Microsoft Modern Workspace

Eskil Uhlving Larsen Magnus Reitan Lien
eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Innhold

Modern Workspace - Forstudierapport

v.2.2

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

13. februar 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
10.01.2019	1.0	Opprettet forstudie
10.01.2019	1.1	Første utkast introduksjon fullført
11.01.2019	1.2	Bakgrunn for prosjekt og prosjektmål påbegynt
14.01.2019	1.3	Prosjektmål ferdigstillt. Interessenter og rammebetingelser påbegynt. Kritiske suksessfaktorer ferdigstilt og risikoanalyse ferdigstilt
16.01.2019	1.4	Fullført krav til dokumentasjon, anbefaling om videre arbeid og prosjektorganisering
18.01.2019	1.5	Funnet revideringspotensialer, ordforklaringer opprettet og gjort klart til kommende uke
21.01.2019	1.6	Reviderte forstudie, ordliste oppdatert, kost-nytte påbegynt
23.01.2019	1.7	Kost/nytte ferdigstilt, bakgrunn for prosjekt ferdigstilt, mindre revidering
07.02.2019	1.8	Kost/nytte revidert, Interessenter og rammebetingelser oppdatert
08.02.2019	1.9	Kost/nytte revidert, små endringer, dokumentet er overført til latex
11.02.2019	2.0	Kost/nytte revidert, mindre revisjon, latex-versjon oppdatert
13.02.2019	2.1	Lagt til logo. Oppdatert tittel. Gjennomlest og feilrettet. Lagt til referanser
21.02.2019	2.2	Lagt til draw.io for diagrammer. Endret få språkfeil

Innhold

Tabeller

Figurer

1 Introduksjon

Prosjektet vil gå ut på å migrere en fiktiv bedrifts lokale IT-system og dets brukere til en skybasert løsning. Denne løsningen vil være bygget på M365 og bruker Azure som leveringsplattform. Dette dokumentet vil danne en oversikt og gi et forståelig overblikk over dagens situasjon, hvilke endringer som vil finne sted og avslutningsvis gjøres en beslutning om prosjektet skal videreføres.

Bakgrunn for prosjektet introduserer den fiktive bedriften, deres nåværende situasjon, deres krav og ønsker som blir stilt til prosjektet og nåværende problemer.

Prosjektmål vil avklare prosjektgruppens og den fiktive bedriftens målsettinger. Her synliggjøres prosjektets omfang, underliggende hovedoppgaver og milepæler underveis i prosjektarbeidet.

Interessenter og rammebetingelser viser hvem som vil være involvert i prosjektet og dets resultat, samt rammebetingelsene for prosjektet. Her vil også taushetsplikt og rettigheter knyttet til prosjektet og underliggende dokumenter fremstilles.

Kritiske suksessfaktorer forklarer hva som kreves for at prosjektet skal lykkes og beskriver dokumenter og rapporter som skal leveres for å sikre dette.

Risikoanalysen ser på hendelser som kan ha innvirkning på prosjektets suksess, deres sannsynlighet og de eventuelle konsekvensene de vil medbringe. Her presenteres også tiltak for å begrense enten sannsynligheten eller utfallet av disse hendelsene.

Kost/nytte-analysen vil forsøke å formidle nytten av prosjektet, og om kostnaden av gjennomføring vil være forsvarlig i sammenligning.

Retningslinjer og standarder tar for seg dokumentasjonskrav, hva som skal leveres underveis og hvem som vil gjennomføre kvalitetskontroll. Her settes også krav til programvare som vil benyttes i løpet av prosjektets gang.

Prosjektorganisering gir oversikt over prosjektets gjennomføring med deltakere, ledere og andre involverte i prosjektet.

Anbefaling om videre arbeid oppsummerer forstudierapportens resultat og gir en anbefaling for arbeid videre i prosjektet.

2 Bakgrunn for prosjektet

Et økende antall bedrifter opplever at deres IT-tjenester trenger oppdatering for å henge med konkurrentene. Markedet etterspør at tjenester er tilgjengelige døgnet rundt, uavhengig av hvor man måtte befinne seg og på hvilken enhet. Nedetid eller andre problemer som senker effektiviteten fører med seg tap for bedriften, noe som gjør IT-tjenestene deres svært sårbare for digitale angrep. Ansatte stiller også stadig større krav til arbeidsgiver og sin arbeidsplass. Blant disse finnes krav om hvilke tjenester og verktøy de vil arbeide med, og det er opp til bedriften og deres IT-avdeling å etterkomme disse.

Skybaserte tjenester spiser stadig større markedsandeler fra de mer tradisjonelle serverløsningene, og dette av god grunn. Konvensjonelle løsninger går ut på å selv drifte infrastrukturen plassert on-prem, altså lokalt hos en bedrift. Skybaserte løsninger flytter infrastruktur og tjenester ut i skyen, altså til et eller flere datasenter lokalisert eksternt fra bedriften. Slike skyløsninger stiller med høy oppetid, redundans, skalerbar datakraft, oppdatert programvare, bruksstatistikk og stabile driftskostnader. Disse fordelene lar bedriftene holde fokuset på egne arbeidsoppgaver og overlater driften av dyre og kompetansekrevende ressurser til aktører med ferdighetene og kapasiteten til å håndtere slike datasystemer.

I dette prosjektet skal vi flytte de lokale IT-systemer ut i skyen på oppdrag for en fiktiv bedrift. Bedriften har en IT-strategi som sier “Cloud first”, og nå skal nye løsninger designes. Hele arbeidsflaten skal bygges på Microsoft 365 Enterprise og skal leveres i Azure.

2.1 Beskrivelse av problemer og behov

Bedriften opererer i dag med en tradisjonell arbeidsflate med maskiner on-prem. For at de ansatte skal ha tilgang til applikasjonene sine må de inn på kontoret og få tilgang til disse. De lokale maskinene er en del av det lokale AD og driftes gjennom SCCM. Med dette oppsettet finnes det ingen mulighet for hjemmekontor eller tilgang til applikasjonene på jobbrelaterte reiser og i møter hos kunder.

Det nåværende systemet er kun satt opp til å omfatte servere, stasjonære og bærbare maskiner. Det er i det siste framkommet et behov for å også kunne administrere mobile enheter. Et nytt system må dermed inkludere støtte for administrasjon av håndholdte enheter som mobiltelefoner og nettbrett.

Krav om BYOD har blitt normalisert i næringslivet, noe som gjør at bedriften må designe sine løsninger rundt funksjonalitet på mange ulike enheter. Videre etter-

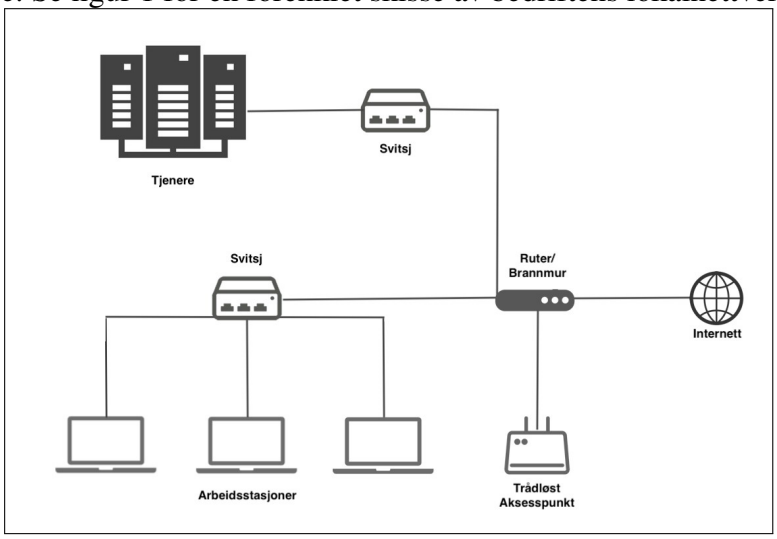
spør ansatte at tjenestene de skal bruke må fungere slik at de raskt kan komme i gang med arbeidet og ha høyest mulig effektivitet. Klarer ikke en bedrift å etterkomme disse kravene vil det kunne hindre dem ifra å innhente ny arbeidskraft og kan samtidig føre til at ansatte går til konkurrenter som oppfyller de.

Bedriften har bestemt at en ny løsning skal designes. Den nye løsningen som skal settes opp må gjenspeile bedriftens nye IT-strategi som sier cloud first. Strategien krever dermed at bedriftens infrastruktur flyttes ut i skyen, at ansatte får tilgang på tjenester og verktøy som moderniserer arbeidsplassen og at bedriften kun drifter infrastruktur som ikke kan erstattes i skyen. Den nye løsningen må være tilgjengelig uavhengig av hvor man måtte befinne seg og samtidig være robust i fall angreps- og innbruddsforsøk på bedriftens systemer.

2.2 Kort om dagens systemer og rutiner

Bedriften består av 500 ansatte fordelt over flere ulike kontor rundt om i landet, med hovedkontor i Trondheim. Ledelsen har tatt en avgjørelse om at det nåværende systemet skal flyttes ut i Azure cloud og har leid inn konsulenter med riktig kompetanse til å utføre prosjektet.

Bedriftens nåværende system består av en on-prem løsning, hvor de drifter sine egne servere. Serverløsningen inkluderer en AD-kontroller med en skog og en server med SCCM for administrering av ansattes maskiner. Løsningen har tilstrekkelig maskinkraft og tillater de 500 ansatte å utføre sine daglige arbeidsoppgaver. Dersom bedriften ser et behov for økt datakraft, vil de måtte gå til innkjøp av ny maskinvare. Se figur 1 for en forenklet skisse av bedriftens lokalnettverk.



Figur 1: Bedriftens lokalnett

3 Prosjektmål

Prosjektmålene deles inn i 3 ulike måltyper:

Effektmål - Beskriver hva som er de ønskede effektene av prosjektets resultat.

Resultatmål - Beskriver hva som konkret skal foreligge når prosjektet er ferdig.

Prosessmål - Beskriver mål for egenutviklingen hos prosjektdeltakerne gjennom hele prosjektet.

