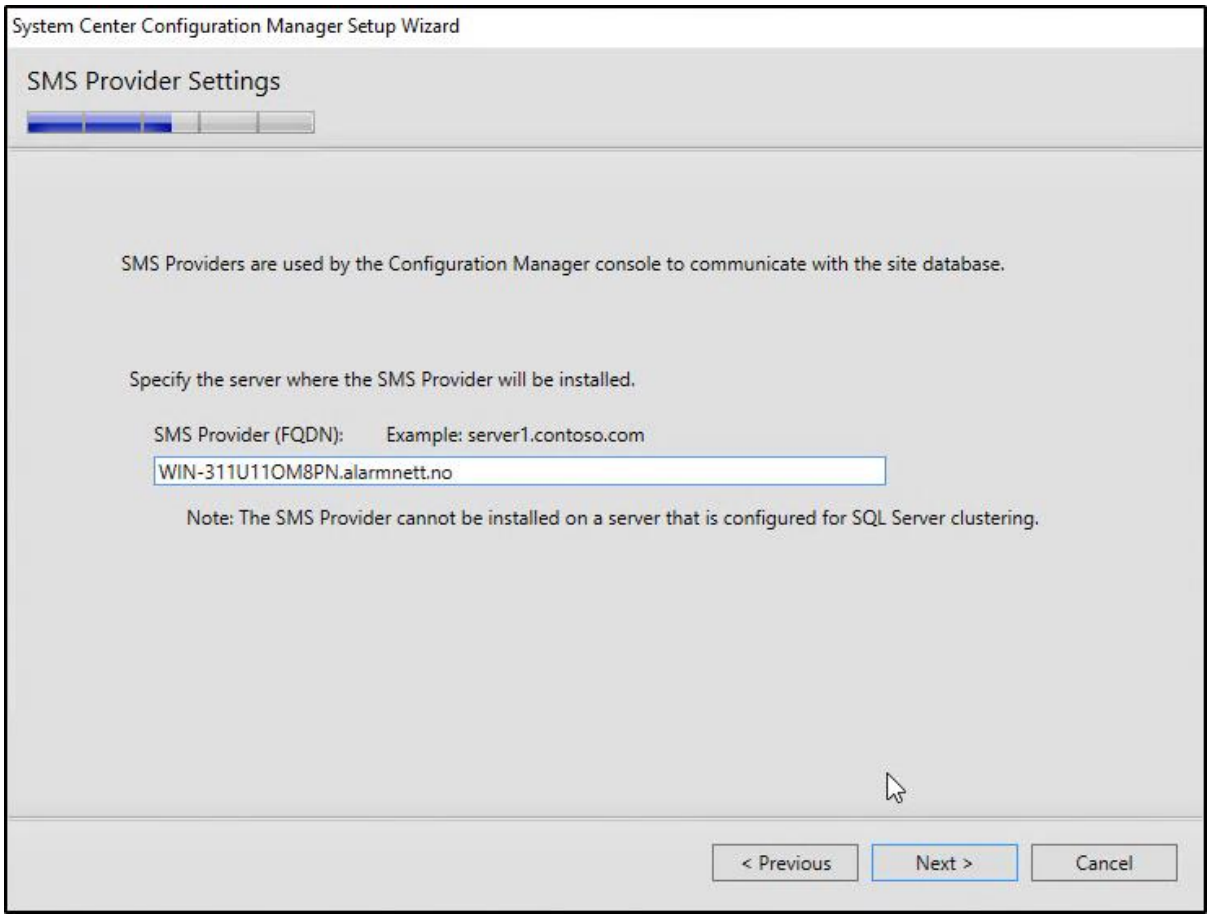
Figur 48: System Center Configuration Manager – Installasjon

Her igjen velger vi å ta i bruk to av diskene som vi opprettet tidligere, slik at vi får skilt hvor de forskjellige dataene ligger. Trykker deretter **Next**.



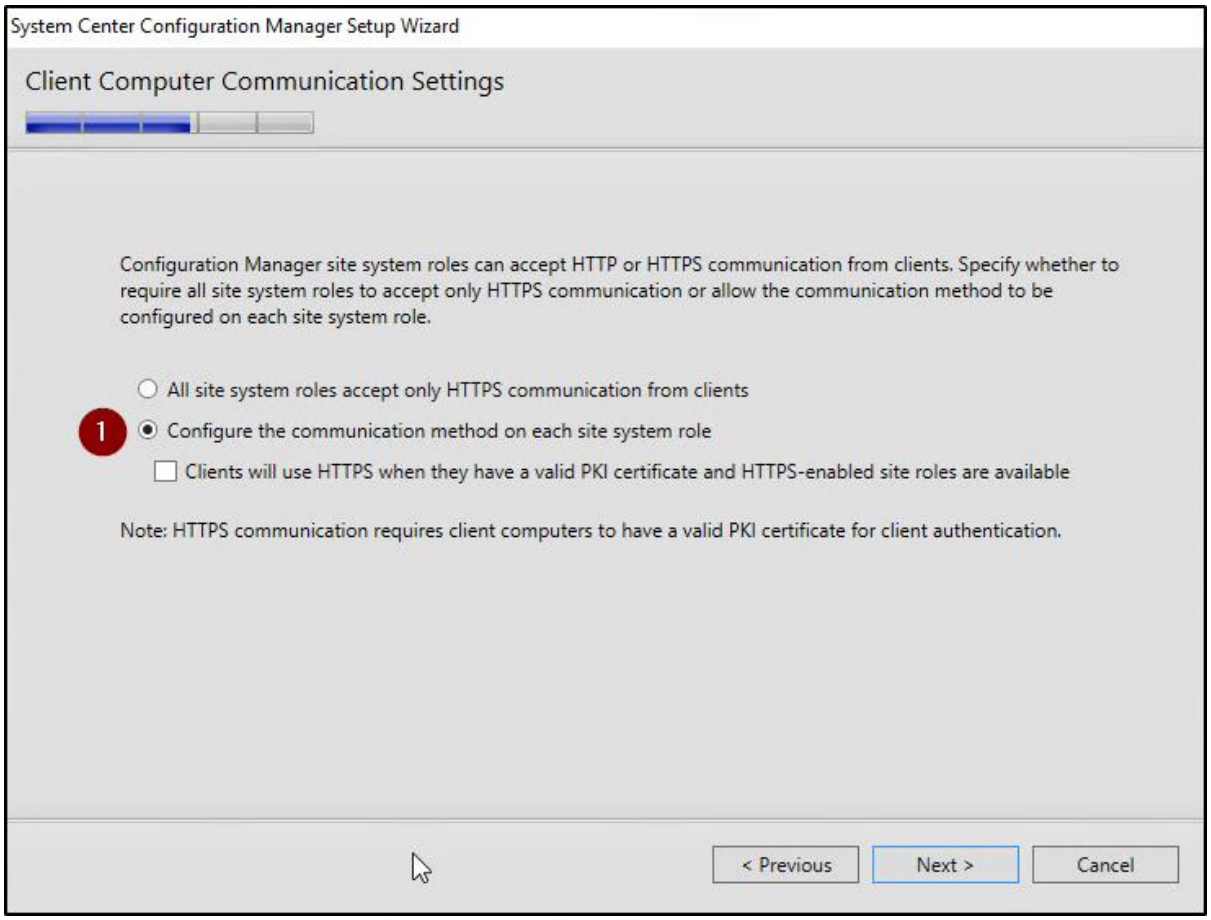
Figur 49: System Center Configuration Manager – Installasjon

Beholder standardinnstillinger og trykker **Next.**



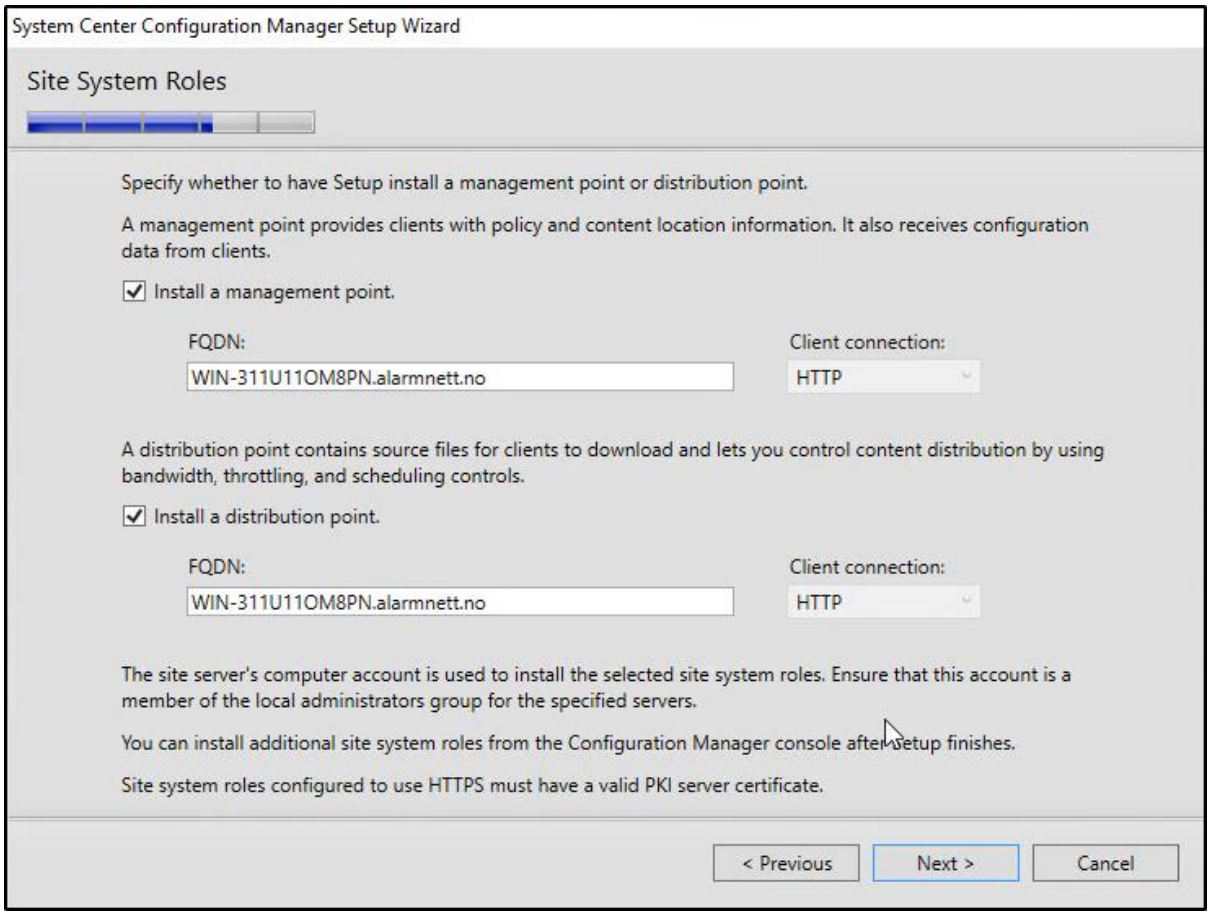
Figur 50: System Center Configuration Manager – Installasjon

Velger «Configure the communication method on each site system role» og trykker **Next**.



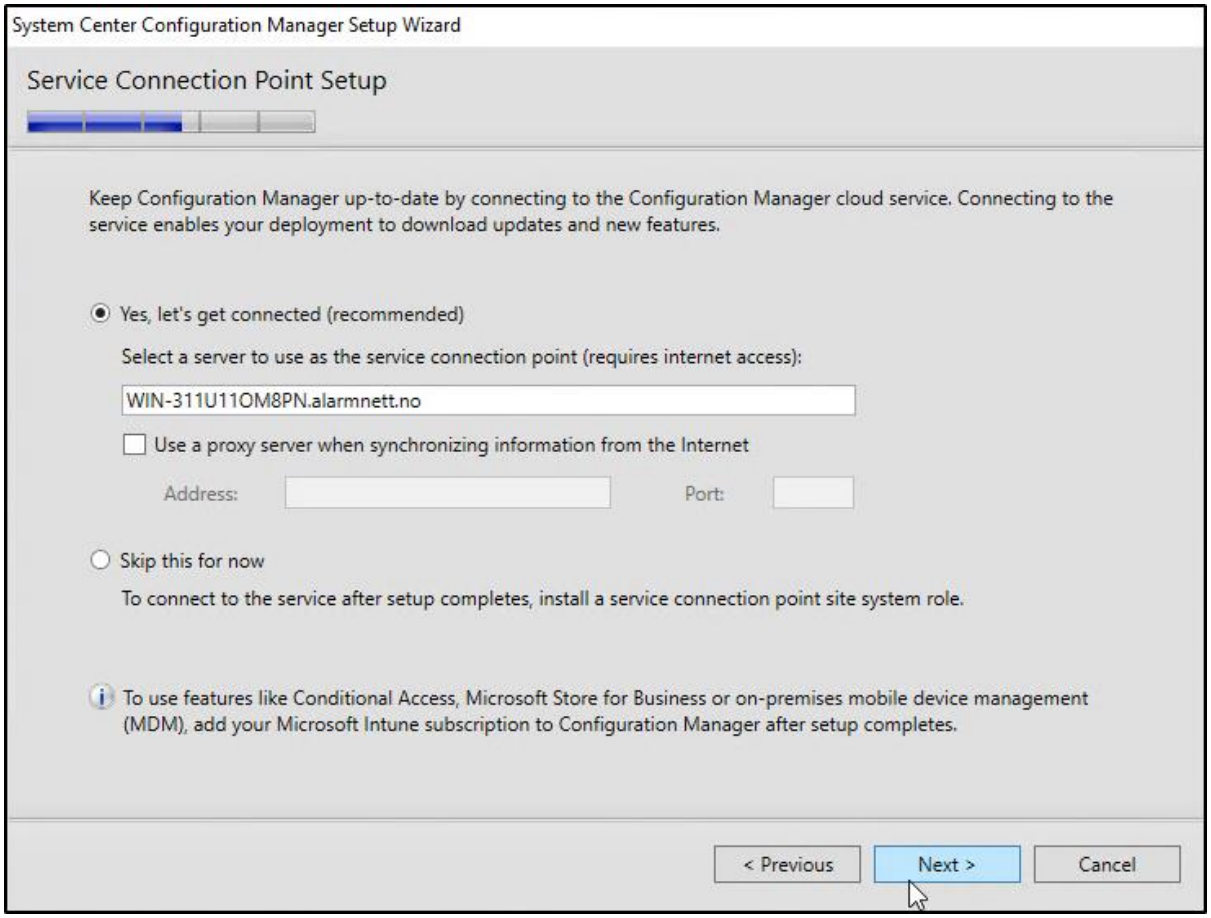
Figur 51: System Center Configuration Manager – Installasjon

Beholder standardinnstillinger og trykker **Next.**



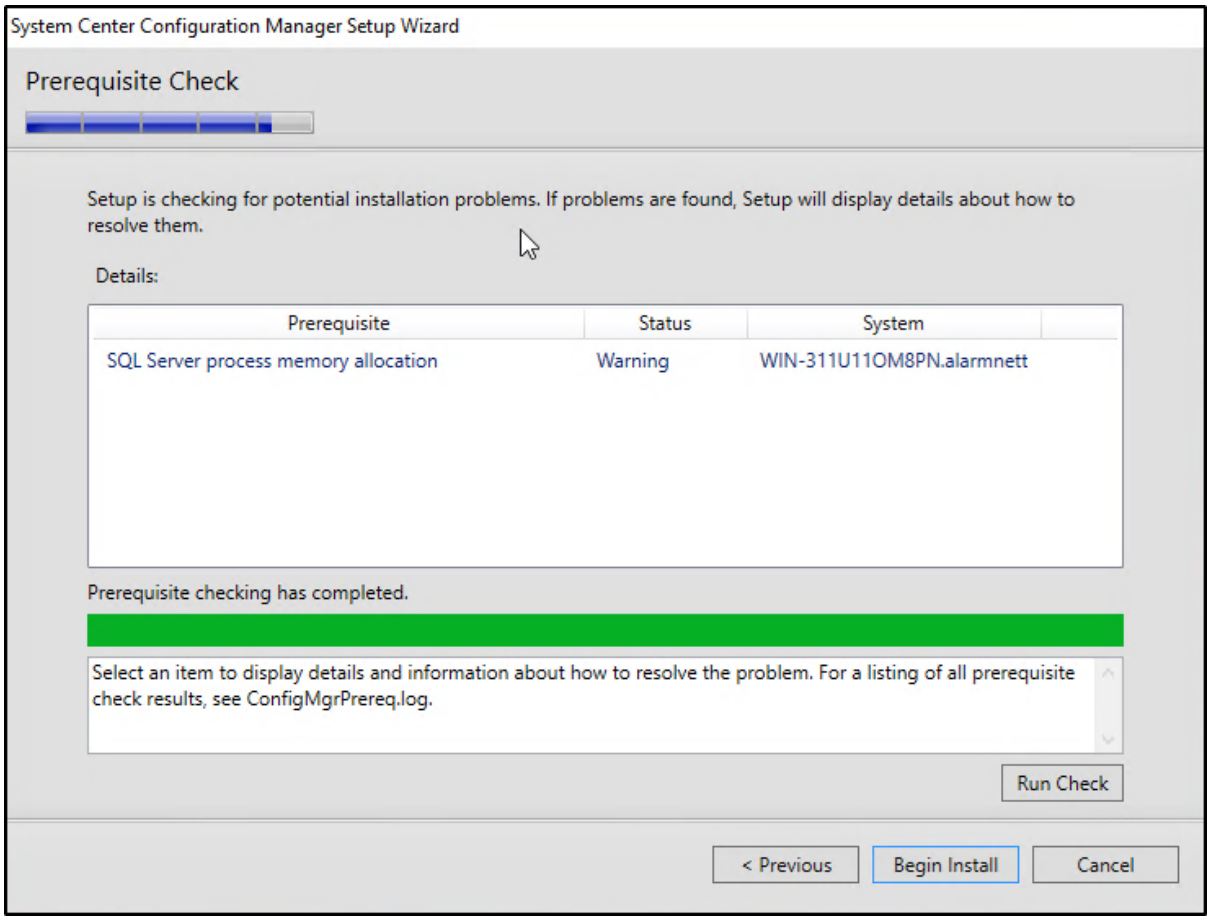
Figur 52: System Center Configuration Manager – Installasjon

Beholder standardinnstillinger og trykker **Next.**



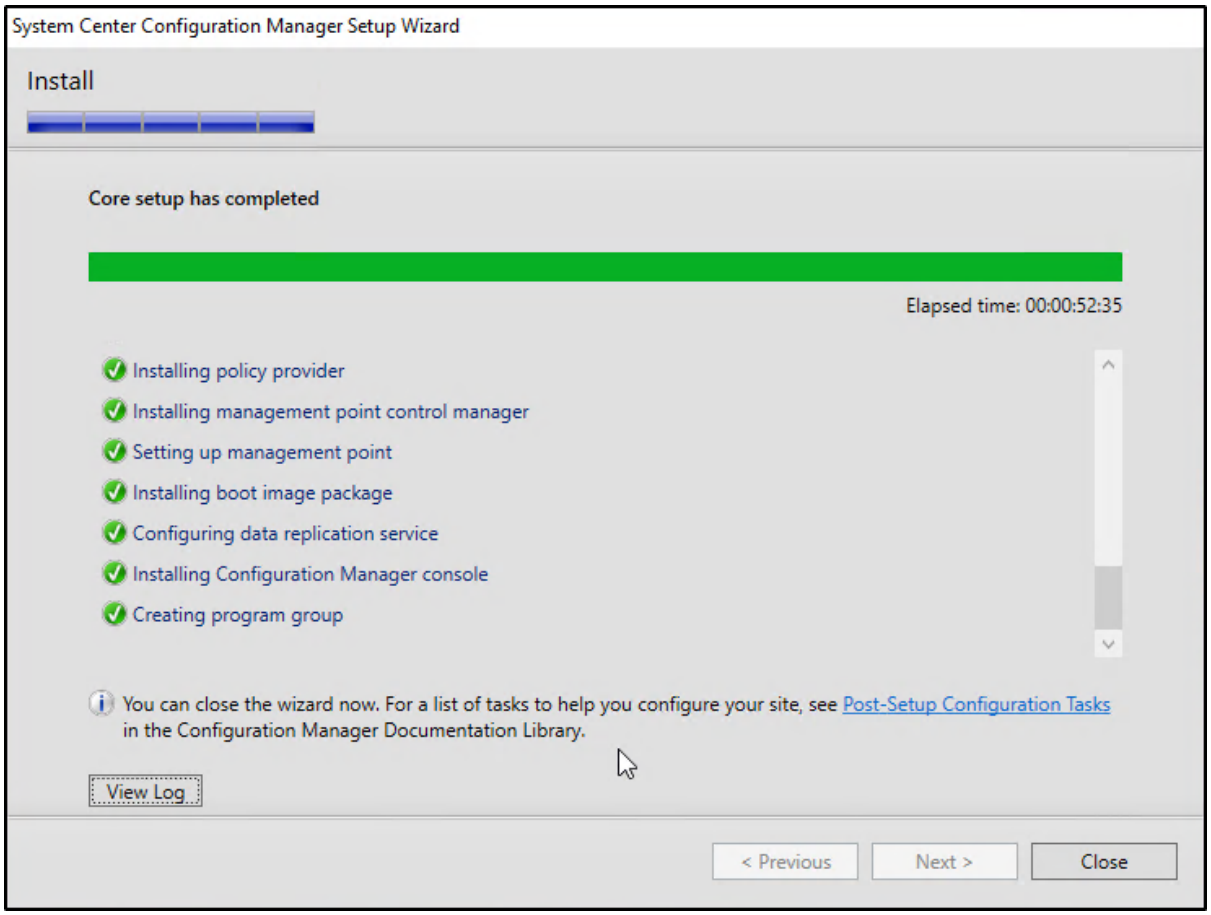
Figur 53: System Center Configuration Manager – Installasjon

Ser til at vi kun får denne ene advarselen. Dette er en advarsel for å minne oss på om at vi må sette nok RAM til maskinen. Vi har allerede satt memory allocation til over 8GB, så det er bare å fortsette med installasjonen. Vi velger **Begin Install**.



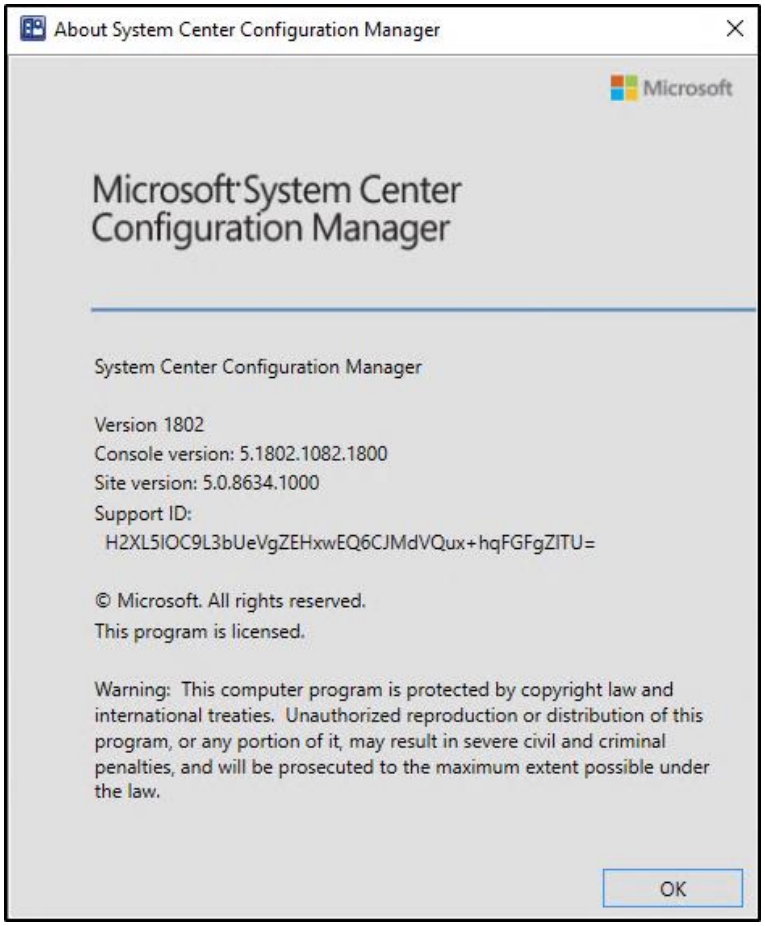
Figur 54: System Center Configuration Manager – Installasjon

Installasjonen er gjennomført.



Figur 55: System Center Configuration Manager – Installasjon

Når installasjonen er ferdig, kan vi her se at vi har fått riktig versjon. I vårt tilfelle installerte vi versjon 1802, da dette var den nyeste versjonen som er tilgjengelig for oss.



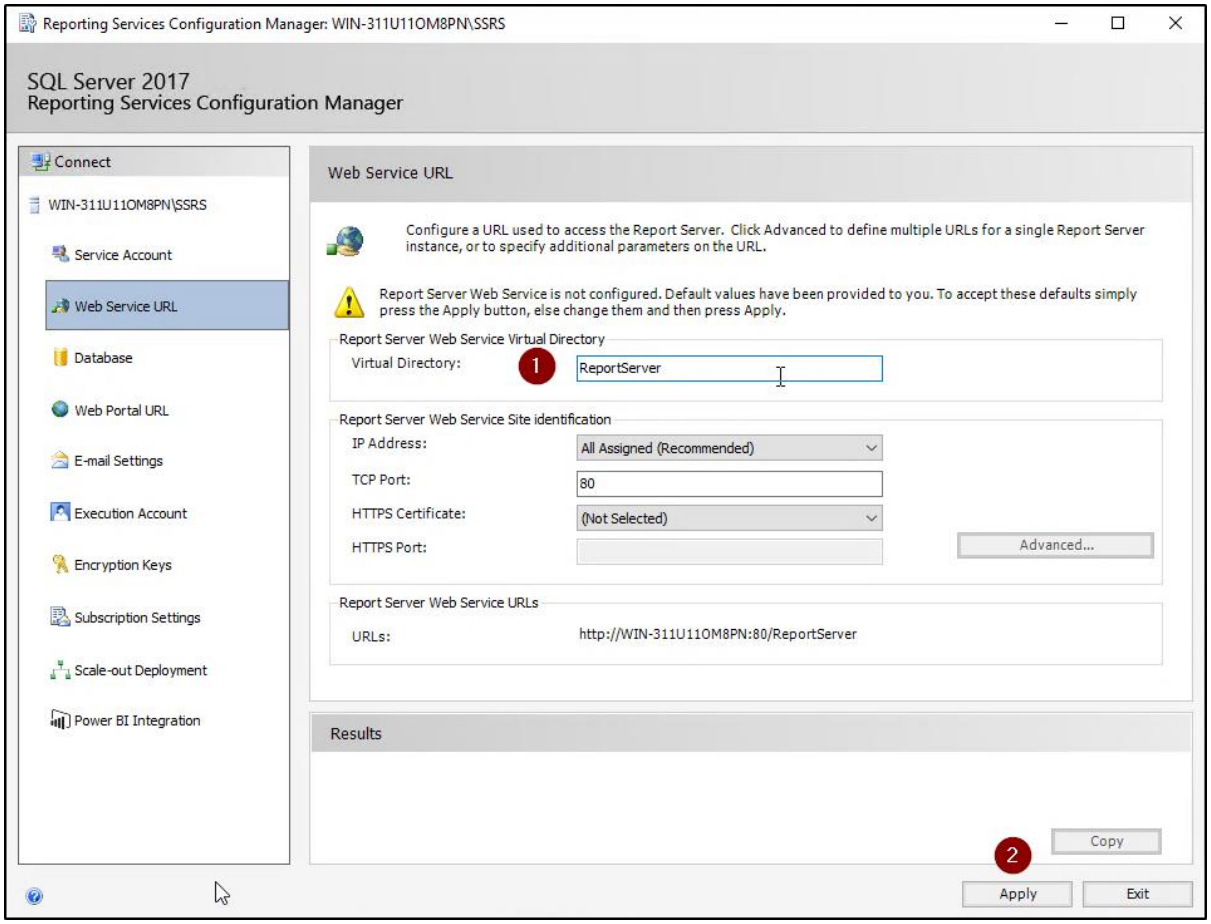
Figur 56: System Center Configuration Manager - Installasjon

Fase 2 – Post-konfigurasjon av SCCM

SCCM Post-Konfigurasjon

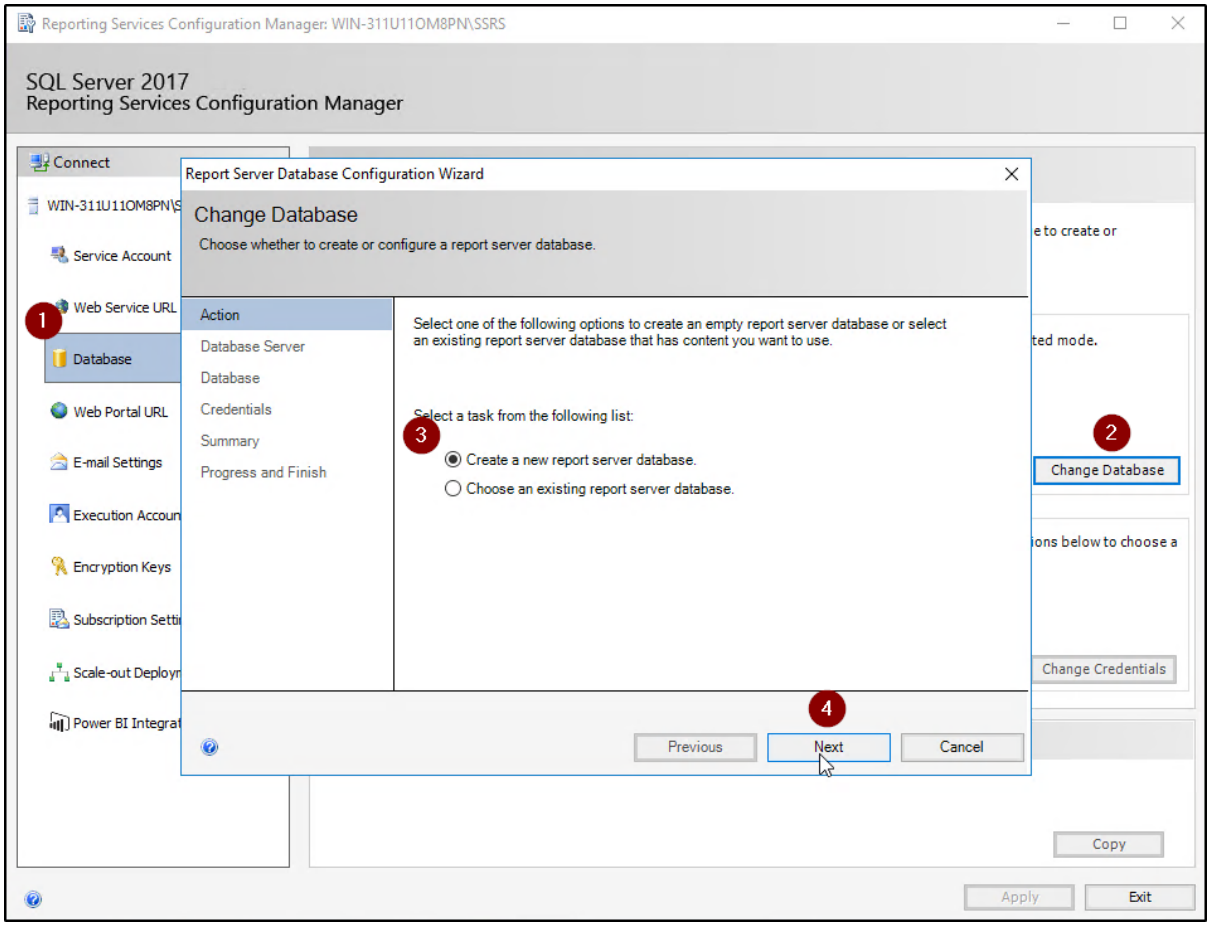
Post-konfigurasjon av SQL Server Reporting Services

En av konfigurasjonene vi må gjøre i SQL Server Reporting Services, er å sette et Virtual Directory. Gir det et navn og trykker **Apply**.



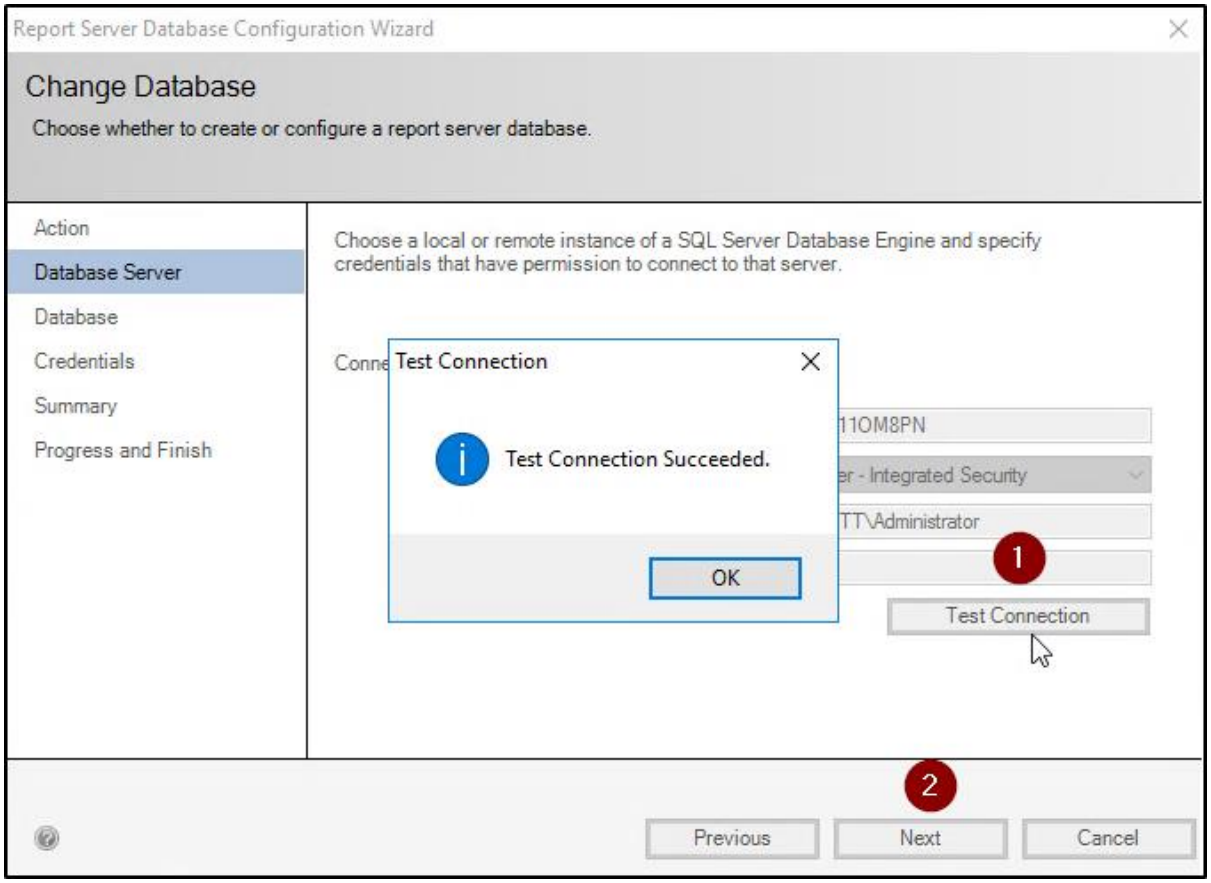
Figur 57: SQL Server Reporting Services - Post-konfigurasjon

Vi må deretter opprette en database. Velger «*Create a new report server database*», og trykker **Next**.



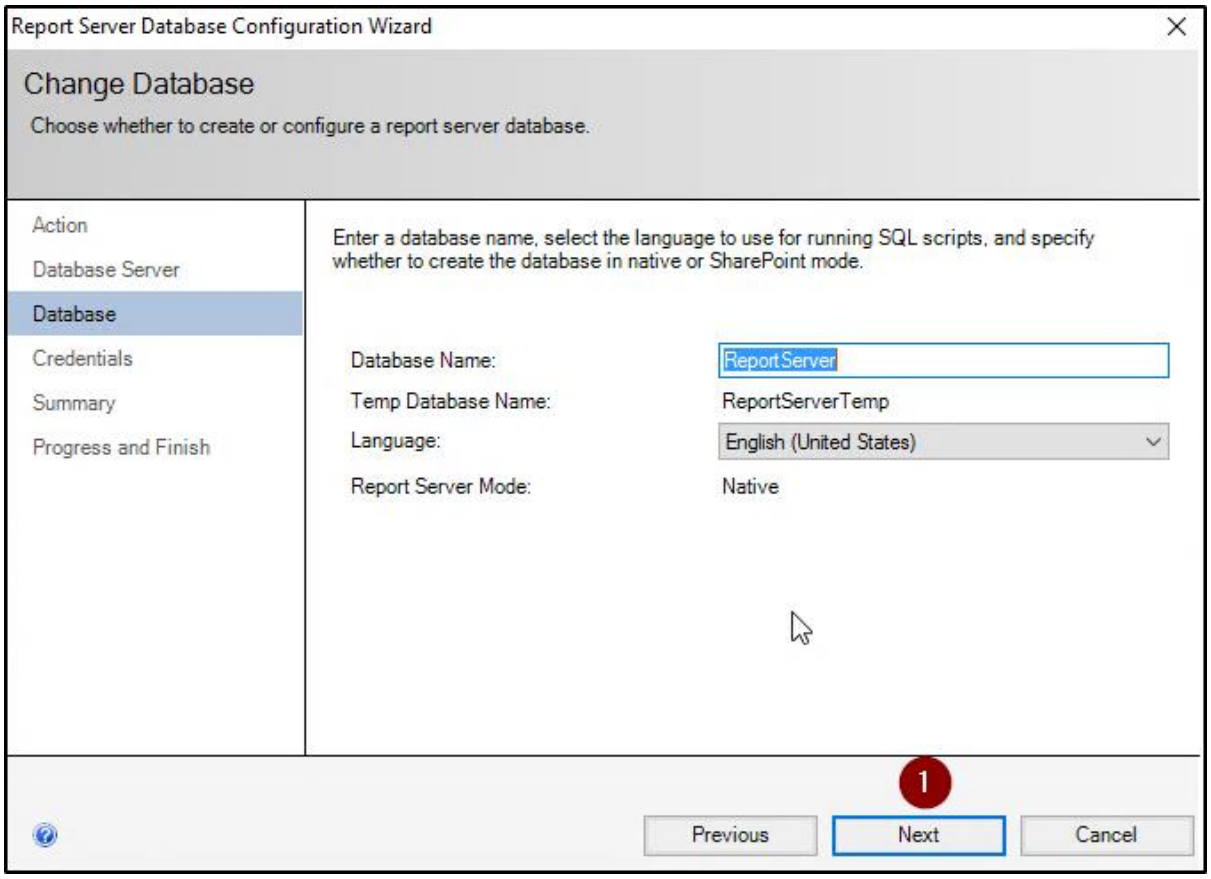
Figur 58: SQL Server Reporting Services - Post-konfigurasjon

Under ***Database Server***, velger vi å teste tilkoblingen ved å trykke på **Test Connection** og trykker **Next**.



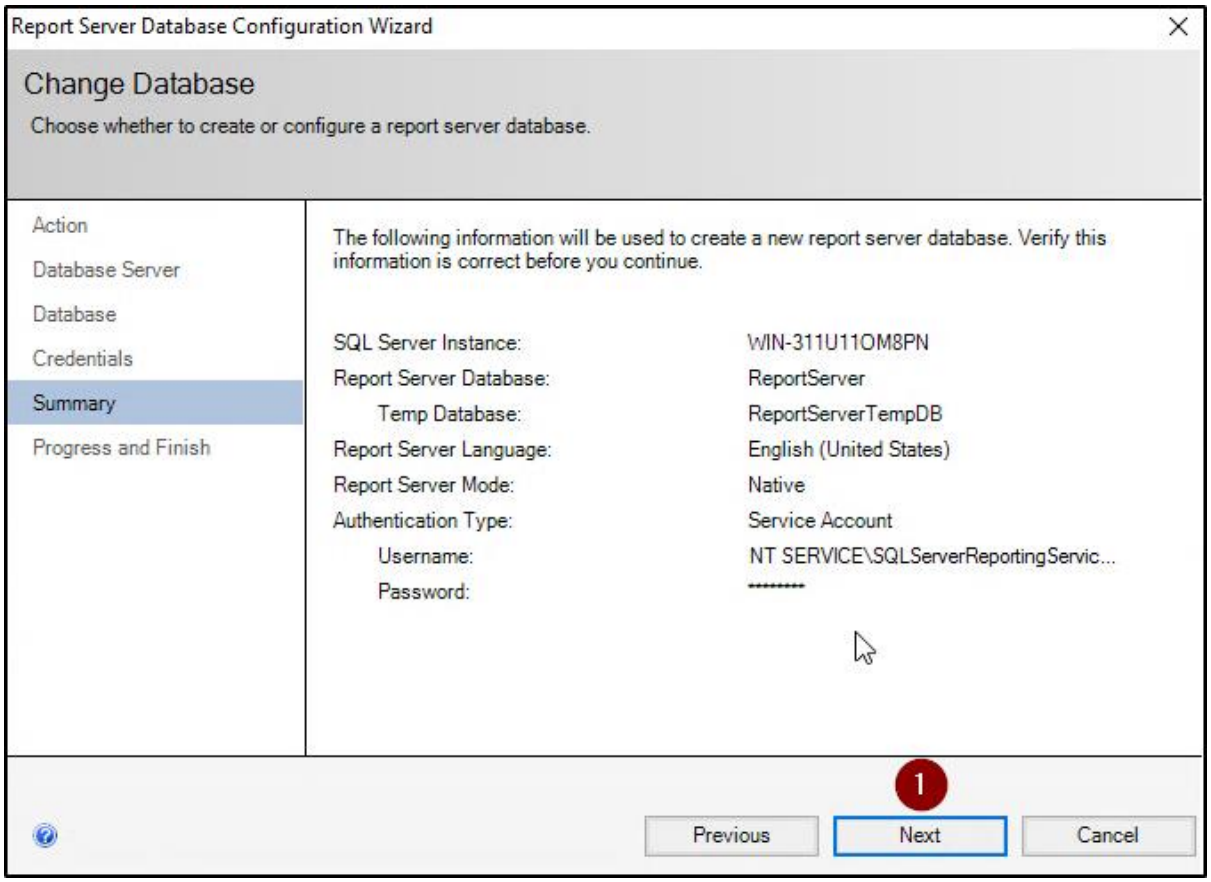
Figur 59: SQL Server Reporting Services - Post-konfigurasjon

Under ***Database*** legger man til et *Database name* og trykker **Next**.



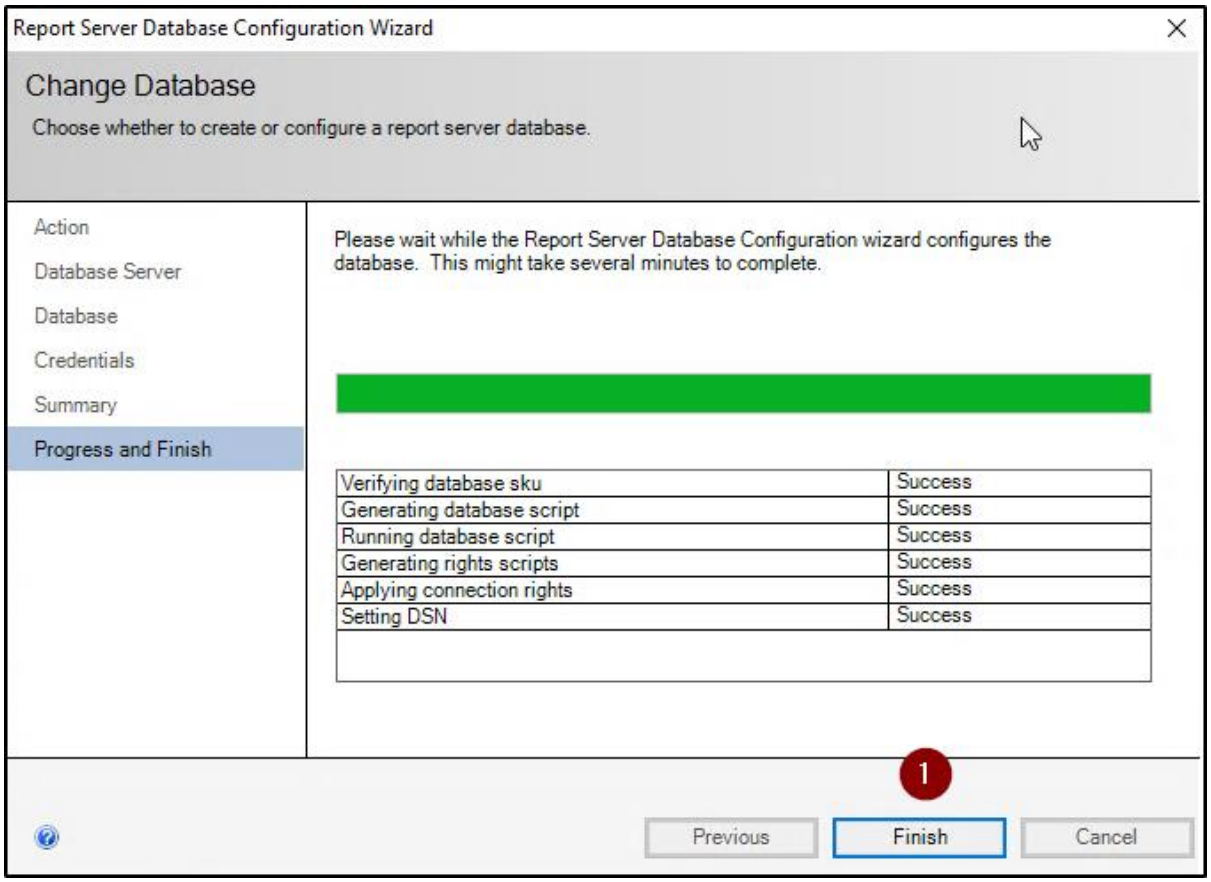
Figur 60: SQL Server Reporting Services - Post-konfigurasjon

Under ***Summary,*** ser vi over at alt stemmer og trykker **Next**.



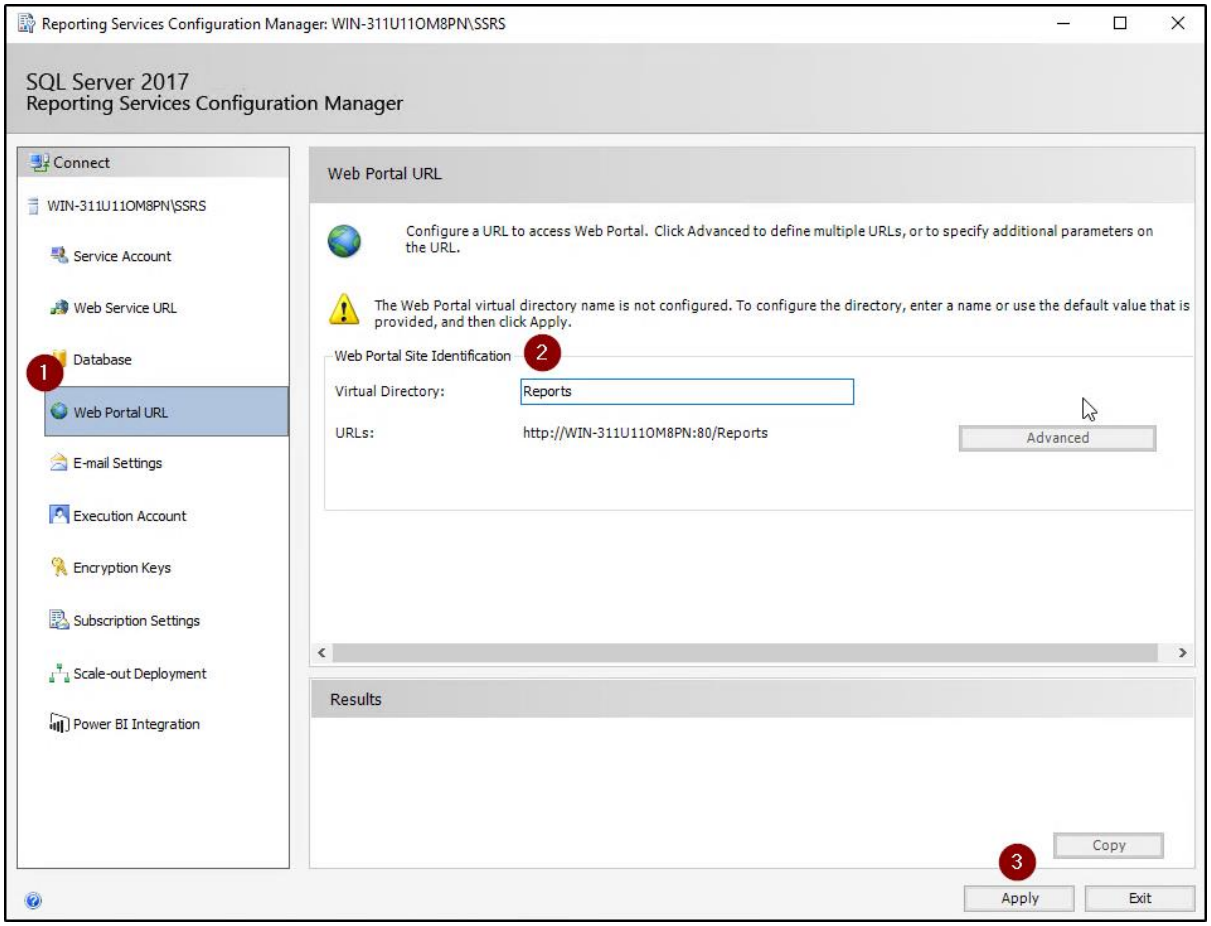
Figur 61: SQL Server Reporting Services - Post-konfigurasjon

Observerer at databasen har blitt opprettet uten problemer og trykker **Finish.**



Figur 62: SQL Server Reporting Services - Post-konfigurasjon

Til slutt setter vi en Web Portal URL, slik at vi kan få tilgang til denne i en nettleser og trykker **Apply.**



Figur 63: SQL Server Reporting Services - Post-konfigurasjon

Installasjon av roller

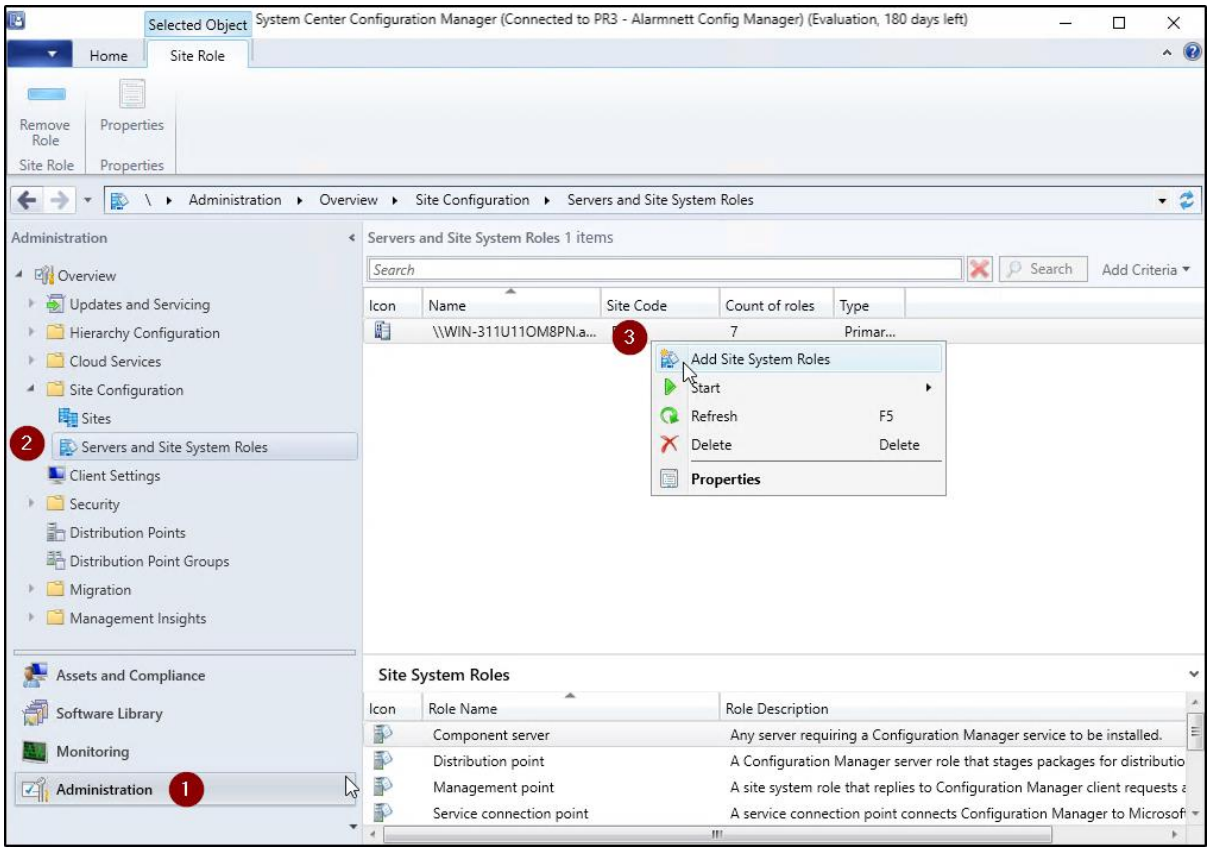
Under dette punktet vil vi nå installere diverse roller som kan komme til nytte i vårt testmiljø.

Vi vil nå gå gjennom hvordan følgende roller installeres:

- Reporting Site Role
- Software Update Point Role
- Endpoint Protection Point role
- Fallback Status Point Role

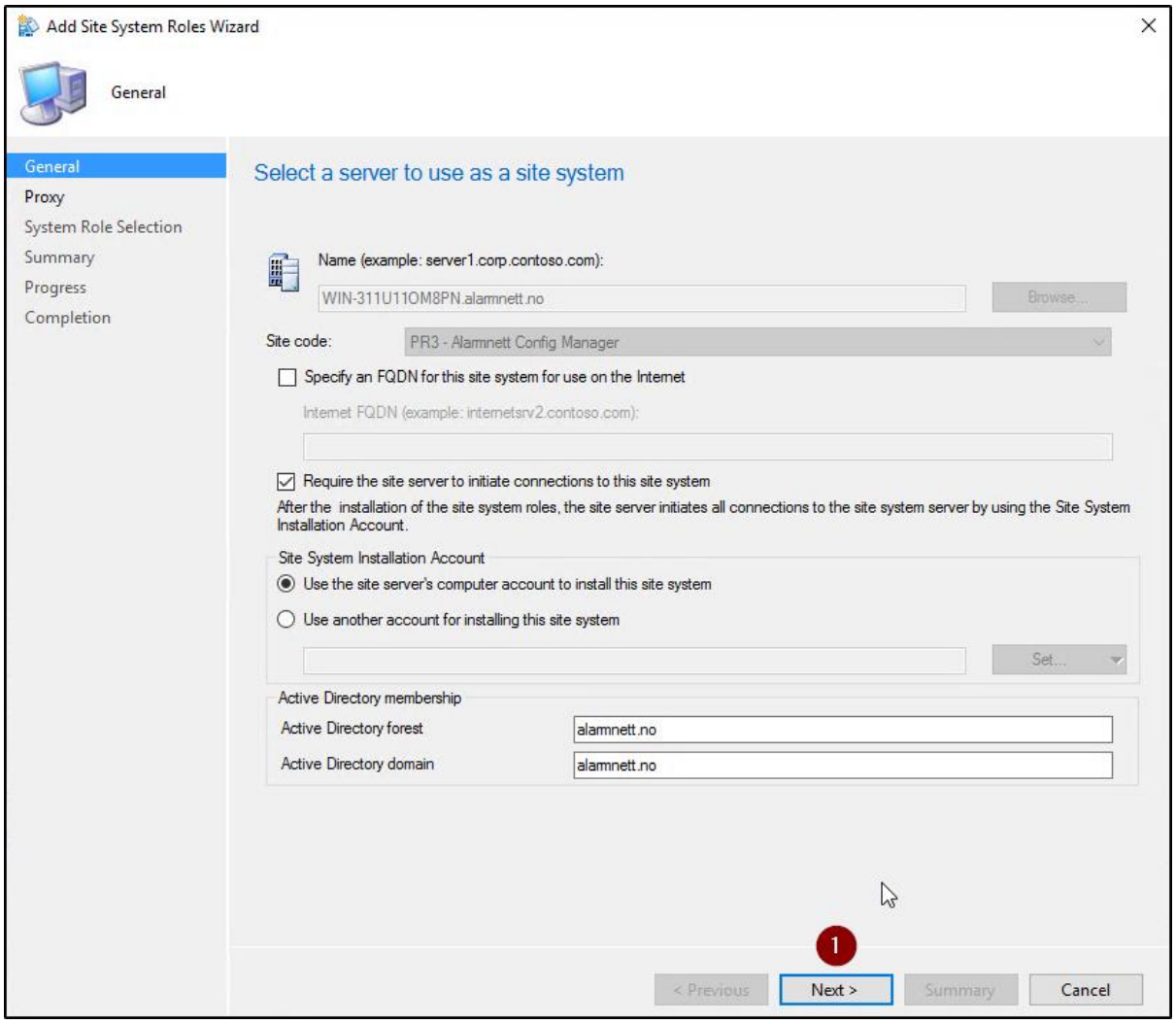
Installasjonen av roller utføres i Configuration Manager konsollet.

Under ***Servers and site System Roles***, velger vi å legge til nye **Site Systems Roles**.



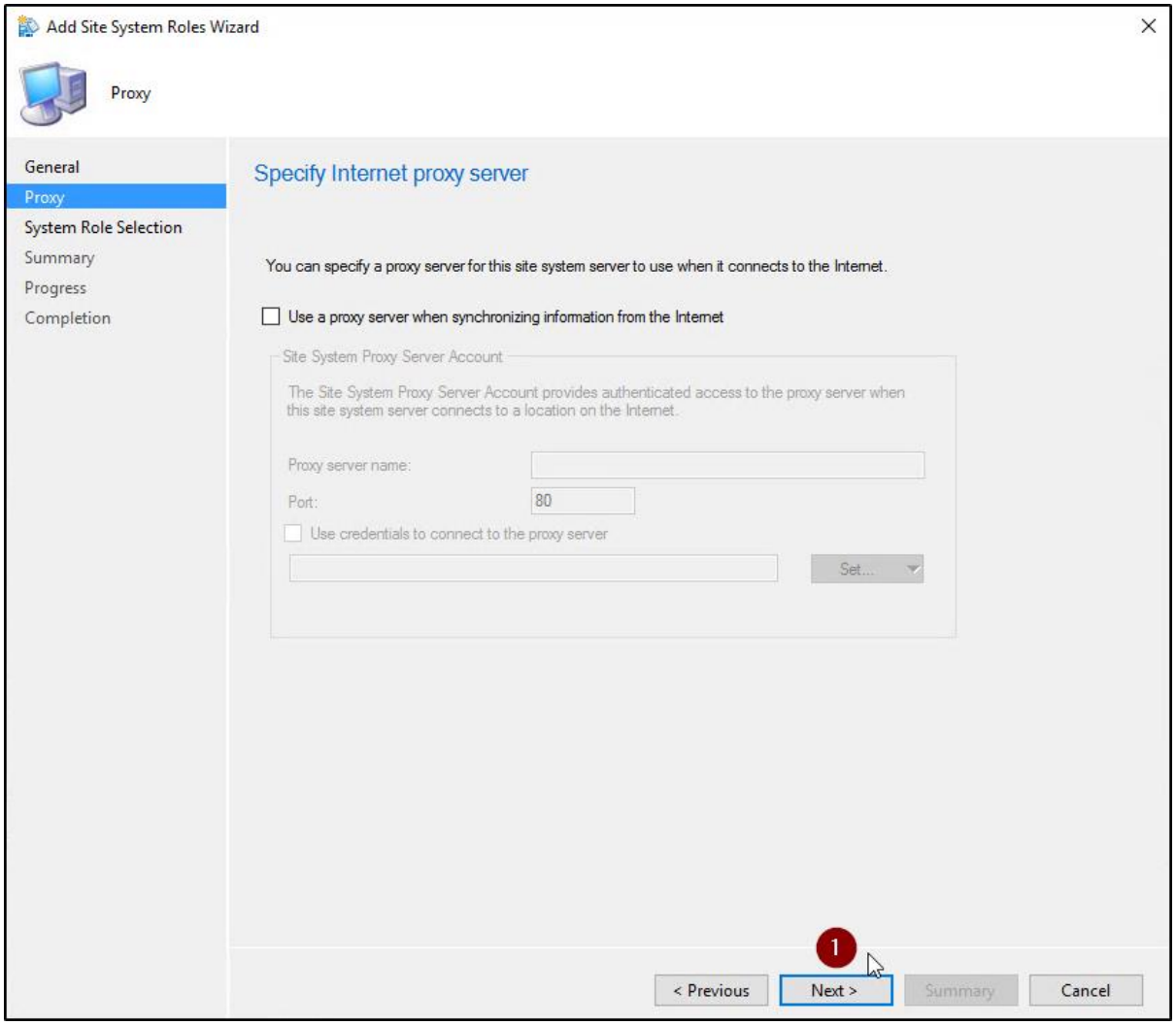
Figur 64: Roller i SCCM – Installasjon

Vi begynner med å se til at alt stemmer på denne siden og trykker **Next**.



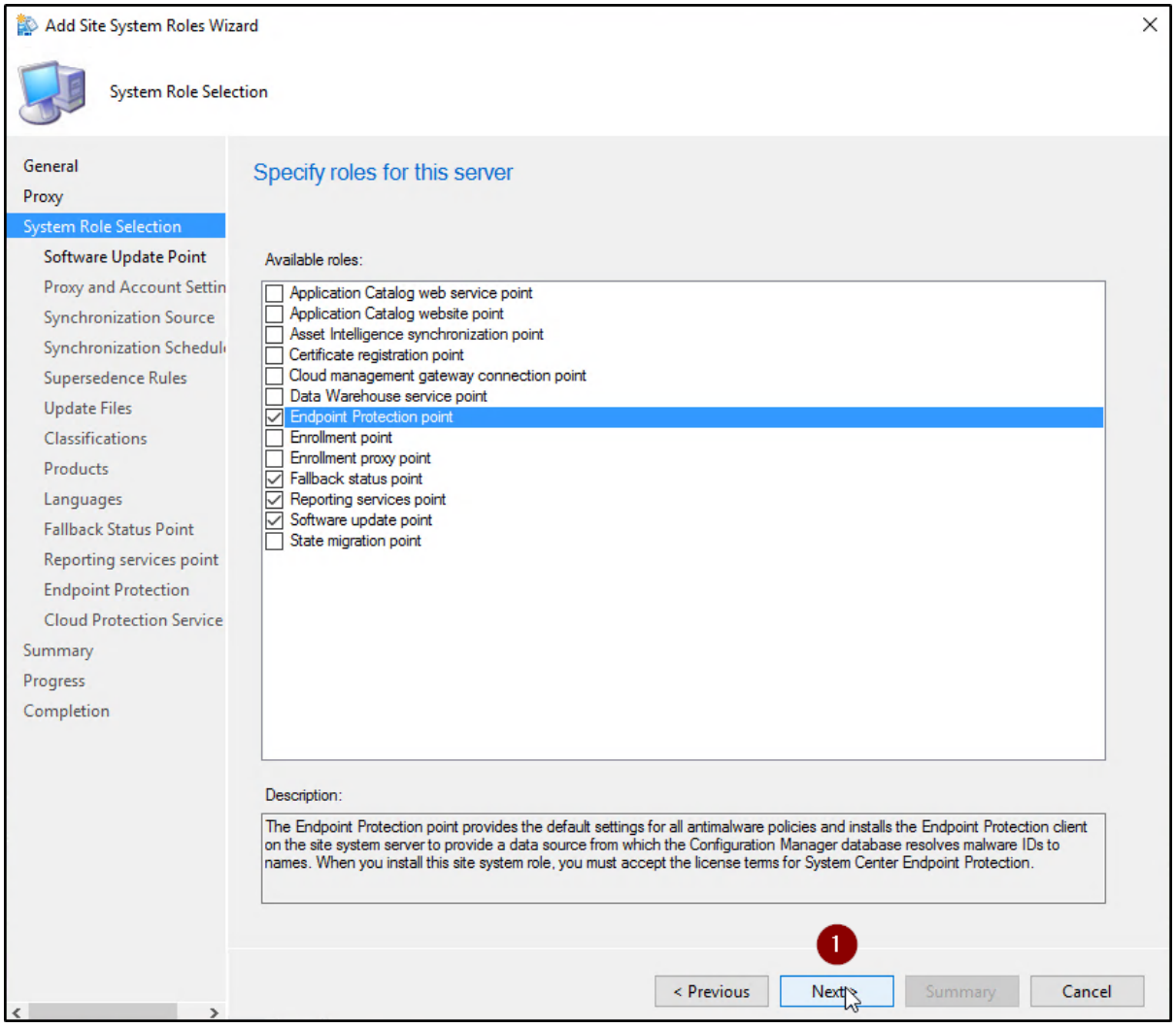
Figur 65: Roller i SCCM – Installasjon

Hvis man ønsker å benytte seg av en proxy, kan dette konfigureres her. I vårt tilfelle går vi bare videre og trykker **Next**.



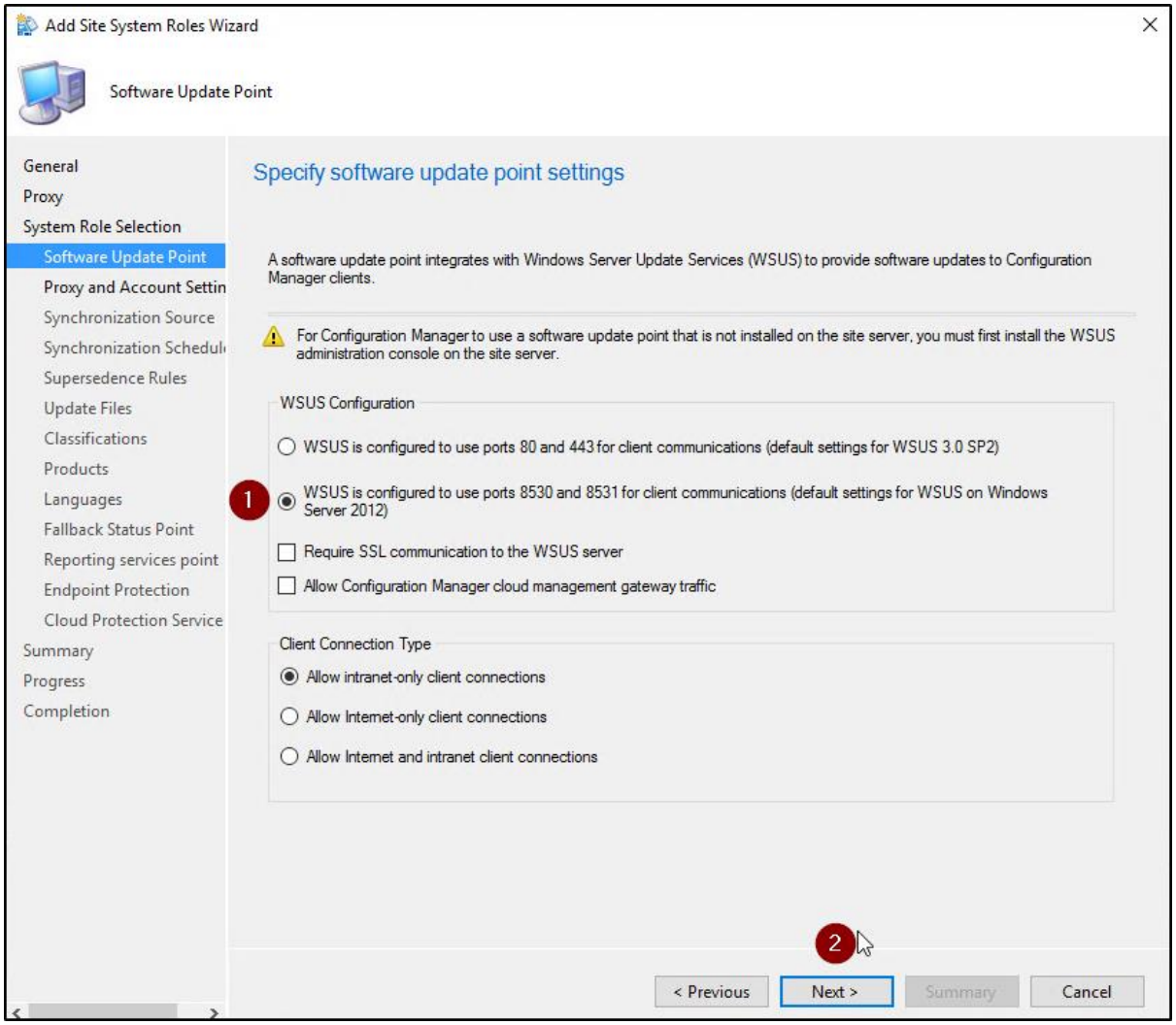
Figur 66: Roller i SCCM – Installasjon

Vi må nå velge hvilke roller vi ønsker å installere. Vi velger de fire rollene vist nedenfor og trykker **Next**.



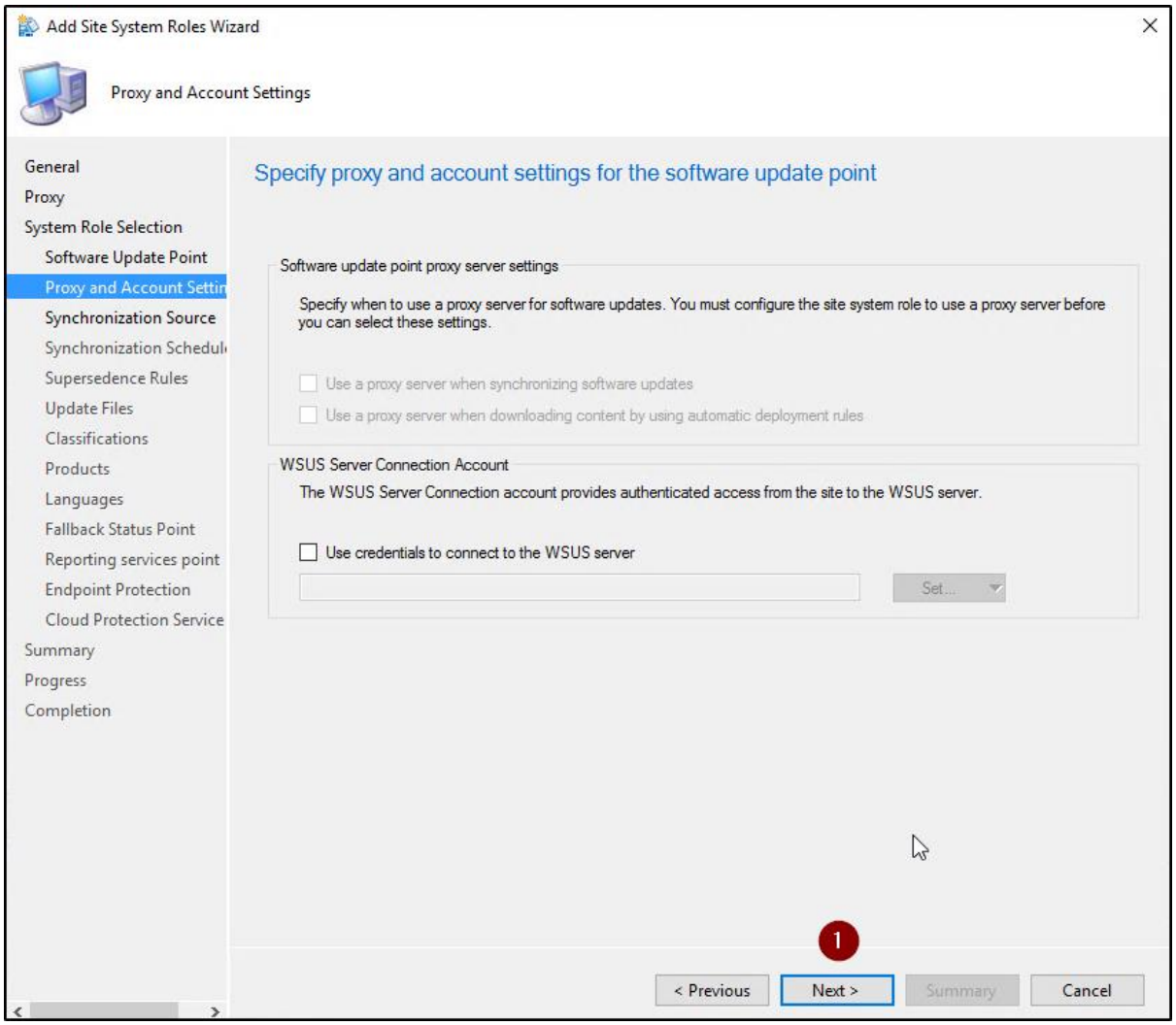
Figur 67: Roller i SCCM – Installasjon

Velger her valg 2. som vist nedenfor, da vi benytter oss av en nyere versjon av Windows server (2012 eller nyere) og trykker **Next**.



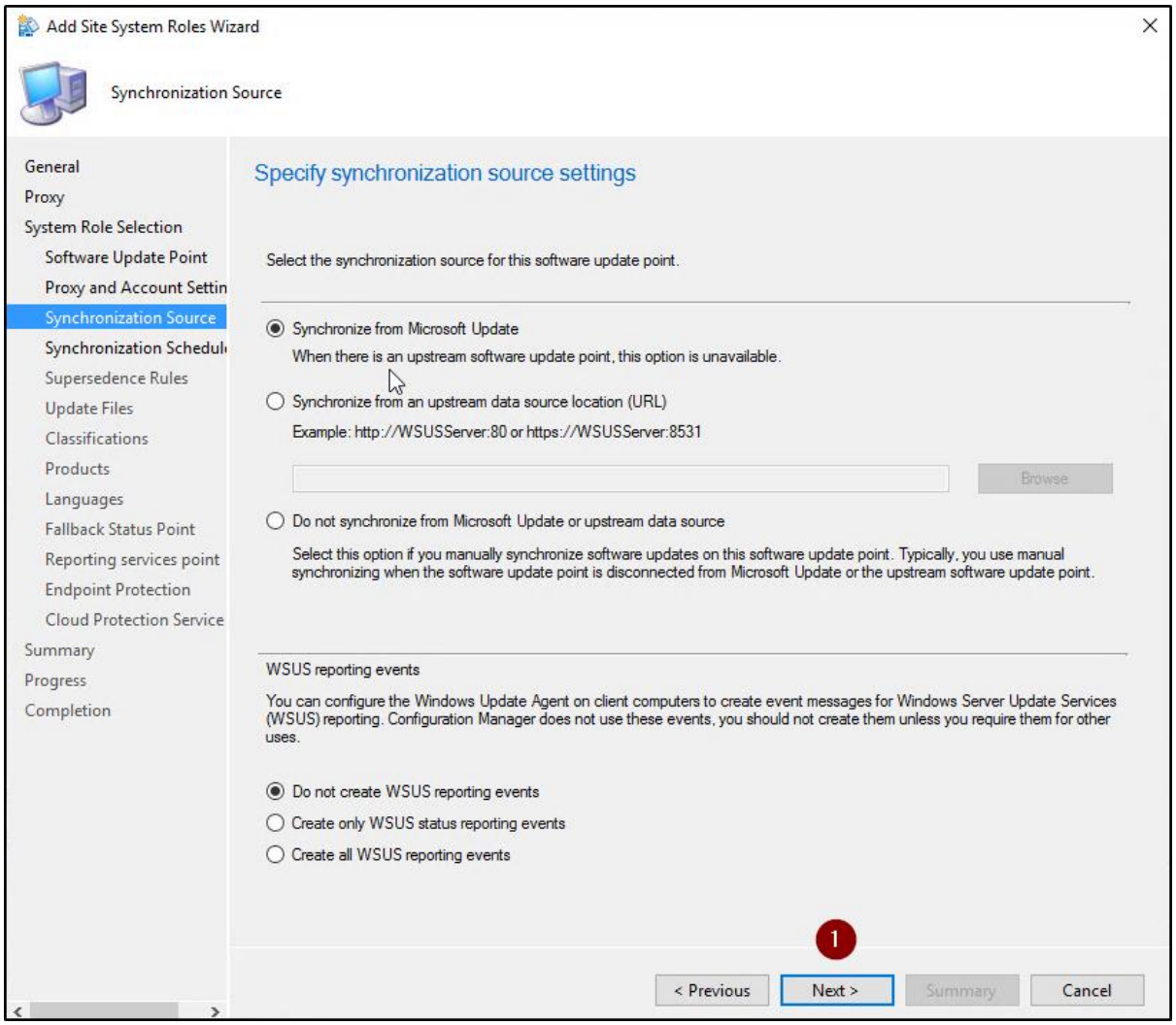
Figur 68: Roller i SCCM – Installasjon

Går videre på dette punktet, da vi ikke benytter oss av noen form for proxy og trykker **Next**.



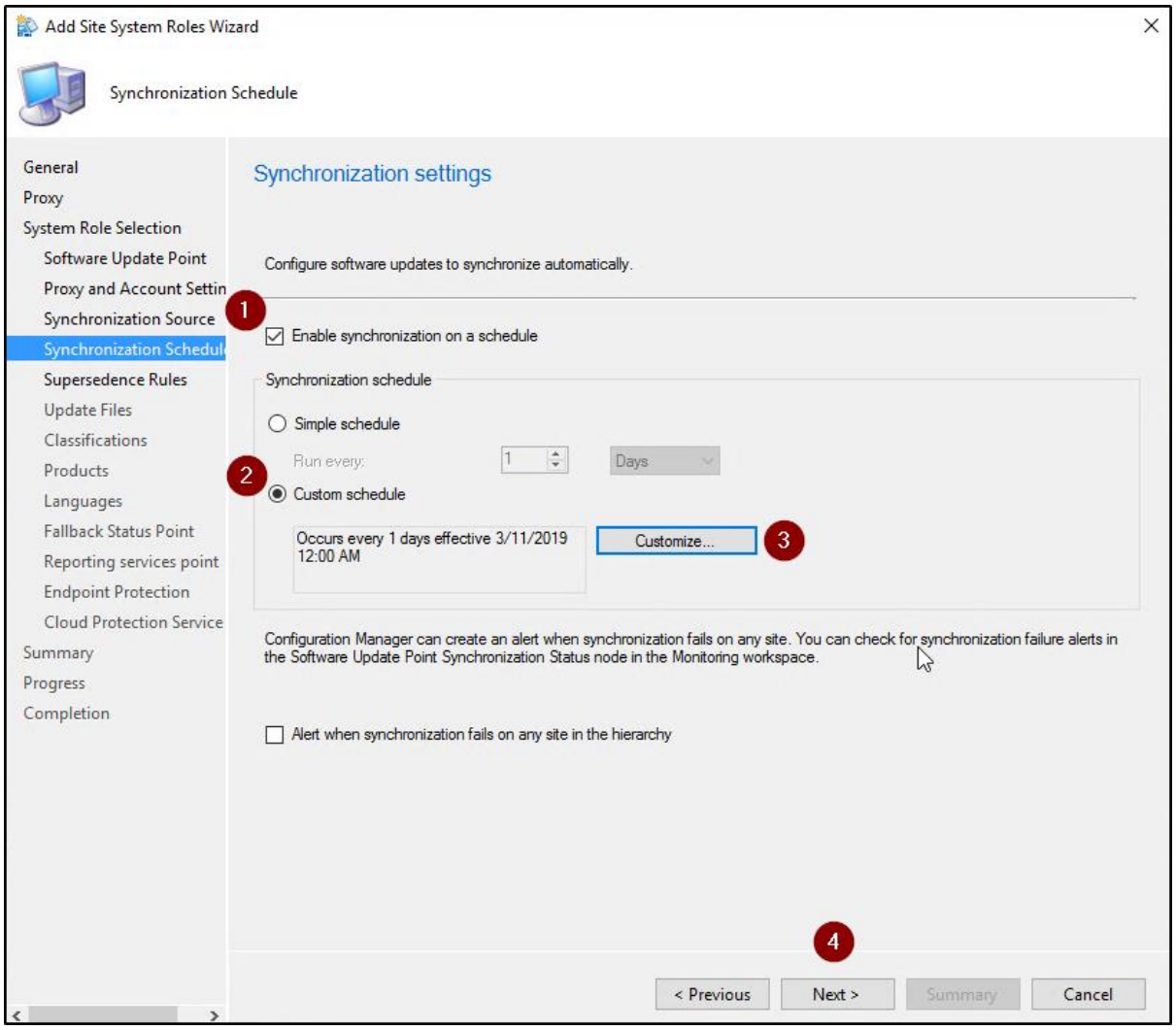
Figur 69: Roller i SCCM – Installasjon

Velger her å synkronisere fra Microsoft Updates og trykker **Next**.



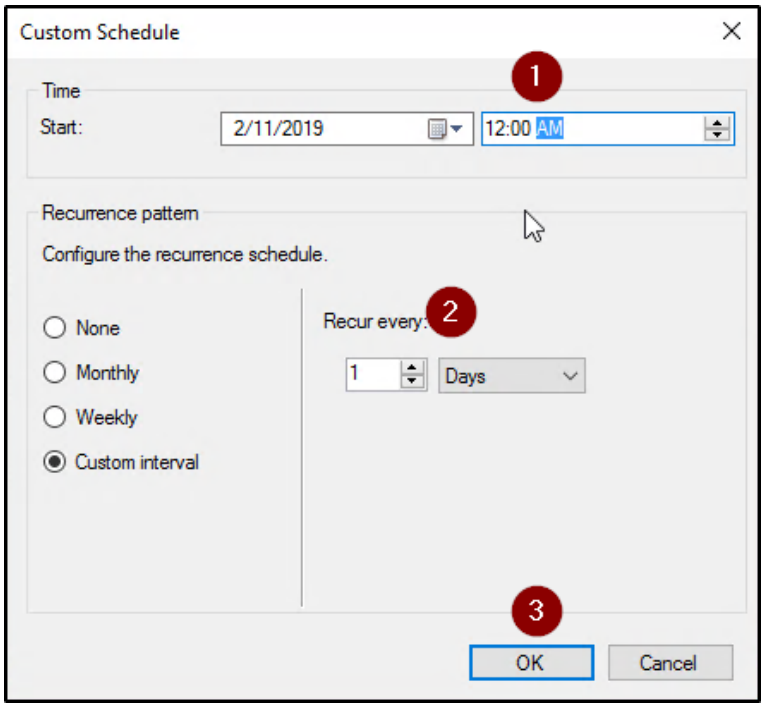
Figur 70: Roller i SCCM – Installasjon

Konfigurerer når og hvor ofte software updates skal synkroniseres og trykker **Next**.



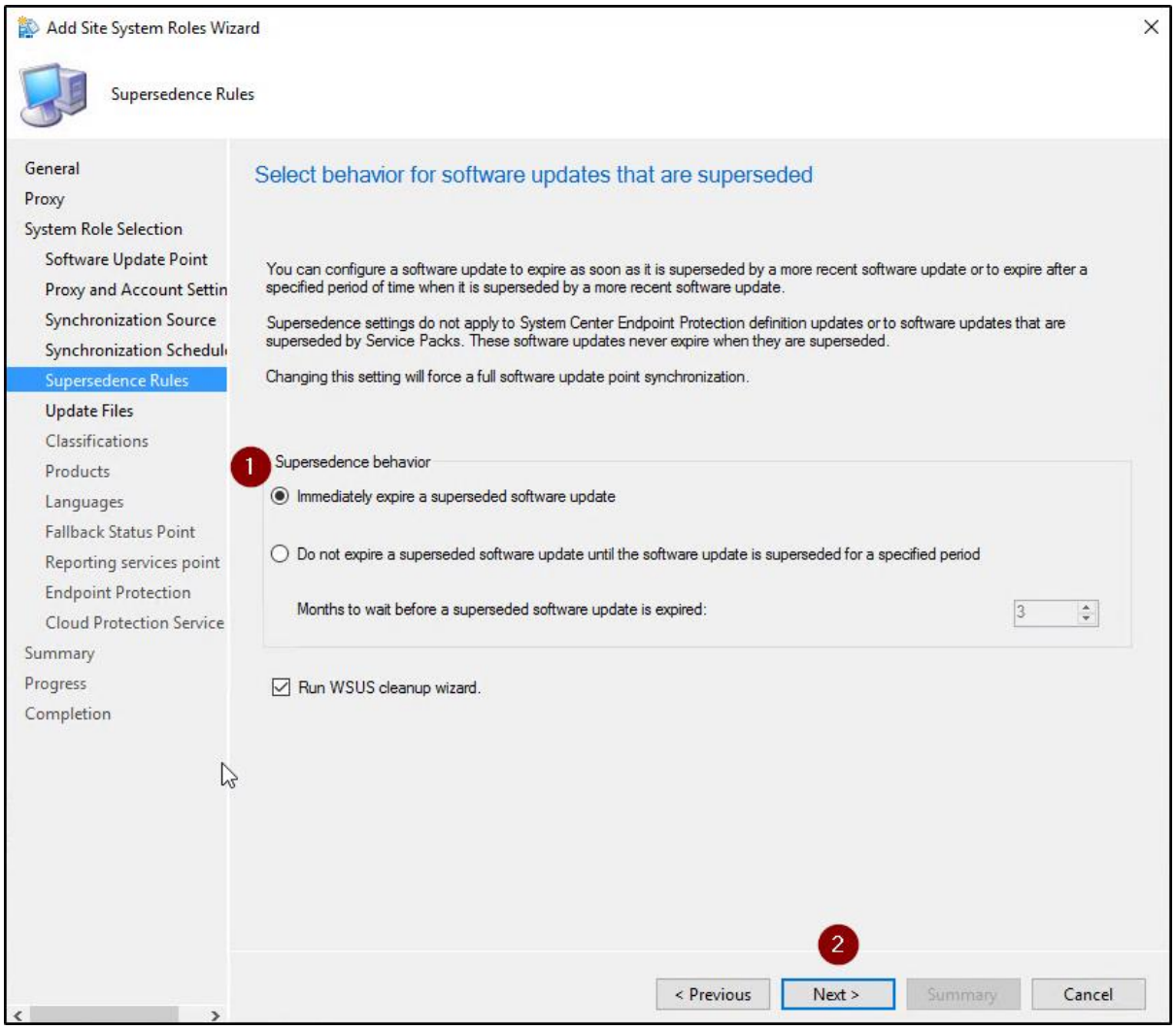
Figur 71: Roller i SCCM – Installasjon

Setter Schedule til ønsket tidspunkt og trykker **OK**.



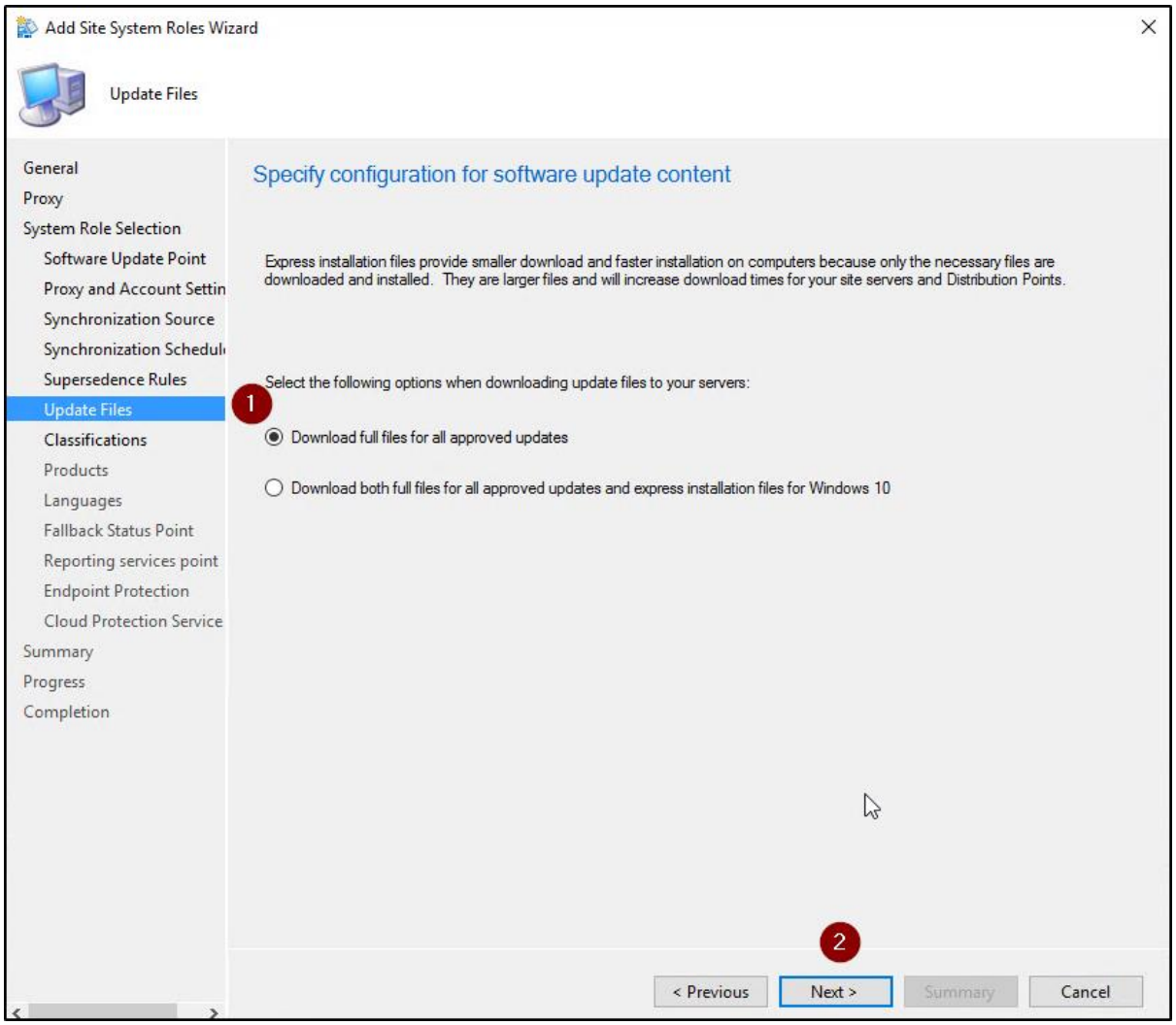
Figur 72: Roller i SCCM – Installasjon

Ser til at *Supersedence behavior*, er satt til første valg og trykker **Next**.



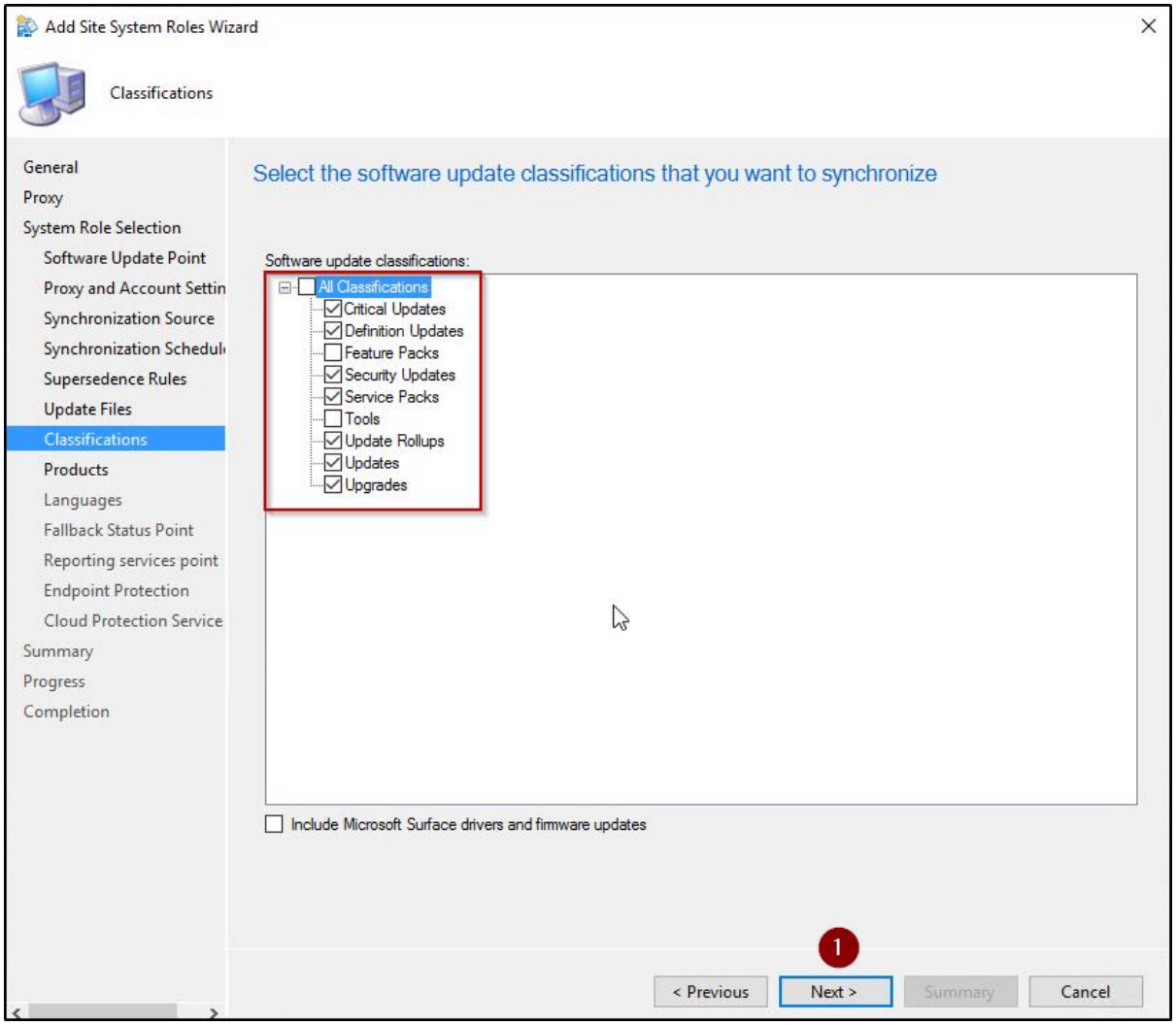
Figur 73: Roller i SCCM – Installasjon

Velger det første valget og trykker **Next**.



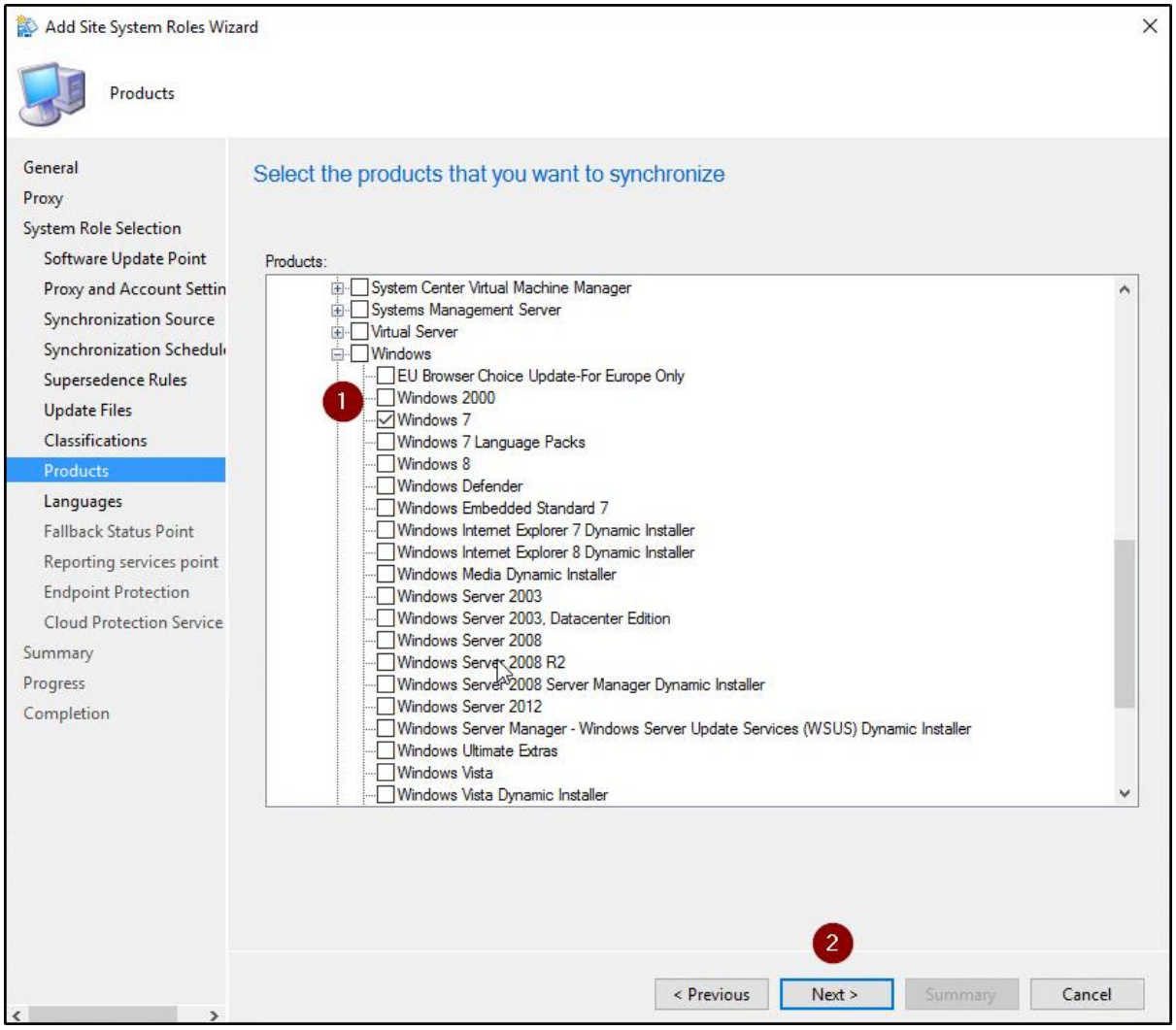
Figur 74: Roller i SCCM – Installasjon

Velger software update classifications, i forhold til de rollene vi har valgt å ta med og trykker **Next**.



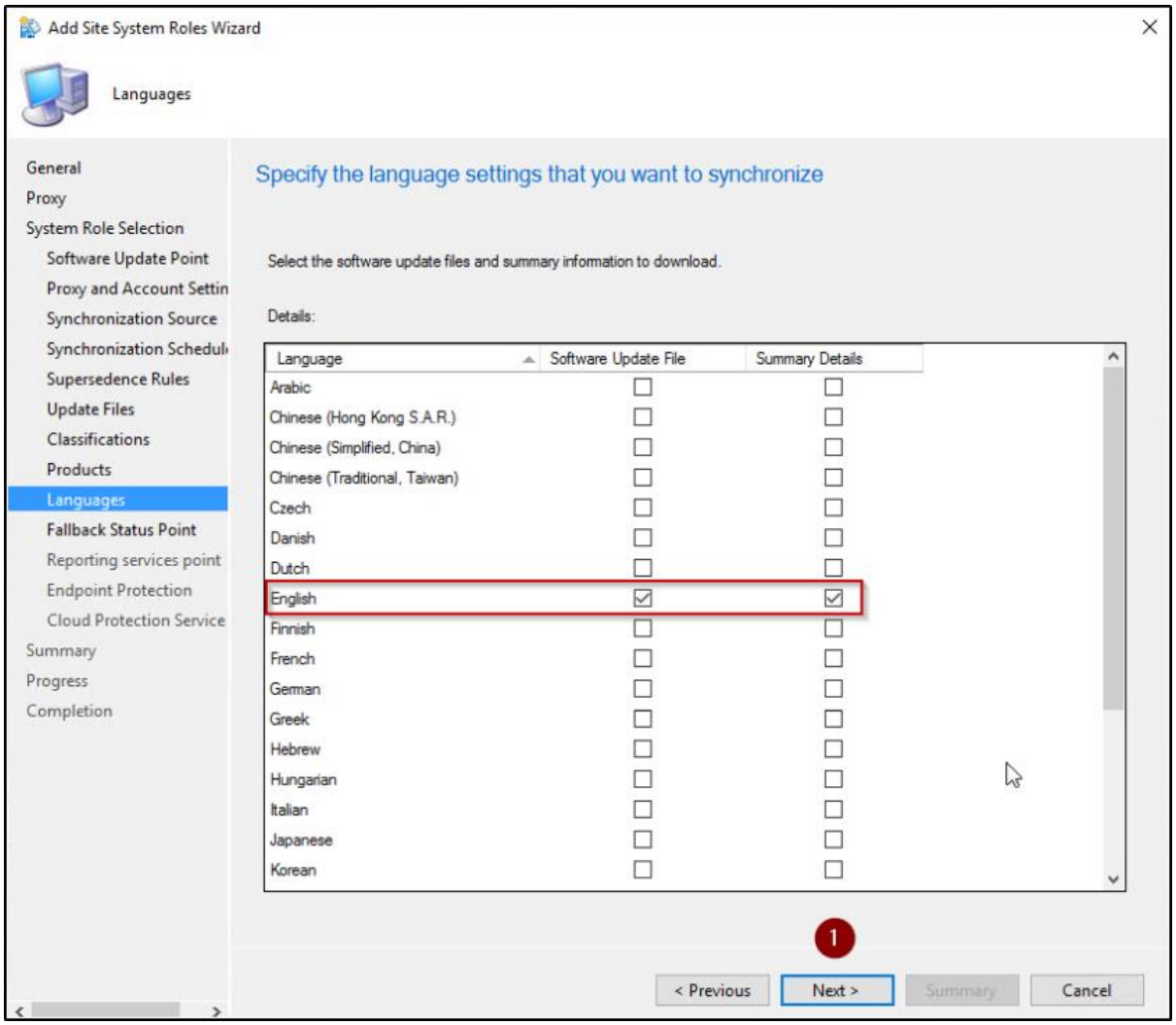
Figur 75: Roller i SCCM – Installasjon

I og med at vi ikke har kjørt en full synkronisering fra update katalogen, vil hverken Windows 10 eller Windows Server 2016 komme opp i listen nedenfor. Vi velger derfor kun Windows 7 midlertidig, og legger til Windows 10 og Windows server 2016 senere. Vi trykker **Next**.



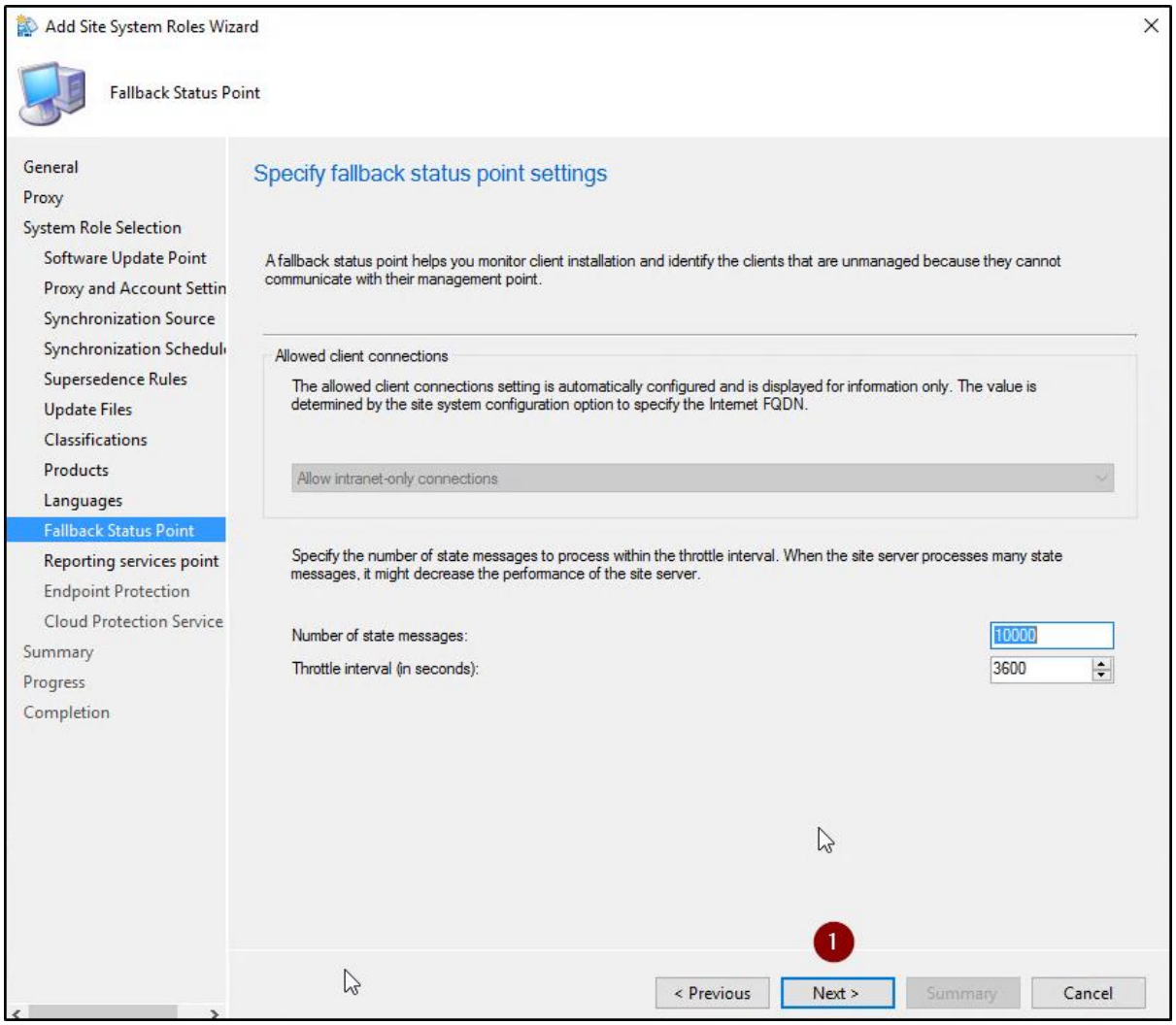
Figur 76: Roller i SCCM – Installasjon

Velger språk og trykker **Next**.



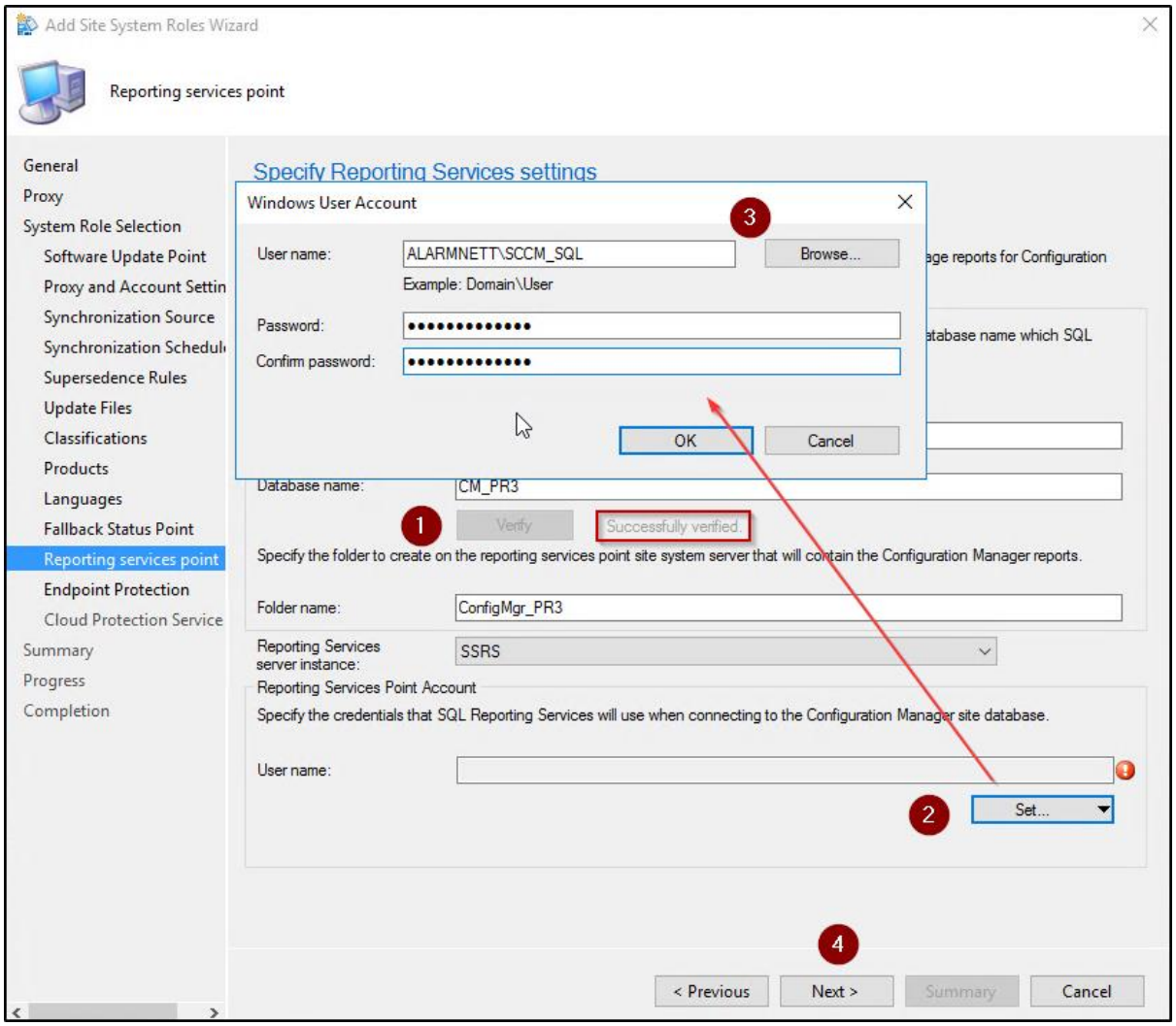
Figur 77: Roller i SCCM – Installasjon

Under punktet ***Fallback Status Point***, trykker vi **Next**.



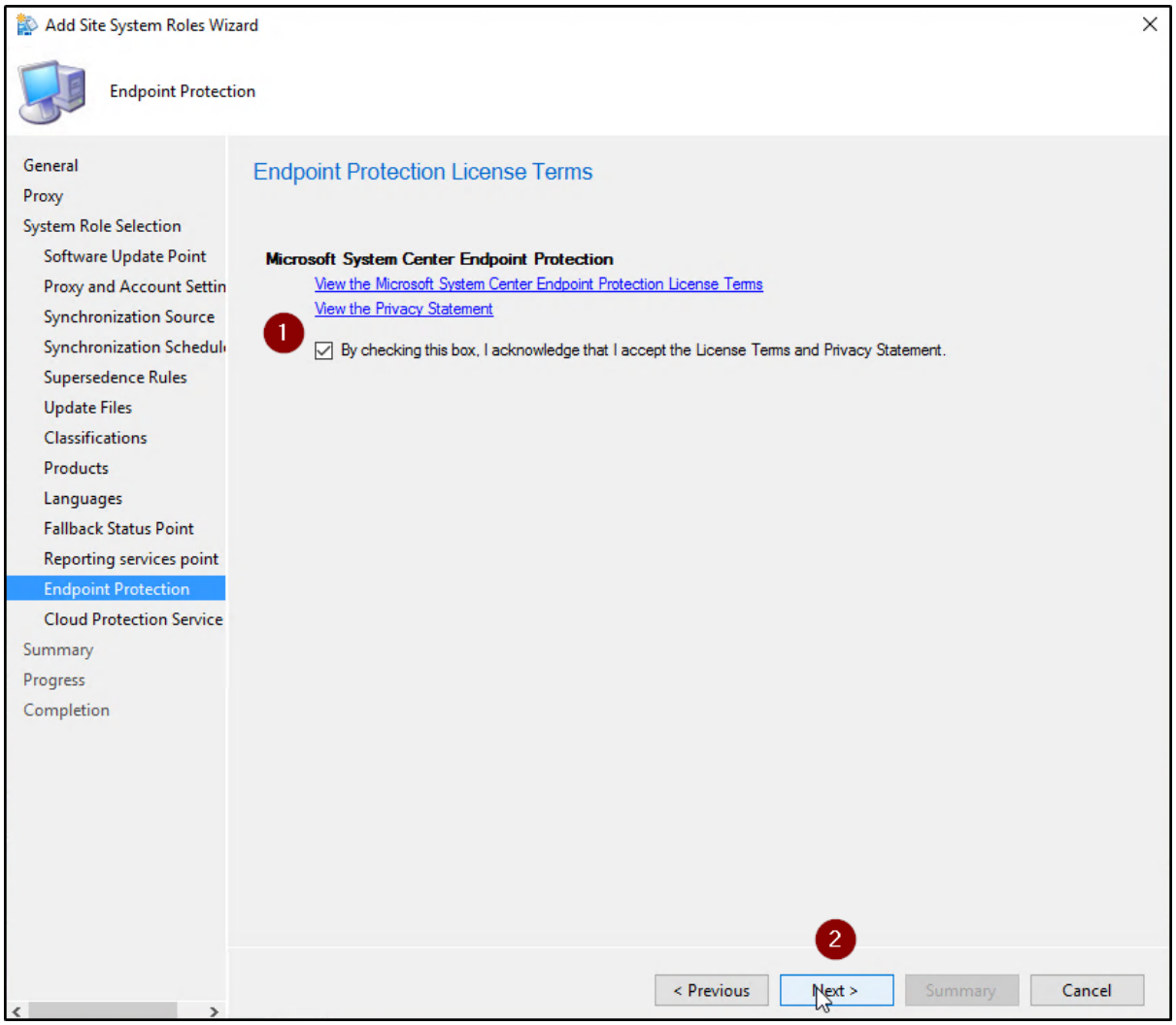
Figur 78: Roller i SCCM – Installasjon

Setter en brukerkonto som skal brukes til å laste opp service reports med. Gjør dette ved å trykke på **Set**, velger brukeren, i vårt tilfelle velger vi å ta i bruk brukeren: *SCCM_SQL*. Skriver inn passord og trykker **OK.** Deretter trykker vi **Next**.



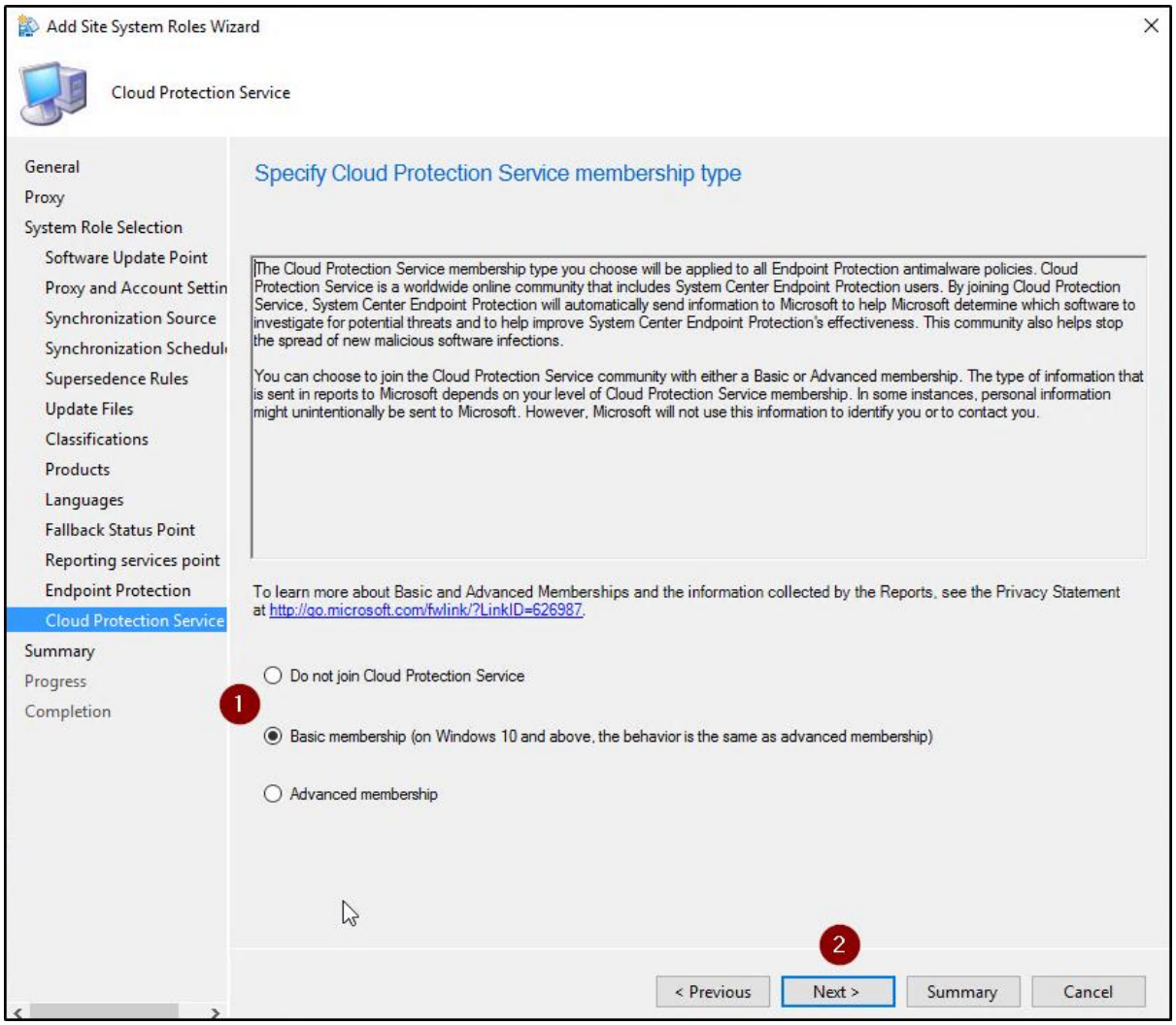
Figur 79: Roller i SCCM – Installasjon

Aksepterer Terms of Service og trykker **Next**.



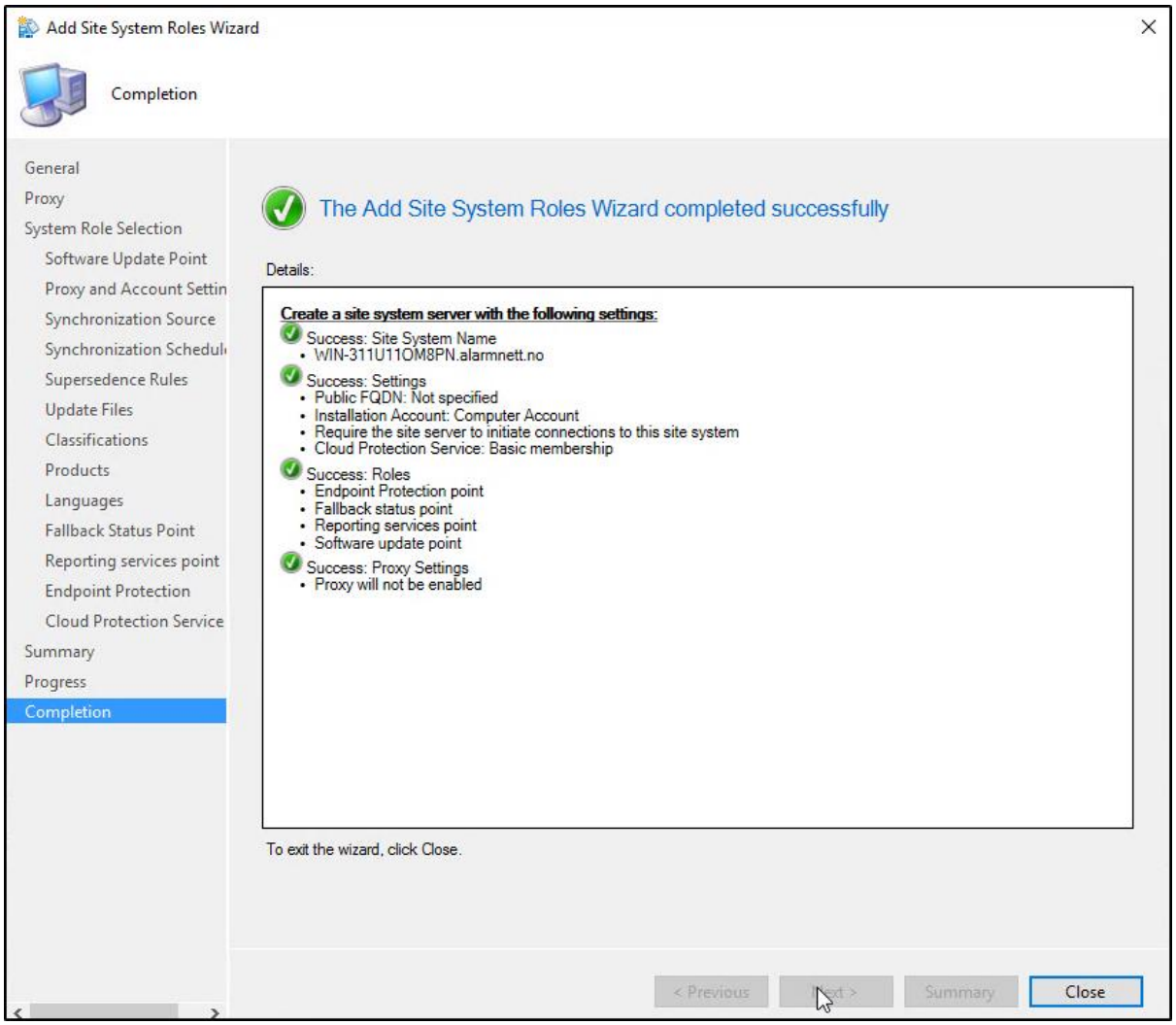
Figur 80: Roller i SCCM – Installasjon

Under ***Cloud Protection Services***, velger vi *Basic membership* og trykker **Next**.



Figur 81: Roller i SCCM – Installasjon

Ser til at installasjonene av de enkelte rollene har blitt gjennomført.

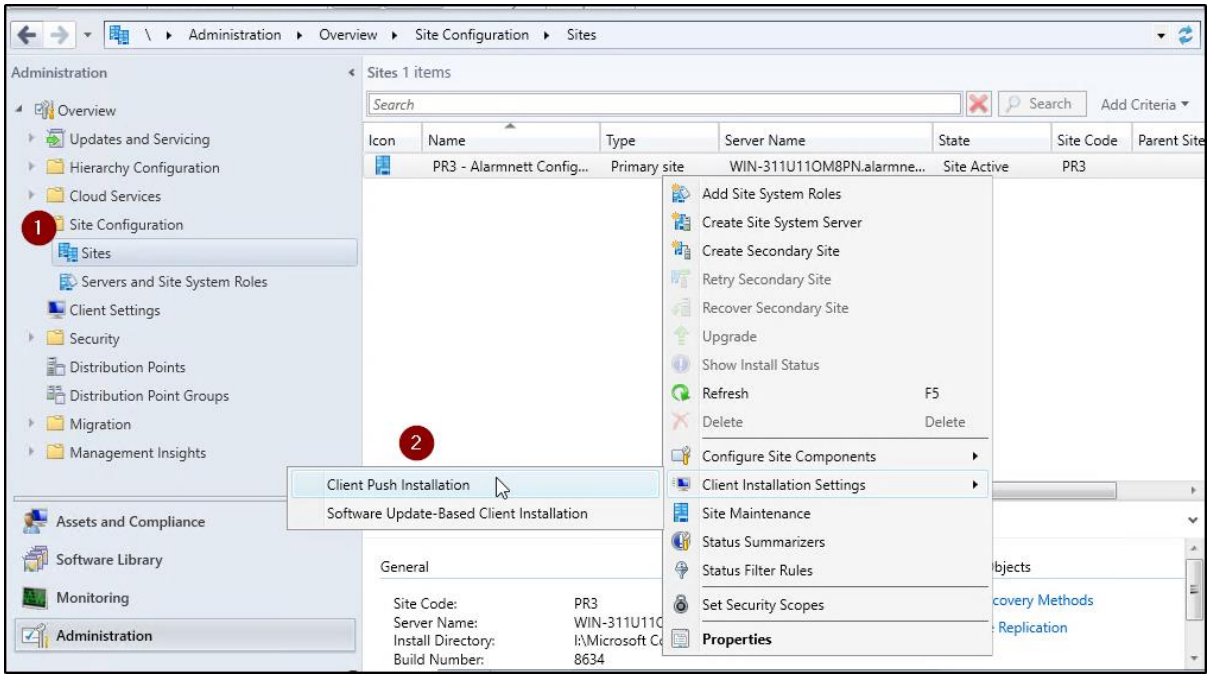


Figur 82: Roller i SCCM – Installasjon

Konfigurasjon av Client Push Account

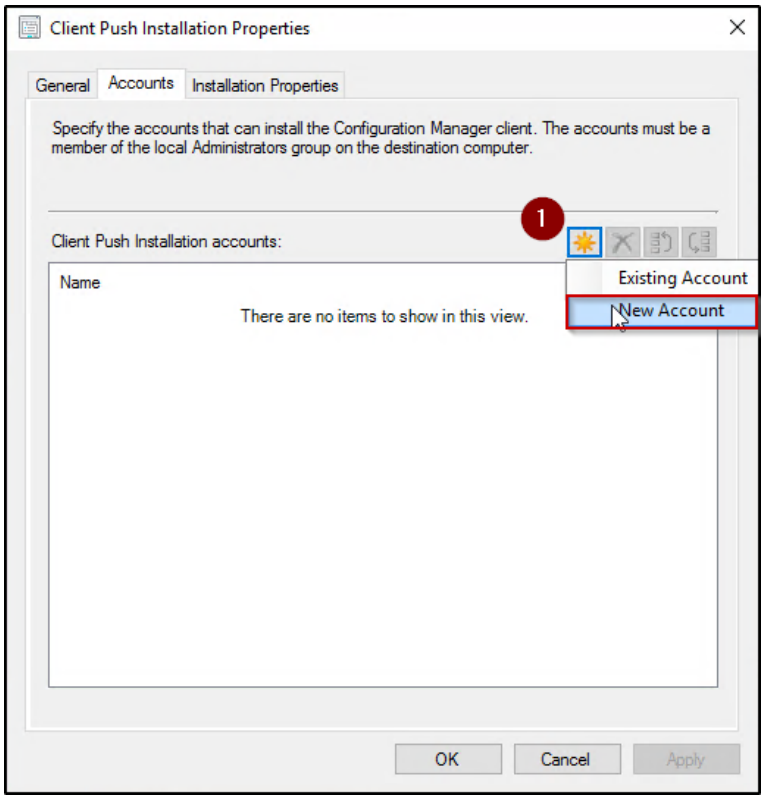
Brukes for å installere SCCM klienten (Client) på maskiner og mobile enheter ved å ta i bruk Client push.

Navigerer oss til ***Administration*** og velger **Sites**. Høyreklikker på **Site System** rollen som vi opprettet tidligere og velger **Client Push Installation.**



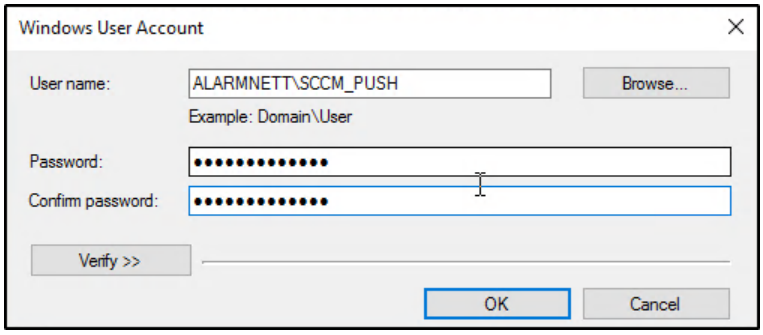
Figur 83: Konfigurasjon av Client Push Account

Under ***Accounts***, velger vi **New Account.**



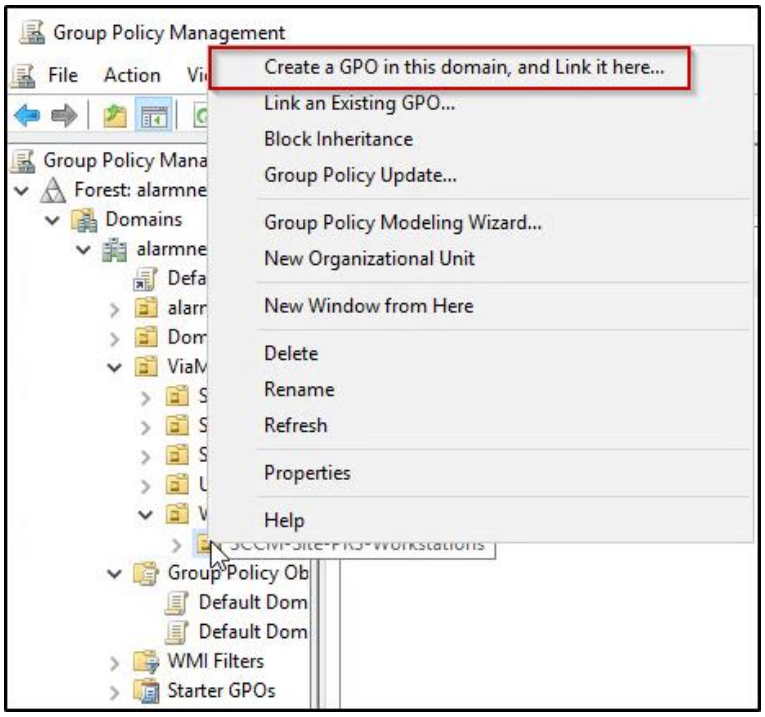
Figur 84: Konfigurasjon av Client Push Account

Vi tar i bruk *SCCM_PUSH* brukeren vår og skriver inn passord og trykker **OK**.



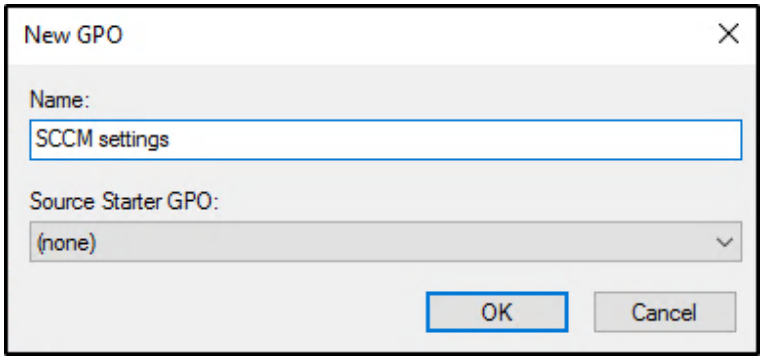
Figur 85: Konfigurasjon av Client Push Account

Går deretter inn på **Group Policy Management** og velger å opprette en ny GPO.



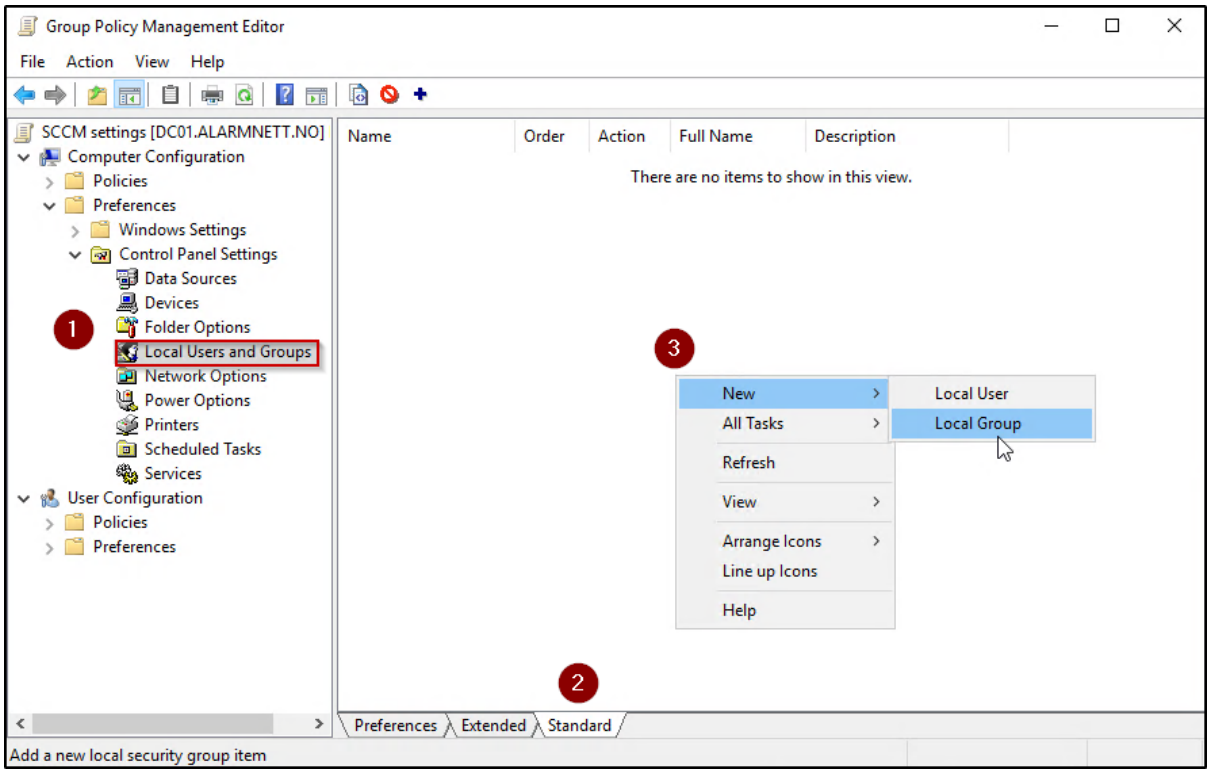
Figur 86: Konfigurasjon av Client Push Account

Gir den et navn og trykker **OK.**



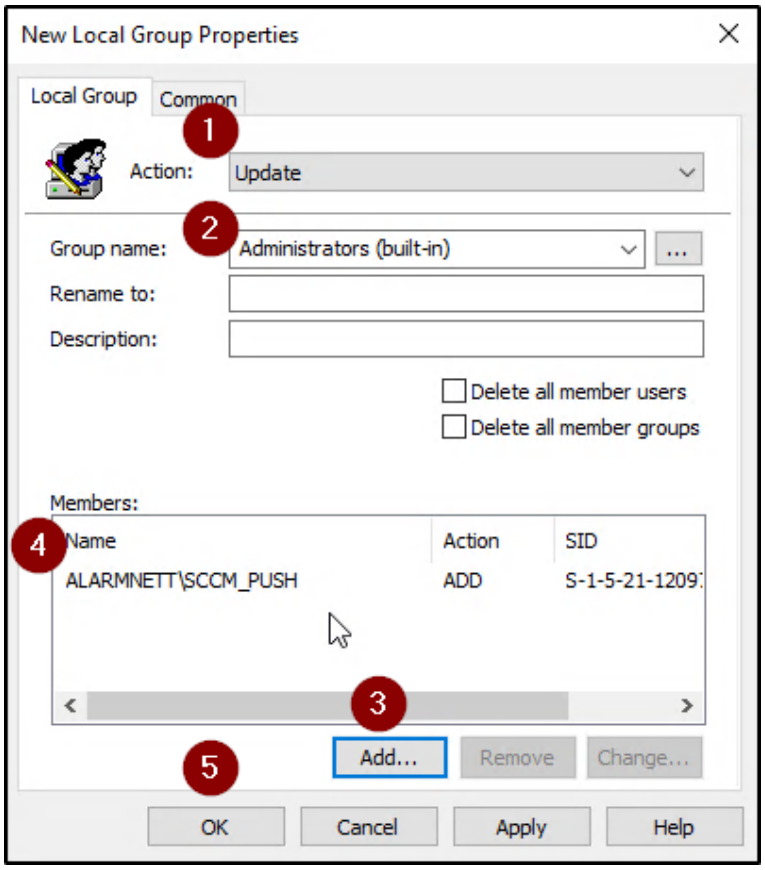
Figur 87: Konfigurasjon av Client Push Account

Går ned til ***Local Users and Groups*** og velger **New** og oppretter en **Local Group**.



