Bacheloroppgave

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

Kristoffer Selbekk Hille

# Klientadministrasjon med Intune og Autopilot

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Stein Meisingseth
Mai 2019

NTNU
Kunnskap for en bedre verden

Kristoffer Selbekk Hille

# Klientadministrasjon med Intune og Autopilot

Bacheloroppgave i Informatikk, drift av datasystemer
Veileder: Stein Meisingseth
Mai 2019

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

Kristoffer Selbekk Hille

# Klientadministrasjon med Microsoft Intune og Autopilot
# Forstudierapport

**Versjon 1.4**

# Revisjonshistorie

| Dato | Versjon | Beskrivelse | Forfatter |
|---|---|---|---|
| 23.01.2019 | 1.0 | Oppstart | Kristoffer Selbekk Hille |
| 15.02.2019 | 1.1 | Første utkast | Kristoffer Selbekk Hille |
| 06.03.2019 | 1.2 | Kostnadsanalyse | Kristoffer Selbekk Hille |
| 09.05.2019 | 1.3 | Formatering av dok. | Kristoffer Selbekk Hille |
| 16.05.2019 | 1.4 | - | Kristoffer Selbekk Hille |

# Innhold

# 1. Introduksjon

Hensikten med dette dokumentet er å vise fram til hva som må redegjøres for før vi kan starte på prosjektet. Vi vil blant annet forklare våre mål, suksesskriterier, kostnader knyttet til prosjektet og forventninger mot det endelige resultatet.

Samtidig vil vi forklare hvorfor dette prosjektet er blitt startet opp, behov som foreligger hos AquaGen, samt fordeler og mulige ulemper med den skisserte løsningen. Dokumentet inneholder en risiko- og kostnads-analyse som vil redegjøre for hvordan prosjektet berører organisasjonen. Til slutt vil det bli oppsummert hva man har kommet fram til, og om prosjektet bør gjennomføres med forskjellige alternativer.

# 2. Bakgrunn for prosjektet

På lik linje med andre moderne bedrifter, benytter også AquaGen seg av datautstyr til forskjellige arbeidsoppgaver. I dag har bedriften ganske mange maskiner uten en reell oversikt over dem. Ønsket med dette prosjektet er å skissere og demonstrere et system som kan samle IT-driften av dette datautstyret.

Det skisserte systemet vil ta for seg maskiner som brukes i fra alt til produksjon, kontorarbeid og diverse andre støttesystemer i bedriften. For å unngå at produksjon blir stoppet opp av dårlig vedlikeholdt utstyr, er det essensielt å få samlet denne driften i ett system slik at man enkelt kan administrere både maskin- og programvare sentralt. I forbindelse med en ny IT-strategi innad i AquaGen vil det være hensiktsmessig å gjennomføre denne prosessen for å forenkle dette arbeidet for nåværende IT-ansvarlig.

## Beskrivelse av problemer og behov

AquaGen mangler som nevnt i dag en løsning som samler alle disse enhetene inn i et system. Det betyr at oppgaver som involverer oppdatering, administrering og feilsøking av disse maskinene tar svært mye tid. For en bedrift som har avdelinger flere plasser rundt om i både inn- og utland, er det svært vanskelig å gjennomføre IT-drift på denne måten.

For å forenkle denne oppgaven har man behov for et system som kan administrere alle disse maskinene på en smart og effektiv måte. Dette systemet bør være enkelt å forholde seg til, og bør kreve minst mulig opplæring for de endelige sluttbrukerne. Det vil være sterkt anbefalt at dette systemet knyttes sammen med de eksisterende brukerkontoene. For superbrukere av dette systemet vil det nok være nødvendig med opplæring for å ha oversikt over all funksjonaliteten et slikt system innebærer. Det er en stor fordel om systemet kan administreres fra skyen (over internett) med mulighet for pålogging hvor som helst i verden.

AquaGen har også programvare som installeres i ulik grad på forskjellige maskiner. For at et slikt system skal få økt nytteverdi er det også ønskelig at man ved nytt oppsett av en maskin kan få installert denne programvaren automatisk. Utrulling av denne programvaren bør kunne skje både på bruker- og maskin-basis. Utrullingen bør helst skje over Internett uten hjelp av interne servere og utstyr.

## Kort om dagens systemer og rutiner

I dagens løsning blir alle datamaskiner satt opp individuelt. Det betyr at de settes opp hver for seg, med lokale brukerkontoer. Programvare installeres også manuelt, og eventuell feilsøking skjer gjennom tredjeparts-programvare for fjernstyring eller fysisk til stede på avdelingene. Et problem som kommer med individuelle maskiner er at passord ofte forblir uendret, noe som fører til dårlig sikkerhet tvers over organisasjonen.

Brukere av disse systemene varierer fra avdeling til avdeling, men det er i all hovedsak snakk om relativt enkel bruk. Oppdatering, konfigurering og oppsett av dette utstyret inngår ikke som en del av arbeidsoppgavene for de ansatte. Altså, per dags dato finnes det ikke noen ansatt med oppgave i å opprettholde drift av datamaskinene og utstyr. I stedet blir disse oppgavene tatt fortløpende av personer som har mulighet, kunnskap og tid til dette.

# 3. Prosjektmål

Det overordnede målet med dette prosjektet er å skissere og demonstrere et system som på en effektiv måte kan administrere maskinene til bedriften. Bedriften har som mål få mer kontroll og oversikt over sitt eget utstyr, og vil forhåpentligvis gjennom dette systemet få oppfylt dette målet.

## Effektmål

- AquaGen ønsker å bruke mindre tid på oppsett av nye maskiner – dette skal skje automatisk
- Ansatte ute i produksjon skal bruke mindre tid på å løse dataproblemer – og dermed få mer tid til andre arbeidsoppgaver
- Datautstyret rundt om i bedriften skal bli enklere å holde oversikt på – enkel administrasjon
- Man ønsker å spare kostnader knyttet til uvettig bruk og stadig utbytting av utstyret – mer kostnadseffektiv drift

## Resultatmål

- Prosjektet skal levere et system som klarer å oppfylle kravene som er satt
- Det endelige systemet skal leveres innen 20. mai 2019
- Enheter skal til enhver tid være oppdatert, så fremt det lar seg gjøre
- Levetiden på maskiner bør kunne standardiseres gjennom jevnlig oppfølging og vedlikehold
- Bedriften skal få økt sikkerhet – eks. tvungen kryptering av maskiner samt krav til sterke passord

## Prosessmål

- AquaGen skal få mer kjennskap i måter å administrere IT-utstyret sitt på
- AquaGen skal bli mer oppdatert på aktuelle sikkerhetsproblemer rundt slike systemer
- Ansattes holdning mot nytt IT-utstyr skal bli bedre
- Organisasjonens forhold til sikkerhet skal bli bedre

## Prosjektets omfang

Innføringen av Microsoft Intune i bedriften skal i all hovedsak gjelde maskiner som kjører **Windows 10**, herunder **bærbare PCer, stasjonære arbeidsstasjoner** og andre maskiner som brukes ute i produksjon. Mobile enheter som smarttelefoner, nettbrett og annet utstyr tas ikke med som en del av dette prosjektet. Grunnen til at disse enhetene ekskluderes er at de har egne utfordringer med rutiner og prosedyrer for innføring i et slikt system. Vi velger derfor å heller bruke tiden på datamaskiner for dette prosjektet.

Systemet bør i en viss grad erstatte manuell oppfølging og vedlikehold av hver enkelt maskin, noe som i dag er en tungvint prosess som tar tid. Hovedfokuset med denne oppgaven er ikke å erstatte den manuelle installasjonen av programvare, men heller redegjøre for måter man kan utføre dette på slik at man kan innføre dette ved en senere anledning.

Oppsummert skal prosjektet bidra til å finne et system som hjelper AquaGen med å administrere sine datamaskiner, mest med tanke på overvåkning av tilgjengelig utstyr og sammenkobling med den eksisterende brukerdatabasen som bedriften allerede innehar.

# 4. Interessenter og rammebetingelser

I denne delen introduserer vi de ulike partene som deltar i prosjektet og de forskjellige suksesskriteriene som berører disse.

## Interessentanalyse

- Oppgavestiller: IT-sjef i AquaGen
  - Suksesskriterier: få mer kontroll over data-utstyr som ansatte i AquaGen disponerer
- Bruker(e) av systemet: alle ansatte i AquaGen
  - Suksesskriterier: få mer tid til å utføre andre arbeidsoppgaver, lettere teknologisk hverdag
- Godkjenner av løsningen: IT-sjef for AquaGen / IT-personell
  - Suksesskriterier: utstyret kan enkelt administreres gjennom en portal, liten terskel for å benytte seg av denne
- Berører: ansatte i AquaGen, IT-sjef for AquaGen
  - Suksesskriterier: løsningen bør innføres på en måte slik at arbeidshverdagen ikke blir vanskeligere for sluttbruker
- Bør vite noe om produktet: IT-sjef og ledelsen ved AquaGen
  - Suksesskriterier: mer effektiv bruk av datautstyret, lengre levetid på utstyret, gjenbruk av utstyr, bedre sikkerhet rundt lagring av filer og tilgang til systemer
- Prosjektforløpet: IT-avdeling, veileder, andre interesserte
  - Suksesskriterier: godt dokumentert arbeid som kan repliseres og iverksettes i bedriften ved prosjektets slutt
- Utfører arbeidet: oppgaveskriver
  - Suksesskriterier: godt gjennomført arbeid, god vurdering fra faglærer, arbeid som faktisk er av betydning av bedriften
- Bidrar/leverer: (Evry), Microsoft, AquaGen
  - Suksesskriterier: oppgaveskriver får nok informasjon fra alle parter til å få skissert og iverksatt løsningen på en god og effektiv måte

| Interessent | Suksesskriterier | Bidrag til prosjektet |
|---|---|---|
| **Eksterne (kunde)** | | |
| - AquaGen | Inntjening på å bruke IT-løsningen | Utstyr og oppgave |
| - IT-sjef/IT-personell | Bedre oversikt over AquaGens IT-utstyr, lettere administrering | Veiledning |
| - Sluttbruker (ansatte) | Arbeidslettelse | Kunnskap om problemområde |
| - Evry/Microsoft | Fungerende system | Teknisk løsning |
| **Interne (leverandør)** | | |
| - Oppgaveskriver | Vellykket produkt og prosjektrapport, fornøyd oppdragsgiver | Ansvar |
| - Veileder | Godt gjennomført prosjekt | Kunnskap, veiledning |

## Rammebetingelser

Her viser vi til de absolutte krav for systemet som må være tilstede for at prosjektet kan gå sin gang.

- Systemet må være ferdig testet og skissert til 20.05.2019.
- Systemet krever tilgang til et testmiljø/maskiner for å demonstrere funksjonaliteten.
- Løsningen må være kompatibel med de maskinene som det skal knyttes til
- Systemet må ikke overstige forventede kostnader for bedriften
- Systemet må gi merverdi for organisasjonen kontra manuell løsning.
- Systemet skal være skybasert og følge *best practice* for den tekniske løsningen fra Microsoft.

# 5. Kritiske suksessfaktorer

Dette er de faktorene som vi ønsker oppfylt for at den endelige løsningen skal bli ansett som vellykket.

## Suksessfaktorer

- Det nye systemet skal samle alle AquaGens datamaskiner i et lett og oversiktlig system
- Brukere i AquaGen skal ha enkel pålogging til tjenester, dvs. løsningen kan ikke være noe vanskeligere enn dagens system
- Ny IT-sjef hos AquaGen må få nok kunnskap om systemet
- Prosjektet bør sikre bedriften en overordnet sikrere og mer robust klient- og serverplatform som er klar for morgensdagens krav
- Den nye systemet bør ikke overstige tidsbruken som går til utførelse av samme arbeid på en manuell måte.

## Informasjonsbehov

Veileder hos NTNU og veileder hos AquaGen ønsker/er:

- Viktig informasjon vedrørende prosjektes sluttdato eller resultat så snart det lar seg gjøre
- Møteinnkalling samt referat fra hvert møte
- Tilgjengelig for spørsmål over mail/Skype
- En viss pekepinn på prosjektets framgang, og eventuelle utfordringer knyttet til det

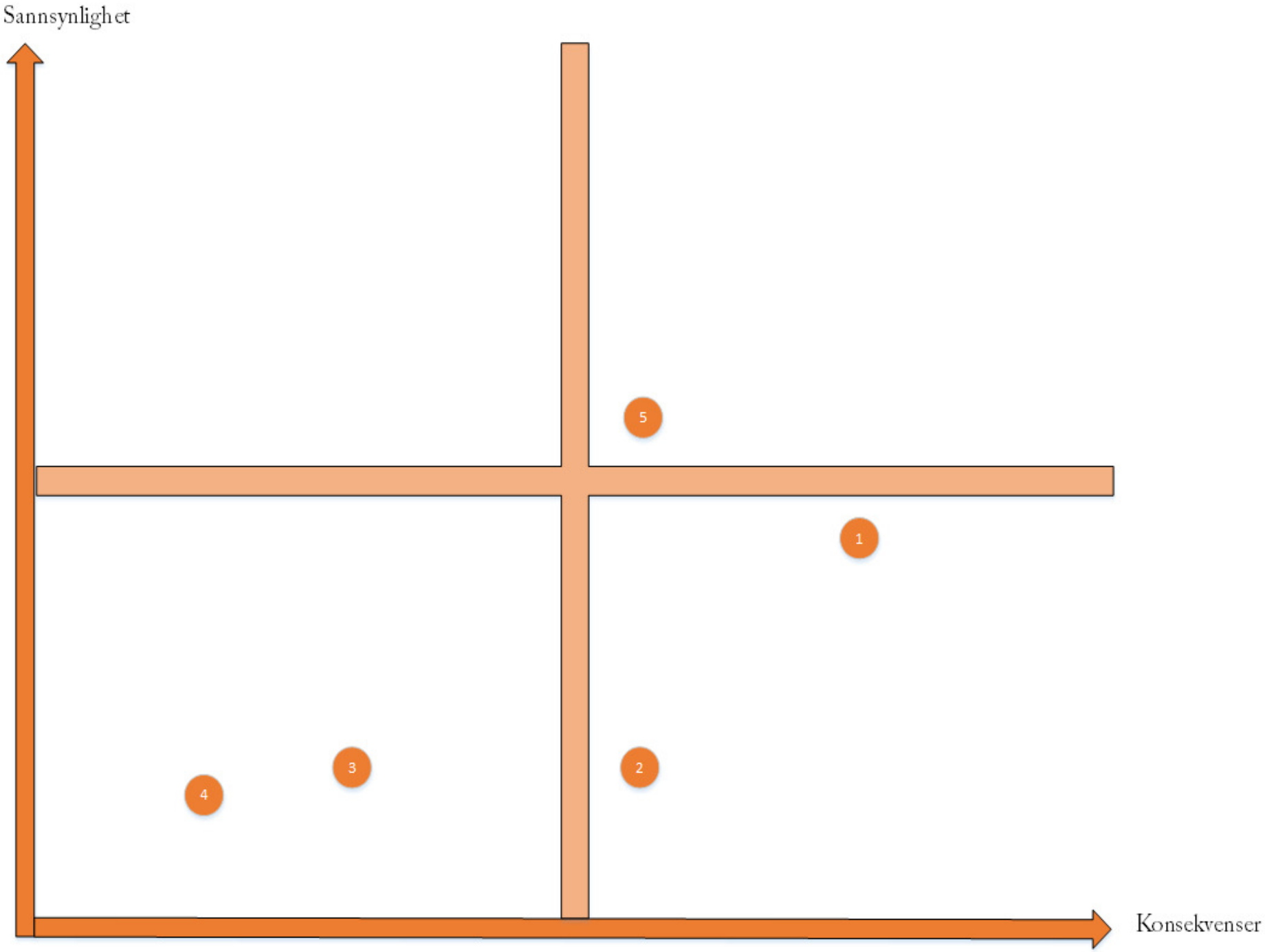
Spørsmål som omhandler den tekniske løsningen skal rettes til Evry evt. Microsoft på mail i god tid før endelig innlevering.

# 6. Risikoanalyse

Risikoanalysen tar for seg mulige hendelser som kan oppstå i løpet av prosjektet. Disse hendelsene vil være av betydning for prosjektets sluttdato og det endelige resultatet.

Først beskriver vi de de ulike risikoene, før vi plasserer dem i en oversikt på neste side.

1. Manglende tilgang til informasjonssystem hindrer prosjektet fra å gå videre
    - **Risiko**: får ikke ferdigstilt prosjektet og dermed ikke fullført bacheloroppgave, må ta opp igjen prosjektet
    - **Tiltak**: snakke med leverandør om tilganger, vise viktigheten av tilgang for ferdigstillelse av prosjektet
2. Prosjektet mister fokus på grunn av andre, viktigere prioriteringer i bedriften
    - **Risiko**: prosjektet mister tilgang til ressurser og forhindres i å gå videre
    - **Tiltak**: vurdere viktigheten til prosjektet for bedriften, vise hvorfor prosjektet bør ferdigstilles
3. Brukere slutter å bruke utstyr fordi det er for tungvint
    - **Risiko**: innføringen av nytt system hindrer arbeidsoppgaver i bedriften
    - **Tiltak**: vurdere enklere løsning på ting, finne kompromiss for å løse problematikken
4. Utfordringer mellom leverandør/AquaGen ift. leveranser av system
    - **Risiko:** avtale mellom Evry og AquaGen blir brutt – får ikke lenger tilgang til systemer som er kritiske for oppgavens ferdigstillelse
    - **Tiltak**: sørge for at tilgang til systemene består til oppgaven er ferdig, eventuelt vurdere å migrere mot annen leverandør
5. Manglende kobling mot Internett, nettverksutfordringer (dvs. ikke tilgang til skyen)
    - **Risiko**: mister tilgang til systemer, får ikke fortsatt på oppgaven
    - **Tiltak**: ha mobilt nettverk tilgjengelig, jobbe med andre oppgaver i mellomtiden


Sannsynlighet
5
1
3
2
4
Konsekvenser

# 7. Kost/nytte for prosjektet

I denne delen skal vi se litt på hvilken nytte prosjektet har for bedriften, og sammenligne dette med den forventede kosten dette vil ha for bedriften. Det er viktig at prosjektet gir mening å innføre, også økonomisk sett. En for høy kostnad vil nødvendigvis kreve mer nytte fra systemet, noe som man risikerer ikke er mulig.

## Kvantifiserbar og ikke-kvantifiserbar nytte

Her ser vi på både den kvantifiserbare og ikke-kvanitifiserbare nytten basert på de effektmålene vi har satt oss. Med dette skal vi prøve å forklare hva de ulike målene faktisk gir til bedriften, og hva det vil koste å oppnå dem.

Effektmål:

- AquaGen ønsker å bruke mindre tid på oppsett av nye maskiner – dette skal skje automatisk
- Arbeidere i ute produksjon skal bruke mindre tid på å løse dataproblemer – og dermed få mer tid til andre arbeidsoppgaver
- Datautstyret rundt om i bedriften skal bli enklere å holde oversikt på – enkel administrasjon
- Man ønsker å spare kostnader knyttet til uvettig bruk og stadig utbytting av utstyret – mer kostnadseffektiv drift

Kvantifiserbar nytte:

- Mindre kostnader knyttet til oppsett og feilsøking av datamaskiner
- Ta mer nytte av datautstyret ved å gjenbruke, få mest ut av pengene
- Tar bedre nytte av et system som fra før av eksisterer i bedriften

Ikke-kvantifiserbar nytte:

- En mer smidig arbeidshverdag for ansatte
- Positiv holdning for nytt datautstyr i bedriften – forenkling av arbeidshverdagen
- Bedre sikkerhet i bedriften
- Mer modernisert drift – klar for fremtiden

## Bortfall av direkte kostnader

Vi antar at ved vedlikehold eller feilretting betales det enten ansatte eller eksterne konsulenter for å utføre dette arbeidet. De kostnadene som inngår i å betale disse til å utføre vedlikehold og feilsøking på datamaskiner vil til en viss grad bli erstattet av dette systemet. Slike oppgaver omhandler først og fremst løsning av problemer som ellers kunne vært unngått hvis utstyret hadde vært konfigurert riktig fra starten eller problemet oppdaget på forhånd. Med Intune kjører man standardoppsett som fordeles på brukere, noe som minimerer tilfeller der enkelte enheter ikke inneholder riktig konfigurasjon.

Det brukes også en del ressurser i dagens system på å sette opp nye maskiner. Dette er en prosess som gjerne tar litt tid i forhold til oppdateringer og manuell sjekk som må utføres før enheten kan utleveres. Med Autopilot vil man automatisere mange av prosessene rundt dette, noe som minimerer tidsbruken betraktelig for de som skal utføre arbeidet.

## Kort om Microsoft 365

I dag betaler AquaGen for en rekke enkelte-lisenser for å få tilgang til den ønskede programvaren i organisasjonen. Dette er typisk tilfellet når man kjøper inn tjenester etter hvert som man trenger dem.

Det finnes en relativt ny tjeneste fra Microsoft som heter Microsoft 365. Med M365 kan man i tillegg til Office, også få tilgang til Windows-lisenser, MDM og ved E5-utgaven, også Windows ATP i en og samme pakke. En pakke av tjenester slik som Microsoft 365 tilbyr kan være aktuelt å bytte ut dagens system med hvis man har behov for den ekstra funksjonaliteten.

- Man risikerer økte kostnader ved et slikt bytte, men hvis den reelle nytteverdien overstiger kostnaden er det en endring man med gode hensikter kan innføre i organisasjonen.
- Nytteverdien ved et slikt bytte forsvares ikke nødvendigvis bare på sparte kostnader, men kan også gi rom for en mer fornuftig bruk av kostnadene som for øyeblikket går til brukeradministrasjon og lisenser.

## Kostnadsanalyse

### Estimerte kostnader under prosjektet

- Kostnadene rundt utvikling av det nye systemet kommer primært fra lisensen for Intune
    - Denne tildeles i dag på brukerbasis, altså hver sluttbruker av systemet har én lisens.
- Under utvikling vil det være behov for et testmiljø for å demonstrere funksjonaliteten, kostnadene for dette dekkes av NTNU.
    - Testmiljøet kjøres i NTNU sin Azure-portal og har satte begrensninger på hvor mye det kan benyttes/størrelse på miljøet.
    - Disse begrensingene blir ikke ansett som problematisk for prosjektet.
- Alt annet utstyr som trengs til prosjektet er tilgjengelig for utlån fra bedriften, og kommer ikke som en ekstrakostnad i prosjektet.
    - Eksempel på dette er fysiske maskiner, Windows-lisenser etc.

Videre innføring og drift av systemet vil nødvendigvis ha flere tilknyttede kostnader.

- For at systemet skal holdes vedlikeholdt vil det være nødvendige å ansette eller hyre inn noen til å drifte dette. Kosten blir i hovedsak knyttet til betaling av de som skal utføre denne oppgaven.
- Det blir kostnader tilknyttet dette uansett om det ansettes IT-personell i organisasjonen eller om oppgaven utføres av en ekstern leverandør.

### Sammenligning mellom Office og Microsoft 365

Kostnadene for Intune-lisens ligger på ca. 53,20,- hver måned per bruker (pr 08.02.2019).

- Per 08.02.2019 innehar bedriften 170 slike Intune lisenser.
    - Dette betyr i praksis kostnader på 9044,- pr måned og 108 528,- per år bare i Intune-lisenser.

Bedriften har også i dag en blanding av Office 365 E3 og E5 lisenser på samme antall brukere. Vi kommer kun til å sammenligne E3 brukere her for enkelhetsskyld.

- Estimert pris for én Office 365 E3 bruker er på ca. 200,- pr måned (pr 08.03.2019).
    - Det betyr i praksis kostnader på rundt 34 000,- pr måned og rundt 408 000,- i året kun for Office 365
    - Legger man til Intune i beregningen får man kostnader på rundt 43000,- per måned og rundt 516 000,- i året for Office 365 E3 + Intune

- Til sammenligning koster en Microsoft 365 E3 bruker ca. 280kr per bruker (pr 08.03.2019).
    - Det vil gi kostnader på rundt 47 600,- i måneden og rundt 571 000,- i året
    - Dette gir tilgang til både Office, Intune og Windows 10 Enterprise

Den regjerende forskjellen mellom de to løsningene blir da at Microsoft 365 E3 kommer med Windows 10 Enterprise lisens.

Hvis man legger inn Windows 10 Enterprise lisensen som kommer med Microsoft 365 til Office 365, vil man øke kosten med 60,- per bruker i måneden

- Kost på Office 365 E3 + Intune + Windows 10 Enterprise for 170 brukere blir da på hele 53 210,- hver måned, og rundt 638 000,- i året.

Sammenlignet med Microsoft 365 sparer man da altså rundt 67 000,- hvis man uansett skal ha både Office 365 E3, Intune og Windows 10 Enterprise.

## Oppsummering

Vi sitter da igjen med følgende alternativer:

- Beholde dagens løsning uten Windows 10 Enterprise
- Kjøpe lisenser enkeltstående, altså Office 365 E3 + Intune + Windows 10 Enterprise for rundt 122 000,- mer i året
- Gå for Microsoft 365 E3 som inkluderer alt ovenfor for ca. 55 000,- mer i året

Det må understrekes at man ikke er avhengig av å skifte til Microsoft 365 for at systemet skal virke. Det vil også fungere helt ypperlig med dagens løsning, men det finnes andre alternativer om man uansett ønsker å få med en Windows 10 Enterprise. I så fall er det billigere å gå for Microsoft 365 E3-lisenser. Med en Microsoft 365 **E5**-lisens får man også med Windows ATP, som også gir kostnadsbesparelse i form av antivirus-programvare.

Alle prisene funnet er bare estimater fra Microsoft og det vil garantert være mulighet til å innføre en avtale med leverandør og dermed få en enda billigere månedspris for innføring av Microsoft 365. Vi minner om at de nevnte alternativene bare er grovt anslått ut ifra disse estimatene.

Per dags dato ser vi ikke noen umiddelbare store kostnader ved å utføre det avtalte prosjektet, men videre drift vil nødvendigvis ha arbeidsoppgaver tilknyttet som vil innfører moderate kostnader. Ingen av disse kostnadene virker særlig urimelige i innføringen av så omfattende system og vi anbefaler fra kost/nytte-perspektiv å fortsette prosjektet som planlagt.

# 8. Retningslinjer og standarder

## Krav til dokumentasjon

I løpet av prosjektet skal følgende dokumenter foreligge:

- Forstudierapport – første utkast ferdig uke 7
- Systemkrav/rapport – første utkast bør være ferdig uke 14
- Driftsrapport – første utkast bør være ferdig til uke 18
- Sluttrapport – må være ferdig til innleveringsdato
- Prosjekthåndbok – må være ferdig til innleveringsdato

I løpet av prosjektet skal følgende oversikter foreligge:

- Timeliste – oppdateres hver dag
- Ukesrapporter – oppdateres for hver uke
- Møtereferater – legges ut fortløpende etter hvert møte
- Rapport fra prosjektplanlegging (MS Project) – oppdateres jevnlig, publiseres på SharePoint
- SharePoint-nettsted – oppdateres med relevant info ved anledning

## Krav til kvalitetsgjennomganger

I løpet av prosjektet skal følgende oppgaver være utført:

- Gjennomgang av brukerkrav for systemet
    - Forhøre seg med interessenter om hva som er ønskelig funksjonalitet i et slikt system
- Brukertest av systemet, gjerne med flere funksjoner
    - Gjennomføre en praktisk test for å verifisere/demonstrere funksjonaliteten og eventuelt avdekke feil/flere ønsker
- Eventuelt testing av andre funksjoner som ønskes
    - Testing hvis mer funksjonalitet ønskes

## Krav til standarder og metoder

- Prosjektet skal benytte seg av Intune og Autopilot fra Microsoft
    - Man benytter seg av Microsoft sin Azure Portal for å administrere systemet
    - Systemet skal følge Microsoft sin *best practice* på området og innføringen av systemet
- Prosjektplanlegging gjøres i Microsoft Project
- Informasjon om og dokumenter i prosjektet deles på egen SharePoint-side
- Navngivning for enheter gjøres slik:
    - AQG + LT/ST(laptop/stasjonær) + NOR (land) + tilfeldig tre-sifret nummer
    - Eksempel: AQG-LT-NOR-434

### Endringshåndtering

Ved forslag til endring fra interessenter utføres det på følgende måte for å avgjøre hvorvidt endringen gir mening å legge inn i prosjektet basert på tidsbruk/nytte:

1. Endringen noteres og kategoriseres ut ifra omfang
2. Konsekvenser og kost/nytte evalueres
3. Endringen godkjennes
4. Endringen logges, flettes inn i plan
5. Andre interessenter informeres
6. Endringen settes i verk

## 9. Prosjektorganisering

I dette prosjektet finnes følgende roller:

a. Oppdragsgiver: AquaGen v/ Truls Theting og Arnfinn Amdam
b. Veileder og kvalitetskontroll: Stein Meisingseth v/ NTNU
c. Oppgaveskriver: Kristoffer S. Hille v/ NTNU
d. Brukertest/referansegruppe: Rolf Myklebust og Arnfinn Amdam v/ AquaGen

# 10. Anbefaling om videre arbeid

**Alternativ 1:**
Prosjektet avsluttes på grunn av manglende ressurser eller behov for løsningen. Dette kan skyldes at den nåværende løsningen virker «bra nok» og at det derfor ikke er et behov for den skisserte forslaget.

**Alternativ 2:**
Prosjektet videreføres, men med vesentlige endringer vedrørende bruk av ressurser eller omfanget av oppgaven. Dette innebærer gjennomgang av endringshåndtering fra oppgaveskriver. Alt annet tilsier at oppgaven kan utføres og at det finnes et dokumentert behov for den skisserte løsningen.

**Alternativ 3:**
Prosjektet videreføres som over, men uten vesentlig store endringer. Det er et forstått behov for løsningen og oppdragsgiver har tid og ressurser til å gjennomføre prosjektet. Bruk av ressurser er godkjent, og oppdragsgiver er innforstått med den foreslåtte bruk av kostnader under prosjektet.

Ut ifra oppgaven kan man ganske sikkert falle mot alternativ 3. Det er ingen vesentlige ulemper med løsningen som vil gå utover den faktiske arbeidet som bedriften utfører, og man har analysert og funnet et behov som bedriften trenger å få fylt uten at det medfører store kostnader.

**Det anbefales å gå for alternativ 3.**

Kristoffer Selbekk Hille

# Klientadministrasjon med Microsoft Intune og Autopilot
# Systemkravdokument

**Versjon 1.1**

# Revisjonshistorie

| Dato | Versjon | Beskrivelse | Forfatter |
|---|---|---|---|
| 06.03.2019 | 1.0 | - | Kristoffer Selbekk Hille |
| 09.05.2019 | 1.1 | Fiks av layout/formatering | Kristoffer Selbekk Hille |

# Forkortelser og definisjoner

| ***Begrep*** | ***Uforkortet/alt. skrivemåte*** | ***Betydning*** |
|---|---|---|
| Compliant | - | Godkjent til bruk for et formål |
| AD | Active Directory, AD-tjener | System/server for å administrere domener med brukere, maskiner etc. |
| Azure | - | Sky-basert levering av tjenester fra Microsoft |
| SCCM | System Center Configuration Manager | Konfigurasjonsverktøy fra Microsoft, forgjengeren til Intune |
| Beta | | |
| Tanking | Tanke PC | Legge inn nytt image på PC-en, egendefinert utgave av Windows |
| Virtualisering | | Kjøre flere virtuelle maskiner i en annen, typisk fysisk maskin |

# Innhold

# 1. Introduksjon til løsningsdesign

## Introduksjon om kunden og behov

AquaGen AS er et avlselskap som er en ledende leverandør av befruktet rogn fra laks og ørret. Bedriften har behov for en løsning for å administrere sin PC-park, en god blanding mellom stasjonære og bærbare PC-er. Disse maskinene brukes i forskjellige områder i bedriften som omfavner bla. produksjon, forskning og kontorbruk. Systemet som iverksettes bør være oversiktlig og legge rette for fjernadministrasjon av viktige funksjoner på maskinene. Ønsket med denne innføringen er å skape en mer problemfri arbeidshverdag for de ansatte, som samtidig ikke går utover kompleksiteten til systemet for sluttbrukeren.

De overordnede behovene i en slik løsning er å få god oversikt over maskiner, uavhengig av hvor de befinner seg. I og med at AquaGen i dag ikke har egen IT-avdeling for hver lokasjon, er det greit å kunne begynne med å utføre fjernsupport og vedlikehold uten at man trenger å være til stede på hver avdeling. Systemet bør være kompatibelt med «alle» nyere versjoner av Windows 10, og samtidig støtte ny funksjonalitet som kommer i operativsystemet. Det bør være mulig å legge inn maskiner som både er nye, men også maskiner som allerede er satt opp som ønskelig. Hvis man må reinstallere alle enhetene kommer dette til å ta masse unødig tid. Hvis det er mulig er det ønskelig å legge rette til at eksiterende enheter kan rulles ut «på nytt» til å følge en standard satt av organisasjonen, mest rettet til når de skal tas ut av produkjosn etc.

## Valg av produkt og dekning av behov

For å gjennomføre dette prosjektet har vi valgt å bruke Microsoft Intune sammen med Microsoft Autopilot.

### *Microsoft Intune*

Microsoft Intune [2] er en plattform som samler sammen ulike enheter i et lett og oversiktlig system. Det gir tilgang til en del funksjonalitet som muliggjør for administrator å fjern-administrere enheter, uavhengig av lokasjon. Dette inkluderer oppgaver som fjernsletting, installasjon og oppdatering av programvare, kontroll over tilganger på systemet og så videre.

Intune-prosjektet ble startet av Microsoft for noen år tilbake, og har utviklet seg mye siden da. Prosjektet blir stadig utviklet for å støtte ny funksjonalitet i de nyeste utgavene av Windows 10, og Microsoft gir som regel tilgang til disse så snart de er klar for testing. Intune støtter også administrasjon av Apple- og Android-enheter som gir gode muligheter til å samle alle bedriftens enheter i et lett og oversiktlig system. Intune blir med andre ord utgangspunkt for en veldig sentral og enkel administrering av bedriftens IT-utstyr.

Før Intune brukte man som regel SCCM for å administrere Windows-enheter. SCCM er fortsatt en mye brukt måte å utføre administrering på, men i dag er dette å anse som litt gammeldags og tungvint. Dette gjelder spesielt for en stor bedrift som har mange ulike avdelinger i flere steder verden. Intune gjør dette veldig enkelt ved at man kobler opp enheten ved hjelp av Internett. Kravet om lokal infrastruktur faller dermed bort og gjør det mulig å utføre endringer på maskinen fra hvor som helst i verden. Dette åpner opp for mange nye tilnærminger å drive IT-drift på.

Det finner mange oppgaver som i dag kan gjøres via Intune, og det kommer stadig flere. Microsoft har bygget Windows 10 slik at uavhengig av installasjon, skal man ha mulighet til å legge inn maskinen i Intune og deretter sette de innstillingene man ønsker. Man slipper altså her å tanke PC-er til riktig utgave, og kan starte allerede med installasjonen som maskinen kommer sendt med. Dette er med på å spare tid.

Bedriften innehar allerede Intune-lisenser for de aller fleste brukere, så disse kommer ikke til å bli en ekstra kostnad under prosjektet.

### *Microsoft Autopilot*

Microsoft Autopilot [3] er en tjeneste i Intune som gjør det lett å egendefinere hvordan maskiner setter seg opp for sluttbruker. Autopilot opererer med maskinvare-IDer som administrator legger inn i Autopilot-portalen. Dette er en helt unik identifikator som beskriver en maskin slik at den kan koble seg opp mot Intune. Denne kan hentes ut manuelt på maskinene, også på maskiner som fortsatt er i installasjonsfasen (ikke satt opp enda). Hvis en potensiell leverandør henter ut disse IDene på forhånd kan maskinen sendes rett til sluttbruker uten å først måtte innom IT-avdelingen. Dette sparer tid, og gjør drift av maskinparken til en betydelig enklere oppgave.

Autopilot redegjør for at enheten automatisk kobles opp mot Intune og henter ned de policyer, konfigurasjoner og apper som organisasjonen har gitt til brukeren. På denne måten kan brukeren logge seg på hvilken som helst maskin og deretter få tilgang til de applikasjoner og filer som man bruker. Man kan også låse ned maskinen slik at den ikke kan brukes før maskinen er satt opp helt.

Man har også i Autopilot muligheten til å sette opp enhetene helt automatisk med funksjonen «self-deployment», som kun krever tilkobling mot Internett. Dette er mest rettet mot «offentlige» maskiner som blir brukt på flyplasser, kafeer etc. Man kan konfigurere at disse kun kjører en nettleser med bestemte sider, at alle filer og innstillinger blir slettet ved hver omstart og så videre.

Autopilot er kanskje mest relevant for nye maskiner, men også for maskiner som skal brukes til nye formål. I Autopilot lager man profiler som definerer hvordan enheten skal settes opp og til hvem. Dette gjør det smertefritt og enkelt å sette opp en maskin for en ny bruker. Hvis en ansatt slutter og ikke skal ha enheten lengre, kjører man bare en fjernsletting på enheten og den vil automatisk hente inn innstillinger for den nye brukeren.

Autopilot krever ikke egen lisens, da det er innebygd støttefunksjonalitet i Intune.

### *Oppsummering*

Microsoft Intune er noe bedriften allerede betaler for i dag og både Intune og Autopilot er derfor allerede tilgjengelig for prosjektet sin del. Autopilot er som nevnt en del av Intune, og krever ikke egen lisens.

Prosjektet påvirker derfor ikke organisasjonen noe kostnadsmessig, annet enn hvis bedriften velger å drifte dette systemet videre. Dette vil nødvendigvis stille krav for noen til å drifte det.

## 2. Beskrivelse av tekniske løsninger

### Hardware

Løsningen Azure fra Microsoft kjøres direkte i skyen, og har derfor ikke noe behov for noen lokale servere eller lignende hos AquaGen. All skalering i forhold til bruk av systemet vil skje automatisk hos Microsoft, og vi trenger derfor ikke tenke på maskinvaren som kjører dette.

Hos Evry kjøres det en lokal AD-tjener som blir synkronisert opp mot organisasjonens Azure AD. Dette er en katalogtjeneste som inneholder informasjon om brukere som finnes i AquaGen. Denne vil også fungere med prosjektet i dagens løsning.

De delene av oppsettet som blir kjørt lokalt er klient-maskiner og annet utstyr som skal koble seg opp mot Azure AD og Intune. Vi kommer her også til å virtualisere noen maskiner for testing av kllientfunksjonalitet - i praksis vil disse være å anse som fysiske maskiner. Under brukertesting vil man for øvrig også komme til å benytte seg av fysiske maskiner for å få testet systemet i praksis.

### Software

#### *Azure AD, Intune og Autopilot*

For å i det hele tatt få tilgang til Intune, er man nødt til å ha tilgang på en Azure-portal. I Azure kjøres det en tjeneste som heter Azure AD [1]. For at Intune skal fungerere som ønsket er man nødt til å ha tilgang til brukerkontoer for å tilegne policyer, apper og innstillinger.

Denne Azure AD-en synkroniseres mot EVRY sin lokale AD-tjener, Hazor. Dette er i utgangspunktet en speiling av brukerkontoene som benyttes til andre tjenester som AquaGen får fra EVRY. Dette påvirker ikke prosjektet på noen som helst måte. Både Azure AD og den lokale AD-tjeneren Hazor fungerer i dag med Intune-løsningen som vi skal benytte oss av.

Intune og Autopilot kjøres hos Microsoft på Azure-portalen. Man får her tilgang til et kontrollpanel der man får oversikt over maskinene som beskrevet tidligere. Denne portalen gir ulik tilgang avhengig av hvilken bruker man logger inn med. For administratorer har man full tilgang til all funksjonaliteten i portalen, men det er fullt mulig å avgrense dette som ønsket.

Tjenestene fra Microsoft skalerer seg helt automatisk, og skal fullt mulig støtte det antallet enheter som er forventet å legge inn, både under testing og bruk i praksis. Vi kan derfor ikke anta at det blir noen problemer ved bruk av Azure AD, Intune og Autopilot med dagens system.

#### *Operativsystem*

For at enhetene skal bli meldt inn i domenet, er de nødt til å kjøre et kompatibelt operativsystem. Nyeste versjon av Windows 10 Pro er fullt kompatibel [4] med Intune og MDM uten bruk av ekstra programvare. Systemet er påregnet brukt med Pro- eller Enterprise-utgaver av Windows, men vil antageligvis også virke med Windows 10 Home med noen begrensninger.

For enkelhetsskyld velger vi kun å bruke **Windows 10 Pro** og **Enterprise** på maskinene under prosjektet.

## Klienter

Klientene som vi ønsker å administrere med dette systemet kobler seg opp mot bedriftens ressurser på flere måter. Felles for alle er at de har tilgang til Internett, som er det eneste kravet for å få de koblet opp mot Azure AD og Intune. Det gjør det enkelt å innføre systemet uten vesentlige endringer i dagens infrastruktur.

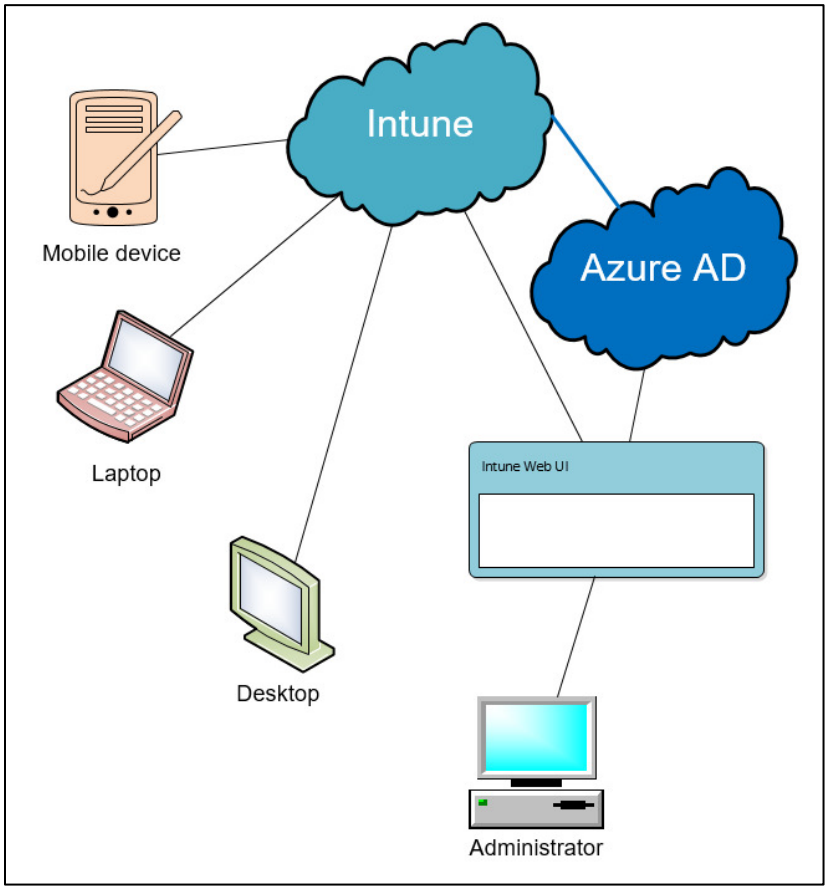
De aller fleste klientene kjører Windows 10 Pro. Det er forventet at det fleste kommer til å støtte Intune, men noen enkeltenheter kan kreve en oppdatering for å bli helt fungerende i systemet. Det kommer stadig ny funksjonalitet i Intune som krever tilsvarende nyere utgaver, og derfor er ikke kompatibilitet med alle eldre utgaver av Windows 10 ventet. De maskinene som kjører Home-utgaver og/eller gamle versjoner av Windows vil bli vurdert utbyttet med mindre noe annet er nevnt.

Siden vi ønsker å utføre testene våre fortløpende og kjapt vil det bli brukt en skyløsning hos Azure for å opprette virtuelle maskiner i oppsettet. Denne løsningen er for øyeblikket underlagt NTNU sin Azure-konto. Grunnen til at også ønsker virtuelle er for å ha muligheten til å teste ut funksjoner på en kjapp måte, og over flere maskiner. De fysiske maskinene skal benyttes til brukertestene, samt for å teste funksjonalitet som ikke er mulig å teste på de virtuelle klientene.

De fysiske enhetene vil bestå av et par bærbare maskiner til bruk som testmaskiner i oppsettet. Disse lånes av bedriften til prosjektet ved anledning. Det som er viktig for å teste funksjonaliteten er at maskinene støtter Secure Boot og TPM. Enkelte funksjoner i Intune, slik som «self-deployment» fungerer for øyeblikket kun med fysiske enheter og må nødvendigvis også bli testet der.

## 3. Løsningsbeskrivelse

### Skisse av oppsettet




## 4. Beskrivelse av skisse

### Enheter

I et ferdig implementert oppsett er det ventet at en bruker har flere enheter

- Mobil
- Laptop
- Stasjonær PC

I utgangspunktet skal man enkelt kunne sette policyer hos alle disse enheten fra en enkelt portal. Det er her Intune-portalen med MDM kommer inn i bildet.

- Intune og Azure AD er koblet sammen for å utveksle info om brukeren
- Administrator får tilgang til Azure og Intune gjennom Azure sitt web-grensesnitt

I dette prosjektet skal vi kun sette søkelyset på Windows-klienter – mobiler/nettbrett er bare gitt som eksempel på hva Intune kan håndtere av enheter hvis i fremtiden, hvis ønskelig. Først og fremst ønsker man en oversikt over klientmaskinene som finnes i bedriften.

## Bruker og tilkobling til PC

Når en bruker logger seg på en Microsoft-applikasjon på en PC, vil denne automatisk registrere seg i Intune-portalen som registered eller joined. Maskinen er da altså registrert i systemet og er klarert for de ulike appene, men kan ikke administreres fra Intune slik man ønsker det.

Når man setter opp PCen for første gang får man valg mellom å koble denne opp mot bedriften eller opprette en lokal konto.  De aller fleste PCene som AquaGen har er blitt satt opp med lokal konto, for enkelhetsskyld. Systemet som skisseres bør helst klare å legge til maskinen i «domenet» i ettertid slik at man slipper å reinstallere den fra scratch.

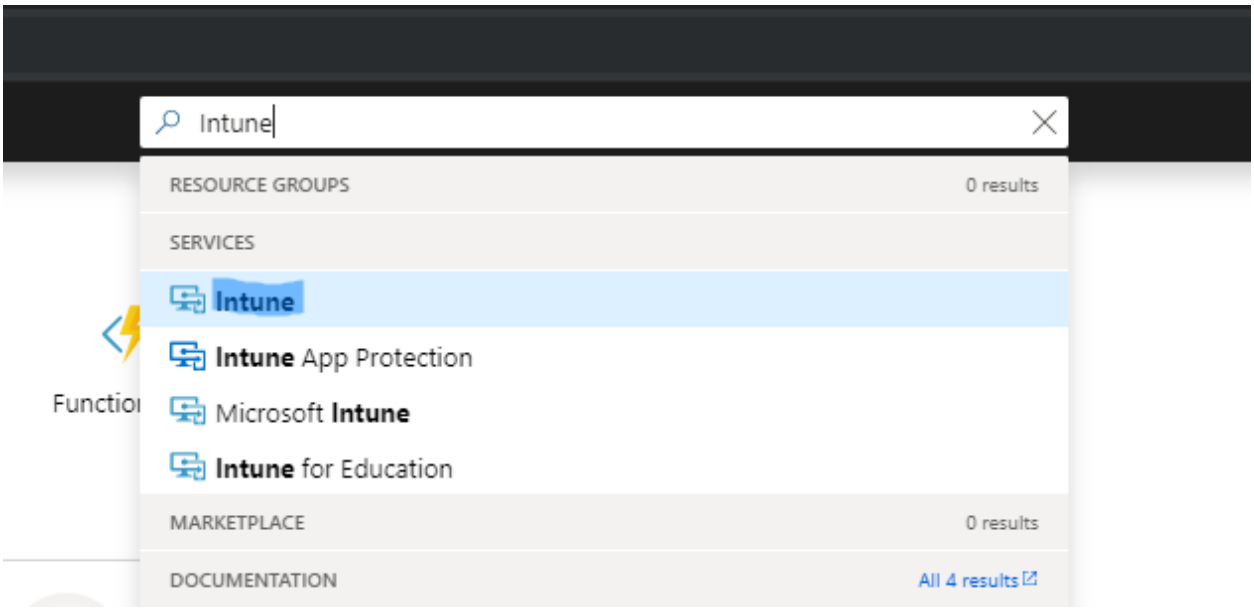
## Brukergrupper/tilganger

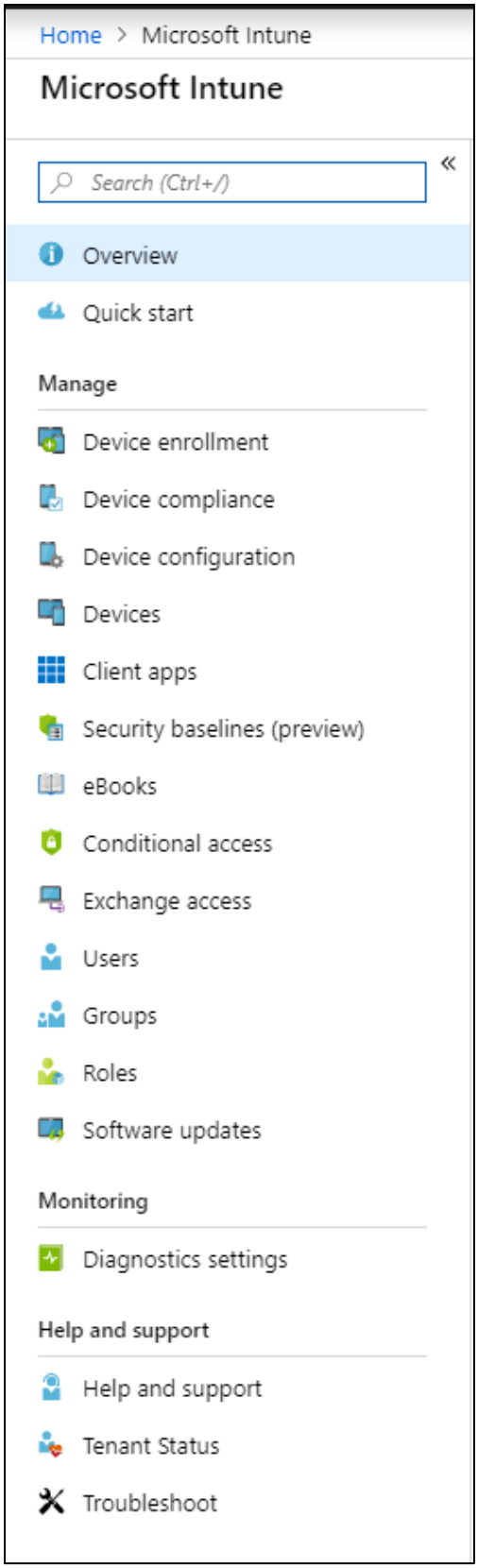
Administrator får tilgang til systemet ved Azure-portalen. Denne tilgangen gis ikke til vanlig brukere og blir gitt ut ettersom folk har behov for dette. Det skal i utgangspunktet ikke være noen grunn til at vanlige brukere skal ha tilgang til Intune-panalet med fulle rettigheter.

## Brukergrensesnitt, administator

For å komme til Intune sitt admin-panel, må man gå inn via http://portal.azure.com

Intune finnes som en integrert del av Azure, og kan åpnes ved å søke opp Intune i det øverste søkefeltet






## Funksjonalitet

Til venstre er alle de ulike områdene som kan administres i Intune sitt kontrollpanel.
Her ligger det masse ulike funksjoner som vi skal prøve å ta bruk av for å mest mulig effektivisere administrasjon av klientene.

De delene vi kommer til å være mest innom i dette prosjektet er følgende:

- **Device enrollment**
- **Device compliance**
- **Device configuration**
- **Devices**
- **Client apps**
- **Users**
- **Groups**

**Vi kommer til å beskrive disse delene i mer detalj i driftsdokumentet.**

## 5. Oppsummering

Vi har i dette dokumentet fått vist til de kravene som er satt for systemet som vi har planlagt å sette opp. Det man i all hovedsak ønsker med dette prosjektet er å skissere en løsning som kan ivareta drift av klientene som bedriften innehar.

For å løse dette kommer vi til å ta i bruk to løsninger fra Microsoft; Intune og Autopilot. Dette er to relativt nye verktøy som har begynt å bli mer og mer kjent. Det er allerede godt dokumentert, men det kommer stadig mer informasjon om nye funksjonaliteten. Begge disse er allerede tilgjengelige i bedriften, noe som gjør valget av løsning ganske enkelt. Vi ønsker å ta nytte i et system som bedriften allerede betaler for, noe som definitivt forsvarer prosjektets grunnlag.

Systemet som blir satt opp skal i all hovedsak være sky-basert. Det gir større muligheter i fremtiden, men vil samtidig også øke kravet for stabilitet på internett-forbindelser i samme system. Per dags dato ser vi ikke på dette som et problem, og tror løsningen vil fungere veldig fint med de systemene som bedriften allerede benytter seg av.

Vi vil i størst mulig grad beholde oppsettet som allerede finnes på maskinene for å hindre nedetid, men det er klart at en slik løsning vil fungere mest optimalt hvis alle maskinene innenfor samme avdeling/kontor etc. får samme oppsett. Dette skal man også klargjøre for at er mulig, selv på de maskinene som allerede er i bruk.

# Referanseliste


1. What is Azure Active Directory? Fra Microsoft. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis (aksessert 26.02.2019)
2. Microsoft Intune Overview. Fra Microsoft. Hentet https://www.microsoft.com/en-ca/cloud-platform/microsoft-intune (aksessert 25.02.2019)
3. Overview of Windows Autopilot. Fra Microsoft. https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot (aksessert 25.02.2019)
4. Supported operating systems and browsers in Intune. https://docs.microsoft.com/en-us/intune/supported-devices-browsers (aksessert 27.02.2019)

Kristoffer Selbekk Hille

# Klientadministrasjon med Microsoft Intune og Autopilot
# Driftsdokument

**Versjon 1.2**

## Revisjonshistorie

| Dato | Versjon | Beskrivelse | Forfatter |
|---|---|---|---|
| 30.04.2019 | 1.0 | - | Kristoffer Selbekk Hille |
| 01.05.2019 | 1.1 | Mangler brukertest | Kristoffer Selbekk Hille |
| 08.05.2019 | 1.2 | Formatering og diverse | Kristoffer Selbekk Hille |

## Forkortelser og definisjoner

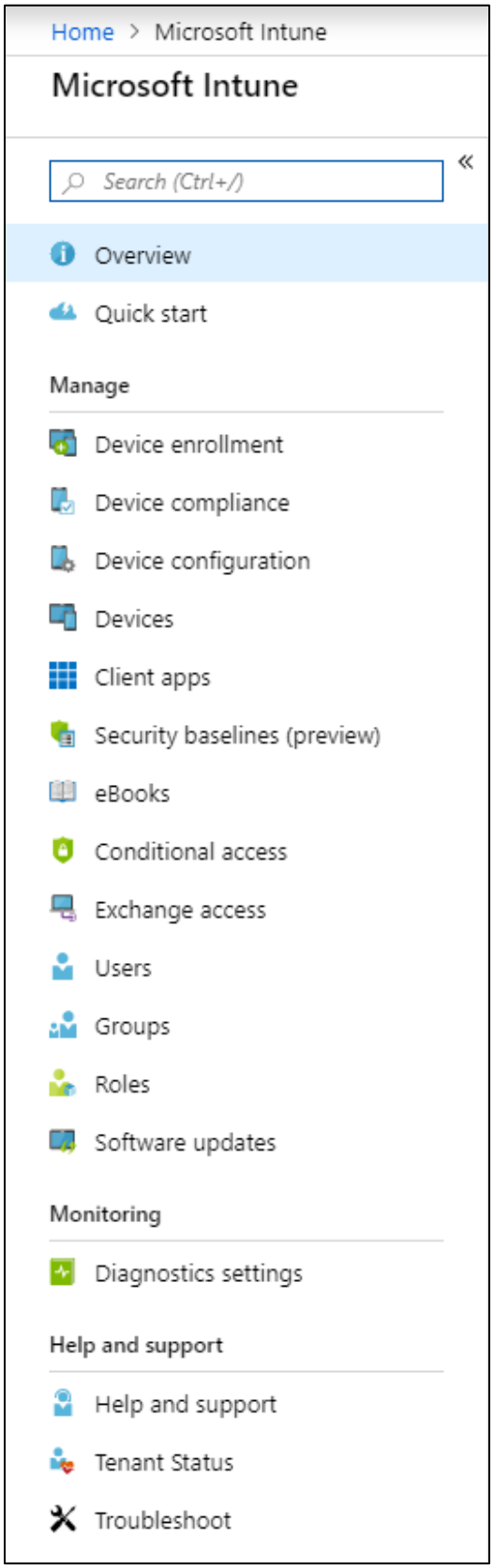
| ***Begrep*** | ***Uforkortet/alt. Skrivemåte*** | ***Betydning*** |
|---|---|---|
| Active Directory | AD | Katalogtjeneste fra Microsoft, benyttes til brukeradministrering i gjerne større organisasjoner. Finnes i flere utgaver |
| BitLocker | | Krypteringsverktøy fra Microsoft. Brukes for å beskytte innholdet på enheten. |
| Compliance | Compliant | At en enhet er godkjent for bruk til et formål |
| Compliance policy | Policy | En rekke krav som må godtas/bekreftes før bruk av utstyret |
| CSV-fil | Comma-seperated-values | En standard for å legge inn data i system på. Hver verdi er separert med komma. |
| Deploy | Deployment | Sette til verks en konfigurasjon, o.l. |
| Enrol | Enrollment | Registrering av (en) profil på en enhet/bruker/gruppe |
| EULA | End-user-license-agreement / Sluttbrukerlisens | Avtale mellom leverandør av og sluttbruker av tjenesten/programmet |
| Evaluation-edition | Prøveutgave | Utgaver som er ment for testing, har som regel en begrenset prøveperiode, f.eks. Windows Evaluation |
| Hardware-ID | Maskinvare-ID | Unik identifikator for Windows-enheter. Brukes for å importere enheten i Windows Autopilot. |
| Hyper-V | | Virtualiserings-programvare fra Microsoft. Brukes for å opprette virtuelle maskiner. |
| Kiosk-PC | | PC med begrensninger mot et bestemt formål, eks. bare vise nettleser eller som en infoskjerm |
| Kommandolinje | CMD | Vindu der man kan utføre kommandoer. Tekstbasert. |
| MDM | Mobile Device Management | Samlebegrep for måter å administrere mobile enheter på |
| OOBE | Out-of-box-experience | Første erfaring/interaksjon bruker har med en enhet, eks første gang den slås på |
| OS | Operativsystem | Eks. Windows. |

| | | |
|---|---|---|
| PowerShell | PS | Kommandolinjeverktøy fra Microsoft, tar over for vanlige «cmd» |
| SCCM | System Center Configuration Manager | Alternativt verktøy for å administrere enheter fra Microsoft, Intune bygger til dels på dette |
| Scope | Skop | Bestemt samling av enheter, basert på kriterier |
| Secure Boot | | Sørger for at kun godkjente installasjoner av operativsystem kan kjøre på maskinen |
| Security baseline | | En rekke innstillinger som er anbefalt av Microsoft. Leveres gjerne i pakker som man kan legge inn. |
| Shared multi-user device | | Enhet som kan brukes av flere brukere, eks. en delt maskin |
| Standalone app | | Apper som installeres ved hjelp av programfiler, ikke via App Store etc. |
| TPM | Trusted Platform Module | Innebygd enhet i maskinen som lagrer nøkler ift. kryptering, autentisering etc. |
| Windows ATP | Advanced Threat Protection | Kraftig antivirus-software fra Microsoft. |
| Windows Defender | | Standard antivirus fra Microsoft, følger med alle Windows 10-enheter |
| Arkitektur | | 32- eller 64-bit. Avhengig av maskinvare i enheten. Sistnevnte er standard i dag. |

# Innhold

## Faser i implementasjonen

- **Fase 1:** *Konfigurasjon av Intune og Autopilot*
- **Fase 2:** *Klargjøring av enheter*
- **Fase 3:** *Uthenting og importering av maskinvare-ID i Autopilot*
- **Fase 4:** *Importering av eksisterende enheter i Intune*
- **Fase 5:** *Policyer, programvare og konfigurasjon*
- **Fase 6:** *Test av Microsoft Autopilot*
- **Fase 7:** *Self-deployment med Autopilot*
- **Fase 8:** *Test av funksjonalitet i Microsoft Intune*
- **Fase 9:** *Brukertest v/Rolf og Arnfinn*




## Fase 1: Konfigurasjon av Intune og Autopilot

For at vi skal kunne få installert maskinene slik vi ønsker, er det nødvendig å sette forskjellige innstillinger i Intune og Autopilot på forhånd. Disse innstillingene berører blant annet hvilke rettigheter en bruker skal ha på maskinen sin, hvilken programvare som skal være installert, og hvilke policyer som skal være satt fra maskinen startes opp for første gang.

- Intune og Autopilot er tjenester som allerede ligger installert i organisasjonens Azure-portal, og er derfor allerede knyttet opp mot vår AD.