3.1 Effektmål

Prosjektets effektmål:

- Cloud first strategien vil realiseres
- Bedriften ser en reduksjon i behov for lokal infrastruktur
- Administrasjon IT-systemet vil effektiviseres ved blant annet automatisering
- Administrasjon av IT-systemet vil bli mer sentralisert
- IT-systemets oppetid blir 99.9%[1]
- Ansatte vil oppleve økt tilgjengelighet til data og applikasjoner
- Muliggjør *BYOD*
- Bedriften får en moderne arbeidsflate
- Eliminere skygge-IT

3.2 Resultatmål

Prosjektets resultatmål:

- Sitte igjen med bare én on-prem server
- IT-administrasjon går hovedsakelig via skyen
- Alle tjenester, applikasjoner og data er flyttet ut i skyen, bare AD er on-prem
- Ansatte har tilgang på tjenester utenfor bedriftens lokaler

- Mobile enheter som telefoner og nettbrett kan administreres (Android og iOS)

3.3 Prosessmål

Prosjektets prosessmål:

- Skape en helhetlig teknisk forståelse for konseptet modern workspace
- Prosjektgruppen skal forstå konseptet og prosessen i migrering av systemer fra on-prem til skytjenester
- Prosjektgruppen får kjennskap til de ulike tjenestene i Office 365

3.4 Prosjektets omfang

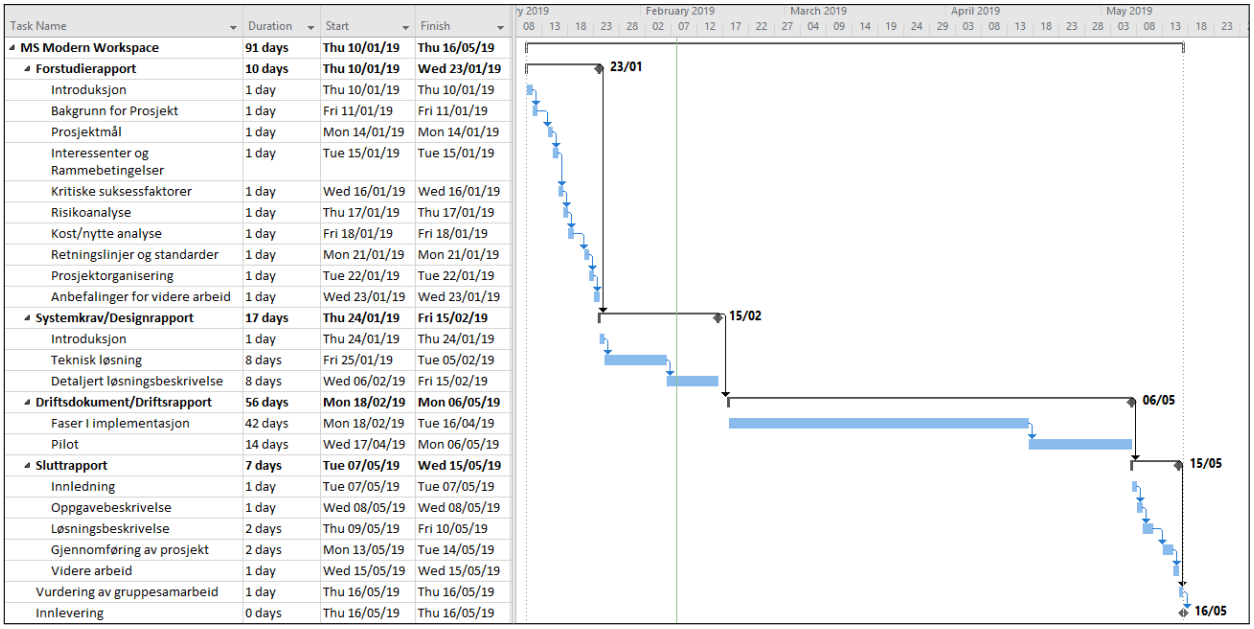
- Prosjektet vil ikke drive opplæring i bruk av nye systemer
- Prosjektet vil migrere en ferdig-oppsatt løsning til skyen
- Programvare: AD, AAD, Intune, SCCM, Office 365, Teams, SharePoint
- Operativsystemer: Windows 10, Windows Server, Android og iOS
  - Enheter med Windows 10 1809+, Android 4.4+ og iOS 10.0+ skal kunne administreres[2]
  - Enheter med MacOS og Unix distribusjoner vil ikke være kompatible
- Prosjektet vil foregå i Azure Cloud
- Microsoft 365 E3 og E5 vil benyttes
  - Lisenser vil leveres av oppgavestiller
- Oppgavestiller vil på forhånd ha satt opp lab-miljøet

3.5 Prosjektets milepæler og hovedaktiviteter

Planlagte milepæler for prosjektet er:

Forstudierapporten	23.01.2019
Designdokument	15.02.2019
Driftsdokument	06.05.2019
Sluttrapport	15.05.2019
Innlevering	16.05.2019

For en mer utfyllende og innholdsrik oversikt, se Gantt-diagrammet i figur 2.



Task Name	Duration	Start	Finish
MS Modern Workspace	**91 days**	**Thu 10/01/19**	**Thu 16/05/19**
Forstudierapport	**10 days**	**Thu 10/01/19**	**Wed 23/01/19**
Introduksjon	1 day	Thu 10/01/19	Thu 10/01/19
Bakgrunn for Prosjekt	1 day	Fri 11/01/19	Fri 11/01/19
Prosjektmål	1 day	Mon 14/01/19	Mon 14/01/19
Interessenter og Rammebetingelser	1 day	Tue 15/01/19	Tue 15/01/19
Kritiske suksessfaktorer	1 day	Wed 16/01/19	Wed 16/01/19
Risikoanalyse	1 day	Thu 17/01/19	Thu 17/01/19
Kost/nytte analyse	1 day	Fri 18/01/19	Fri 18/01/19
Retningslinjer og standarder	1 day	Mon 21/01/19	Mon 21/01/19
Prosjektorganisering	1 day	Tue 22/01/19	Tue 22/01/19
Anbefalinger for videre arbeid	1 day	Wed 23/01/19	Wed 23/01/19
Systemkrav/Designrapport	**17 days**	**Thu 24/01/19**	**Fri 15/02/19**
Introduksjon	1 day	Thu 24/01/19	Thu 24/01/19
Teknisk løsning	8 days	Fri 25/01/19	Tue 05/02/19
Detaljert løsningsbeskrivelse	8 days	Wed 06/02/19	Fri 15/02/19
Driftsdokument/Driftsrapport	**56 days**	**Mon 18/02/19**	**Mon 06/05/19**
Faser I implementasjon	42 days	Mon 18/02/19	Tue 16/04/19
Pilot	14 days	Wed 17/04/19	Mon 06/05/19
Sluttrapport	**7 days**	**Tue 07/05/19**	**Wed 15/05/19**
Innledning	1 day	Tue 07/05/19	Tue 07/05/19
Oppgavebeskrivelse	1 day	Wed 08/05/19	Wed 08/05/19
Løsningsbeskrivelse	2 days	Thu 09/05/19	Fri 10/05/19
Gjennomføring av prosjekt	2 days	Mon 13/05/19	Tue 14/05/19
Videre arbeid	1 day	Wed 15/05/19	Wed 15/05/19
Vurdering av gruppesamarbeid	1 day	Thu 16/05/19	Thu 16/05/19
Innlevering	0 days	Thu 16/05/19	Thu 16/05/19

Figur 2: Gantt-diagram

Påskeuken tar prosjektdeltakerne ferie og vil ikke være tilgjengelig dagene 15. – 22. April 2019. Dette blir ikke gjenspeilet i gantt-diagrammet. Prosjektdeltakerne har eksamen 16. Mai, noe som kan påvirke arbeidsmengden denne perioden.

4 Interessenter og rammebetingelser

4.1 Interessentanalyse

Interessentene i dette prosjektet blir prosjektdeltakerne, veileder og ATEA.

Prosjektdeltakerene skal gjennom dette prosjektet tilegne seg kompetanse og teknisk forståelse for konseptet modern workspace. Deltakerne vil også få erfaringer gjennom bruk av ulike systemer og tjenester som Azure Cloud og produktene som inngår i Microsoft 365. Prosjektgruppen vil utføre det tekniske arbeidet og ta beslutninger ved arbeidet.

Veileder Stein Meisingseth vil hjelpe prosjektdeltakerne å sette rammer rundt prosjektet, samt å velge ut fokusområder for vurderingsgrunnlaget. Ved prosjektslutt vil han være en del av gruppen som vil vurdere resultatet av prosjektet. Veileder vil kunne bidra med sin kompetanse, men ønsker samtidig å selv kunne tilegne seg ny kompetanse.

Oppgavestiller ATEA, ved Marius André Langseth-Nilsen, vil være en ressurs for prosjektgruppen. De vil bidra med kompetanse, lab-miljø, arbeidslokaler og lisenser for å hjelpe til med gjennomføring av prosjektet. De ønsker samtidig å bygge kunnskap og kompetanse ut ifra prosjektet.

4.2 Rammebetingelser

- Prosjektstart 07. januar 2019
- Prosjektet skal være ferdigstilt og all dokumentasjon levert innen innleveringsfristen 20. mai 2019
- Tidsbruk for prosjektet estimeres til 500 timer (+/- 5%) per deltaker. Total tidsforbruk vil dermed ligge mellom 950 og 1050 timer sammenlagt for deltakerne
- Prosjektet krever lisenser til flere av produktene som vil brukes
- Alle lisenser skal skaffes i henhold til norske lover og regler
- Lab-miljøet vil settes opp av ATEA før arbeid påbegynnes

4.3 Eiendomsrett

Prosjektdeltakerne vil ikke ha opphavsrett til dokumentene prosjektet produserer. Opphavsretten vil ligge hos oppgavestiller ATEA innenfor tilknyttede lover og regler.

Dokumentene vil deles mellom prosjektdeltakerne, veileder og oppgavestiller under prosjektets gang. Etter ferdigstilling vil dokumentene være under eiendom av oppgavestilleren ATEA, og skal ikke deles av noen parter før det tidsbestemte forbeholdet utløper.

Forbeholdet mot deling av dokumenter og informasjon vil vare ut året 2019.

4.4 Taushetsplikt

Prosjektdeltakerne har taushetsplikt knyttet til all bedriftsrelatert informasjon delt av eller oppdrevet hos oppgavestiller.

Prosjektdeltakerne har taushetsplikt knyttet til prosjektet og dets dokumentasjon ut året 2019.