Figur 88: Konfigurasjon av Client Push Account

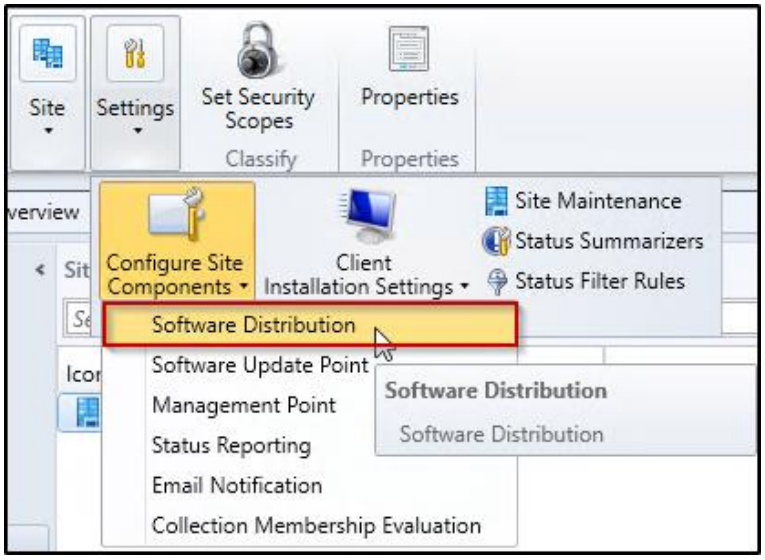
Ser til at alt stemmer i forhold til skjermbildet nedenfor og trykker **OK**.



Figur 89: Konfigurasjon av Client Push Account

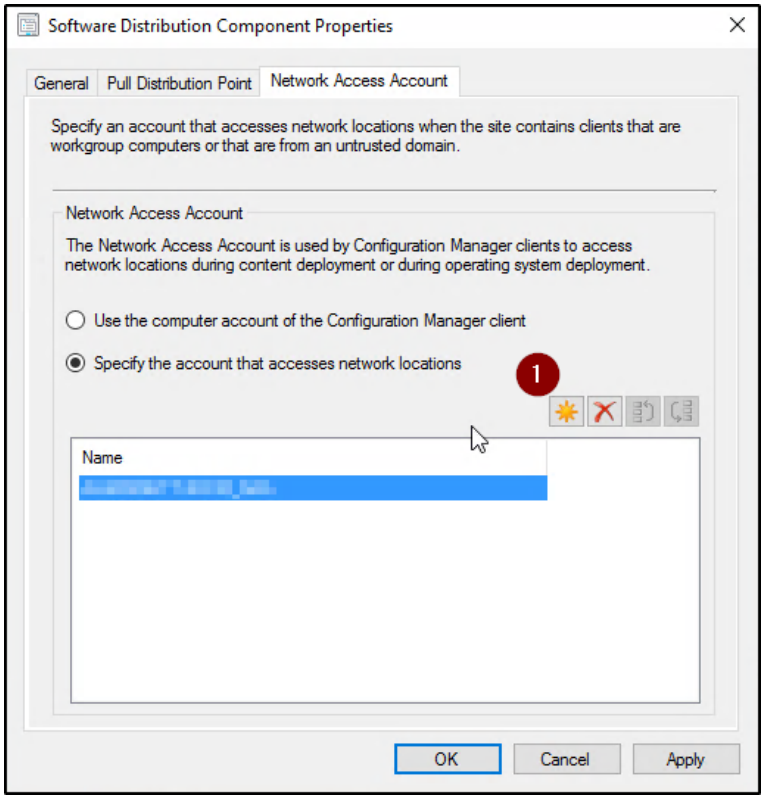
Konfigurasjon av Network Access Account

Brukes av maskiner som ikke er domain joined. Dette vil da komme til nytte dersom man skal utføre OS deployment til «tomme maskiner» eller andre maskiner som er med i en workgroup. Vi velger derfor å gå gjennom konfigurasjonen nå, da det er en fin funksjon, selv om vi ikke nødvendigvis kommer til å ta den i bruk.



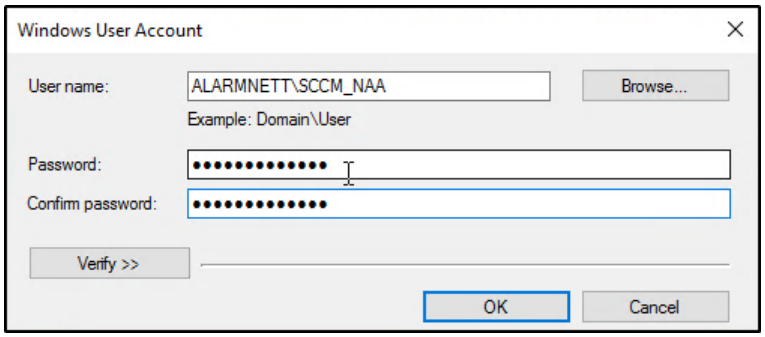
Figur 90: Konfigurasjon av Network Access Account

Velger en bruker som skal aksessere nettverkslokasjoner.



Figur 91: Konfigurasjon av Network Access Account

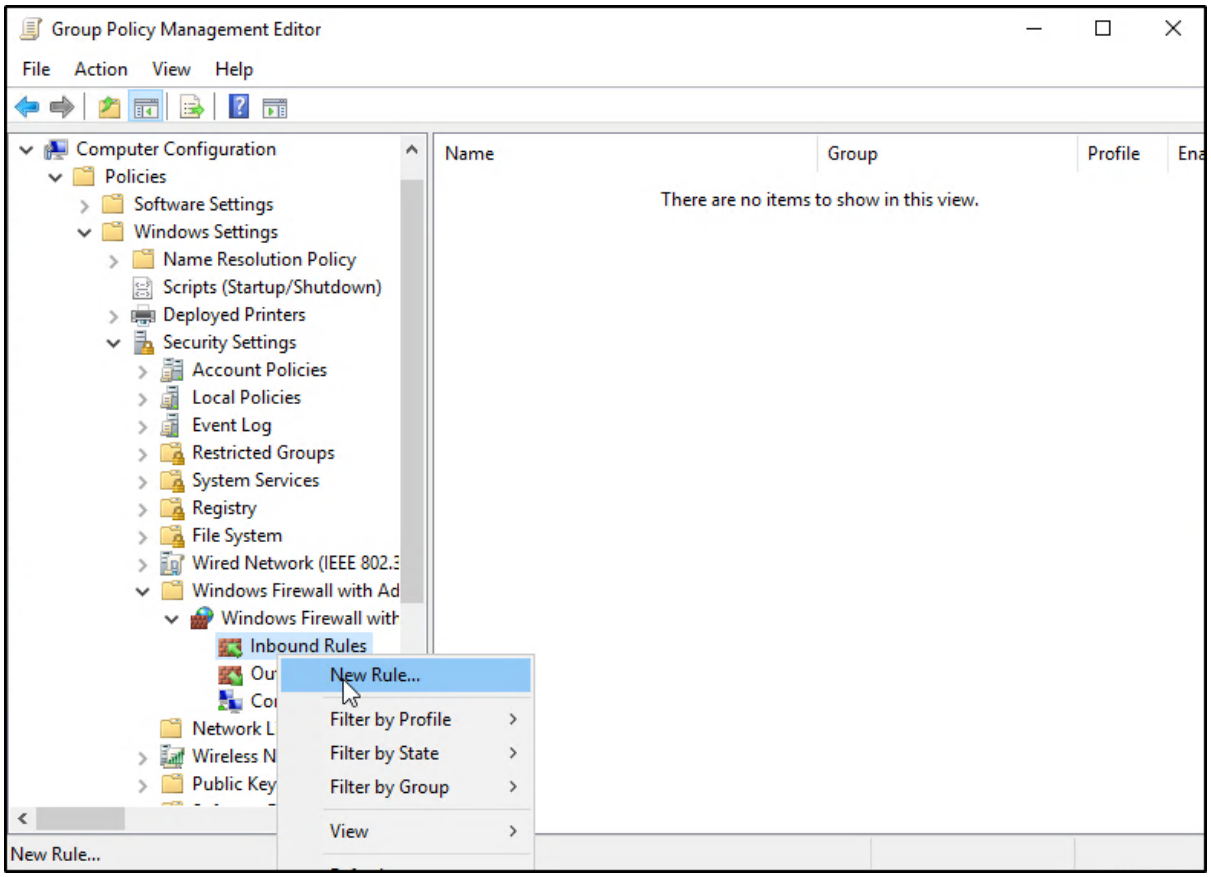
Vi tar i bruk brukeren: *SCCM_NAA* og skriver inn passord, deretter trykker vi på **OK**.



Figur 92: Konfigurasjon av Network Access Account

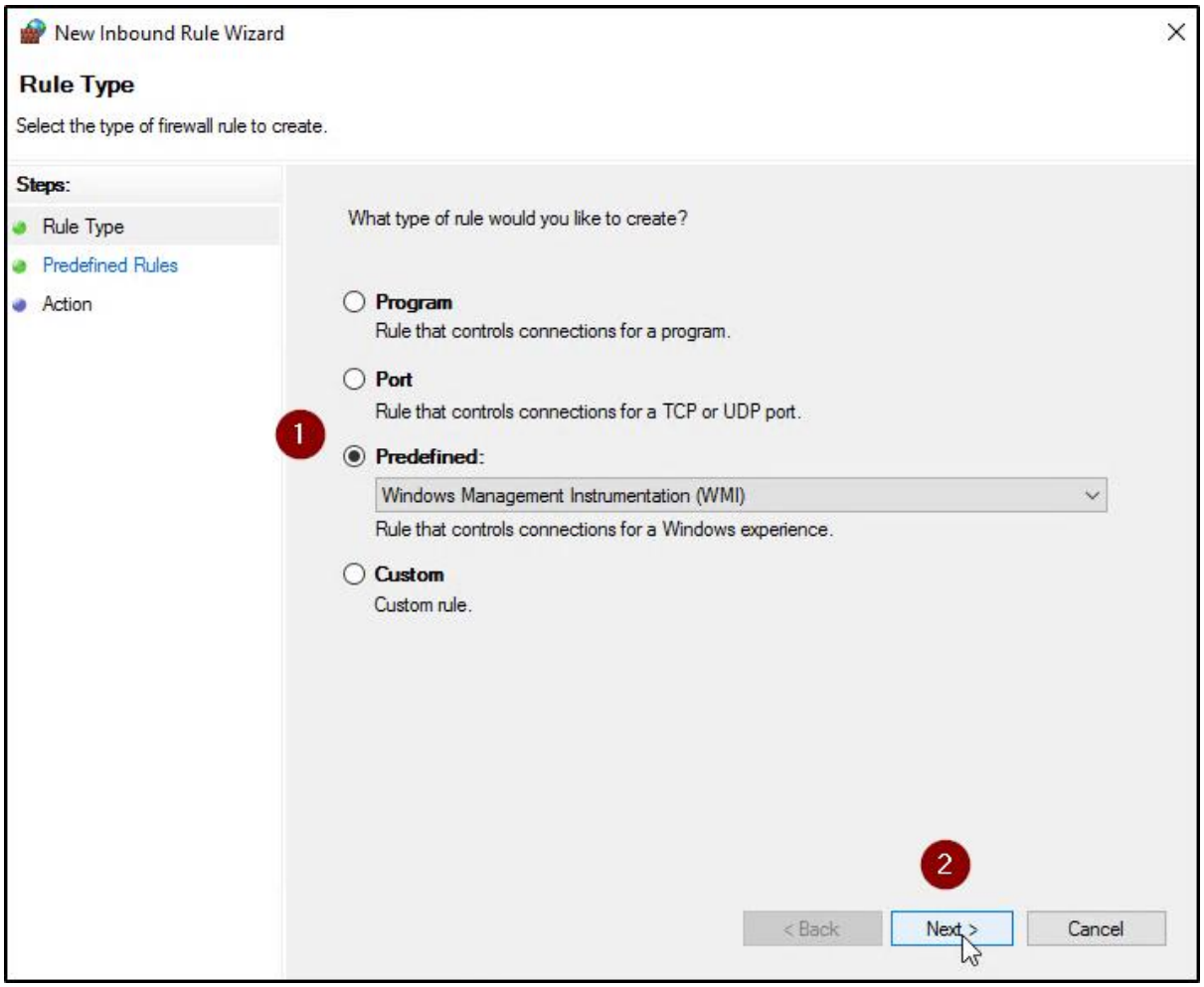
Konfigurasjon av Group Policy Firewall Exceptions for WMI

Vi skal nå se på hvordan man kan sette opp Group Policy Firewall Exceptions for WMI. Vi benytter Group Policy Management editor for å gjøre dette.



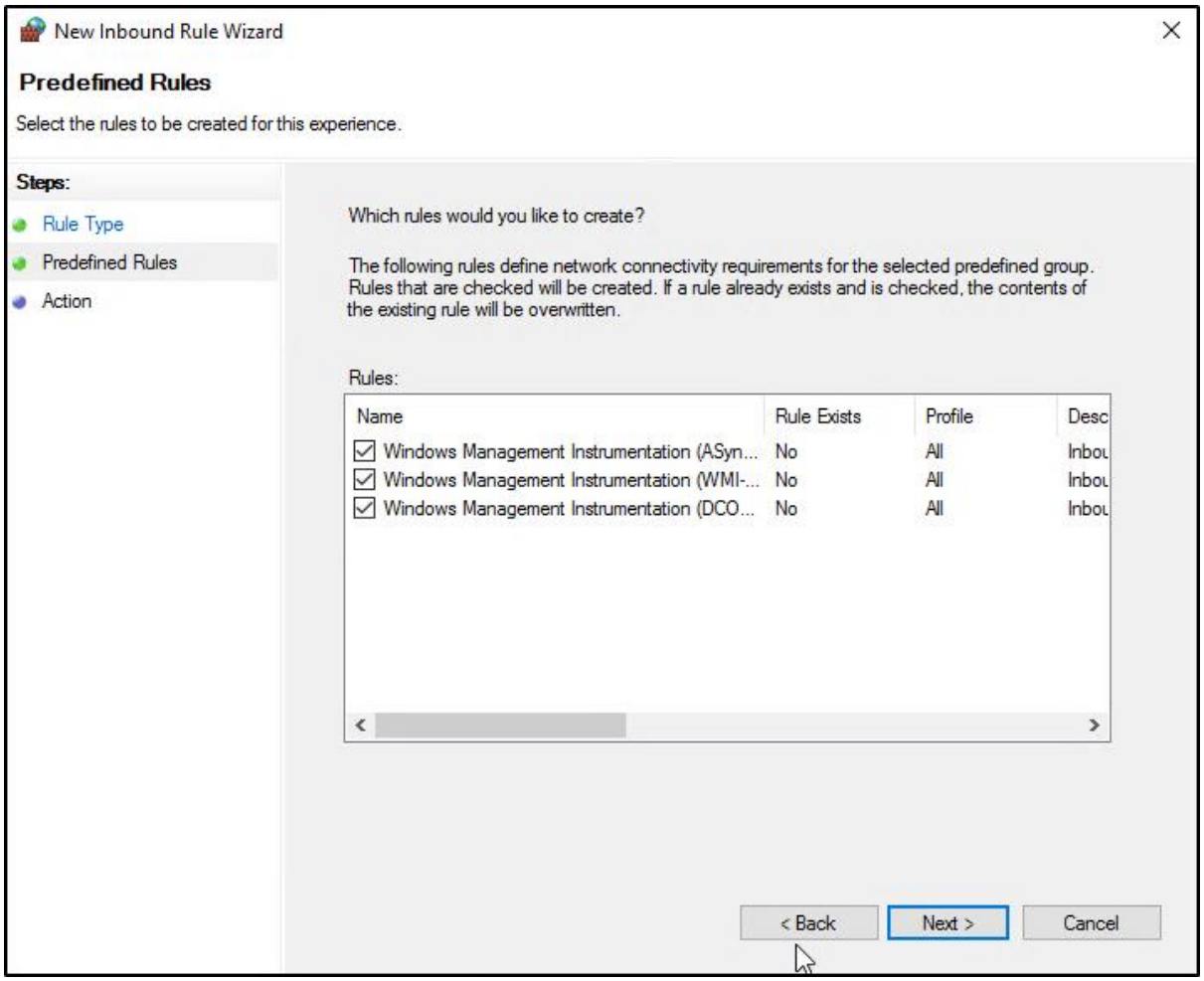
Figur 93: Konfigurasjon av Group Policy Firewall Exceptions for WMI

Velger **Predifined (Windows Management Instrumentation (WMI))** og trykker **Next**.



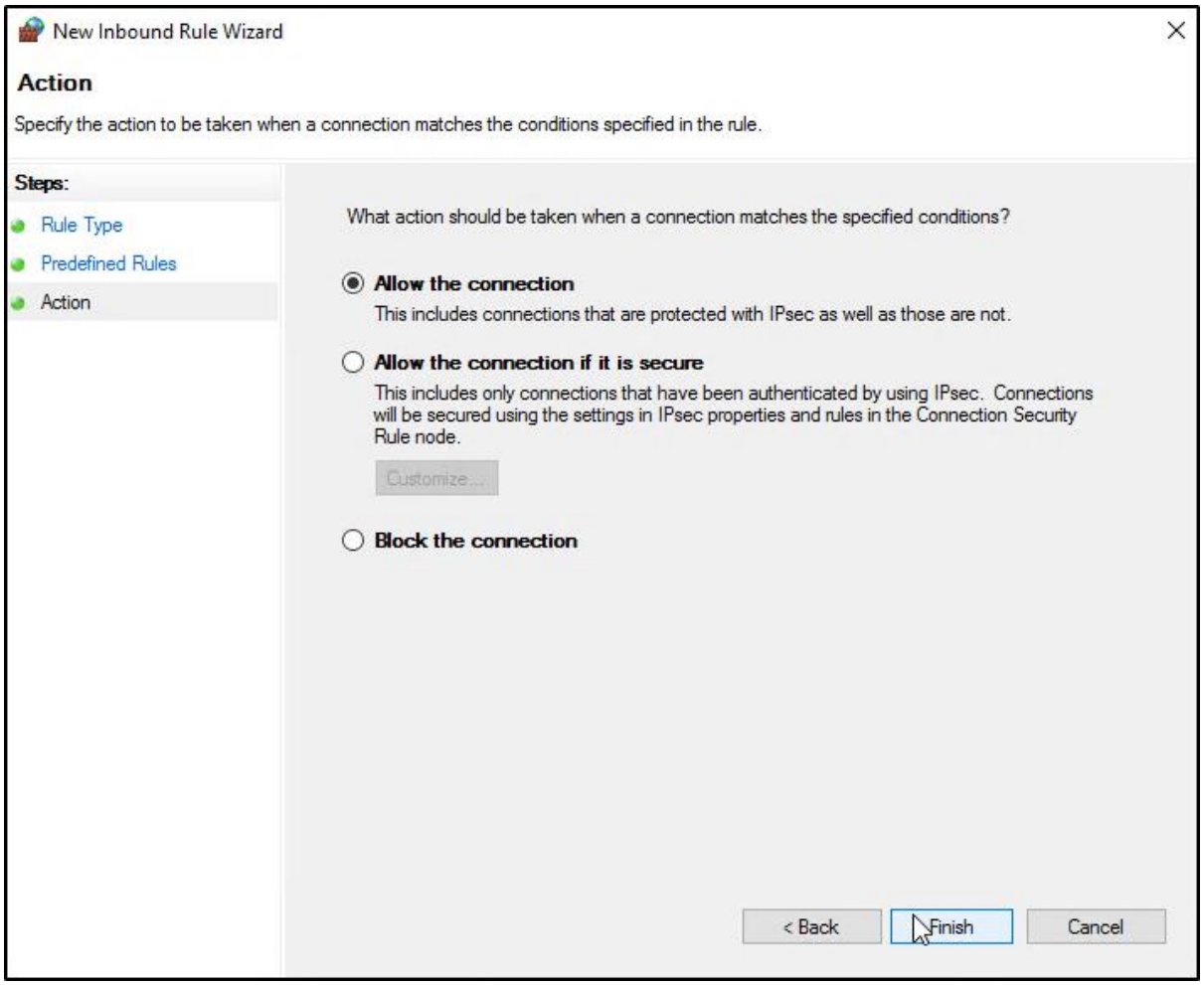
Figur 94: Konfigurasjon av Group Policy Firewall Exceptions for WMI

Ser til at samtlige *rules* er valgt under ***Predefined Rules*** og trykker **Next**.



Figur 95: Konfigurasjon av Group Policy Firewall Exceptions for WMI

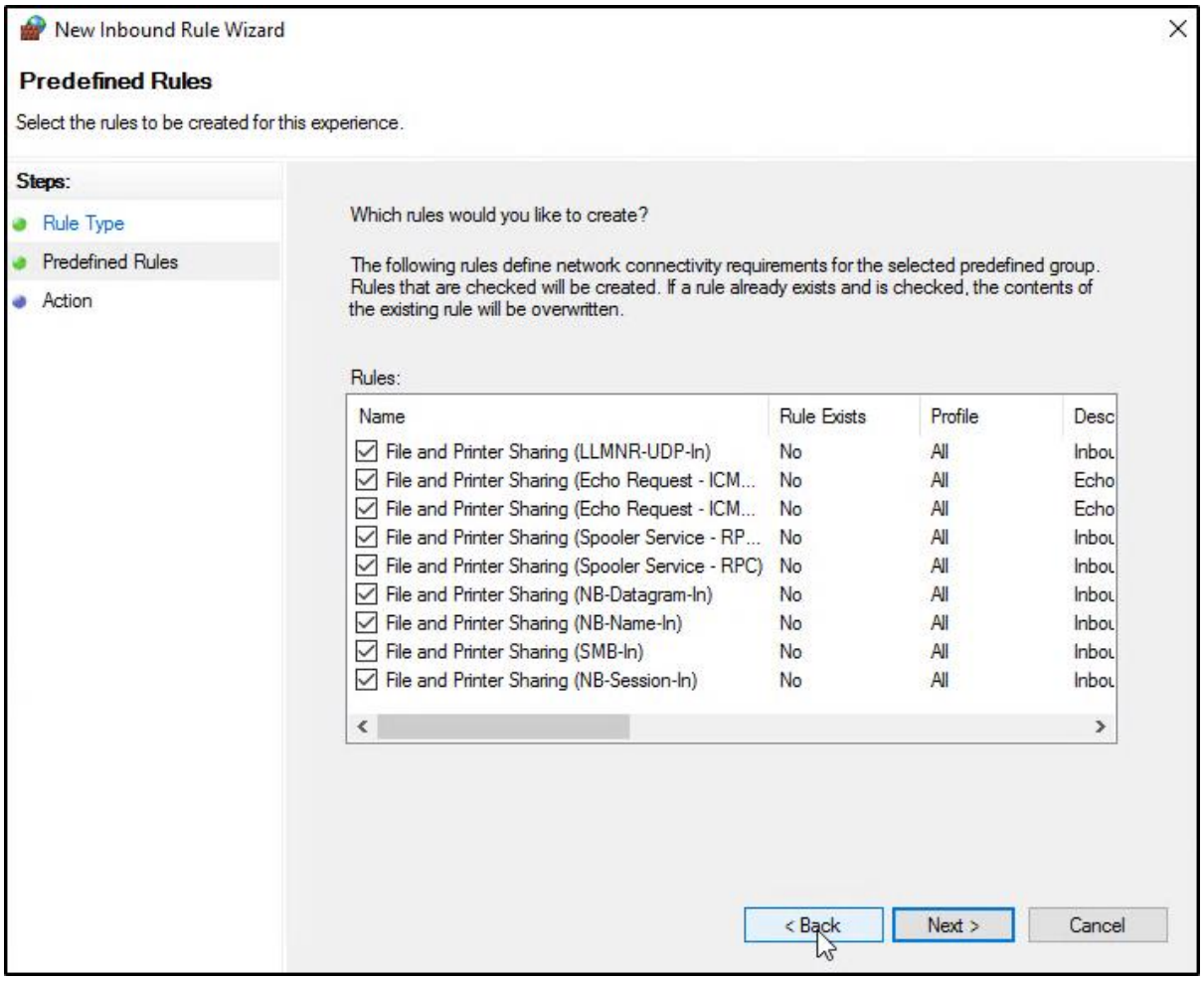
Under ***Action***, velger vi **Allow the connection** og trykker **Finish**.



Figur 96: Konfigurasjon av Group Policy Firewall Exceptions for WMI

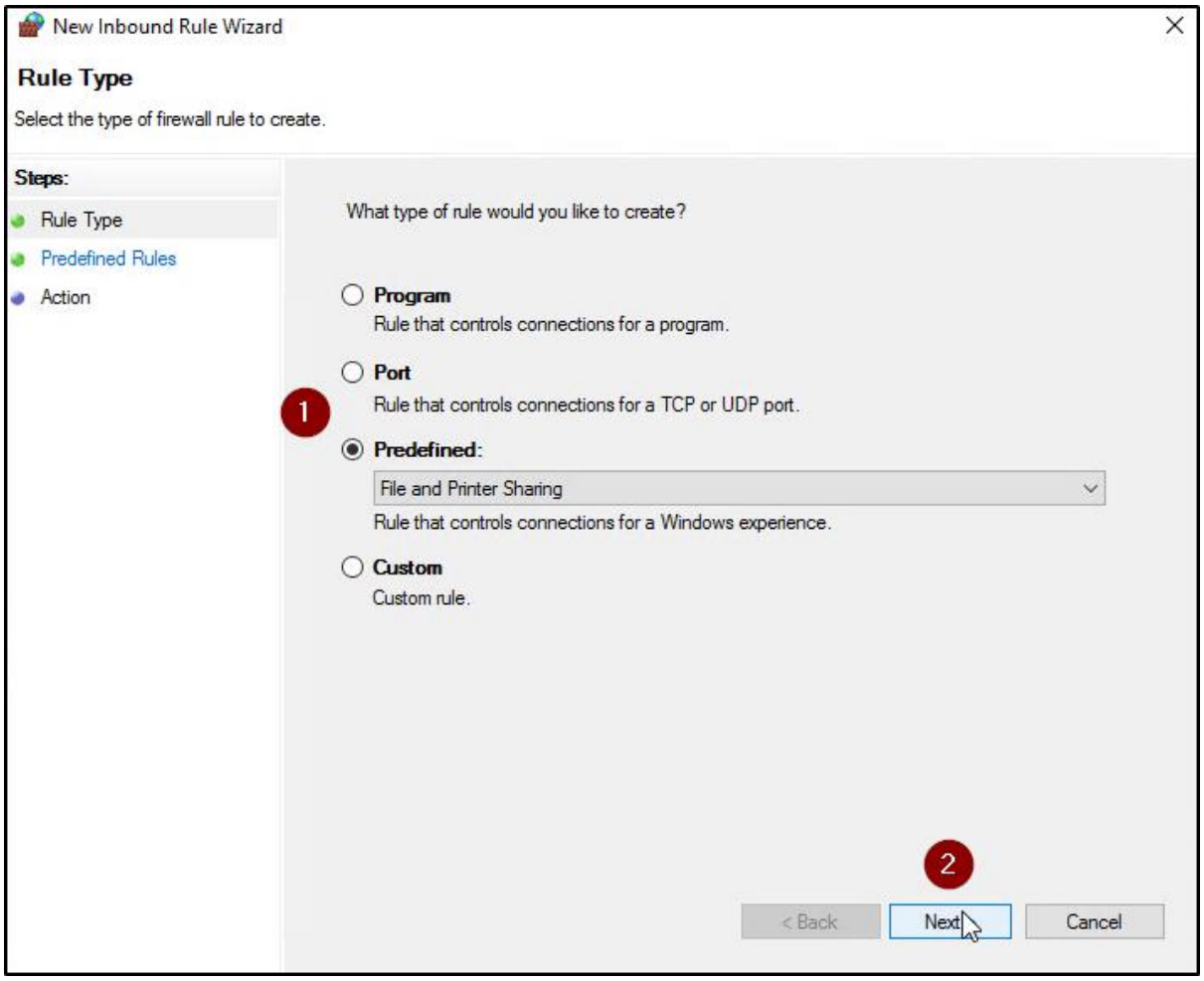
Konfigurasjon av File sharing

Vi skal nå sette opp tilgang i brannmur for File sharing. Velger å opprette en **New Inbound Rule**. Ser til at alle reglene er huket av og trykker **Next**.



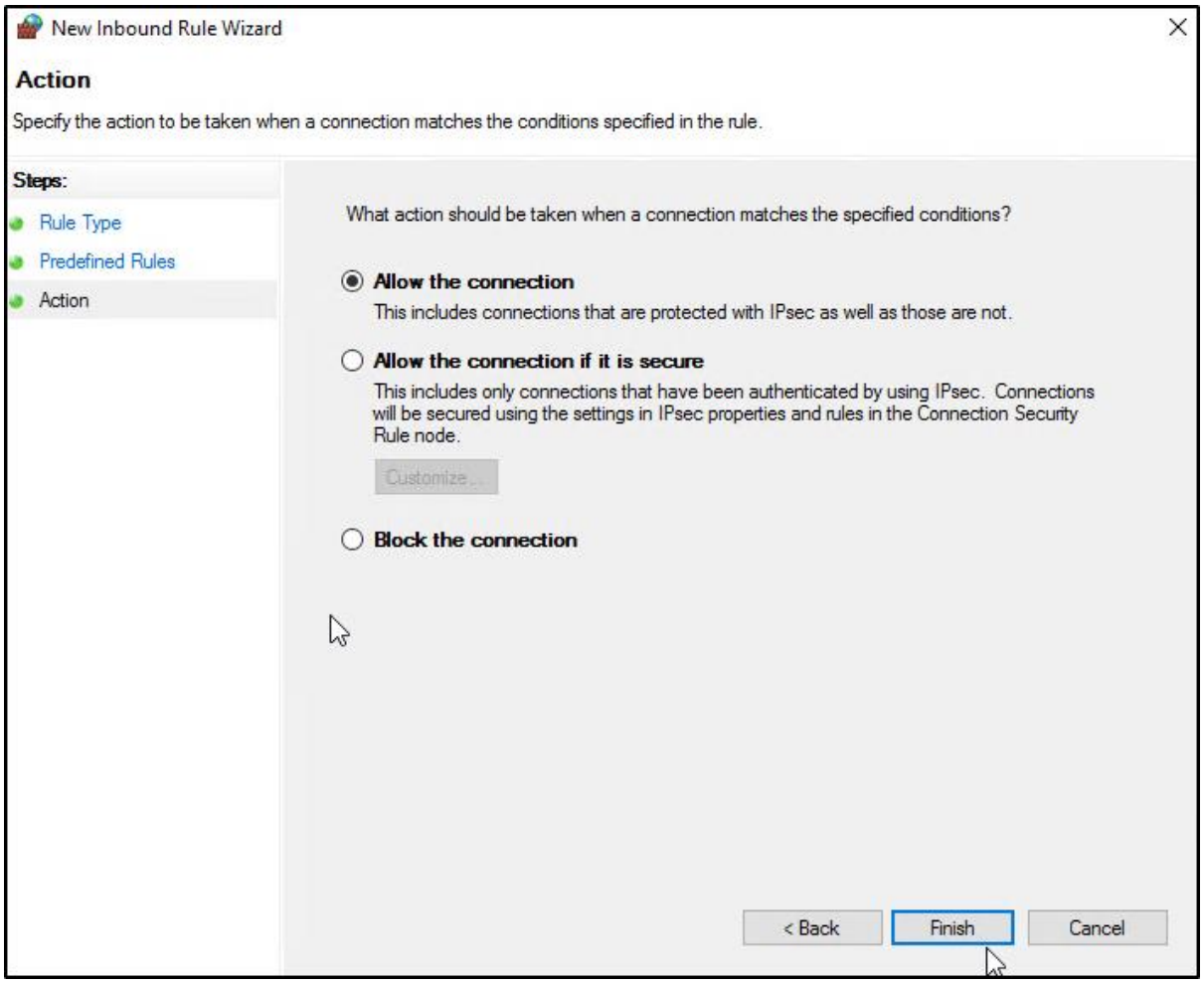
Figur 97: Konfigurasjon av File Sharing

Under ***Predefined Rules***, velger vi **File and Printer Sharing** og trykker **Next**.



Figur 98: Konfigurasjon av File Sharing

Under ***Action,*** velger vi **Allow the connection** og trykker **Finish**.

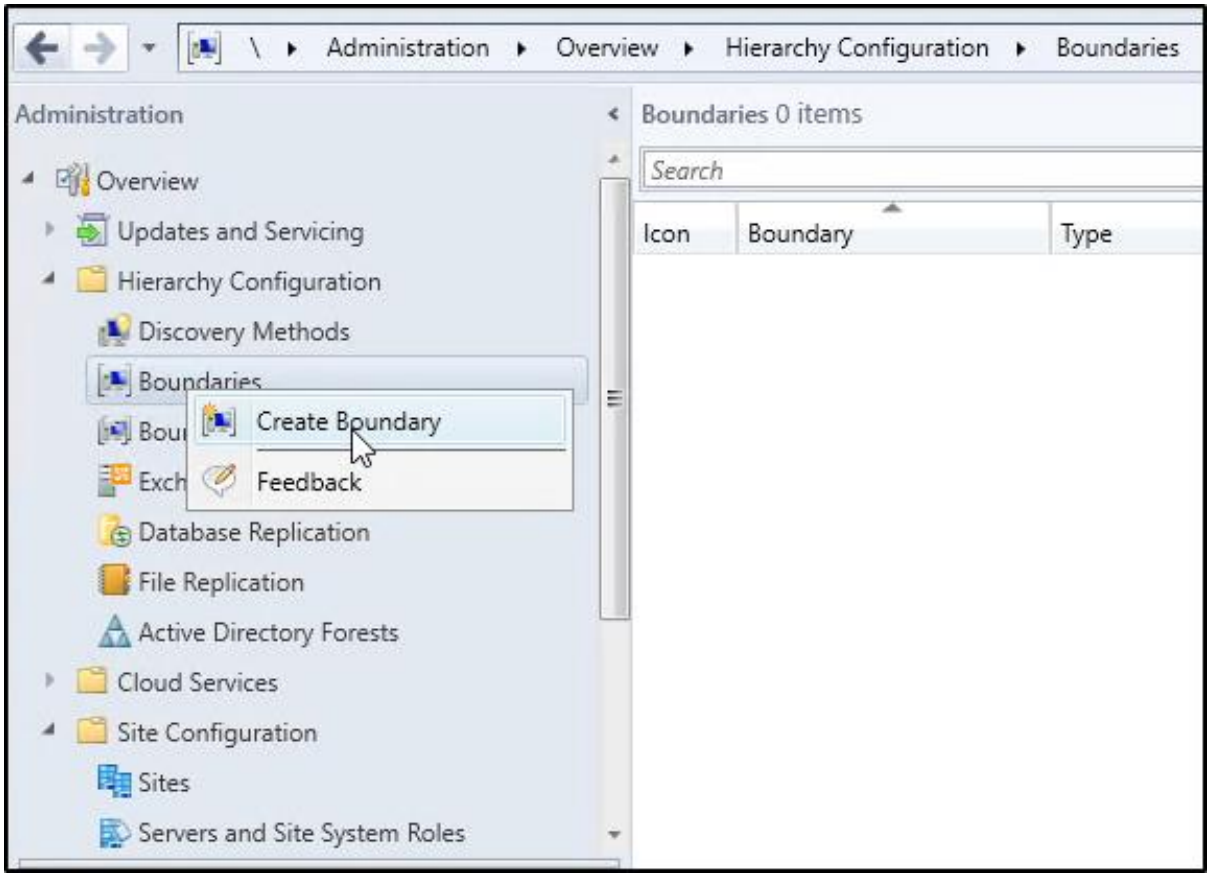


Figur 99: Konfigurasjon av File Sharing

Konfigurasjon av Boundaries and Boundary Groups

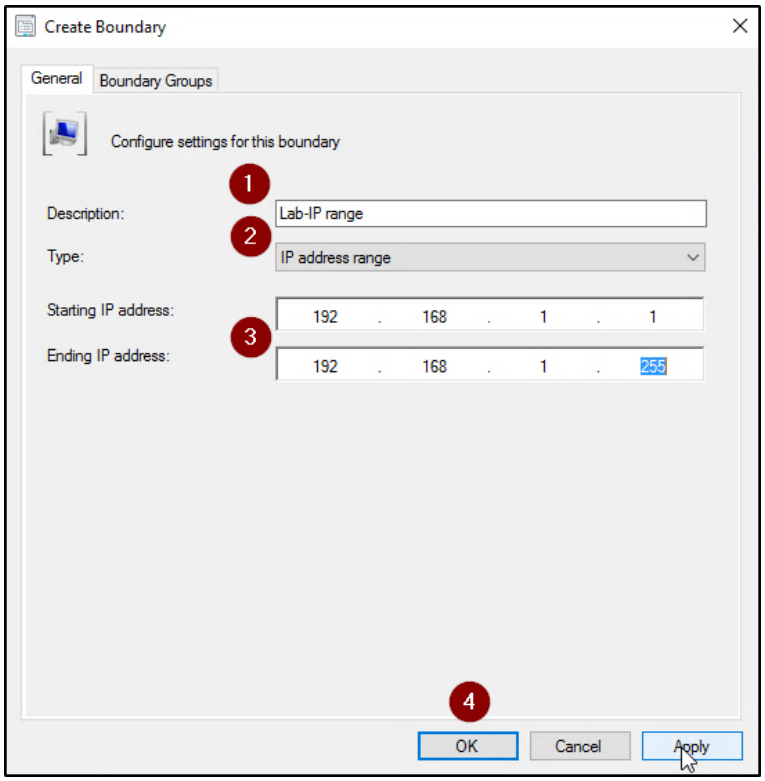
Vi konfigurerer Boundaries og Boundary Groups for å kunne definere nettverkslokasjoner i vårt nettverk hvor vi ønsker å administrere enheter.

Vi navigerer oss til ***Administration - Hierarchy Configuration*** og trykker **Create Boundary.**



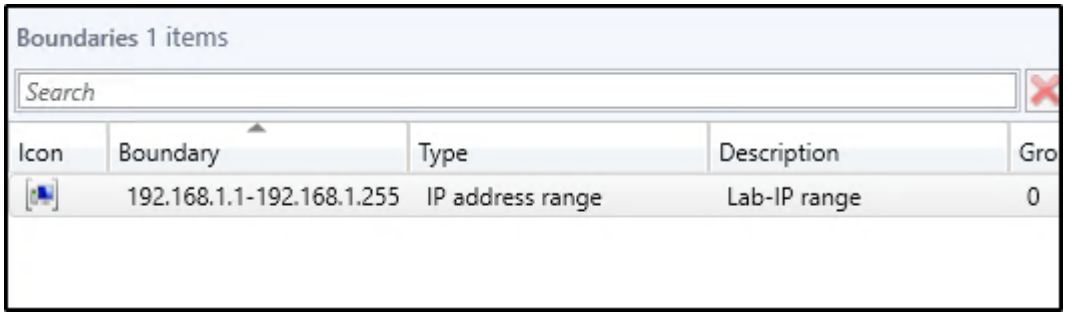
Figur 100: Konfigurasjon av Boundaries og Boundary Groups

Vi setter et **navn** og velger **start**- og **slutt-IP** og trykker **Apply**.



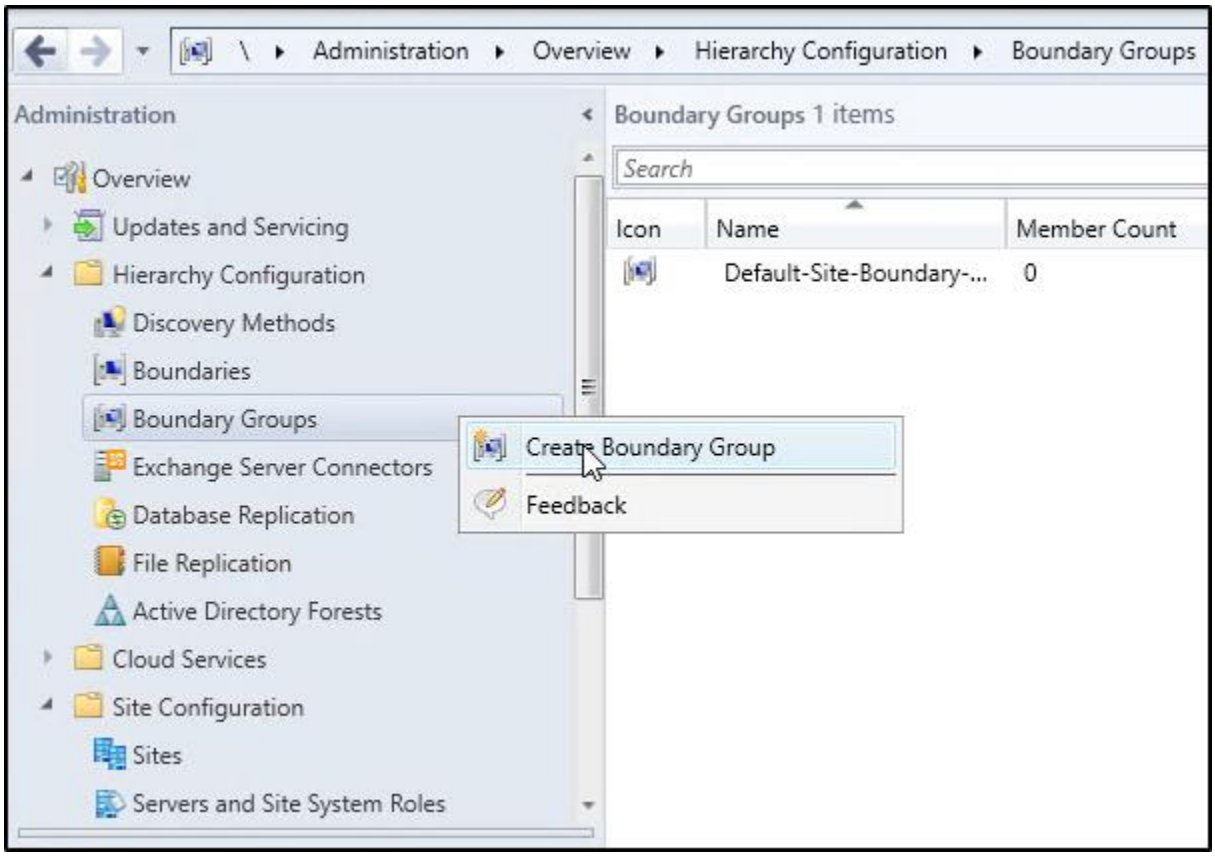
Figur 101: Konfigurasjon av Boundaries og Boundary Groups

Vi ser her at vi nå har fått en Boundary med satt IP-range.



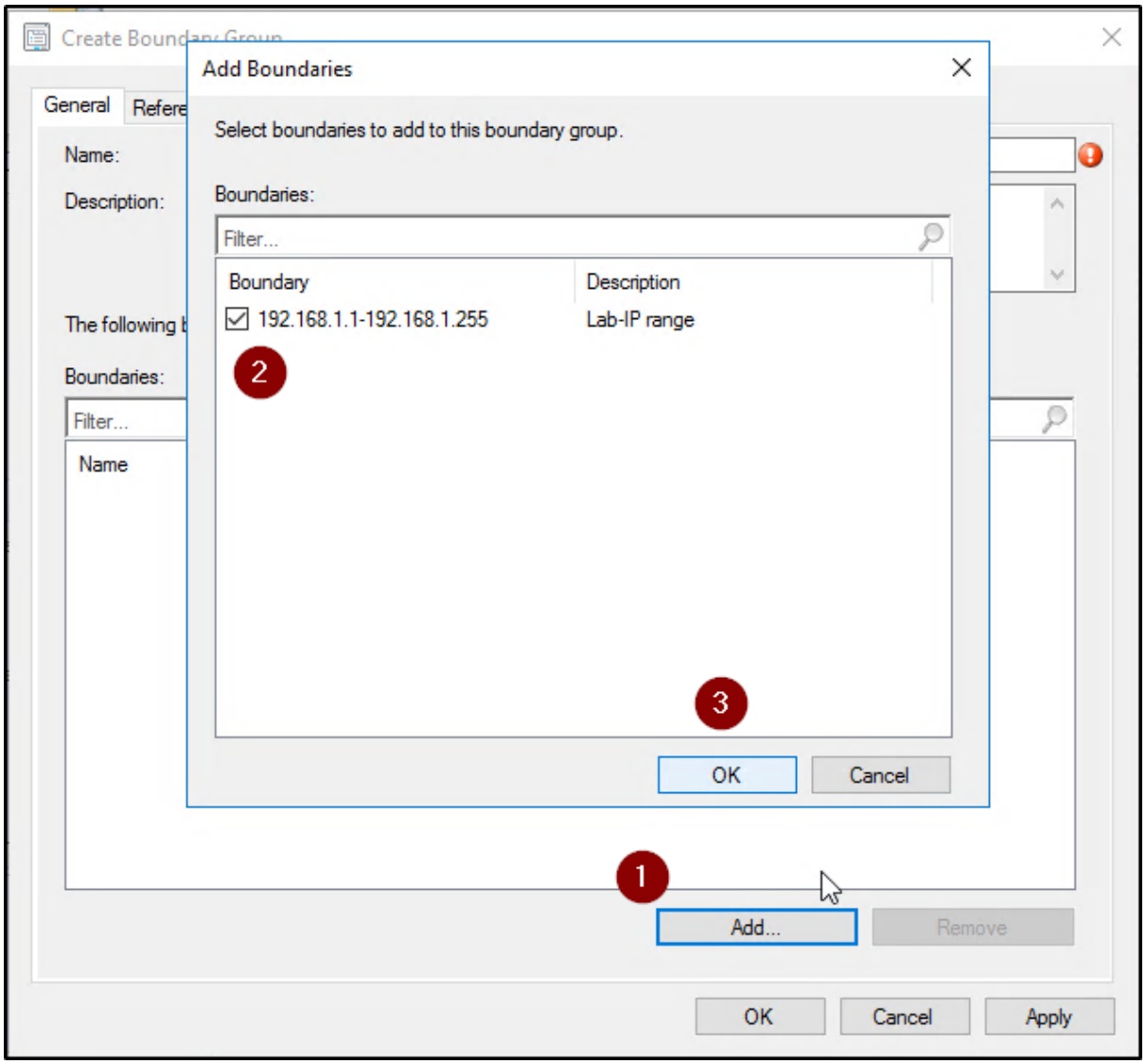
Figur 102: Konfigurasjon av Boundaries og Boundary Groups

Videre kan vi nå opprette en Boundary Group. Vi velger **Create Boundary Group**.



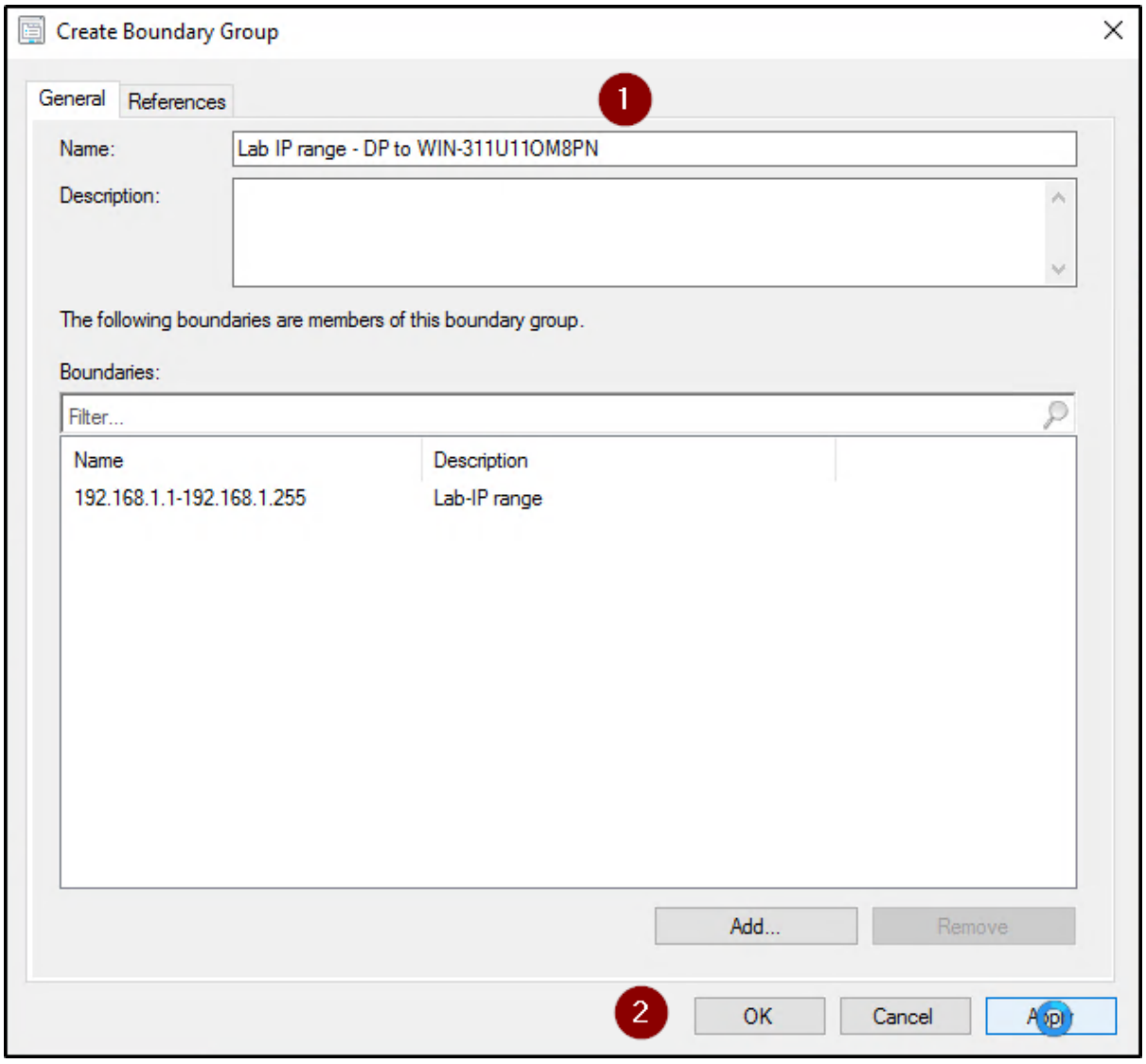
Figur 103: Konfigurasjon av Boundaries og Boundary Groups

Vi trykker på **Add…** og velger Boundary som vi lagde tidligere. Vi trykker på **Ok**.



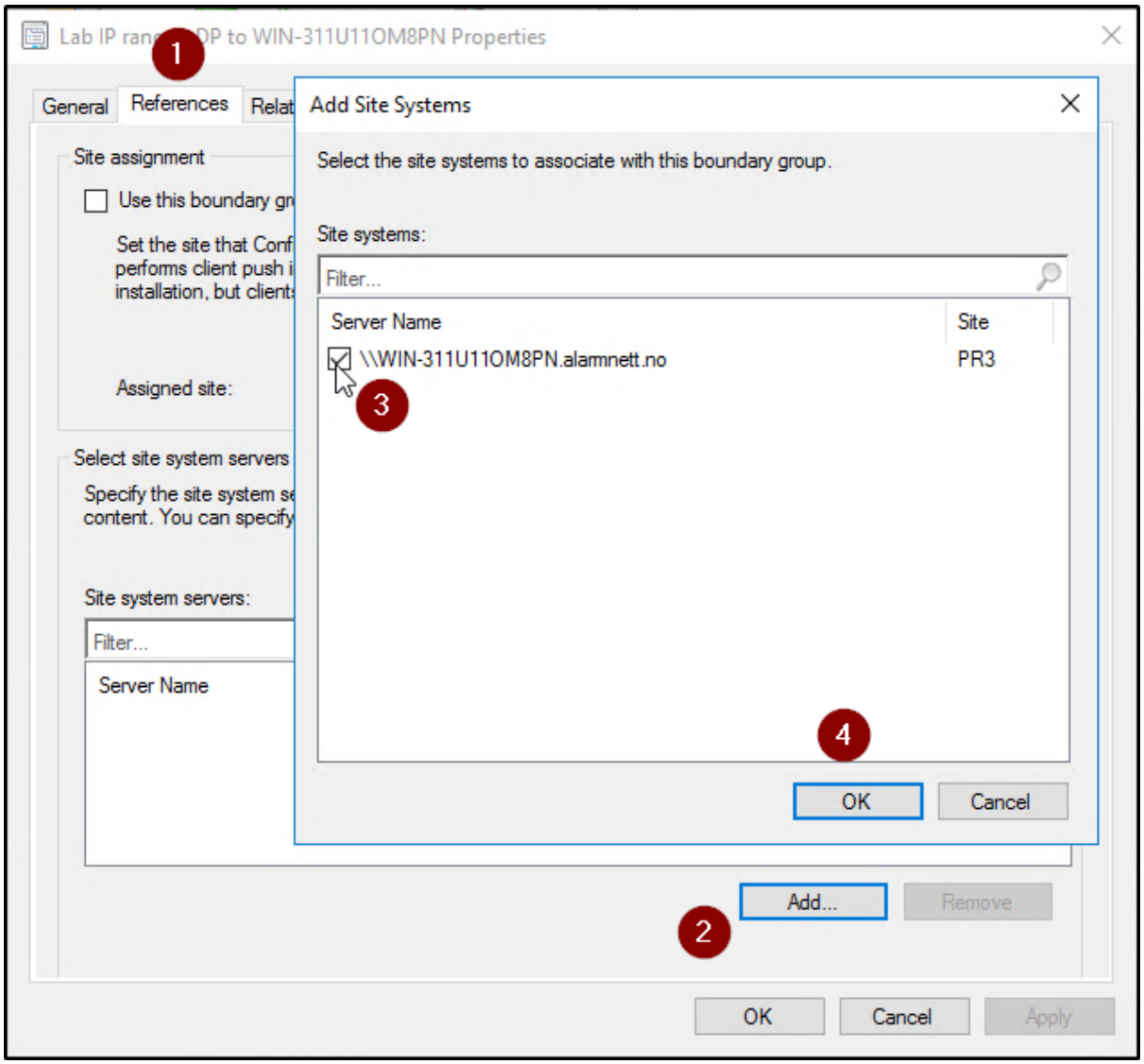
Figur 104: Konfigurasjon av Boundaries og Boundary Groups

Vi gir den et navn dersom dette ikke er satt fra før og trykker **Apply**.



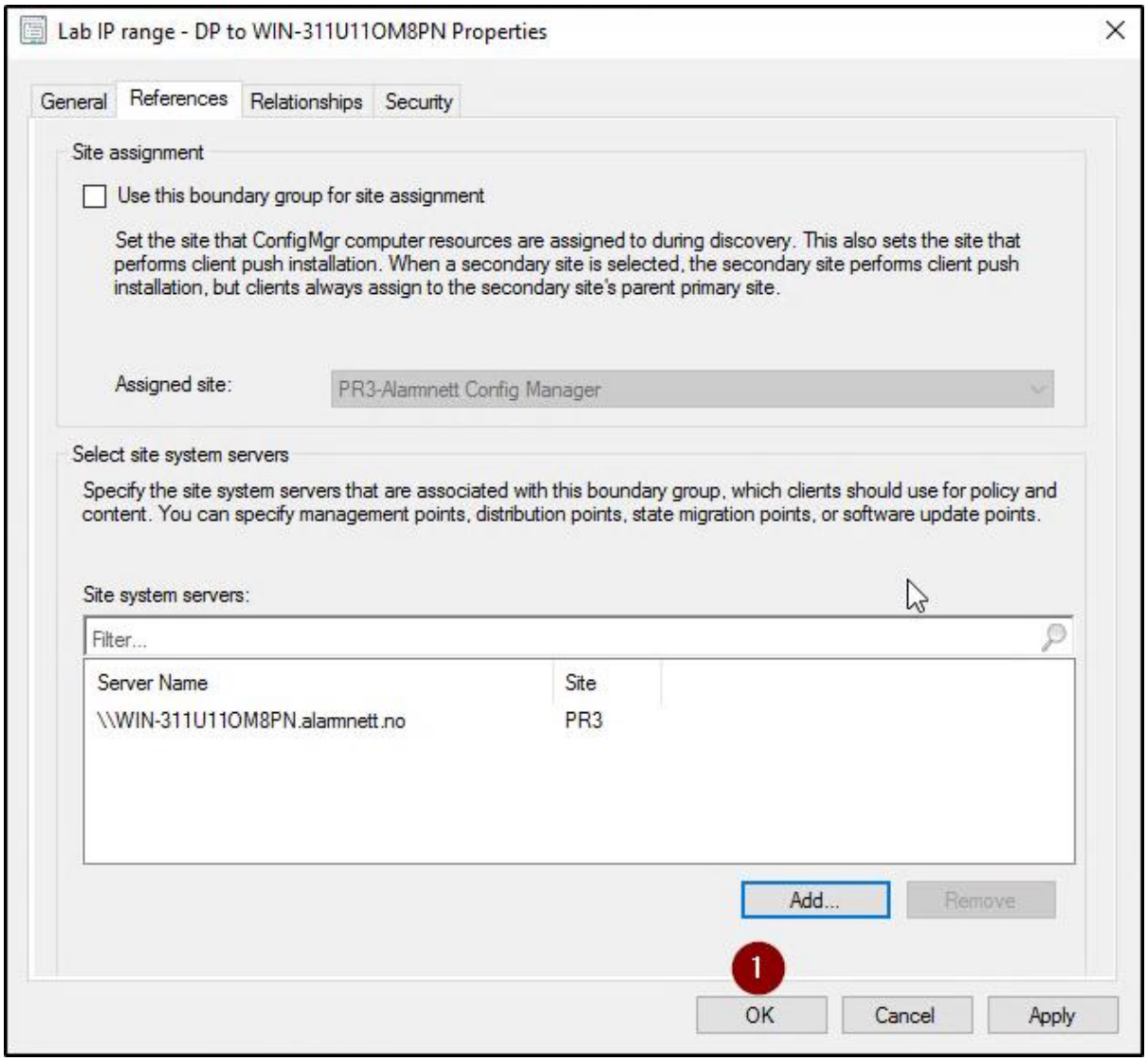
Figur 105: Konfigurasjon av Boundaries og Boundary Groups

Vi høyreklikker på Boundary-gruppen som vi lagde, og velger **Properties**. Deretter trykker vi på **References**, og huker av for hvilken Site System som det skal gjelde for. Vi trykker **OK** og deretter **Add…**



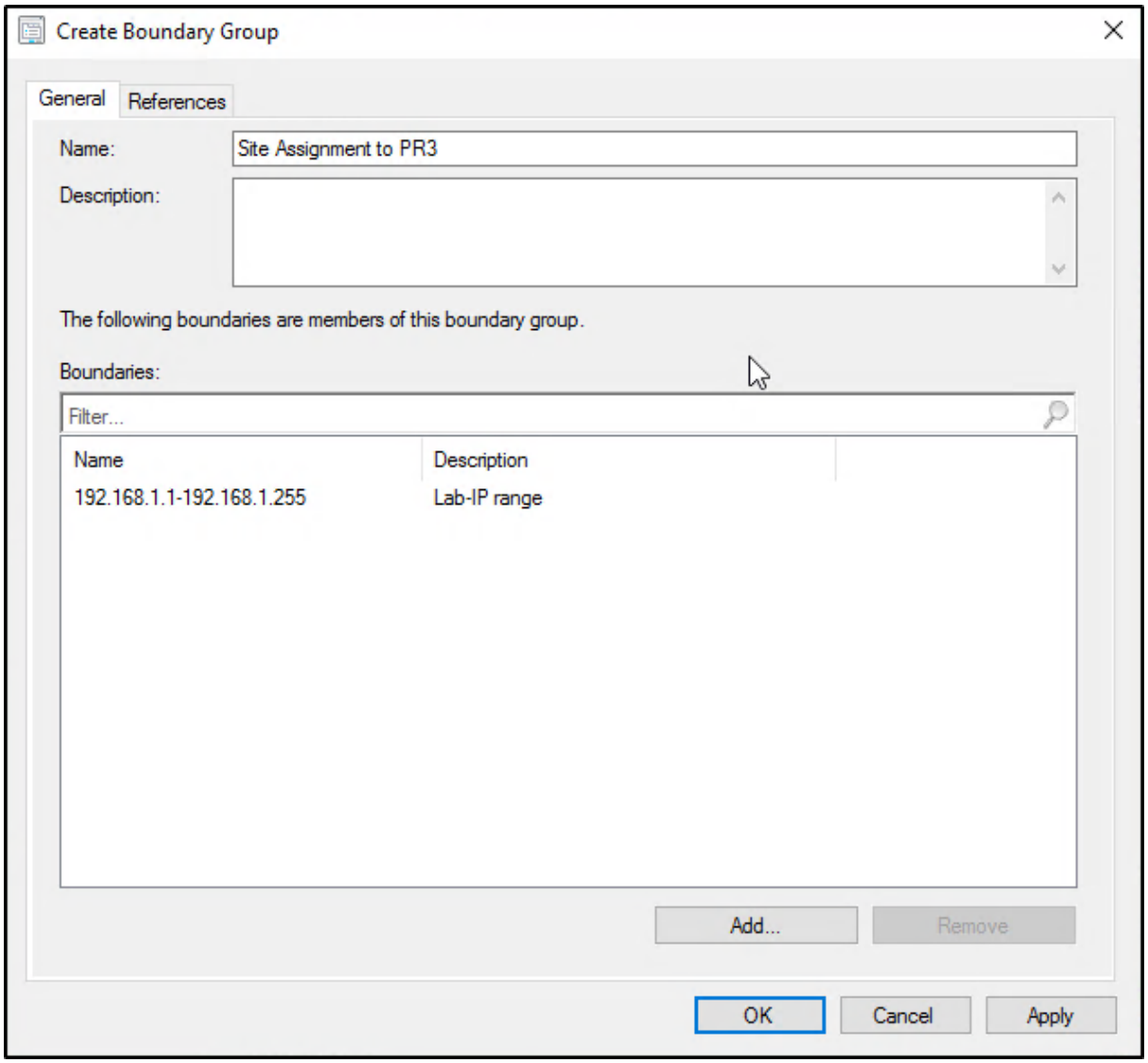
Figur 106: Konfigurasjon av Boundaries og Boundary Groups

Til slutt trykker vi på **OK**.



Figur 107: Konfigurasjon av Boundaries og Boundary Groups

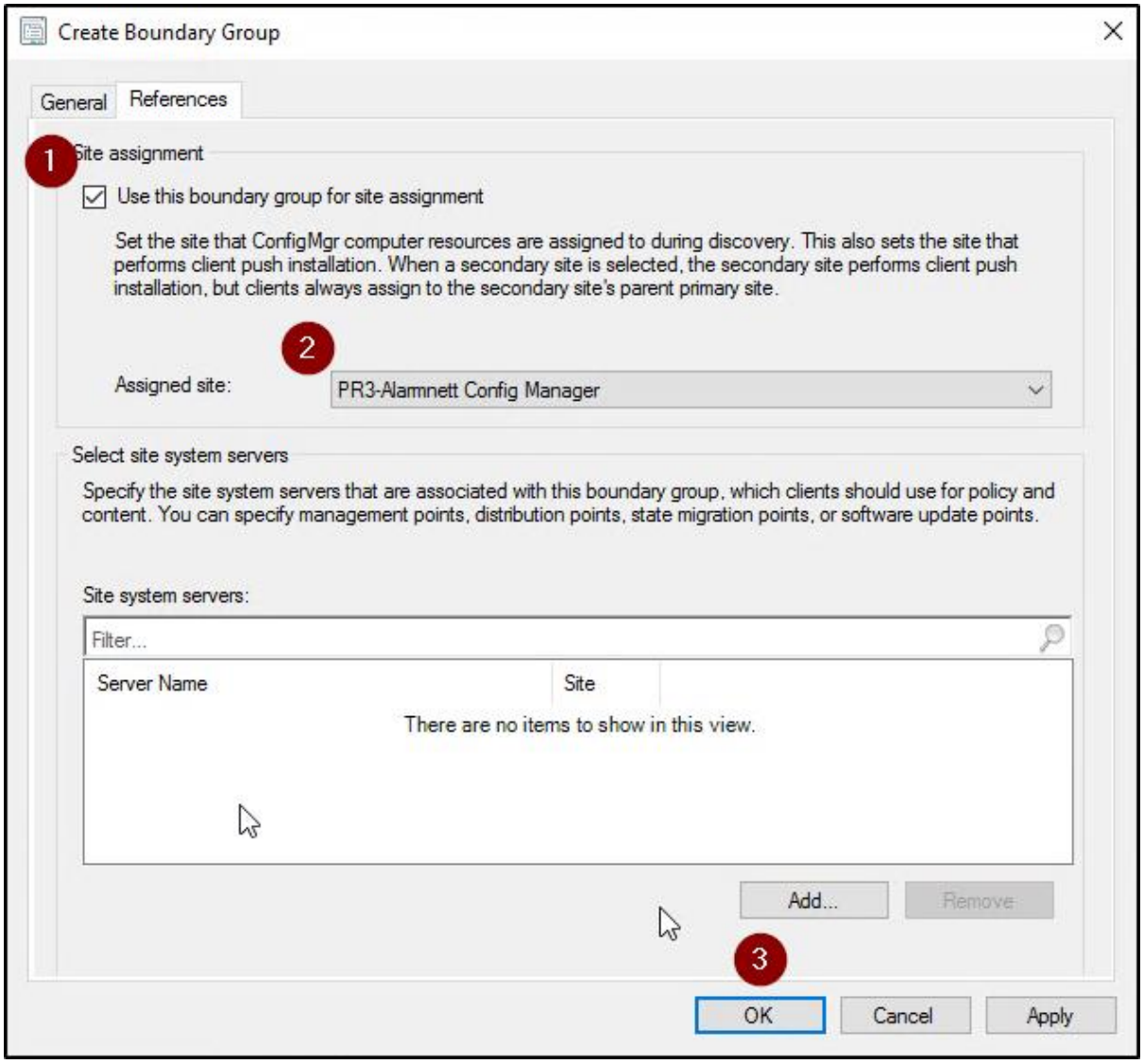
Vi lager enda en Boundary Group, gir den et navn og trykker på **References**.



Figur 108: Konfigurasjon av Boundaries og Boundary Groups

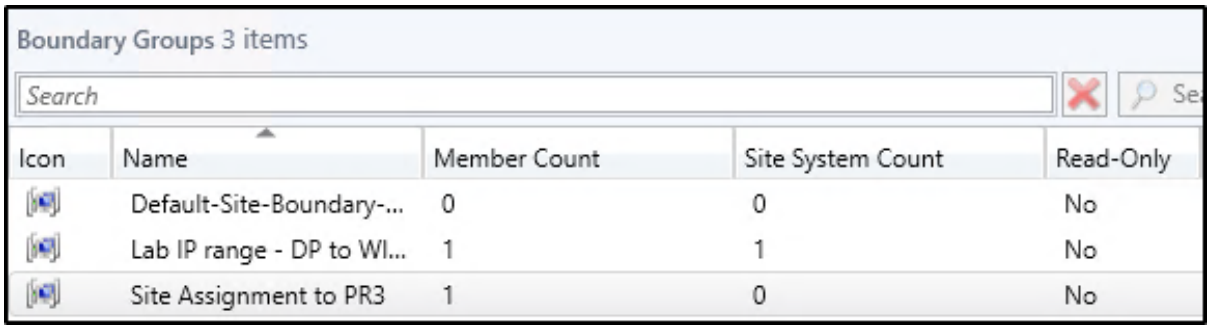
Huker av for **Use this boundary group for site assignment**, og velger **Assigned site**.

Deretter trykker vi på **OK**.



Figur 109: Konfigurasjon av Boundaries og Boundary Groups

Her ser vi en oversikt over Boundary Groups som vi har laget.

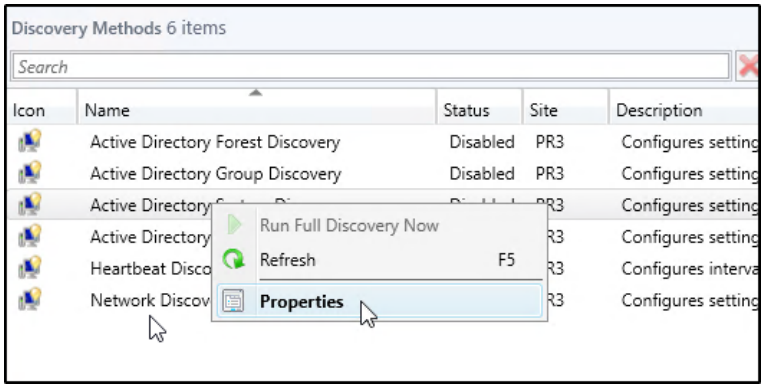


Figur 110: Konfigurasjon av Boundaries og Boundary Groups

Enable Active Directory System Discovery

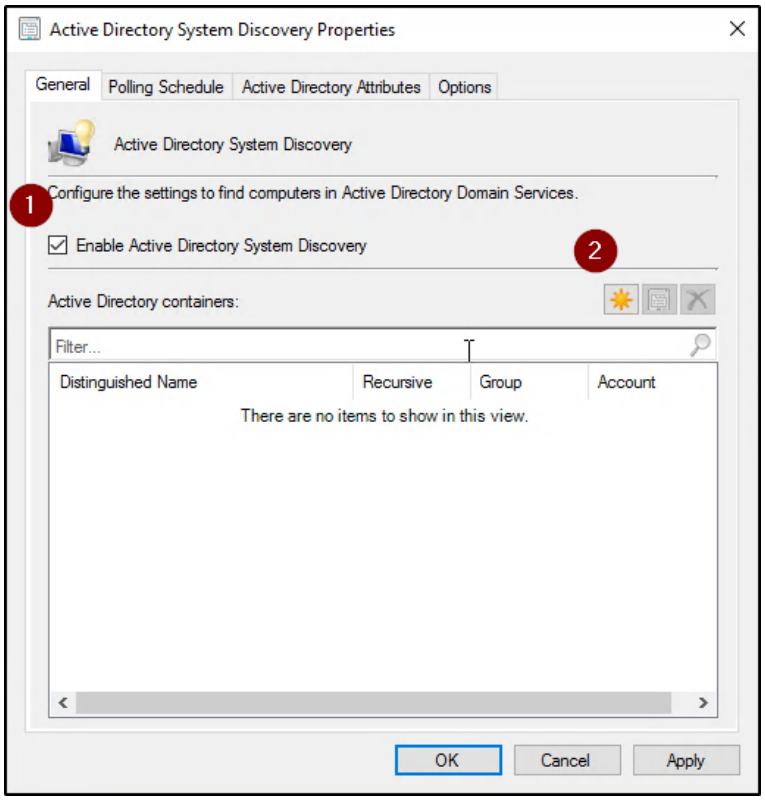
Vi skal nå gå inn å slå på Active Directory System Discovery. System Discovery vil gjøre det mulig for SCCM å få tilgang til enheter i lokalt Active Directory.

Vi navigerer oss til ***Discovery Methods*** og høyreklikker på **Active Driectory System Discovery** og velger **Properties**.



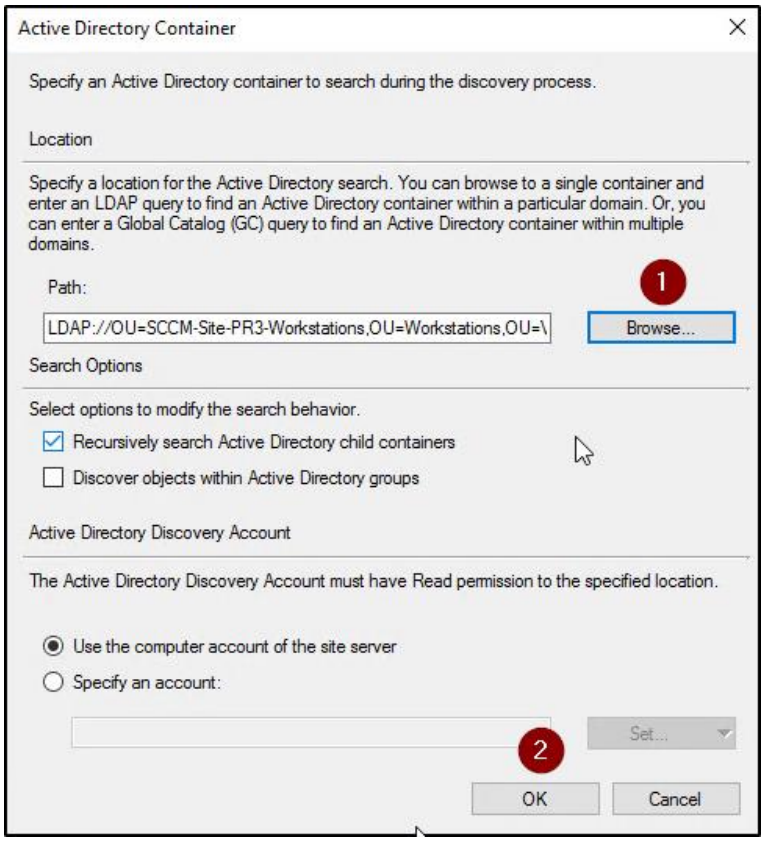
Figur 111: Enable System Discovery

Huker av for **Enable Active Directory System Discovery**, og trykker på sol-ikonet.



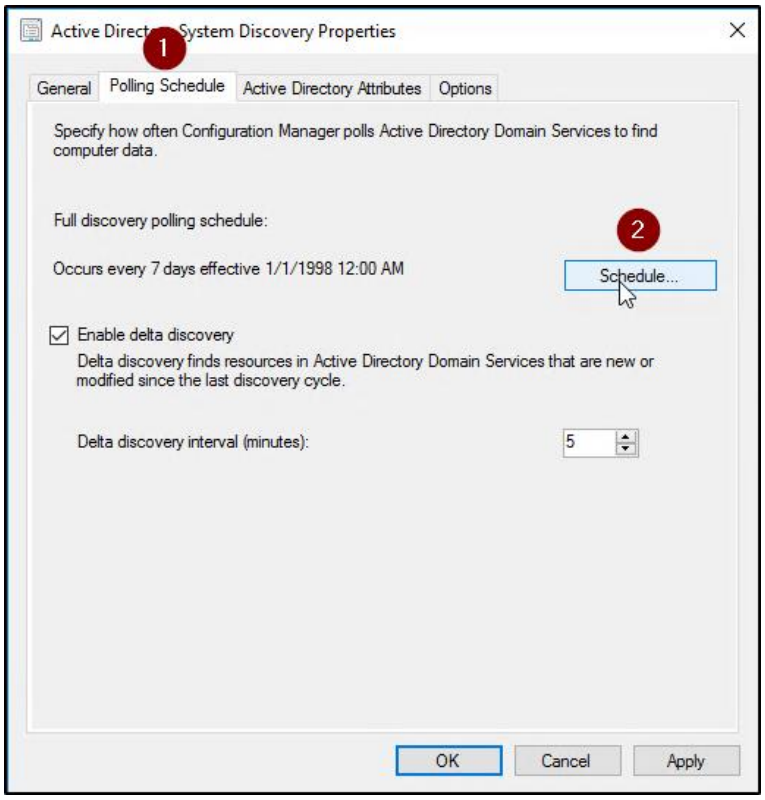
Figur 112: Enable System Discovery

Trykker **Browse** og velger stien til våre arbeidsstasjoner og trykker **OK**.



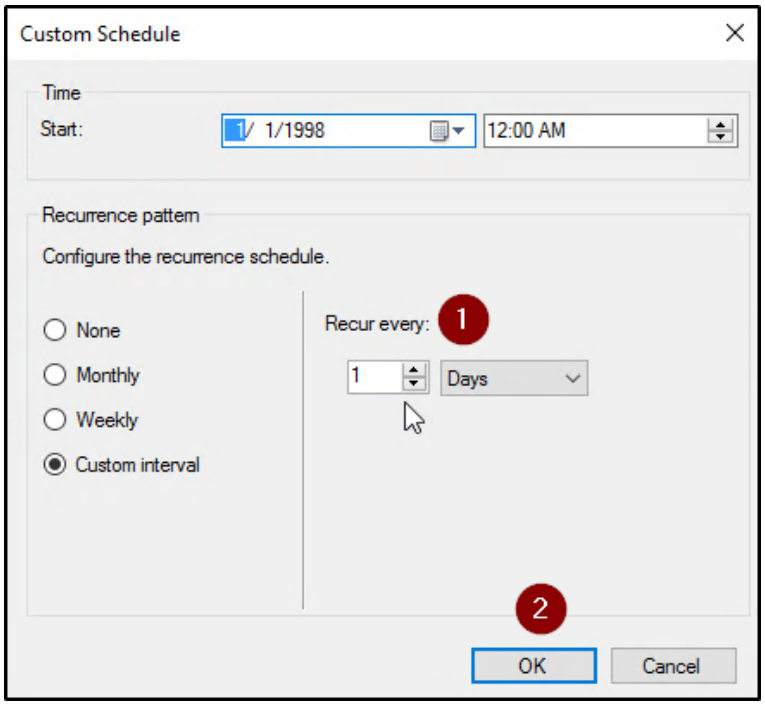
Figur 113: Enable System Discovery

Deretter går vi til ***Polling Schedule***, og trykker på **Schedule…**



Figur 114: Enable System Discovery

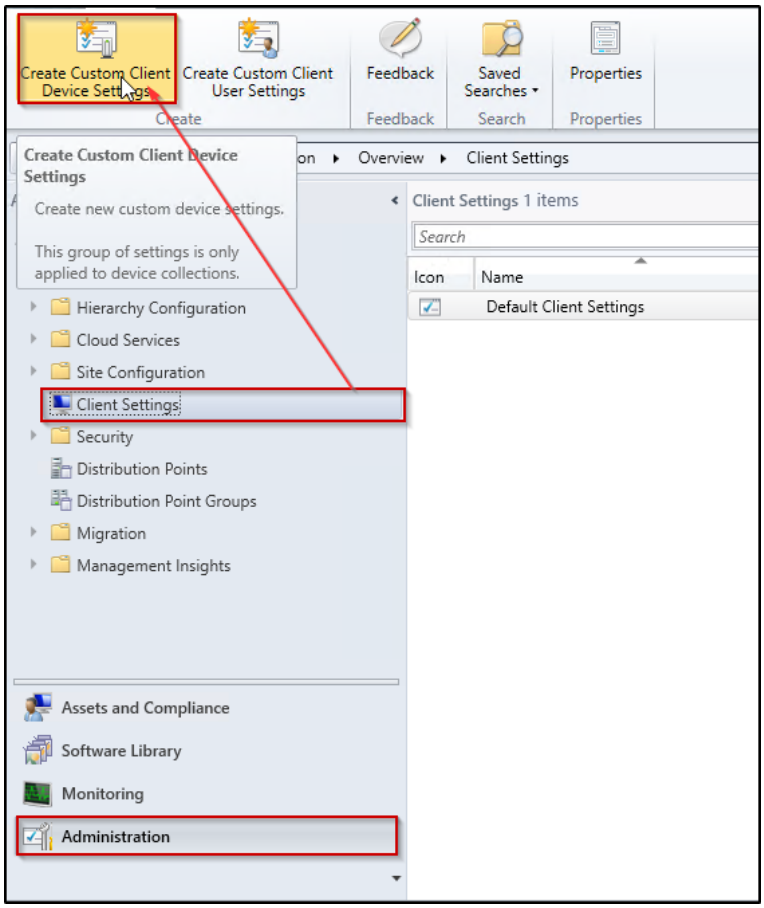
Setter hvor ofte System Discovery skal synkronisere nye enheter som legges til. Vi setter vår Schedule til 1 gang hver dag. Dette kan selvfølgelig endres på, om det skulle være behov, f.eks. ved testing.



Figur 115: Enable System Discovery

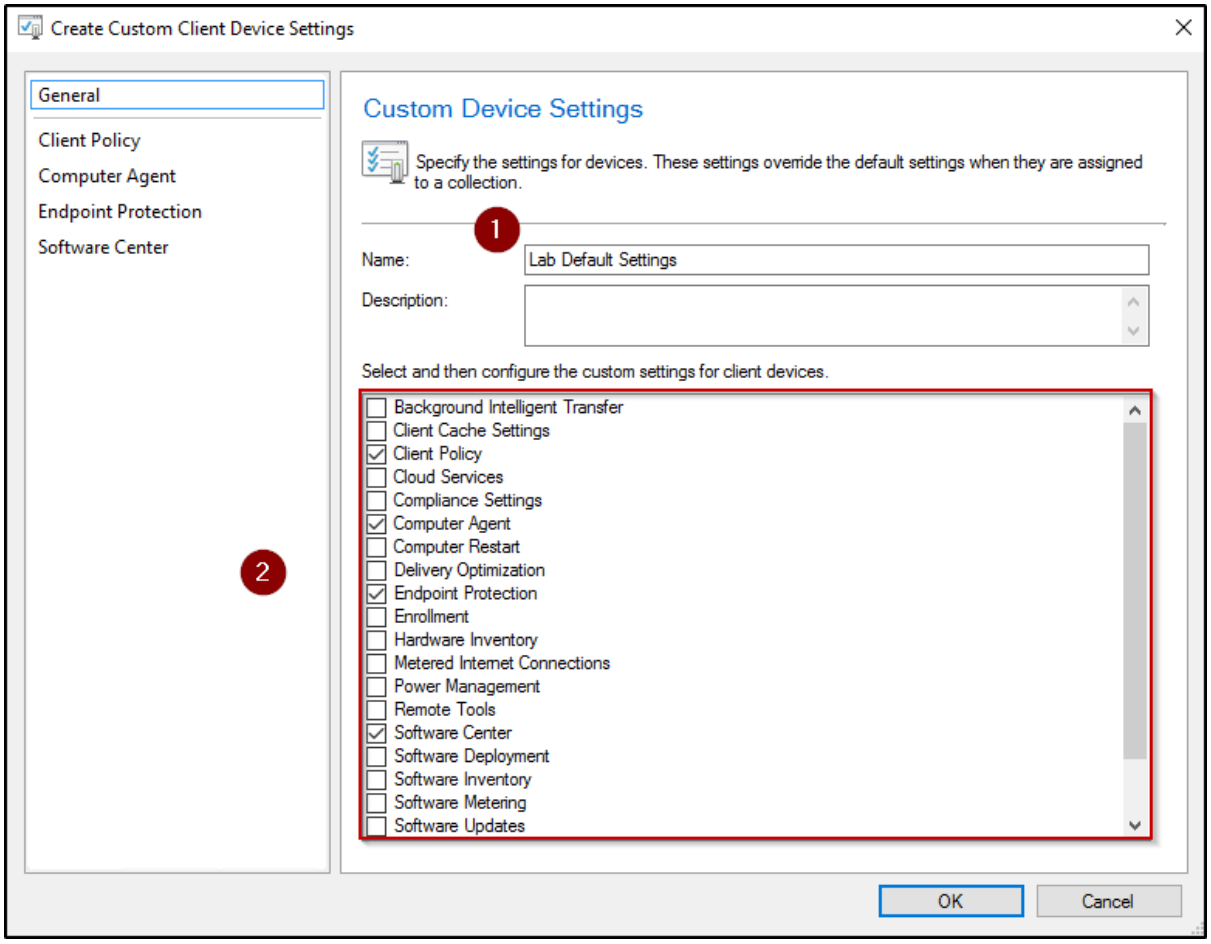
Konfigurasjon av Custom Client Settings

Vi skal nå gå gjennom hvordan vi har satt opp vår egen SCCM klient. Vi gjør dette ved å navigere oss til ***Administration*** og trykker på **Create Custom Client Device Settings**.



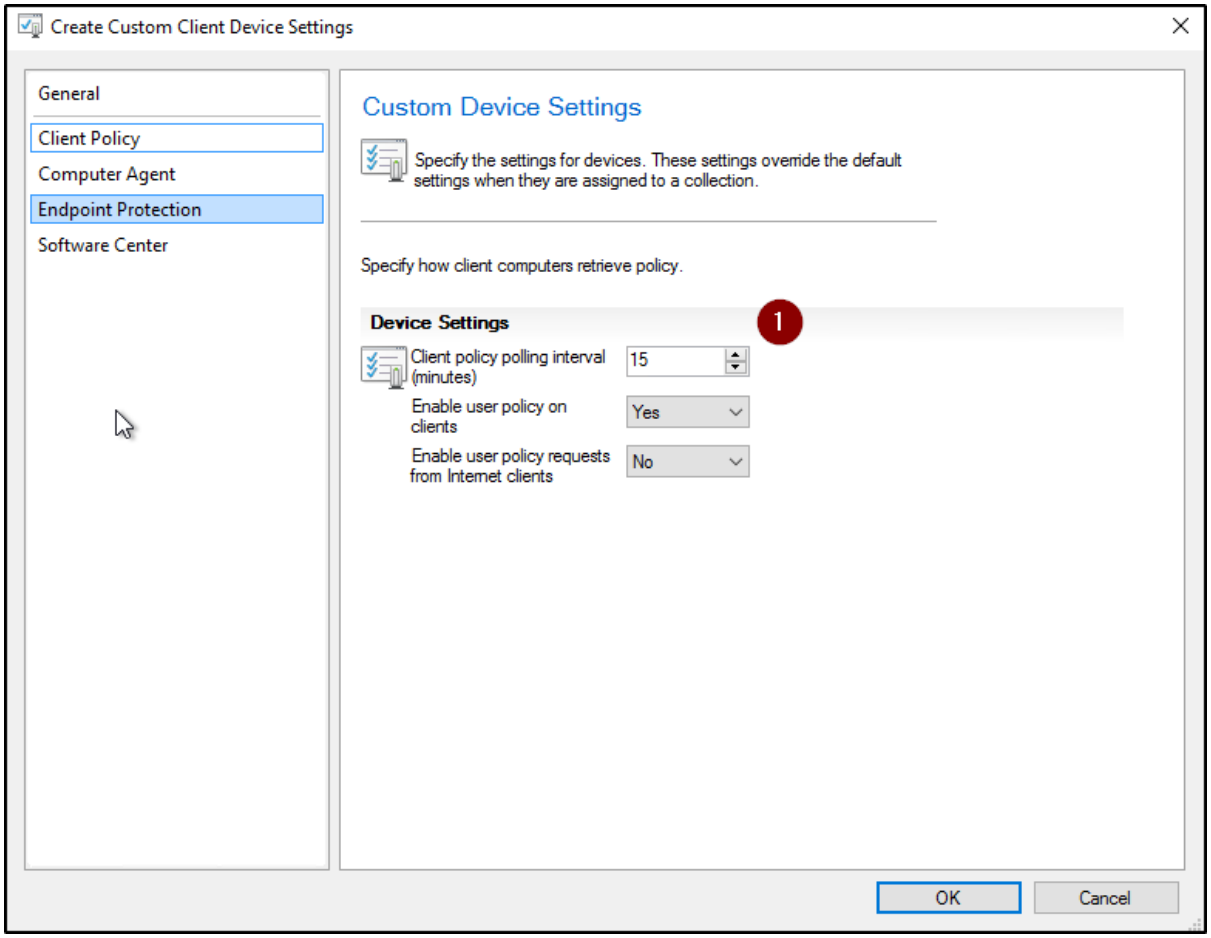
Figur 116: Konfigurasjon av Custom Client Settings

Velger de innstillingene som vi ønsker å ha med i vår klient. Nedenfor har vi valgt **Client Policy**, **Computer Agent**, **Endpoint Protection** og **Software Center**.



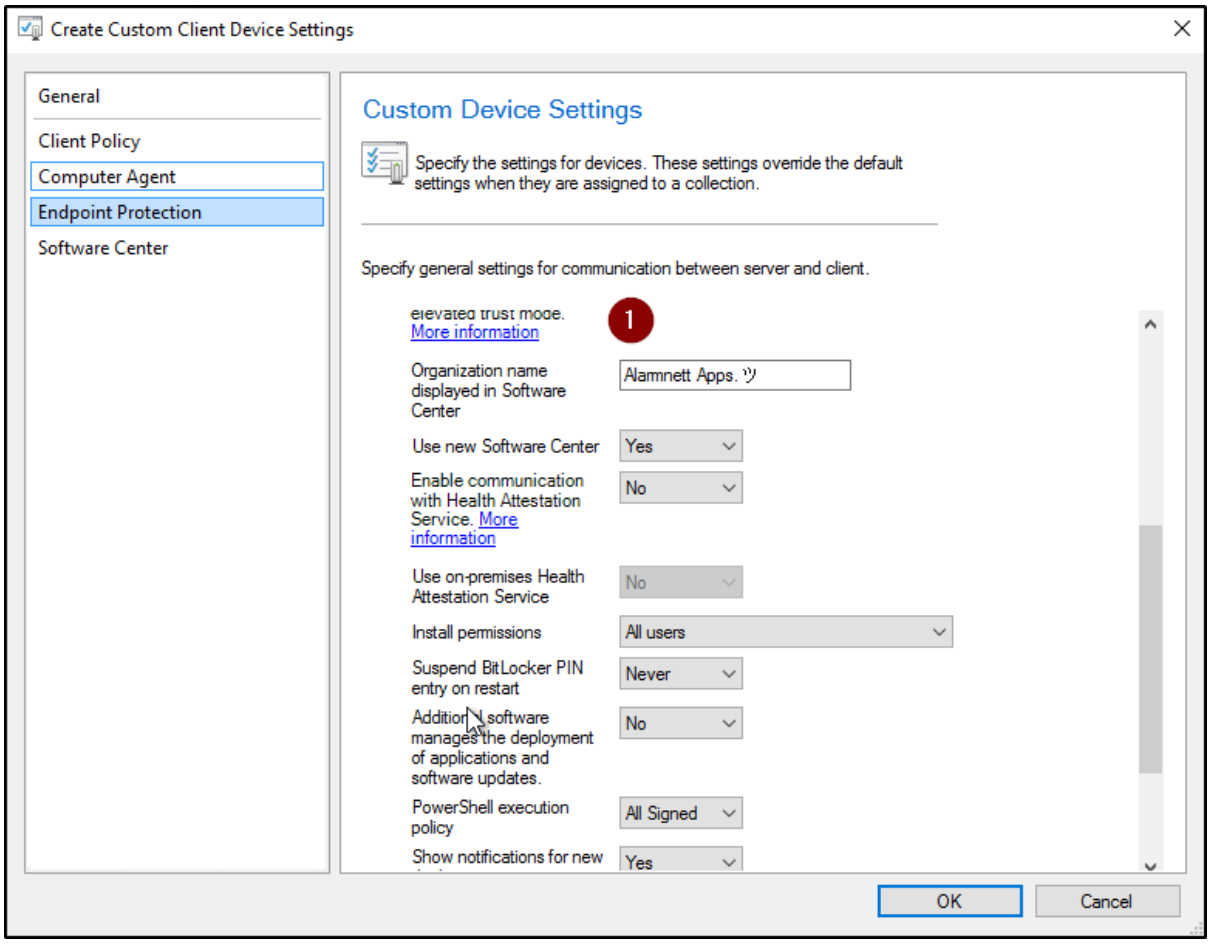
Figur 117: Konfigurasjon av Custom Client Settings

Vi setter et *Client Policy polling interal*. I vårt tilfelle setter vi denne til 15 minutter, da dette er et testmiljø, og vi ønsker at ting skal skje litt raskt. Vi trykker deretter på ***Computer Agent***.



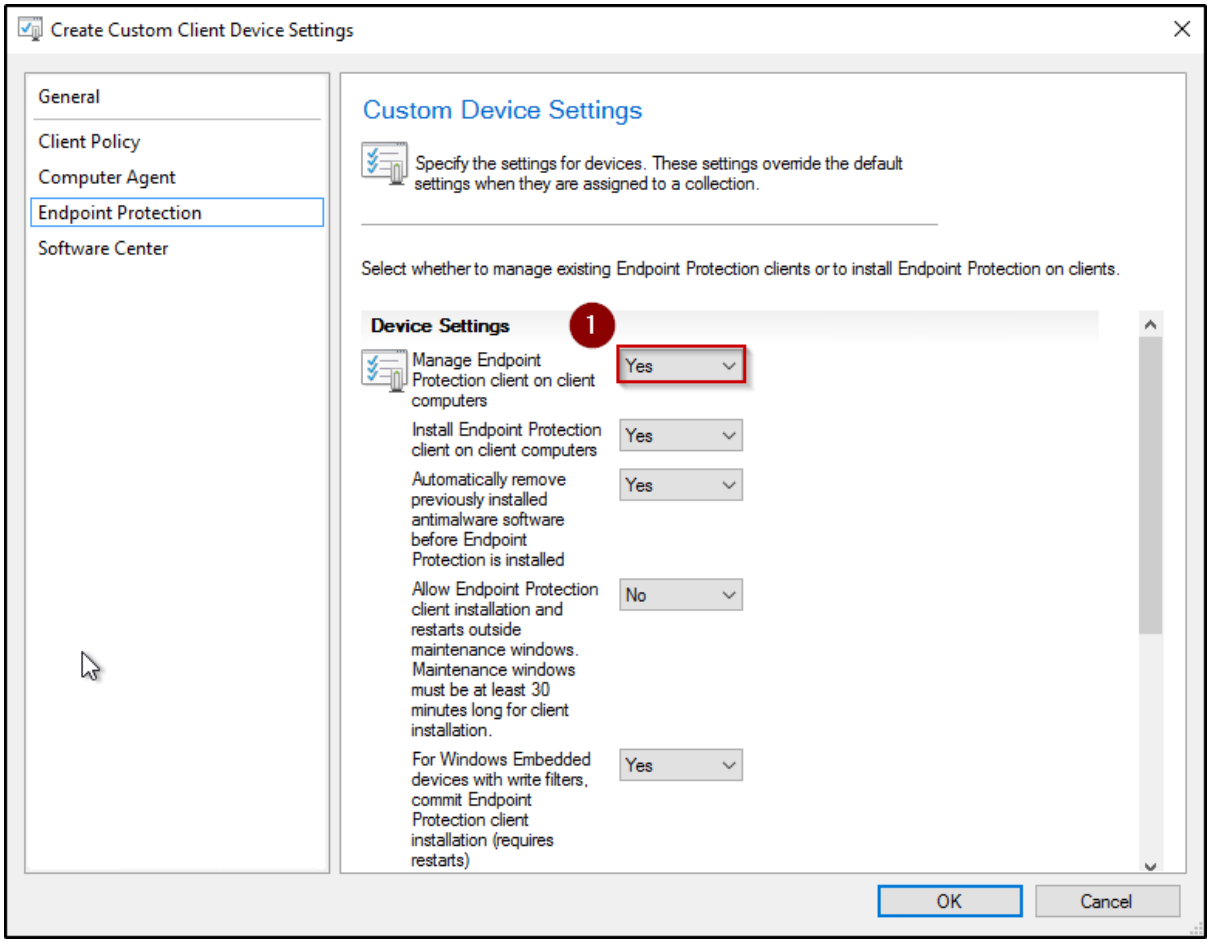
Figur 118: Konfigurasjon av Custom Client Settings

Under ***Computer Agent***, kan vi sette navn på organisasjonen og diverse andre ting som kommer opp i Software Center, når en bruker slår på applikasjonen. Vi kan også velge andre innstillinger som f.eks. installation permission. Deretter trykker vi på ***Endpoint Protection***.



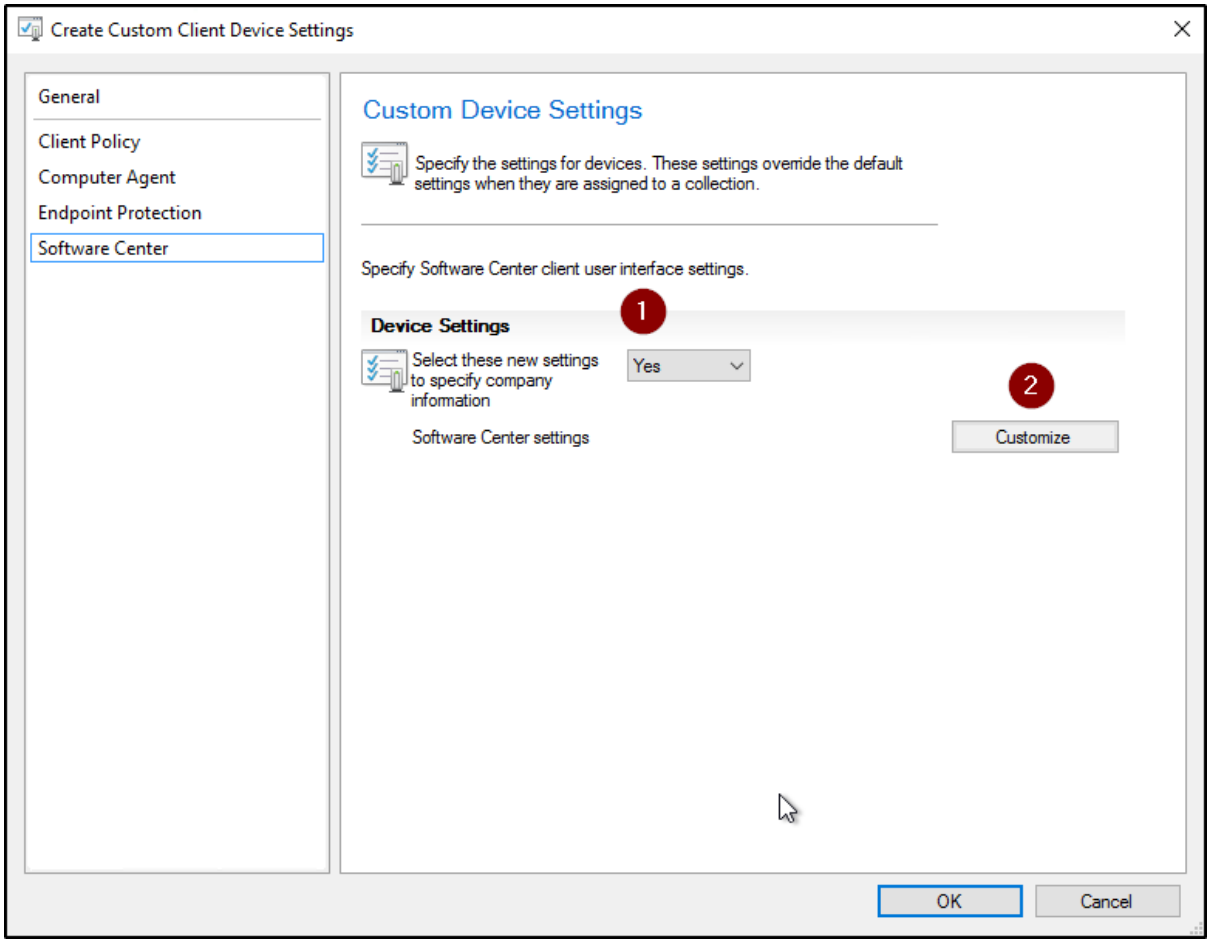
Figur 119: Konfigurasjon av Custom Client Settings

Under ***Endpoint Protection***, velger vi **Yes**, for *Manage Endpoint Protection Client on Client computers.* Vi velger deretter å gå til ***Software Center***.



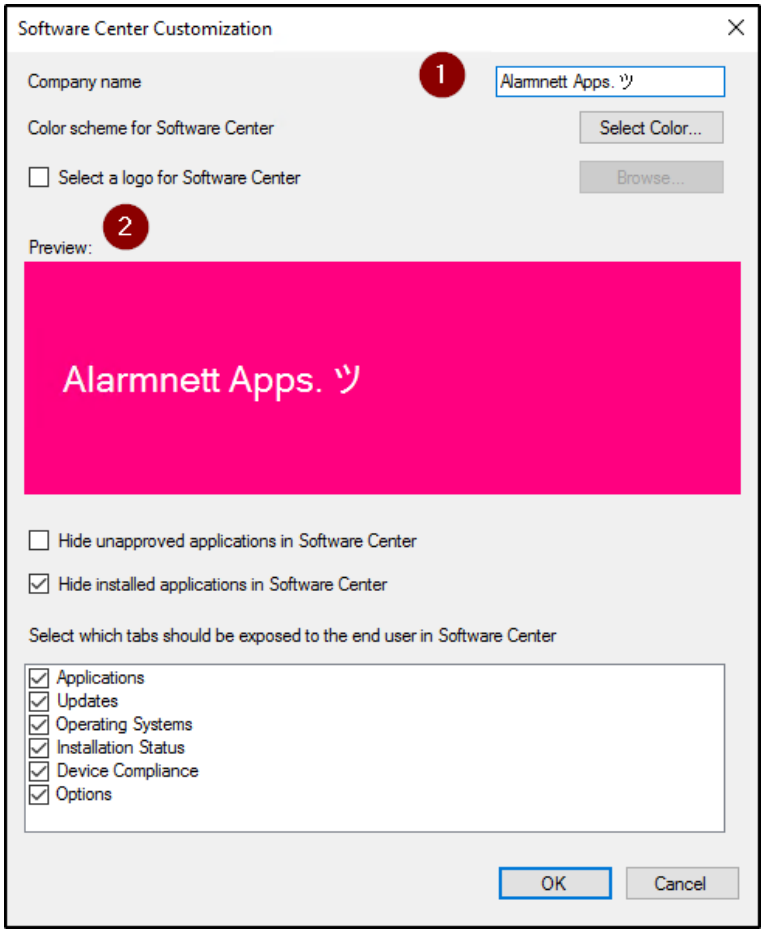
Figur 120: Konfigurasjon av Custom Client Settings

Under ***Software Center***, velger vi **Yes**, på *Select these new settings to specify company information*. Videre trykker vi på **Customize**.



Figur 121: Konfigurasjon av Custom Client Settings

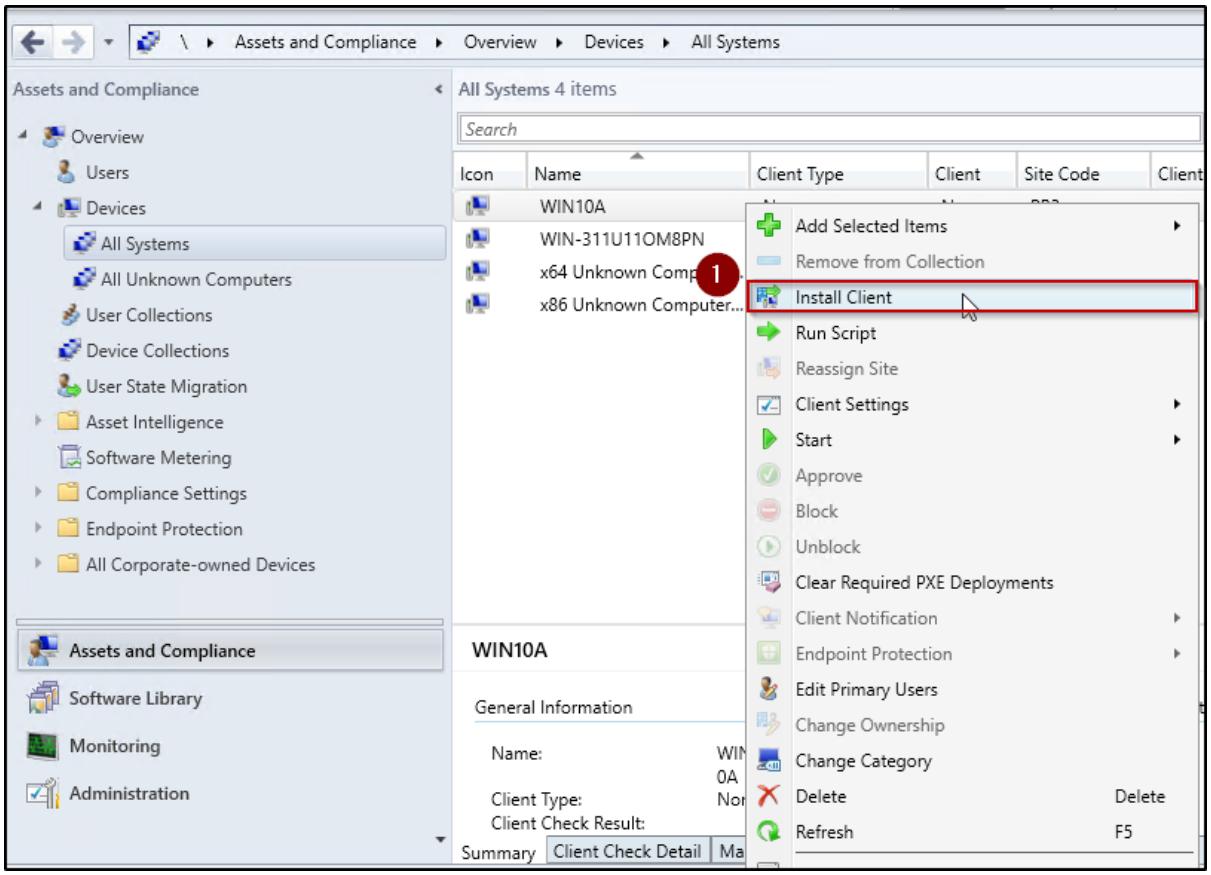
Her setter vi navn, farger og hvilke tabs som skal vises til brukeren når han går inn på applikasjonen.



Figur 122: Konfigurasjon av Custom Client Settings

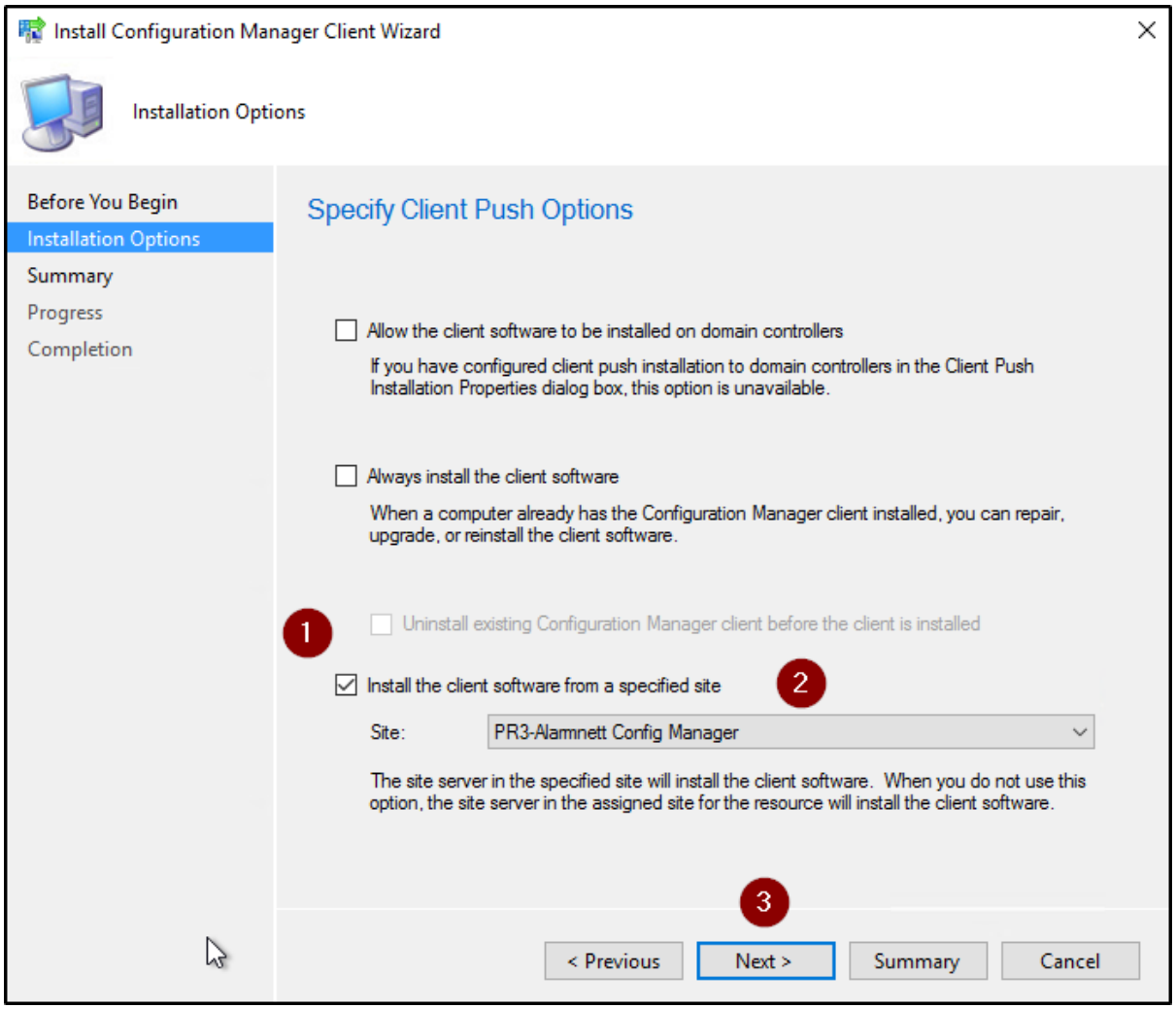
Client – Installasjon

Vi skal nå vise hvordan vi kan installere SCCM klienten direkte på en maskin. Vi høyreklikker på maskinen og trykker **Install Client**.



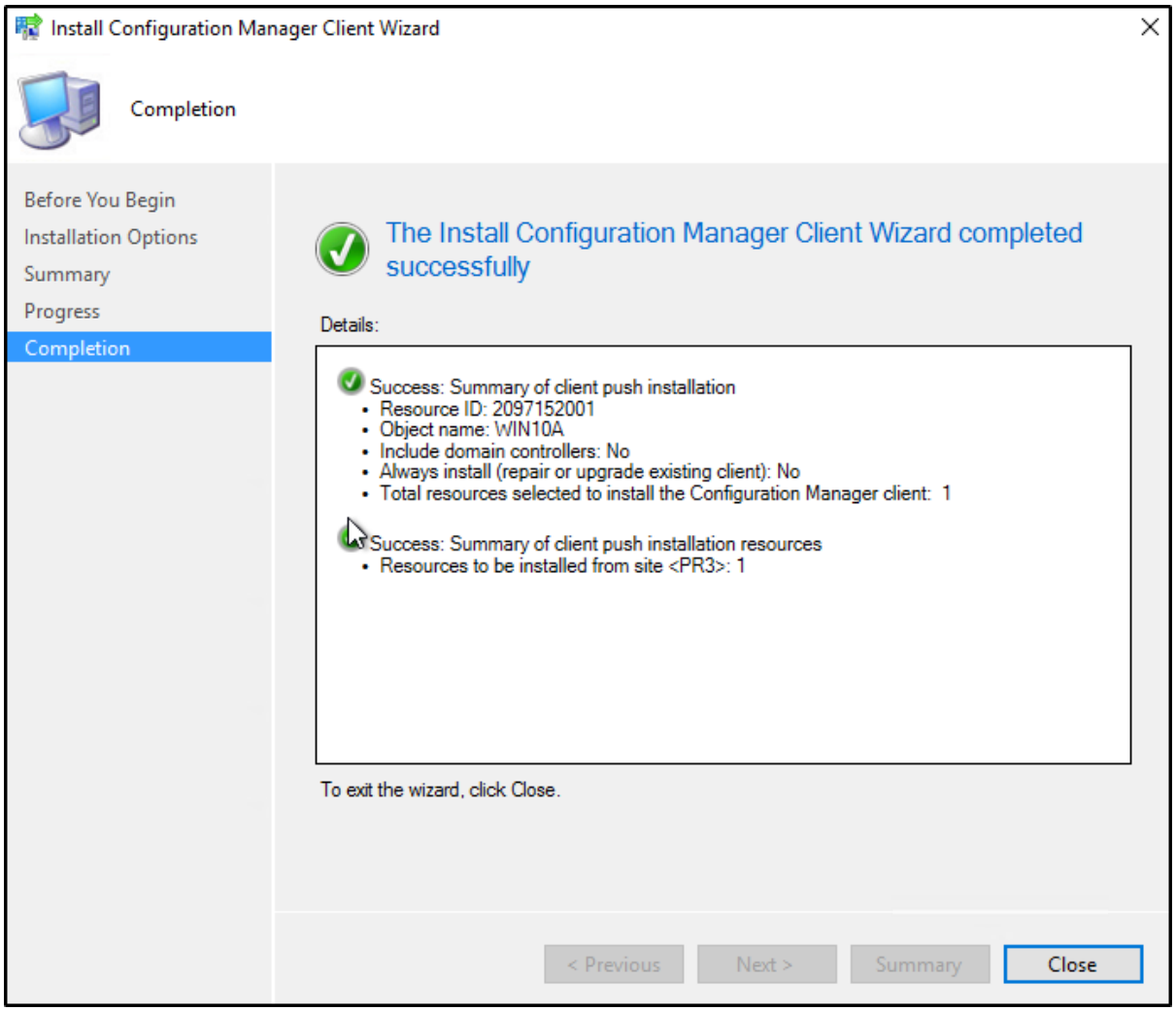
Figur 123: Client - Installasjon

Velger hvor vi skal installere SCCM klienten fra. Velger **Site** og trykker **Next**.



Figur 124: Client - Installasjon

Vi ser her at klienten nå blir rullet ut.



Figur 125: Client - Installasjon

Fase 3 - Veien til Co-Management

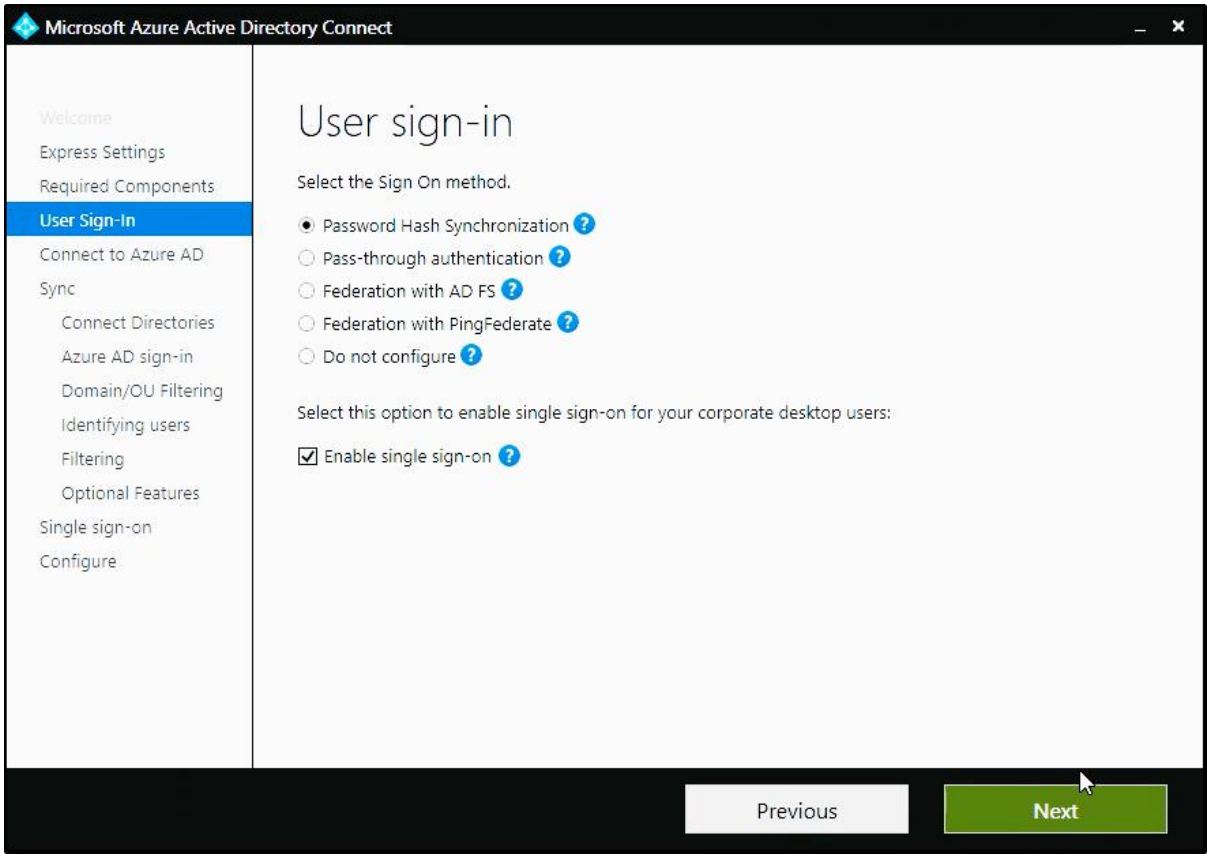
Azure AD Connect

Det første vi starter med for å komme i gang med Co-Management er å laste ned og konfigurere Azure Active Directory Connect. Azure AD Connect kan lastes ned fra Microsoft sine offisielle sider, lenke:

https://www.microsoft.com/en-us/download/details.aspx?id=47594

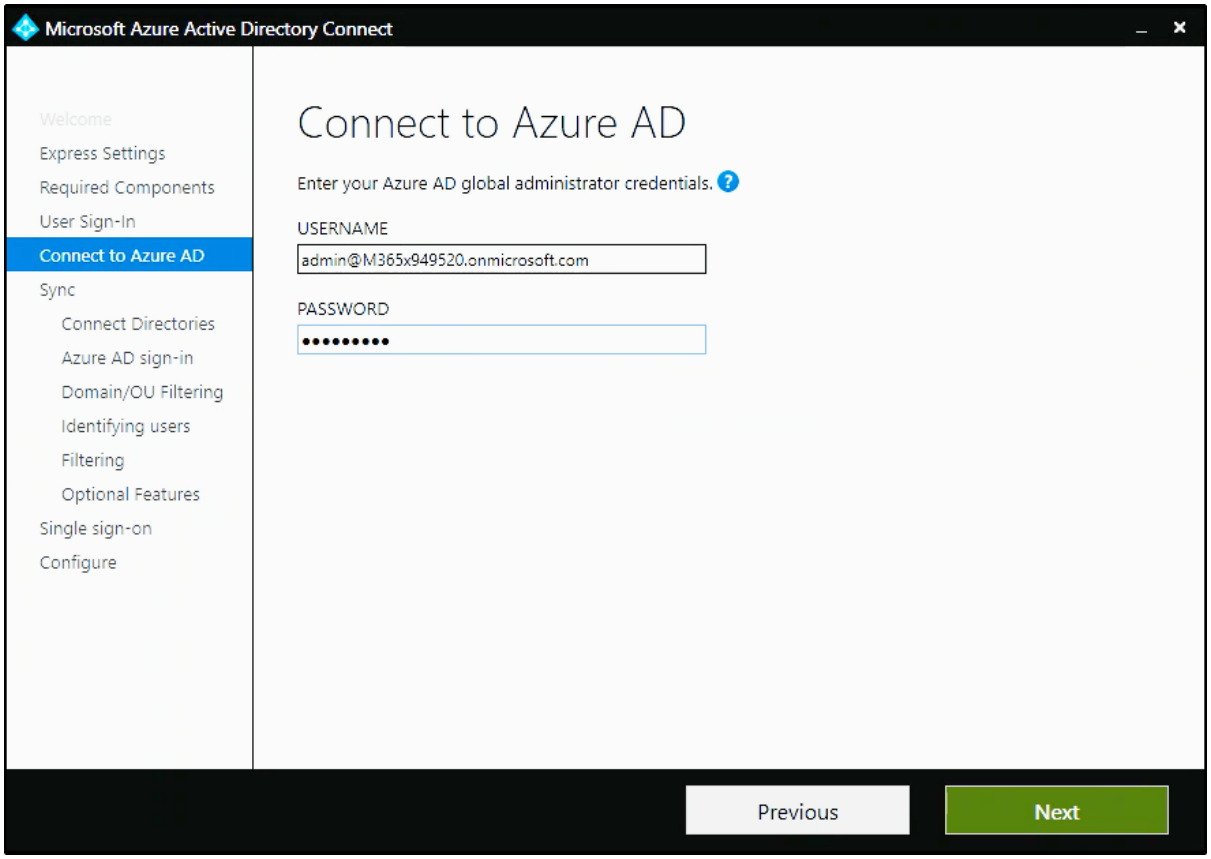
Videre så følger vi oppsett som vist i skjermbildene nedenfor.

Velger *Password Hash Synchronization* og trykker **Next**.



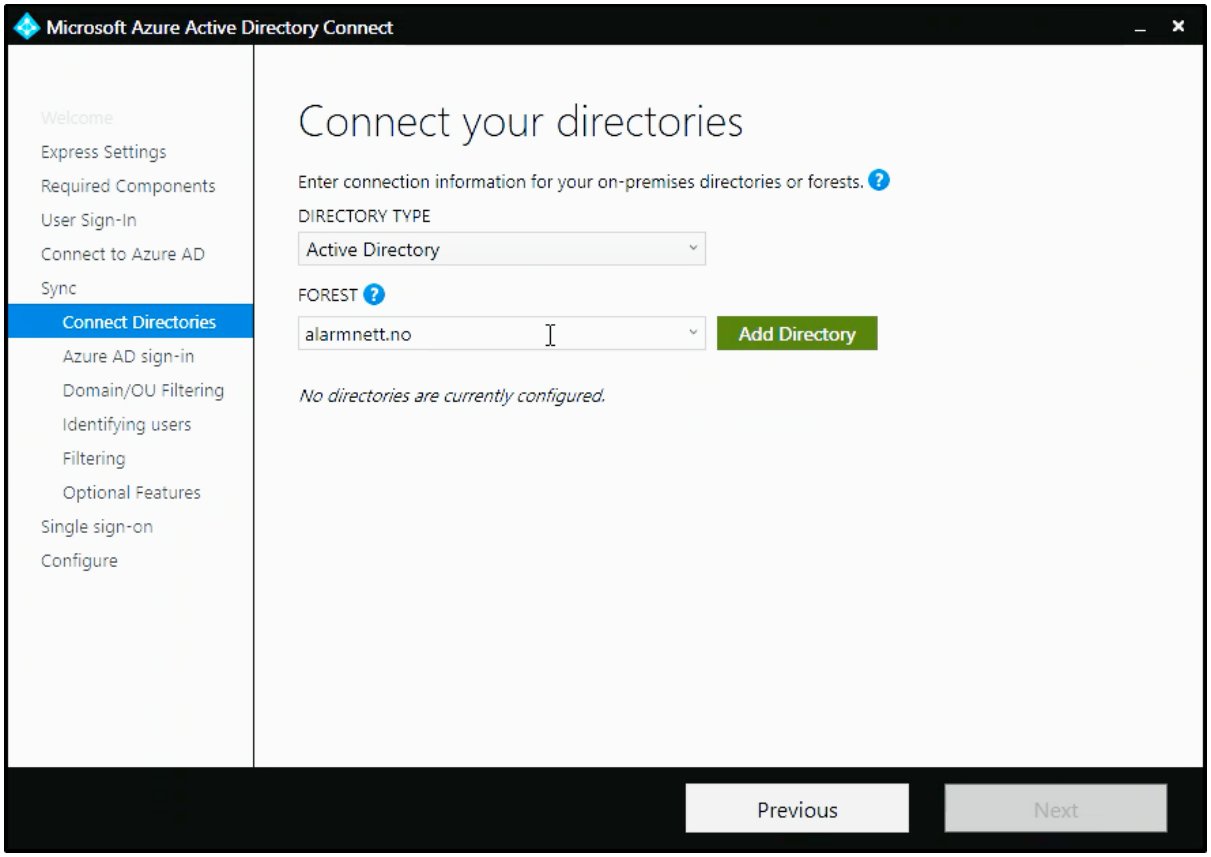
Figur 126: Azure AD Connect

Vi blir nå bedt om å koble oss til Azure AD. Da tar vi i bruk administratorbruker på tenant og skriver inn passord og trykker **Next**.



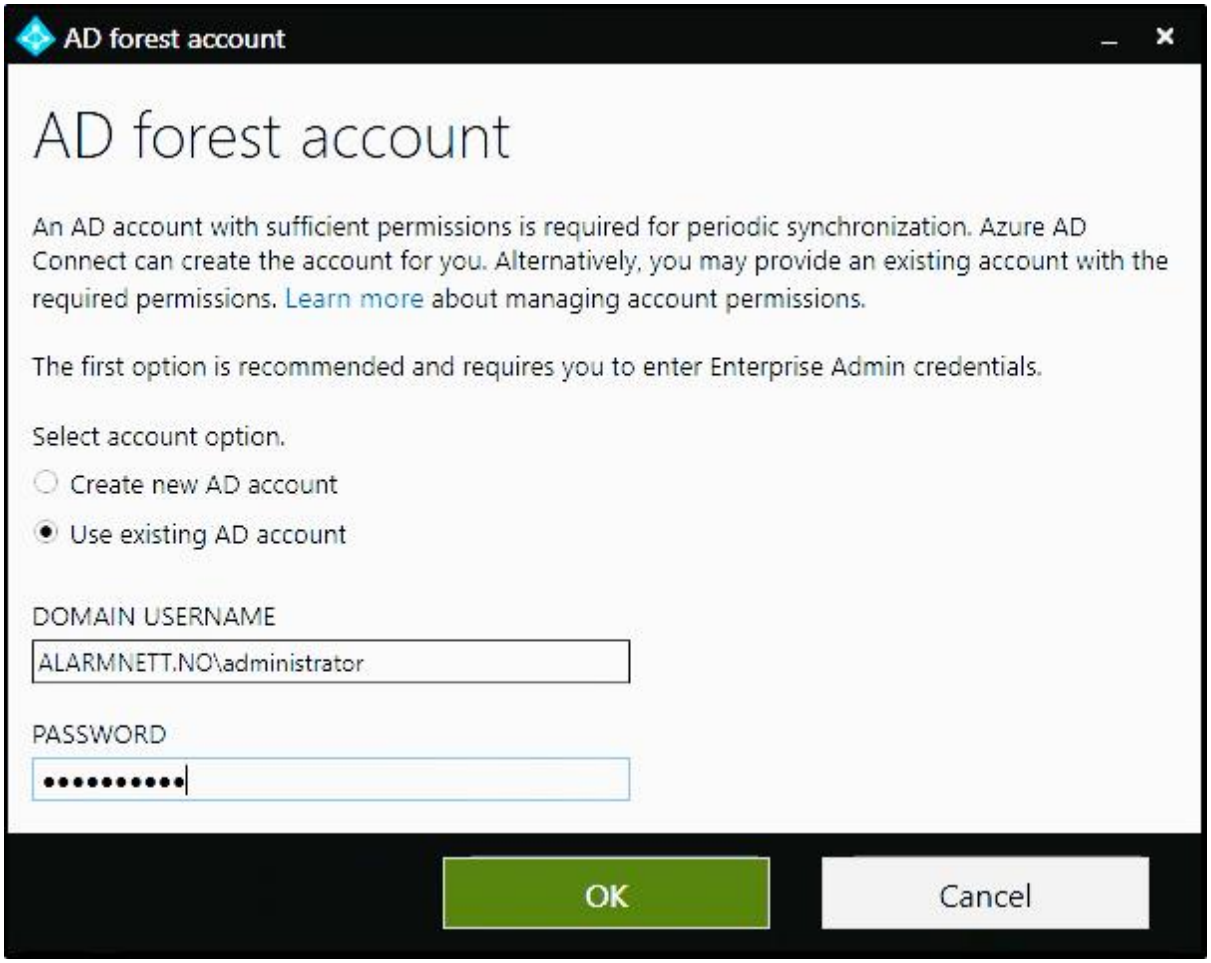
Figur 127: Azure AD Connect

Videre blir vi bedt om å skrive inn informasjon om on-premise domenet vårt. Vi velger *directory type*: **Active Directory** og legger til vår *forest*: **alarmnett.no** og trykker **Next**.



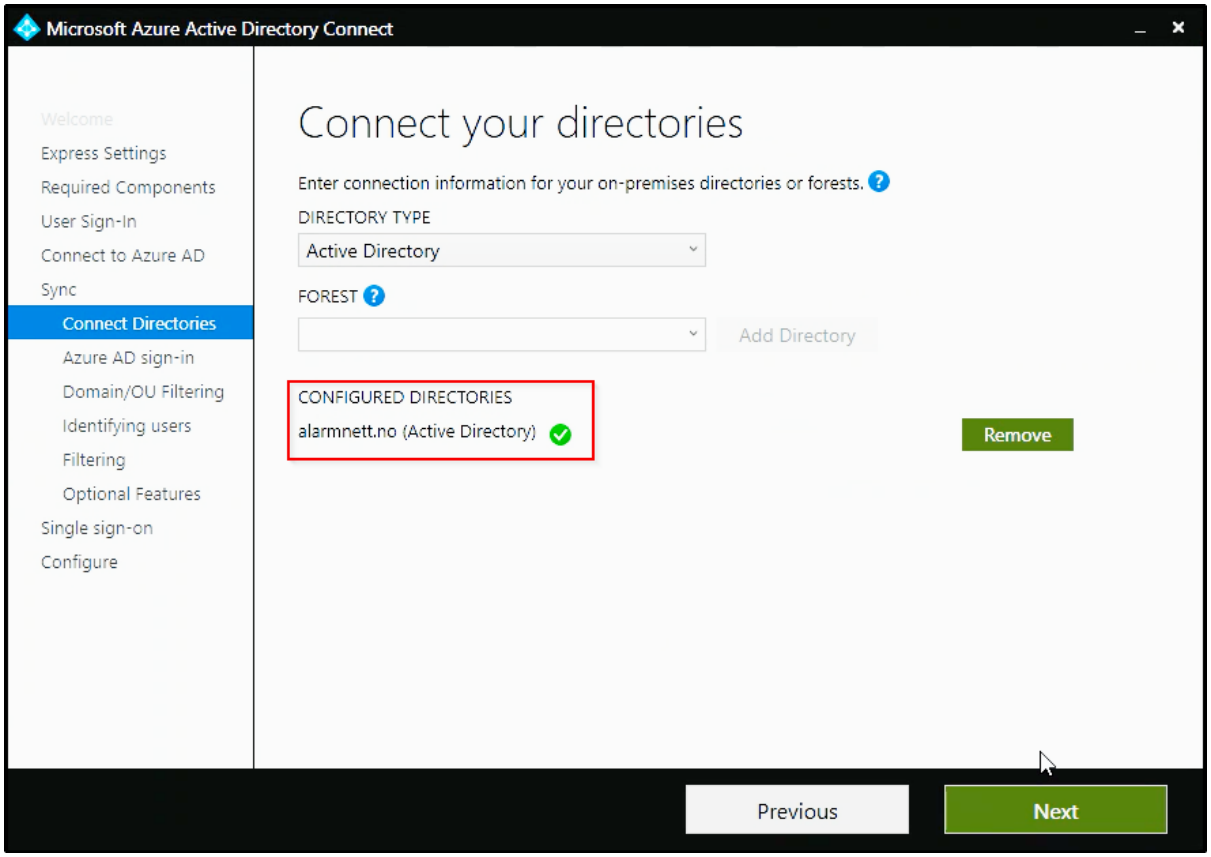
Figur 128: Azure AD Connect

Her blir vi bedt om å skrive inn en bruker i domenet samt passord. Vi velger å ta i bruk administratorbruker og skriver inn passord, deretter trykker vi **OK**.



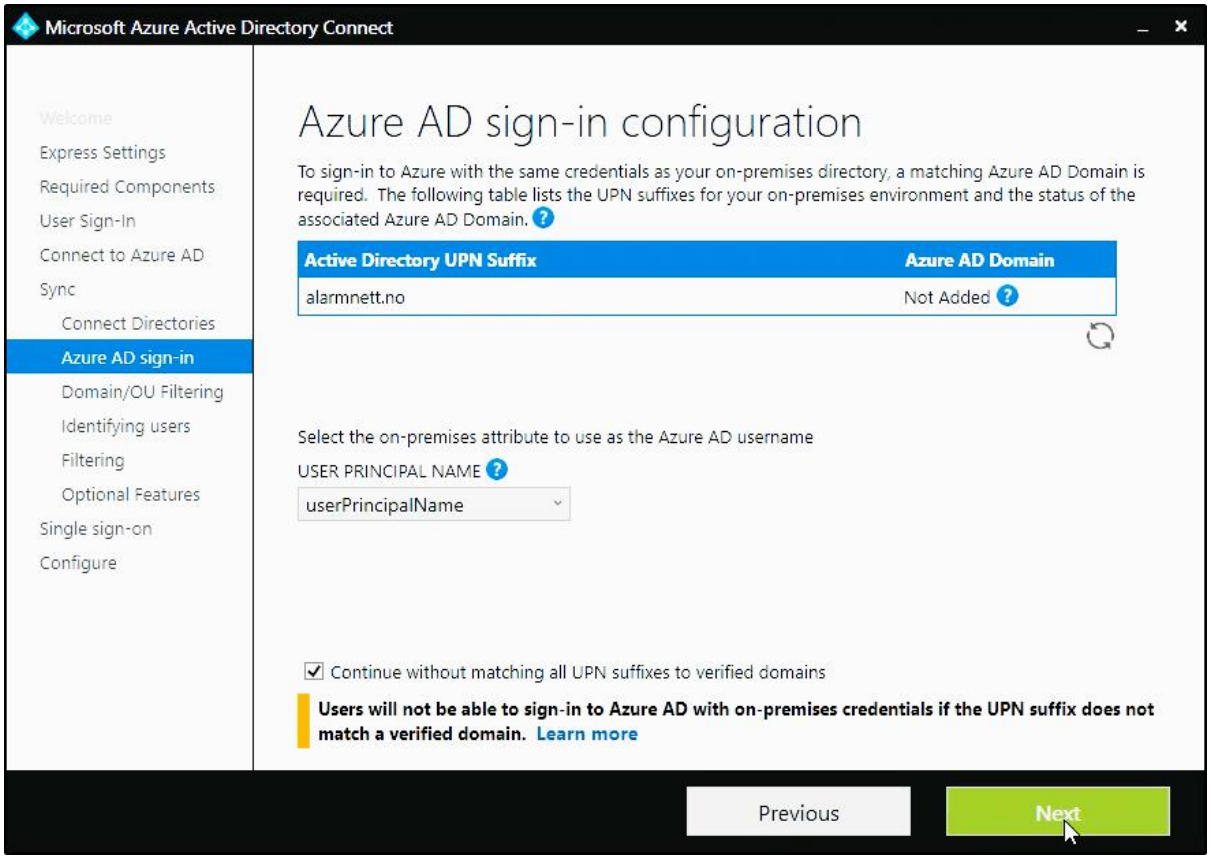
Figur 129: Azure AD Connect

Under ***Connect Directories***, vil vi nå se at vi har fått opp *alarmnett.no* som et konfigurert directory og vi trykker **Next**.