Til venstre er en skjermdump fra Intune-portalen i Azure.

Listen til venstre viser flere av valgene som finnes i hoved-menyen til Intune, men de vi i hovedsak kommer til å se på er:

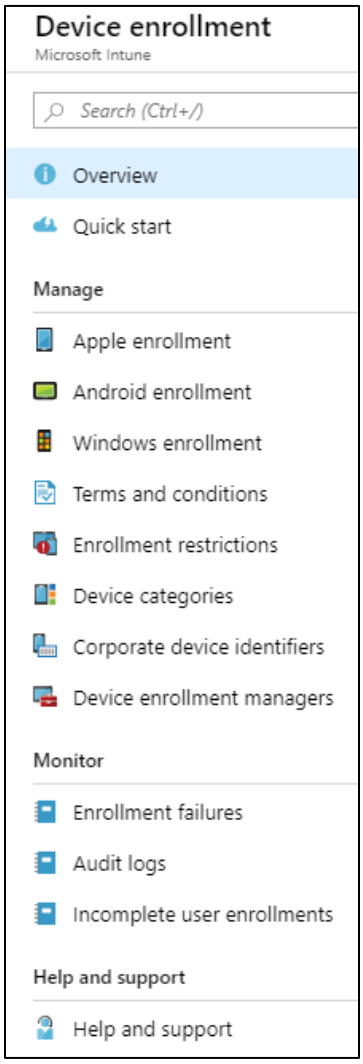
- **Device enrollment** - innstillinger for utrulling
- **Device compliance** – innstilling for policyer
- **Device configuration** – profiler for enheter
- **Devices** – viser alle enheter som er «compliant»

Noen kategorier vi også kommer til å berøre i dette dokumentet er:

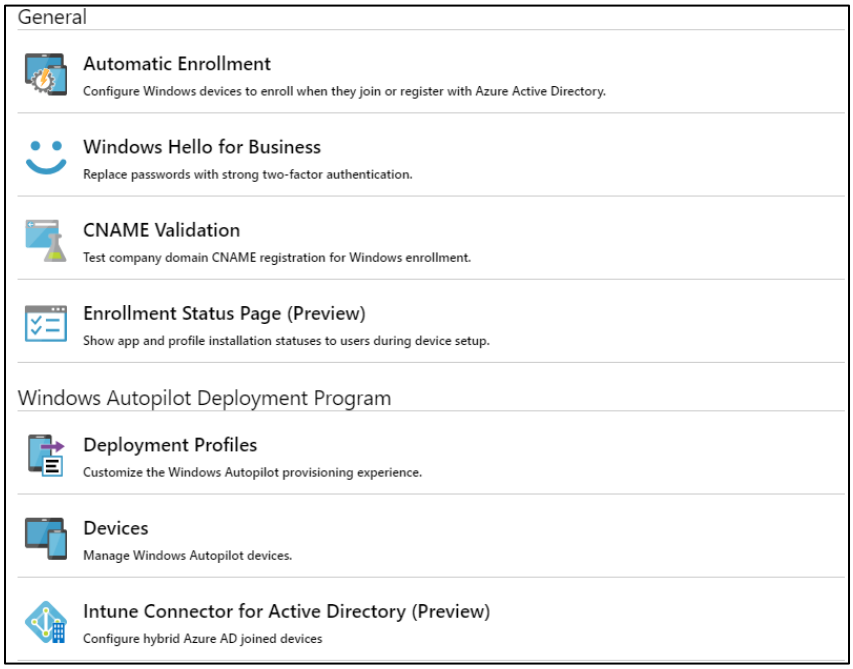
- **Client apps** – utrulling av programvare
- **Security baselines** – anbefalte innstillinger fra Microsoft
- **Users** – viser alle brukere og deres enheter
- **Groups** – bruker- og enhets-grupper

## Device enrollment

*Device enrollment* brukes for å sette innstillingene som bestemmer **hvordan** enhetene legges inn i domenet. Vi skal i all hovedsak fokusere på **Windows Enrollment** her.




Under *Windows Enrollment* finner man følgende alternativ:

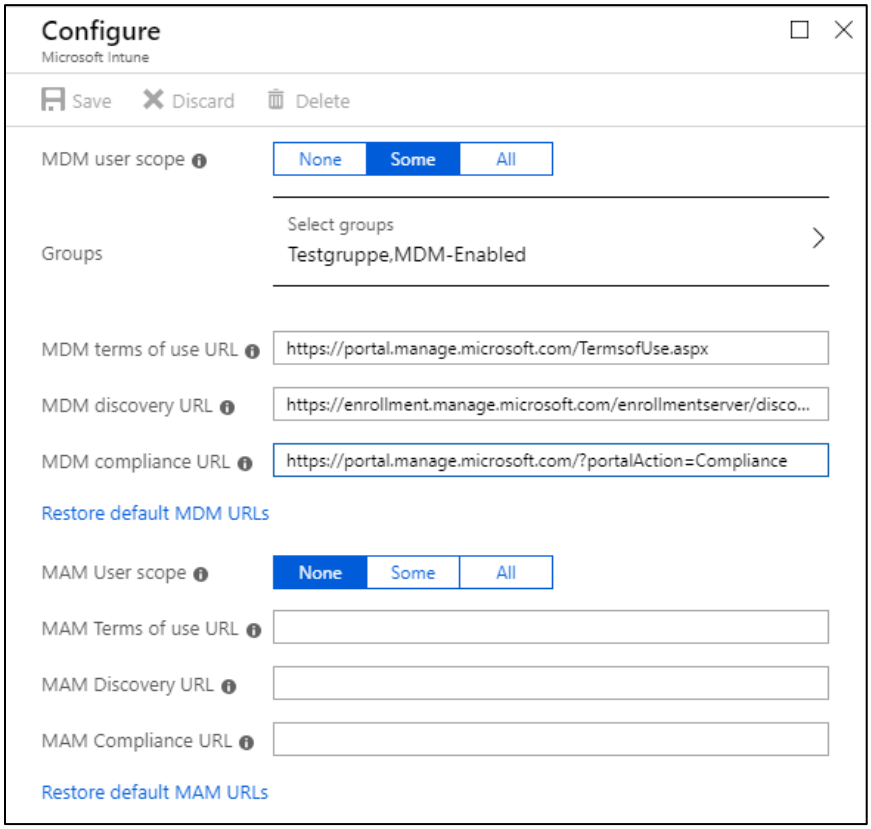



De delene vi skal se mest på her er:

- *Automatic Enrollment*
- *Enrollment Status Page*
- *Deployment Profiles*
- *Devices*

**Windows Hello for Business, CNAME-validation** og **Intune Connector for AD** er allerede satt opp, og trenger derfor ikke ekstra konfigurering.

## Automatic Enrollment




Under *Groups* setter vi gruppene som skal kunne benytte seg av *Automatic Enrollment.*

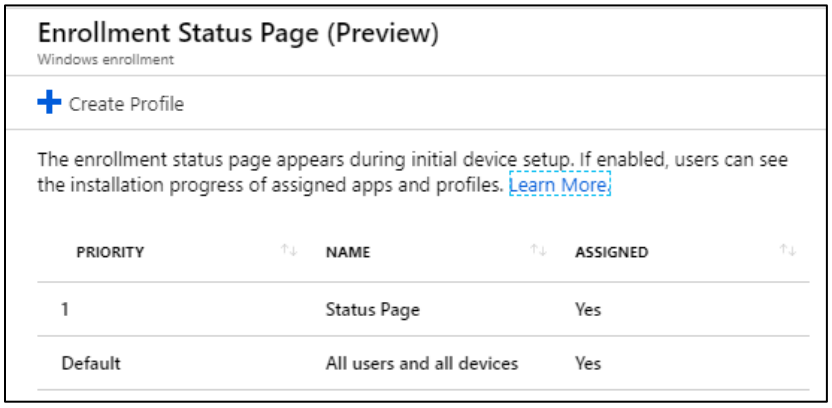
Under testing brukes dette kun på grupper opprettet for prosjektet.

- I praksis vil denne bli satt til å gjelde alle maskiner, eventuelt en gruppe maskiner som skal legges inn i domenet.

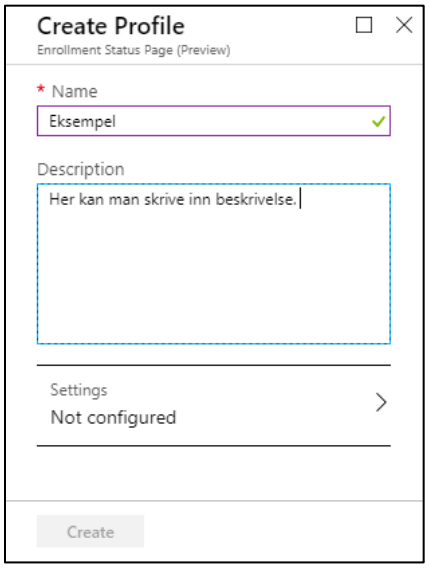
I dette prosjektet skal vi kun bruke Windows 10-enheter som benytter seg av **MDM**, og vi trenger derfor ikke å konfigurere **MAM** akkurat nå.

## Enrollment Status Page

Under registreringen (enrollment) kan vi velge å gi brukeren en egendefinert status-side som viser hvor langt maskinen er kommet i utrullingen.



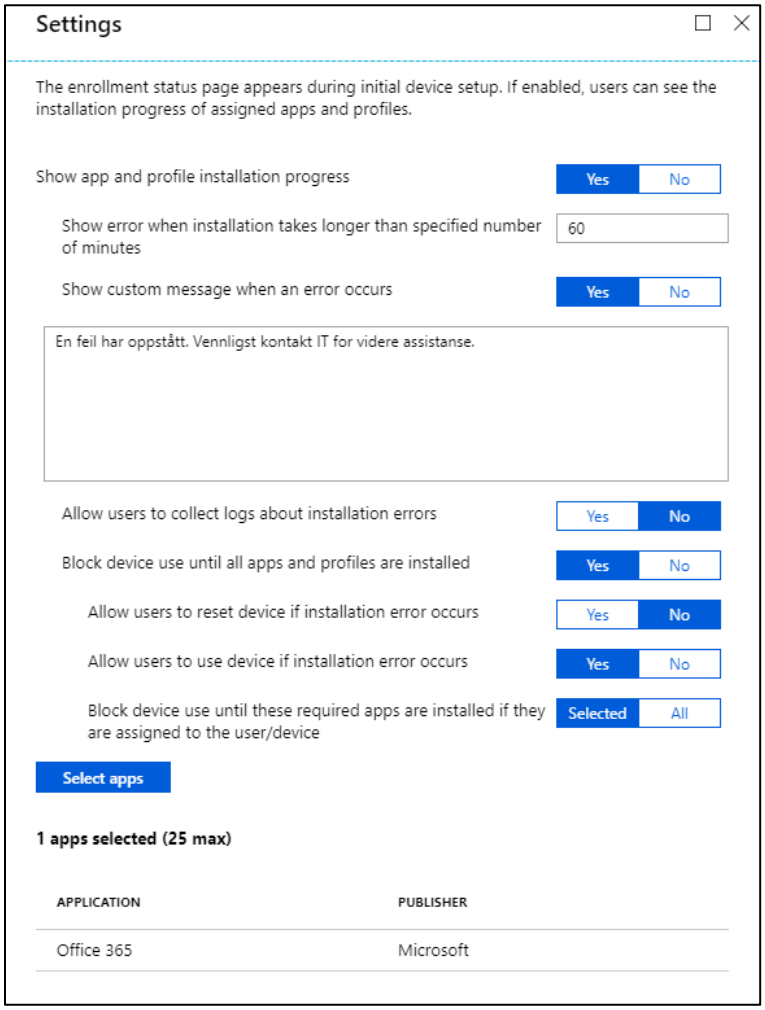

Vi kan lage en «profil» ved å trykke på 


Her oppretter man en profil og setter navn og beskrivelse som man selv ønsker.

For å sette de faktiske alternativene trykker man på *Settings*

Under *Settings* får man endel alternativer.




For å i det hele tatt begynne må man sette første valg «Show app and profile installation progress» til «Yes».

Videre kommer disse valgene:

- Valg om å vise feilmelding etter en satt tid, også egendefinert feilmelding
- Tillate at brukere kan hente ut logger ved feil
- Blokkere bruk av enheten under enkelte omstendigheter som eks. manglende profiler eller applikasjoner
- Tillate at brukeren enten kan bruke eller resette enheten ved feil i oppsettet

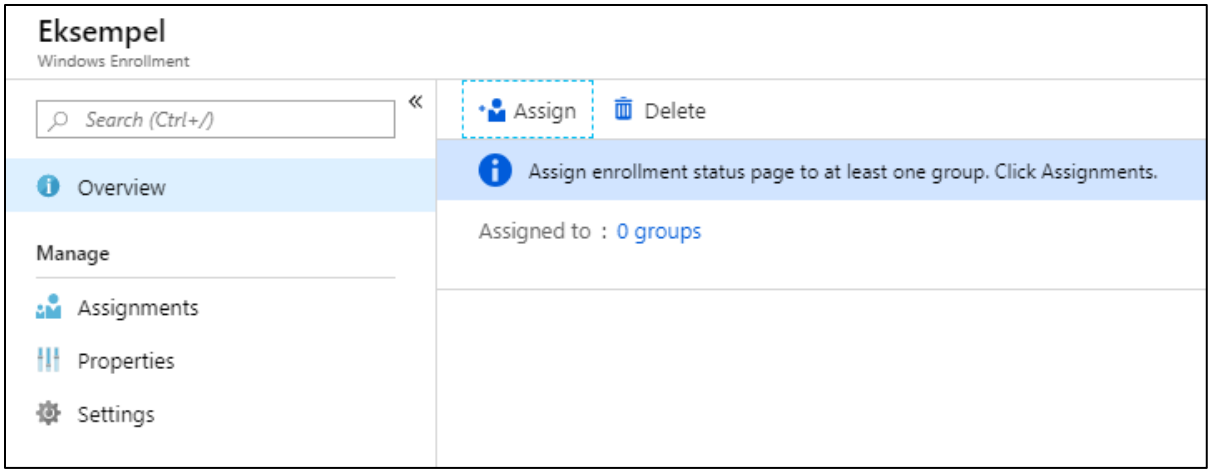
Når man er ferdig trykker man *Save* og deretter *Create*

Profilen er nå opprettet.

| PRIORITY | NAME | ASSIGNED |
|---|---|---|
| 1 | Status Page | Yes |
| 2 | Eksempel | No |
| Default | All users and all devices | Yes |

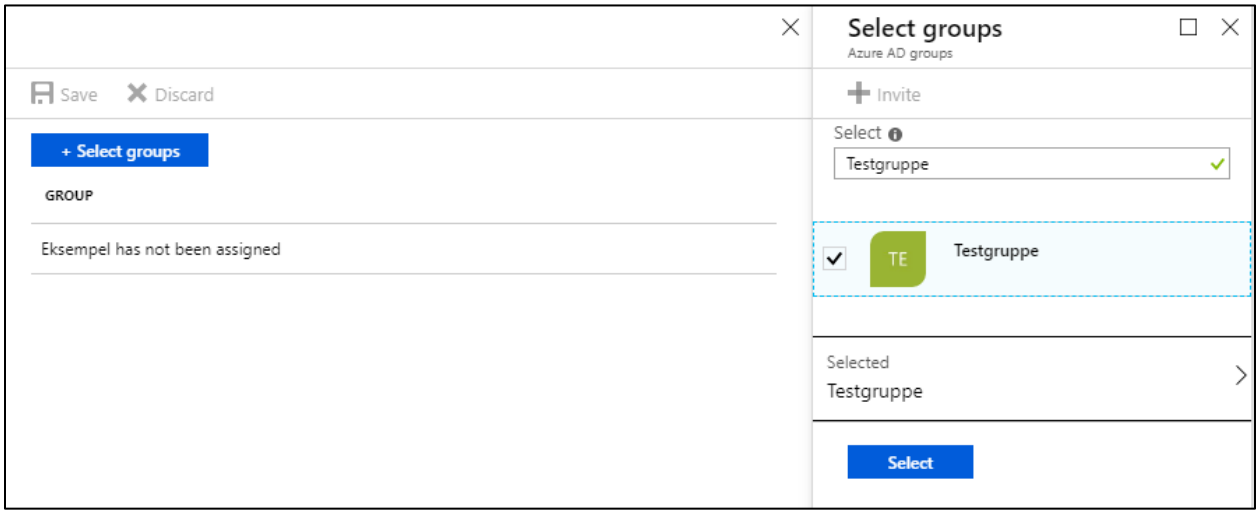
For å kunne bruke profilen må man først tilegne den til en gruppe

Dette gjøres ved å først trykke på profilen.




Når man kommer inn i på profilen ser man at man at den for øyeblikket ikke er tilknyttet en gruppe.

Vi trykker derfor på *Assign*

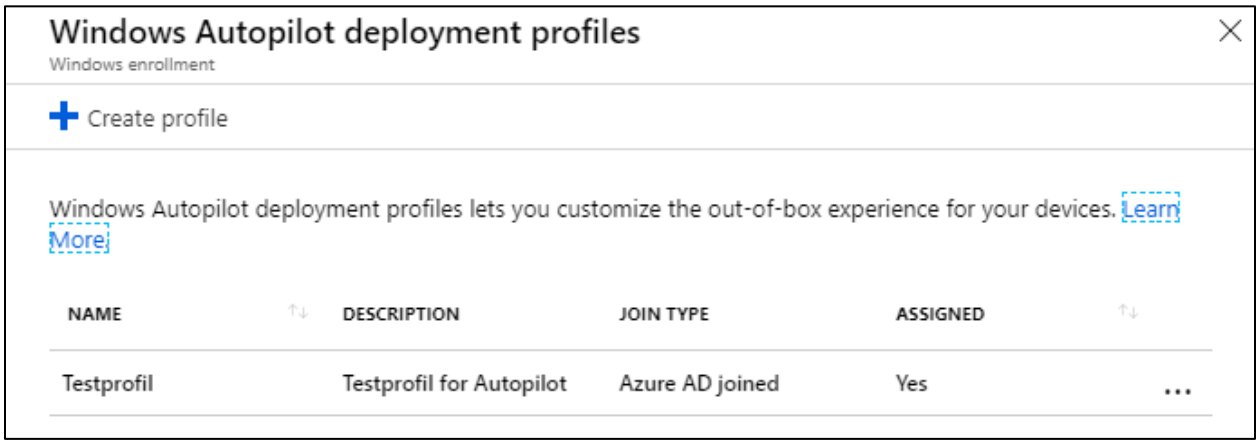



Vi trykker *Select Groups*, skriver inn navnet på gruppa, trykker på den og trykker *Select* For å lagre endringene trykker vi på *Save*.

**Profilen er nå opprettet og tilknyttet en gruppe.**

## Windows Autopilot Deployment Profiles

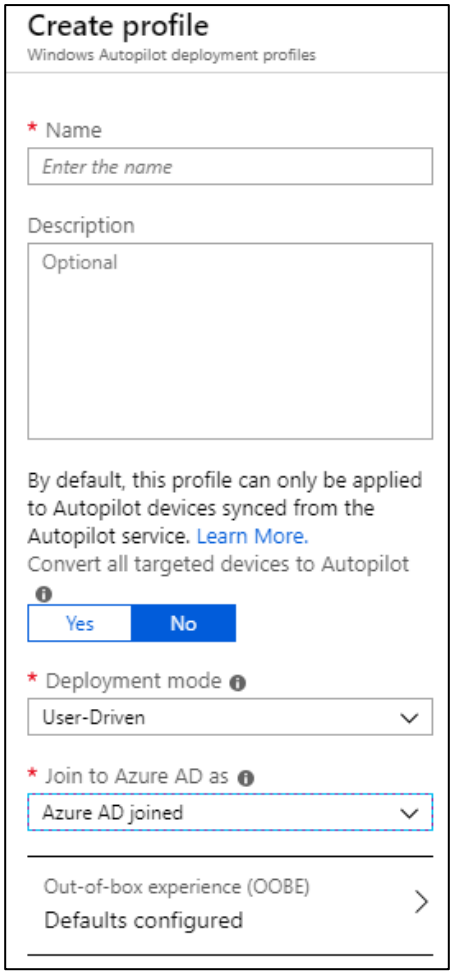
I den forrige menyen satte man en status-side som skal vises under *deployment*.




I denne menyen setter man **predefinerte valg** som skal settes under en Autopilot-deployment

Her kan man trykke på  for å opprette en profil.


Her har man noen valg:




Det første man må sette er navn og beskrivelse.

Det neste valget omfatter hvorvidt man ønsker å konvertere alle berørte enheter til å bli konvertert til typen Autopilot. Vi gjør dette da disse profilene kun virker på enheter som er av typen Autopilot.

*Deployment mode* handler om hvorvidt man ønsker at brukeren skal være delaktig i prosessen rundt oppsett av enheten.

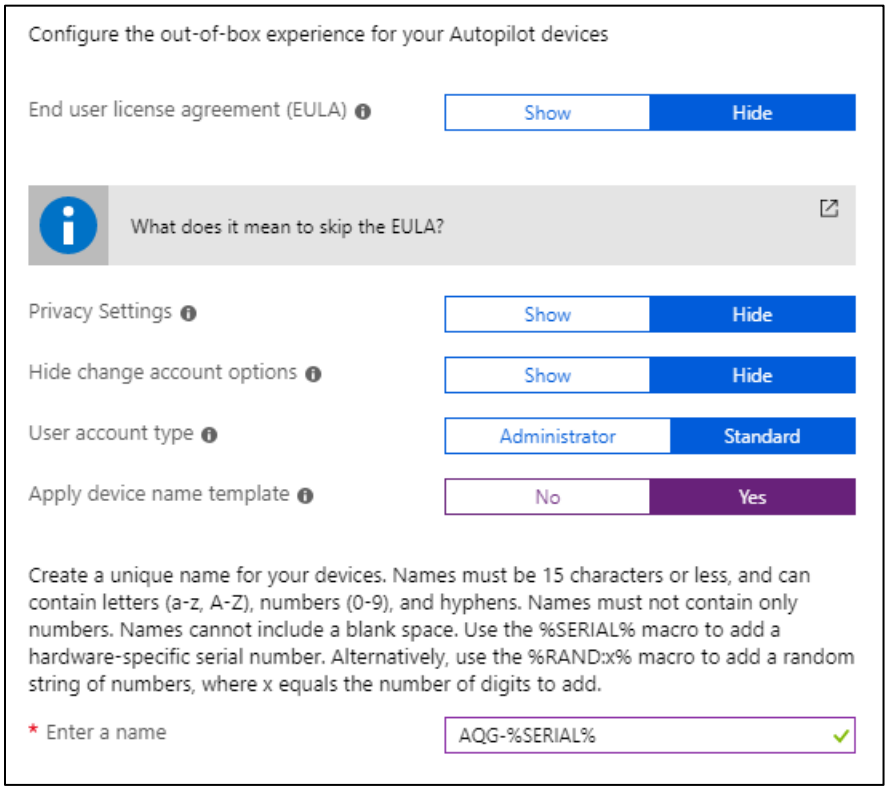
- **User-Driven:** Hvis man skal levere ut maskiner til ansatte kan de selv logge inn på maskinen for å sette den opp
- **Self-Deployment:** ved oppsett av flere maskiner på forhånd kan det være tidsbesparende at maskinene setter seg opp på egenhånd, uten brukerinteraksjon

*Join to Azure AD as* viser til hvordan man ønsker at enheten kobler seg opp mot domenet.

I dette eksempelet skal vi bruke **Azure AD joined** da vi kun benytter cloud-løsningen av Azure AD. Hvis man også har en lokal AD-server brukes **Hybrid Azure AD-joined**.

De neste valgene finnes i *Out-of-box-experience (OOBE)*

*Out-of-box-experience (OOBE)*



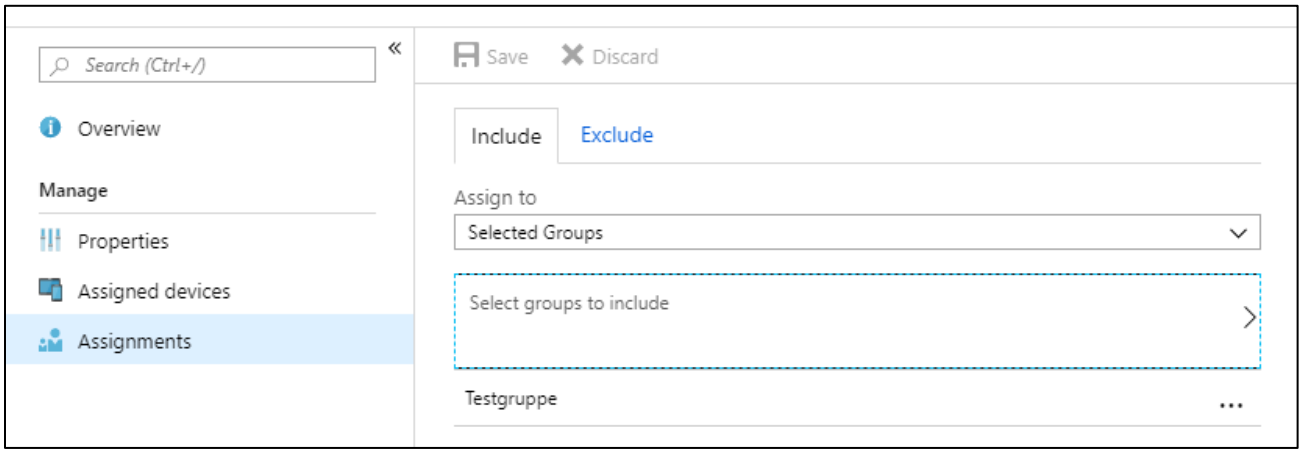

Her kan man sette noen alternativ på deployment profilen:

- Første valg er om man ønsker å vise EULA til brukeren eller ikke
- Om man ønsker at brukeren selv velger hva som skal deles og ikke fra maskinen
- Om brukeren selv kan velge å bruke lokal konto (altså ikke bruke firma-konto)
- Hvorvidt brukeren som opprettes blir Administrator eller Standard-bruker

- Man har også mulighet til å sette et egendefinert navn på enheten.
    - Per dags dato kan man kun bruke serienummer på maskinen eller et tilfeldig tall til å danne navn på maskinen. I fremtiden forventer vi at man får mulighet til å sette brukernavn som del av PC-navn, noe som kan være ønskelig.

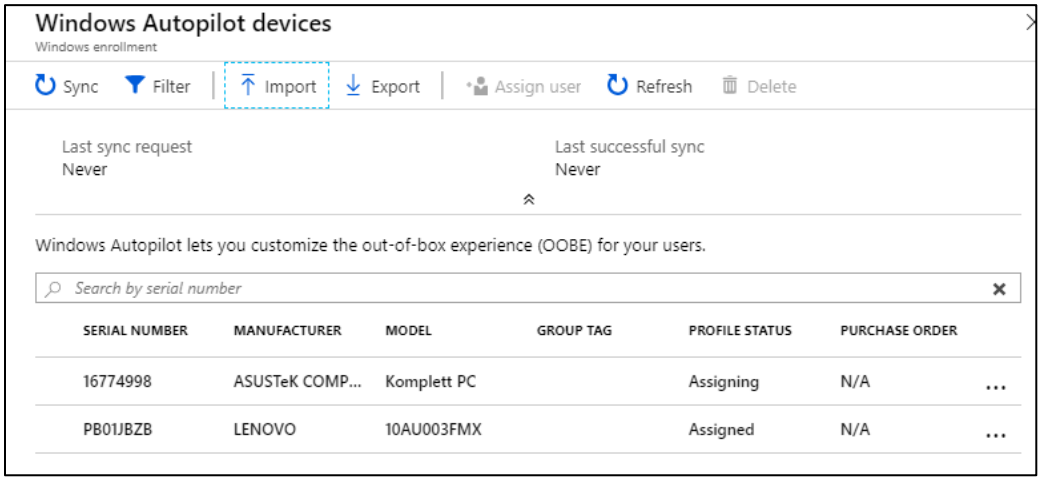
Når man har satt alle valgene trykker man *OK* for å lukke vinduet og deretter *Create* for å lage profilen.

For at profilen skal virke må den tilegnes en gruppe. Dette gjøres på samme måte som ved oppretting av *Enrollment Status Page*




**Profilen er nå opprettet og tilegnet en gruppe.**

## Devices (Windows Autopilot devices)

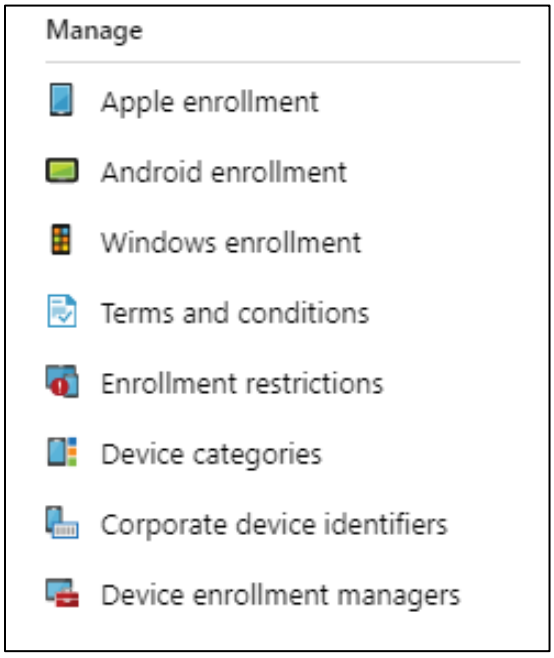



I denne menyen vises alle enheter som er av typen Autopilot. Vi får vite serienummer, produsent, hvilken modell enheten er, hvorvidt den er tilknyttet en bruker og eventuelt om den tilhører en navngitt bestilling.

I dette tilfellet har maskinene blitt importert ved hjelp av en **CSV** fil som er blitt generelt manuelt på hver maskin gjennom et script i PowerShell. Dette scriptet henter ut maskinvare-ID, på enheten, som er en helt unik nøkkel som beskriver systemet for Autopilot.

- Det er denne nøkkelen som gjør at Autopilot når tak i enheten når den skal konfigureres
- Når systemet settes ut i faktisk bruk vil det være mer vanlig å få denne filen fra produsent/leverandør som har høstet inn disse nøklene på forhånd. Å utdele PCer til brukere vil derfor bli en mye mindre manuell oppgave for den som skal drifte systemet.

**Vi kommer tilbake til importering av maskinvare-ID i fase 3.**

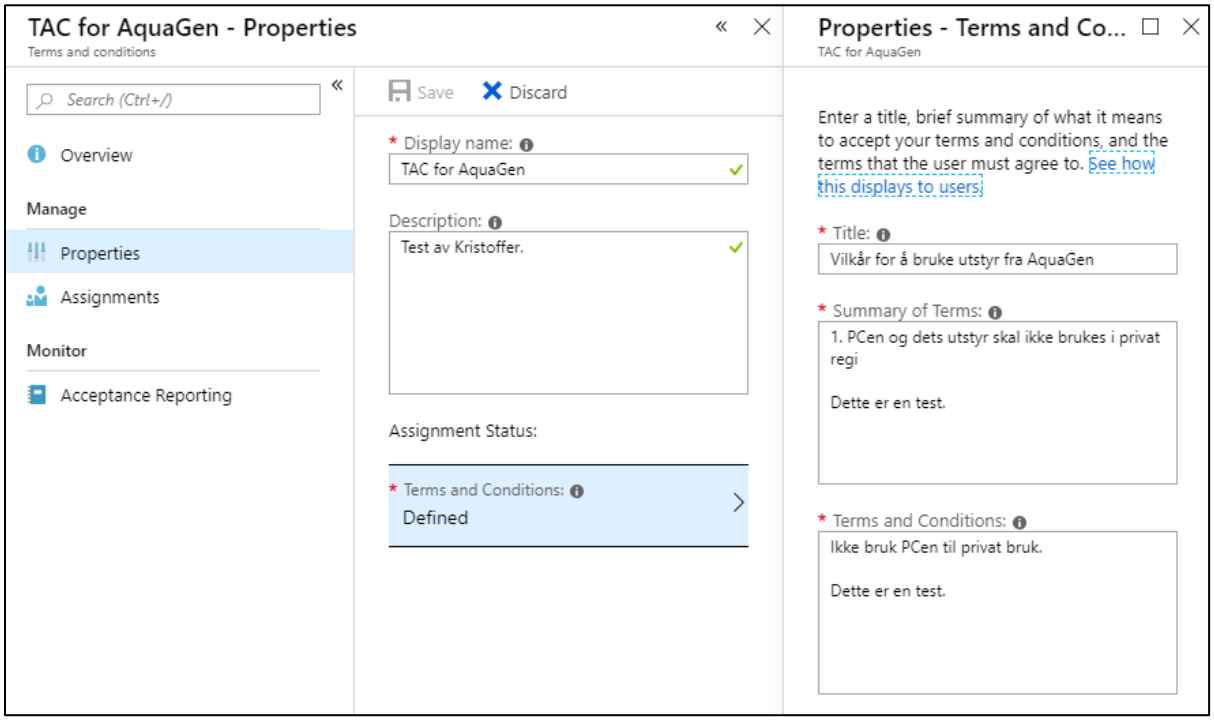



Det finnes også noen andre innstillinger under *Device deployment*. Disse er ikke vesentlige for prosjektet, men kan fint konfigureres hvis ønskelig senere.

Vi kan beskrive dem kjapt for å vise til hva som kan konfigureres her.

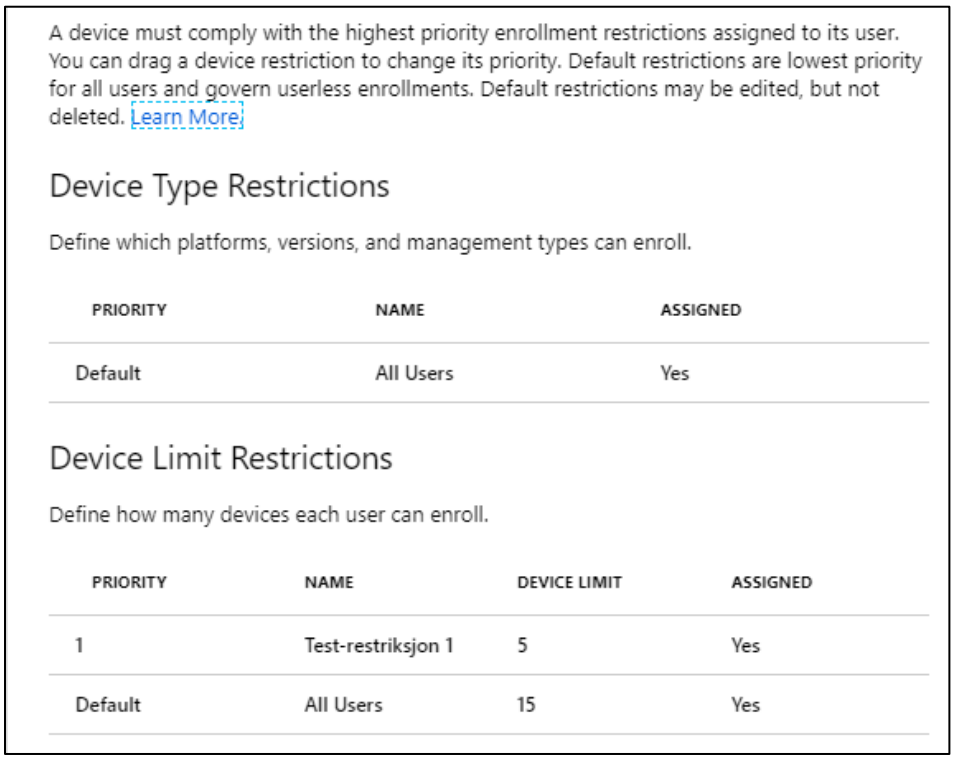
### *Terms and conditions*

Her kan man sette inn egendefinerte brukervilkår som må aksepteres før utstyret tas i bruk.



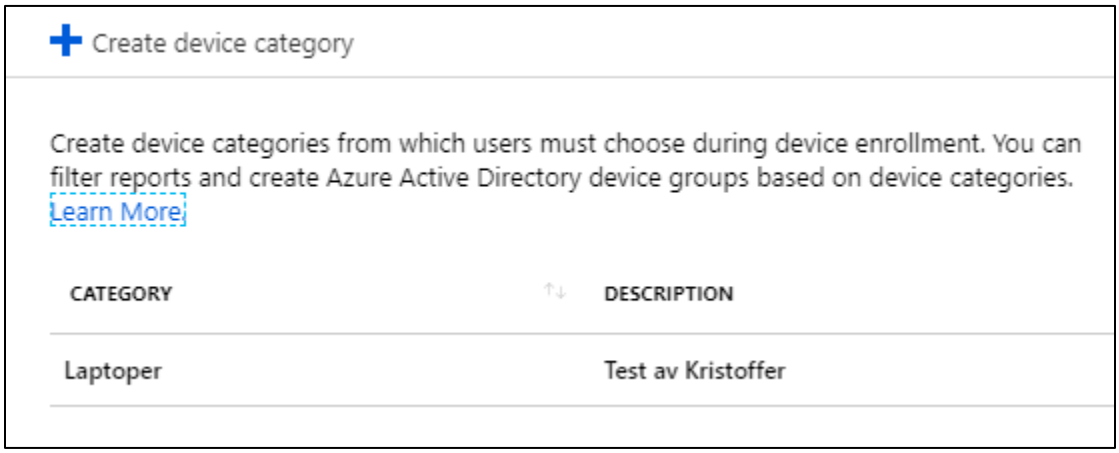

### *Enrollment restrictions*

Her kan man sette begrensninger på hvor mange enheter en bruker kan inneha i domenet, samt hvilke typer av enheter som er tillatt å bruke i domenet



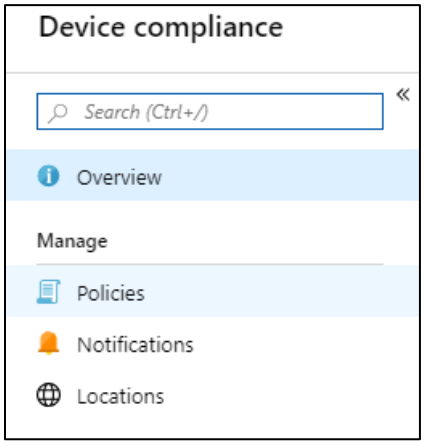
### *Device categories*

Kategoriene brukes ikke til stort mer enn å definere grupper med forskjellige typer enheter som bedriften administrerer. Det brukes også i *enrollment restrictions.*




De andre alternativene som ikke er nevnt er ikke relevant for prosjektet og/eller gjelder kun for mobile enheter slik som smarttelefoner, nettbrett etc.

## Device compliance

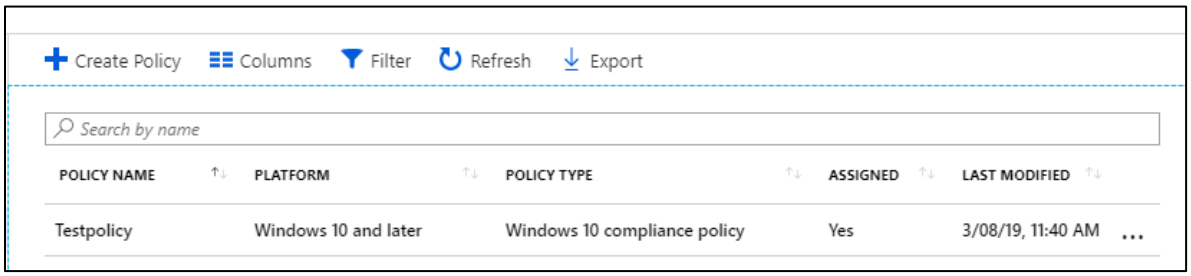


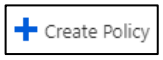

Her setter man ulike krav som enhetene må oppfylle før de kan brukes på bedriftens tjenester og/eller nettverk.

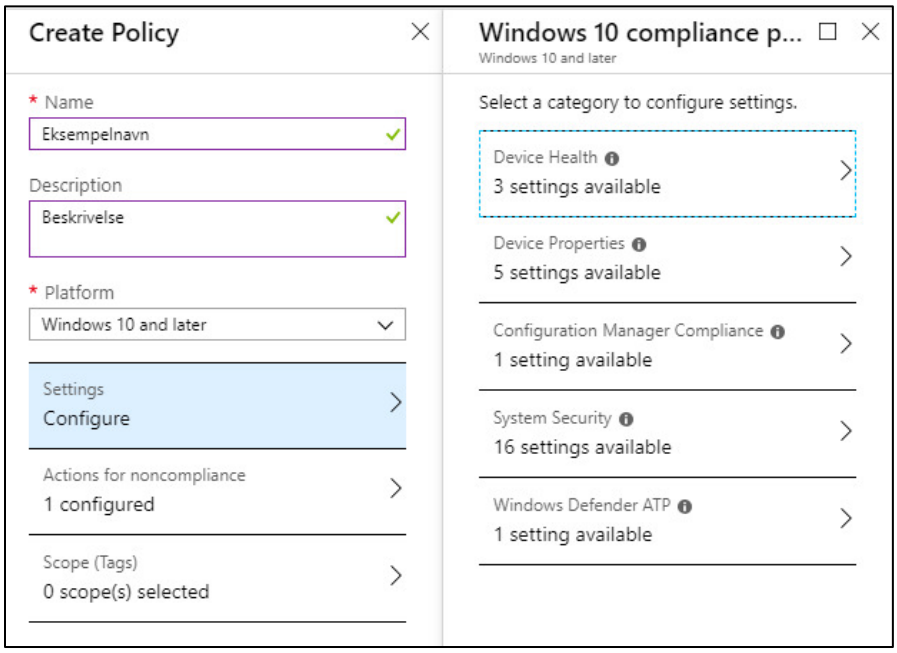
De alternativene vi har under her er:

- Policies - her setter man de ulike kravene som stilles for at en enhet skal kunne bruke ressurser i organisasjonen
- Notifications – et verktøy for å sende ut meldinger til en gruppe basert på handlinger
- Locations – per dags dato: nettverk som man kan bruke som «godkjente» soner for om en enhet skal oppfylle policy

## Policies




Her kan man se de ulike *policy-ene* som allerede er opprettet.
Vi oppretter en policy ved å trykke 


Under oppretting av policy har man noen valg:

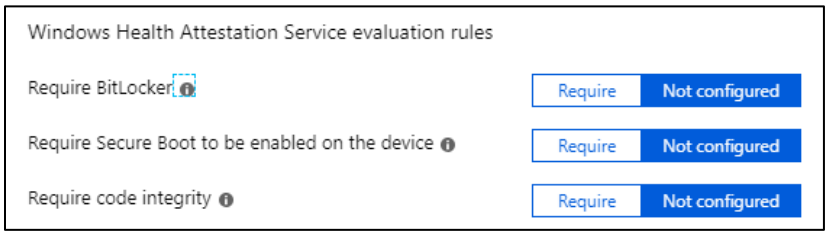
- Navn og beskrivelse

Under *Platform* får man valget mellom ulike enheter/OS

- Vi skal bruke Windows 10 og velger dette

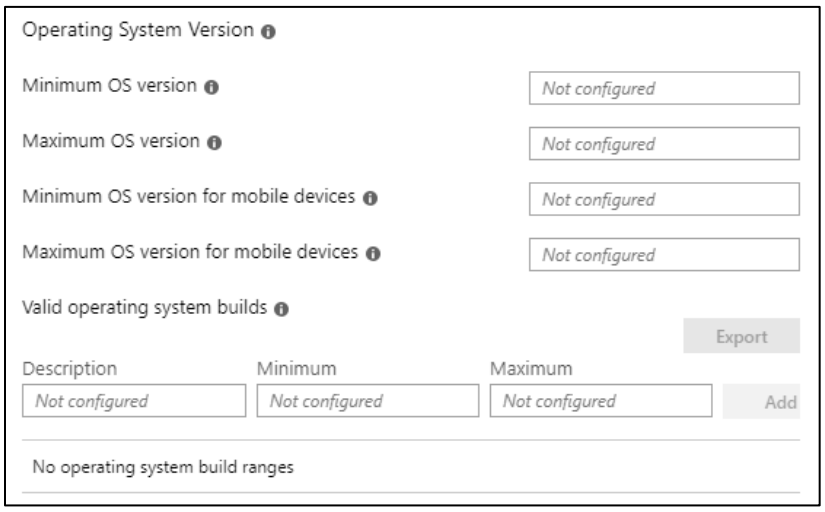
Under Settings får vi opp endel alternativ som vi skal ta for oss nedenfor.

### *Device Health*




Her kan man sette krav til *BitLocker* (kryptering), *Secure Boot* og *code integrity*.

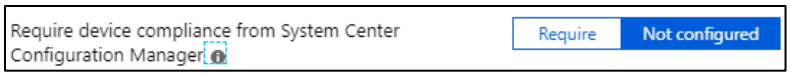
### *Device Properties*




Her kan man velge minste og høyeste versjon av Windows som blir satt som compliant.

- Dette kan være greit for å stenge ute maskiner som ikke får oppdatert seg til nyeste versjon (sikkerhetsoppdateringer)

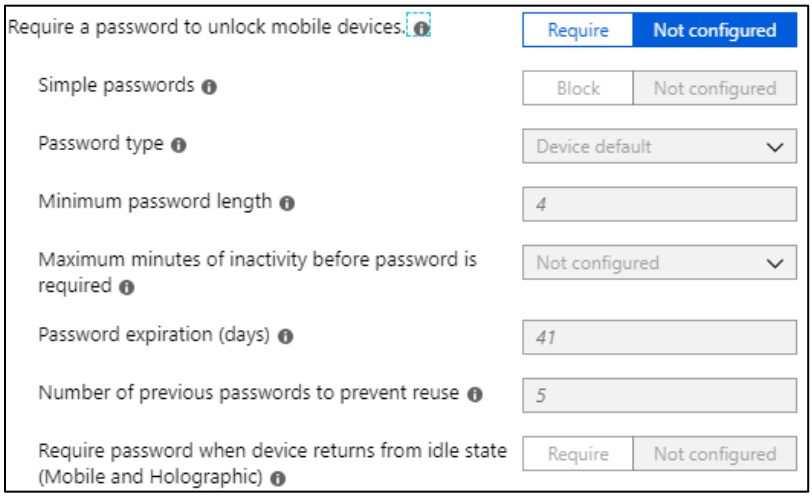
### *Configuration Manager Compliance*




Hvis man også bruker SCCM kan man kreve at enheten også er merket som compliant her.

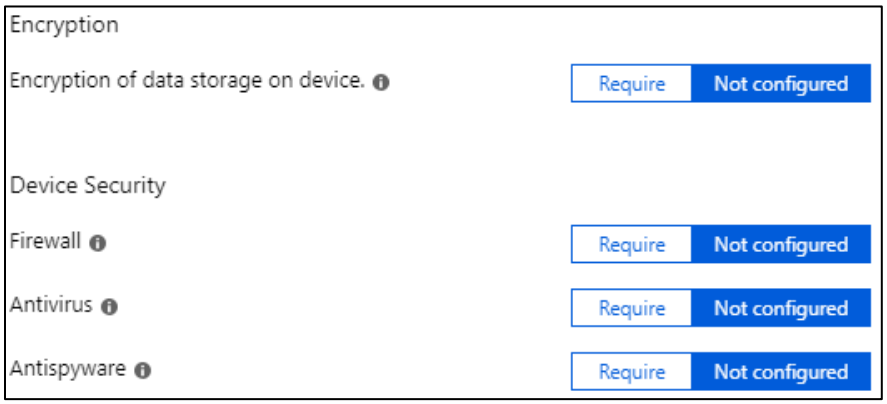
### *System Security*

Her kan man sette hvilke krav man har til passord:

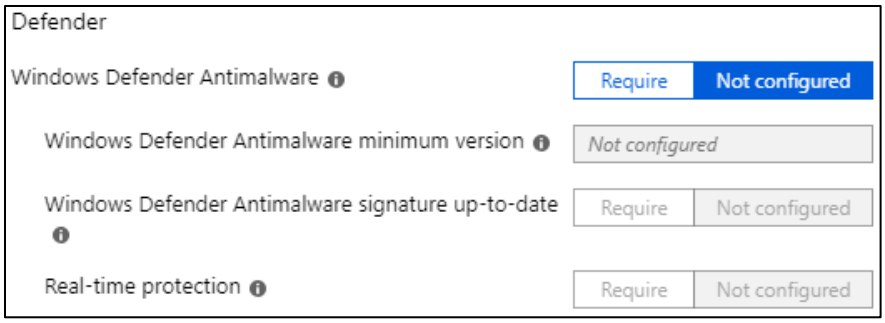



- *Simple passwords* betyr enkle passord slik som «1234» eller «1111» etc.
- Password type betyr om man krever passord med tall OG bokstaver, eventuelt standard-policy på enheten
- Lengde på passordet
- Hvor lenge maskinen kan stå ulåst før den må låses opp
- Hvor lenge passordet kan forbli aktivt
- Hvor mange tidligere passord som ikke kan bli brukt om igjen
- Det siste kravet går på om enheten krever passord for når den våkner fra eks. standby

Videre kan det stilles krav til hvorvidt enheten skal ha:

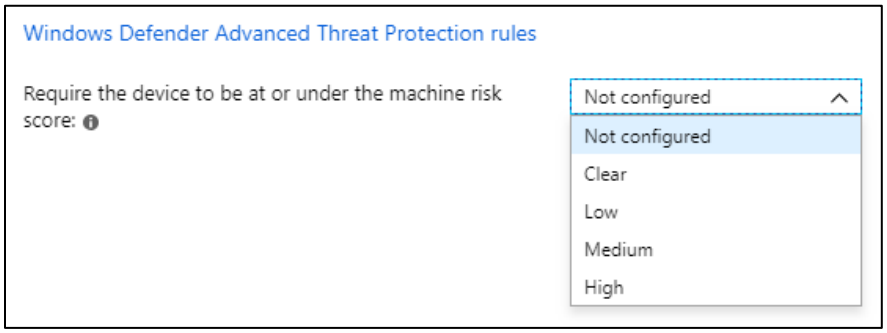



- Kryptering av lagringsmedier tilknyttet maskinen
- Brannmur aktivert
- Antivirus (som er kompatibelt med Windows Security Center)
- Anti-Spyware (som er kompatibelt med Windows Security Center




Her kan man sette krav til Windows Defender:

- Minste versjon
- Oppdatert database
- Sanntidsbeskyttelse



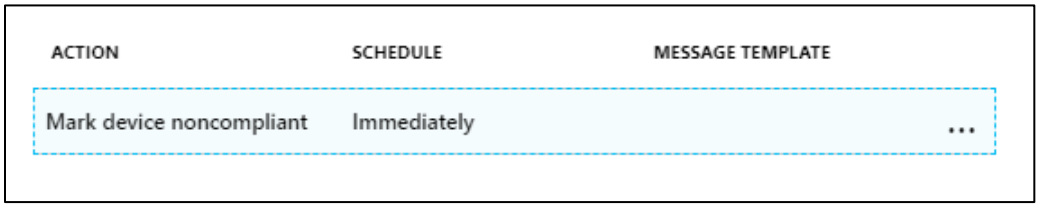

De siste alternativene gjelder mest hvis man har Windows Defender med ATP (Advanced Threat Protection)

Dette går ut på om enheten må ha en viss score for å kunne bli compliant.

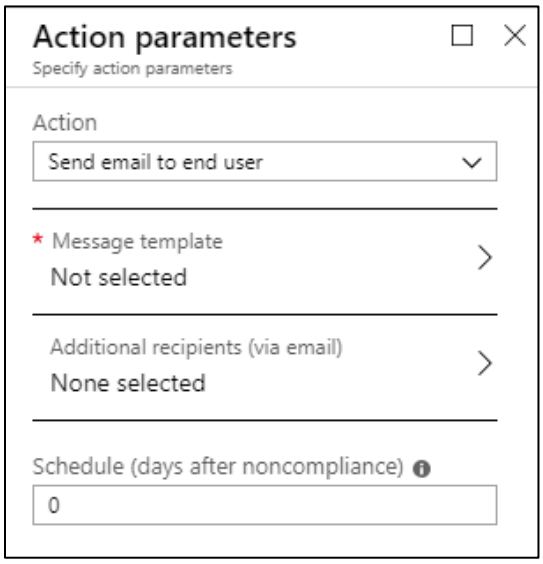
Når man har satt alt som ønsket kan man trykke *OK.*

- *Hvis en enhet ikke lenger oppfyller de nevnte kravene blir den merket som noncompliant*

Under *Actions for noncompliance* kan man sette noen handlinger som tres i kraft så snart en enhet ikke lenger er compliant.




Et eksempel på dette er over, hvor man kan definere en Message Template, som vi skal forklare senere.




Man kan også legge til flere mottakere som varsles når en enhet blir «*noncompliant*».

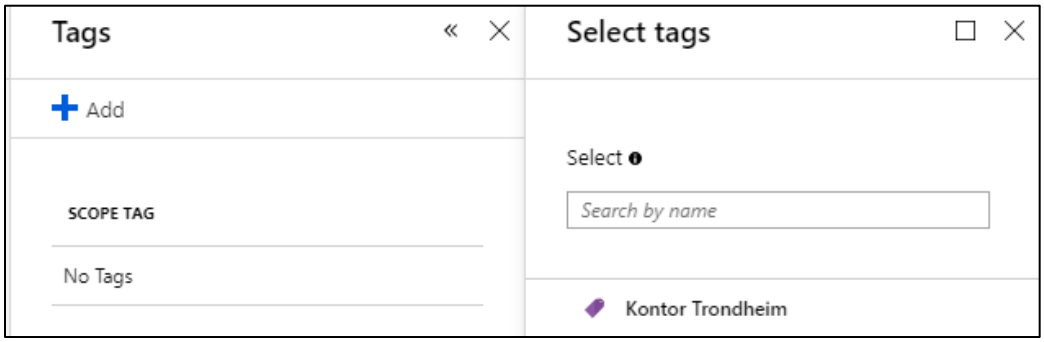
Dette defineres ved hjelp av bruker-grupper.

### *Scope Tags*

Videre kan man legge inn en *scope tag* der denne policyen gjelder

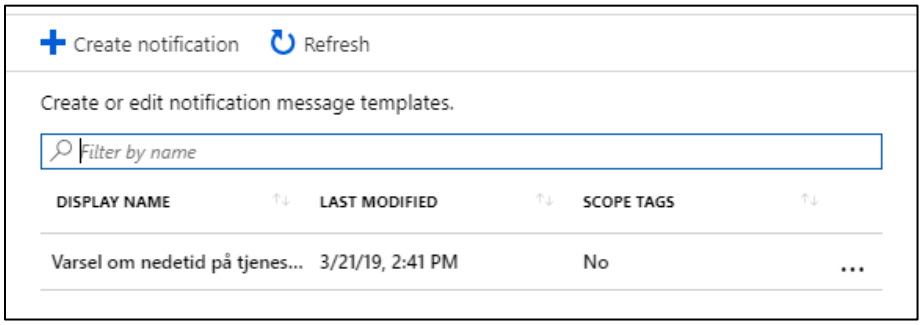
- Scope tags er noe man definerer i Intune-portalen under *Roles* og *Scope (Tags)*
- Scope tags benyttes **kun** som en indikator – de faktiske endringene vil kun skje via tilegning mot bruker-/enhets-grupper

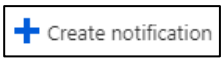
Når man så har definert *scope tags* kan man trykke *Create***.**

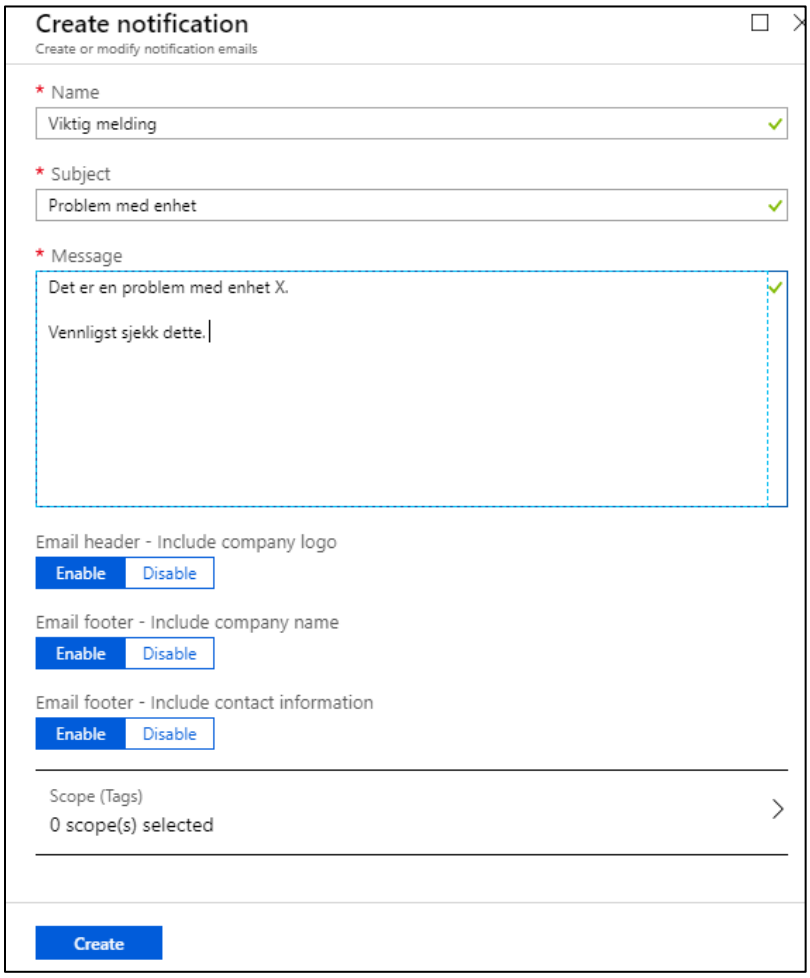



**Policyen er nå opprettet og tildelt en gruppe.**

### *Notifications (message templates)*




Her kan man lage meldinger som sendes ut f.eks. hvis en enhet ikke lenger oppfyller de gitte kravene. For å lage en slik *notification* trykker man på 


Her har man noen alternativer:

- Navn, emne og melding

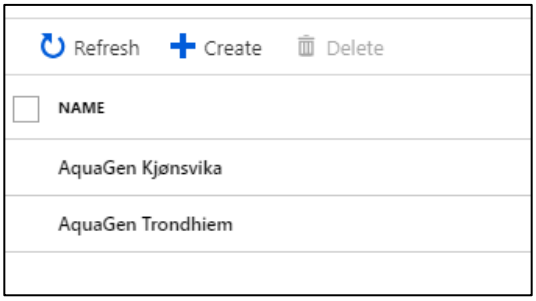
Videre kan man velge om man vil legge inn logo, navn og kontaktinformasjon for bedriften i meldingen.

Man kan også her definere *Scope (Tags)* for å velge hvem meldingen gjelder.

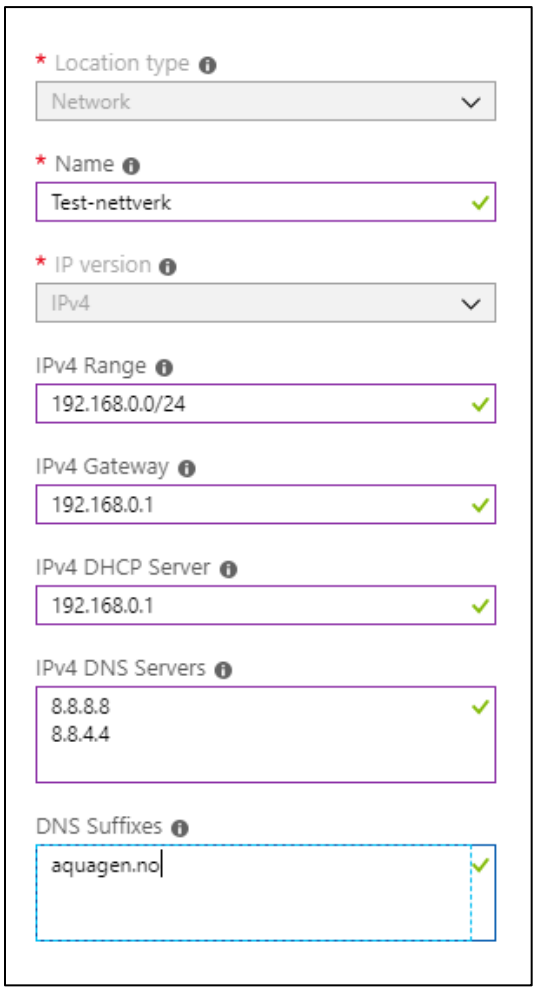
Trykker *Create* og malen blir så opprettet.