4.5 Gradering

Prosjektrapporter og sluttprodukt har ingen gradering i henhold til Sikkerhetsloven § 11 og § 12. Jf. Offentlighetsloven § 5a.

5 Kritiske suksessfaktorer

Kritiske suksessfaktorer er de forutsetningene som kreves for at prosjektets resultat vil anses som vellykket for alle interessenter involvert. Disse står som retningslinjer for prosjektets gjennomføring og vil hjelpe prosjektgruppen holde fokus underveis.

Informasjonsbehov er de ulike dokumentene, rapportene og listene som skal produseres og leveres i løpet av prosjektet. Samlet vil denne dokumentasjonen danne et bilde av arbeidet som gjøres og i hvilket tidsperspektiv.

5.1 Suksessfaktorer

- Behovet for on-prem miljøet er eliminert, AD vil stå igjen
- Funksjonaliteten ifra det gamle systemet er bevart eller utbedret
- Prosjektdeltakerne klarer å tilegne seg tilstrekkelig kunnskaper underveis
- Tydelig kommunikasjon mellom alle interessenter, som tilbakemelding, oppfølging, rapportering og kontroll
- Tidsplaner må følges, og milepæler må nås innen satte frister

5.2 Informasjonsbehov

Følgende informasjon blir lagt ut og er tilgjengelig på prosjektets SharePoint-side.

- Timelister
- Ukesrapporter
- Møtereferater
- Forstudierapport – Prosjektets rammeverk
- Designdokument – Designet til den nye løsningen
- Driftsdokument – Detaljert beskrivelse av migrering til det nye systemet
- Sluttrapport – Tar for seg prosjektets gjennomførelse
- Vurdering av gruppesamarbeid
- Presentasjon av prosjektet
- Gantt-diagram – Prosjektets planlagte gang og tidsperspektiv

6 Risikoanalyse

Det finnes utallige faktorer som har innvirkning på prosjektets utfall. Vi har vurdert disse punktene til å være de mest kritiske faktorene for vårt prosjekt:

- Prosjektets omfang blir for stort
- Sykdom i prosjektgruppen
- Klarer ikke tilegne seg tilstrekkelig kompetanse/kunnskap
- Splid i gruppen
- Tidsplaner blir ikke overholdt

6.1 Kritiske suksessfaktorer

Nedenfor finnes en videre analyse av de mest kritiske faktorene for vårt prosjekt. I vår analyse av risikoene har vi valgt å se på sannsynligheten, konsekvensene, risikoen, tiltak og prioritering. Sannsynligheten for at den aktuelle risikoen skal inntreffe blir vurdert på en skala fra 1-10, mens konsekvensene av risikoen vurderes fra 1-5. Risikofaktoren vurderes til produktet av sannsynligheten og konsekvensene. Prioritering settes ut ifra risikofaktoren og vil bruke skalaen "Lav", "Middels" og "Høy".

- **Prosjektets omfang blir for stort**

  Dersom prosjektets omfang blir for stort kan dette føre til at økt kompetanseøkning ikke nås, tidsfrister blir ikke holdt eller i verste fall resultere i et ufullstendig resultat.

  - Sannsynlighet: 6
  - Konsekvens: 4
  - Risiko: 24
  - Prioritering: Høy
  - Tiltak: Tidlig forsøke å tilspisse oppgaven. Fokusere på helheten av oppgaven og ikke bli opphengt i detaljer.

- **Sykdom i prosjektgruppen**

  Prosjektet er stort og krever mange arbeidstimer, noe som resulterer i at det vil ikke være tilstrekkelig tid for å ta igjen et større sykefravær.

  - Sannsynlighet: 2
  - Konsekvens: 5
  - Risiko: 10
  - Prioritering: Middels
  - Tiltak: Unngå smittesoner. Bruke antibac og oppretthold god hygiene gjennom prosjekttiden.

- **Klarer ikke tilegne seg tilstrekkelig kompetanse/kunnskap**

  Med tanke på at kompleksiteten av prosjektet og at prosjektdeltakerne mangler forhåndskunnskaper på flere av viktige områder, vil det ha konsekvenser dersom kunnskapen ikke opparbeides og gjenspeiles i arbeidet med prosjektet.

  - Sannsynlighet: 5
  - Konsekvens: 3
  - Risiko: 15
  - Prioritering: Middels
  - Tiltak: Prosjektdeltakerne planlegger godt og setter av tid på egenhånd til å orientere seg om prosjektets omfang og nødvendigheter om nødvendig.

- **Splid i gruppen**

  Uenigheter mellom prosjektdeltakerne kan føre til at tiden ikke blir brukt produktivt og senke fremgangen i prosjektet.

  - Sannsynlighet: 1
  - Konsekvens: 4
  - Risiko: 4
  - Prioritering: Lav

  - Tiltak: Ha god dialog. Involvere tredjepart ved uenigheter.

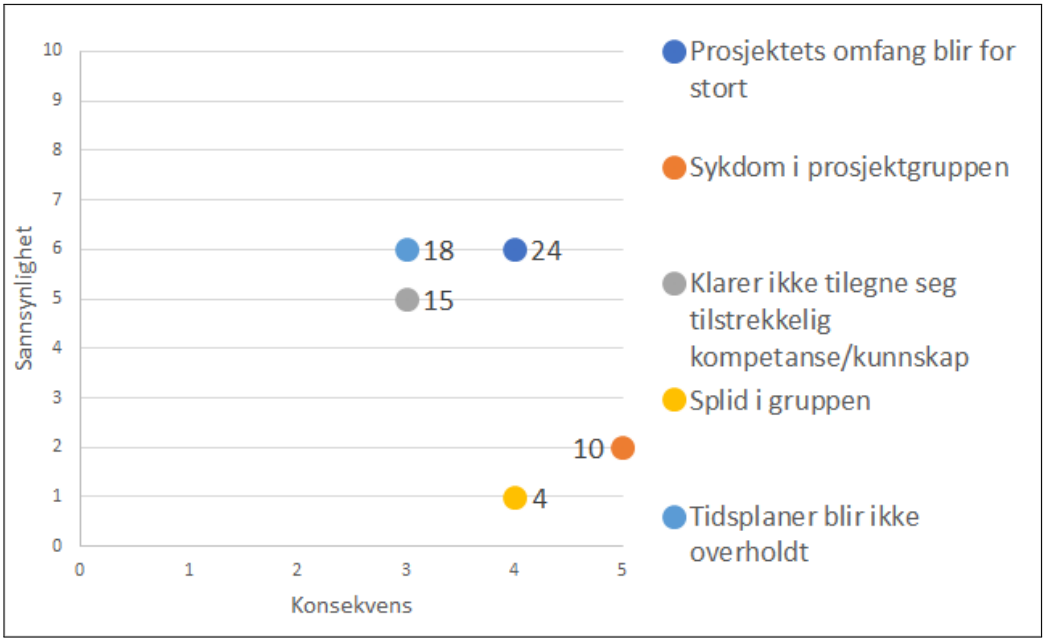
- **Tidsplaner blir ikke overholdt**

  Tidsplanen er grovt satt opp ved prosjektstart og vil revideres med nærmere info for hver uke som går. Avvik vil gi ringvirkninger utover hele prosjektet og kan føre til tidsmangel.

  - Sannsynlighet: 6
  - Konsekvens: 3
  - Risiko: 18
  - Prioritering: Høy
  - Tiltak: Tidsplanen ses på som hellig og unnvik bør være minimale. Ukentlig gjennomgang av fremgang og nærmere planlegging ved hver ukestart. Hele tiden ha en god oversikt over hvilke oppgaver som skal gjennomføres og når de skal være ferdig. Skrive gode ukesrapporter, som gir et godt overblikk over prosjektets fremgang.

6.2 Risikodiagram

I figur 3 har vi plottet truslene inn i et diagram.



Figur 3: Risikoanalyse

7 Kost/nytte-analyse

Prosjektet vil ha et begrenset behov for kost/nytte-analysen på bakgrunn av at prosjektet av natur er et investeringsprosjekt og ikke et kostnadsprosjekt. Dette vil si at prosjektet ikke ønskes gjennomført på bakgrunn av besparinger i form av kostnadskutt, men ønskes gjennomført for å investere i et system som gjør arbeidsplassen moderne og lukrativ for ansatte. Analysen vil dermed ha vansker med å kvantifisere nytte, da modernisering ikke direkte vil kunne oversettes til en satt sum. Som et resultat vil kost/nytte analysen være redusert i både omfang og størrelse.

Bedriften vil ikke anse den kvantifiserbare nytten som viktig i sitt beslutningsgrunnlag, og vil i stedet fokusere på de ikke-kvantifiserbare parameterne. Det er derimot fordelaktig for bedriften å få en oversikt over kostnader knyttet til prosjektets gjennomføring, og det ønskes derfor at analysen gjennomføres i redusert grad.

Pengesummer som produseres vil alle være estimater basert på informasjon tilgjengelig på internett. Ingen av disse estimatene vil forsøke å ta høyde for avgifter eller skatter som vil kunne oppleves i realiteten.

7.1 Kvantifiserbar og ikke-kvantifiserbar nytte

7.1.1 Kvantifiserbar nytte

Som hentydet i avsnitt 7, vil det ikke fremstilles kvantifiserbar nytte, da det ikke er grunnlag for å utrede dette ut ifra prosjektets mål. Målene er i all hovedsak rettet mot modernisering bedriftens image og IT-systemer framfor kostnadsmessige aspekter.

7.1.2 Ikke-kvantifiserbar nytte

Moderne arbeidsplass. Bedriften vil moderniseres slik at ansatte kan bruke oppdatert programvare på de enhetene, både mobile og stasjonære, de selv ønsker. De vil også få tilgang til filer og programvare utenfor arbeidsplassen, noe som gjør det lettere å arbeide på den måten man selv ønsker. Dette vil ha en positiv innvirkning på moral og effektivitet, samtidig som det vil gjøre bedriften til en mer attraktiv arbeidsplass.

Effektivisert drift og administrasjon. Ved overgang til en skytjeneste vil administrasjon og driften kunne gjøres via nettleseren, og krever dermed få steg for å gjøre endringer. Siden all drift gjøres via nettleseren er også all drift sentralisert til samme sted. Dette vil gjøre arbeidshverdagen til drifterne enklere og smidigere.