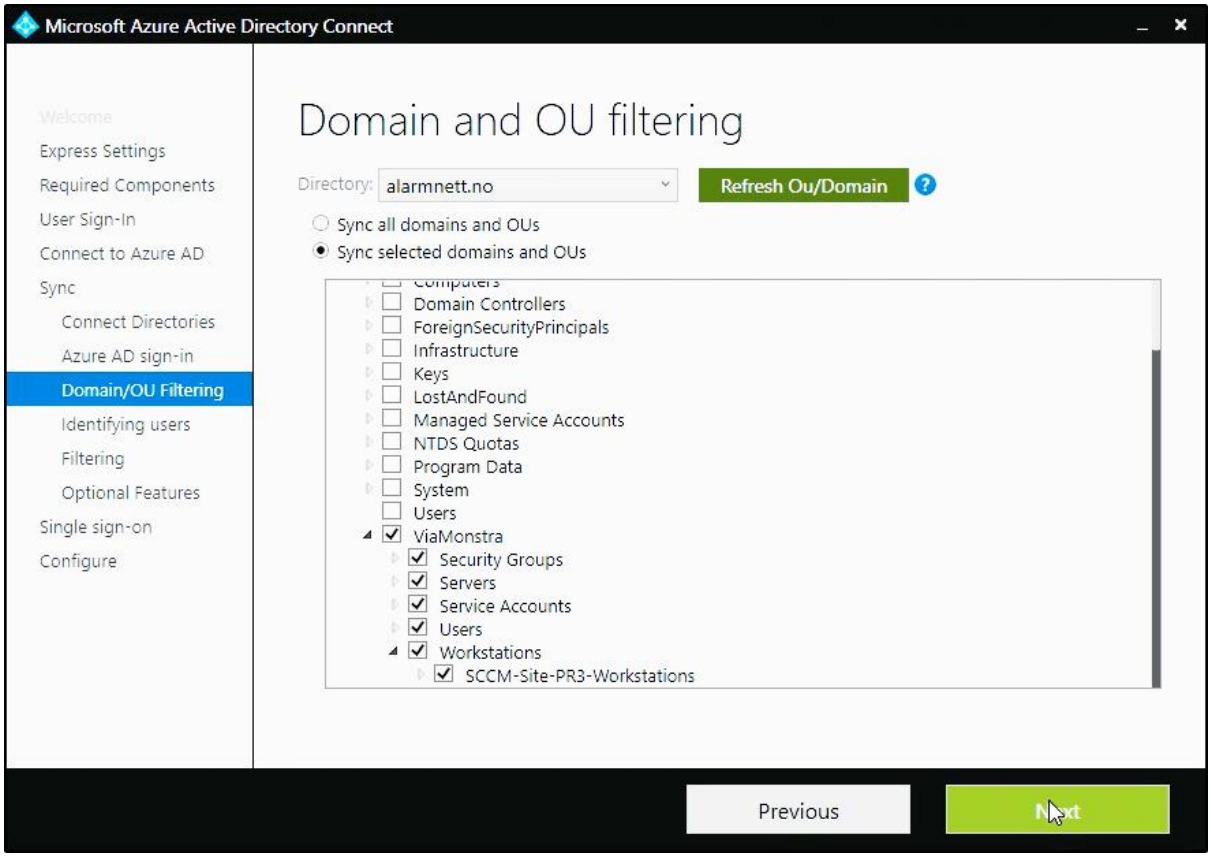
Figur 130: Azure AD Connect

Her velger vi å huke av for *Continue without matching all UPN suffices to verified domains*, og trykker **Next**.



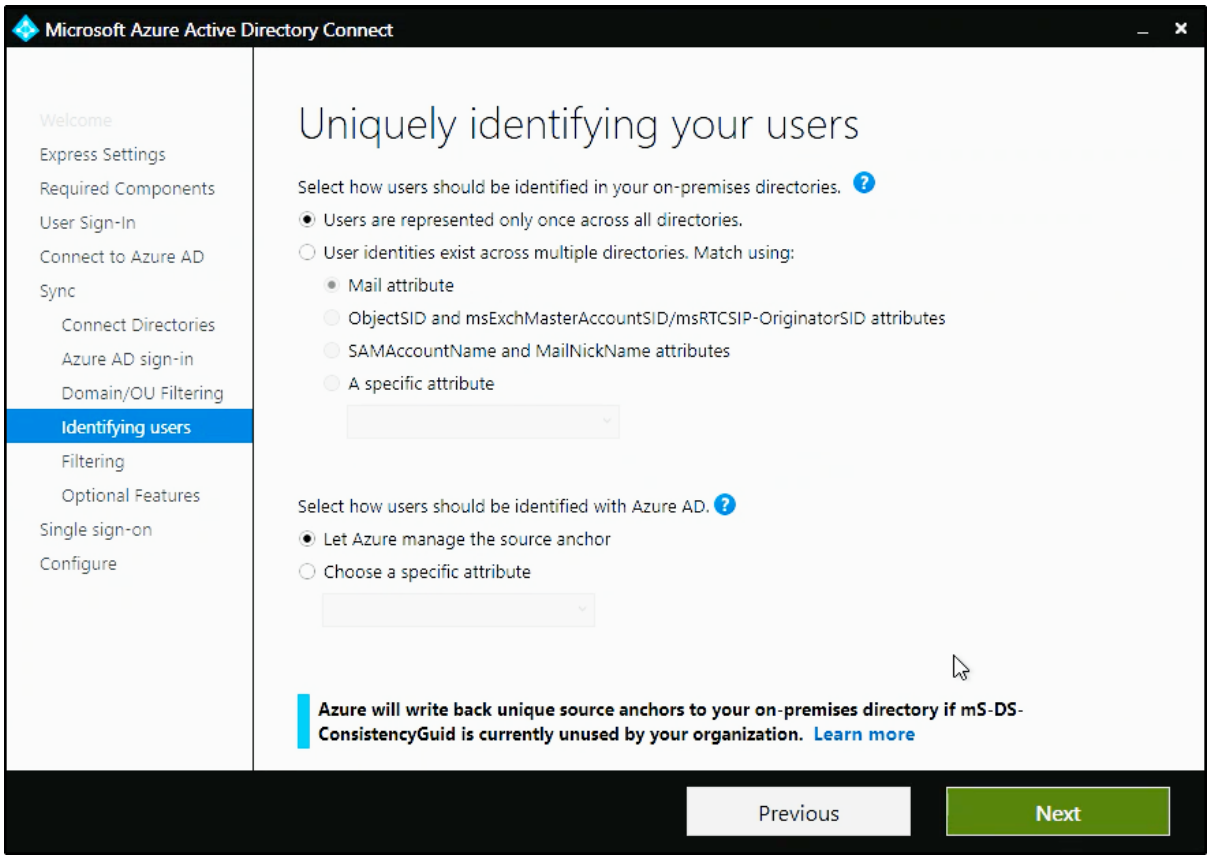
Figur 131: Azure AD Connect

Under ***Domain/OU Filtering*** er det viktig at vi velger samtlige OU-er, som inneholder maskiner og brukere, fra on-premise AD, som vi ønsker å synkronisere opp til Azure AD. Nedenfor har vi valgt å ta med samtlige OU-er som finnes i OU-en «ViaMonstra», da det er her vi oppbevarer våre maskiner og brukere for dette prosjektet.



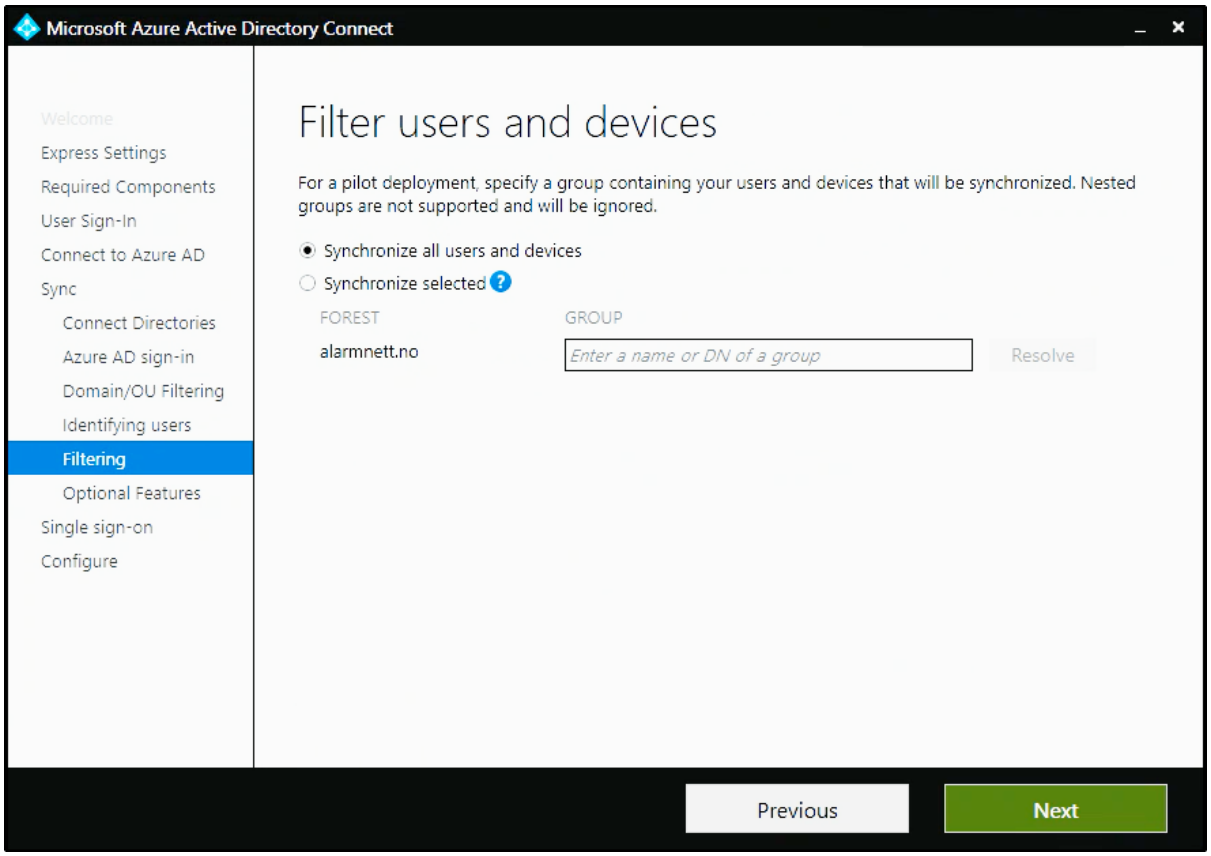
Figur 132: Azure AD Connect

Ser til at vi har valgt disse to valgene som vi ser nedenfor og trykker **Next**.



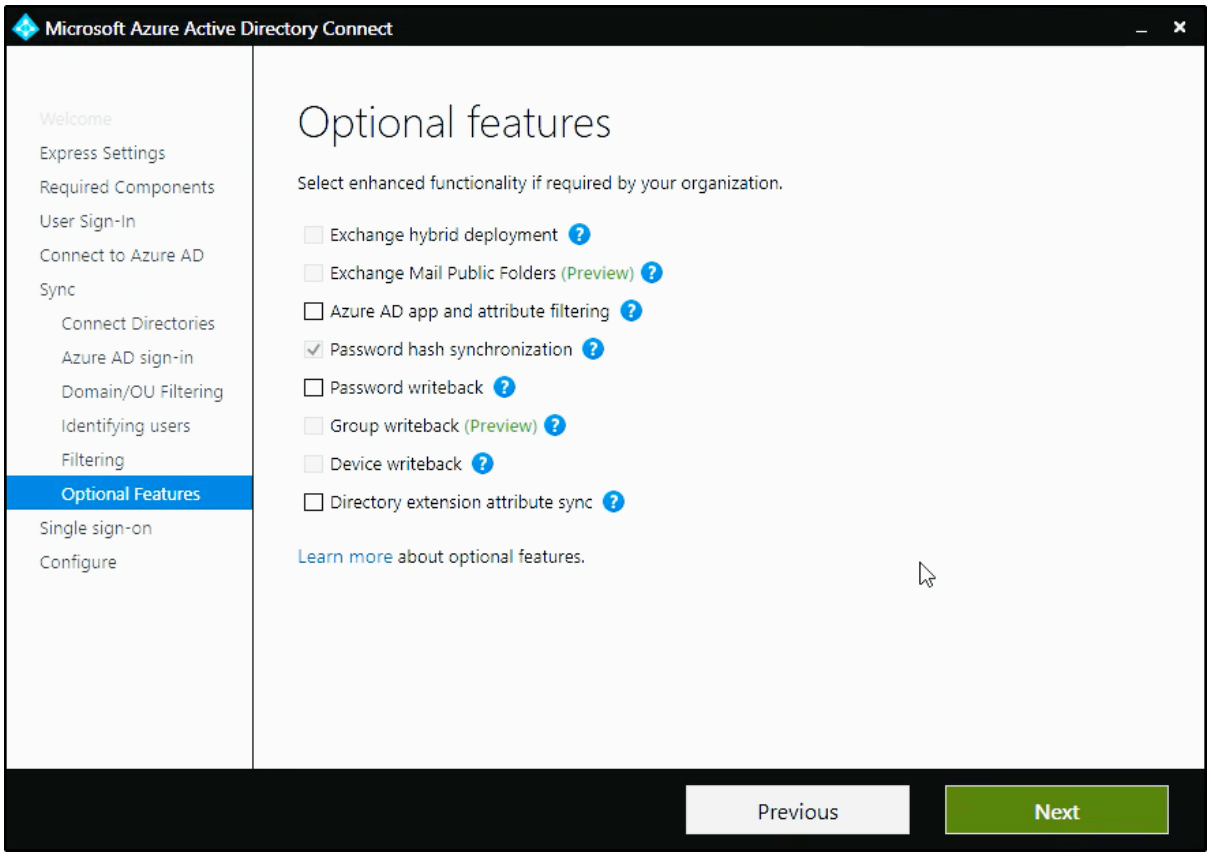
Figur 133: Azure AD Connect

Velger her å synkronisere alle brukere og enheter, og trykker **Next**.



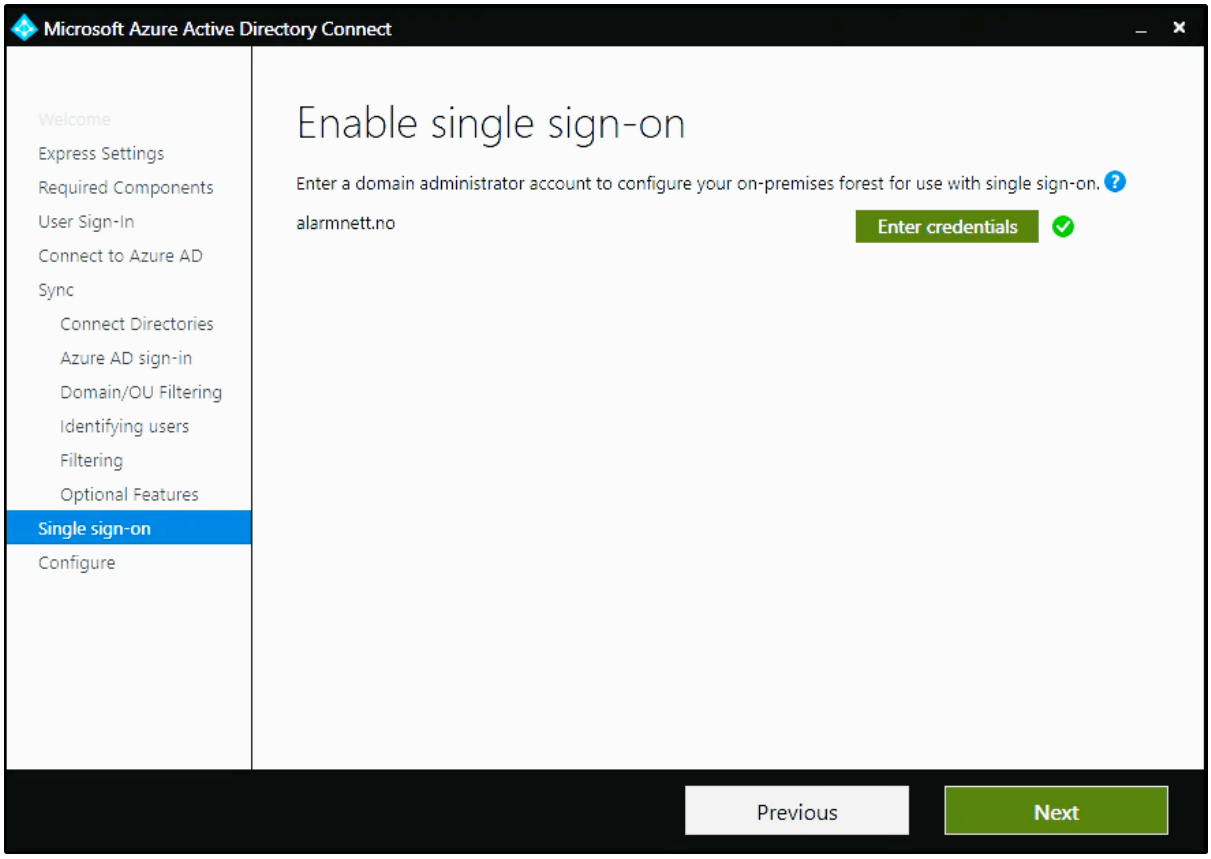
Figur 134: Azure AD Connect

Beholder standardinnstillinger her og trykker **Next**.



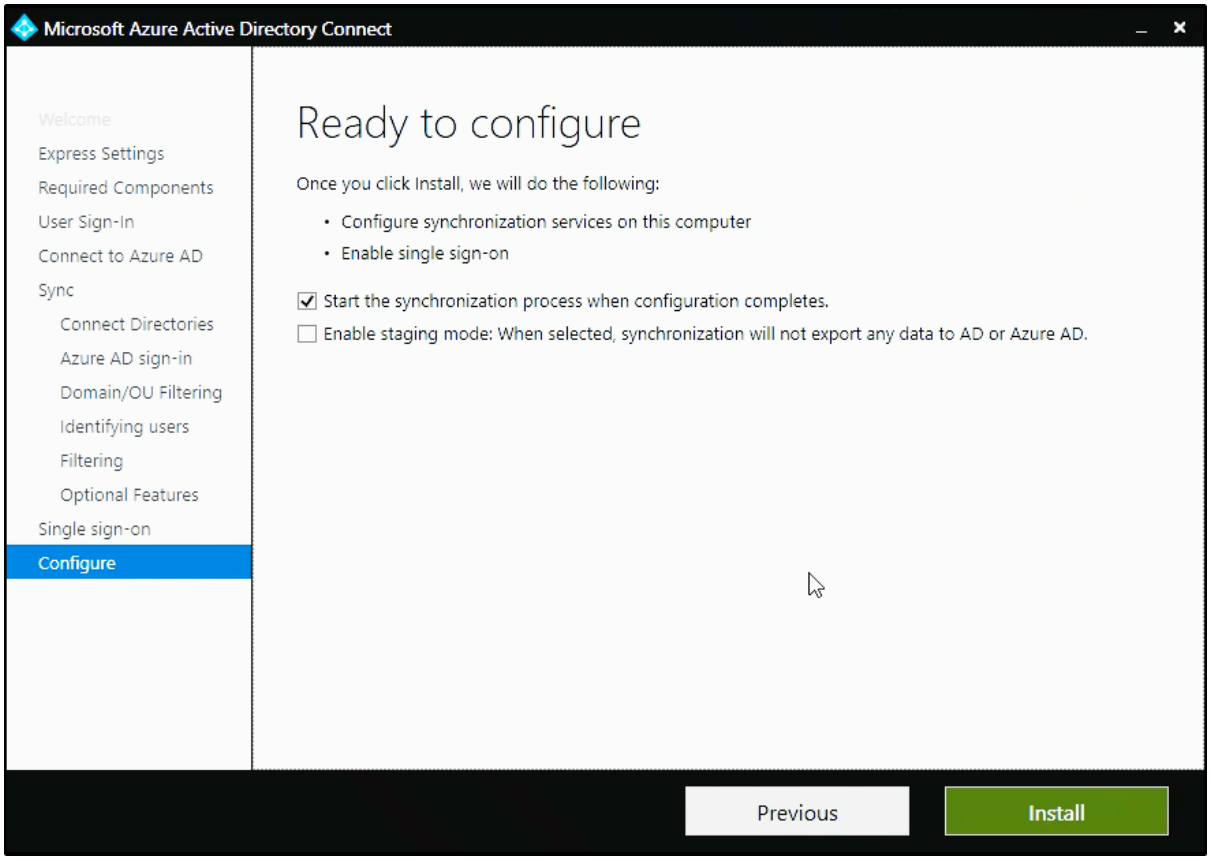
Figur 135: Azure AD Connect

Under ***Single sign-on***, trykker vi på **Enter credentials**, logger inn med administratorbruker, slik at vi får en grønn hake og trykker **Next**.



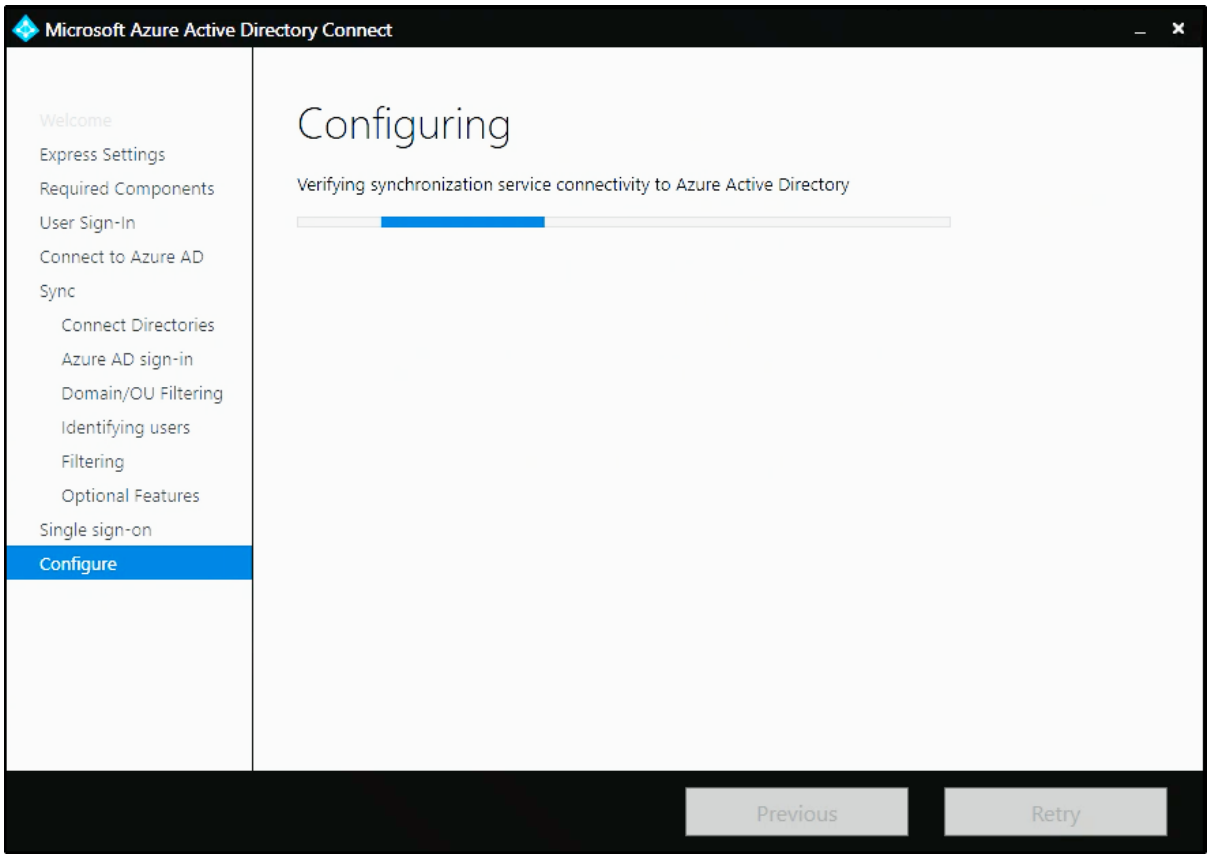
Figur 136: Azure AD Connect

Velger her å starte synkroniseringen, når konfigurasjonsprosessen er gjennomført. Vi trykker deretter **Install**.



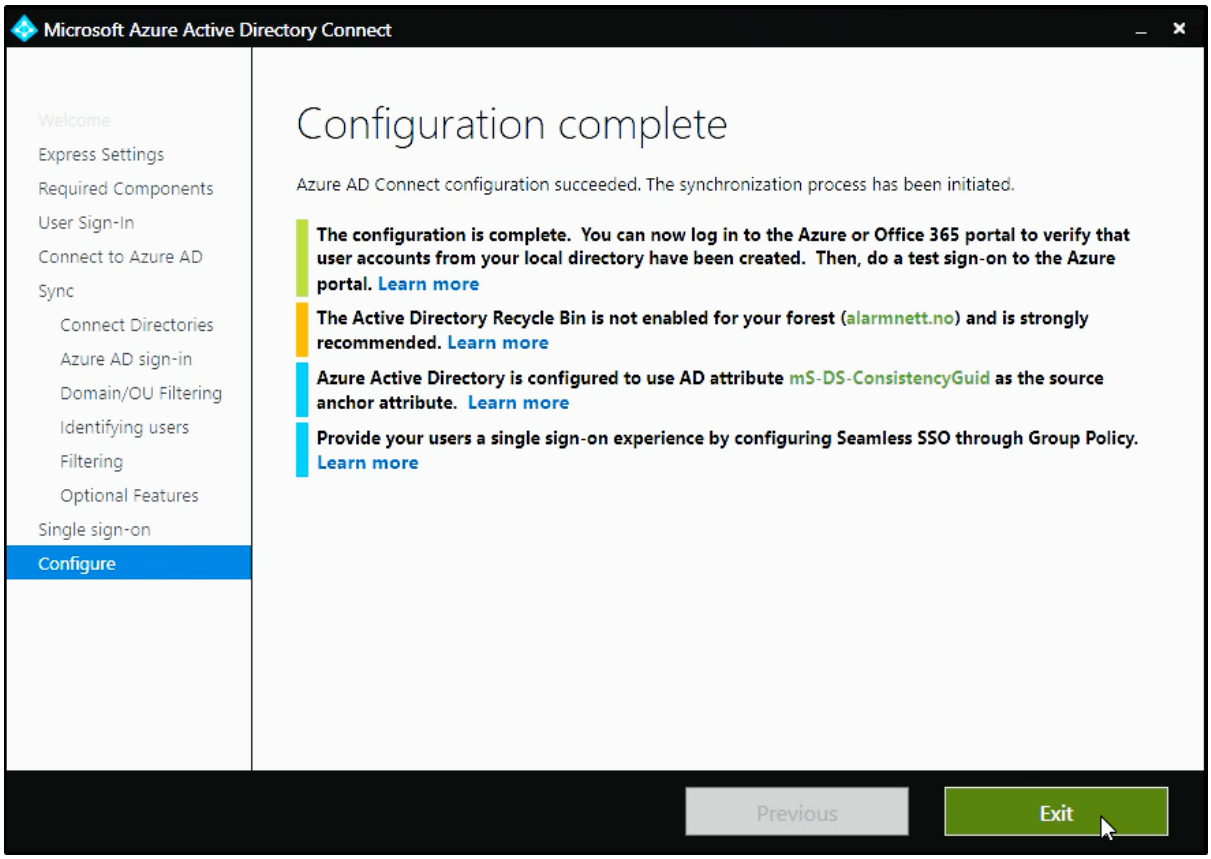
Figur 137: Azure AD Connect

Azure AD Connect konfigureres.



Figur 138: Azure AD Connect

Når konfigurasjonen er gjennomført, ser vi til at alt stemmer og trykker **Exit**.

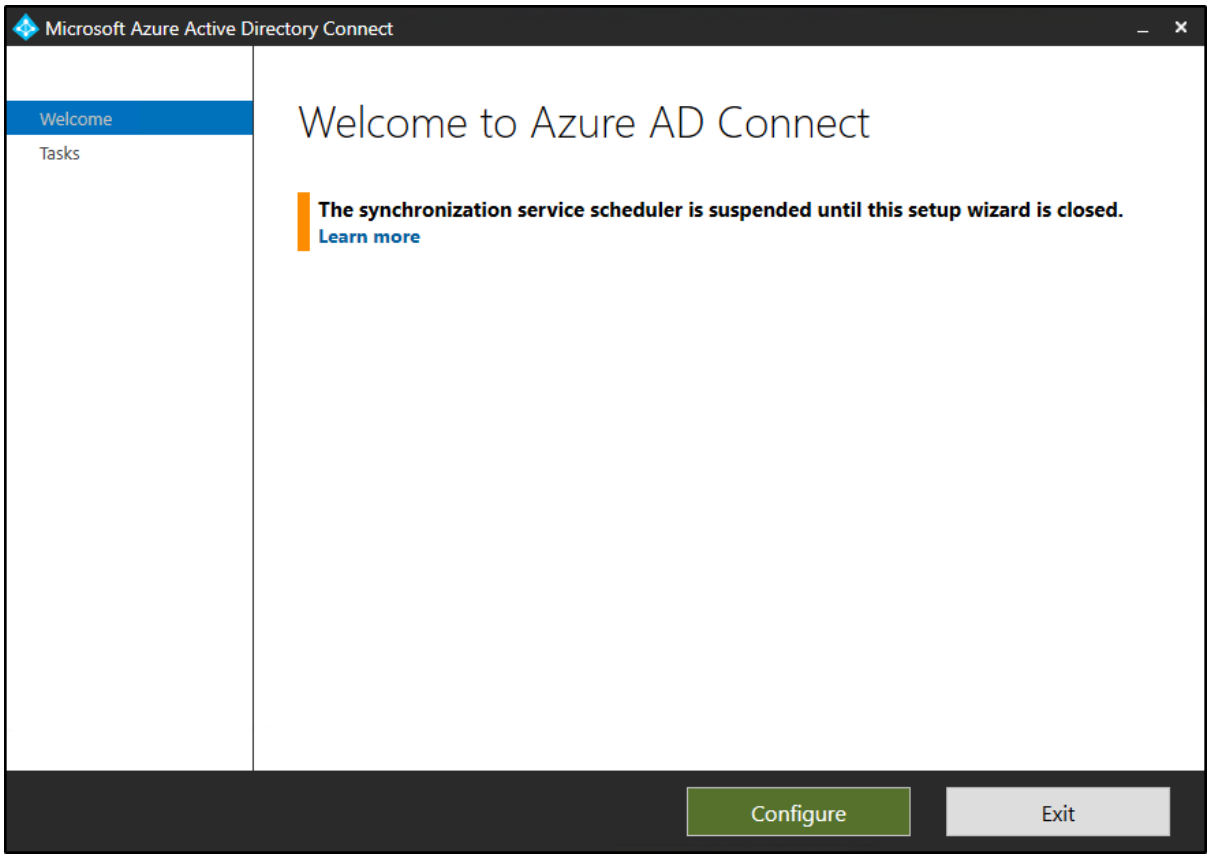


Figur 139: Azure AD Connect

Hybrid Azure AD Join

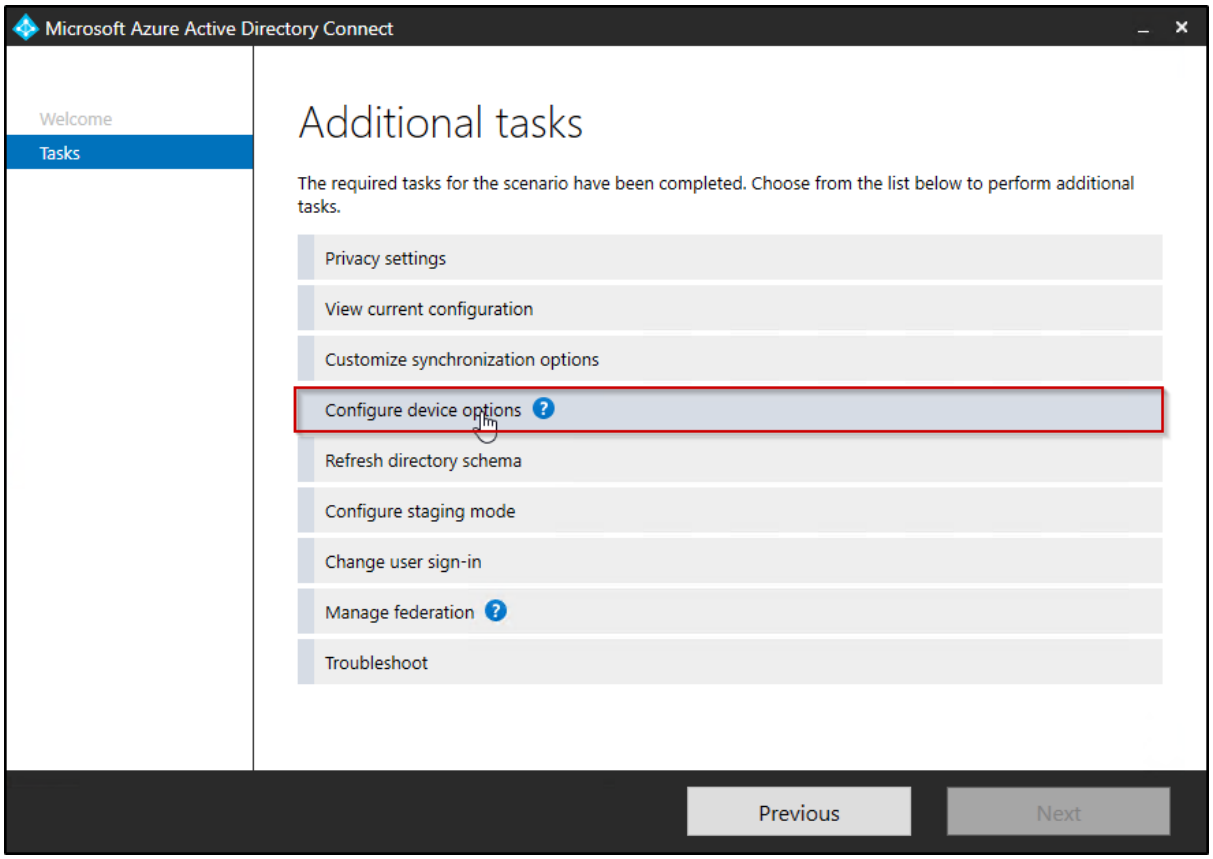
Når konfigurasjonen av Azure AD Connect er gjennomført, er vi nødt til å gjøre post-konfigurasjon. Vi skal nå aktivere Hybrid Azure AD Join. Vi velger derfor å starte opp Azure AD Connect programmet, ved å kjøre Azure AD Connect, som er tilsvarende det samme programmet som vi brukte for å konfigurere Azure AD Connect.

Velger **Configure**.



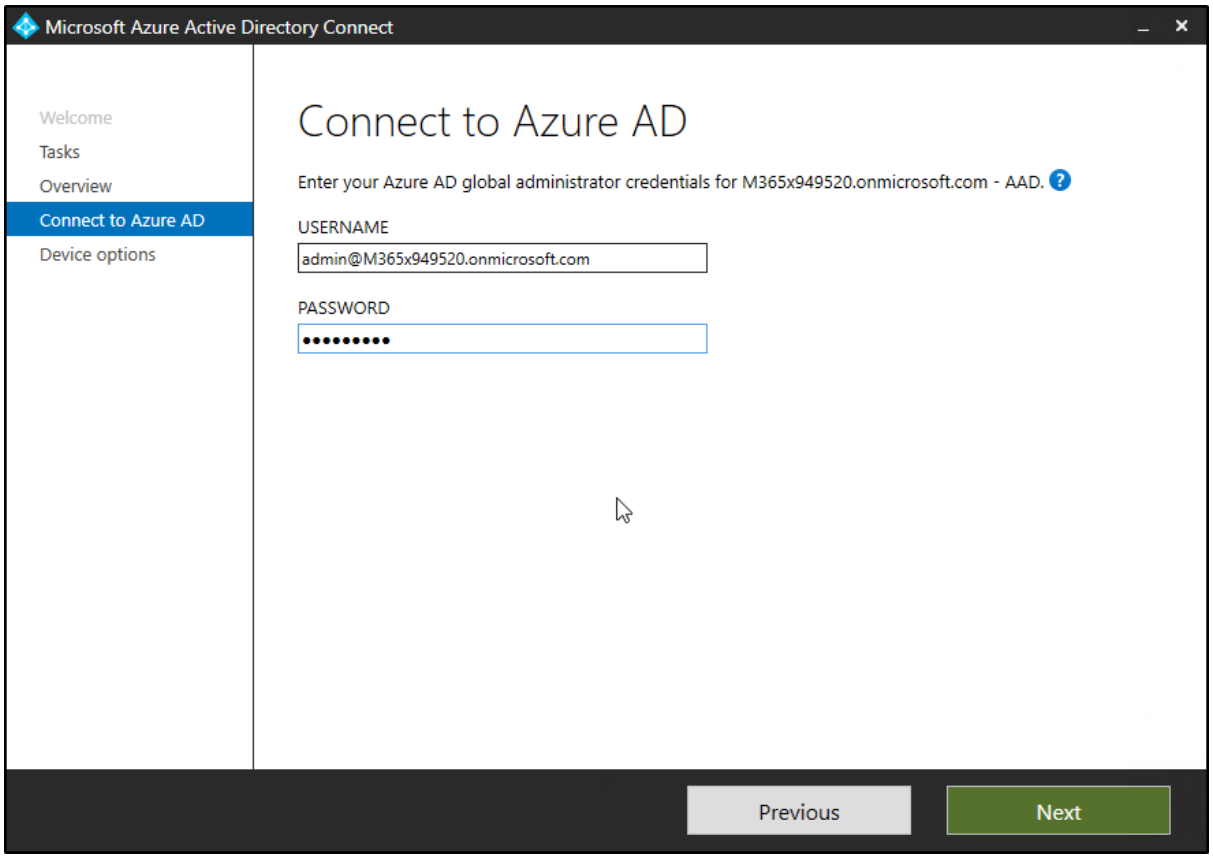
Figur 140: Konfigurasjon av Hybrid Azure AD Join

Velger **Configure device options**.



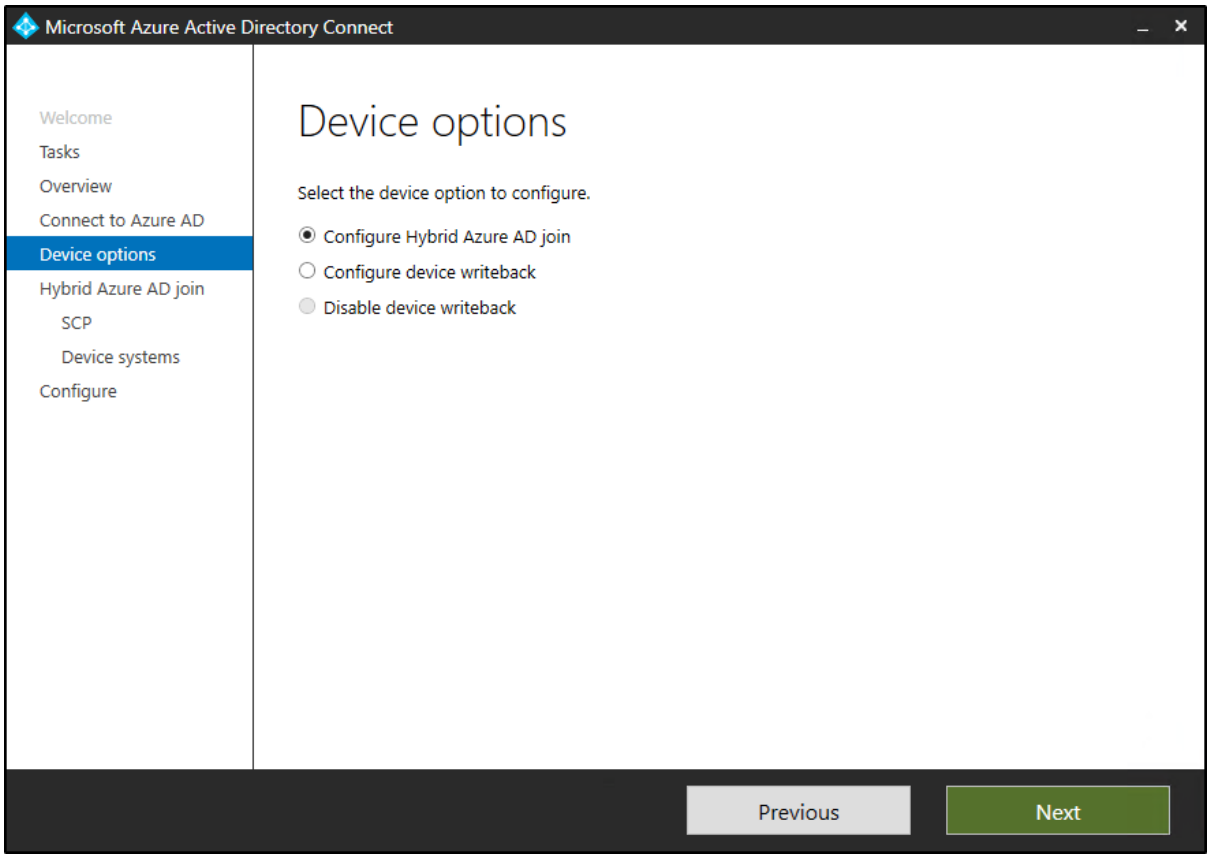
Figur 141: Konfigurasjon av Hybrid Azure AD Join

Logger inn med Azure tenant adminstratorbruker og trykker **Next**.



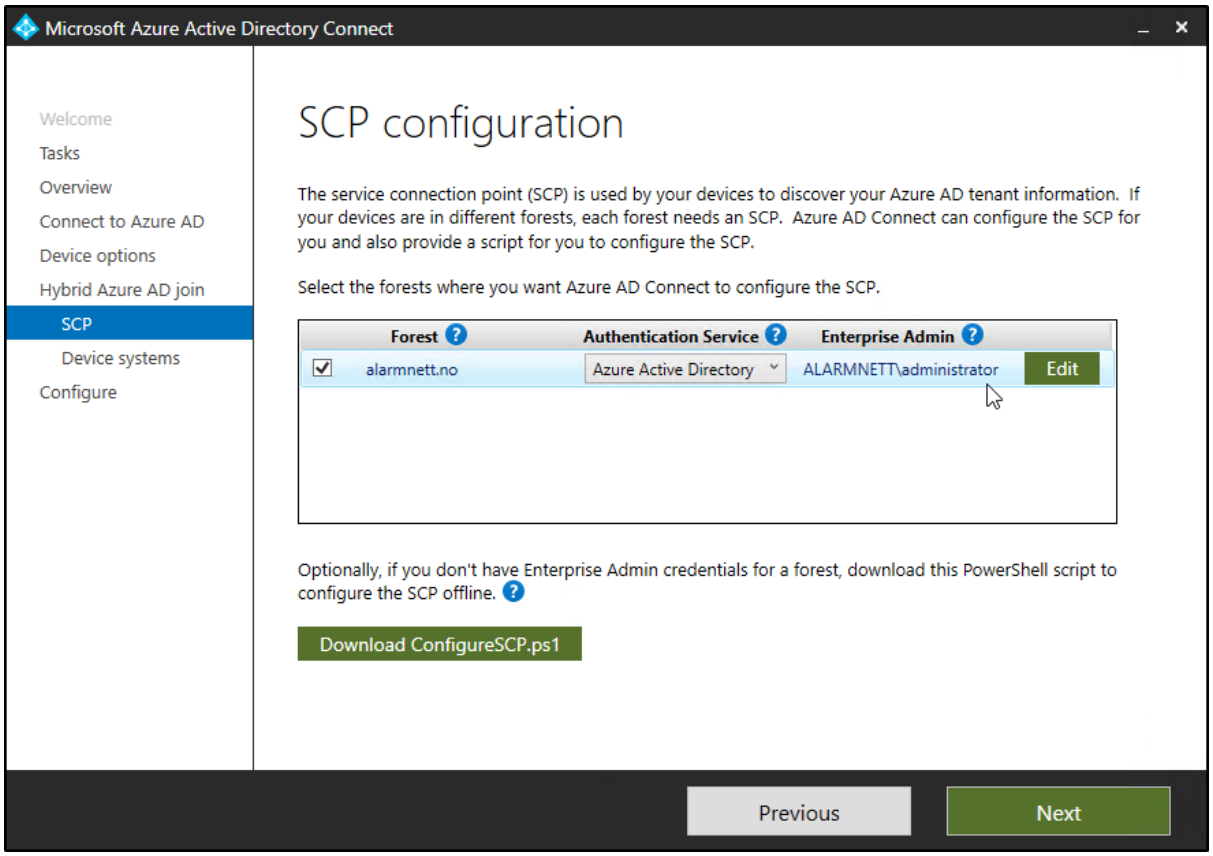
Figur 142: Konfigurasjon av Hybrid Azure AD Join

Under ***Device options***, velger vi *Configure Hybrid Azure AD join* og trykker **Next**.



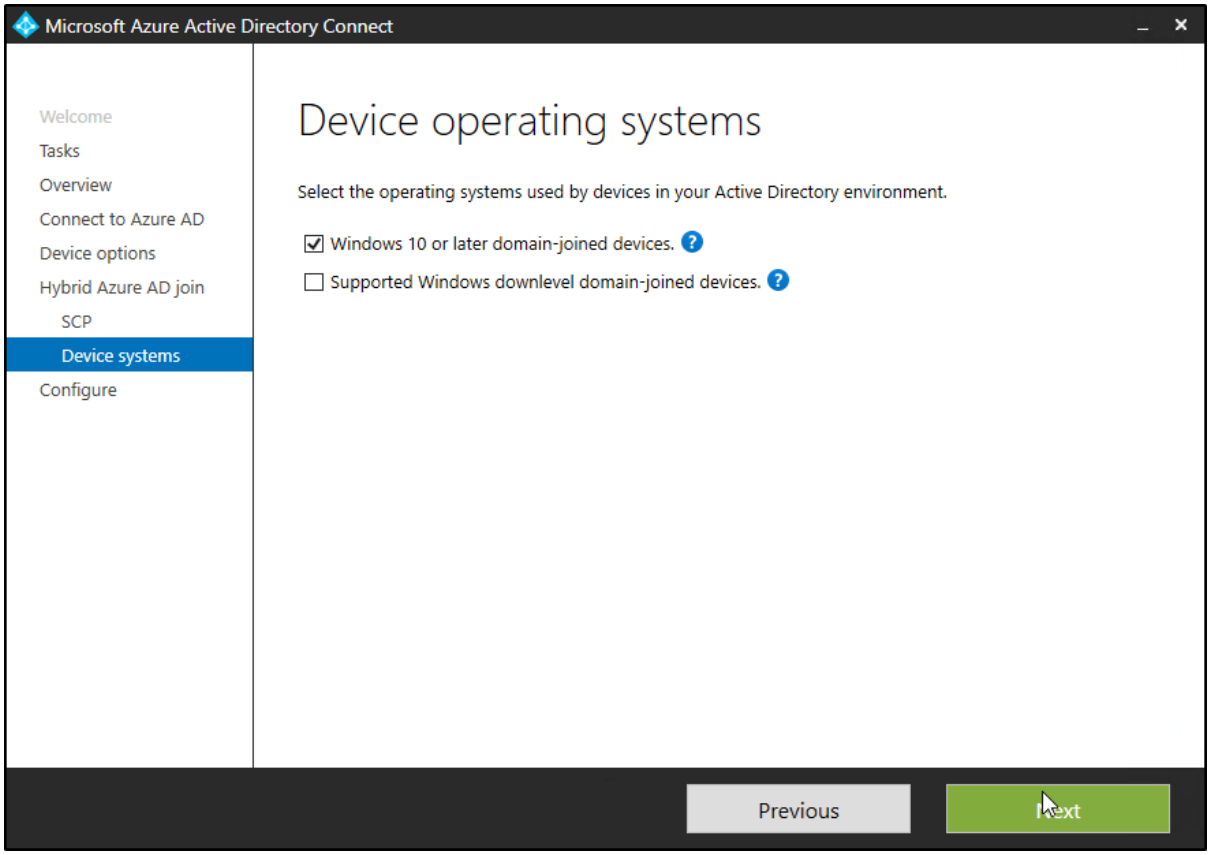
Figur 143: Konfigurasjon av Hybrid Azure AD Join

Velger forest ved å huke av for alarmnett.no og trykker **Next**.



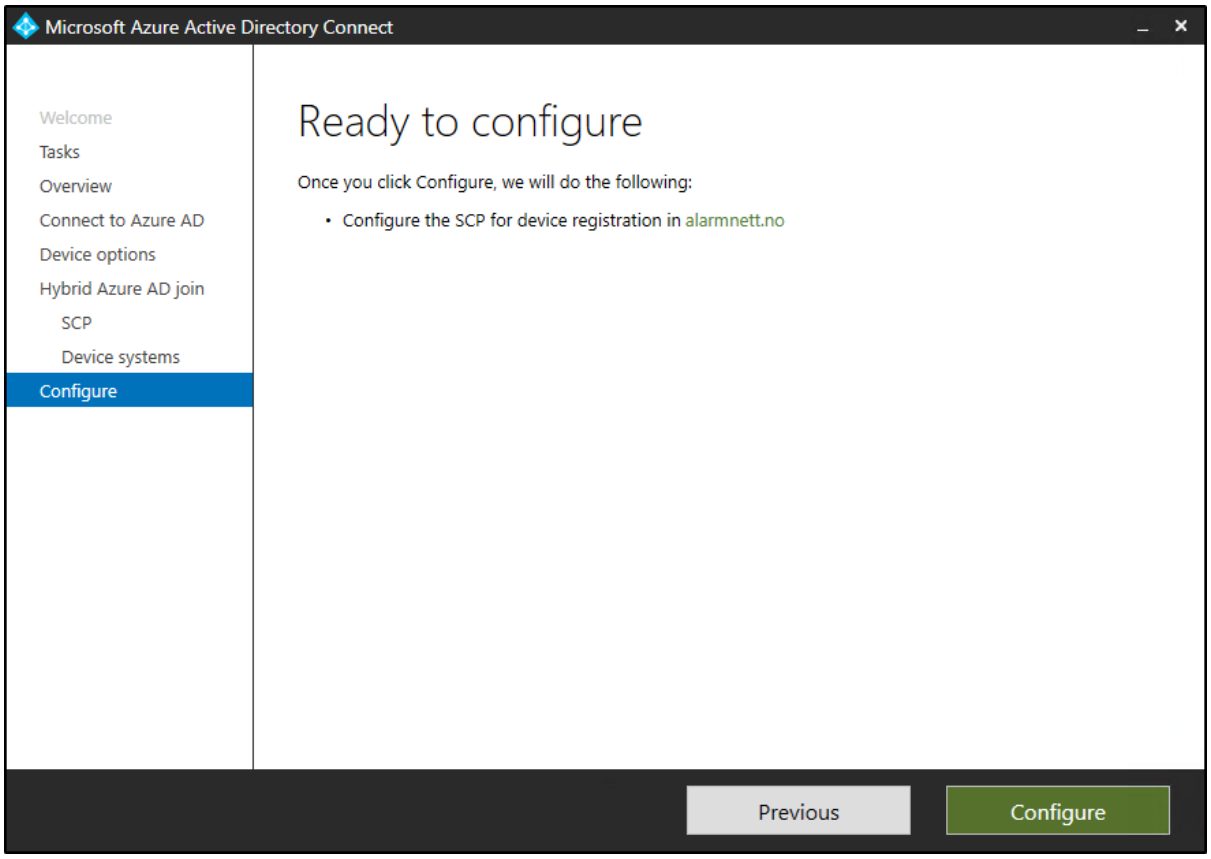
Figur 144: Konfigurasjon av Hybrid Azure AD Join

Velger om man ønsker å støtte legacy-systemer eller ikke. Vi velger her å støtte kun Windows 10 eller nyere enheter og trykker **Next**.



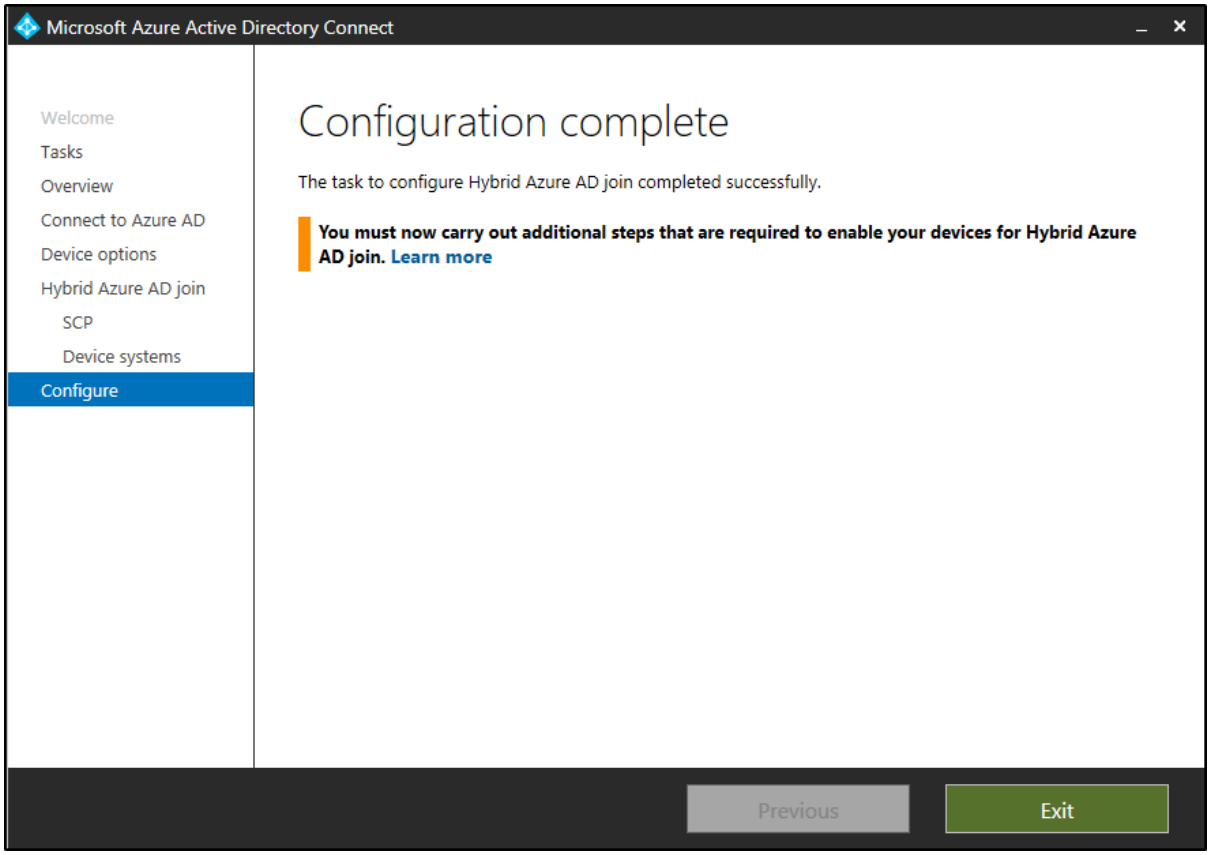
Figur 145: Konfigurasjon av Hybrid Azure AD Join

Velger så **Configure**.



Figur 146: Konfigurasjon av Hybrid Azure AD Join

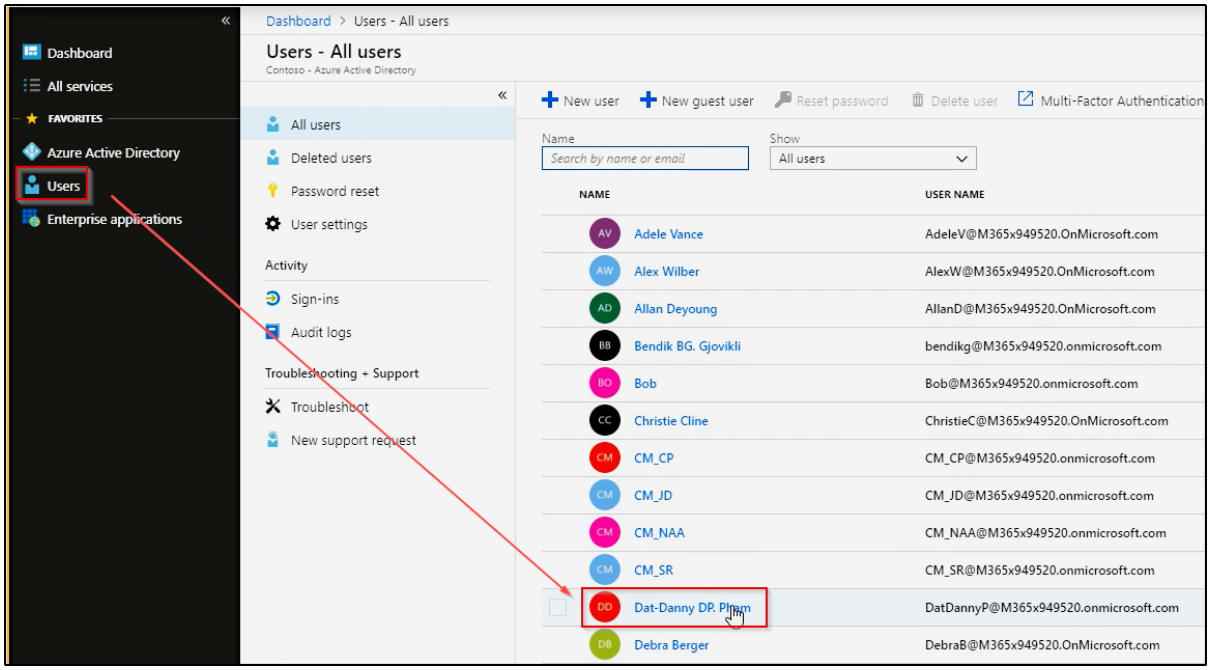
Når vi ser denne skjermen, har vi kommet oss gjennom konfigurasjonen og Hybrid Azure AD Join er satt opp.



Figur 147: Konfigurasjon av Hybrid Azure AD Join

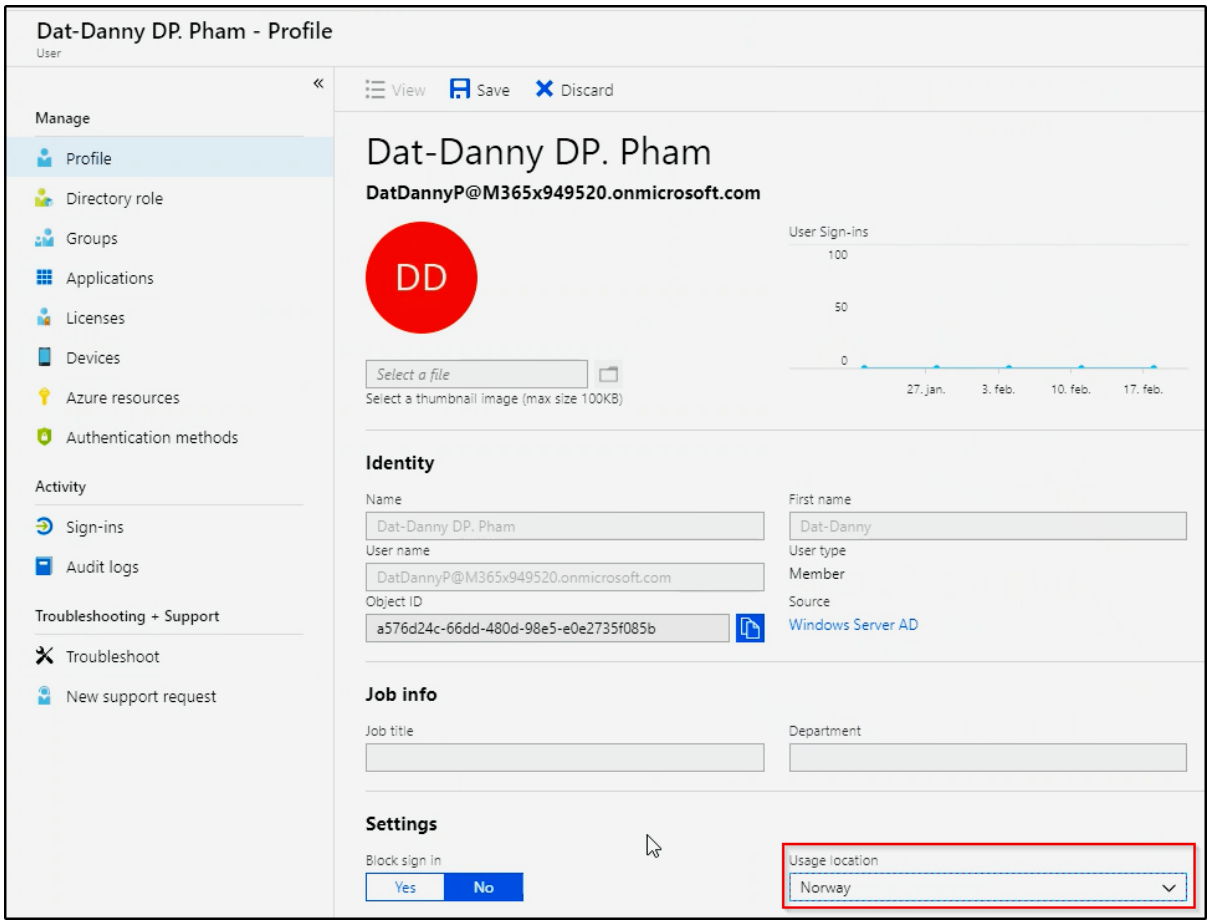
Tildele lisenser til On-Premise-brukere

For å tildele lisenser til brukere, navigerer vi oss til ***Users*** i Azure. Velger en bruker som vi ønsker å tildele lisenser til, i denne demonstrasjonen har vi valgt å tildele lisens til brukeren: Dat-Danny Pham.



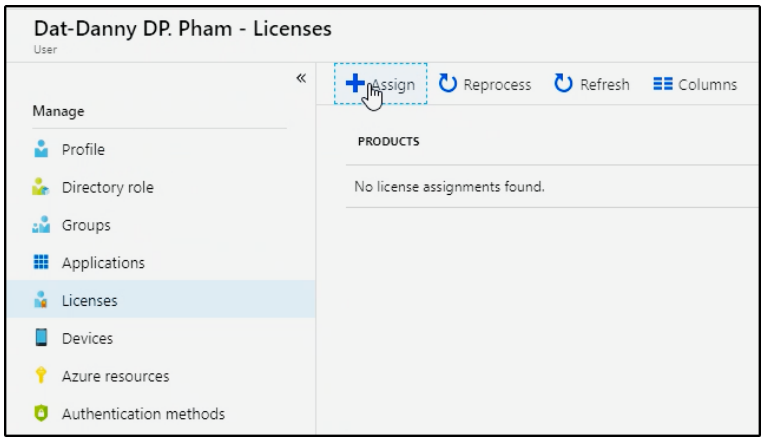
Figur 148: Tildele lisenser til brukere fra On-Premise miljø

Det første vi må gjøre, i og med at denne brukeren er en bruker som er synkronisert over fra lokal Active Directory, er å sette *Usage location*. Dersom dette ikke er satt, vil man ikke kunne tildele lisenser til brukeren. Vi setter denne til **Norway**.



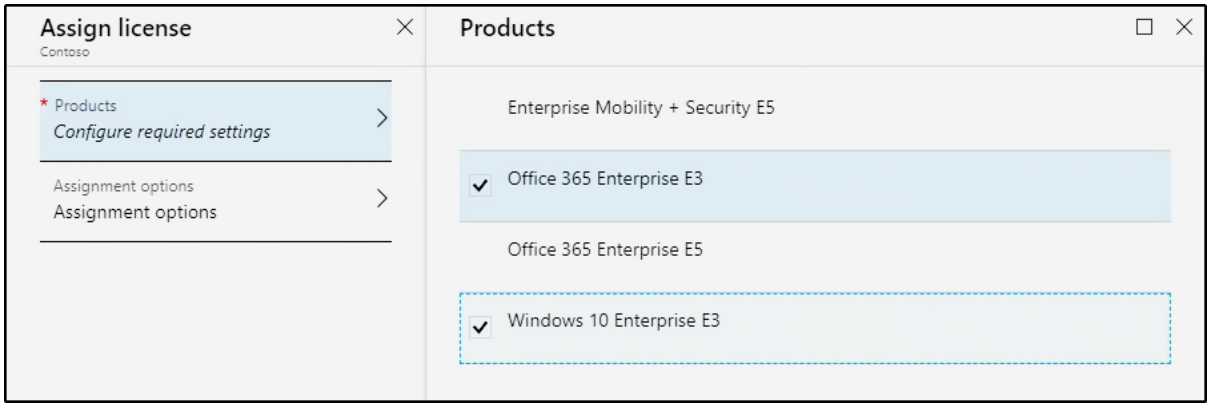
Figur 149: Tildele lisenser til brukere fra On-Premise miljø

Deretter trykker vi på **Assign**, for å få opp vinduet som viser mulige lisenser brukeren kan få.



Figur 150: Tildele lisenser til brukere fra On-Premise miljø

For denne demonstrasjonen har vi valgt å gi brukeren *Office 365 enterprise E3* og *Windows 10 Enterprise E3* og trykker **Assign**.



Figur 151: Tildele lisenser til brukere fra On-Premise miljø

Co-Management

Vi skal nå se på Installasjon og oppsett av Co-Management, prerequisites, problemer vi møtte på og hvordan vi løste dem.

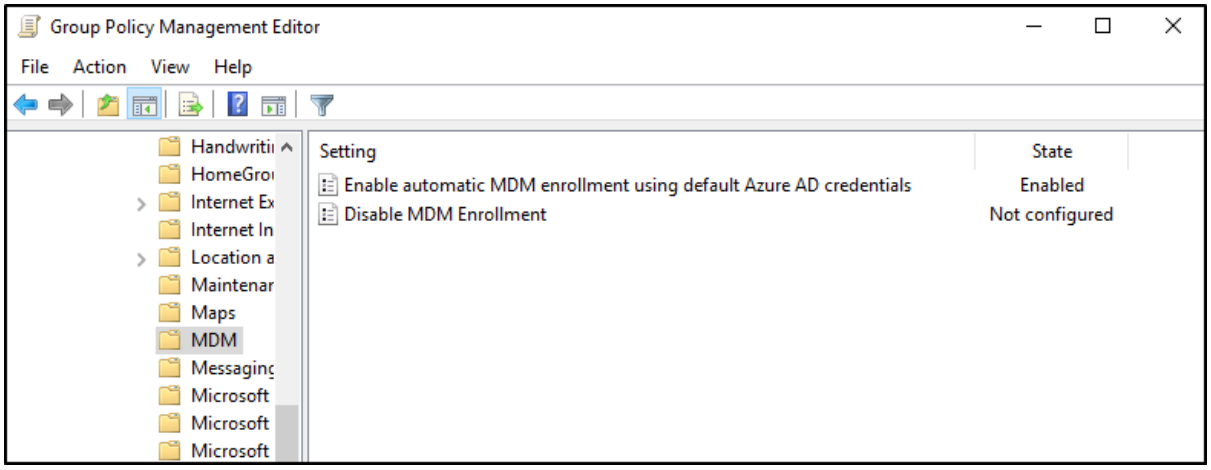
Co-management er en tilstand, hvor SCCM og Intune jobber sammen, for å håndtere diverse funksjoner og tjenester. Avhengig av workloads som flyttes over til Intune, vil drift av co-managed enheter gradvis overtas av Intune.

Når Co-Management er konfigurert, vil vi videre se på workloads og hvordan vi velger å fordele disse mellom Configuration Manager og Intune.

Prerequisites	**Forklaring**
Lisenser	Når det gjelder lisenser trenger man Azure AD Premium og EMS eller Intune lisens for samtlige brukere som skal kunne ha mulighet til å ta nytte av Co-Management. I vårt tilfelle har vi valgt å benytte oss av **Enterprice Mobility + Security E5**.
Configuration Manager	SCCM versjon 1710 eller nyere, hvis man tar i bruk versjon 1806 har man mulighet til å koble flere Configuration Manager instanser til en enkelt intune tenant. Man vil også få mulighet til å la intune administrere flere workloads.
Azure AD	
Windows 10 enheter må være joined til Azure AD.	Hybrid Azure AD-joined Azure AD-joined
Microsoft Intune	
Windows 10	Co-Management støtter kun Windows 10 enheter med versjon 1709 eller nyere.
Aktivering	Aktivere Co-Management i Configuration Manager.
GPO	Man må opprette en GPO som aktiverer mulighet for innrulling av enhet til MDM (Intune), samt sette delegation.
Aktivere Domain Trust	Sette opp trust fra domenekontroller opp mot Azure tenant, slik at man får mulighet til å opprette brukere med Tenant UPN, samt endre UPN på brukere. Dette muliggjør innlogging med brukere som benytter tenant UPN, slik at man får innrullet maskiner til Intune.

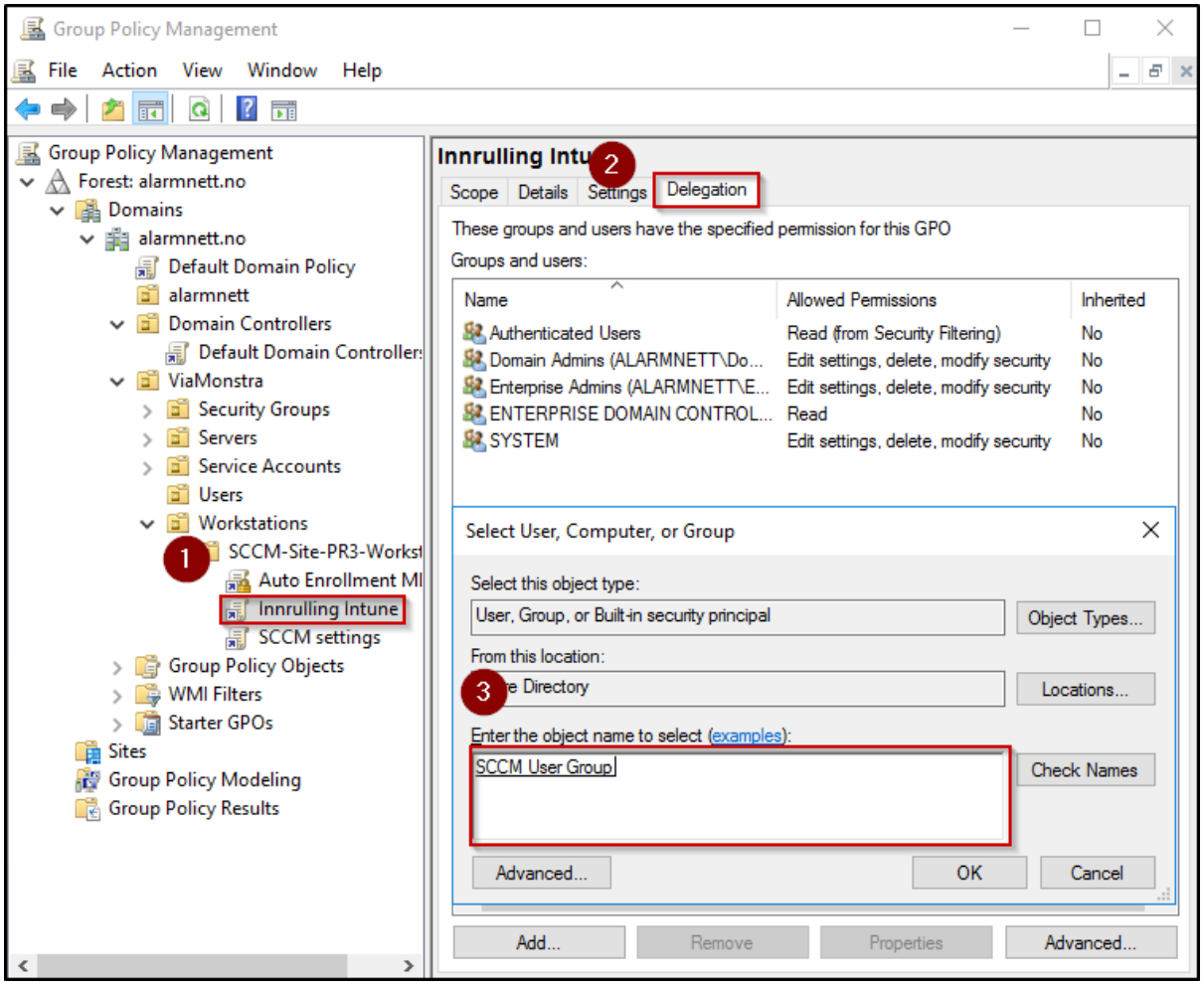
GPO - Innrulling til MDM

Som nevnt ovenfor, må vi benytte oss av en GPO for å kunne ta i bruk automatisk innrulling av maskiner fra vårt on-premise miljø. Vi lager derfor et Group Policy objekt, hvor vi setter **Enabled**, på *Enable automatic MDM enrollment using default Azure AD credentials*.



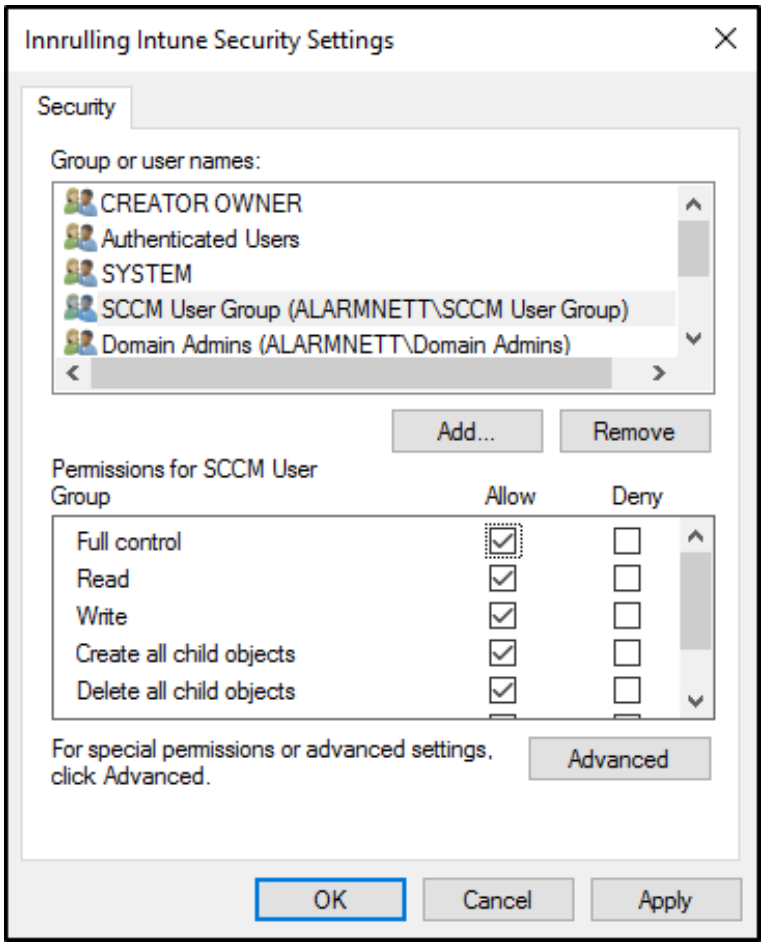
Figur 152: GPO - Innrulling til MDM

Linker GPO-en til OU-en hvor våre enheter ligger og velger deretter å sette *Delegation.* Vi gjør dette slik at brukerne har mulighet til å kjøre GPO-en på sin maskin.



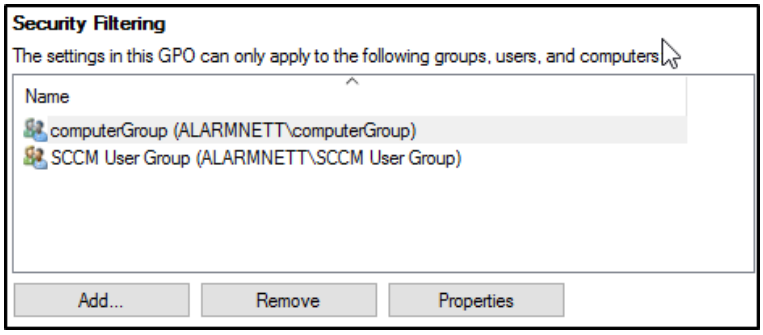
Figur 153: GPO - Innrulling til MDM

Vi velger også å sette rettighetene *Full control* på gruppen.



Figur 154: GPO - Innrulling til MDM

Vi setter også *Security Filtering*, slik at vi får avgrenset hvem som skal ta i bruk denne GPO-en.

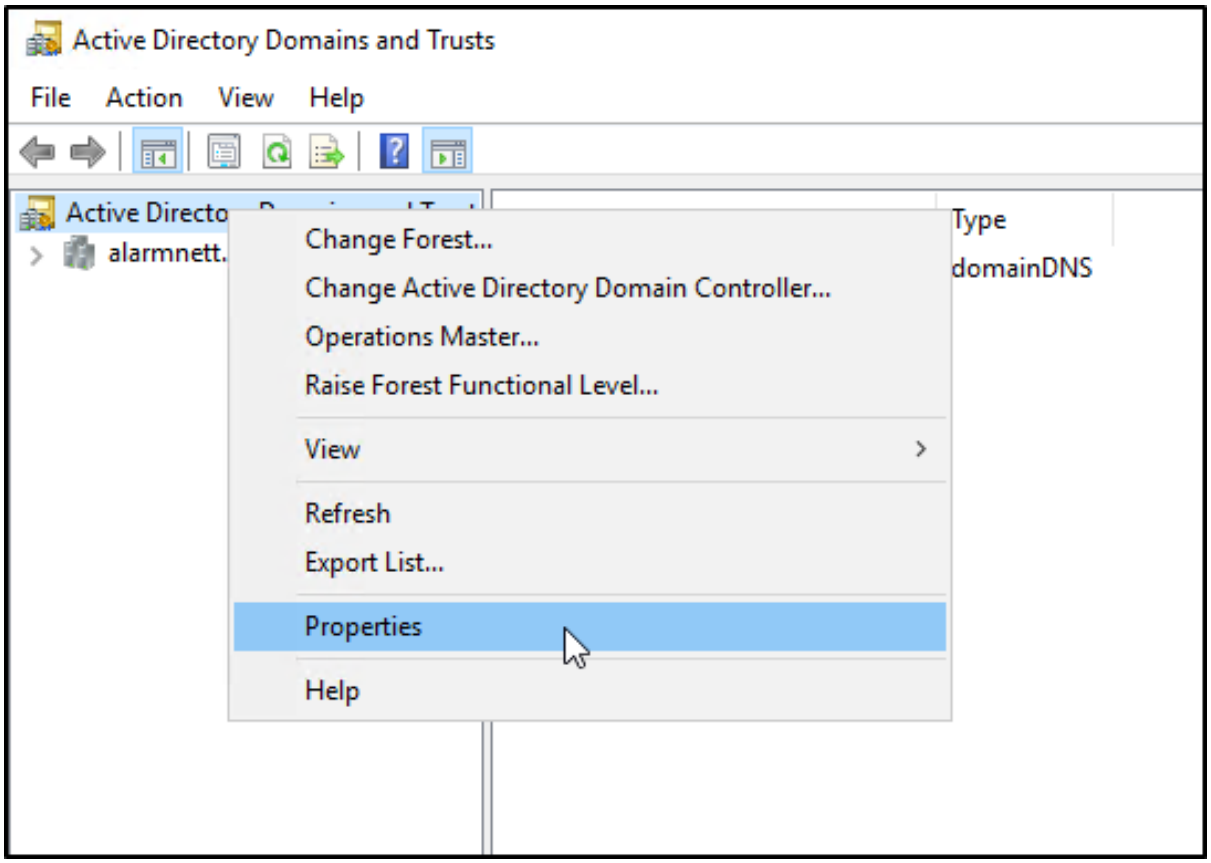


Figur 155: GPO - Innrulling til MDM

Aktivere domain trust

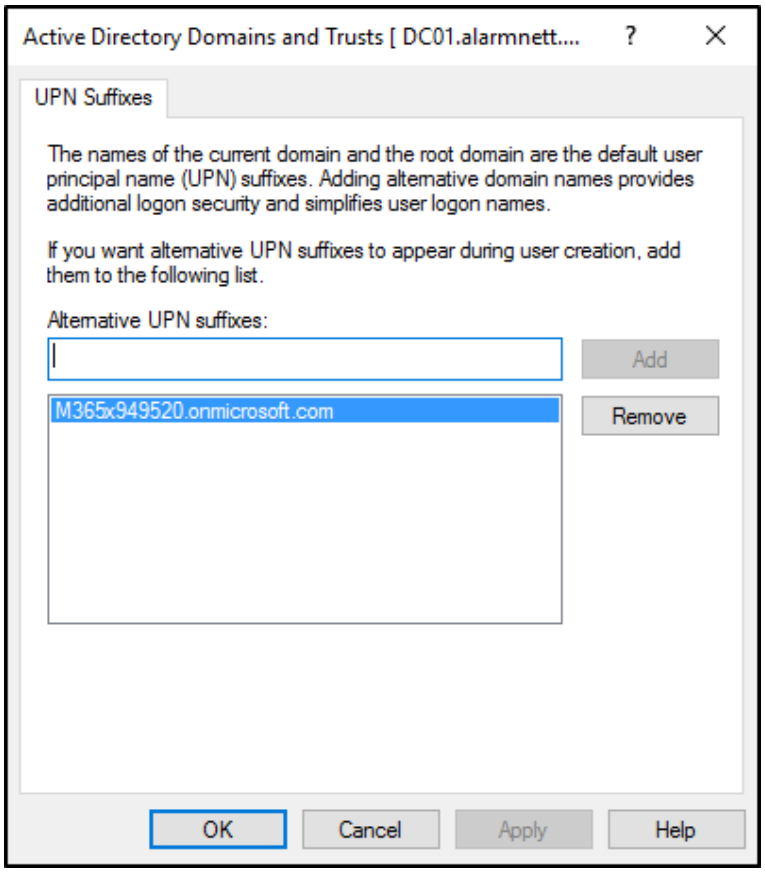
I og med at det er her snakk om on-premise brukere som er hovedbrukere av disse enhetene, må vi aktivere domain trust mellom lokal AD og Azure AD. Vi gjør dette slik at våre on-premise brukere i lokal AD kan benytte seg av UPN til vår Azure tenant.

Vi åpner opp Active directory Domains and Trust, høyreklikker på **Active Directory Domain Trust** og velger **Properties**.



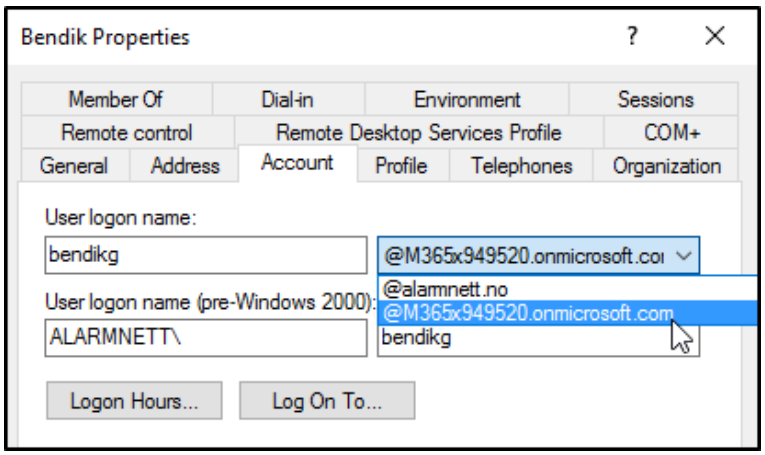
Figur 156: Aktivere domain trust

Vi velger her å legge til vår Azure tenant UPN.



Figur 157: Aktivere domain trust

Deretter må vi gå inn på hver bruker i vår lokal AD og bytte fra alarmnett.no til Azure tenant UPN.

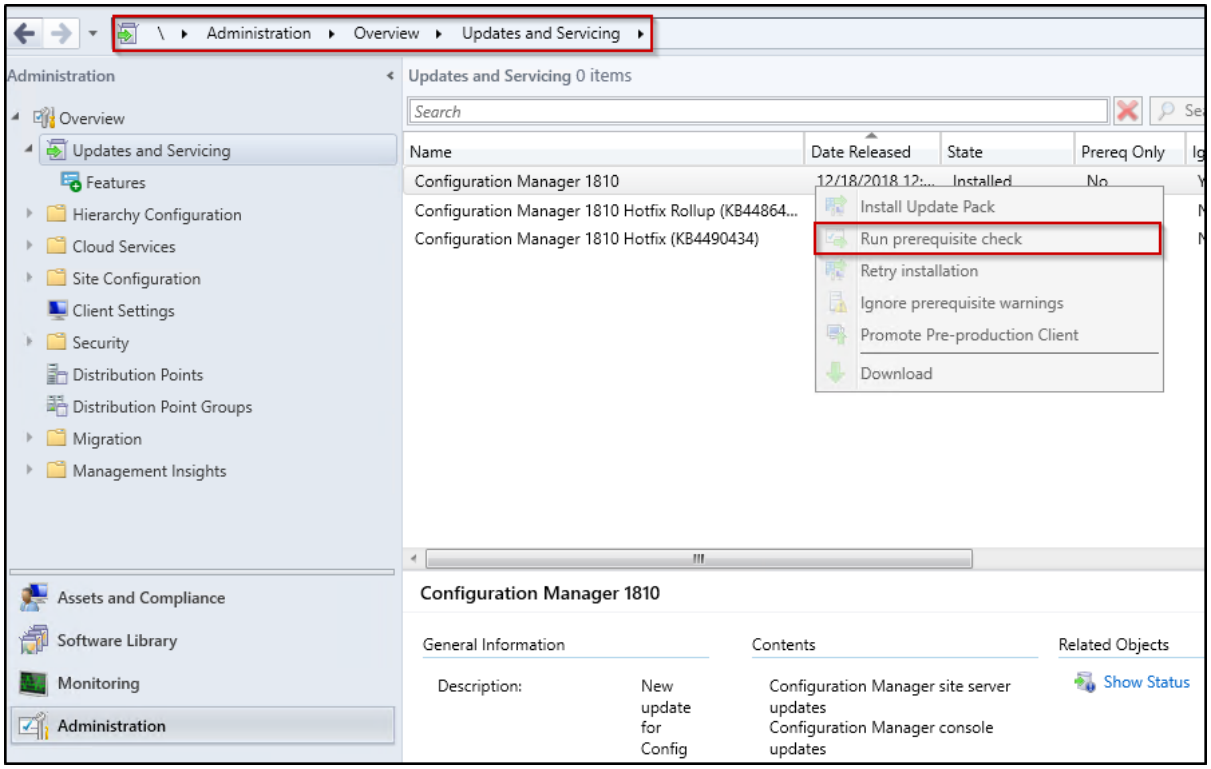


Figur 158: Aktivere domain trust

Oppgradere SCCM til versjon 1810

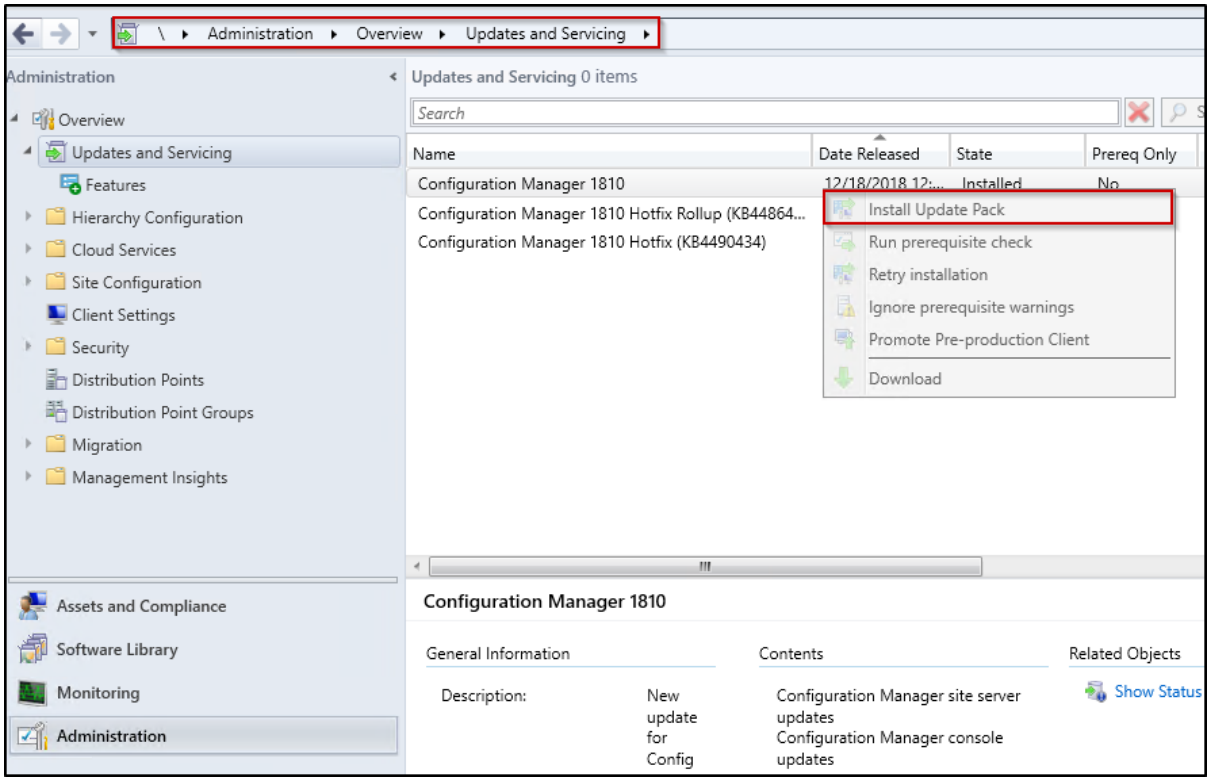
For å få tilgang til diverse nye innstillinger i SCCM er vi nødt til å oppgradere til siste versjon. Akkurat nå operer vi på versjon 1802. Denne gamle versjonen mangler funksjonalitet for Co-Management som er hovedfokuset i oppgaven. Vi velger derfor å oppgradere til SCCM 1810 versjonen.

Vi starter med å kjøre en Prerequisite check, for å se til at alt ligger til rette for at vi kan oppgradere til en nyere versjon. I Configuration Manager, under ***Administration – Updates and Services***, velger vi *Configuration Manager 1810* og kjører prerequisite check.



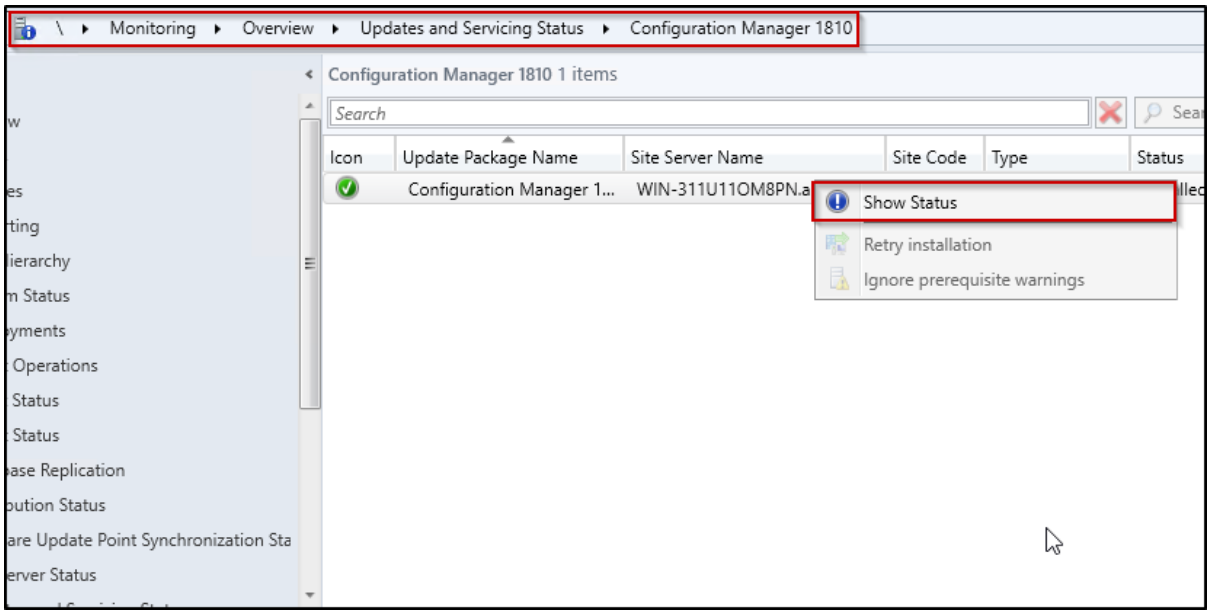
Figur 159: Oppgradere SCCM til versjon 1810

Dersom prerequisite-sjekken går gjennom uten problemer, kan vi videre starte installasjon av SCCM 1810. Vi velger her **Install Update Pack**.



Figur 160: Oppgradere SCCM til versjon 1810

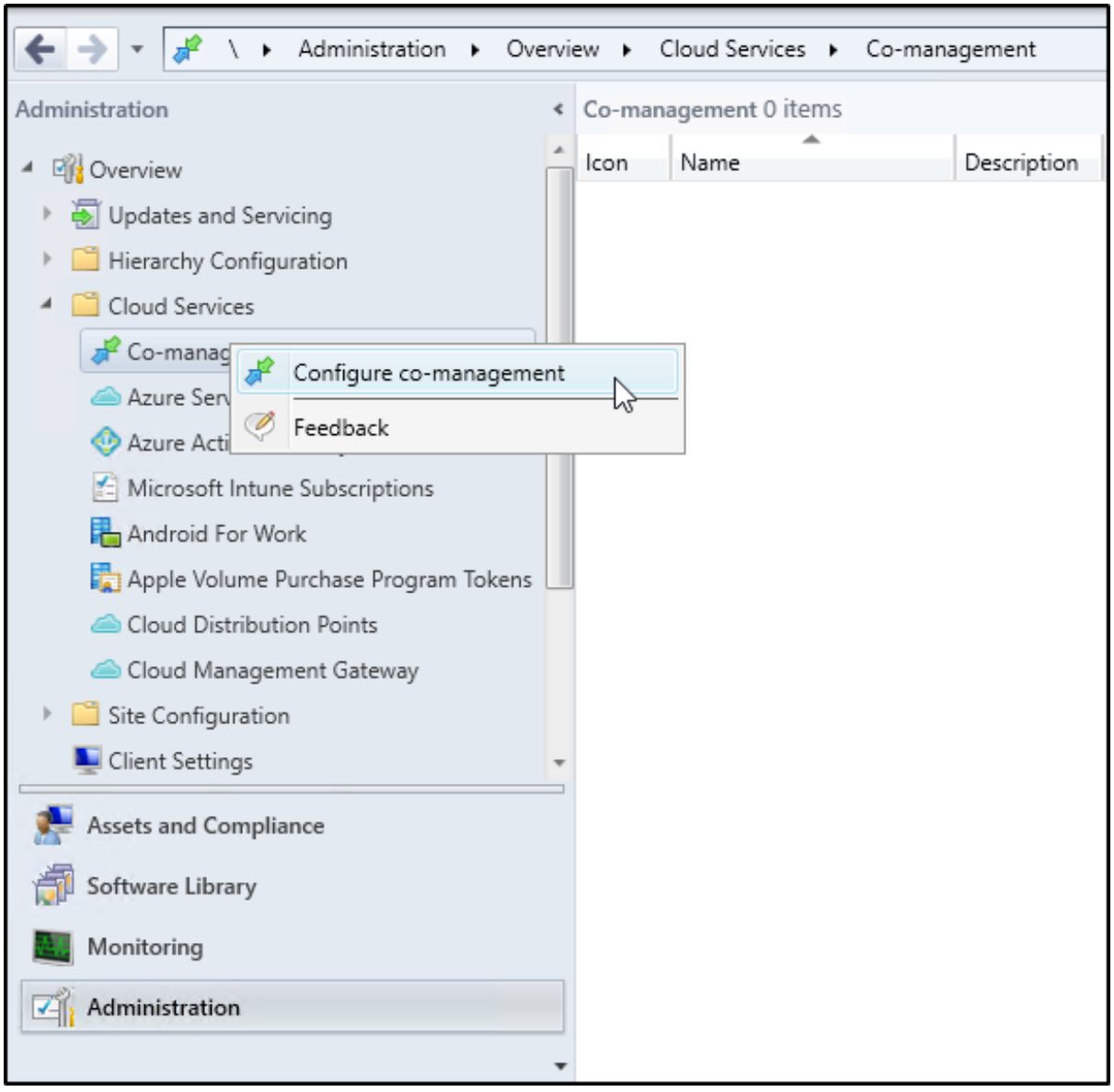
Dersom man ønsker å følge med på progresjonen under prerequsite-sjekken eller under selve oppgraderingen, kan man velge **Show Status** under Monitorering.



Figur 161: Oppgradere SCCM til versjon 1810

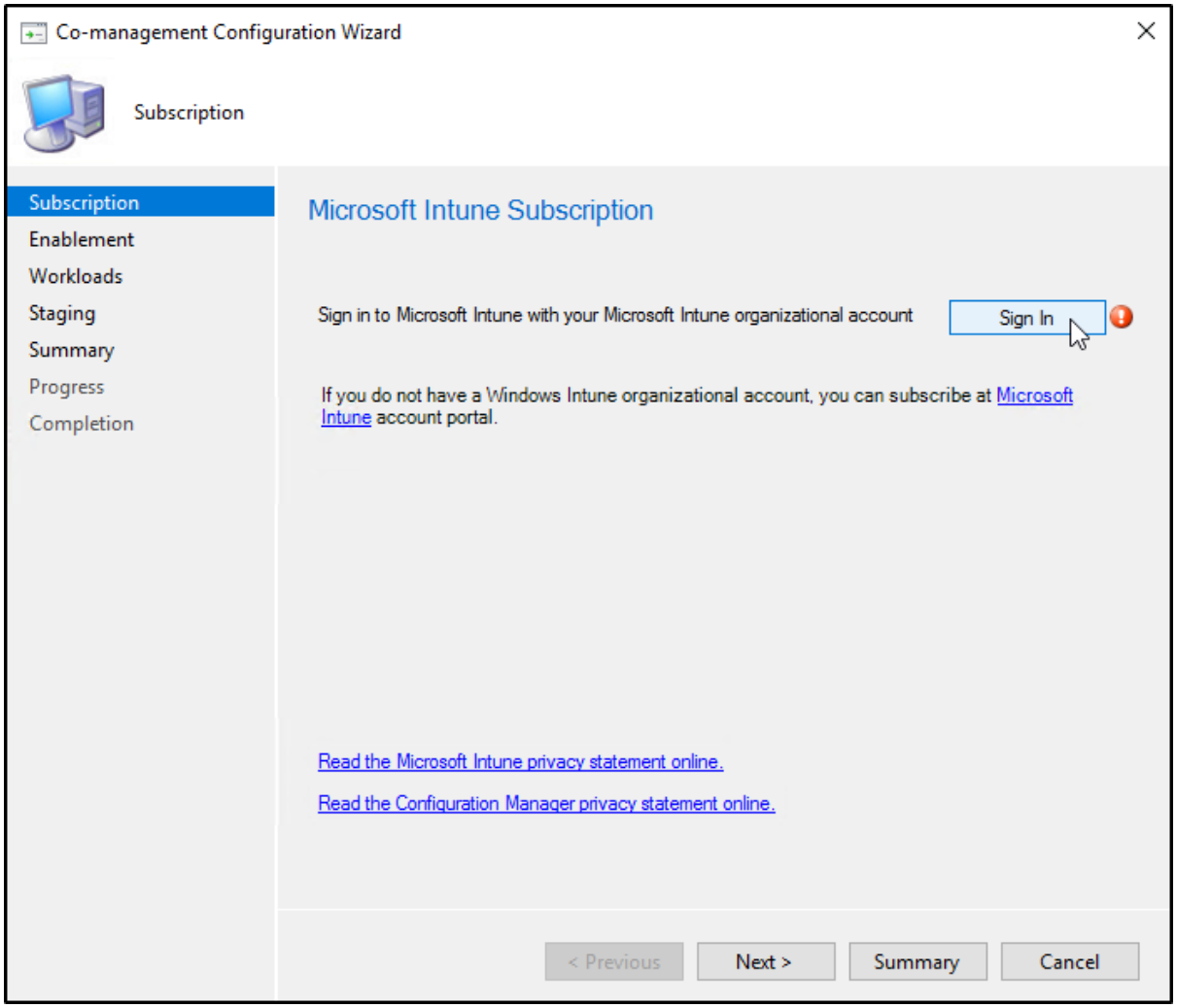
Aktivere Co-Management

Til nå har vi gjort en del forberedelser i forhold til å kunne ta i bruk Co-Management. Vi skal nå endelig begynne å se på hvordan vi konfigurere Co-Management i Configuration Manager. Vi navigerer oss til ***Administration – Cloud Services – Co-Management***, og velger **Configure co-management**.



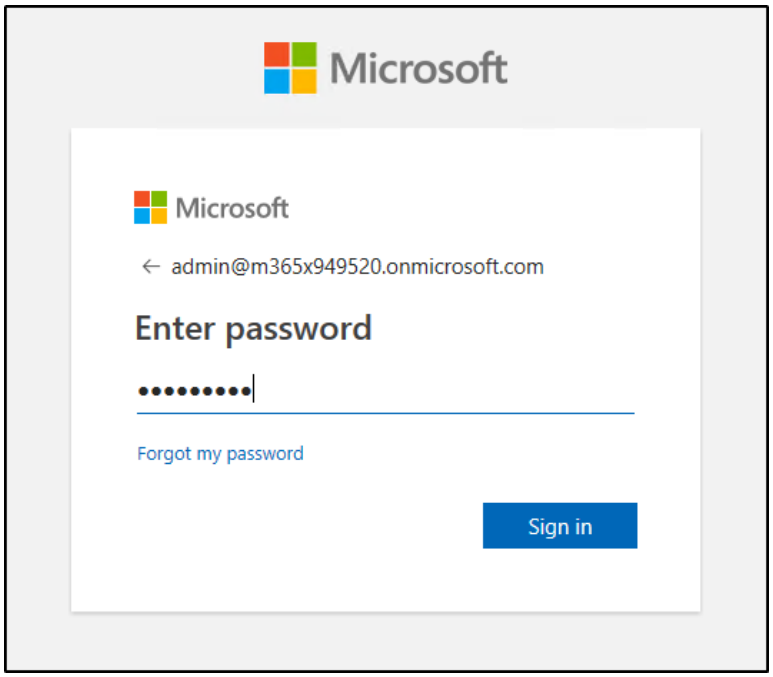
Figur 162: Slå på Co-Management

Vi begynner med å logge inn til vår Microsoft Intune administratorbruker ved å trykke på **Sign In**.



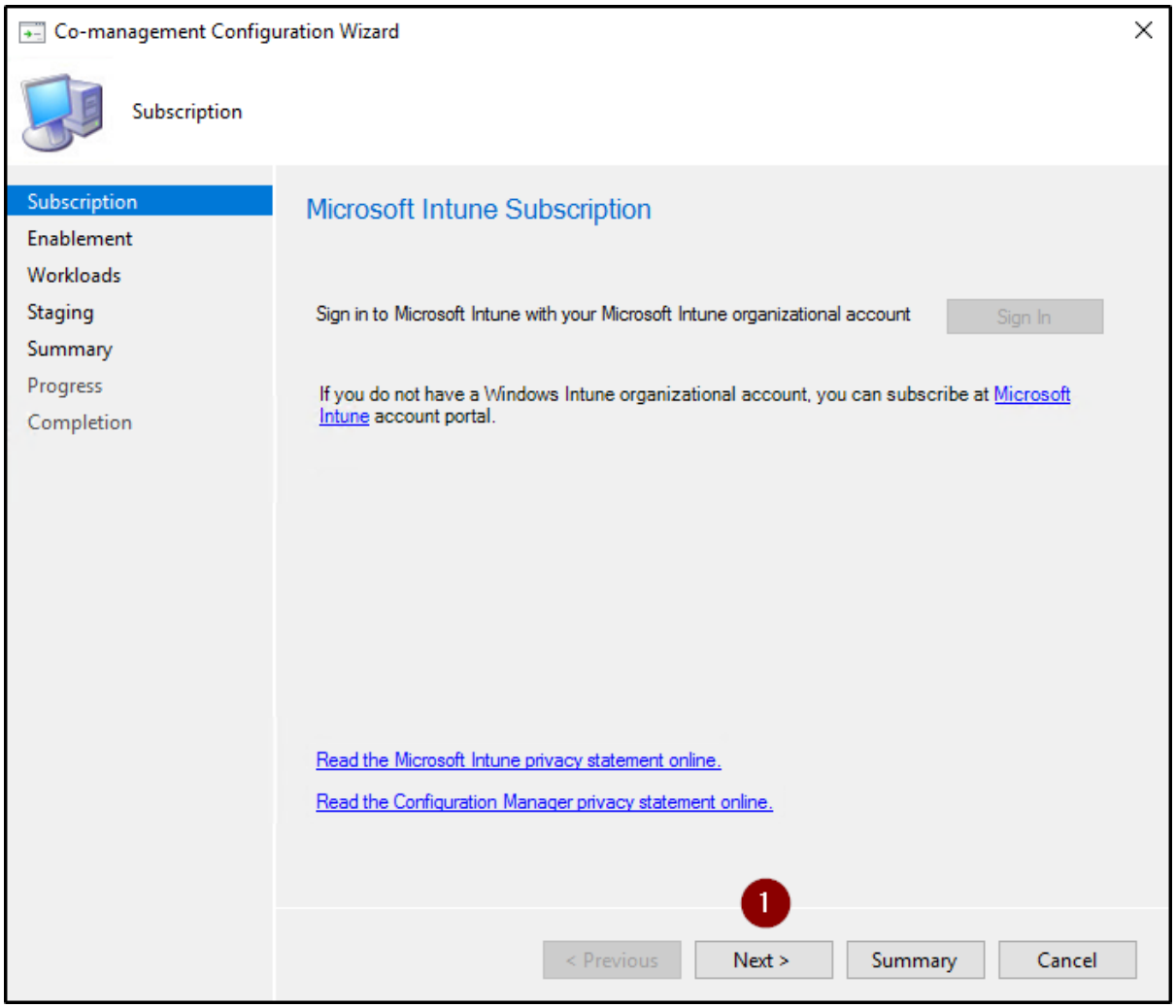
Figur 163: Slå på Co-Management

Skriver inn brukernavn og passord.



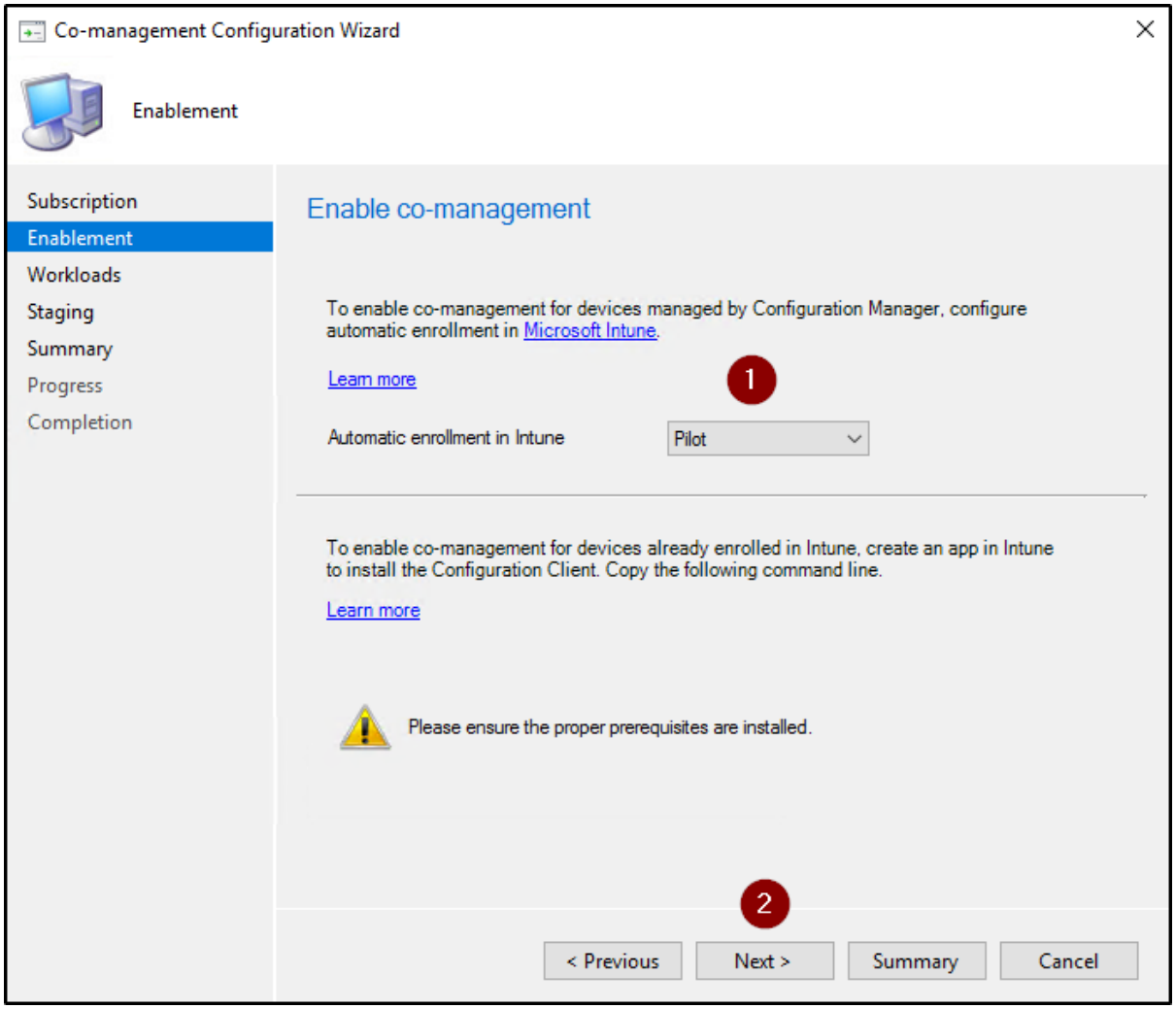
Figur 164: Slå på Co-Management

Når man har fått logget inn, trykker man på **Next**.



Figur 165: Slå på Co-Management

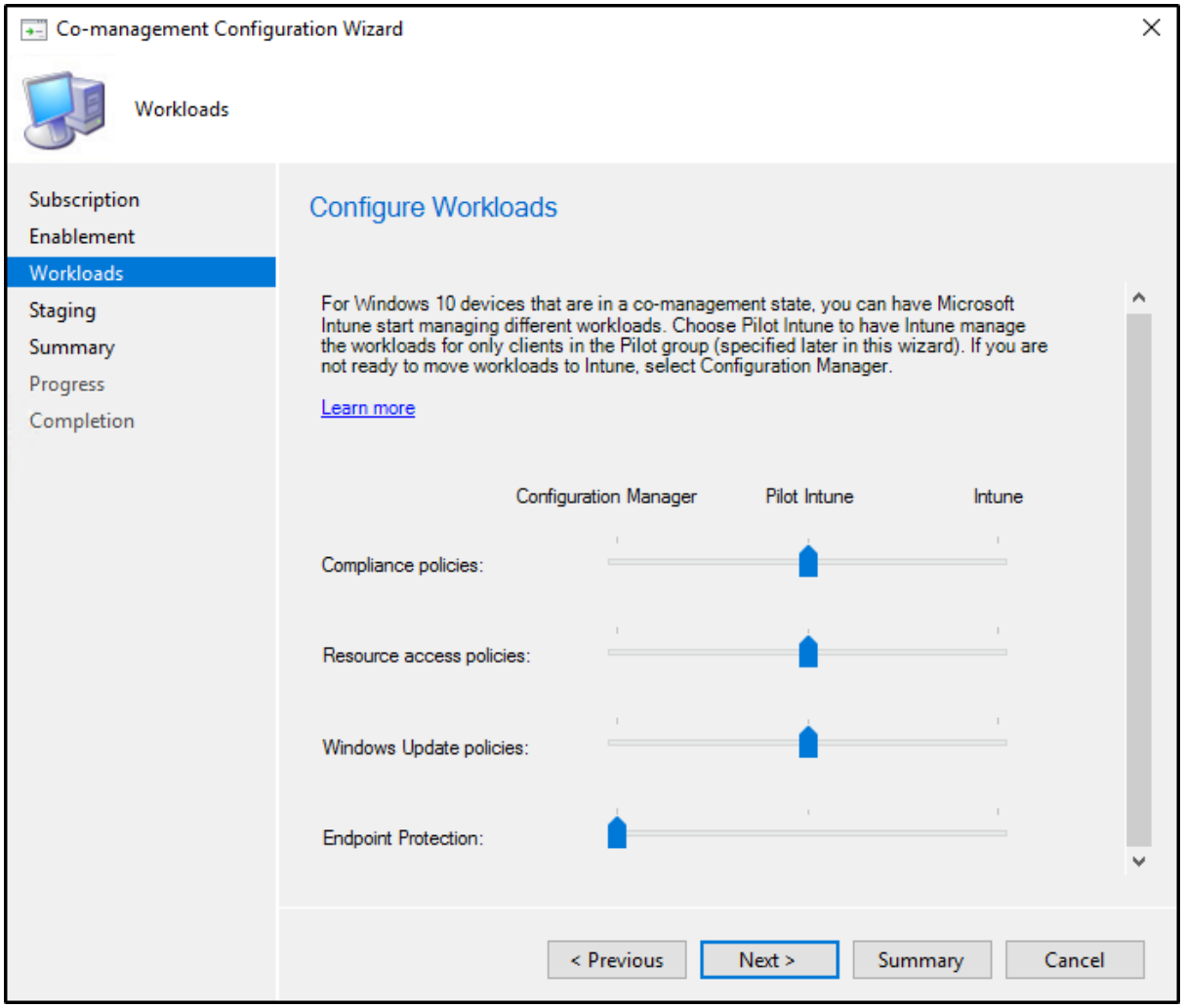
Under ***Enablement***, kan man velge om man ønsker å slå på automatisk enrollment til Intune for samtlige enheter eller for en pilot gruppe. I vårt tilfelle har vi valgt å sette den til Pilot, som vi ser nedenfor, men det vil egentlig ikke ha noe si, da vi senere under steget ***Staging***, setter *Pilot Collection* til *All Dektop and Server Clients*. Når dette er gjort, trykker vi **Next**.



Figur 166: Slå på Co-Management

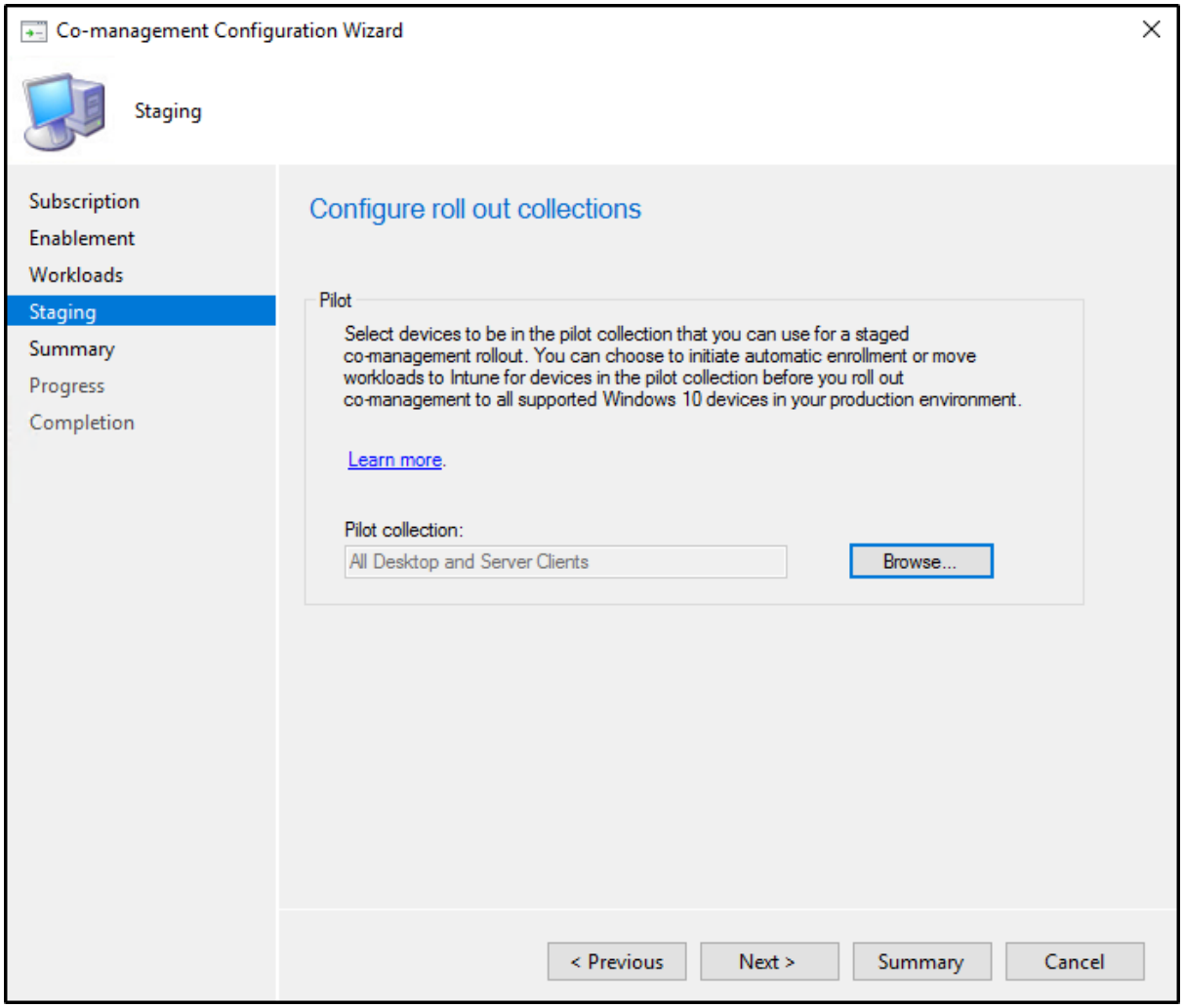
Nedenfor under ***Workloads***, ser vi forskjellige typer workloads som kan justeres. Nå er vi ikke nødt til å gjøre noen endringer her enda, men om man ønsker, kan man begynne å flytte over workloads som man selv ønsker og trykker **Next**.

NB: Skjermbildet nedenfor viser workloads som var tilgjenglig i versjon 1802 av SCCM. Når vi senere skal se mer på Worklaods, vil vi ha tilgang til flere workloads.



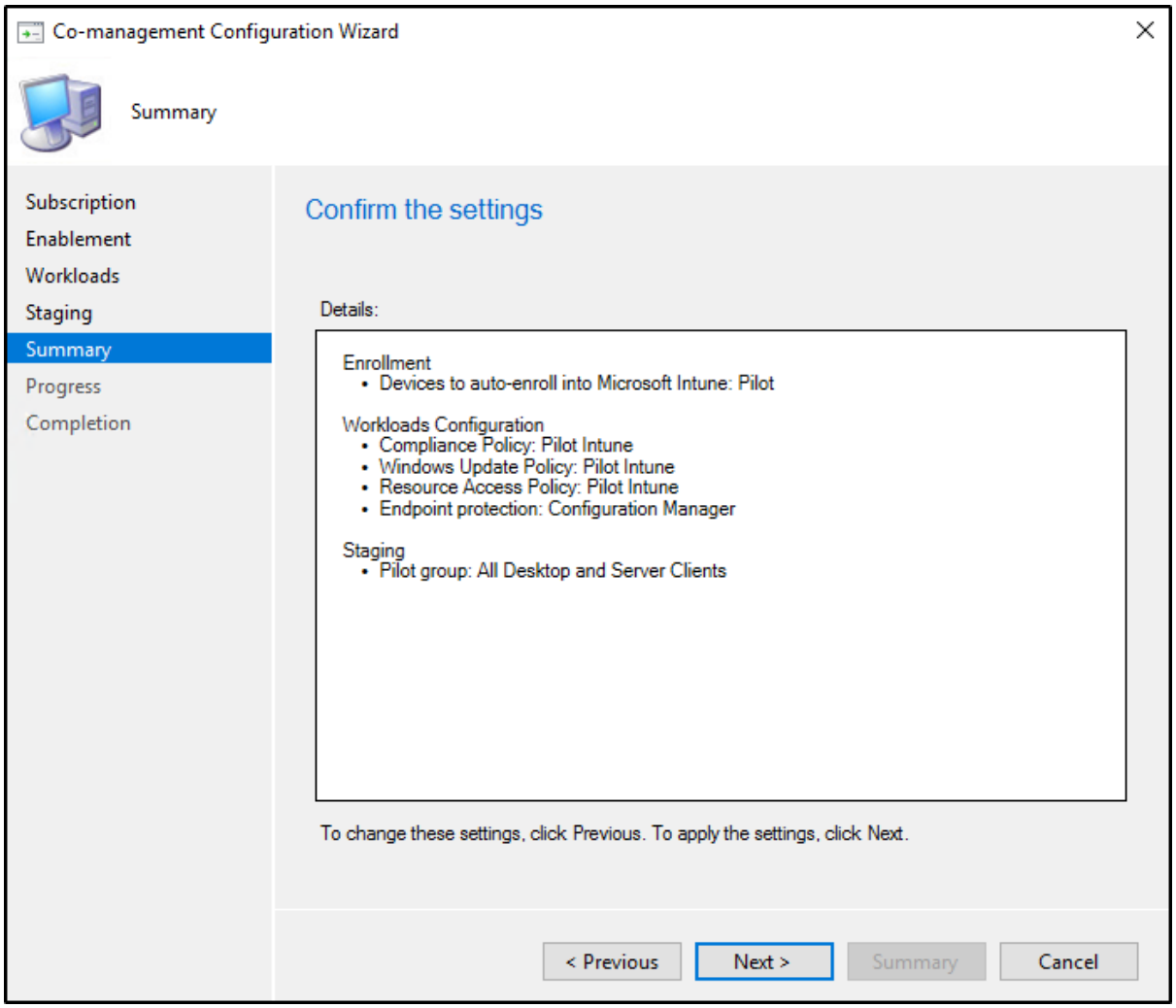
Figur 167: Slå på Co-Management

Nå er vi kommet til steget ***Staging***, som ble nevnt tidligere. Vi setter her *Pilot Collection*, til *All Dekstop and Server Clients* og trykker **Next**.



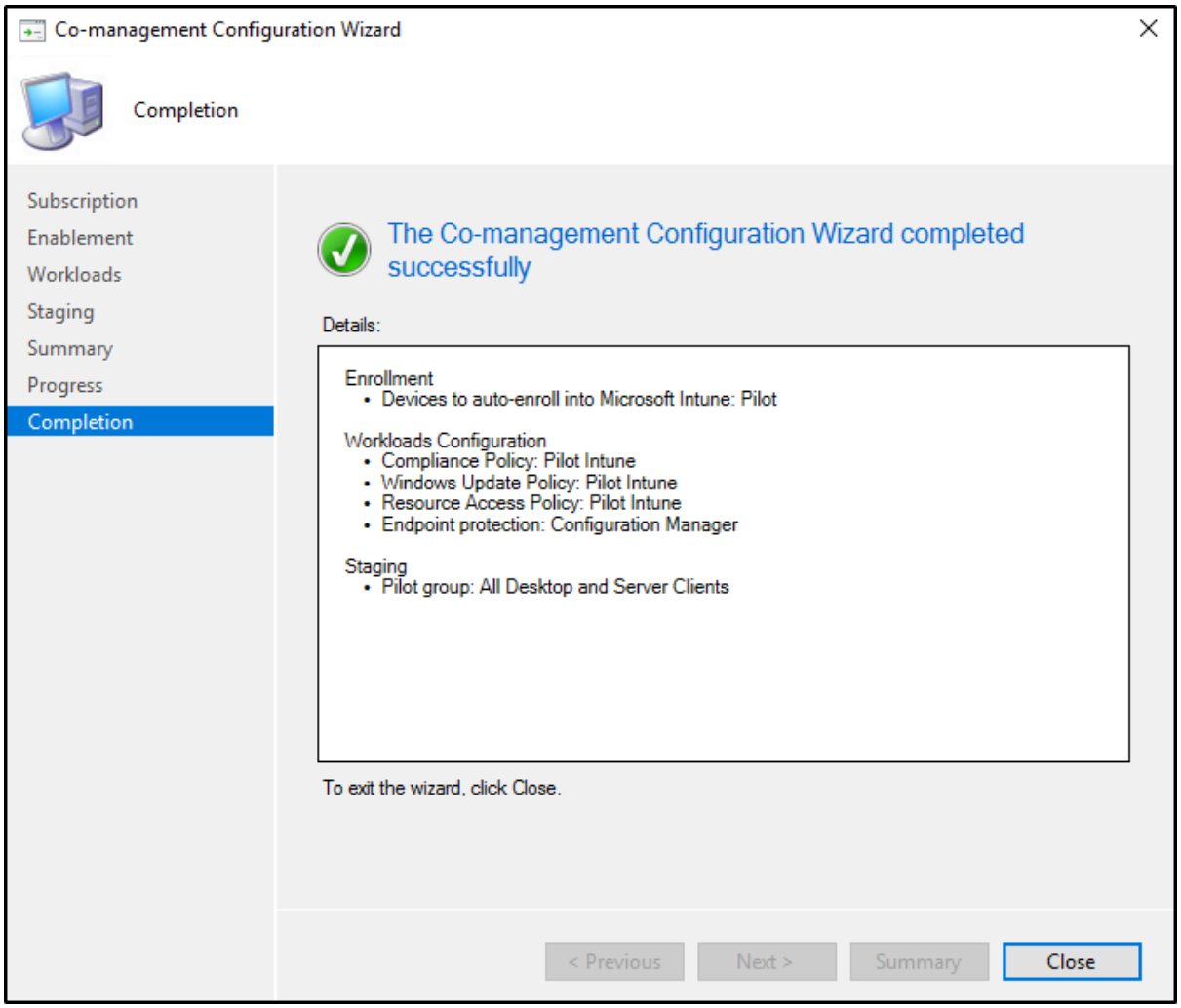
Figur 168: Slå på Co-Management

Ser over at alt stemmer og trykker **Next**.



Figur 169: Slå på Co-Management

Vi ser her at vi har konfigurasjonen av Co-Management har blitt gjennomført.

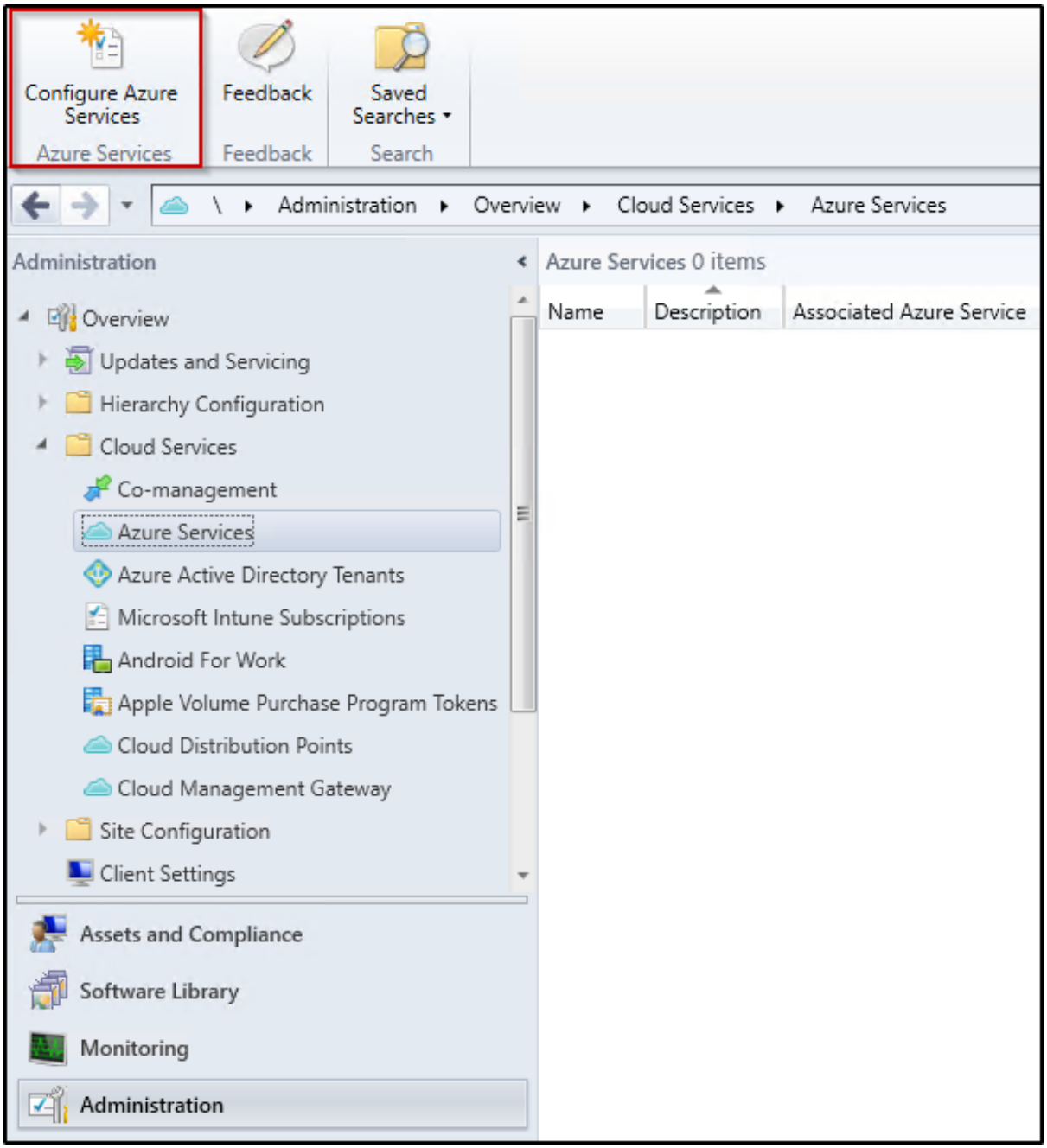


Figur 170: Slå på Co-Management

Konfigurere Azure Services

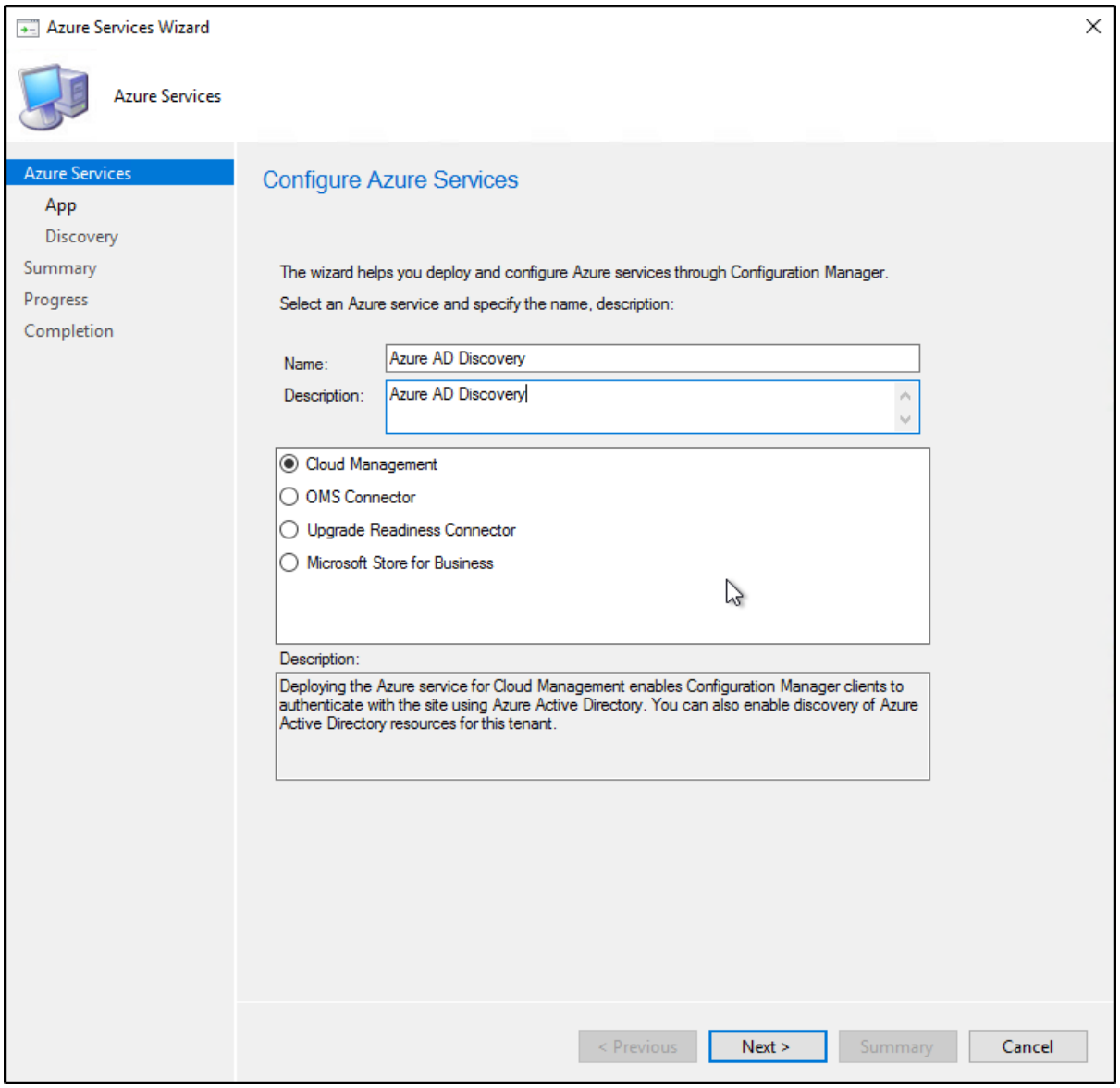
Tjenesten lar deg autentisere sites og brukere ved hjelp av Azure AD, og kan brukes for å installere Windows 10 med Azure AD autentifikasjon. Den vil også synkronisere data til Log analytics.

Vi setter opp tjenesten ved å navigere oss til ***Administration – Cloud Services – Azure Services,*** og trykker på **Configure Azure Services**.



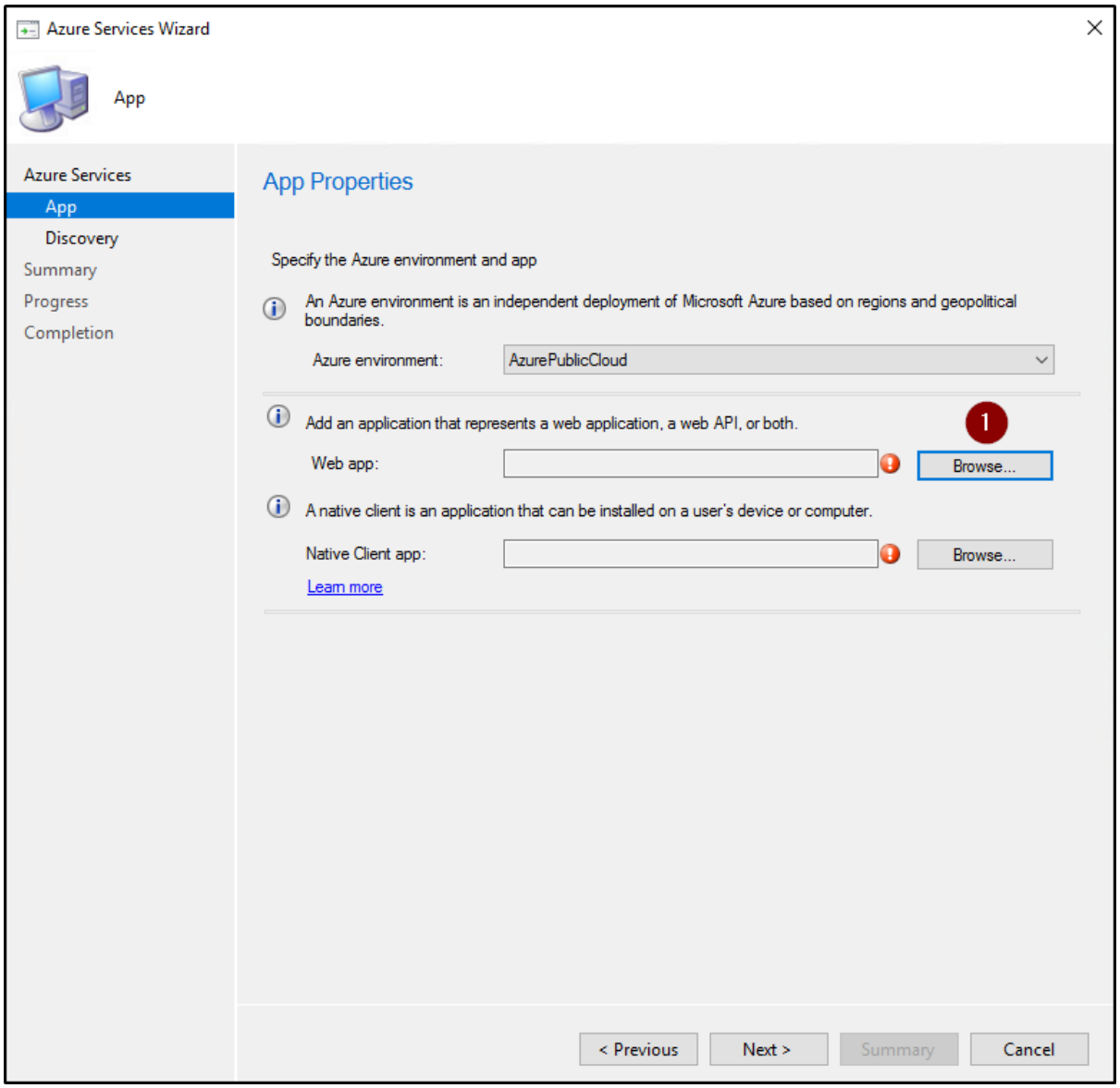
Figur 171: Konfigurere Azure Services

Vi legger til navn og beskrivelse og velger *Cloud Management* og trykker **Next**.