## Locations

Man har også mulighet til å opprette en liste med godkjente nettverk, såkalte *locations* (sted) hvor en enhet kan sies å være *compliant*




Trykker på **Create**




Under vises noen alternativer

For øyeblikket er det ikke mulig å endre *Location type* eller *IP version.*

- Vi antar at det blir mulig å bytte til IPv6 adresser ved en senere anledning

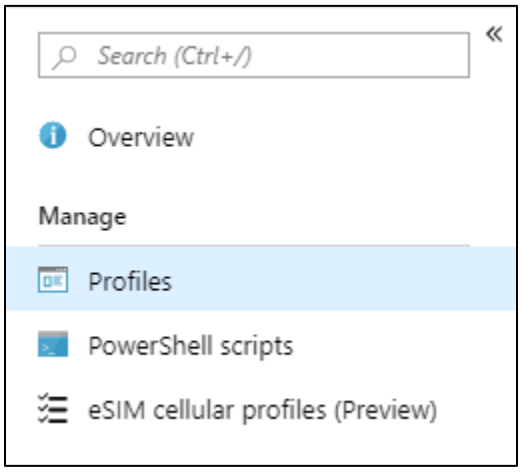
Videre kan man sette blant annet:

- IP-range for nettverket
- Gateway for nettverket
- DHCP-server i nettverket
- DNS-servere i nettverket
- Eventuelt også DNS-navn i nettverket

Trykk på Create for å opprette lokasjonen.

**En ny lokasjon (nettverk) er nå opprettet og kan brukes for å lage en policy.**

## Device configuration

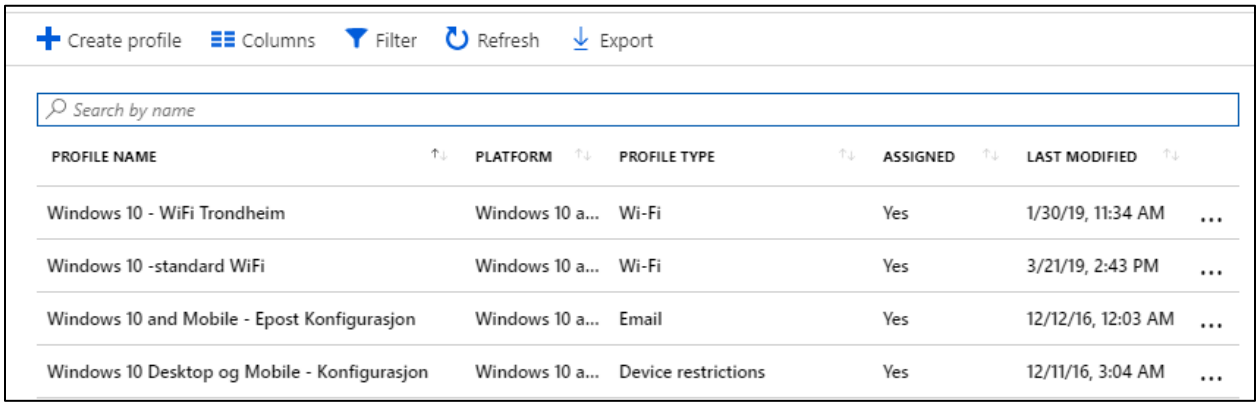



Device configuration har ganske få undermenyer, men det er i all hovedsak *Profiles* som vi skal se på her.

*Profiles* er ganske omfattende, og inneholder mye funksjonalitet som beskrevet nedenfor.

eSIM er ikke relevant for dette prosjektet, men PowerShell scripts kan bli nyttig på et senere tidspunkt.

## Profiles



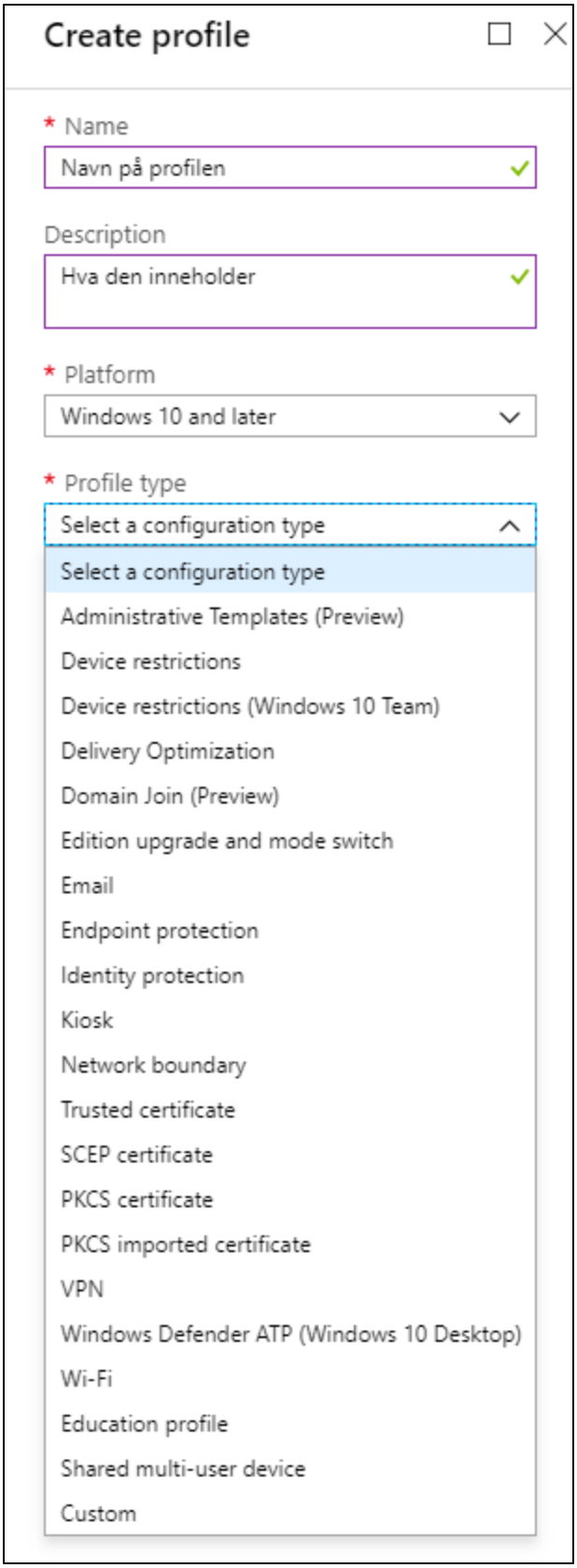

Disse profilene brukes til å sette ulike innstillinger på en enhet.

- Dette kan være alt fra hvilke WiFi-nettverk som enheten skal koble seg opp til, hvordan Windows skal motta oppdateringer og hvilken data som kan deles og ikke.

Man har altså mulighet til å både få og begrense tilgang til store deler av enheten her, samt konfigurere oppsett av en enhet som kiosk-maskin, delt enhet etc.

Som vist over er det allerede opprettet noen profiler for WiFi-nettverk, e-post og en generell konfigurasjon. Det står også hvilken plattform disse gjelder, hvilken type profil dette er, hvorvidt den er tilegnet til en enhet/gruppe og når den sist ble endret.

Vi trykker på  for å opprette en profil



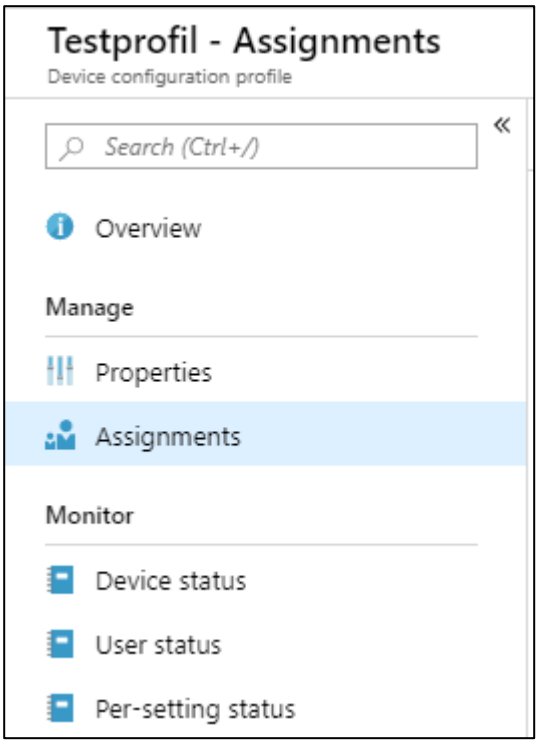

Når man skal opprette en profil trengs det noen hovedelementer

- Navn og beskrivelse
- Platform

Når det kommer til type er det mange valg å velge mellom. I utgangspunktet har man tilgang til nesten alle innstillinger i Windows fra denne menyen

Ikke alle disse typene av profil er relevante for prosjektet, men her beskrives noen som kan tenkes å bli brukt:

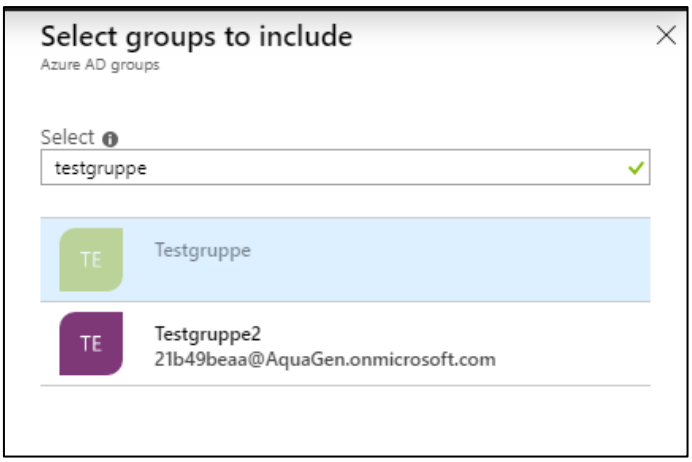
- Device restrictions – begrenser hva som kan brukes på enheten
- Delivery Optimization – brukt for å sette egne rutiner rundt oppdateringer
- Domain Join – bli med i et domene
- Edition upgrade / mode switch – oppgradere til en større oppgave av Windows
- Email – e-post innstillinger
- Endpoint protection – innstillinger for antivirus-programvare fra Microsoft
- Kiosk – sette opp ett spesifikt bruksområde for enheten, eks. infoskjerm eller offentlig PC
- Network boundary – begrense hvilke nettverk enheten kan brukes i
- VPN – sette opp en VPN som kan brukes på enheten
- Wi-Fi – definere nøkkel på nettverk
- Shared multi-user-device – enhet for flere brukere, kan f.eks. la enheten slette all data hver gang den startes på nytt




Når profilene er opprettet kan man tilegne den til en datamaskin ved å trykke på *Assignments*

Det vil være noe forskjell mellom innstillingene på hver profil, men tilegningen av gruppe er lik for alle.

Her søker man opp gruppen man vil at profilen skal gjelde for, og trykker *Select* på den eller de valgte gruppene.




**Profilen er nå opprettet og tilegnet gruppen Testgruppe.**

## Fase 2: Klargjøring av enheter

For å starte utrulling ved hjelp av Autopilot, er man nødt til at få maskinene inn i installasjonsveiviseren på nytt. Dette gjøres raskest ved å starte opp en ny installasjon av Windows.

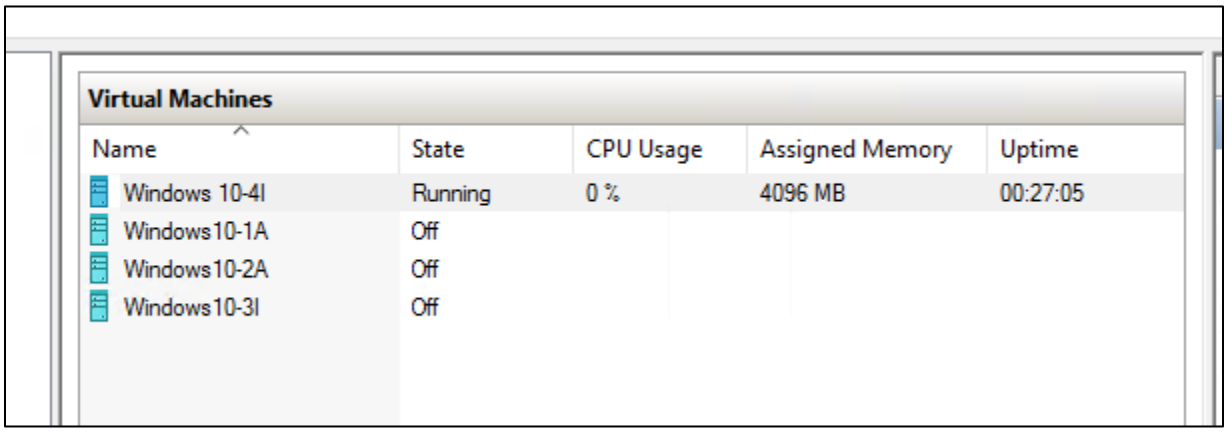
I praksis kan man også resette eksisterende maskiner, men på grunn av dårlig erfaring med denne framgangsmåten velger man her heller å reinstallere for å sikre jevnt resultat.

- **Det skal nevnes at eksisterende maskiner også kan legges inn i Intune uten Autopilot. Dette vil man gå gjennom i fase 4.**

Denne demonstrasjonen vil først foregå i et virtuelt miljø. Dette fordi det er enklere å teste ulike konfigurasjoner uten å ha flere fysiske enheter tilgjengelig.

Enkelte funksjoner i Autopilot krever fortsatt fysiske maskiner for å virke. Noen funksjoner vil derfor bli utprøvd på fysiske maskiner for å demonstrere denne funksjonaliteten.

Vi kjører en Hyper-V host i en VM fra Azure. På denne har vi flere virtuelle maskiner som brukes til testing.




Her er noen maskiner som har blitt opprettet.
De kjører en evaluation-utgave av **Windows 10 Enterprise.**

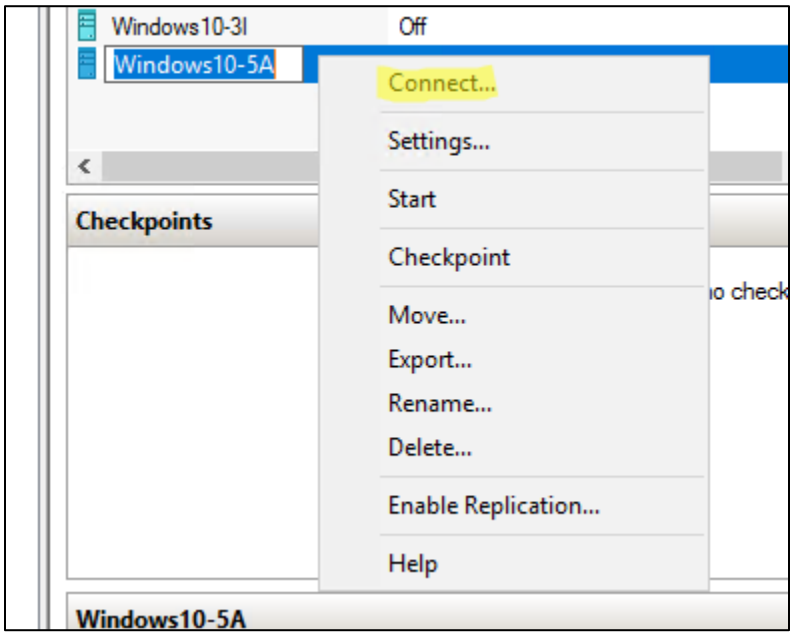
Vi har to forskjellige typer maskiner som vi setter opp. Felles for dem begge er at de skal inn i Intune, men det er et par forskjellige måter å gjøre dette på.

- **Autopilot-enheter** – disse har fått installert Windows, men vi har stoppet installasjonsprosessen for å hente ut maskinvare-ID for å rulle ut disse ved hjelp av Autopilot
    - Disse skal simulerer nye enheter som organisasjonen har fått tak i.
    - Ved å pause installasjonsprosessen slipper vi å senere måtte resette enhetene for at Autopilot skal virke
    - Windows **10-1A** og **10-2A** er eksempelvis Autopilot-enheter her
- **Intune-enheter** – disse har fått installert ferdig Windows, og kommer til å bli lagt inn i Intune på en manuell måte.
    - Disse skal simulere enheter som allerede finnes i organisasjonen og som ikke trenger å bli reinstallert.
    - Windows **10-3I** og **10-4I** er eksempelvis Intune-enheter her

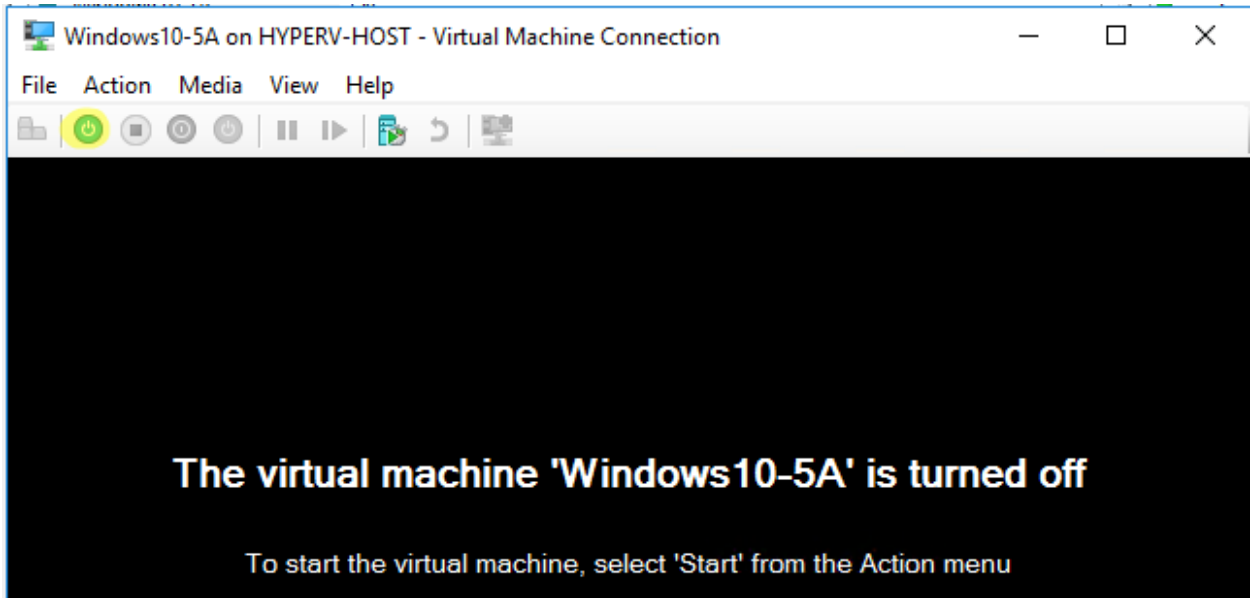
I klargjøringen av Autopilot-enheter starter vi med en tom virtuell maskin der vi vil installere Windows 10 Enterprise fra start.

For en fysisk maskin er denne prosessen tilsvarende, foruten det ekstra laget mellom bruker og maskin.

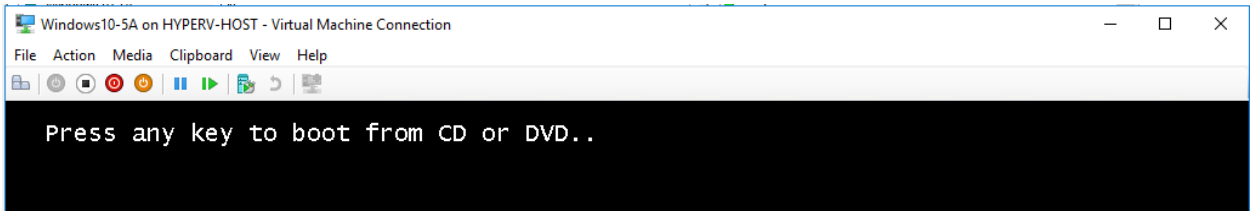
Vi skal ikke bruke lang tid på å beskrive prosessen ved å installere Windows, men beskriver noe rundt Hyper-V og virtualiseringsmiljøet.



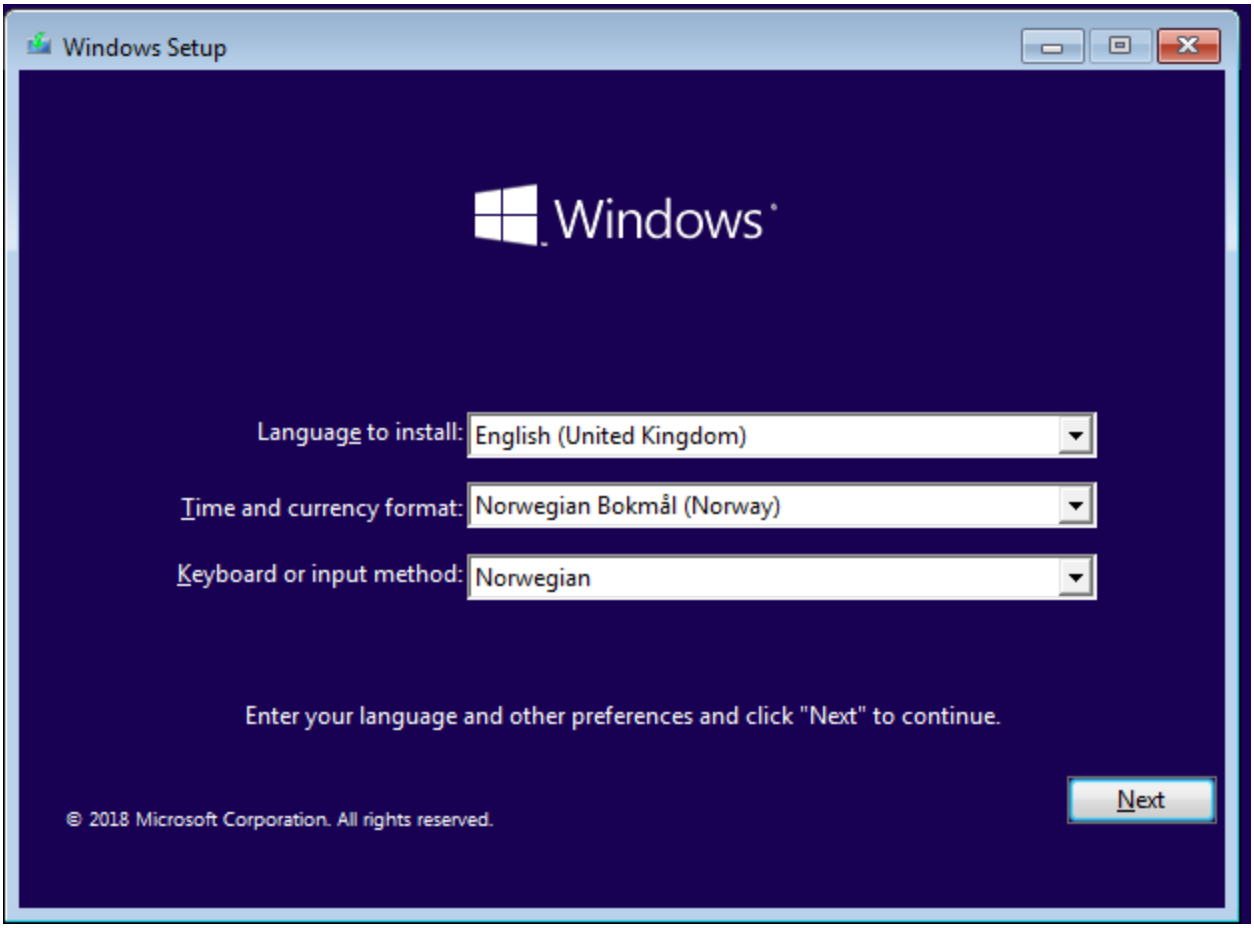

Vi starter med å koble oss til den nye VM-en.




Vi starter VM-en ved å trykke på den markerte knappen.

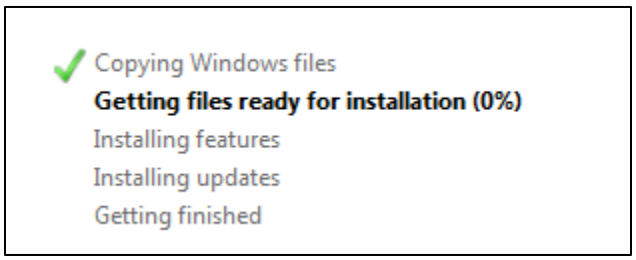



Trykker en tast for å få maskinen til å laste fra installasjonsmediet til Windows.

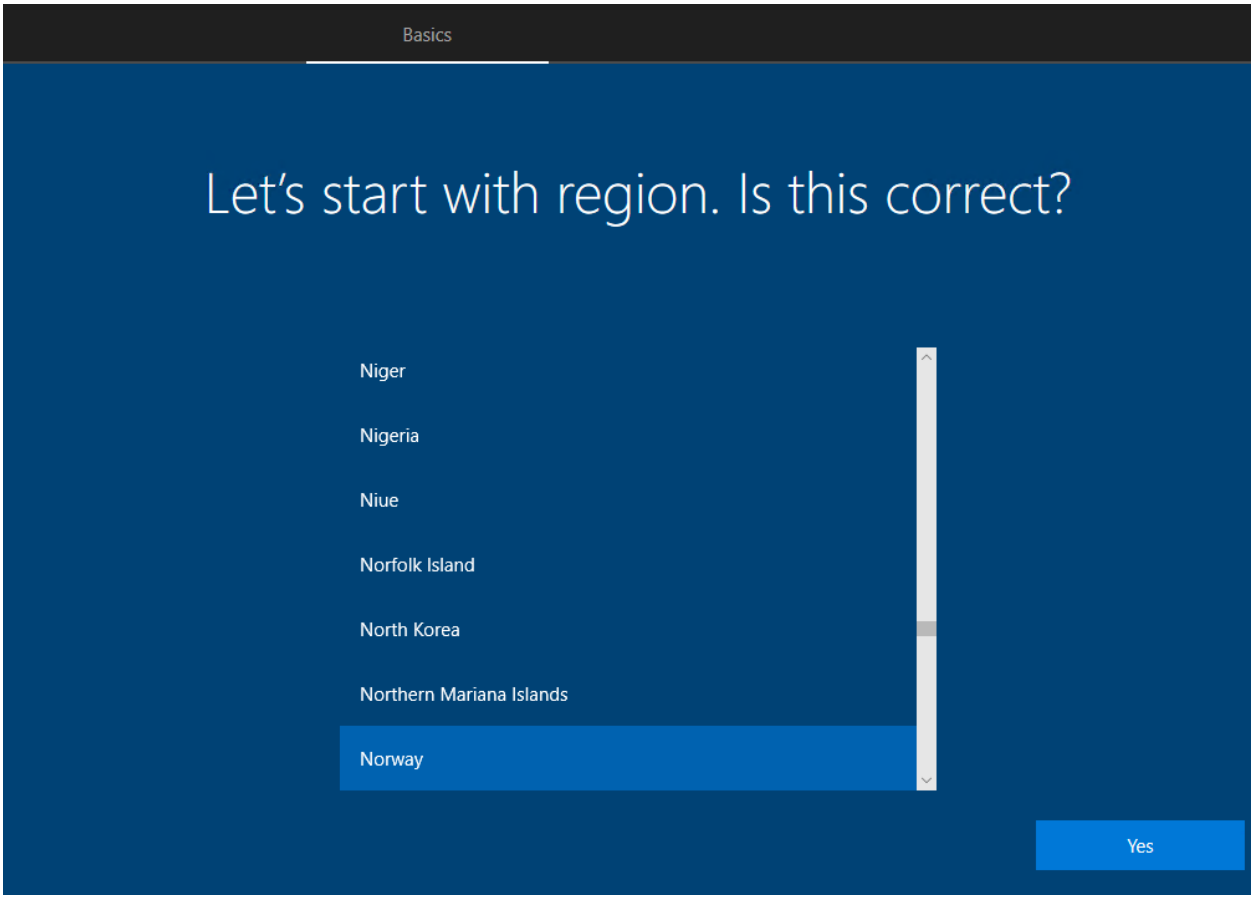



Velger språk her, trykker *Next*
Ellers går man gjennom installasjonsprosessen på vanlig måte.

- For vanlige utgaver av Windows må man kanskje ha en produktnøkkel. Siden vi kjører en evaluation-utgave trenger vi ikke dette her.



Når enheten har startet om blir man møtt med dette bildet.




**Hvis man skal sette opp maskinen på vanlig måte og senere legge den inn i Intune, går man nå fram og lager bruker som man ellers ville ha gjort.**

Vi fortsetter nå med fase 3 der vi skal se på hvordan man henter ut og importerer maskinvare-ID fra maskinene til bruk i Windows Autopilot.

# Fase 3: Uthenting og importering av maskinvare-ID i Autopilot

## Uthenting av maskinvare-ID

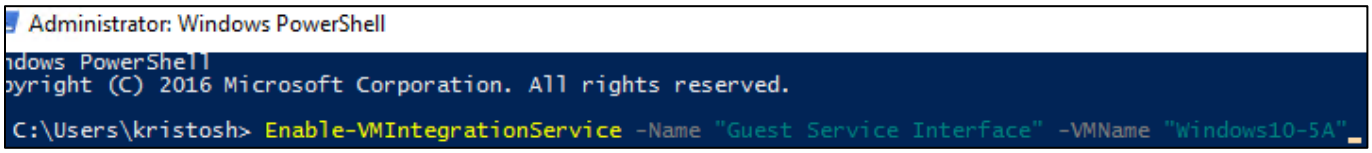
Dette gjøres med et Powershell-script som leser ut denne nøkkelen fra systemet. Filen som blir lagret er en CSV-fil.

Hvordan dette scriptet flyttes inn og nøkkelen hentes ut er mye avhengig av maskinen som brukes. Er det en fysisk maskin vil det enkleste være å bruke en minnepenn. Vi bruker i dette tilfellet en virtuell maskin gjennom Hyper-V og må derfor gjennom noen omveier for å hente inn, samt lese ut filene.

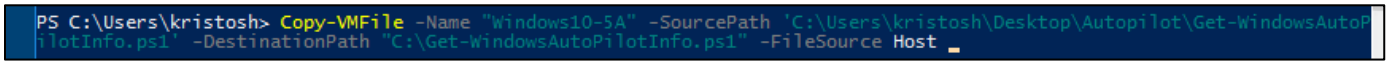
For å overføre filen benytter vi oss av en funksjon som heter *Copy-VMFile*.

For at dette skal virke må vi først skru på *VMIntegrationService* på den VM-en vi skal laste inn filen til. Dette gjøres via et Powershell-skall på maskinen som hoster de virtuelle maskinene, altså Hyper-V hosten

- En «host» er en maskin med ressurser som de virtuelle maskinene igjen benytter seg av

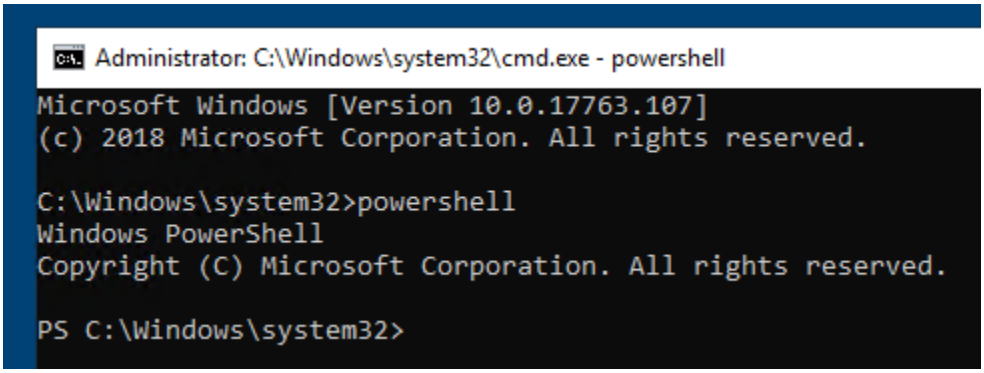



I neste steg utfører vi kommandoen som kopierer **filene fra hosten**. Her spesifiserer vi navn på VM vi ønsker å **kopiere til**, hvor filen befinner seg og hvor vi ønsker at den skal bli kopiert på den aktuelle maskinen.




Nå kan man gå tilbake til enheten som man skal hente ut maskinvare-ID fra.

Når man er på det første bildet av installasjons-veiviseren trykker man *Shift + F10.* Man får da opp en kommandolinje (CMD) på skjermen




Vi skriver *powershell* her og trykker Enter. Vi er nå i et Powershell-vindu.

- For at vi skal få kjørt scriptet er vi nødt til å endre *ExecutionPolicy.* Dette bestemmer hvilke typer script som er tillatt å kjøre på maskinen.

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
PS C:\Windows\system32> _
```

Siden vi flyttet filen til *C:* navigerer vi oss hit. Som vi ser med kommandoen *ls* ligger scriptet her.

```
PS C:\Windows\system32> cd c:\
PS C:\> ls


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        15.09.2018     09:33                PerfLogs
d-r---        04.04.2019     12:10                Program Files
d-r---        15.09.2018     19:33                Program Files (x86)
d-r---        04.04.2019     12:15                Users
d-----        04.04.2019     12:16                Windows
-a----        04.04.2019     12:31           5656 Get-WindowsAutoPilotInfo.ps1
```

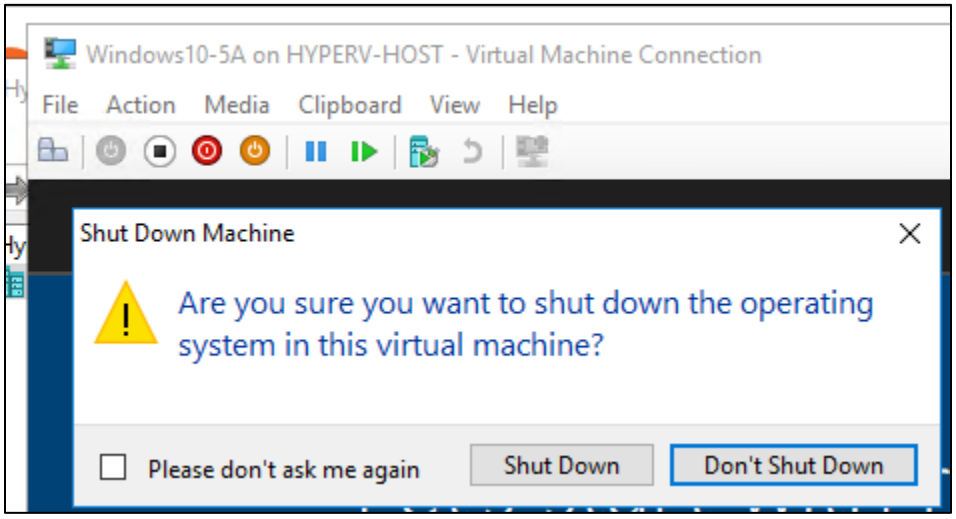
Vi kjører nå scriptet og legger utdata i filen windows10-5a.csv i samme mappe (C:\)