Et moderne bedriftsimage. Bedriften vil, med cloud first strategien, kunne bygge et omdømme som både signaliserer at de er en fremtidsrettet ressurs i næringslivet, og gjenspeiler deres ambisjon om å være markedsleder på teknologi. Dette vil ha positiv innvirkning på både nåværende og potensielle kunder, samtidig som det vil ha tilsvarende effekt på de ansatte.

Forenkle arbeidshverdagen. Ansatte vil kunne oppleve at de nye verktøyene gjør at arbeidsoppgaver går smidigere og reduserer teknologiske komplikasjoner. En slik arbeidshverdag er mer motiverende og givende, noe som sikrer fornøyde ansatte.

7.2 Bortfall av direkte kostnader

Strømkostnader. På bakgrunn av migreringen til skytjenester vil det forsvinne kostnader knyttet til elektrisitet for store deler av infrastrukturen. Basert på gjennomsnittlige strømpriser estimeres det at prosjektet vil kutte strømkostnader tilsvarende 20 000 kr årlig. [3]

Oppgradering av maskinvare. Dagens løsning trenger årlig vedlikehold som nye disker til redundans eller sikkerhetskopiering. I budsjettet er det lagt av 60 000 kr årlig for slik vedlikehold. På bakgrunn av antall servere som vil kunne stenges, estimeres det at dette vedlikeholdsbudsjettet kan reduseres med 50 000 kr, fra 60 000 kr til 10 000 kr.

Redusere behov for arbeidskraft. Dagens serverpark krever at vedlikehold, administrering og oppdateringer utføres av ansatte i bedriften. Med dagens behov krever det i årlig 1,5 årsverk. Etter prosjektet ferdigstilles ser vi at dette kan reduseres til 0,5 årsverk, altså en 50% stilling. Det estimeres at kostnadene knyttet til arbeidskraft kan reduseres med 500 000 kr årlig.

Windows 10 lisenser. De ansattes datamaskiner krever en Windows 10 lisens, der hver enkelt bruker har en egen lisens. Av disse vil 100 være Windows 10 Enterprise E5 og 400 være Windows 10 E3. Disse lisensene estimeres til en årlig kostnad på 430 000 kr. [4]

Microsoft Office Home & Business. De ansatte bruker i dag Office programvaren som krever en lisens for hver enkelt bruker. Lisensene vil vare over en lengre tidsperiode enn kost/nytte-analysen vil kunne gjenspeile, men må fornyes for å kunne

opprettholde kompatibilitet og være oppdaterte. Disse lisensene har en estimert kostnad på 1 070 000 kr. [5]

Windows Server lisenser. Dagens serverpark krever Windows Server lisenser for de ulike tjenerne som kjører. Disse lisensene vil vare over en lengre tidsperiode enn kost/nytte-analysen vil kunne gjenspeile, men må byttes ut når støtte fra Microsoft slutter. Estimert kostnad på disse er 25 000 kr. [6]

SQL Server lisenser. Dagens SQL-tjener krever lisenser basert på antall kjerner i prosessoren. Disse lisensene vil vare over en lengre tidsperiode enn kost/nytte-analysen vil kunne gjenspeile, men må byttes ut når støtte fra Microsoft slutter. Estimert kostnad på disse er 127 000 kr. [7]

System Center Configuration Manager lisens. Dagens SCCM krever lisenser basert på antall kjerner i prosessoren. Disse lisensene vil vare over perioder på 2 år før de må fornyes. Estimert kostnad på disse er 11 500 kr. [8]

7.3 Estimerte kostnader

Prosjektgruppen vil ta timebetaling for arbeidet gjort i planleggingsprosessen og selve gjennomføringen av prosjektet. Prosjektet har et tidsperspektiv på omtrent 5 måneder, hvor konsulenter vil bruke ca. 1000 timer totalt. Kostnaden for dette arbeidet blir dermed 700 000 kr sammenlagt dersom timeplanen overholdes.

Lisenser vil bli en større og vedvarende kostnad for bedriften. Kostnadene vil vedvare så lenge bedriften ønsker å ta i bruk produktene Microsoft leverer via skyen. Lisensene som kjøpes inn er 400 Microsoft 365 E3 lisenser og 100 Microsoft 365 E5 lisenser. E3-lisensene vil ha en estimert årlig kostnad på 1 392 000 kr. E5-lisensene vil ha en estimert årlig kostnad på 648 000 kr. [9]

7.4 Sammenstilling kost/nytte

År 0 i tabell 2 vil referere til planlegging, gjennomføring og ferdigstilling av prosjektet, og vil derfor kun ha kostnader knyttet til gjennomføringen av prosjektet. Besparelser og videre kostnader som kommer som et resultat av prosjektet vil starte fra år 1.

Tabell 2: Kost/Nytte

	År 0	**År 1**	**År 2**	**År 3**	**År 4**	**Sum**
Kvantifiserbar nytte	0	0	0	0	0	**0**
Bortfall av kostnader	0	70 000	70 000	70 000	70 000	**280 000**
Bortfall av lisenskostnader	0	1 663 500	430 000	441 500	430 000	**2 965 000**
Bortfall av arbeidskraft	0	500 000	500 000	500 000	500 000	**2 000 000**
Sum nytte	**0**	**2 233 500**	**1 000 000**	**1 011 500**	**1 000 000**	**5 245 000**
Utviklingskostnader	700 000	0	0	0	0	**700 000**
Drifts- og forvaltningskostnader	0	0	0	0	0	**0**
Lisenskostnader	0	2 040 000	2 040 000	2 040 000	2 040 000	**8 160 000**
Sum kostnader	**700 000**	**2 040 000**	**2 040 000**	**2 040 000**	**2 040 000**	**8 860 000**
Beregnet nytte	**-700 000**	**193 500**	**-1 040 000**	**-1 028 500**	**-1 040 000**	**-3 615 000**

7.4.1 Ikke-kvantifiserbar nytte

Det er mange parameter som bidrar til en økt ikke-kvantifiserbar nytte og disse lar seg ikke omgjøre direkte til økonomisk fordel. Som nevnt i avsnitt 7.1.2 vil denne ikke-kvantifiserbare nytten resultere i økt moral og en mer forenklet og motiverende arbeidshverdag for de ansatte. Arbeidsplassen vil derfor også være attraktiv for jobbsøkere samtidig som trivselen for nåværende ansatte vil være høy. Bedriftens kunder og eksterne personer vil også få et nytt bilde av bedriften som moderne og fremtidsrettet, noe som vil kunne hente nye kunder og holde nåværende kunder trofaste.

8 Retningslinjer og standarder

8.1 Krav til dokumentasjon

Tabell 3: Dokumentasjon

Navn	Dato	Form	Merknader
Forstudierapport	20.05.2019	Elektronisk	
Designdokument	20.05.2019	Elektronisk	
Driftsdokument	20.05.2019	Elektronisk	
Sluttrapport	20.05.2019	Elektronisk	
Vurdering av gruppesamarbeidet	20.05.2019	Elektronisk	
Timelister	20.05.2019	Elektronisk	Inkl. i sluttrapport
Ukesrapporter	20.05.2019	Elektronisk	Inkl. i sluttrapport

Dokumentasjonen som skal leveres er vist i tabell 3.

Veileder har fremmet ønske om at alle rapporter skal leveres digitalt og det kommer ikke fram noen krav om papireksemplarer fra NTNUs side. Eventuelle ønsker om papirutgaver av de ulike dokumentene må fremmes til prosjektdeltakerne i tilstrekkelig tid før de ulike fristene. Alle innleveringer vil følge frister satt av NTNU.

All dokumentasjon som produseres i løpet av prosjektets livstid vil tilgjengeliggjøres fortløpende på prosjektets SharePoint-side, og vil være tilgjengelig til alle døgnets tider. SharePoint-siden (krever innlogging) kommer du til ved å klikke her. Siden vil bare være tilgjengelig for prosjektpartene.

8.2 Krav til kvalitetsgjennomganger

Rapportene i tabell 3 leveres inn til de gitte datoene i samme tabell. De skal være tilgjengelig for alle på SharePoint-siden. Tilbakemeldingene vil danne grunnlaget for videre revisjon av rapportene.

Både styringskomiteen og prosjektdeltakerne skal sammen utføre kontroll av dokumentene som leveres.

Dokumentene som leveres inn, deres kvalitet og hvordan prosjektet er blitt gjennomført vil legge grunnlaget for vurderingen. Tidsfrister som brytes vil kunne påvirke denne vurderingen negativt. Når prosjektet er ferdig skal det holdes en presentasjon som også vil stille som grunnlag for vurderingen.

8.3 Krav til standarder og metoder

Dokumentmaler som brukes er enten utlevert av NTNU eller hentet direkte fra NTNUs nettsider. Disse vil tilgjengeliggjøres via prosjektets SharePoint-side (krever innlogging).

Prosjektet vil bruke følgende standarder:

- Referansestil: Harvard
- Møtereferater vil følge navnestandarden **dd-mmm-Møtereferat**
- Ukesrapportene vil følge navnestandarden **Uke X-Ukesrapport**
- Figurer vil følge navnestandarden **Figur X**
- Tabeller vil følge navnestandarden **Tabell X**

Prosjektet vil benytte følgende verktøy:

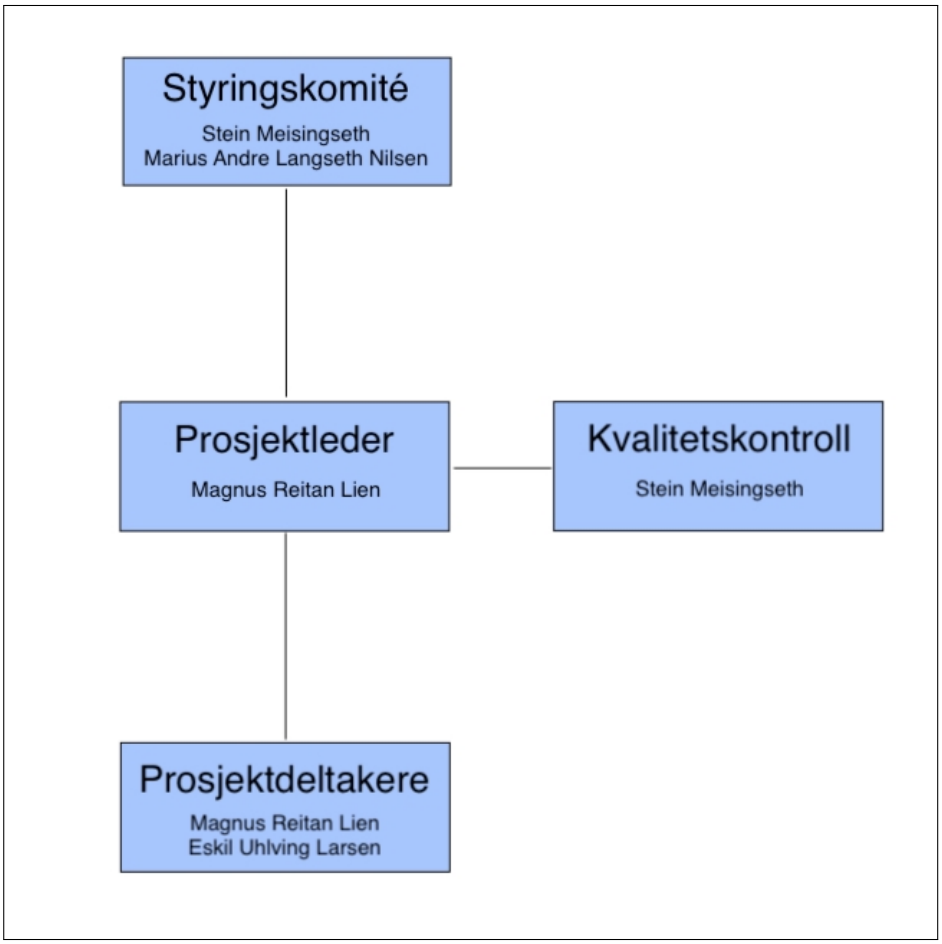
- MS Project for utforming av gantt-diagram
- Draw.io for utforming av andre diagrammer
- MS Word for rapportskriving og annen dokumentasjonskriving
- LaTeX for ferdig dokumentasjon
- MS Excel for timelister
- Azure som nettskyplatform
- Microsoft 365 E5 og E3

8.4 Endringshåndtering

Ønsker om endringer av dokumentasjon tas opp og avtales på møter, og vil være grunnlaget for nye revisjoner. Godkjenning av endringene gjøres på påfølgende møte.

Ved avvik fra prosjektplanen må det meldes ifra til veileder og oppgavegiver snarest.

9 Prosjektorganisering



Figur 4: Prosjektorganisering

Prosjektorganiseringen er vist i figur 4.

Kontaktperson for oppgavestiller (ATEA) er Marius Andre Langseth-Nilsen. Stein Meisingseth er valgt til veileder. Sammen utgjør disse styringskomiteen.

Stein Meisingseth fungerer som kvalitetskontroll.

Prosjektlederen er Magnus Reitan Lien, som også er en del av prosjektdeltakerne. Eskil Uhlving Larsen utgjør resten av prosjektdeltakerne. Fordelingen av arbeidsoppgavene blir vurdert etter hvert som de klargjøres.

10 Anbefaling om videre arbeid

På bakgrunn av arbeidet gjort i forstudierapporten, konkluderes det med at prosjektet anbefales å videreføres. Det kommer også frem at videre arbeidet med prosjektet burde utføres innenfor de rammene og planene som er lagt frem. Ved å gjennomføre prosjektet vil flere mål realiseres og bedriftens nye strategi etterfølges.

Gjennom det videre arbeidet i prosjektet vil dagens system erstattes med et nytt system, der tilnærmet alle tjenester og data er flyttet ut i skyen.

Ordforklaringer

Tabell 4: Ordforklaringer

Ord	Forklaring
AD	Active Directory er en katalogtjeneste for Windows-domener levert av Microsoft.
AAD	Azure Active Directory. Skybasert katalogtjeneste levert av Microsoft.
Azure (cloud)	Skyløsning levert av Microsoft.[10]
BYOD	Bring your own device er en policy som tillater ansatte å bruke personlige maskiner på jobb og lar disse få tilgang på bedriftens arbeidsverktøy og informasjon.
Cloud First	IT-strategi som går ut på at flest mulige tjenester skal leveres gjennom en skyløsning.
Intune	Administrasjonsverktøy for datamaskiner og mobile enheter.
M365 E	Microsoft 365 Enterprise er programvareabonnement for arbeidshverdagen levert av Microsoft. Abonnementet inkluderer blant annet operativsystem til datamaskiner, samarbeidsverktøy, produktivitetsverktøy, sikkerhetsverktøy og administrasjonsverktøy. Det kommer i to varianter E3 og E5. Der E5 er den mest omfattende varianten, med de nyeste og mest avanserte verktøyene for sikkerhet, samarbeid og beskyttelse mot trusler. (advanced threat protection, security and collaboration tools)[11]
Office 365	Programvareabonnement for arbeidsverktøy som Word, Excel osv. Leveres av Microsoft
On-Prem	On-premise er når infrastruktur står i bedriftens lokaler.
Ord	Forklaring
SCCM	System Center Configuration Manager er programvare for administrasjon av grupper av datamaskiner som kjører samme eller ulikt operativsystem levert av Microsoft.
SharePoint	Web-basert samarbeidsplattform som integrerer med office-programmer som Word, Excel osv. Leveres av Microsoft.

Fortsetter på neste side

Tabell 4 – fortsettelse ifra forrige side

Ord	Forklaring
Skygge-IT	Beskriver systemer og filer IT-ansvarlige i en bedrift ikke kan gjøre rede for. Eksempelvis vil være bedriftsdokumenter lagret i en personlig Dropbox eller på en ekstern harddisk ikke eid av bedriften. IT-ansvarlige vil ikke kunne holde oversikt over, endre, slette eller på annet vis administrere slike dokumenter.
Teams	Samarbeidsverktøy som integrerer chat, møter, notatskriving og deling av filer i en og samme programvare. Leveres av Microsoft og er en del av Office 365.

Referanser

[1] Microsoft. *SLA for Cloud Services*. 2017. URL: https://azure.microsoft.com/en-us/support/legal/sla/cloud-services/v1_5/ (sjekket 13.02.2019).

[2] Microsoft. *Supported operating systems and browsers in Intune*. 2018. URL: https://docs.microsoft.com/en-us/intune/supported-devices-browsers (sjekket 23.01.2019).

[3] Statistisk sentralbyrå. *Elektrisitetspriser*. 2018. URL: https://www.ssb.no/elkraftpris/ (sjekket 13.02.2019).

[4] Mary Jo Foley. *Microsoft acknowledges price increases coming for Office 2019 and Windows 10 Enterprise users*. 2018. URL: https://www.zdnet.com/article/microsoft-acknowledges-price-increases-coming-for-office-2019-and-windows-10-enterprise-users/ (sjekket 13.02.2019).

[5] Microsoft. *Choose the best Office for your business*. 2019. URL: https://products.office.com/en-us/get-started-with-office-2019#compare_table (sjekket 13.02.2019).

[6] Microsoft. *Pricing and licensing for Windows Server 2019*. 2019. URL: https://www.microsoft.com/en-us/cloud-platform/windows-server-pricing (sjekket 13.02.2019).

[7] Microsoft. *SQL Server pricing*. 2019. URL: https://www.microsoft.com/en-us/sql-server/sql-server-2017-pricing (sjekket 13.02.2019).

[8] Microsoft. *How to buy System Center*. 2019. URL: https://www.microsoft.com/en-us/cloud-platform/system-center-pricing (sjekket 13.02.2019).

[9] Lisa Curry. *Microsoft 365 Business vs Microsoft 365 Enterprise*. 2018. URL: https://www.chorus.co/resources/news/microsoft-365-business-vs-microsoft-365-enterprise (sjekket 13.02.2019).

[10] Microsoft. *Din visjon. Din sky.* 2019. URL: https://azure.microsoft.com/nb-no/ (sjekket 13.02.2019).

[11] Microsoft. *Discover the Microsoft 365 Enterprise solution that's right for you*. 2018. URL: https://www.microsoft.com/en-us/microsoft-365/compare-all-microsoft-365-plans (sjekket 13.02.2019).

Modern Workspace - Designdokument

v.2.5

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

25. februar 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
17.01.2019	1.0	Rapport opprettet.
24.01.2019	1.1	Introduksjon opprettet og ferdigstilt.
28.01.2019	1.2	Beskrivelse av teknisk løsning begynt.
31.01.2019	1.3	Videre arbeid på beskrivelse av teknisk løsning, detaljert løsningsbeskrivelse opprettet.
01.02.2019	1.4	Videre arbeid på detaljert løsningsbeskrivelse.
04.02.2019	1.5	Arbeid gjort på detaljert løsningsbeskrivelse og beskrivelse av teknisk løsning. Ordforklaringer oppdatert.
06.02.2019	1.6	Slått sammen deler av rapporten. Lagt til punkter for OS, autopilot og sikkerhet.
07.02.2019	1.7	Sikkerhet, enhetsregistrering oppdatert, OS og Intune ferdigstilt.
11.02.2019	1.8	Ordforklaringer oppdatert, sikkerhet ferdigstilt.
14.02.2019	1.9	Lagt inn grenser for Office 365, revidert OneDrive og SharePoint.
15.02.2019	2.0	Lagt til løsningsdiagram og flytdiagram, oppdatert ordforklaringer, revidert introduksjon, lagt til Single Sign-On og Intune connector.
18.02.2019	2.1	Løsningsdiagram beskrevet, teknisk avgrensning lagt til, teknisk løsning ferdigstilt, referanser ryddet, ordforklaringer oppdatert, introduksjon revidert, veien videre ferdigstilt, detaljert løsningsbeskrivelse ferdigstilt.
20.02.2019	2.2	Teknisk løsningsbeskrivelse omorganisert, Office 365 opprettet og ferdigstilt.
21.02.2019	2.3	Dokument overført til LaTeX, løsnings- og flytdiagram revidert, lagt til referanser, introduksjon revidert, Cloud App Security opprettet og ferdigstilt, språkfeil fikset.
22.02.2019	2.4	Beskrivelse av løsningsdiagram revidert, referanser oppdatert, bilder reorganisert, språkfeil rettet, tabeller revidert, gjennomgang av hele dokumentet.
25.02.2019	2.5	Ordforklaringer oppdatert og mindre skrivefeil rettet.