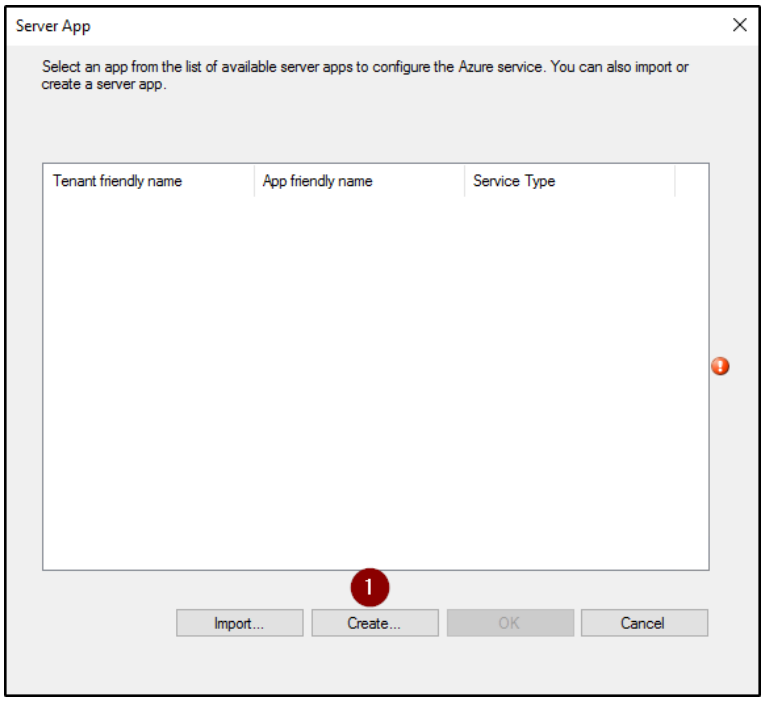
Figur 172: Konfigurere Azure Services

Under ***App***, velger vi *AzurePublicCloud* og trykker **Browse.**



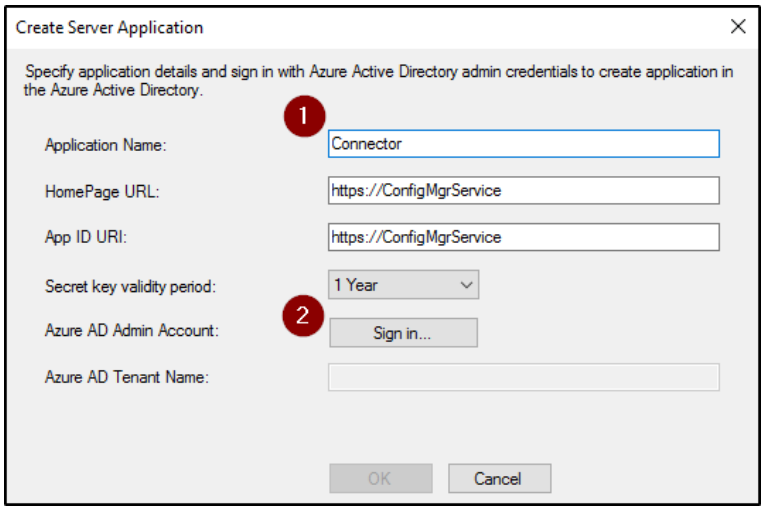
Figur 173: Konfigurere Azure Services

Velger **Create**.



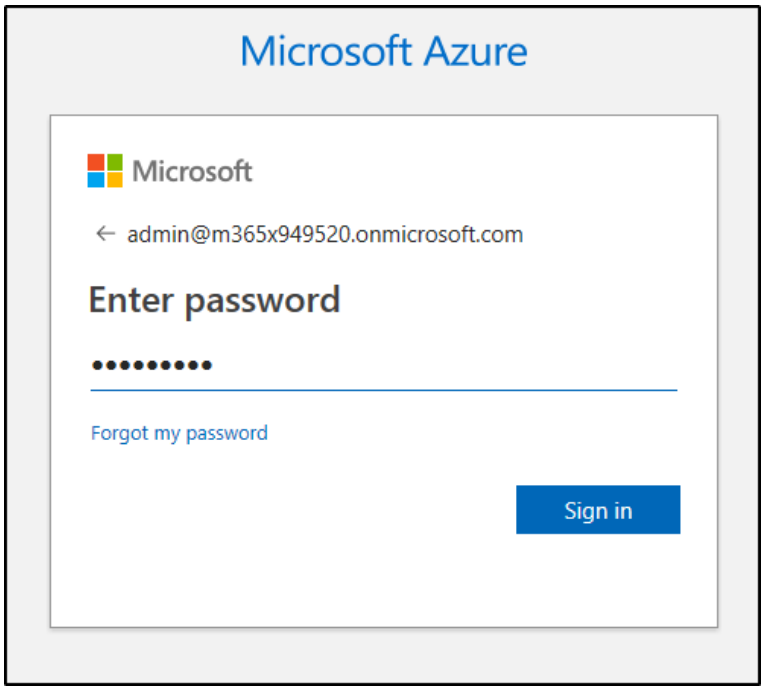
Figur 174: Konfigurere Azure Services

Legger til informasjon om applikasjonen og trykker **Sign in**.



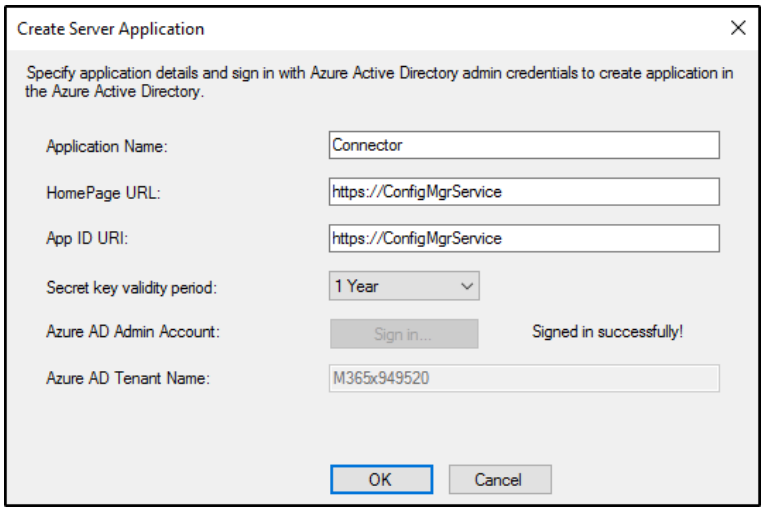
Figur 175: Konfigurere Azure Services

Logger inn med Azure tenant Administratorbruker.



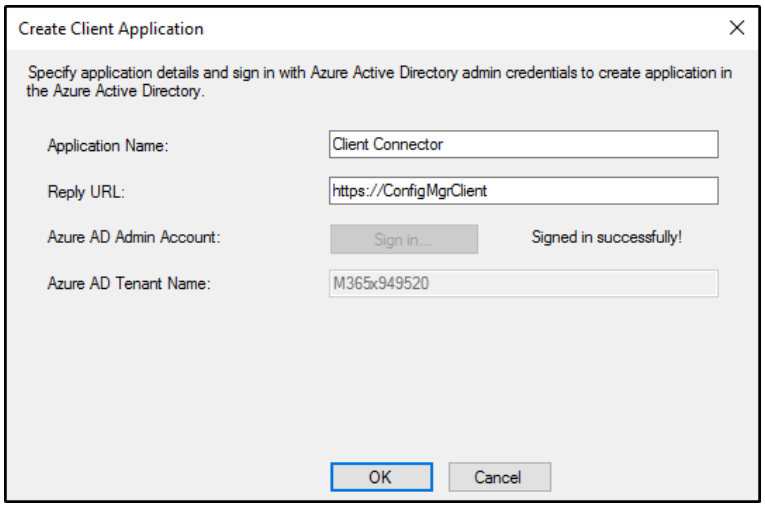
Figur 176: Konfigurere Azure Services

Trykker **OK.**



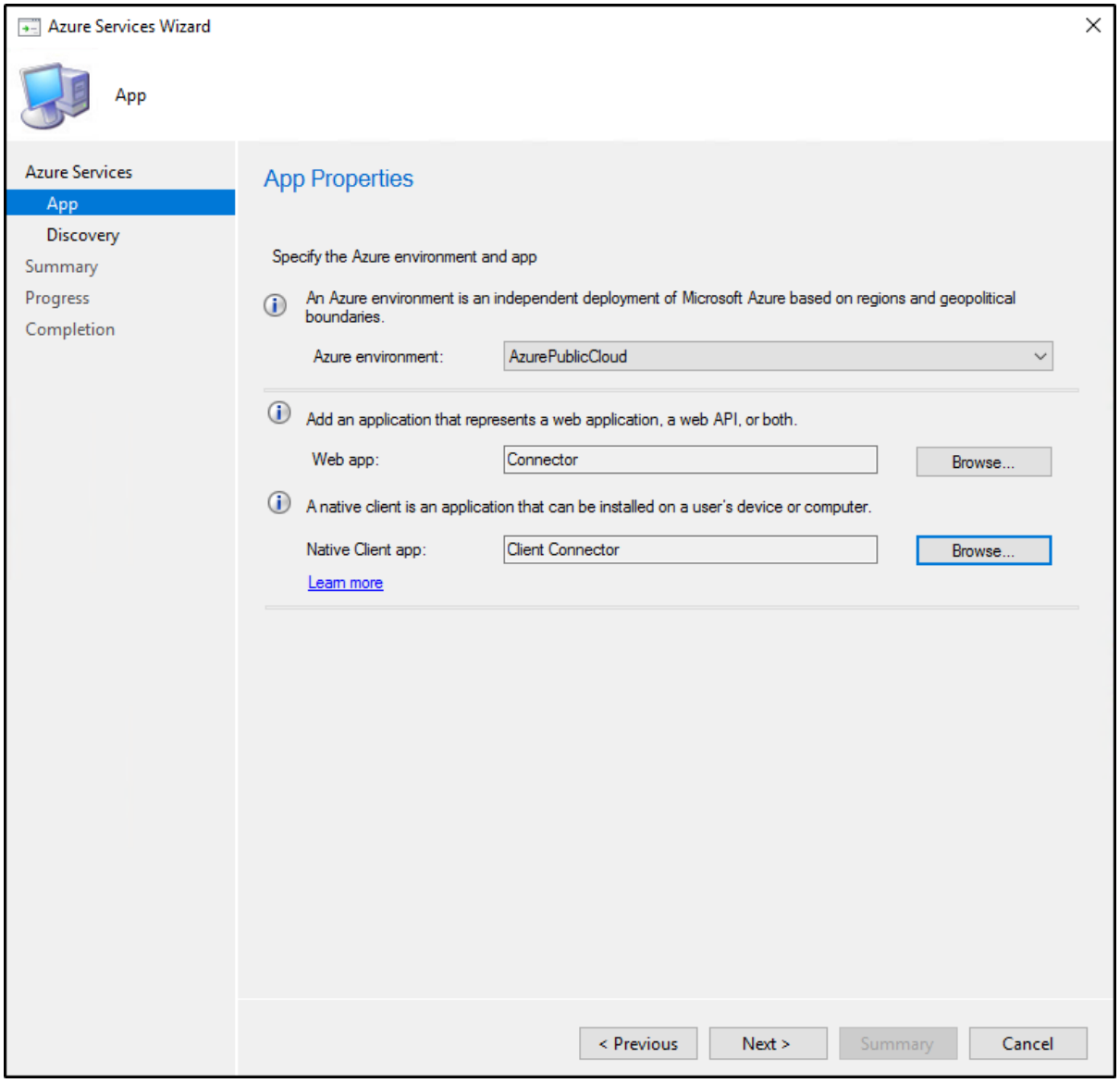
Figur 177: Konfigurere Azure Services

Lager også en native client.



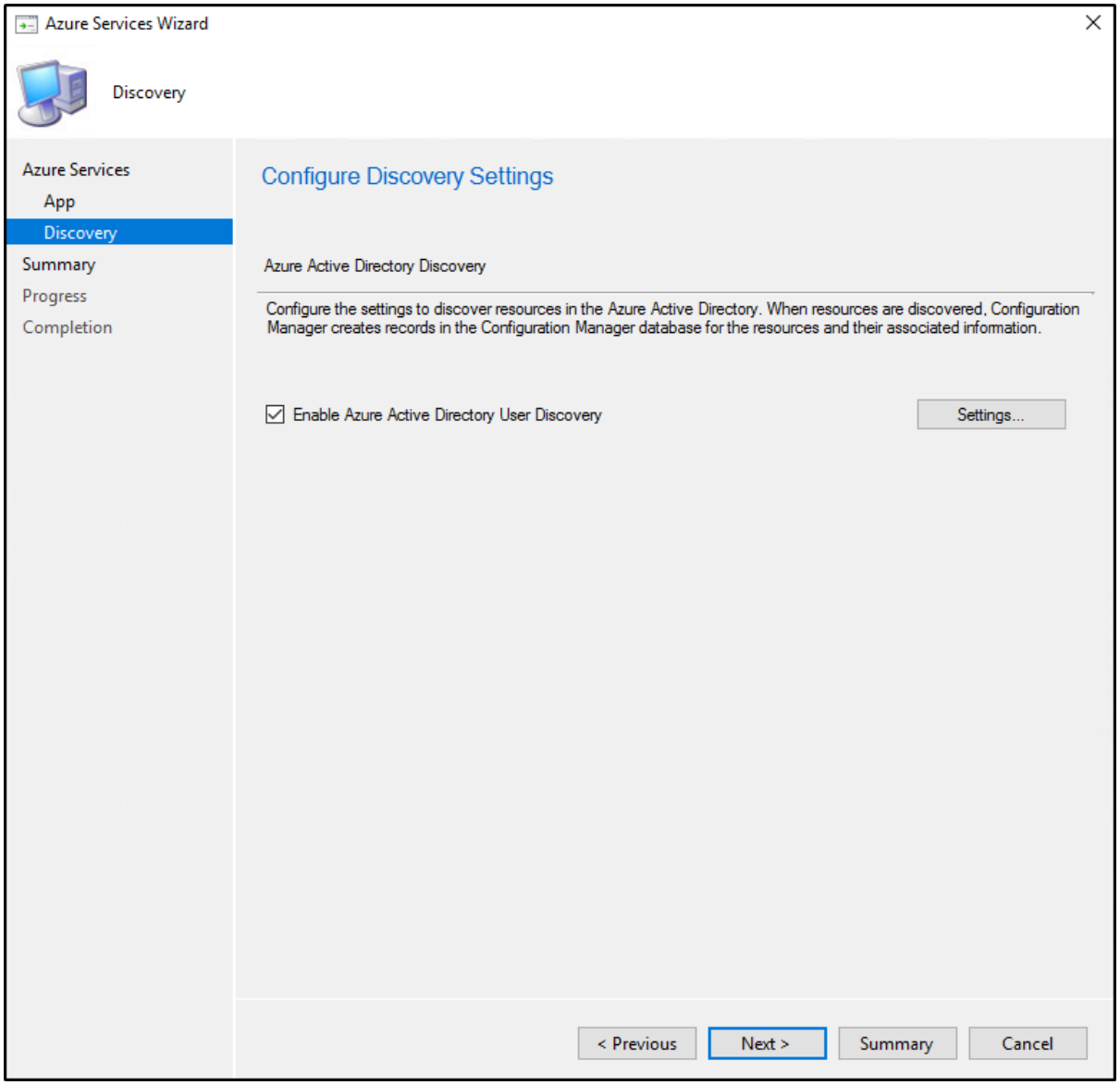
Figur 178: Konfigurere Azure Services

Når både web-applikasjonen og den native-klienten er opprettet går vi videre og trykker **Next**.



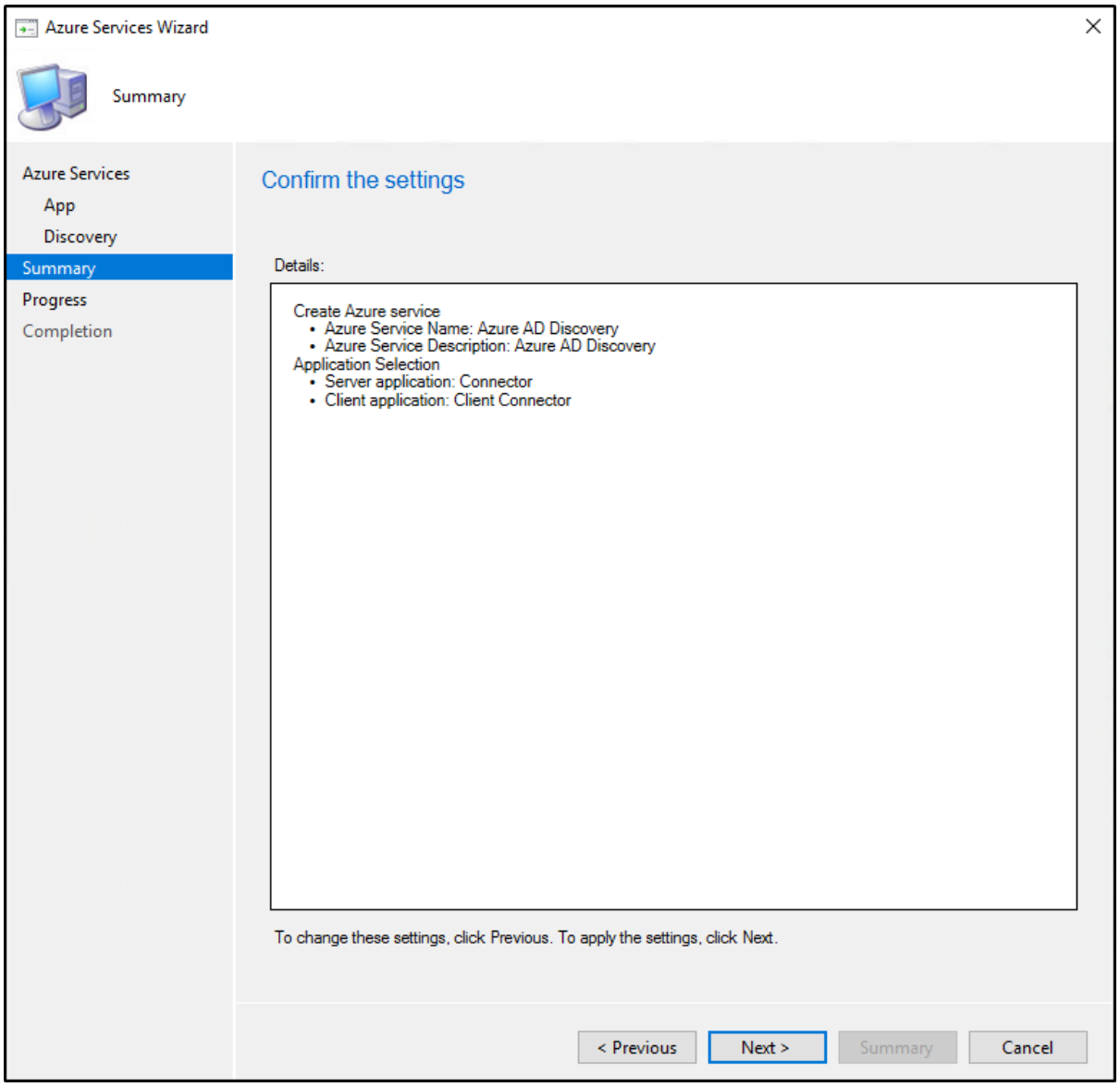
Figur 179: Konfigurere Azure Services

Under ***Discovery***, ser vi til at *Enable Azure Active Directory User Discovery* er huket av og trykker **Next**.



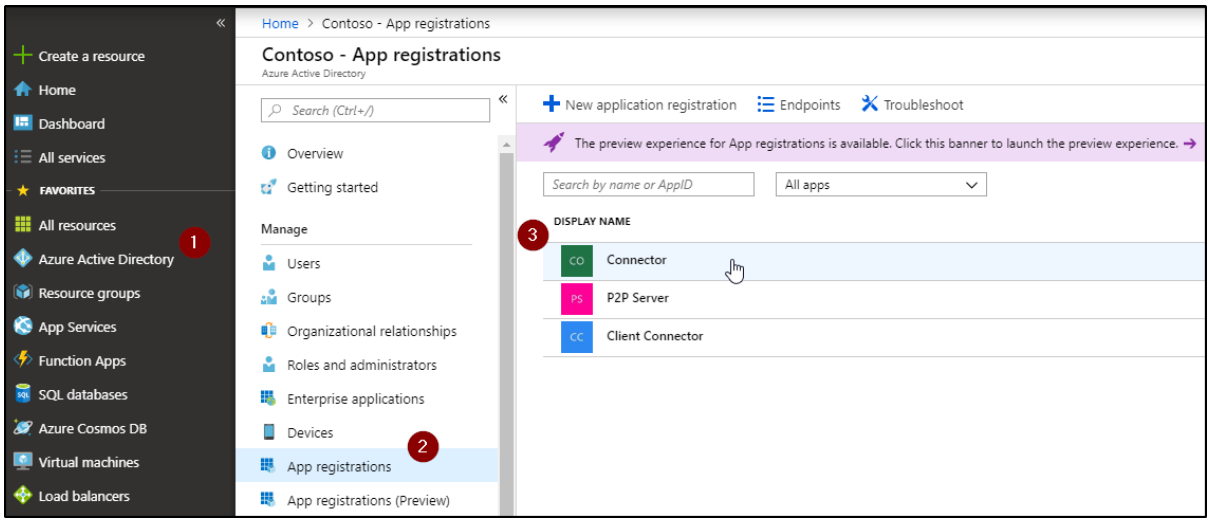
Figur 180: Konfigurere Azure Services

Ser over at alt er satt opp etter behov og trykker **Next**.



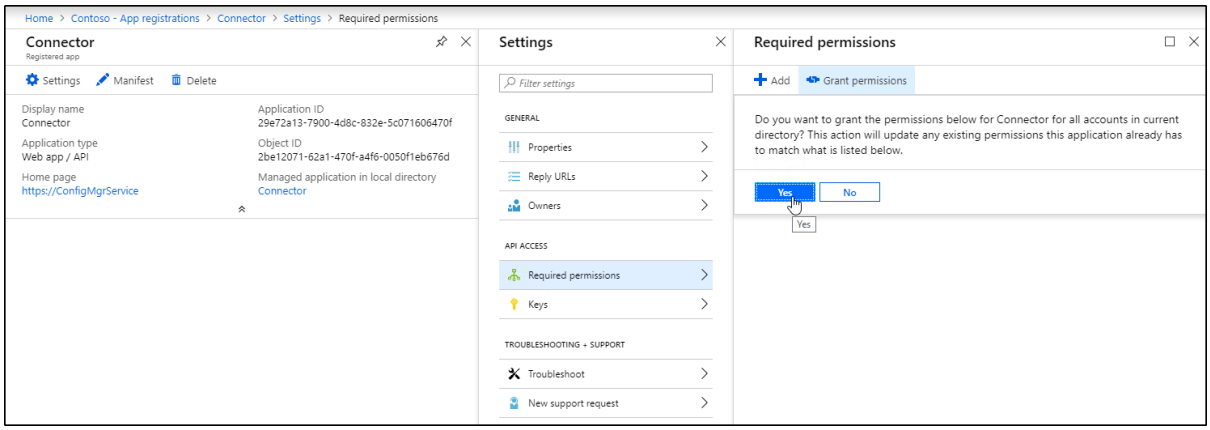
Figur 181: Konfigurere Azure Services

Vi må gi tilgang og rettigheter til applikasjonene vi har opprettet.



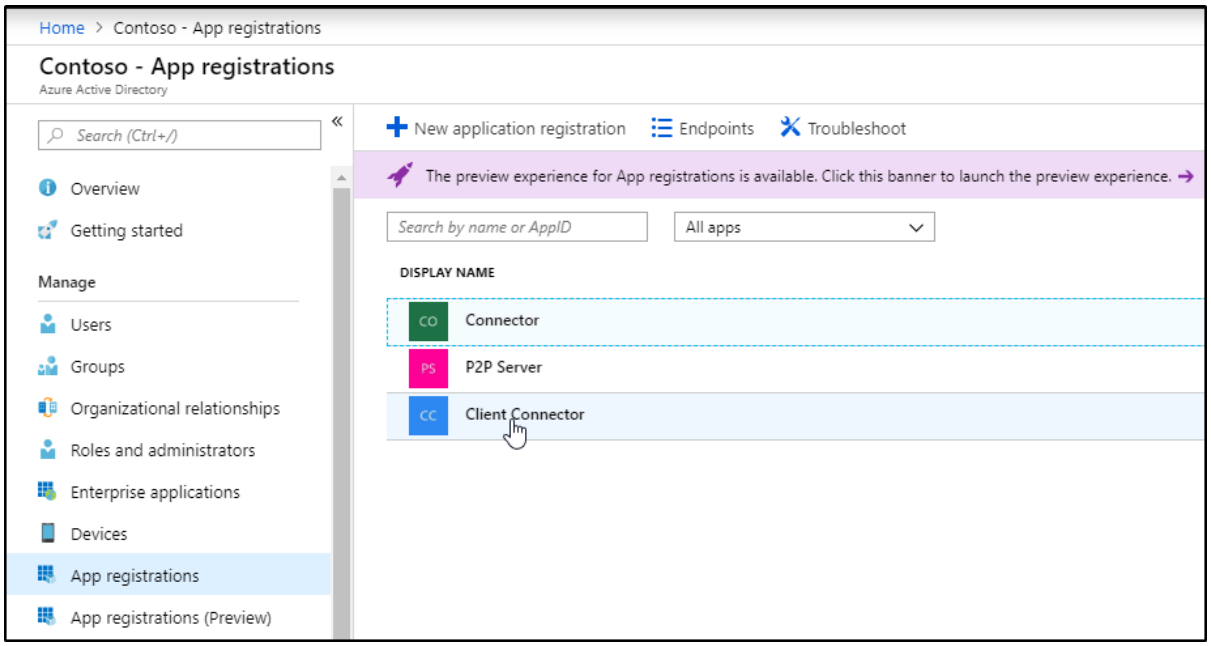
Figur 182: Konfigurere Azure Services

Navigerer oss til ***Required permissions***, og velger **Grant permissions**, og trykker **Yes**.

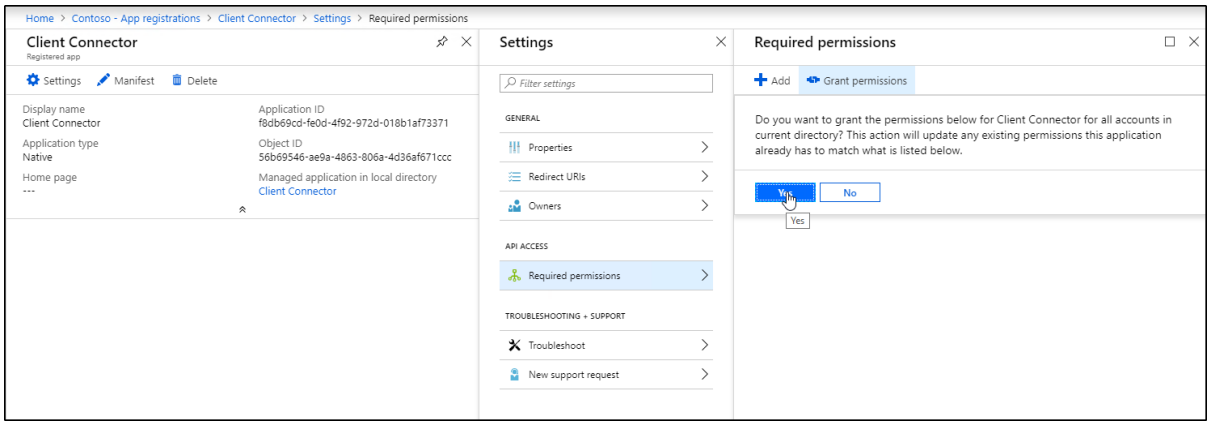


Figur 183: Konfigurere Azure Services

Gjør det samme for Client Connector.

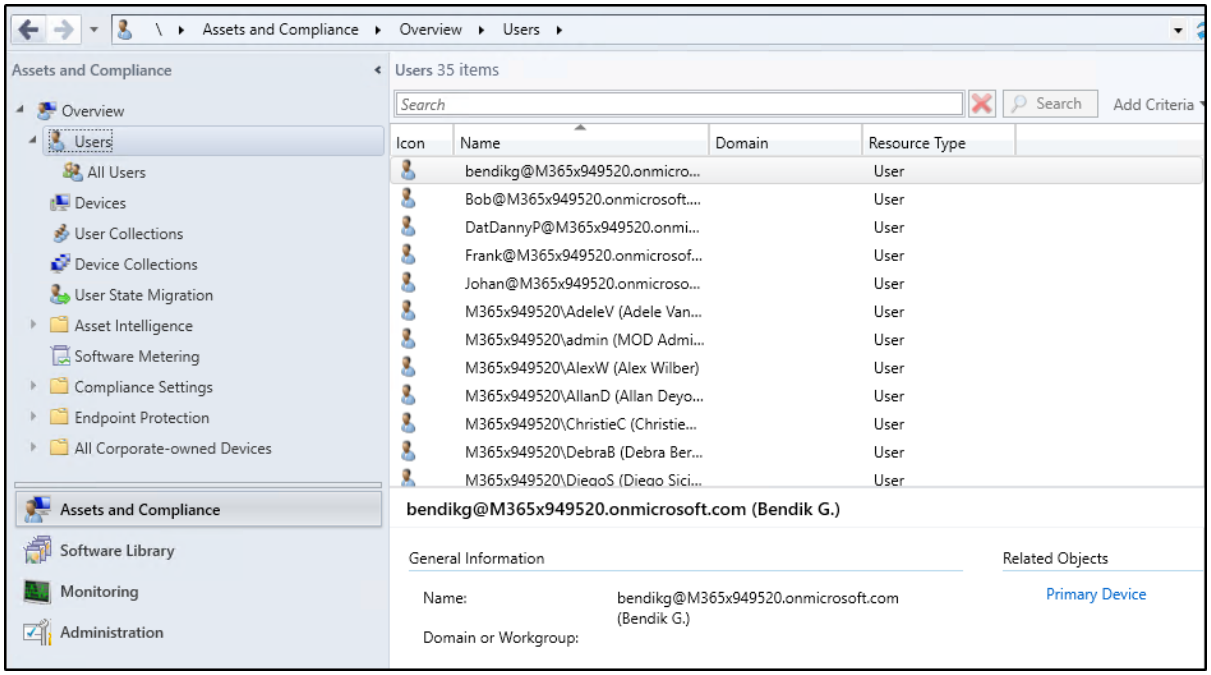


Figur 184: Konfigurere Azure Services



Figur 185: Konfigurere Azure Services

Etter noen minutter skal du kunne se brukerne fra både lokal AD og fra AAD på SCCM, som vist på bildet.



Figur 186: Konfigurere Azure Services

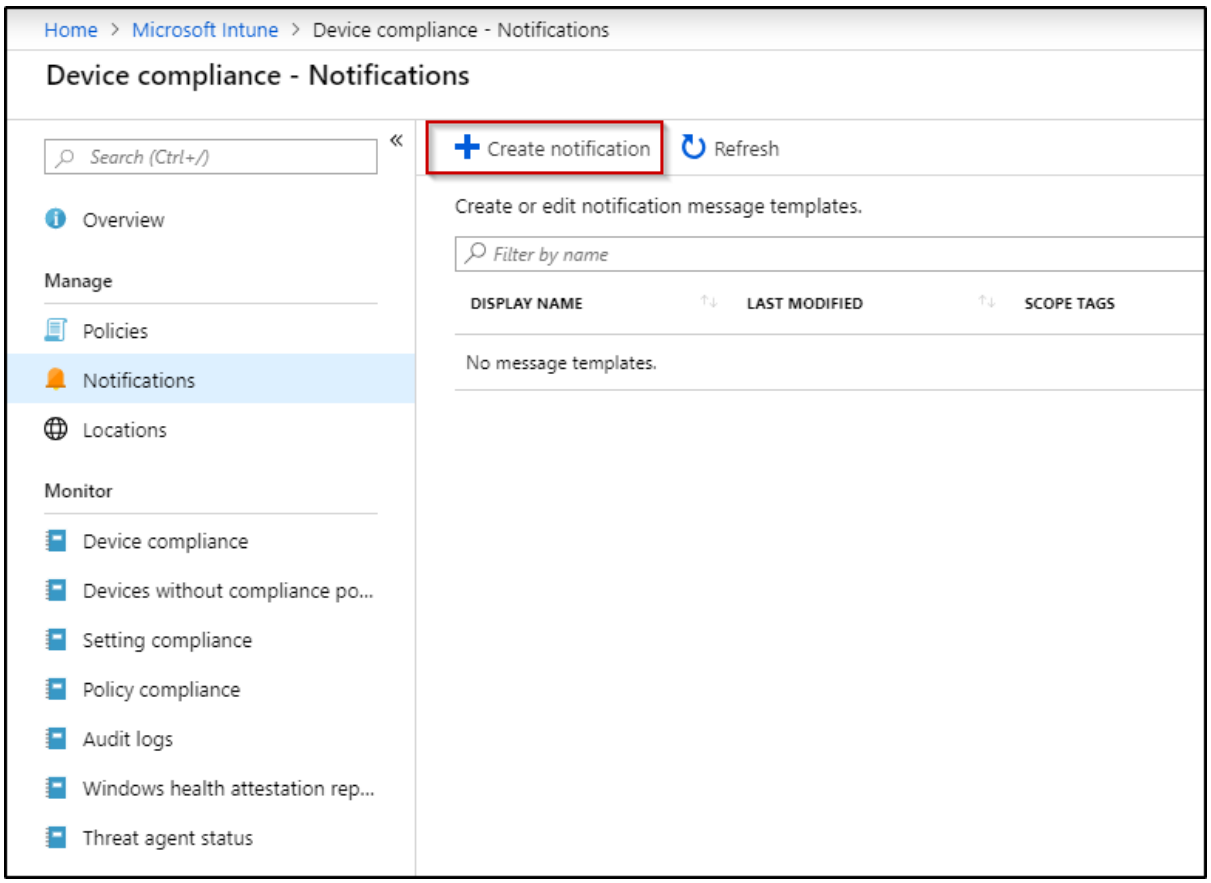
Workloads

Compliance Policies

Vi skal nå se på det som kalles for Compliance Policy. En slik policy beskriver visse krav som en bedrift stiller til sine ansattes enheter, for at enheten skal være "compliant", altså at de oppfyller kravene til sikkerhet o.l.

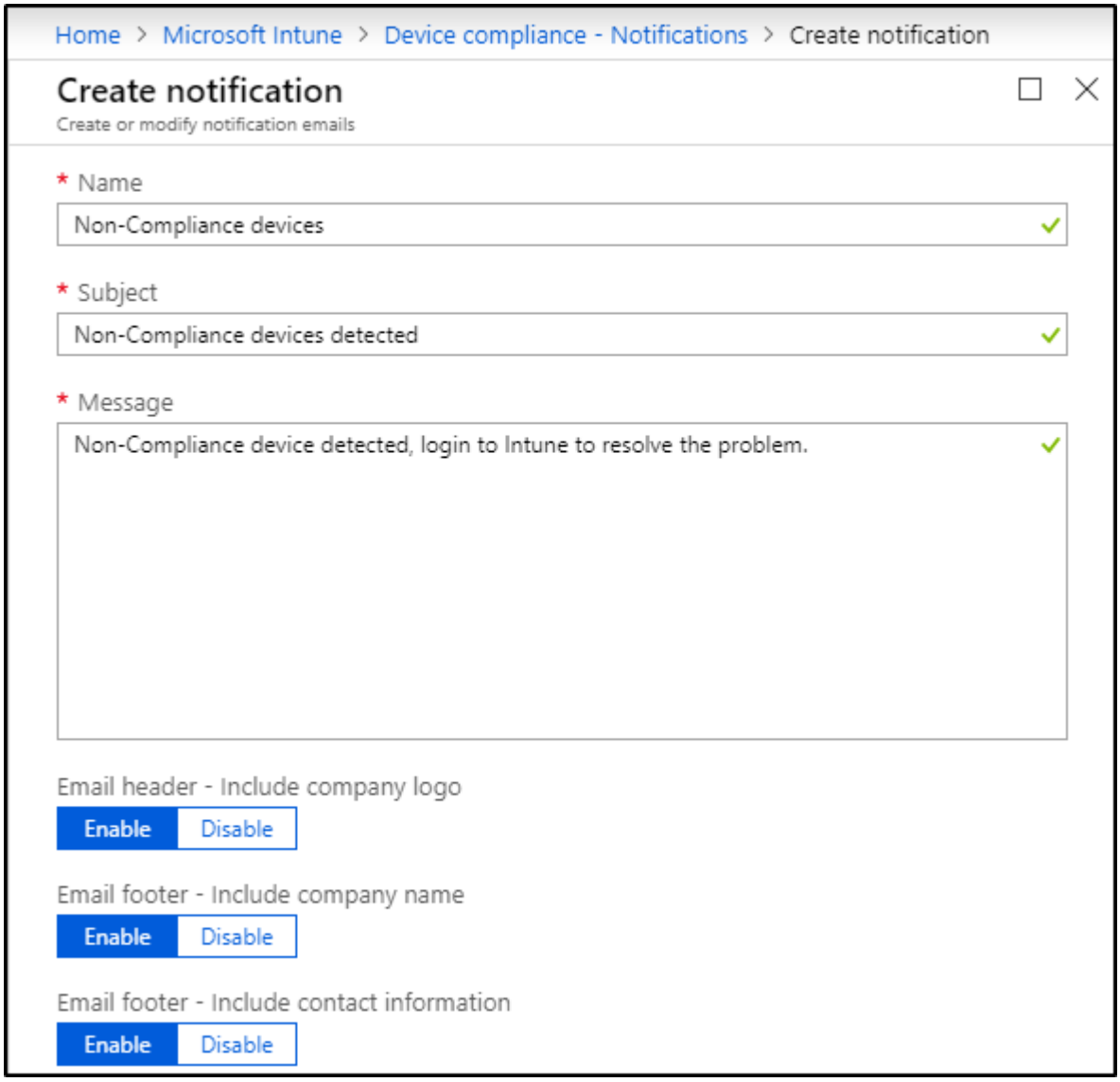
Vi starter med å navigere oss til ***Microsoft Intune – Device Compliance – Notification – Create Notification***. Her vil vi nå lage en email template som vi skal bruke når en policy merker at en enhet ikke oppfyller kravene som er satt.

Vi trykker på **Create notification**.



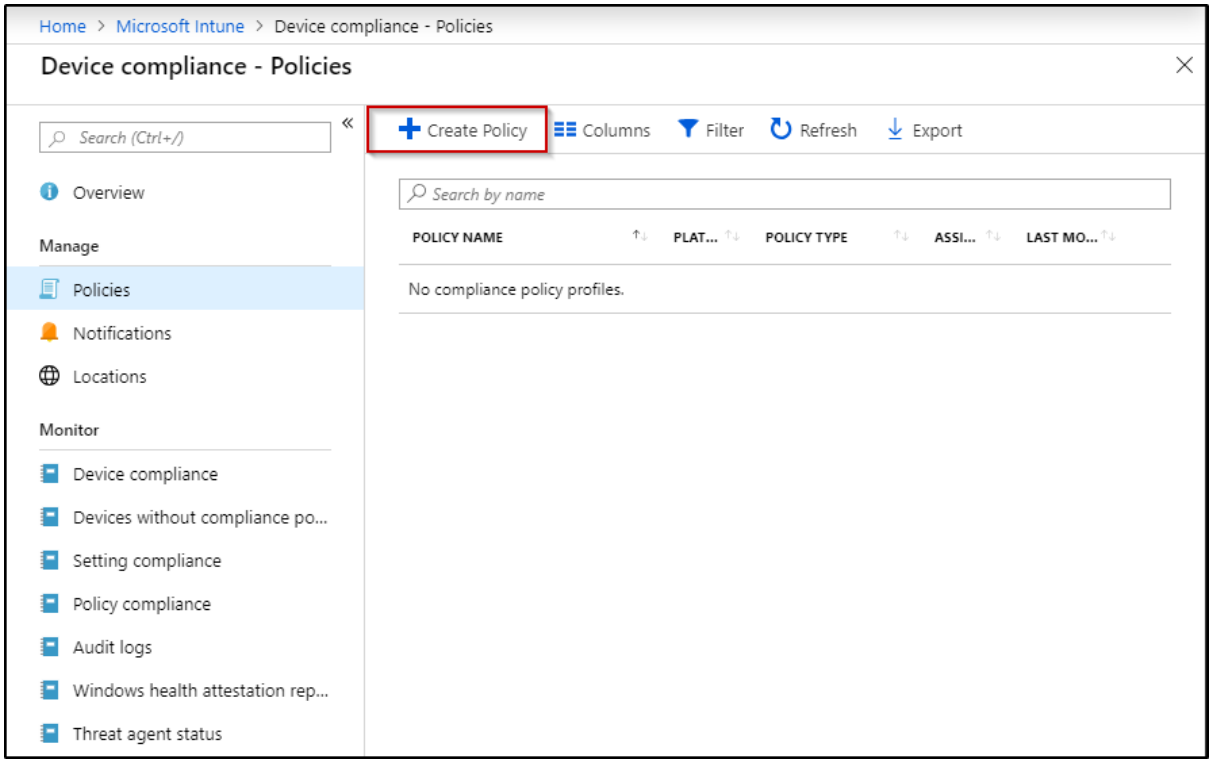
Figur 187: Workloads - Compliance Policy

Når vi oppretter email templaten, gir vi den et *Navn*, *Subject* og *Message*. Deretter trykker vi på **Create**.



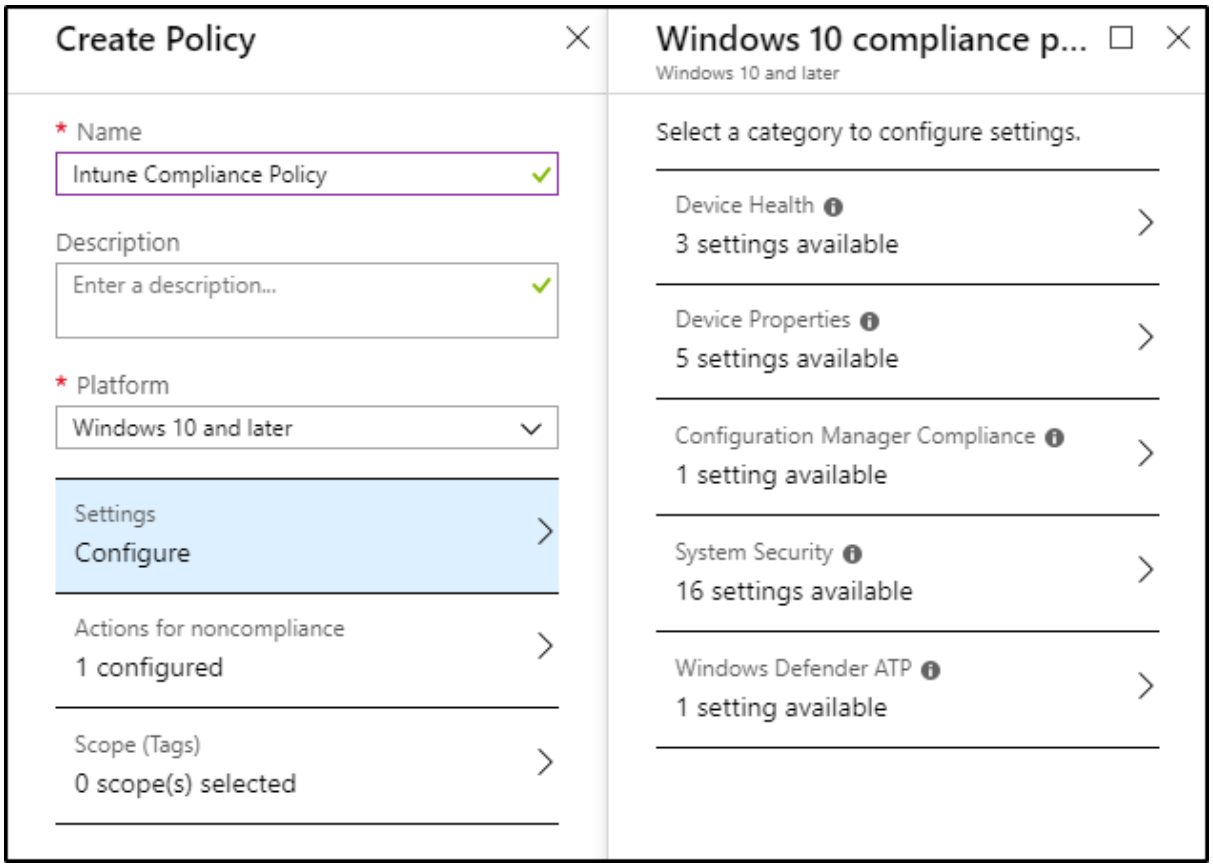
Figur 188: Workloads - Compliance Policy

Vi kan nå begynne å se på hvordan vi oppretter selve device compliance policy-en. Vi navigerer oss til ***Microsoft Intune – Device compliance – Policies***, og velger **Create Policy**.



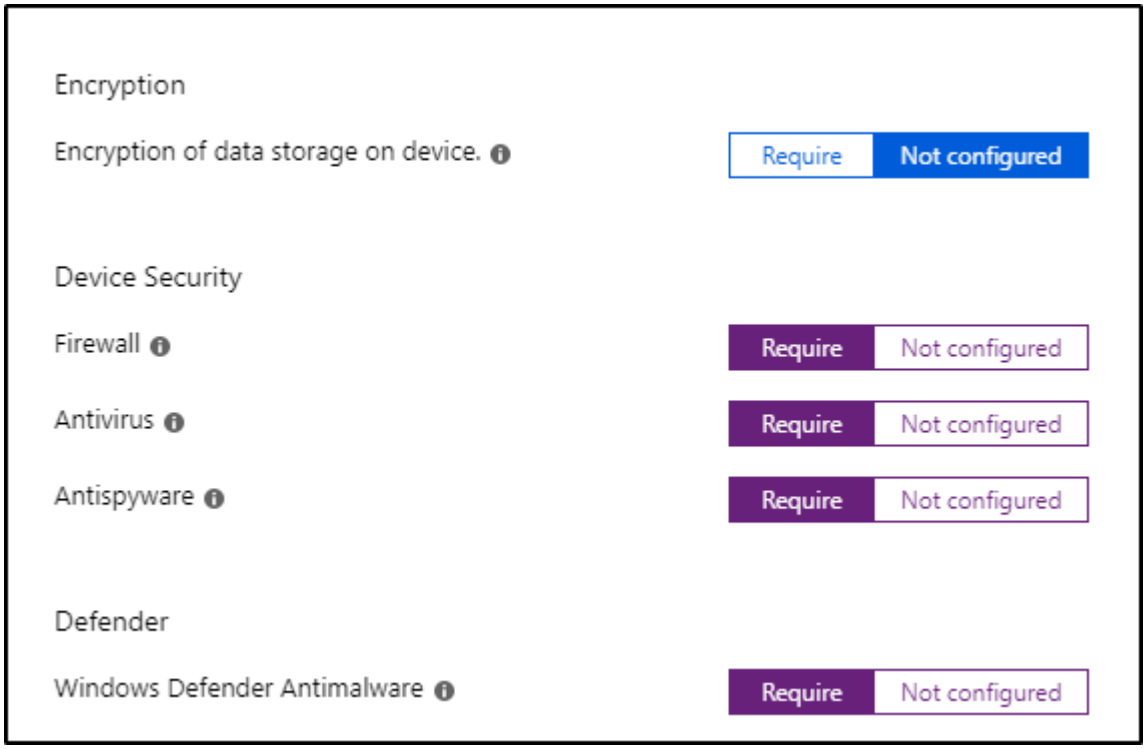
Figur 189: Workloads - Compliance Policy

I vårt tilfelle setter vi den til Windows 10 eller nyere versjoner. For akkurat dette eksempelet skal vi nå demonstrere en policy som ser til at maskinene har firewall, antivirus og Antispyware & Defender. Vi velger derfor ***Configure – System Security***.



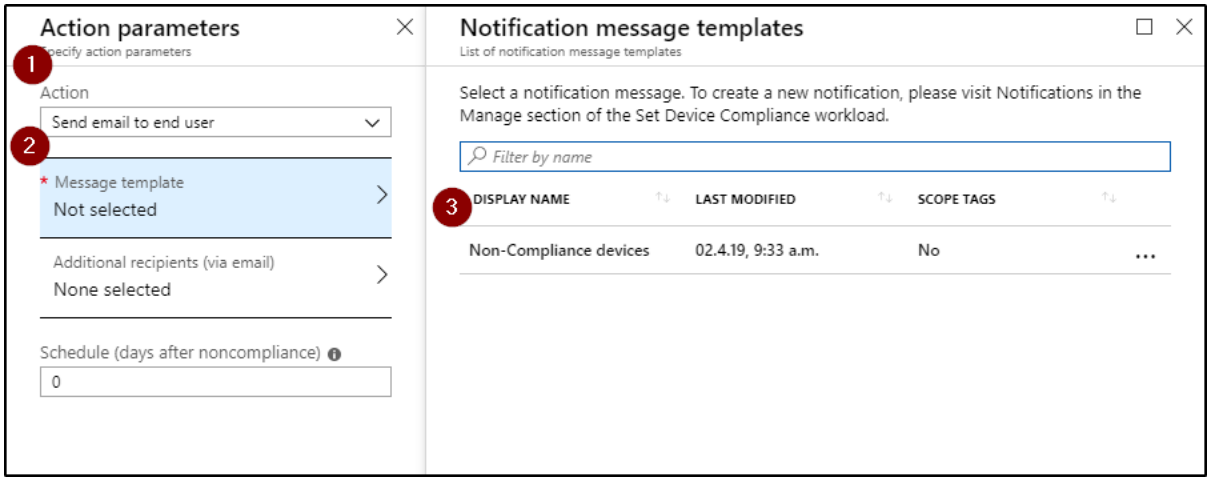
Figur 190: Workload - Compliance Policy

Vi velger her at **Firewall, Antivirus**, **Antispyware** og **Windows Defender Antimalware**, skal eksistere på enheten for at den skal bli compliant. Deretter trykker vi **OK**, for å fortsette.



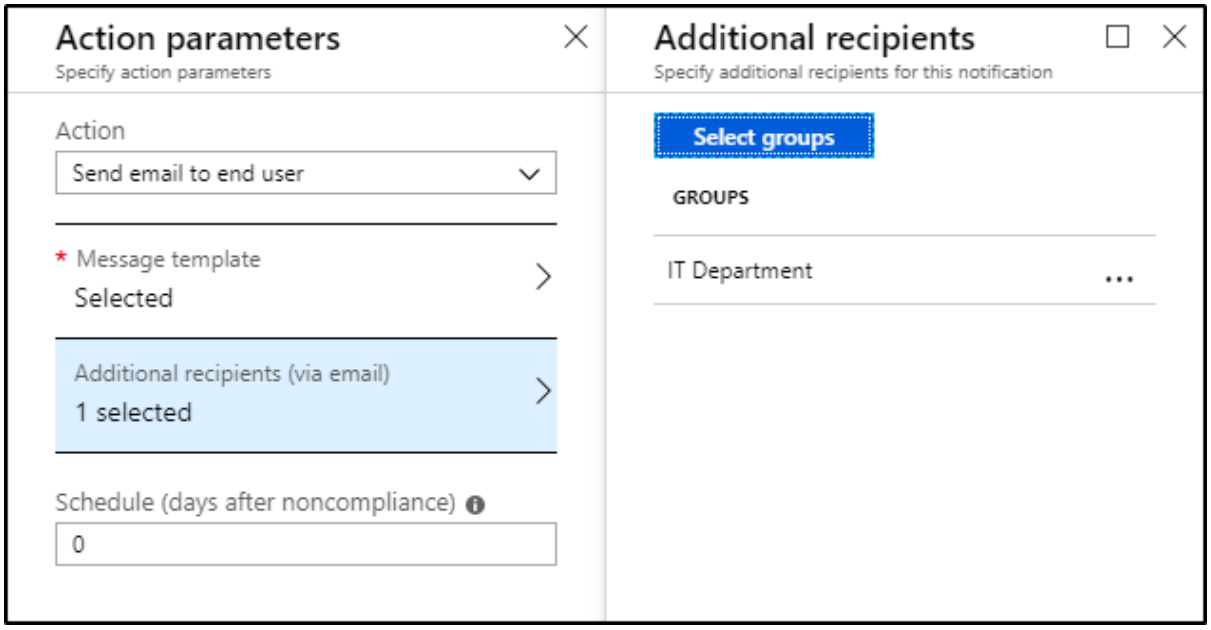
Figur 191: Workloads - Compliance Policy

Vi skal nå ta i bruk email templaten som vi har laget tidligere. Vi navigerer oss først til ***Create Policy – Actions for noncompliance***. Deretter velger vi **Send email to end user** (1), som vist nedenfor, trykker **Message template** (2), og velger templaten som vi lagde tidligere (3). Trykker deretter **Select** + **Add** + **OK** + **Create**, for å avslutte. Dette vil sende en beskjed til eieren av enheten dersom en enhet ikke er compliant.



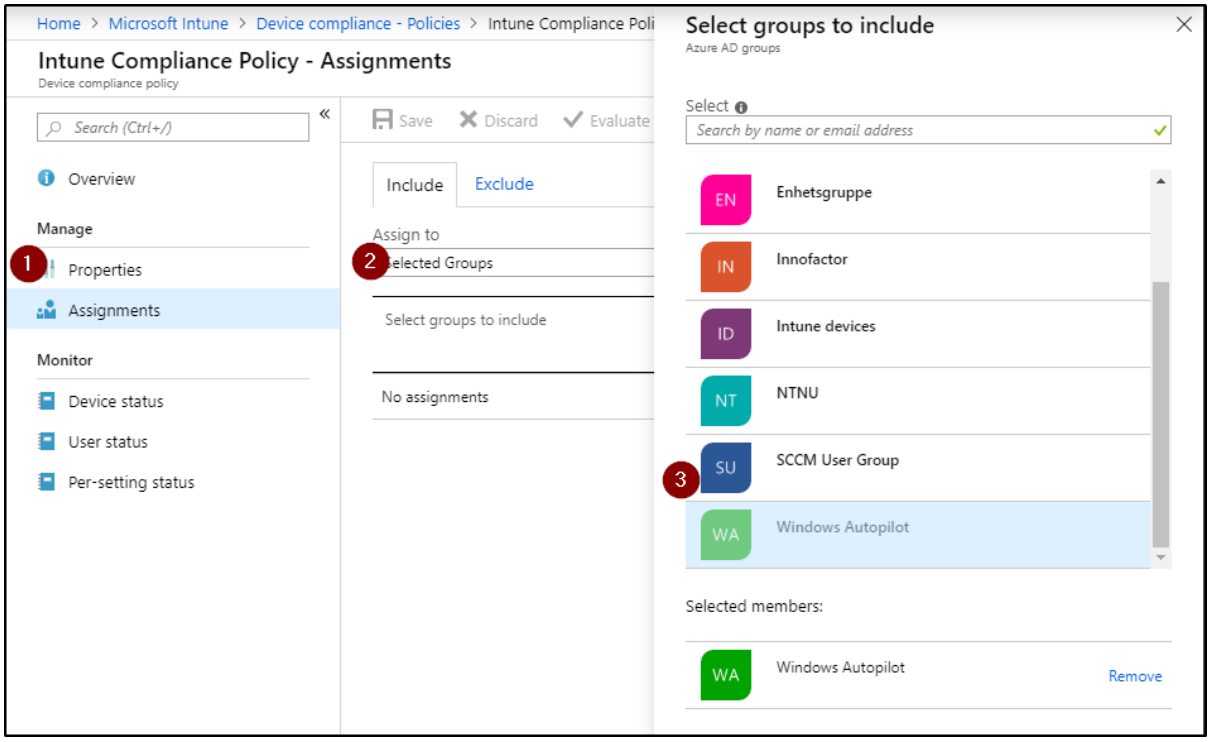
Figur 192: Workloads - Compliance Policy

Vi vil også lage en tilsvarende «Action» som sendes til IT-Avdelingen, slik at de blir varslet om problemet.



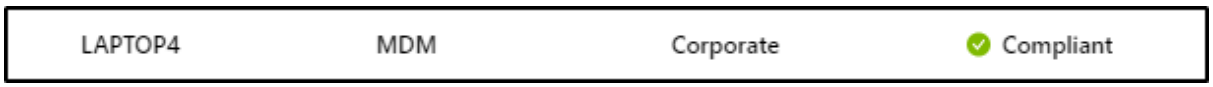
Figur 193: Workloads - Compliance Policy

Når Device Compliance Policy-en er laget, skal vi nå tildele den til en gruppe med enheter som vi ønsker at skal ha denne policy-en. Vi navigerer oss til ***Microsoft Intune – Device compliance – Policies***. Velger Policy-en som vi nettopp lagde og trykker på **Assignments**. Deretter trykker vi på **Select group to include** og legger til ønsket gruppe og trykker deretter på **Save**.



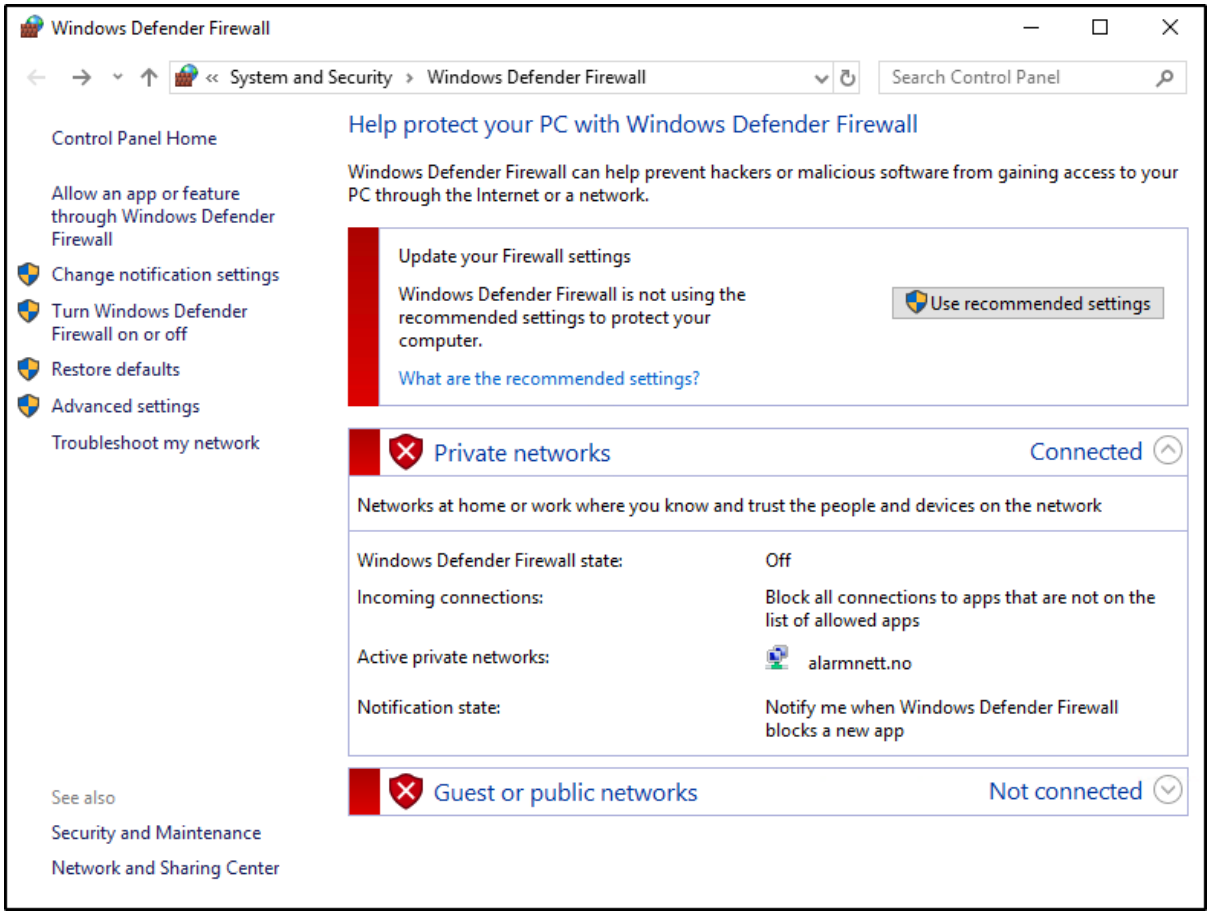
Figur 194: Workloads - Compliance Policy

Som vi ser på skjermbildet nedenfor, er enheten satt til Compliant. Vi vil nå teste ved å slå av brannmuren på enheten og se om enheten blir satt til Non-Compliant, samt sjekke at admin blir tilsendt en e-post om dette.



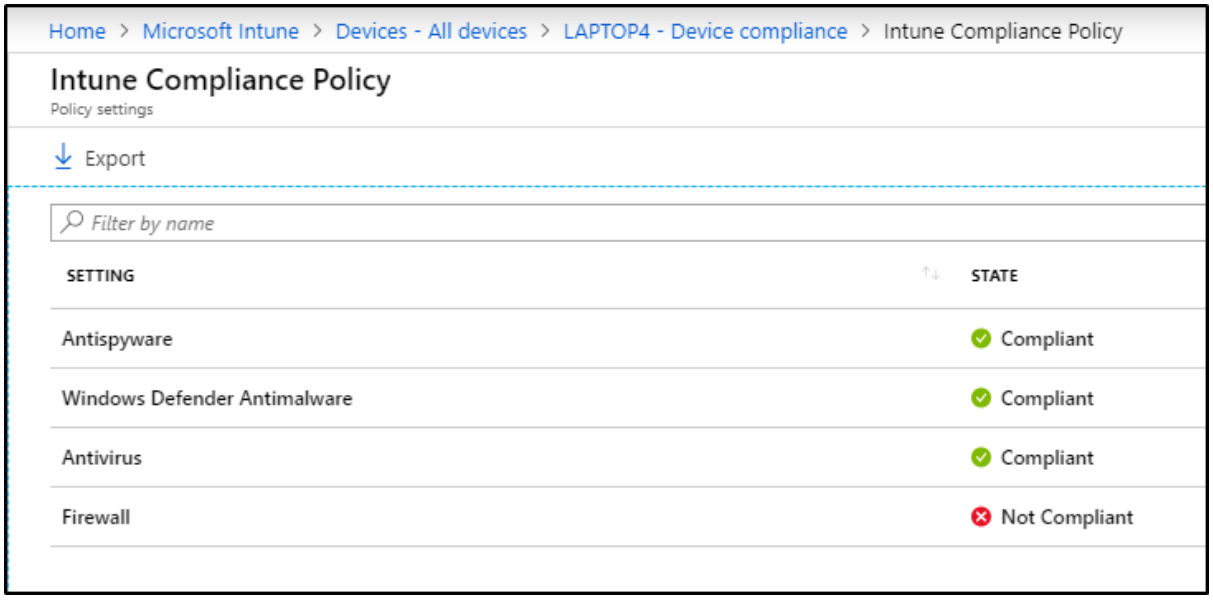
Figur 195: Workloads - Compliance Policy

Som vi ser har vi nå slått av brannmuren på enheten, som tidligere testet som Compliant. Vi venter litt og ser om dette endrer seg.



Figur 196: Workloads - Compliance Policy

Hvis vi navigerer oss til ***Devices – laptop4*** (Maskinen som vi testet på) **– *Device Compliance***. Vil vi nå se at Compliance er satt til Non-Compliant. Vi ser også at det skyldes **Firewall**.

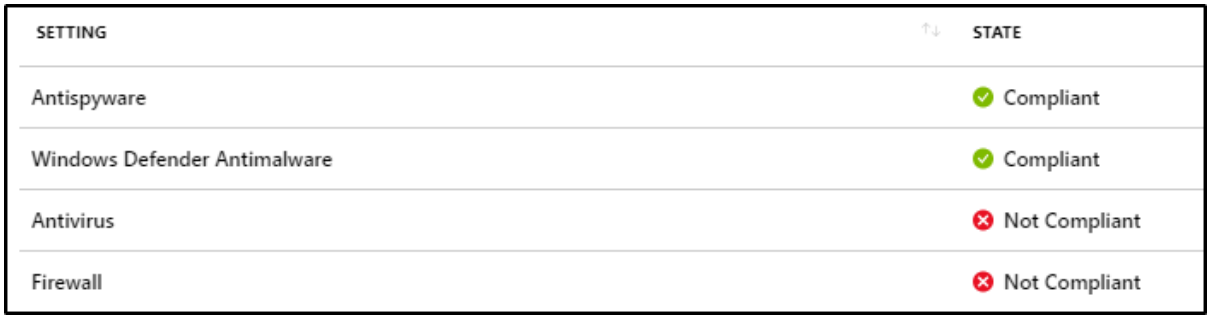


Figur 197: Workloads - Compliance Policy

I og med at vi har flyttet Device Compliance workloaden til Intune, vil Device Compliance i Intune også gjelde for co-managed enheter. Vi kan vi se at hvis vi tildeler en Compliance Policy til co-managed device gruppen, vil man også bli varslet dersom disse enhetene skulle bli Not Compliant.

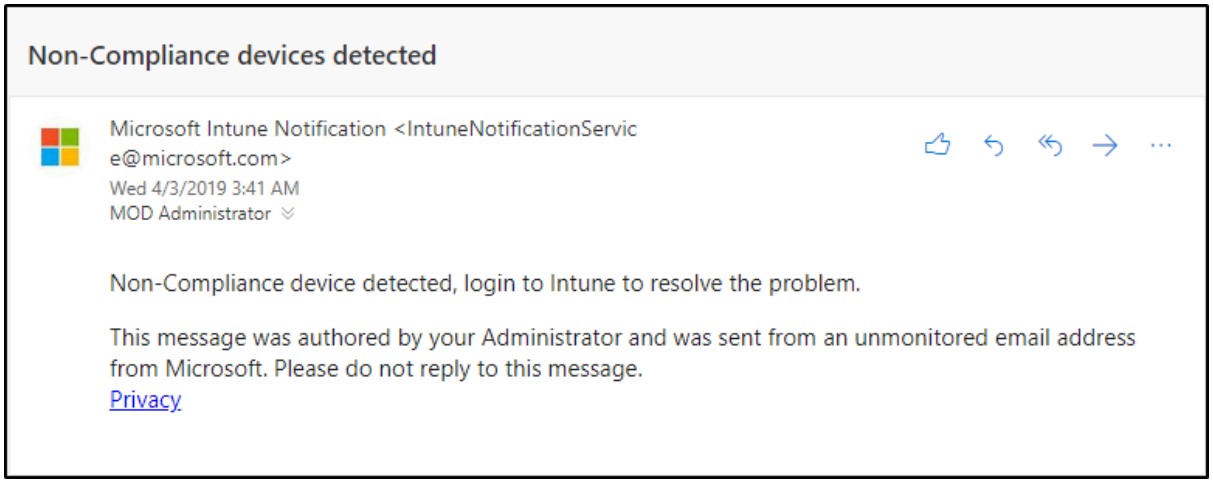
I skjermbildet nedenfor vil man se at enheten *WIN10B*¸ er Non-Compliant, etter at vi slo av Firewall.

Figur 198: Workloads - Compliance Policy



Figur 199: Workloads - Compliance Policy

Etter at det oppdages at en enhet er Non-Compliant, sendes en mail til IT-Department, samt sluttbrukeren. Mailes ser slik ut:



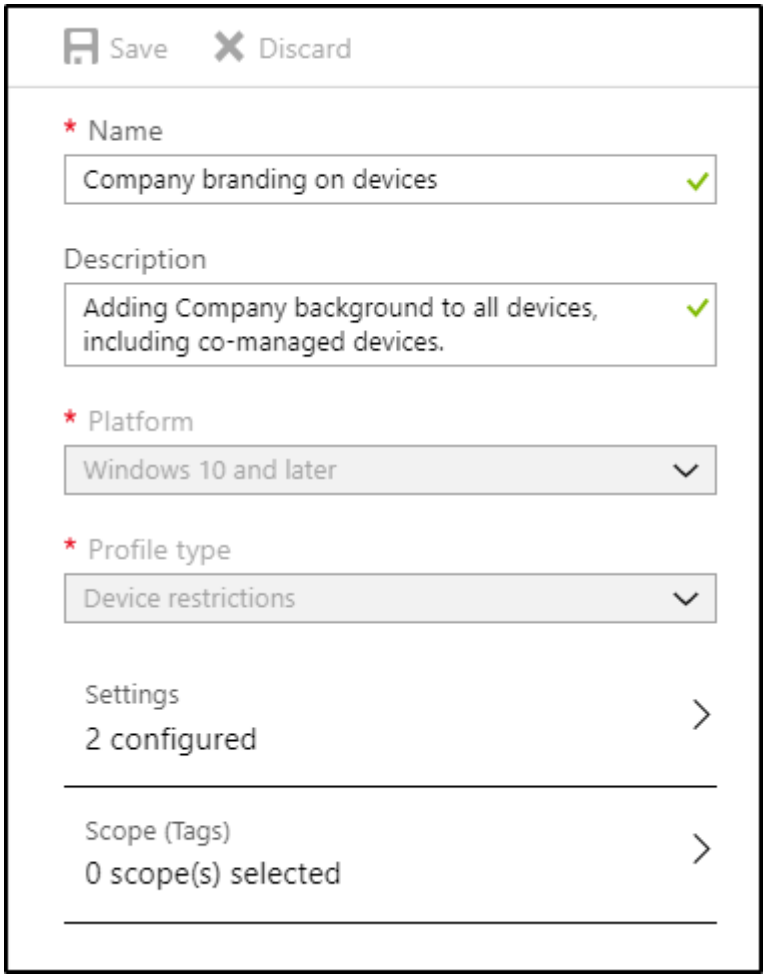
Figur 200: Workloads - Compliance Policy

Device Configuration

La oss nå se på hvordan vi kan ta i bruk Device Configuration i Intune, for å kunne utføre operasjoner lignende Group Policy Management i Active Directory. I denne demonstrasjonen, vil vi ta for oss to enkle innstillinger, for å teste om det fungerer.

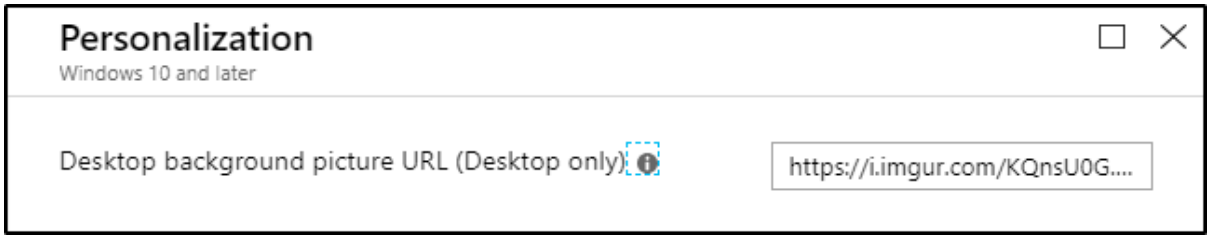
Vi navigerer oss til ***Microsoft Intune – Device Configuration – Profiles*** og trykker på **Create Profile**.

Videre legger vi til *name*, *description* og trykker på **Settings**.



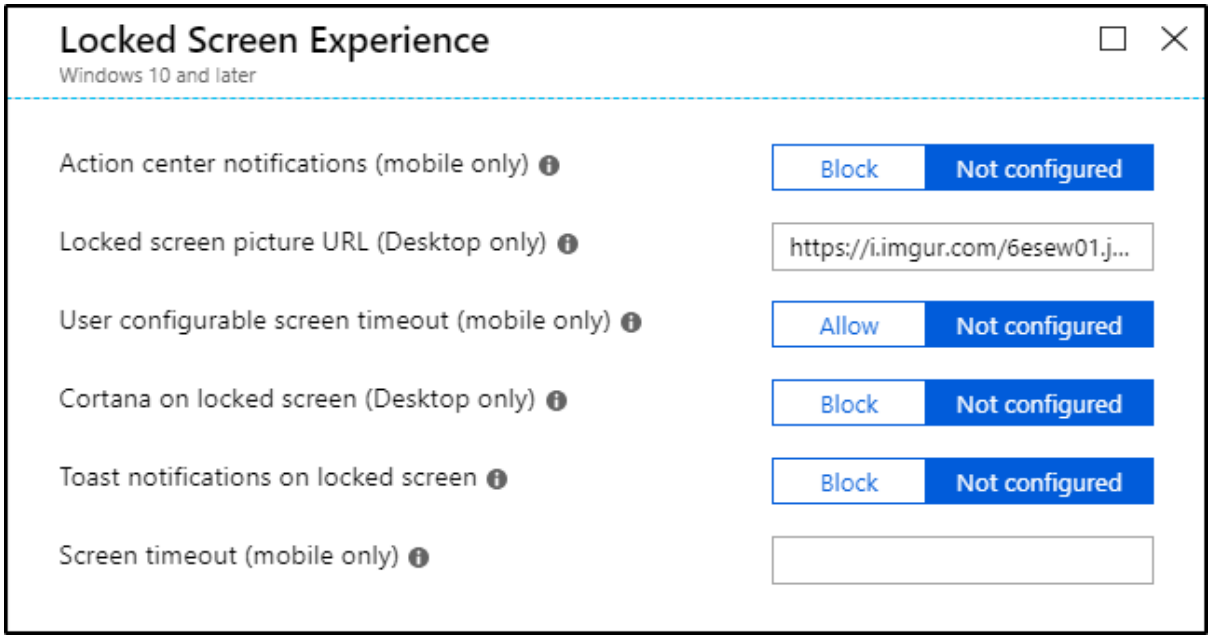
Figur 201: Workload - Device Configuration

Vi vil nå vise hvordan man kan sette desktop bakgrunn på maskinene, denne innstilligen finner vi under ***Personalization***.



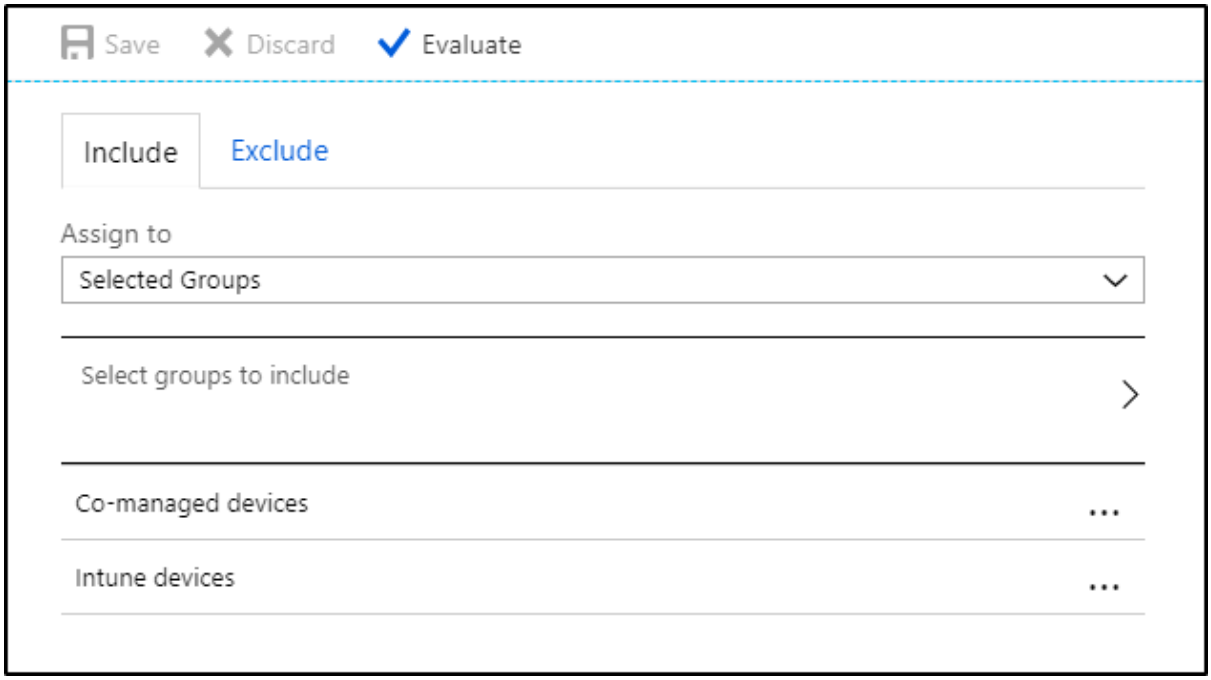
Figur 202: Workload - Device Configuration

Vi vil også og legge til et lock-screen bilde, denne innstillingen finner vi under ***Locked Screen Experience***. Deretter trykker **OK** og **Create**.



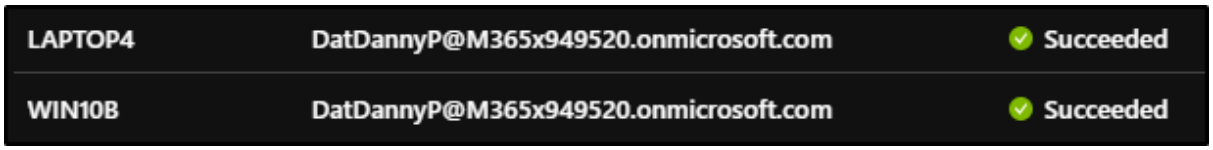
Figur 203: Workload - Device Configuration

Videre går vi inn på profilen vi har laget og velger **Assignment**. Her legger vi til de gruppene som vår device configuration policy skal gjelde for.



Figur 204: Workload - Device Configuration

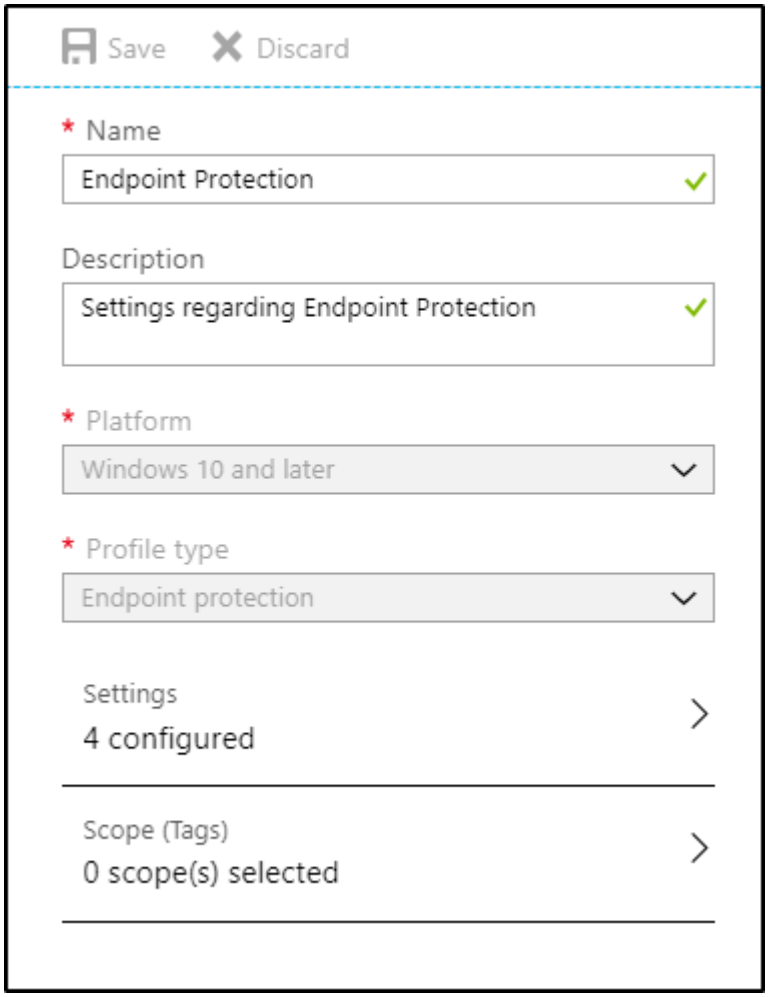
På skjermbildet nedenfor ser vi at LAPTOP4 og WIN10B, har fått tildelt profilen. Dette sier oss at de innstillingene som er satt i configuration policy-en, kan gjelde for både Intune og co-managed enheter.



Figur 205: Workload - Device Configuration

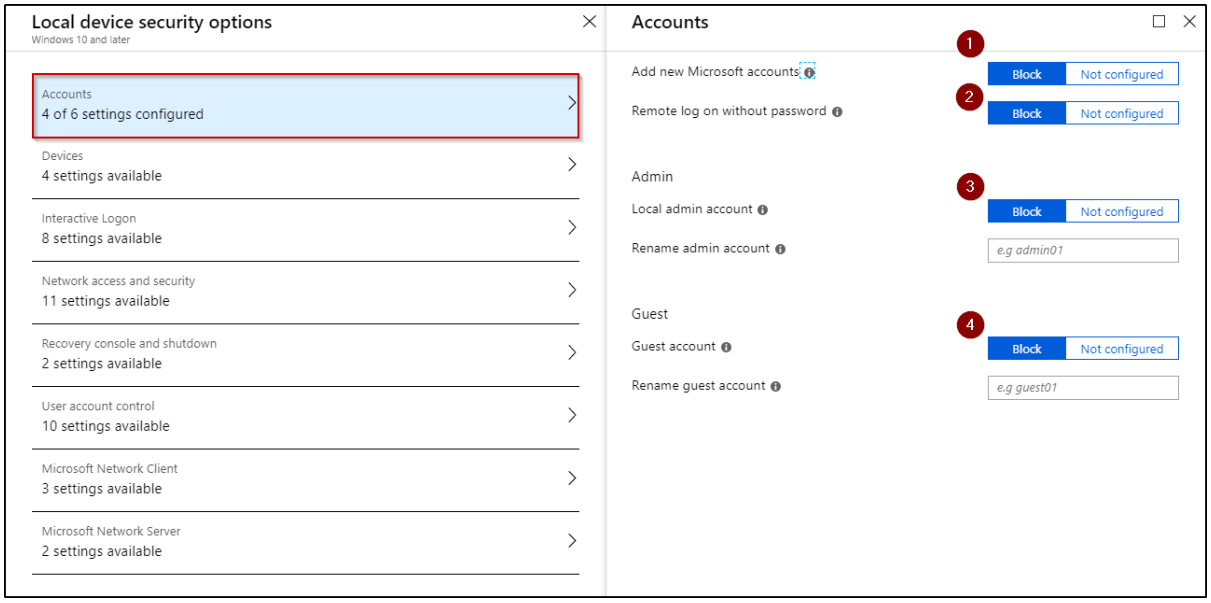
Endpoint Protection og Resource access policies

La oss nå ta en titt på Endpoint Protection til å begynne med. Vi oppretter en ny Device Configuration Profile og velger at denne skal gjelde for *Profile type: Endpoint protection*. Vi trykker deretter på **Settings**.



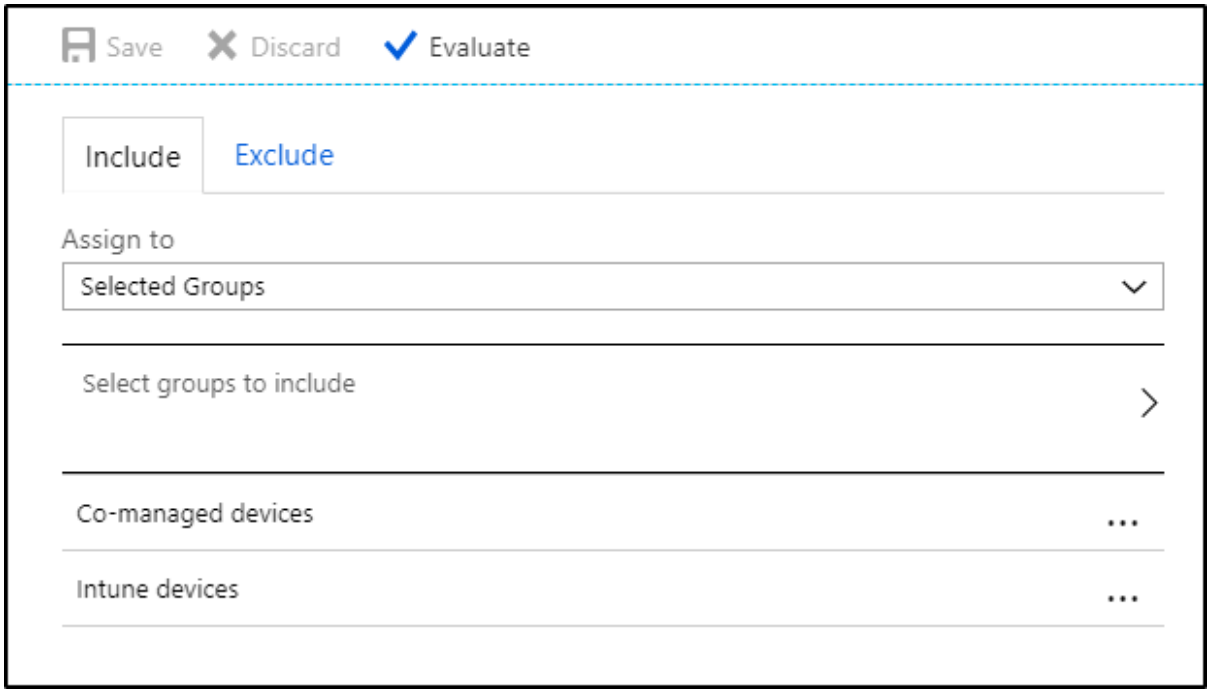
Figur 206: Endpoint Protection og Recourse access policies

Vi går inn og setter de innstillingene som måtte gjelde for vår bedrift, når det kommer til Endpoint Protection. I denne demonstrasjonen, benytter vi noen innstillinger som tar for seg restriksjoner om oppretting og bruk av forskjellige typer kontoer på enheten. Blar oss tilbake ved å trykke på **OK**, og trykker deretter på **Create**.



Figur 207: Endpoint Protection og Recourse access policies

Når profilen er opprettet, navigerer vi oss inn på profilen og velger **Assignments**, hvor vi legger til gruppene som profilen skal gjelde for. Her velger vi både Intune devices og Co-managed devices, for å teste at den fungerer på både Intune og co-managed enheter.



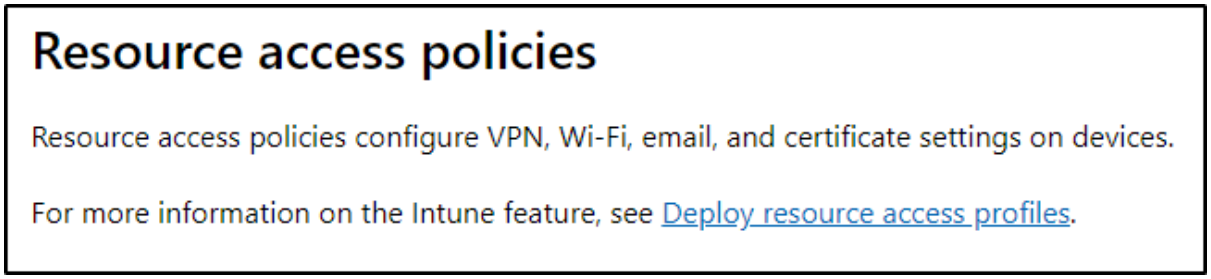
Figur 208: Endpoint Protection og Recourse access policies

Hvis vi nå går inn på ***Device Status***, under profilen, vil vi se at både WIN10B (Co-managed enhet) og LAPTOP4 (Intune managed only enhet), har fått tildelt profilen.

DEVICE	USER PRINCIPAL NAME	DEPLOYMENT STATUS
WIN10B	DatDannyP@M365x949520.onmicrosoft.com	Succeeded
LAPTOP4	DatDannyP@M365x949520.onmicrosoft.com	Succeeded

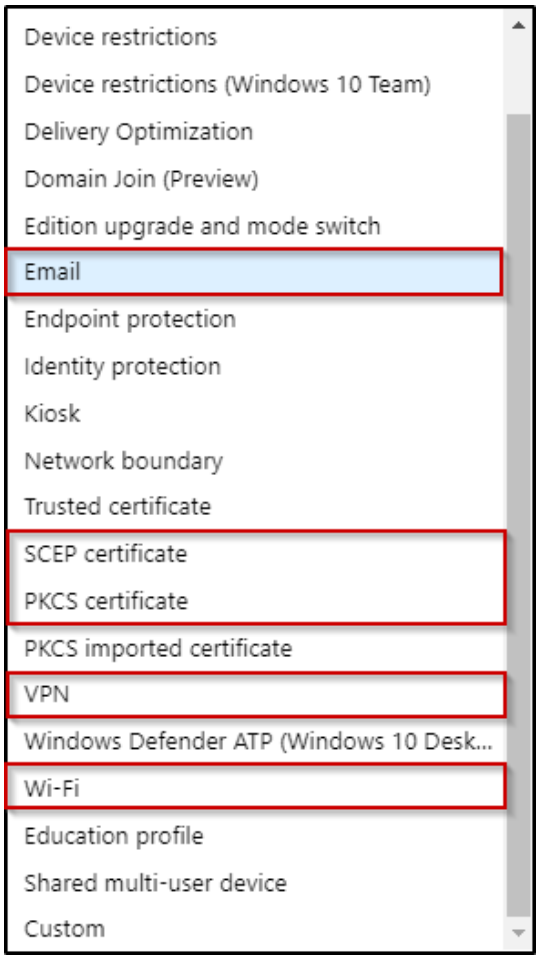
Figur 209: Endpoint Protection og Recourse access policies

Hvis vi ser på dokumentasjon over workloads hos Microsoft sine egne nettsider, forteller de at Resource access policies, dekker VPN, Wi-Fi, email og sertifikat innstillinger. Når vi videre skal opprette en Device Configuration Policy, for resource access policies, må vi da velge en av disse. For denne demonstrasjonen skal vi opprette en resource access policy for VPN.



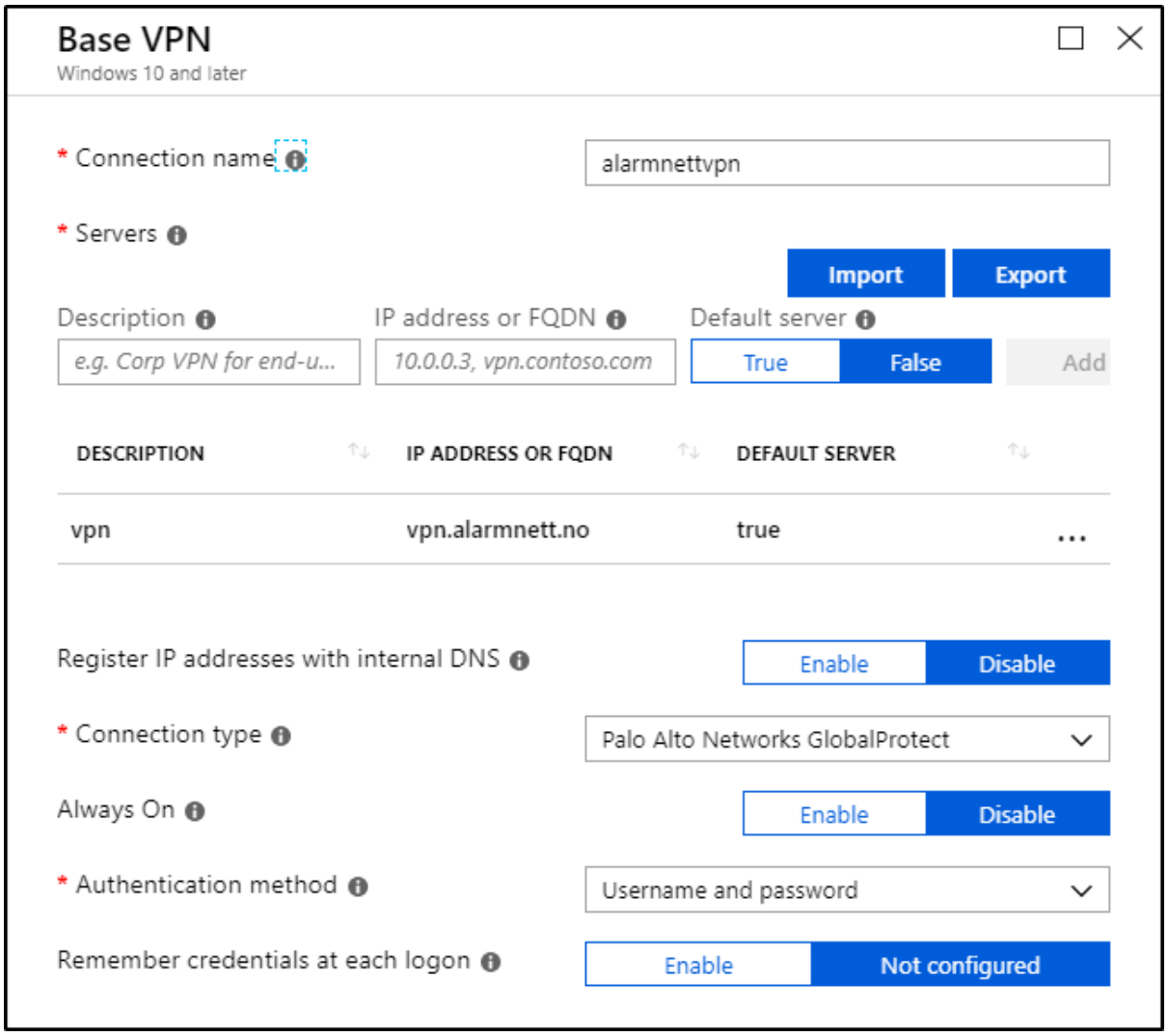
Figur 210: Endpoint Protection og Recourse access policies

I skjermbildet nedenfor ser vi igjen de fem ulike mulighetene som vi kan konfigurere, som Resource access policies dekker. Vi velger **VPN**.



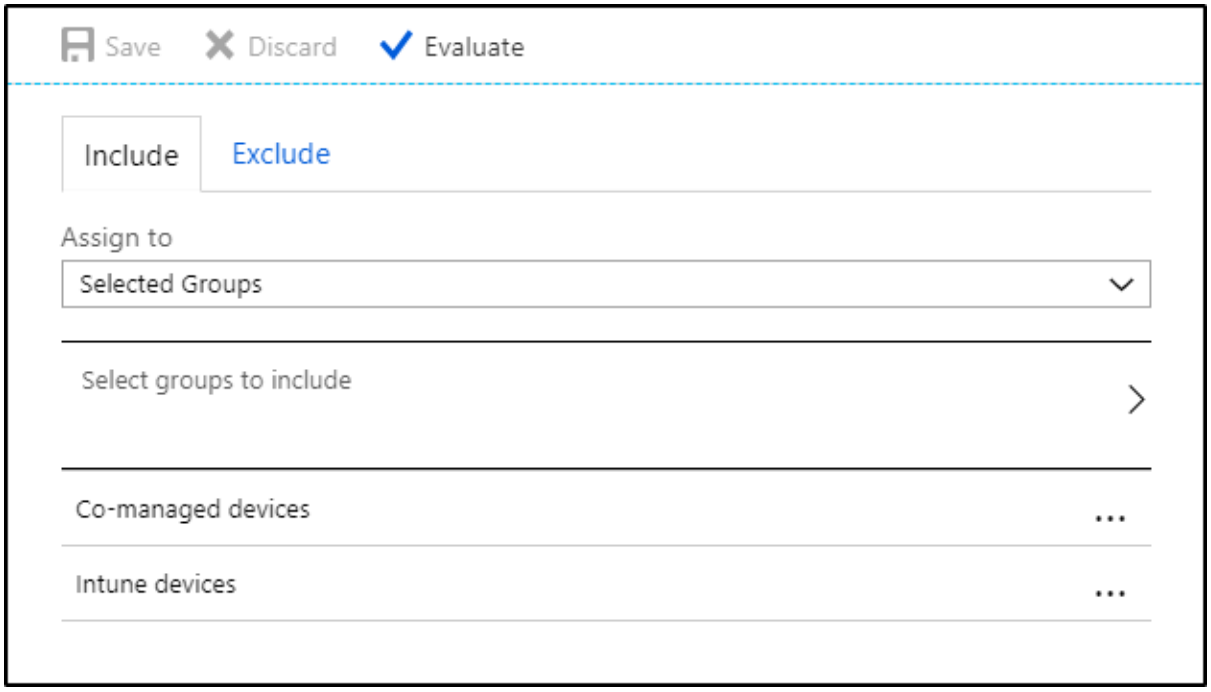
Figur 211: Endpoint Protection og Recourse access policies

Videre går vi inn og legger til informasjon i de feltene som er påkrevd. Skal sies at informasjonen som vi legger til ikke er reell, men kun for å teste at både intune only managed enheter og co-managed enheter vil få policy-en fra Intune.



Figur 212: Endpoint Protection og Recourse access policies

Deretter velger vi policy-en og trykker **Assignments**, her legger vi til gruppene som policy-en skal gjelde for.



Figur 213: Endpoint Protection og Recourse access policies

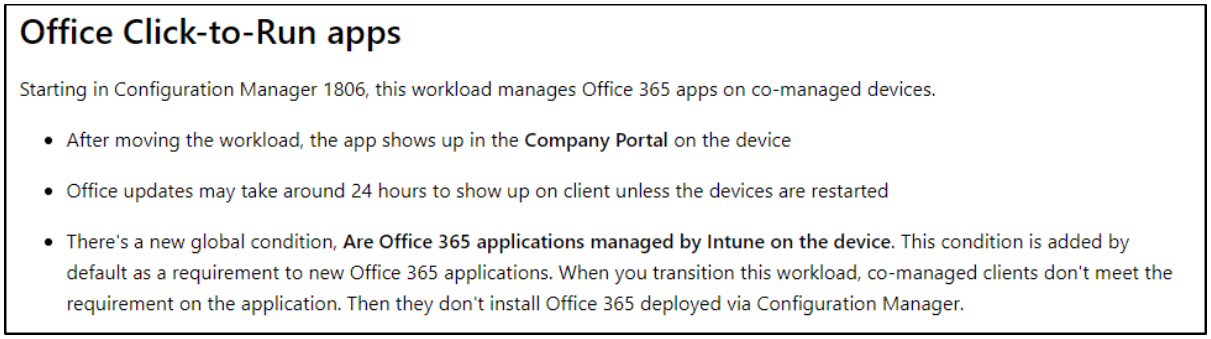
Nedenfor ser vi her at både WIN10B og LAPTOP4, har fått policy-en. Dette betyr at Resource access policy-en fungerer for både co-managed- og Intune only managed enheter.

DEVICE	USER PRINCIPAL NAME	DEPLOYMENT STATUS
WIN10B	DatDannyP@M365x949520.onmicrosoft.com	Succeeded
LAPTOP4	DatDannyP@M365x949520.onmicrosoft.com	Succeeded
WIN10A	None	Pending
LAPTOP3	None	Pending
LAPTOP2	None	Pending
Laptop1	None	Pending
WIN10D	None	Pending

Figur 214: Endpoint Protection og Recourse access policies

Office Click-to-Run apps og Client apps

Under dette kapittelet skal vi ta for oss to workloader, som begge jobber med applikasjoner. Vi vil først se på **Office Click-to-Run apps** og deretter ta en titt på **Client apps**.
Office Click-to-Run Apps, kommer med i versjon 1806 av SCCM. Ifølge Microsoft sine nettsider, skal man kunne administrere Office 365 applikasjoner på co-managed enheter med Intune. Det skal sies at det ikke ligger ute så mye informasjon på nettet, men prosessen skal være ganske grei å gjennomføre. Skjermbildet nedenfor viser dokumentasjon om Office Click-to-Run apps, som ligger ute på Microsofts nettsider.



Office Click-to-Run apps

Starting in Configuration Manager 1806, this workload manages Office 365 apps on co-managed devices.

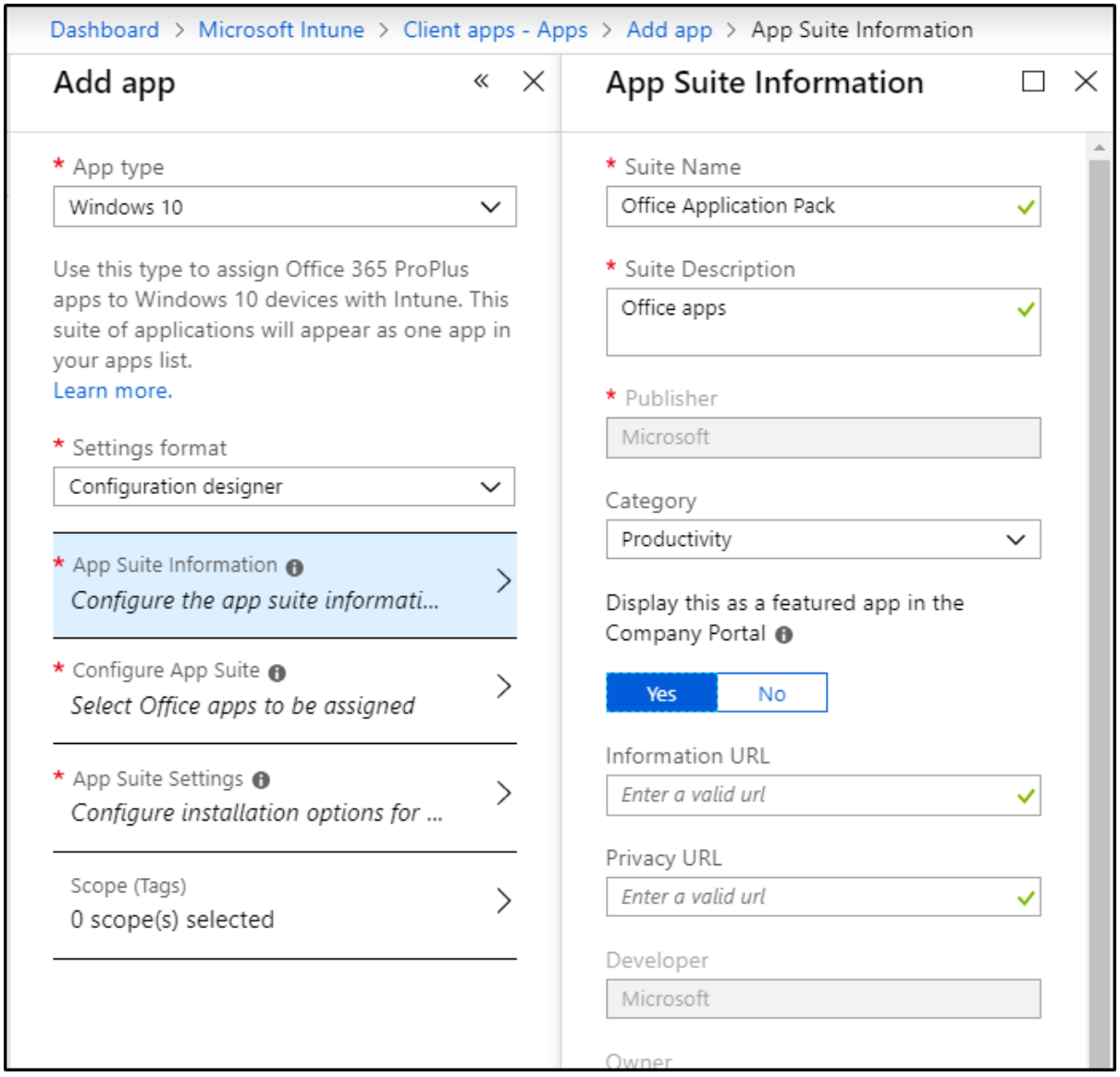
- After moving the workload, the app shows up in the **Company Portal** on the device
- Office updates may take around 24 hours to show up on client unless the devices are restarted
- There's a new global condition, **Are Office 365 applications managed by Intune on the device**. This condition is added by default as a requirement to new Office 365 applications. When you transition this workload, co-managed clients don't meet the requirement on the application. Then they don't install Office 365 deployed via Configuration Manager.

Figur 215: Office Click-to-Run apps og Client apps

Vi starter med å opprette en applikasjon i Intune.

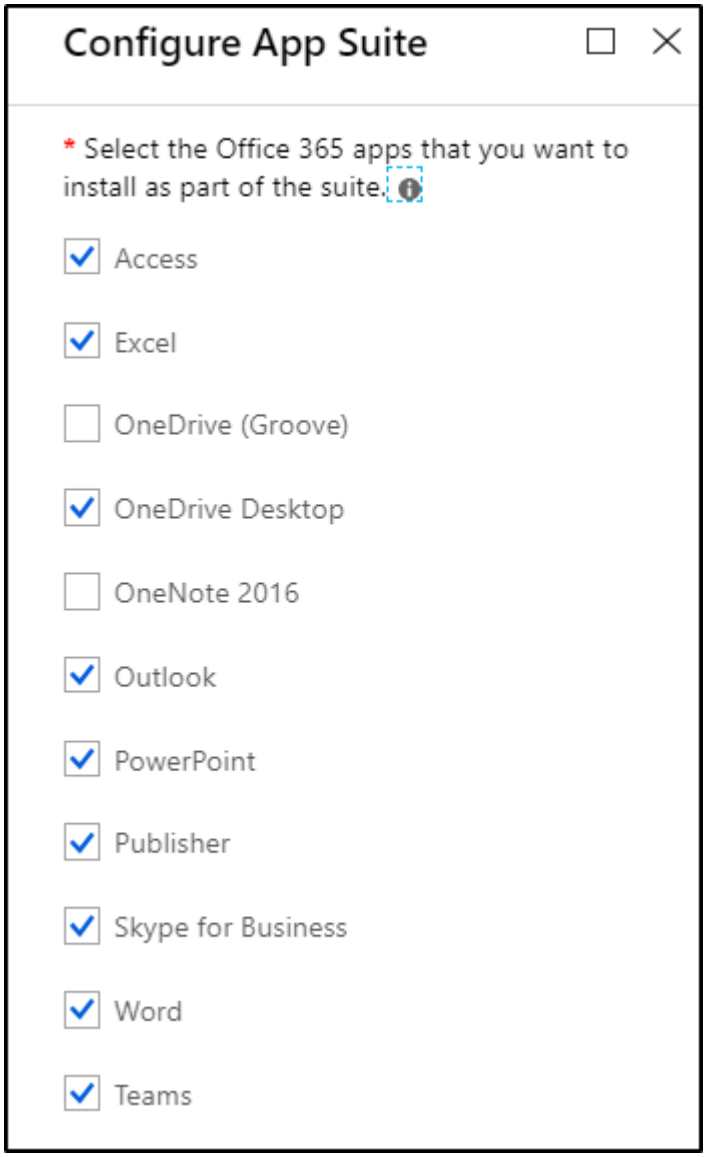
Vi navigerer oss til ***Microsoft Intune – Client apps*** og velger **Add**.

Deretter velger vi *App type*, og setter denne til **Windows 10**. Videre går vi inn på ***App Suite Information***, her setter vi navn og velger at applikasjonen skal vises i Company Portal.



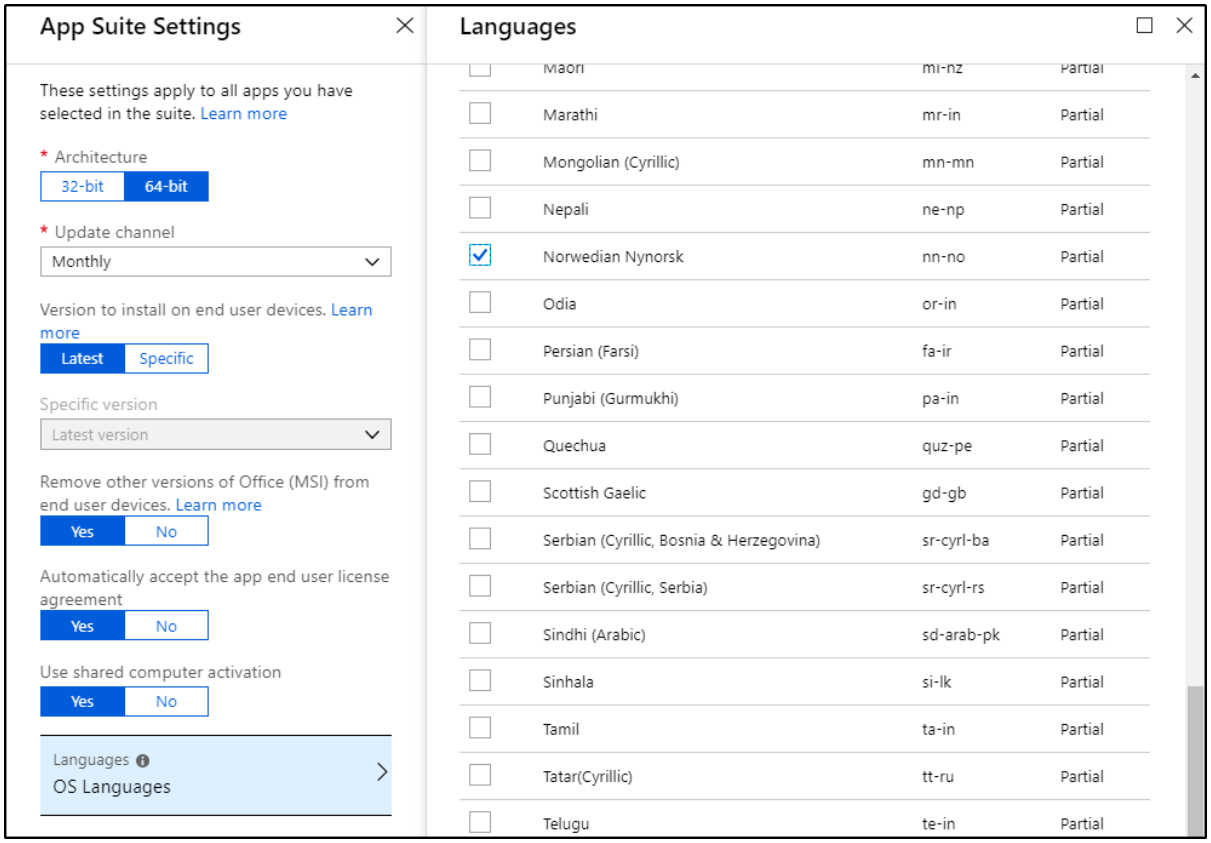
Figur 216: Office Click-to-Run apps og Client apps

Videre velger vi ***Configure App Suite***. Her velger vi de programmene som vi ønsker å installere. Man kan også legge til MS Viso og MS Project, hvis man har lisenser for disse.



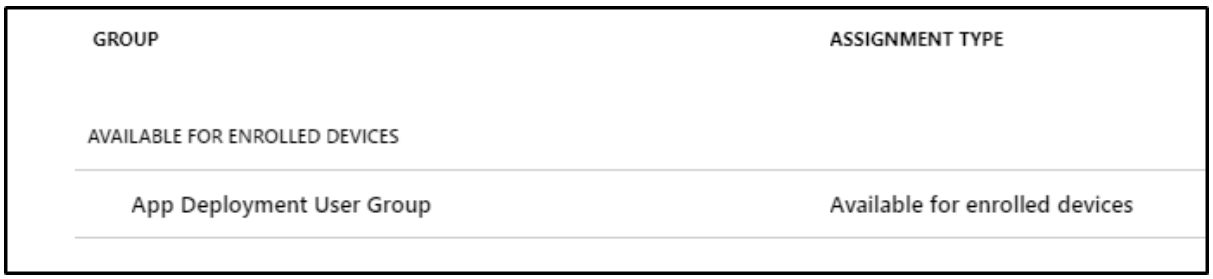
Figur 217: Office Click-to-Run apps og Client apps

Under ***App Suite Settings***, gjør vi de valgene som vi føler passer best, og velger til slutt språk.



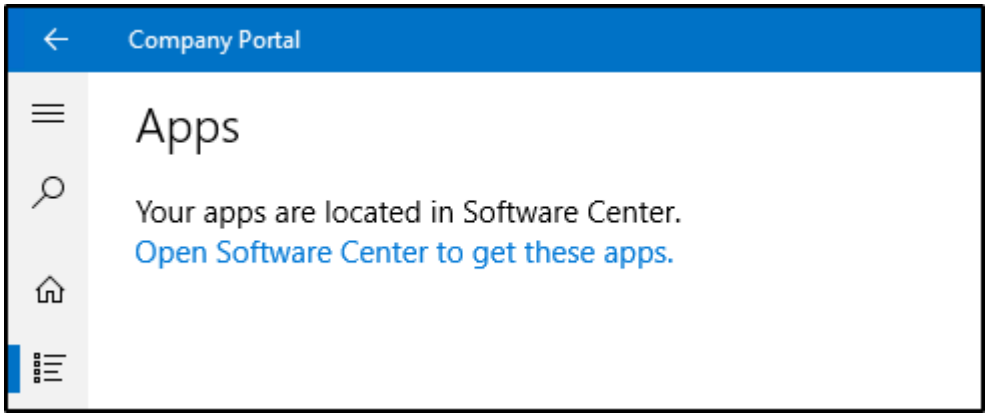
Figur 218: Office Click-to-Run apps og Client apps

Når applikasjonen er laget, tildeler vi applikasjoner en gruppe eller flere, som vi ønsker å rulle ut applikasjonen til. Nedenfor har vi lagt til gruppen **App Deployment User Group**. En ting som man kan merke seg er at vi tildeler en gruppe med brukere og ikke devices, når vi ønsker å rulle ut applikasjoner til co-managed enheter, da det har blitt hintet til oss gjennom andre som har hatt problemer med applikasjonsutrulling fra forum på nettet.



Figur 219: Office Click-to-Run apps og Client apps

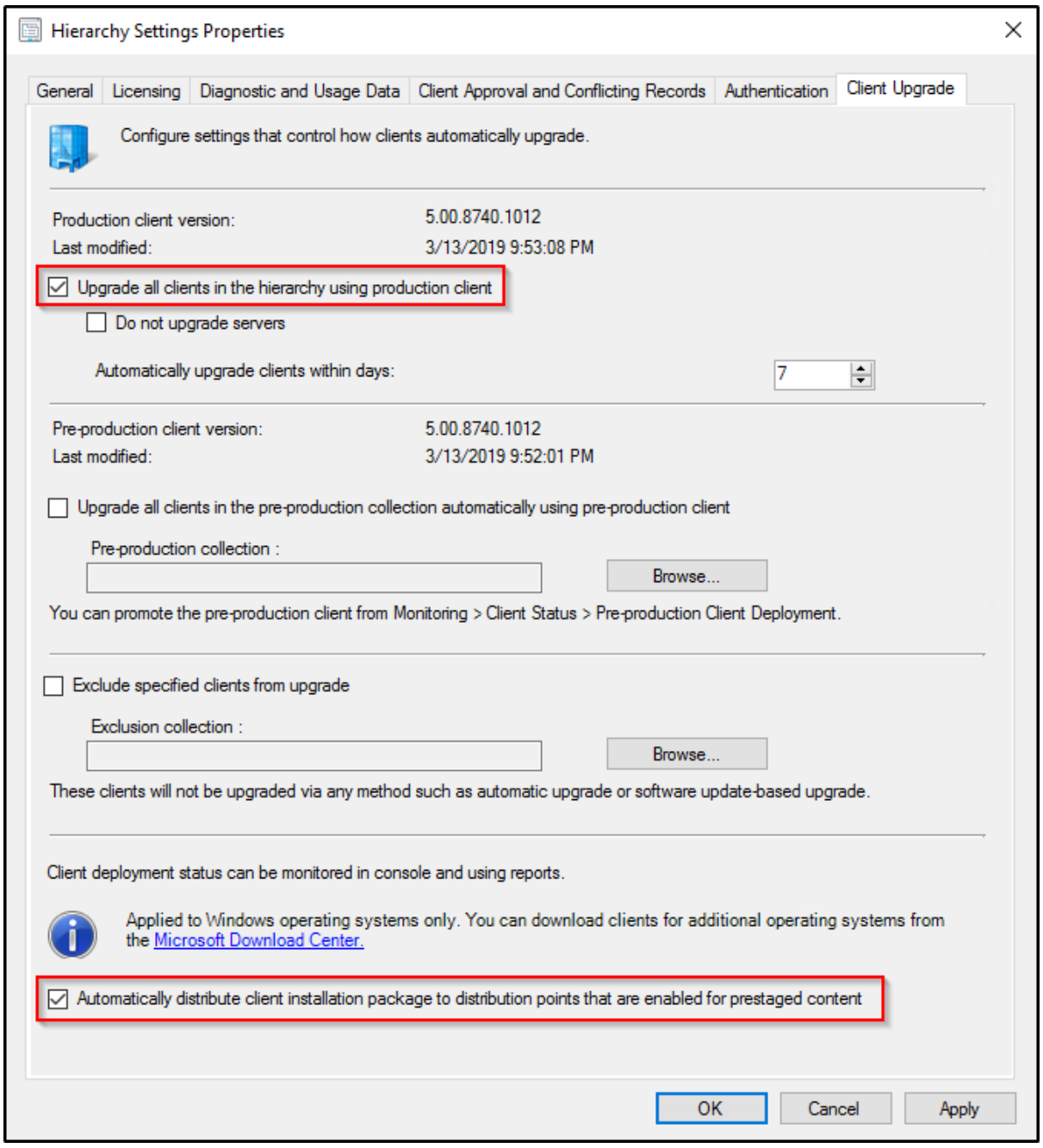
Når vi har laget ferdig applikasjonen i Intune, og lagt til en gruppe i ***Assignments***, skal man kunne få tilgang til applikasjonen i Company Portal. Det er her vi møter på et problem. Når man går inn på en co-managed enhet, kommer det ikke opp noen applikasjoner i Company Portal. Man henvises i stedet til Software Center for applikasjoner, som vist i skjermbildet nedenfor.



Figur 220: Office Click-to-Run apps og Client apps

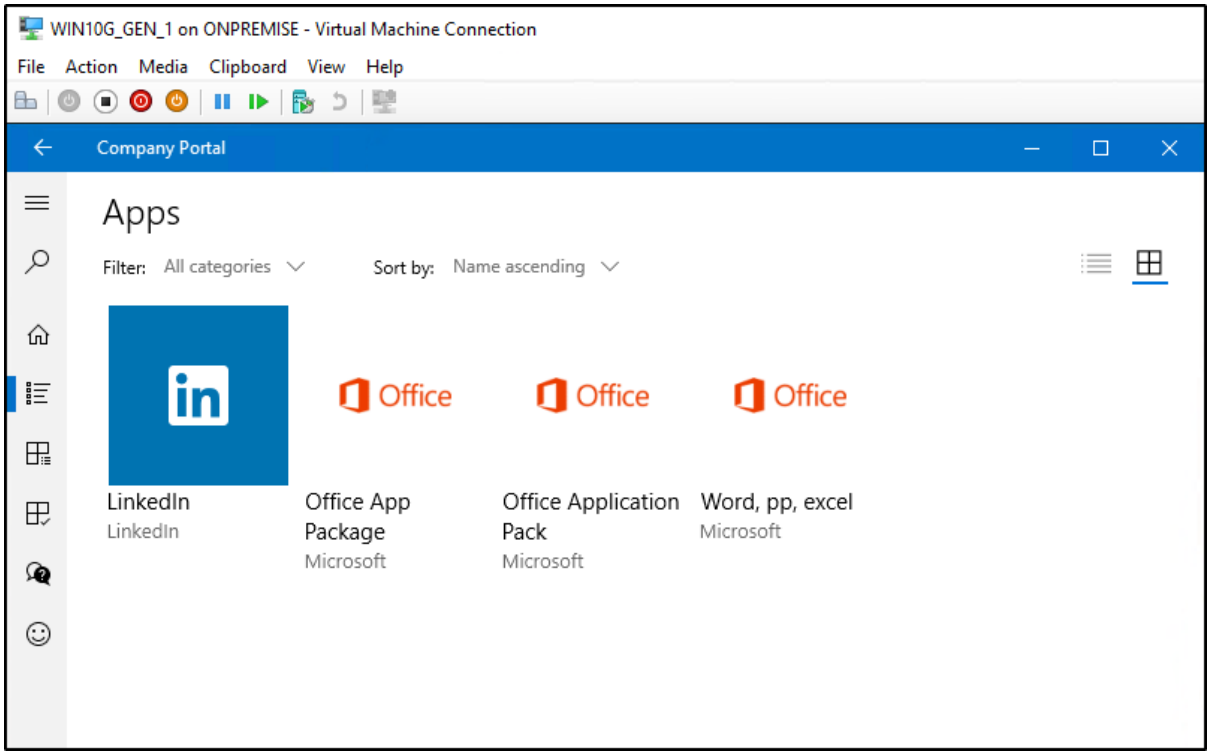
Årsaken til at denne meldingen kommer opp, er at SCCM klienten som rulles ut til våre co-managed enheter, ikke har blitt oppdatert etter vi har flyttet over workloads til Intune. La oss derfor gjøre det nå!

Vi navigerer oss til ***Administration – Sites - Hierarchy Settings – Client Upgrade***. Her huker vi av for: "*Upgrade all clients in the hierarchy using production client*" og "*Automatically distribute client installation package to distribution points that are enabled for prestaged content*". Deretter trykker vi på **OK**.



Figur 221: Office Click-to-Run apps og Client apps

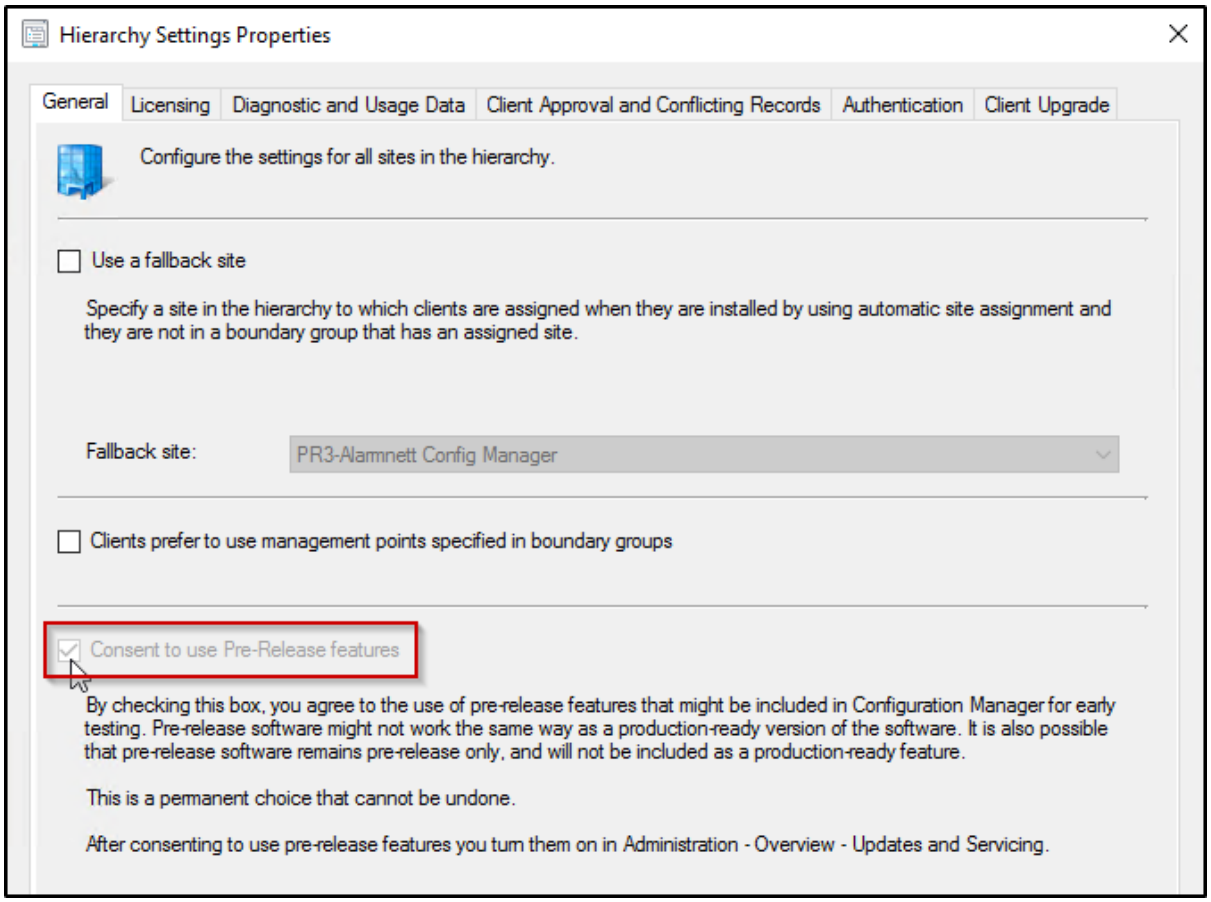
Hvis vi da går inn på Company Portal på en av våre co-managed enheter, ser vi her at WIN10G maskinen har fått tilgang til Office Application Pack, som vi opprettet tidligere.



Figur 222: Office Click-to-Run apps og Client apps

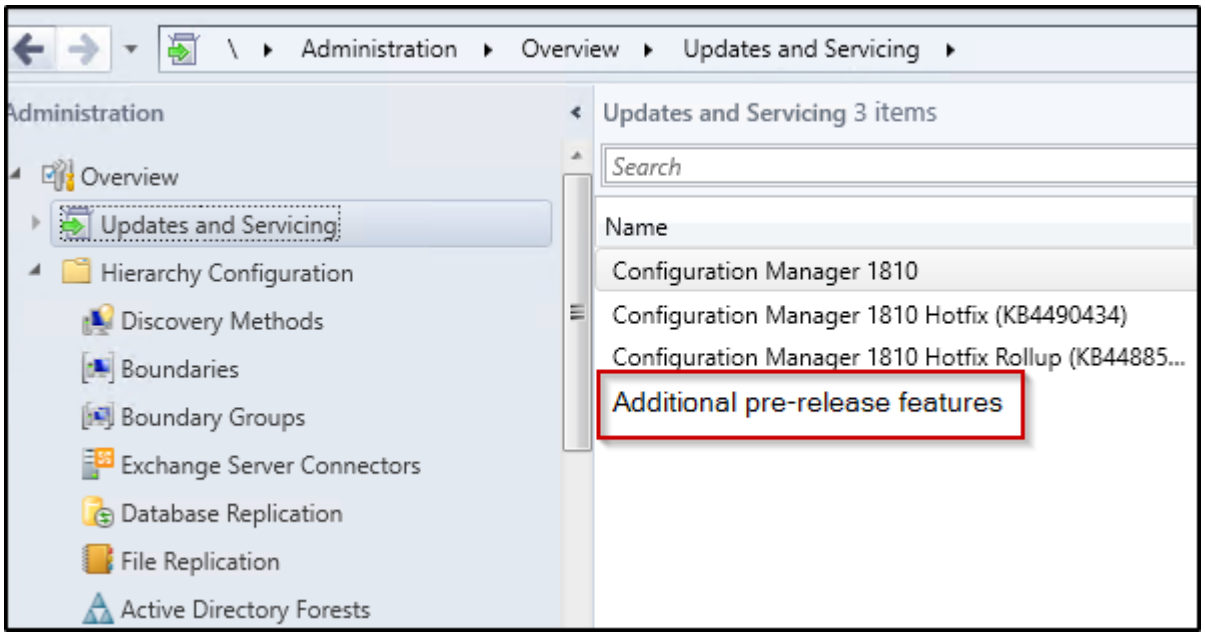
Client Apps, kommer med versjon 1806 av SCCM som en pre-release feature, som man selv må legge til, for å kunne benytte seg av. Workloaden muliggjør for applikasjonsutrulling fra Intune til co-managed enheter.

For å få tilgang til å installere denne beta-funksjonen, må man navigere seg til ***Site Configuration – Sites***, og velge **Hierarchy Settings**. Man må deretter huke av for **Consent to use Pre-Release features**.



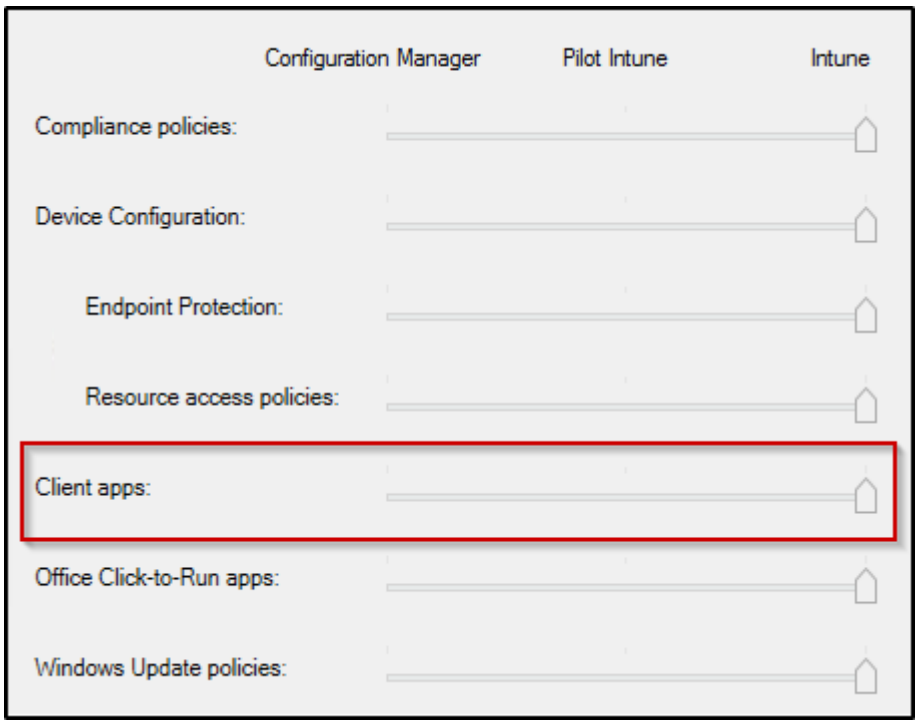
Figur 223: Office Click-to-Run apps og Client apps

Videre kan vi navigere oss til ***Updates and Servicing***, hvor vi nå har mulighet til å installere nye tilgjengelige features. I skjermbildet nedenfor, har vi allerede installert denne funksjonen, men det vil se noe lignende ut.



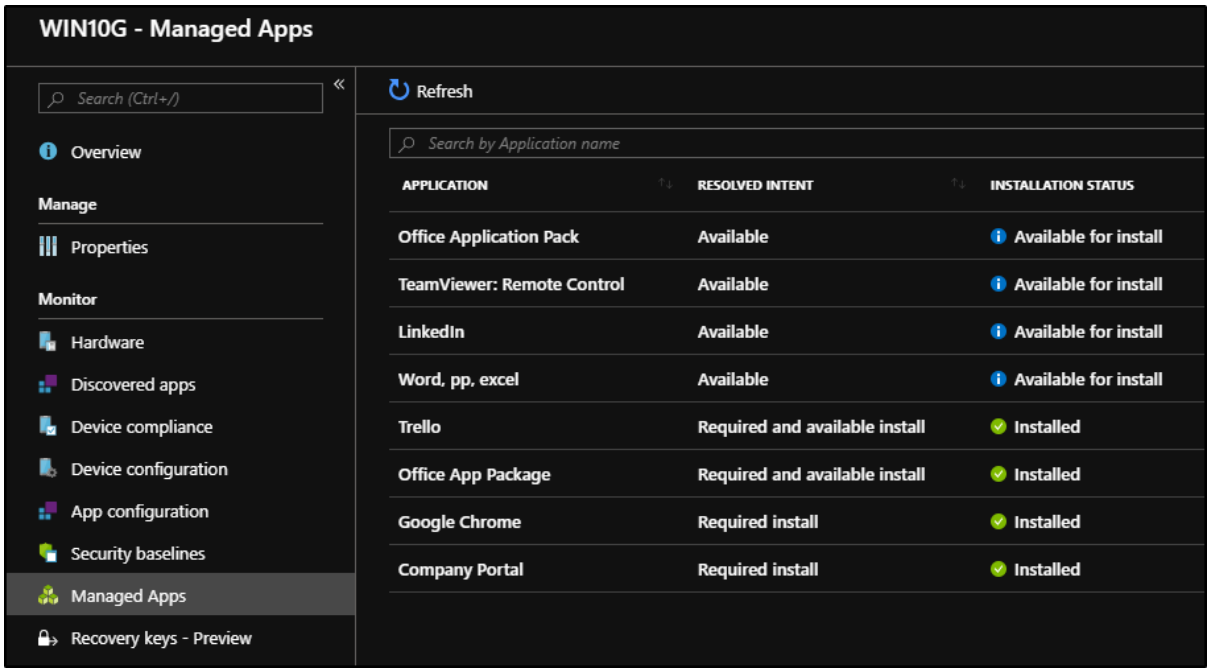
Figur 224: Office Click-to-Run apps og Client apps

Når installasjonen er gjennomført, vil vi få mulighet til å flytte over workloaden til Intune, som vist nedenfor.



Figur 225: Office Click-to-Run apps og Client apps

Vi kan i bildet nedenfor se at WIN10G maskinen som er en co-managed enhet, har fått installert applikasjoner som er satt til «required» og andre applikasjoner har blitt gjort tilgjengelig i Company Portal.



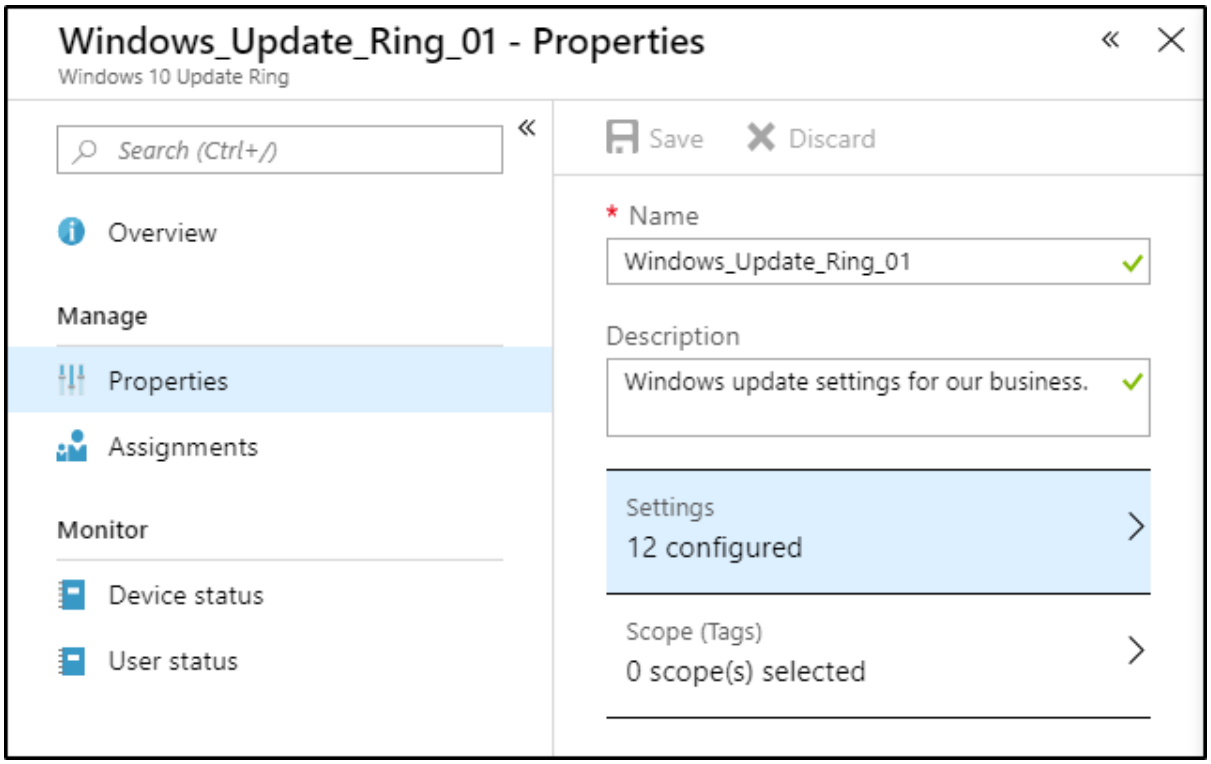
Figur 226: Office Click-to-Run apps og Client apps

Windows Update Policies

Vi skal nå gå gjennom Windows Update Policies, og se på hvordan vi kan konfigurere hvordan og når, Windows as a Service oppdaterer våre Windows 10 enheter.