```
PS C:\> .\Get-WindowsAutoPilotInfo.ps1 -OutputFile windows10-5a.csv
PS C:\> _
```

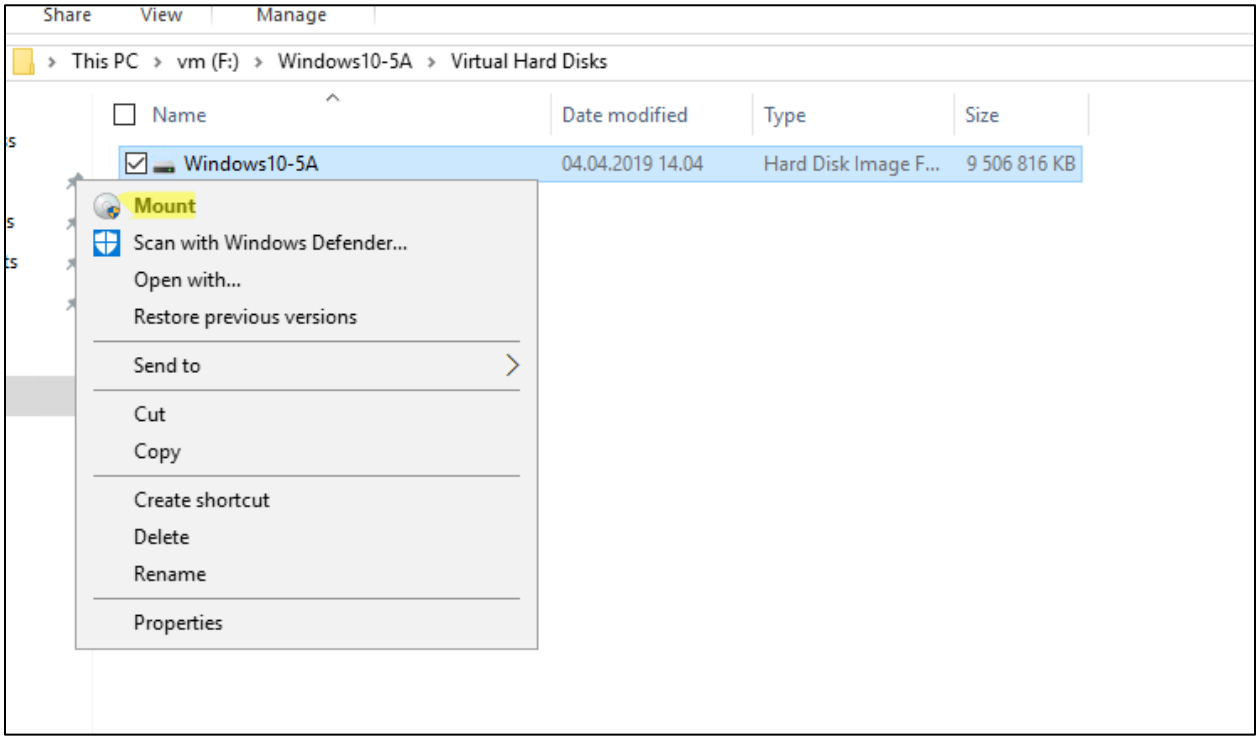
Vi har nå fått ut maskinvare-ID fra enheten og kan nå hente ut denne.

- Siden vi ikke har direkte tilgang til maskinen går vi inn i filsystemet på den direkte for å hente ut fila.
- Med fysiske maskiner henter man dette ut med minnepenn, en betydelig enklere prosess

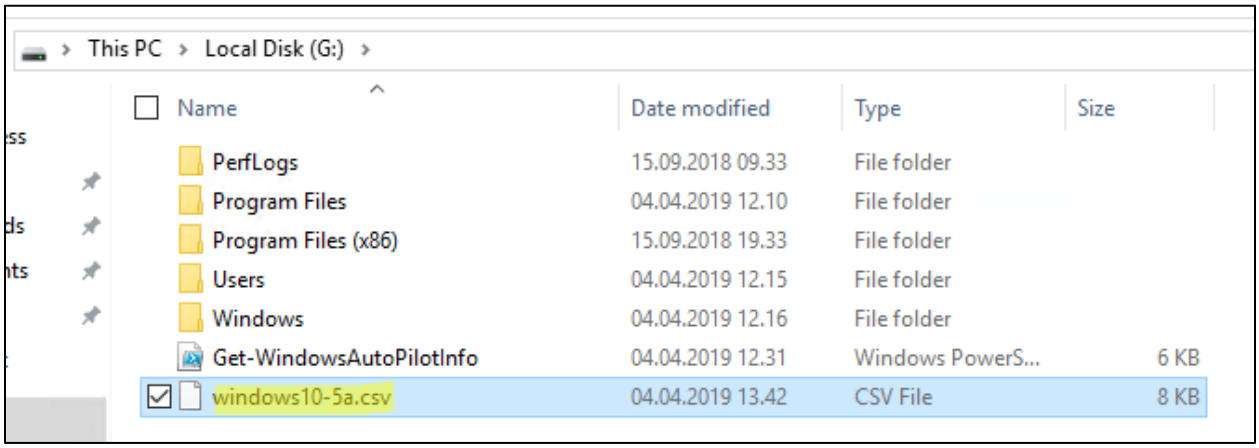
Vi begynner med å skru av maskinen i Hyper-V Manager.



Vi finner så hvor harddiskfilen til maskinen er plassert på hosten, høyreklikker på denne og trykker *Mount*




Vi navigerer oss inn på disken og ser nå at filen ligger her, der den ble opprettet på den virtuelle maskinen.

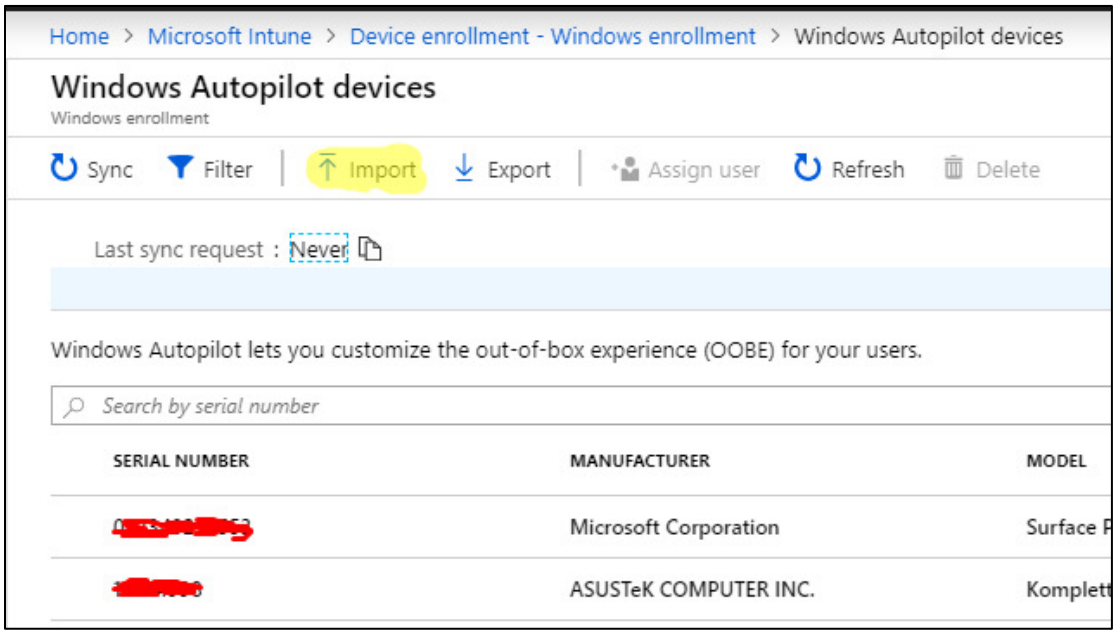



**Vi flytter så filen til en fornuftig plass på maskinen og bruker den videre når vi skal importere maskinen i Autopilot.**

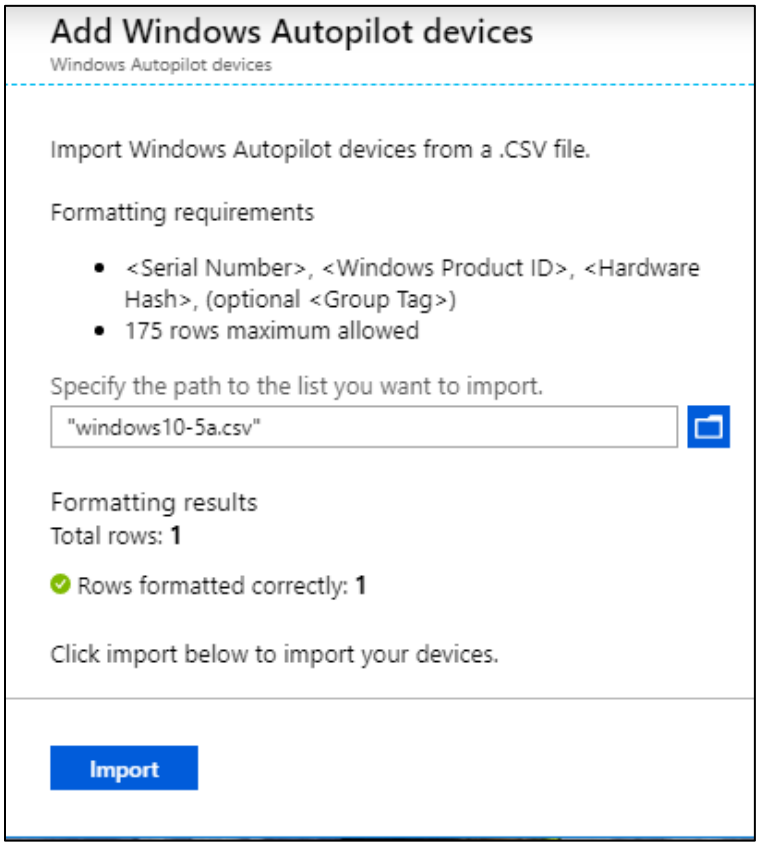
## Importering i Windows Autopilot

Nå som vi har fått tak i maskinvare-ID fra enheten, kan vi nå importere denne inn i Windows Autopilot.

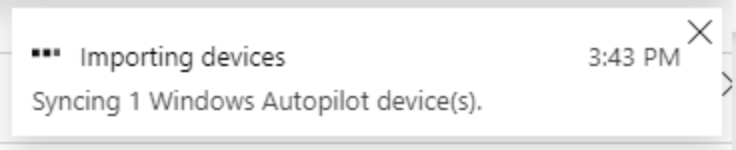
Denne finner vi Intune-delen av Azure Portalen.



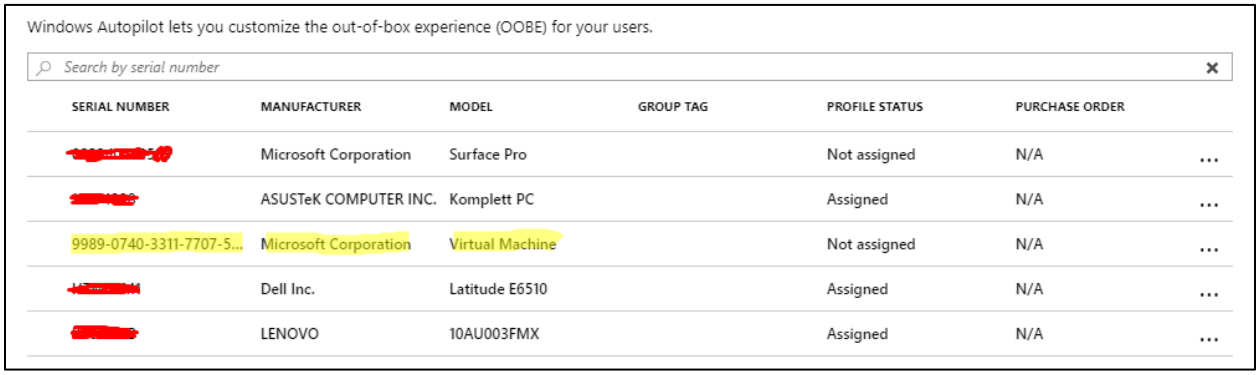

Vi trykker på Import for å importere en ny enhet




Vi velger her filen vi lagde på den virtuelle maskinen og trykker på *Import*.




Autopilot vil nå begynne å importere enheten. Hvis man importerer flere enheter kan dette ta litt tid.




**Enheten har nå blitt importert i Microsoft Autopilot og kan nå tilegnes profiler og andre innstillinger.**

- Siden enheten enda ikke har blitt installert enda slipper vi å resette den for å teste Autopilot senere.

## Fase 4: Importering av eksisterende enheter i Intune og AD

Hvis man har en rekke med Windows 10-enheter som allerede er konfigurert og satt opp som ønsket, blir det kanskje sett på som unødvendig å gå gjennom stegene for å importere dem i Autopilot.

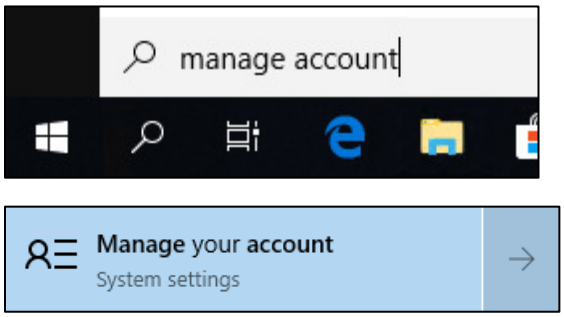
For at vi skal få lagt inn brukeren i Intune må vi sørge for at brukeren som benyttes enten er i en gruppe som er tilknyttet *Automatic Enrollment* eller at *Automatic Enrollment* er satt til å gjelde alle enheter i organisasjonen. I praksis vil man sette dette til å gjelde alle brukere, men i denne demonstrasjonen setter vi den aktuelle brukeren i en aktiv gruppe som eksempel.

I dette steget får man to måter å legge inn en enhet i domenet

1. **Kobling til AD + MDM** – dette vil melde inn enheten i AD samt MDM i Intune – dette muliggjør at brukeren kan logge seg på maskinen med sin egen AD-bruker. Hvis man skal tilegne programvare til bruker-grupper er man nødt til å logge inn ved hjelp av AD-bruker
2. **Enrol only in device management** – dette vil kun melde enheten inn i MDM hos Intune – dette betyr at man fortsatt benytter sin lokale bruker på maskinen og derfor ikke får all programvaren som er tilegnet AD-brukeren. Maskinen vil likevel hente policyer og enkelte konfigurasjoner, men man får noe begrenset funksjonalitet i forhold til det første valget.

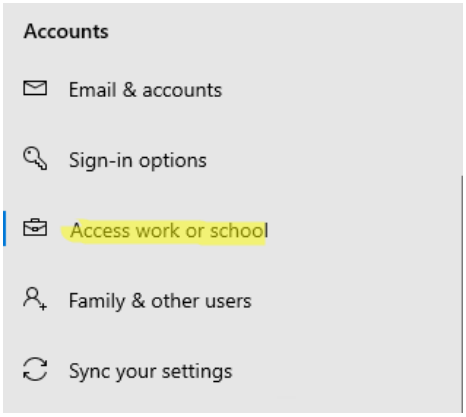
Framgangsmåten for de to metodene er ganske like - vi beskriver dem fortløpende her uansett

Vi starter med en ferdig satt opp maskin, men som ellers **ikke** er del av noe domene/MDM.




Vi starter med å gå inn på *Manage your account* ved å søke opp dette i Windows sin startmeny.

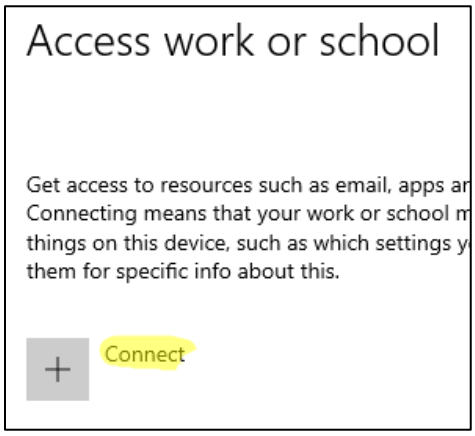
Dette finnes også under *Windows-settings* og *Accounts*




Vi går deretter inn på *Access work or school*.

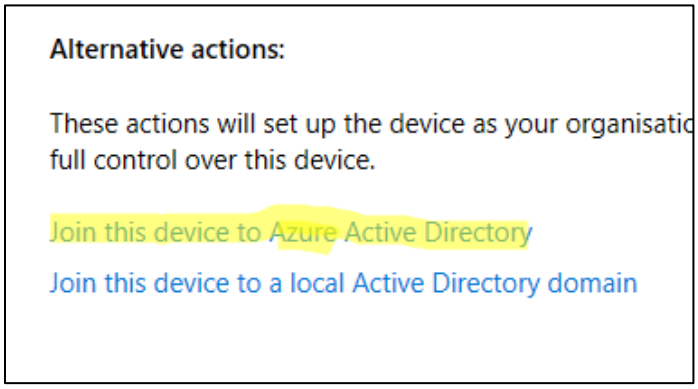
## AD + MDM kobling

Hvis man skal legge inn maskinen med AD + MDM er man nødt til å trykke på den øverste knappen med navnet *Connect*

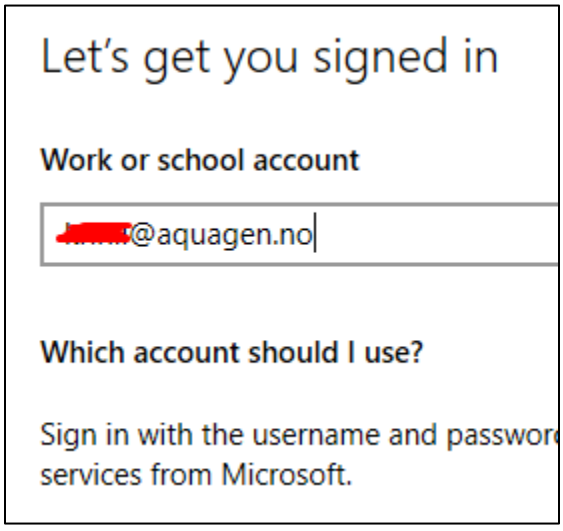



Man får så opp et vindu der man har noen valg på bunnen. Her trykker vi på

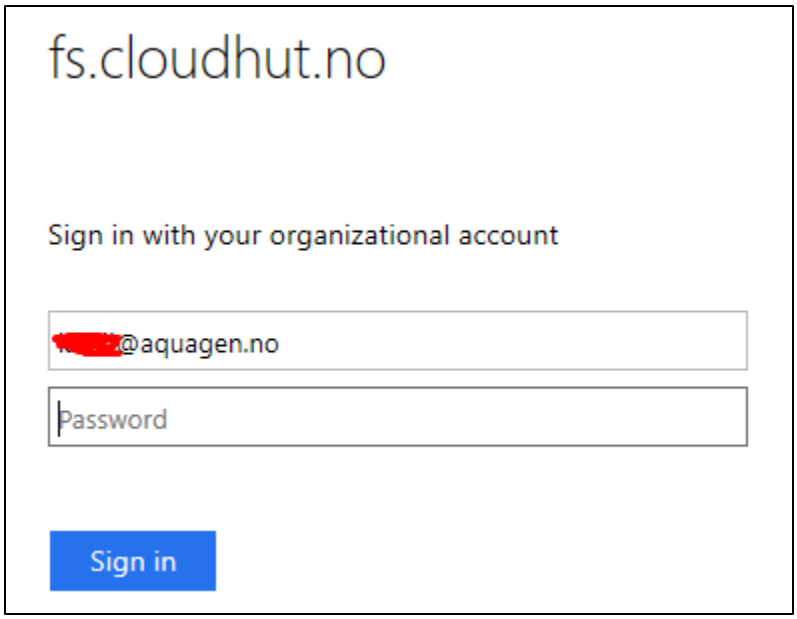
*Join this device to Azure Active Directory*



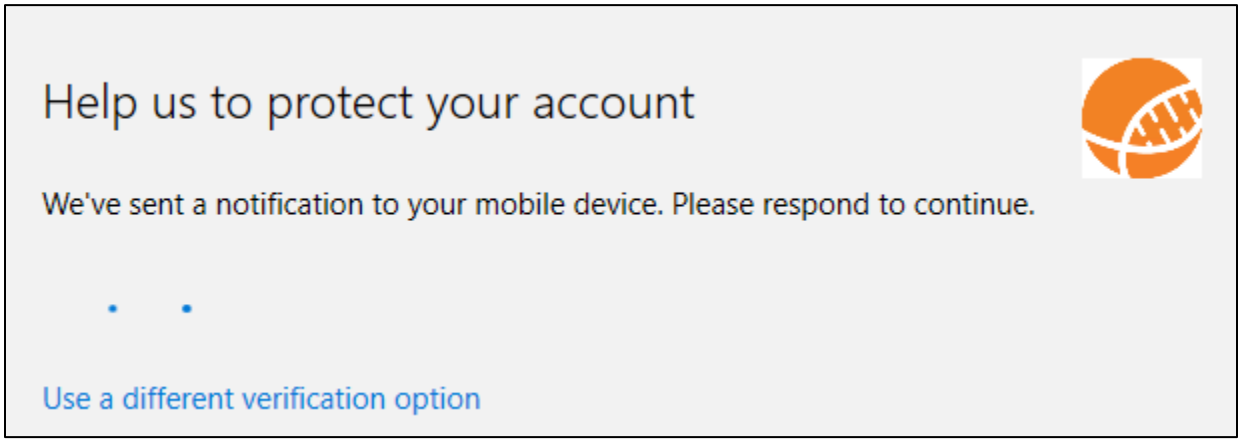

Skriver inn brukernavn som man logger inn med ellers



Blir så sendt til påloggingsvinduet for organisasjonen

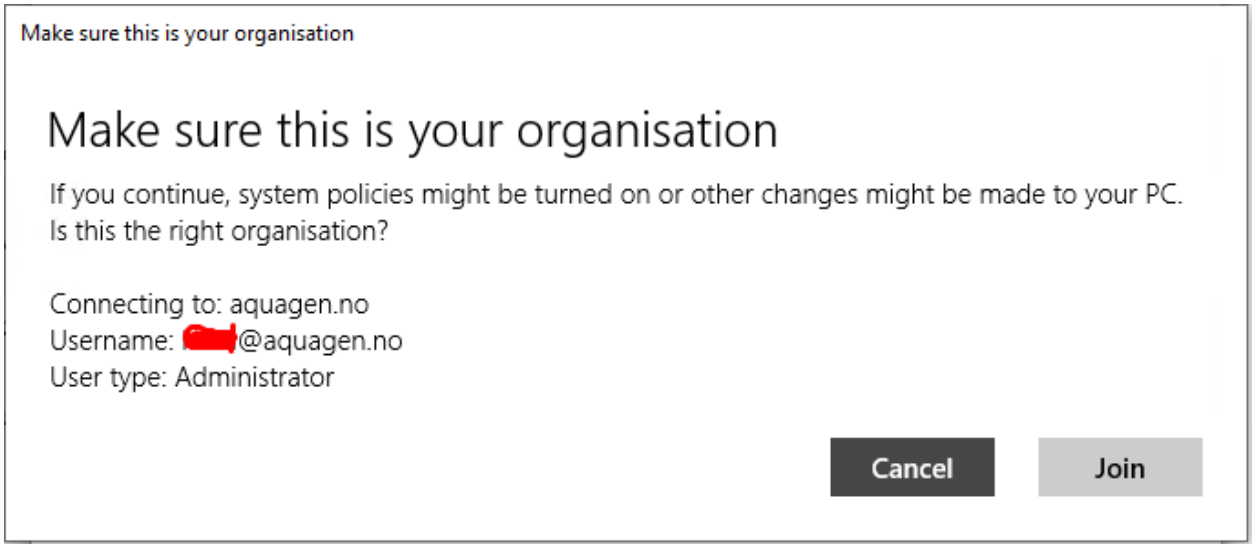



Har man to-faktor autentisering vil man måtte identifisere seg

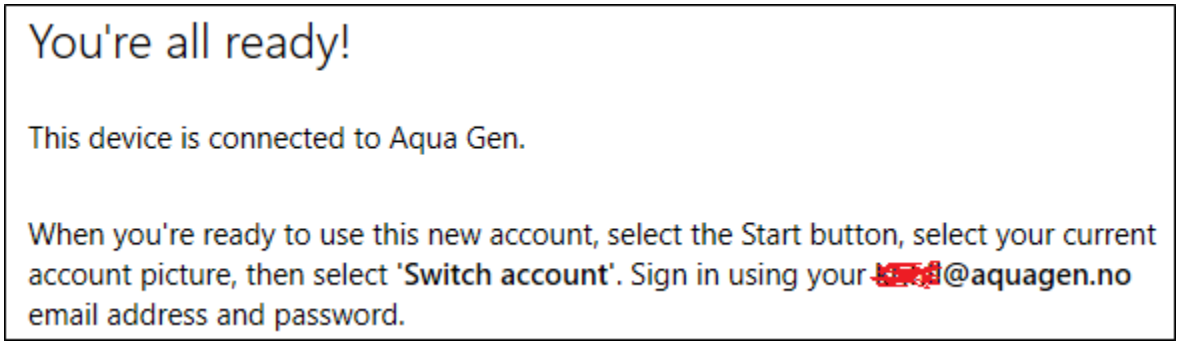



Må vente litt for at enheten skal hente ned nødvendig informasjon fra Intune/Azure AD

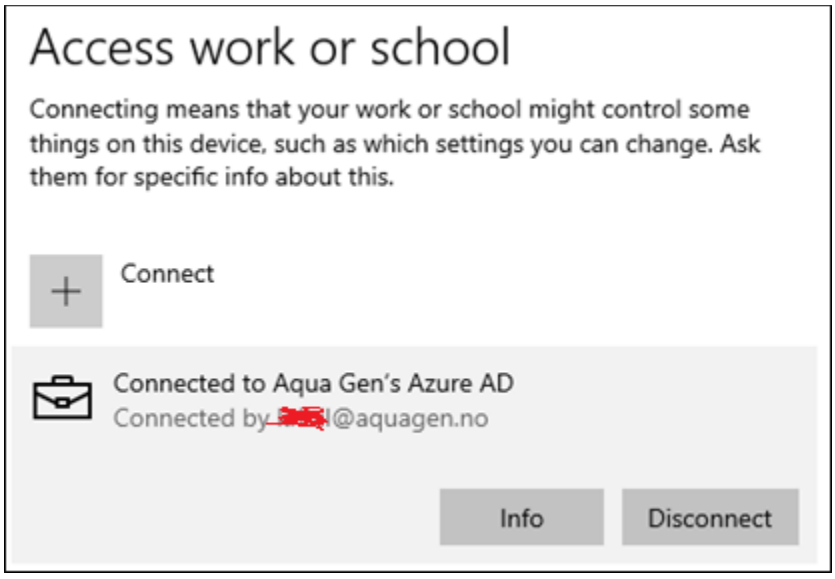
Enheten vil så spørre om man virkelig vil koble seg opp. Vi trykker *Join*



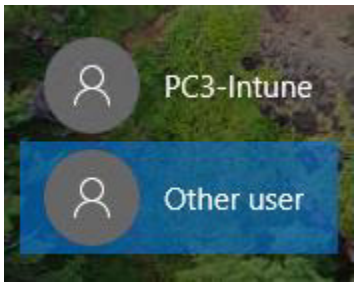

Vi får så melding om at enheten er koblet opp mot bedriften og at man nå kan logge seg på med AD-brukeren sin



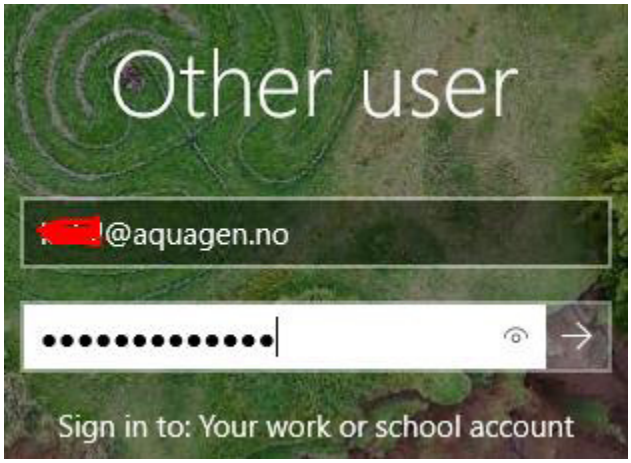

Viser at enheten er koblet opp mot domenet



Når vi logger ut av den lokale brukeren ser vi nå at vi har fått valget om å logge inn på en annen bruker på innloggingsskjermen




Vi skriver inn brukernavn og passord på AD-brukeren vår og forsøker å logge inn

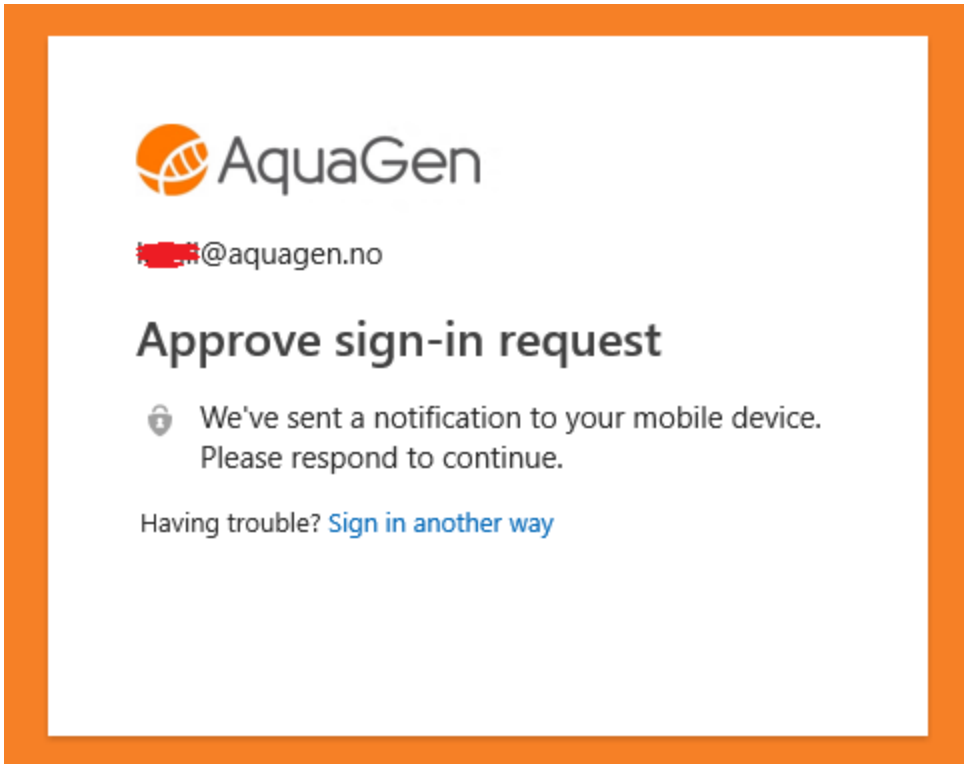




- Når navnet på brukeren endres til faktisk navn er det en god pekepinn på at innloggingen virker som den skal

Maskinen kommer så til å spørre brukeren til å sette en egen PIN, hvis dette er konfigurert i Windows Hello

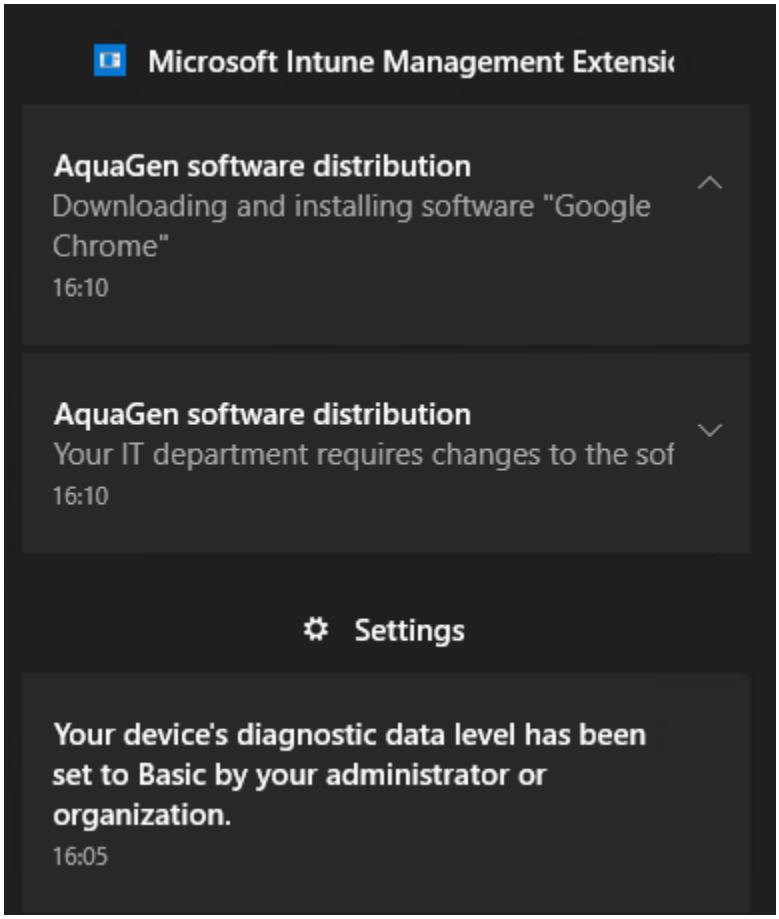
- Har man to-faktor autentisering er man nødt til å identifisere seg først




Skriver inn en PIN-kode som skal benyttes for pålogging på maskinen

Etter innlogging blir man møtt med en del varsler. Her ser man at maskinen allerede begynner å installere apper, policyer og konfigurasjonen som er satt på brukeren.

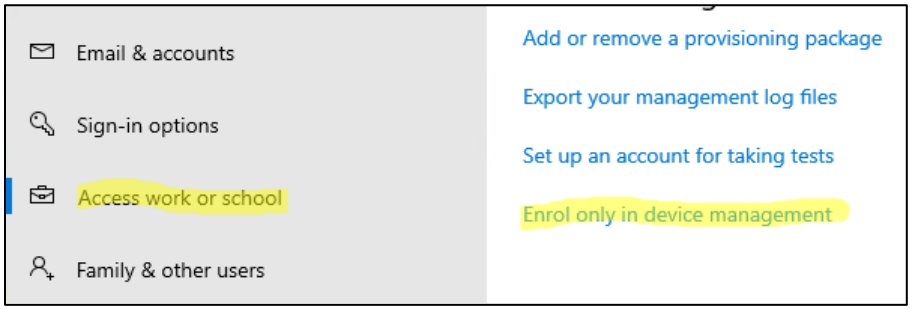
- Merk at det kun er brukeren som er tilegnet disse innstillingene og appene; enheten installerer disse kun basert på av dette



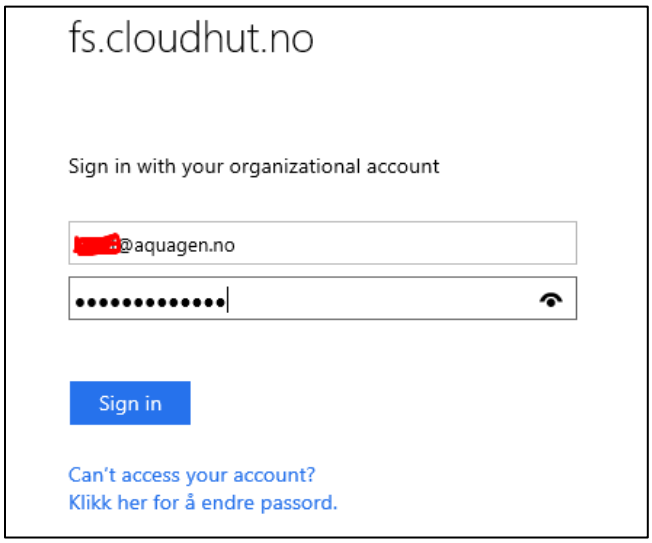

**Enheten er nå lagt inn både i Azure AD og som en MDM-enhet i Intune**

## Kun MDM-tilkobling

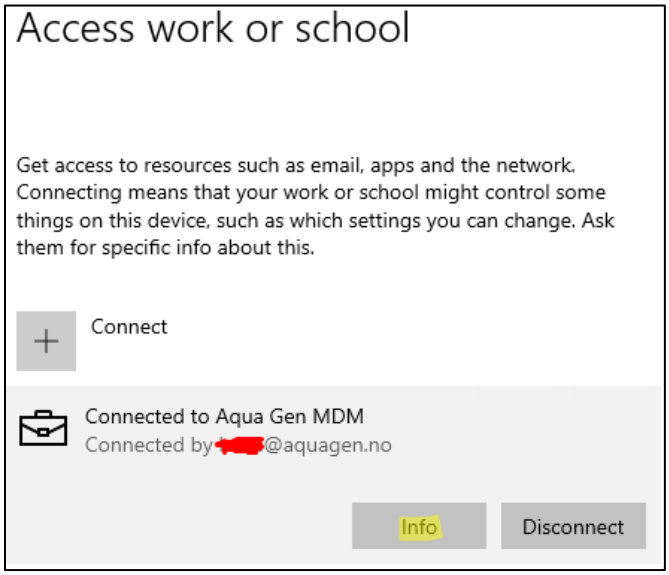
Her begynner vi med å gå inn på *Windows-settings, Account*



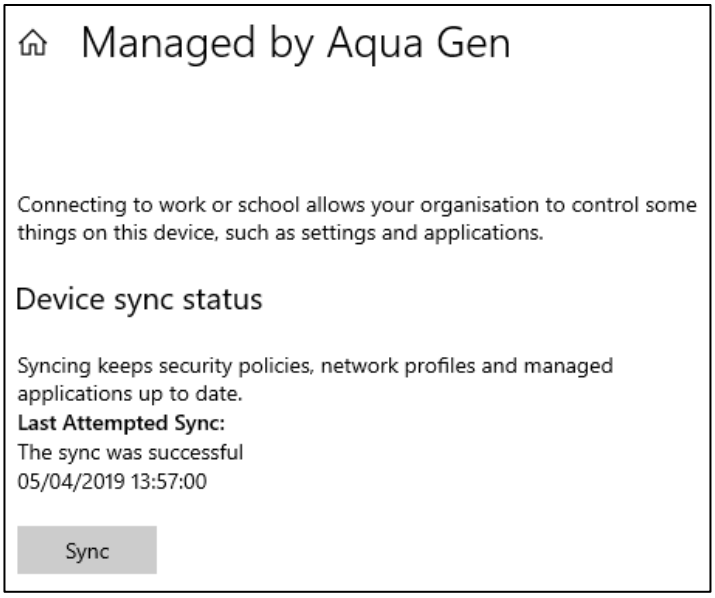

Vi trykker deretter på *Enrol only in device management* under *Access work or school*




Som i den andre metoden, logger vi deretter på med brukeren som vi ønsker å melde inn enheten med




Vi ser nå at enheten er koblet til organisasjonen sin MDM.
Vi trykker på *Info* for å se mer om tilknytningen.

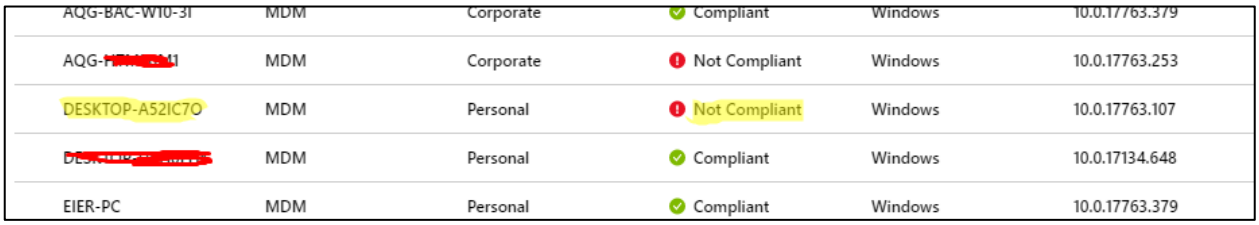



**Som vi kan se er nå enheten lagt inn i Intune kun som en MDM-enhet.**

- Dette betyr at vi nå kan administrere denne enheten.

I bildet nedenfor tar vi en titt på hvordan dette ser ut i Intune-portalen når enheten har blitt tilkoblet på en av de to framgangsmåtene

Som vi ser så har den nye enheten nå dukket opp i listen over enheter. For øyeblikket ser vi at den er satt som en personlig enhet, i tillegg til at den ikke oppfyller kravene som er stilt i *compliance*-policyen på brukergruppen.



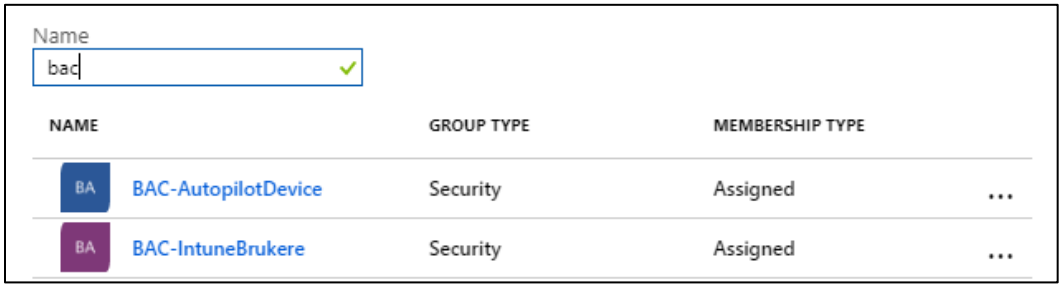
| | | | | | |
|---|---|---|---|---|---|
| AQG-BAC-W10-3I | MDM | Corporate | Compliant | Windows | 10.0.17763.379 |
| AQG-[redacted] | MDM | Corporate | Not Compliant | Windows | 10.0.17763.253 |
| DESKTOP-A52IC7O | MDM | Personal | Not Compliant | Windows | 10.0.17763.107 |
| [redacted] | MDM | Personal | Compliant | Windows | 10.0.17134.648 |
| EIER-PC | MDM | Personal | Compliant | Windows | 10.0.17763.379 |

Vi skal se på hvordan vi kan løse dette, samt legge til nye policyer og enhetskonfigurasjoner i neste fase.

## Fase 5: Policyer, programvare og konfigurasjon

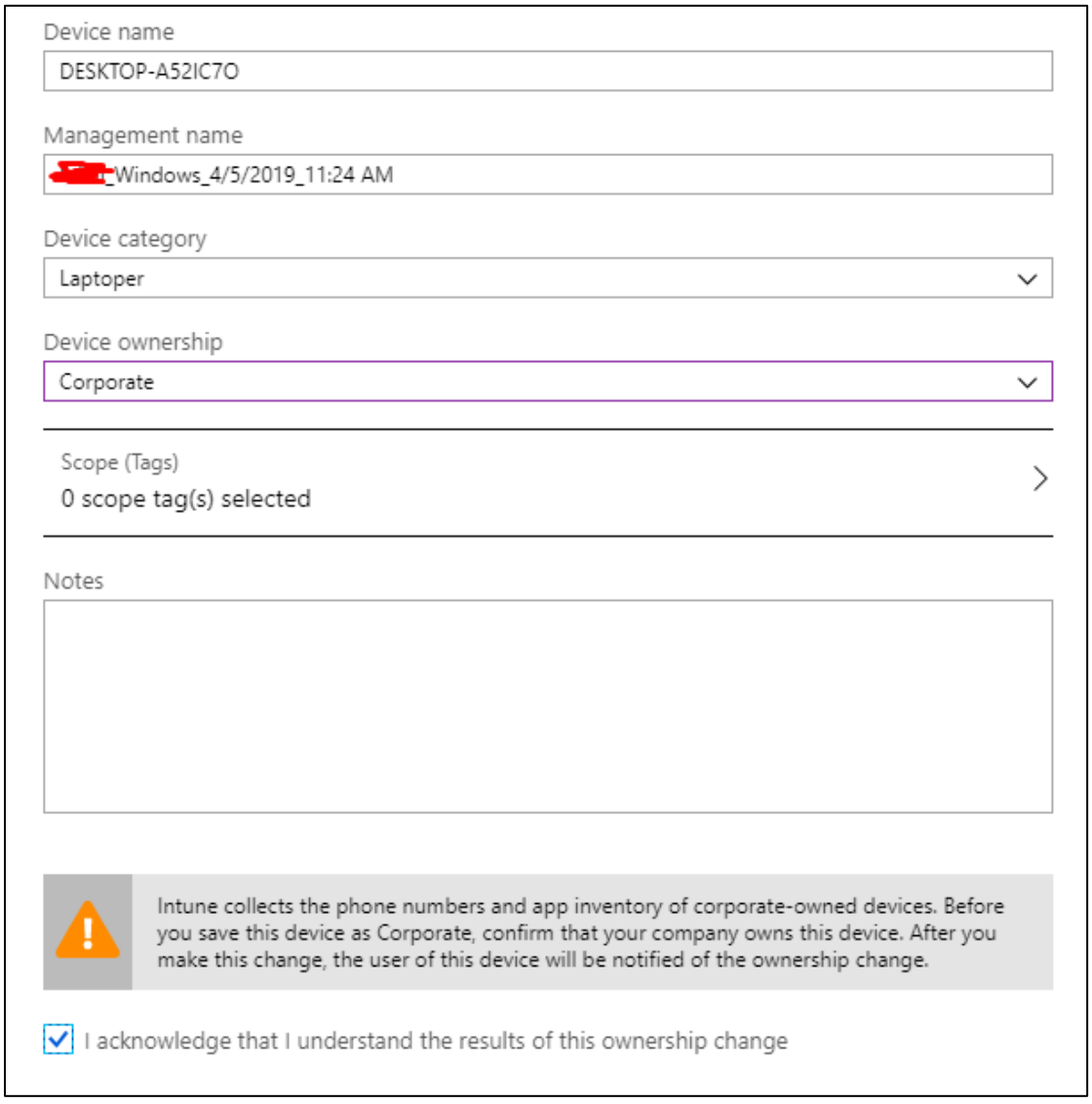
I dette steget skal vi se på å sette egne policyer, konfigurasjon og programvare på enhetene.

Vi starter med å opprette to grupper, av typen *security*




Vi skiller her mellom Autopilot-**enheter** og Intune-**brukere**, for å gjøre det enklere for oss senere.

- Vi bruker likevel de samme policyene, konfigurasjonen og programvaren på begge gruppene.

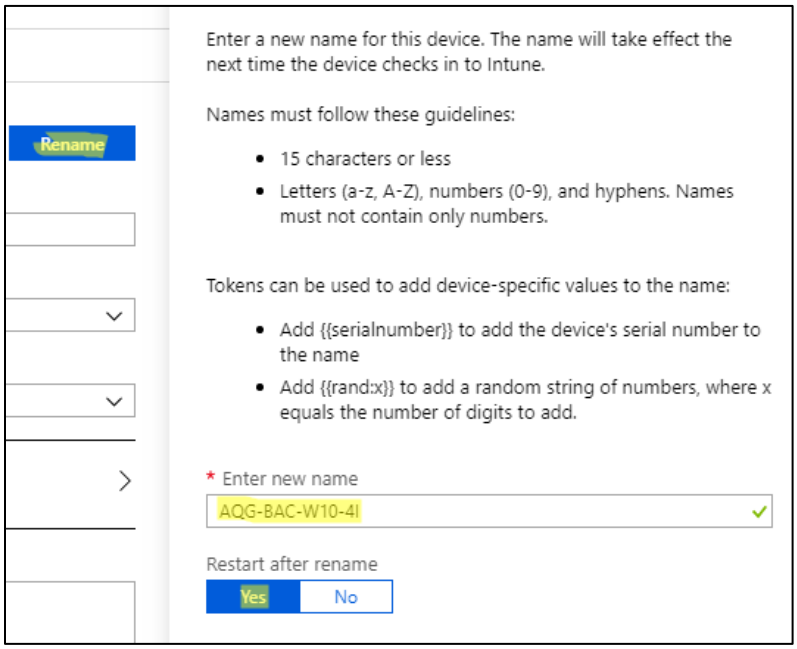


Vi starter her med å gå inn på Intune-enheten som vi la til i forrige steg.

- Her endrer vi *Device Category* til *Laptoper.* Man kan opprette flere slike kategorier, som vist i Fase 2.
- *Device ownership* endrer vi fra *Personal* til *Corporate*. Siden enhetene ble satt opp som personlige enheter fra starten vil de bli importert som dette.
    - For å endre navn på enheten må dette være satt til *Corporate*

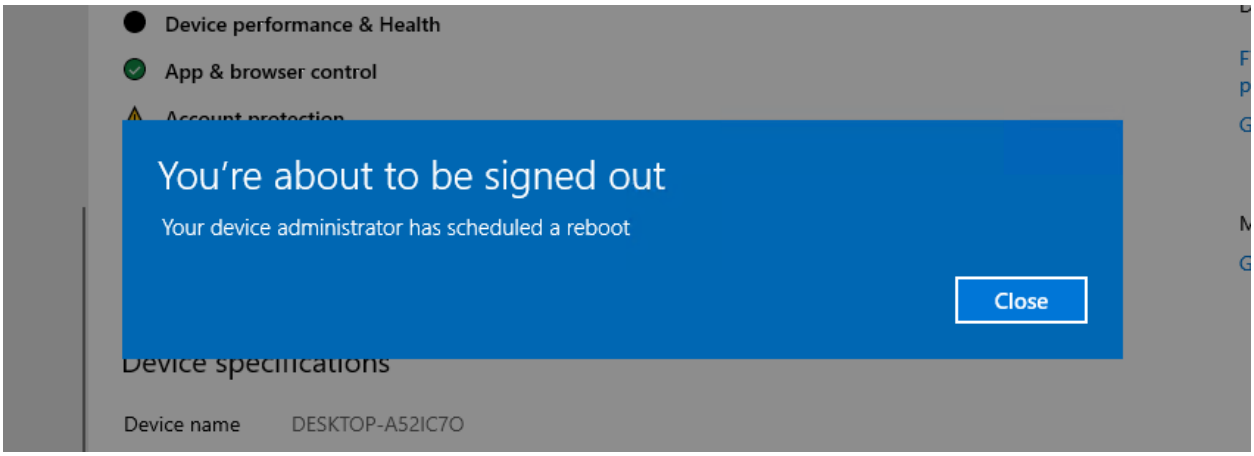
Trykker *Save* for å lagre innstillinger.

Vi går nå inn på enheten igjen og ser at vi nå får mulighet til å endre navnet




Trykker på *Rename*, velger et nytt navn og trykker for at vi vil starte enheten på nytt

- Navnet blir ikke tatt i bruk på maskinene før man restarter.



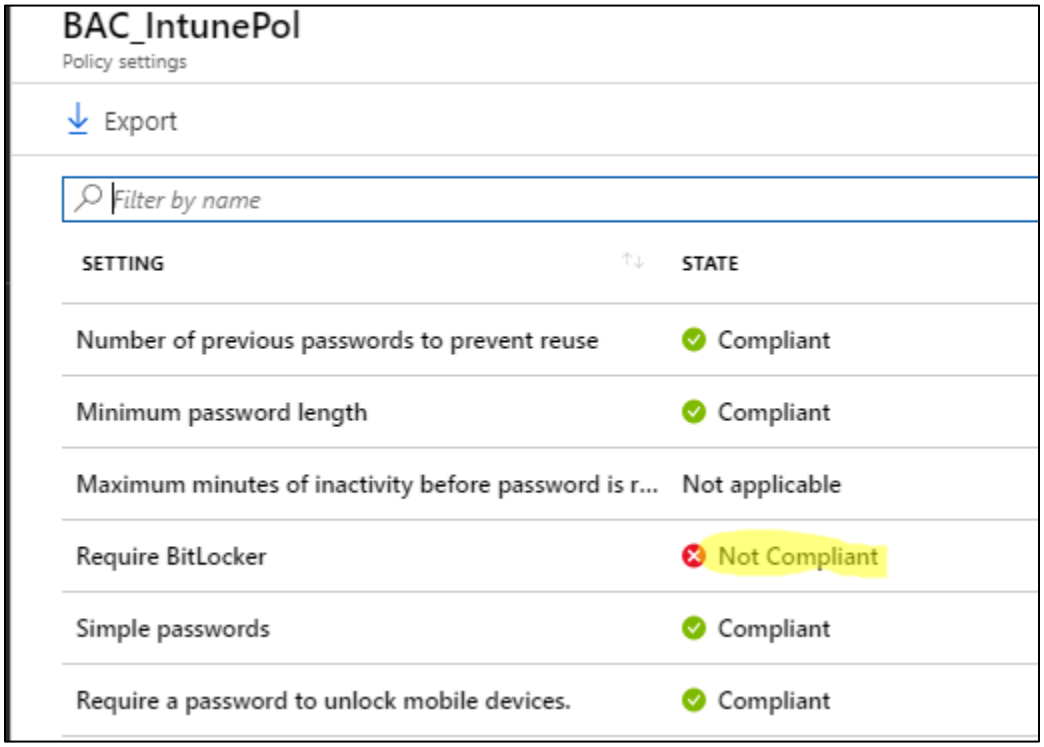

Vi får så opp en melding på den aktuelle enheten at det er blitt planlagt en omstart. Det tar typisk 5 minutter før maskinen restarter seg.

## Policyer

Som vi nevnte i fase 4, så vi at enheten ikke var compliant. Vi tar en titt på Device Compliance for å finne ut av dette.


Her står det at enheten ikke oppfyller kravene som er satt i *BAC_IntunePol*.

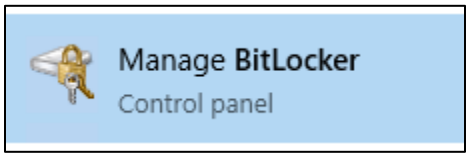
- Dette er en policy som er satt til gruppen *BAC-IntuneBrukere*.
    - Det betyr at om enheten blir tilknyttet eller innmeldt med en **bruker fra denne gruppen**, vil den måtte tilpasse seg disse kravene.



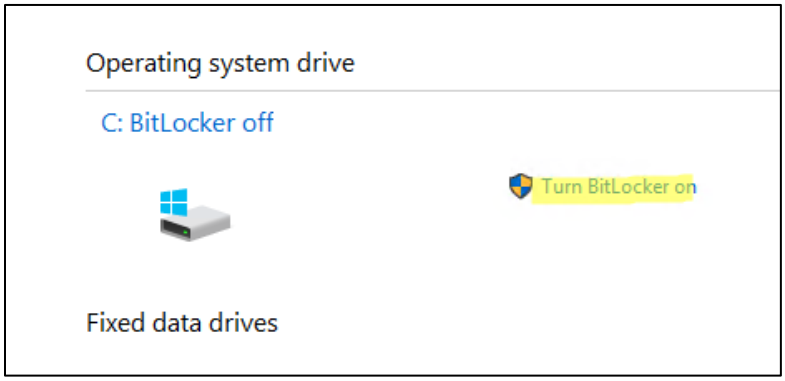

Når vi går inn på policyen ser vi at enheten ikke er «compliant» fordi den ikke har BitLocker-aktivert.

- Hvis man tilegner en policy som krever BitLocker til en enhet som fra før av er i bruk, vil ikke BitLocker automatisk bli aktivert. Hvis vi prøver det samme på en Autopilot enhet vil BitLocker derimot bli aktivert i installasjonsprosessen.
    - I dette tilfellet må vi manuelt inn på maskinen for å aktivere BitLocker. En annen mulighet er selvfølgelig å skru av kravet om BitLocker.

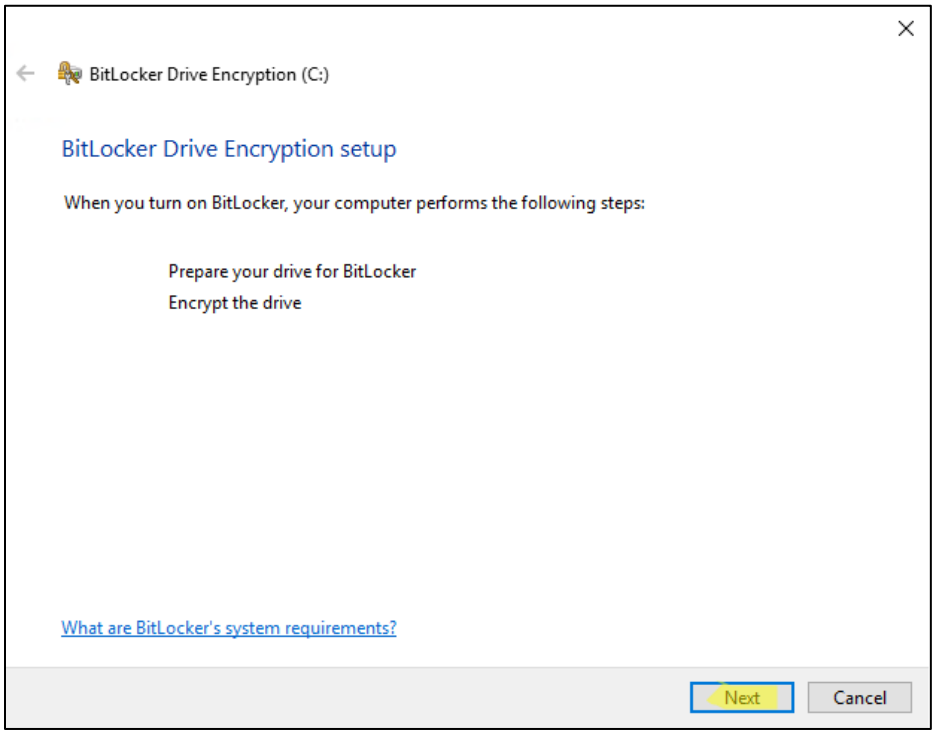
Vi går nå inn på den aktuelle maskinen for å forsøke å løse dette.


Søker opp BitLocker i start-menyen, og trykker oss inn på innstillingene

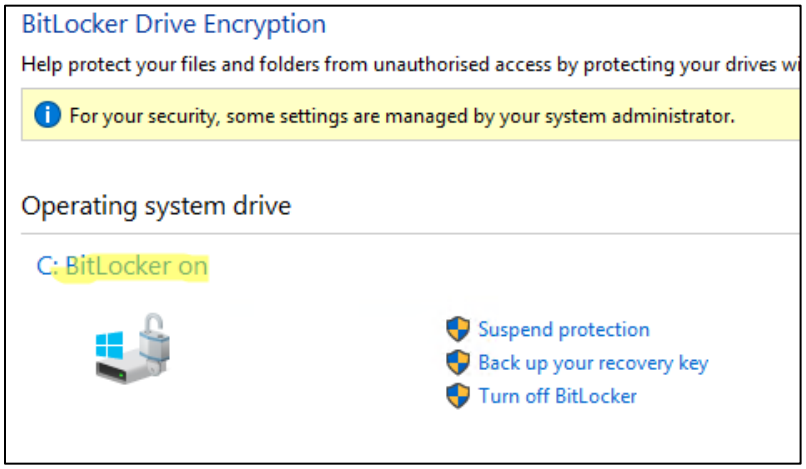



Her skrur vi på BitLocker ved å trykke på den markerte knappen.



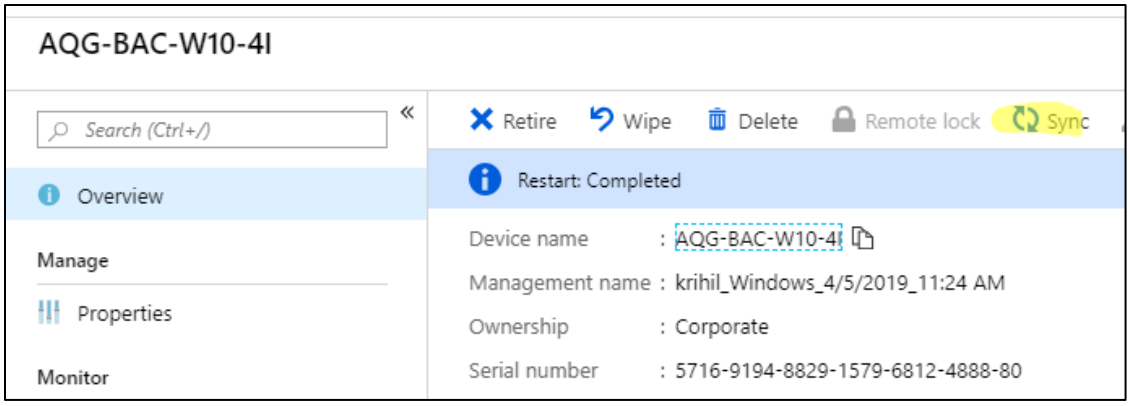

Bekrefter at vi vil skru på BitLocker ved å trykke på *Next*

Når vi er ferdige med å sette opp BitLocker, blir vi bedt om å starte maskinen på nytt.




Vi må deretter vente til det står «*BitLocker on*» slik som på bildet ovenfor.

- Hvis det står «*BitLocker encrypting*» har ikke BitLocker blitt aktivert enda.




Hvis vi nå går i panelet til enheten og trykker på *Sync* vil enhetens «*compliance*» snart bli oppdatert. Det tar som regel opptil 10 minutter før maskinen faktisk blir satt som «compliant».


Som vi ser er nå maskinen blitt compliant med en policy satt på bruker-basis.

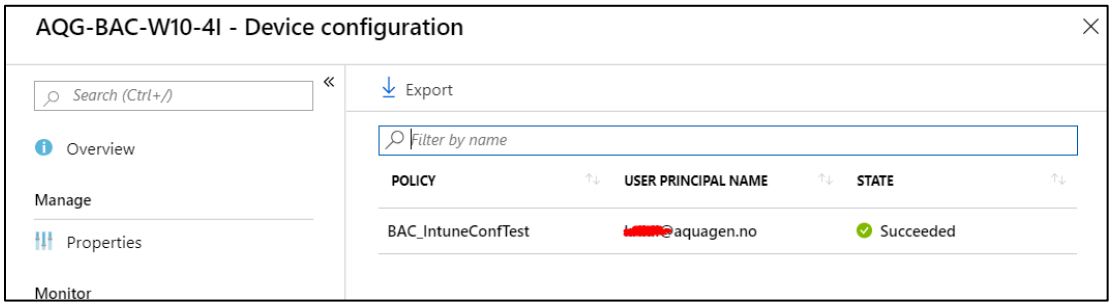
Vi kan nå eventuelt legge til andre policyer hvis vi har andre krav vi ønsker å stille for enheten.

## Enhetskonfigurasjon

I dette steget vil vi nå prøve å legge til en enhetskonfigurasjon.

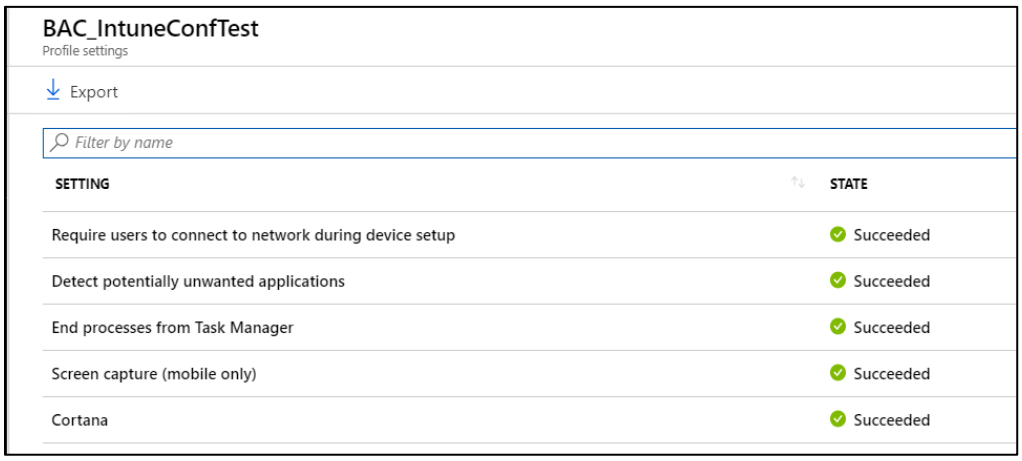
- Siden dette er en Intune-enhet vil vi sette konfigurasjonen på brukere, ikke maskinbasis.
    - Så fremt enheten er tilknyttet maskinen med brukerkonto vil den komme til å følge kravene som brukerkontoen har fått

Vi går nå til *Device Configuration* og ser på profilen som er tilegnet der.




Her kan man se at profilen *BAC_IntuneConfTest* er blitt tilegnet maskinen gjennom brukeren som er logget inn.

Hvis vi trykker oss inn på profilen kan vi se hva den inneholder, og hva som eventuelt ikke har blitt satt



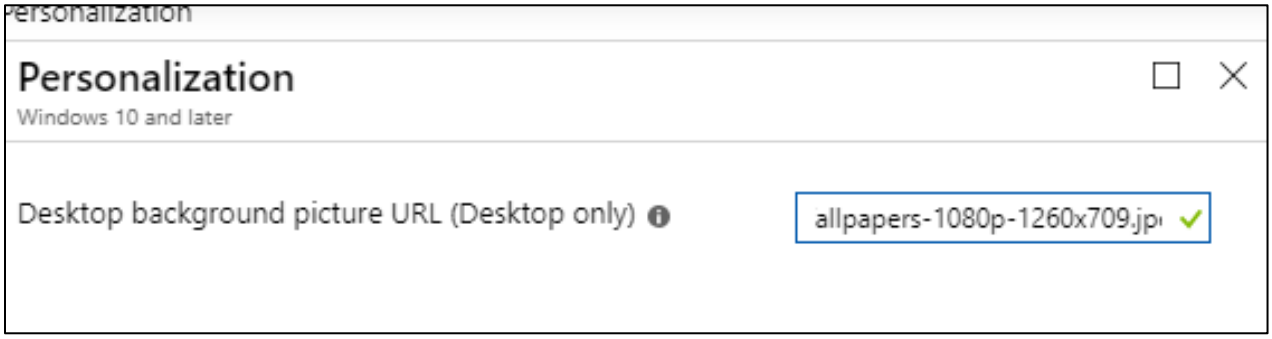

Som vi ser her har alt blitt satt som det skal.

- Merk at det ikke viser hva innstillingen gjør, bare hva den gjelder.

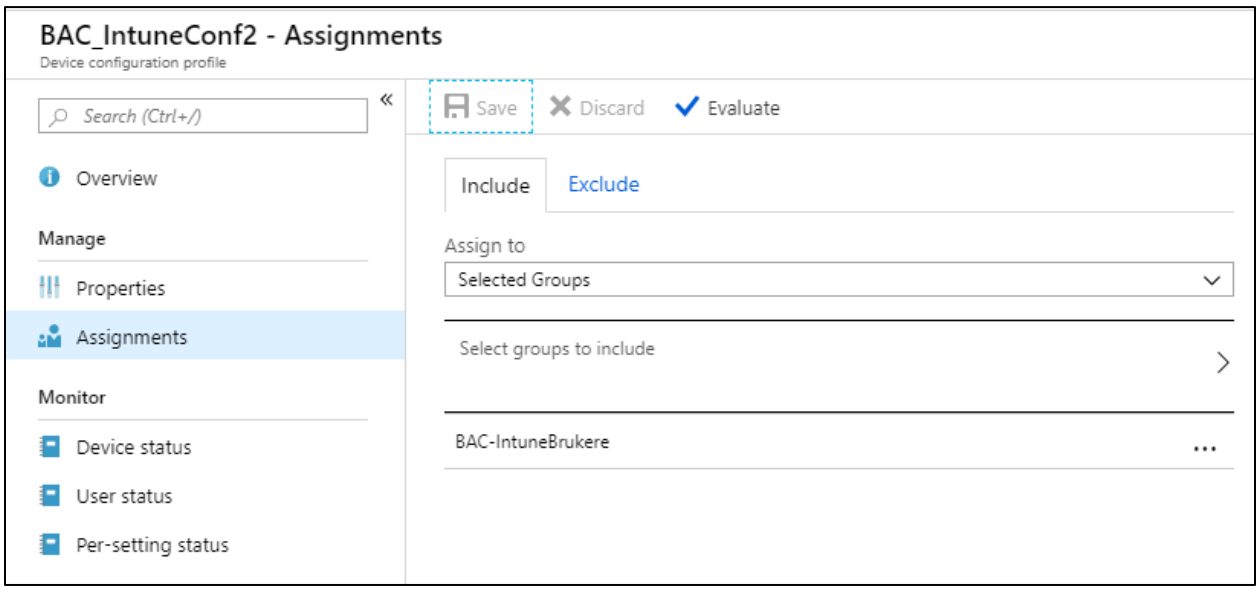
Vi kan opprette en ny konfigurasjon for å forsøke med flere innstillinger på maskinen.

- For at vi skal se om den har effekt skal vi prøve å finne noe som kan vises visuelt.

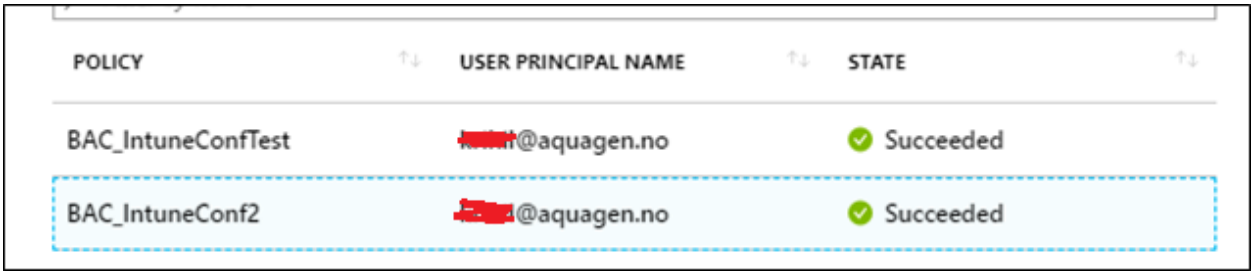
Vi velger en innstilling som lar oss spesifisere bakgrunnsbildet på datamaskinen. Denne må hente bakgrunnsbilde fra en internett-lenke, så vi finner et bilde som vi kan prøve med.



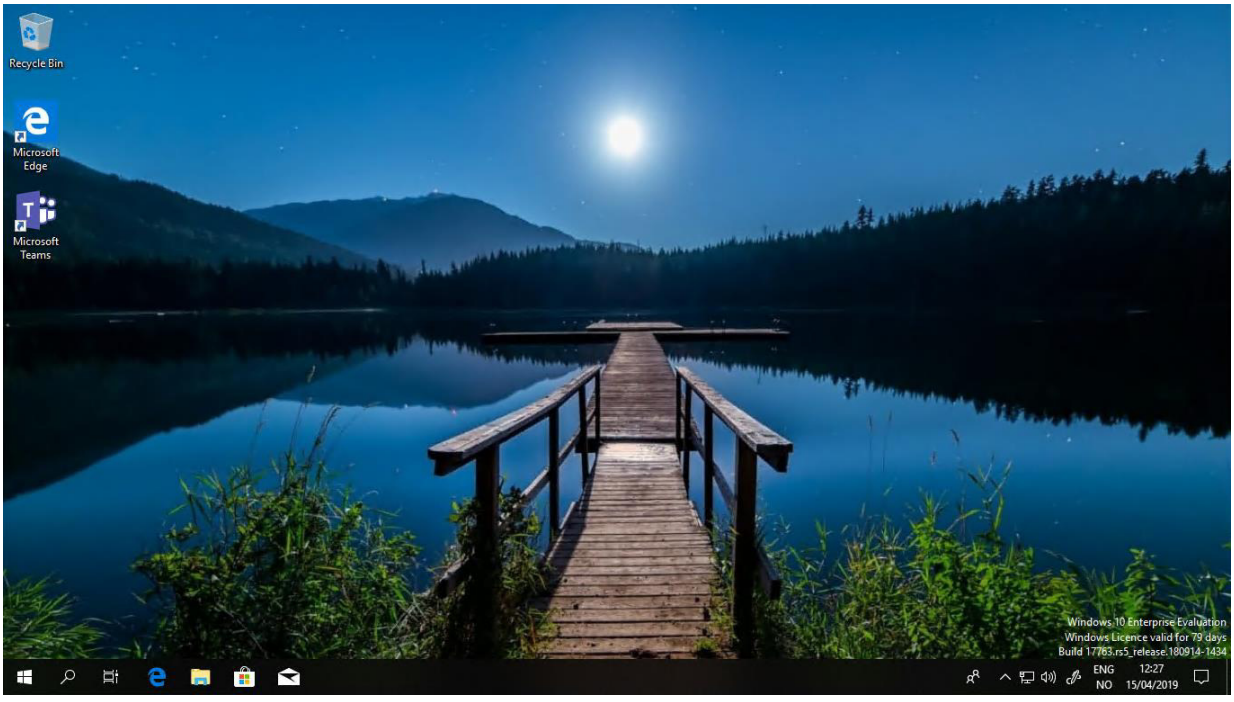

Vi tilegner deretter profilen til brukergruppen vår for at den skal gå i effekt.




Vi går deretter inn på enheten i Intune og ser at profilen har blitt satt uten problem.




På enheten ser vi derimot ikke at bakgrunnen har blitt satt enda. Vi prøver å starte maskinen på nytt.



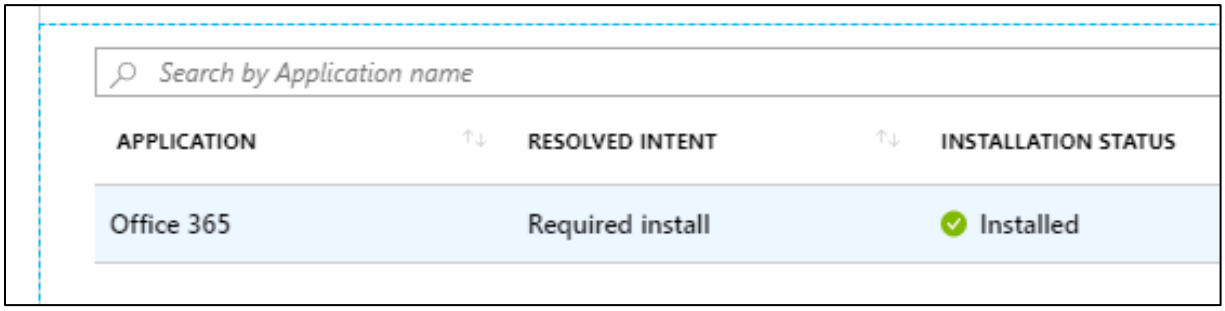

**Etter en omstart av maskinen ser vi nå at profilen har blitt tatt i bruk og bakgrunnen er blitt endret.**

## Programvare/apper

Vi skal nå ta en titt på programvaren som finnes på maskinen.

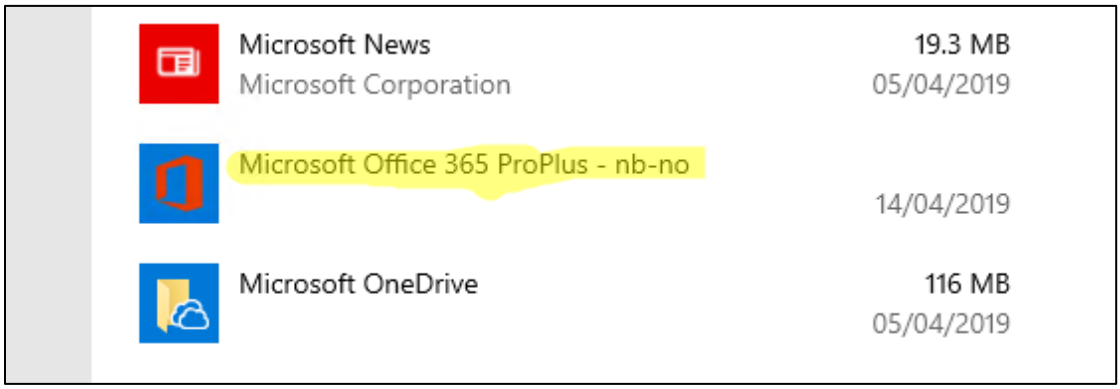
Vi skal ikke fokusere så alt for mye på programvare, men for å bekrefte at dette virker skal vi prøve Office-pakken, pluss et annet program

- I praksis kan man få inn nesten all ønsket programvare gjennom Intune.




I menyen *Managed Apps* ser vi at Office 365 er blitt installert. Dette er en app som tidligere ble opprettet og tildelt brukergruppen *BAC_IntuneBrukere.*

Som vi ser på bildet nedenfor kan vi bekrefte av appen er installert på enheten.




Vi skal prøve å legge inn enda en egen applikasjon som skal tildeles enheten.