Innhold

Tabeller

Figurer

1 Introduksjon

I dette dokumentet vil vi se nærmere på løsningen som skal leveres, hvilke produkter som vil brukes og hvilke steg som skal tas for å møte bedriftens krav og behov. Dette dokumentet bygger på kunnskapen opparbeidet i forstudierapporten, og vil ta utgangspunkt i avgjørelser tatt i denne. Eventuelle avvik fra veiplanen lagt i forstudierapporten vil beskrives og begrunnes slik at leser kan følge prosjektets gang.

Introduksjonen vil se på bedriften, deres nåværende funksjonalitet og behov, og begrunne valgene som tas for prosjektet. Her vil vi også avgrense prosjektet, slik at ikke finnes noen uklarheter i hva dokumentet dekker og hvorfor noe eventuelt ikke vil dekkes.

Teknisk løsningsbeskrivelse vil gå i dybden på hva som vil erstattes og med hva. Her vil fokuset ligge på infrastrukturen, tjenestene og programvaren som vil introduseres for bedriften, hvordan opplevelse brukerne vil få av det nye systemet og veien som tas for å migrere. Her vil de foreligge detaljerte beskrivelser av ulike produkter og deres attributter for å gi leser en forståelse både for hva som introduseres, men også verdien av å introdusere det. Det vil avklares ulike tjenester som ikke implementeres og hvorfor.

Begrensninger tar for seg begrensninger i programvare, applikasjoner og tjenester som kommer til å tas i bruk. Dette vil kunne gi leser referansepunkter for hvorfor spesifikke avgjørelser tas underveis.

Detaljert løsningsbeskrivelse vil se på prosjektets planlagte vei videre og prosjektere det nye systemet som vil implementeres. Her vil det legges frem en visuell og en tekstlig beskrivelse, slik at leser enkelt kan følge prosessen.

Veien videre vil se på målene som forventes å nås som resultat av gjennomføring av prosjektet og hvordan det forventes at implementasjonsprosessen vil foregå. Denne prosessen blir skissert gjennom et flytdiagram.

Dokumentet er konstruert slik at behovet for kunnskap innad drift, infrastruktur og generell IT er begrenset. Med hjelp av ordforklaringer og beskrivelser av teknisk innhold, forsøker vi å forme dokumentet slik at ufaglærte kan forstå innhold og avgjørelser som tas. Beslutningen om å utforme dokumentet på denne måten er for å være imøtekommende, etterkomme behovene og tilpasse innholdet til leseren.

1.1 Bakgrunn for valg av løsning

Microsoft 365 E3 og E5 bygget på Azure-plattformen vil tilby bedriften skaleringsmuligheter, høy oppetid, høy sikkerhet, tilgang på oppdatert og brukerorienterte verktøy, sentralisert administrering samt tids- og kostnadsbesparende automatisering av tjenester. Microsoft har også vist gjennom sine hyppige oppdateringer og fokus på kundene at de er dedikerte, og at forplikter seg til å lage den beste skyplattformen med de beste verktøyene for bedrifter.

Valget av Azure støtter også opp mot bedriftens nye cloud first-strategi. Dette er en strategi som vil være markedsledende i et norsk næringsliv som opplever et enormt moderniseringsengasjement. Microsoft 365 E er samtidig en av få verktøy som inkluderer en helhetlig pakke med OS, programvare og sikkerhetsfunksjoner. Sammen gir disse bedriften en arbeidsplass som er effektiv, moderne og brukerorientert.

Løsningen kommer ikke til å være kostnadsbesparende, som vist i kost-/nytteanalysen i forstudiet. Prosjektet er valgt som et investeringsprosjekt grunnet moderniseringsengasjementet i bedriften.

1.2 Avgrensning

Oppgaven er designet for en bedrift med 500 ansatte, hvor de på nåværende tidspunkt drifter sin egen infrastruktur. Prosjektgruppen vil ikke ha kapasitet til å realisere infrastrukturen som foreligger i oppgaven, men vil bruke et forenklet lab-miljø som vil gjengi bedriften i liten skala.

Det foreligger også krav om en helhetlig forståelse for konseptet Modern Workspace, noe som krever at prosjektdeltakerne vil sitte igjen med kunnskap innad Office 365, Intune, Teams, sikkerhet i sky og SharePoint. På bakgrunn av tidsbegrensninger vil det ikke være mulig å bedrive omfattende arbeid på alle punkter, og fokuset vil derfor ligge i å få en underliggende forståelse for alle områder.

1.3 Kort om kunden og behov

Bedriften er et selskap med 500 ansatte fordelt på flere kontor rundt om i Norge, med hovedkontor i Trondheim. De har per i dag en on-prem løsning som driftes in-house av ansatte i driftsavdelingen. På bakgrunn av en avgjørelse om endring i strategi og modernisering av bedriftens infrastruktur og arbeidsverktøy, ønsker de

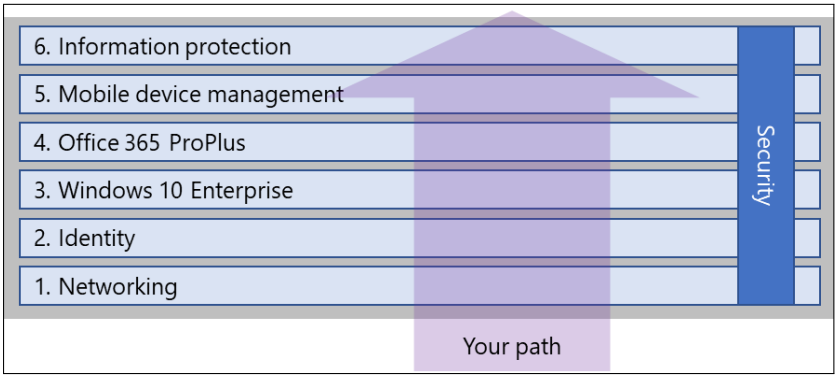
å flytte infrastrukturen ut i skyen samt å ta i bruk arbeidsverktøy gjennom innkjøp av M365 E-lisenser.

Bedriften ser på prosjektet som et investeringsprosjekt som i lengden vil ha positiv innvirkning på ansatte, kunder og bedriftsimage. Investeringen vil ikke nødvendigvis ha umiddelbar positiv innvirkning på inntjeninger og utgifter, men det understrekes at dette ikke er fokuset for prosjektet sett fra et kortere tidsperspektiv.

2 Teknisk løsningsbeskrivelse

Her vil vi se på programvare, fastvare, tjenestene og programvaren som vil implementeres i det nye systemet. Dagens løsning vil kort beskrives for å kontekstualisere eventuelle endringer i brukeropplevelse og for å fremheve ny funksjonalitet. Vi vil ikke her gå i dybden på stegene som må tas for å migrere infrastruktur, tjenester, drift eller programvare til skyen.

Siden store deler av infrastrukturen er ønsket vekk, kan prosjektet fort bli stort. Valgt løsning går ut på å sette opp en ny løsning i skyen, og gradvis flytte deler av on-prem løsningen over til skyløsningen. Ved å bryte prosessen ned i mindre deler, kalt moduler, vil det bli færre faktorer som kan feile samtidig og feilsøking vil kunne skje på et konsentrert område.



Figur 1: Migreringsprosessen

Rekkefølgen på de ulike modulene vil skje i samsvar med figur 1. Prosjektet kommer til å fokusere på punktene to til seks. Identitetene vil være første fase mens sikkerhetstiltak for oppsatt løsning vil være det siste som skjer i prosjektet.

2.1 Operativsystemer

Med Intune har Microsoft lagt til rette for støtte av mange ulike operativsystemer. På bakgrunn av bedriftens behov og krav, vil det kun legges opp til støtte for de viktigste operativsystemene i markedet.

Her vil operativsystemene kort presenteres og forklares. Vi vil komme tilbake til oppsett og konfigurasjon av disse senere i dokumentet.

2.1.1 Windows 10

Det nyeste OS for klientmaskiner er Windows 10 1809. Windows 10 inneholder de nyeste funksjonene for å driftes effektivt gjennom skyen. Windows 10 vil kommunisere med Intune og Azure AD. For å sikre tilgang til lokale tjenester, som skrivere, vil Windows 10 også bli med i det lokale domenet gjennom en "hybrid-join". Siden store deler av kommunikasjonen går gjennom sky kan man jobbe effektiv uten å måtte tenke på om man er på lokalnettet eller på et annet eksternt nettverk.

Windows 10 styres av Intune gjennom MDM protokollen over HTTP med TLS.[1] I Intune kan man opprette policies for alle maskinene. Hvis det er behov for egne policies for kun lokale maskiner, kan dette gjøres gjennom Group Policy eller Intune-policies med conditional access.

2.1.2 iOS

iOS er Apples mobile operativsystem som alle Apple-mobiltelefoner kommer preinstallert med. I Norge bruker omtrent halvparten av alle nordmenn iOS som sitt mobile operativsystem[2], og det vil derfor være viktig for en bedrift å imøtekomme ansatte som ønsker å bruke operativsystemet.

Intune lar deg registrere både ansattes personlige og bedriftseide iOS-enheter, og står samtidig for driften av disse. Dette betyr at det er støtte for mobile enheter distribuert gjennom bedriften og BYOD for ansatte som ønsker å bruke en selvvalgt mobil enhet til arbeid.[3]

2.1.3 Android

Android er Googles mobile operativsystem og kommer preinstallert på mobiler fra mange ulike produsenter. Android brukes av omtrent halvparten av alle nordmenn[2], og det er derfor viktig for bedrifter å kunne tilby støtte for operativsystemet til de ansatte.

Android kan, på lik linje med iOS, fjerndriftes gjennom Intune. Android-enheter vil kunne registreres i løsningen ved å laste ned "Intune Compant Portal" fra Google Play butikken på enheten. Når registreringen er fullført vil man gjennom Intune kunne konfigurere enheten og dens innstillinger, samt kunne distribuere applikasjoner fra Google Play butikken.[4]

2.2 Azure Active Directory

Azure Active Directory er Microsofts egne katalogtjeneste i skyen.[5] Azure AD kan inneholde mye av den samme informasjonen som lokal AD. Her kan det opprettes digitale brukerkontoer, og alle egenskapene som tilhører den kan lagres. Dette kan være brukernavn, passord-hash, roller, lisenser, gruppe-tilhørlighet, etc. Enheter som datamaskiner og mobiler kan også registreres i Azure AD. Siden Azure AD ligger i skyen, kan man autentisere seg selv om man ikke har direkte tilgang til lokal AD, dette gir høyere tilgjengelighet enn med en lokal AD.