Vi begynner med å navigere oss til ***Microsoft Intune – Software updates – Windows 10 Update Rings***, og trykker på **Create**.

Vi navngir vår Windows update ring, og trykker på **Settings**.

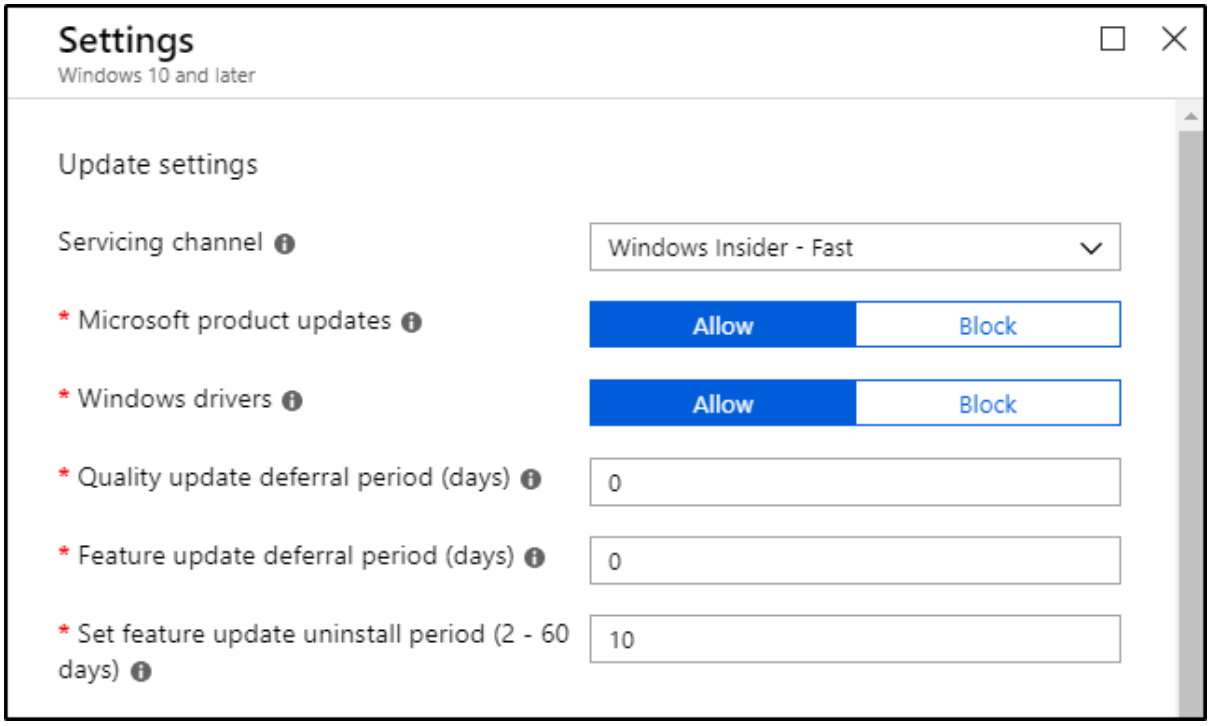


Figur 227: Windows Update Policies

Under ***Settings***, kan vi nå gjøre de valgene som passer best for vår bedrift.

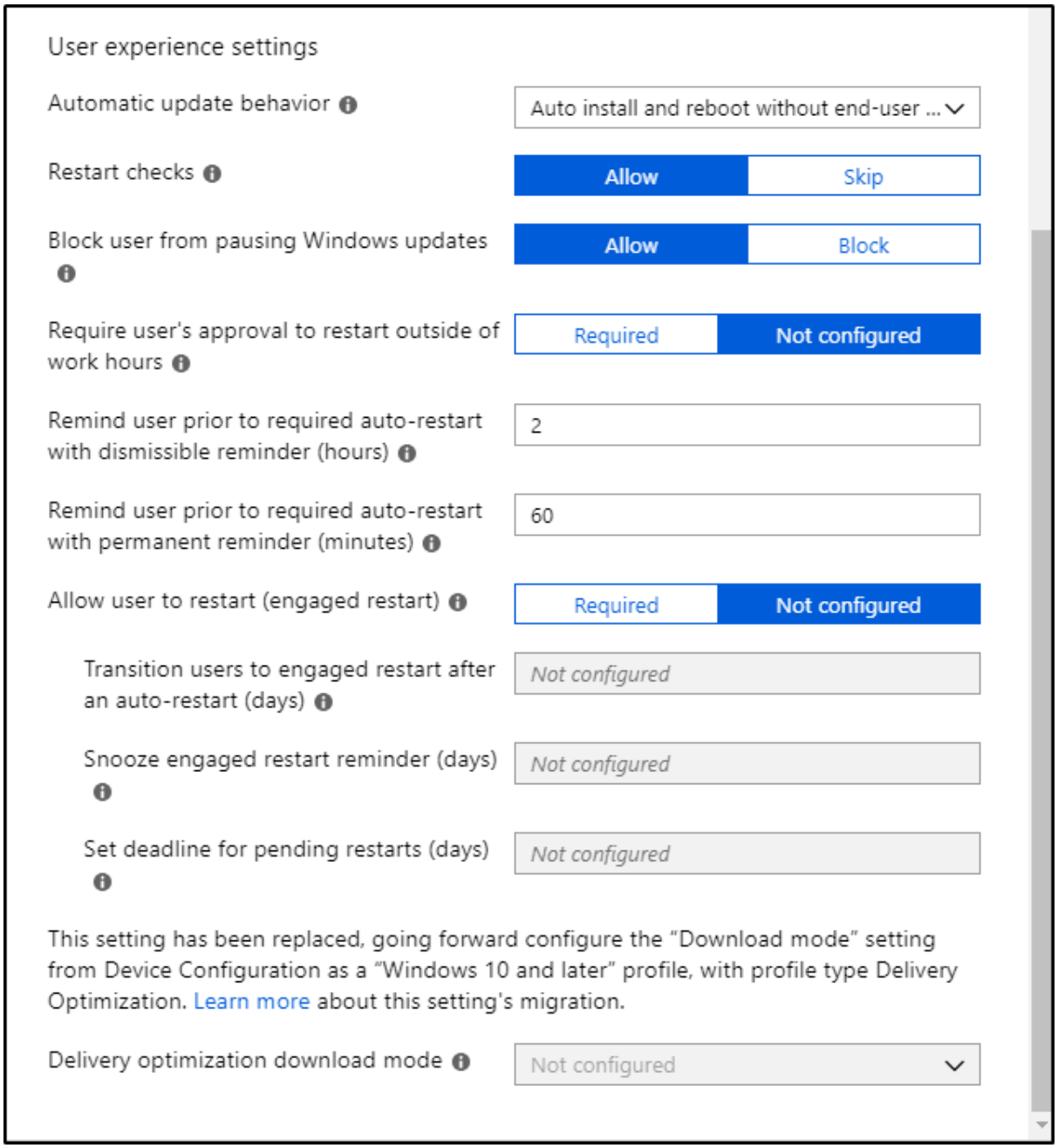
Vi gjør disse valgene:

- **Servicing channel:** Windows Insider – Fast
    - Dette er for å melde maskinene til Insider programmet for å se og teste nye funksjoner. For en vanlig bedrift anbefales et av semi-annual valgene da de er mer stabile oppdateringer fra Microsoft.
- **Automatic update behavior:** Auto install and reboot without end-user control
    - Vi setter dette slik at vi kan forsikre oss om at enhetene blir oppdatert og ikke utgjør en risiko.
- **Remind user prior to required auto-restart with dismissible reminder (hours):** 2
    - Innstillingen vil gi brukeren en notifikasjon om at maskinen kommer til å restarte innen gitt tid. Denne notifikasjonen kan lukkes.
- **Remind user prior to required auto-restart with permanent reminder (minutes):** 60
    - Innstillingen vil gi brukeren en notifikasjon om at maskinen kommer til å restarte innen gitt tid. Denne notifikasjonen kan ikke lukkes.



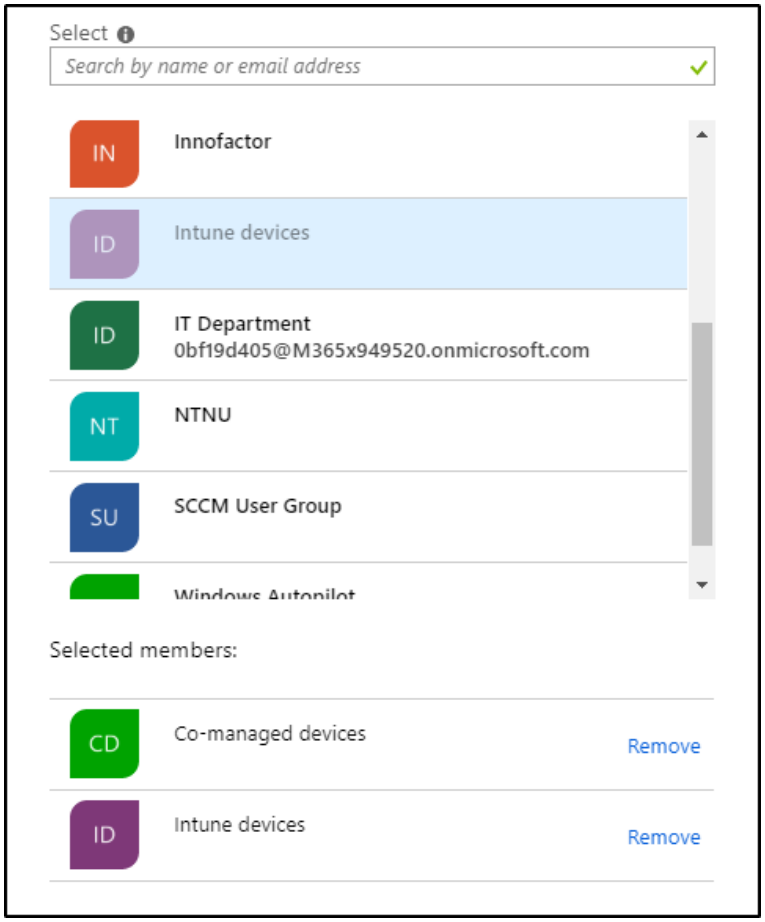
Figur 228: Windows Update Policies

Når vi har gjort de valgene vi ønsker, trykker vi på **OK** og **Create**.



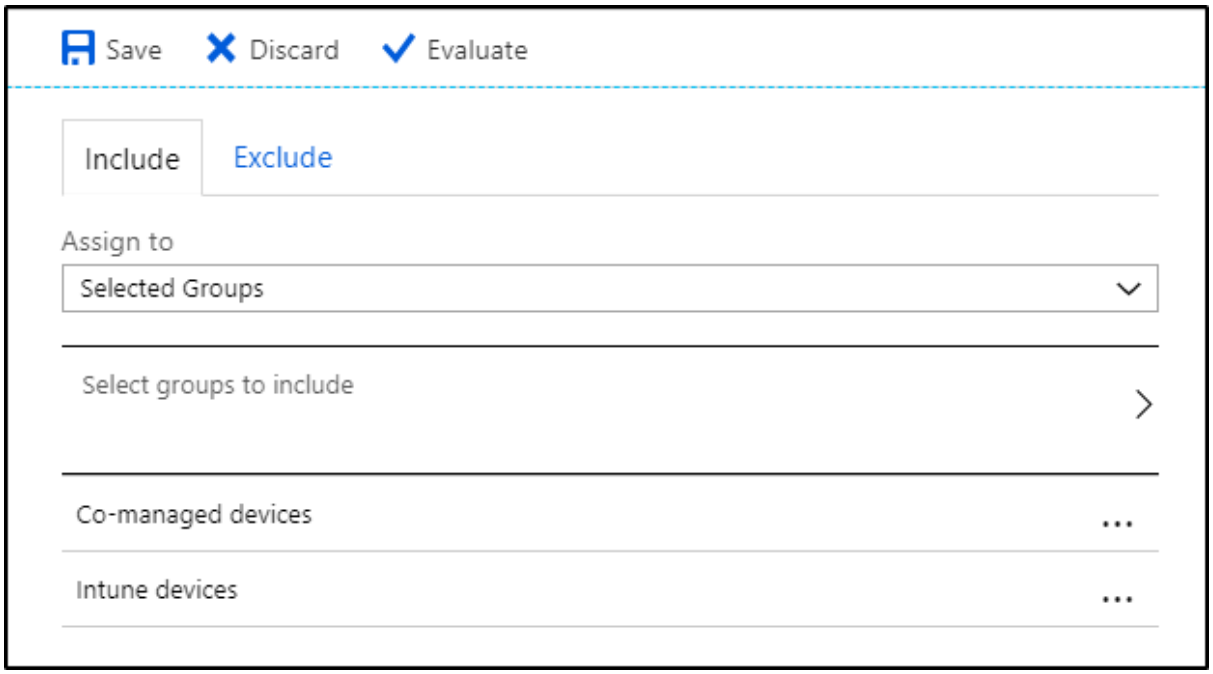
Figur 229: Windows Update Policies

Videre vil vi tildele enhetsgrupper til vår Windows 10 Update Ring. Vi navigerer oss til ***Windows_Update_Ring_01 – Assignments***, og legger til gruppene vi ønsker.



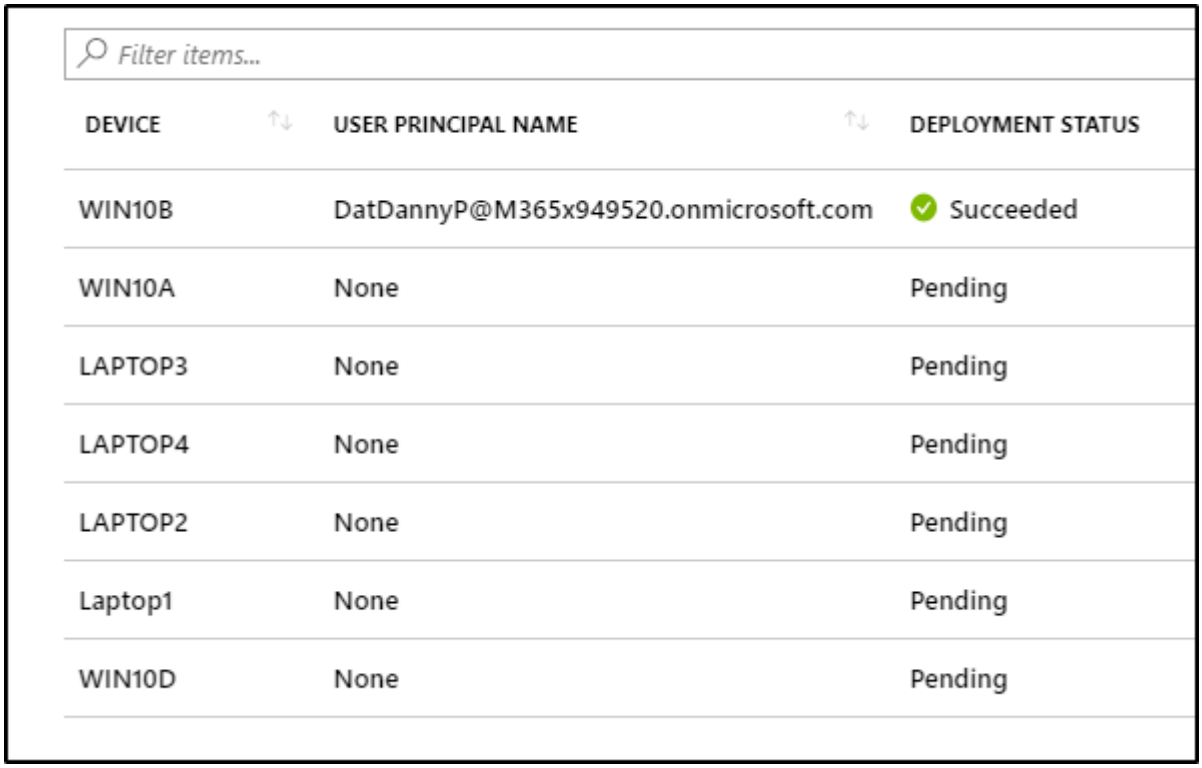
Figur 230: Windows Update Policies

Videre trykker vi på **Save**.



Figur 231: Windows Update Policies

I skjermbildet nedenfor ser vi at like etterpå, så har *WIN10B*, fått tilordnet Windows Update Policy-en. *WIN10B*, er en co-managed enhet, som også betyr at denne Intune funksjonen fungerer for Co-Managed enheter, så lenge workloaden er satt til Intune. Når det gjelder resterende enheter, så vil disse få policy-en når de slås på.



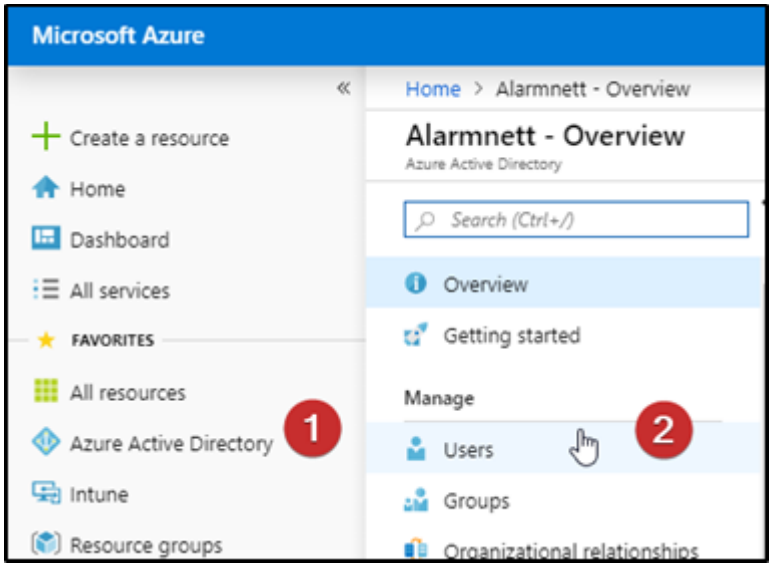
Figur 232: Windows Update Policies

Fase 4 – Funksjoner i Azure AD og Intune

Azure AD brukere og grupper

Legg til bruker i Azure

Det er mulig å legge til brukere i Azure. Ved å lage brukere kan man enkelt tilordne en person sin egen profil og begrensninger for å lettere styre tilgang og rettigheter. Det vil også være mye lettere å holde styr på ting som lisenser og enheter personen har ved å lage brukere. For å legge til brukere i Azure starter vi med å navigere oss til sidemenyen i Azure. Her vil du finne **Azure Active Directory** – og gå til **Users**

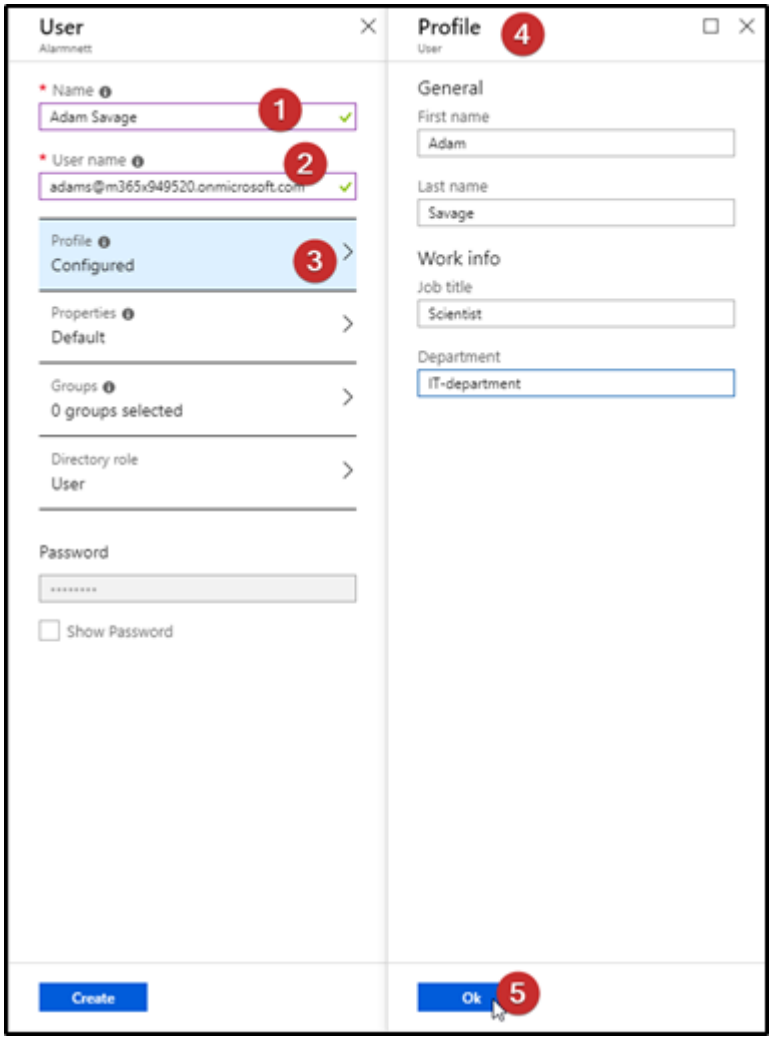


Figur 233: Azure AD brukere og grupper

Her vil du finne en oversikt over alle brukerne i din Directory (du vil eventuelt finne on-premise brukerne dine her om du har satt opp et co-managed miljø). Lag en ny bruker ved å trykke på **New user**.

Figur 234: Azure AD brukere og grupper

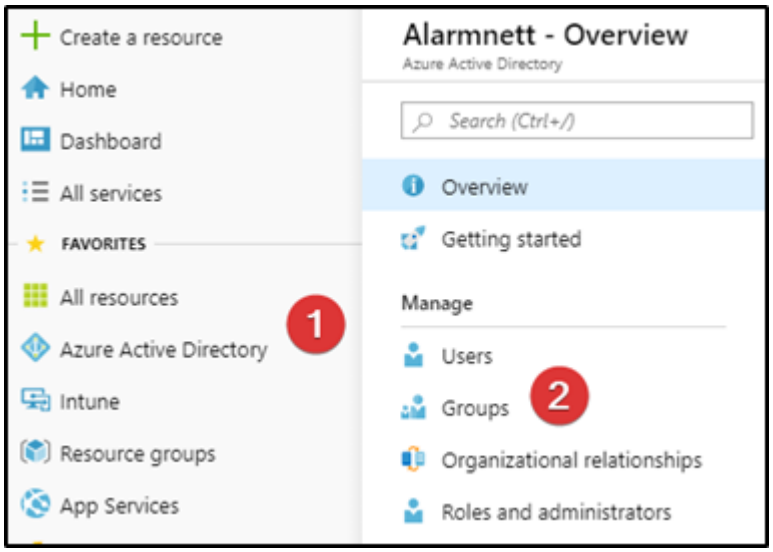
Da vil du bli møtt med en side hvor du må fylle ut informasjon om den nye brukeren. Legger til informasjon om brukeren. Kan eventuelt også legge til brukeren i grupper. **Under Directory role** kan vi velge hva slags bruker du skal lage, for eksempel om du skal lage en bruker eller administrator. Det er mulig å endre eller legge til rettigheter senere.



Figur 235: Azure AD brukere og grupper

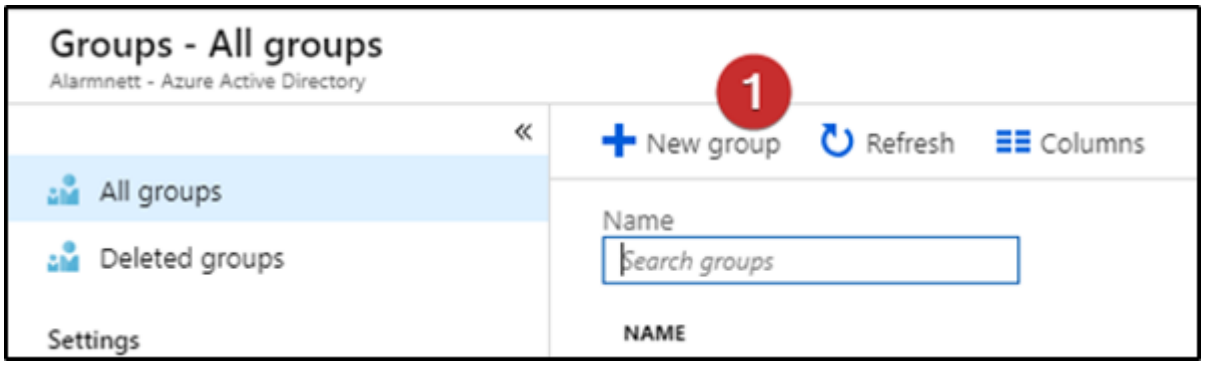
Opprette og tilordne bruker til en gruppe

Det er smart å tilordne brukere og maskiner til grupper, på den måten kan man gi flere samme rettigheter eller samme profiler uten å måtte gjøre det for hver enkelt maskin eller bruker. Gå til ***Azure AD*** - ***Groups***.



Figur 236: Opprette og tilordne bruker til en gruppe

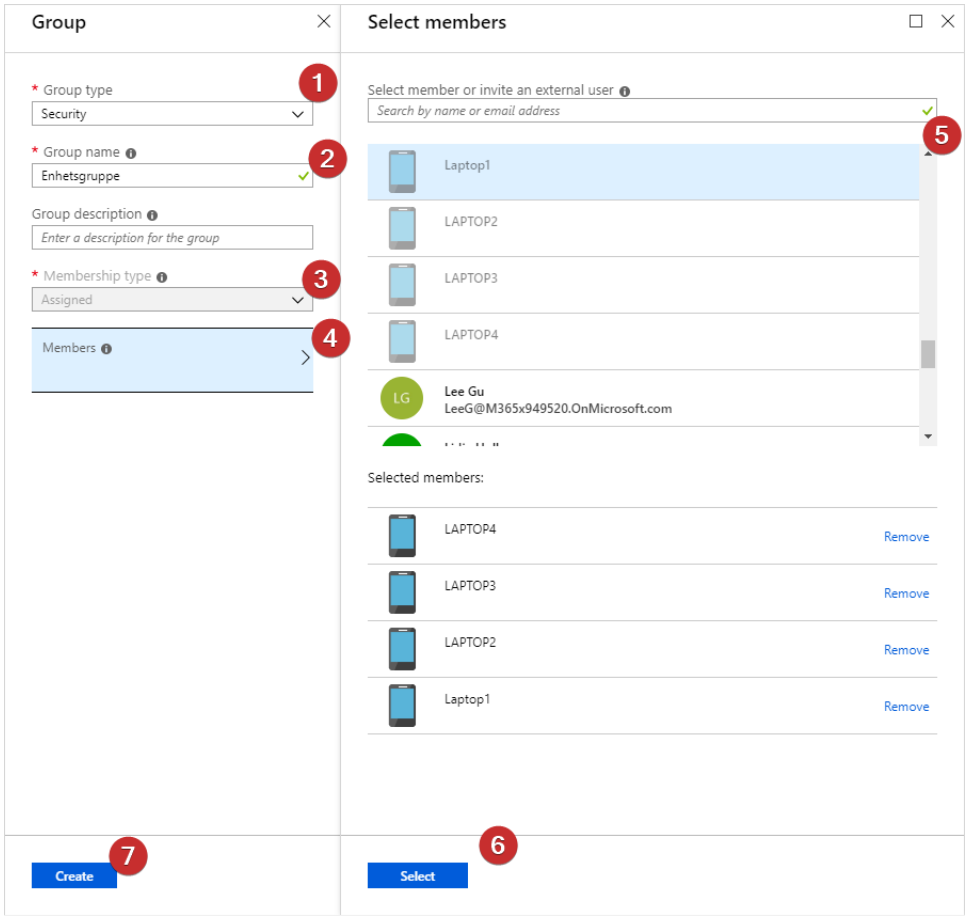
Inne i ***Groups*** oppretter du en ny gruppe, ved å trykke **New group**.



Figur 237: Opprette og tilordne bruker til en gruppe

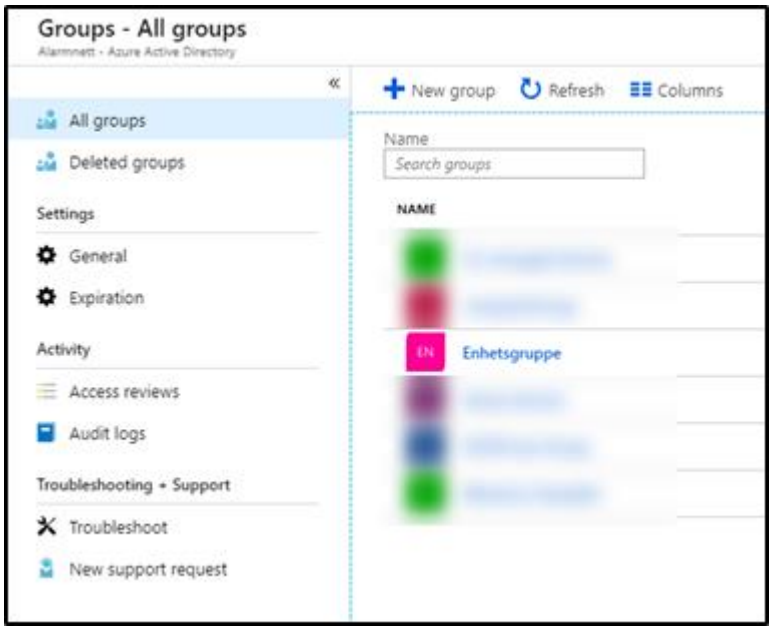
Her velger man Group type **Security group** – **navn på gruppen** og medlemstype **assigned**. Så trykker du på **Members**, siden vi har laget en gruppe for enheter så velger vi enhetene som skal være med.

Vi bekrefter valgene ved å trykke **Select** og så **Create**.



Figur 238: Opprette og tilordne bruker til en gruppe

Etter en liten stund vil du kunne se den nye gruppen din.



Figur 239: Opprette og tilordne bruker til en gruppe

Det er mulig å legge til eller fjerne brukere i etterkant ved å gå inn på gruppen trykke på **members**, trykke på de **tre prikkene** og så **remove** for å fjerne bruker. Det er også mulig å legge til bruker ved å trykke **add members** i samme vindu.

Figur 240: Opprette og tilordne bruker til en gruppe

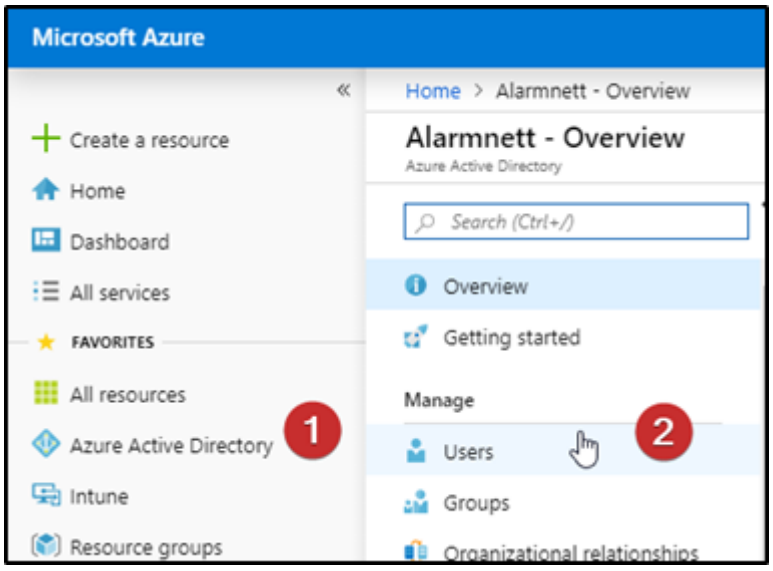
.

Tilordne lisenser

I Azure har man gjort det veldig enkelt å tilordne lisenser. Man kan tilordne lisenser til brukeren slik at lisensen slipper å være låst til en maskin. Dersom den maskinen skulle bli borte så vil ikke dette skape et problem, siden lisensen ligger på brukeren. Man kan raskt fjerne ressurser fra ansatte som slutter og tilordne det til nye ansatte. Det finnes flere metoder å tilordne lisenser til bruker på i Azure, men vi skal ta for oss to metoder.

Via bruker

Først kan vi ta for oss metoden hvor vi direkte går inn på brukeren for å legge til en lisens. Dette kan være hendig når man skal gjøre mange forskjellige endringer på brukeren og kan være hendig ved at du slipper å gå ut fra brukeren. Da kan vi starte med å navigere til brukere i Azure. Vi trykker på **Azure AD** – **Users**.

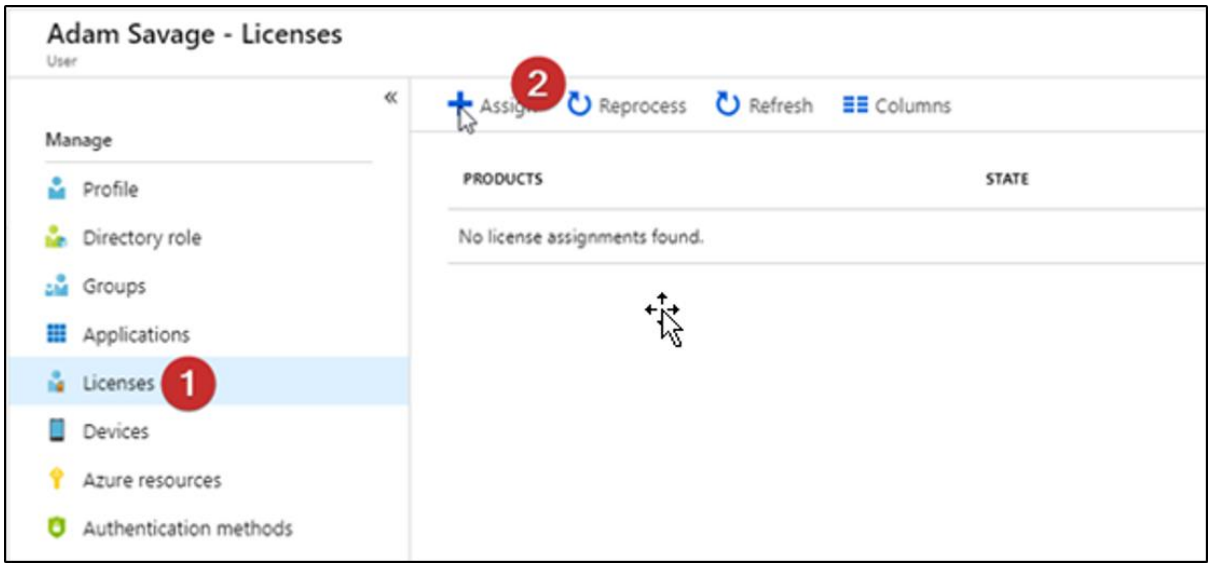


Figur 241: Tilordne lisenser

Trykker på det **blå navnet** til brukeren

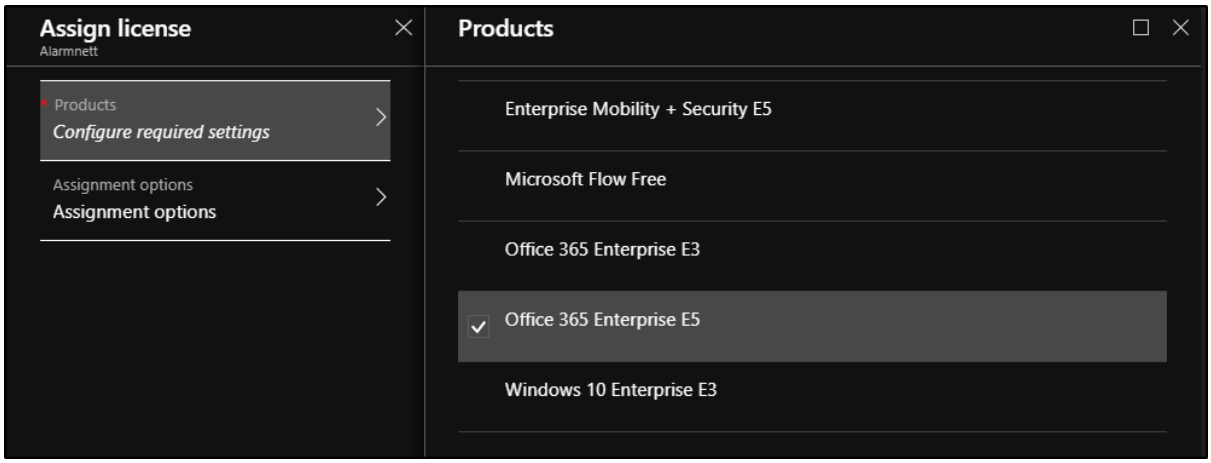
Figur 242: Tilordne lisenser

Her går vi til sidemenyen og finner fram til **Lisenser** – Trykker på **Assign** som vist på bildet.



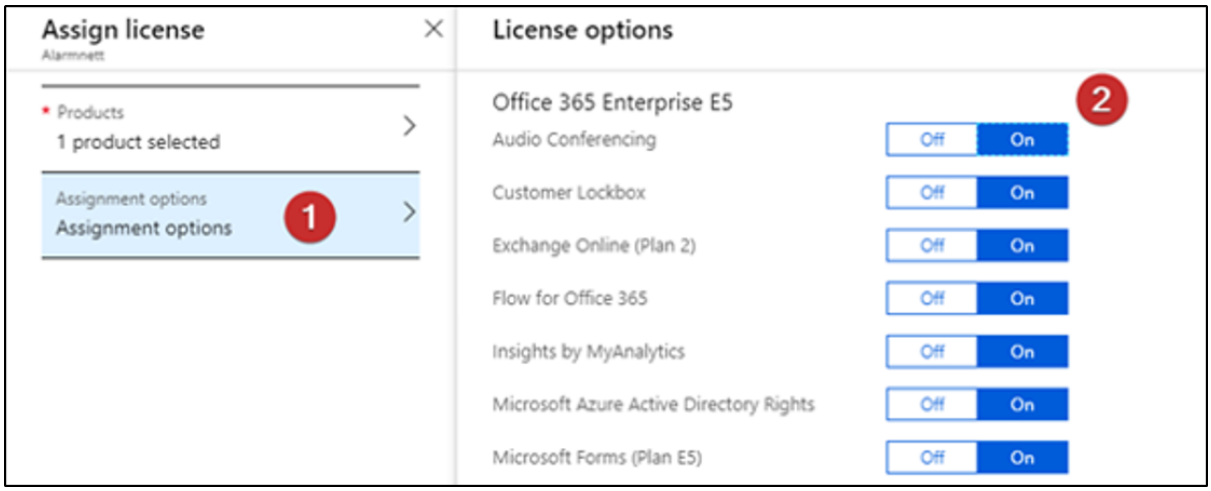
Figur 243: Tilordne lisenser

Nå har vi kommet til ***Assign license*** og her kan vi tilordne lisenser. Vi trykker på **Products** og velger hvilken lisens vi ønsker å tilordne.



Figur 244: Tilordne lisenser

Vi går så til ***Assignment options*** og velger hvilke tjenester brukeren skal ha tilgang til. I utgangspunktet er alle funksjoner slått på, så det er bedre å si at man kan velge hvilke funksjoner vi skal begrense brukeren tilgang til. Trykker så **OK** og så **assign**.

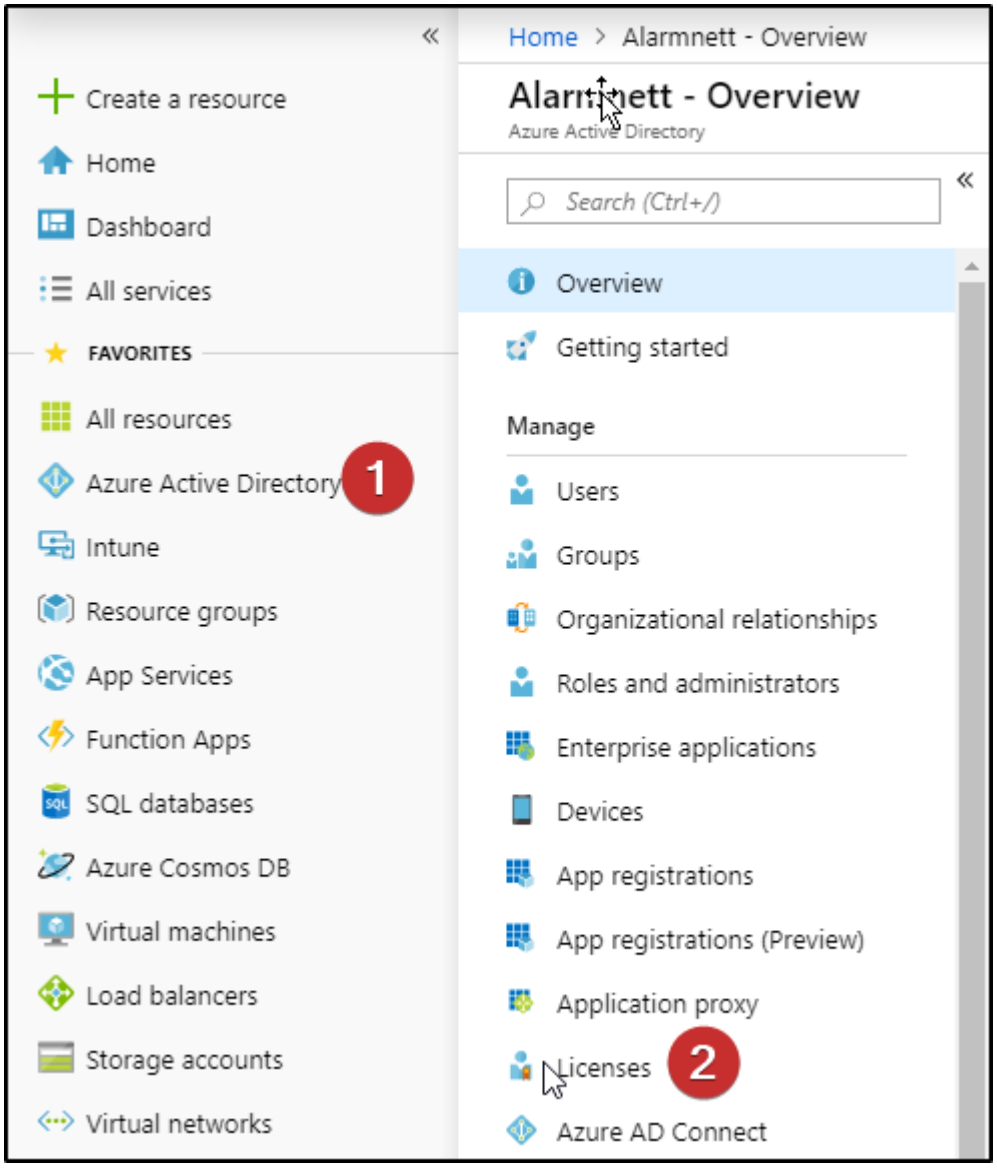


Figur 245: Tilordne lisenser

Via lisenser

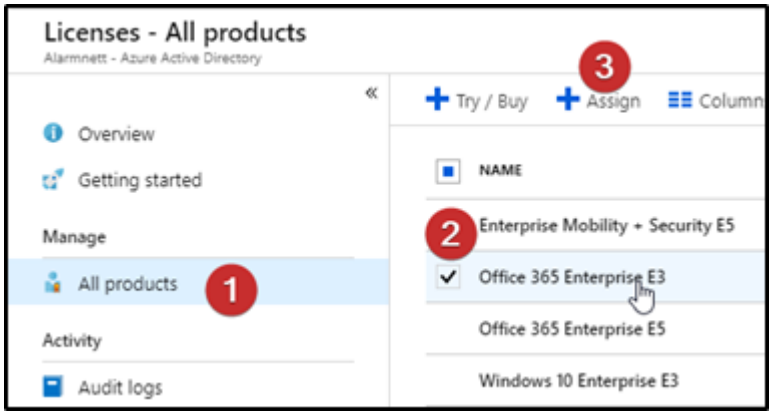
Den andre metoden vi skal vise frem er å tilordne lisenser via lisens-siden. Dette er den normale måten å tildele lisenser til brukere på, og brukes ofte når man har opprettet brukere på forhånd og deretter får lisenser. Man vil helst ikke gå inn på hver enkelt bruker for å legge til en og en lisens hvis man for eksempel har 300 lisenser man skal dele ut. Da er det greit å ha en side hvor man har oversikt over alle lisensene og raskt kan dele ut alle lisensene på en gang.

Da kan vi starte med å gå til ***Azure Active Directory – Licenses***



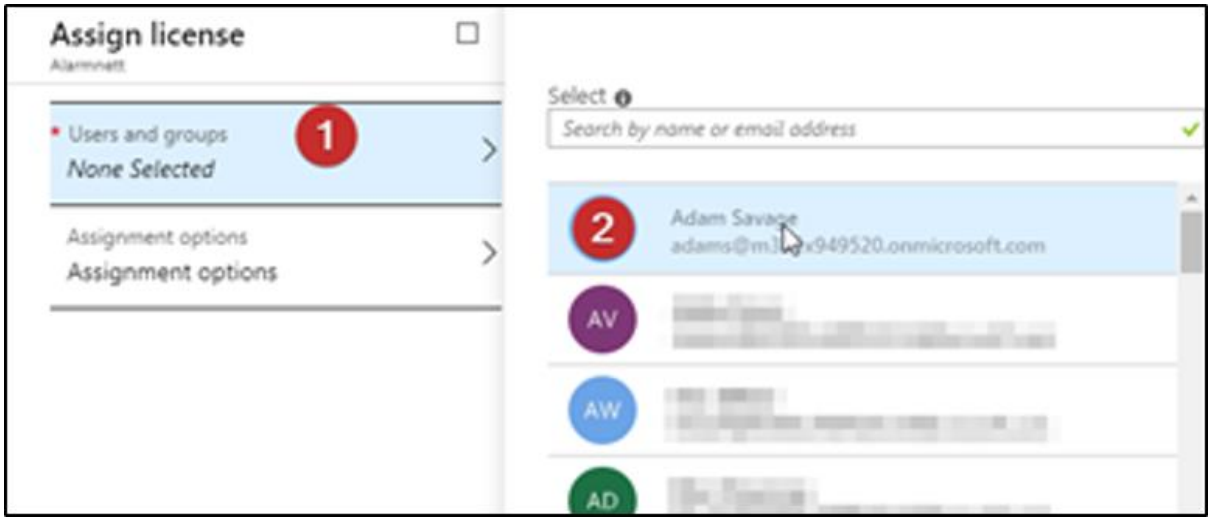
Figur 246: Tilordne lisenser

Vi havner da på oversiktssiden til lisenser. Her trykker vi på **all products** og velger den lisensen vi skal tilordne brukeren.



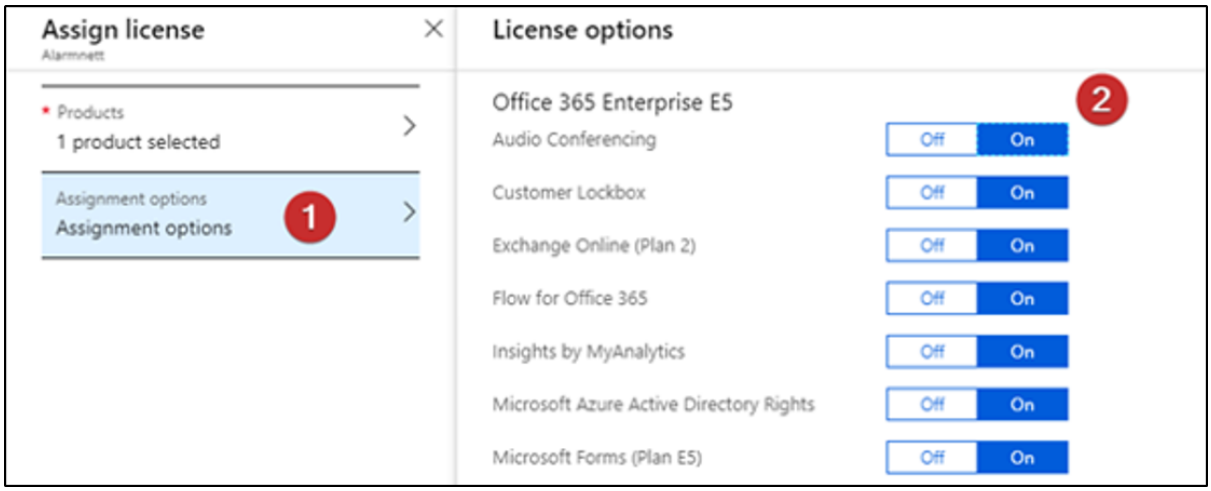
Figur 247: Tilordne lisenser

Her vil du få opp en lignende Assign license side som når du legger til lisens via bruker. Forskjellen her er at man kan legge til brukere, mens på den andre kan man legge til lisenstyper.



Figur 248: Tilordne lisenser

Vi går så til ***Assignment options*** og velger hvilke tjenester brukeren skal ha tilgang til. I utgangspunktet er alle funksjoner slått på, så det er bedre å si at man kan velge hvilke funksjoner vi skal begrense brukeren tilgang til. Trykker **OK** og **assign**.



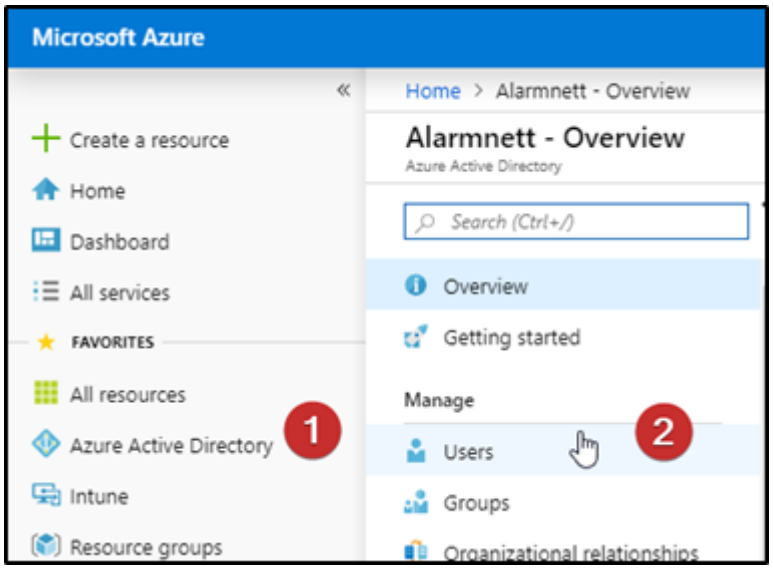
Figur 249: Tilordne lisenser

Endre eller fjerne lisenser

Vi kan like lett fjerne lisenser vi har tilordnet til brukerne. Dette kan være nødvendig når en bruker slutter i bedriften. Da er det viktig at de ikke får tilgang til bedriftens ressurser, slik at hemmeligheter og programmer ikke kommer på avveie. Dog per dags dato er det ikke noen måte å endre lisenser, som å begrense tilgang til tjenester i lisensene, til mange brukere på en gang. Dette er noe vi skulle ønsket å se mer av.

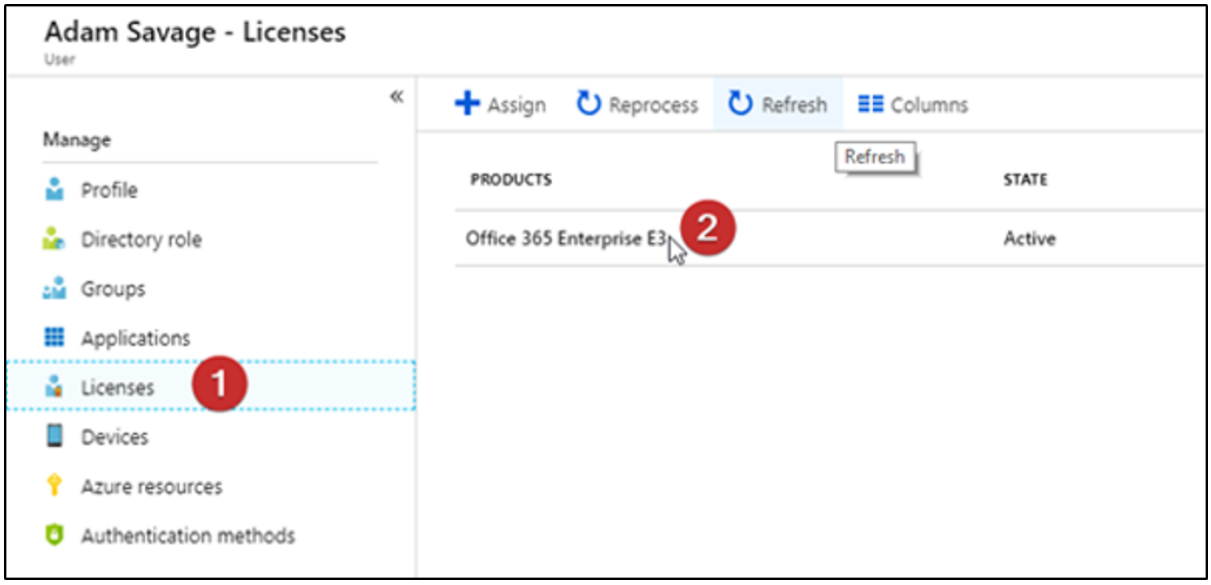
Via bruker

Vi kan endre eller fjerne lisenser under hver enkelt bruker. Dette kan være smart når en bruker har sluttet i avdelingen og man vil fjerne eller endre alle lisensene tilordnet brukeren. Dette er muligens også den raskeste måten å endre hvor mange funksjoner brukeren skal få fra lisensen. Da går vi først til brukeren via ***Azure AD*** – ***User***.



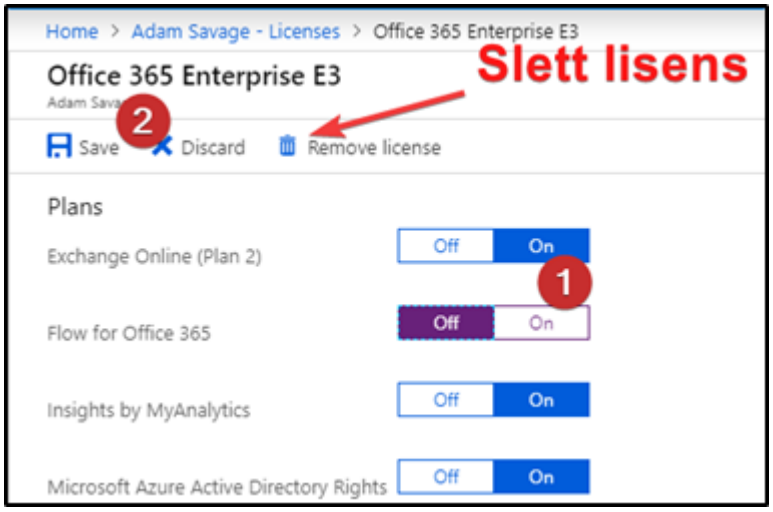
Figur 250: Endre eller fjerne lisenser

Under brukere har vi nå mulighet til å velge Lisenser. Da går vi til ***Licenses*** og velger deretter den lisensen vi vil fjerne. I vårt tilfelle er det **Office 365 Enterprise E3**



Figur 251: Endre eller fjerne lisenser

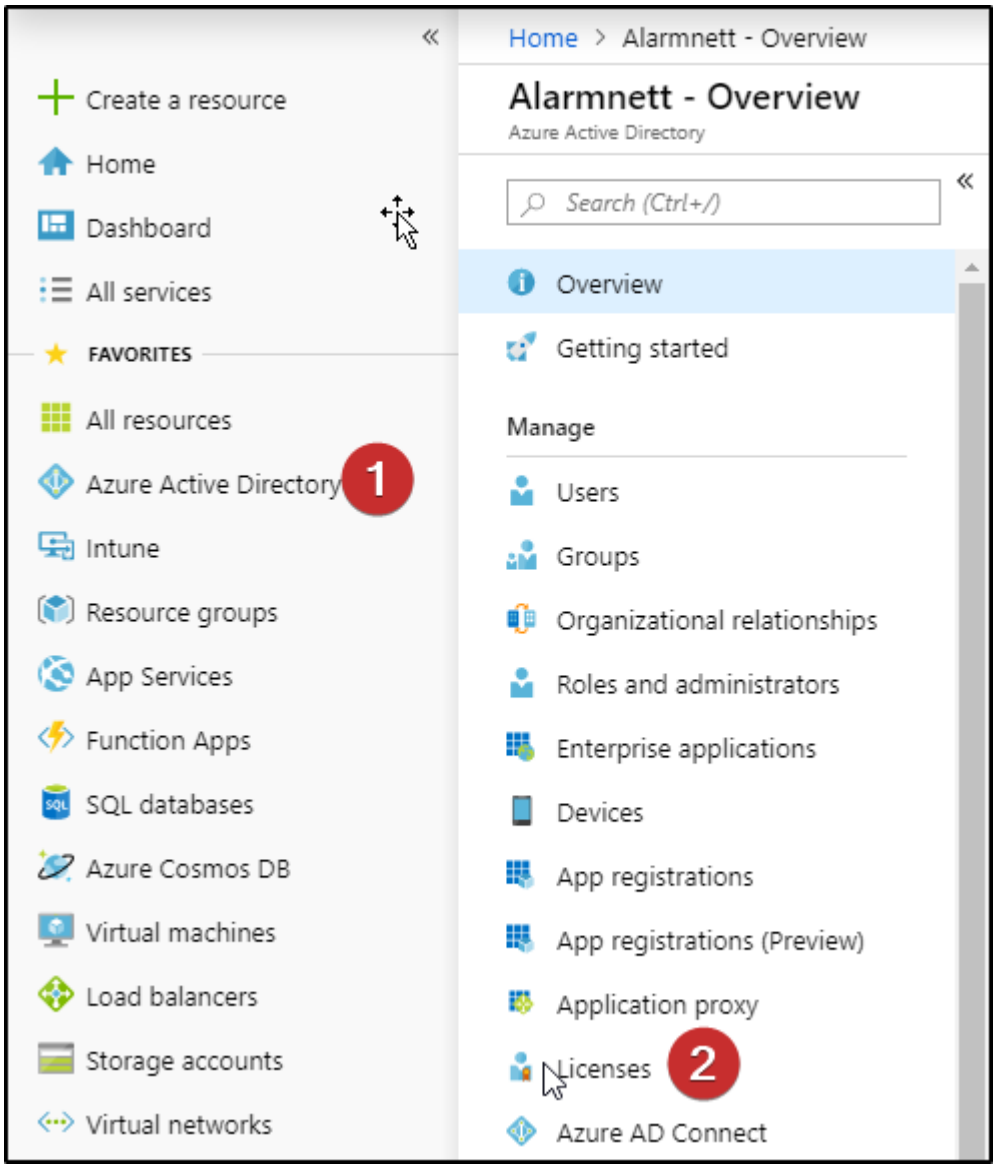
Inne på den enkelte lisensen kan vi så gjøre endringer som vi måtte ønske. Vi har da mulighet til å endre og lagre, eller å slette lisensen.



Figur 252: Endre eller fjerne lisenser

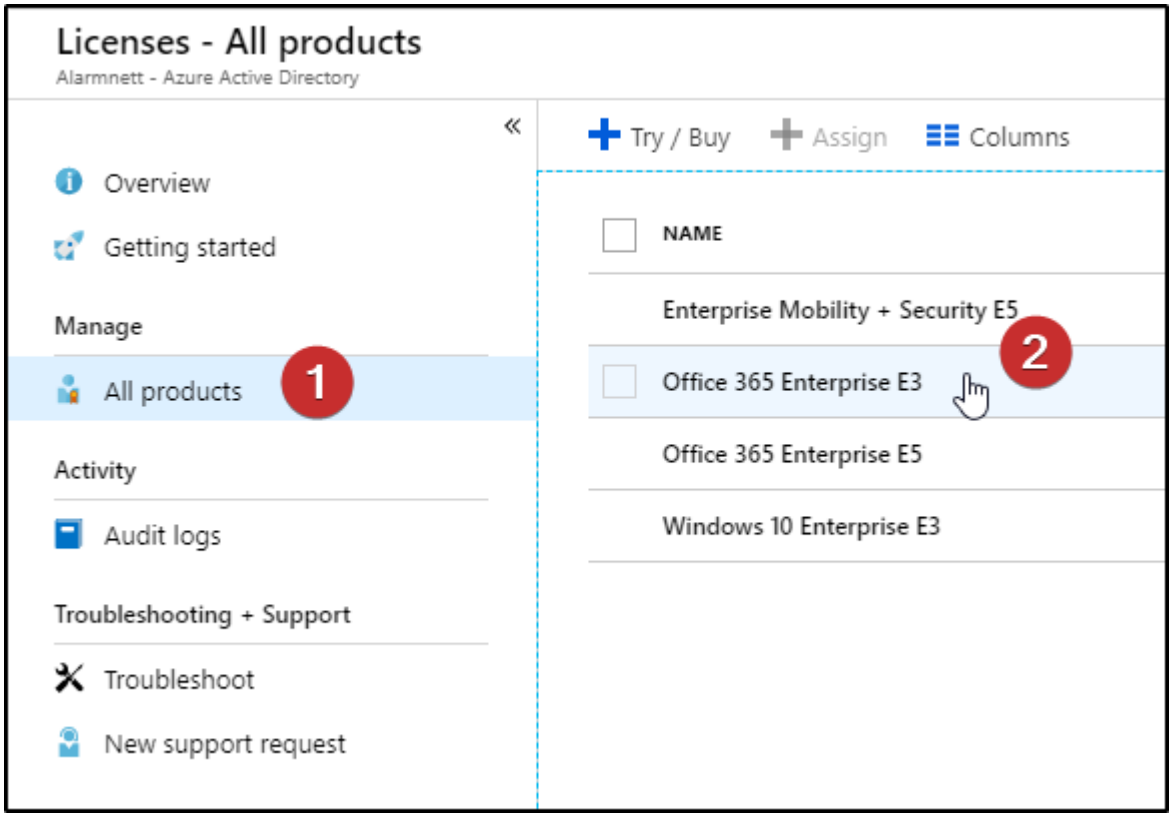
Via lisenser

Den andre måten vi kan fjerne lisenser på er ved å gå til oversikten over lisenser under Azure AD. Dette kan være smart når vi skal fjerne en lisens hos mange brukere. Da går vi først til **Azure AD** – **Licenses**.



Figur 253: Endre eller fjerne lisenser

Under ***Licenses*** vil vi trykke **All products** og produktet vi skal endre eller fjerne. I vårt tilfelle er det **Office 365 Enterprise E3.**



Figur 254: Endre eller fjerne lisenser

Her inne kan vi gjøre to ting: Fjerne lisens og endre lisens.

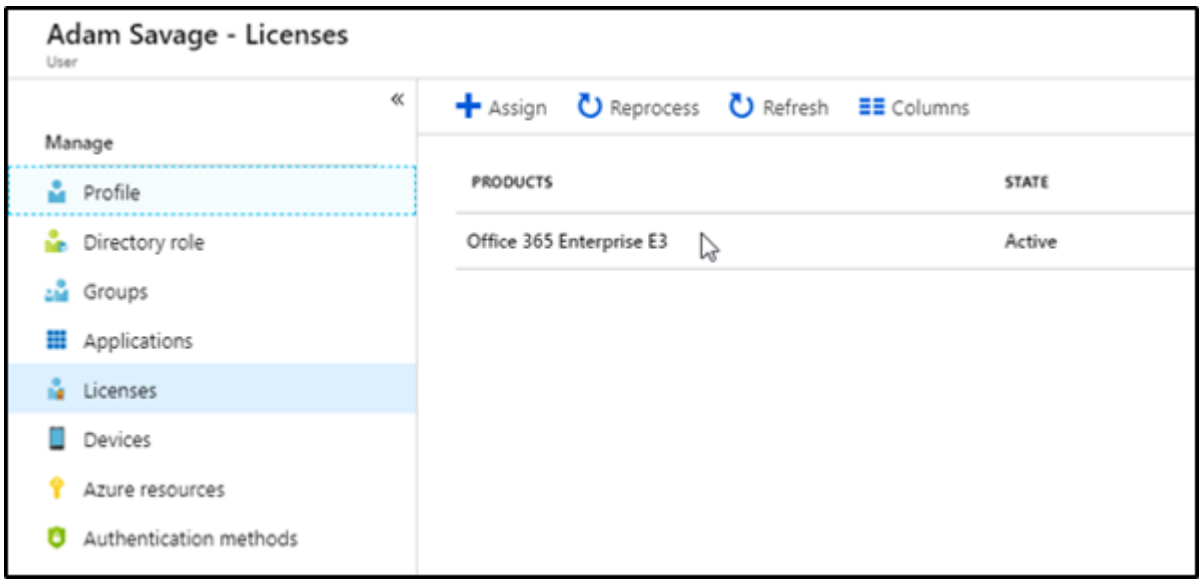
Vi starter med Fjerning av lisens. Da velger du brukere du skal fjerne lisensen fra ved å huke av til venstre for navnet deres, som vist på bildet under. Trykk så på **Remove License**.

Figur 255: Endre eller fjerne lisenser

For å endre lisens kan vi trykke på **navnet** til brukeren, som vist under.

Figur 256: Endre eller fjerne lisenser

Da vil vi komme til oversikten over lisenser for brukeren og kan enkelt velge lisensen vi vil endre på.

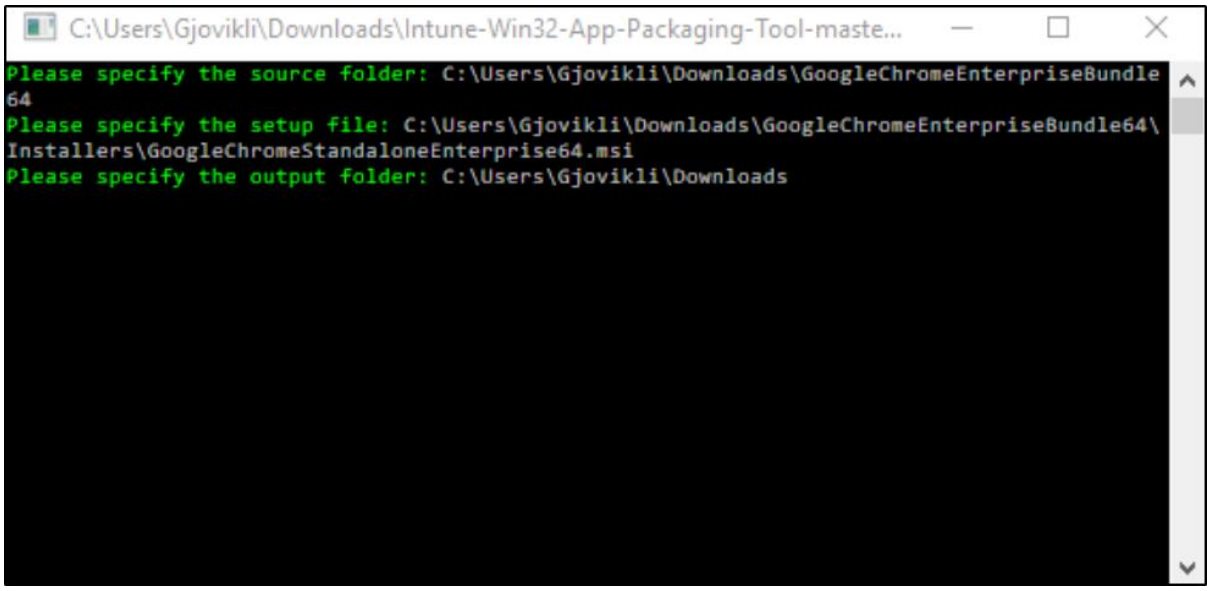


Figur 257: Endre eller fjerne lisenser

Forslag til utbedring: Det hadde vært mer hendig å direkte kommet inn på selve lisensen vi trykket på, siden vi allerede kom fra en spesifikk lisens, men det får bare bli et forslag fra vår side for nå.

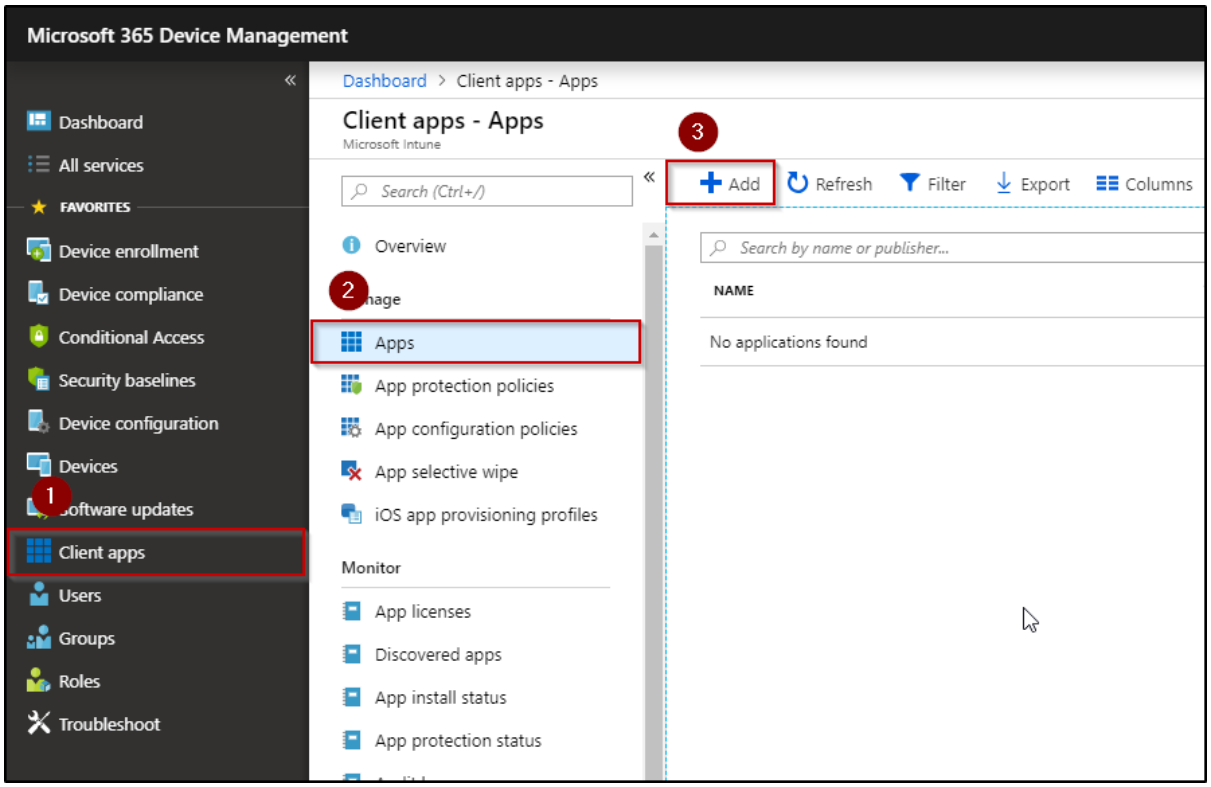
Software Deployment i Intune

Vi skal nå se på hvordan vi ruller ut programvare til maskiner som er administrert av Intune. Før vi kan rulle ut programvare, er vi nødt til å opprette en .WIM-fil (Windows Imaging Format). Denne filtypen er den Microsoft bruker for blant annet utrulling av programvare i Intune. WIM-filen opprettes ved å bruke et program som heter «Intune Application Packaging Tool». Man laster ned programmet som man ønsker å rulle ut til maskinene og spesifiserer, hvor source mappen, setup-filen og hvor output-mappen skal ligge, som vist i skjermbildet nedenfor.



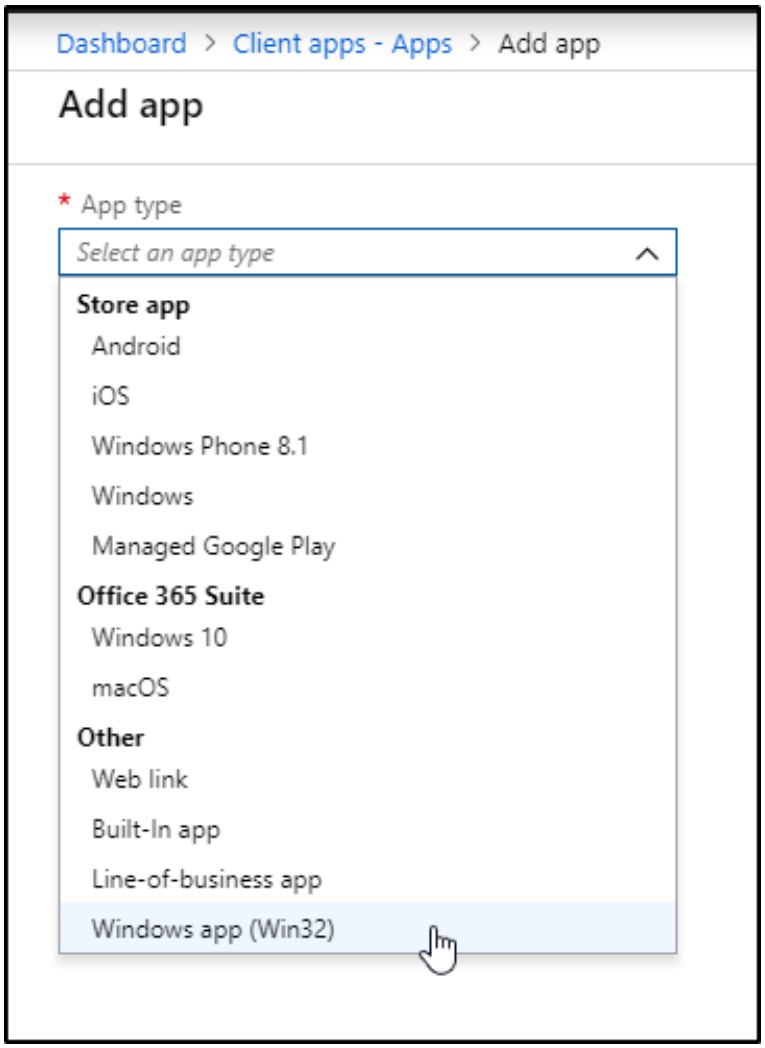
Figur 258: Software Deployment i Intune

Velger **Add** i Intune for å opprette en ny applikasjon.



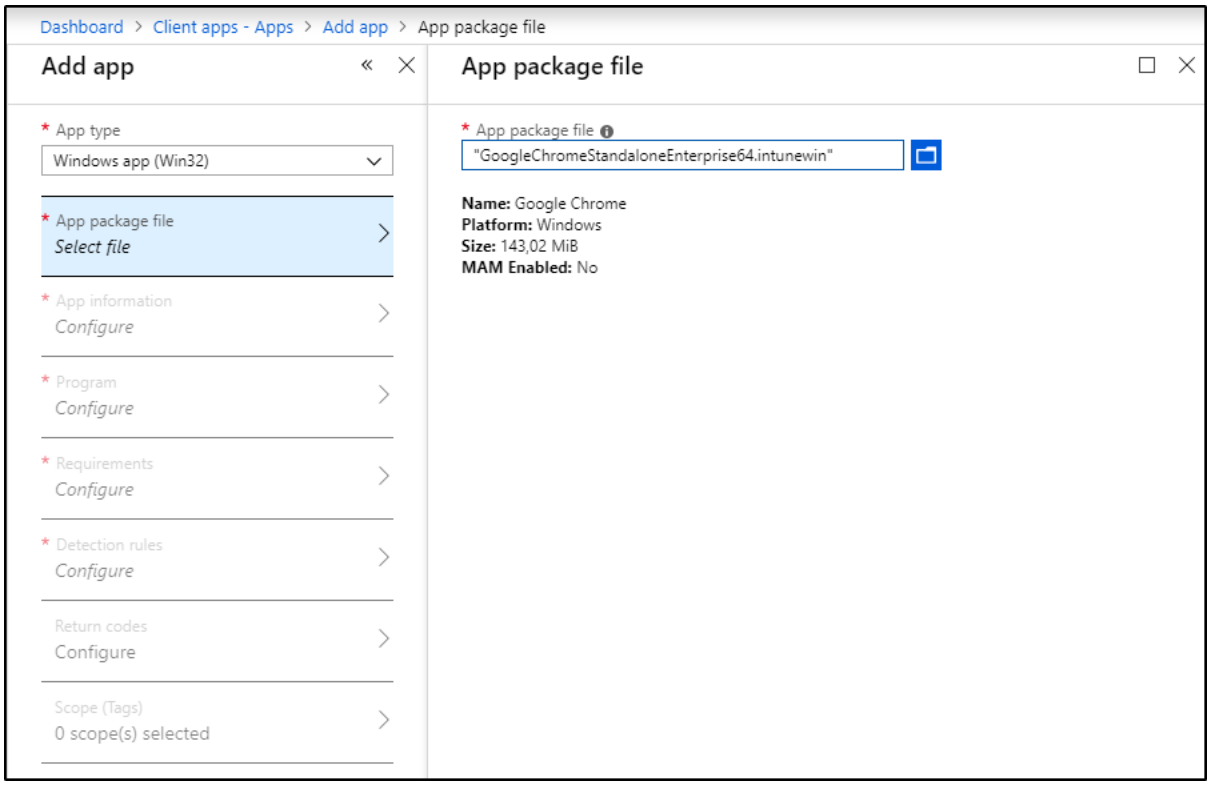
Figur 259: Software Deployment i Intune

Velger applikasjonstype.



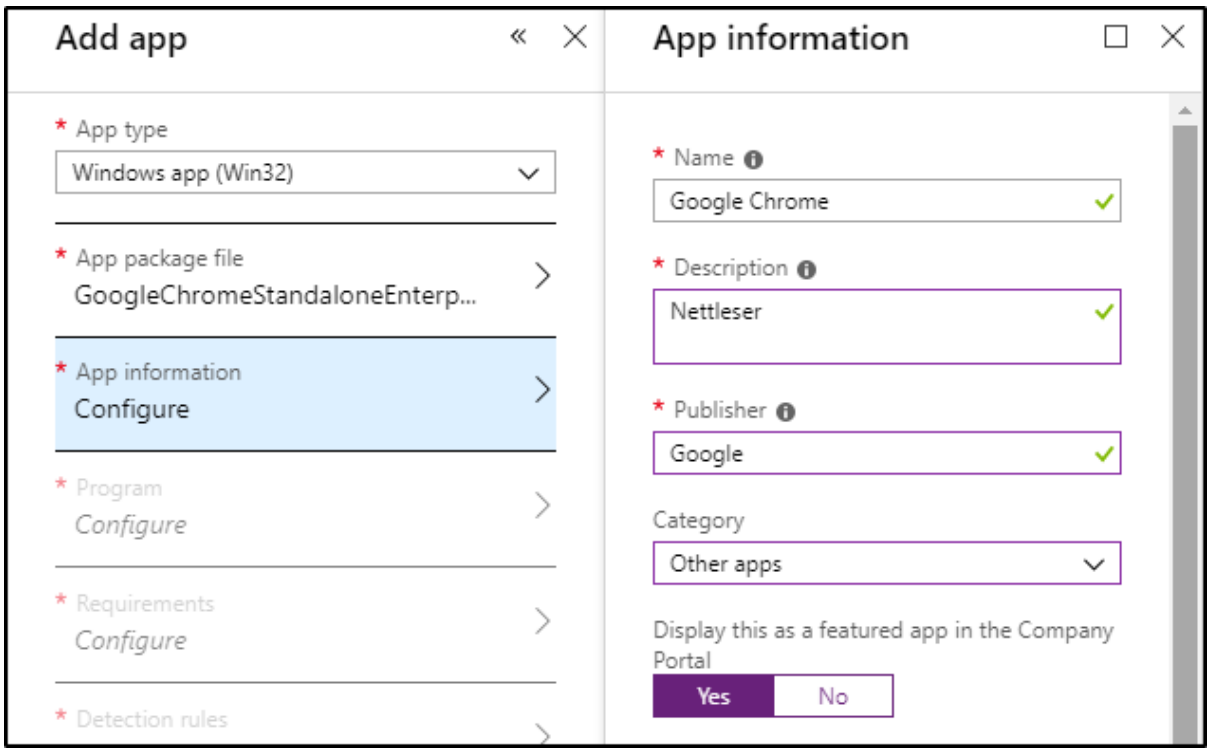
Figur 260: Software Deployment i Intune

Velger WIM-filen som vi opprettet.



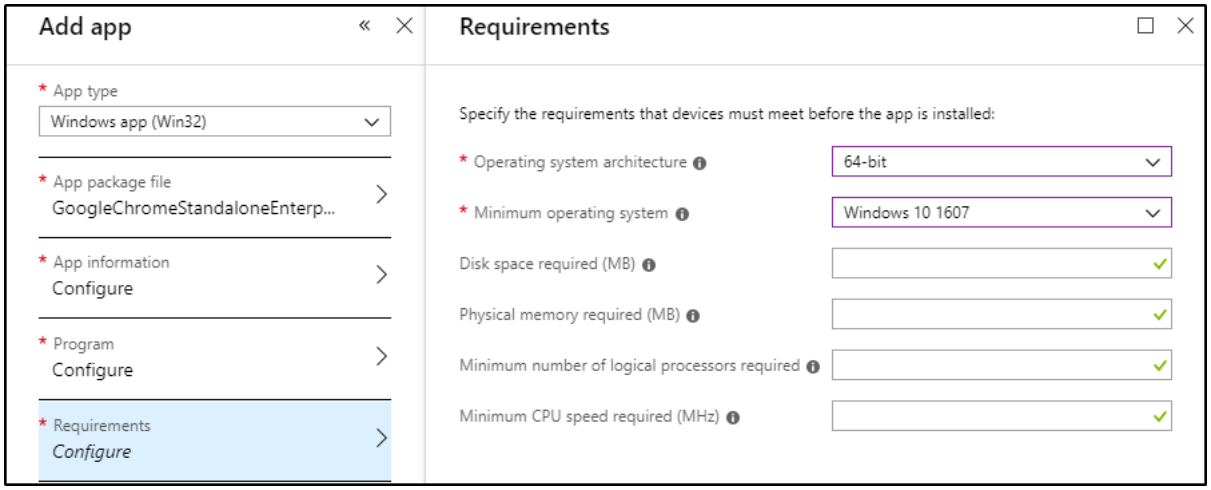
Figur 261: Software Deployment i Intune

Legger inn informasjon om applikasjonen.

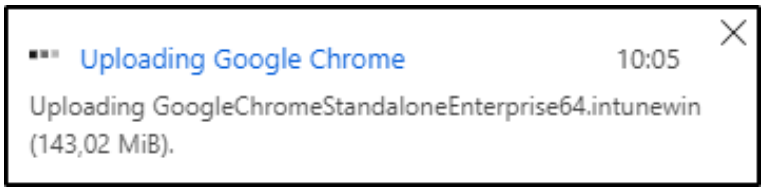


Figur 262: Software Deployment i Intune

Setter requirements.

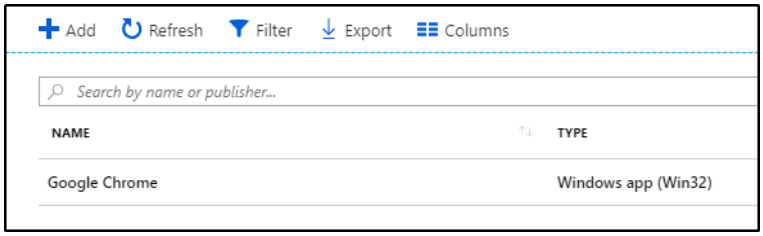


Figur 263: Software Deployment i Intune



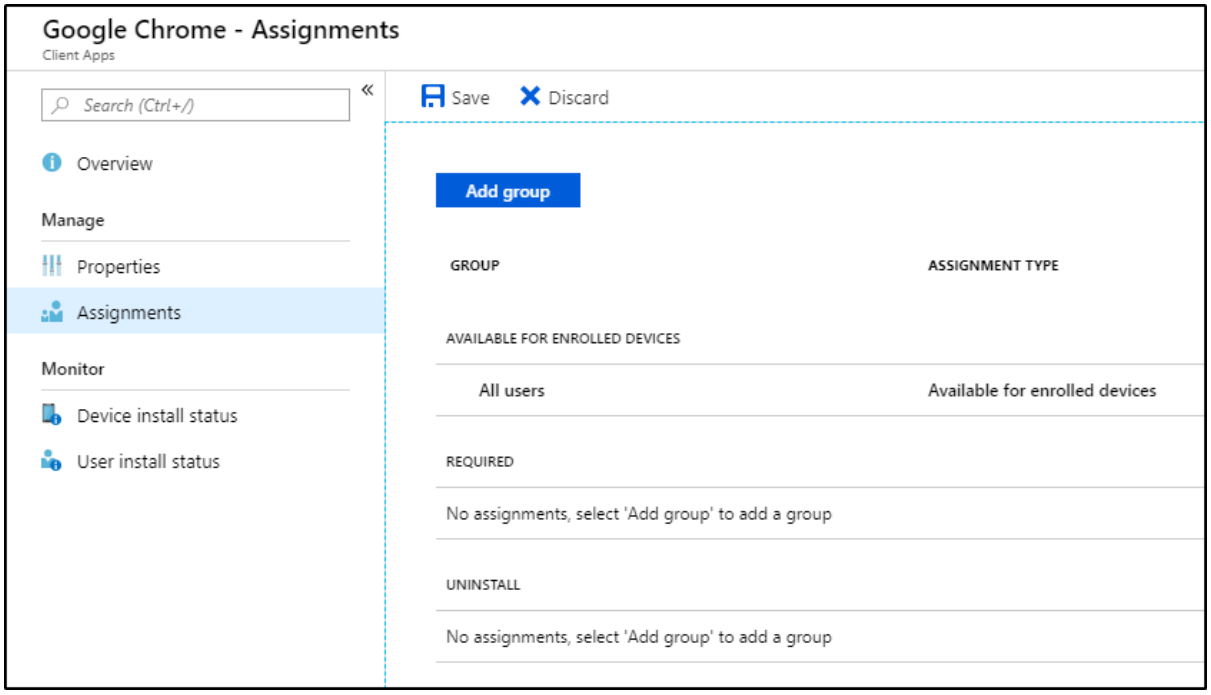
Figur 264: Software Deployment i Intune

Når Applikasjonen er lagt til i Intune, vil man se at den dukker opp under Apps.



Figur 265: Software Deployment i Intune

Hvis man navigere seg til ***Assignments***, kan man legge til grupper av maskiner eller brukere som skal ha denne applikasjonen.

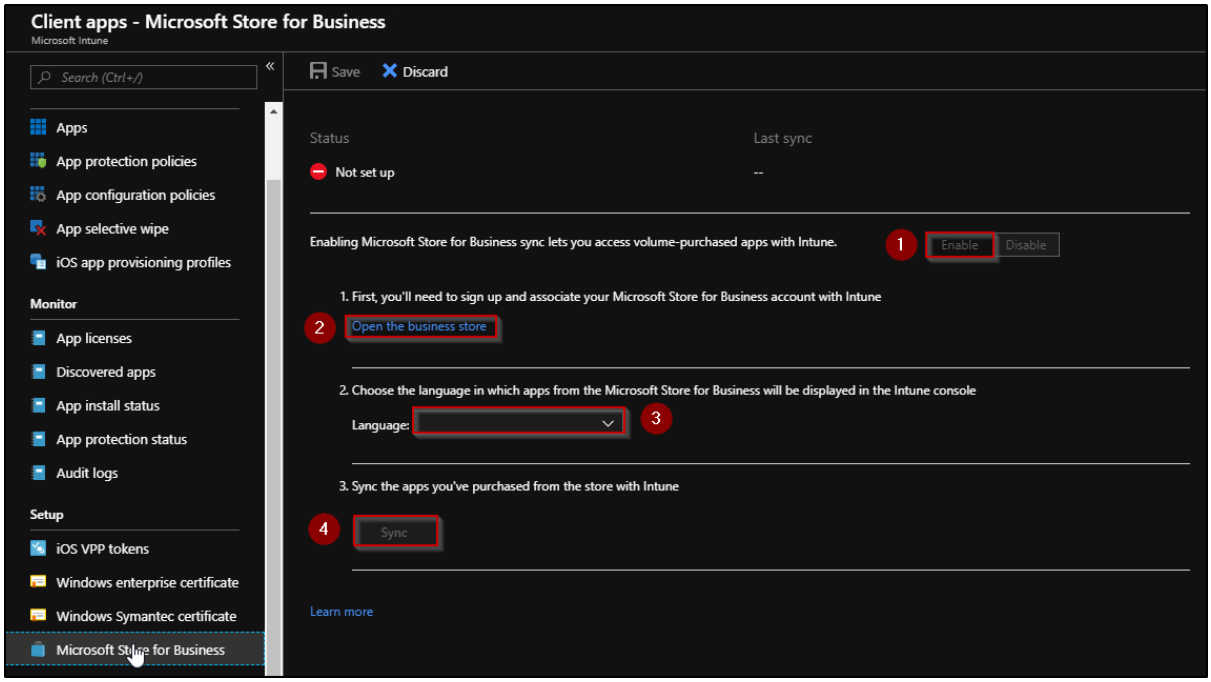


Figur 266: Software Deployment i Intune

Microsoft Store for Business

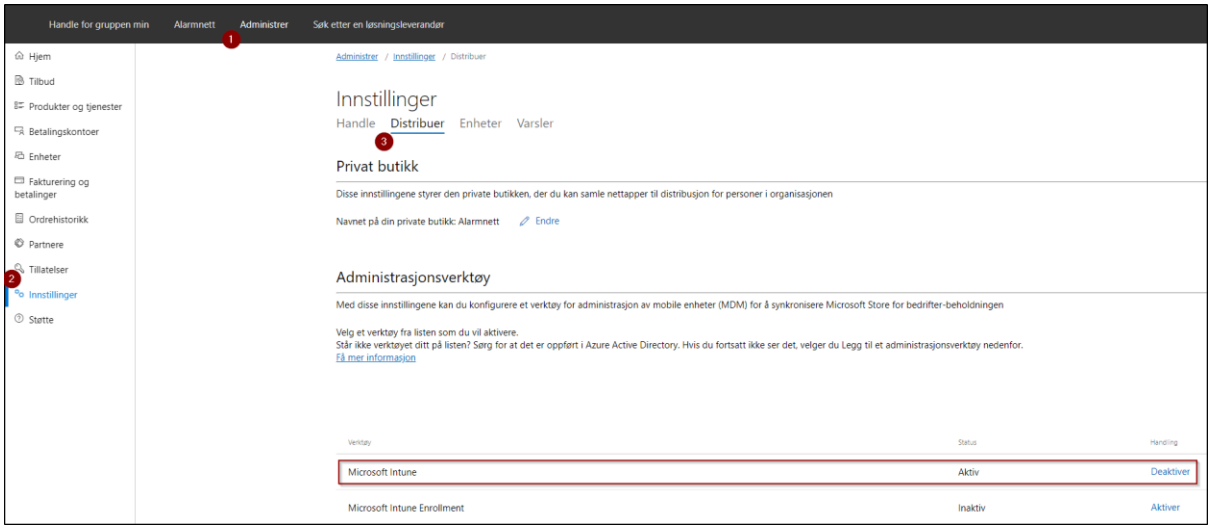
Vi kom bort i et problem, hvor vi ønsket gjøre det enklere for de ansatte i Alarmnett å ta i bruk applikasjonskatalogen til Intune (Company Portal). For å få tak i applikasjonskatalogen, var de ansatte nødt til å laste den ned på egen hånd. Vi så for oss at dette ville sannsynlig bli et problem for enkelte ansatte med begrensede datakunnskaper. Vi tenkte derfor at det ville være lurt å installere applikasjonskatalogen automatisk, så lenge maskinene deres var administrert av Intune og det er her problemet oppsto. Det var ikke mulig ved vanlig oppsett av applikasjon og sette «required» altså å rulle ut applikasjonen automatisk uten brukerens samtykke, på applikasjon fra Microsoft Store. Vi måtte derfor ty til løsningen som vi viser til nedenfor.

Vi navigerer oss til ***Client apps - Microsoft Store for Business*** og setter opp innstillingene som vist i skjermbildet nedenfor.



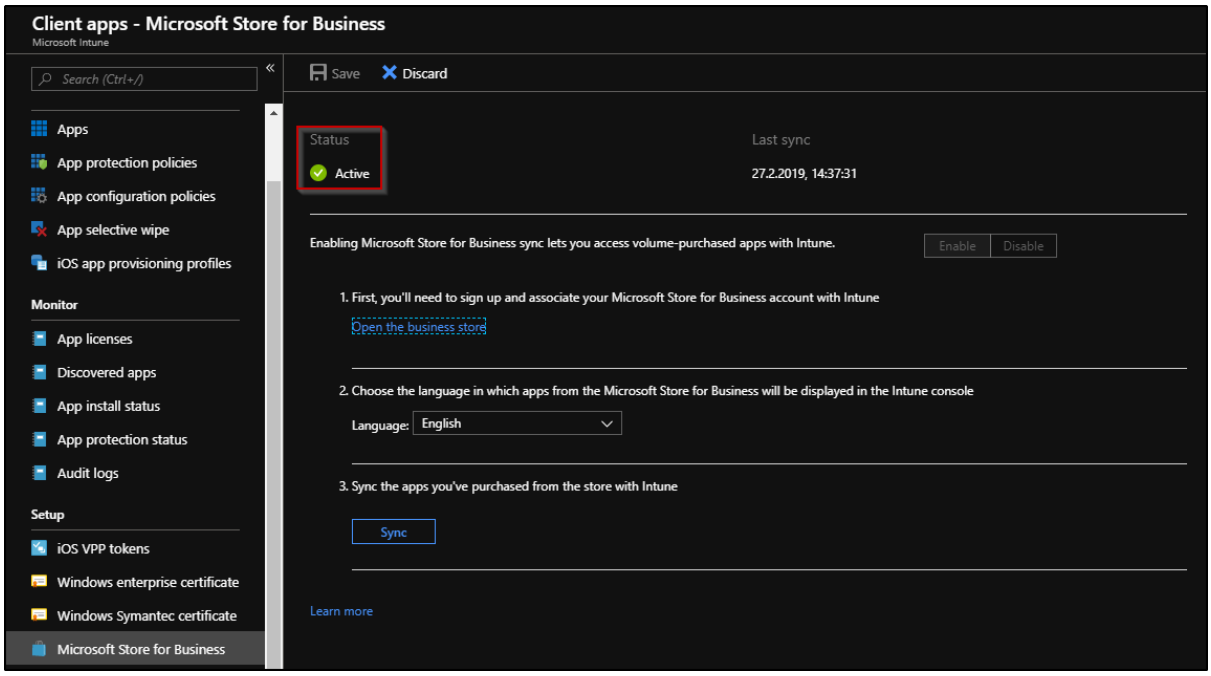
Figur 267: Microsoft Store for Business

Se til å aktivere Microsoft Intune ved å navigere seg til ***Alarmnett – Innstillinger – Distribuer***, og deretter trykke **Aktiver**.



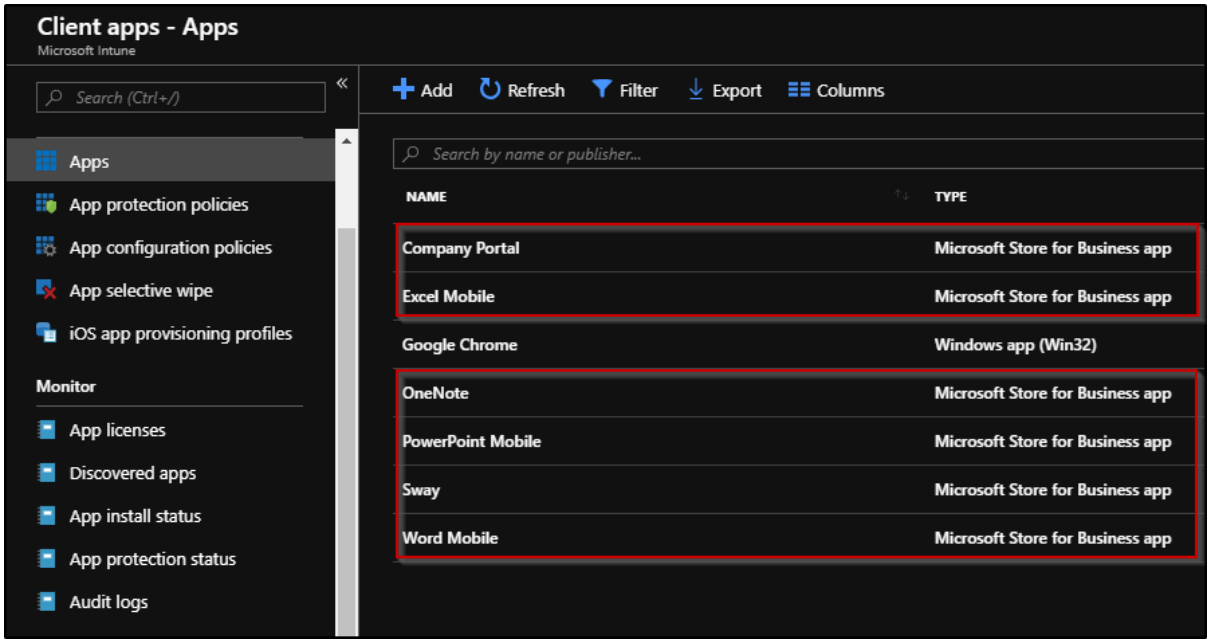
Figur 268: Microsoft Store for Business

Vi ser her at den nå har blitt satt til «Active».



Figur 269: Microsoft Store for Business

Under ***Apps*** har vi nå fått opp samtlige applikasjoner i applikasjonskatalogen som ble synkronisert i starten av dette kapittelet. Nedenfor kan man se disse applikasjonen, samt Company Portal som vi ønsker å installere. Ved å ta i bruk denne metoden kan vi nå sette denne applikasjonen til **required** og rulle den ut til samtlige brukere.



Figur 270: Microsoft Store for Business

Windows Autopilot

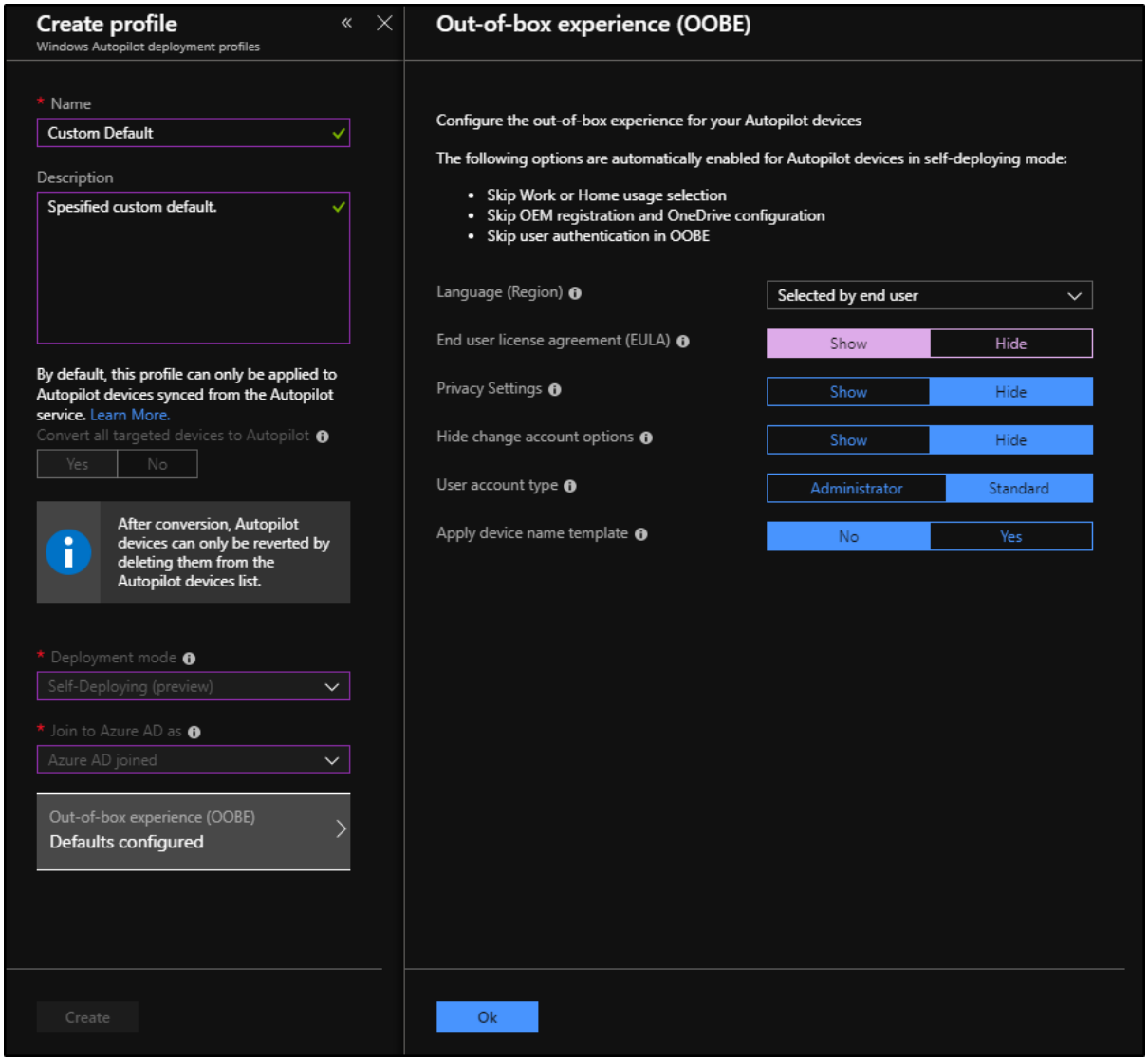
Windows Autopilot gir mulighet for automatisk innrulling av enheter til domenet, når en mobil enhet blir sendt ut fra leverandør til sluttbruker. Windows Autopilot kan også brukes for å oppdatere operativsystemet på eldre maskiner i en bedrift. Denne funksjonen kan på mange måter sammenlignes med muligheten for OSD (Operating system deployment) og innmelding av enheter til domene ved bruk av Task Sequence, som vi er kjent med fra SCCM. Vi skal nå stegvis sette opp det vi trenger for å ta i bruk Windows Autopilot, og tilslutt demonstrere innrulling.

Windows Autopilot Deployment Profile

Vi lager en deployment profile slik at maskinene følger et satt oppsett når de skal reinstalleres. Det er viktig at de tilordnes en profil før de skal rulles inn i Intune.
Det er mulig å sette to forskjellige deployment modes, Self-deployment eller User driven. Forskjellen er at man under Self-deployment vil kunne på forhånd sette innstillinger som region og tastaturspråk, mens man under User driven må sette alle innstillinger selv under installasjonen. Det skal nevnes at Self-deployment krever en enhet med TPM 2.0, som er en krypterings chip på maskinen som håndterer krypteringskoder for enheten, for ting som for eksempel autentisering. Til å begynne med hadde vi vanskeligheter med å teste denne funksjonen, men fant ut at man kan skru på TPM 2.0 på virtuelle maskiner under innstillingene til maskinen i Hyper-V. Husk å slå av maskinen før innstillingene skal endres.

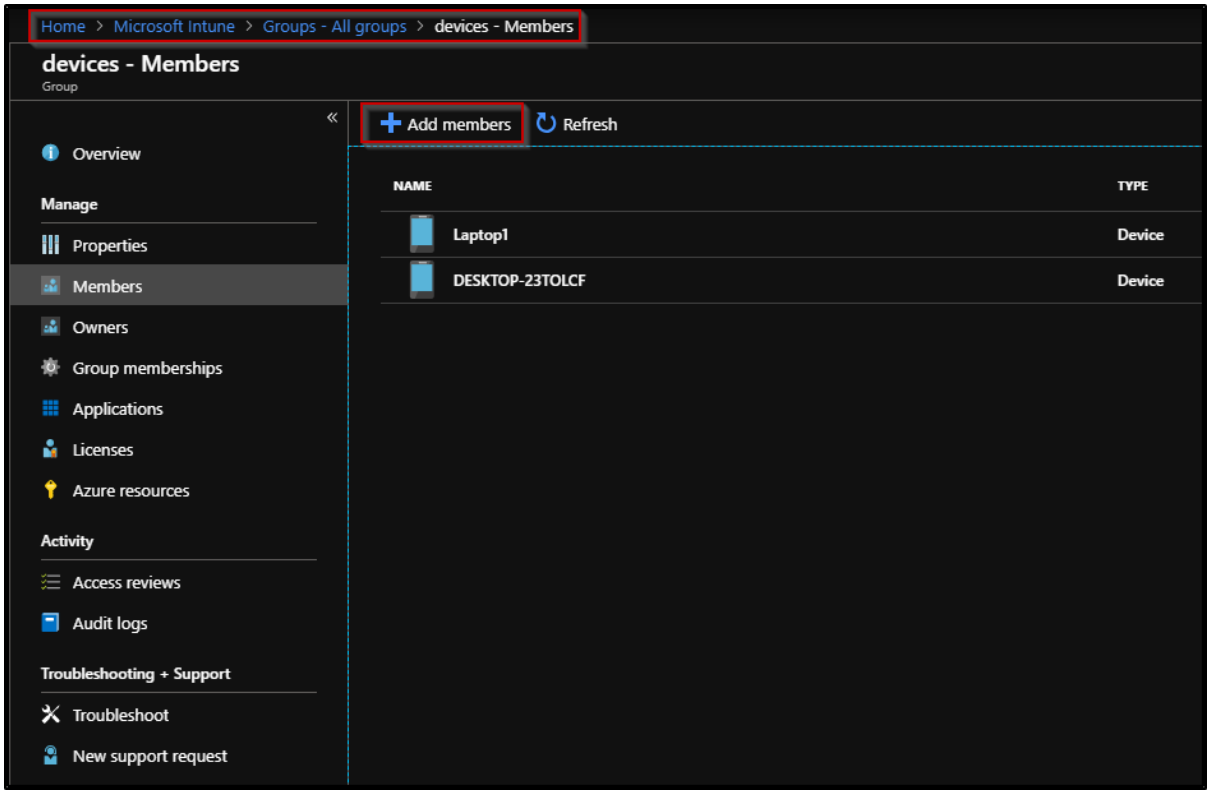
Oppsett av Deployment profile

Under Create profile kan vi gi profilen et navn og en passende beskrivelse. For å bedre passe til alle enheter kan vi velge **User driven** under Deployment mode. Vi har satt Self-deployment for å teste innstillingen mot enheter med TPM 2.0, ellers kan vi trykke **Yes** under convert all targeted devices to Autopilot. Til sist kan vi konfigurere OOBE, hvor vi kan sette opp språk, tastaturspråk og om vi skal vise diverse vilkår for bruk og betingelser. Trykker så **OK** og **Create** etter.



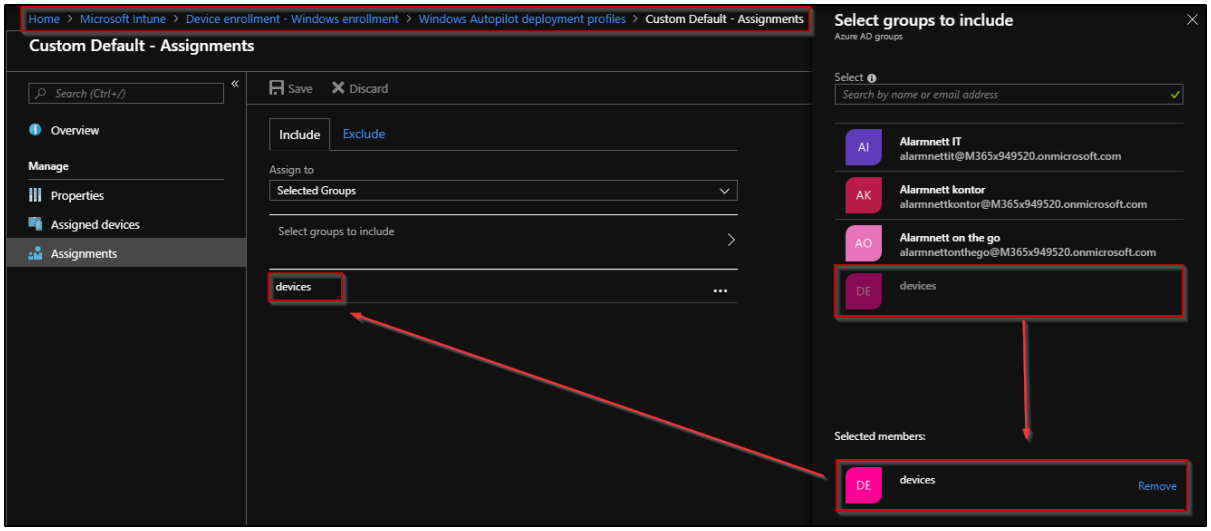
Figur 271: Windows Autopilot Deployment Profile

Vi navigerer oss til ***Microsoft Intune – Groups – All groups – Devices – Members*** og legger til medlemmer ved å trykke på **Add members**.



Figur 272: Windows Autopilot Deployment Profile

Nå som vi har selve deployment-profilen og lagt til enheter i gruppen, kan vi tildele gruppen deployment-profilen, som vist nedenfor.

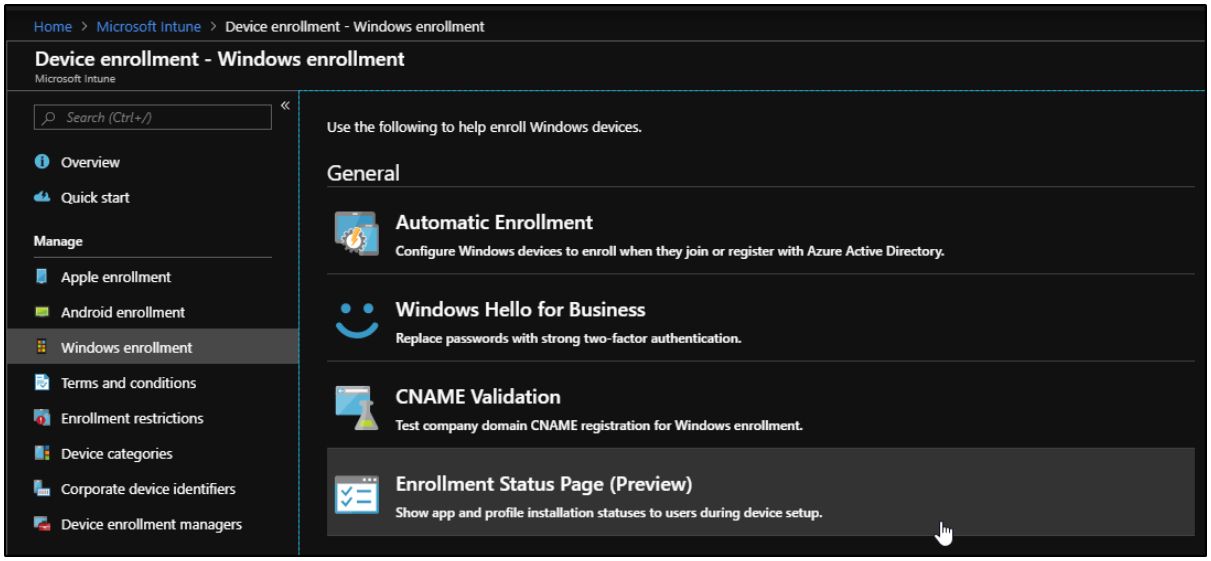


Figur 273: Windows Autopilot Deployment Profile

Enrollment Status Page

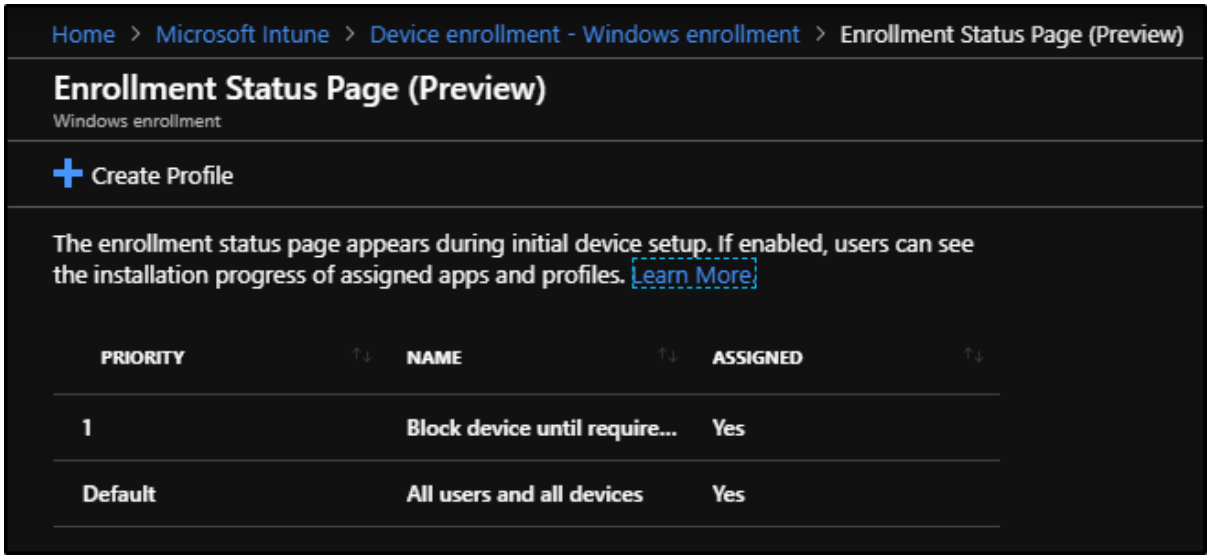
Vi skal nå se på hvordan vi kan sette opp en Enrollement Status Page Profile, for enheter under maskin-oppsett. Vi finner Enrollment Status Page, som en funksjon i Intune, under ***Microsoft Intune – Device Enrollment – Windows Enrollment***.

Vi starter med å trykke på **Enrollment Status Page (Preview)**.



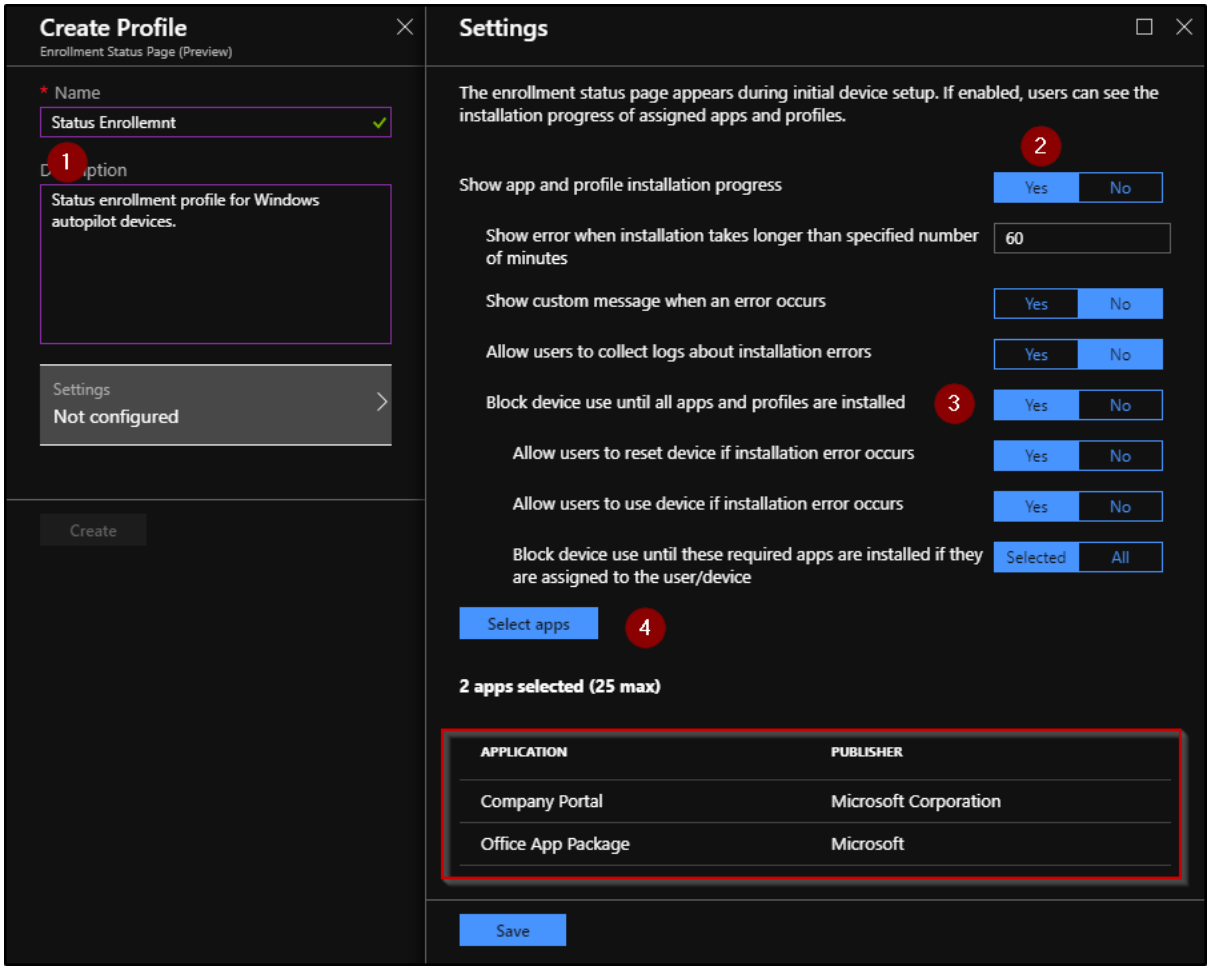
Figur 274: Enrollment Status Page

Velger deretter **Create Profile**.



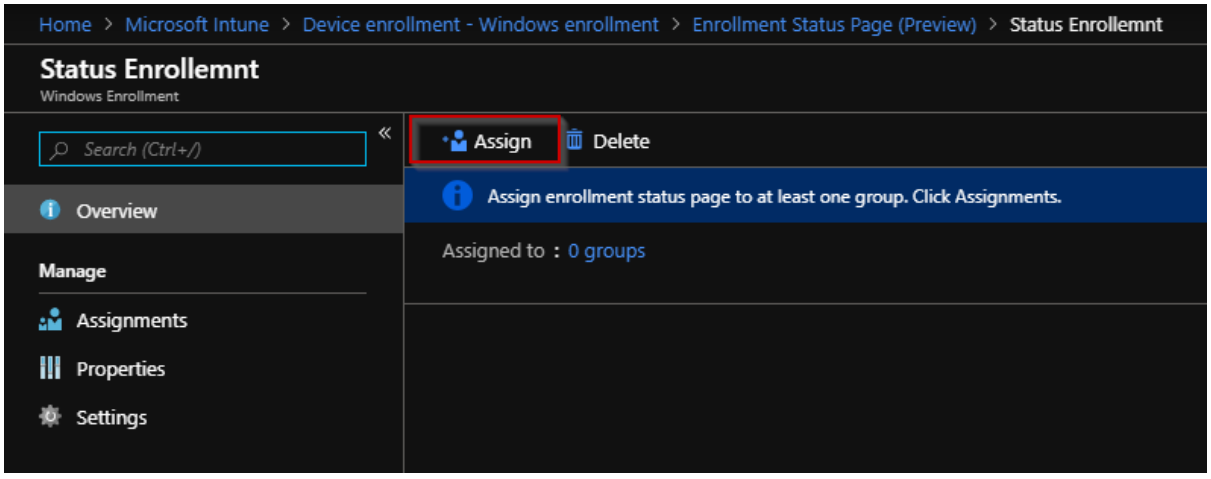
Figur 275: Enrollment Status Page

Legger til *Name*, og trykker på hvor det står **Not configured**. Deretter vil vi få opp skjermen som viser mange innstillinger. Her velger vi først å bytte til **Yes** (2), deretter å bytte til **Yes** (3), for så å trykke på knappen **Select apps**, hvor man da velger hvilke applikasjoner som skal være installert før brukeren får tilgang til maskinen sin. Trykker deretter på **Save**.



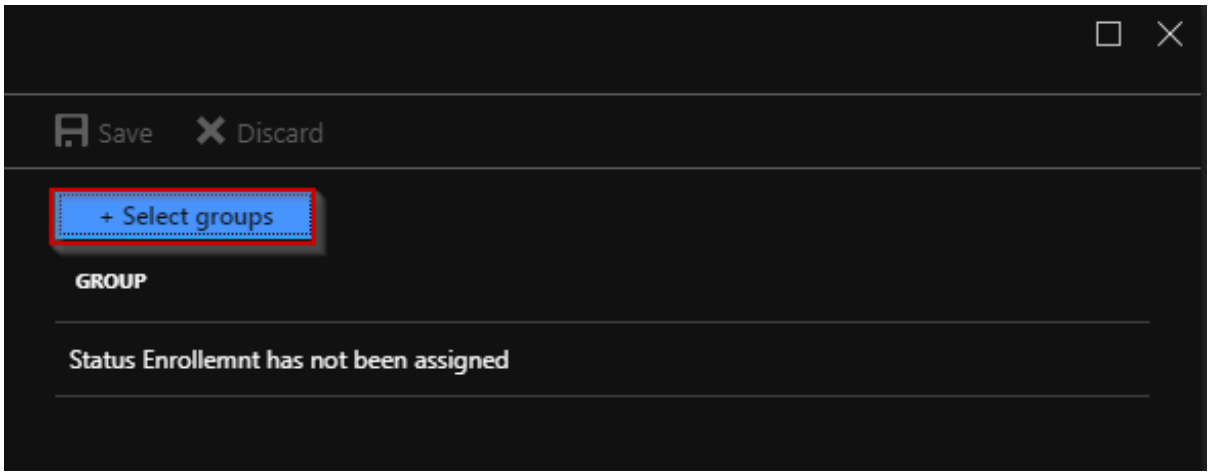
Figur 276: Enrollment Status Page

Når profilen er laget, velger man **Assign**, for å tildele profilen til en gruppe med enheter.



Figur 277: Enrollment Status Page

Velger **Select groups**.

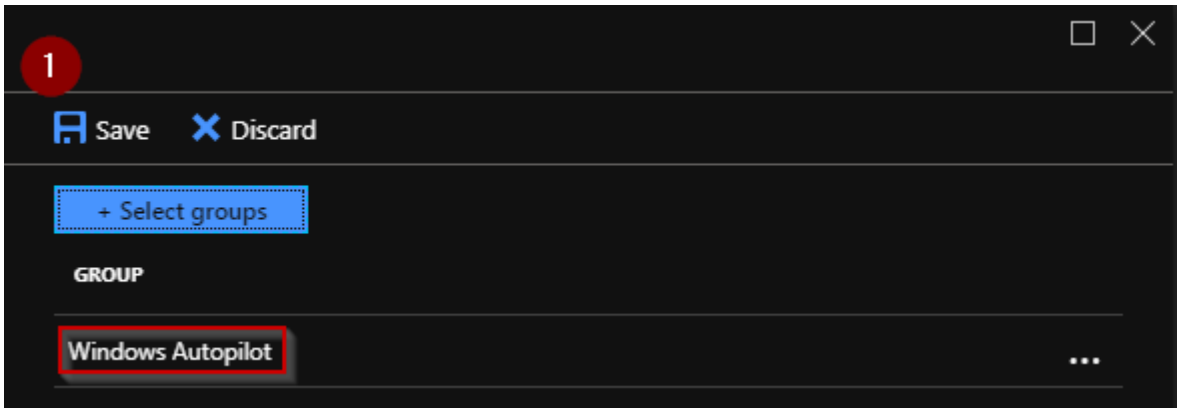


Figur 278: Enrollment Status Page

Velger en gruppe som vi ønsker å tildele profilen til.

Figur 279: Enrollment Status Page

Vi ser her at gruppen har blitt lagt til og vi trykker **Save**.

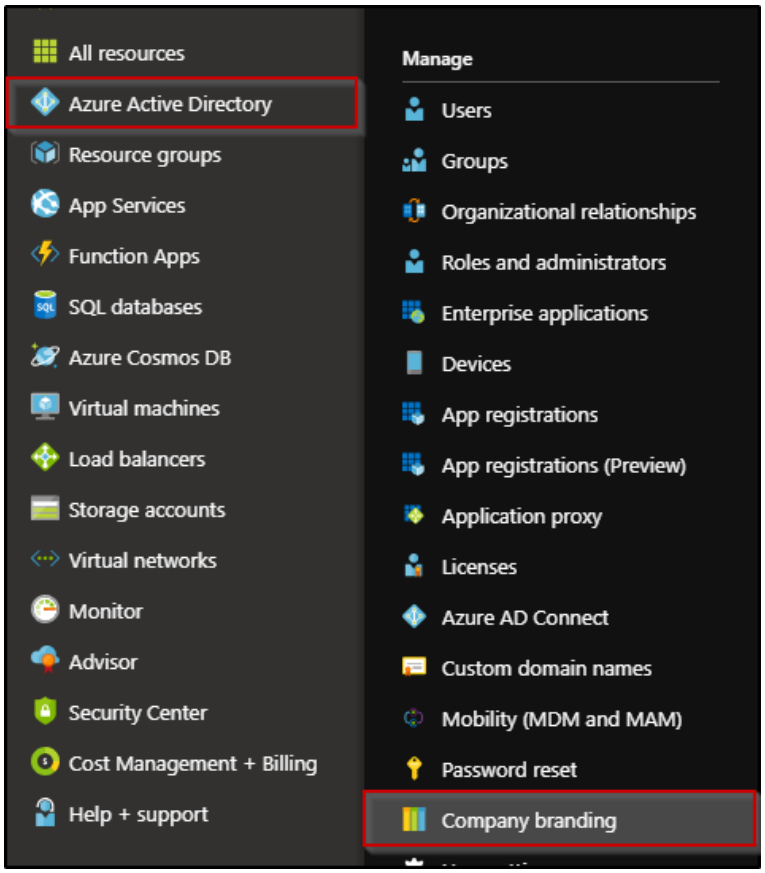


Figur 280: Enrollment Status Page

Company Branding

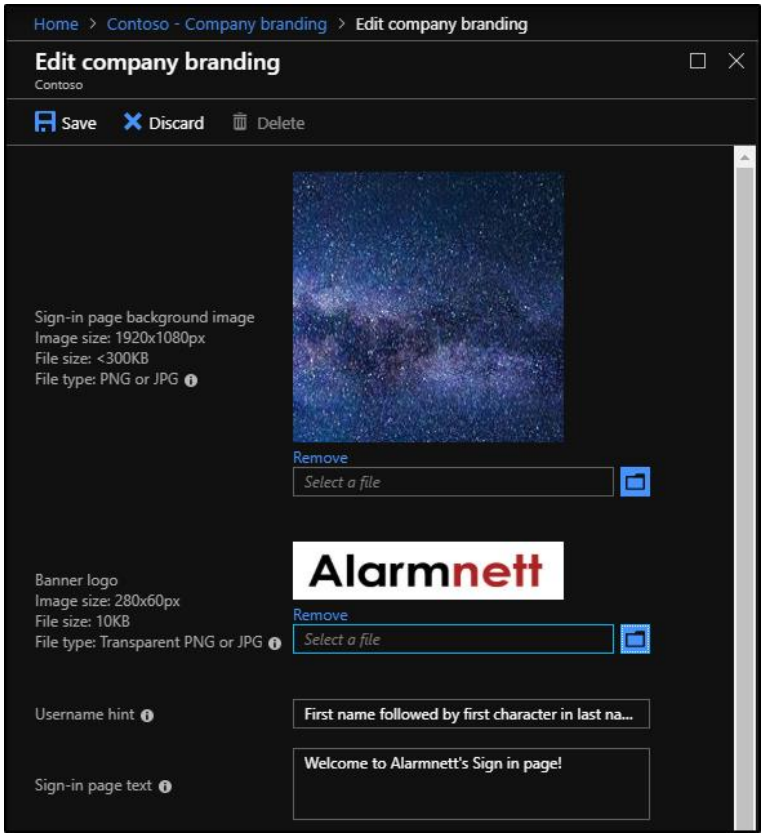
Vi skal nå gi ressursene våre et personlig preg, vi starter konfigurasjon av Company Branding. Ved å sette opp Company Branding kan vi sette opp bedriftslogo og andre personlige preg på innlogging til bedriften. Dette inkluderer innlogging via nettsider, innmelding til domenet og andre former for innlogging til domenet.

Vi navigerer oss til ***Azure Active Directory – Company branding***.



Figur 281: Company Branding

Vi velger **Edit**, og får opp en del muligheter, som vist nedenfor. Vi gjør de endringene vi ønsker og trykker **Save.**



Figur 282: Company Branding

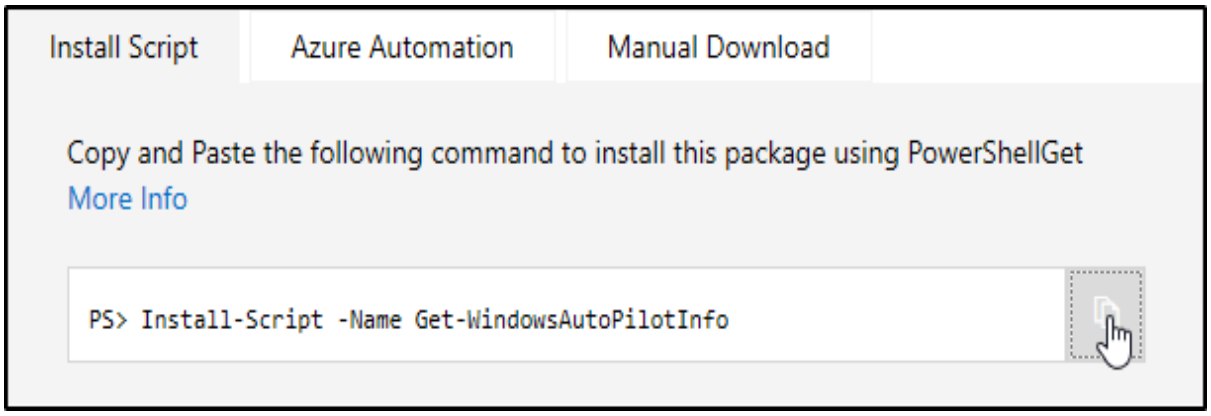
Innrulling ved bruk av Windows Autopilot

Før vi kan legge til enheten som en device i Azure, er vi nødt til å ha en del informasjon om enheten som skal legges til. Det er her snakk om: «Device Serial Number», «Windows Product ID» og «Hardware Hash". Det er to metoder som kan brukes for å få tak i denne informasjonen. Vi skal nå demonstrere hvordan dette kan gjøres med et PowerShell-script på selve enheten som skal innrulles med Windows Autopilot. Senere skal vi se på hvordan vi kan gjøre det samme, men for flere enheter samtidig ved å ta i bruk SCCM.

Uthenting av Windows Autopilot informasjon ved bruk av PowerShell

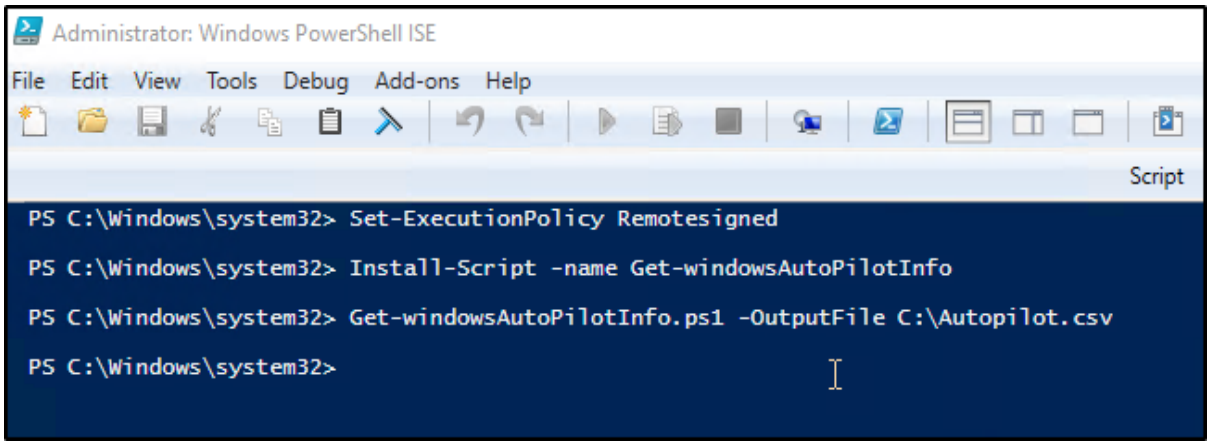
Gå til denne nettsiden (https://Aka.m s/Autopilotshell) for å få tilgang til PowerShell kommando som installerer en cmdlet som vil gjøre det mulig å opprette en CSV-fil, som senere skal brukes til å få kjørt inn den unike enhetens enhets-informasjonen, som skal håndteres av Windows Autopilot.

Kommandoen skal kjøres på maskinen som vi ønsker å hente informasjon om enheten fra.