## Importere egne apper i Intune

Det er mulig å legge inn egne apper i Intune og her skal vi prøve på å legge inn Google Chrome.

For å importere standalone-apper i Intune krever det at man lager en såkalt INTUNEWIN-fil. Denne inneholder informasjon som Intune bruker for å installere appen, i forskjellige miljø og på forskjellige enheter. Vi har benyttet oss av en guide [1] som forklarer steg for steg hvordan man oppretter en slik fil.

I guiden bruker man verktøyet **Win32-Content-Prep-Tool** fra Microsoft. Dette har vi hentet ned fra Microsoft sin GitHub-side [2]

Det er et kommandolinjeverktøy, men er ganske enkelt i bruk med noen få, ganske enkel parameter. Den kan opprette INTUNEWIN-filer ut ifra flere forskjellige typer installasjonsfiler, blant annet MSI-filer.

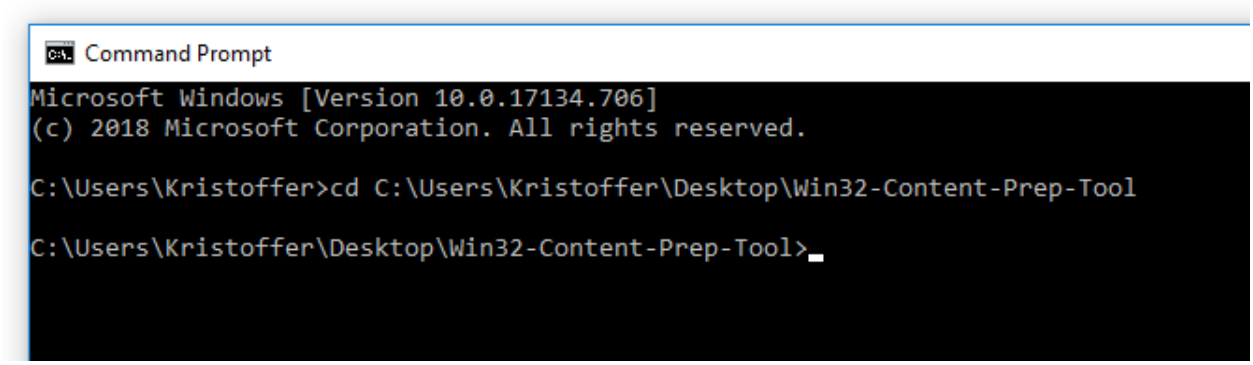
- Fordelen med MSI-filer er at de i stor grad inneholder den informasjonen som trengs for å installere programmet. Da slipper man å fylle ut denne informasjonen manuelt i Intune.

Vi går inn på sidene til Google for å hente ned installasjonsfilene for Google Chrome

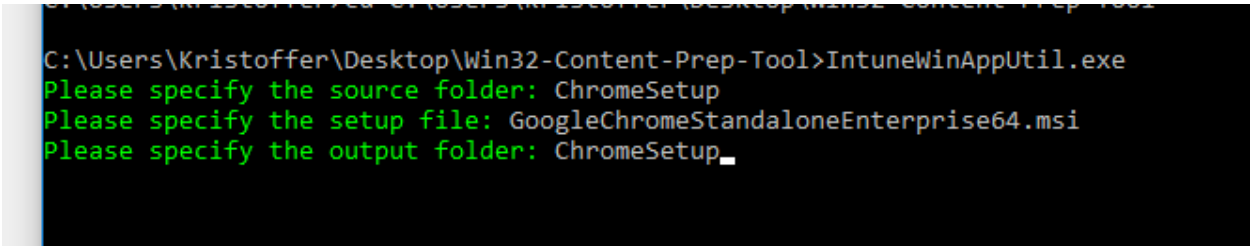
- Google Chrome og annen programvare kommer typisk i EXE-filer. Vi trenger derfor å gå inn på Enterprise-sidene [3] til Google for å finne MSI-filene.

Vi laster ned og pakker ut filen i samme mappe som vi la verktøyet fra Microsoft.

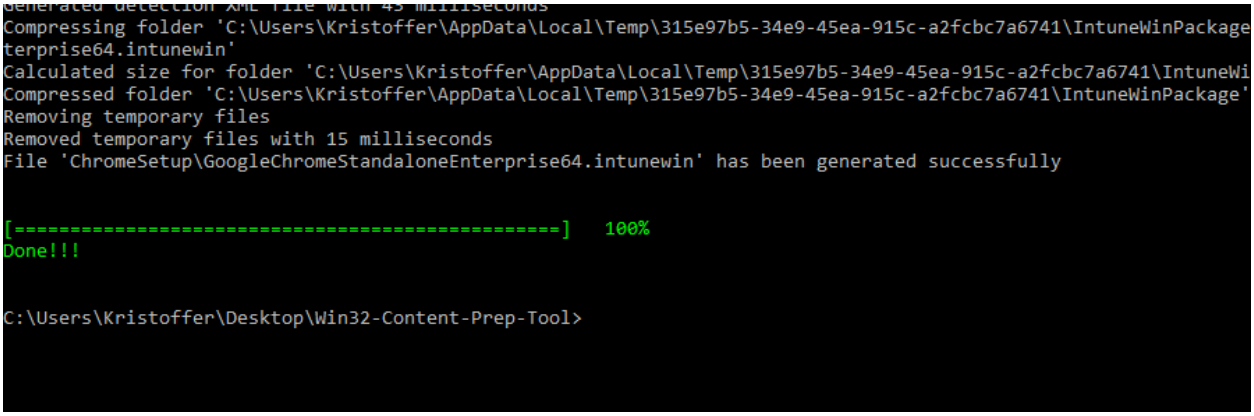

Når filen er lastet ned starter vi programmet Win32-Content-Prep-Tool ved å først åpne kommandolinjen og navigerer oss til den riktige mappen



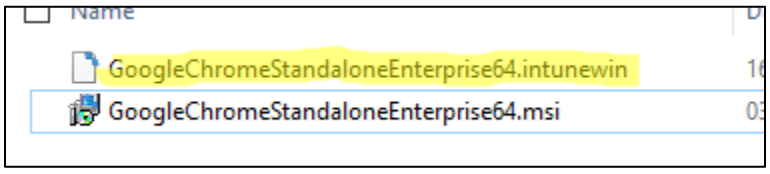

Vi starter deretter programmet ved å skrive inn navnet og trykker Enter.




Som vist i bildet ovenfor skriver vi inn parameter fortløpende. Dette kan man også fylle inn på forhånd.

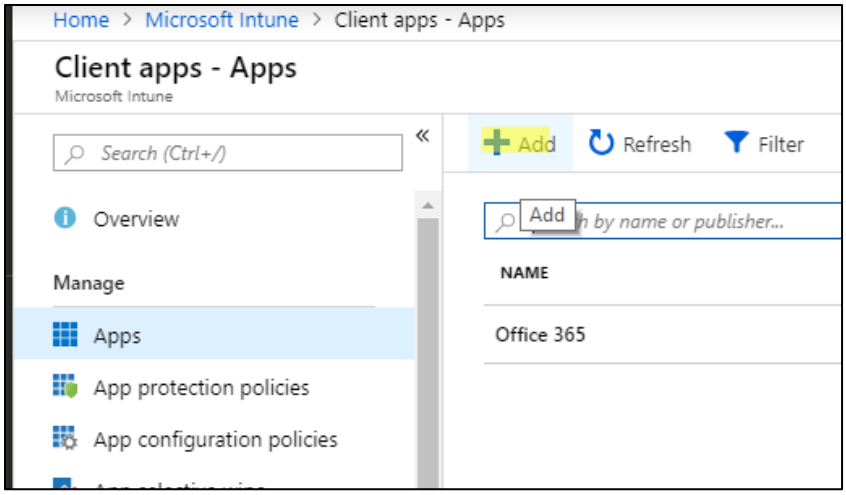



Når vi har trykket Enter ser vi at filen når har blitt opprettet.



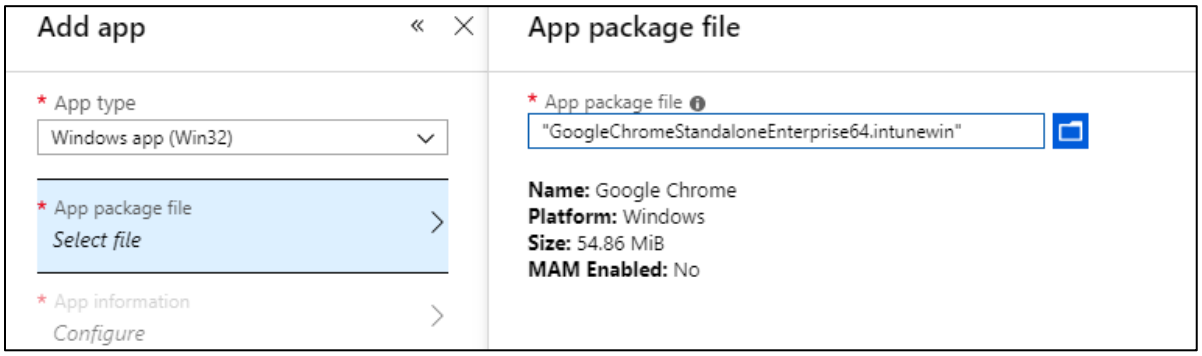

Vi kan bekrefte dette ved å se at vi nå har en ekstra fil i mappen.

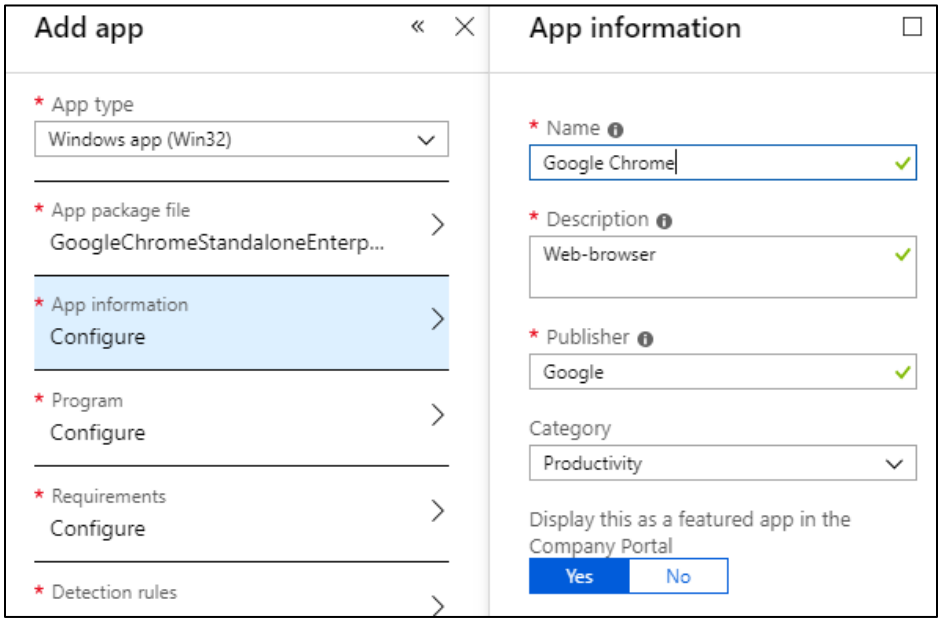
Vi går nå inn på *Client Apps* i Intune.




Vi trykker på *Add* for å legge til enda en applikasjon.

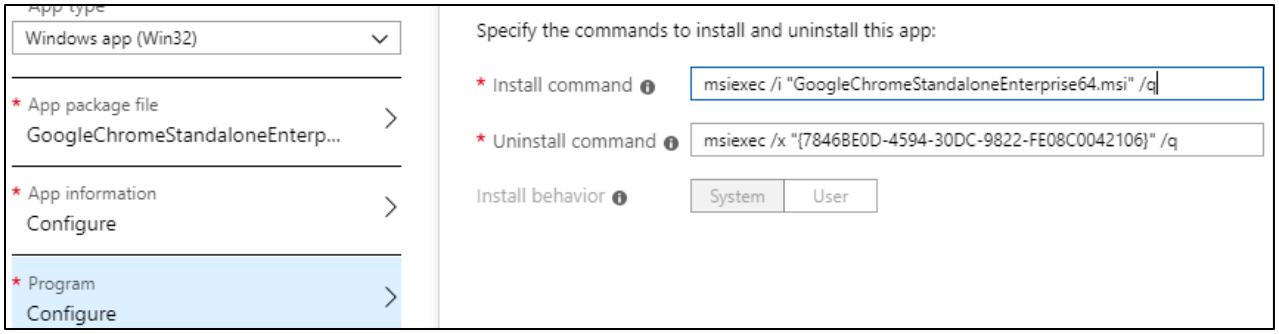
Vi begynner med å velge app av typen *Windows app (Win32)* og velger så filen som opprettet



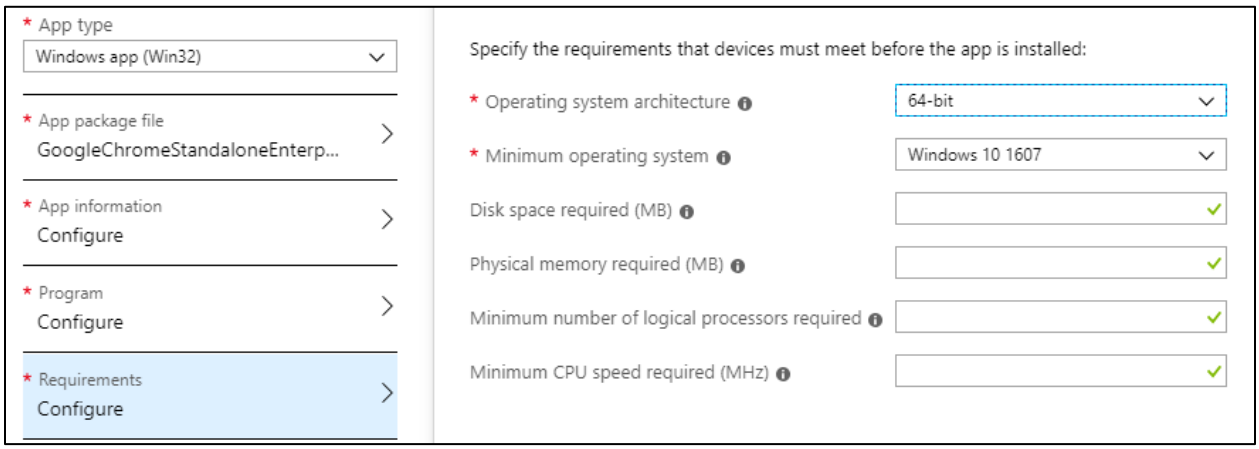




I fanen *App information* må vi sette blant annet navn, beskrivelse og utgiver på applikasjon

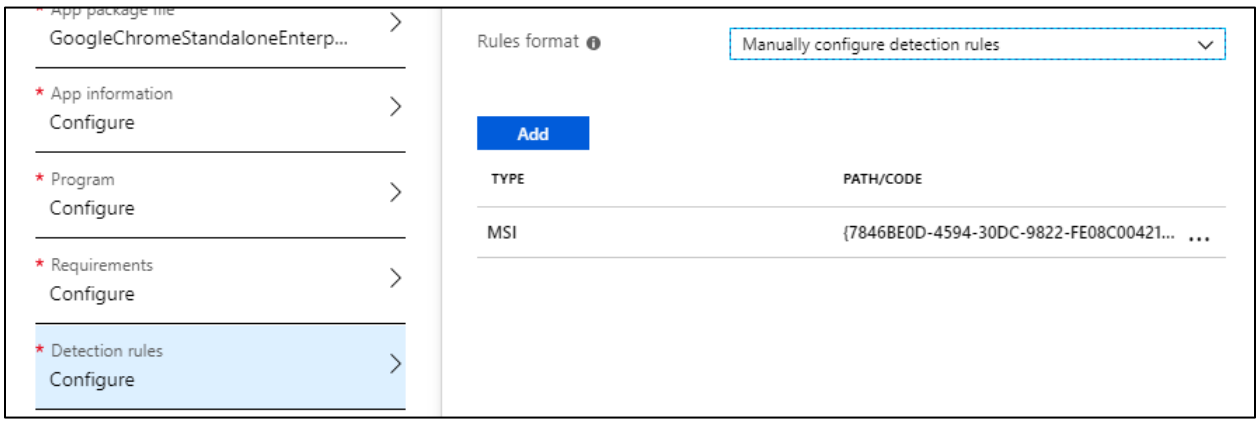
Kategori, pluss en del annen informasjon kan legges inn ved behov.




Under fanen *Program* har vi muligheten til å sette egne installasjons-parameter, ved behov. Vi velger å beholde standard-parameterne.



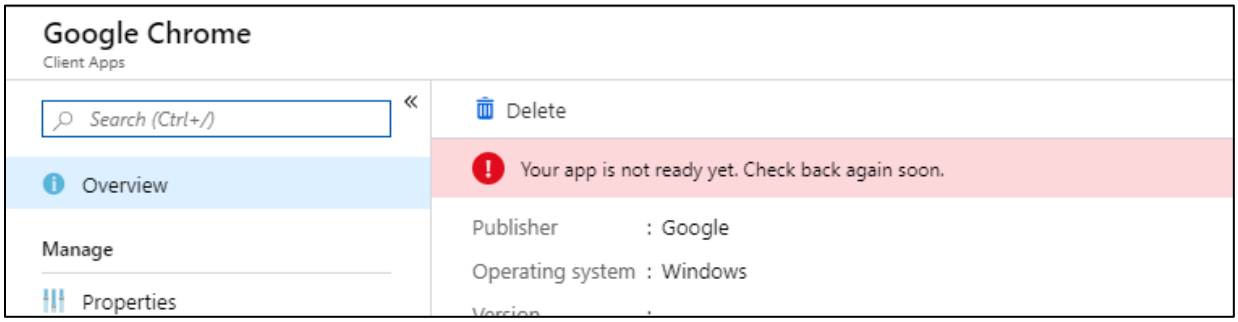

Under fanen *Requirements* må vi sette hvilken arkitektur programmet kjører på, samt den eldste versjonen av Windows som programmet kan installeres på. Resten er valgfritt å fylle inn om man ønsker.



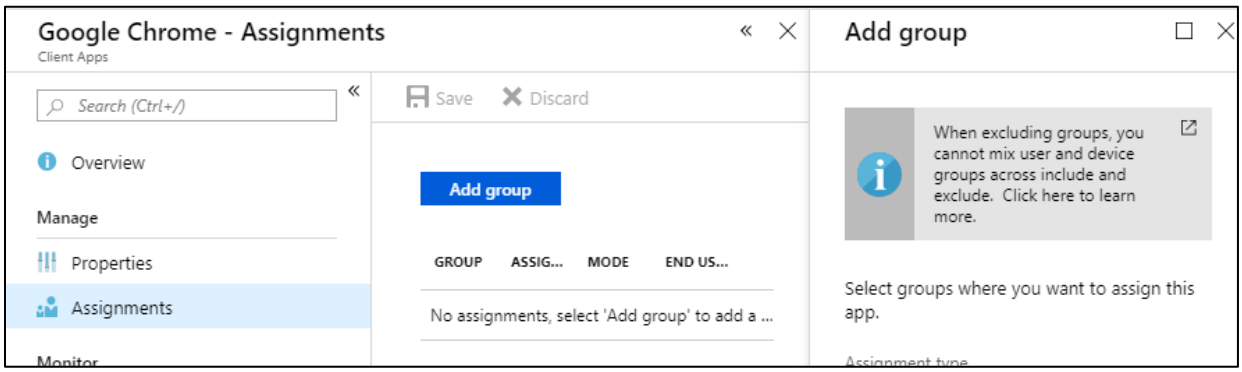

Neste fane, *Detection rules,* bestemmer hvordan Intune og Windows finner ut om programmet faktisk er installert. Man kan legge til egendefinerte måter å undersøke dette på, men vi tar standard-metoden ved å detektere ID-en på programmet som installeres.

Vi har nå satt alle innstillinger for appen og kan nå trykke *Add* for å legge inn appen i Intune.

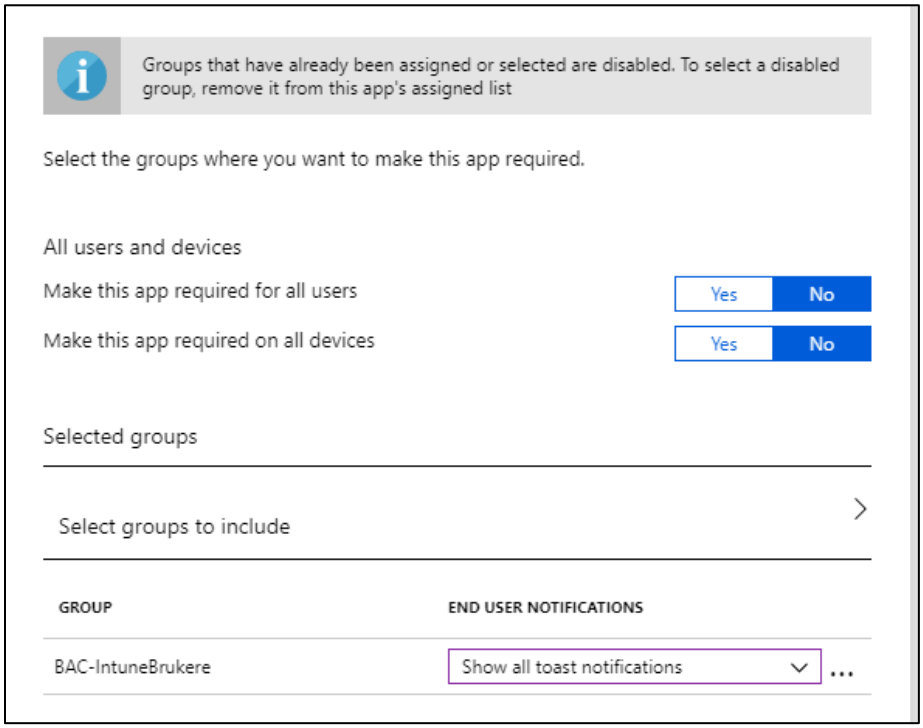
Etter at vi har fått laget appen får vi opp følgende melding. Det tar opptil 10 minutter før appen blir ferdig, mye avhengig av størrelsen på appen.



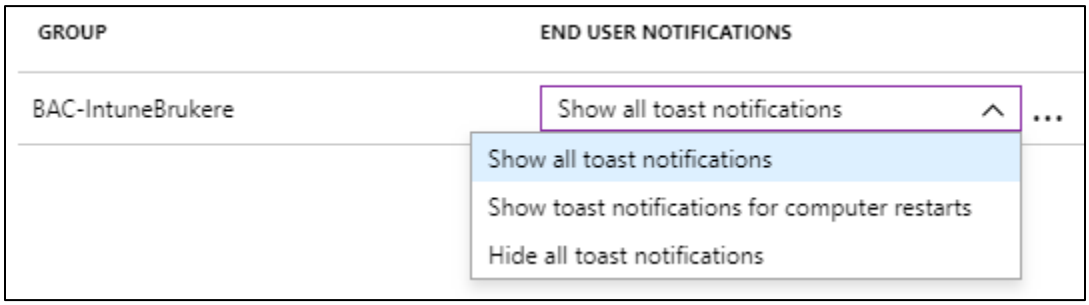

Når appen har blitt ferdig konfigurert kan man tilegne den til en gruppe.




Vi legger så til gruppen *IntuneBrukere* her for å tildele appen til disse brukerne



- Man har her valget å sette *Make this app required for all users* og *Make this app required on all devices.*
    - Hvis man setter disse til *Yes* «ignorerer» Intune hvilke grupper som settes, og vil tildele appen til alle enheter uavhengig dette.
    - Man bør derfor være varsom og se over innstillingene før man lagrer de.



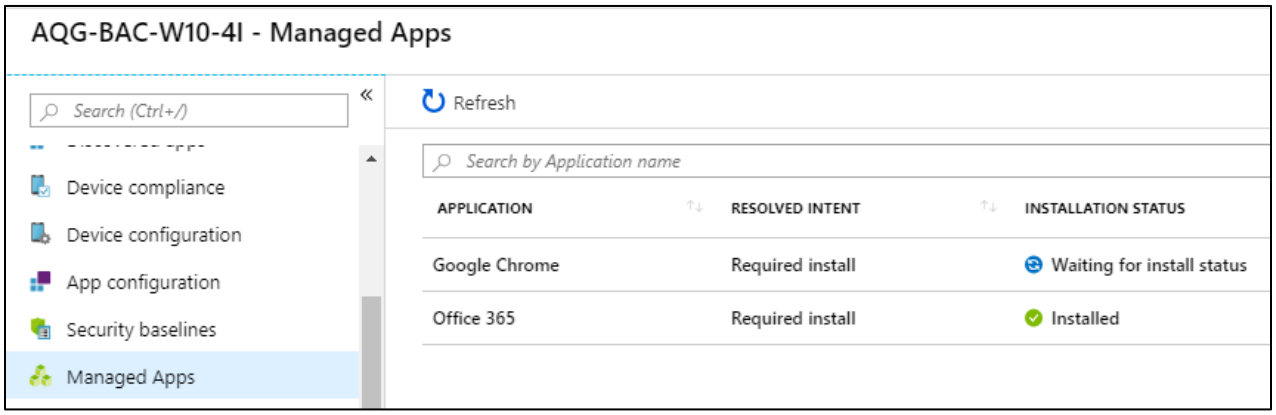

Nederst har man valget mellom såkalte *toast*-varsler på enhetene

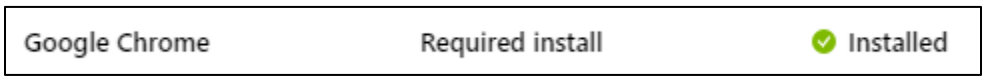
- Show all toast notifications – varsler brukeren om alle stegene i installasjonsprosessen
- Show toast notifications for computer restarts – varsler brukeren kun når enheten trenger å bli restartet etter installasjon av programvare
- Hide all toast-notifications – skjuler alle varsler

Vi velger her å vise alle slik at vi kan sjekke installasjonsprosessen underveis.

Vi trykker **Save** og gruppen har nå blitt tilegnet programvaren.

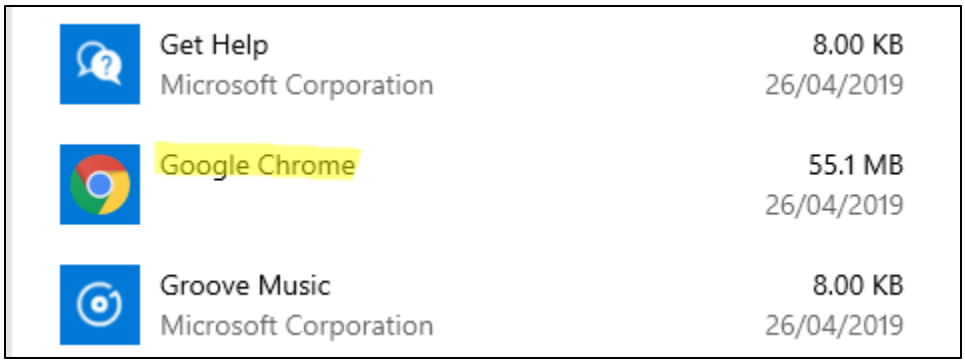
Vi går inn på enheten og ser nå at den har blitt tildelt en ny app.




**Etter en liten stund kan man sjekke igjen og ser nå at appen er merket som installert.**

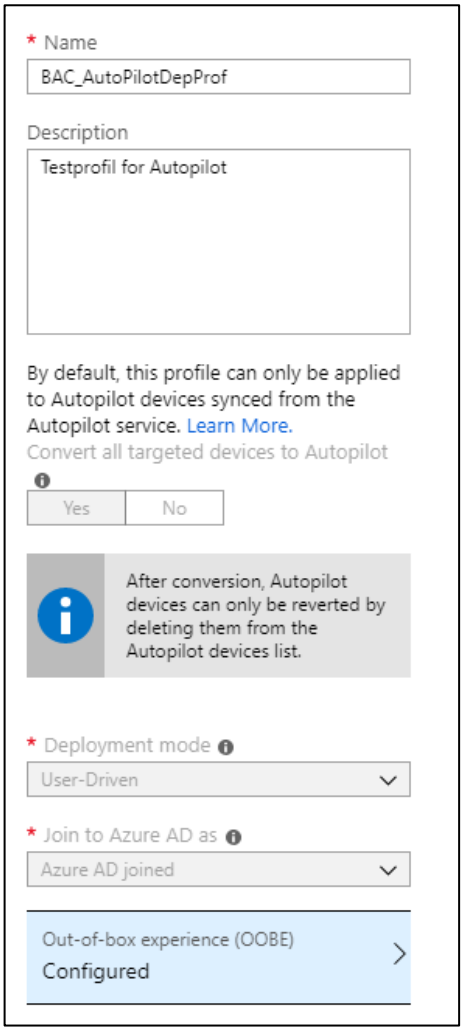
For å bekrefte dette går vi inn på den aktuelle maskinen.




**Også her kan vi se at appen er blitt installert.**

## Fase 6: Test av Microsoft Autopilot

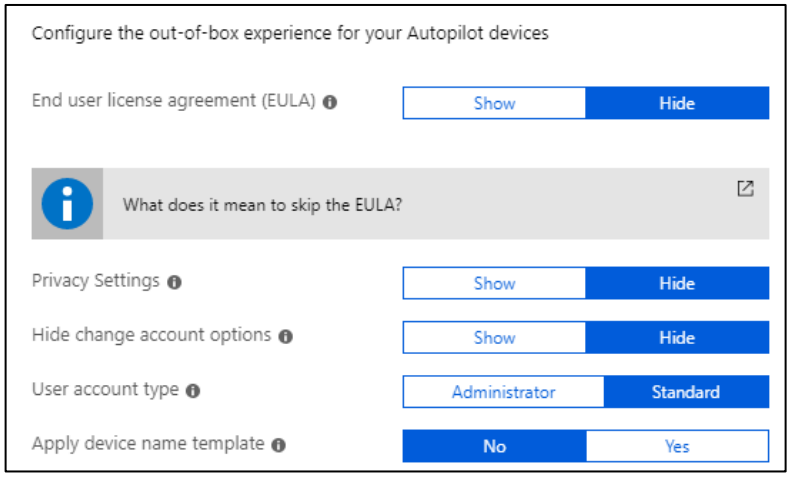
Så langt har vi testet å rulle inn eksisterende enheter inn i Intune, samt å tildele de policyer, konfigurasjoner og apper.



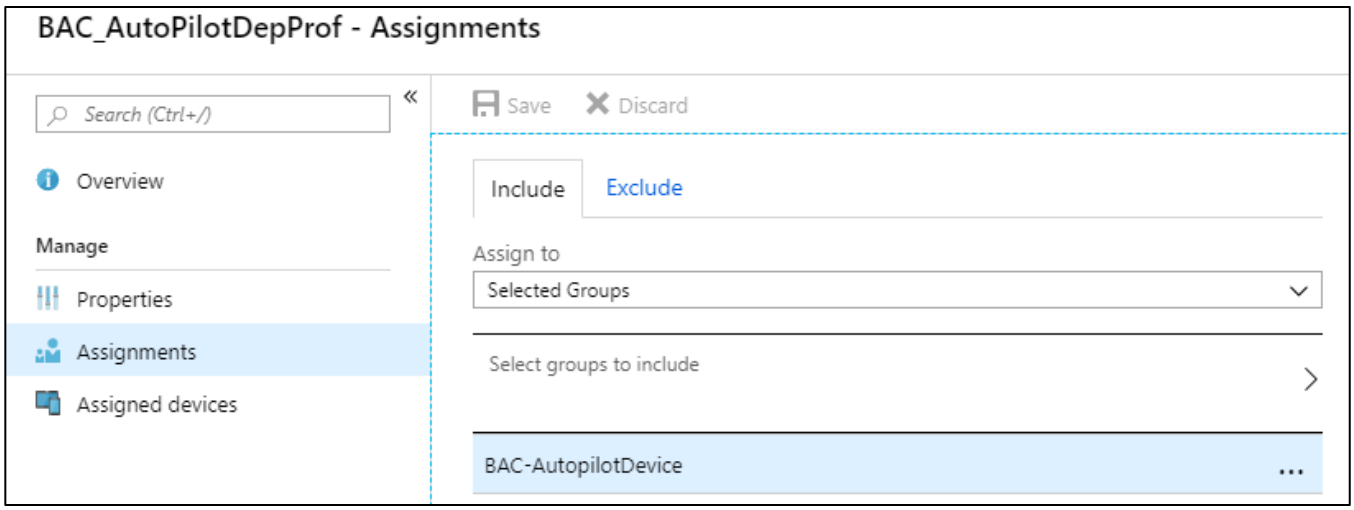

Nå vil vi prøve å få dette ut automatisk til en enhet som ikke har vært i bruk før, eller som har blitt reinstallert fra tidligere installasjon. Hvis man får satt opp dette riktig kan det spare mye tid for utdeling av enheter og datautstyr i organisasjonen

Vi starter med å sette opp en profil som vi skal bruke til å rulle ut maskinen med.

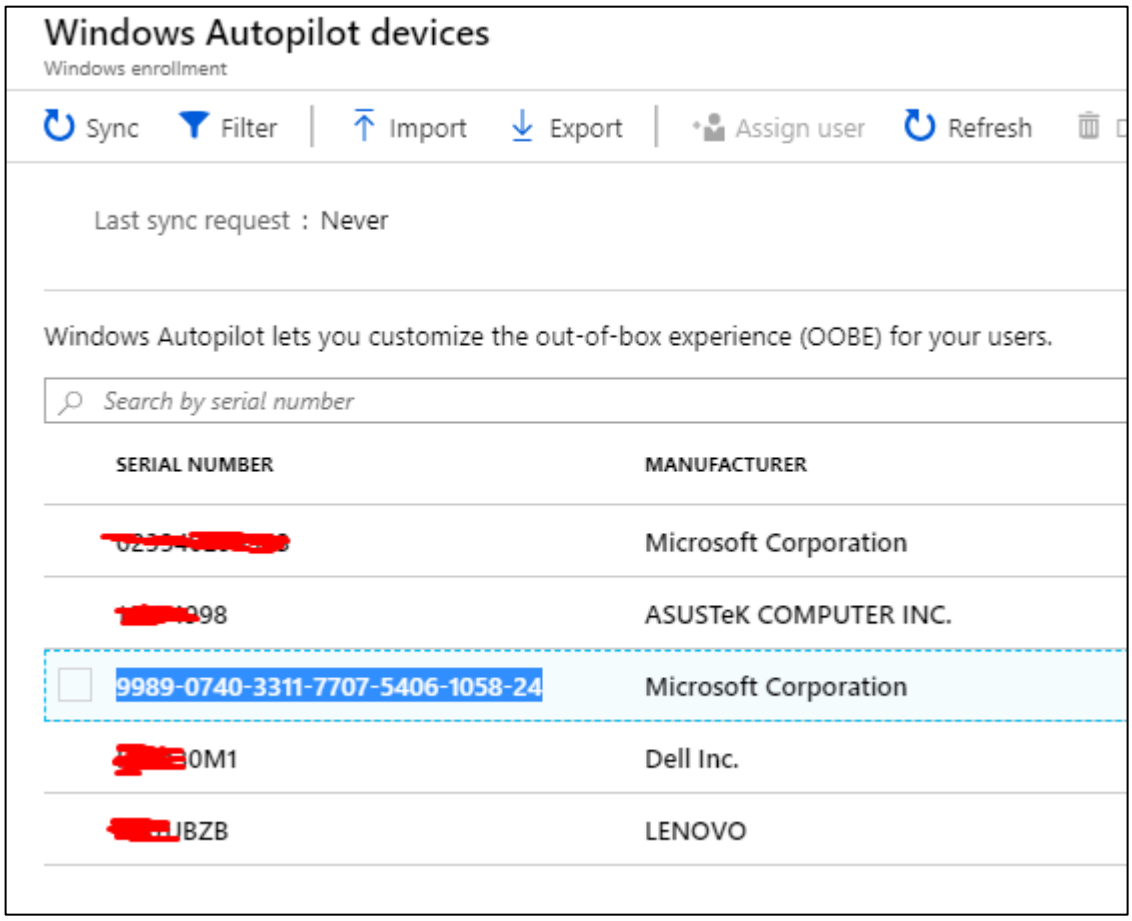
Dette kalles en *Deployment Profile*, og finnes under Windows Deployment i Intune.




Vi setter nevnte valg på profilen og tilegner den til gruppen **BAC-AutopilotEnheter**

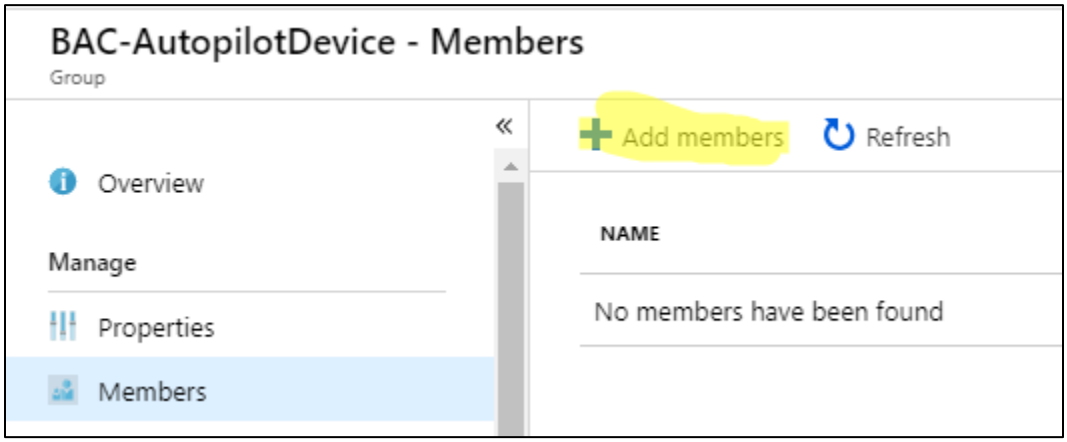


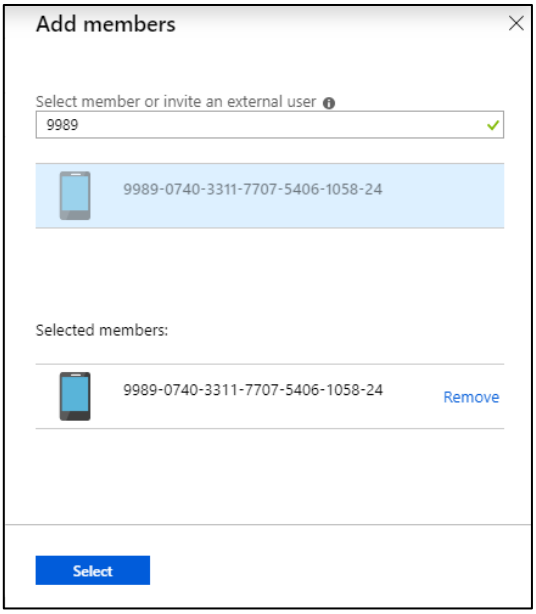
Neste steg går ut på å legge inn Autopilot-enheten inn i gruppa som vi tilegnet profilen til.



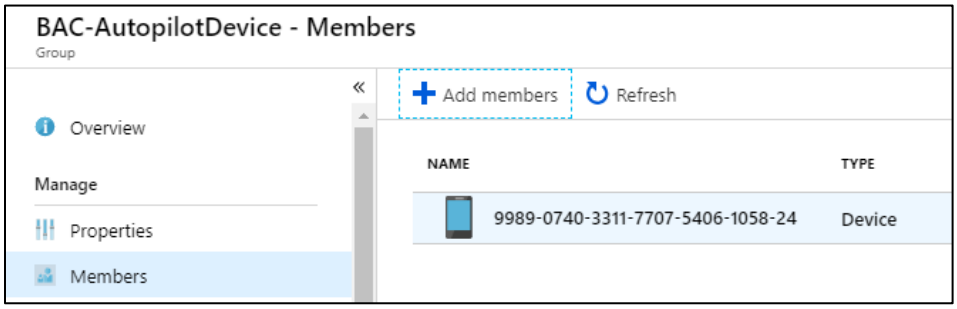

Vi går inn på *Autopilot devices* og noterer ned navnet på maskina.

Vi går så inn på *Gropus*, søker opp gruppen og trykker på *Add members*



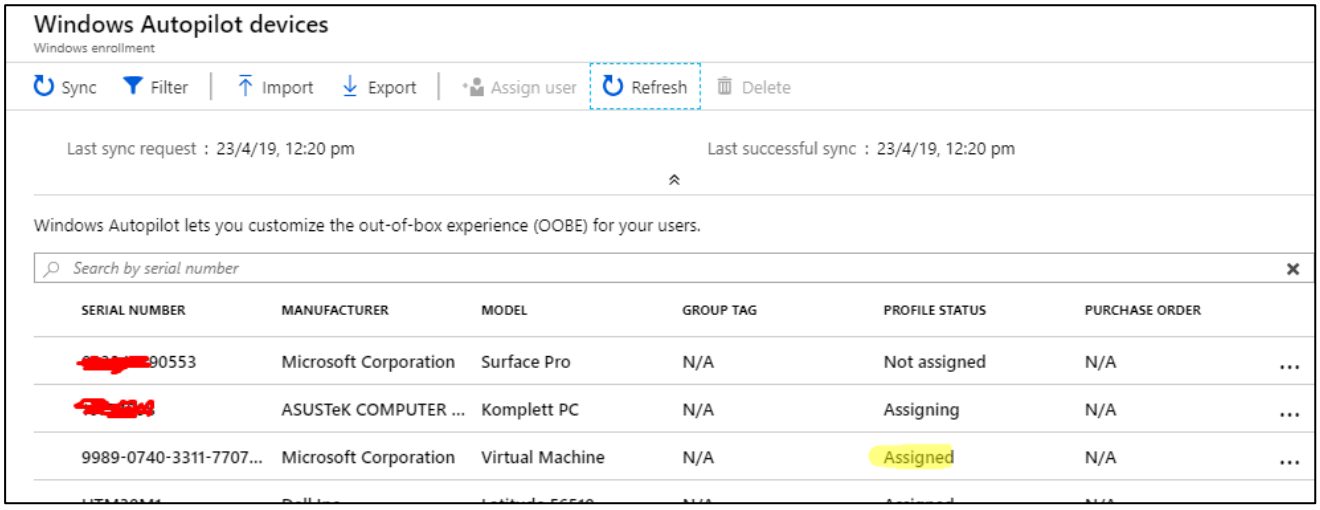



Vi søker opp enheten, trykker på *Add* og deretter *Select*.

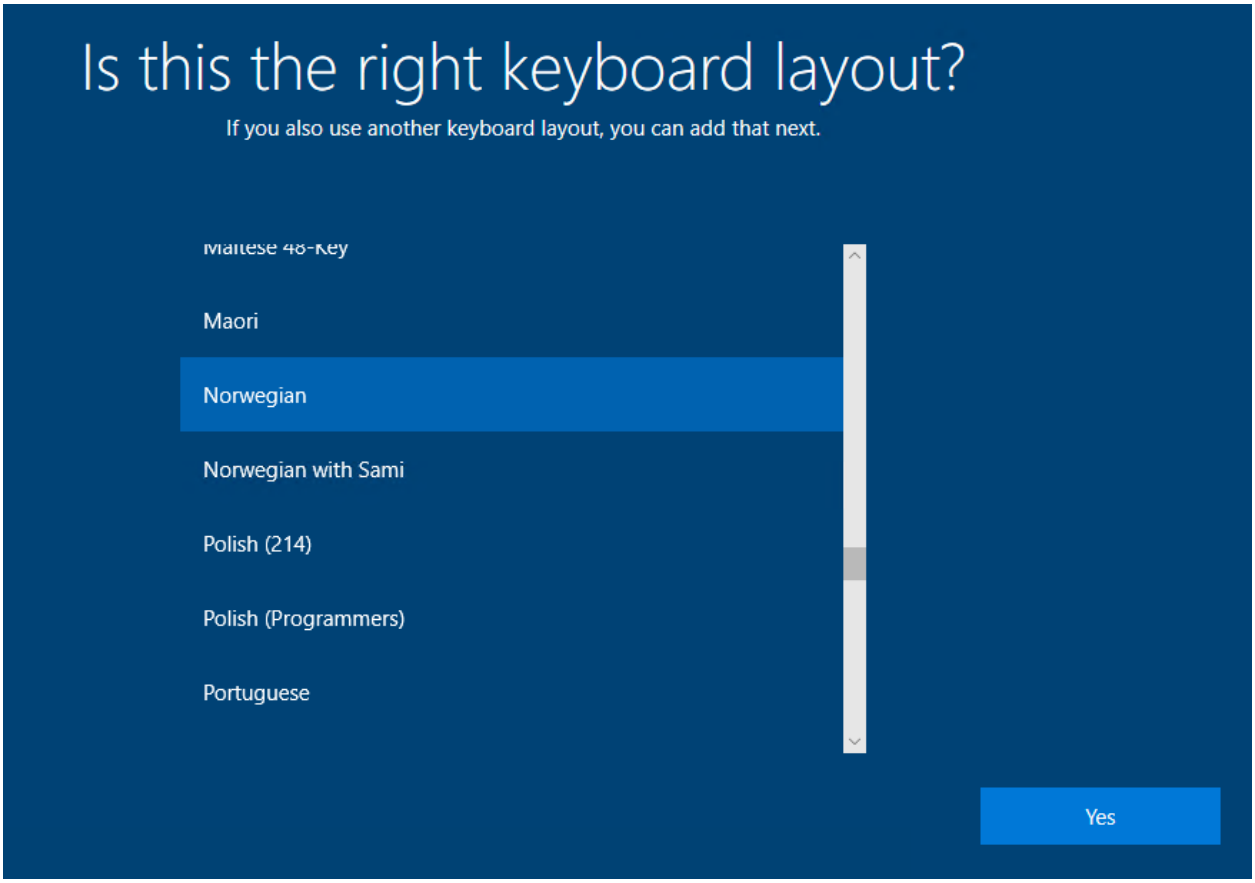



Vi ser nå at enheten er lagt inn i gruppen, og kan sjekke status.

Her ser vi at enheten nå har fått tilegnet en profil.

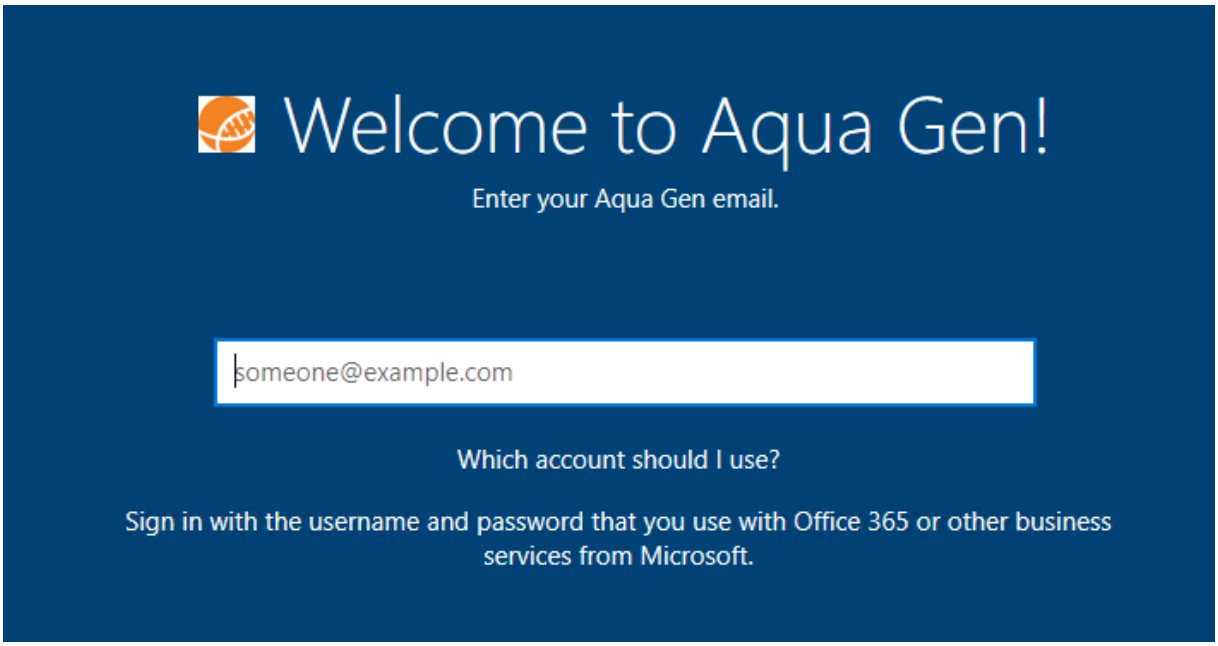


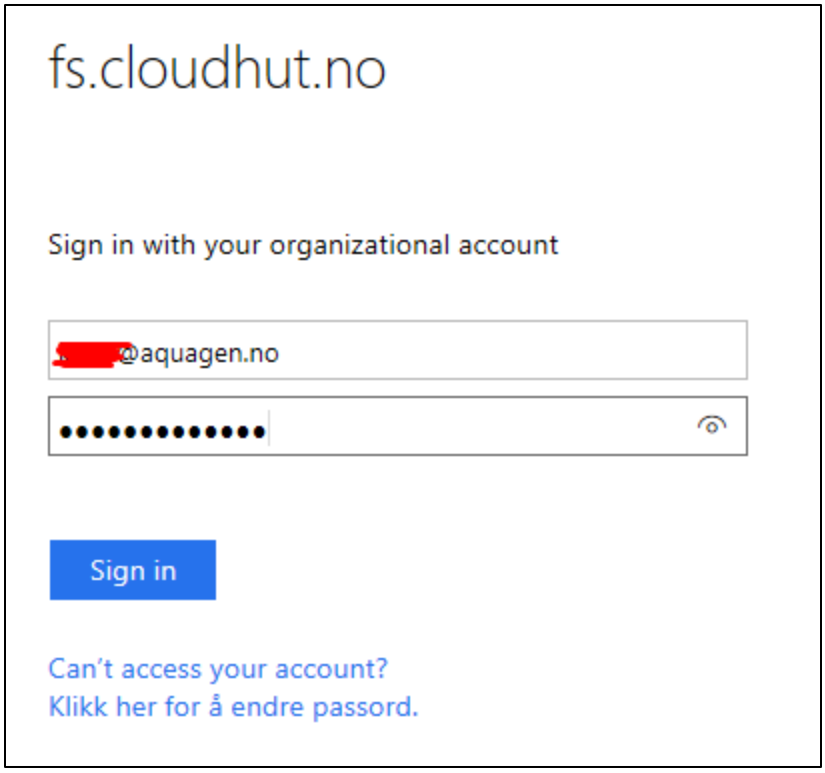
Vi kan nå starte opp den aktuelle maskinen for å se om den henter ned riktig konfigurasjon.




Velger først språk og tastatur-layout og trykker neste.

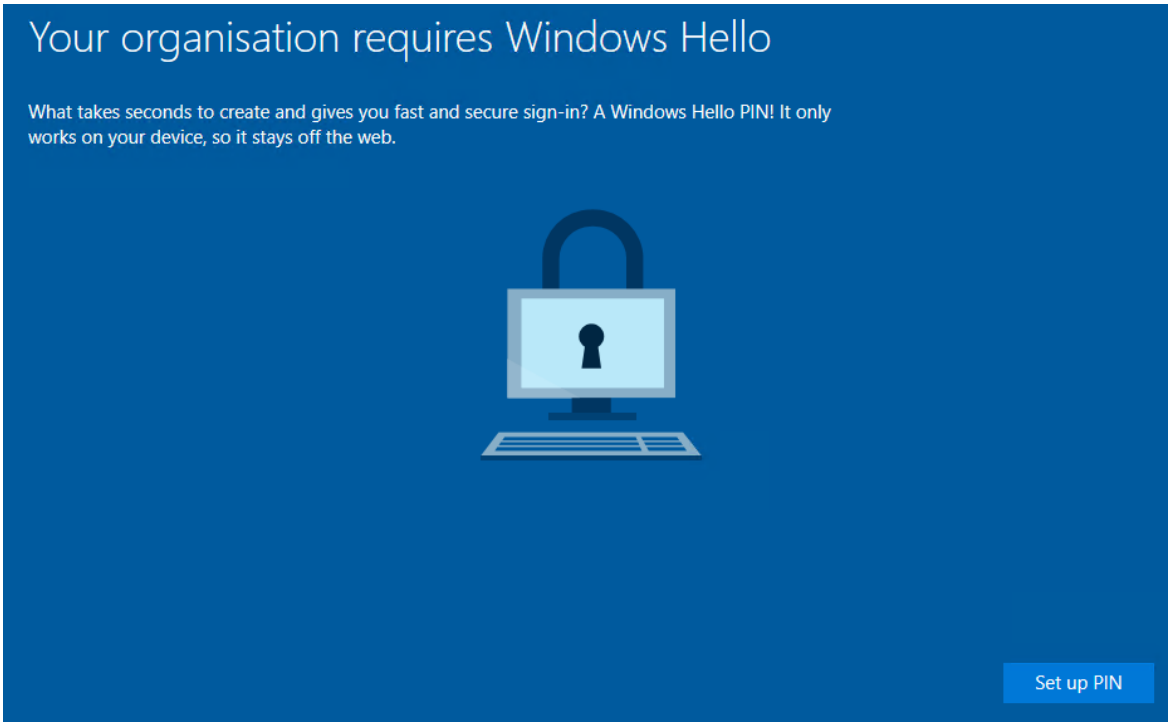
Maskinen starter så på nytt, og laster inn en del innstillinger før vi blir møtt med dette innloggingsvinduet.





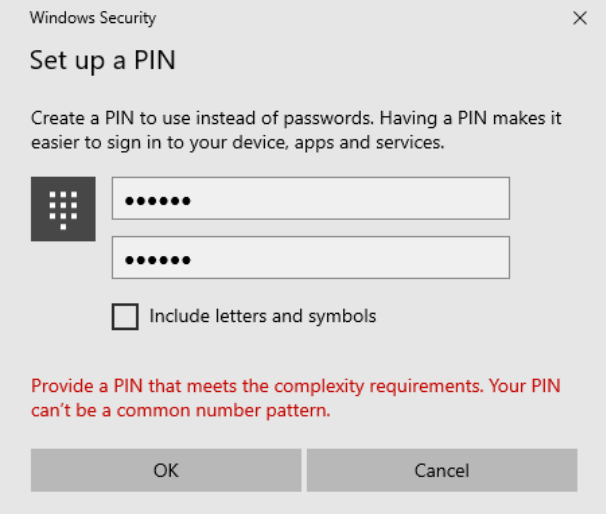

Vi skriver så inn e-postadressen, og blir tatt til en ny innloggingside.

- Denne innloggingsiden vil være forskjellig fra organisasjon til organisasjon.
- Har man 2-faktor autentisering vil man også bli spurt om å autentisere seg her.

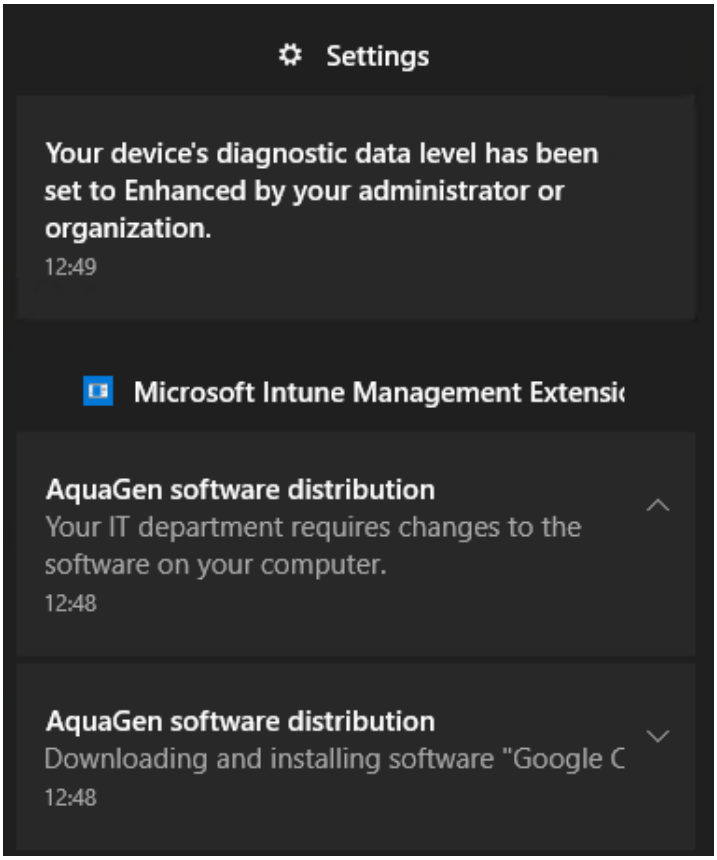



Siden vi har satt egne policyer på passord-sikkerhet, er vi nødt til å sette en egen PIN første gang vi logger på enheten.

- Denne koden/passordet blir kun gyldig på denne enheten.




Som man ser vil ikke standard-koder slik som '123456' og '123123' virke her, da vi har blokkert dette.



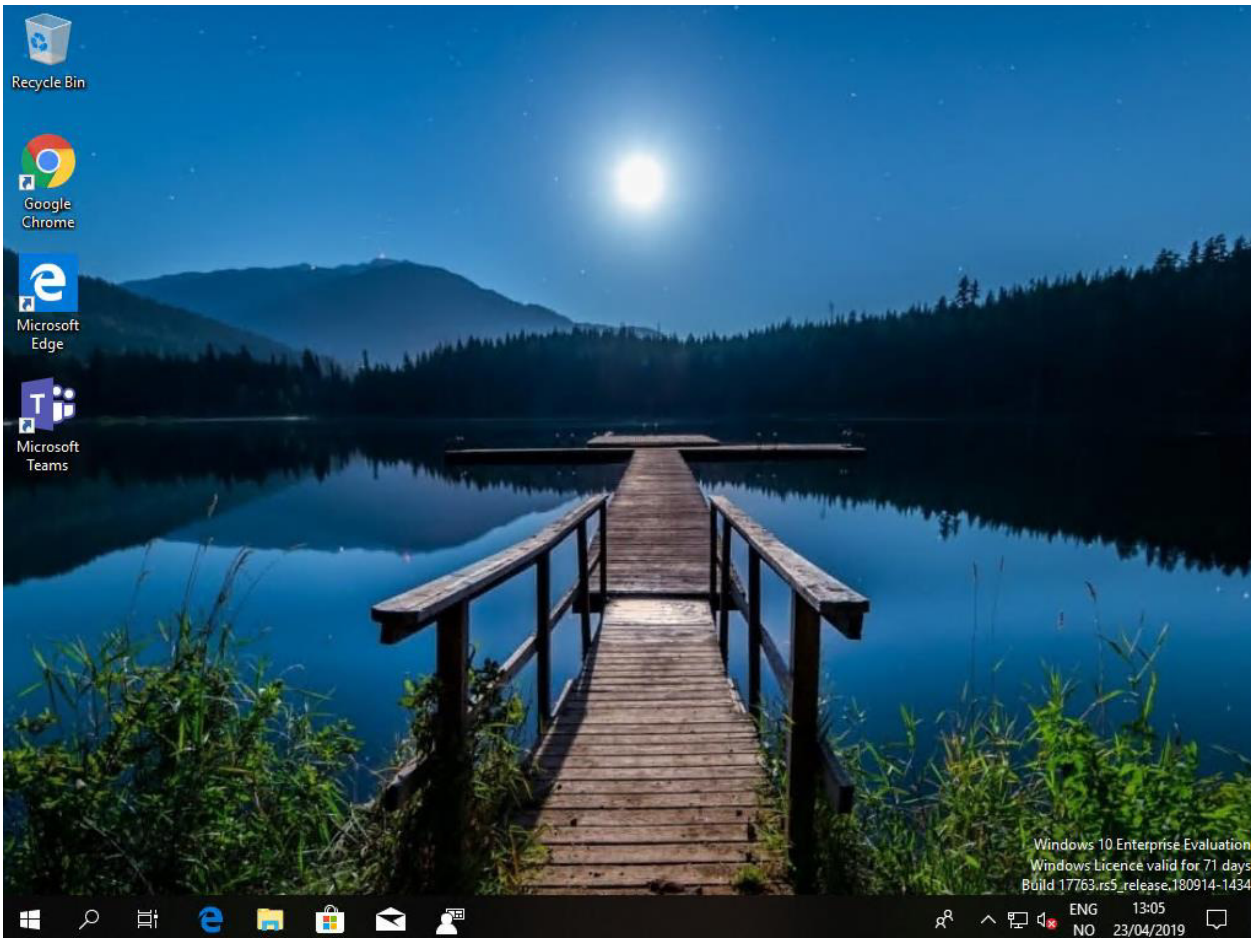

Når vi har fått ordnet passord og logger inn ser vi at enheten straks begynner å hente inn innstillinger satt av organisasjonen.


Vi ser også at Chrome har blitt installert.

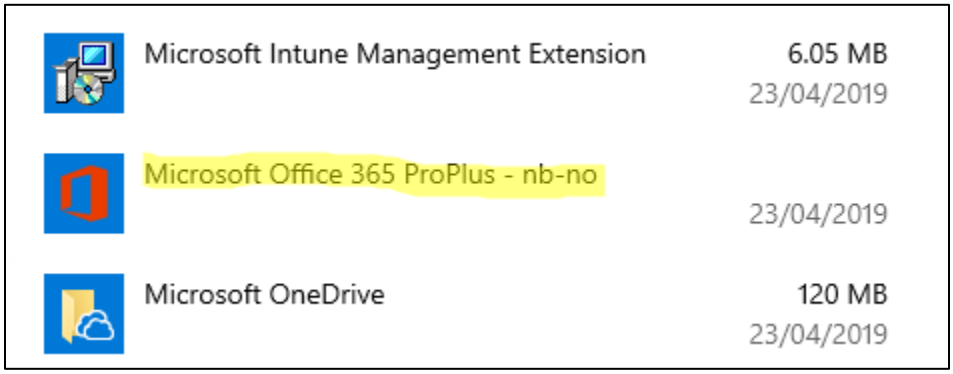
**Vi ser derimot at noen andre applikasjoner, blant annet Office 365, ikke enda er blitt installert.**

- Det tar typisk litt tid å installere større applikasjoner.


Vi forsøker med en omstart av maskinen, og kan nå se at bakgrunnsbildet har blitt endret.




Sjekker vi status nå kan vi se at riktig versjon av Office 365 er blitt installert




**Maskinen har altså blitt rullet ut automatisk med Windows Autopilot, og brukeren kunne logge seg rett inn og få alle applikasjoner som er tilegnet kontoen.**

## Fase 7: Self-deployment med Autopilot

En annen egenskap med Autopilot er at man kan rulle ut maskiner automatisk, nesten helt uten noen form for interaksjon fra brukeren.

Det betyr at maskiner kan settes opp i bulk av IT-avdelingen, kun ved hjelp av maskinvare-IDen enheten har. I utgangspunktet kan maskinene da sendes rett til brukeren noe som sparer tid og kost for IT-avdelingen.

I dette eksempelet bruker vi en fysisk PC, da man ikke har all nødvendig maskinvare i de virtuelle maskinene til å utføre *self-deployment.*

**Det skal bemerkes at denne funksjonen fortsatt er under utvikling under prosjektets gang, og at den derfor ikke innehar all funksjonalitet som den antageligvis vil få når den blir ferdig**

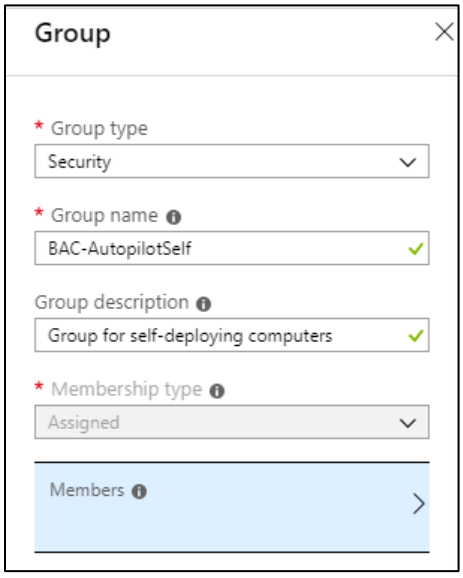
- Per dags dato må man tilegne policyer, innstillinger og Microsoft Store-apper **direkte** til datamaskinen når man kjører en såkalt *self-deployment*. Det vil si at det ikke hjelper om brukeren som logger seg inn har tilegnet disse innstillingene og appene. Det antas at støtte for dette blir lagt inn senere.

Vi starter med å importere maskinvare-ID på samme måte som tidligere.

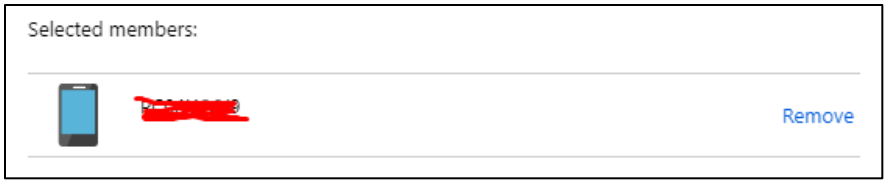
Maskinen vi bruker har allerede Windows, så vi henter ut maskinvare-ID som vist i fase 4 før vi reinstallerer maskinen.

| SERIAL NUMBER | MANUFACTURER | MODEL | GROUP TAG | PROFILE STATUS | PURCHASE ORDER | |
|---|---|---|---|---|---|---|
| [redacted] | Microsoft Corp... | Surface Pro | N/A | Not assigned | N/A | ... |
| [redacted] | LENOVO | 20BUS3GN02 | N/A | Not assigned | N/A | ... |

Her ser vi at den nederste enheten har blitt importert. Den er enda ikke medlem av noen gruppe, og har derfor heller ikke fått tildelt noen profil.

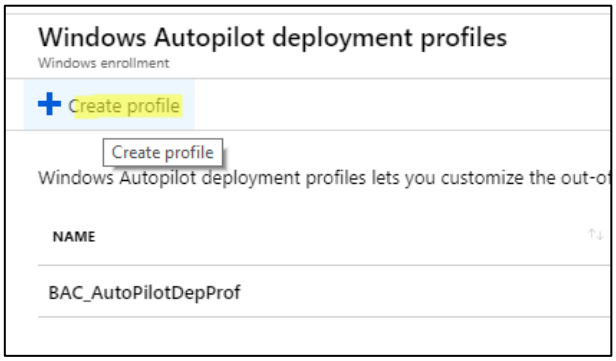


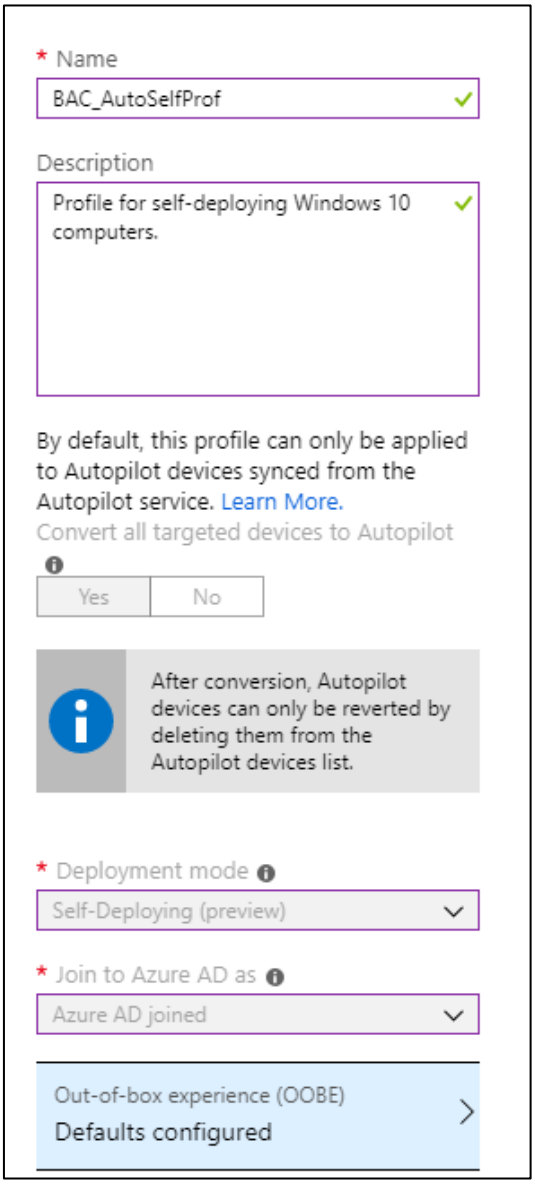

Vi oppretter en gruppe til maskinen ved navn *BAC-AutopilotSelf*.




Vi legger inn maskinen vi akkurat importerte inn i gruppen.

Vi går inn på *Autopilot deployment profiles* og oppretter en ny profil

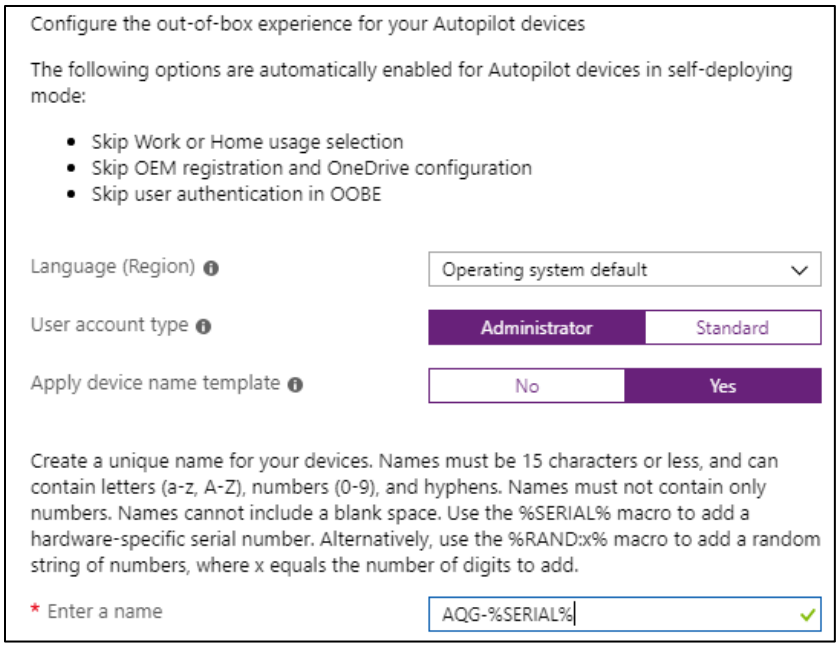


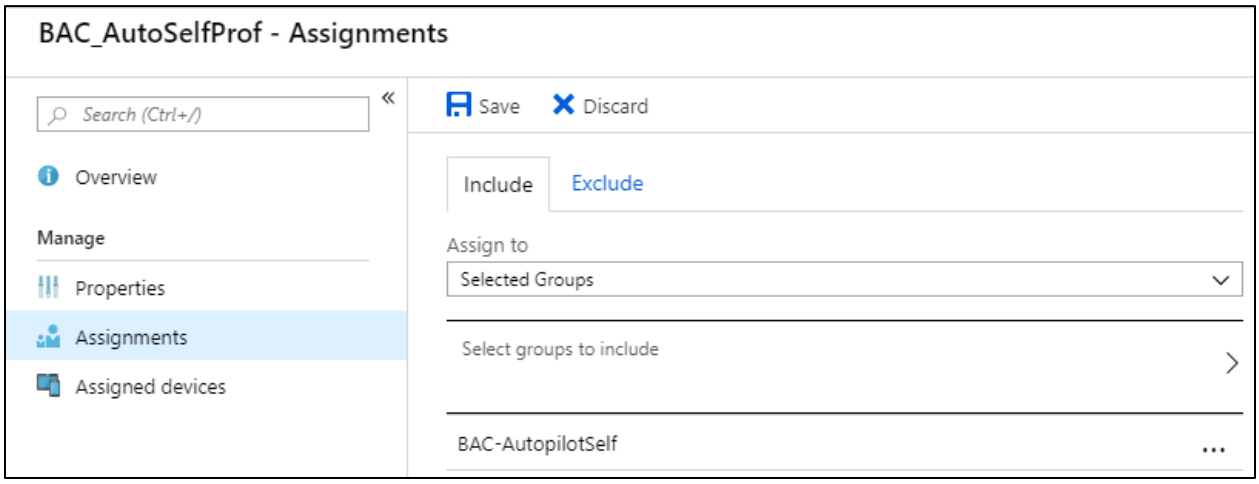

Vi oppretter deretter en *Deployment profile* med følgende egenskaper

- Når man velger *Self-Deploying* under Deployment mode vil man være låst til kun *Azure AD joined*. Man har deretter litt begrensede muligheter sammenlignet med «manuelle» Autopilot-enheter inntil videre

I *Out-of-box experience* setter vi følgende innstillinger

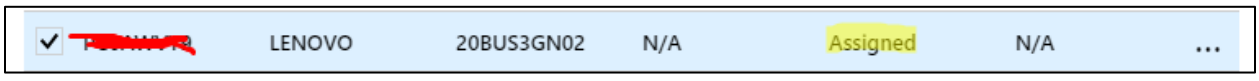



Når vi har opprettet profilen tilegner vi den til gruppen som maskinen ligger i.



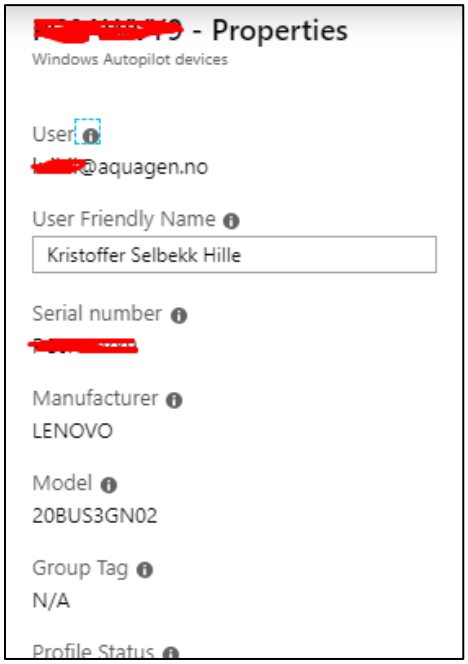

Vi går nå tilbake til *Devices* under Autopilot og ser at enheten nå har blitt tildelt en profil.

- Det kan ta litt tid før profilen faktisk når maskinen, alt fra 1 til 10 minutter

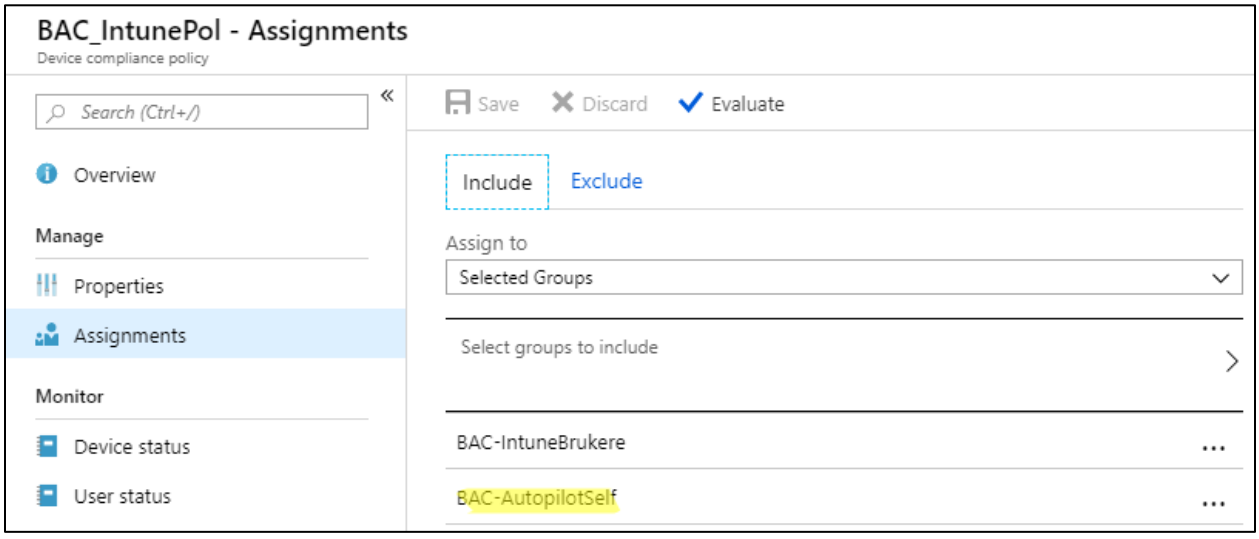


Vi trykker på *Assign User* og legger til en bruker som «eier» av maskinen

- Dette er kun for å lettere holde orden på enhetene – at brukeren blir lagt inn her betyr **ikke** at den også blir lagt inn på maskinen. Brukere må fortsatt logge seg inn på maskinen manuelt.

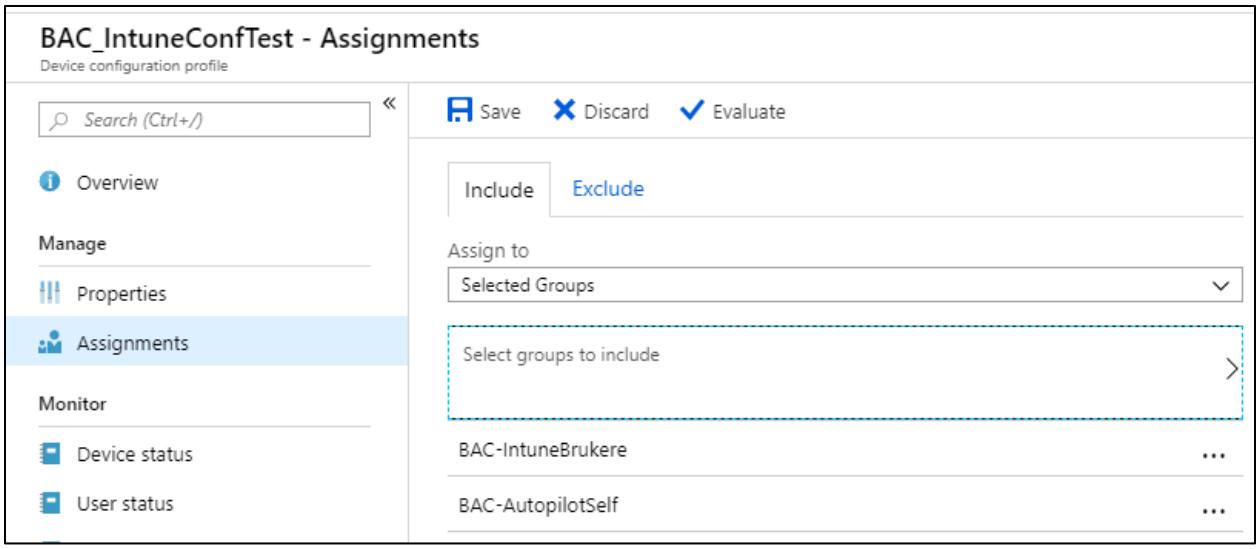



Siden vi må tilegne policyer, innstillinger og apper direkte til gruppen maskinen er i, gjør vi dette nå.

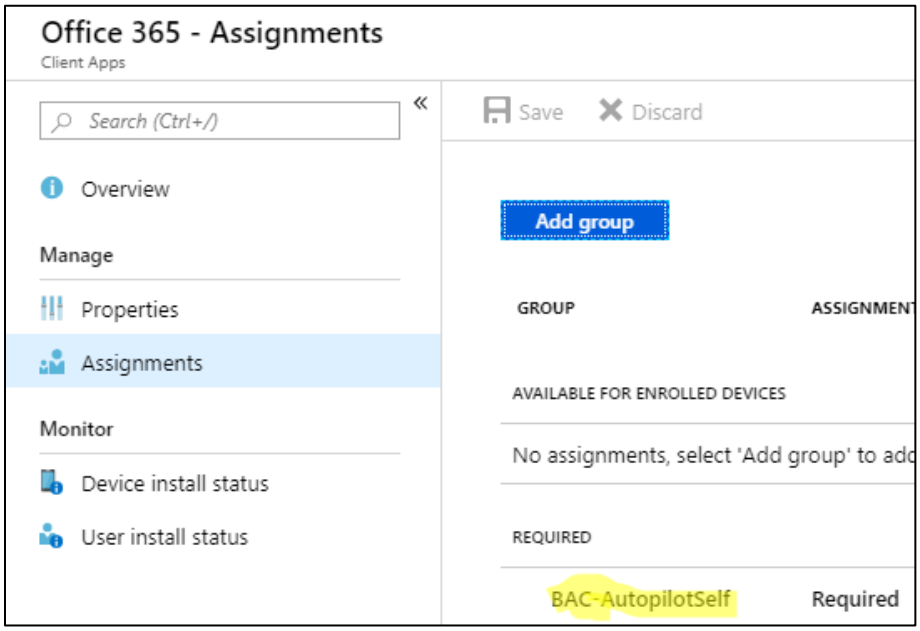


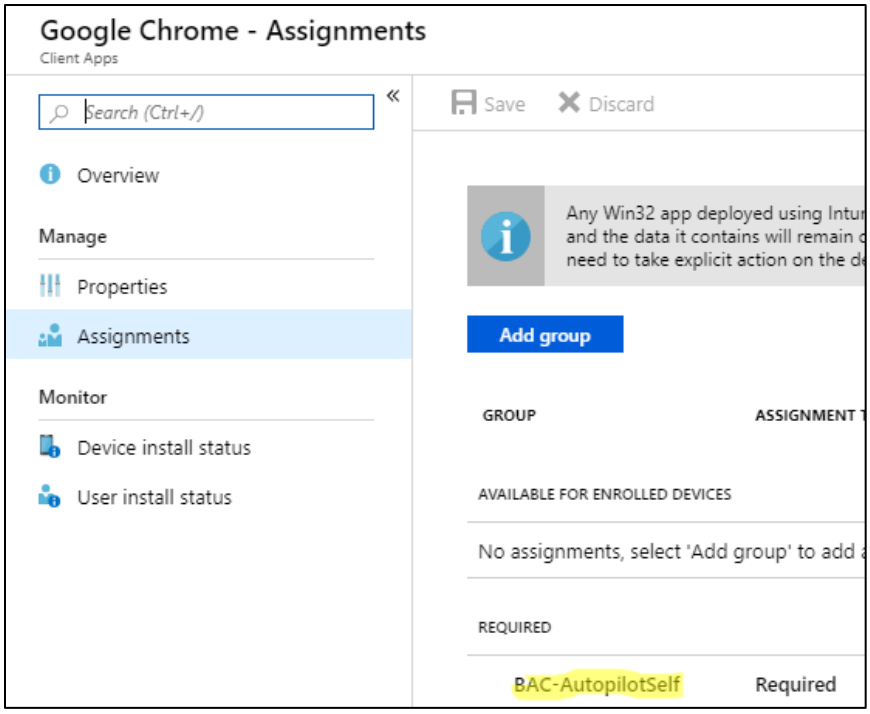

Her er policyen *BAC_IntunePol* tilegnet enhets-gruppen *BAC-AutopilotSelf* som inneholder den aktuelle maskinen.

Vi gjør det samme også på *device configuration* ved navn *BAC_IntuneConfTest*




Og det samme på appene Office og Chrome

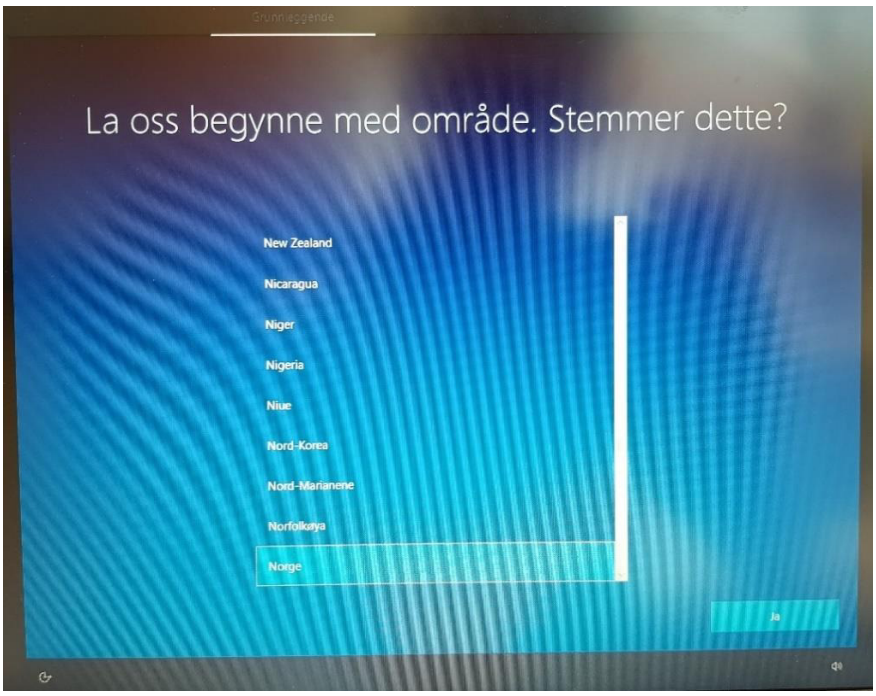




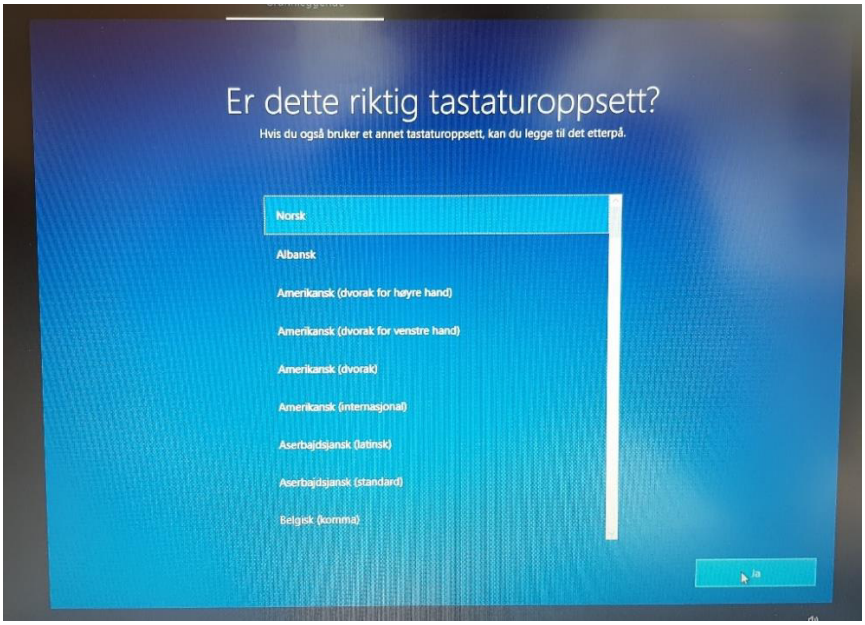

**Vi skal nå prøve å reinstallere Windows på maskinen for så å rulle den ut ved hjelp av Autopilot.** Siden vi har importert maskinvare-IDen skal enheten nå få konfigurasjonen sin og sette seg selv opp automatisk.

- Bildene nedenfor er tatt med mobilkamera da man ikke enkelt får tatt skjermbilde under installasjonsprosessen

Etter ny installasjon av Windows blir vi møtt med denne skjermen



Her velger man språk som skal brukes på enheten.

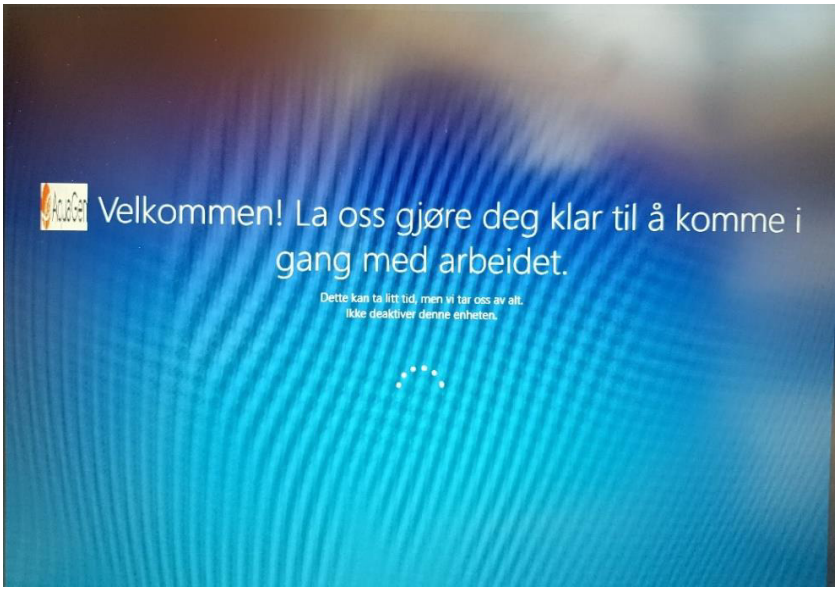



Videre må man velge riktig tastatur-oppsett. Trykker ja for å gå videre.

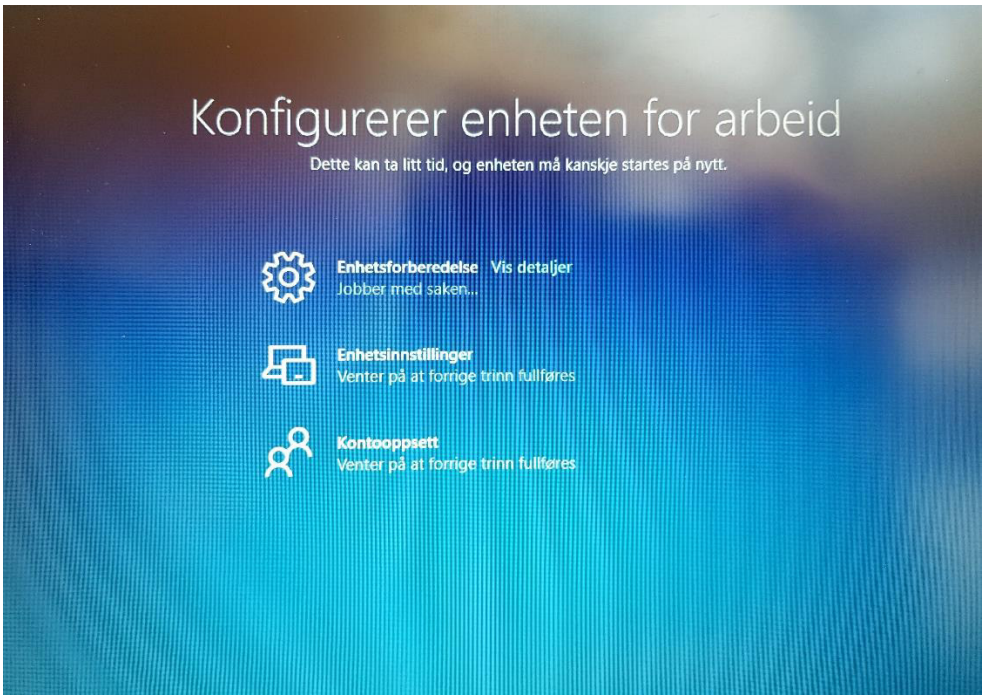
I neste steg kobler maskinen seg mot nettverket.

- Hvis man har plugget inn maskinen ved hjelp av nettverkskabel, som gjort her, vil maskinen automatisk hente innstillingene for å koble seg mot Internett
- Har man ikke nettverkskabel tilgjengelig kan man i dette steget koble seg opp mot et WiFi-nettverk.

Når maskinen har koblet seg opp mot nettverket vil den etter hvert starte på nytt for å sette blant annet enhetsnavnet.



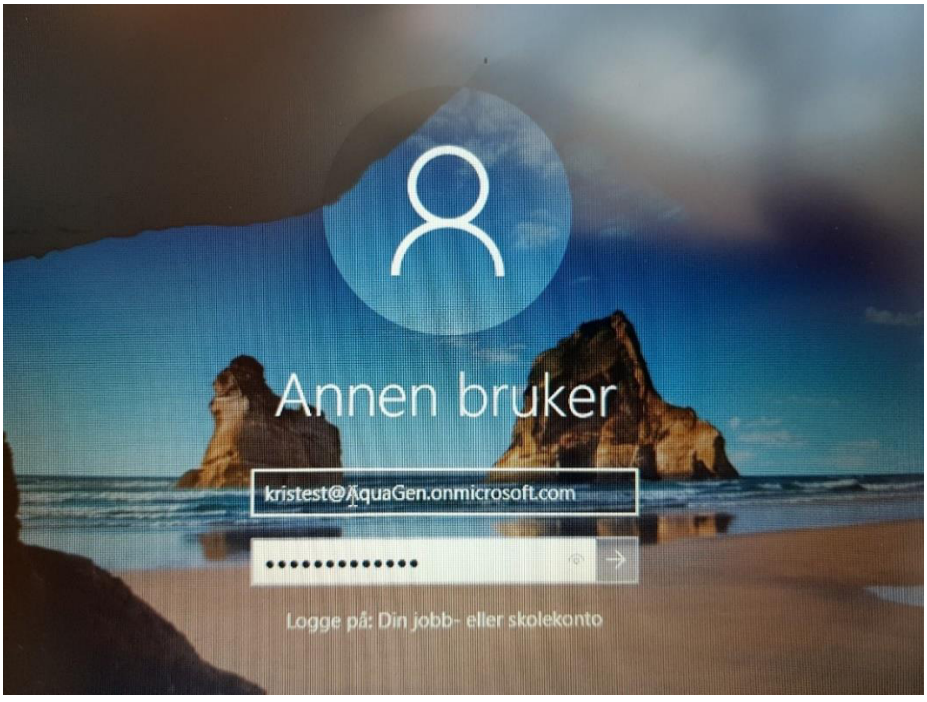
Her ser man at maskinen nå har hentet ned innstilligene fra Azure, og begynner installasjonsprosessen på egenhånd




Her får vi opp statussiden som forteller hvor langt man er kommet i konfigureringen.

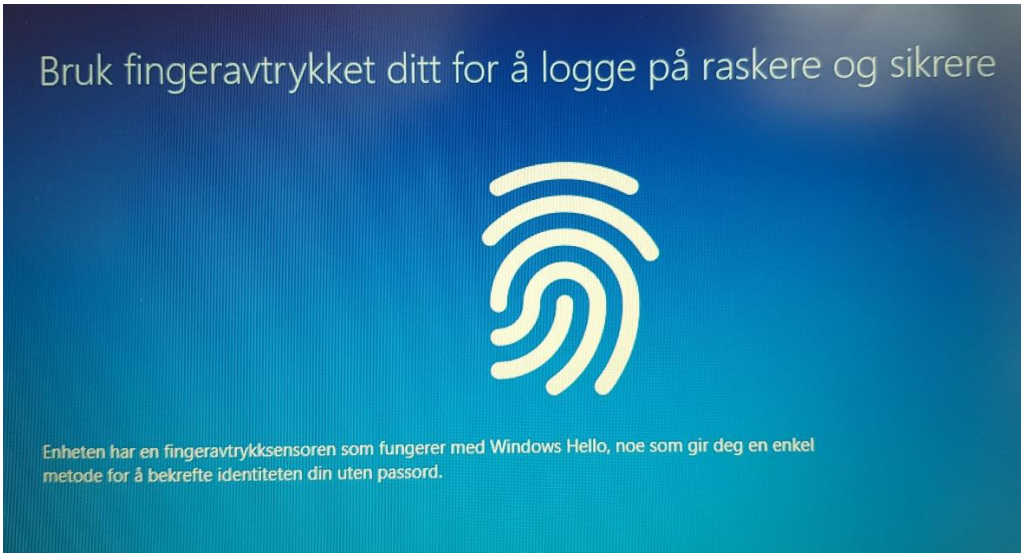
- Som vist i Fase 1 kan man tilpasse denne statussiden. Denne er imidlertid kun mulig å tilegne til bruker-grupper, og fungerer altså ikke med enhets-grupper inntil videre.