Siden ansattes digitale identitet brukes i flere tjenester til autentisering, er det svært viktig at denne informasjonen beholder sin integritet og konfidensialitet. For å gi sanntidsbeskyttelse av brukerobjektene i Azure AD, vil vi ta i bruk Microsoft Azure Identity Protection som følger med MS365. Med Microsoft AIP vil man kunne oppdage mistenkelig brukeradferd eller kompromitterte brukerkontoer og kunne blokkere de. Overvåkingen skjer i sanntid og varsler kan sendes ut med en gang trusler oppdages.

Azure AD vil ikke erstatte den lokale AD serveren i det nye systemet. I stedet vil de to bli knyttet opp imot hverandre, synkroniseres og dele på informasjon som brukernavn og passord-hash. Da oppnås den høye tilgjengeligheten som Azure AD tilbyr, samtidig som det fortsatt vil være mulig å katalogisere lokalt utstyr som skrivere. Denne synkroniseringen er det programmet Azure AD Connect som skal sørge for.

2.2.1 Azure Active Directory Connect (Azure AD Connect)

Microsoft har utgitt en programvare kalt Azure Active Directory Connect, eller bare Azure AD Connect. Denne programvaren installeres på AD-tjeneren og tar for seg synkroniseringen mellom lokal AD og Azure AD, slik at de alltid inneholder den samme informasjonen om en identitet.[6] For å sikre oss fra motstridende data må det sikres at informasjonsendringer synkroniseres begge veier, slik som password writeback.[7]

I programvaren kan man blant annet velge spesifikke OU'er som skal synkroniseres. Enheter kan også synkroniseres ved bruk av Azure AD Connect. Siden dagens AD bare har en skog vil der være tilstrekkelig med en AAD Connect.[8]

2.2.2 Azure Active Directory Seamless Sign-On

Ved å benytte AAD og AAD Connect vil det være mulig for brukerne og logge inn på tjenester helt uten å måtte oppgi innloggingsinfo. Dette er Azure AD Seamless SSO (AAD Seamless SSO).[9] Når brukerne er koblet på bedriftsnettverket med registrerte enheter vil de bli logget inn automatisk med samme brukernavn og passord som de er logget inn med på selve enheten, Dette gir kjapp tilgang til skytjenester uten behov for noe ekstra infrastruktur on-prem.

2.3 Intune

Microsoft Intune er en skybasert løsning for administrering av mobile enheter og operativsystemer, en MDM løsning (Mobile Device Management Solution). Intune inneholder mye av den samme funksjonaliteten som SCCM, men Intune har sin funksjonalitet i skyen og ikke on-prem. Via Intune kan man definere strategier for administrasjon av mobilenheter som passer organisasjonens behov.[10]

Intune støtter et bredt spekter av mobile økosystemer og gjør det hele å administrere på én enkel løsning. Uansett om enheten kjører Windows, MacOS, iOS eller Android er det mulig å administrere den. Når en Windows 10 enhet registreres i Intune vil en kunne overvåke klientens helsestatus i sanntid.

Intune kan også stå for sikkerhet. Ved bruk av smarte regler og policies får man beskyttet selve enheten og all informasjon som finnes på den. Policies i Intune bidrar til å holde bedriftens data sikre. Gjennom Intune kan man også fjerne all firmadata på registrert enheten ved uten å påvirke personlig og privat data på enheten. Dette kan være nyttig ved tyveri eller avsluttet arbeidsforhold.

Intune samarbeider med Azure AD. Azure AD benyttes for delegering av tilganger til applikasjoner i selvbetjeningsportal og publisering av tvangsinstallerte applikasjoner. Det vil opprettes dynamiske grupper med organisatoriske roller slik at ulik programvare kan distribueres til ulike grupper samt ulike grupper kan ha ulike sikkerhetstiltak.

2.3.1 SCCM

Dagens infrastruktur inneholder en SCCM-server for administrering av de lokale arbeidsstasjonene. Alle applikasjoner og programvare som dyttes ut til brukere går gjennom denne tjeneren. Også lokalmaskinenes antivirus, antimalware og brannmur administreres gjennom SCCMs Endpoint Protection. Disse sikkerhetsfunk-

sjonene er helt essensielle for å opprettholde konfidensialitet og hindre skadelig programvare fra å infiltrere bedriftens nettverk.

Når det nye systemet med Intune skal settes opp, vil det kun være applikasjonsutrullingene som skal tas med til det nye systemet. Sikkerhetsregler vil settes opp på nytt i det nye systemet gjennom Intune. For å flytte applikasjonsutrullingsdata fra SCCM til Intune vil prosjektet benytte Intune Data Importer.[11]

Når prosjekter er over vil det ikke lengre være behov for SCCM-serveren.

2.3.2 SQL

SQL-serveren har i dagens system kun vært påkrevd på grunn av SCCM-serveren. Dette betyr at denne kunne avvikles ved prosjektets slutt og det vil ikke settes opp en erstatning i skyen.

2.4 Office 365

Her vil vi se på programvarepakken Office 365 som skal implementeres for å erstatte store deler av enbrukerlisensprogramvaren som brukes i dagens system. Pakken inneholder Exchange Online, OneDrive, SharePoint, Teams og kontorprogrammer som Word, Excel og PowerPoint.[12] Vi vil komme nærmere inn på de individuelle produktene og hva som inngår i overgangen til disse i egne punkter under.

2.4.1 Exchange Online

Epost- og kalenderfunksjonalitet er i dag uunnværlig funksjonalitet som bedriften og de ansatte er avhengig av for kommunikasjon og planlegging. Den nye løsningen som vil introduseres, Exchange Online og Office 365, vil erstatte den gamle løsningen, en on-prem Exchange-tjener og Outlook programvare installert på arbeidsstasjonene. Denne nye løsningen vil ha samme, eller bedre, brukeropplevelse og vil oppleves som en evolusjon framfor en revolusjon for de ansatte. Dette betyr at de vil kunne kjenne seg igjen i bruken av den nye løsningen, men samtidig oppleve ny og utvidet funksjonalitet.

Brukeropplevelsen

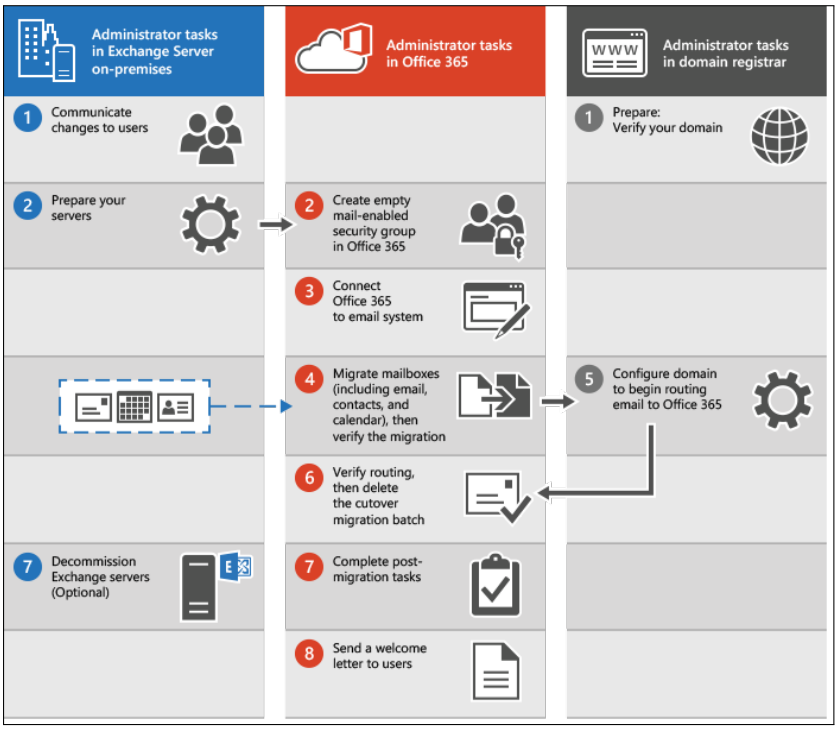
De ansatte i bedriften er i dag kjent med bruken av epost gjennom Outlook-applikasjonen installert på deres arbeidsstasjon. Inne i applikasjonen har de tilgang på epost, kalendere, kontakter med mer, heretter kalt mailbox. Den nye løsningen inkluderer programvare fra Office 365 pakken, som inkluderer nyeste versjon av Outlook. Dette innebærer at den nye løsningen ikke vil medføre nevneverdige endringer på interaksjonen mellom sluttbruker og deres mailbox. Exchange Online lar også brukere aksessere mailboxen sin via web-grensesnittet, noe som vil oppleves annerledes for de ansatte, men fortsatt fortrolig for de fleste.

Det er også viktig å understreke at migreringsprosessen ikke vil ha innvirkning på de ansattes mailbox. Dette betyr at alle eposter, kalendere, kontakter og oppgaver vil bli med til skyen og være tilgjengelig for de ansatte når de åpner Outlook. Målet er å gjøre overføringen så sømløs og umerkbar som overhodet mulig for de ansatte.

Migreringsprosessen

Migreringen fra Exchange til Exchange Online vil, som nevnt, være en prosess som de ansatte skal merke lite til. For å legge opp til dette har Microsoft utarbeidet flere ulike migreringsmetoder for ulike serveroppsett. På bakgrunn av bedriftens nåværende infrastruktur, vil Cutover-metoden være optimal. Denne metoden støtter opp til 2000 mailboxer, tjenere med Exchange 2003 og nyere, krever ikke hybridløsning og vil flytte alle brukerne på en gang. Løpet i migreringen er skissert i figur 2 vist under.

Når mailboxen er flyttet ut i skyen, og alle de ansatte har tilgang på den via Office 365, vil det ikke lengre være behov for den gamle Exchange-tjeneren. Den vil da anbefales sikkerhetskopiert før den kan stenges av. Etter dette kan alt av administrasjon utføres gjennom Office 365s administratorpanel i Azure.