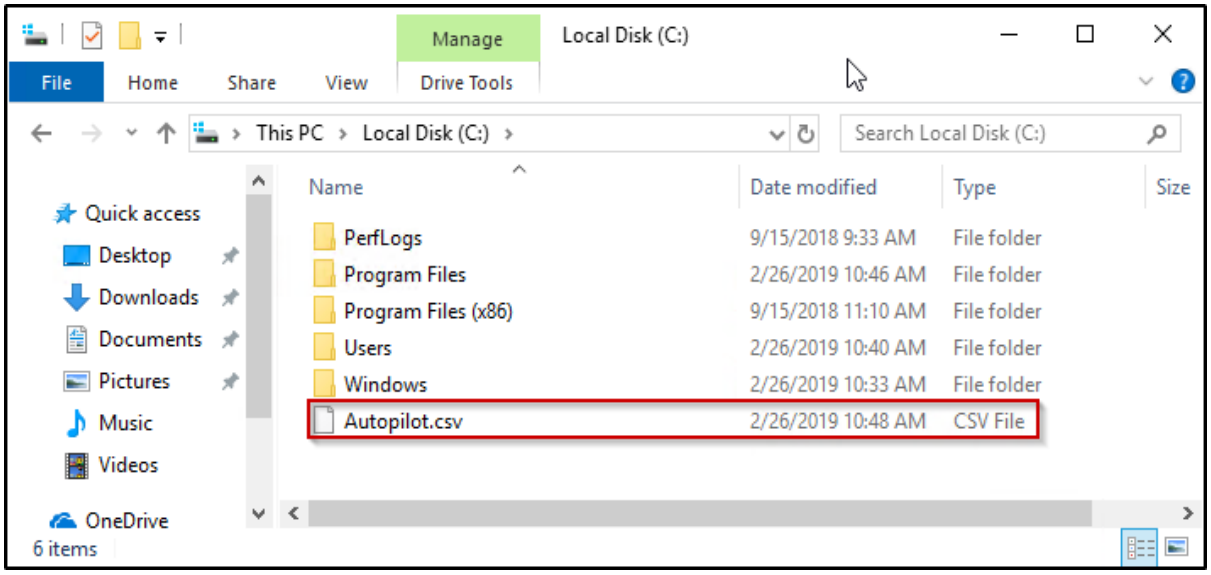
Figur 283: Uthenting av Windows Autopilot informasjon ved bruk av powershell

Nedenfor ser vi et utklipp av kommandoene som vi måtte kjøre for å få tak i informasjonen til enheten. Vi ser ut ifra den siste kommandoen at vi lagrer denne informasjonen i en CSV-fil som heter *Autopilot.csv.*



Figur 284: Uthenting av Windows Autopilot informasjon ved bruk av powershell

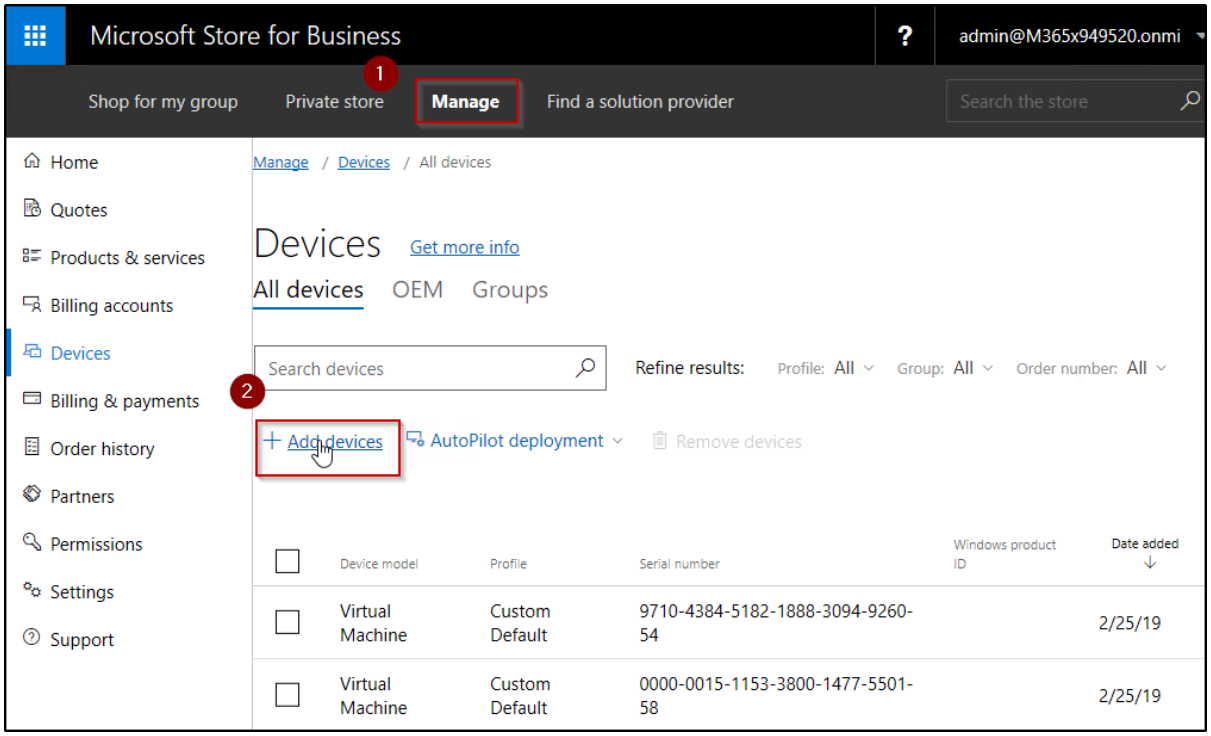
Autopilot.csv filen er nå lagret



Figur 285: Uthenting av Windows Autopilot informasjon ved bruk av powershell

Går til https://Businesstore.microsoft.com/en-us/store og logger inn med administratorbruker.

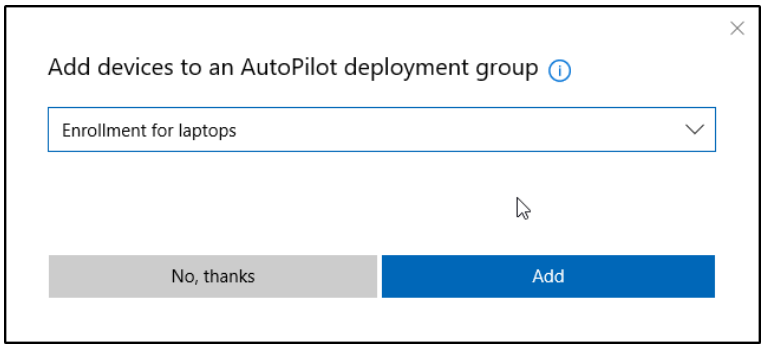
Navigerer oss til ***Devices***, og velger **Add devices**. (Det er også mulig å gjøre dette i Intune)



Figur 286: Uthenting av Windows Autopilot informasjon ved bruk av powershell

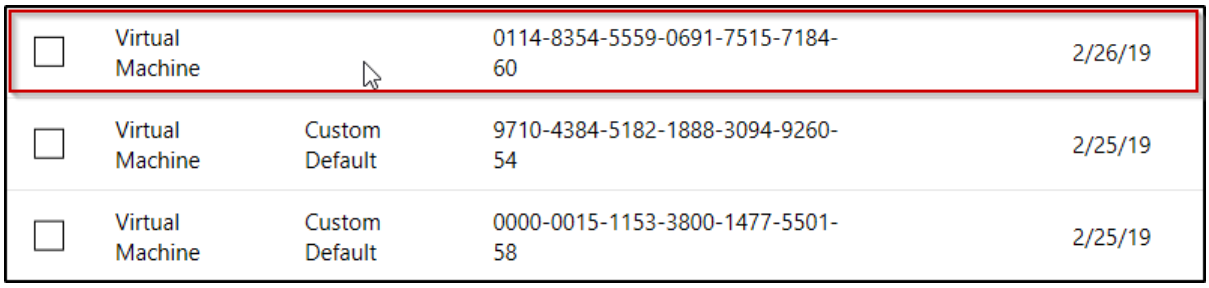
Velger Autopilot.csv filen som vi opprettet tidligere.

Velger å legge til enheten i en AutoPilot deployment group. Dersom man ikke har en gruppe fra før, velger man å opprette en gruppe først.



Figur 287: Uthenting av Windows Autopilot informasjon ved bruk av powershell

Vi ser her at maskinene har blitt lagt til

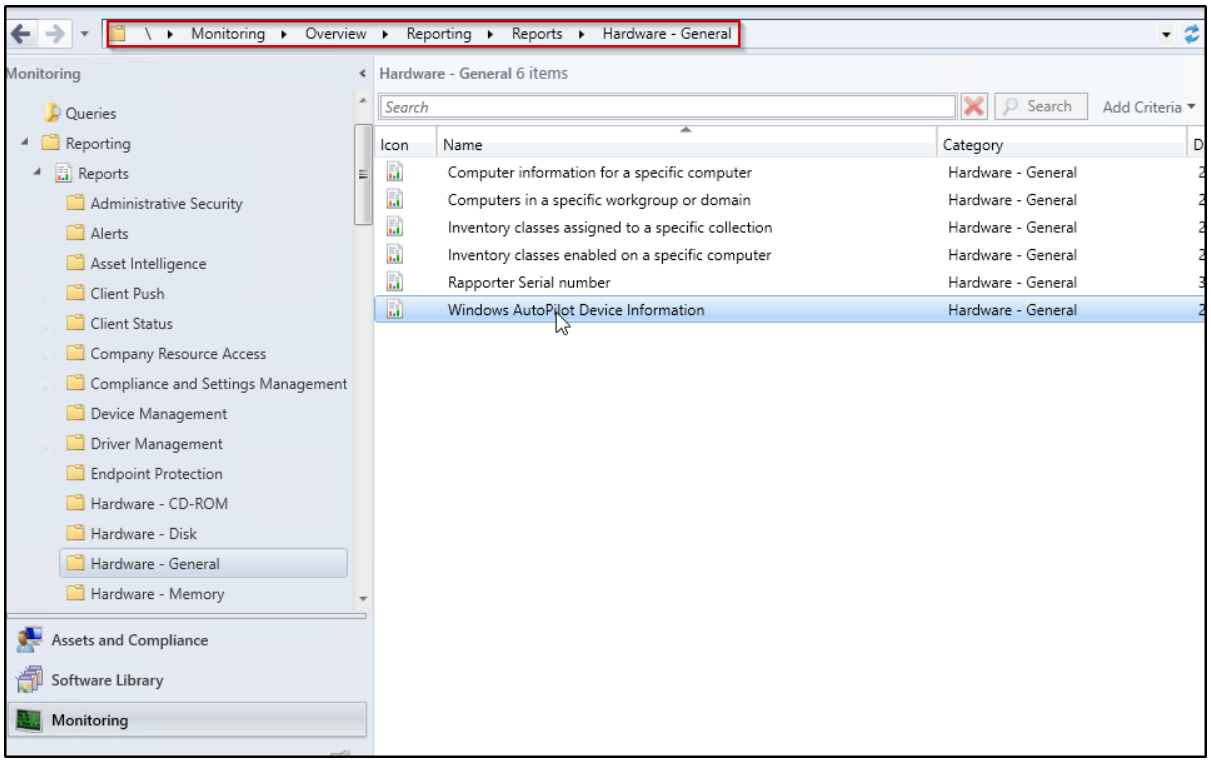


Figur 288: Uthenting av Windows Autopilot informasjon ved bruk av powershell

Uthenting av Windows Autopilot informasjon ved bruk av SCCM

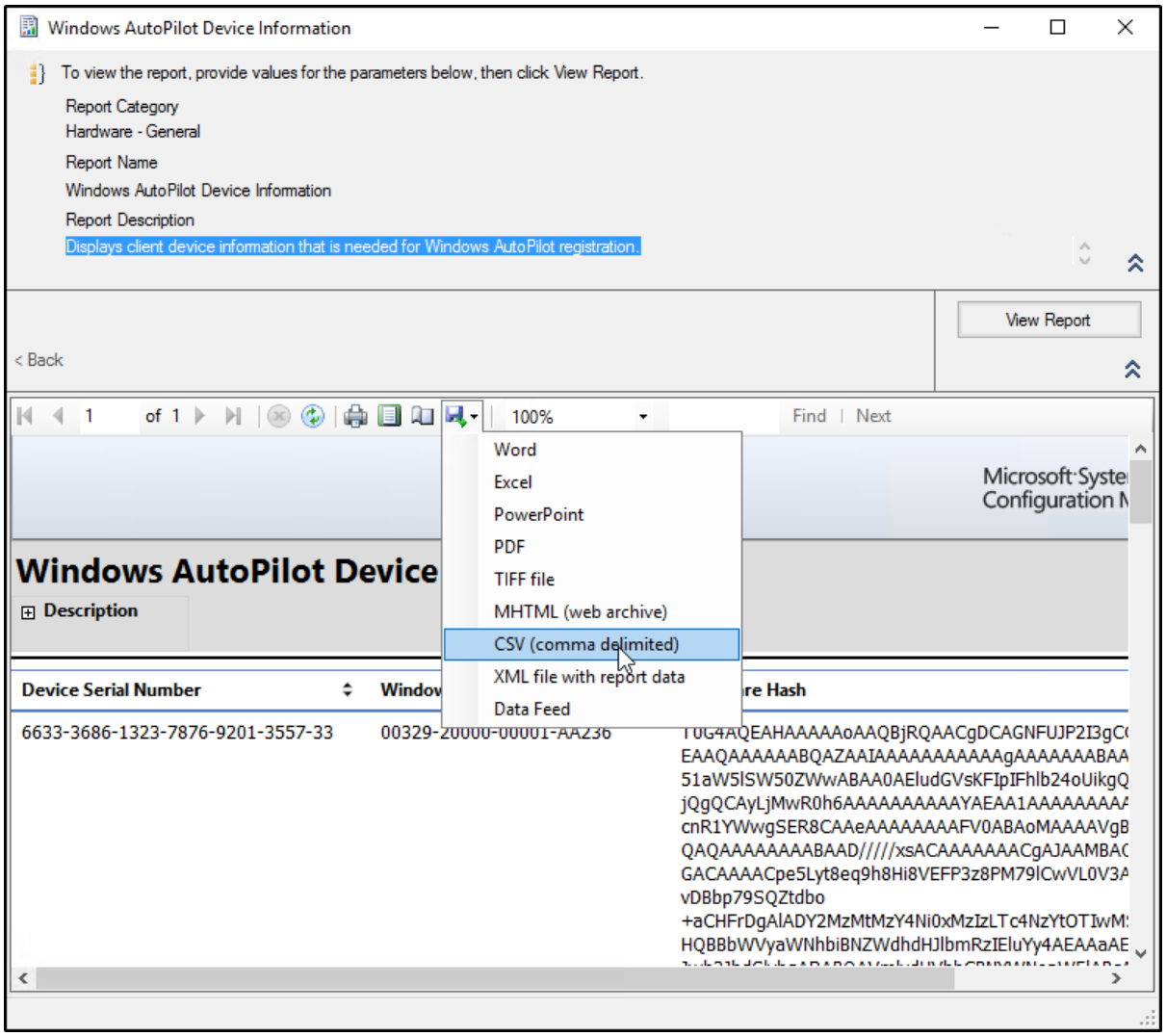
Vi skal nå se på hvordan den samme prosessen kan gjøres ved bruk av SCCM.

Vi åpner Configuration Manager og navigerer oss til rapportsiden for i SCCM ***Monitoring – Overview – Reporting – Reports – Hardware – General***. Her velger vi å åpne rapporten som heter *Windows AutoPilot Device information*.



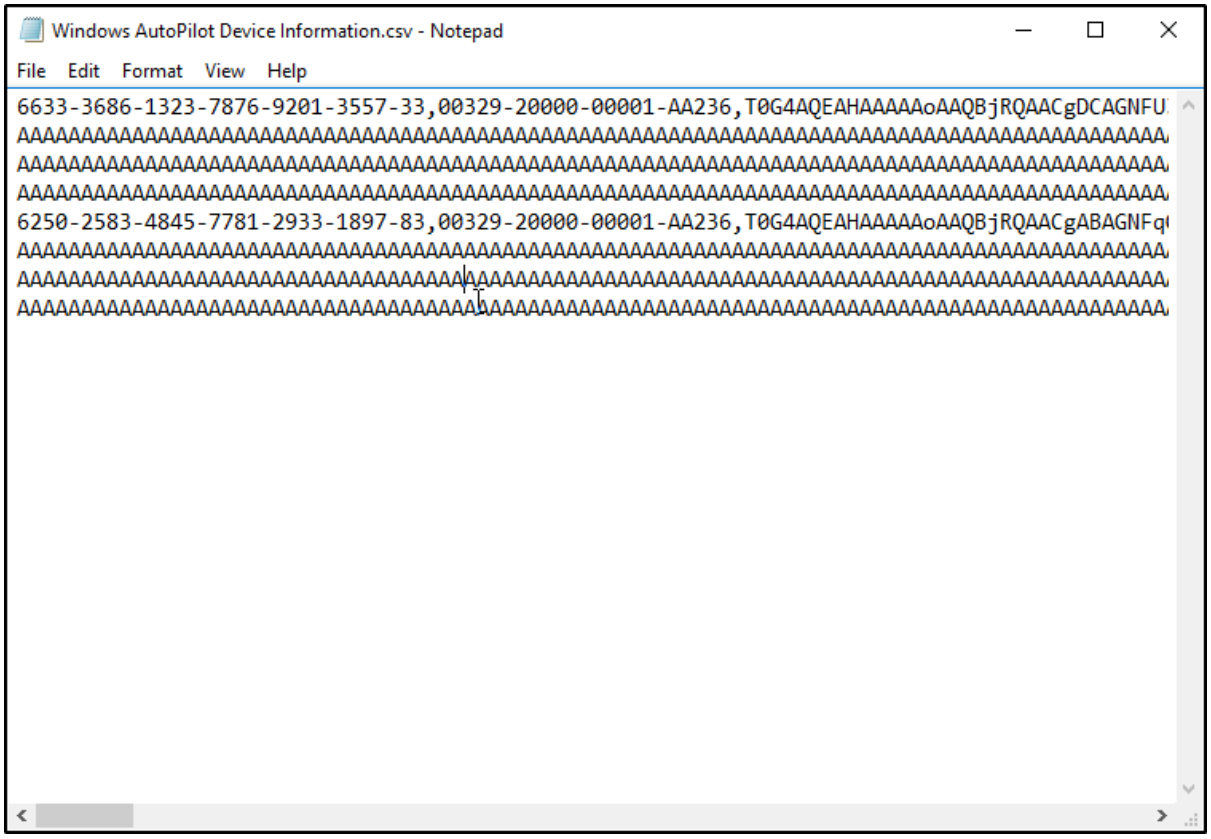
Figur 289: Uthenting av Windows Autopilot informasjon ved bruk av SCCM

Vi trykker på **View Report** og får deretter opp informasjon om maskinene som ligger inne i Configuration Manager. Det er her snakk om «Device Serial Number», «Windows Product ID» og «Hardware Hash».



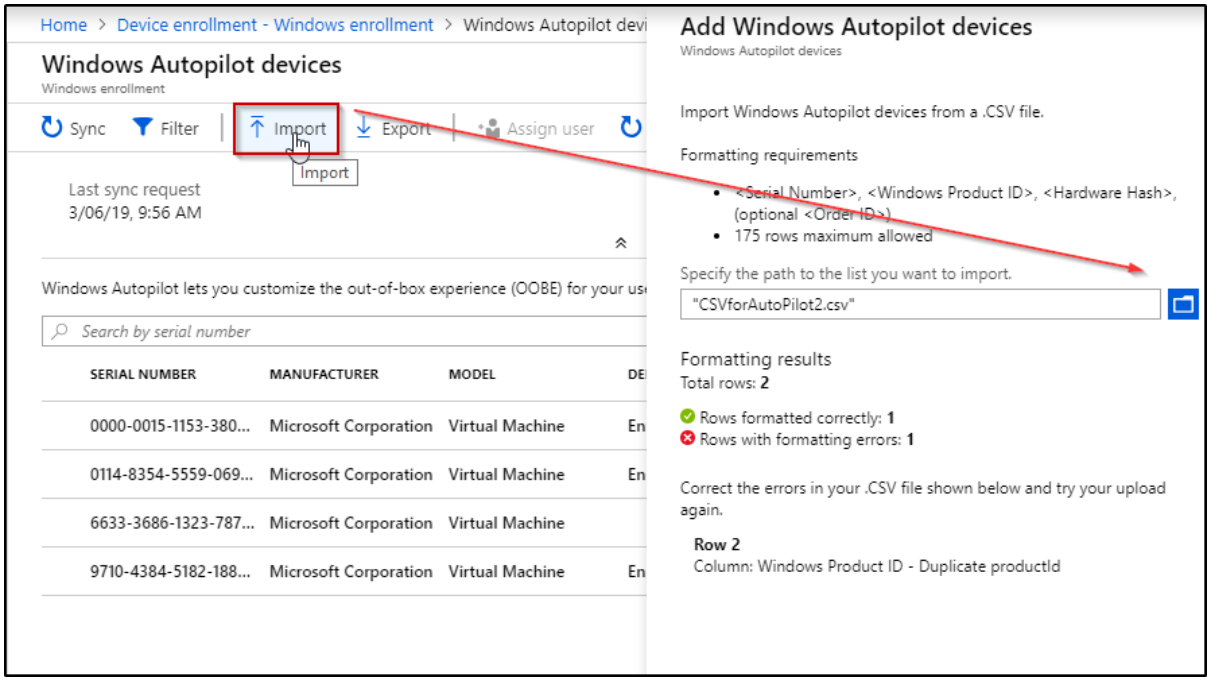
Figur 290: Uthenting av Windows Autopilot informasjon ved bruk av SCCM

Når vi eksporterer CSV-filen vil den komme med litt ekstra informasjon som man må ta vekk. Nedenfor på bildet ser vi at vi kun har «Device Serial Number», «Windows Product ID» og «Hardware Hash», som skilles med komma (,). Dette er et resultat fra et script vi kjørte for å kovertere CSV-filen vår slik at vi kan laste den opp til Intune. (Se vedlegg 3)



Figur 291: Uthenting av Windows Autopilot informasjon ved bruk av SCCM

Når CSV-filen er gjort klar, kan man gå inn på sin Azure tenant, navigere seg til Windows Autopilot Devices og deretter velge å importere nye maskiner. I bildet nedenfor ser vi at vi får en feil (error). Denne feilen sier at filen som vi lastet opp inneholder en enhet som allerede eksisterer. Dette kommer av at vi allerede har importert denne enheten inn i Windows Autopilot devices.

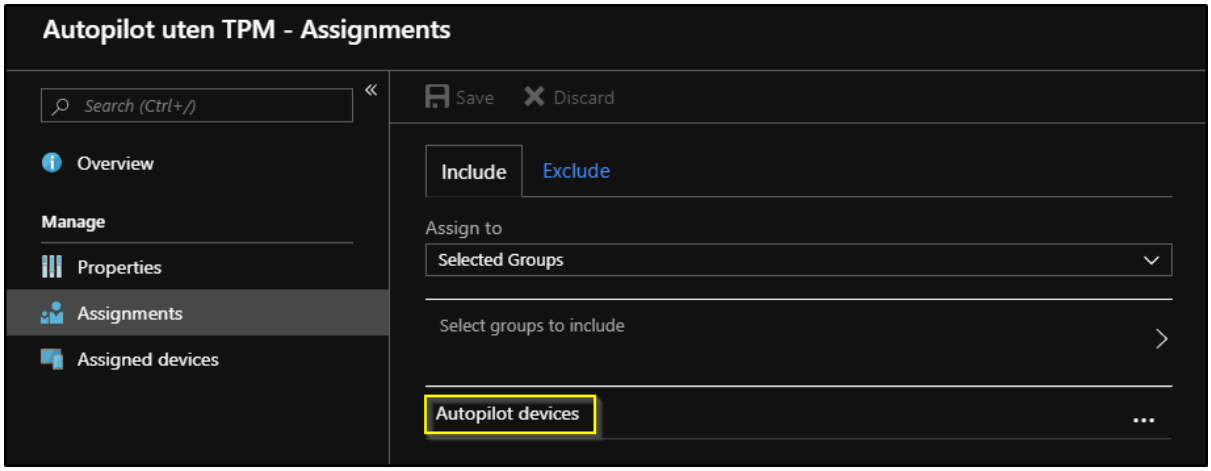


Figur 292: Uthenting av Windows Autopilot informasjon ved bruk av SCCM

Demonstrasjon av innrulling med Windows Autopilot

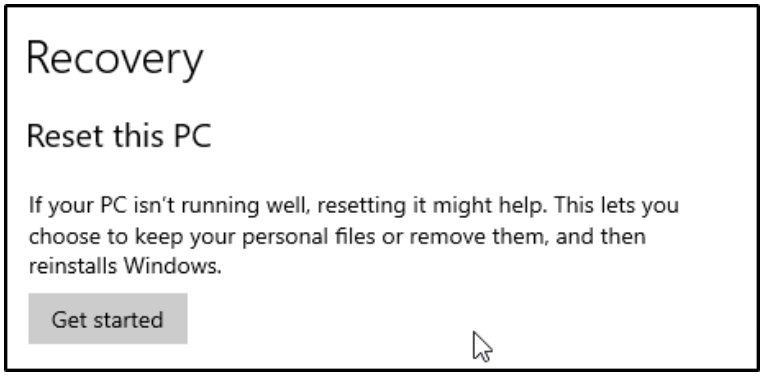
Prosessen med å hente ut enhets-informasjonen er nå gjennomført. La oss videre se på hvordan vi går frem for å rulle disse inn med Windows Autopilot.

Vi begynner med å legge maskinene inn i en gruppe. Vi må gjøre dette slik at maskinene får tildelt en Deployment Profil. I bildet nedenfor ser vi at Deployment Profilen "Autopilot uten TPM" gis til gruppen "Autopilot devices". Nye maskiner som skal rulles inn med Windows Autopilot, må derfor være medlem av denne gruppen.



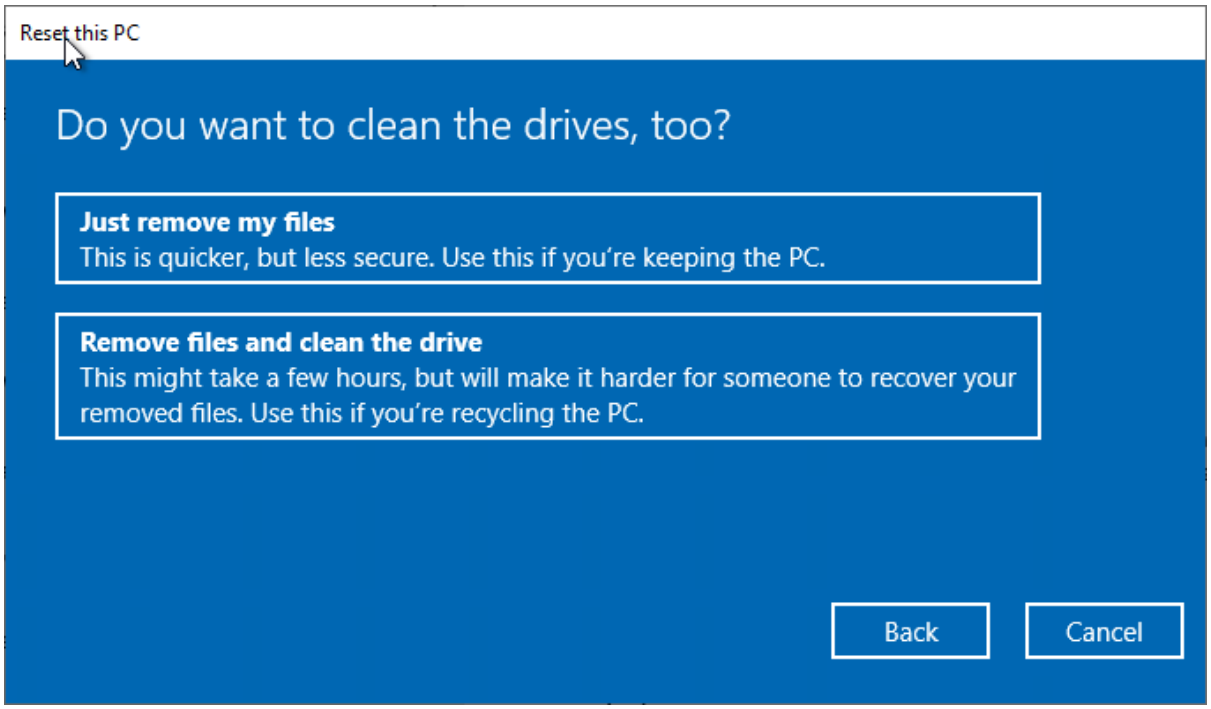
Figur 293: Demonstrasjon av innrulling med Windows Autopilot

Etter å ha lagt til maskinen i Intune vil vi resette maskinen. Dette vil ta tid. Dette gjøres ved å navigere seg til ***Settings – Oppdatering og sikkerhet – Gjenoppretting***, og trykke på **Kom i gang** eller **Get started** som vist nedenfor.



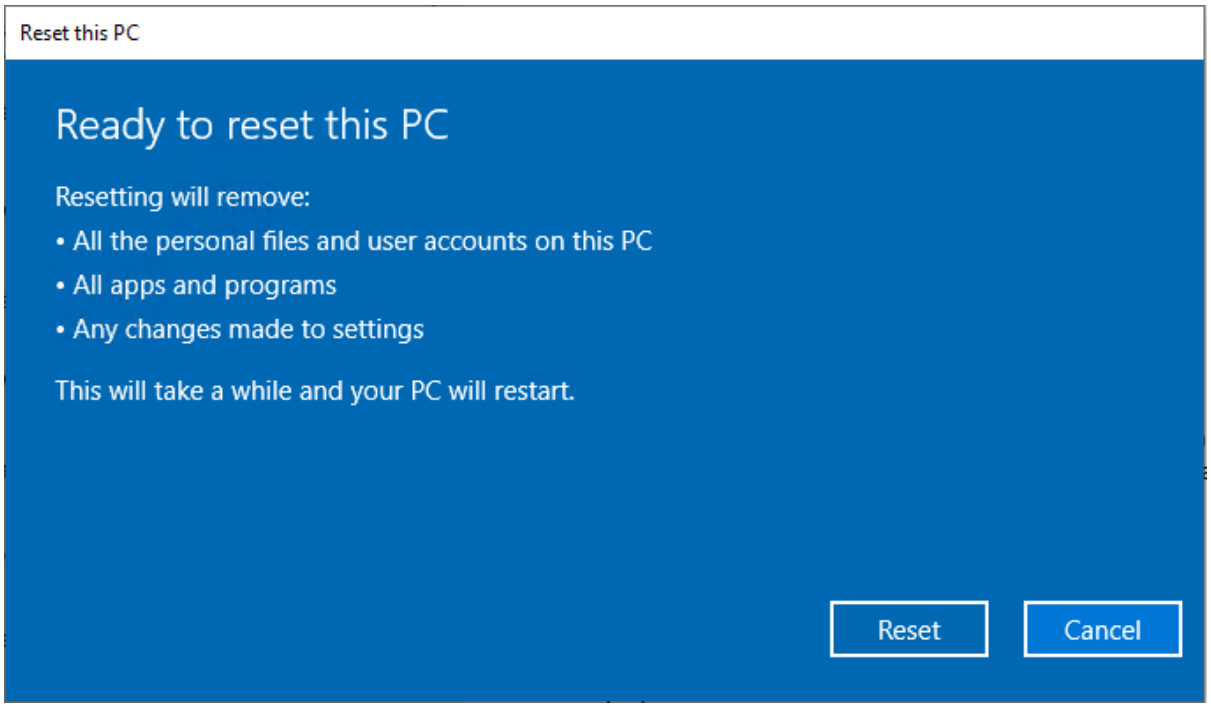
Figur 294: Demonstrasjon av innrulling med Windows Autopilot

Nedenfor vil man se at vi velger å **Remove files and clean the drive**.



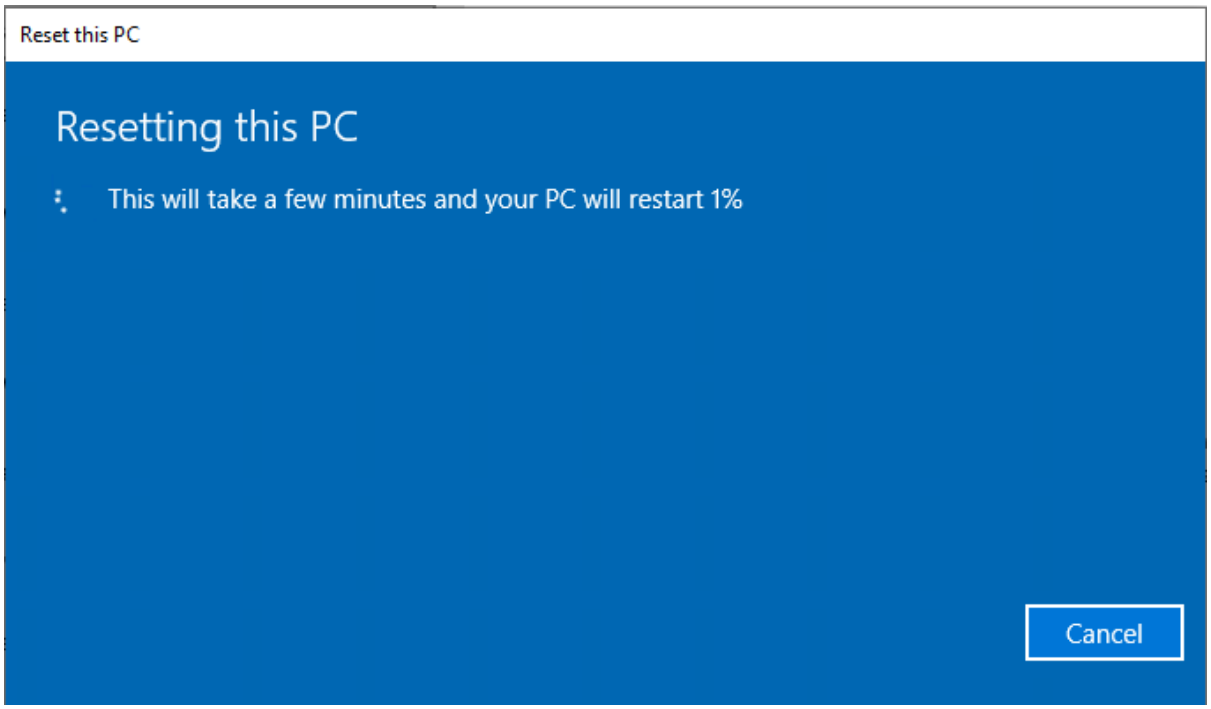
Figur 295: Demonstrasjon av innrulling med Windows Autopilot

Velger **Reset**.



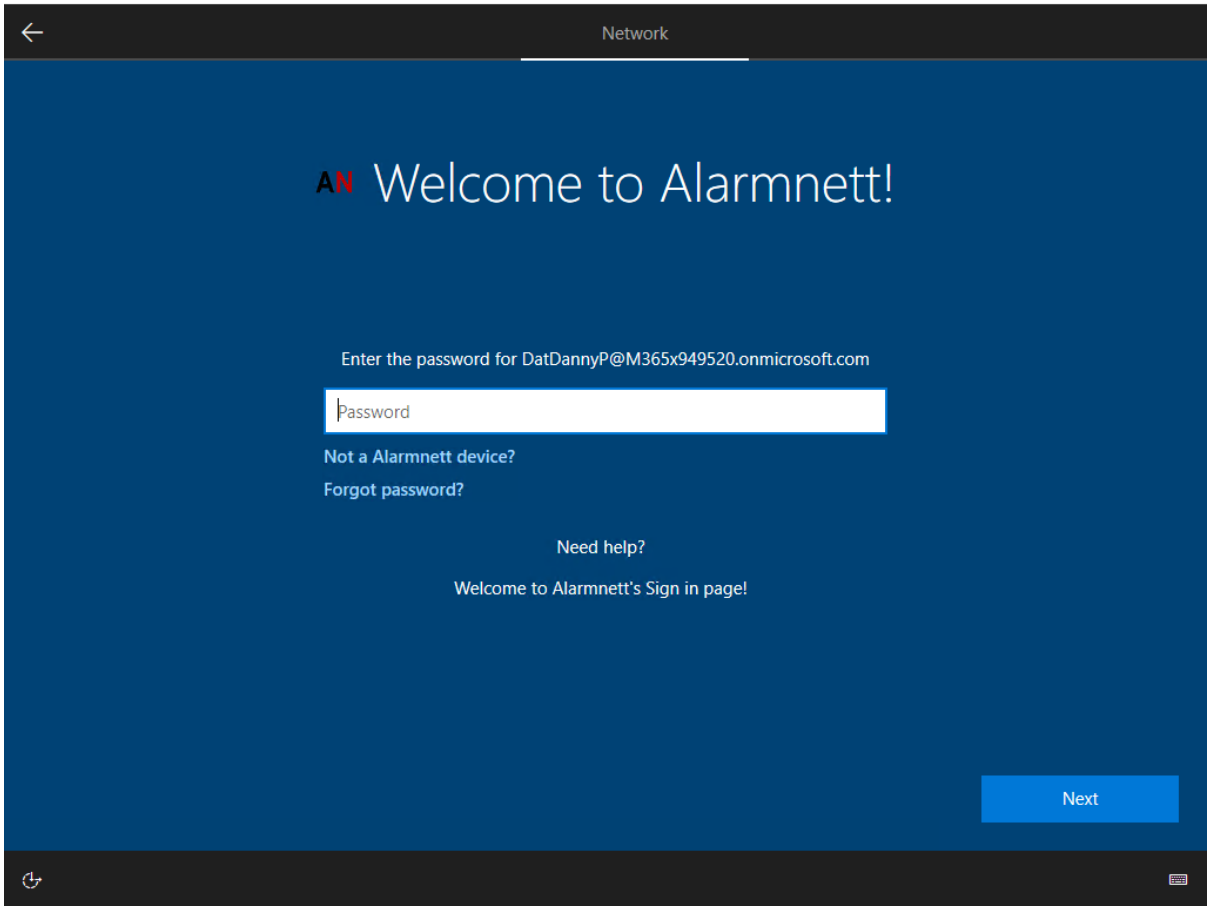
Figur 296: Demonstrasjon av innrulling med Windows Autopilot

Enheten er i gang med å resette.



Figur 297: Demonstrasjon av innrulling med Windows Autopilot

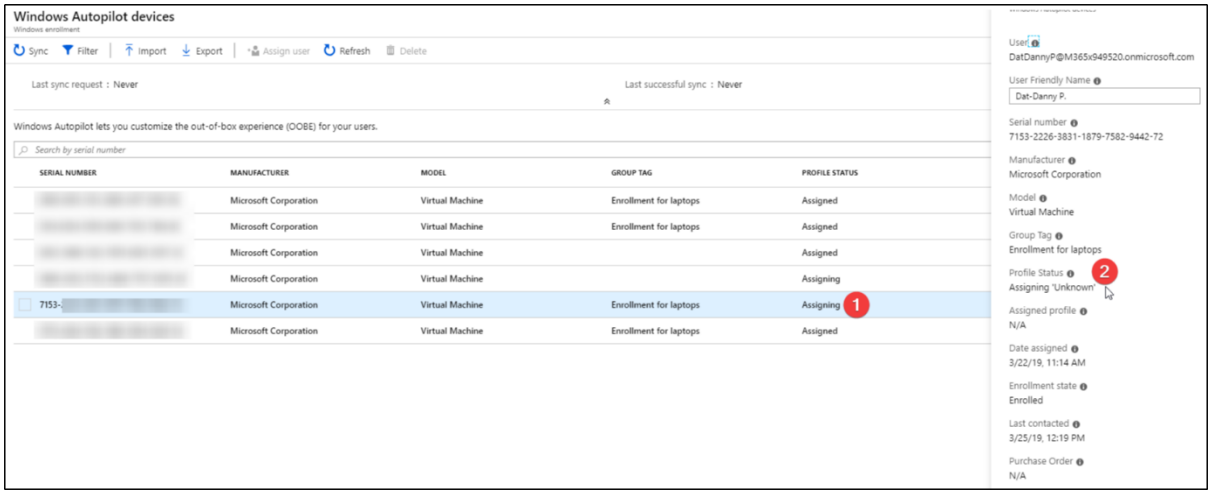
Etter hvert vil man komme til bedriften sin innloggingsside hvor man må logge inn. Etter innlogging får man mulighet til å sette opp “Windows Hello”, som gir mulighet for å benytte en pin i stedet for passord.



Figur 298: Demonstrasjon av innrulling med Windows Autopilot

Unassigned Profile

Hvis man skulle komme over at maskinen eller maskinene ikke får tilordnet en profil selv om du har satt det i profile, som vist under. Kan man prøve å legge inn maskinen til gruppen på nytt, ved først å slette den fra gruppen og så legge den til igjen. Vi kom over dette problemet da vi tilordnet en profil til maskinen og så tilordnet en ny igjen da vi fant ut at den ikke fungerte.



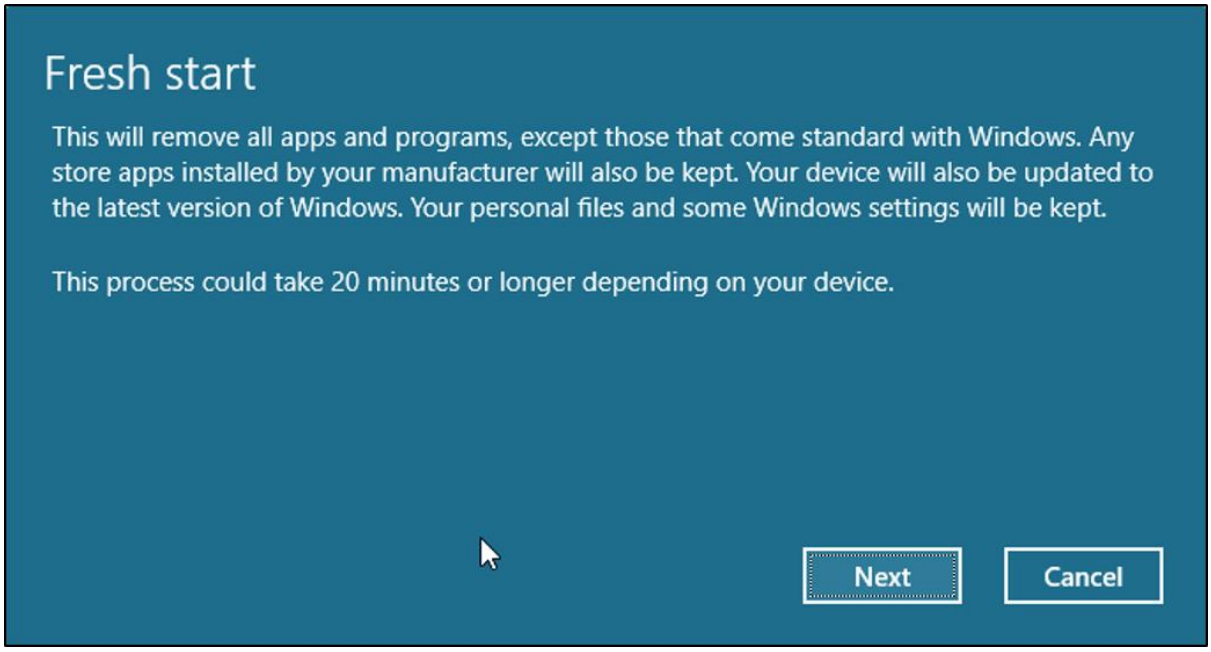
Figur 299: Unassigned Profile

Automatisering av Windows Autopilot Innrullingsprosessen

For å forenkle prosessen med å rulle inn maskiner ved hjelp av Windows Autopilot, har vi utarbeidet et script. Scriptet tar hånd om store deler av arbeidet som må gjøres for å få Windows Autopilot prosessen i gang. Først må vi nevne at scriptet må kjøres fra en konsoll med administratorrettigheter.

Til å begynne med, vil scriptet hente ut enhets-informasjonen fra enheten, som scriptet kjører på. Videre har vi lagt inn kode som laster opp CSV-filen til Intune. Når dette er gjort tar scriptet hånd om å tildele en bruker til maskinen, samt legger maskinen inn i en gruppe, slik at den får tildelt en deployment profil. Scriptet vil deretter sjekke regelmessig om maskinen har fått tildelt deployment profilen, før den setter i gang med å resette maskinen.

Administrasjonsansvarlig må deretter trykke **next** (vist på bildet nedenfor) to ganger før maskinen resettes.



Figur 300: Automatisering av Windows Autopilot Innrullingsprosessen

Avhengig av deployment profilen som brukes, vil prosessen gjennomføres av seg selv eller med svært lite brukerinput.

Script for automatisering av Windows Autopilot prosessen legges med som vedlegg. (Se vedlegg 1)

Innrulling til Intune

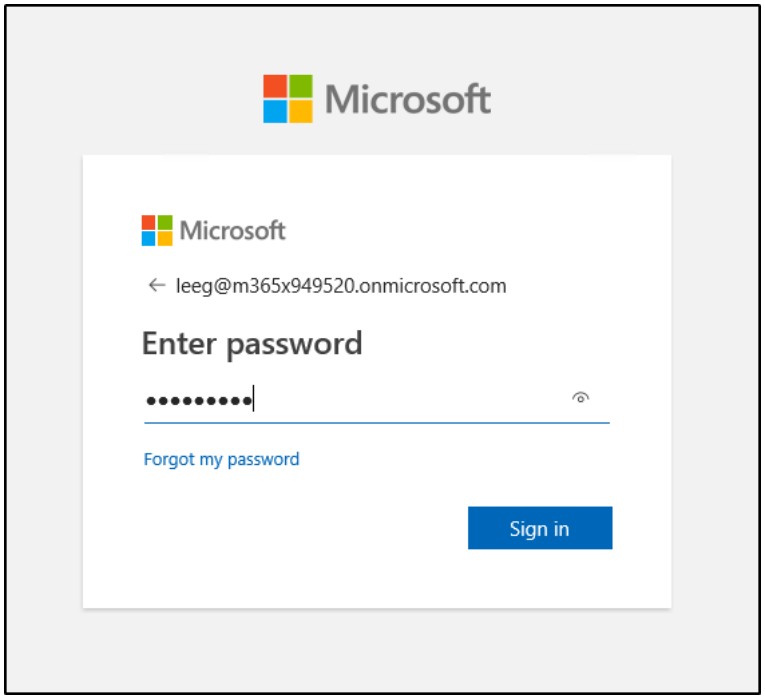
Innrulling av Intune administrerte enheter

Vi kan rulle inn en enhet med Windows 10 til domenet i Azure ganske enkelt fra enheten. Dette er hendig for å kunne styre og kontrollere sikkerhet og tilgang til ressurser som sluttbrukeren skal ha.

Her er det to enkle metoder. Vi starter med metode en:

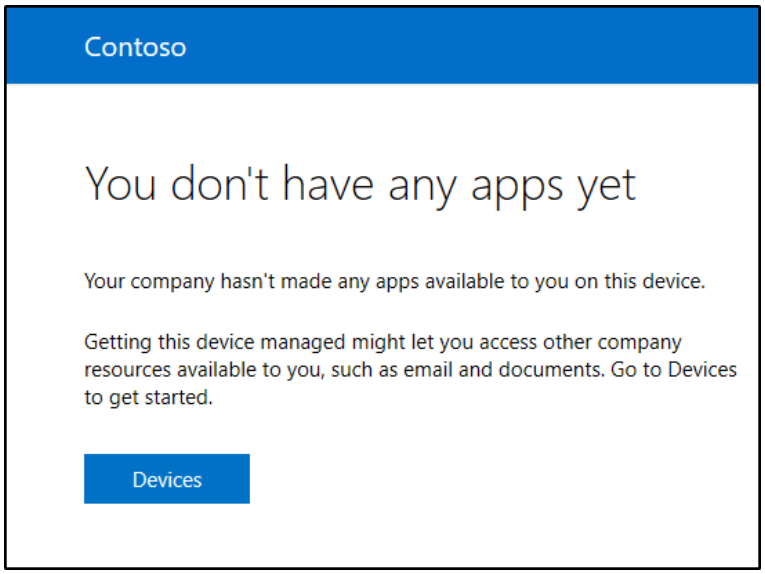
Metode 1

Vi begynner med å logge inn på http://portal.manage.microsoft.com med den nye Windows-enheten. Her benyttes brukerens egen jobb-bruker.



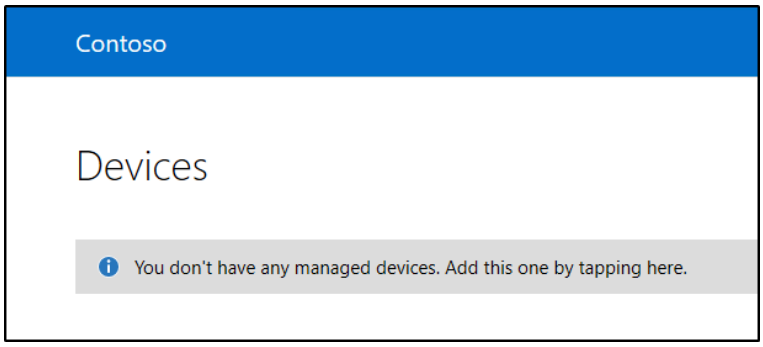
Figur 301: Innrulling av Intune administrerte enheter

Når man har logget inn trykker man på **Devices**.



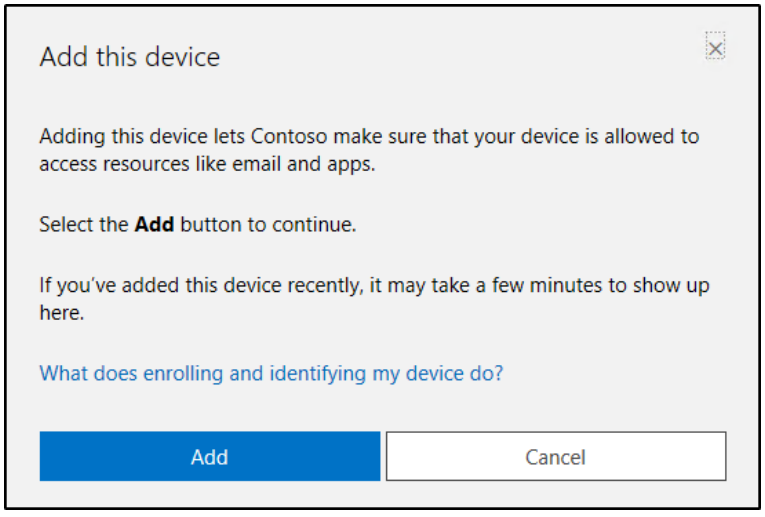
Figur 302: Innrulling av Intune administrerte enheter

Vi vil her se at brukeren ikke har fått tilordnet noen devices. Vi trykker derfor på meldingen som vi ser på skjermbildet nedenfor.



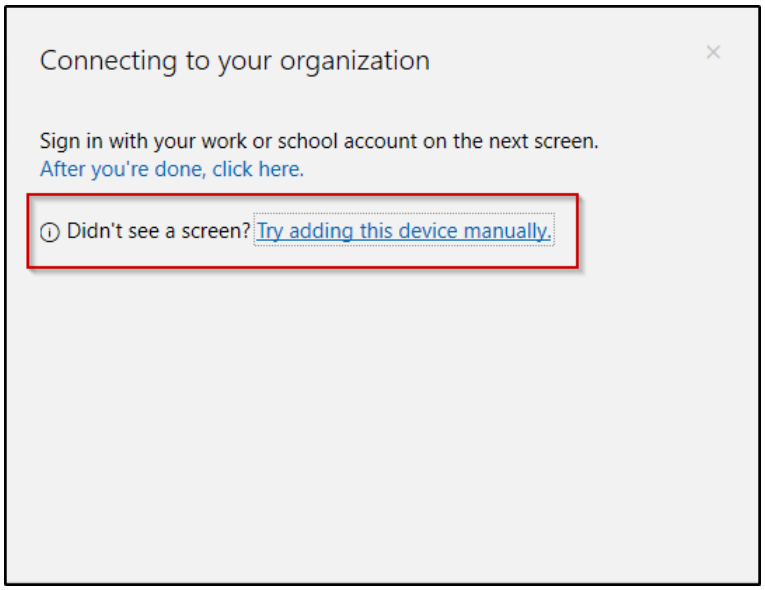
Figur 303: Innrulling av Intune administrerte enheter

Velger **Add**.



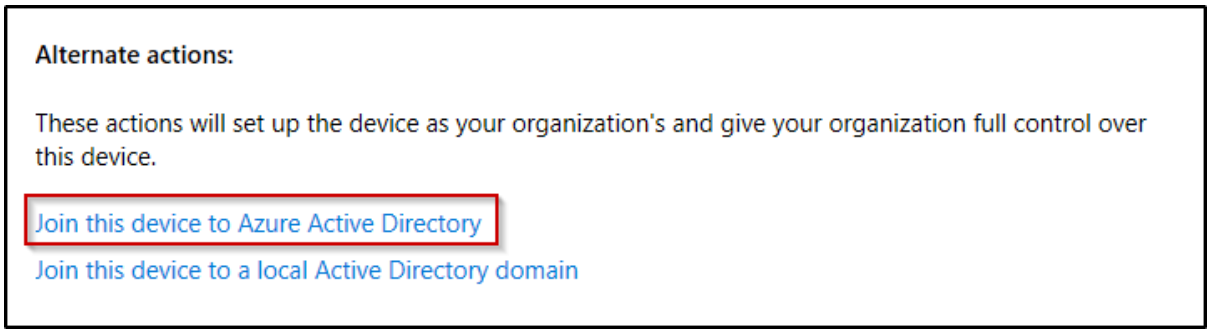
Figur 304: Innrulling av Intune administrerte enheter

Velger **Try adding this device manually**.



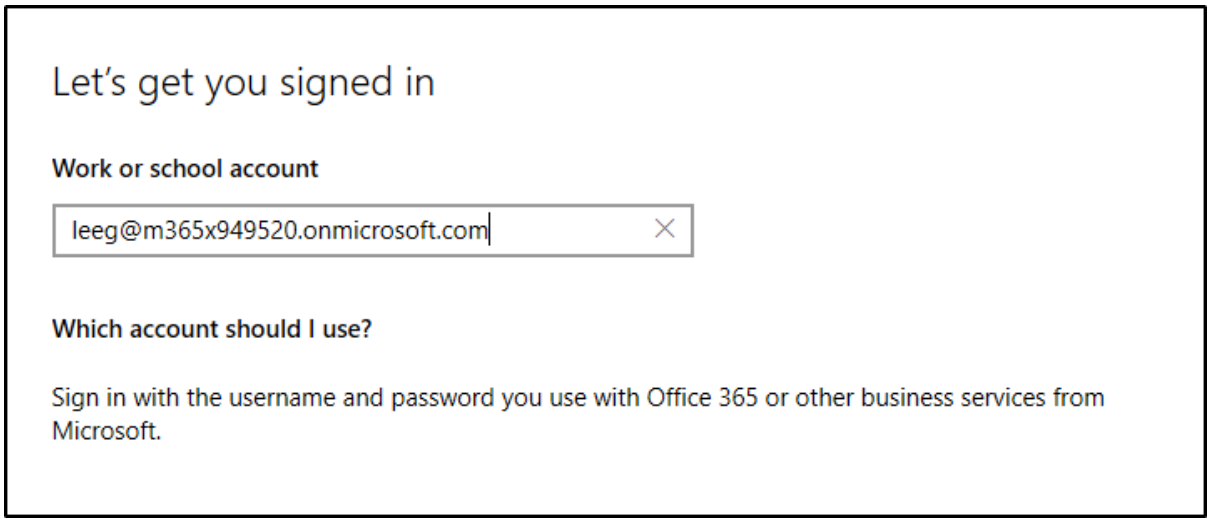
Figur 305: Innrulling av Intune administrerte enheter

Velger **Join this device to Azure Active Directory**.



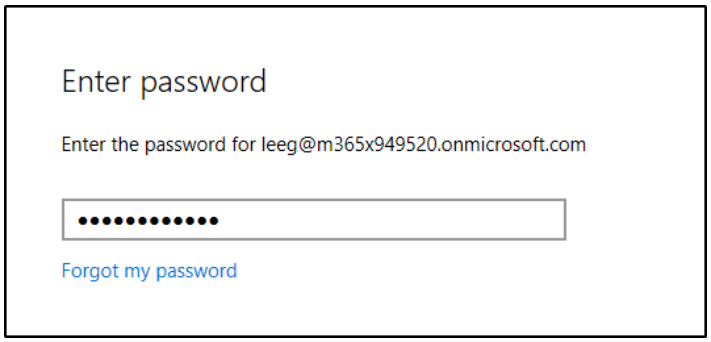
Figur 306: Innrulling av Intune administrerte enheter

Logger inn med Jobb-bruker.



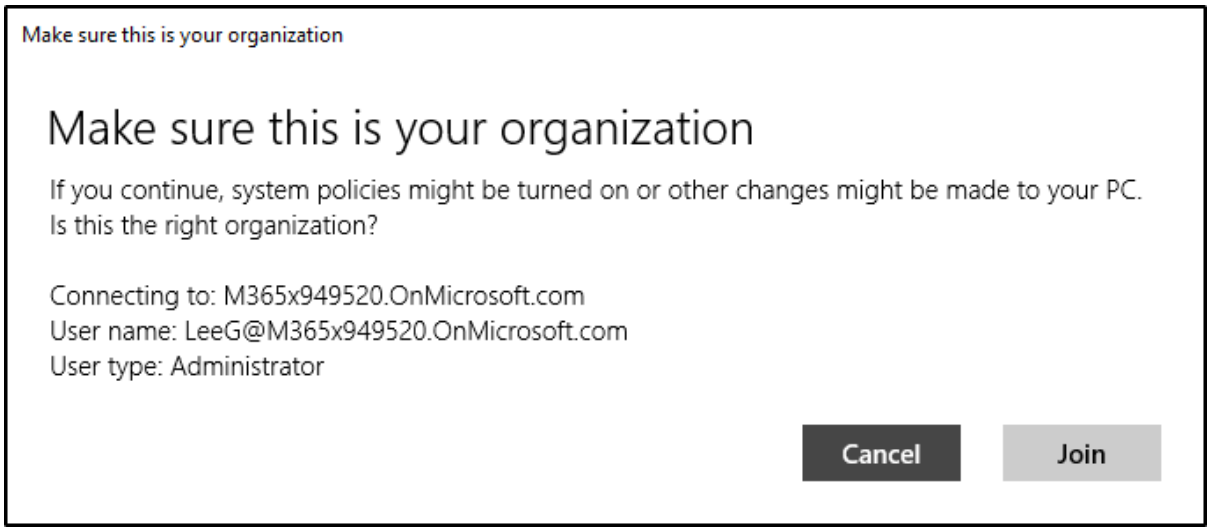
Figur 307: Innrulling av Intune administrerte enheter

Skriver inn passord.



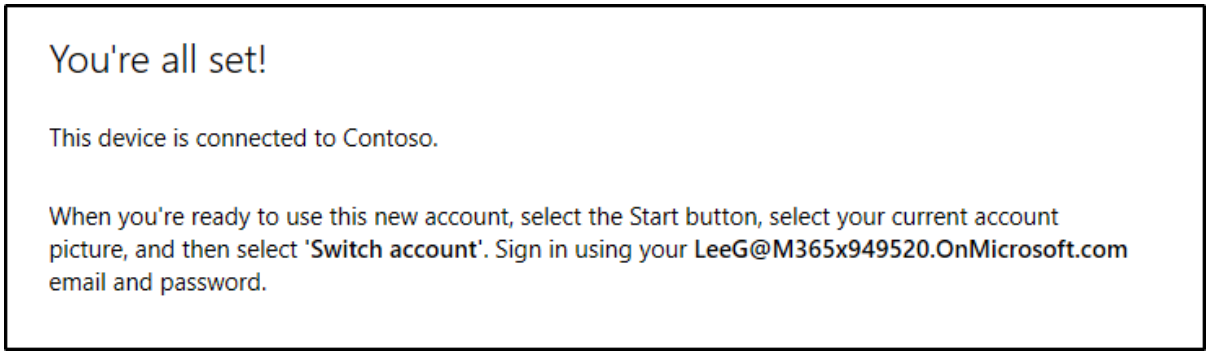
Figur 308: Innrulling av Intune administrerte enheter

Velger her **Join**.



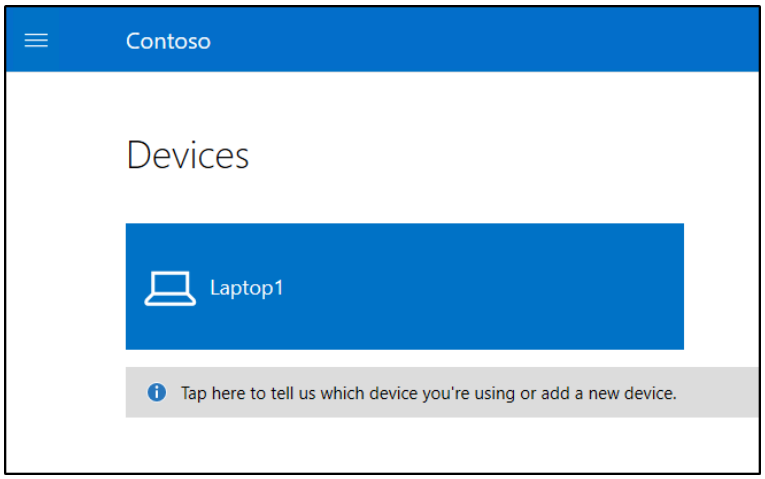
Figur 309: Innrulling av Intune administrerte enheter

Vi ser nå at brukeren har fått meldt inn sin enhet til Intune.



Figur 310: Innrulling av Intune administrerte enheter

Vi kan også se her at brukeren har fått tilordnet en enhet under sin bruker.

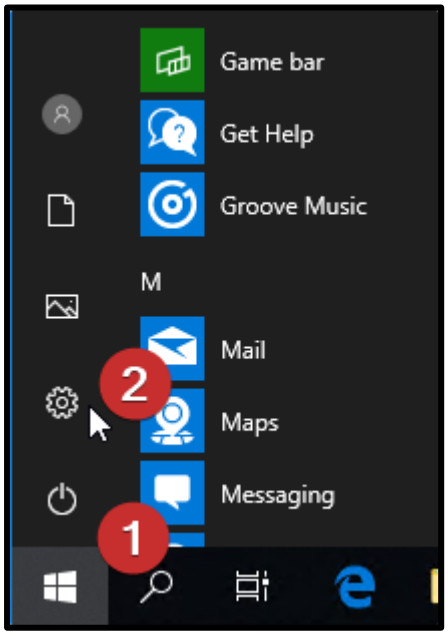


Figur 311: Innrulling av Intune administrerte enheter

Metode 2

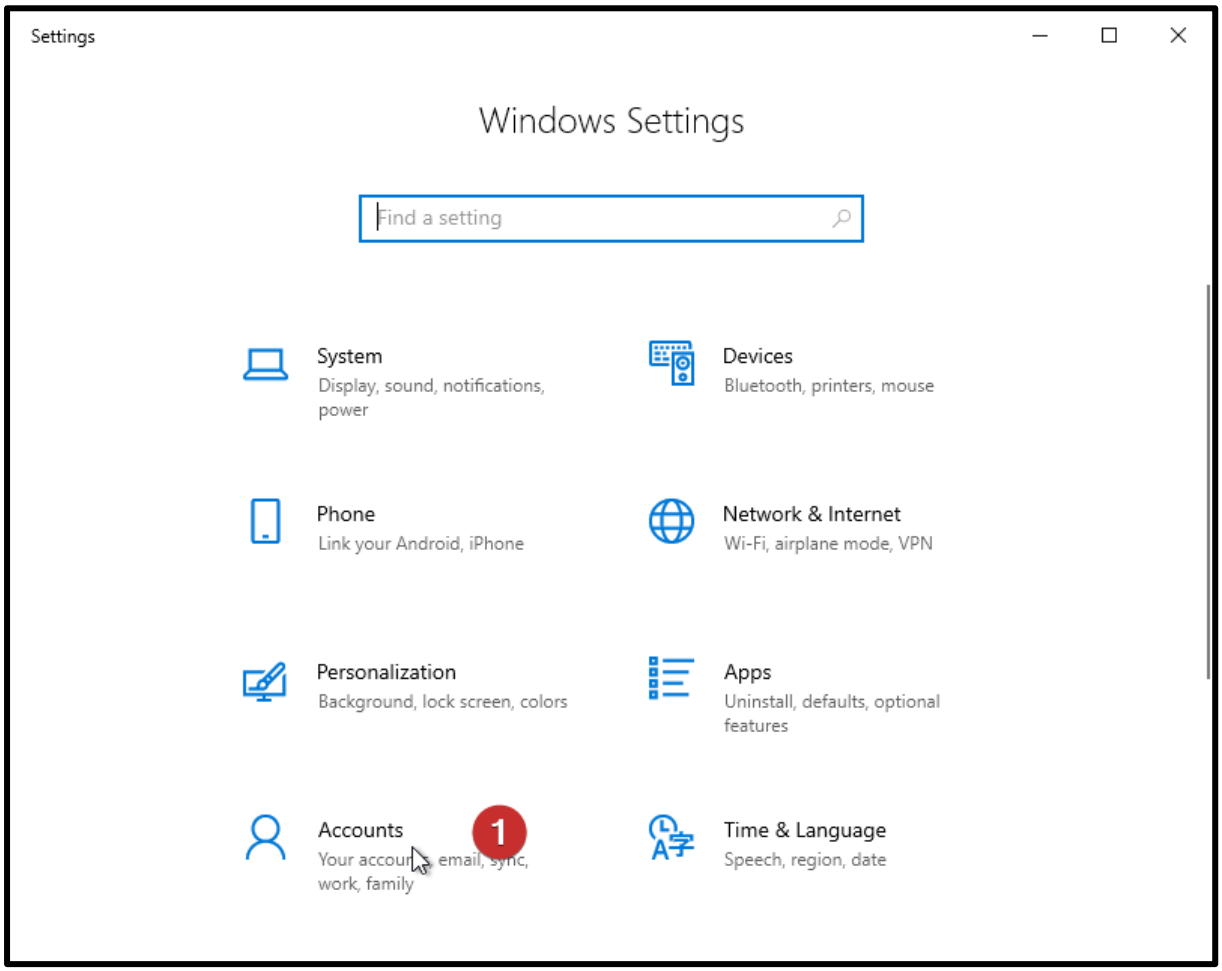
Denne metoden tar for seg en litt lettere metode å melde inn maskinen i domenet og kan enkelt gjøres «hjemmefra» uten kompliserte verktøy.

For å gjøre dette går vi først til ***startmenyen*** – Trykker på **Settings**



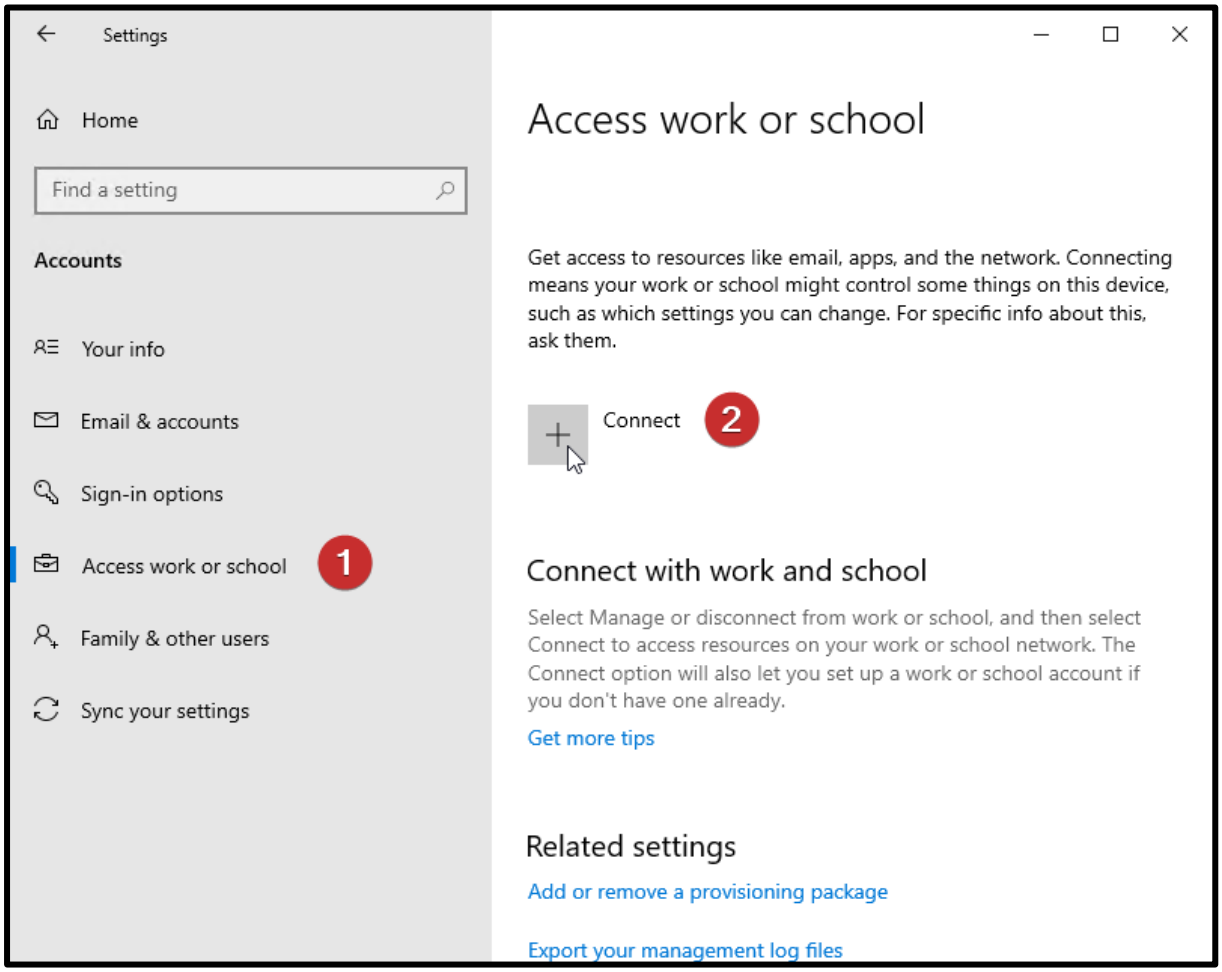
Figur 312: Innrulling av Intune administrerte enheter

Navigerer oss til ***Settings – Accounts***.



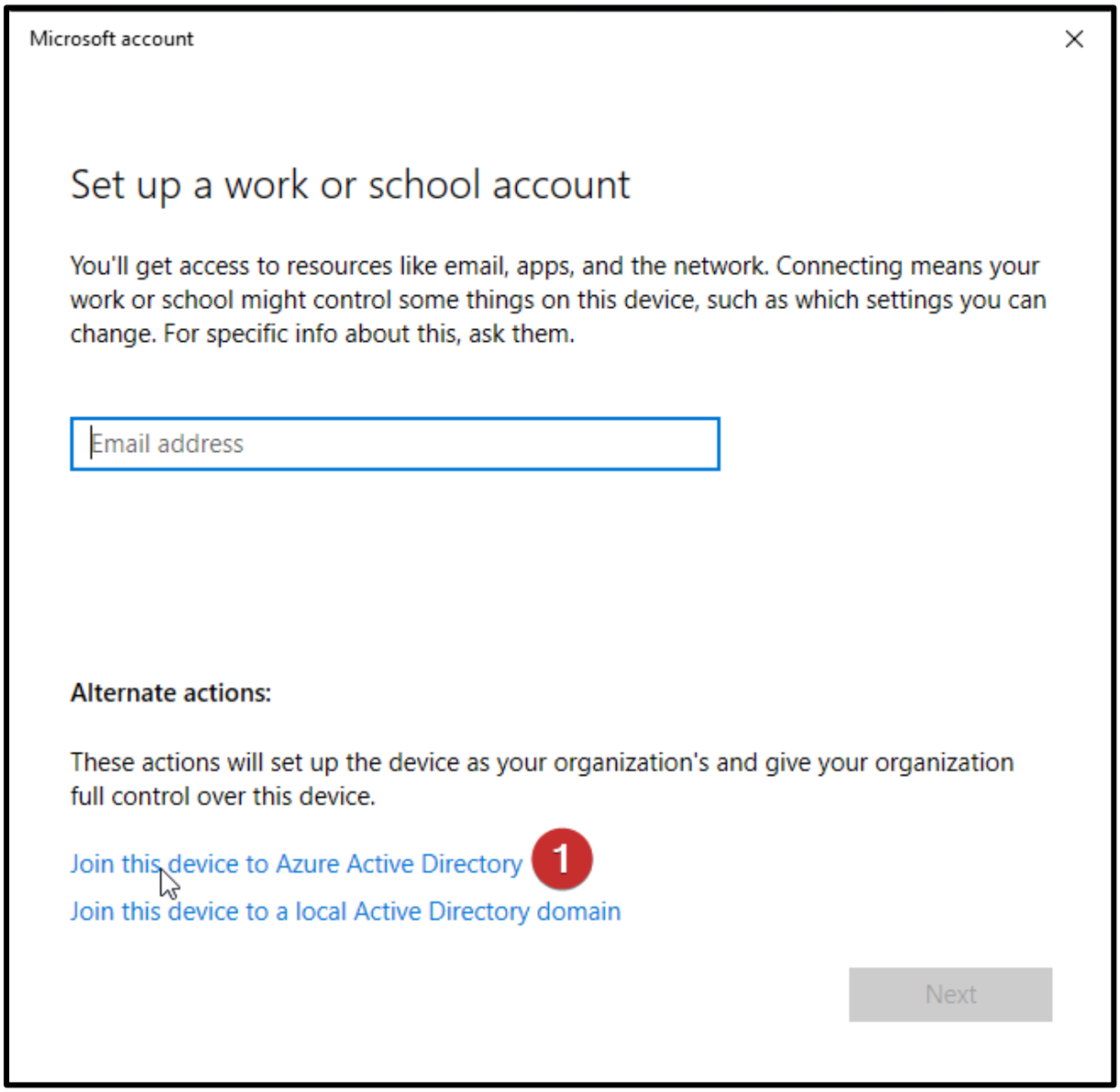
Figur 313: Innrulling av Intune administrerte enheter

Her finner vi en oversikt over brukeren din og eventuelle andre brukere. Vi går til ***Access work or school***. Her trykker vi **connect**.



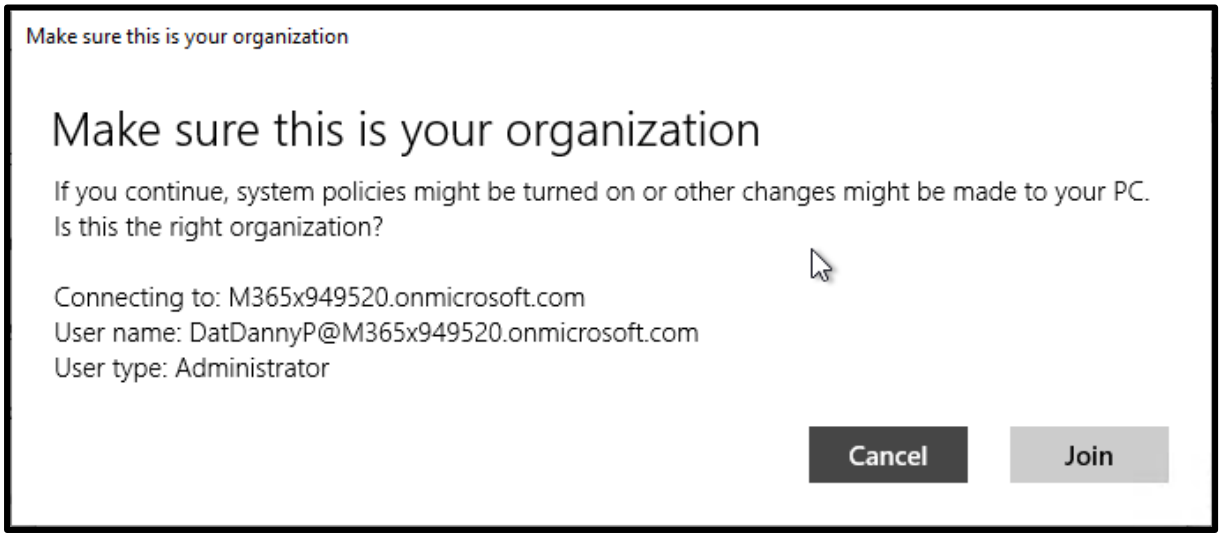
Figur 314: Innrulling av Intune administrerte enheter

Vi velger **Join this decive to Azure Active Directory** for å melde oss inn i domenet



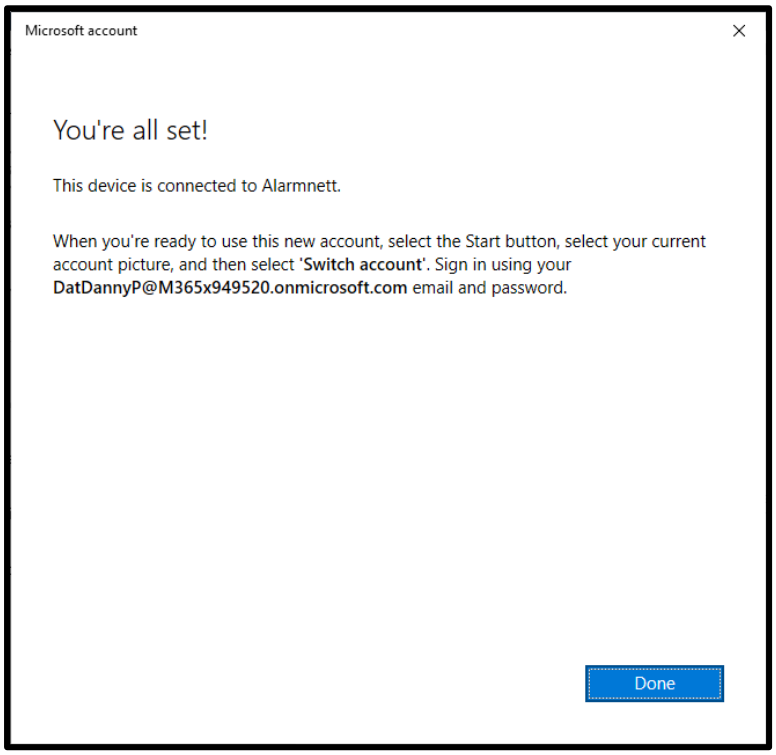
Figur 315: Innrulling av Intune administrerte enheter

Vi vil da måtte logge inn til Azure med vår bruker. Etter å ha logget oss på vil vi få et spørsmål om å bekrefte innrullingen av vår enhet. Vi trykker **Join**.



Figur 316: Innrulling av Intune administrerte enheter

Da er vi meldt inn i domenet.



Figur 317: Innrulling av Intune administrerte enheter

Vi kan bekrefte dette i Azure.

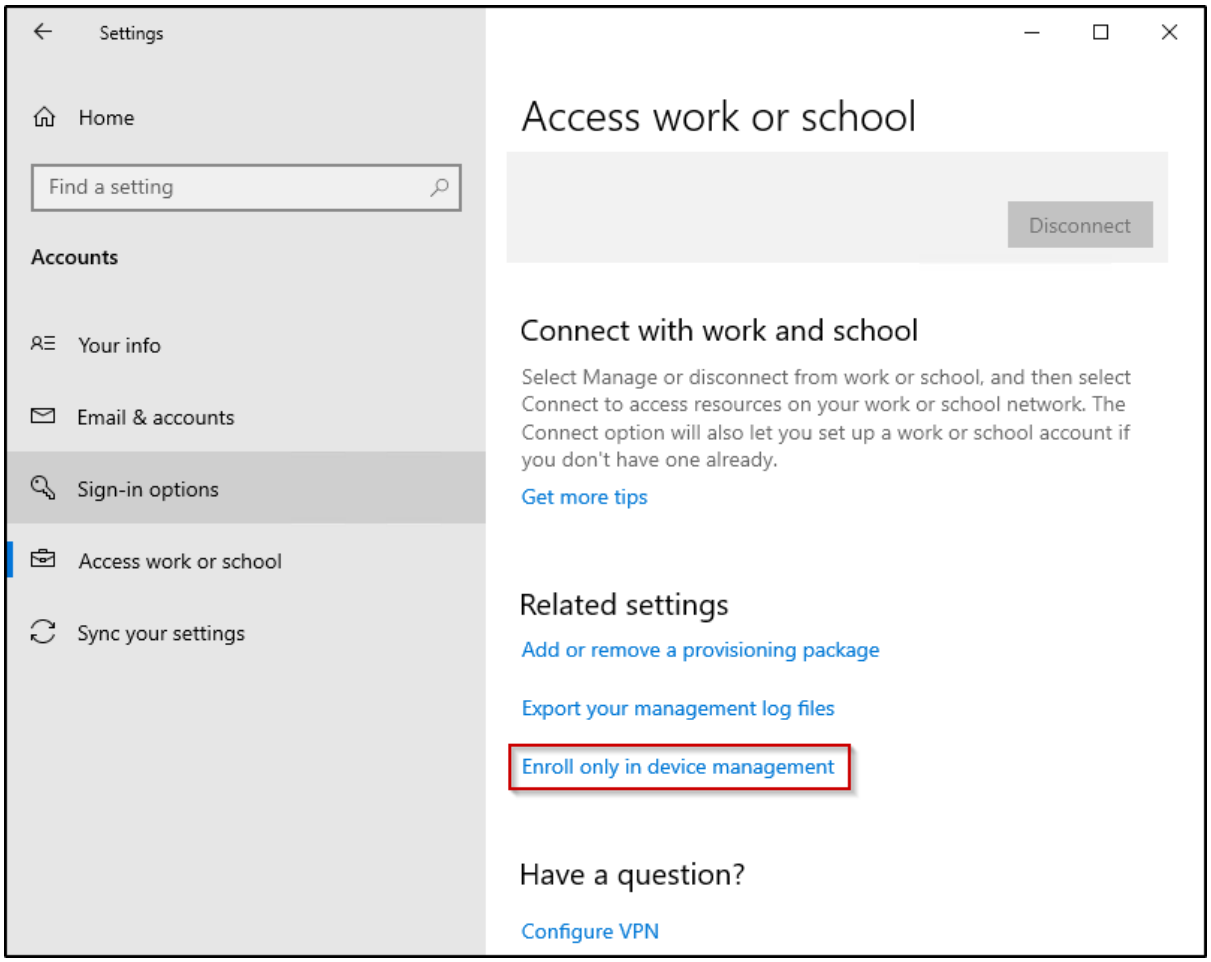
Figur 318: Innrulling av Intune administrerte enheter

Manuell innrulling av co-managed enheter

Vi skal nå demonstrere hvordan man kan rulle inn en co-managed enhet til Intune.

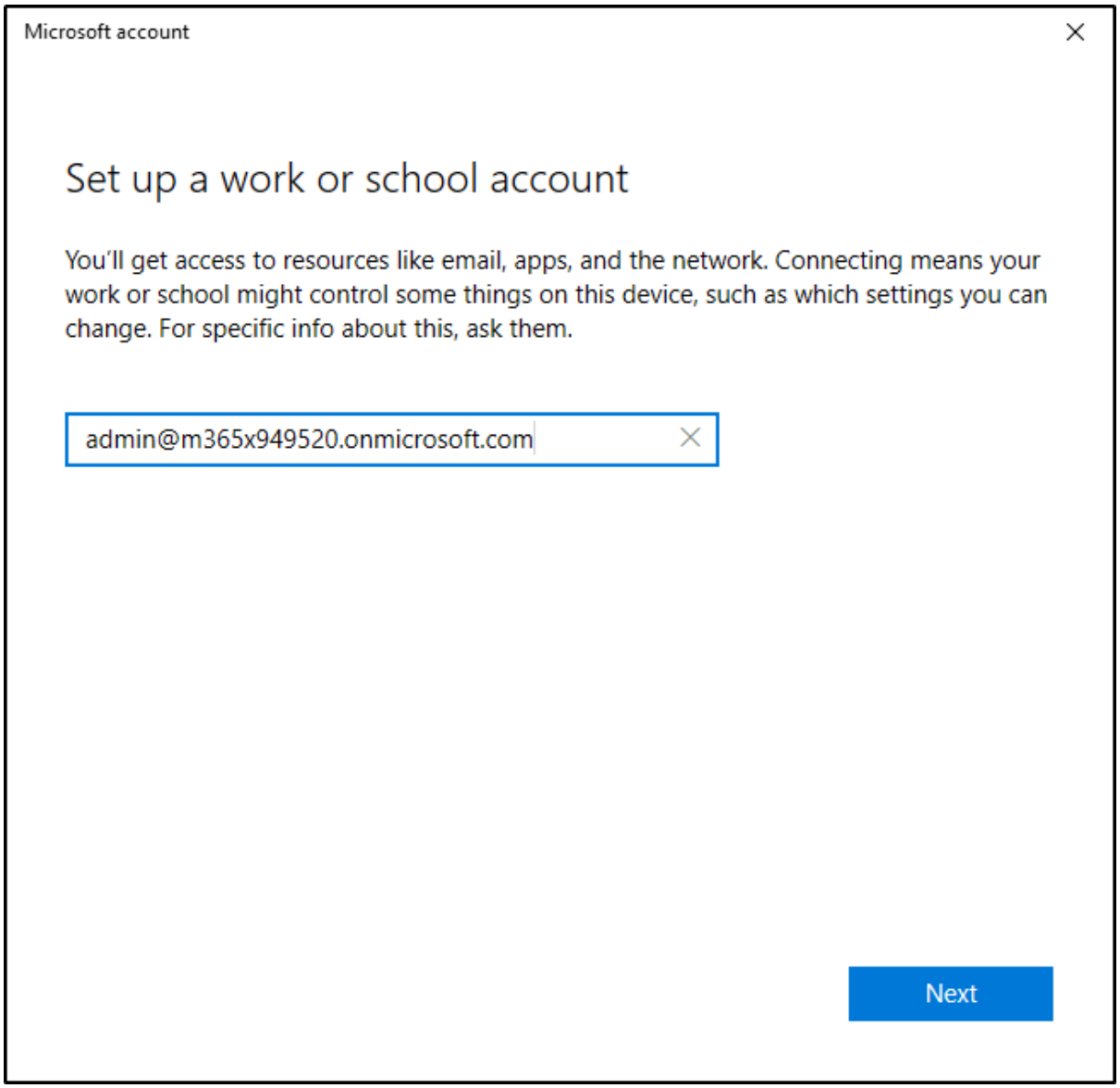
NB: Forutsetter at man er logget inn med lokal administrator bruker på enheten.

Vi starter med å navigere oss til **Access work or school** settings under ***Control panel*** – ***Accounts***. Her velger vi **Enroll only in device management**.



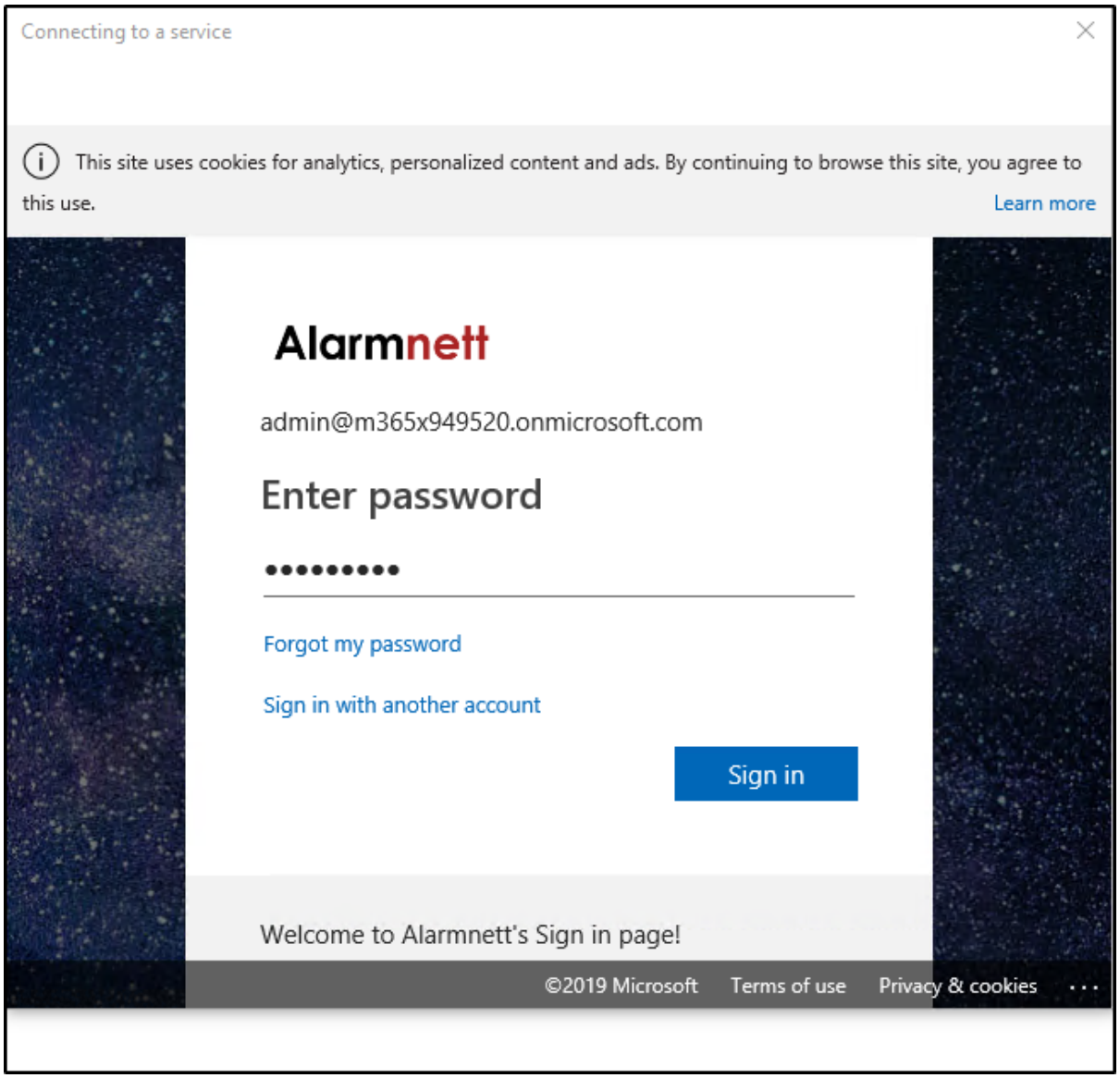
Figur 319: Manuell innrulling av co-managed enheter

Videre skriver vi inn Administratorbruker for Azure tenant og trykker **Next**.



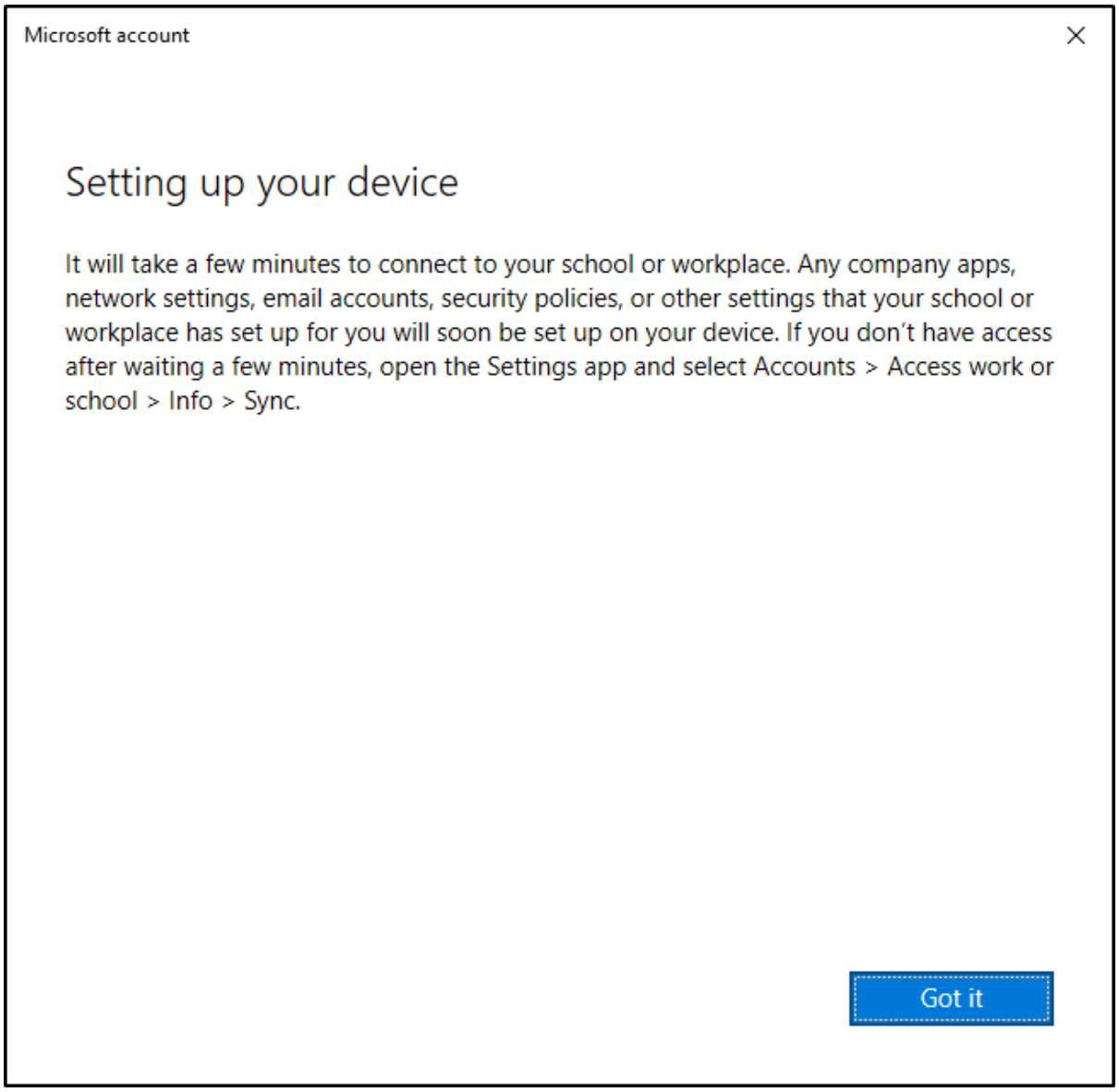
Figur 320: Manuell innrulling av co-managed enheter

Når man får opp Sign in Page til organisasjonen, skriver man inn passord og trykker **Sign in**.



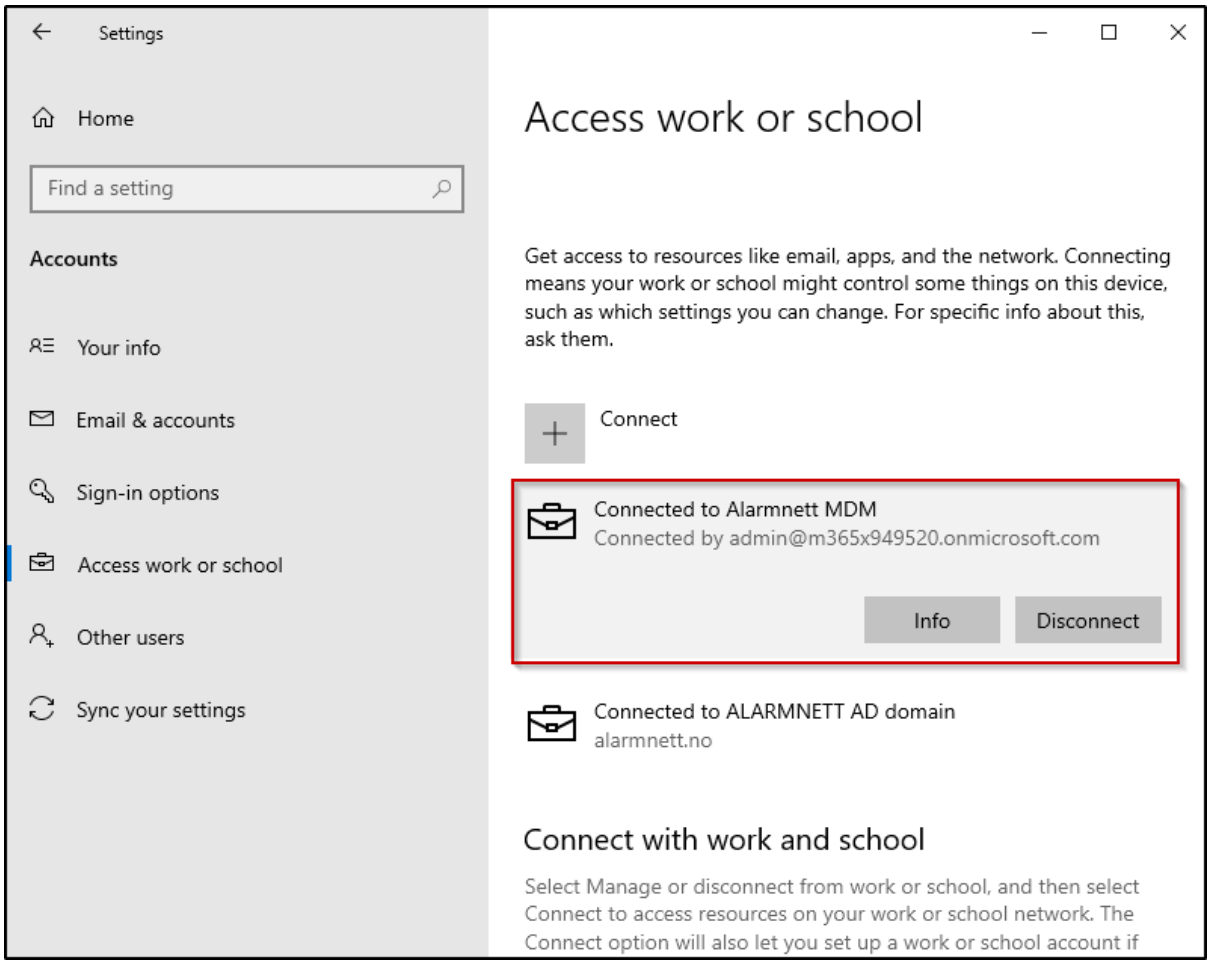
Figur 321: Manuell innrulling av co-managed enheter

Etter litt venting, vil dette vinduet komme opp. Innrulling er i gang og man kan gå tilbake til vanlig arbeid. Dersom innrullingen ikke skulle starte opp, kan man navigere seg til ***Accounts – Access work or school – Info – Sync***.



Figur 322: Manuell innrulling av co-managed enheter

Skjermbildet nedenfor viser at innrullingen er gjennomført.



Figur 323: Manuell innrulling av co-managed enheter

Automatisk innrulling av co-managed enheter

Ved automatisk innrulling av co-managed enheter er dette en prosess som skjer automatisk, som gjør det litt vanskelig å skulle demonstrere. Skal nå forklare hvordan denne prosessen foregår. Før innrulling starter er det verdt å legge merke til at denne prosessen gjelder for enheter som allerede administreres av Configuration Manager. Vi ser derfor bort i fra å skulle melde inn enheten i domenet, og vi forutsetter at enheten har fått tildelt SCCM klienten og har tilgang til blant annet Software Center.

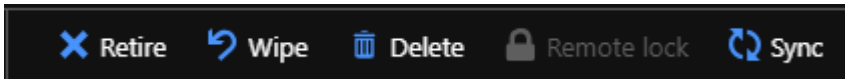
Innrulling skjer først i det group policy for MDM innrulling, fra domene kontrolleren, starter å kjøre på enheten. Enheten vil rulles inn i bakgrunnen, og deretter begynne å installere applikasjoner, samt tildele device configuration policies, device compliance policies og annet som enheten skal ha. Man kan starte denne prosessen ved å flytte enheten over til OU-en som GPO-en er satt til.

Etter en stund, vil enheten bli co-managed og man vil få tilgang til å kunne utføre operasjoner mot maskinen fra Intune.

Til høyre for enhetens navn i enhetsoversikten i Intune, vil man se at enheten nå er «Managed by» **MDM/ConfigMgr Agent**, som vist nedenfor.

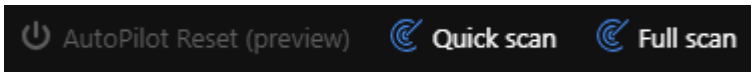
Figur 324: Automatisk innrulling av co-managed enheter

I skjermbildene nedenfor ser vi noen av operasjonene man kan gjøre mot enheten fra Intune. Enkelte operasjoner som man burde merke seg, er **Wipe**, **Retire**, **Restart** og **Fresh start**.
Wipe, kan brukes for å slette alt av data på enheten og resette enheten til sin opprinnelige tilstand (Factory default settings). Dette er en veldig viktig operasjon å kjenne til i et sikkerhetsperspektiv, da dette kan brukes for å hindre at f.eks. bedriftshemmeligheter kommer på avveie.
Retire, er en operasjon som brukes for å fjerne enhetens tilgang til ressurser i Intune.
Restart, er en operasjon som brukes til å kunne restarte enheten remote, uten å koble seg til enheten.
Fresh start, brukes for å slette alt av forhåndsinstallerte win32 applikasjoner som ofte kommer med på en enhet, samt installere Windows 10 på enheten.

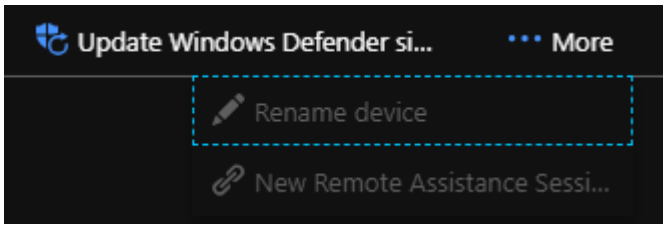


Figur 325: Automatisk innrulling av co-managed enheter

Figur 326: Automatisk innrulling av co-managed enheter



Figur 327: Automatisk innrulling av co-managed enheter

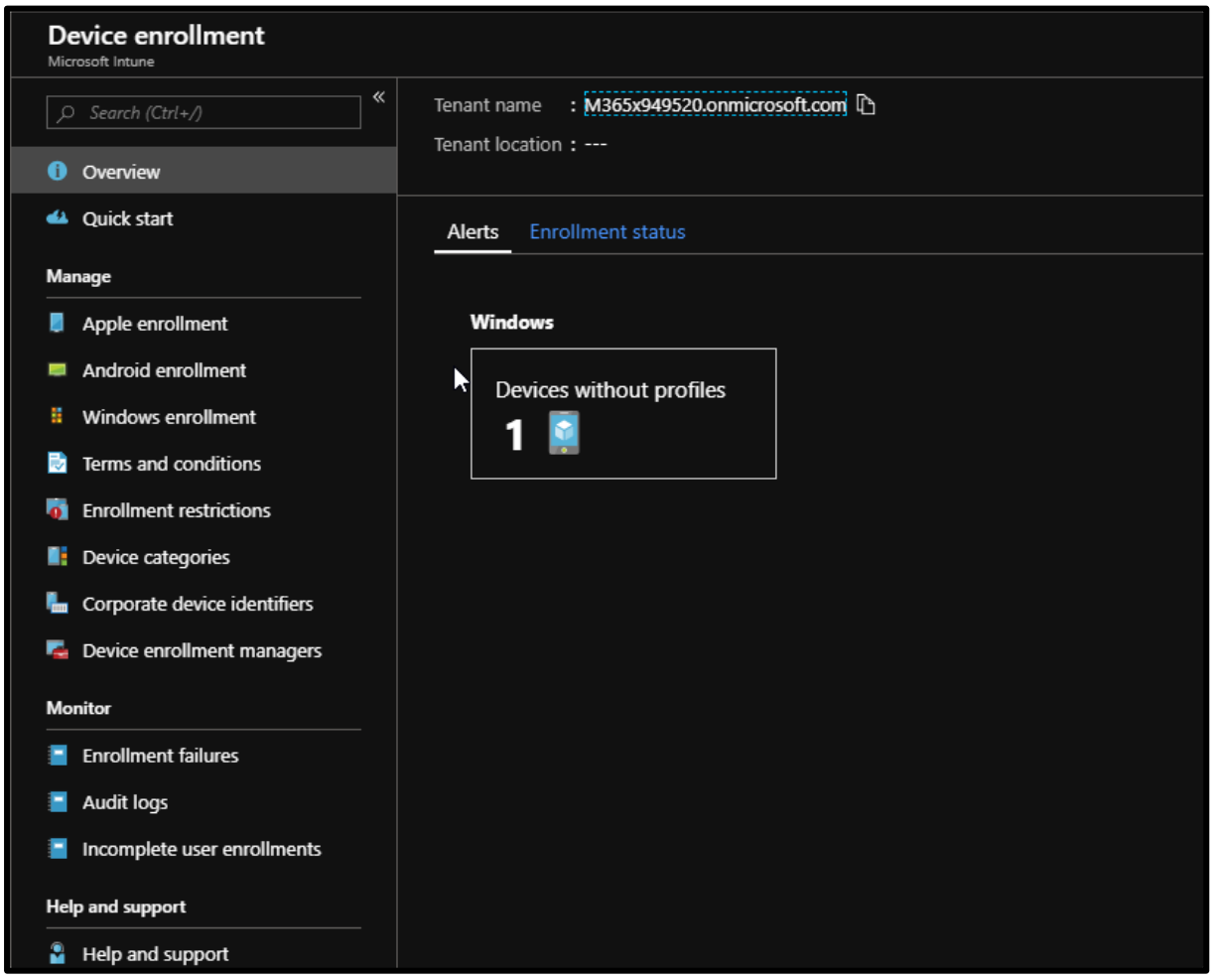


Figur 328: Automatisk innrulling av co-managed enheter

Tilordning av bruker til enhet i Autopilot

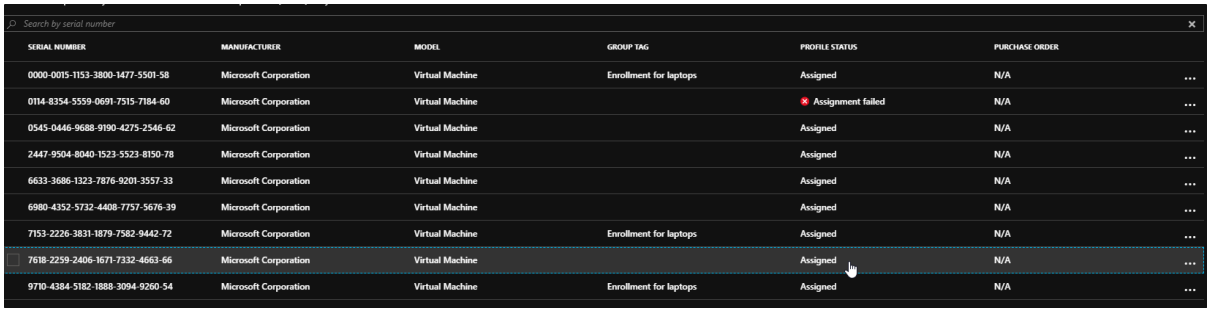
Hvis man tilordner enheten en gruppe med en profil som sier at alle enhetene vil rulles inn til autopilot enheter automatisk så vil dette komme opp etter hvert.

Man kan følge dette under device enrollment. Med en gang maskinen kommer inn hit (merk at den ikke har en profil med en gang den kommer til Autopilot devices), kan vi tilordne en bruker til enheten. Det går bra at den ikke har fått tilordnet profil med en gang, så lenge maskinen er meldt i en gruppe med en profil tilordnet. Profilen vil da bli tilordnet etter hvert av seg selv. Vi befinner oss på ***oversiktsmenyen*** til ***Device enrollment*** i bildet under.



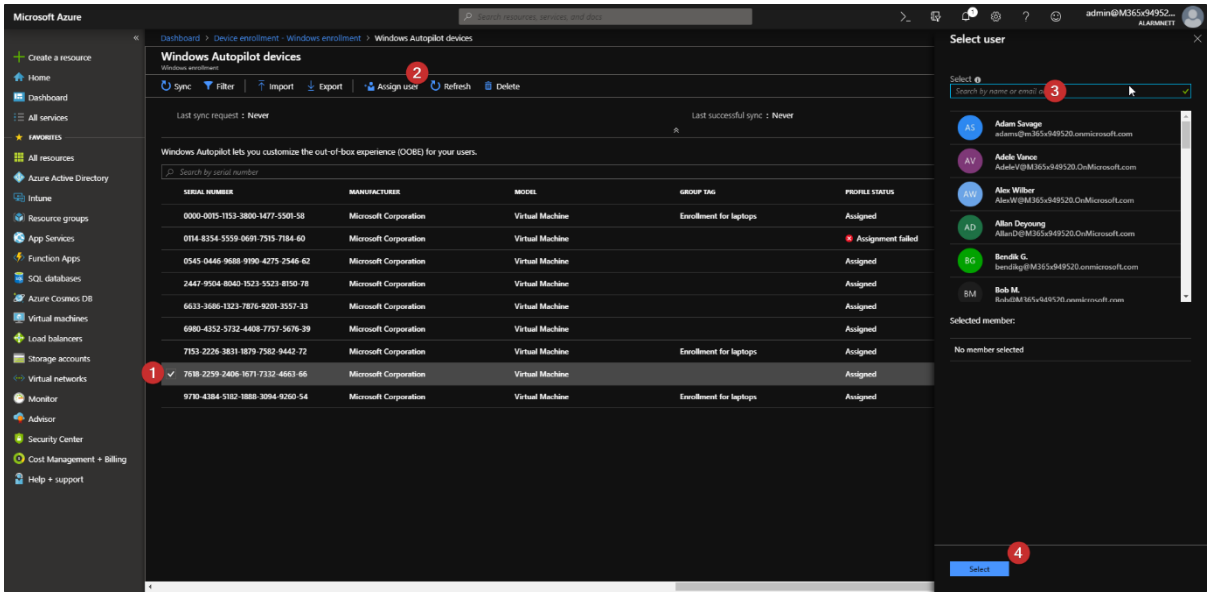
Figur 329: Tilordning av bruker til enhet i Autopilot

Da kan vi trykke oss inn til enhetene enten ved å trykke på vinduet hvor det står **Devices without profiles**, eller ved å trykke på **Windows enrollment** og **Devices**.



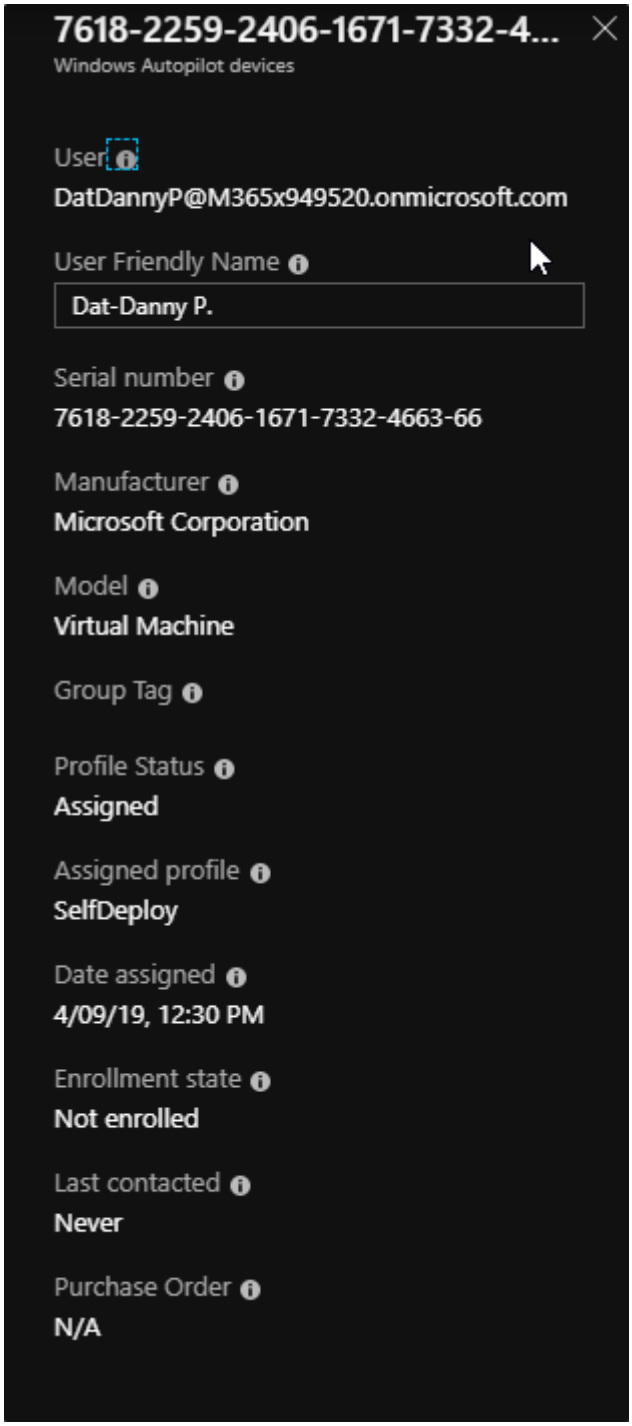
Figur 330: Tilordning av bruker til enhet i Autopilot

Vi kan nå tilordne maskinen til en bruker, siden den vil bli tilordnet en profil av seg selv. Det gjøres ved å **huke av maskinen** – **Assign user** – søk etter navn på bruker og **velg bruker** – **Select**



Figur 331: Tilordning av bruker til enhet i Autopilot

Nå har vi tilordnet en bruker til maskinen. Dette kan vi bekrefte ved å trykke på **maskinen** og vi får opp informasjon om maskinen.



Figur 332: Tilordning av bruker til enhet i Autopilot

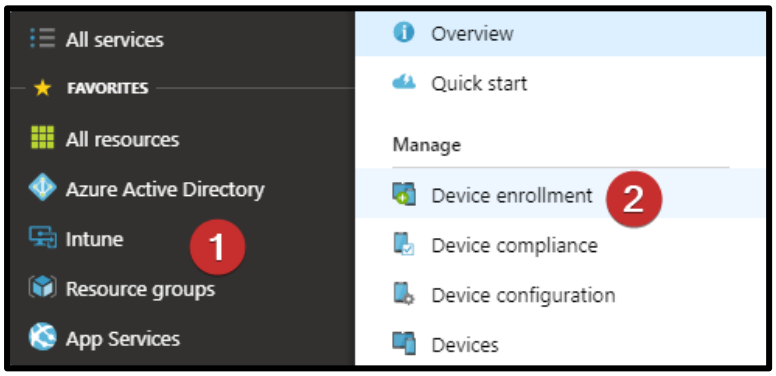
Innrulling av Android til Intune

Det fine med Intune er at den kan håndtere mobile enheter. Dette inkluderer også mobiler, og kan gjøres veldig enkelt. Vi benytter oss av en emulator for å illustrere dette. For enkelhetsskyld har vi valgt å utføre dette for Android, da det ikke kreves noen rettigheter eller lisenser, men i en virkelig situasjon er det minst like lett for å utføre dette for iOS/ Windows mobil-enheter.

Vi starter da med å koble Intune med Google play.

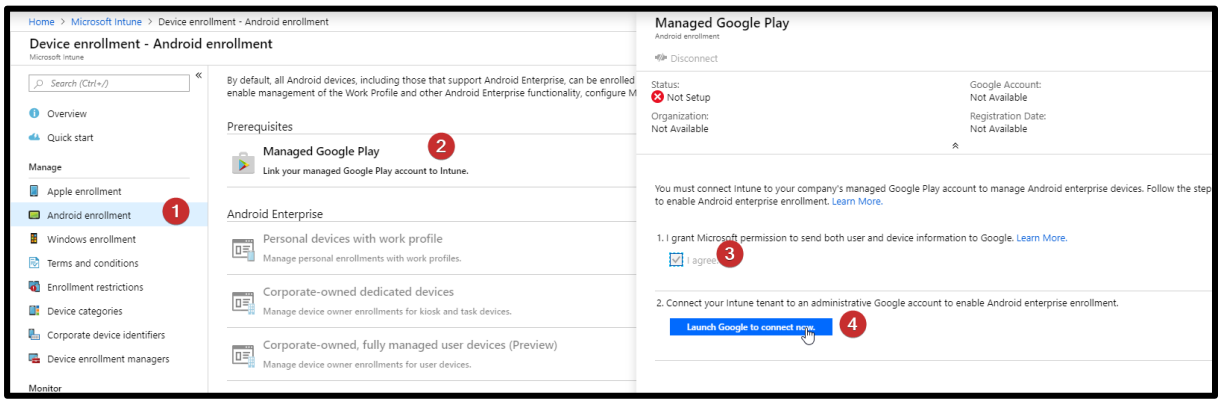
Kobling av Intune til Google play

Det gjør vi ved å gå til ***Intune*** og til ***device enrollment***.



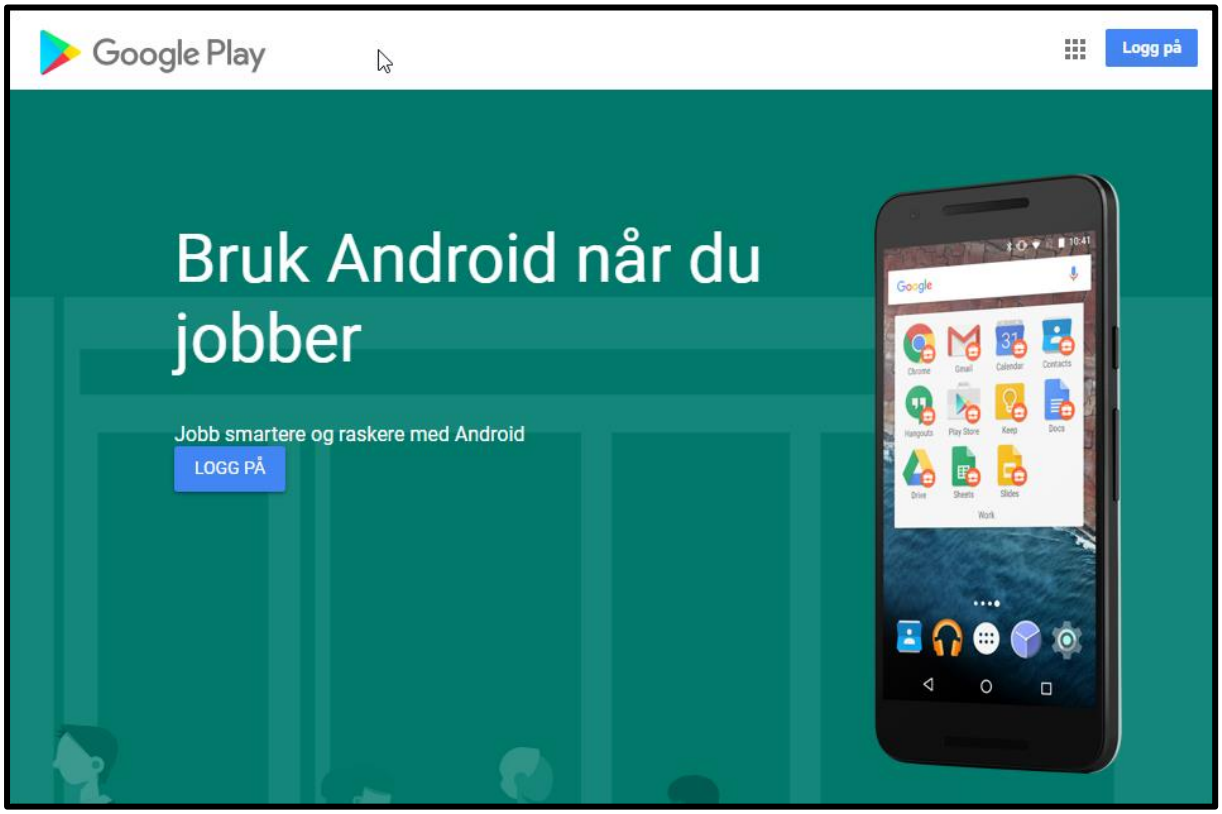
Figur 333: Kobling av Intune til Google play

Vi går så til ***Android enrollment*** trykker på **managed google play**. Her ser vi at vi ikke har satt opp noen konto enda og velger **I agree** og trykker **launch google to connect now** for å koble til.



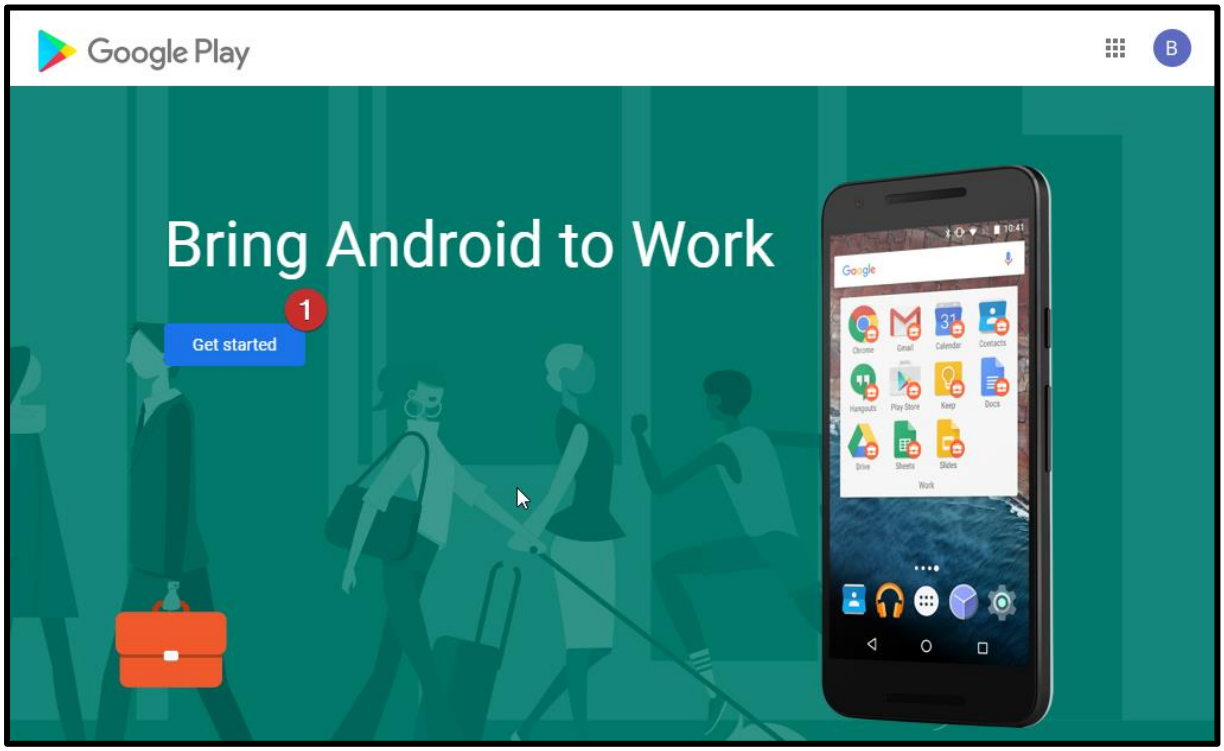
Figur 334: Kobling av Intune til Google play

Du vil få opp et nytt vindu hvor du må logge på google om du ikke allerede har logget på. Vi vil nå logge på med en google bruker.



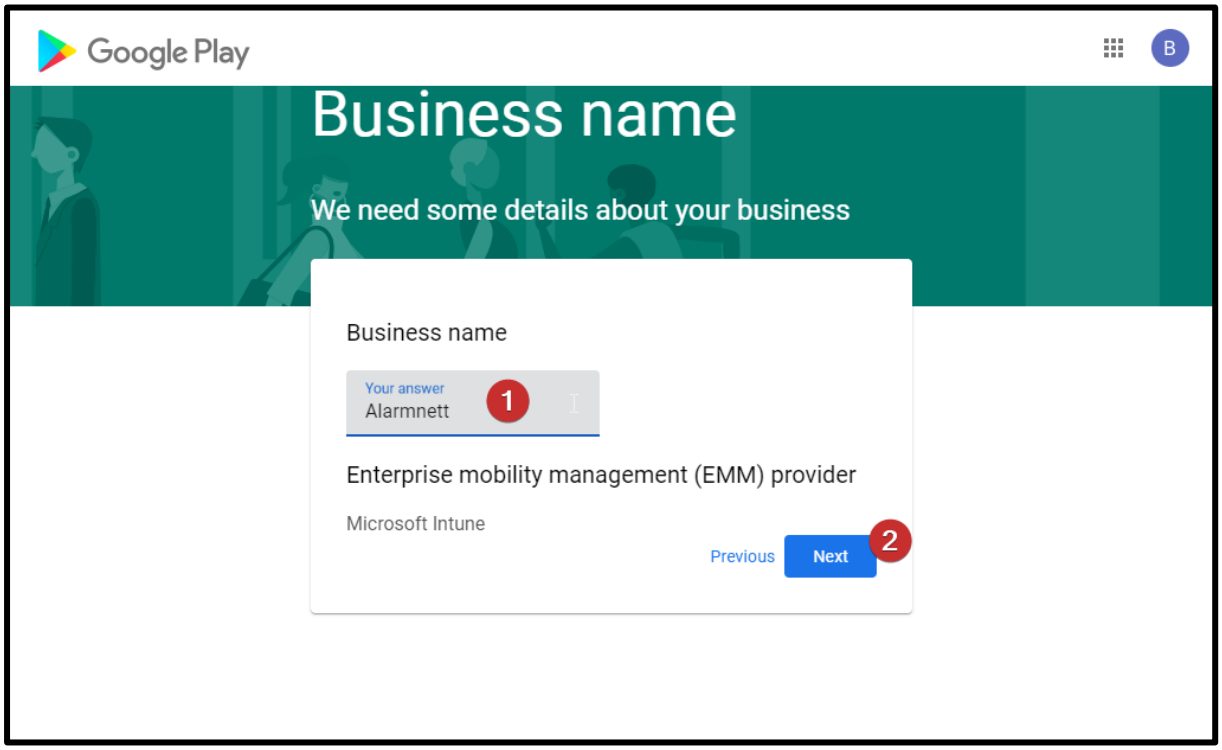
Figur 335: Kobling av Intune til Google play

Vi vil så komme til en side som sier Bring Android to work og fortsetter med å trykke **Get Started.**



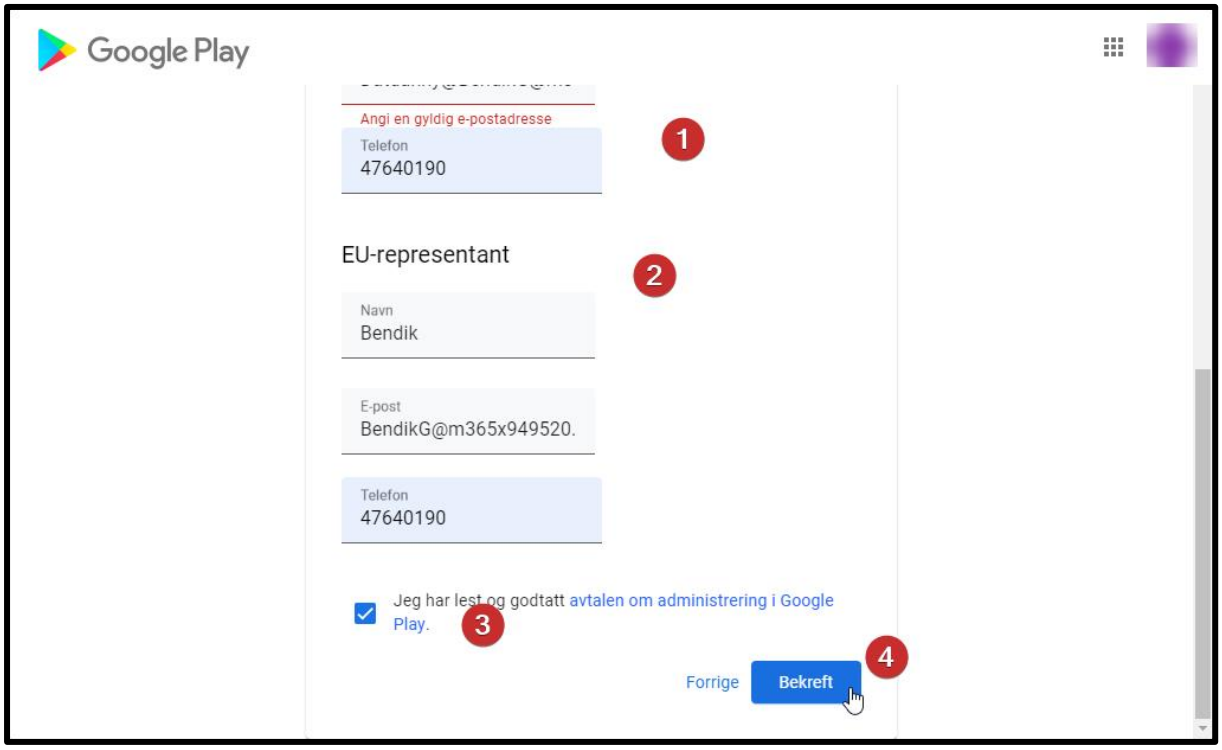
Figur 336: Kobling av Intune til Google play

På neste side fyller vi ut navnet til bedriften og trykker neste.



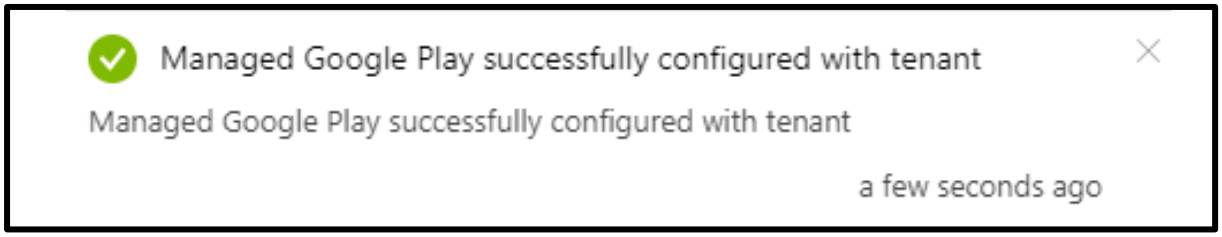
Figur 337: Kobling av Intune til Google play

Her må vi fylle ut kontaktinformasjon for de to, som Google skal kontakte angående informasjonen de får tilgang til gjennom deres tjenester. Dette er bare hvis de noen gang måtte kontakte bedriften, så må de ha noen å kontakte.



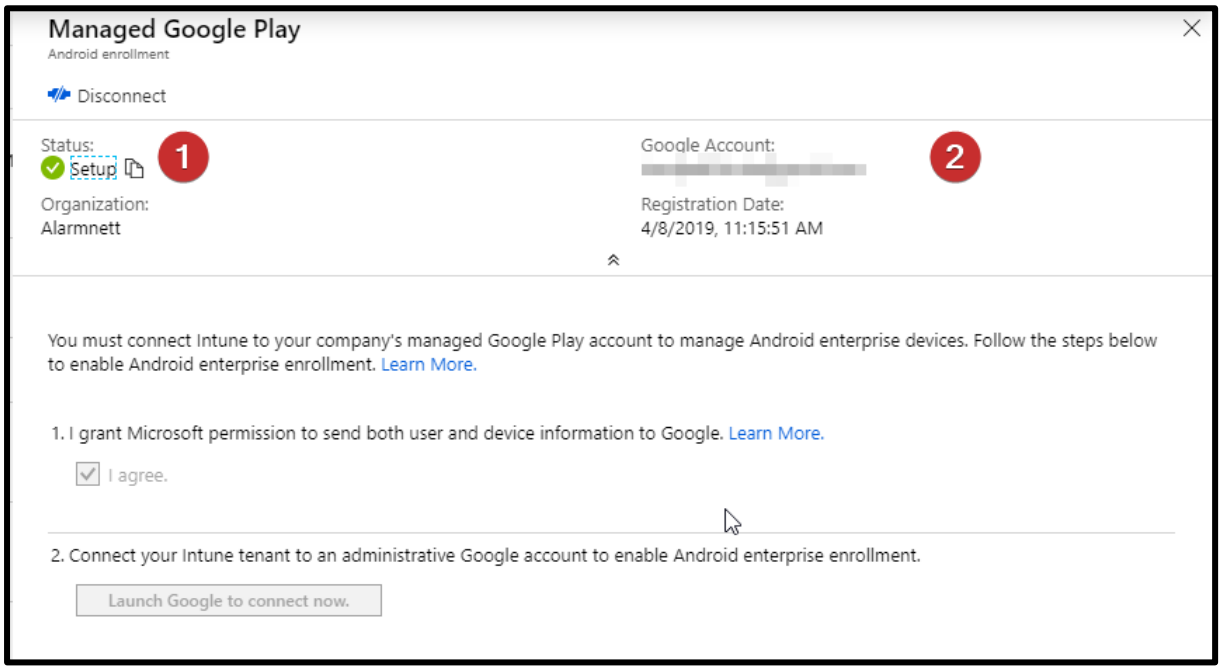
Figur 338: Kobling av Intune til Google play

Du vil få opp en melding som sier at google play har blitt tilkoblet til vår tenant.



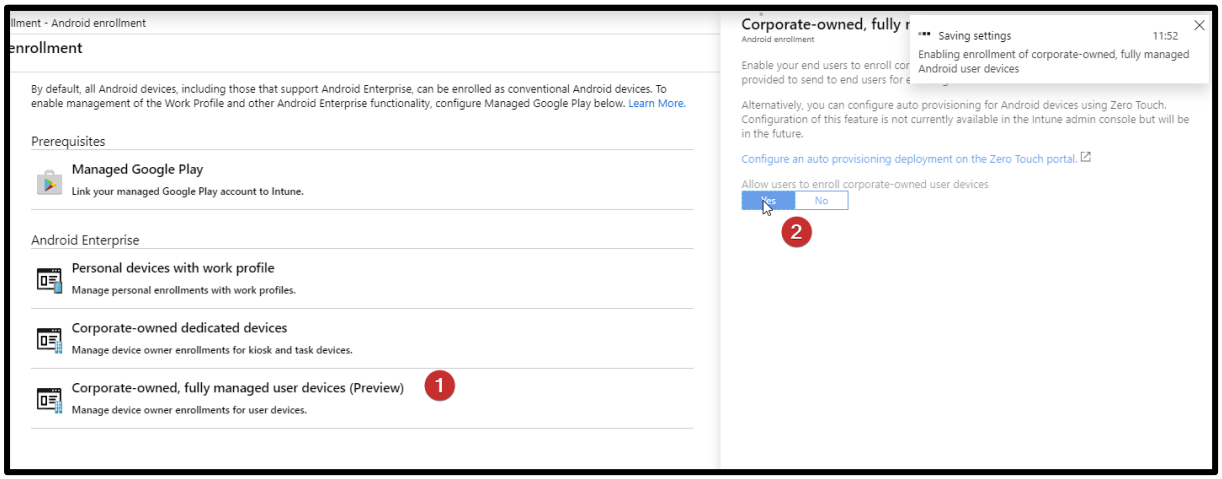
Figur 339: Kobling av Intune til Google play

Da kan vi gå tilbake til siden og se om vi får kontakt med Google play.



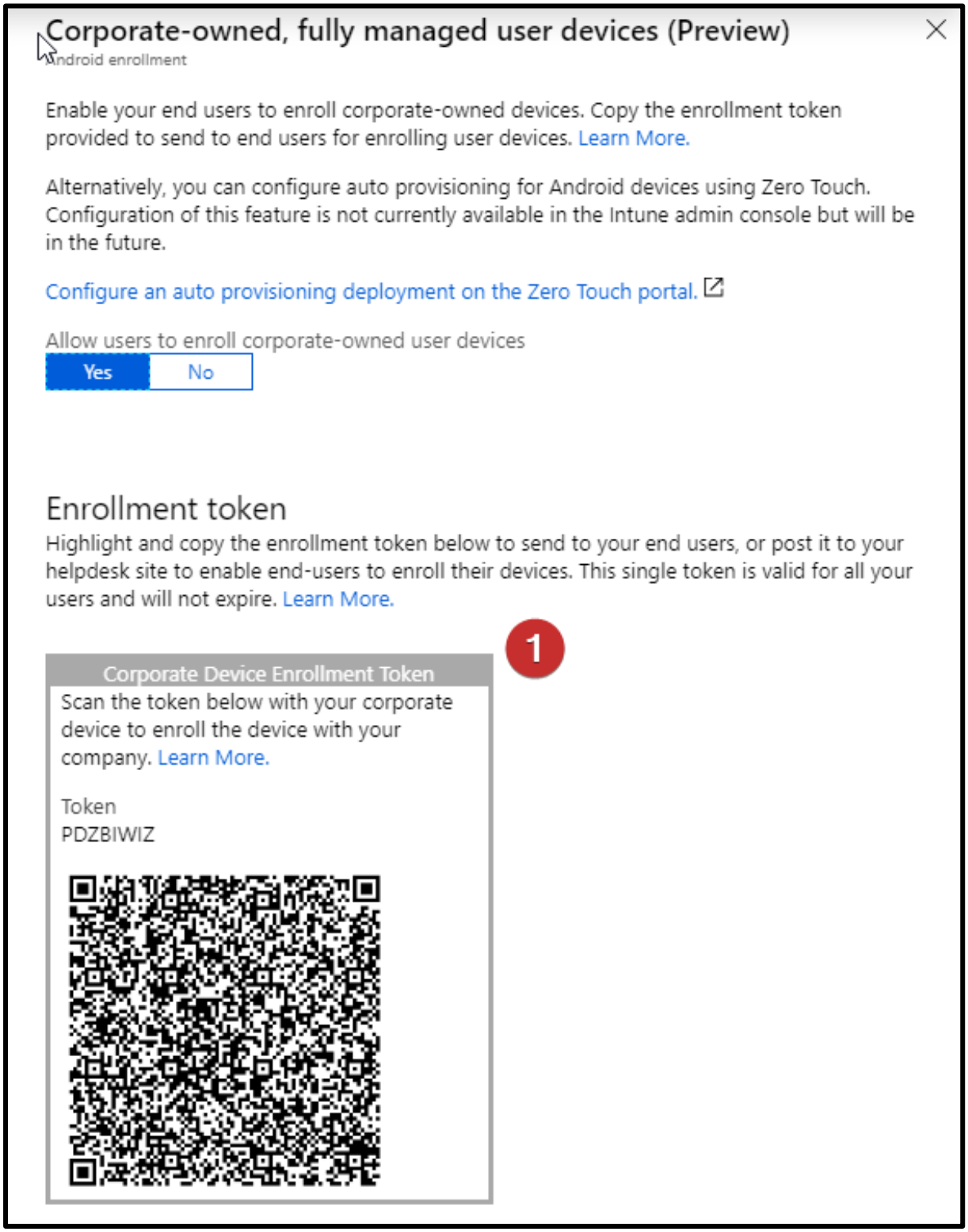
Figur 340: Kobling av Intune til Google play

Nå kan vi få brukerne til å rulle inn til vårt domene. Vi kan også skru på slik at enhetene kan automatisk rulles inn i domenet ved å gå til ***Corporate-owned - fully managed user devices (Preview)*** og trykke på **Yes** under ***Allow users to enroll corporate-owned user devices***.