Når enheten er ferdig med å konfigurere kommer man inn til innloggingsbildet på maskinen.



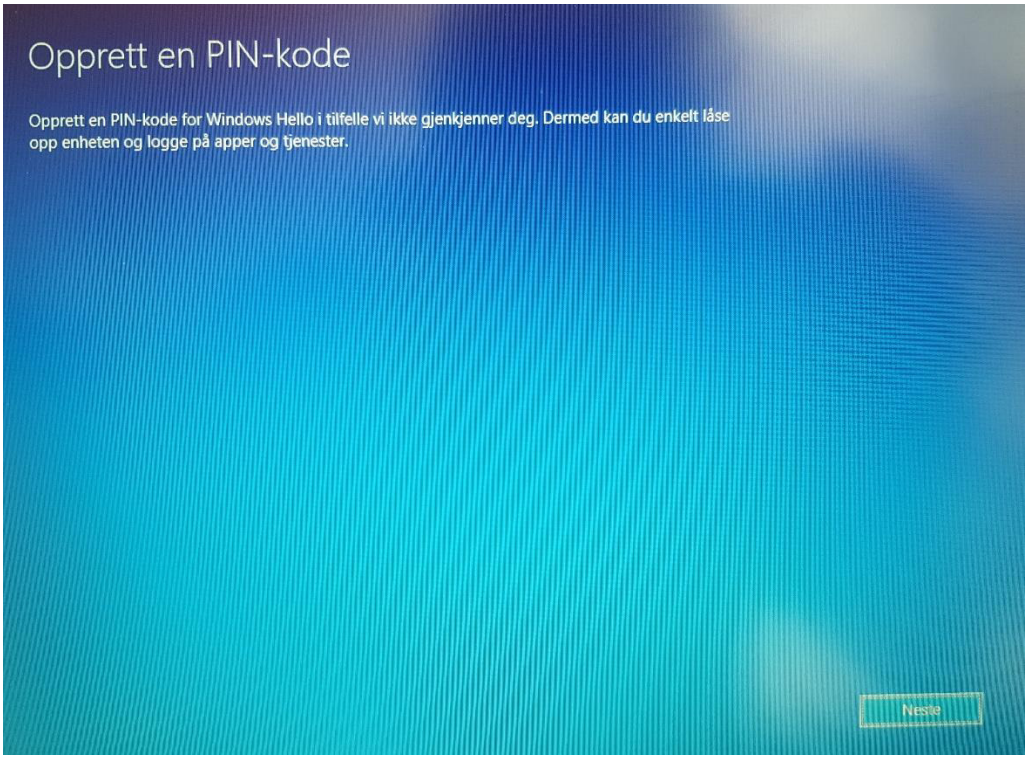
Her kan man logge inn med sin Office 365-bruker, som man gjør ellers.

- Som nevnt fungerer *Self-deployment* kun med Azure AD-brukere for øyeblikket. Vi må derfor bruke en ren Azure-bruker for å logge inn her.



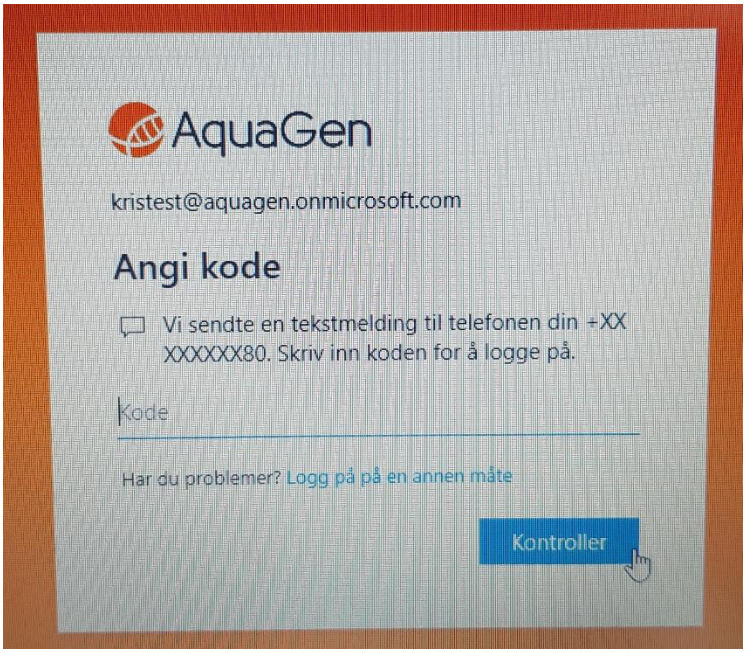

Siden denne maskinen har en fingeravtrykksleser vil Windows Hello spørre brukeren om man ønsker å bruke dette som en påloggingsmetode.

- Det finnes også kamera som kan brukes med Windows Hello til å åpne opp enheten på samme måte som med mange moderne smarttelefoner i dag.

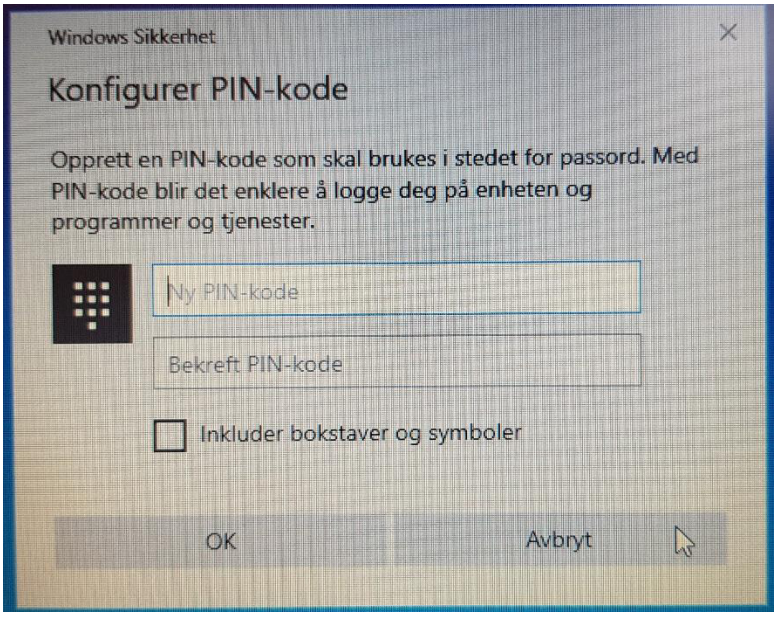


Etter å ha lagt inn fingeravtrykk blir man også bedt om å legge inn en egen PIN-kode, i tilfelle man ikke får logget seg inn med fingeravtrykk lenger.

- Maskinen vil uansett be om PIN-kode uavhengig av man bruker fingeravtrykksleser, basert på krav satt i policyen som enheten ligger under.

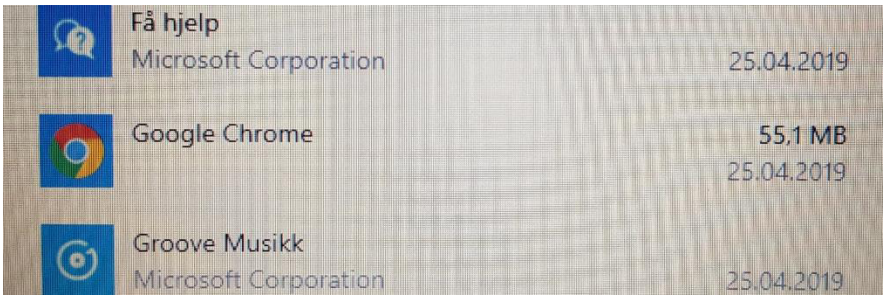


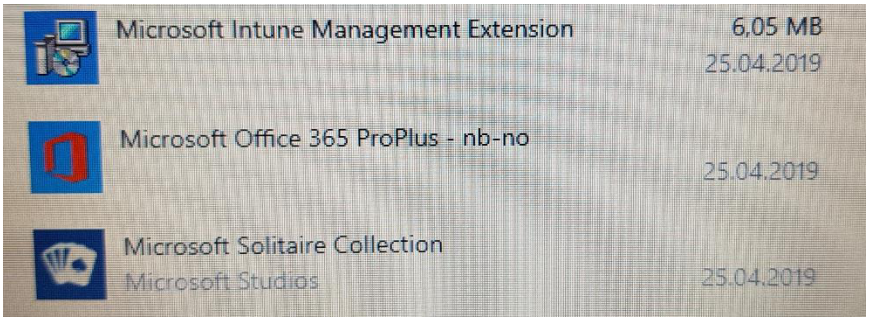

Har man også to-faktor autentisering på brukeren vil man bli forespurt å skrive inn kode som kommer på ønsket måte.



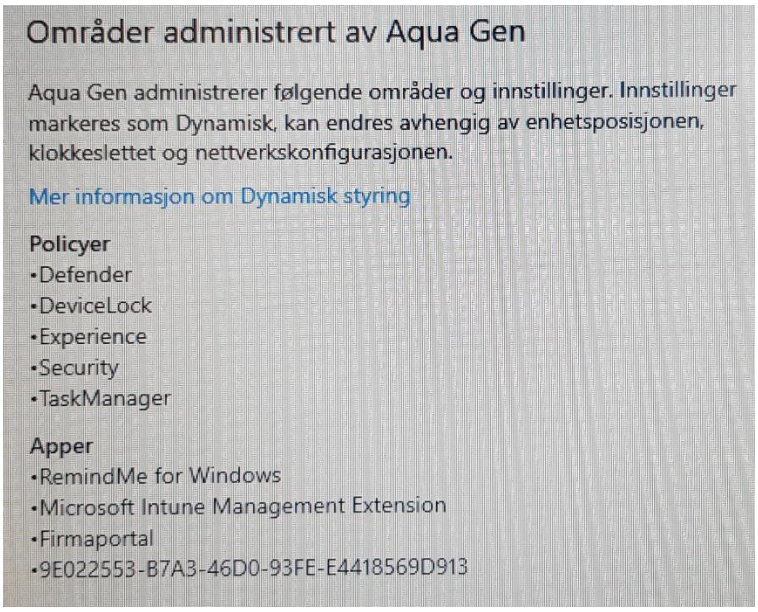

Skriver inn ønsket PIN-kode her.

- Som satt via policyen vil denne PIN-koden ha begresninger slik at man ikke setter enkle passord som «123123» etc.




Som vi kan se har både Google Chrome og Office 365 blitt installert på enheten.




Går vi inn på *Kontoer* i *Windows-innstillinger* kan vi se hvilke områder det er som blir administrert av Intune. Dette gir en god pekepinn på hva som faktisk er blitt konfigurert på maskinen.

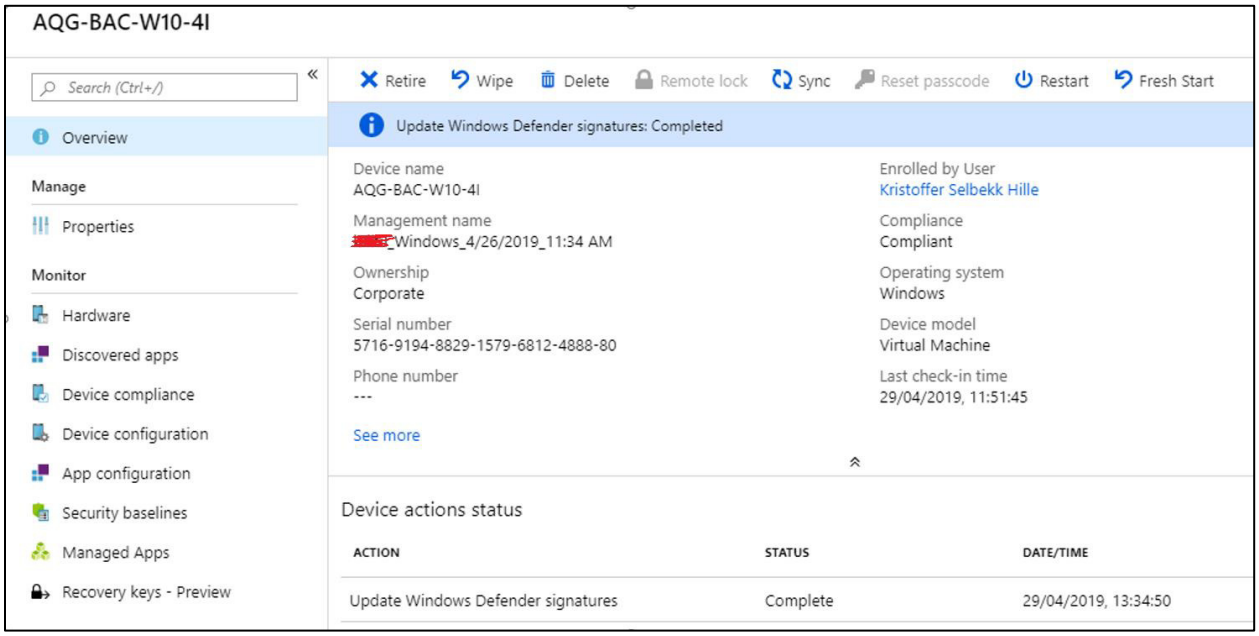
**Maskinen har altså satt seg selv opp på egenhånd.**

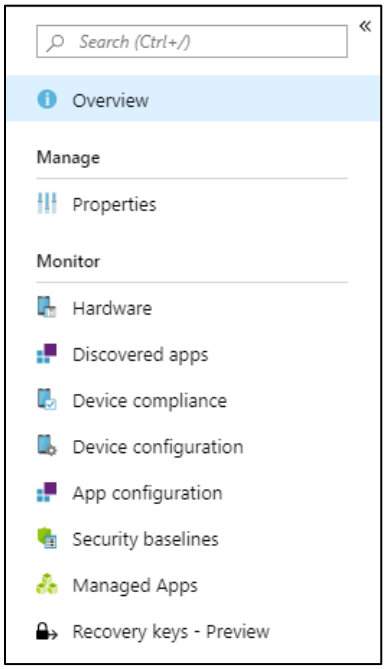
## Fase 8: Test av funksjonalitet i Microsoft Intune

Når en maskin er lagt inn i Intune har man fått kontroll over denne enheten. Man kan for eksempel kjøre en fjernsletting, starte enheten på nytt, gi den nytt navn, slette spesifikt data og mer.

Vi skal gå gjennom de ulike funksjonene vi har tilgjengelig i Intune nedenfor.

Når man har klikket seg inn på en enhet i Intune, får man opp følgende bilde



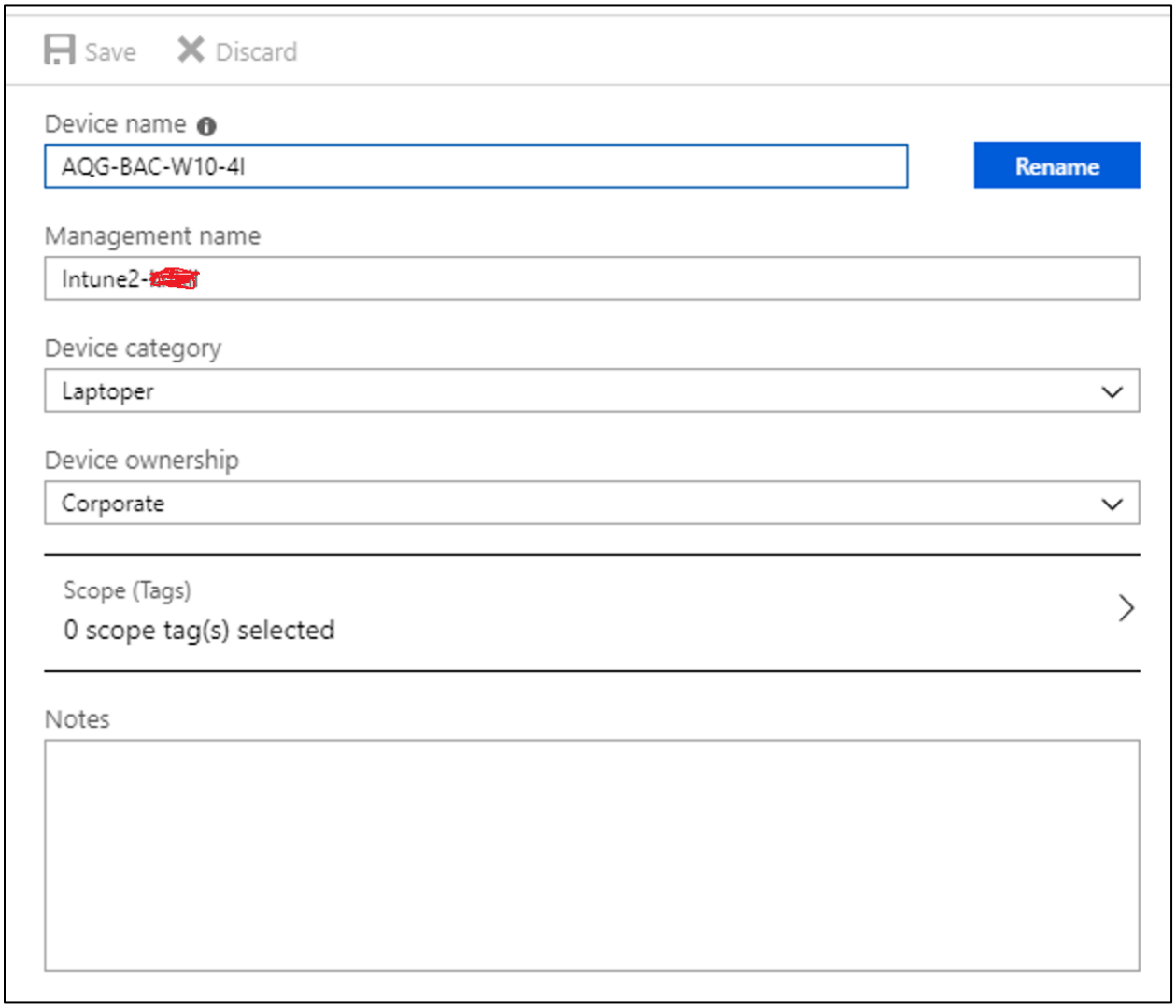

Bildet over viser oss en oversikt over den aktuelle enheten. Her kan vi se detaljer som navn, administreringsnavn, eierskap, serienummer, hvilken bruker som er tilknyttet enheten, operativsystem osv.

Til venstre har man en kolonne som viser egenskaper, samt de ulike delene av enheten som kan overvåkes.


Horisontalt har man en linje med forskjellige funksjoner som man kan utføre på enheten.

- Tilgjengeligheten på disse er avhengig av hvilken enhet man er på. Windows 10-maskiner har for eksempel ikke mulighet til *Remote Lock.*

## Properties (Egenskaper)

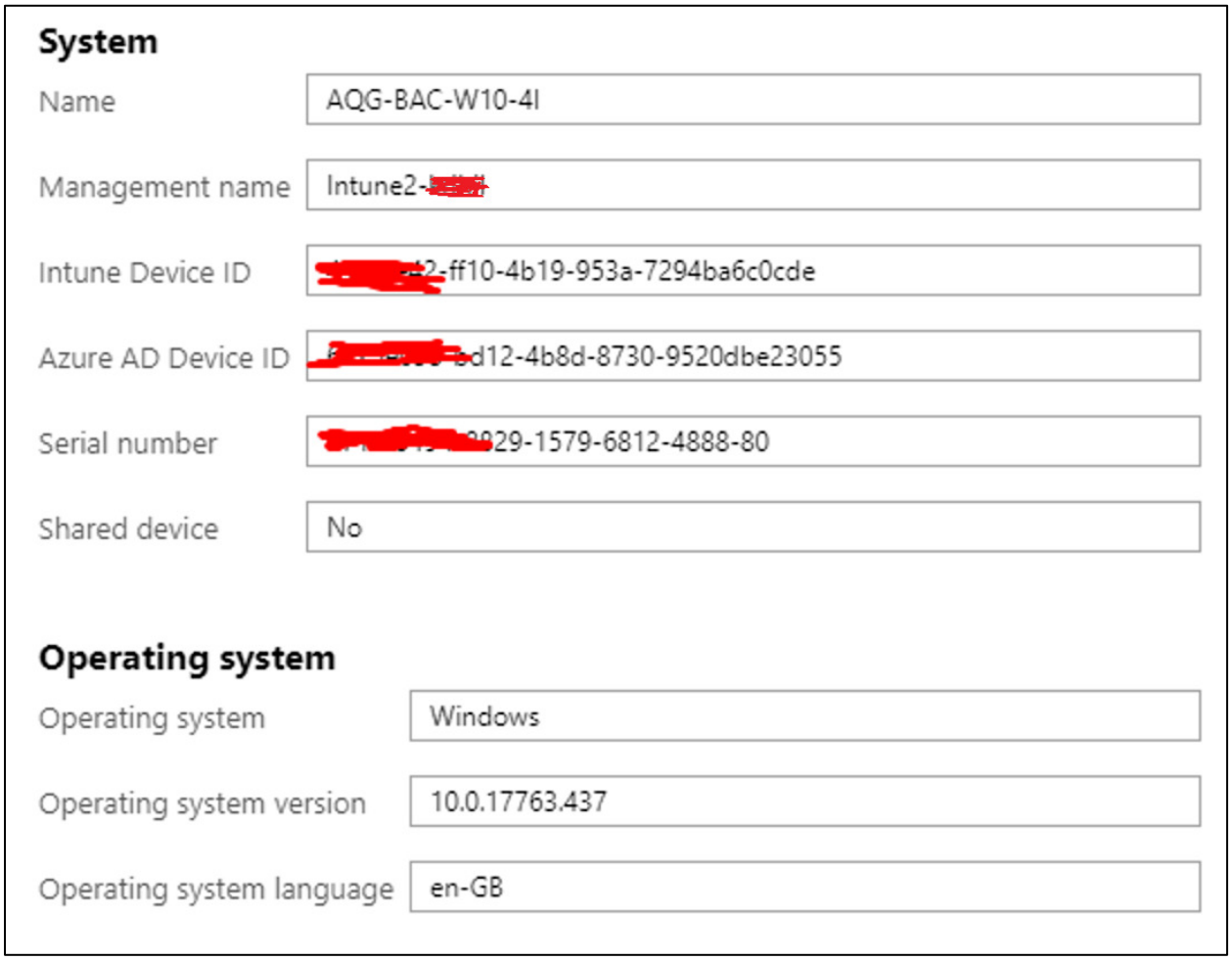



Under *Properties* kan man endre noen av de egenskapene som man så i oversiktsbildet, blant annet enhetsnavnet, administrasjonsnavn, enhetskategori og eier av enheten. Man kan også legge inn *scope tags* og eventuelle notater.

## Overvåkning av enheten

Vi begynner med å beskrive de ulike delene av enhetene som kan overvåkes

### Hardware




*Hardware* beskriver mer I detalj maskinvaren som enheten består av og kjører på.

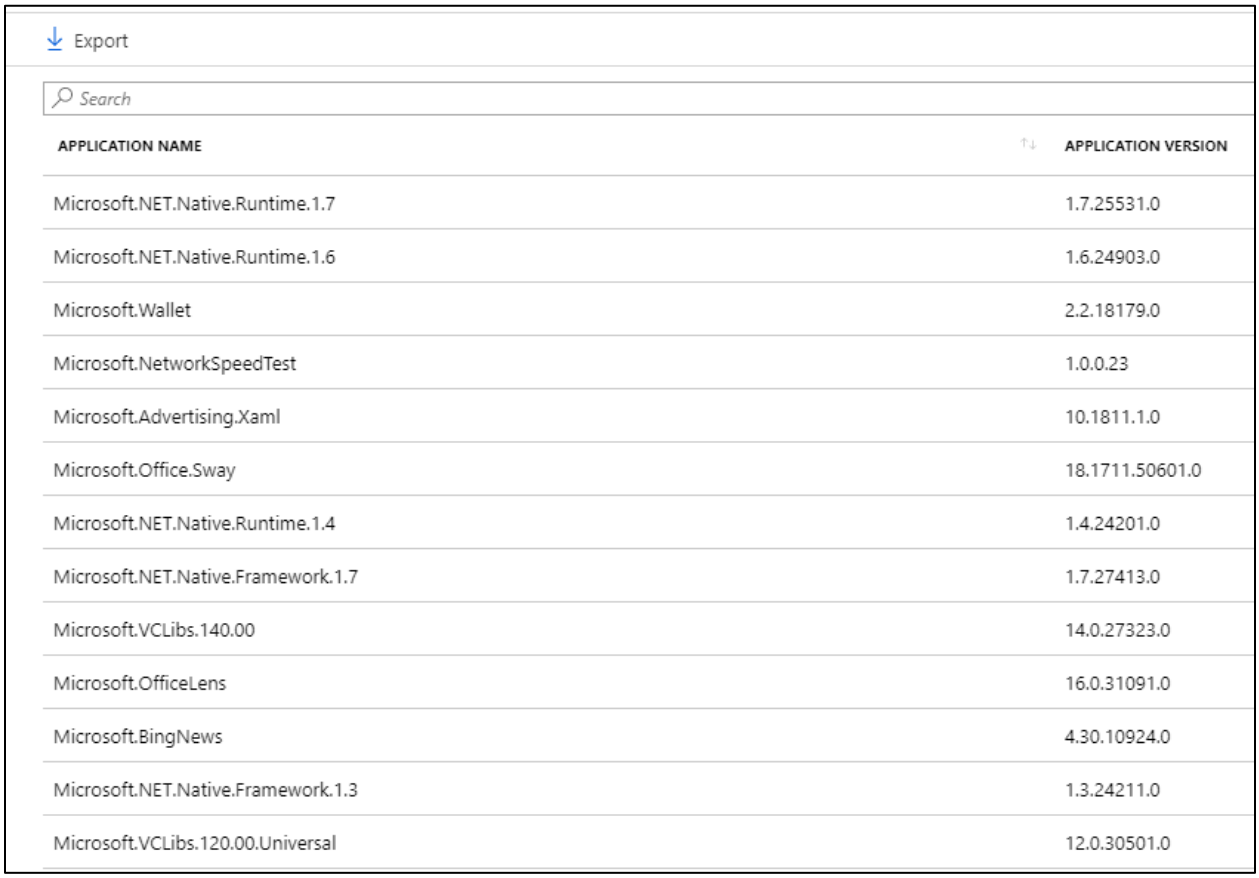
Her vil man få opp informasjon om de ulike komponentene som befinner seg i enheten, hvilket operativsystem som kjøres, serienummer på maskinen og mer.

Det finnes flere grupperinger her, blant annet:

- System
- Operating system (operativsystem)
- Storage (lagring)
- System enclosure (informasjon om enheten)
- Network details (mobiltilkobling)
- Network service (utrullingsdato, siste kontakt)
- Conditional access (hendelsesstyrt tilgang)

## Discovered apps

I denne fanen vil man finne alle applikasjoner som Intune har detektert at er installert på enheten. På en maskin med en ny installasjon av Windows vil man fortsatt finne en del applikasjon fra Microsoft her



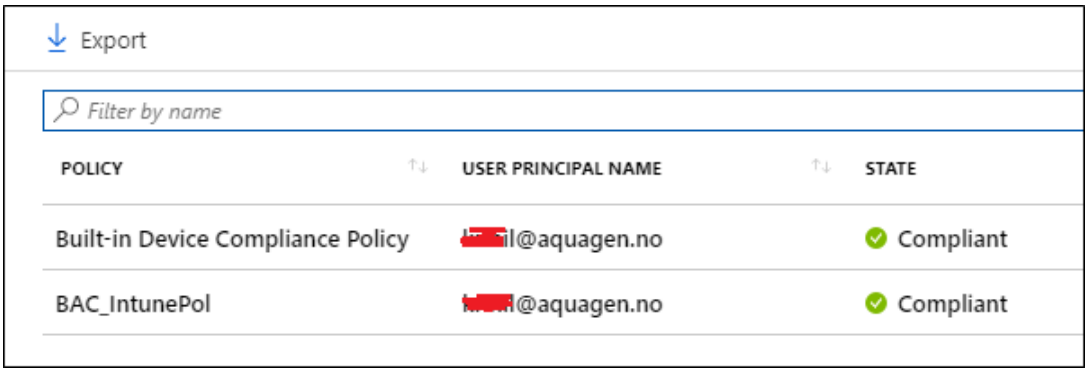

| APPLICATION NAME | APPLICATION VERSION |
|---|---|
| Microsoft.NET.Native.Runtime.1.7 | 1.7.25531.0 |
| Microsoft.NET.Native.Runtime.1.6 | 1.6.24903.0 |
| Microsoft.Wallet | 2.2.18179.0 |
| Microsoft.NetworkSpeedTest | 1.0.0.23 |
| Microsoft.Advertising.Xaml | 10.1811.1.0 |
| Microsoft.Office.Sway | 18.1711.50601.0 |
| Microsoft.NET.Native.Runtime.1.4 | 1.4.24201.0 |
| Microsoft.NET.Native.Framework.1.7 | 1.7.27413.0 |
| Microsoft.VCLibs.140.00 | 14.0.27323.0 |
| Microsoft.OfficeLens | 16.0.31091.0 |
| Microsoft.BingNews | 4.30.10924.0 |
| Microsoft.NET.Native.Framework.1.3 | 1.3.24211.0 |
| Microsoft.VCLibs.120.00.Universal | 12.0.30501.0 |

Man kan også eksportere listen over apper hvis man ønsker det.

## Device compliance

Her vises de ulike policyene som er tilegnet brukeren eller enheten. User principal name viser hvilken bruker dette er, står det «System Account» er profilen blitt tilegnet enheten direkte.

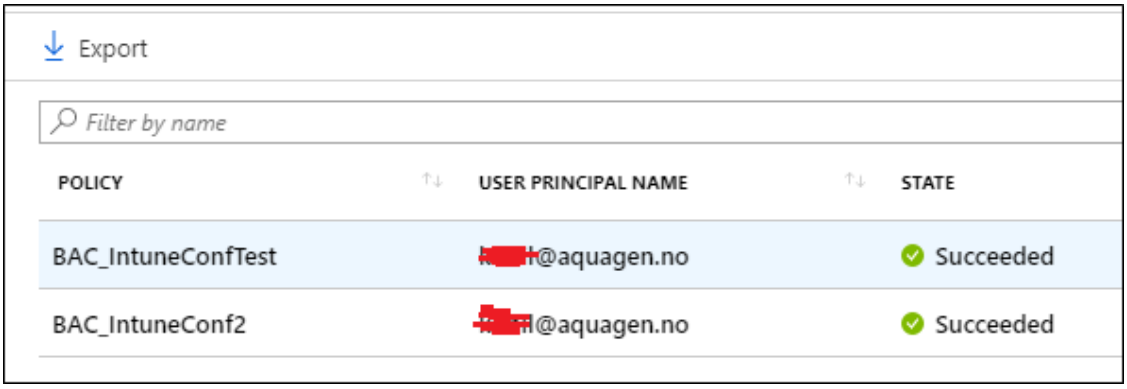
Også her kan man eksportere listen over policyer.




| POLICY | USER PRINCIPAL NAME | STATE |
|---|---|---|
| Built-in Device Compliance Policy | [redacted]@aquagen.no | Compliant |
| BAC_IntunePol | [redacted]@aquagen.no | Compliant |

## Device configuration

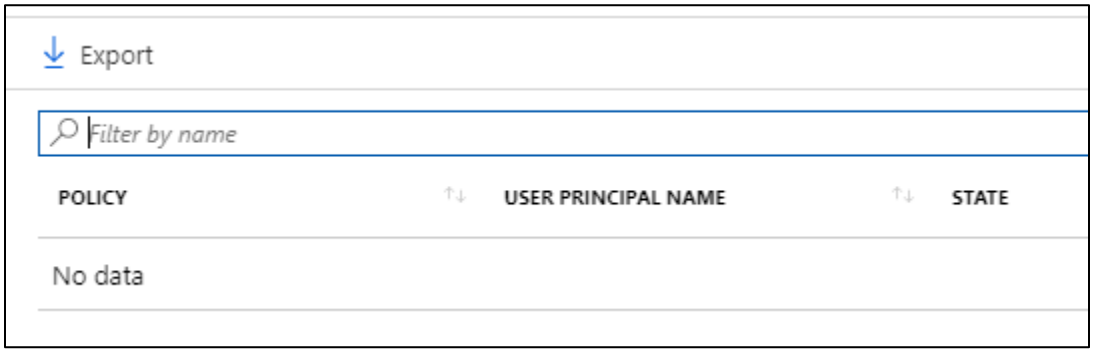
Under denne fanen får man opp de ulike konfigurasjonene som er tilegnet brukeren eller enheten. Også her viser user principal name bruker dette gjelder, evt. «System Account» om den er tilegnet enheten direkte.




## App configuration

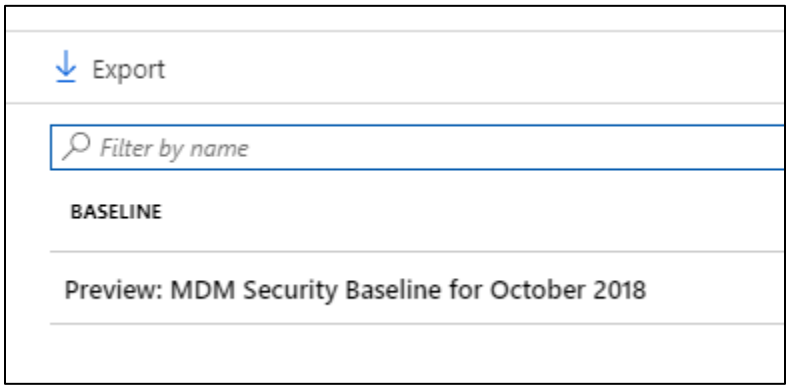
Her kan man sette egne konfigurasjoner på apper som man installerer på enheten.

- Vi har ikke satt noen her, listen er derfor tom

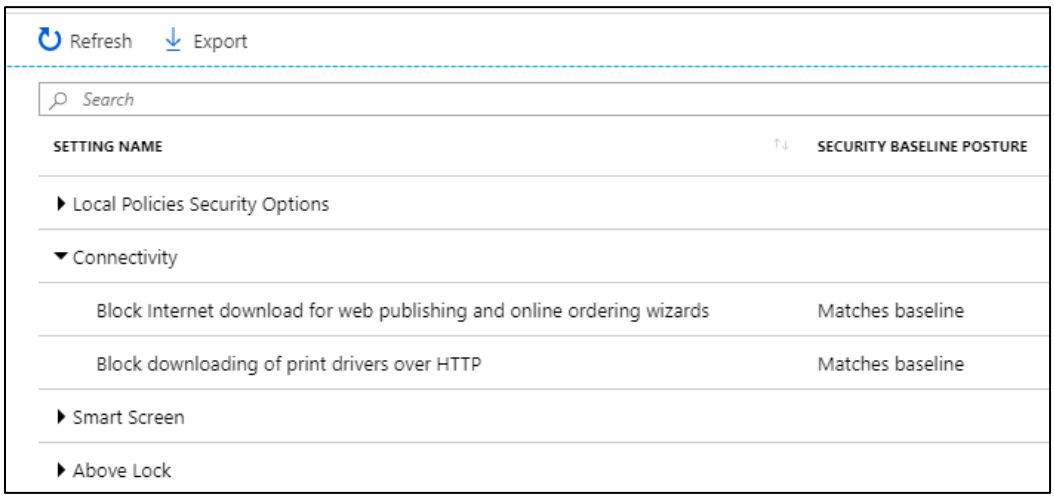



## Security baselines

Her finner man *security baselines* som er satt tidligere. Dette kan for eksempel være krav om BitLocker (kryptering), passord ved innlogging etc. Disse er basert på anbefalte innstillinger og kan være en god måte å starte med bedre sikkerhet i organisasjonen.

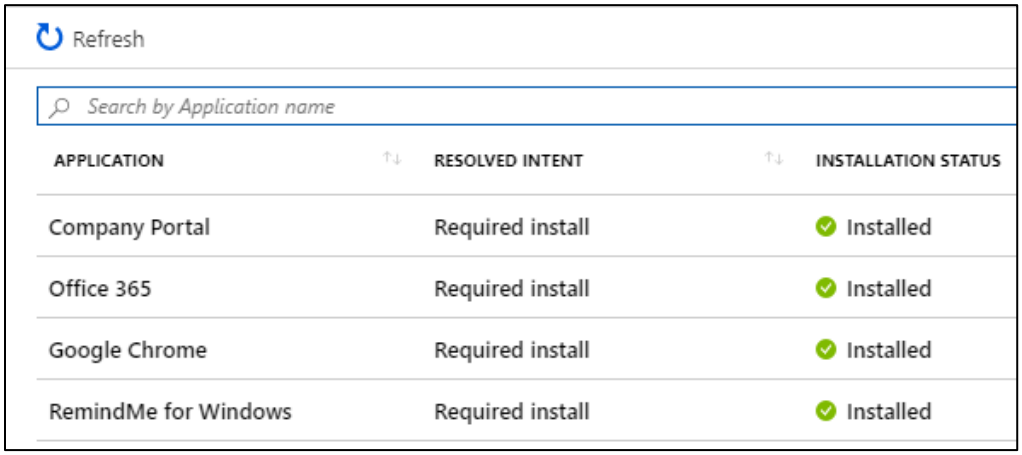


Man kan trykke seg inn på den spesifikke baselinen og se på status på de forskjellige valgene



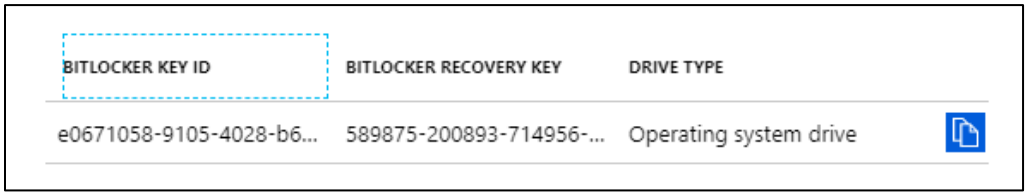

## Managed apps

Denne oversikten viser alle apper som er installert på enheten gjennom Intune/MDM. Man får også opp en status på installasjon, som forteller om appen er installert, om enheten venter på å installere eller om den ikke kan installeres.




## Recovery Keys

Hvis enheten har BitLocker aktivert vil den vise ID og gjenopprettings-nøkkel hvis man skulle ha behov for å låse opp enheten på et senere tidspunkt.




Vi har nå gått gjennom de ulike område av en enhet som kan overvåkes gjennom Intune.

I neste avsnitt skal vi se på de ulike områdene på enhet som kan administreres gjennom Intune-portalen

## Administrering

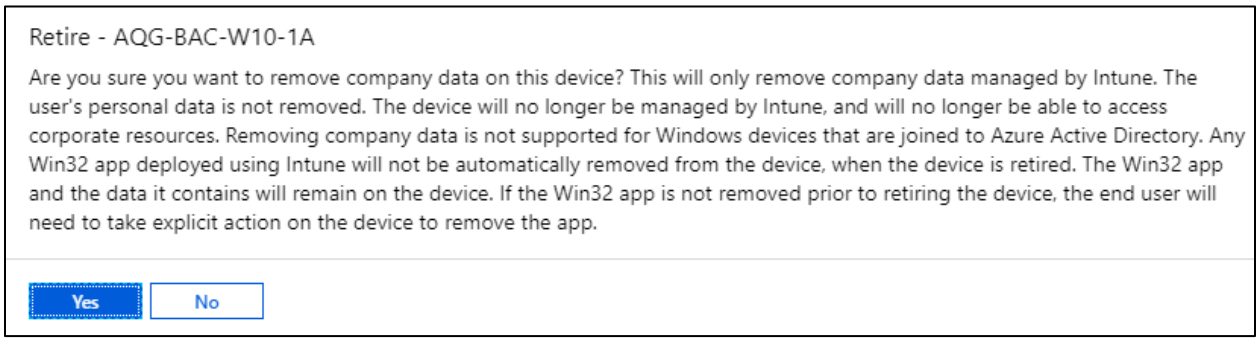
Intune har også endel verktøy som kan brukes for å administrere enhetene som er lagt inn. Det er ikke all funksjonaliteten som virker på alle enheter, men Windows 10-maskiner støtter de aller viktigste funksjonene for fjernadministrering.

### Retire

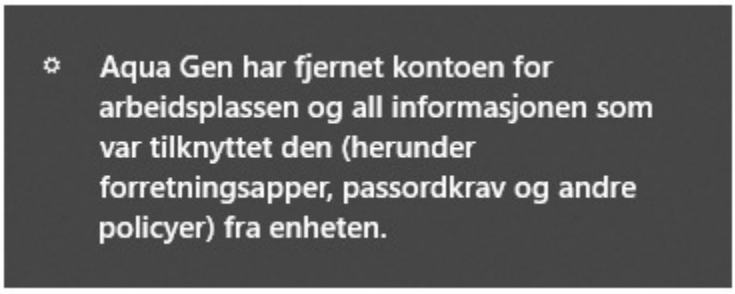
Retire vil koble enheten fra domenet og fjerne alle apper på enheten som er tilgjengelig via organisasjonen. All data som brukeren selv har opprettet vil fortsatt ligge igjen på maskinen.  Enheten vil fortsatt være brukbar, men man krever en lokal bruker for at man skal kunne logge seg på igjen.

- Vanligvis får man varsel om dette, men i noen tilfeller har vi opplevd at det ikke har kommet. Vi anbefales derfor å opprette en ny lokal bruker før man «pensjonerer» enhetene.

Trykker på *Retire* i Intune-portalen.




Tilbake på enheten får man nå opp følgende beskjed.



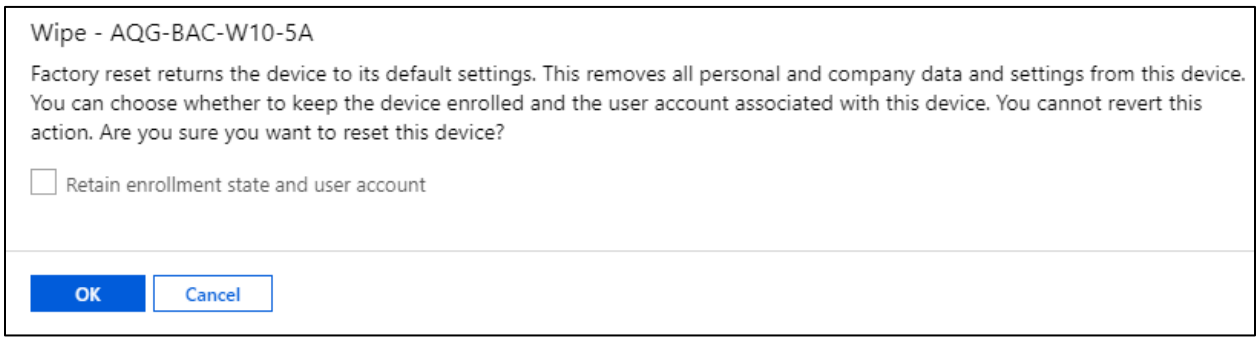

Ved neste utlogging må man så logge på med en lokal bruker for å fortsette å bruke datamaskinen.

## Remote Wipe

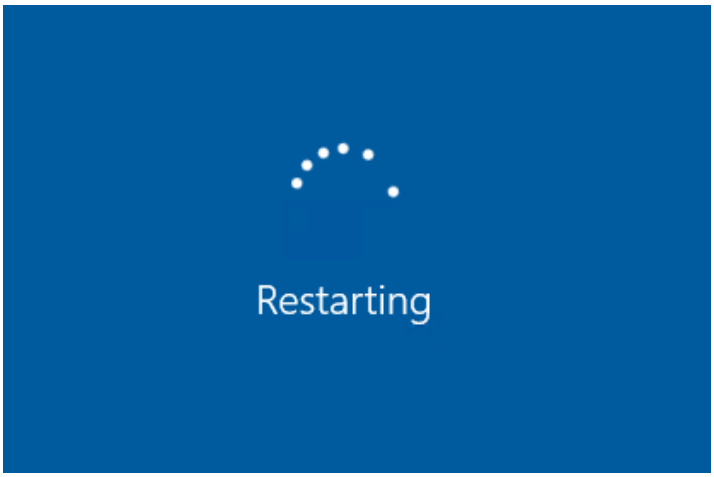
Wipe fjerner all data som er på enheten. I praksis er dette å anse som en fullstendig reset av maskinen. I tillegg blir også maskinen fjernet fra Intune.

- Hvis enheten fortsatt er registrert i Windows Autopilot vil den hente nye profiler derifra når den starter igjen.

Som vist kan man også velge å la enheten være koblet i Intune med brukeren etter fjernslettingen

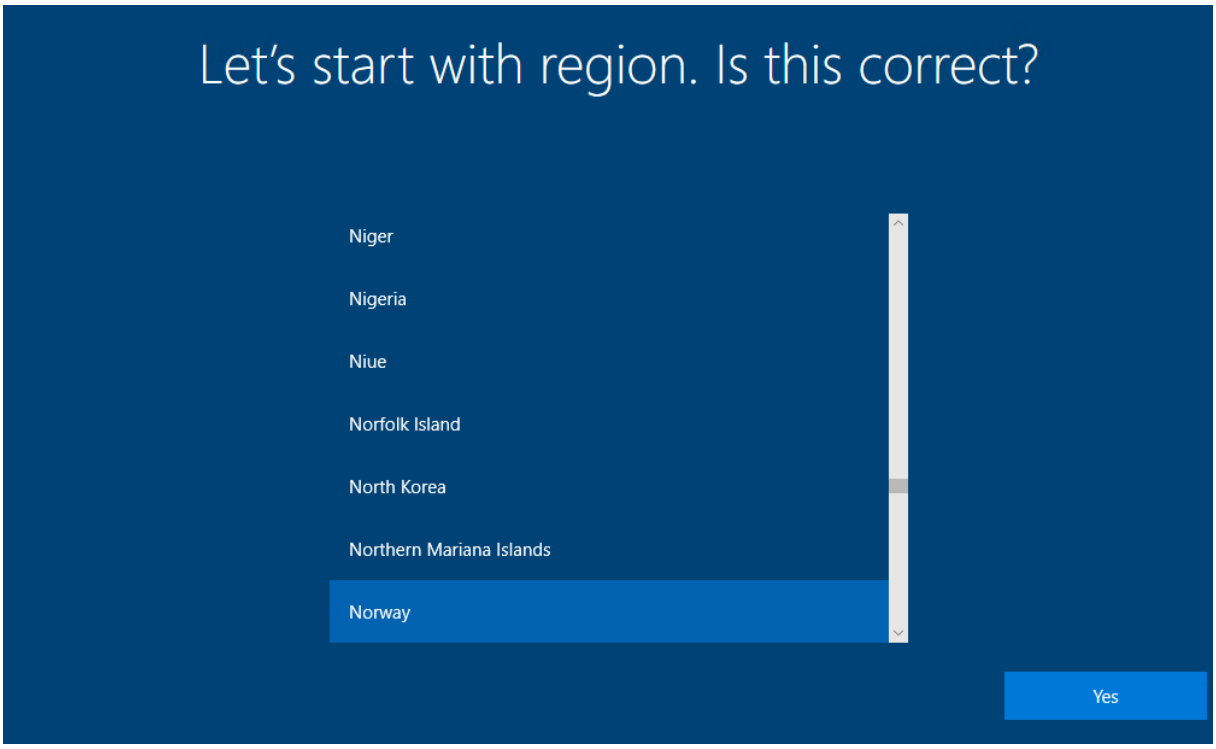



Tilbake på enheten ser vi at den etterhvert starter på nytt. Intune sender ut en forespørsel om å synkronisere så snart enheten blir tilgjengelig.

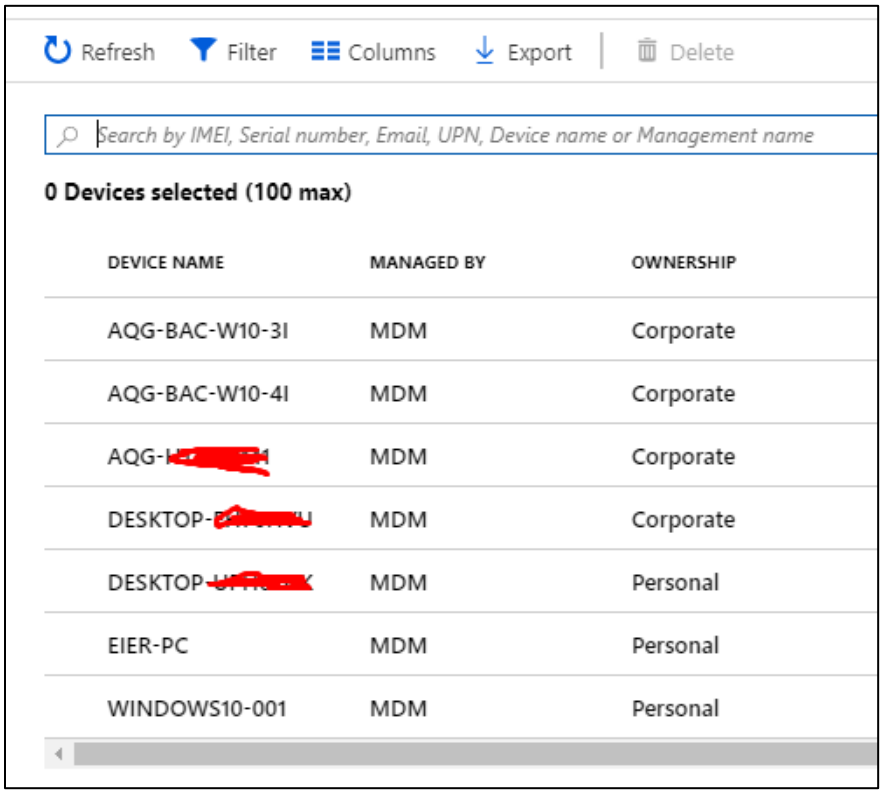



Etterhvert omstart vil enheten starte prosessen


Enheten begynner så førstegang-oppsett av Windows.

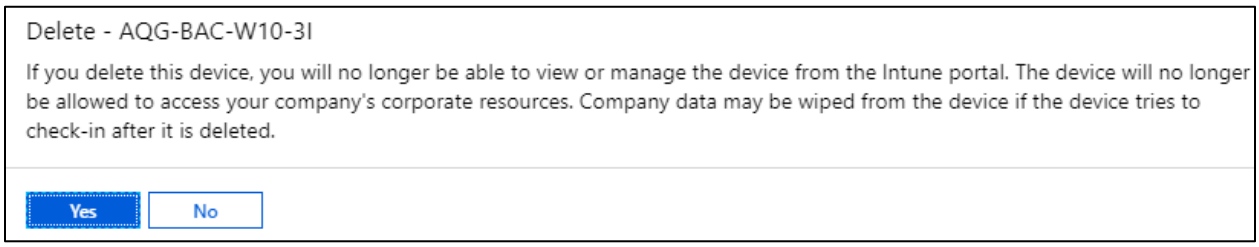



I Intune kan vi også se at enheten har forsvunnet fra listen.



## Delete

Hvis man vil slette en enhet fra Intune-portalen bruker man Delete knappen. Dette gjør ikke noe med personlig data på enheten, men gjør det slik at enheten mister videre tilgang til data fra organisasjonen.

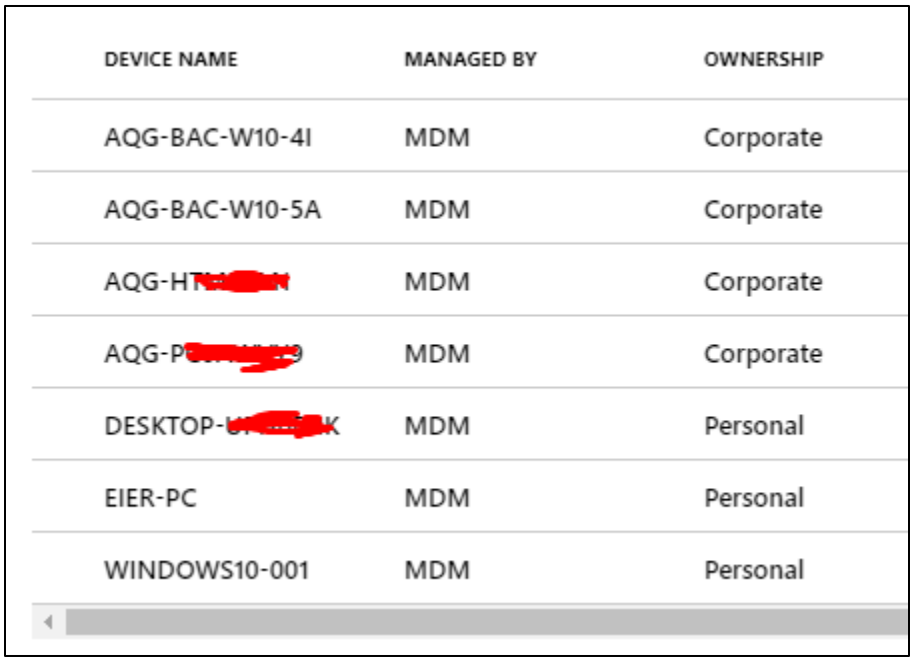



Når dette er utført vil maskinen etter hvert få beskjed om at den er fjernet og at den så vil miste tilgang til organisasjonens ressurser.


Maskinen vil så fjerne brukeren fra enheten.

- Hvis enheten ikke har en lokal bruker fra før må man opprette dette før maskinen blir avkoblet.

Enheten har nå også blitt slettet fra listen i Intune.

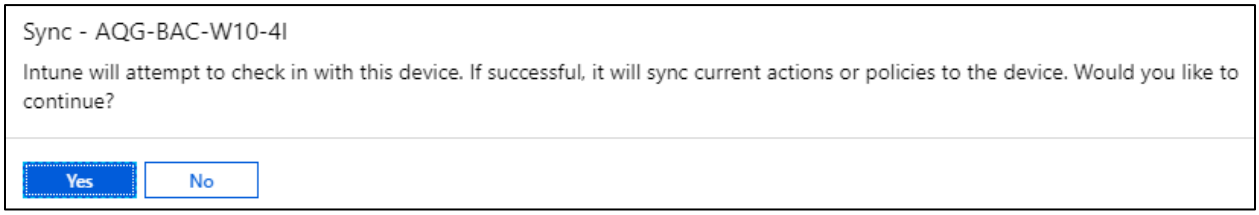


| DEVICE NAME | MANAGED BY | OWNERSHIP |
|---|---|---|
| AQG-BAC-W10-4I | MDM | Corporate |
| AQG-BAC-W10-5A | MDM | Corporate |
| AQG-HT[redacted] | MDM | Corporate |
| AQG-P[redacted] | MDM | Corporate |
| DESKTOP-[redacted] | MDM | Personal |
| EIER-PC | MDM | Personal |
| WINDOWS10-001 | MDM | Personal |

## Sync

Sync kjører en synkronisering mot den aktuelle enheten. Enhetene skal i utgangspunktet synkronisere seg selv, men hvis det ikke har skjedd på en stund kan man forsøke en manuell synkronisering.

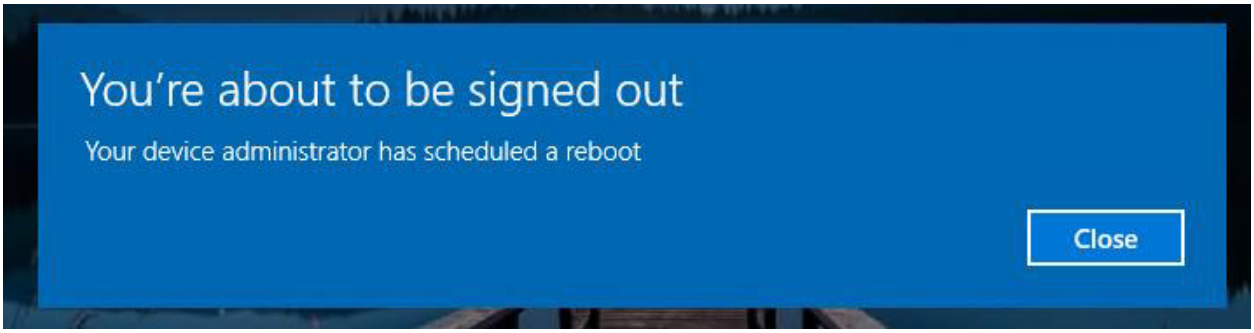
- Hvis enheten ikke har blitt synkronisert på en stund kan det hende den mangler endringer i policyer, apper, policyer o.l.



### Restart

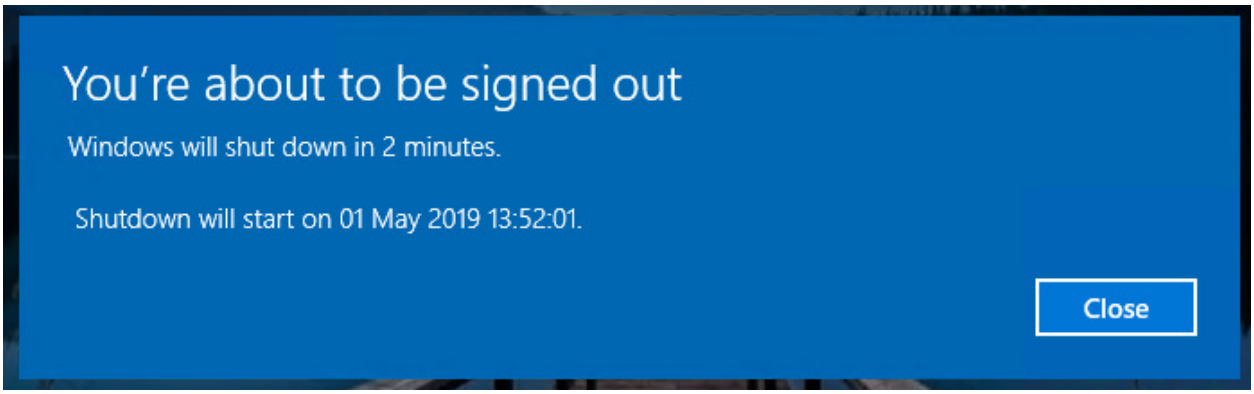
Restart gjør akkurat det navnet tilsier. Det kan for eksempel brukes hvis man har avtalt service på enheten, hvis programvare ikke har installert seg o.l.

- Når man trykker på Restart får brukeren beskjed at dette er blitt gjort. De har så et par minutter på seg til å lukke eventuelle dokumenter og applikasjoner som er oppe.



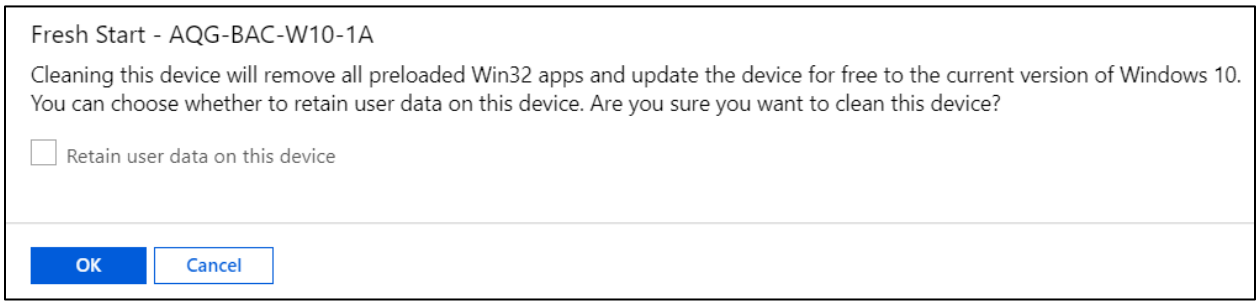

Brukeren får så varsel om tidspunkt når maskinen skal startes om.

- Hele prosessen fra man trykker på knappen til maskinen startes om tar typisk 5 minutter.



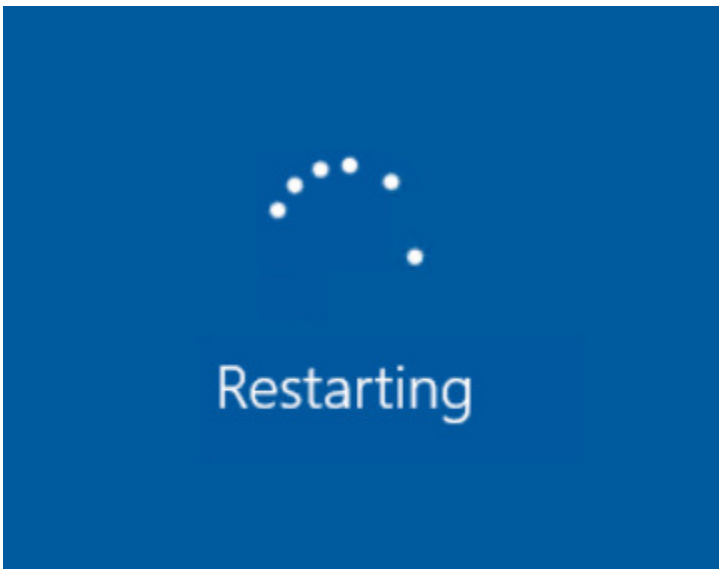
## Fresh Start

Fresh Start vil fjerne alle applikasjoner som følger med enheten, og så oppdatere den til siste versjon av Windows.

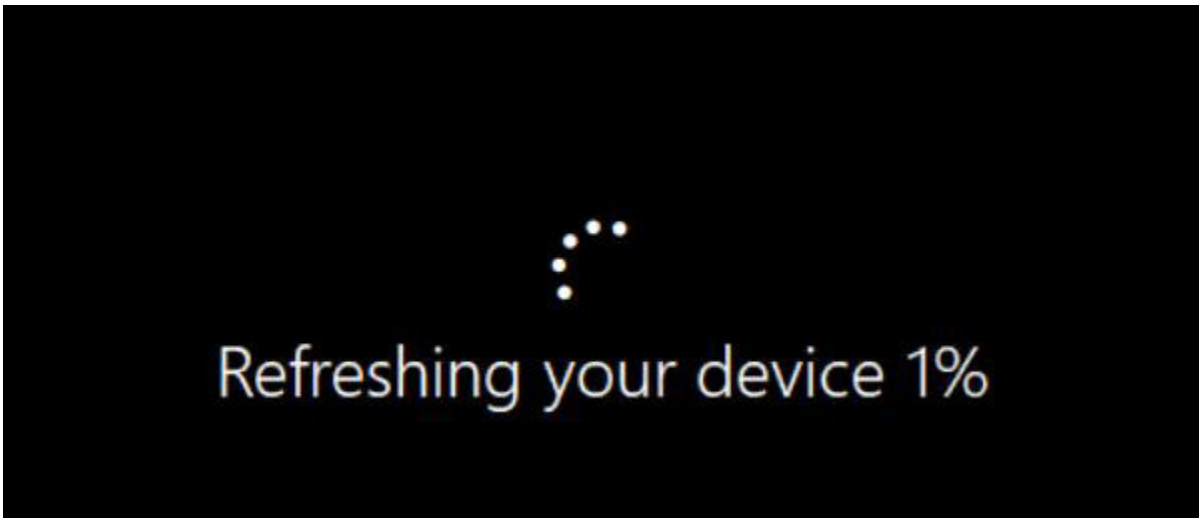



- Man har også her valget mellom å beholde brukerdata på enheten.

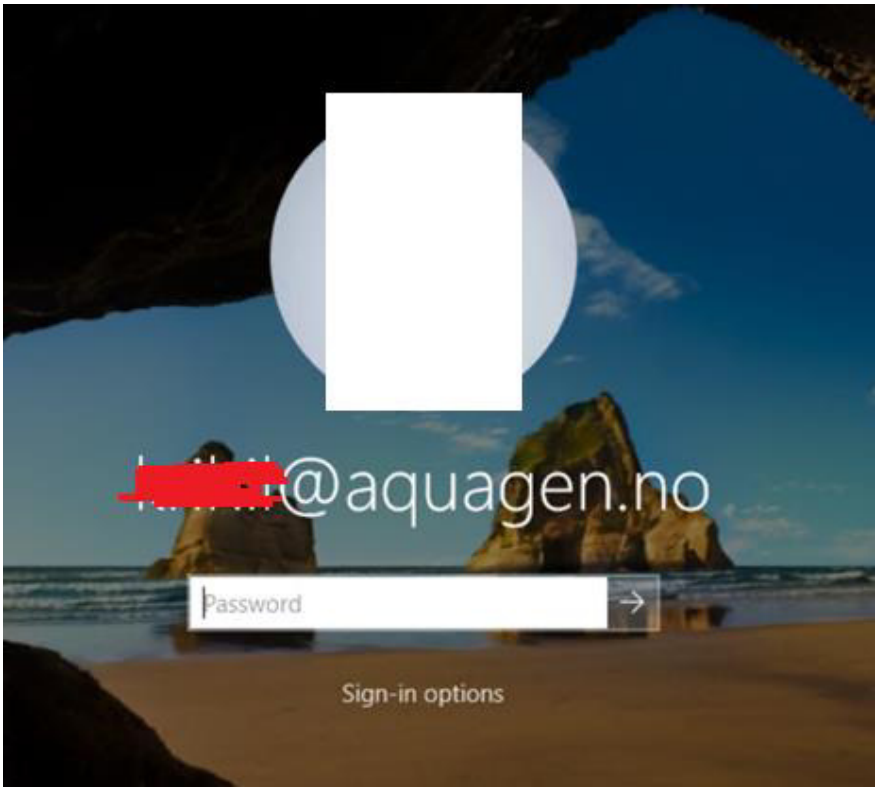
Også her vil enheten starte på nytt seg så snart den får synkronisert seg med Intune



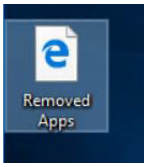

Etter omstart får man melding om at Windows «fornyer» enheten



Etter at enheten er ferdig blir vi møtt med innlogging-skjermen i Windows




Etter innlogging får vi opp en snarvei på skrivebordet.




Her kan vi se alle appene som ble fjernet fra enheten under Fresh Start.

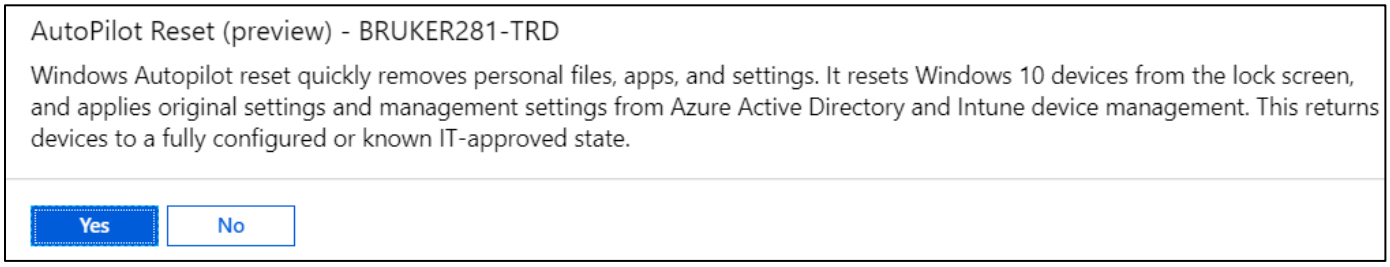
## Apps removed while resetting your PC

| App name | Publisher | Version |
|---|---|---|
| (EMCO EVALUATION PACKAGE) - AquaSpor3 | Marel | 4.10.5.0 |
| Google Chrome | Google LLC | 74.0.3729.131 |
| Microsoft Intune Management Extension | Microsoft Corporation | 1.18.104.0 |
| Microsoft Office 365 ProPlus - nb-no | Microsoft Corporation | 16.0.11601.20144 |
| Microsoft OneDrive | Microsoft Corporation | 19.043.0304.0007 |
| Microsoft Teams | Microsoft Corporation | 1.2.00.10168 |
| Teams Machine-Wide Installer | Microsoft Corporation | 1.2.0.10168 |

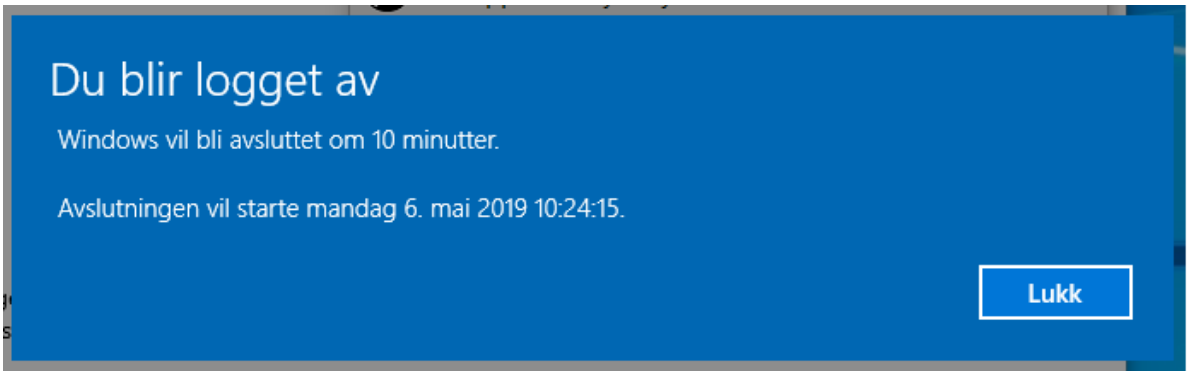
## Autopilot Reset

Autopilot Reset er en kjapp måte å klargjøre en eksisterende enhet for en ny bruker, ved at den blir resatt og satt opp med godkjente innstillinger fra IT-avdelingen.

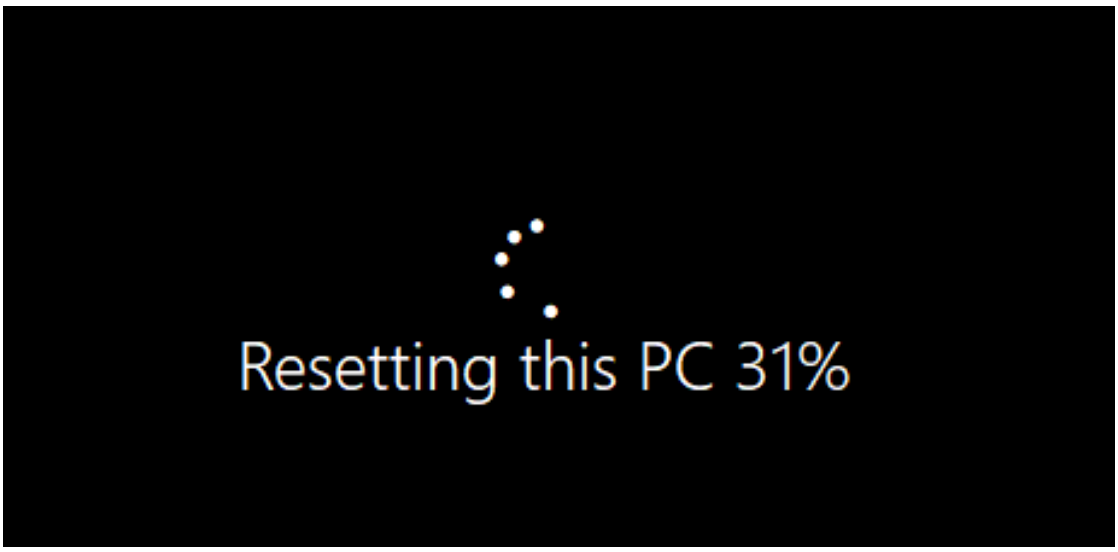
- Det tar ca. 45 minutter fra man har trykket på knappen før enheten får beskjed om dette.



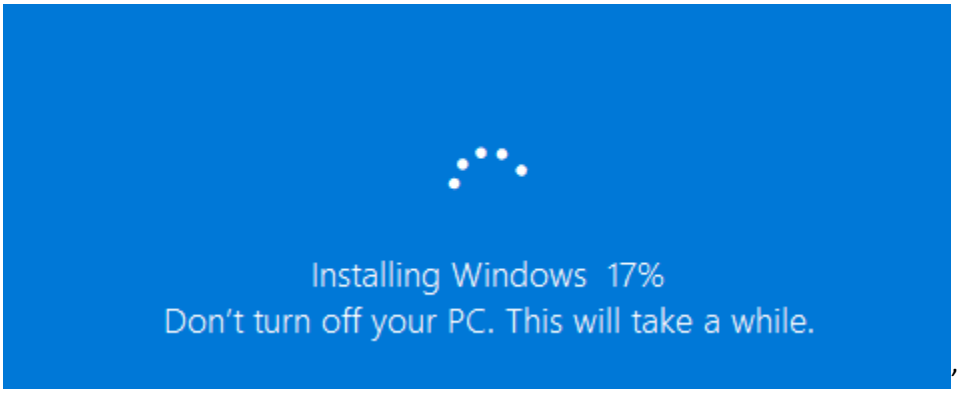

Det kommer så opp en meldingsboks på enheten som forteller om når enheten vil restarte seg for å begynne tilbakestillingen.

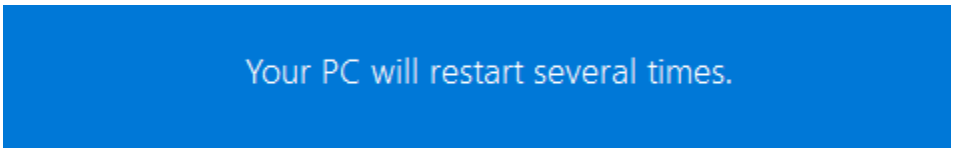



Enheten starter på nytt og man får opp følgende skjerm.



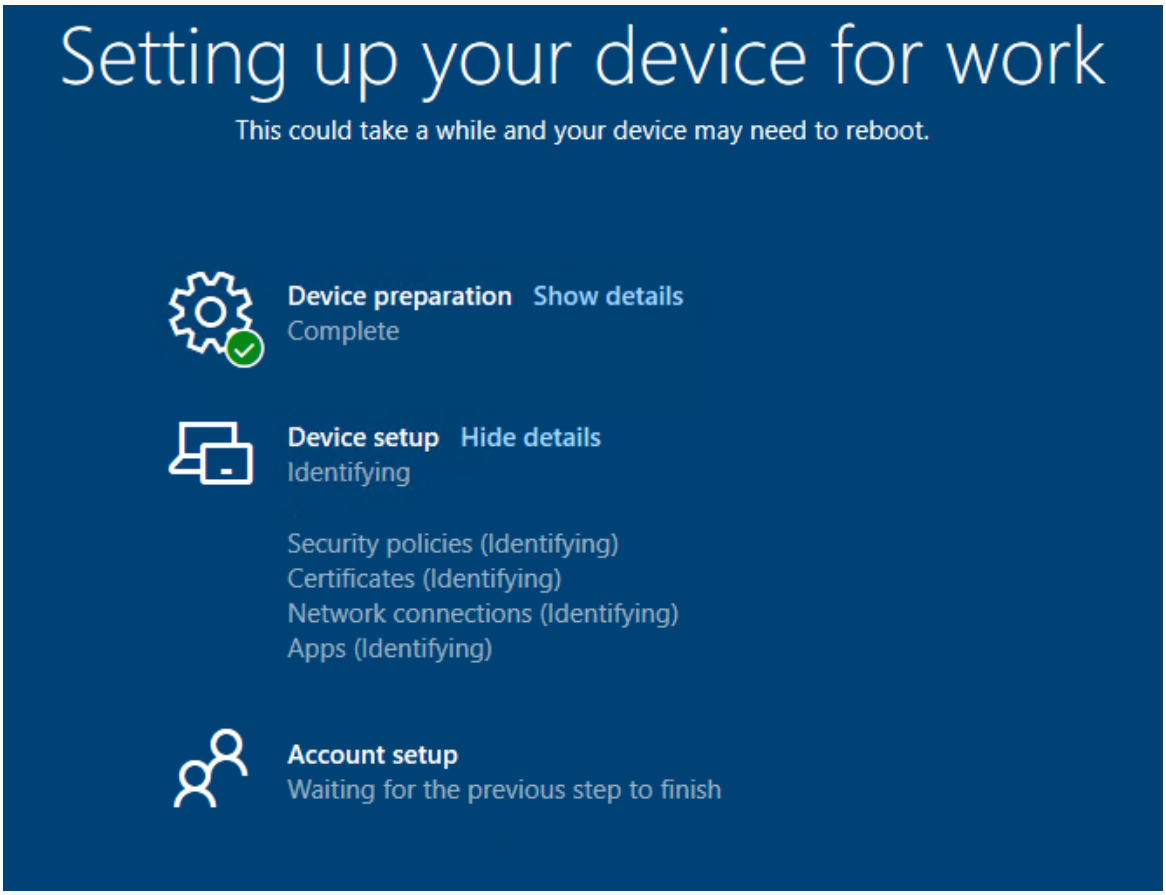
Etter hvert får man opp dette skjermbildet.




Etter flere omstarter vil enheten etter hvert begynne å koble seg opp mot Intune.

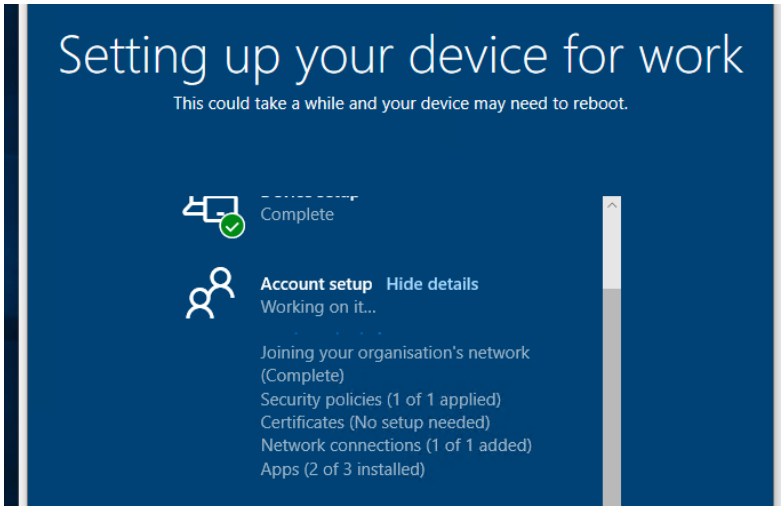
Man får så opp status på de forskjellige delene som skal settes opp

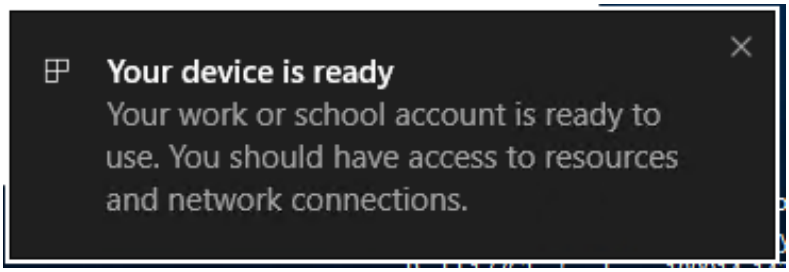



Etter ferdig konfigurering blir man så møtt med innlogging-skjermen. Den forrige brukeren som lå inne er nå fjernet, og man må logge inn på nytt.