Figur 341: Kobling av Intune til Google play

Du skal da få opp en QR-kode. Da får vi to måter å rulle inn enhetene på. Via ***Play store*** eller via ***QR kode.***

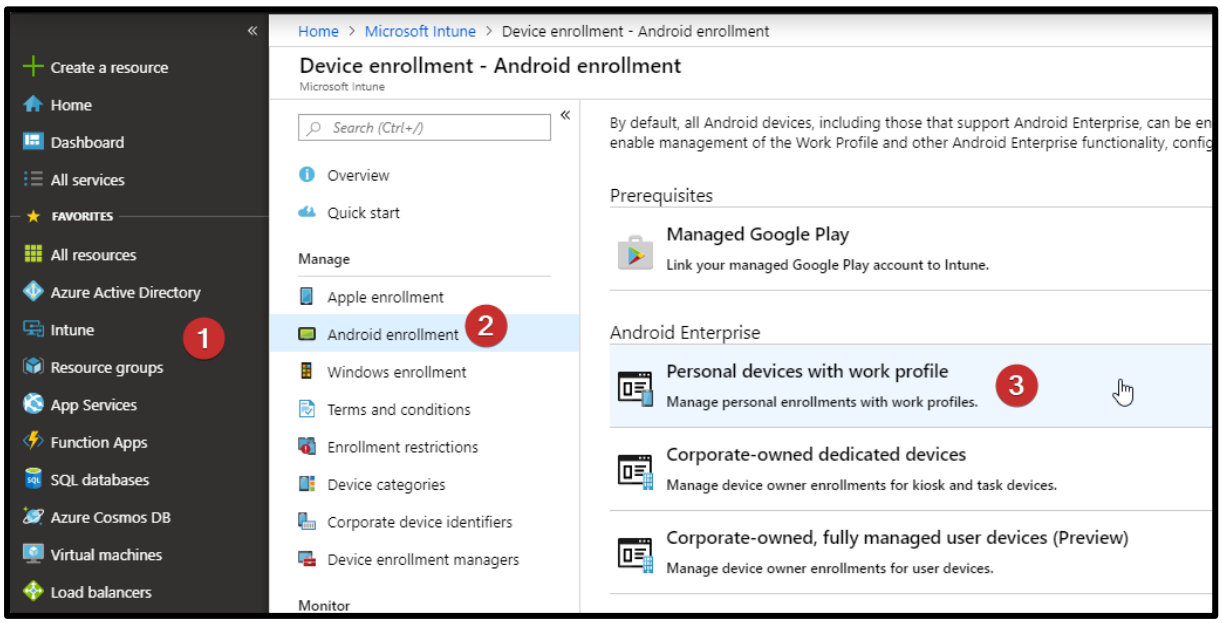


Figur 342: Kobling av Intune til Google play

Enrollment Profiles (Android)

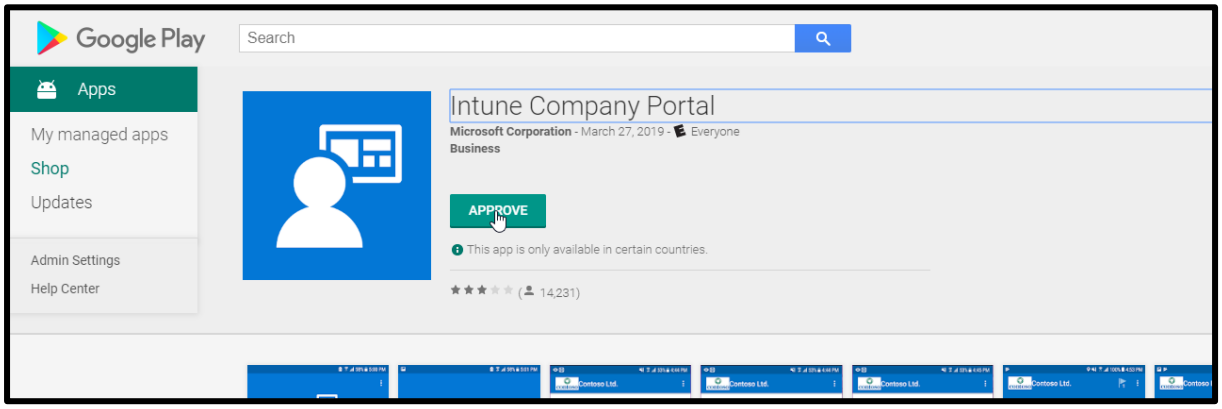
Man kan også konfigurere enrollment profiles for å sette restriksjoner og kontrollere innrullingen til Intune bedre.

Da går vi til ***Android enrollment*** under ***Intune*** og trykker på **Personal Devices with work profiles**



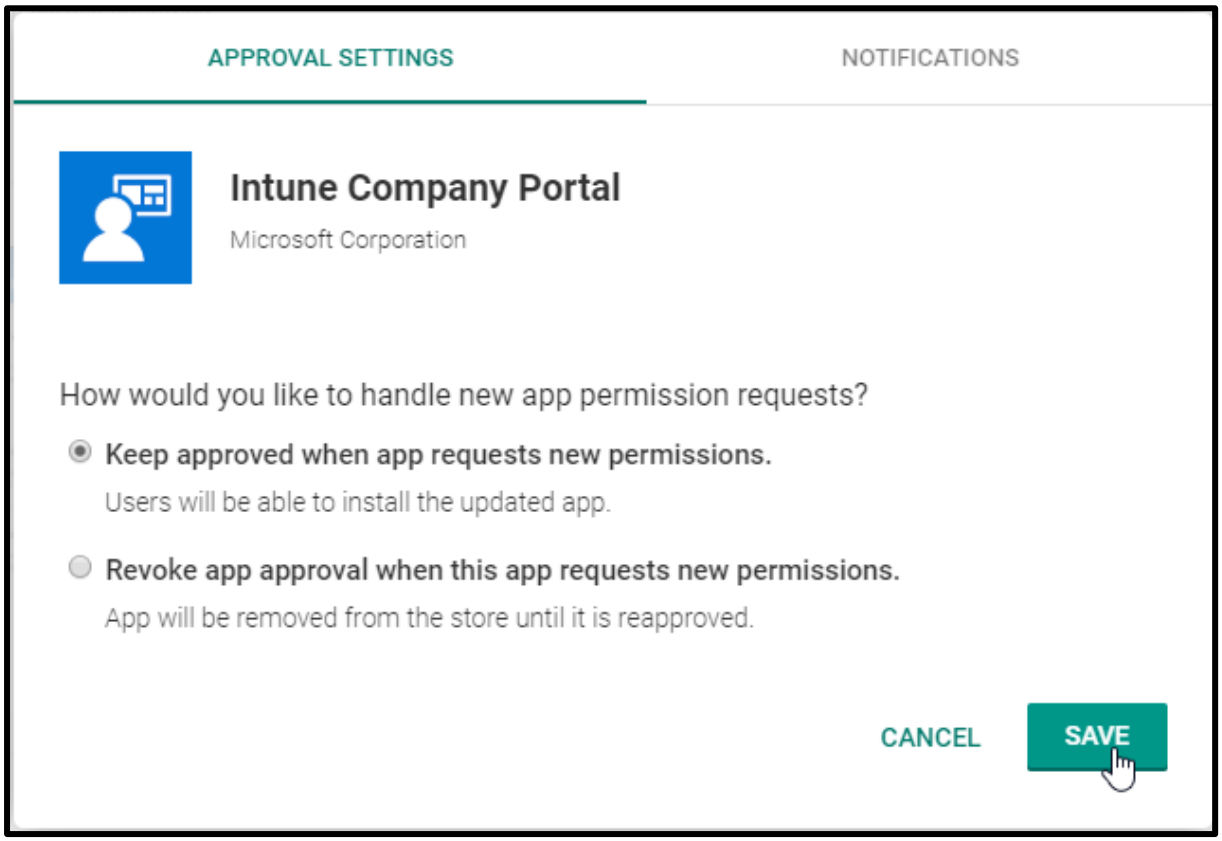
Figur 343: Enrollment Profiles (Android)

Vi vil komme til en ny side og trykker på **Approve.**



Figur 344: Enrollment Profiles (Android)

Velger «*Keep approved when app requests new permissions*» og trykker **Save.**



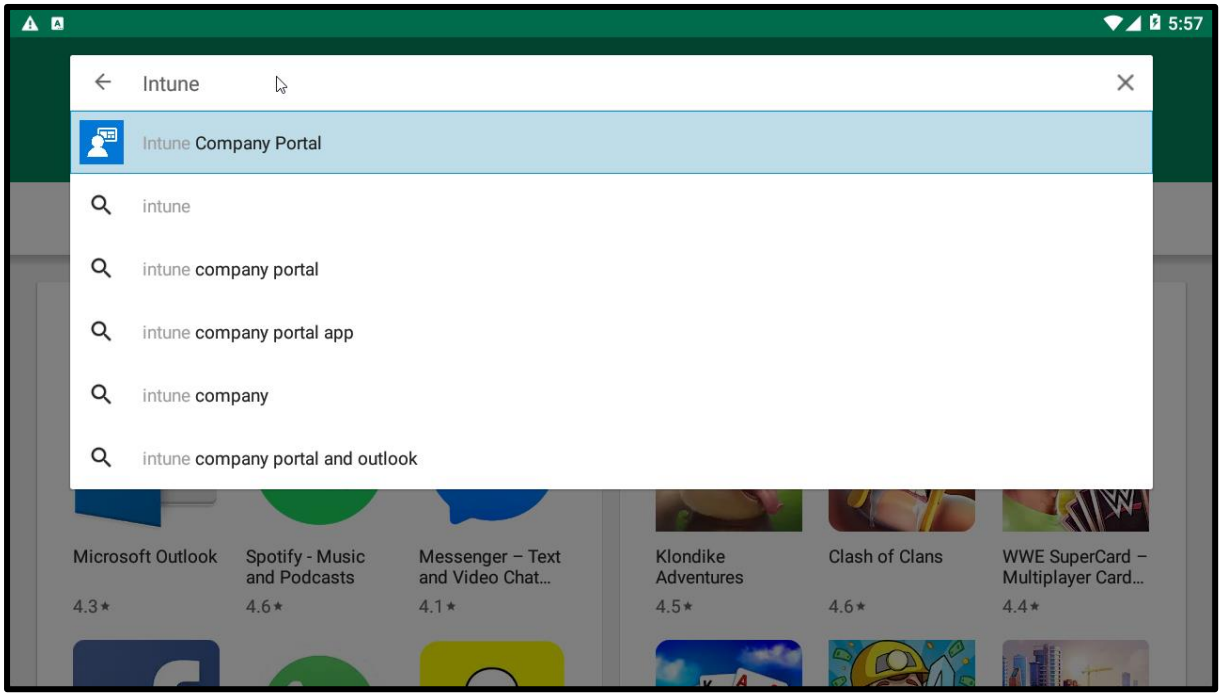
Figur 345: Enrollment Profiles (Android)

Innrulling av Android enheter

Det er generelt to måter å rulle inn Android enhetene på enten via Intune Company portal eller via Tokens. Det er også en stor forskjell mellom resultatet, men i bunn og grunn vil man kunne styre dem fra Intune når de er rullet inn. Intune Company Portal vil rulle inn hele Android enheten slik at man får full kontroll over enheten, mens Innrulling via token vil sette av et avgrenset område på mobilen til arbeidsrelaterte ting som bedriften har kontroll over.

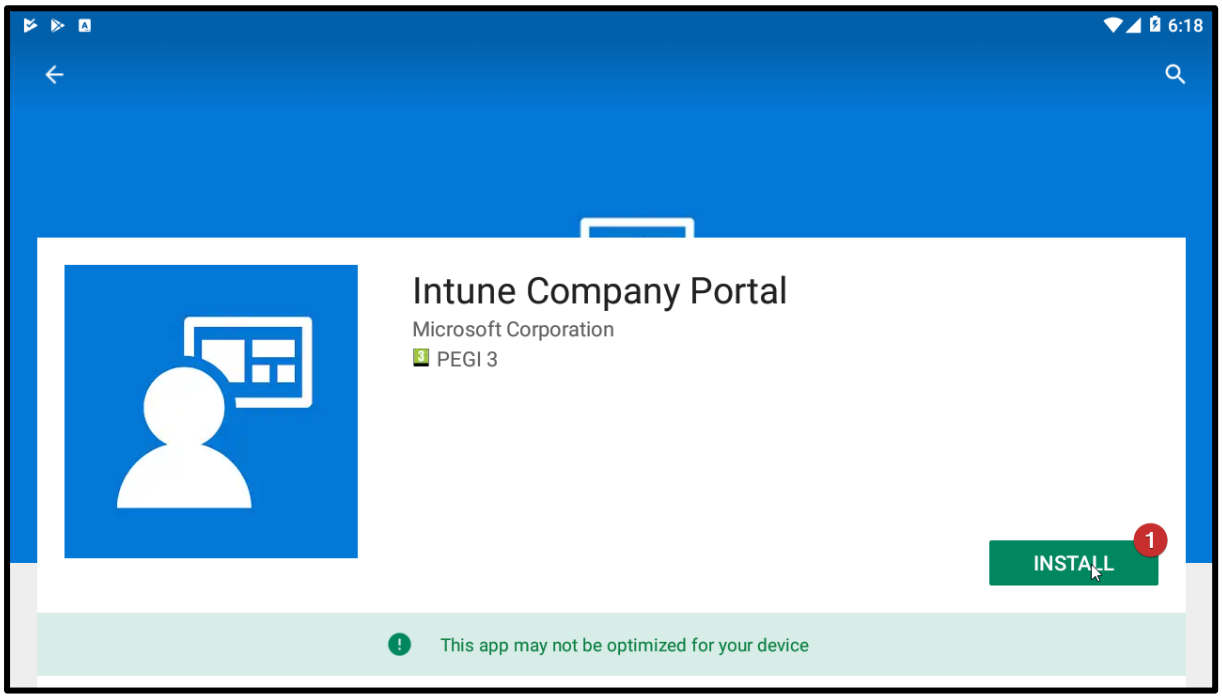
Via Play Store

Logg inn på enheten din og gå til ***Play Store.*** Her søker du på **Intune Company portal.**



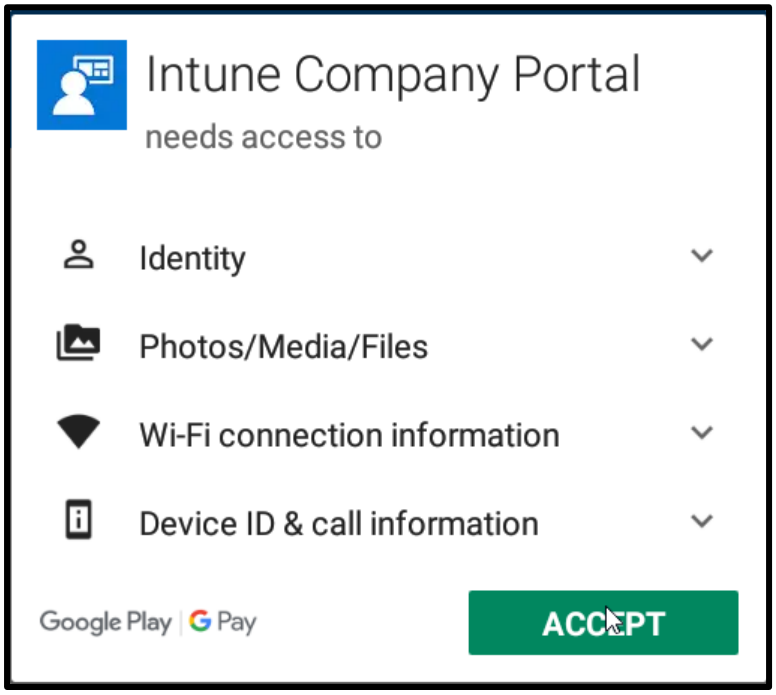
Figur 346: Innrulling av Android enheter - Via Play Store

Trykk på **Intune Company portal** som er utgitt av Microsoft og så **Install.**



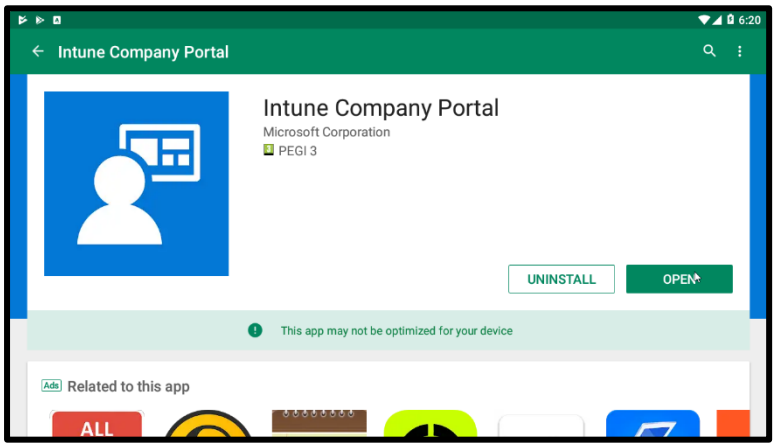
Figur 347: Innrulling av Android enheter - Via Play Store

Vi vil få opp et nytt vindu hvor vi bare trykker **Accept.**



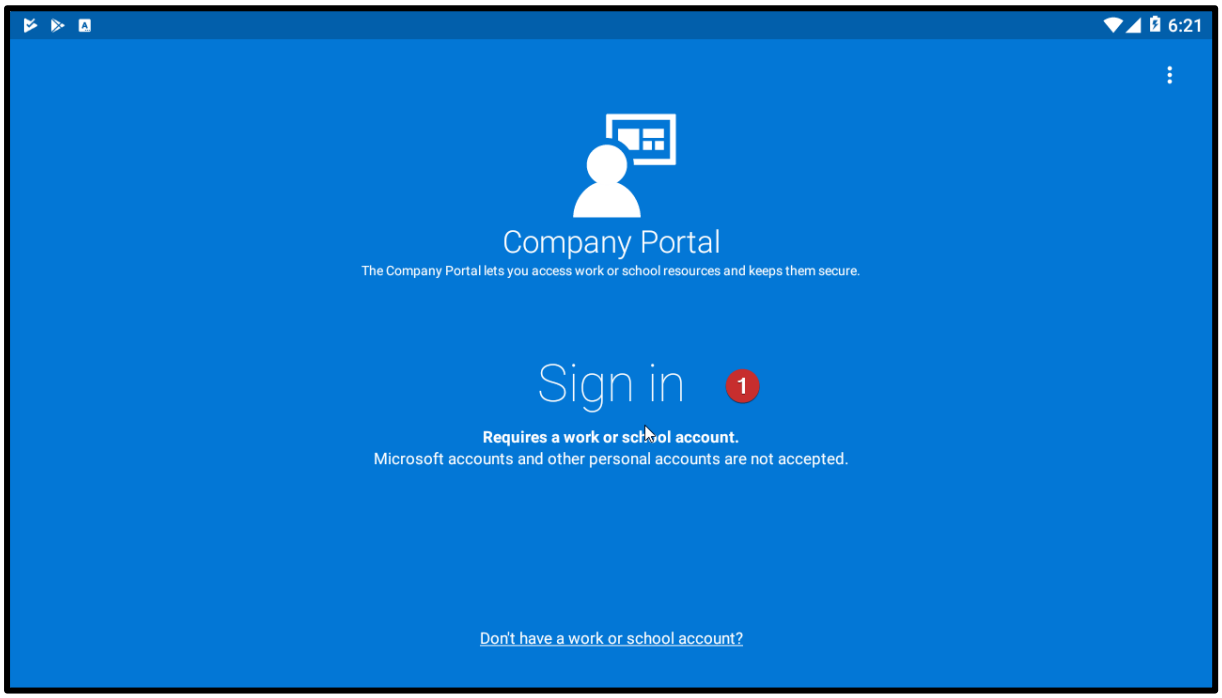
Figur 348: Innrulling av Android enheter - Via Play Store

Nå får vi mulighet til å åpne appen, ved å trykke **OPEN.**



Figur 349: Innrulling av Android enheter - Via Play Store

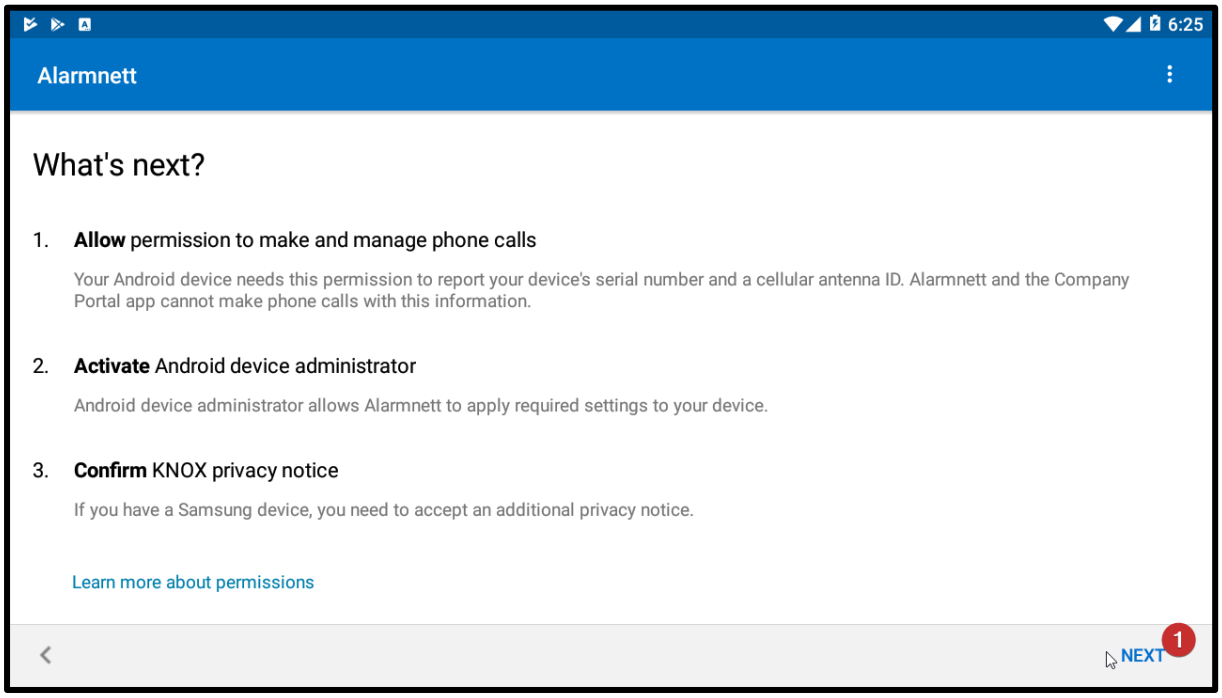
Bildet kan virke litt forvirrende men det er bare å trykke på **Sign in**.



Figur 350: Innrulling av Android enheter - Via Play Store

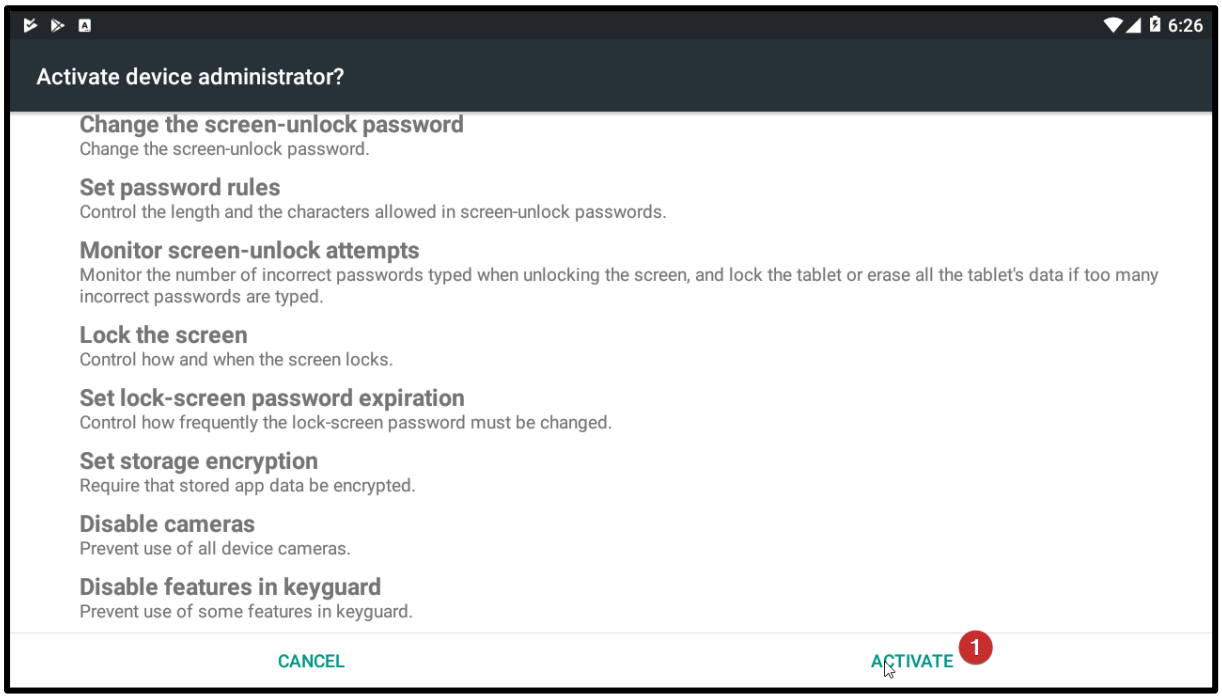
Det kan hende du blir bedt om å logge inn på nytt og da er det bare å logge seg inn med brukeren din fra Intune, eller arbeidsplassen.

Trykker så på **next**.



Figur 351: Innrulling av Android enheter - Via Play Store

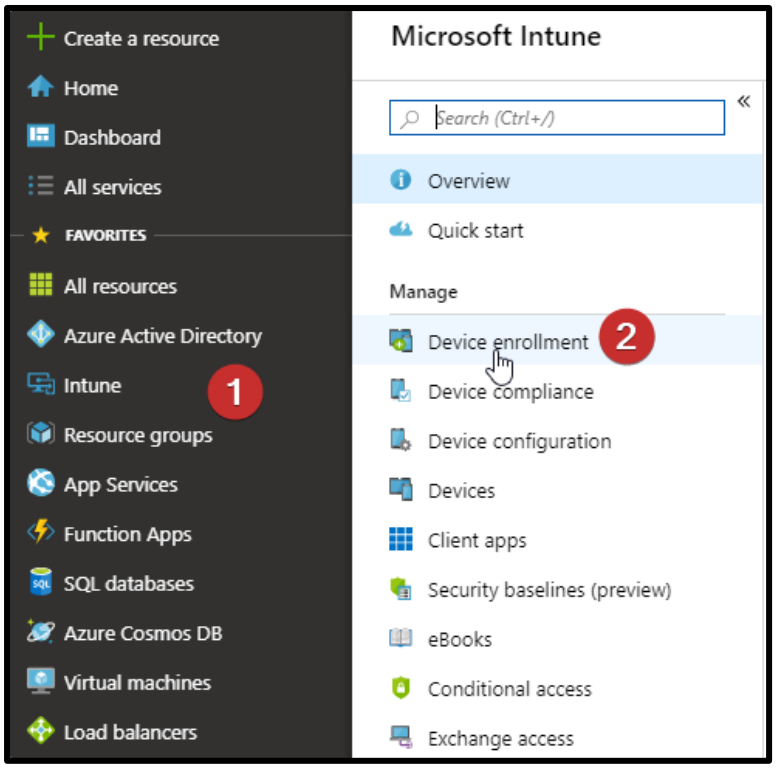
Her kan vi trykke på **Activate**.



Figur 352: Innrulling av Android enheter - Via Play Store

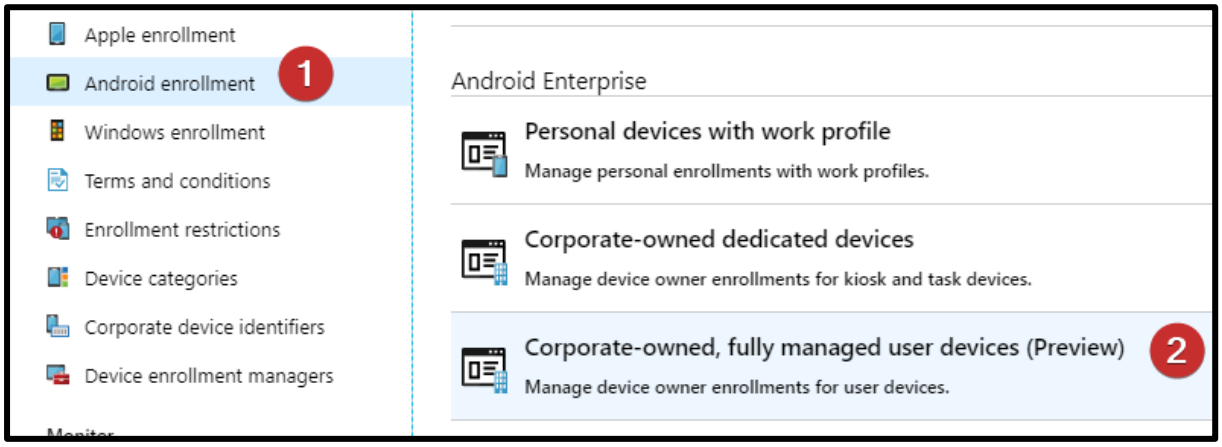
Via QR-kode

Først kan vi nevne at denne funksjonen er en preview-funksjon, som vil si at funksjonen ikke er ferdigutviklet. For vår del vil dette si at den kun støtter fysiske enheter og ikke virtuelle maskiner. For å utføre denne måten å rulle inn på, må vi sette opp tokens på intune. Dette gjøres under ***Android Enrollment***. For å komme oss dit kan vi navigere til ***Intune*** – **Device enrollment.**



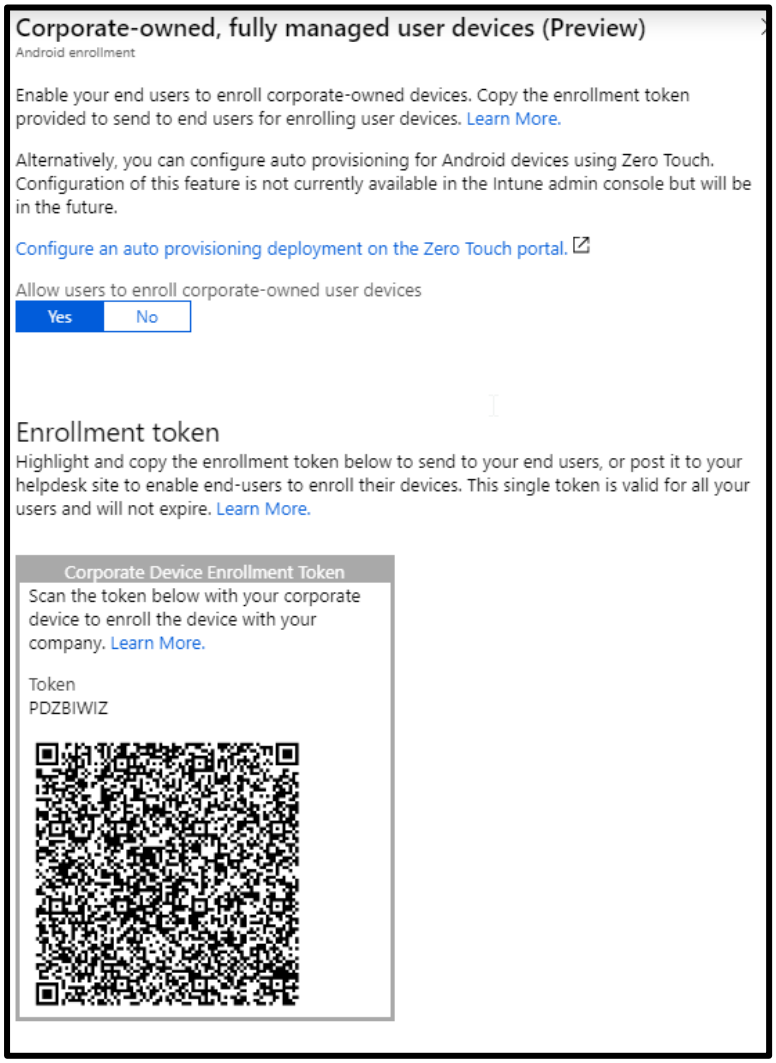
Figur 353: Innrulling av Android enheter - Via QR-kode

Vi trykker på ***Android enrollment*** **– Corporate owned, fully managed user devices (Preview).**



Figur 354: Innrulling av Android enheter - Via QR-kode

Her vil du få opp en Token som man kan rulle inn brukerne med. Ta vare på den, vi kommer til å få bruk for den.

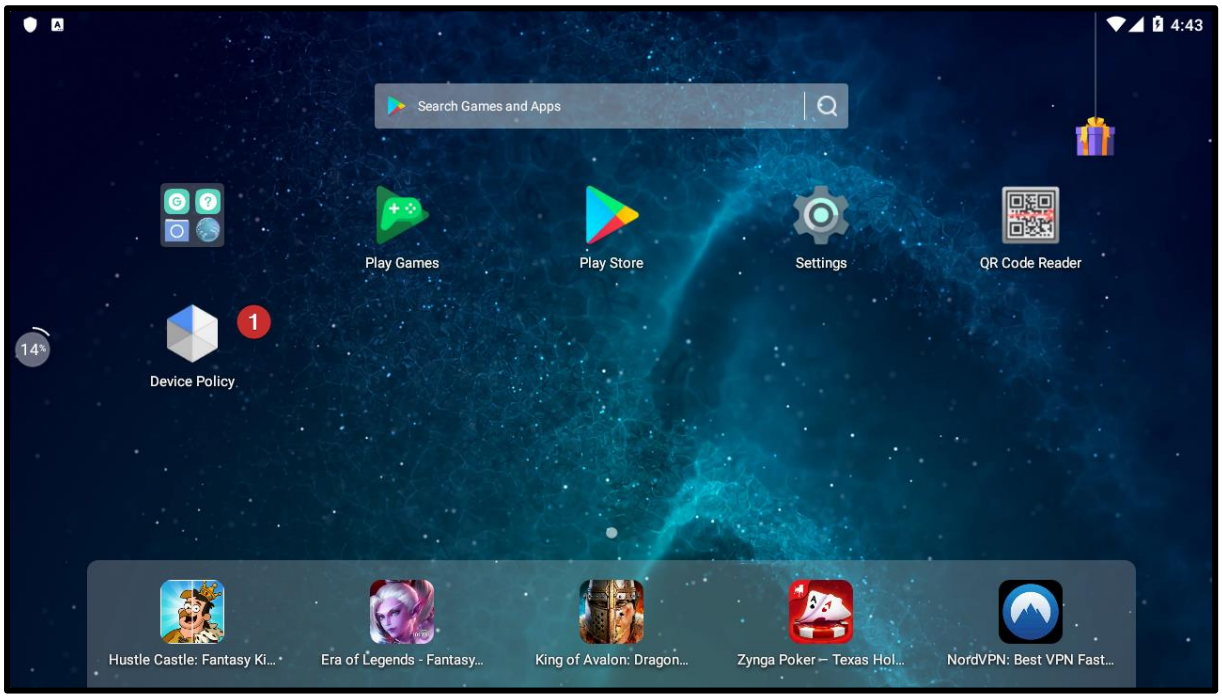


Figur 355: Innrulling av Android enheter - Via QR-kode

For å kunne rulle inn maskinen laster vi ned Android Device Policy på enheten vi skal rulle inn. Legger ved bilde av QR-kode for å gjøre det lettere for brukere å finne riktig applikasjon. Vi har ikke satt opp denne QR-koden til å vare for alltid, så vi tar ikke ansvar for om koden har løpt ut. Det er derimot mulig å sette opp sin egen QR-kode, eller bare laste ned applikasjonen fra Play store.

Figur 356: Innrulling av Android enheter - Via QR-kode

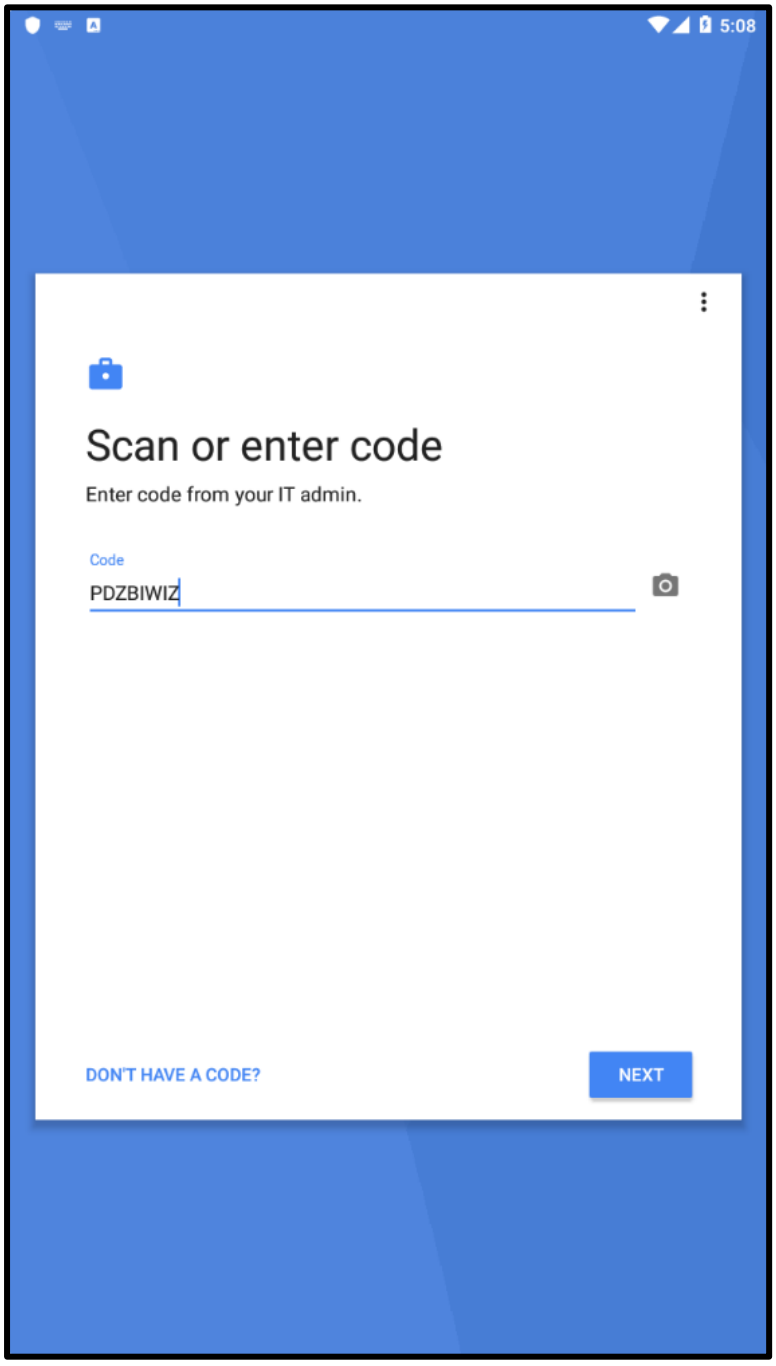
Når vi har lastet ned ***Device Policy*** kan vi gå inn på appen.



Figur 357: Innrulling av Android enheter - Via QR-kode

Her trykker vi på **Get started** og **Next** til vi kommer til en side hvor vi får beskjed om å Scanne en ***QR-kode***.

QR-koden vi skal scanne er en kode vi får fra Intune som vi tidligere hentet. Det er også mulighet for å skrive inn Token-koden om man har et kamera som ikke er optimal eller ødelagt. Man vil da få en Workspace på enheten sin. Man får også apps som vil være administrert og beskyttet av Intune. Dette er illustrert med en lås over appene.

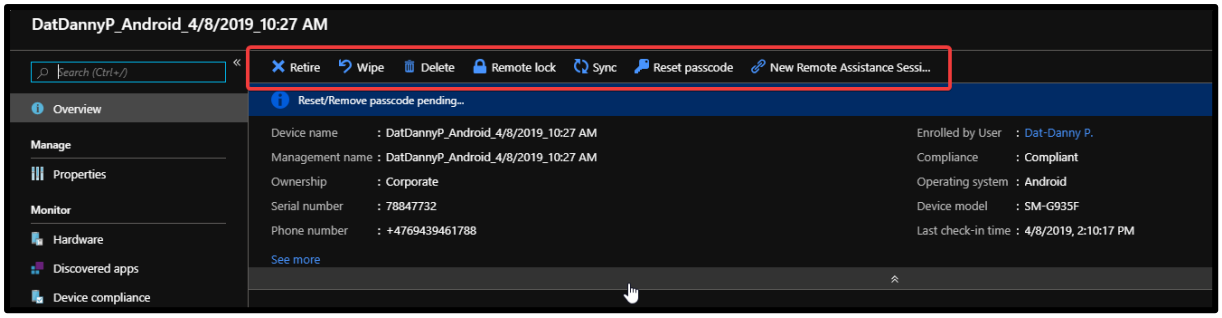


Figur 358: Innrulling av Android enheter - Via QR-kode

Muligheter for fjernstyring av Android

I likhet med fjernstyring av Windows-enheter er det mulig å sende spesifikke kommandoer til Android enhetene som er innrullet til domenet. Det er snakk om å utføre Wipe, Delete, Lock, remote controll, sync og reset passcode. Mulighetene til fjernstyring er derimot færre enn hos Windows enhetene, så man har ikke mulighet til Reset, remote scan og andre funksjoner ved Windows defender.

For å utføre fjernstyringen går vi like enkelt inn på enheten under ***Devices*** som vi ellers hadde gjort om vi hadde hatt en Windows-enhet. I stedet trykker vi på Android enheten vi skal kontrollere. Man vil få en menylinje i øvre del av skjermen hvor man kan se hvilke muligheter man har til fjernstyring.



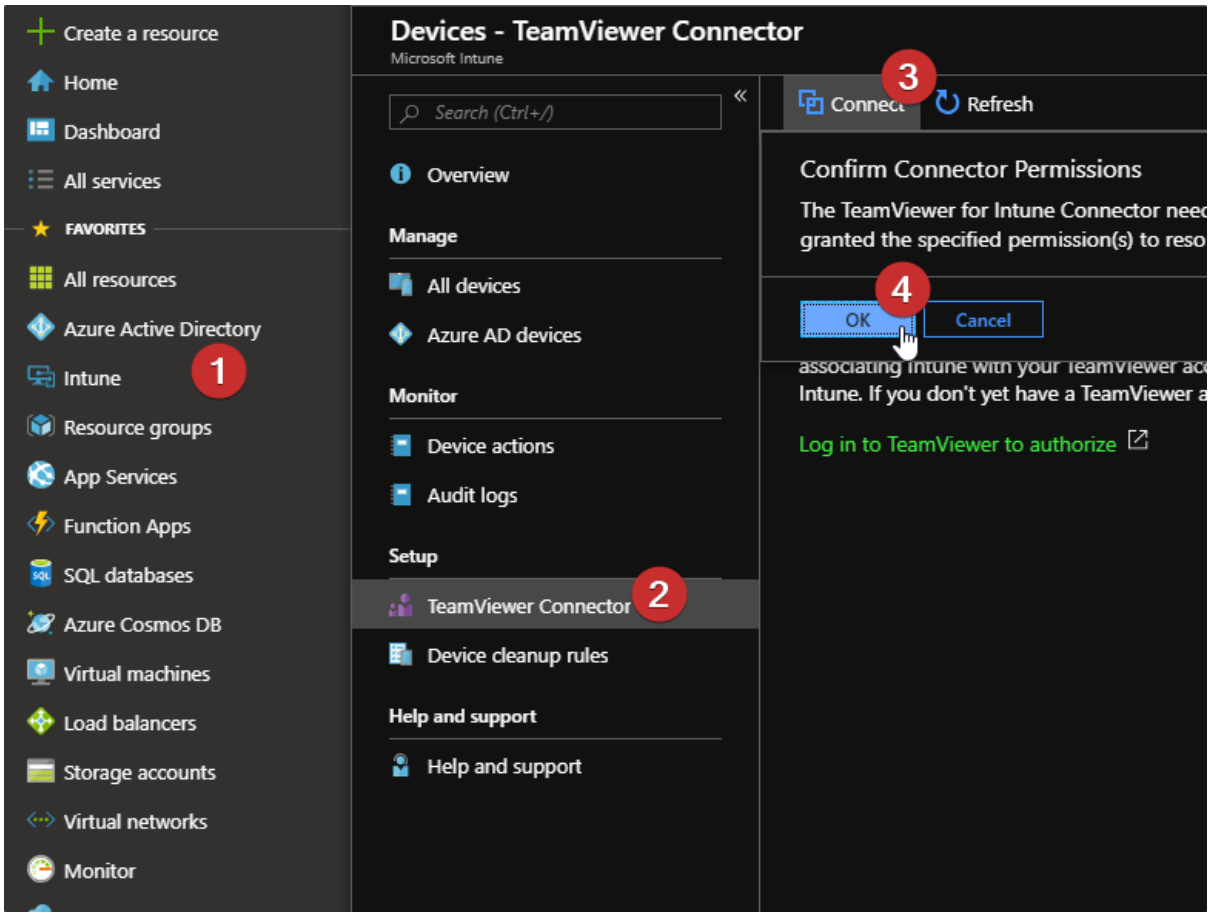
Figur 359: Muligheter for fjernstyring av Android

Remote Assistanse ved hjelp av TeamViewer

Det er noen ganger nødvendig for support, hvor man direkte styrer maskinen til brukeren. Dette kan være fordi brukeren ikke er så datakyndig eller at de mangler funksjonaliteter. En slik assistanse kan spare tid både for bruker og support. Den bør helst brukes hvis man skal gjøre noe som krever flere steg, tar lang tid eller krever presise tastetrykk, som support kan bistå med. Vi kan anbefale at hjelperen fra support laster ned TeamViewer på forhånd. Da går man til TeamViewer sin hjemmeside og laster ned installasjonsfilen der. Det viktige under installasjonen er at man installerer basic-versjonen og på hvem som skal bruke; Corporate eller both (corporate og personal).

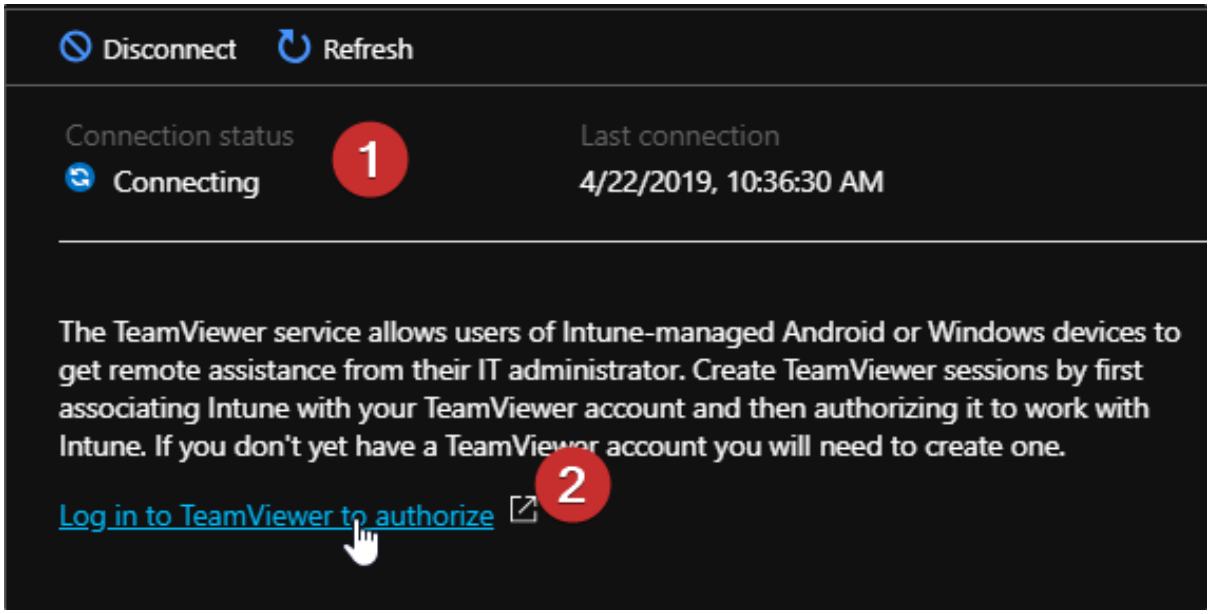
Sette opp tilkobling til TeamViewer

Først navigerer vi oss til ***Intune – Teamviewer Connector***, og trykker **connect** og deretter **OK.**



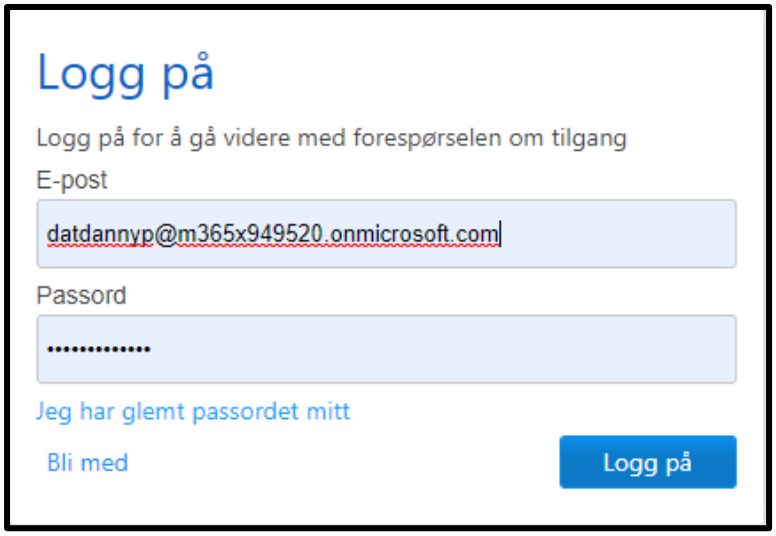
Figur 360: Sette opp tilkobling til TeamViewer

Vi vil da se at Connection status vil endre seg. Når den har endret seg til Connection kan vi trykke på **Log in to TeamViewer to authorize.**



Figur 361: Sette opp tilkobling til TeamViewer

Vi vil da få opp en skjerm som ber oss om å logge på TeamViewer. Vi har allerede lagd en bruker i TeamViewer for enkelhetsskyld, men om man ikke har, kan man opprette en ved å trykke på **bli med**.

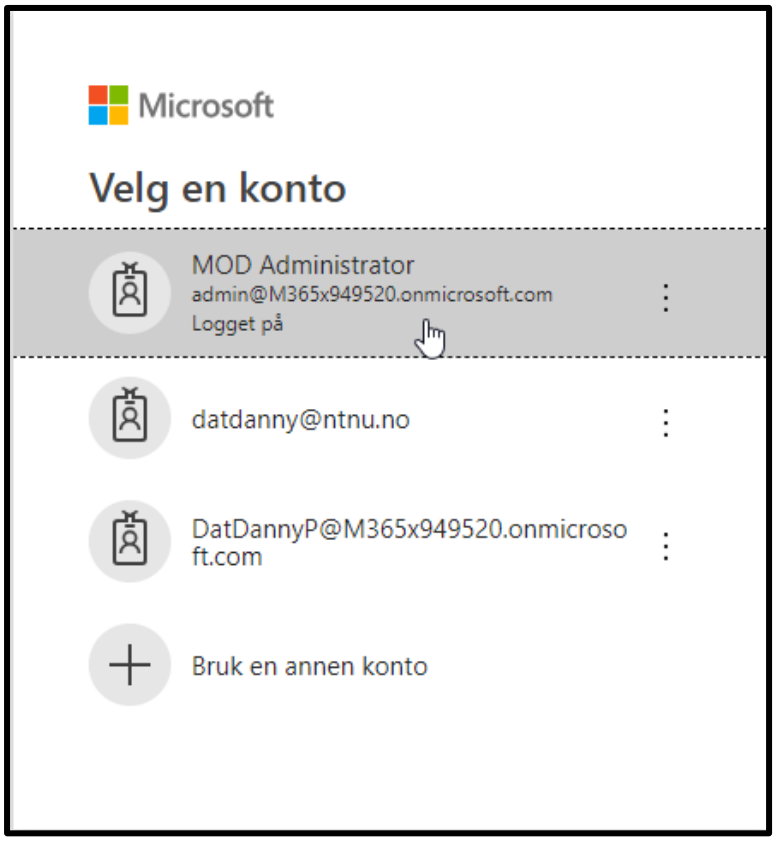


Figur 362: Sette opp tilkobling til TeamViewer

Vi vil da komme til en side som vil spørre om din tillatelse for å koble til domenet vi skal bruke TeamViewer for. Siden brukeren vår ikke egentlig er en administrator, kan det hende vi ikke har nok rettigheter. Hvis vi fortsetter videre kan vi logge inn med administratorbrukeren til domenet og gi administratorrettigheter til koblingen mellom TeamViewer og domenet. Vi trykker **Tillat.**

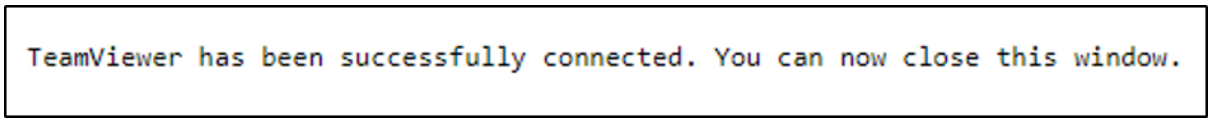
Figur 363: Sette opp tilkobling til TeamViewer

Vi får mulighet til å logge inn med en bruker slik at vi har nok tillatelse for å autorisere koblingen.



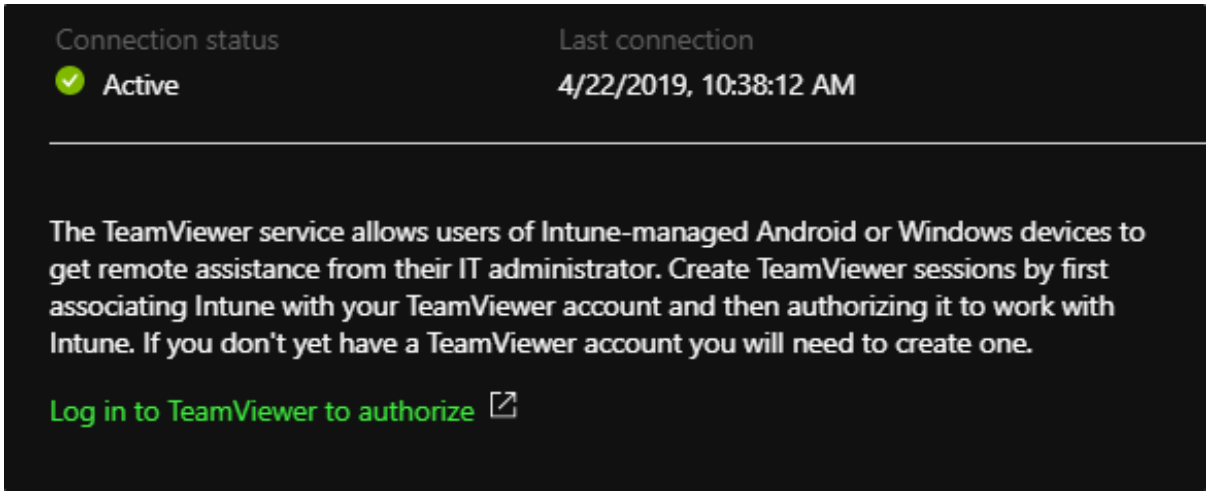
Figur 364: Sette opp tilkobling til TeamViewer

Da får vi opp en ny side som sier vi nå har opprettet en kobling mellom TV og Domenet.



Figur 365: Sette opp tilkobling til TeamViewer

Vi kan bekrefte dette i Intune der vi var ved å trykke på **refresh**, da vil vi se Connection status er satt til *Active*.

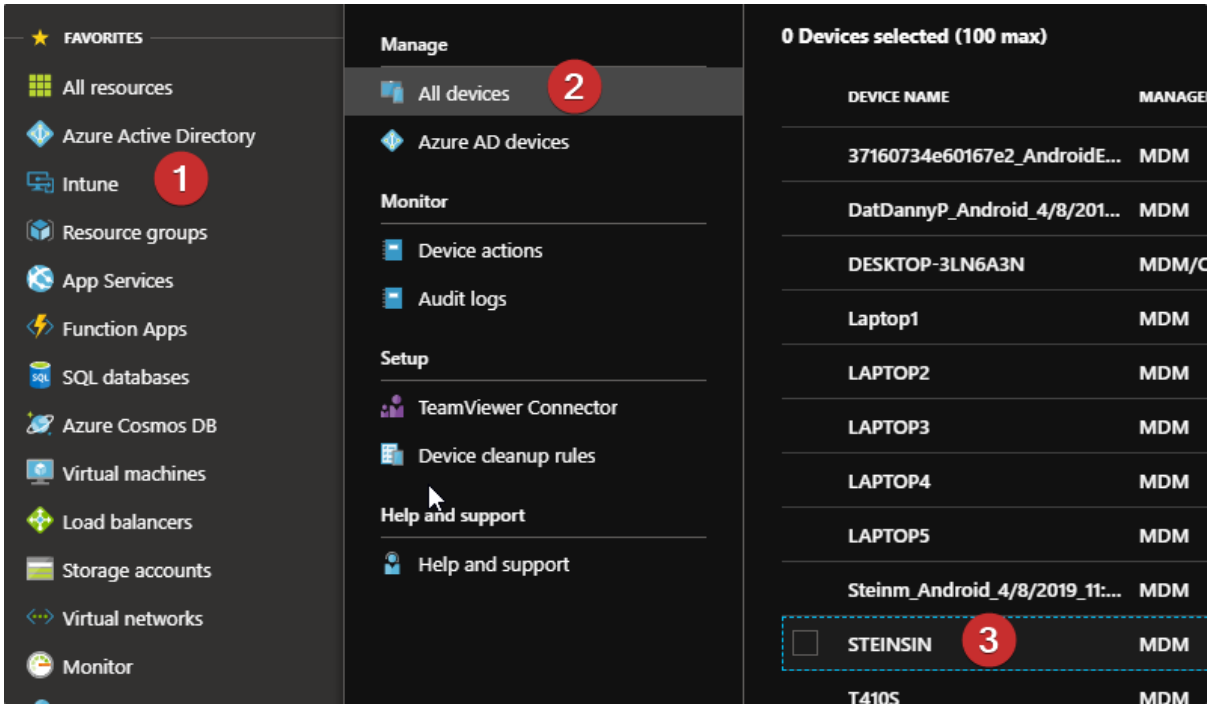


Figur 366: Sette opp tilkobling til TeamViewer

Sette opp Remote Assistanse til bruker

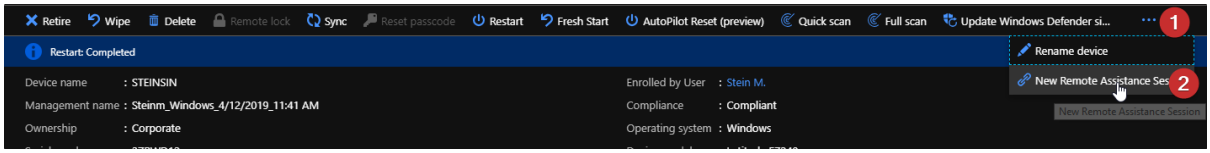
Anbefaler som sagt at den som setter opp remote session (drifteren/hjelperen) har lastet ned og installert TeamViewer på forhånd.

Da kan vi starte med å lokalisere brukeren som skal ha hjelp. Vi går til ***Intune*** – **all devices** – Trykker på **brukeren som trenger hjelp**.



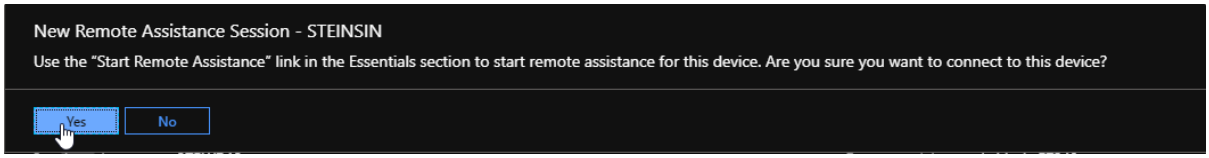
Figur 367: Sette opp Remote Assistanse til bruker

Vi går så til **de tre prikkene** på høyre side og trykker på **new remote assistance session** (posisjonen vil variere ut ifra dimensjonen på nettleservinduet).



Figur 368: Sette opp Remote Assistanse til bruker

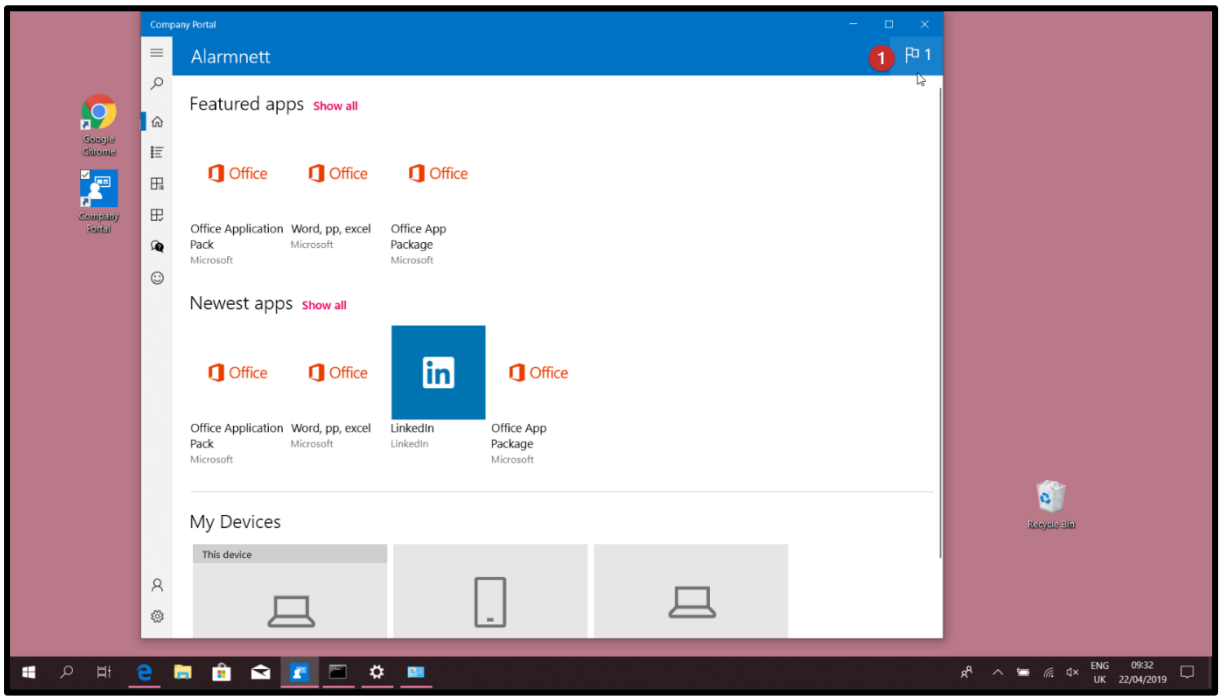
Da får vi opp en boble som spør om vi er sikre på om vi vil gjøre dette. Vi trykker **Yes**.



Figur 369: Sette opp Remote Assistanse til bruker

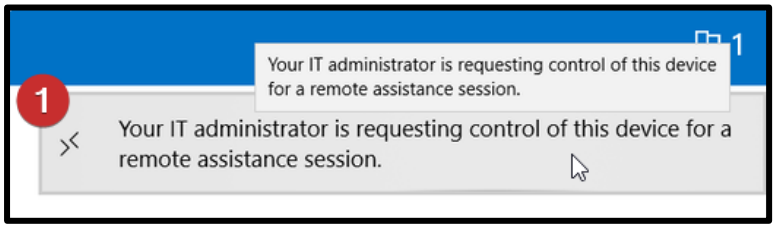
Brukeren sin side

Vi hopper da over til hva brukeren ser. I ***Company portal*** vil brukeren se et lite flagg i høyre hjørne. Vi ber brukeren trykke på **Flagget i hjørnet**.



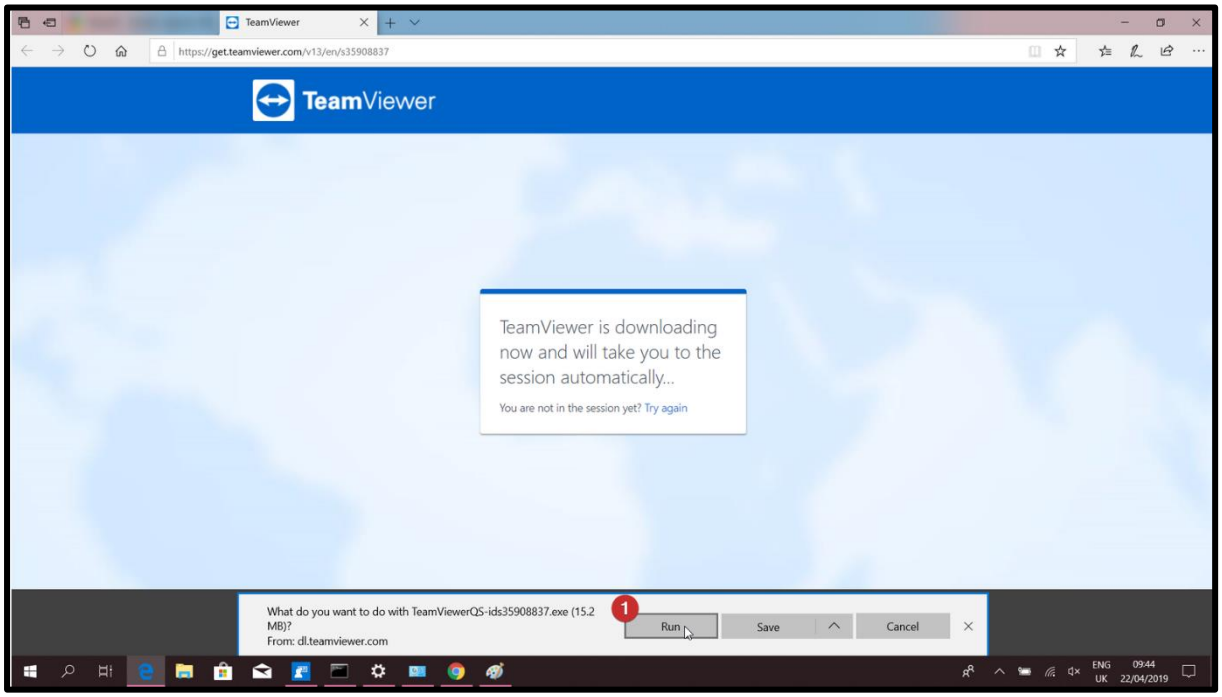
Figur 370: Sette opp Remote Assistanse til bruker

Da vil det komme opp en boble som sier at vi har spurt om en Remote Session. Vi ber brukeren om å trykke på **boblen**.



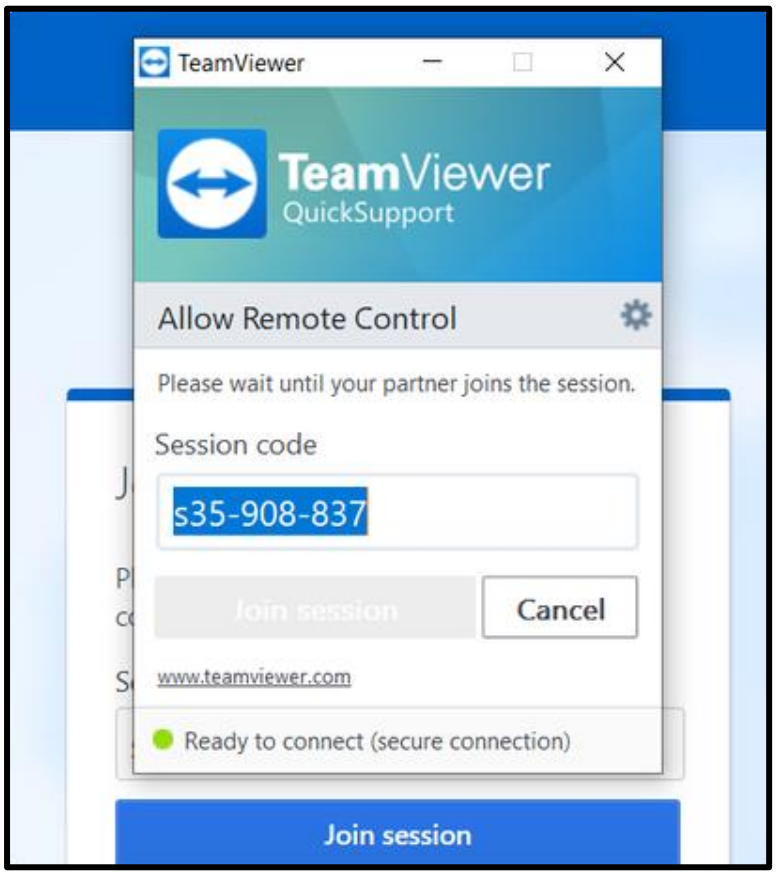
Figur 371: Sette opp Remote Assistanse til bruker

Denne vil ta brukeren til en side som ber brukeren om å enten laste ned eller kjøre en fil. Vi ber brukeren om å **kjøre filen**.



Figur 372: Sette opp Remote Assistanse til bruker

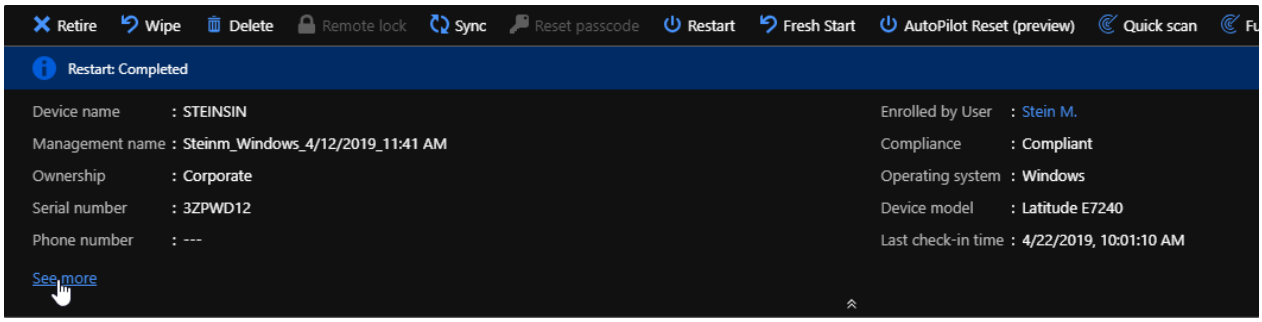
Brukeren vil nå få opp en TeamViewer QuickSupport Panel på skjermen sin, og vi kan be brukeren om å vente til vi får ordnet vår del. Vi skal ikke bruke sesjonskoden, så brukerne trenger ikke å oppgi den.



Figur 373: Sette opp Remote Assistanse til bruker

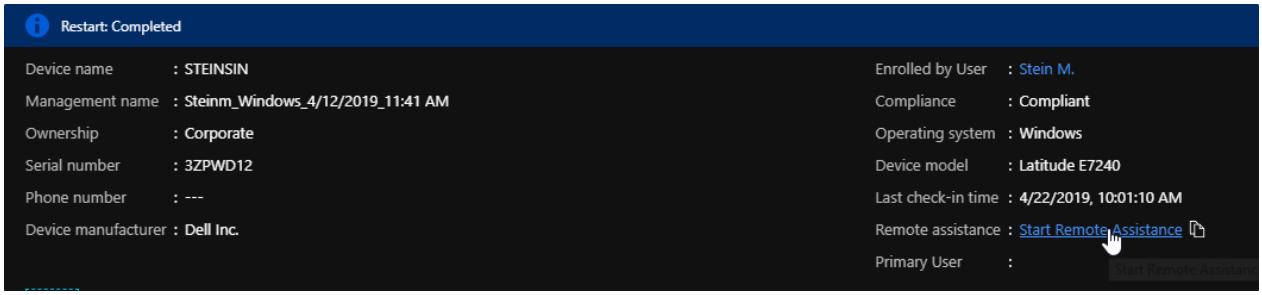
Hjelperens side

For å åpne Remote sessionen som vi har sendt, må vi på ***Device*** siden til enheten vi hjelper. Det kan være forvirrende å finne frem første gang. Trykk på **see more**.



Figur 374: Sette opp Remote Assistanse til bruker

Her finner vi Remote assistance og en lenke. Vi trykker på **lenken**.

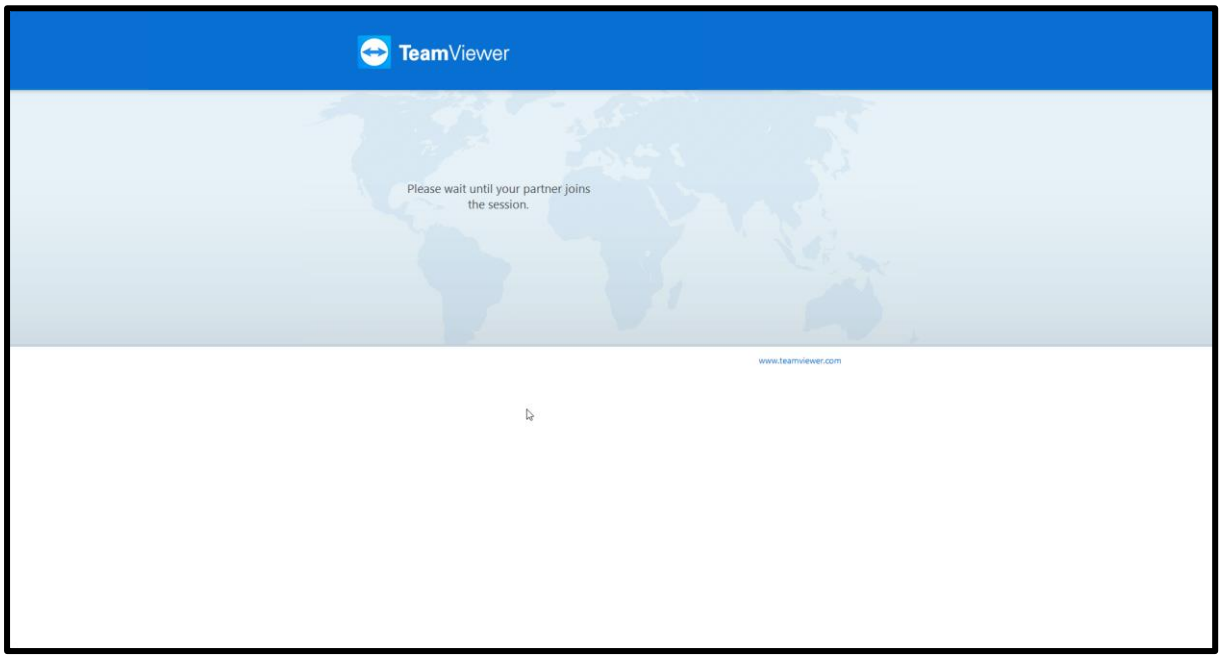


Figur 375: Sette opp Remote Assistanse til bruker

Her kom vi noen ganger til et problem hvor vi fikk feilmeldingen error reason unknown. Vi kom fram til at det bare er å lukke vinduene (fra hjelperen side) og åpne pånytt (Start remote assistance som vist i bildet over) til den fungerer. Den pleier å åpne seg etter to til fem forsøk.

Figur 376: Sette opp Remote Assistanse til bruker

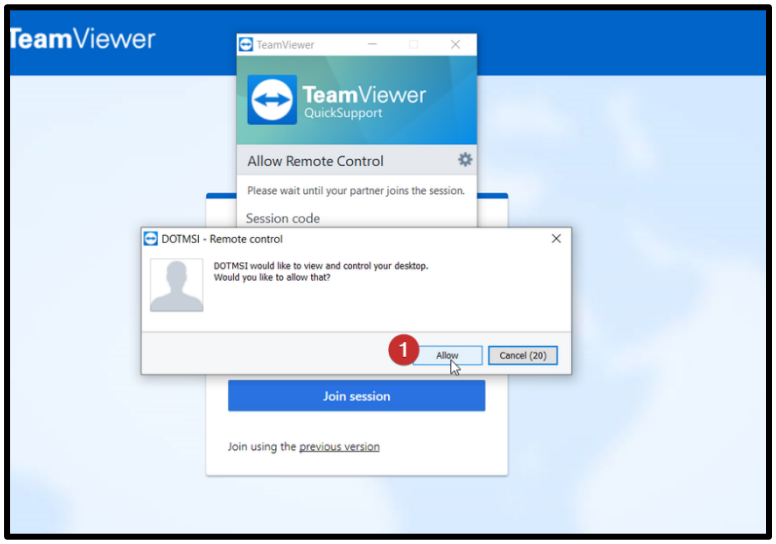
Når den åpner seg riktig vil vi få et stort vindu som ser noenlunde slik ut.



Figur 377: Sette opp Remote Assistanse til bruker

Brukerens side

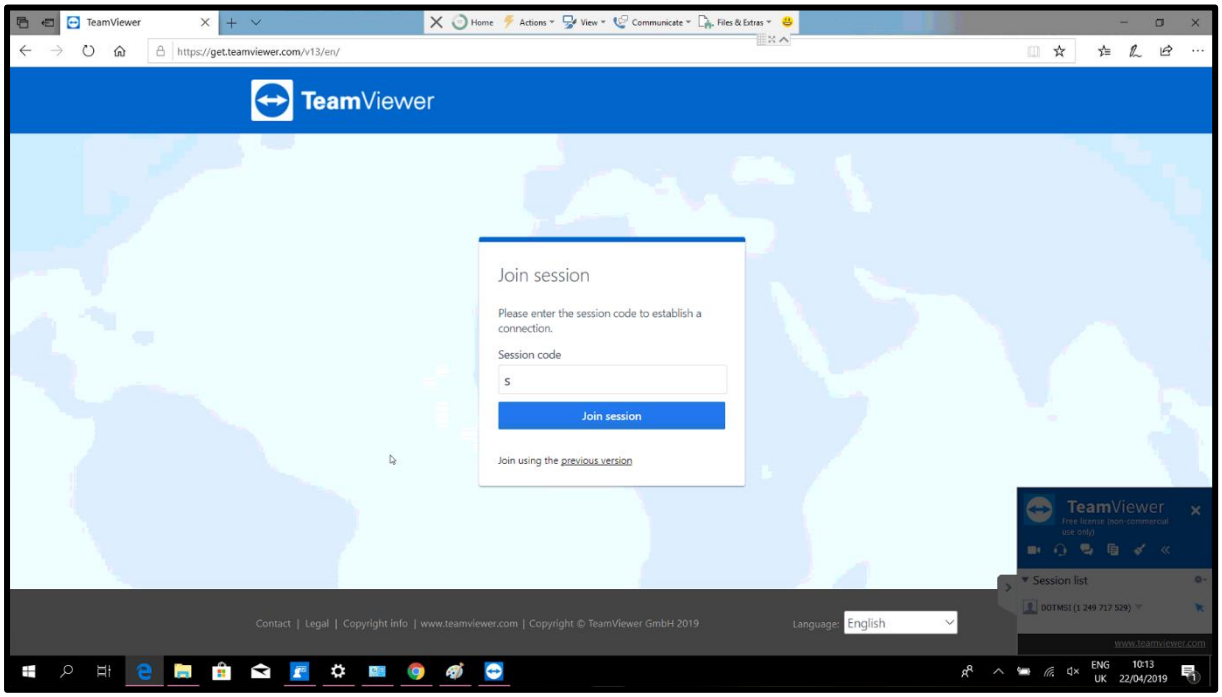
Brukeren vil nå få en forespørsel om en Remote assistance session fra den maskinen som hjelperen jobber fra. Vi ber brukeren trykke **allow** slik at vi kan hjelpe.



Figur 378: Sette opp Remote Assistanse til bruker

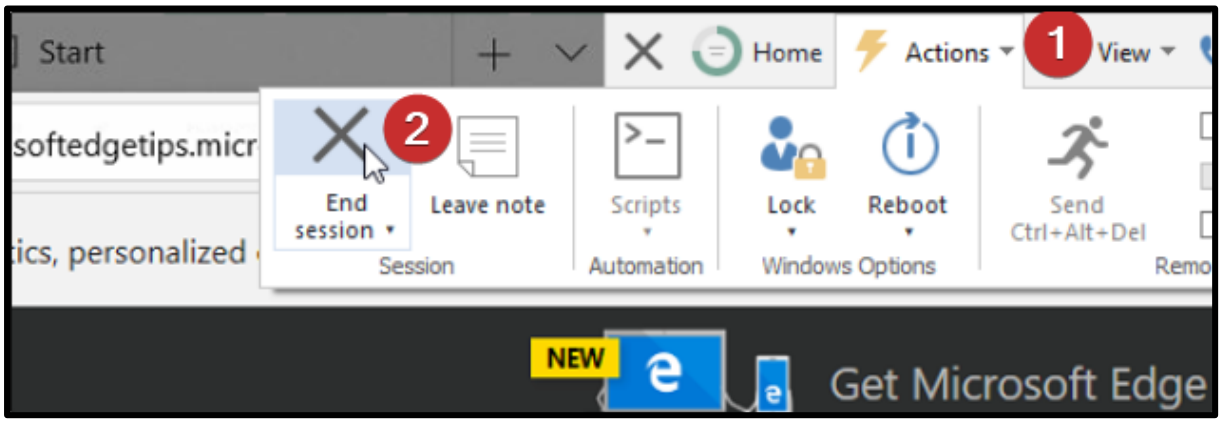
Hjelperens side

Vi vil nå kunne se og styre maskinen til brukeren og kan lettere assistere brukeren. Her er det mange funksjoner som er inkludert til TeamViewer. Disse skal vi ikke ta for oss i denne guiden.



Figur 379: Sette opp Remote Assistanse til bruker

Når vi er ferdig kan vi lukke tilkoblingen og si oss ferdige. Vi trykker **action** – **End session**.



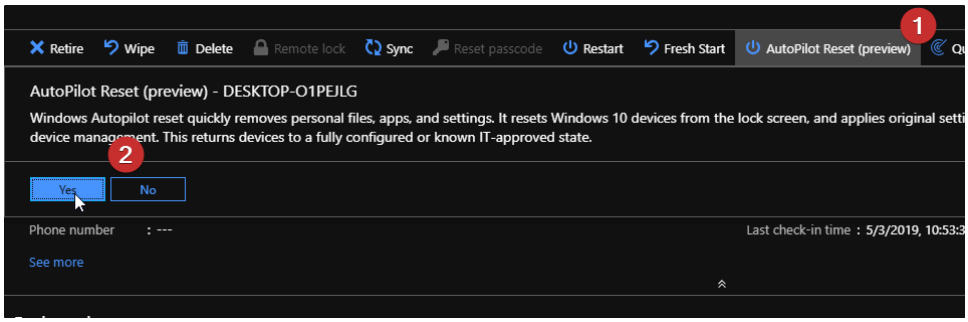
Figur 380: Sette opp Remote Assistanse til bruker

Autopilot reset (Preview)

Vi testet ut flere av funksjonene og oppdaget at denne funksjonen virket spesielt vanskelig å utføre, for øyeblikket. Dette kan være fordi den har spesifikke krav og fungerer per dags dato kun på ganske nye enheter som er rullet inn på spesifikke måter. Kravet for å bruke denne funksjonen er for det første at enheten som den skal utføres på har TPM 2.0, i tillegg til at det må være en fysisk enhet. Problemet vi støttet på da vi skulle teste funksjonen var at vi bare hadde tilgang til VM-er med TPM 2.0, som ikke oppfyller kravene satt for å utføre funksjonen. For det andre krever den at man ikke har brukt Self-deployment når man rullet inn til Azure. Dette er en av måtene man kan rulle inn til domenet på gjennom autopilot, hvor den andre er user-driven. Det betyr at denne prosessen kan gjøres automatisk via denne innstillingen. Vi kan derimot ikke bruke denne innstillingen. Self-deployment krever også at man har TPM 2.0 og man skulle tro at den ville fungert bra sammen med andre ting som trenger TPM 2.0, men det gjør den da ikke. I tillegg til dette kreves det da standard ting som at du har satt opp en enrollment status page, enheten må være MDM managed og være Azure AD joined.

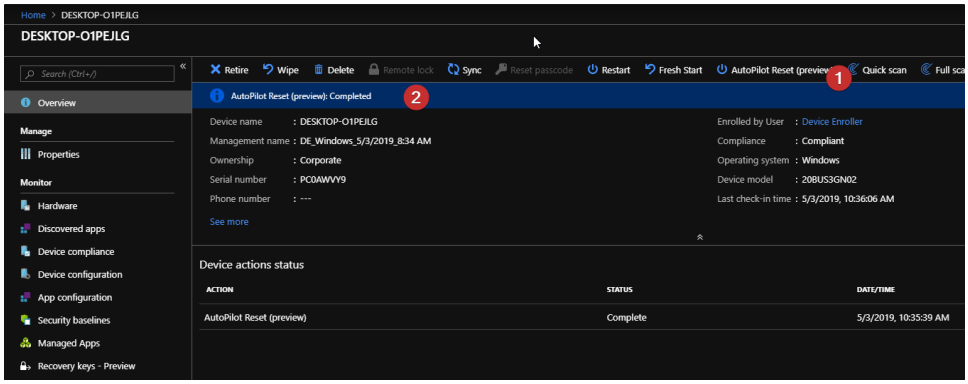
Utføre Autopilot reset

Da for å utføre funksjonen går vi ganske enkelt til enheten vi skal utføre reseten på. Vi ser på menyen over hvilke funksjoner vi kan utføre på enheten og velger **Autopilot reset (preview)** - Trykker så på **yes**.



Figur 381: Autopilot reset (Preview)

Vi venter så til reseten blir utført.

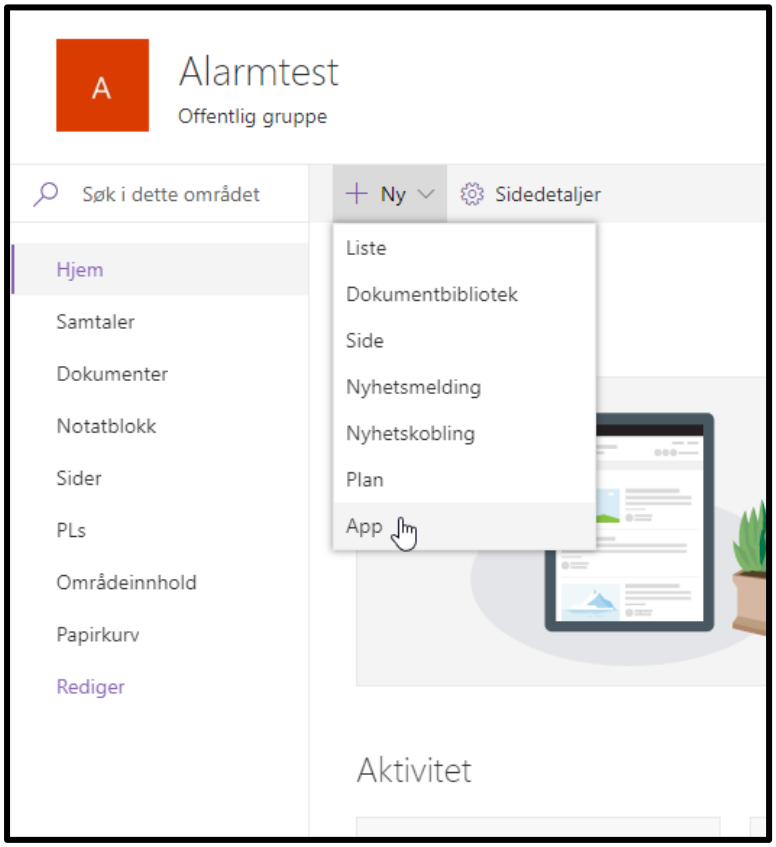


Figur 382: Autopilot reset (Preview)

På brukeren sin side vil de få opp en liten pop-up som forteller dem om at administrasjonen har utført en reset og at de vil bli logget ut om noen minutter. Tjenesten vil så utføre en standard reset av maskinen, som man kan gjøre i settings på maskinen.

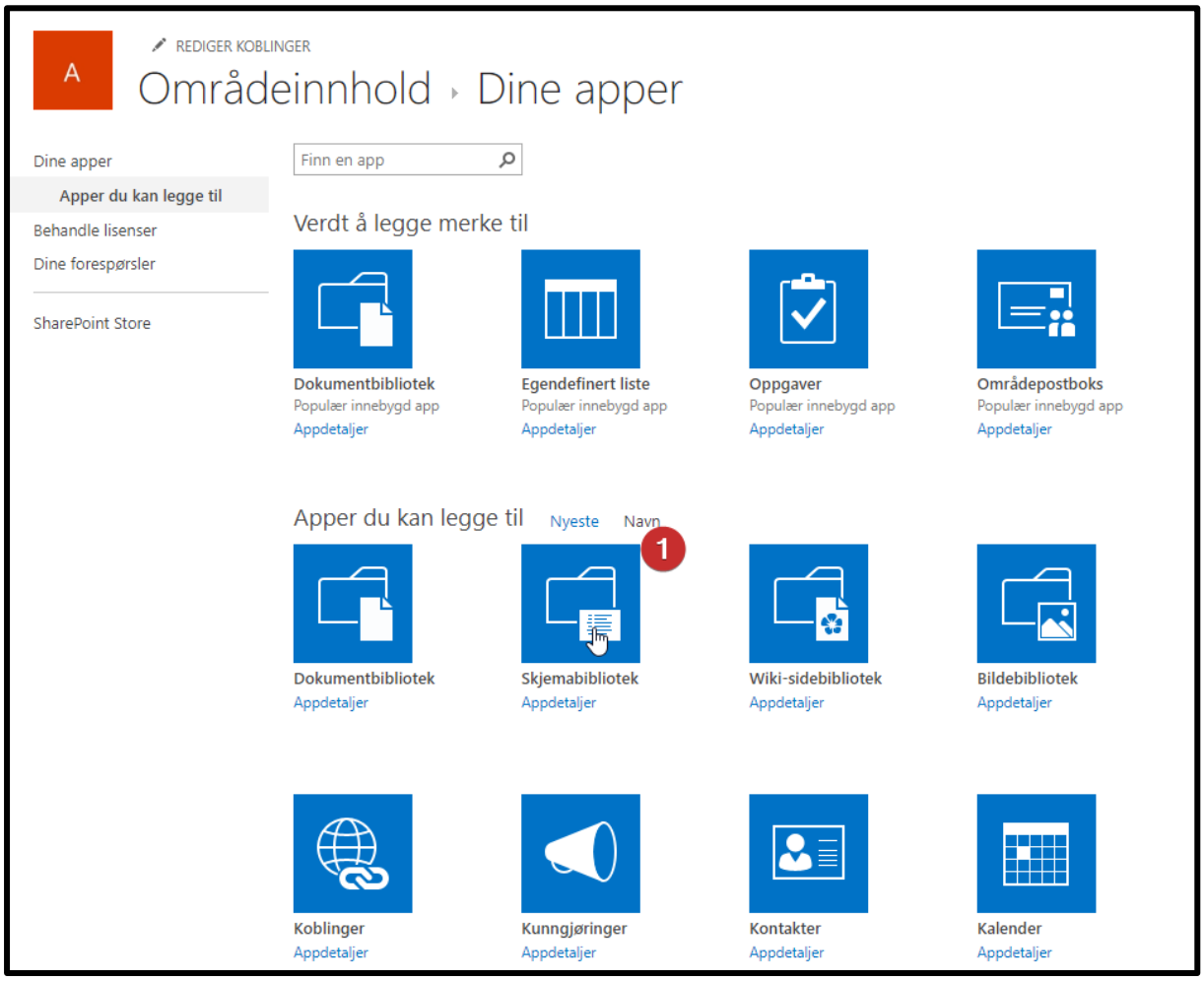
Opprette og redigere skjema

For å effektivisere dokumentering kan vi lage et skjema som de ansatte skal følge når de er ute hos en kunde. Om disse skjemaene benyttes av montørene, vil dette spare bedriften for mye tid og penger ved at de ansatte får mer tid til å gjøre andre ting enn å dokumentere.
For å opprette fine skjema som vi kan håndtere via PowerApps kan vi først opprette en extension for PowerApps. Dette vil da legge seg på områdeinnhold. Vi går til området vårt på SharePoint og hjem. Her trykker vi på **Ny** – **App**.



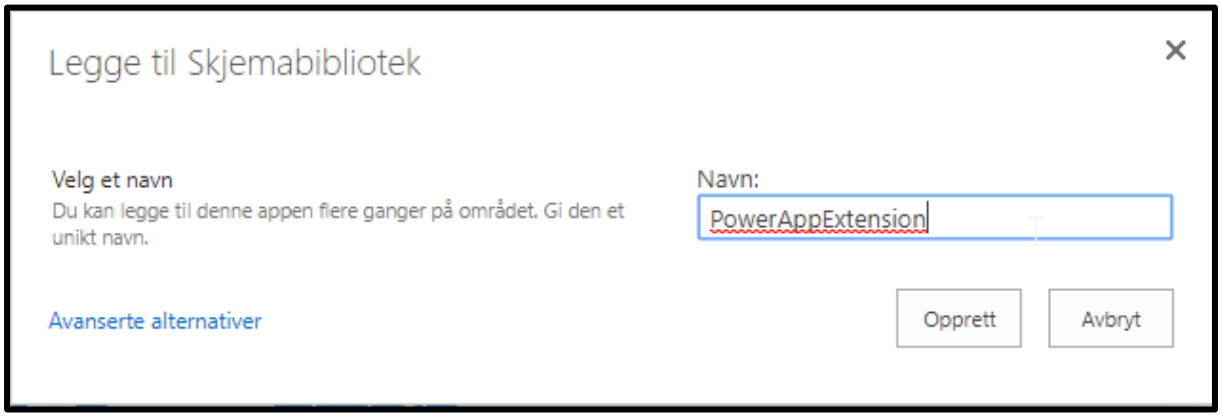
Figur 383: Opprette og redigere skjema

Vi velger så **skjemabibliotek**, som vist på bildet.



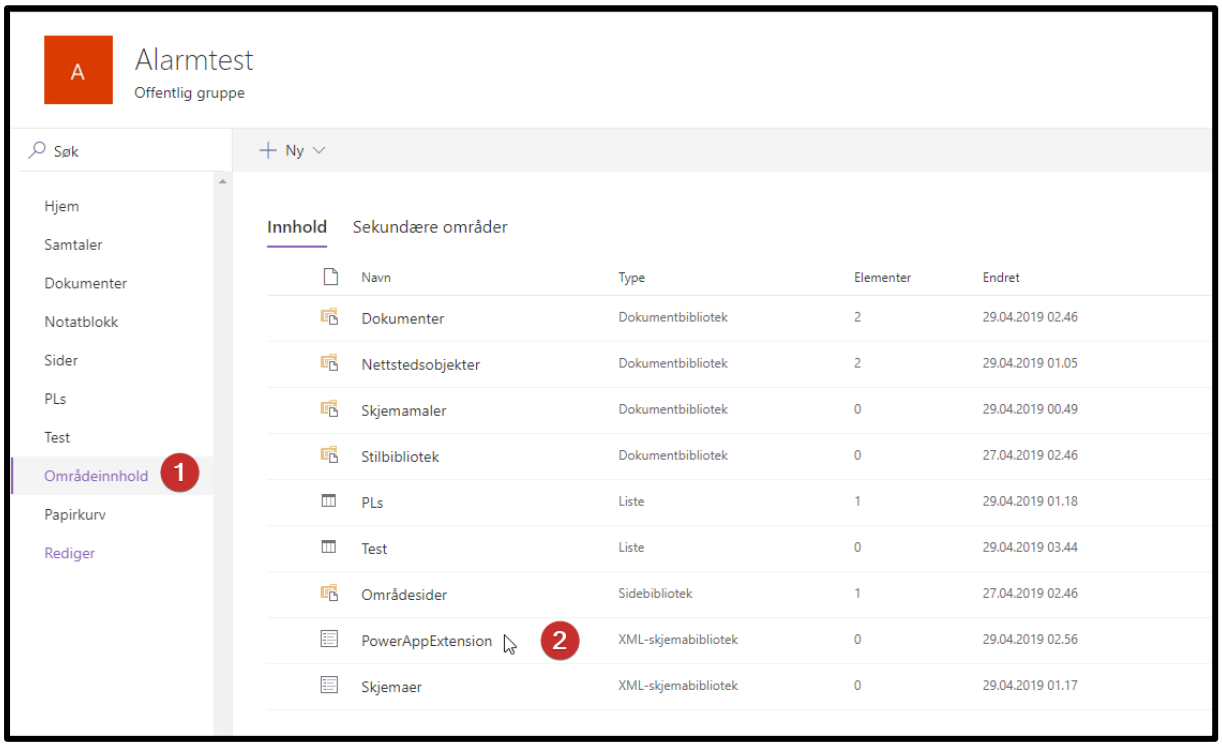
Figur 384: Opprette og redigere skjema

Når vi skal legge til skjemabibliotek blir vi bedt om å legge til et navn. Velger et passende navn. Trykker deretter **Opprett**.



Figur 385: Opprette og redigere skjema

Vi ser at vi har lagt til Extensionen ved å gå til områdeinnhold.

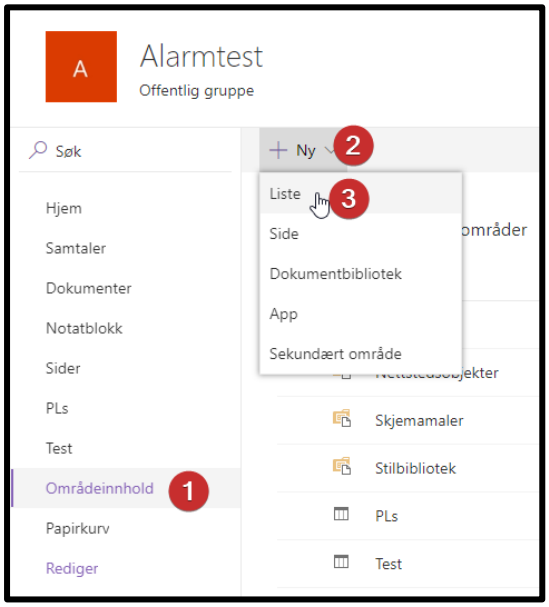


Figur 386: Opprette og redigere skjema

Opprette liste

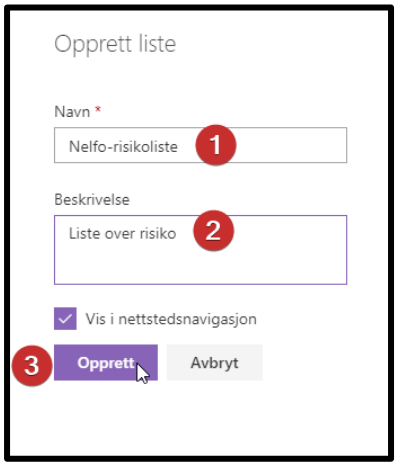
Nå kan vi lage en liste som vi kan bruke.

For å gjøre det går vi til områdeinnhold – Trykker **Ny** – **Liste**.



Figur 387: Opprette og redigere skjema - Opprette liste

Da kommer det opp et nytt vindu og vi blir bedt om å skrive inn et passende navn sammen med en beskrivelse. Vi trykker så **Opprett**.



Figur 388: Opprette og redigere skjema - Opprette liste

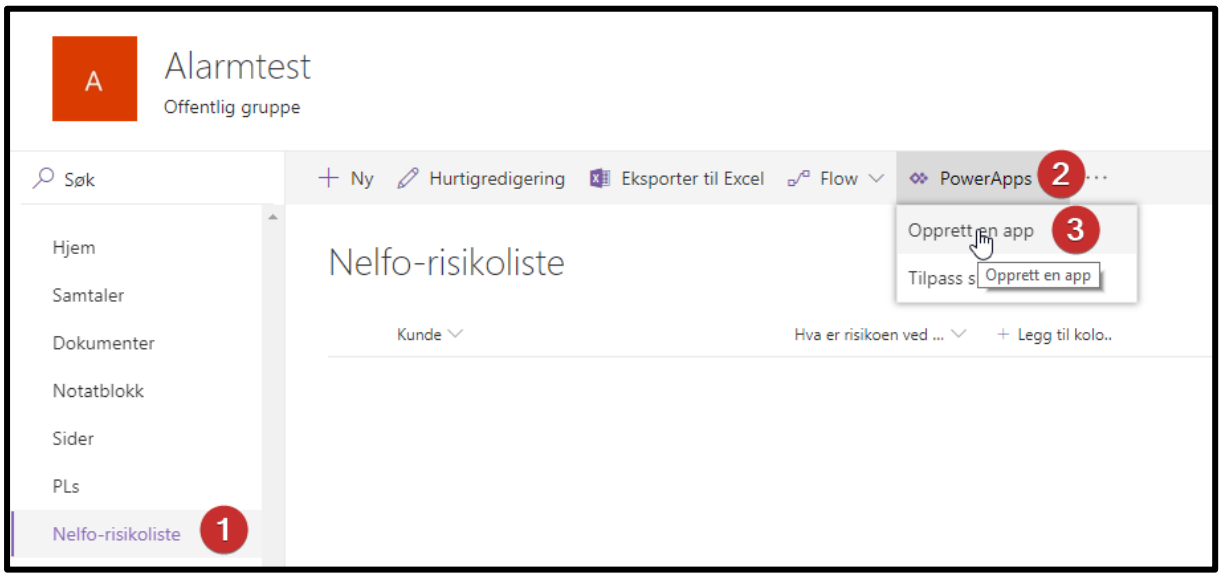
Nå blir vi sendt til den nye listen vi har opprettet. Først kan det virke litt forvirrende siden det ikke ser ut som en liste. Man kan legge til kolonner i skjemaet sitt ved å trykke **legg til kolonne** og velge et av alternativene som dukker opp. Vi går for **en enkelt linje med tekst**.

Figur 389: Opprette og redigere skjema - Opprette liste

Da får vi opp en boks som spør oss om hva kolonnen skal inneholde og fyller ut informasjonen. Trykker **lagre** når vi er ferdig.

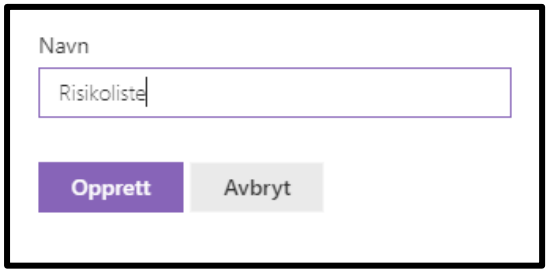
Figur 390: Opprette og redigere skjema - Opprette liste

Når vi har lagt til nok kolonner kan vi trykke på **PowerApps** – **Opprett app**. Om du ikke er på listen du opprettet kan du trykke på **listen** på venstre side for å komme tilbake som vist på bildet.



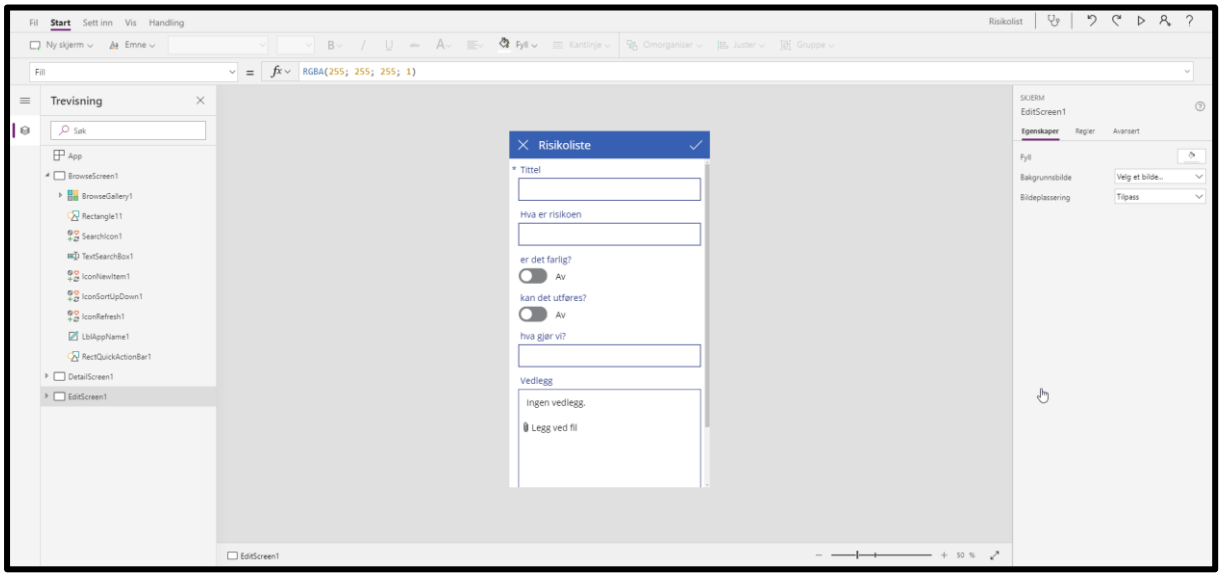
Figur 391: Opprette og redigere skjema - Opprette liste

Da blir vi bedt om å opprette et navn for applikasjonen. Vi gir den et passende navn og trykker **opprett**.



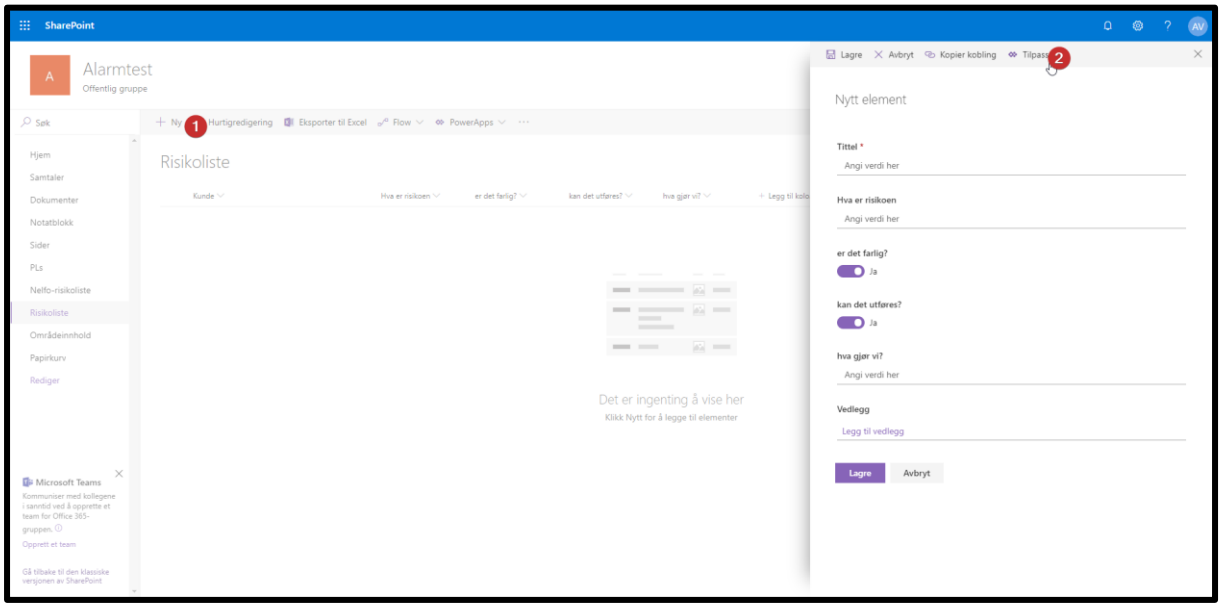
Figur 392: Opprette og redigere skjema - Opprette liste

Nå har vi laget en app for listen og her kan vi endre på hvordan resultatet til listen ser ut. Vi lukker dette vinduet.



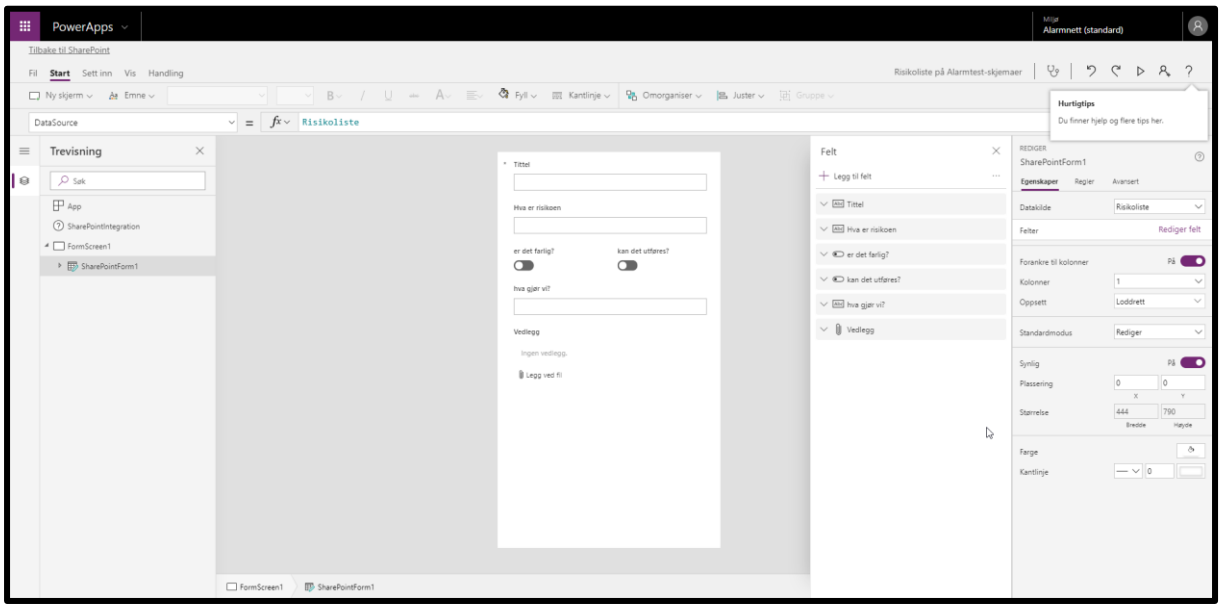
Figur 393: Opprette og redigere skjema - Opprette liste

Det vi ønsker å gjøre er å endre på skjemaet som de ansatte skal bruke, dermed må vi gå til **Ny** – trykk på **tilpass** på skjemaet.



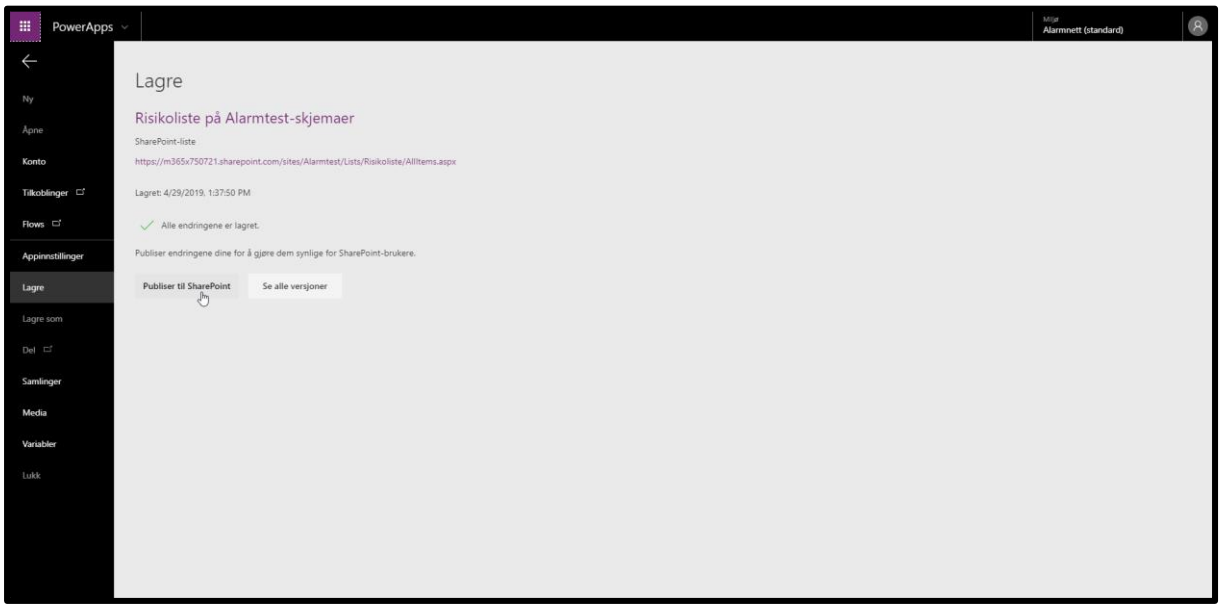
Figur 394: Opprette og redigere skjema - Opprette liste

Det vil åpne et nytt vindu av PowerApps, men forskjellen er at denne er av skjemaet de ansatte skal benytte seg av for å sende inn informasjon. Her kan du dra figurene slik at de passer til din smak.



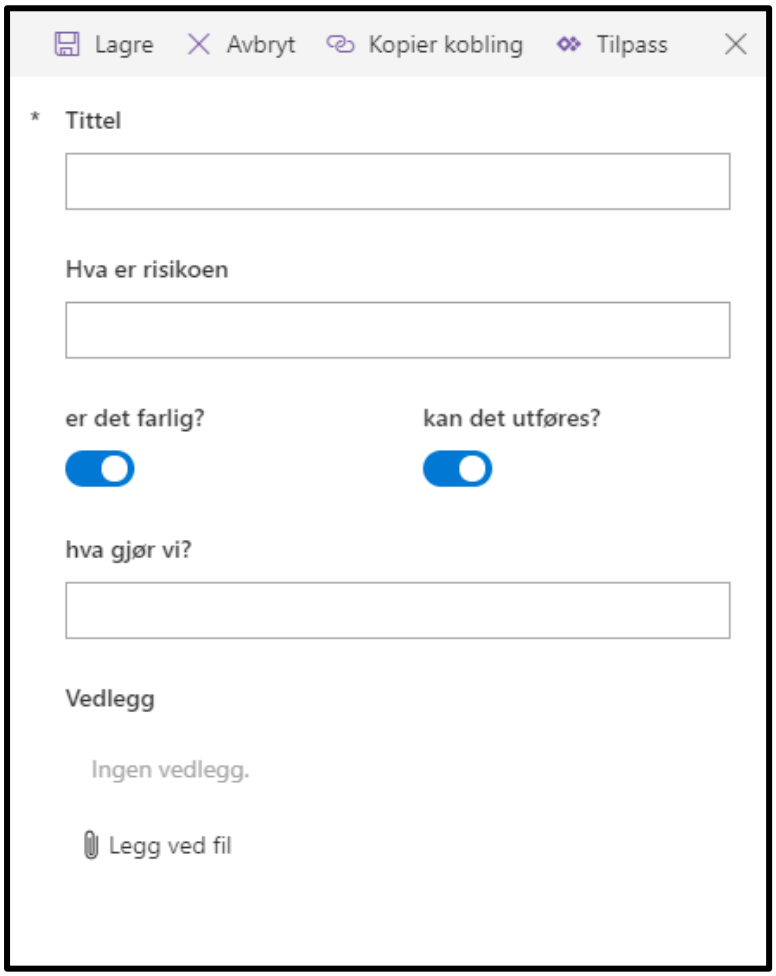
Figur 395: Opprette og redigere skjema - Opprette liste

Når du er ferdig kan du lagre og publisere skjemaet. Trykk **Fil** – **Publiser til SharePoint**.



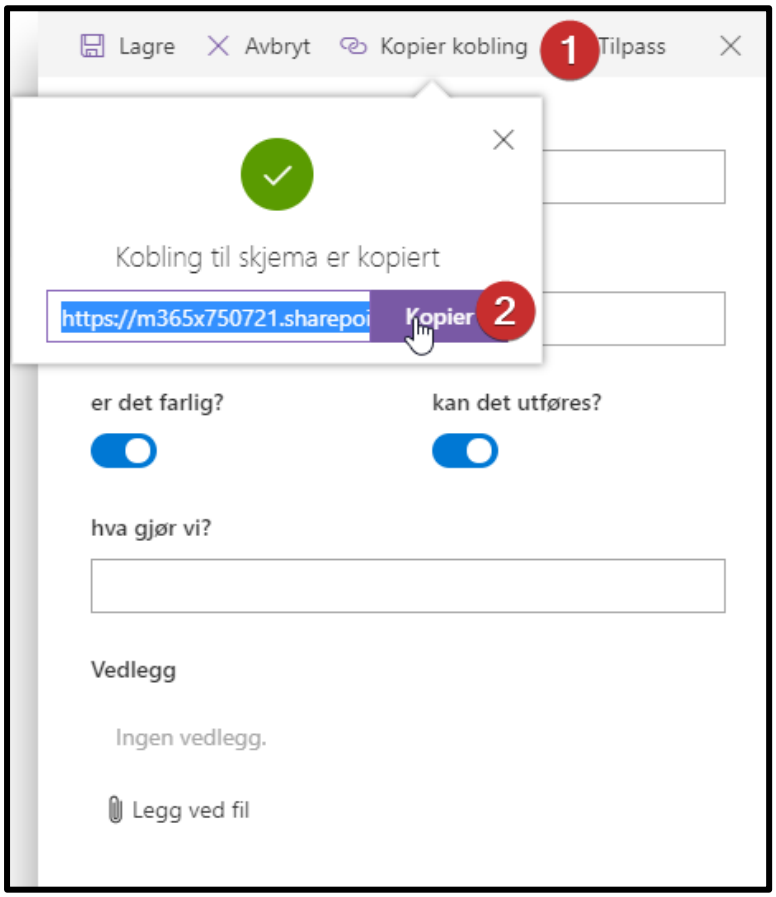
Figur 396: Opprette og redigere skjema - Opprette liste

Vi ser endringen vi har gjort på skjemaet i listen vi opprettet.



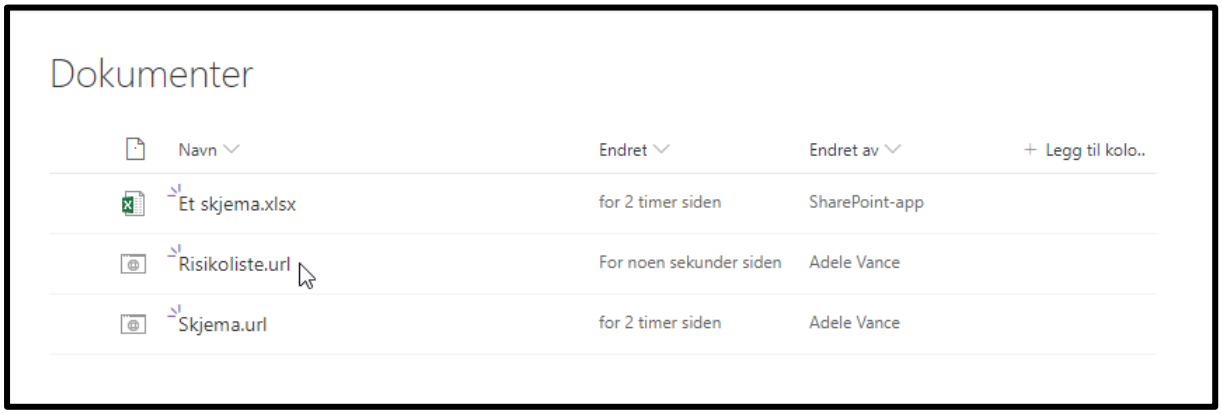
Figur 397: Opprette og redigere skjema - Opprette liste

Da kan vi dele skjemaet ved å trykke **kopier kobling** og **kopier**.



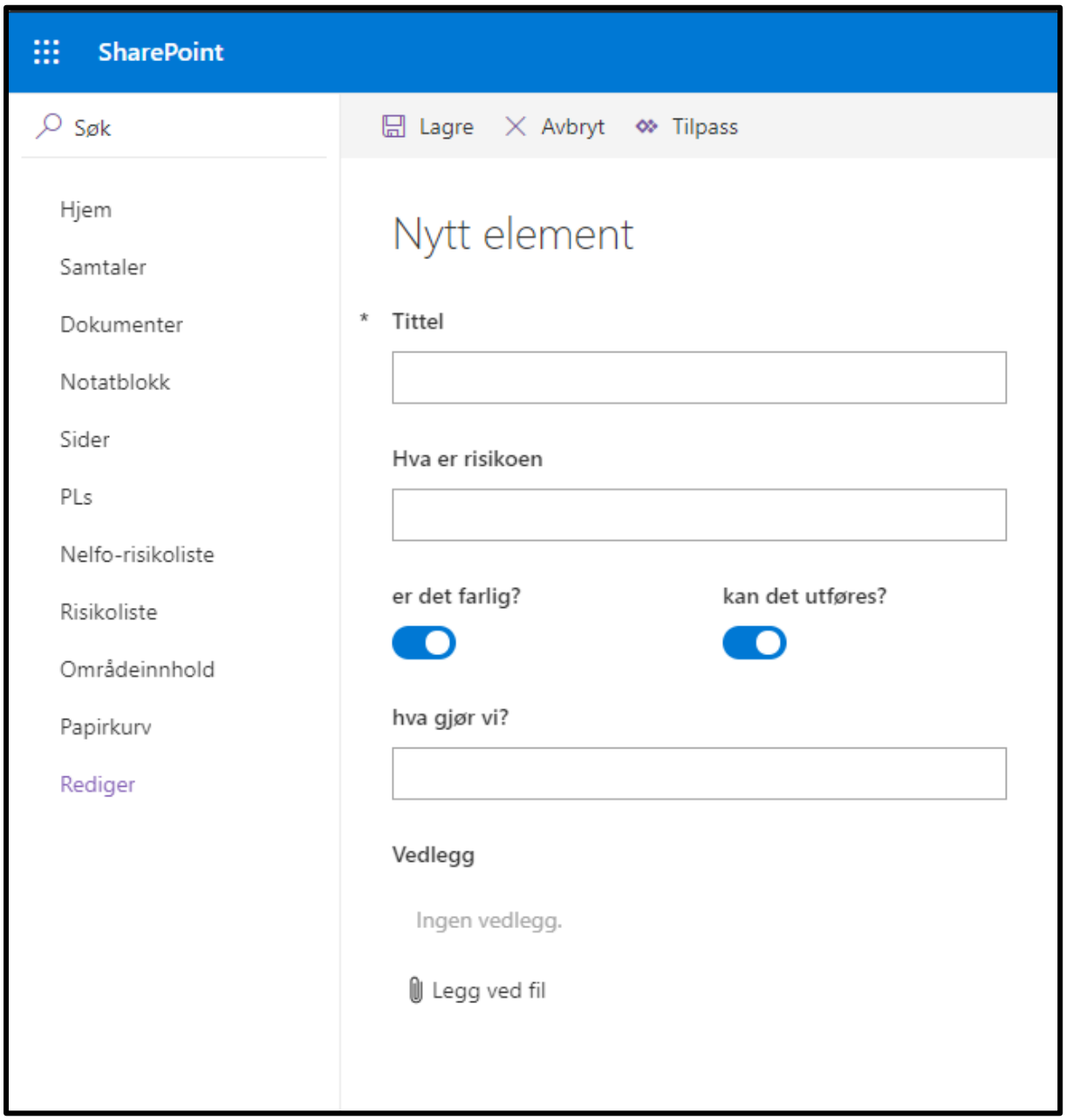
Figur 398: Opprette og redigere skjema - Opprette liste

Vi lager så en lenke i dokumenter ved å trykke **ny** – **kobling** og legger lenken i vinduet som kommer opp. Gi den et passende navn og fullfør. Vi ser da en lenke til skjemaet vårt.



Figur 399: Opprette og redigere skjema - Opprette liste

Trykker vi på skjemaet vårt vil vi få opp et skjema som er klar til å fylles ut. Kan fjerne PowerApps fra brukerne så de ikke kan redigere skjemaene. Utenom dette er skjemaet klart til å brukes.



Figur 400: Opprette og redigere skjema - Opprette liste

Fase 5 – Administrasjon av Intune ved hjelp av PowerShell

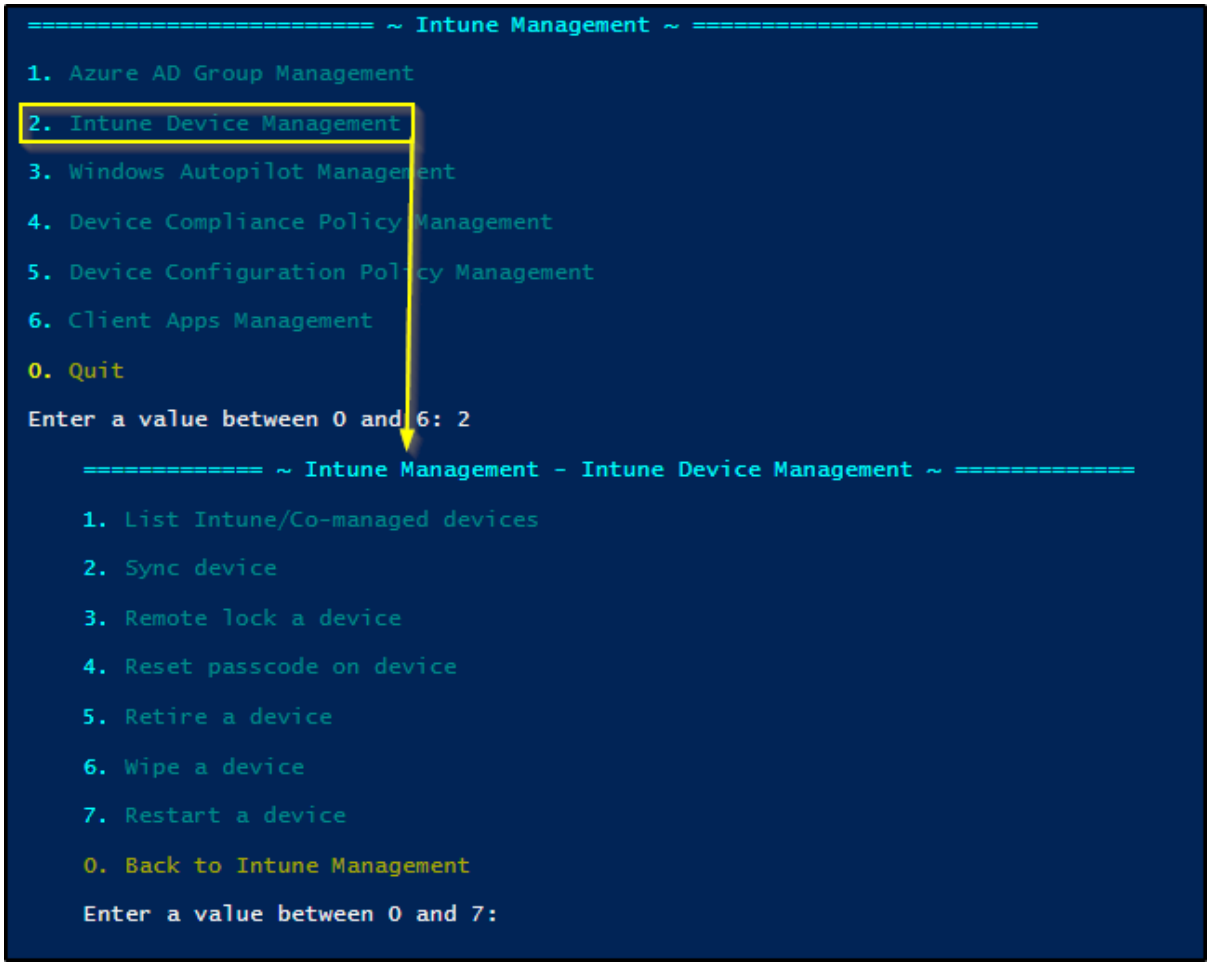
Brukermanual

Brukermanualens innhold

I starten av manualen vil vi enkelt vise hvordan scriptet er bygget opp og hvordan administrasjonsansvarlig kan koble seg til, navigere seg gjennom scriptet og utføre forskjellige oppgaver. Videre vil vi gå dypere inn på hvordan samtlige funksjoner utføres. Scriptet må kjøres fra en konsoll med administratorrettigheter.

Navigasjon i scriptet

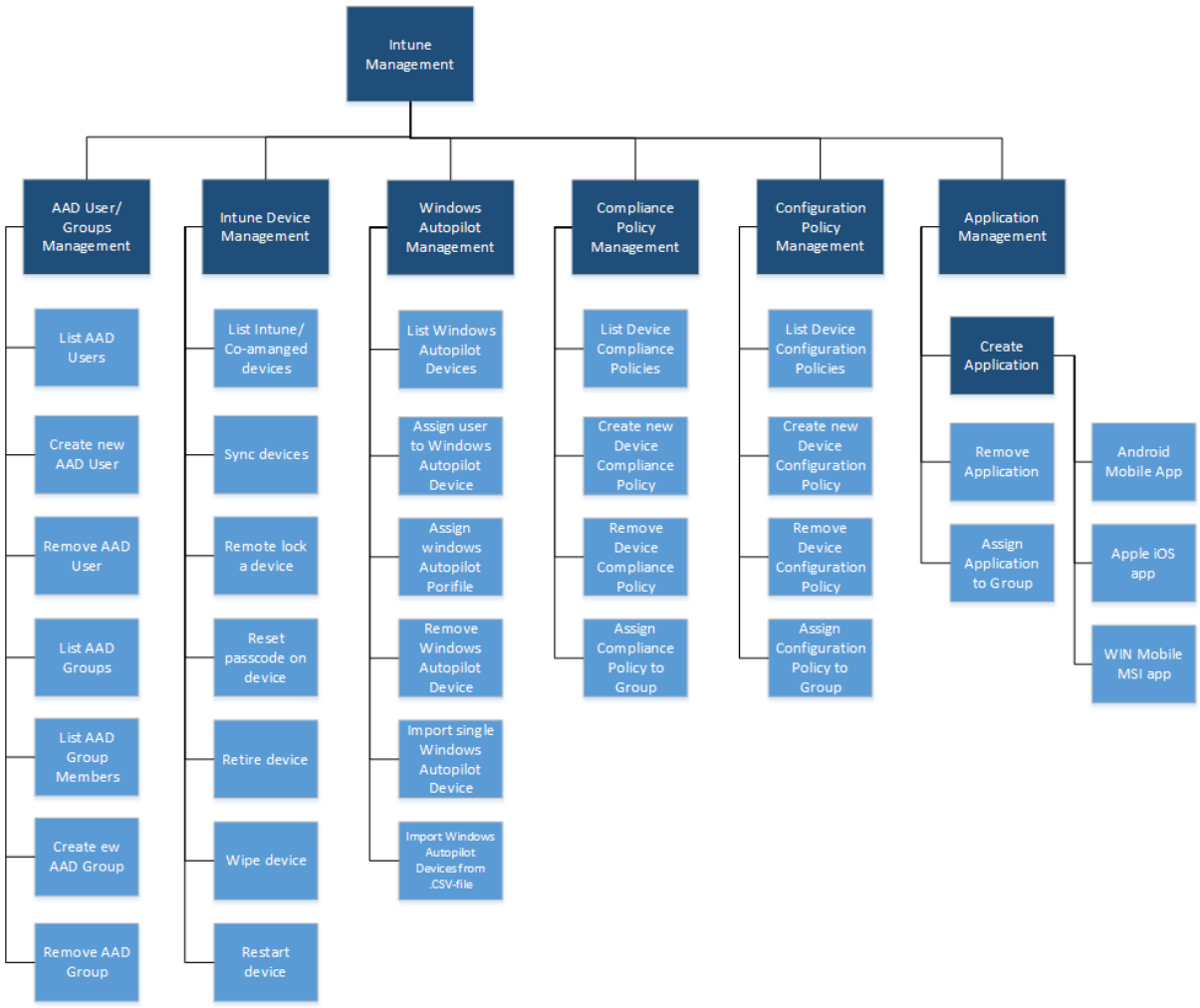
For å navigere seg i scriptet, har vi tatt i bruk menyer for å organisere de forskjellige funksjonene og gjøre scriptet så oversiktlig som mulig. Nedenfor kan vi se hvordan meny-systemet fungerer, med undermenyer og funksjoner inne i disse. Eksempelet nedenfor viser at vi går fra «hovedmenyen», til «Intune Device Management». Slike meny-systemer benyttes gjennom store deler av scriptet.



Figur 401: Navigasjon i scriptet

Funksjoner

Nedenfor har vi laget et diagram som viser en oversikt over alle funksjonene, hvor de ligger, og man får et bedre bilde av hvordan menysystemet fungerer.



Figur 402: Intune PowerShell funksjoner

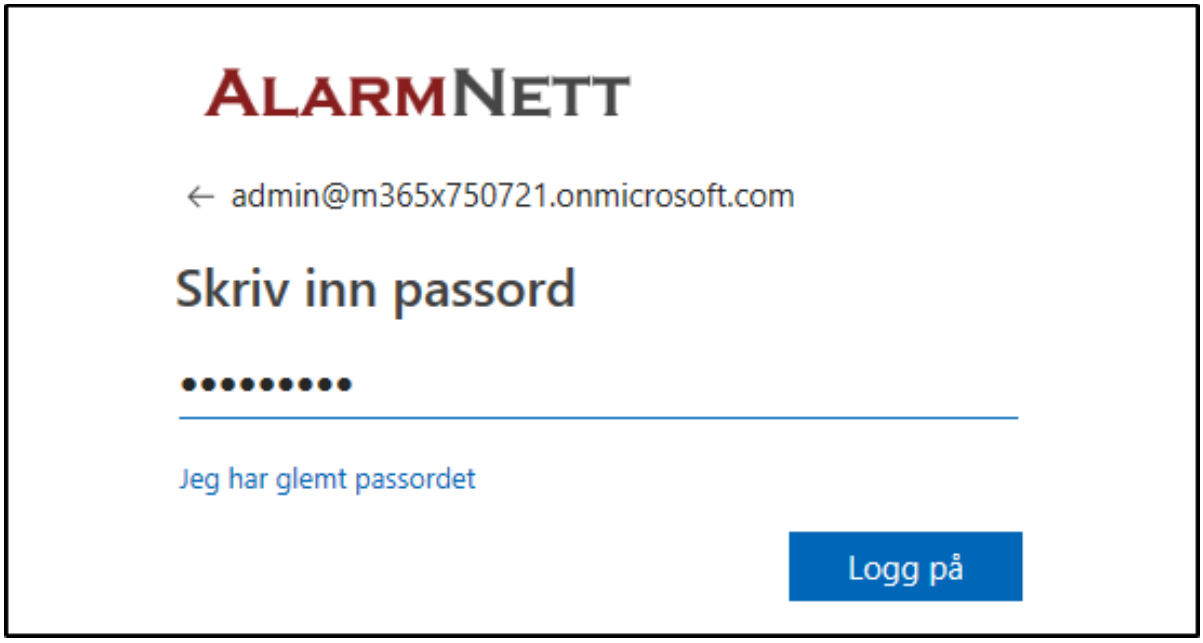
For å kunne ta i bruk scriptet, må man først kjøre gjennom koden én gang. Deretter må man kjøre funksjonen **Connect**. Denne Installerer modulene man trenger for Azure AD, Intune og Windows Autopilot, samt logger oss inn. For innlogging må man benytte Administratorbruker for tenanten og i tillegg legge til passord.