Etter innlogging må man som vanlig sette opp PIN-kode, samt autentisere seg hvis man har 2-faktor verifisering aktivert.

Etter dette kan man fortsatt se videre framgang med konfigurasjon av enheten.



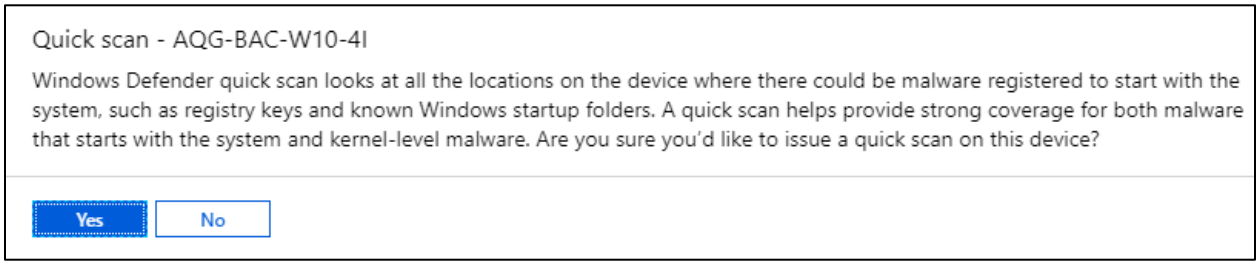



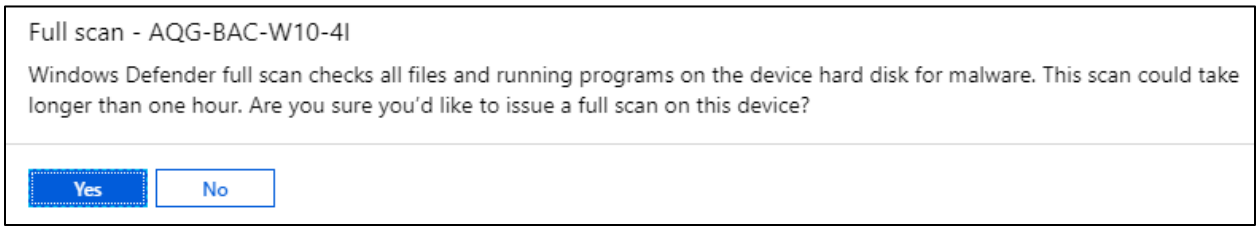

Til slutt vil man få beskjed om at enheten er klar til bruk.

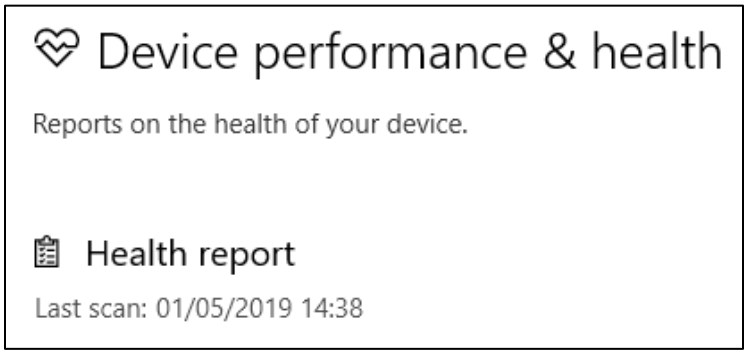
## Quick scan/Full scan

*Quick scan* og *Full scan* setter i gang en skann fra Windows Defender.

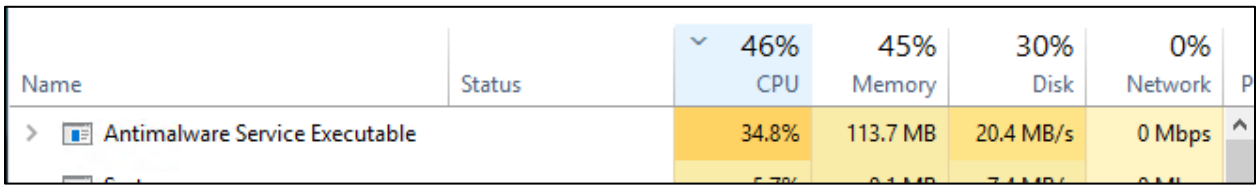
- Windows Defender er installert på enheten med mindre brukeren har en annen antivirus-programvare.



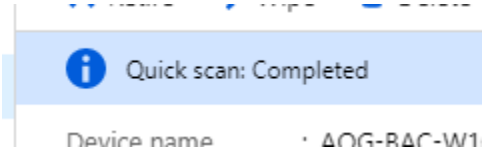




Som vi ser i Windows Defender vinduet på klient-maskinen ble siste skann startet.




Også i Oppgavebehandling kan vi se at Windows Defender kjører ved å sjekke CPU-bruk.

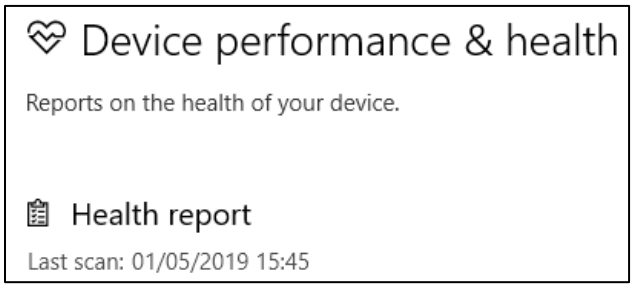



Når den er ferdig får man opp melding i Intune.

## Update Windows Defender signatures

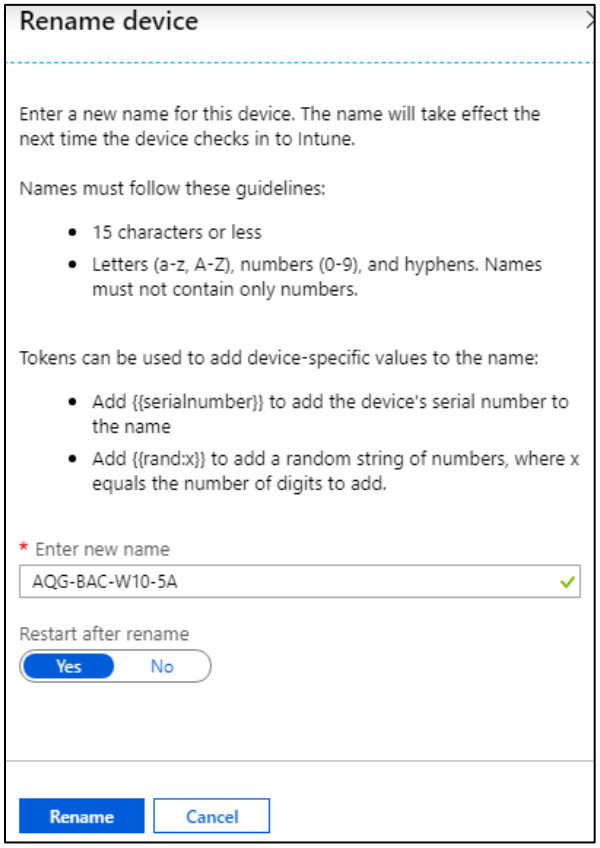
Brukes for å oppdatere Windows Defender på en Windows 10-enhet. Når man utfører dette vil Defender oppdatere seg slik at man er beskyttet mot de seneste virusene som er kjent.

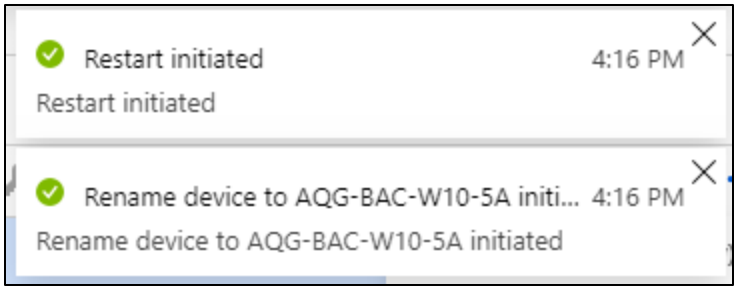

Også her får man opp i Windows Defender vinduet når siste «sjekk» ble utført



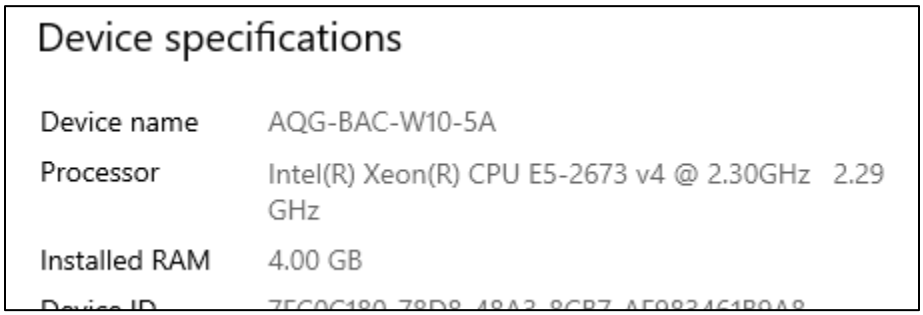

## Rename Device

Rename Device gjør akkurat det navnet sier: den gir enheten et nytt navn. I dette tilfellet er det ikke bare visningsnavnet i Intune, men også navnet på selve enheten.






Etter at enheten har restartet går vi inn på innstillingene og sjekker navnet




Som vi ser har navnet nå blitt endret.

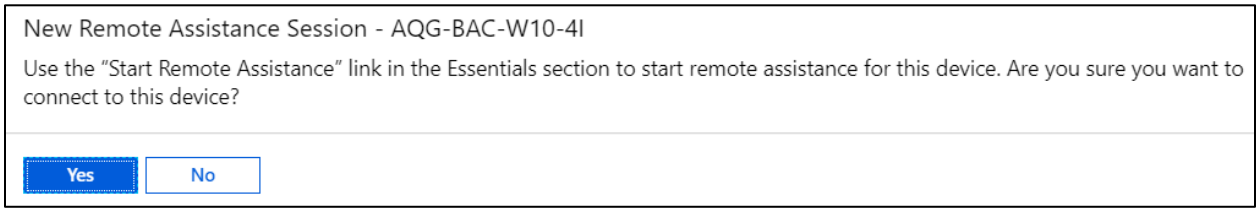
| ACTION | STATUS | DATE/TIME |
|---|---|---|
| Restart | Complete | 01/05/2019, 16:16:07 |
| Rename device to AQG-BAC-W10-5A | Complete | 01/05/2019, 16:16:06 |

Kan også bekrefte dette i Intune-portalen.

## New Remote Assistance Session

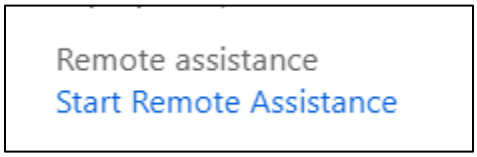
Remote Assistance Session bygger på tilknytning med TeamViewer. Vi skal ikke vise hvordan dette er satt opp da det går litt utenfor oppgaven, men vi skal vise hvordan dette fungerer i praksis.

- For at en enhet skal kunne bli fjernstyrt er den nødt til å ha Company Portal installert.



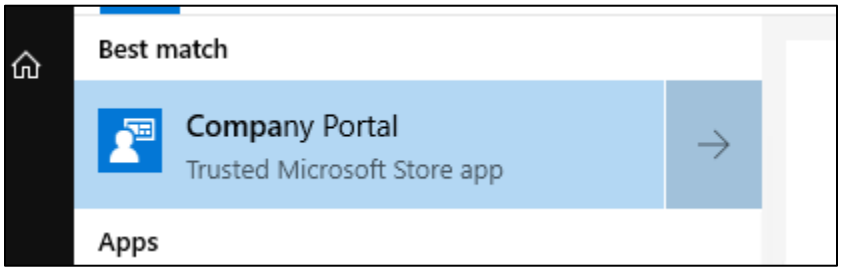

Vi trykker deretter på *See more.*


Og til slutt på *Start Remote Assistance.*

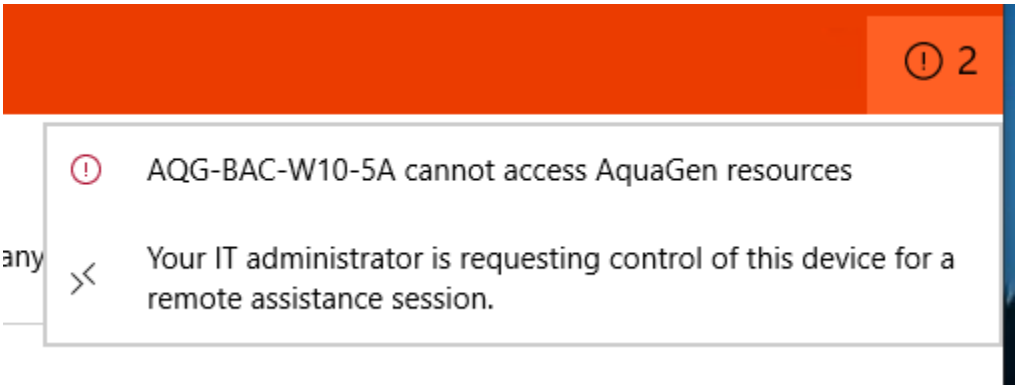



TeamViewer vil deretter åpne opp applikasjonen på enheten for system-administrator.

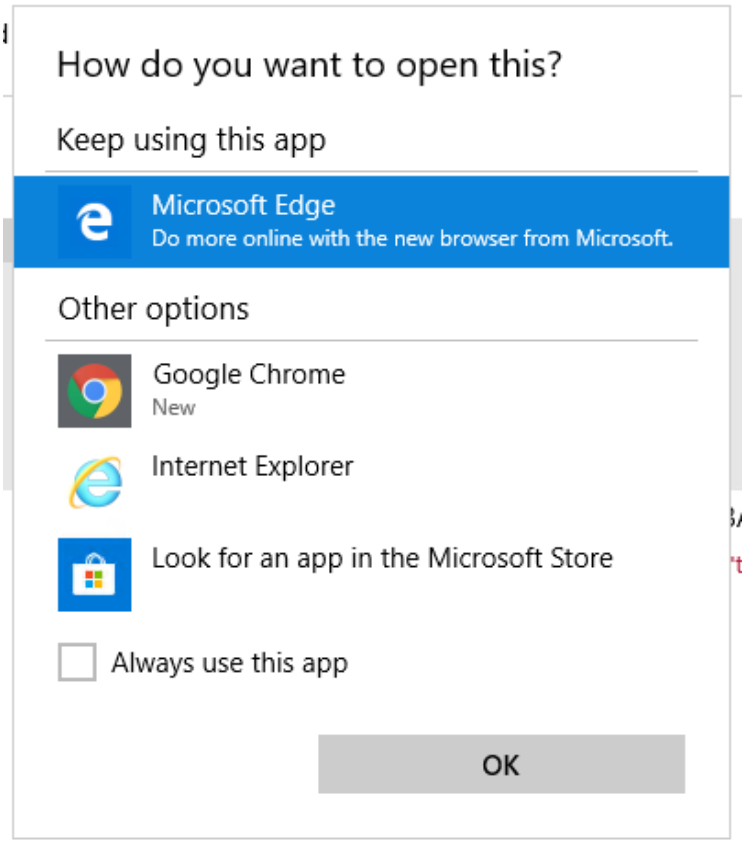
Vi går tilbake til bruker-enheten og åpner opp Company Portal.



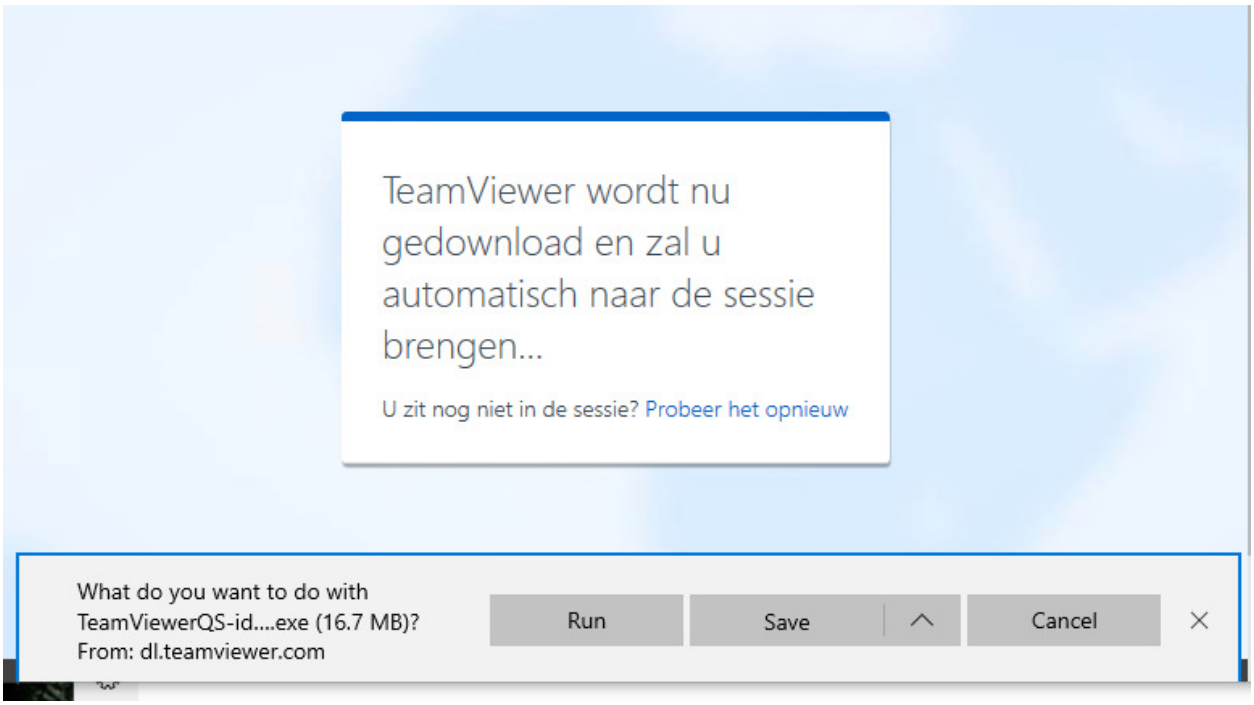

Vi klikker oss opp i varsellinjen og ser at vi har fått en forespørsel om tilkobling.

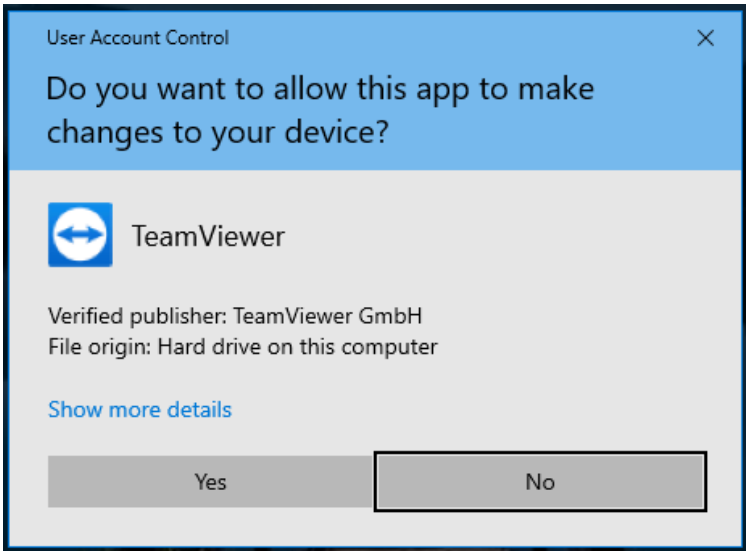


Vi trykker på denne og for så valg i hvilken nettleser man vil benytte. Vi velger bare enkelt Edge.

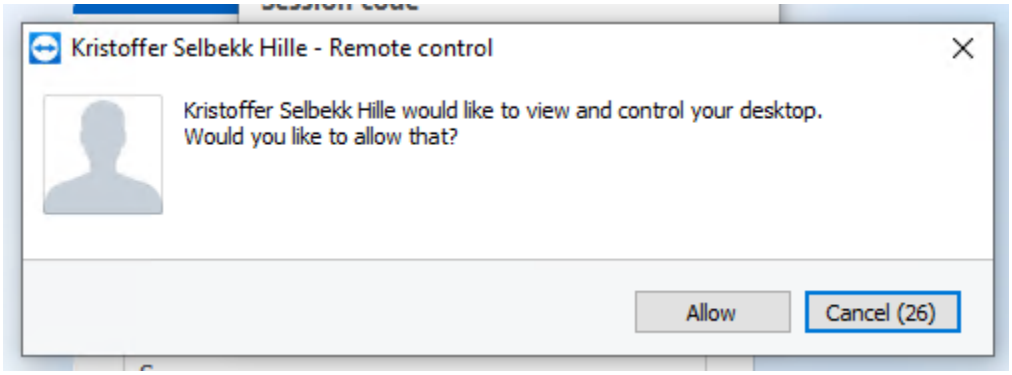



TeamViewer starter så å laste ned klienten, og vi trykker på *Run* for å starte applikasjonen.

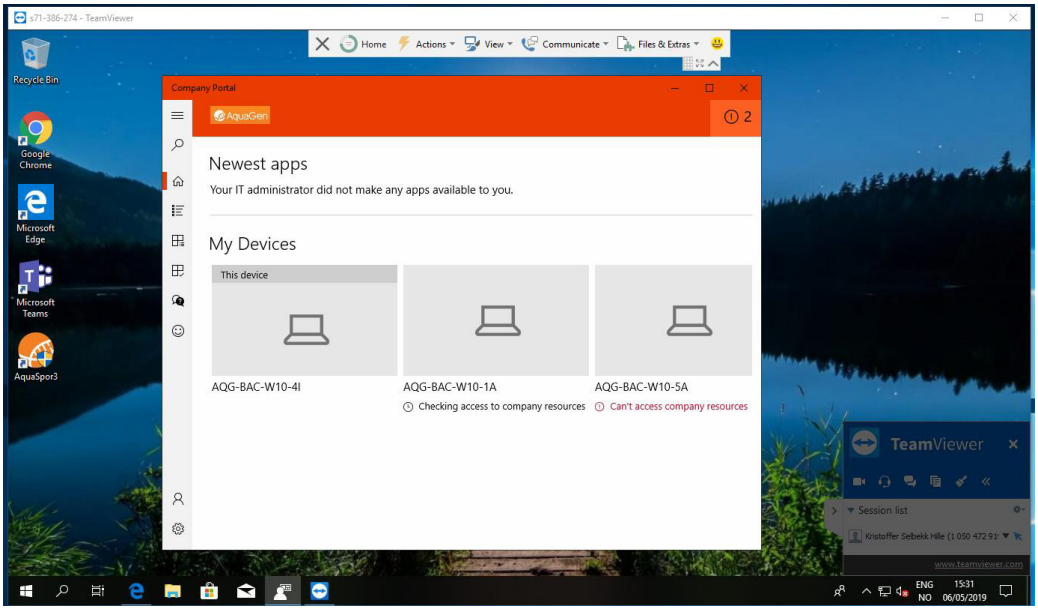





Etter at appen kjører blir man så spurt om man vil tillate personen til å koble seg til maskinen.




IT-administrator har nå fjerntilgang til enheten og kan utføre endringer.




For å lukke tilkoblingen lukker man simpelthen bare TeamViewer-vinduet.

## Fase 9: Brukertest v/ Rolf og Arnfinn

Brukertesten blir en ganske rask test for å sjekke at også andre brukere kan logge seg inn i domenet og MDM slik at enhetene blir tilgjengelige for IT-administrator.

For å gjøre klar brukertest har man opprettet noen profiler og konfigurasjoner som skal settes på enhetene som skal rulles inn i domenet. Det vil også rulles ut noen apper spesifikt til organisasjonen.

I dette eksempelet vil vi bruke fysiske maskiner for å demonstrere at ting fungerer i praksis.

Maskinvaren vi kommer til å teste på er:

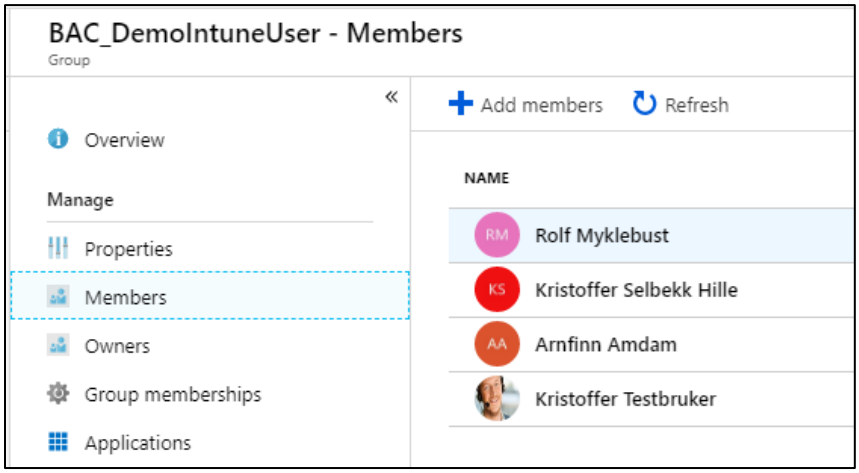
- Microsoft Surface Pro 4 – ny maskin som skal rulles ut ved hjelp av Autopilot.
    - Denne testes av Rolf Myklebust
- Dell XPS 15 9370 – eksisterende maskin som skal legges inn med manuell innmelding.
    - Denne testes av Arnfinn Amdam

## Klargjøring for brukertest

### Grupper

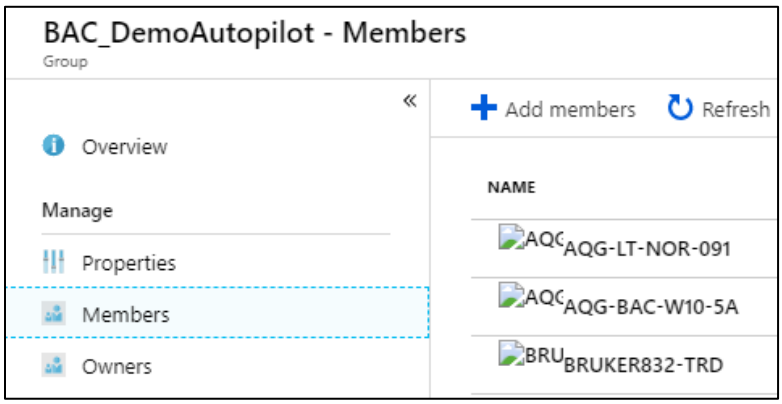
For denne testen har vi opprettet to grupper, *BAC_DemoIntuneUser* og *BAC_DemoAutopilot.*

I *BAC_DemoIntuneUser* har vi lagt inn følgende brukere.




I *BAC_DemoAutopilot* har vi lagt inn følgende enheter.

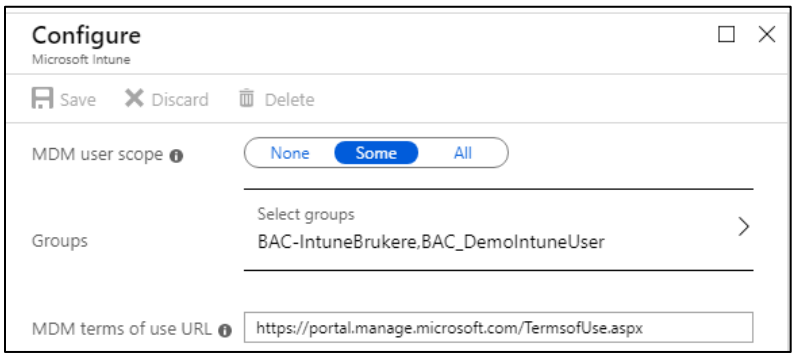
- Noen av disse enhetene har skiftet navn underveis.



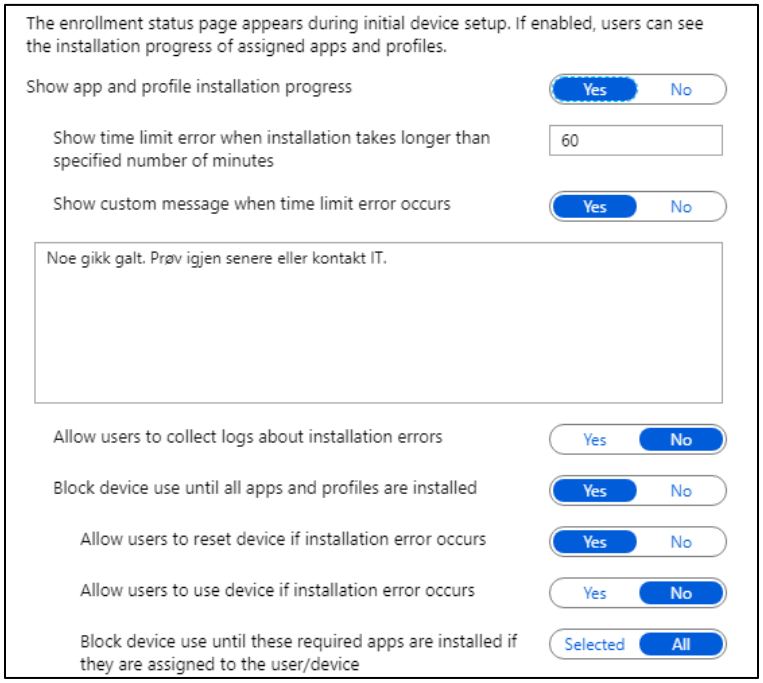
## Device enrollment

### *Automatic Enrollment*

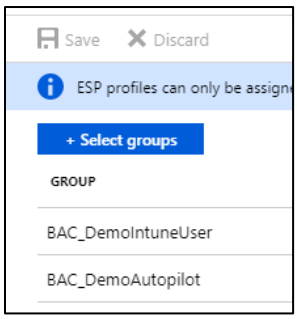
Under *Automatic Enrollment* har vi simpelthen lagt inn brukergruppen vi opprettet tidligere, *BAC_DemoIntuneUser*




Vi har også lagt inn en ESP (Enrollment Status Page) med følgende innstillinger

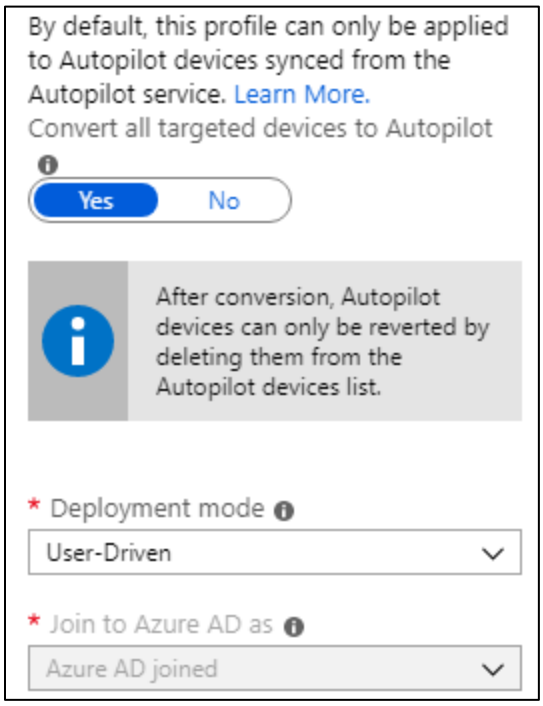



Den er tilegnet de følgende gruppene



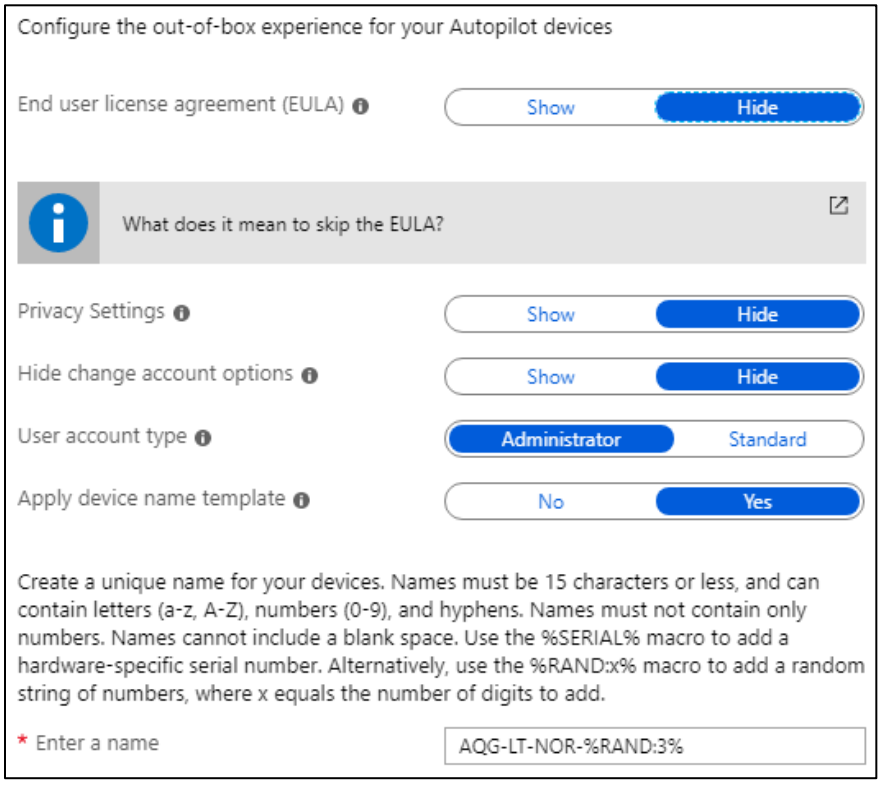
### *Deployment profile*

Vi har også lagt inn en *Deployment Profile* med følgende egenskaper.

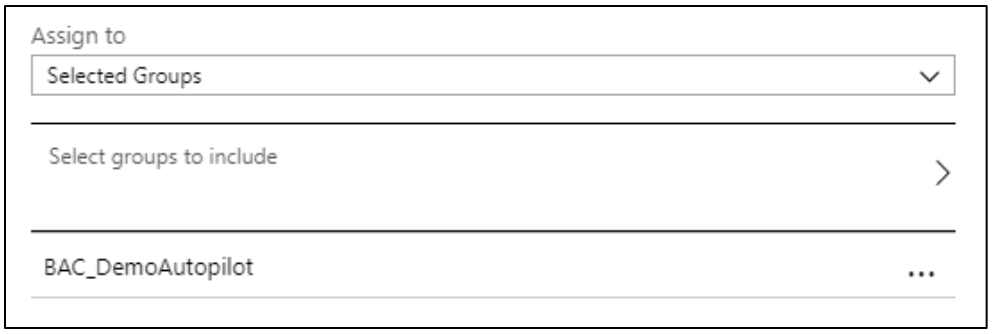



Her har vi også satt navnegivningen til å foregå på dette formatet.

- AQG-enhet-land-tilfeldig tall.



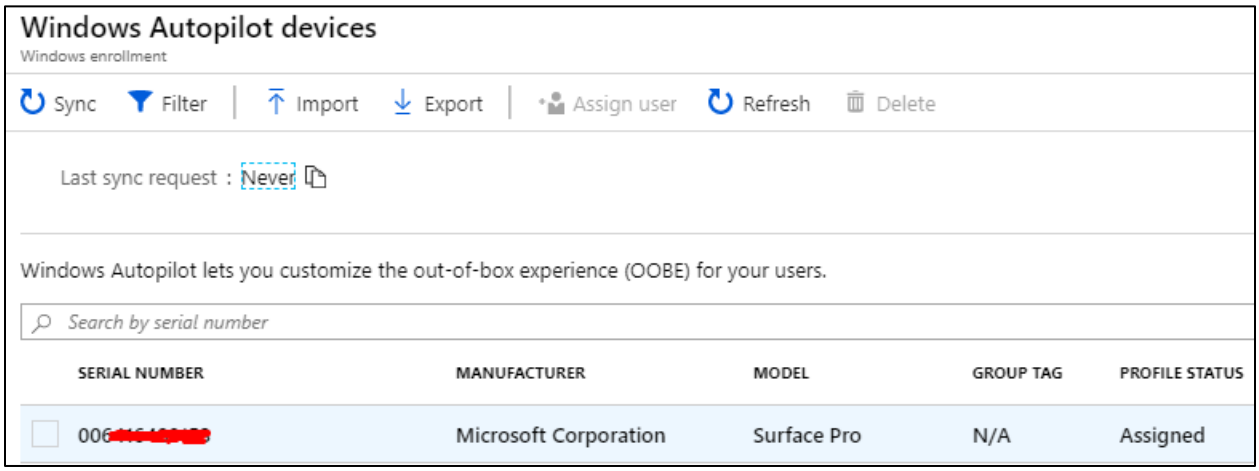
Vi har tilegnet denne profilen til følgende gruppe.




### *Devices*

Her har vi importert følgende enhet til Autopilot ved hjelp av maskinvare-IDen.

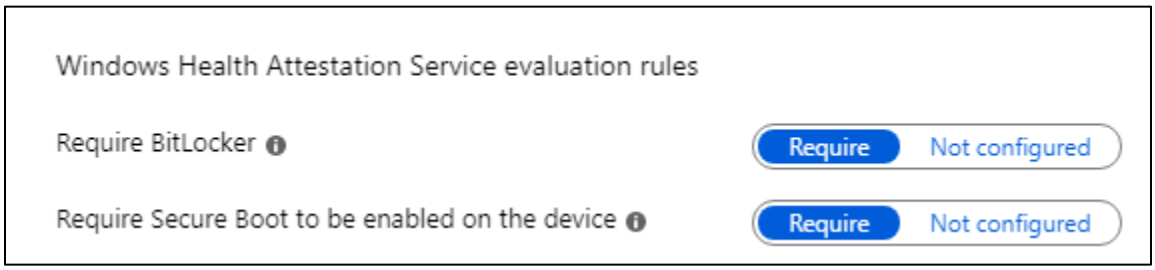
Vi har også lagt inn denne enheten i gruppen *BAC_DemoAutopilot*, som videre har gitt den *deployment profile* som vi opprettet tidligere.



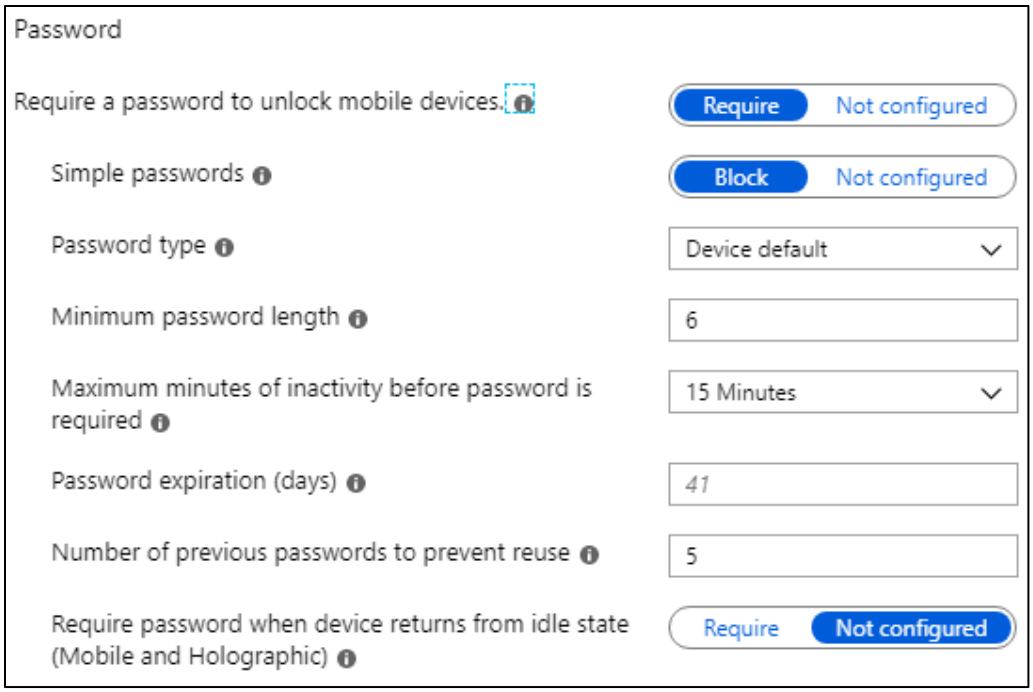

## Device compliance

Her har vi opprettet en profil med følgende egenskaper:

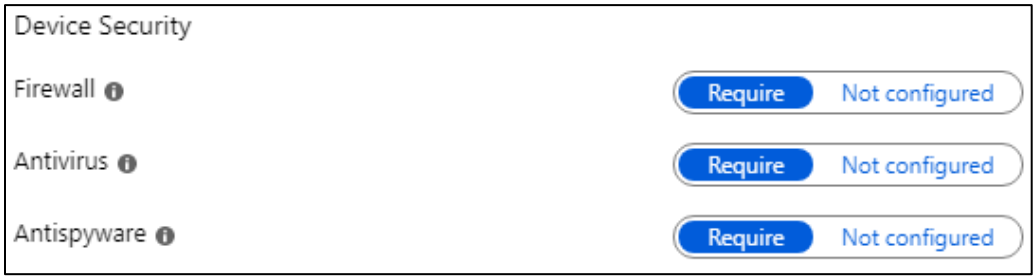
Krav om **BitLocker** og **Secure Boot** på enheten.



Krav til **passordet** som settes på enheten.

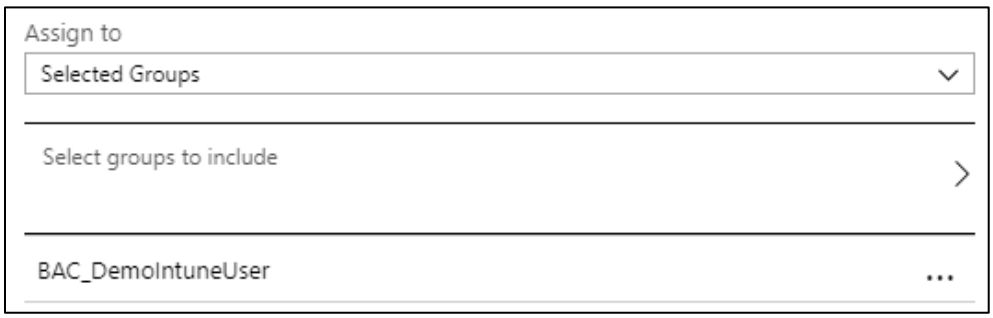



Krav til **sikkerheten** på enheten.




Krav til **antivirus-programvare** på enheten.


Denne er tilegnet den følgende gruppen.



## Device configuration

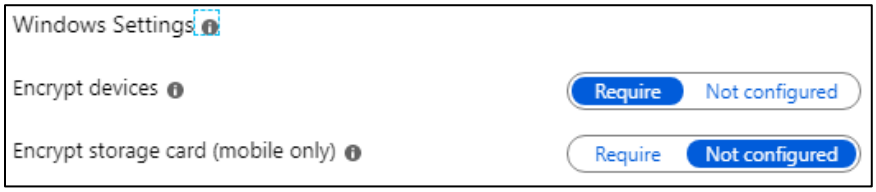
Her har vi opprettet følgende profiler.

| PROFILE NAME | PLATFORM | PROFILE TYPE | ASSIGNED | LAST MODIFIED |
|---|---|---|---|---|
| BAC_DemoProfil2 | Windows 10 and later | Endpoint protection | Yes | 5/07/19, 3:07 PM |
| BAC-DemoProfil-WiFi | Windows 10 and later | Wi-Fi | Yes | 5/02/19, 1:14 PM |
| BAC-DemoProfil-1 | Windows 10 and later | Device restrictions | Yes | 5/02/19, 1:11 PM |

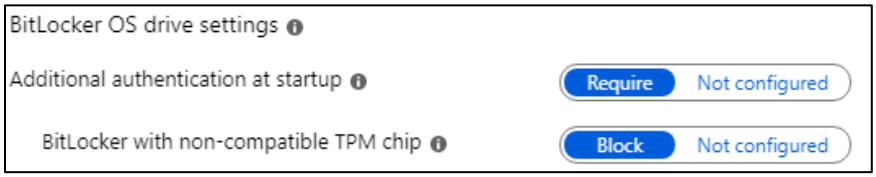
Den første profilen, BAC_DemoProfil2 brukes for å skru på BitLocker på enhetene som blir med i Intune.

Den inneholder de følgende egenskapene:

Innstilling for å skru på kryptering på enheten.



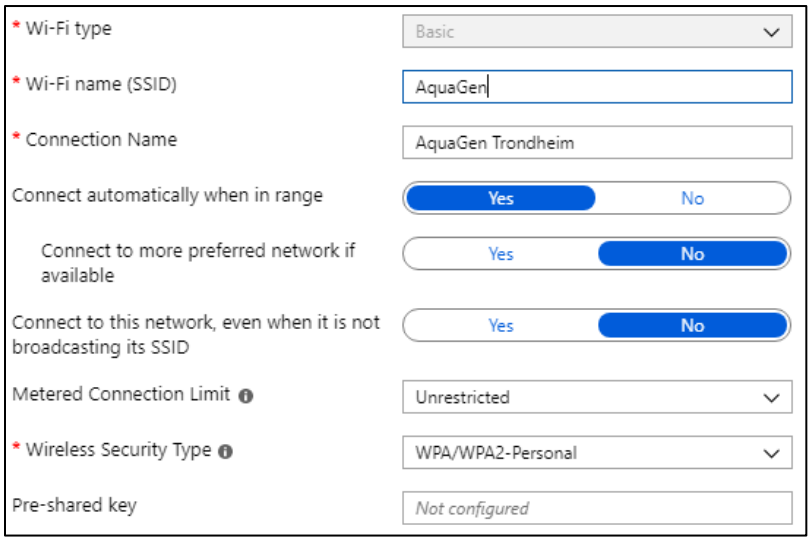

Innstilling som må settes for å kreve at BitLocker kun virker med TPM-modul.




Den andre profilen, BAC_DemoProfil-Wifi brukes for å legge til standard-WiFi på enheten.

- Om enheten allerede er koblet på WiFi vil denne ikke bli lagt inn

Profilen har følgende egenskaper:



Den siste profilen, BAC_DemoProfil-1 brukes for å sette en rekke generelle innstillinger på enhetene

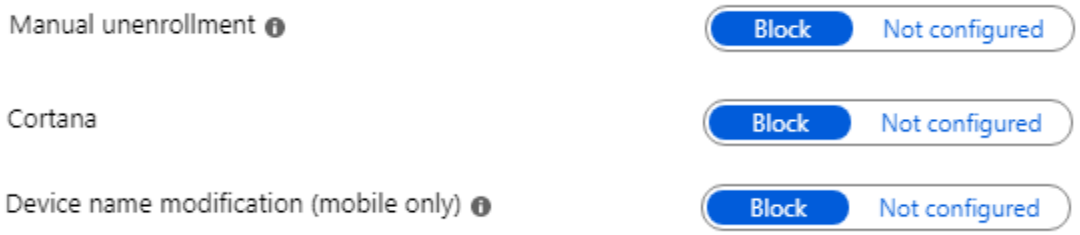
Den har følgende egenskaper satt:

**Control Panel and Settings**

Kun for å blokkere tilgang til enkelte innstillinger.

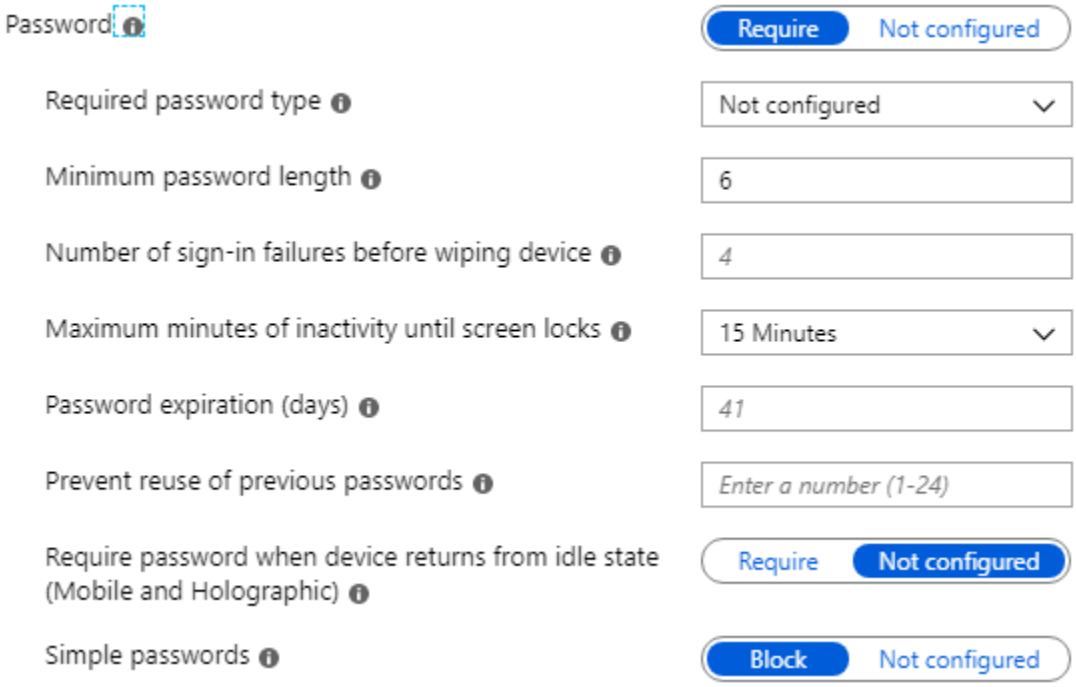

**General**

Blokkere brukeren fra å gjøre enkelte handlinger.




**Password**

Setter begrensninger til hvilke passord som brukeren kan opprette.



**Personalization**

Setter et spesifisert bilde som bakgrunnsbilde.


**Reporting and Telemetry**

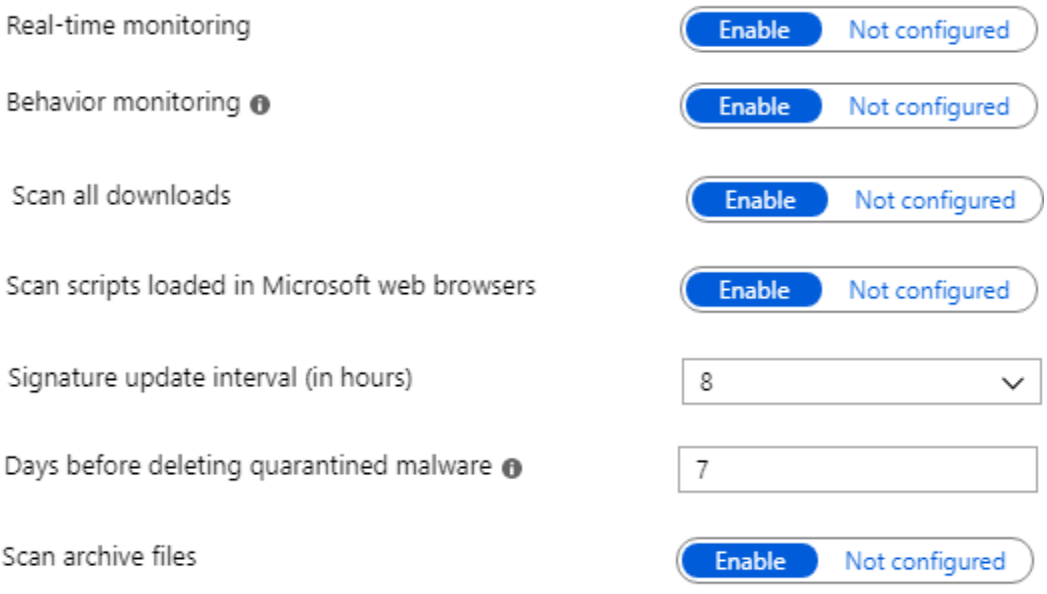
Velger hvor mye informasjon som skal sendes til Microsoft ved feilsøking.


**Windows Defender SmartScreen**

Spesifiserer hva som kreves av sikkerhet for brukeren.

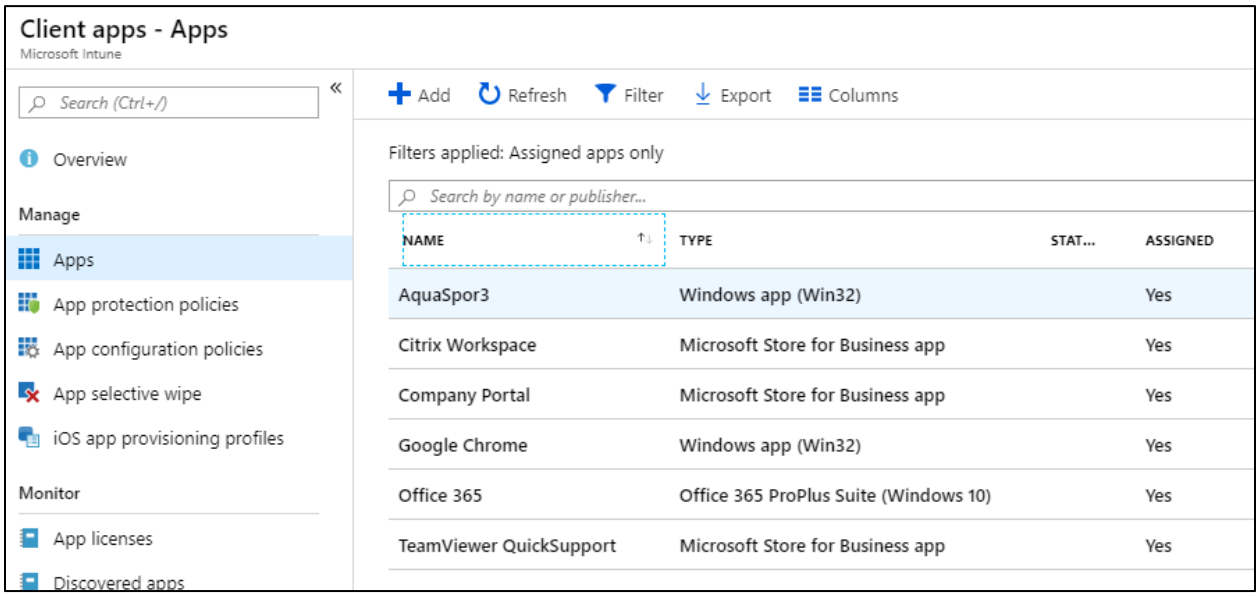

**Windows Defender Antivirus**

Velger hvor mye Defender skal skanne på enheten.



## Client apps

Under *client apps* har brukerne fått tildelt følgende apper:



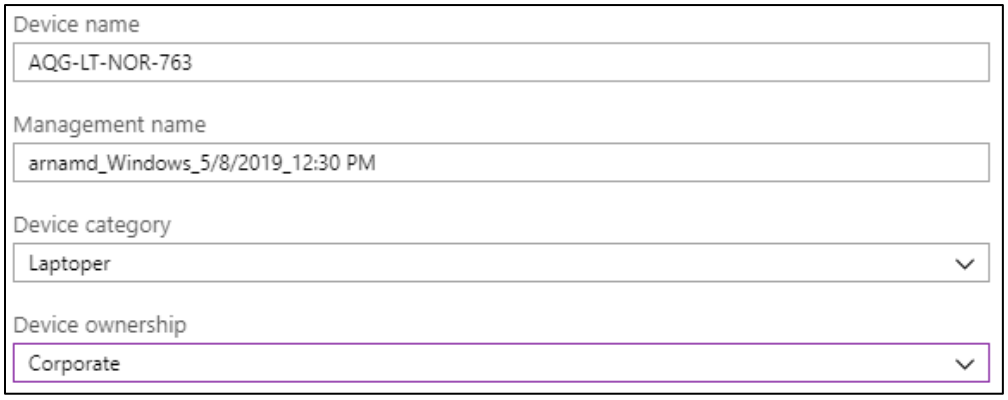
## Test av manuell innlegging i Intune og AD v/ Arnfinn Amdam

Vi bruker Dell-laptopen som blir lagt inn i Intune på samme måte som vist i **Fase 4,** via innstillingene som finnes på enheten.

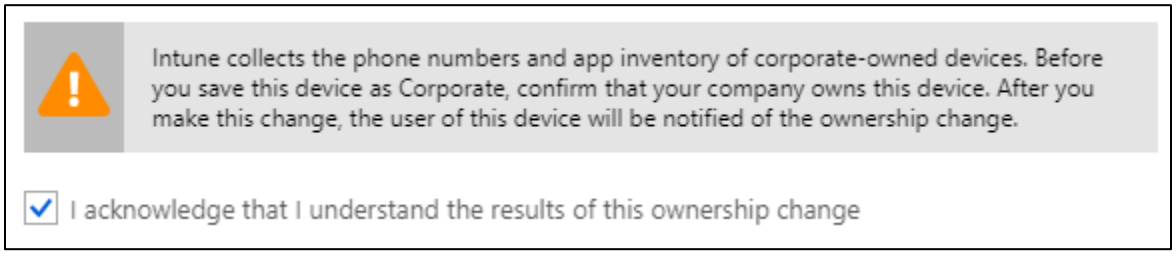
| DEVICE NAME | MANAGED BY | OWNERSHIP | COMPLIANCE | OS | OS VERSION | EMAIL ADDRESS |
|---|---|---|---|---|---|---|
| AQG-LT-NOR-763 | MDM | Personal | Not Evaluated | Windows | 0.0.0.0 | Arnfinn.Amdam@aquagen.no |

Ved første innmelding i domenet vil enheten dukke opp som en personlig enhet. Man får også opp hvem som har meldt inn maskinen og når den sist ble sjekket inn i Intune.

Vi går inn på *Properties,* setter enhetstype til Laptop og endrer *Device ownership* til *Corporate.*




Vi må bekrefte når vi endrer *Device ownership* til *Corporate.*




Enheten er nå lagt inn og begynner å nå å laste inn de policyer, konfigurasjoner og apper som vi har tildelt brukeren.

## Tilbakemelding fra Arnfinn

Gjennom testing av Intune fikk vi bekreftet det som var arbeidshypotesen; nemlig at bruk av Intune/Autopilot i stor grad automatiserer og forenkler klienthåndtering. I utgangspunktet ser jeg ingen ulemper med å ta i bruk en slik løsning, men store fordeler i form av bedret sikkerhet, mindre muligheter for personlig feil og manuelt arbeid.

For sluttbruker oppleves dette som profesjonelt og enkelt, man trenger bare å forholde seg til brukernavn og passord og få satt opp PC/programmer uten å måtte håndtere ting på egen hånd. Slik som løsningen er designet i dag, slipper også brukeren også å håndtere brukernavn/passord til trådløs nett.

Selve pilottesten gikk som forventet, oppsett av helt ny maskin gikk knirkefritt. Vi hadde noen utfordringer ved innrullering av eksisterende/ferdig oppsatt pc (kryptering kom ikke på plass pga. feil oppsatt BIOS), men dette varslet systemet om, og det ble håndtert manuelt.

Ettersom løsningen beskrevet i oppgaven følger best-practice fra Microsoft har jeg ingen kommentarer til systemet -det er satt opp på best mulig måte og dekker de behovene vi har!

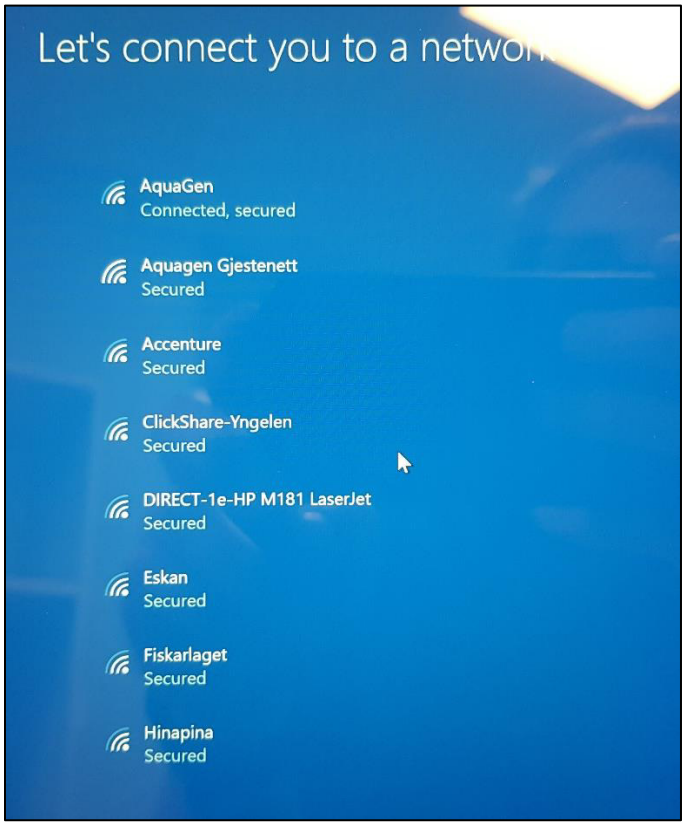
-Arnfinn Amdam, AquaGen

## Utrulling ved hjelp av Autopilot v/Rolf Myklebust

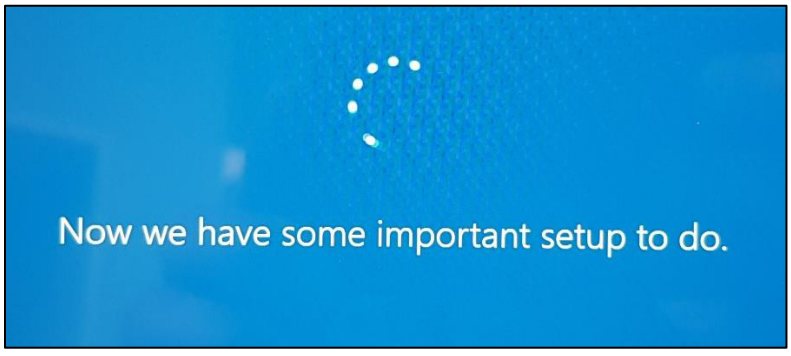
Som vist har vi lagt Surface-enheten i Autopilot ved hjelp av maskinvare-ID som vi hentet ut tidligere.

Det eneste som nå gjenstår på denne enheten er å tildele riktig konto slik at brukeren får testet denne.

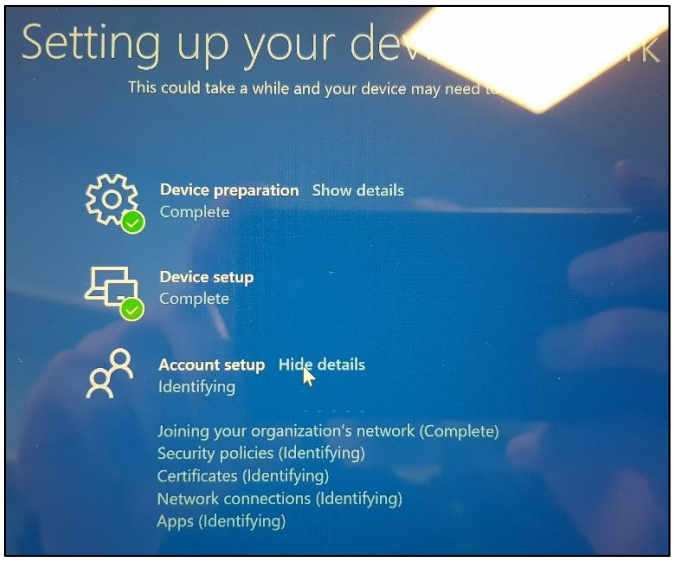
Etter tildeling har vi valgt språk og kobler så enheten til organisasjonens nettverk



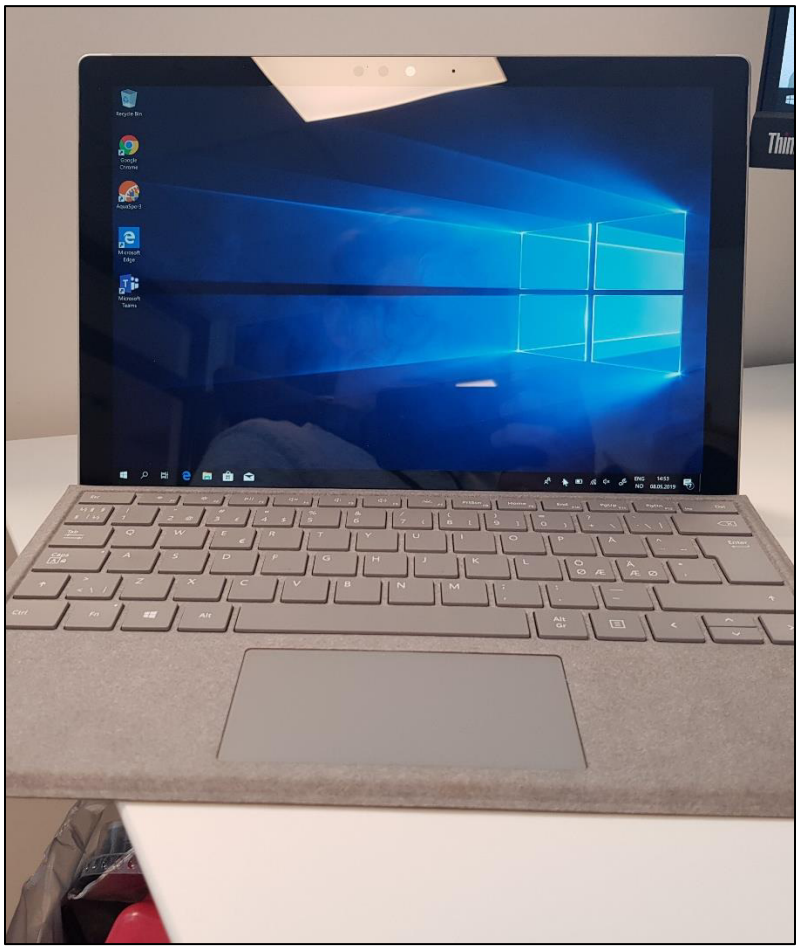

Etter tilkobling begynte enheten å hente ned konfigurasjonen fra Intune-portalen



Etter innlogging fra bruker begynner enheten å hente ned de ulike innstillingene




Etter dette er enheten nå blitt fullt satt opp og vi er tilbake på skrivebordet



## Tilbakemelding fra Rolf

En slik løsning vil gjøre at oppsett av pc-er bli mer standardisert, samt mindre ressurskrevende for den som skal gi support. Sluttbruker vil normalt kunne gjøre alt på egenhånd.

Den som skal gi support trenger ikke å ha fysisk tilknytning til pc-ene i det hele tatt. Ansatte i AquaGen er geografisk spredt. Den enkleste og kjappeste er å få sendt nye pc-er rett fra leverandør og til mottaker.

Testen ble utført på en Microsoft Surface. Hele oppsettet tok ca. 1 time. Det var enkelt og ingen tvil om framgangsmåten. Ingen feilmeldinger underveis. Eneste bemerkning var at Windows fikk engelsk skjermspråk, det kan muligens ha med tidligere oppsett på denne pc-en. Den var fjernslettet via Intune før denne testen startet.

I oppsettet ble produksjonsstyringsprogrammet AquaSpor lagt til. Det fungerte utmerket. Det var en stor fordel å få det utført på denne måten siden programmet ikke har eget installasjonsprogram, men må manuelt plasseres i rett mappe og gitt administratortilgang for at det skal fungere. Det er ønskelig å få lagt til automatisk oppdatering også.

-Rolf Myklebust, AquaGen

# Referanser


1. Guide for importering av egne Win32-apper i Intune. Fra Peter van der Woude.
   https://www.petervanderwoude.nl/post/deploy-customized-win32-apps-via-microsoft-intune/
   (aksessert 14.04.2019)
2. Kilde for Win32 Content Prep Tool. Fra Microsoft.
   https://github.com/Microsoft/Intune-Win32-App-Packaging-Tool
   (aksessert 14.04.2019)
3. Lenke for Chrome MSI-fil. Fra Google.
   https://cloud.google.com/chrome-enterprise/browser/download/
   (aksessert 15.04.2019)

Kristoffer Selbekk Hille

# Klientadministrasjon med Microsoft Intune og Autopilot
# Sluttrapport

**Versjon 1.1**

# Revisjonshistorie

| Dato | Versjon | Beskrivelse | Forfatter |
|---|---|---|---|
| 18.05.2019 | 1.0 | - | Kristoffer Selbekk Hille |
| 20.05.2019 | 1.1 | Formatering | Kristoffer Selbekk Hille |

# Innhold

# Forord

Dette prosjektet er skrevet av Kristoffer Selbekk Hille ved NTNU. Prosjektet kommer som bakgrunn av bacheloroppgave for linjen Informatikk, drift av datasystemer. Linjen er veldig praktisk orientert, og tar for seg både teknologi som allerede er på plass, men også ny måter man kan utføre arbeidsoppgaver på. Jeg er glad for at jeg valgte denne studieretningen, og føler at jeg lært masse i løpet av studieløpet.