Nedenfor ser vi Connect funksjonen som må kjøres for å installere modulene, samt koble til.

```
function connect{
    install-module azuread
    install-module windowsautopilotintune
    Install-Module -Name Microsoft.Graph.Intune
    import-module windowsautopilotintune
    connect-MSGraph
    Connect-AzureAD
    Connect-AutoPilotIntune -user admin@m365x750721.onmicrosoft.com
    }
```

Figur 403: Intune PowerShell funksjoner

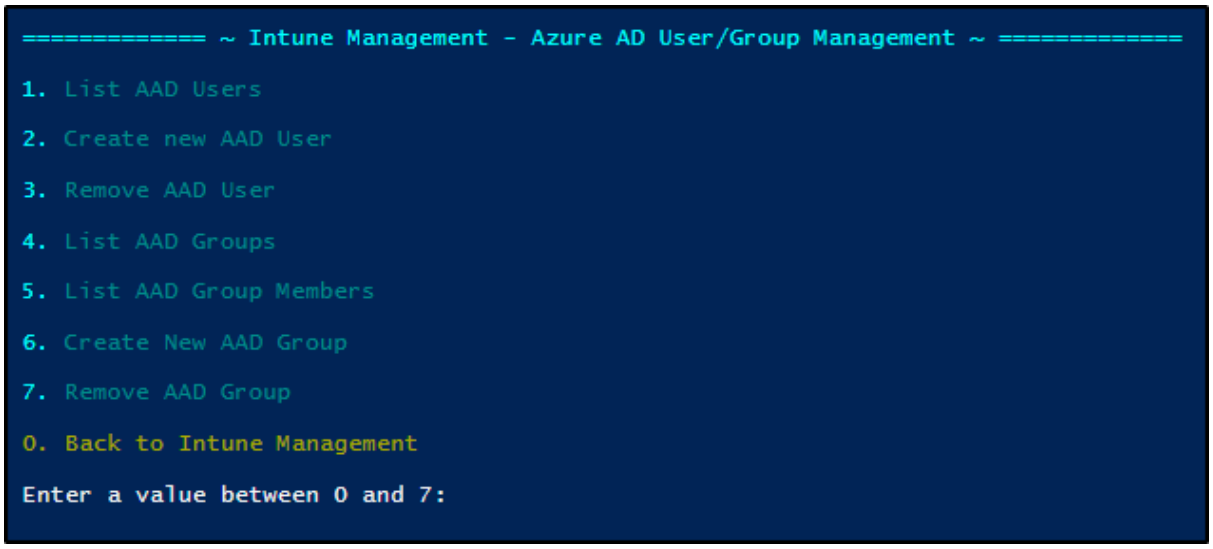
Bildet nedenfor viser oppkobling.



Figur 404: Intune PowerShell funksjoner

Azure AD Group/User Management

Under Azure AD Group Management, får administrasjonsansvarlig muligheten til å opprette grupper og utføre utlistinger av grupper samt brukere i brukergrupper.



Figur 405: Azure AD User/Group Management

List AAD users

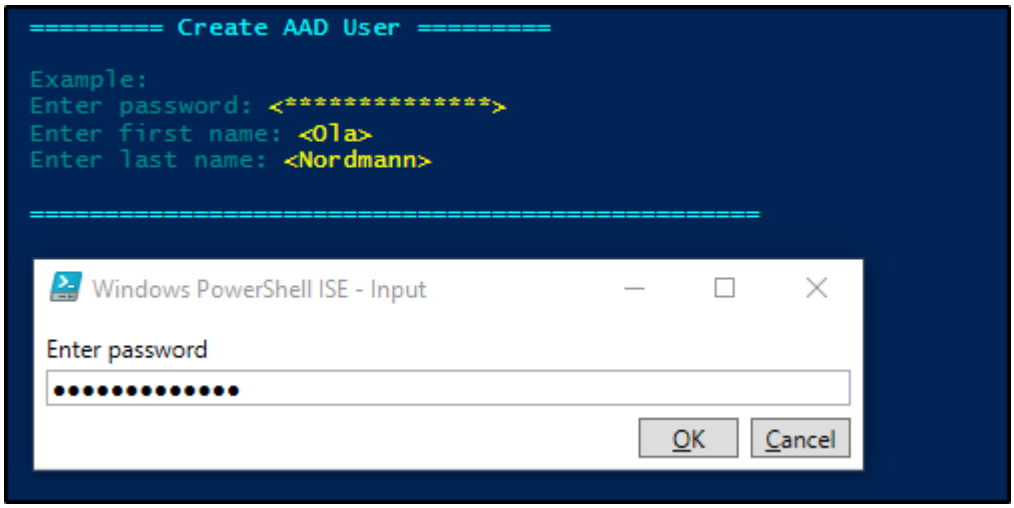
Administrasjonsansvarlig får opp en oversikt over samtlige AAD-brukere.

```
========================= List AAD Users =========================

DisplayName                                                 UserPrincipalName
-----------                                                 -----------------
Adam Savage                                                 adams@m365x949520.onmicrosoft.com
Adele Vance                                                 AdeleV@M365x949520.OnMicrosoft.com
MOD Administrator                                           admin@M365x949520.onmicrosoft.com
Alex Wilber                                                 AlexW@M365x949520.OnMicrosoft.com
Allan Deyoung                                               AllanD@M365x949520.OnMicrosoft.com
Bendik G.                                                   bendikg@M365x949520.onmicrosoft.com
Bob M.                                                      Bob@M365x949520.onmicrosoft.com
Christie Cline                                              ChristieC@M365x949520.OnMicrosoft.com
Dat-Danny P.                                                DatDannyP@M365x949520.onmicrosoft.com
Debra Berger                                                DebraB@M365x949520.OnMicrosoft.com
Diego Siciliani                                             DiegoS@M365x949520.OnMicrosoft.com
Emily Braun                                                 EmilyB@M365x949520.OnMicrosoft.com
Frank C.                                                    Frank@M365x949520.onmicrosoft.com
Grady Archie                                                GradyA@M365x949520.OnMicrosoft.com
Henrietta Mueller                                           HenriettaM@M365x949520.OnMicrosoft.com
Irvin Sayers                                                IrvinS@M365x949520.OnMicrosoft.com
Isaiah Langer                                               IsaiahL@M365x949520.OnMicrosoft.com
Johan B.                                                    Johan@M365x949520.onmicrosoft.com
Johanna Lorenz                                              JohannaL@M365x949520.OnMicrosoft.com
Joni Sherman                                                JoniS@M365x949520.OnMicrosoft.com
Jordan Miller                                               JordanM@M365x949520.OnMicrosoft.com
Lee Gu                                                      LeeG@M365x949520.OnMicrosoft.com
Lidia Holloway                                              LidiaH@M365x949520.OnMicrosoft.com
Markus R.                                                   Markus@M365x949520.onmicrosoft.com
Mathilda M.                                                 Mathilda@M365x949520.onmicrosoft.com
Megan Bowen                                                 MeganB@M365x949520.OnMicrosoft.com
Michael J.                                                  Michael@M365x949520.onmicrosoft.com
Mike W.                                                     Mike@M365x949520.onmicrosoft.com
Miriam Graham                                               MiriamG@M365x949520.OnMicrosoft.com
Nestor Wilke                                                NestorW@M365x949520.OnMicrosoft.com
Patti Fernandez                                             PattiF@M365x949520.OnMicrosoft.com
Pradeep Gupta                                               PradeepG@M365x949520.OnMicrosoft.com
Stein M.                                                    Steinm@M365x949520.onmicrosoft.com
On-Premises Directory Synchronization Service Account       Sync_DC01_1e0ae5af8883@M365x949520.onmicr
```

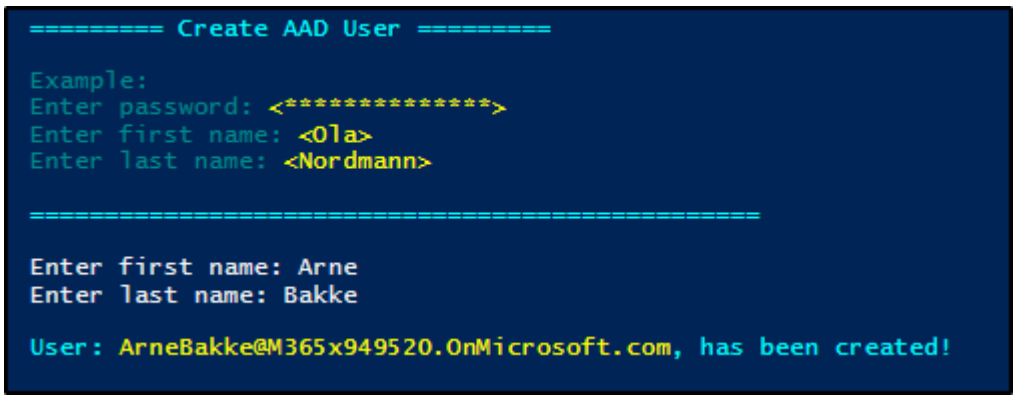
Figur 406: List AAD users

Create new AAD user

Administrasjonsansvarlig kan opprette en ny bruker ved å skrive inn passord, fornavn og etternavn på bruker.



Figur 407: Create new AAD user



Figur 408: Create new AAD user

Remove AAD user

Administrasjonsansvarlig har mulighet til å slette en bruker ved å skrive inn UserPrincipalName for brukeren som skal slettes.

```
========= Delete AAD User =========

Example:
Enter user principalname from list above: <LidiaH@M365x949520.OnMicrosoft.com>

=============================================


DisplayName                                                 UserPrincipalName
-----------                                                 -----------------
Adam Savage                                                 adams@m365x949520.onmicrosoft.com
Adele Vance                                                 AdeleV@M365x949520.OnMicrosoft.com
MOD Administrator                                           admin@M365x949520.onmicrosoft.com
Alex Wilber                                                 AlexW@M365x949520.OnMicrosoft.com
Allan Deyoung                                               AllanD@M365x949520.OnMicrosoft.com
Bendik G.                                                   bendikg@M365x949520.onmicrosoft.com
Bob M.                                                      Bob@M365x949520.onmicrosoft.com
Christie Cline                                              ChristieC@M365x949520.OnMicrosoft.com
Dat-Danny P.                                                DatDannyP@M365x949520.onmicrosoft.com
Debra Berger                                                DebraB@M365x949520.OnMicrosoft.com
Diego Siciliani                                             DiegoS@M365x949520.OnMicrosoft.com
Emily Braun                                                 EmilyB@M365x949520.OnMicrosoft.com
Enrico Cattaneo                                             EnricoC@M365x949520.OnMicrosoft.com
Frank C.                                                    Frank@M365x949520.onmicrosoft.com
Grady Archie                                                GradyA@M365x949520.OnMicrosoft.com
Henrietta Mueller                                           HenriettaM@M365x949520.OnMicrosoft.com
Irvin Sayers                                                IrvinS@M365x949520.OnMicrosoft.com
Isaiah Langer                                               IsaiahL@M365x949520.OnMicrosoft.com
Johan B.                                                    Johan@M365x949520.onmicrosoft.com
Johanna Lorenz                                              JohannaL@M365x949520.OnMicrosoft.com
Joni Sherman                                                JoniS@M365x949520.OnMicrosoft.com
Jordan Miller                                               JordanM@M365x949520.OnMicrosoft.com
Lee Gu                                                      LeeG@M365x949520.OnMicrosoft.com
Lidia Holloway                                              LidiaH@M365x949520.OnMicrosoft.com
Markus R.                                                   Markus@M365x949520.onmicrosoft.com
Mathilda M.                                                 Mathilda@M365x949520.onmicrosoft.com
Megan Bowen                                                 MeganB@M365x949520.OnMicrosoft.com
Michael J.                                                  Michael@M365x949520.onmicrosoft.com
Mike W.                                                     Mike@M365x949520.onmicrosoft.com
Miriam Graham                                               MiriamG@M365x949520.OnMicrosoft.com
Nestor Wilke                                                NestorW@M365x949520.OnMicrosoft.com
Patti Fernandez                                             PattiF@M365x949520.OnMicrosoft.com
Pradeep Gupta                                               PradeepG@M365x949520.OnMicrosoft.com
Stein M.                                                    Steinm@M365x949520.onmicrosoft.com
On-Premises Directory Synchronization Service Account       Sync_DC01_1e0ae5af8883@M365x949520.onmic


Enter user principalname from list above: EnricoC@M365x949520.OnMicrosoft.com

User: EnricoC@M365x949520.OnMicrosoft.com, has been removed!
```

Figur 409: Remove AAD user

List AAD groups

Administrasjonsansvarlig får opp en oversikt over samtlige AAD-grupper.

```
========= List AAD groups =========


displayName                securityEnabled createdDateTime
-----------                --------------- ---------------
App Deployment User Group             True 05.04.2019 07:12:51
AND Ent                               True 10.04.2019 09:10:09
IT Department                        False 02.04.2019 09:07:46
Co-managed devices                    True 06.03.2019 10:51:42
computerGroup                         True 06.03.2019 20:13:26
Intune devices                        True 06.03.2019 10:51:02
Android Devices                       True 08.04.2019 09:46:55
AutoPilot Preview remote              True 02.04.2019 12:31:36
Windows Autopilot                     True 19.03.2019 08:36:07
SCCM User Group                       True 11.03.2019 13:42:34
```

Figur 410: List AAD groups

List AAD group members

Administrasjonsansvarlig skriver inn navn på gruppen som han ønsker å hente ut gruppemedlemmer fra. Funksjonen vil deretter liste ut samtlige medlemmer tilhørende valgt gruppe.

```
========= List AAD group members =========

Example:
Enter group name: <0000-1111-2222-3333>

================================================


displayName   securityEnabled createdDateTime
-----------   --------------- ---------------
IT Department           False 02.04.2019 09:07:46


Skriv inn gruppenavn, for å hente ut brukere: IT Department

givenName surname       mail
--------- -------       ----
MOD       Administrator admin@M365x949520.OnMicrosoft.com
Bendik    Gjovikli      bendikg@M365x949520.onmicrosoft.com
Stein     Meisingseth   Steinm@M365x949520.onmicrosoft.com
```

Figur 411: List AAD group members

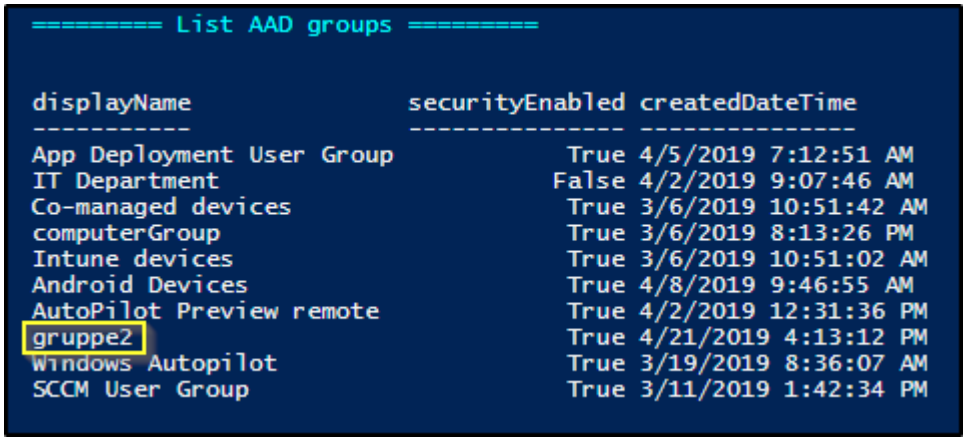
Create new AAD group

Administrasjonsansvarlig kan opprette en ny gruppe ved å skrive inn navnet på gruppen.

```
========= Create new AAD group =========

Example:
Enter group name: <Group 001>

========================================

Enter group name: gruppe2

The group: gruppe2, has been created!
```

Figur 412: Create new AAD group

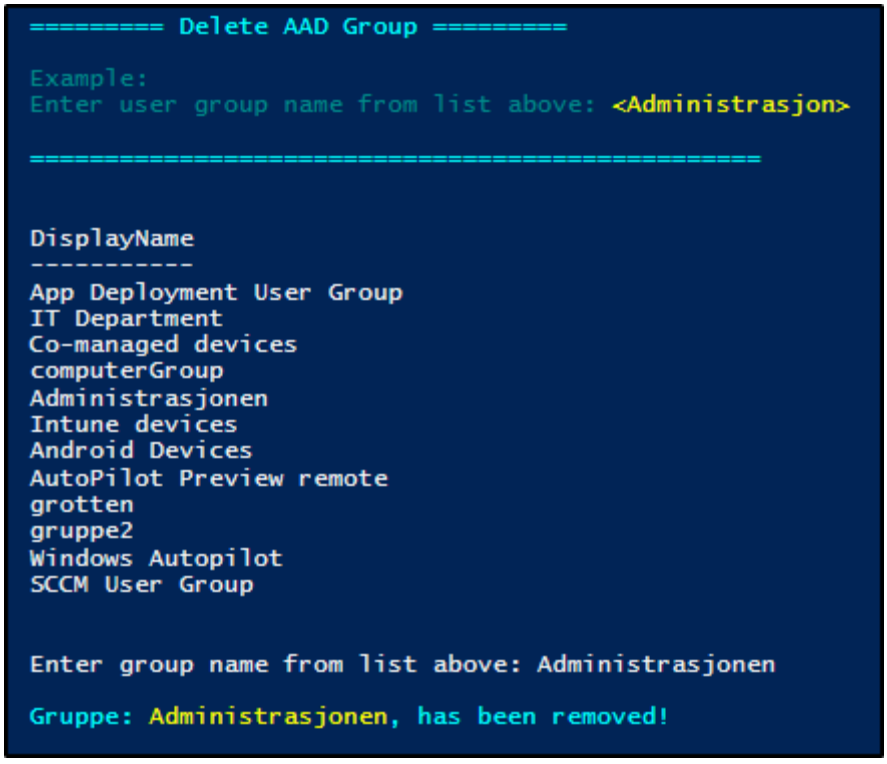
Nedenfor kan vi se at gruppe2 har blitt lagt til, ved å kjøre funksjonen som lister ut AAD-grupper.



Figur 413: Create new AAD group

Remove AAD group

Administrasjonsansvarlig har mulighet til å slette en gruppe ved å skrive inn navnet på gruppen som skal slettes.



Figur 414: Remove AAD group

Intune Device Management

Under Intune Device Management, har vi lagt til diverse funksjoner som vi blant annet finner igjen når man velger en device under ***Microsoft Intune – Devices – All devices***. Administrasjonsansvarlig har også mulighet til å liste ut samtlige Intune/co-managed enheter under denne menyen.

```
============= ~ Intune Management - Intune Device Management ~ =============

1. List Intune/Co-managed devices

2. Sync device

3. Remote lock a device

4. Reset passcode on device

5. Retire a device

6. Wipe a device

7. Restart a device

0. Back to Intune Management

Enter a value between 0 and 7:
```

Figur 415: Intune Device Management

List Intune/Co-managed devices

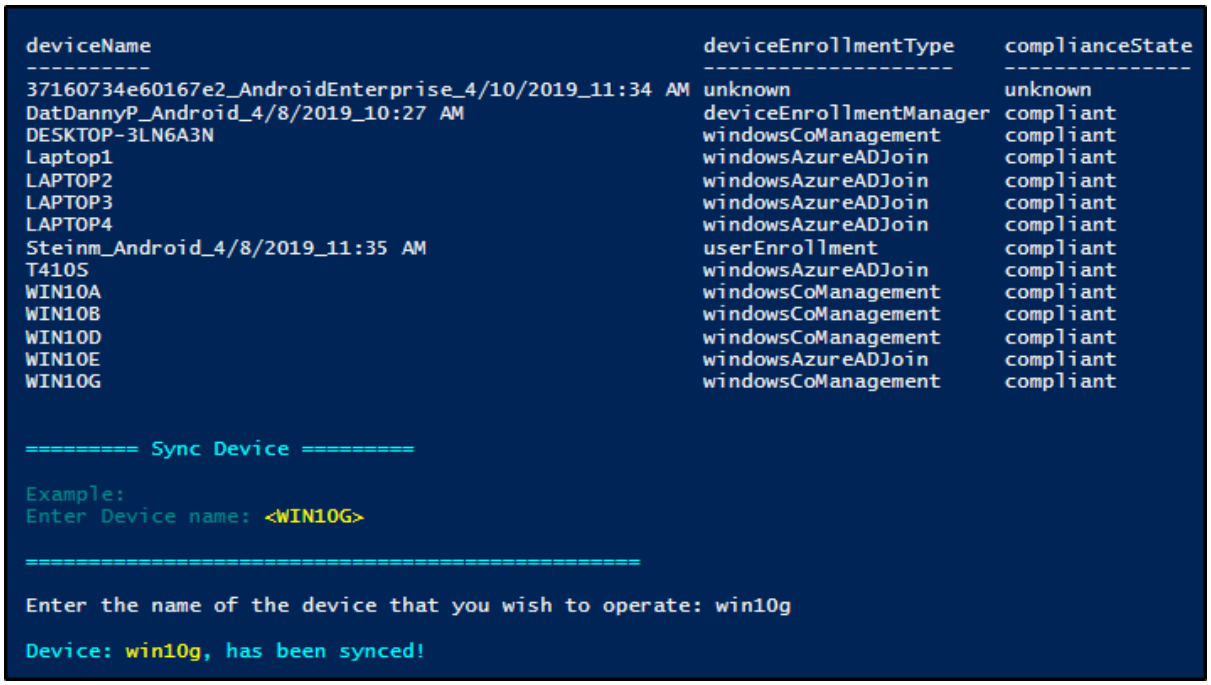
Denne funksjonen lister ut samtlige Intune/co-managed-enheter.

```
========= List Intune/Co-managed Devices =========


deviceName                                          deviceEnrollmentType    complianceState
----------                                          --------------------    ---------------
37160734e60167e2_AndroidEnterprise_4/10/2019_11:34 AM unknown               unknown
DatDannyP_Android_4/8/2019_10:27 AM                 deviceEnrollmentManager compliant
DESKTOP-3LN6A3N                                     windowsCoManagement     compliant
Laptop1                                             windowsAzureADJoin      compliant
LAPTOP2                                             windowsAzureADJoin      compliant
LAPTOP3                                             windowsAzureADJoin      compliant
LAPTOP4                                             windowsAzureADJoin      compliant
LAPTOP5                                             windowsAzureADJoin      compliant
Steinm_Android_4/8/2019_11:35 AM                    userEnrollment          compliant
STEINSIN                                            windowsAzureADJoin      compliant
T410S                                               windowsAzureADJoin      compliant
WIN10A                                              windowsCoManagement     compliant
WIN10B                                              windowsCoManagement     compliant
WIN10D                                              windowsCoManagement     compliant
WIN10E                                              windowsAzureADJoin      compliant
WIN10G                                              windowsCoManagement     compliant
```

Figur 416: List Intune/co-managed devices

Sync device

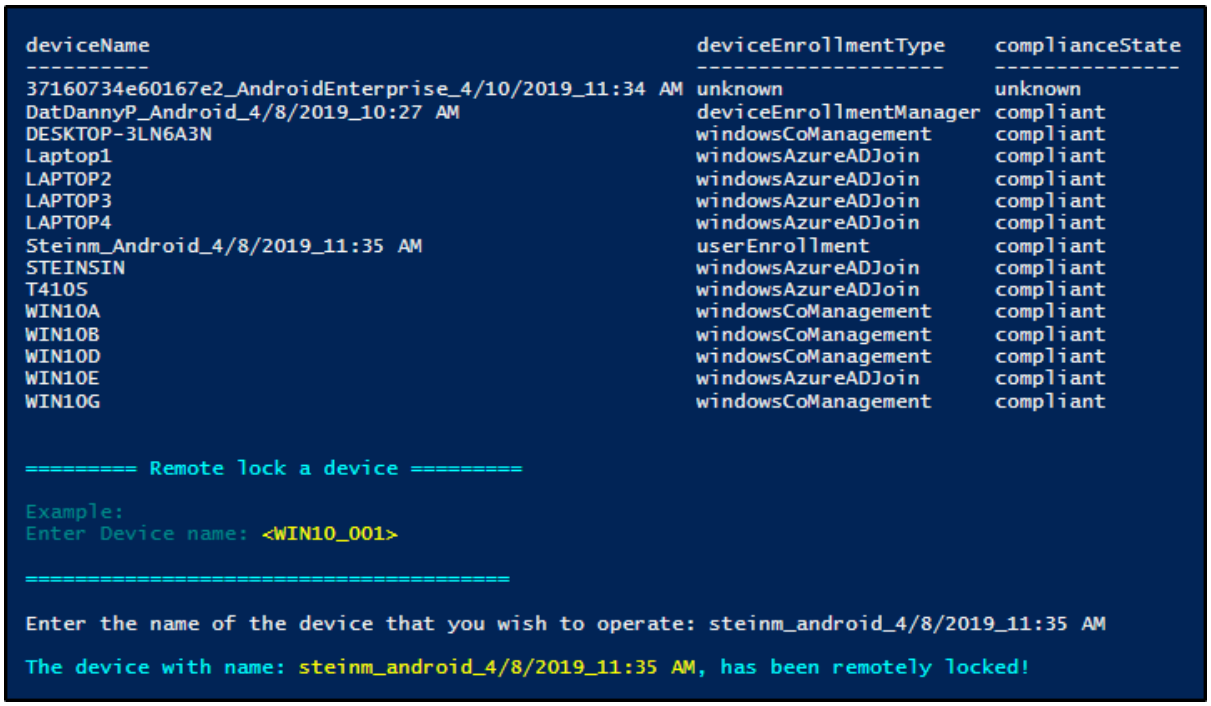
Synkroniseringsfunksjonen gjør det mulig for administrasjonsansvarlig å utføre synkronisering på én enkelt enhet, ved at man skriver inn navnet på enheten.



Figur 417: Sync device

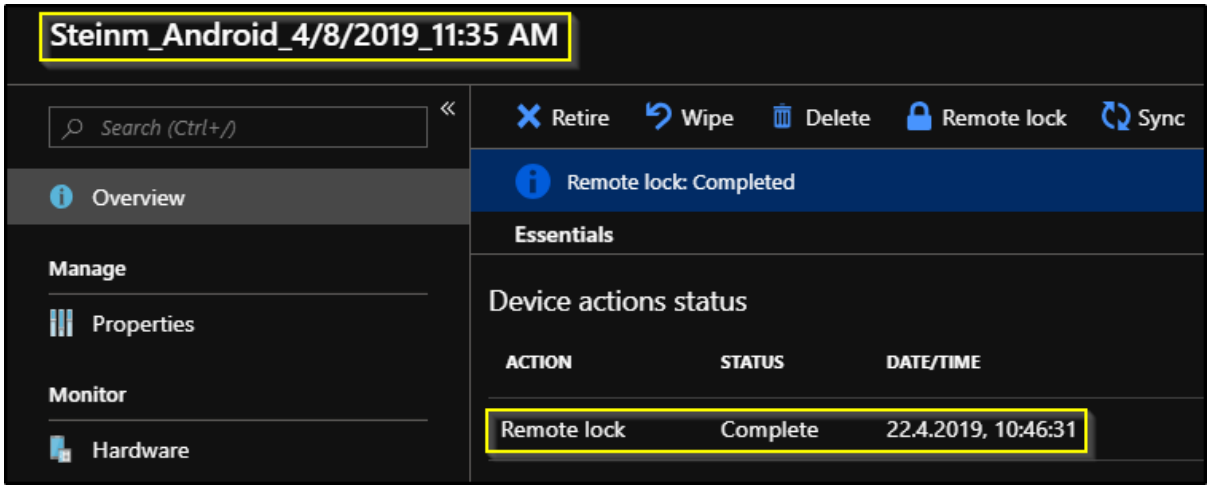
Remote Lock a device

Administrasjonsansvarlig kan ved bruk av denne funksjonen låse en enhet ved at han skriver inn navnet på enheten som man ønsker å låse. Denne funksjonen fungerer kun på mobiler.



Figur 418: Remote Lock a device

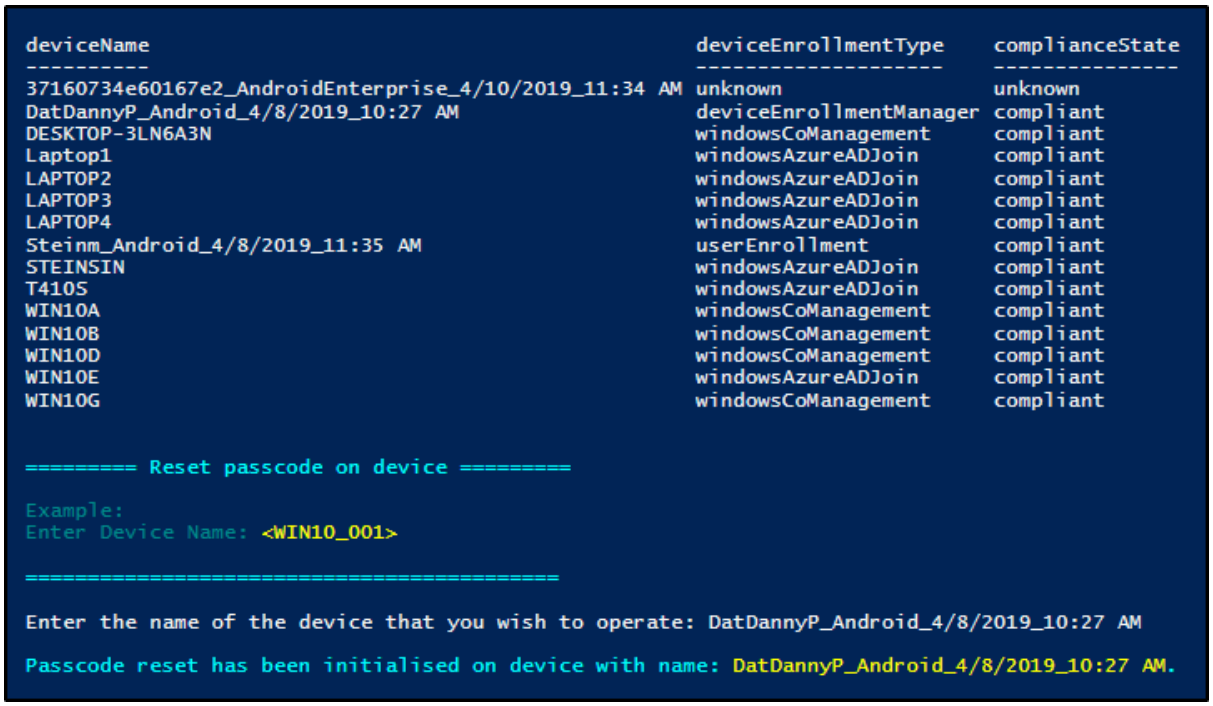
Nedenfor ser vi at remote lock har blitt kjørt på enheten også i Intune.



Figur 419: Remote Lock a device

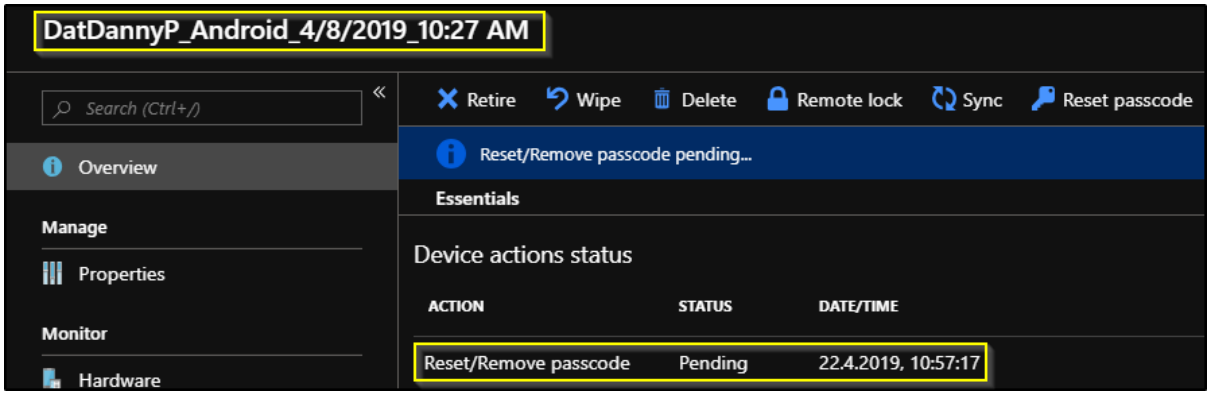
Reset passcode on device

Administrasjonsansvarlig kan ved bruk av denne funksjonen utføre passcode reset på en enhet, ved å skrive inn navnet på enheten. Denne funksjonen fungerer kun på mobiler.



Figur 420: Reset passcode on device

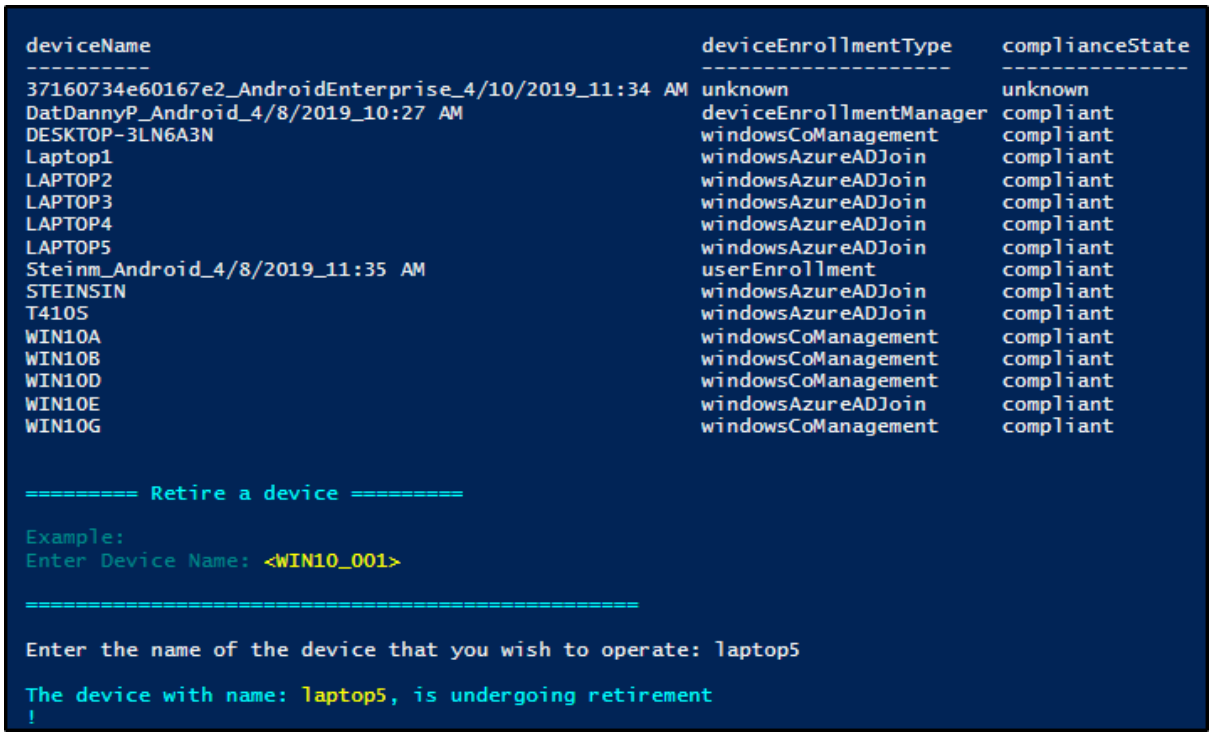
Nedenfor ser vi at reset passcode-funksjonen har blitt kjørt også i Intune.



Figur 421: Reset passcode on device

Retire a device

Administrasjonsansvarlig kan ved bruk av denne funksjonen "retire" en enhet. Dette gjøres ved å skrive inn navnet på enheten man ønsker å utføre operasjonen på.



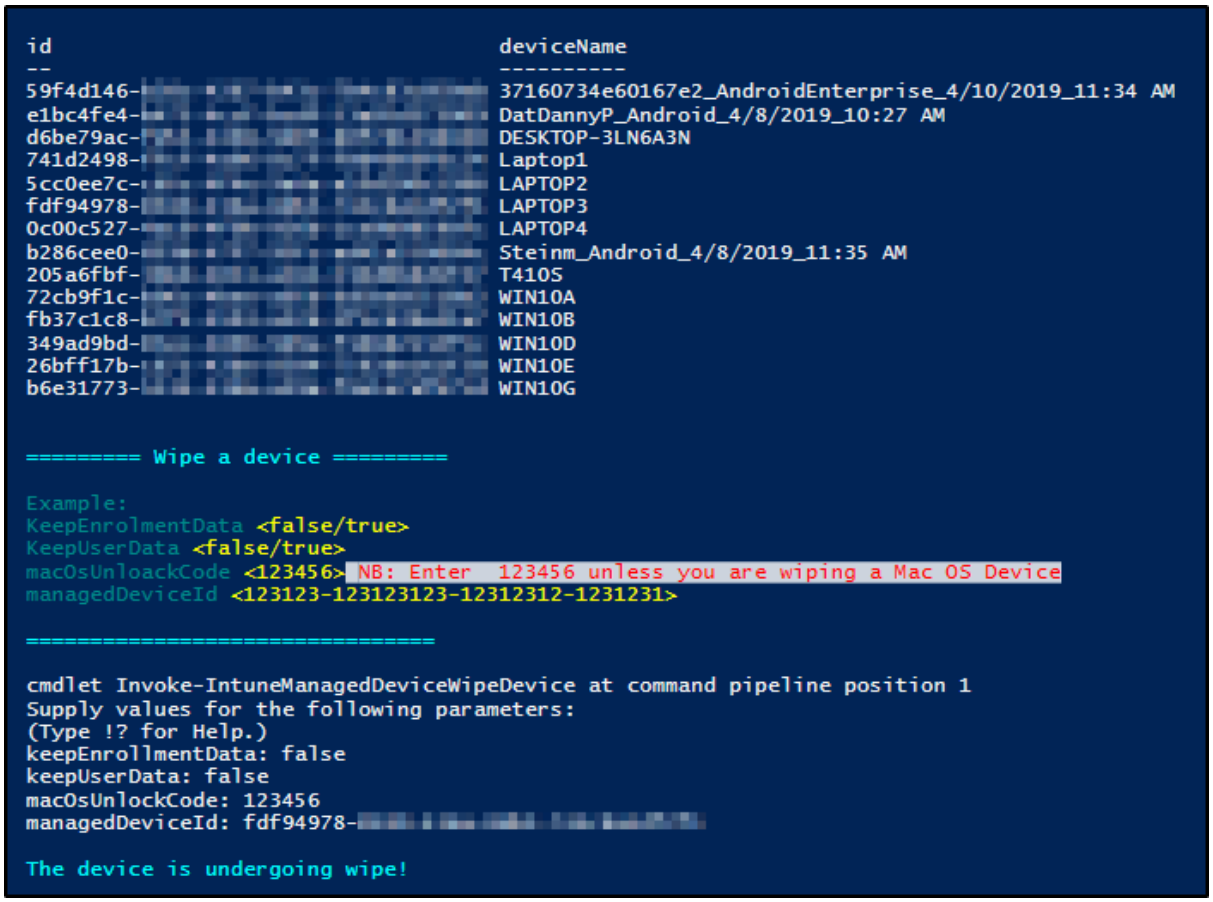
Figur 422: Retire a device

Nedenfor ser vi i Intune at "Retire pending" på laptop5. Når Retire-prosessen har blitt gjennomført, vil enheten bli fjernet fra listen.

Figur 423: Retire a device

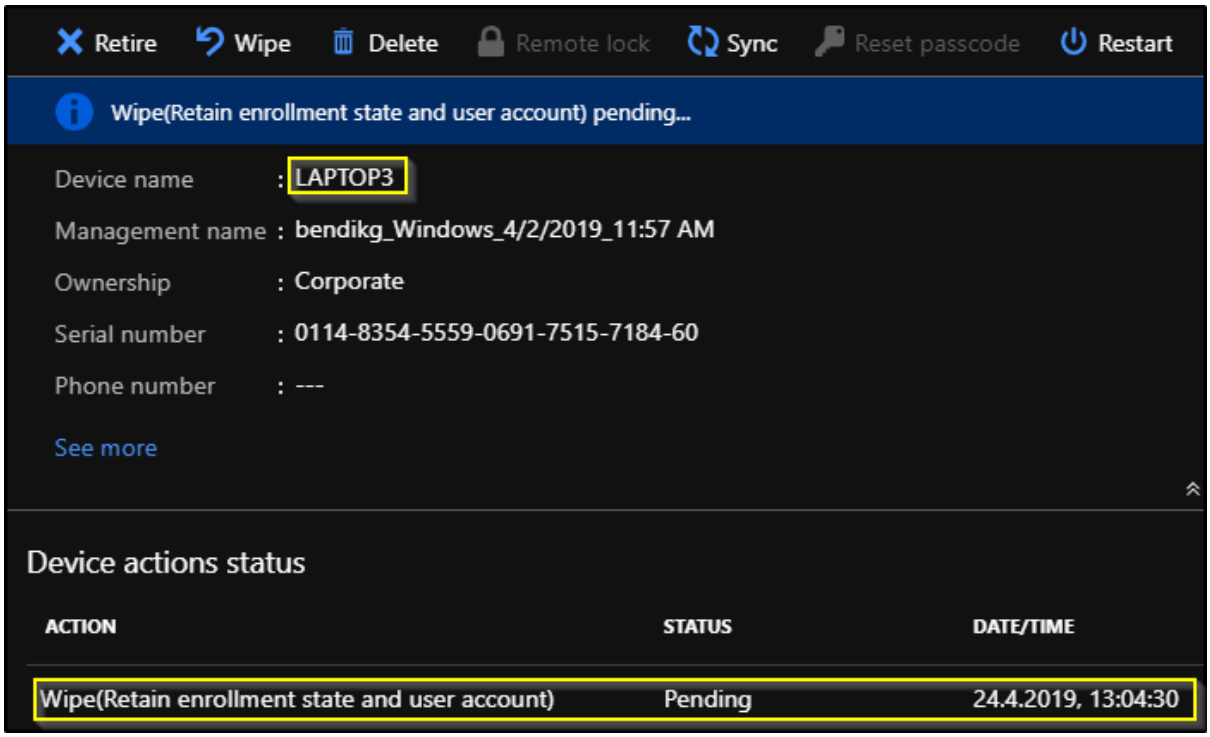
Wipe a device

Administrasjonsansvarlig kan ved bruk av denne funksjonen "wipe" en enhet. Dette gjøres ved at man velger om man ønsker å beholde enrollmentdata og userdata, deretter legger man til "Mac OS Unlock Code" dersom man har det. Hvis man ikke skal "wipe" en Mac OS enhet, skriver man inn verdien "123456", som beskrevet I eksempelet når man kjører funksjonen. Til slutt legger man til Device ID. Denne funksjonen er ikke helt brukervennlig da, da man ikke kan legge til alle parameterne på en gang, når man kjører **Invoke-IntuneManagedDeviceWipeDevice** cmdleten.



Figur 424: Wipe a device

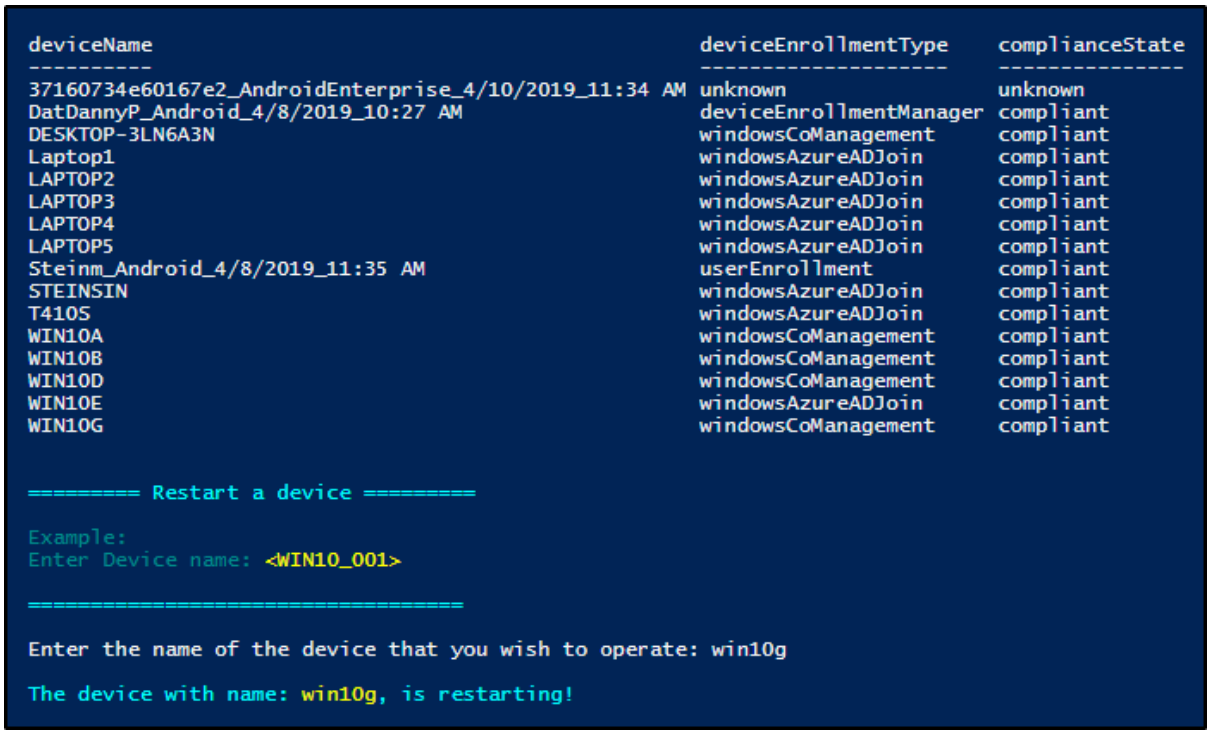
Nedenfor ser vi at “Wipe” er satt til til “Pending” under status i Intune.



Figur 425: Wipe a device

Restart a device

Administrasjonsansvarlig kan ved bruk av denne funksjonen restarte en enhet. Man skriver inn navnet på enheten man ønsker å restarte.



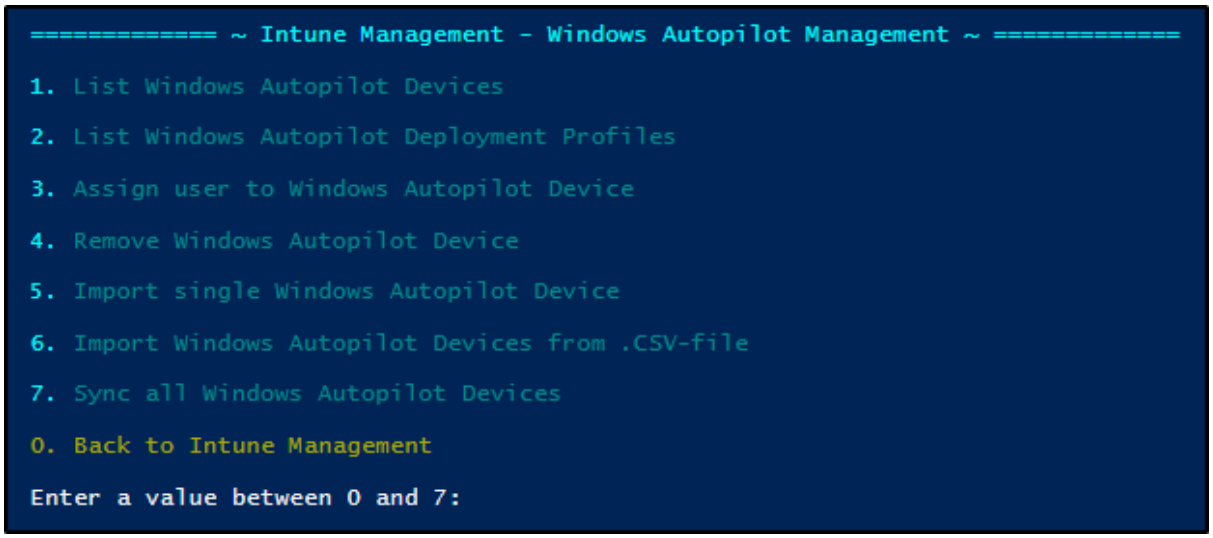
Figur 426: Restart a device

Når man kjører denne funksjonen, vil ikke enheten restarte umiddelbart, men sluttbrukeren vil få en beskjed om at administrator restarter enheten.

Figur 427: Restart a device

Windows Autopilot Management

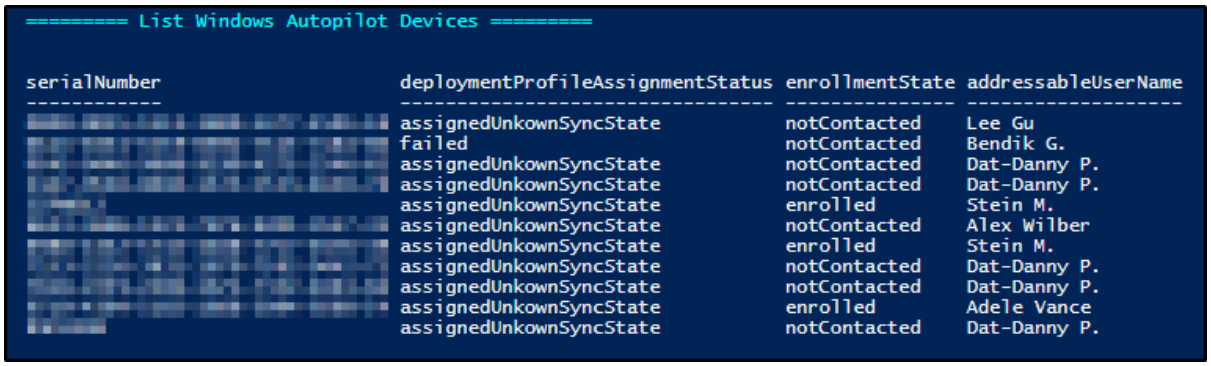
Under Windows Autopilot Management, har vi lagt til funksjoner som brukes til å ta hånd om diverse oppgaver når det gjelder Windows Autopilot.



Figur 428: Windows Autopilot Management

List Windows Autopilot Devices

Administrasjonsansvarlig kan ved bruk av denne funksjonen liste ut samtlige Windows Autopilot enheter.



Figur 429: List Windows Autopilot Devices

List Windows Autopilot Deployment Profiles

Administrasjonsansvarlig kan ved bruk av denne funksjonen liste ut samtlige Deployment-profiler.

```
========= List Windows Autopilot Deployment Profiles =========

displayName    deviceType
-----------    ----------
Custom Default windowsPc
SelfDeploy     windowsPc
```

Figur 430: List Windows Autopilot Deployment Profiles

Assign user to Windows Autopilot Device

Administrasjonsansvarlig kan ved bruk av denne funksjonen oppgi en bruker som eier av enheten. Dette gjøres ved at man legger til Device ID, User Principal Name og Display Name.

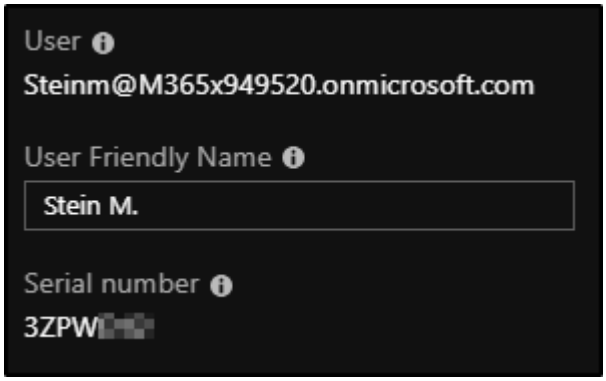
```
========= Assigner User to Device =========

Eksempel:
Enter Device ID: <0000-1111-2222-3333>
Enter User Principal Name <bjarneg@alarmnett.no>
Enter Display Name <Bjarne G>

=======================================


id                                   serialNumber                 deployment
                                                                  atus
--                                   ------------                 ----------
de3eeec9-                            0000-                        assignedUnkownSyncState
3b401d04-                            0114-                        failed
f6aa67d2-                            0545-                        assignedUnkownSyncState
765c9a75-                            2447-                        assignedUnkownSyncState
5b015127-                            3ZPW                         notAssigned
f1eeb9e6-                            6633-                        assignedUnkownSyncState
54156bb2-                            6980-                        assignedUnkownSyncState
978f6c20-                            7153-                        assignedUnkownSyncState
941f0540-                            7618-                        assignedUnkownSyncState
baa7ff7c-                            9710-                        assignedUnkownSyncState
57fb4dcb-                            R9CH                         assignedUnkownSyncState


Enter Device ID: 5b015127-
```

Figur 431: Assign user to Windows Autopilot Device

```
PattiF@M365x949520.OnMicrosoft.com                Patti Fernandez
PradeepG@M365x949520.OnMicrosoft.com              Pradeep Gupta
Steinm@M365x949520.onmicrosoft.com                Stein M.
Sync_DC01_1e0ae5af8883@M365x949520.onmicrosoft.com On-Premises Directory Synchronization Service...


Enter User Principal Name: Steinm@M365x949520.onmicrosoft.com
Enter Display Name: Stein M.

Autopilot device with ID: 5b015127-7d99-4d5a-8992-84ba9f5d8347, has been assigned to user: Stein M..
```

Figur 432: Assign user to Windows Autopilot Device

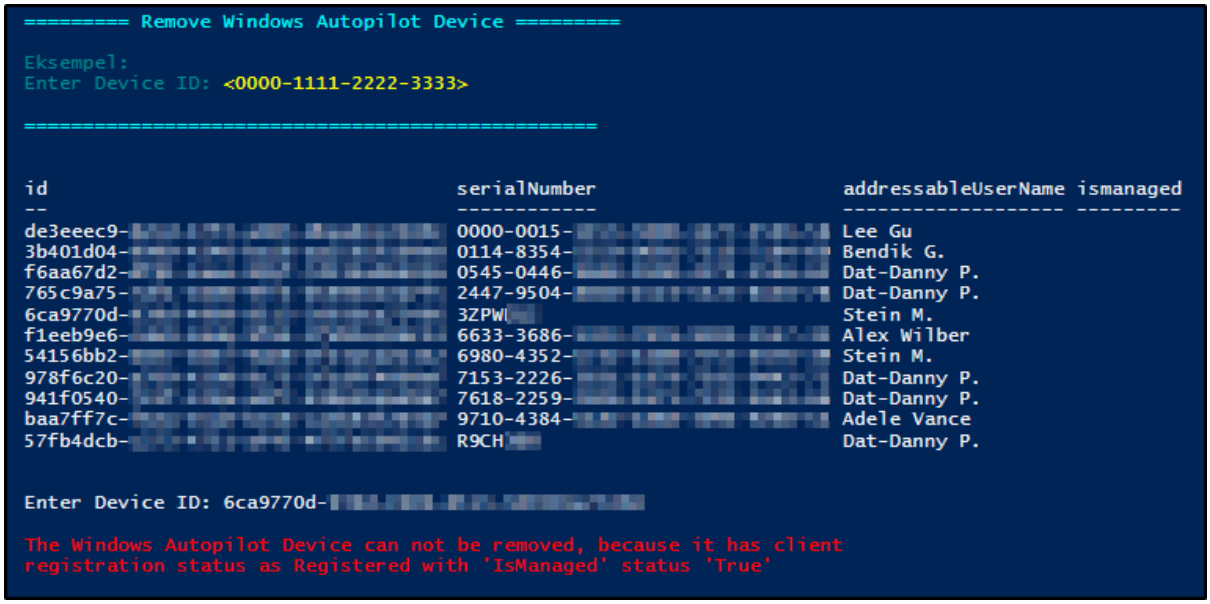
Når funksjonen er kjørt vil brukeren umiddelbart bli lagt til som bruker under Windows Autopilot enheten, som vist i skjermbildet nedenfor hentet fra Intune.



Figur 433: Assign user to Windows Autopilot Device

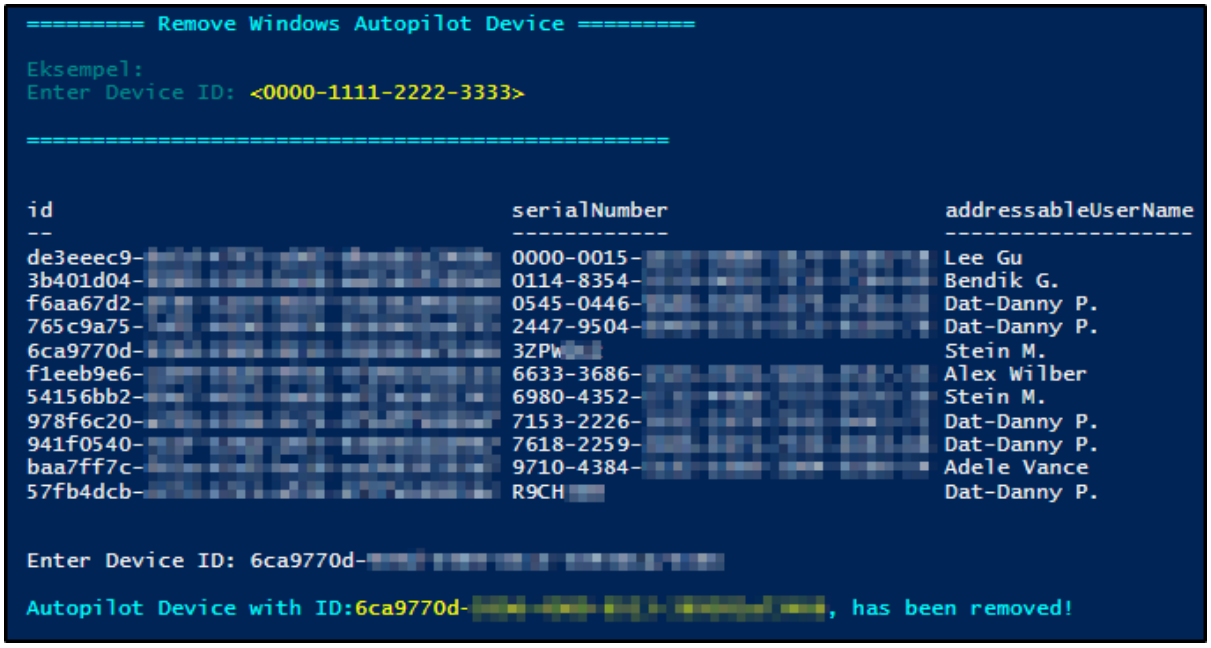
Remove Windows Autopilot Device

Administrasjonsansvarlig kan ved bruk av denne funksjonen slette en Windows Autopilot enhet. Ved å skrive inn Device ID, på enheten man ønsker å slette, blir funksjonen utført. Det forutsettes at enheten kun finnes i Windows autopilot device oversikten og ikke andre steder i Azure. Dersom enheten er enrolled i Intune, vil man få feilmeldingen som vist nedenfor i rød skrift.

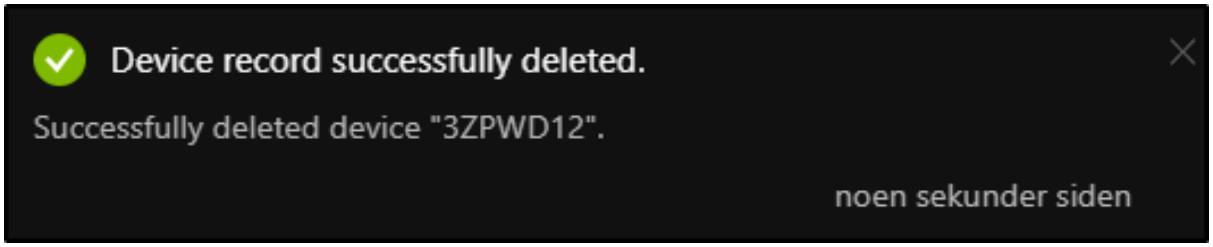


Figur 434: Remove Windows Autopilot Device

Derimot dersom enheten kun er en Windows Autopilot enhet som ikke er rullet inn i Intune, vil enheten bli slettet.



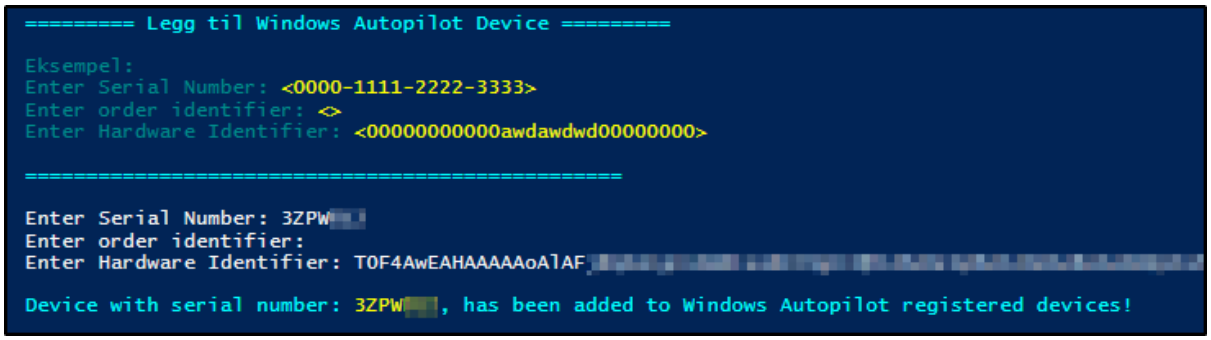
Figur 435: Remove Windows Autopilot Device



Figur 436: Remove Windows Autopilot Device

Import single Windows Autopilot Device

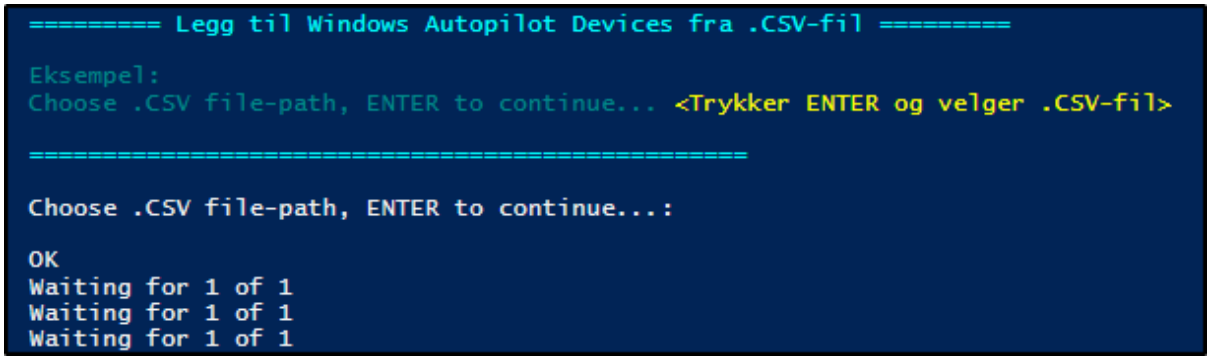
Administrasjonsansvarlig kan ved bruk av denne funksjonen importere en enkelt enhet. Dette forutsetter at man har hentet ut serial nummer og hardware identifier fra enheten. Man legger deretter inn serial-nummer, order identifier (hvis man har) og hardware identifier. Enheten vil nå bli lagt til under Windows Autopilot Devices.



Figur 437: Import single Windows Autopilot Device

Import Windows Autopilot Devices from CSV-file

Administrasjonsansvarlig kan ved bruk av denne funksjonen importere flere enheter ved bruk av en CSV-fil. Dette forutsetter at man har en CSV-fil med flere enheter tilgjengelig. Når man kjører funksjonen, vil et vindu komme opp, hvor man navigerer seg til CSV-filen og velger den. Etter litt venting, vil enhetene bli lagt til.



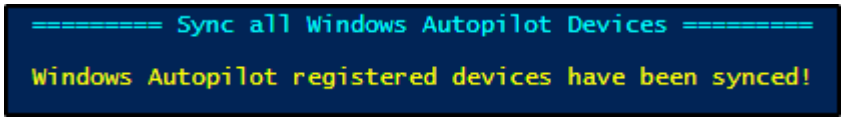
Figur 438: Import Windows Autopilot Devices from .CSV-file

Bildet nedenfor viser et utklipp fra Intune, hvor vi ser at enheten har blitt lagt til.

Figur 439: Import Windows Autopilot Devices from .CSV-file

Sync all Windows Autopilot Devices

Administrasjonsansvarlig kan ved bruk av denne funksjonen synkronisere samtlige Windows Autopilot enheter.



Figur 440: Sync all Windows Autopilot Devices

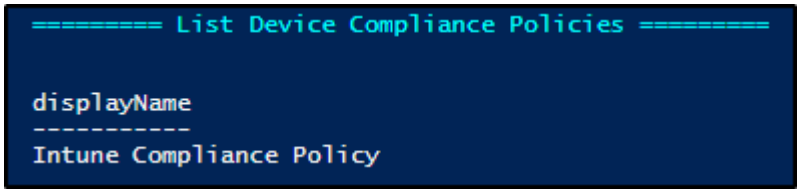
Device Compliance Policy Management

Under Device Compliance Policy Management, har vi lagt til funksjoner som brukes til å ta hånd om diverse oppgaver når det gjelder Device Compliance.

Figur 441: Device Compliance Policy Management

List Device Compliance Policies

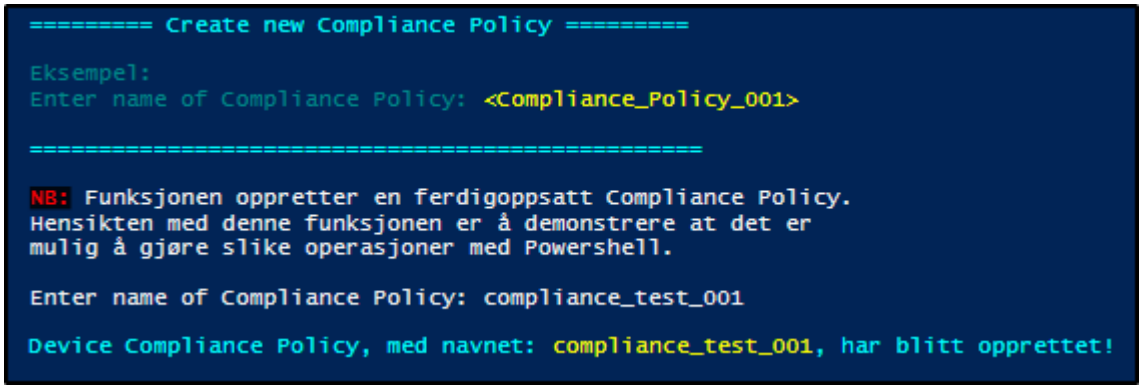
Administrasjonsansvarlig kan ved bruk av denne funksjonen liste ut samtlige Device Compliance Policy-er.



Figur 442: List Device Compliance Policies

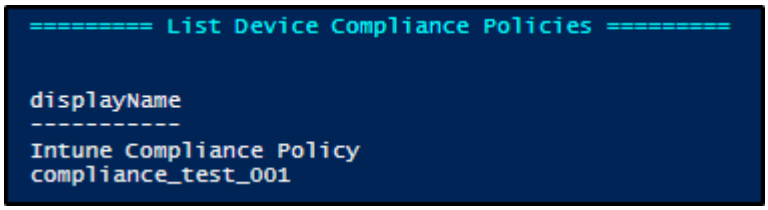
Create new Device Compliance Policy

Administrasjonsansvarlig kan ved bruk av denne funksjonen opprette en Device Compliance Policy. I og med at det finnes så utrolig mange innstillinger som man kan sette for en Device Compliance Policy, er det ikke så hendig å skulle gjøre dette i PowerShell, med mindre man selv skriver scriptet. Vi har derfor valgt å opprette en Device Compliance Policy, hvor vi har på forhånd satt noen innstillinger. Hensikten her er mer å vise at man kan opprette Device Compliance Policy-er ved bruk av PowerShell.



Figur 443: Create new Device Compliance Policy

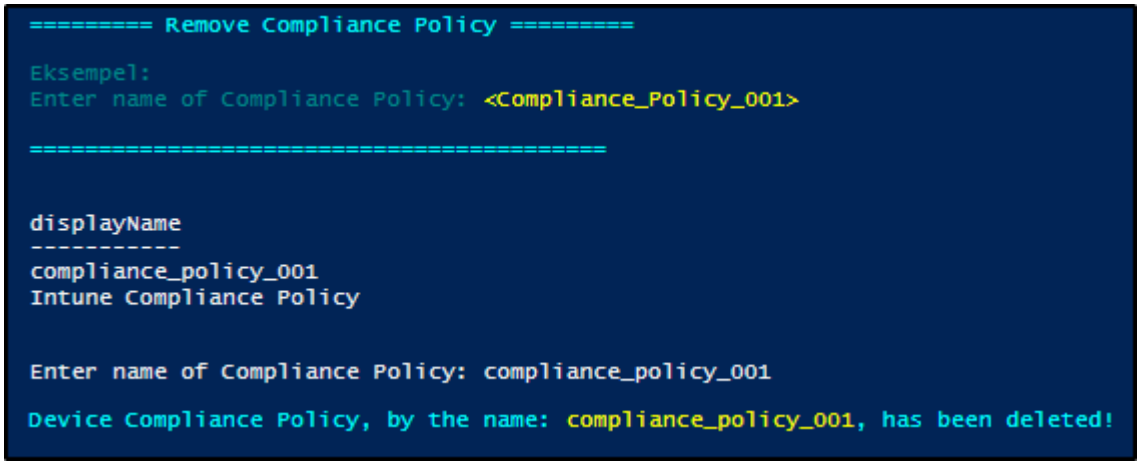
I skjermbildet nedenfor har vi kjørt funksjonen som lister ut Device Compliance Policy-er. Vi ser her at "Compliance_test_001", har blitt opprettet.



Figur 444: Create new Device Compliance Policy

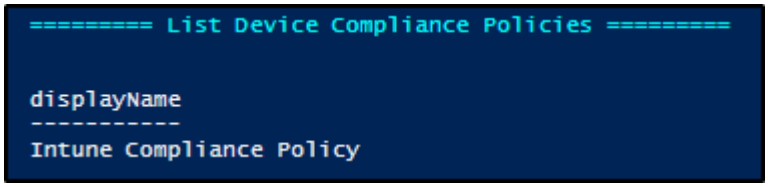
Remove Device Compliance Policy

Administrasjonsansvarlig kan ved bruk av denne funksjonen slette en Device Compliance Policy. Dette gjøres ved at man skriver inn navnet på Device Compliance Policy-en som man ønsker å slette.



Figur 445: Remove Device Compliance Policy

I skjermbildet nedenfor har vi kjørt funksjonen som lister ut Device Compliance Policy-er, og vi ser her at "Compliance_test_001", har blitt slettet.



Figur 446: Remove Device Compliance Policy

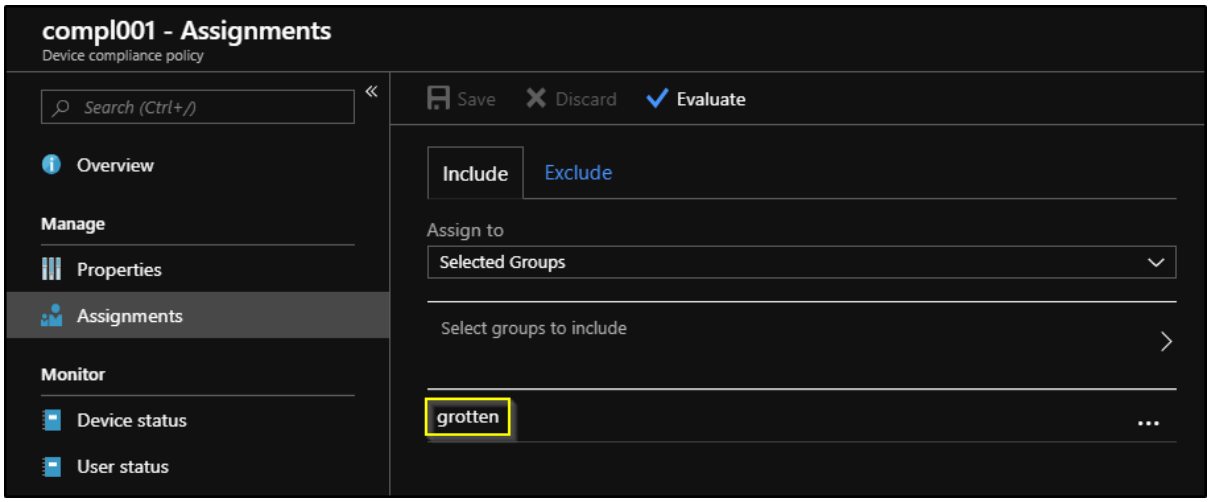
Assign Compliance Policy to Group

Administrasjonsansvarlig kan ved bruk av denne funksjonen tildele en Compliance Policy til en gruppe. Man velger navn på Compliance Policy og navn på gruppen, og funksjonen utføres.

```
========= Compliance Policy Management - Assign Compliance Policy to Group =========

Example:
Enter name of Compliance Policy: <Comp_Policy_001>
Enter name of group: <gruppe_001>

================================================


displayName
-----------
compl001
Intune Compliance Policy
compGrotten


Enter name of Compliance Policy: compl001

displayName
-----------
App Deployment User Group
IT Department
Co-managed devices
computerGroup
Intune devices
Android Devices
AutoPilot Preview remote
grotten
gruppe2
Windows Autopilot
SCCM User Group


Enter name of group: grotten
Compliance Policy with name: compl001, has been assigned to group: grotten.
```

Figur 447: Assign Compliance Policy to Group

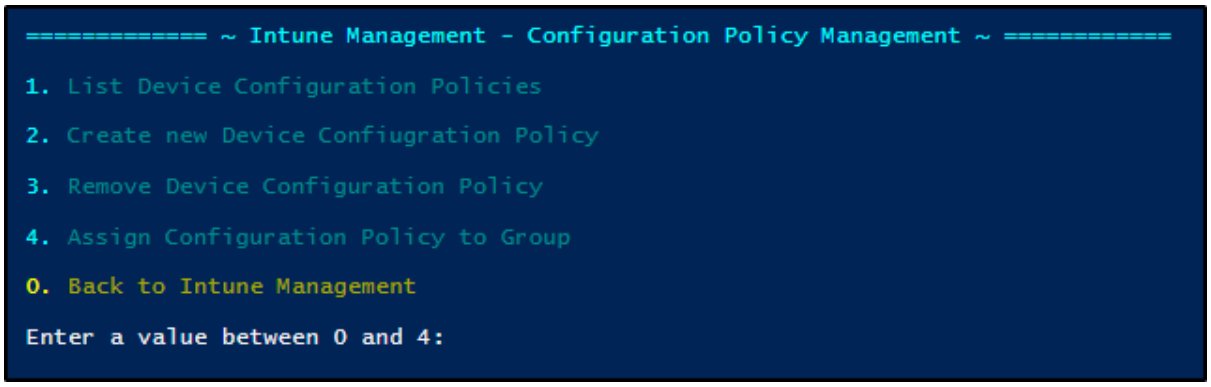
Nedenfor ser vi at gruppen har fått tildelt Compliance Policy-en.



Figur 448: Assign Compliance Policy to Group

Device Configuration Policy Management

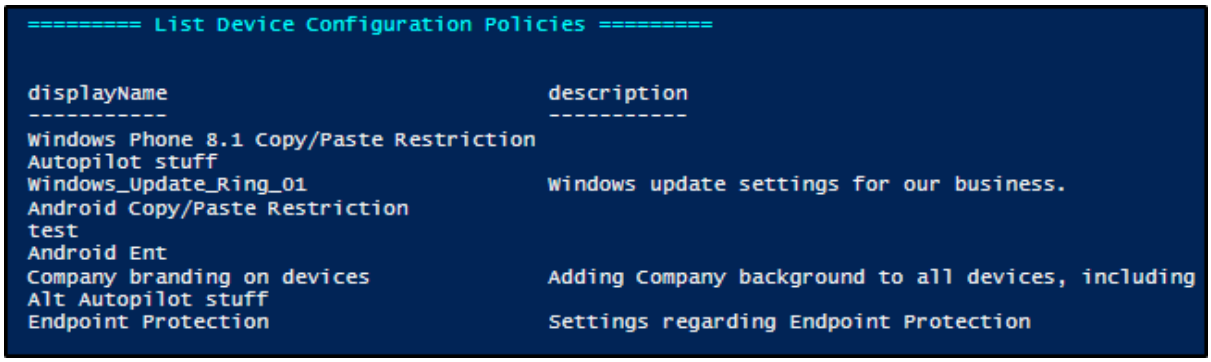
Under Configuration Policy Management, har vi lagt til funksjoner som brukes til å ta hånd om diverse oppgaver som det gjelder Configuration Policy Management.



Figur 449: Device Configuration Policy Management

List Device Configuration Policies

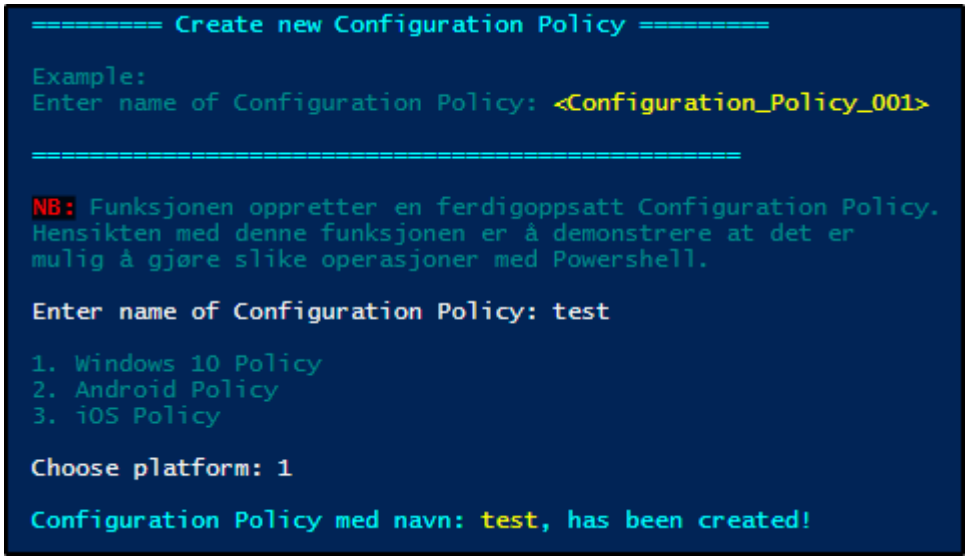
Administrasjonsansvarlig kan ved bruk av denne funksjonen liste ut samtlige Device Configuration Policies.



Figur 450: List Device Configuration Policies

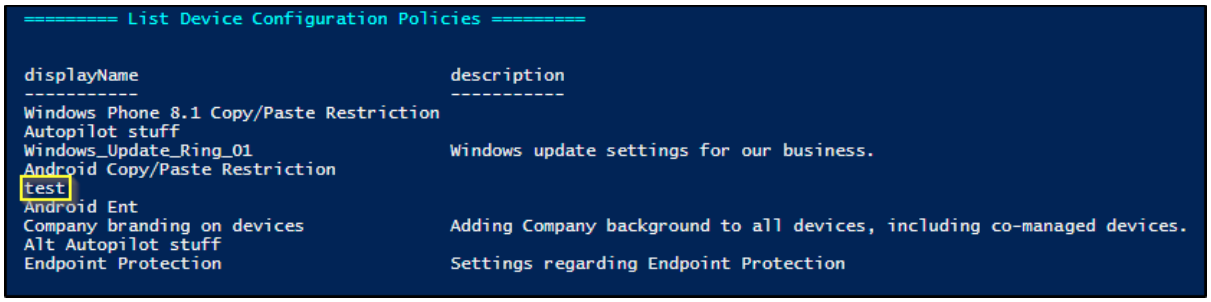
Create new Device Configuration Policy

Administrasjonsansvarlig kan ved bruk av denne funksjonen opprette en ferdigoppsatt Configuration Policy. Hensikten med denne funksjonen er å demonstrere at det er mulig å gjøre slike operasjoner med Powershell. Man får her muligheten til å velge om dette skal være en Windows 10-, Android- eller iOS-policy. Man setter et navn, velger et alternativ og (1, 2, 3) og Policy-en vil bli opprettet.



Figur 451: Create new Device Configuration Policy

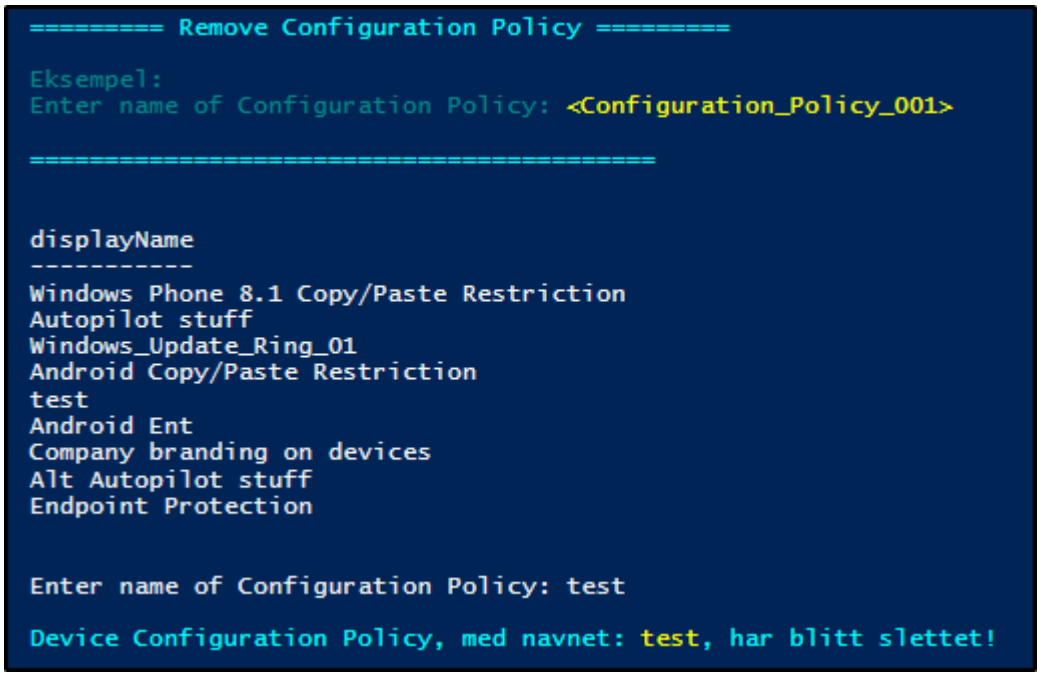
Nedenfor ser vi at policy-en "test" har blitt opprettet ved å kjøre funksjonen som lister ut Device Configuration Policy-er.



Figur 452: Create new Device Configuration Policy

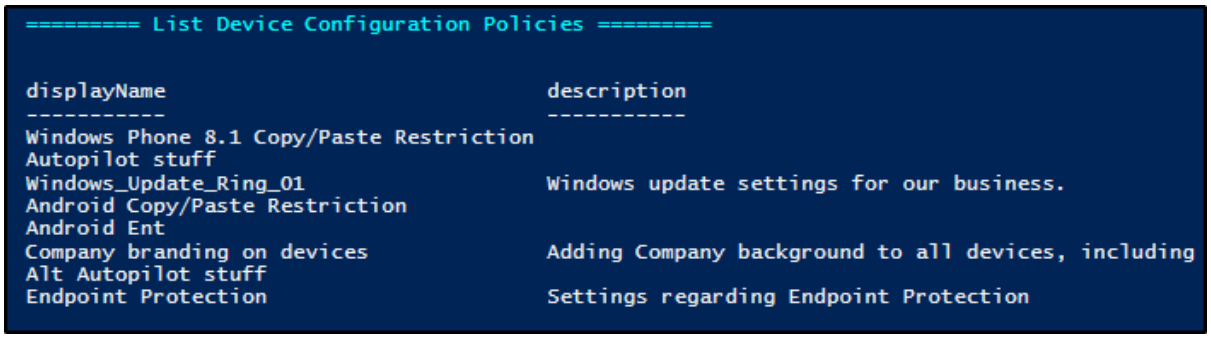
Remove Device Configuration Policy

Administrasjonsansvarlig kan ved bruk av denne funksjonen slette en Device Configuration Policy. Man skriver inn navnet på policy-en man ønsker å slette.



Figur 453: Remove Device Configuration Policy

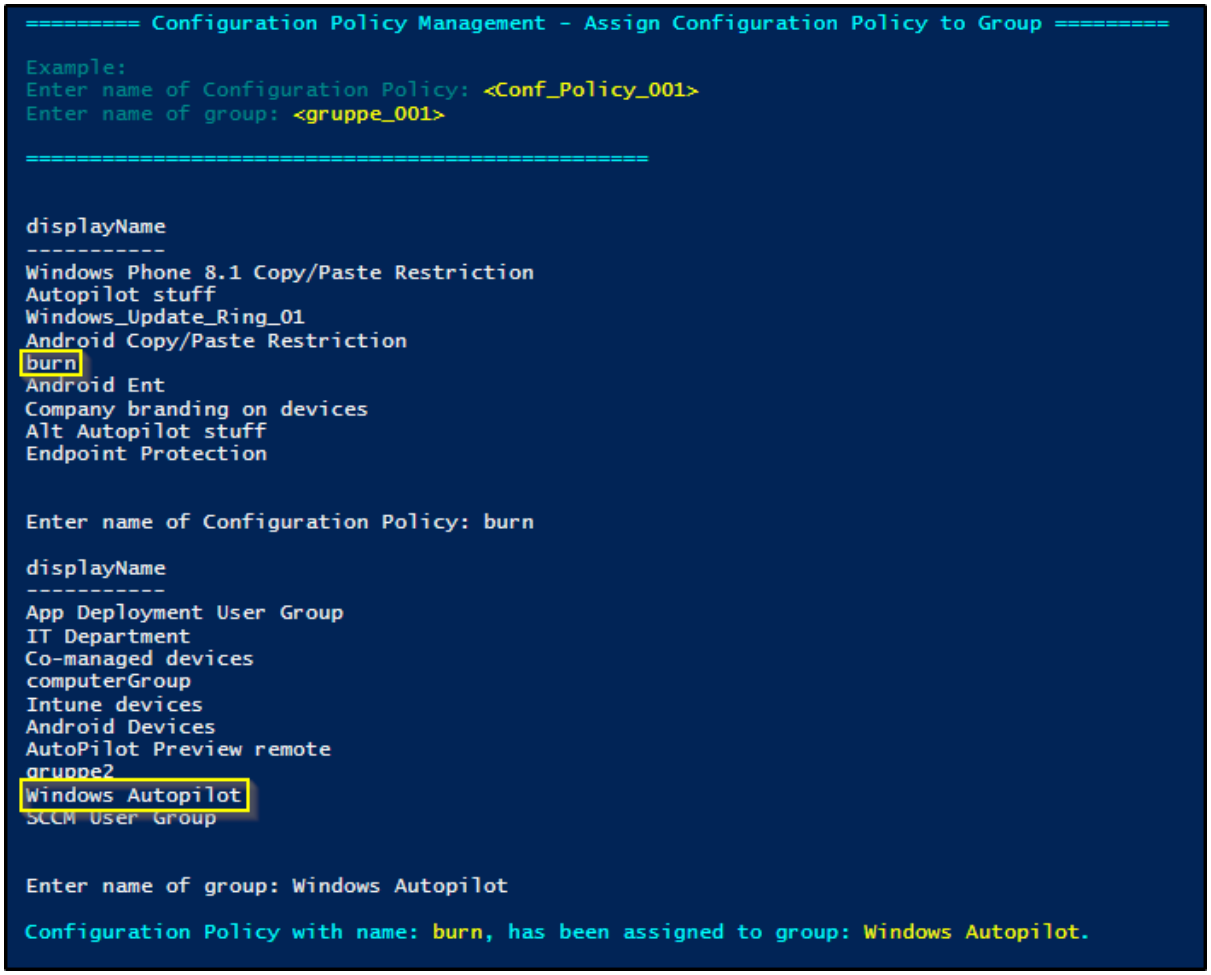
Nedenfor ser vi at Device Configuration Policy-en "test", ikke lenger eksisterer.



Figur 454: Remove Device Configuration Policy

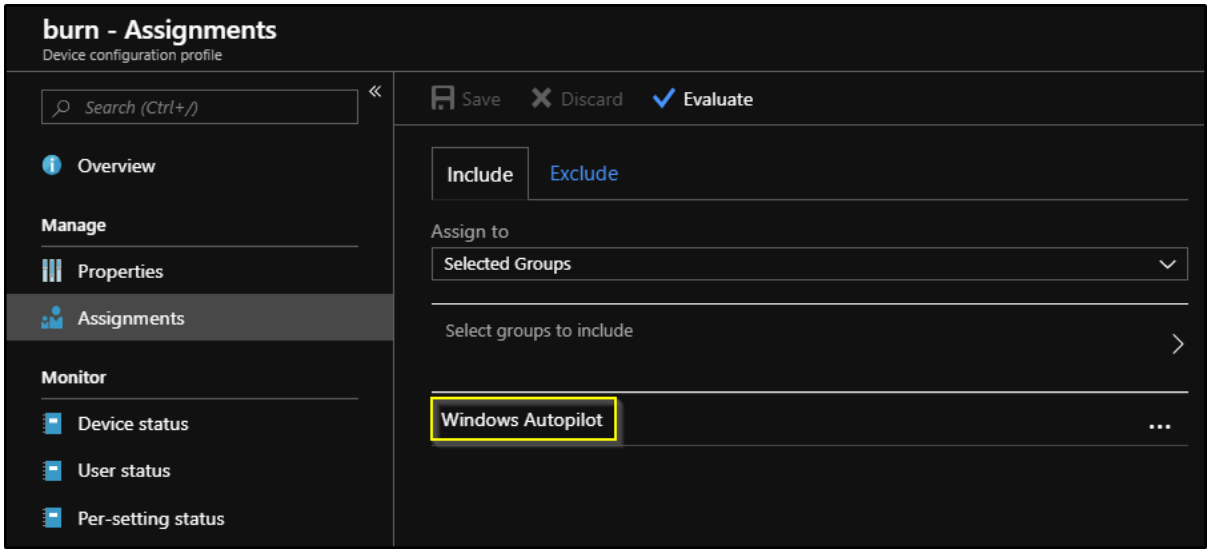
Assign Configuration Policy to Group

Administrasjonsansvarlig kan ved bruk av denne funksjonen tildele en Configuration Policy til en gruppe. Skriver inn navn på Configuration Policy og navn på gruppen, gruppen har nå blitt tildelt policy-en.



Figur 455: Assign Configuration Policy to Group

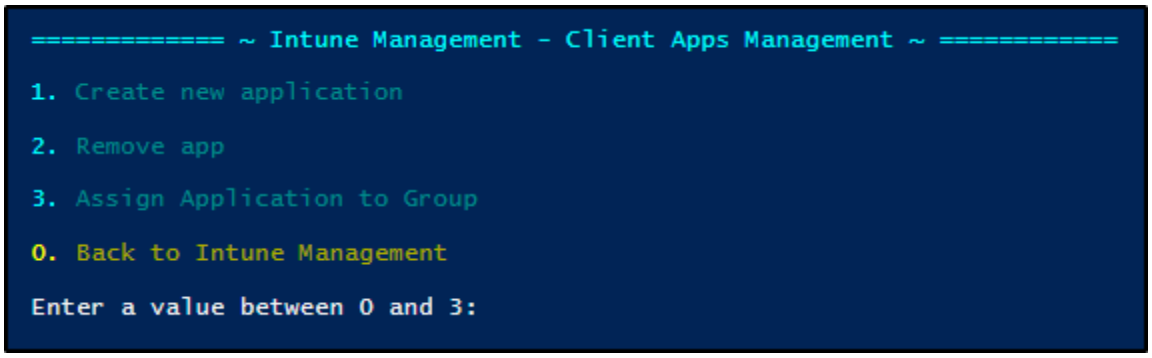
Nedenfor har vi navigert oss til ***Microsoft Intune – Device Configuration – Burn – Assignments.*** Her ser vi at gruppen «Windows Autopilot» er lagt til under Assignments.



Figur 456: Assign Configuration Policy to Group

Client Apps Management

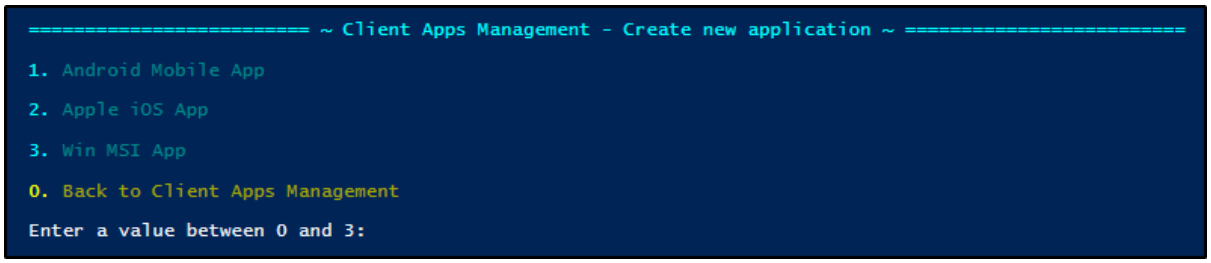
Under Client Apps Management, har vi lagt til funksjoner som brukes til å ta hånd om diverse oppgaver når det gjelder utrulling av applikasjoner med Intune.



Figur 457: Client Apps Management

Create new application

Under Client Apps Management, har vi lagt til funksjoner for oppretting av applikasjoner.



Figur 458: Create new application

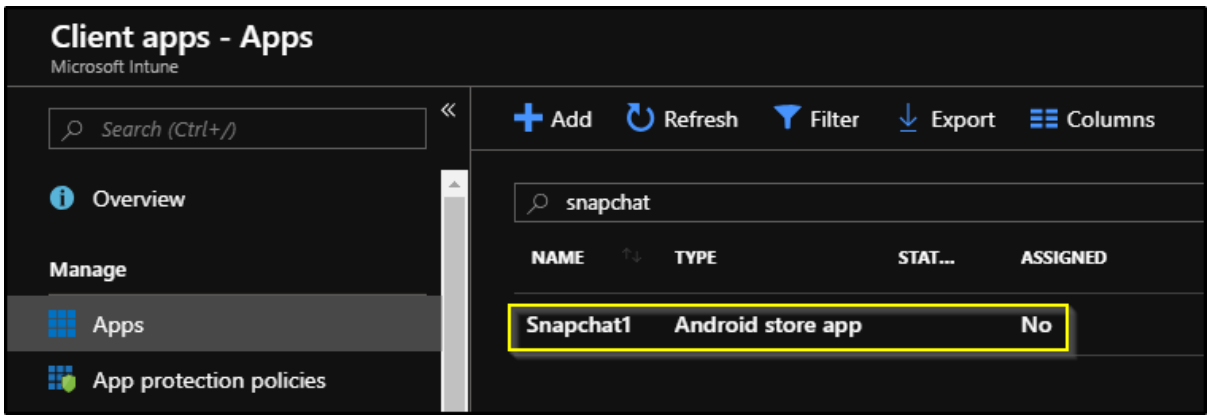
Android Mobile App

Administrasjonsansvarlig kan ved bruk av denne funksjonen opprette en Android applikasjon. Man velger et navn, beskrivelse, applikasjonsutgiver, app store URL og til slutt velger man om applikasjonen skal være tilgjengelig i applikasjonskatalogen.

```
========= Create new Android Application =========

Eksempel:
Displayname: <Andorid_App_001>
Description: <Andorid app>
Publisher: <Squaresoft>
App Sotre URL <www.google.play.store.com/awdadrgdg>
Add Application to Application catalog? <yes> or <no> <yes>

================================================

Displayname: Snapchat1
Description: Social media camera application
Publisher: Snapchat
App Store URL: https://play.google.com/store/apps/details?id=com.snapchat.android
Add Application to Application catalog? <yes> or <no>: yes

Applikasjonen med navnet: Snapchat1, har blitt opprettet!
```

Figur 459: Android Mobile App

Nedenfor ser vi at applikasjonen har blitt opprettet.



Figur 460: Android Mobile App

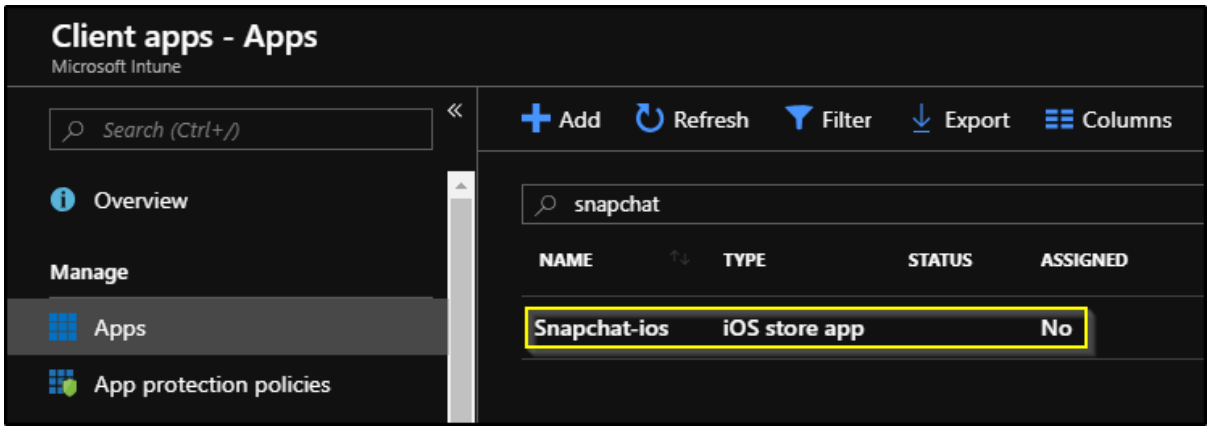
Apple iOS App

Administrasjonsansvarlig kan ved bruk av denne funksjonen opprette en iOS applikasjon. Man velger et navn, beskrivelse, applikasjonsutgiver, app store URL og til slutt velger man om applikasjonen skal være tilgjengelig i applikasjonskatalogen.

```
========= Create new Apple iOS Application =========

Example:
Displayname: <Apple_App_001>
Description: <Apple app>
Publisher: <Squaresoft>
App Store URL <https://itunes.apple.com/us/app/snapchat/id447188370?mt=8>
Add Application to Application catalog? <yes> or <no> <yes>

================================================

Displayname: Snapchat-ios
Description: snapchat
Publisher: snapchat apple
App Store URL: https://itunes.apple.com/us/app/snapchat/id447188370?mt=8
Add Application to Application catalog? <yes> or <no>: yes

Applikasjonen med navnet: Snapchat-ios, har blitt opprettet!
```

Figur 461: Apple iOS App

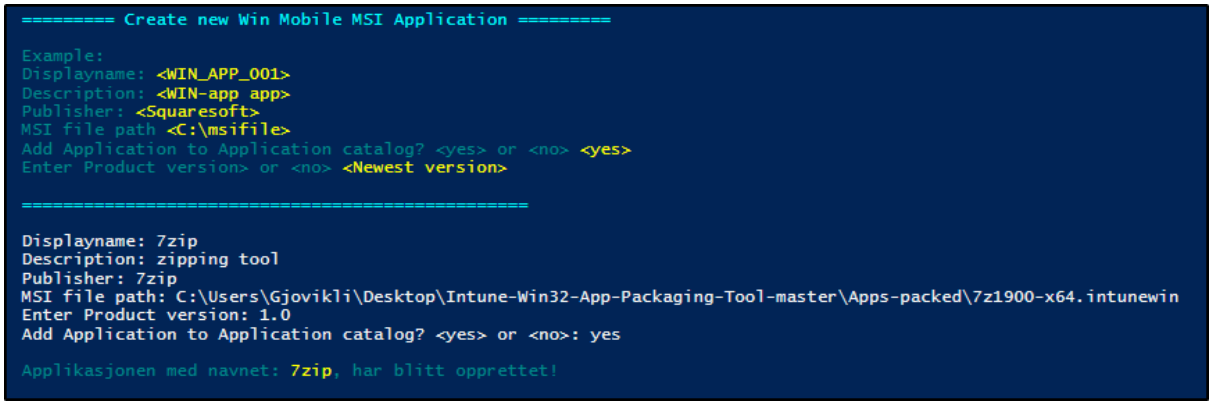
Nedenfor ser vi at applikasjonen har blitt opprettet.



Figur 462: Apple iOS App

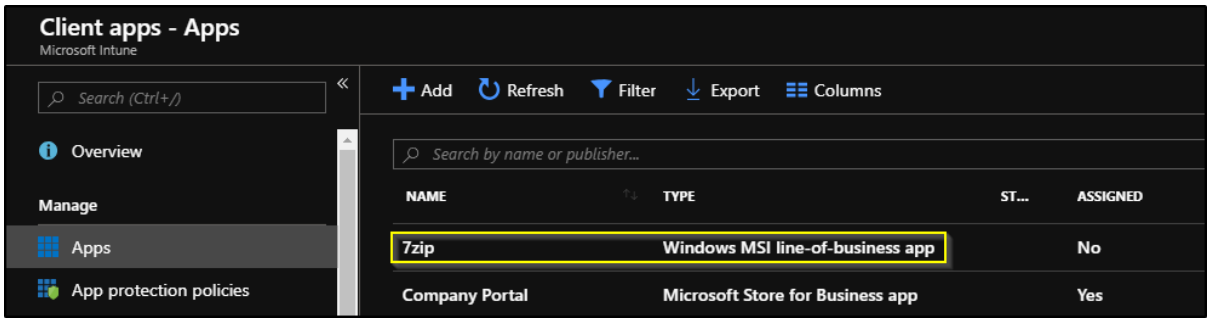
Win32 App

Administrasjonsansvarlig kan ved bruk av denne funksjonen opprette en Windows Mobile MSI applikasjon. Man velger et navn, beskrivelse, applikasjonsutgiver, MSI-sti, produkt versjon og til slutt velger man om applikasjonen skal være tilgjengelig i applikasjonskatalogen.



Figur 463: Win32 App

Nedenfor ser vi at applikasjonen har blitt opprettet.

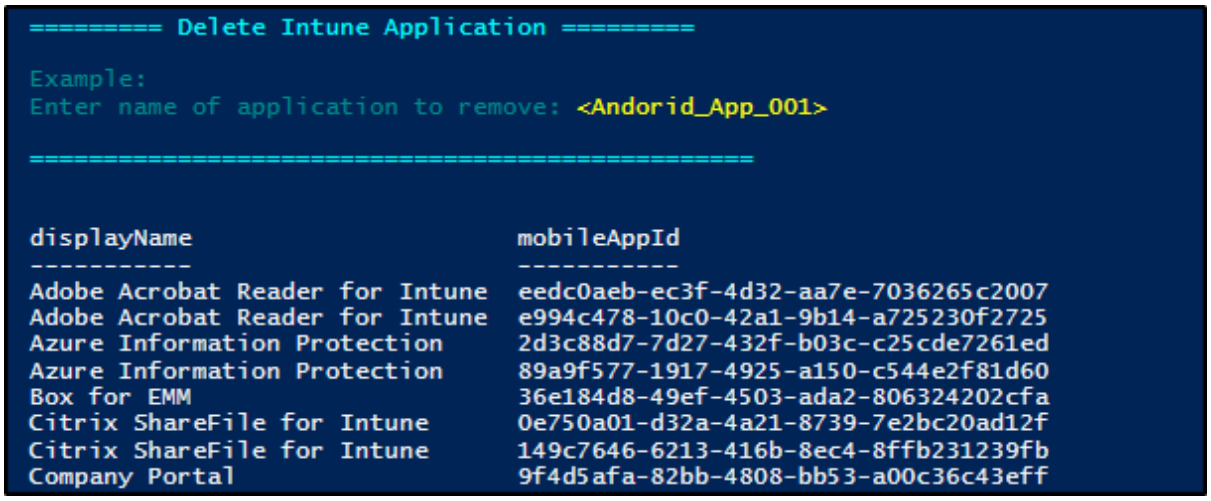


Figur 464: Win32 App

Remove Application

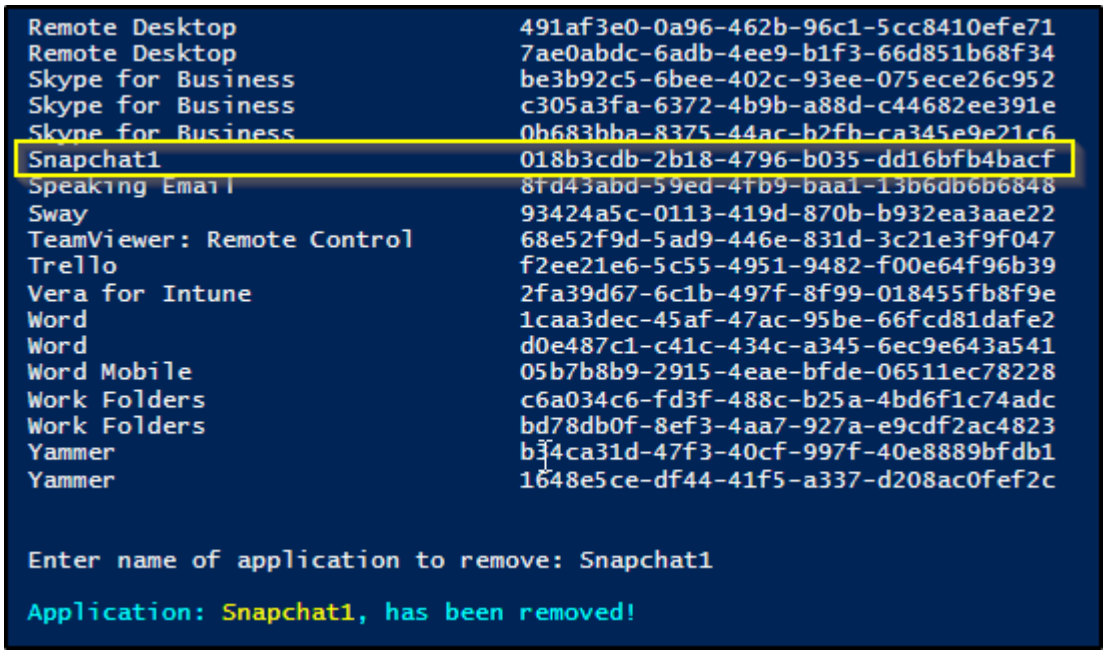
Administrasjonsansvarlig kan ved bruk av denne funksjonen slette en Intune-applikasjon.

Man velger navn på applikasjonen man ønsker å slette.



Figur 465: Remove Application

Applikasjonen blir slettet.



Figur 466: Remove Application

Assign Application to Group

Administrasjonsansvarlig kan ved bruk av denne funksjonen tildele en applikasjon til en gruppe. Man velger applikasjonen og gruppen.

```
========= Client Apps Management - Assign App to Group =========

Example:
Enter name of mobile app: <Apple_App_001>
Enter name of group: <gruppe_001>

================================================


displayName
-----------
7zip
Adobe Acrobat Reader for Intune
Adobe Acrobat Reader for Intune
Azure Information Protection
Azure Information Protection
Box for EMM
Citrix ShareFile for Intune
```

Figur 467: Assign Application to Group

Applikasjonen blir tildelt til gruppen.

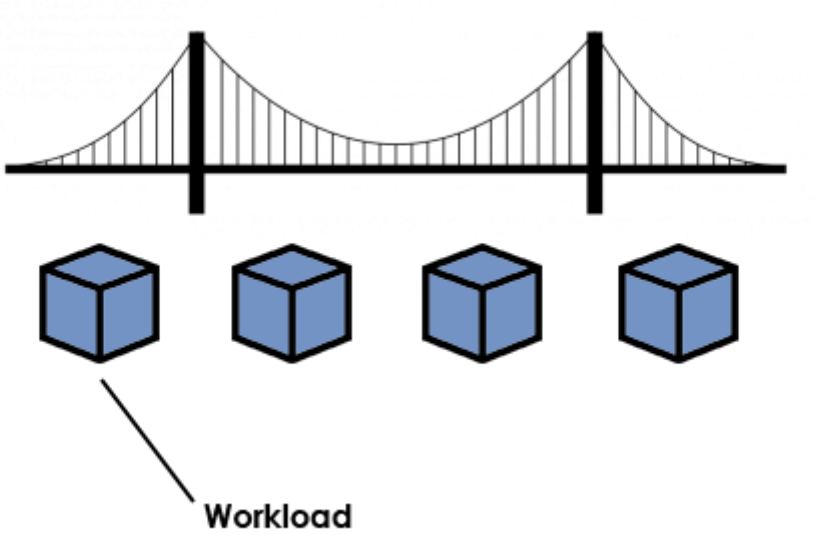
```
Enter name of mobile app: instagram

displayName
-----------
App Deployment User Group
IT Department
Co-managed devices
computerGroup
Intune devices
Android Devices
AutoPilot Preview remote
gruppe2
Windows Autopilot
SCCM User Group


Enter name of group: windows autopilot

App with name: instagram, has been assigned to group: windows autopilot.
```

Figur 468: Assign Application to Group

Vedlegg

1. “WindowsAutopilot_automatisering” – PowerShell script for Automatisering av Windows Autopilot.
2. “Intune_Management” – PowerShell script for Administrasjon av Intune med PowerShell
3. “Konvertingsscript” – Powershell script for konvertering av CSV-fil fra SCCM til importering i Intune.

«Migrering til Azure»



Sluttrapport

Bendik Gjøvikli og Dat-Danny Pham

Trondheim, 20.05.2019

Forord

Denne bacheloroppgaven er skrevet i samarbeid med Innofactor i Trondheim, hvor vi ser på migrering av on-premise systemer til Azure. Prosjektgruppen består av to studenter ved Insititutt for datateknologi og informatikk, NTNU. Oppgaven er relatert til studieprogrammet Informatikk, drift av datasystemer. Hensikten med prosjektet er å tilegne oss kunnskap om nyskapende teknologi innenfor Microsofts skyløsninger. Samtidig vil vi bli bedre kjent med rutinene rundt forskningsarbeid og det å samarbeide i et prosjekt. Gjennom prosjektet har vi blitt kjent med funksjoner i Azure, hvor vi spesielt har fokusert på å koble sammen gamle systemer med nye, som legger til rette for en videre migreringsprosess.

Å skrive bacheloroppgaven har vært veldig spennende og læringsrikt. Det var spesielt spennende da oppgaven tar for seg et emnet som er vi er veldig interessert i, samtidig som oppgaven er veldig relevant i arbeidslivet den dag i dag. Dette ga oss mye motivasjon til å gi ekstra innsats og utforske flere muligheter enn det vi hadde planlagt. Gjennom et ivrig arbeid har vi lært veldig mye og oppnådd god kompetanse innenfor fagfeltet.

Vi ønsker å takke våre veiledere Lars Kristian Granlund, fra Innofactor, og Stein Meisingseth, fra NTNU, for teknisk og faglig bistand, i tillegg til å vise stort engasjement ovenfor prosjektet. De positive tilbakemeldingene og støtten vi har fått, har gitt oss motivasjon og innspill til å lede oss på rett spor, som har resultert i et bedre sluttprodukt.

Innholdsfortegnelse

Oppgavebeskrivelse

Bacheloroppgaven omhandler flere oppgaver, hvor hovedfokuset ligger på migrering til Azure, hvor vi tar i bruk blant annet Co-Management. I og med at migrering er hovedfokuset, er vi først og fremst nødt til å ha noe å migrere fra. Dette betyr at oppsett av lokal Active Directory og System Center Configuration Manager, må være på plass først. Deretter vil vi utforske mulighetene for migrering, samt bli kjent med nye måter å administrere enheter og brukere fra Azure, ved bruk av Azure Active Directory og forskjellige funksjoner i Microsoft Intune. Oppgaven baseres på en case med en fiktiv bedrift, hvor migreringsprosessen skal gjennomføres og ikke i en reell bedrift.

Problemstillingen som skal løses går som følgende:

«På hvilken måte kan kombinasjonen SCCM og Intune konkurrere mot en ren on-premise/skybasert løsning, når det gjelder å løse drifts-oppgaver innen deployment med tanke på tilgjengelighet, kompatibilitet og sikkerhet»

Arbeidets art vil være oppsett, konfigurasjon og drifting av et Co-Managed system, samt forskning på nye måter og administrere et slikt system på.

Oppgaven er utarbeidet i samarbeid med:

- Veileder, Lars Kristian Granlund, Team Lead – Mobility and User Experience ved Innofactor i Trondheim.
- Veileder, Stein Meisingseth, Universitetslektor ved Institutt for datateknologi og informatikk, NTNU.

Metoder og standarder

Vi har benyttet oss av de metodene og standardene som er satt i forstudierapporten. Vi har ikke støttet på noen svakheter med disse og føler at bruken av disse har gått som ønsket.

Bruk av litteratur og Internett

Ved bruk av litteratur og Internett, lister vi opp kilder i referanselister. Mye av arbeidet har foregått ved prøving og feiling og løst ved å teste nye ideer. Ved større problemer, eller problemer som vi ikke har klart og løst på egen hånd, har vi spurt om råd hos veiledere og tatt i bruk forum på nettet. https://social.technet.microsoft.com, er et av de forumene vi selv har spurt spørsmål, samt funnet svar på.

Oversikt over maskinvare

- Vårt on-premise miljø (Domene kontroller, Configuration Manager og Windows 10 maskiner), ligger på en virtuell maskin i Azure.
    - Standard E4s v3 (4 vcpus, 32 GB memory)
    - Standard SSD 500GiB
    - Standard SSD 1023GiB
- For testing av Android klienter, har vi tatt i bruk Bluestacks for virtualisering, samt tatt i bruk en fysisk Android enhet.
- Vi har også tatt i bruk en egen tenant hvor vårt Azure miljø ligger.

Grunnen til at vi har to SDD-disker er fordi vi fant ut at vi trengte mere plass til oppbevaring av Windows 10 klient-maskiner for testing. Det ble derfor lagt til en ekstra disk i etterkant.

Standardprogrammer som er brukt

For dokumentasjon og andre prosjektrelaterte oppgaver, har vi tatt i bruk standardprogrammene:

- Microsoft Office Word – For dokumentasjon av rapporter, ukeplaner, møteinnkallinger, diverse andre dokumenter.
- Microsoft Office Excel – For timeføring.
- Microsoft Office Outlook – For å holde kontakt med andre i prosjektgruppa
- Microsoft Project – For planlegging og tidsestimering av bachelorprosjektet.
- Microsoft Visio – For å lage diagrammer.
- Draw.io – For å lage diagrammer.
- Skype for Business – For å holde online-møter.
- Powershell ISE – For å opprette script.
- Sharepoint – For samhandling og deling av dokumenter.

Fordeling av arbeid

Vi har holdt oss til en veldig jevn arbeidsfordeling. Prosjektmedlemmene har tatt på seg arbeidsoppgaver hvor man føler seg både sterk og mindre sterk, slik at vi oppnår et godt resultat samtidig som vi har mulighet til å forbedre oss på mange områder. På enkelte oppgaver har vi jobbet sammen for å sikre at arbeidet utføres riktig, da det er lettere å kvalitetssikre og gjøre ting rett første gangen da flere er med og overser oppgaven. På andre oppgaver har vi jobbet selvstendig, da disse oppgavene passer best for én person kontra at flere jobber på disse oppgavene samtidig. Vi har i etterkant og underveis i arbeidet med selvstendige oppgaver vært delaktige i de andre prosjektmedlemmenes oppgaver for å kunne tilegne oss kunnskap på samtlige områder.

Oversikt over dokumentasjon

Rapporter:

- Forstudierapport
- Designrapport
- Driftsrapport
- Sluttrapport

Vedlegg:

- Powershell script – «AAD- og Intune-Management»
- Powershell script – «Automatisering av Windows Autopilot Innrulling»
- Timeliste
- Framdriftsplan
- Presentasjon
- Risikoanalyse

Gjennomføring av prosjektet

Ved prosjektstart, satte vi oss resultatmål om å migrere deler av Alarmnetts systemer over til et tilsvarende system i skyen. Migreringsprosessen skulle ikke gå ut over det daglige arbeidet hos bedriften. Vi hadde også satt om mer spesifikke mål om hva migreringsprosessen skulle innebære.

Kort sagt satte vi oss mål om å migrere over brukere, samt sette opp mulighet for å drifte gamle enheter (co-managed maskiner) ved bruk av Intune. Dette innebar også at vi måtte lære oss å ta i bruk de forskjellige funksjonene som Intune har å tilby. Til slutt satte vi oss et mål om å kunne utføre mest mulig av dette ved bruk av Powershell, gjennom et script som vi har laget.

I og med at dette var en case og ikke en reel prosess, måtte vi sette opp de systemene som vi så for oss allerede eksisterte inne i bedriften. Dette innebar å sette opp en domenekontroller (lokal Active Directory Domain Controller) og System Center Configuration Manager. Vi kom godt i gang med denne prosessen, men møtte fort på et problem. Vi fikk kjennskap til at det var mulig å ta i bruk en Task Sequence som satt opp et test-miljø med det vi trengte i denne sammenhengen. Det som skjedde var at de systemene som skulle settes opp ikke fungerte etter at installasjon og konfigurasjon. For å redusere tap av tid, valgte vi derfor å sette opp disse systemene manuelt på egen hånd. Dette gjorde at vi fikk satt opp de systemene vi ønsket på en god måte og de fungerte. Her kunne vi eventuelt gått for å gjøre det på den måten vi endte opp med i og med at det var den metoden vi kjente til fra før av. Uansett var det fint å prøve en annen metode å gjøre det på, som eventuelt kan være fin å kjenne til i en senere sammenheng. Vi oppdaget derimot at mange av problemene vi støtte på relatert til oppsett av On-premise serveren, var besvart i forskjellige forum på nettet. Generelt viste det seg at mange av feilmeldingene vi støtte på, var godt forklart av andre fagfolk og flere gode og detaljerte svar hadde blitt formulert. Dette kan være fordi systemet har vært ute lenge.

Når de systemene som bedriften allerede hadde på forhånd var satt opp, hadde vi som mål å sette opp Azure AD Connect, for å oppnå et samspill mellom lokal Active Directory og Azure Active Directory. Prosessen gikk som vi ønsket og vi oppnådde kontakten mellom det gamle og nye systemet.

Videre satte vi som mål å konfigurere og få Co-Management til å fungere. Dette var en relativt krevende prosess, da det krevde et samspill mellom flere tjenester for å fungere

optimalt. Konfigurasjonen av Co-Management gikk bra. Videre var det å rulle inn eksisterende maskiner som tidligere var administrert med System Center Configuration Manager. Å gjøre dette manuelt på hver enkelt maskin var en enkelt prosess som gikk feilfritt, men å få til dette automatisk gjorde at vi fikk litt problemer. Ved å prøve ut forskjellige løsninger kom vi til slutt frem til en løsning som vi var tilfreds med.

Trinnvis migrering av enkelte funksjoner fra SCCM til Intune for våre co-managed enheter var også et mål som vi hadde satt oss til å løse. Denne prosessen innebar at vi hadde kjennskap til funksjoner i Intune. Vi valgte derfor å bli bedre kjent med disse funksjonene før vi gikk løs på den trinnvise migreringen av funksjonene. Dette gikk veldig bra, da funksjonene som vi testet i Intune fungerte godt på enheter som var administrert kun av Intune.

Da vi skulle gå tilbake å se på hvordan vi trinnvis skulle migrere over funksjoner fra SCCM til Intune møtte vi derimot på et par problemer. Vi løste problemene til slutt, men noe som kunne reddet oss tidligere, eller gjort at vi hadde unngått dette problemet, var om vi hadde konfigurert SCCM riktig første gang vi satte den opp, da det var her problemet lå.

Vi satte også opp som mål å melde inn mobile enheter som Android-mobiler til Intune, da SCCM ikke greier å håndtere enhetene utenfor lokalet. Dette gikk for så vidt greit, men vi så at det var litt vanskelig å legge til gode funksjoner. Om man rullet inn enheten som helhet kunne man lettere installere funksjoner og applikasjoner, men om man gjorde det hvor man satte av et avgrenset område i enheten fikk man ikke mulighet til å installere de samme funksjonene og applikasjonene. Dette kan også ha med at det er en betafunksjon og at den var tiltenkt kiosker.

Videre hadde vi som mål om å kunne drifte Intune ved bruk av et Powershell script. Store deler av scriptet gikk veldig fint å lage, men vi støttet på noen problemer. Problemene fikk vi løst ved å spørre om hjelp på forskjellige forum. Dette viste seg å være til stor hjelp, da temaet var såpass nytt og mange var aktive på forumene hvor vi stilte spørsmål. Vi hadde definitivt brukt denne formen for problemløsning tidligere i prosjektet, hadde vi visst hvor effektivt det var.

Det skal sies at tidlig i prosessen, hvor vi satte oss disse resultatmålene, hadde vi ikke så god kjennskap til hva vi egentlig hadde mulighet til å oppnå med de systemene vi jobbet på. Dette gjorde at vi under selve utførelsen av arbeidet, fant flere funksjoner som vi ønsket å teste da det føltes veldig riktig å ta de med. Dette gjorde at vi fikk flere mål, som var med å bygge det

vi mener ble en mer solid prosjektoppgave. Dette innebar mål om å f.eks. sette opp og teste Remote Assistanse, opprette et skjema i SharePoint som ansatte i bedriften kunne ta i bruk og koble det opp imot deres brukere i Azure Active Directory. Vi gikk også inn for å gjøre mer enn vi egentlig hadde planlagt på andre mål som vi hadde satt, som virket interessant å ha med. Dette innbar f.eks. flere metoder innrulling av enheter til Intune, flere måter å rulle inn maskiner ved hjelp av Windows Autopilot, flytting av flere funksjoner fra SCCM til Intune, enn det vi først hadde planlagt. Vi fant også ut at det var mulig å teste ut «preview»-funksjoner, altså funksjoner som fortsatt var i beta-stadiet, dette gav oss mange av de nye funksjonene vi endte opp med å teste.

Måloppfyllelse i forhold til framdriftsplanen

I starten av bachelorprosjektoppgaven, var det ganske vanskelig å skulle estimere tiden de forskjellige fasene i prosjektet kom til å ta. Til å begynne med gjorde vi oss noen tanker og satte en grov tidsestimering for de forskjellige fasene. Vi lagde deretter et førsteutkast på både forstudierapport og designrapport. Dette gjorde at vi raskt kunne komme i gang med driftsrapporten og deretter finne ut av hva vi egentlig måtte ha med i både design- og forstudierapport. Når vi senere fikk en bedre følelse av omfanget av oppgaven og de forskjellige delene, gikk vi tilbake til framdriftsplanen og satte mer detaljerte tidsestimeringer. Den planlagte tiden ble ikke endret drastisk, men enkelte steder ble det gjort endringer. Når det kommer til planlagt tid, sett opp imot reell tid brukt, ble det relativt likt. Dette kom av at vi hele tiden prøvde å holde oss innenfor tidsfristene, slik at vi i hvert fall ikke lå bak skjema. Med tanke på at uforutsette ting som kunne skje senere i prosjektet, som sykdom eller annet fravær, mente vi det var lurt å holde oss litt i forkant til enhver tid.

Nedenfor vises en grov liste over tid planlagt og brukt tid på hoveddelene i prosjektet. For en mer detaljert oversikt henvises til «GANT-Diagram» som er lagt til som vedlegg.

Hva	Planlagt tid	Reell tid	Kommentar
Forstudierapport	16 dager	11 dager	Vi greide å jobbe mer effektivt enn det vi hadde sett for oss, som var bra siden vi visste vi trengte mer tid andre plasser.
Designrapport	11 dager	11 dager	Her klarte vi å holde oss innenfor tidsfristen som vi satte til å begynne med.
Driftsrapport	53 dager	63 dager	Driftsrapporten var definitivt den rapporten vi visste komme til å ta lengre tid. For å få til alt vi ønsket valgte vi å bruke mer tid på enn først planlagt.
Sluttrapport	4 dager	4 dager	Her klarte vi å holde oss innenfor tidsfristen som vi satte til å begynne med.
Samarbeidsrapport	1 dager	1 dager	Relativt lite arbeid med denne.
Annet	5 dager	5 dager	Underveis i prosessen gjorde vi endringer som medførte at vi måtte gå tilbake og skrive om enkelte deler. Rettskriving og presentasjon går under dette feltet også.
Total tid	**90**	**95**	

Tabell 1: Tidsestimering

Mål som vi har satt oss tidlig i prosjektet var mål som gikk på effekten av de systemene og endringene vi har valgt å gjøre. Til å begynne med ønsket vi å legge til rette for at Alarmnett AS, på et senere tidspunkt kan fortsette migreringssprossen og migrere over til en ren skyløsning. Dette har vi nå oppnådd i og med at Alarmnett AS, nå har tilgang til Intune som er den skyløsningen som er godt i bruk og som Microsoft satser på fremover. Videre kan Alarmnett AS gjøre om sine co-managed enheter til rene Intune administrerte enheter, når tiden føles rett. Ved å la Alarmnett migrere stegvis i stedet for å direkte migrere over til en ren skyløsning med en gang, gjør vi det lettere for bedriften å fortsette med sine vanlige rutiner og heller tilpasse opplæring til når det passer for de ansatte. På den måten vil Alarmnett få med så mange de kan på samme side når de skal benytte seg av tjenestene i skyen, for en smidig overgang. Alarmnett også mulighet til å tilpasse gamle tjenester, applikasjoner og operativsystemer til det nye systemet, slik at de selv kan velge å fortsette med det de har eller oppgradere ved en senere anledning. Til sammenligning må man oppgradere sine tjenester og applikasjoner om man skal direkte flyttes over til skyen, og man kan risikere å miste tjenester og applikasjoner som enda ikke er støttet.

Videre ønsket vi å effektivisere arbeidet med 20%. Det skal sies at det ikke er så enkelt å skulle regne ut om dette prosentmålet er nådd, men ved å redusere tid i forhold til å kunne administrere enheter uavhengig av hvor i verden en ansatt befinner seg, så lenge man har internettilgang, er med og utgjør en stor del av målet med å effektivisere arbeidet med 20%. Tidligere ble dokumenter og filer delt gjennom nettverksmapper, som man bare hadde tilgang til når man var koblet til det lokale nettverket til bedriften. Det var heller ikke noen gode metoder for å dele informasjon eller bedriftsnyheter. Ved å ta i bruk den hybride løsningen kan de ansatte fremdeles benytte seg av den tjenesten de er vant med samtidig som administrasjonen nå får flere kanaler til å nå ut til de forskjellige avdelinger angående nyheter, i tillegg til at de ansatte har bedre muligheter til samhandling og deling av informasjon. Man kan for eksempel opprette et chat-rom i Microsoft Teams for rask respons fra medarbeidere om en uvanlig situasjon skulle oppstå. Det fine med dette er at man nå kan kontaktes fra hvor som helst så lenge man har tilgang til internett, noe som også vil forbedre arbeidsflyten generelt. Vi viste også et eksempel på hva vi kunne bruke SharePoint til og viste i eksempelet hvordan man kan opprette og forme skjema etter sine behov. Dette vil lagres i SharePoint for lettere oppfølgning. Videre hadde vi satt oss et krav, at brukere ikke trenger å logge seg på mer enn en gang per dag. Med dette tenkte vi at brukerne bare trengte å logge på med kontoen sin en gang og hadde dermed tilgang til sine tjenester uten å måtte skrive inn brukernavn

passord for hver tjeneste de brukte. Det som er satt opp er at tjenestene, som Office365, vil huske brukeren og lagre påloggingsinformasjon. På den måten trenger de bare trykke på at de vil logge inn med den brukeren for å komme seg inn til tjenesten. Dette vil redusere tiden brukerne bruker for å logge på tjenestene sine ved å eliminere at de trenger å huske eller skrive inn passord. Utenom dette har de tilgang til Company Portal, bare ved å logge seg inn på maskinen med sin bruker. Her er det også mulig å legge lenker til SharePoint og andre applikasjoner brukeren bruker så det eliminerer flere feil brukere kan gjøre.

Vi ønsket videre å minske nedetiden til serveren til mindre enn 1 time hvert år. I og med at Alarmnett AS, fortsatt beholder sin server og velger å drifte enkelte av sine eksisterende enheter som co-managed enheter, sitter de fortsatt på en lokal domene kontroller og en SCCM server. Dette gjør at nedetiden på disse systemene ikke nødvendigvis minker, men hvis vi tenker på enheter som driftes kun gjennom Intune og i skyen, kan vi være sikre på at nedetiden reduseres med tanke på at nedetiden til tjenestene Microsoft drifter er mye lavere enn Alarmnetts egne tjenester.

Ved bruk av samhandlingsverktøyene Alarmnett sine ansatte har tilgang til gjennom Office365, vil vi nå målet med økt produktivitet og samarbeid mellom de ansatte. Montørene kan registrere sitt arbeid og de på kontoret vil øyeblikkelig få opp det som er dokumentert.

Målet for tilgjengelighet, med tanke på å gjøre hverdagen for de ansatte som jobber utenfor bedriftens lokaler enklere, oppnår vi gjennom bruk av Azure Active Directory og Intune. Vi kan nå legge til rette for at de ansatte har alt de trenger uten å måtte komme innom bedriftens lokaler og koble til bedriftens private nettverk. Skulle en ansatt trenge tilgang til applikasjoner, hjelp til å restarte maskinen sin, slette bedriftshemmeligheter på mobilen dersom den kommer bort o.l. kan dette nå gjøres av en administrasjonsansvarlig uten å ha fysisk tilgang til enheten.

I forhold til problemer vi har møtt under prosjektet, har vi tatt i bruk risikoanalysen som vi skrev tidlig i prosjektet. Enkelte hendelser som vi har beskrevet i risikoanalysen har inntruffet og blitt tatt hånd om på uttenkt metode, eller at konsekvens har blitt redusert i og med at vi har tatt forhåndsregler og vært obs på at enkelte hendelser kan inntreffe. Risikoanalysen har derfor vært til stor hjelp, i både reduksjon av konsekvens, samt redusert sannsynlighet for at hendelser har inntruffet.

Når det gjelder krav til dokumentasjon, har vi oppfylt de kravene som stilles. Vi har utarbeidet en forstudierapport, designrapport, driftsrapport, sluttrapport og en samarbeidsrapport, samt

vedlegg som går under disse rapportene. Prosjektgruppen har og vil godkjenne samtlige rapporter før spesifisert dato i forstudierapporten.

Under krav til kvalitetsgjennomganger, har vi satt krav om å utføre pilottester, for å sikre god standard og at samtlige brukerkrav er innfridd. Dette er gjennomført av oss og ikke av reelle ansatte i bedriften i og med at det er snakk om en fiktiv bedrift. Vi har derfor under testing av systemer utført disse på enkelte systemer før vi har gjort endringer på samtlige systemer.

Ved gjennomførelse av prosjektet med tanke på krav til standarder og metoder, har vi oppfylt de kravene som vi selv har satt oss. Grovt beskrevet har vi fulgt kravene for bruk av standardprogrammer til dokumentasjon og samhandling. Vi har også tatt i bruk de teknologiene som er beskrevet i forstudierapporten, da med tanke på hvordan vi ønsket å sette opp vårt lokale miljø, samt Azure miljøet. Vi har her tatt i bruk Hyper-V og egen Azure tenant, som planlagt. Når det gjelder krav til å endre tidligere dokumenter, har vi fulgt fremgangsmåten for å håndtere endring, slik den er beskrevet i forstudierapporten under endringshåndtering.

Konklusjon

Gjennom prosjektet har vi gjort oss kjent med mulighetene i det eksisterende IT-systemet til Alarmnett, samt mulighetene ved å ta i bruk en skybasert løsning, men også kombinasjonen av disse to.

I en on-premise løsning, har man fordelen med kompatibilitet, med tanke på å kunne drifte eldre enheter. Det er også en godt utforsket løsning med et bredt utvalg av funksjoner og programutvidelser. Ulempene derimot er at en on-premise løsning har redusert tilgjengelighet/mobilitet med tanke på å kunne drifte enheter utenfor bedriftens private nettverk, samt tilgang til ressurser. Reduksjon av samhandling er også noe man støtter på, ved bruk av en ren on-premise løsning.

Ved direkte migrering til en ren skyløsning, vil man kunne øke tilgjengelighet/mobilitet, ved at man har tilgang til å kunne drifte enheter utenfor bedriftens private nettverk og tilgang til bedriftens ressurser. Man vil også ha tilgang til bedre programmer for samhandling, med tanke på Office365. Når det gjelder OS-utrulling, vil Windows Autopilot forenkle arbeidet både for drift og de ansatte. Intune virker også mer oversiktlig og brukervennlig, som gjør jobben med drift enklere og mer effektiv. Ulempene her er kompatibilitet mot eldre enheter, da Intune kun støtter Windows 10 enheter eller nyere. Ved direkte migrering vil man også få mindre kontroll, samt en del nedetid, da gamle systemer må oppgraderes, som vil gjøre at overgangen vil oppleves som veldig brå. Mangel på dokumentasjon og bruk av kun ny teknologi, kan gjøre det vanskelig å finne løsninger på eventuelle problemer.

Ved å ta i bruk en hybrid løsning, vil vi kunne ta med oss fordelene fra begge løsningene, samtidig som ulempene som kommer med de to systemene vil løses av fordelene til hvert system. Vi kan derfor konkludere med at en kombinasjon av SCCM og Intune, vil være et bedre alternativ for å løse drifts-oppgaver innen deployment med tanke på tilgjengelighet, kompatibilitet og sikkerhet.

Videre arbeid

For å kunne drive daglig drift av tjenesten vi har satt opp kan det være smart å innføre en rekke ting. Vi anbefaler først å ta backup av serverne i tilfelle noe skulle skje.

Det kan være en god ide å sette opp monitorering og rapportering i Intune. Vårt oppsett har ikke tatt for seg disse og en viktig del av en drifters hverdag omhandler å passe på at utstyr og tjenester fungerer som dem skal.

Det må settes opp mer sikkerhet i Azure. Vi anbefaler å se på ting som Security Center og andre tjenester som håndterer sikkerhet på maskinene som blir driftet av Intune og Azure AD. Det er mulighet til å begrense ting som geografisk innlogging og innmelding fra enheter utenfor de geografiske områdene som er satt. Da kan vi for eksempel blokkere innmeldinger fra områder med mye hackerangrep.

Intune for Android bør også utvikles videre til å kunne inkludere flere applikasjoner. Det bør også settes opp en direkte tilkobling til SharePoint hvor malene for skjema og eventuelle skjema ligger slik at man slipper å lage skjemaene selv. Det bør også settes opp direkte tilkoblinger til eventuelle andre applikasjoner de ansatte trenger på deres mobile-enheter. Det må også settes opp restriksjoner på hva de mobile-enhetene får lov til å gjøre og slik at bedriftshemmeligheter ikke kommer på avveie.

Det bør også legges til flere applikasjoner til Firmaportal (Company Portal), da vi ikke har lagt til så mange. Man kan også tilpasse applikasjoner og profiler slik at dem passer bedre til bedriften. Det vil si ting som å endre tenant-navnet til Alarmnett, eller laste opp applikasjoner alarmnett har laget.

Powershell scriptene bør også videreutvikles for å ta hensyn til flere tilfeller. For øyeblikket fungerer innmeldingsscriptet bare på maskiner som bruker Windows 10 og som ikke er av generasjon 1, altså eldre maskiner. Den bør dermed utvikles til å ta hensyn til om det kjøres utdatert OS og eventuelt oppgradere dette om det trengs.

Bendik Gjøvikli og Dat-Danny Pham

Migrering til Azure
Migrering til Azure med hovedfokus på Co-Management

NTNU
Kunnskap for en bedre verden