Oppgaven som jeg har skrevet om skulle løse hvordan man på best mulig måte kan administrere Windows-klienter ved hjelp sky-løsninger. Det er et spennende prosjekt da det viser til hvordan man i fremtiden ha et slikt system «helt» på Internett, uten at man har noe lokal infrastruktur som støtter det opp. Det er en litt annen måte å se på klientdrift nå enn for 10 år siden, og det er akkurat denne utviklingen som gjør at jeg valgte dette. I tillegg er det spennende å etablerere et nytt system på «urørt» infrastruktur da klientdrift i bedriften ikke har vært noe tema før nå nylig.

I løpet av prosjektet har jeg vært innom mange kjente områder, men også måtte prøvet meg fram på andre, mer ukjente teknologiske hjelpemidler som jeg ikke har brukt før. Noe av det som gjør prosjektet litt risikabelt er at man bruker endel funksjonalitet som ikke er dokumentert helt enda. Dette øker mulighetene for feil og uventede overraskelser, men jeg synes dette har gått helt greit i prosjektløpet. Hovedessesnen med prosjektet har blitt ivaretatt uavhengig, og så lenge man får løst problemet føler jeg at prosjektet kan bli vellykket.

Jeg ønsker å utrette en takk til min arbeidsgiver, AquaGen, som har vært veldig åpen for prosjektet og som ga meg tillitt til å gjennomføre dette for og i bedriften. Det har vært veldig kjekt å kunne benytte arbeidsplassen som «kontor» - det har hjulpet spesielt på slutten når det har blitt litt hektisk. Jeg vil også takke Stein Meisingseth hos NTNU for god oppfølging og engasjement for prosjektet.

# Oppgavebeskrivelse

Bakgrunnen for prosjektet var et ønske fra arbeidsgiver om å finne et system for å administrere alle datamaskinene rundt om i bedriften. Dette ble presentert hos veileder Stein Meisingseth ved NTNU. Selve oppgaven ble opprettet gjennom en dialog veileder hos NTNU og Truls Theting hos AquaGen. Ettersom AquaGen ansatte en ny IT-sjef mens prosjektet pågikk, ble også Arnfinn Amdam med som kontaktperson hos bedriften.

Prosjektet gikk ut på å skissere og demonstrere et system for å administrere alle disse klientmaskinene innenfor AquaGen sine avdelinger og kontorer. Systemet hadde en rekke krav, blant annet at det skulle være skybasert, støtte nye versjoner av operativsystem (Windows) og ikke gjøre arbeidshverdagen for de ansatte noe vanskeligere. Systemet måtte klare å holde orden på et større antall enheter, og være mulig å nå for disse maskinene uansett hvor de befant seg i verden. Oppgaven gikk mest ut på å bruke eksisterende løsninger framfor å utvikle nye, da slike system ofte blir veldig komplekse og går langt utover oppgavens art å produsere på egenhånd.

Oppdragsgiver, AquaGen AS, er et oppdrettsfirma som leverer lakse- og ørretrogn rundt om i hele verden. På lik linje med andre moderne bedrifter har også AquaGen tatt i bruk datamaskiner og tilhørende utstyr for effektivisering av produksjon. Ellers har bedriften et stort antall maskiner som brukes til kontorbruk rundt om i de forskjellige avdelingene. AquaGen valgte å bruke dette prosjektet for å få oversikt over hvilke moderne løsninger man har tilgjengelig for å holde oversikt på maskiner.

# Oppgaveløsning

I dette kapitlet går man gjennom hvordan de ulike delene ved prosjektet ble løst. Her kommer det frem hvilken maskin- og programvare som ble benyttet, og hvilke dokumenter som foreligger ved prosjektets slutt.

## Metoder og standarder

For å løse oppgaven tok vi bruk av «Best Practice» metodene fra Microsoft. Dette ble gjennomført ved å lese på dokumentasjon for de ulike funksjonene der dette var mulig.

I tillegg ble det etterhvert brukt en standard for enhetsnavn når disse ble lagt inn i systemet. Denne er vist til i systemkrav-rapporten.

Bortsett fra overnevnte ble det ikke brukt noen nevneverdige metoder eller standarder under prosjektets gang.

## Informasjon

For å hente ut informasjon for hver av de forskjellige funksjonene benyttet man dokumentasjonen opprettet av Microsoft. Noen funksjoner var ikke helt klargjort enda; her måtte vi hente dokumentasjon fra andre parter for å få testet funksjonen i sin helhet. Dette er blitt dokumentert i driftsdokumentet der disse funksjonene ble gjennomgått.

Bortsett fra overnevnte bruk av sidene til Microsoft ble det ikke brukt noe nevneverdig mengde med dokumentasjon fra andre parter.

## Maskinvare

Intune og Autopilot er «skyløsninger» og stiller derfor ikke noe krav til lokal maskinvare hos brukeren.

For å demonstrere prosjektet benyttet vi noen virtuelle- og fysiske-maskiner. De virtuelle maskinene ble opprettet hos NTNU sin Azure, og fungerte utmerket under prosjektet. Disse ble i all hovedsak brukt til å teste funksjoner kjapt, da man mye enklere og kjappere kan opprette nye maskiner. De fysiske maskinene bestod av 2 bærbare PC-er lånt av bedriften. Disse ble brukt for å teste funksjonalitet som satte krav utover maskinvaren, og for å demonstrere systemet under brukertesten. Dette var relativt nye PC-er, noe som gjorde at man også fikk testet endel ny funksjonalitet i systemet.

## Programvare

I prosjektet har man benyttet følgende programvare:

- Microsoft Intune – administrering av ulike typer enheter, hovedrammen for prosjektet
- Windows Autopilot – system i Intune, muliggjør utrulling av (nye) maskiner
- Windows 10 Pro/Enterprise – operativsystem fra Microsoft, brukt på klientmaskiner
- Chrome/Firefox – nettleser for tilgang til Azure-kontrollpanelet
- Office 365/SharePoint – dokumentasjon og deling av dokumenter

## Dokumentasjon

I dette prosjektet skal følgende dokumenter foreligge:

- Forstudierapport – analyse av prosjektets deler, samt kost/nytte-analyse. Her finner man også risikoanalyse
- Systemkrav-rapport – her setter man krav til program- og maskinvare som skal brukes under prosjektet
- Driftsdokument – her forklarer man i detalj hvordan oppsettet brukes, og hvordan det driftes i ettertid
- Sluttrapport – oppsummering av alt som har skjedd i prosjektet, anbefaling til videre arbeid

Prosjektet kommer også til å ha følgende vedlegg

- Prosjekthåndbok – inneholder fremdriftsplan, alle møteinnkallinger og referater, samt timelister m/statusrapport
- Presentasjon – den endelige presentasjonen som blir avholdt ved prosjektets slutt

# Gjennomføring av prosjektet

Prosjektet startet greit, hvor på man først begynte på å lese seg opp litt om systemet. Man begynte med forstudierapporten som første del av prosjektet. På grunn av ulike andre arbeidsforhold tok gjennomføringen av denne litt tid, noe som forskjøv tidsbruken i løpet av prosjektet litt. Designdokumentet gikk også greit, foruten litt mangel på informasjon som skulle flettes inn her. På grunn av dette ventet man litt med designdokumentet og gikk over til driftsdokumentet i en periode. Driftsdokumentet hadde ingen store problemer med skrivingen. Det var mye informasjon som skulle inn, men så fremt det var noe å skrive om gikk dette greit. Naturligvis ble det også endel testing av ulike funksjoner under skrivingen av driftsdokumentet, men dette var ventet og gikk veldig fint. Sluttrapporten gikk oppsummert veldig godt å skrive, og den resterende dokumentasjon i prosjektet ble også oppsummert og ferdiggjort på slutten.

Enkelte ting som gikk bra under prosjektet var blant annet testingen av funksjonalitet i Intune. Det var ingen spesielle bemerkninger som ikke virket ved grunn-funksjonaliteten i systemet. Det betyr at man fikk testet dette tidlig i prosjektet, og deretter fikk brukt den resterende tiden på å teste den nye funksjonalitet i systemet. Her var det en del som kanskje ikke virket helt med en gang, men etter litt om og men var det lite som egentlig ikke virket. Dette gjorde oppgaven litt mer spennende, og gir forhåpentligvis et bedre bilde for bedriften om hva systemet kan tilby.

Noe av det som kunne ha blitt gjort annerledes er tidsbruken under prosjektet. I den grad det var planlagt gikk selve framgangen i prosjektet greit, men på grunn av andre arbeidsoppgaver utenfor prosjektet ble det nok litt mye forskjøvet i forhold til hva som var lurt. Likevel har jeg alltid vært sikker på at prosjektet skulle bli ferdig, det var bare snakk om hvor mye som eventuelt måtte unnlates og hvor dårlig tid man fikk mot slutten. Heldigvis fikk man inn det man ønsket, og tidsbruken mot slutten gikk tålelig greit.

Jeg gjorde dette prosjektet for meg selv, noe som gir sine fordeler og ulemper. For min del var det greit å kunne arbeide alene og bestemme sin egen arbeidstid, men det er klart at man er nødt til å ha en helt annen grad av selvdisiplin når man kun er avhengig av seg selv. Jeg jobbet også mye utenfor prosjektet, og det var derfor helt nødvendig at dette prosjektet ble tatt alene. Det skal derimot ikke utelukkes at det nok også hadde vært enda mer utbredt test av funksjonalitet hvis man var flere, men jeg tror nesten oppgavebeskrivelsen i sin nåværende stand hadde blitt i overkant liten for to stk.

## Framdriftsplanen

Framdriftsplanen ble skissert under skriving av forstudierapporten. Her var det vanskelig å vite nøyaktig hvor lang tid man kom til å bruke på de forskjellige delene av prosjektet. Likevel ble det forsøkt å oppdatere denne jevnlig under prosjektet, selv om det kanskje ikke ble så ofte som man burde. Noe av utfordringen her kom også med jobbingen rundt prosjektet, noe som gjorde det litt vanskelig å planlegge spesifikke dager eller uker til de forskjellige delene. Det ble litt hopping mellom de ulike delene mot slutten, på grunn av forskjellig grad av ferdigstillelse på dokumentene.

Den faktiske framdriftsplanen ble litt annerledes enn den skisserte, men ikke spesielt mye. Det ble flyttet litt på ulike faser av prosjektet på grunn av overnevnte grunner. Ellers ble de forskjellige rapportene tatt sånn noenlunde i samme rekkefølge, på unntak av designdokumentet som ble tatt mer mot slutten av prosjektet. Alt i alt ble det et bra oppsett på framdriftsplanen etter litt justeringer.

## Timelister og ukesrapporter

Føring av timelister og gikk veldig greit. Det ble noen smutthull som man måtte fylle ut riktig informasjon på, men dette gikk seg til etterhvert. Jeg lagde en egen plan i Excel for å holde oversikt over tidsbruken. Det største problemet var nok at man i en god stund hang etter i form av timer utført i løpet av prosjektet. Likevel greide man å oppnå målet med 500 timer, selv om det ble litt hektisk mot slutten. Det skal nevnes at systemet på en måte allerede var satt opp i bedriften, noe som gjorde at man sparte endel tid på oppsett. Den ekstra tiden kom uansett godt med til å få skrive ferdig de ulike rapportene som måtte bli ferdig før prosjektets slutt.

Ukesrapportene gikk helt ok. Det var ofte at man glemte å føre ut for enkelte dager, noe som førte til at flere dager ikke fikk ført ut alle de spesifikke arbeidsoppgavene. Likevel skal de aller fleste dager være dokumentert godt nok til å beskrive det arbeidet som ble gjort for hver enkelt uke.

# Videre arbeid

Nå som prosjektet er ferdig finnes det noe arbeid som kan tas for å utvikle dette videre

## Legge inn resterende enheter inn i systemet

Det mest åpenbare steget videre er å utvide systemet til alle de andre enhetene i bedriften. I driftsdokumentet er det beskrevet flere måter å legge inn klientmaskiner på. Disse prosedyrene kan også enkelt utføres av ansatte uten hjelp av IT-ansatte. Når alle enhetene er blitt koblet opp kan man begynne å se fordelene med å ha enhetene lagt inn i ett, felles system. Man får tilgang til mange funksjoner inne på enhetene, og kan utføre «fjerndrift» som tillater å både installere applikasjoner, endre på innstillinger og generelt vite om status på de ulike maskinene. Videre drift av maskinparken vil da bli betydelig enklere for både ansatte og IT-ansvarlige, og man får et mye bedre utgangspunkt til å kjøre felles oppsett og konfigurasjon på alle maskiner.

## Overgang til Microsoft 365

Som skissert i fortstudierapporten har vi også sett på konsekvensene ved å bytte ut Office 365 med Microsoft 365. Som vist koster denne løsningen litt mer, men man får tilgang til Windows 10 Enterprise, som også gir fordeler i form av flere sikkerhets- og administreringsfunksjoner. Som nevnt er det ikke nødvendig å bytte til Microsoft 365 for å bruke systemet da det virker helt utmerket med nåværende løsning også. Men man bør uansett vurdere å få en bedre pakke, kanskje også til samme pris som man betaler nå.

## Mobile enheter

Hvis bedriften ønsker det er det mulig å også legge inn Android- og Apple-enheter inn i systemet. Det er ikke prøvd på dette i systemet, men det skal være tilrettelagt for at man uten store modifikasjoner også kan administrere disse enhetene. Det finnes ikke mange enheter i bedriften som ikke eies av privatpersoner, men man kan definitivt se på dette om man bestemmer seg for å også håndtere disse enhetene.

## Flere applikasjoner

I systemet ble det også beskrevet hvordan man kunne legge inn applikasjoner, både fra Microsoft Store men også importere egne. Dette kan lett utvides med flere applikasjoner om ønskelig. På denne måten kan man rulle ut all standardprogramvare rett fra portalen, og brukeren slipper dermed å legge inn dette i ettertid.

Kristoffer Selbekk Hille

# Klientadministrasjon med Intune og Autopilot

NTNU
Kunnskap for en bedre verden