Figur 2: Cutover Exchange

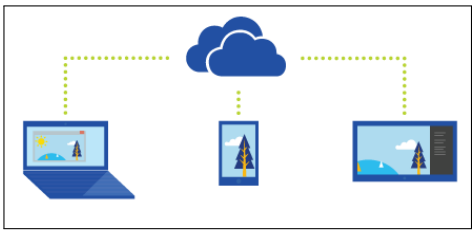
2.4.2 OneDrive

For å eliminere behovet for filtjenere lokalt vil prosjektet ta i bruk OneDrive og SharePoint. Office 365 følger med M365 og i Office 365 ligger både OneDrive for business og SharePoint Online. Disse tjenestene kan benyttes for å lagre ansattes filer og filer som flere i bedriften trenger tilgang til.

Filtjenere benyttes hos bedriften til å oppbevare hele bedriftens dokumentbibliotek. Dette gjelder både felles dokumenter for hele bedriften og dokumenter som bare enkelte grupper skal ha tilgang til. Mer personlige data og dokumenter for hver enkelt ansatt har de på sitt eget hjemmeområde. I den nye løsningen skal fellesfiler flyttes til SharePoint mens mer personlige filer flyttes til ansattes egne OneDrive-område.

Hjemmemapper og andre personlige data som ansatte har, kan flyttes ut i OneDrive for business. Ved å legge filene der vil de synkroniseres opp i skyen og være tilgjengelige på alle enhetene til den ansatte. Dette betyr at ansatte kan få tilgang på filene sine uavhengig av om de er på PC, mobil eller nettbrett. Hvis en ansatt skulle ønske å dele en fil med noen i bedriften, kan en gjøre dette. Da vil man selv bestemme om mottaker skal kunne redigere eller bare få se på filen. Dokumenter

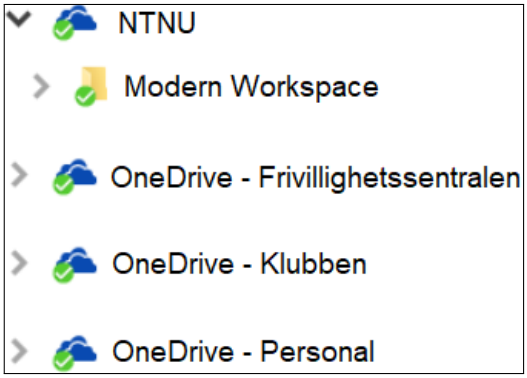
som ligger i OneDrive kan redigeres av flere samtidig, enten i Word Online eller i den lokale versjonen av Word.



Figur 3: OneDrive

Skylagring har blitt særdeles populært i de siste årene. Ved å tilby egen skylagring for de ansatte i bedriften vil bli kvitt problemer som skygge-IT ved at ansatte lagrer konfidensielle data hos andre usikre skyleverandører eller andre steder der de lett blir borte eller glemt. Når alle bruker samme tjeneste er det også lettere å skape en robust katalog med god sikkerhet og som er lett tilgjengelig for ansatte.

Med den nye OneDrive klienten kan man legge inn flere kontoer for personlig eller bedriftsbruk, og man kan også legge til SharePoint sider. Hvordan dette vil se ut for sluttbrukeren ser vi i figur 4.



Figur 4: Filutforsker med OneDrive

Migrering til bruk av OneDrive kan gjøres av IT-administrasjonen, men det anbefales at brukerne selv gjør dette for å lære å bruke programmet. Ved å la sluttbruker gjøre dette selv vil en få muligheten til å erfare hvordan det er å bruke OneDrive, samt gi en mestringsfølelse. Da vil det være lettere for andre sluttbrukere å hjelpe hverandre, i stedet for å måtte henvende seg til IT.

Hvis IT må ta for seg migreringen, vil det være mulig å tvinge OneDrive til å synkronisere innholdet i kjente mapper som Dokumenter, Skrivebord, Nedlastninger og Bilder. Dette gjøres med en «known-folder redirect» policy.[13] En alternativ måte for IT å utføre migreringen vil være ved hjelp av scripts.

2.4.3 SharePoint

SharePoint er en intranett-tjeneste i Office 365-pakken. SharePoint blir hos de fleste bedrifter brukt som en plattform for publisering av nyheter, HR- HMS- og annen deling av bedriftsinformasjon for hele organisasjonen. SharePoint brukes også til prosjektområder og avdelingsområder der dokumenter deles mellom interne og i noen tilfeller eksterne ansatte.[14]

Ved å flytte filer som flere i bedriften trenger tilgang til, ut til SharePoint Online, vil flere ha mulighet til å kunne åpne og redigere disse samtidig, avhengig av hvilke rettigheter de har til filene. Avdelinger eller teams kan opprette egne områder der andre avdelinger ikke har tilgang. Disse filområdene kan lett gjøres tilgjengelig i filutforskeren eller de kan nås gjennom nettleseren, uansett vil lokale endringer hos klienten synkroniseres til skyen. Hvis en ønsker å legge en SharePoint-side inn i filutforskeren benyttes OneDrive-klienten. I figur 4 vises en bruker som har lagt til en SharePoint-side med navnet NTNU - Modern Workspace.

På figur 5 kan vi se at det er dukket opp to tray-ikoner for OneDrive. På Windows maskiner vil den hvite skyen være for personlige OneDrive-kontoer og den blå være for business. På Mac vil bare den hvite være synlig og inneholde funksjonalitet for begge.

Figur 5: OneDrive tray-ikoner

Tidligere når en ansatt har ønsket å samarbeide eller dele et dokument med noen, så har de måttet sende dokumentet selv og så vente på å få det oppdaterte dokumentet sendt tilbake. Slik trafikk skaper mange versjoner av samme dokument og gjør det hele uoversiktlig. Både OneDrive og SharePoint, men spesielt SharePoint, har en meget god støtte for ulike versjoner av samme fil. Det finnes funksjonalitet for å se tilbake på hvordan filen så ut tidligere og mulighet for å reversere endringene slik at man kommer tilbake til en eldre utgave av dokumentet.

2.4.4 Teams

Microsoft Teams stiller som samarbeidsverktøyet vi ønsker å levere til bedriften. Teams er designet rundt bedrifter med ulike avdelinger og behov, dette slik at alle de ansatte har verktøyene de trenger for å få utført sine oppgaver. I sin kjerne er Teams et chatte- og ringeprogram med fokus på kommunikasjon mellom ansatte, men gjennom sin integrasjon med annen Office-programvare åpnes mange nye muligheter. Verdt å nevne er sanntids samarbeid i Word, Excel og PowerPoint, enkel fildeling mellom kollegaer, gruppemøter og forretningssamtaler. Sikkerheten i

Teams garanteres gjennom group-policies i M365, og vil holde den samme høye standarden som andre Microsoft 365 produkter.

Innføringen av Teams for bedriften vil foregå gjennom å sette opp rom for de ulike avdelingene innad i bedriften. For eksempel vil driftsavdelingen, HR-avdelingen og ledelsen kunne ha egne adskilte rom hvor de kan kommunisere seg imellom. Dette hindrer at alle de ansatte inkluderes i samtaler de verken har behov eller klarering for å se. Dette vil være viktig for å forhindre uoversiktlig kommunikasjon og, kanskje viktigere, at konfidensiell informasjon spres til gale ledd. Det settes derimot ingen restriksjoner mot medlemmer av HR-avdelingen fra å sende meldinger, ringe eller samarbeide med medlemmer av driftsavdelingen som eksempel.[15]

2.5 Enhetsregistrering

I det nye systemet vil administrering av enheter foregå via Microsoft Intune. For å kunne drive administrasjon av de ulike enhetene må de først registreres i Intune. Prosessen for registrering vil variere mellom de ulike operativsystemene og vil derfor forklares individuelt.

2.5.1 Autopilot

Nye maskiner med Windows 10 skal benytte Windows Autopilot for å registrere maskinen i Microsoft Intune, i Azure AD og, om ønskelig, i lokal Active Directory.

Det tidligere senarioet der SCCM tok seg av formatering av maskinen og installasjon av nytt OS-image skal fases ut. Med Windows Autopilot slipper man å formatere maskinen på forhånd og maskinen kan settes opp dynamisk ut ifra hvem som skal benytte den.

Windows Autopilot er samling teknologier fra Microsoft som benyttes for å sette opp og pre-konfigurere nye Windows 10 enheter. Hele systemet er bygd slik at enheten kan leveres direkte til sluttbruker og være klar til bruk på kort tid. Det hele skal skje uten at sluttbruker trenger å gjøre mer enn å autentisere seg med sin Azure ID og uten at IT-avdelingen behøver å håndtere den fysiske enheten.[16]

Windows Autopilot krever at bedriften benytter seg av Azure AD, noe infrastruktur utover dette er ikke påkrevd. Siden bedriften planlegger å beholde lokal AD, vil det være fordelaktig å la autopilot registrere maskinen der også.

Når prosessen er ferdig vil det være mulig å gjenopprette enheten eller nullstille den for overtakelse av annen ansatt. Ved å benytte denne løsningen trengs det ikke lengre å opprette og vedlikeholde sine egne Windows-image for ulike installasjoner og konfigurasjoner. Microsoft Autopilot skreddersyr et system basert på hvem som skal benytte enheten og hele prosessen foregår gjennom en OOBE.

Slik foregår prosessen med Microsoft Autopilot:[17]

1. Enheten registreres hos Autopilot.

   Informasjon om enheten registreres i Windows Autopilot systemet. Dette er informasjon som serienummer, Windows produkt-ID og maskinvare-hash.[18]

2. Det opprettes en egendefinert profil med konfigurasjoner.

   Opprettelse av konfigurasjonsprofil for Autopilot trengs bare å gjøres en gang, ved implementasjon. Hvis ulike maskiner trenger ulik konfigurasjon må det opprettes flere profiler. Uansett antall profiler som opprettes burde disse revideres omgående eller ved behov.

   Profilen vil inneholde regler for hvordan enheten skal konfigureres og hvilke brukervalg som skal tas. Her kan man blant annet velge å ikke ha noen lokal administrasjon på enheten.

3. Profilen tildeles enheten.

   Den samme profilen kan brukes til flere enheter. Enheten får her en profil tildelt før den har blitt skrudd på av sluttbruker.

4. Sluttbruker mottar enhet, kobler den til internett og logger inn.

5. Maskinen henter profilen og Autopilot starter konfigurasjonen.

   (a) Maskinen meldes til Intune.

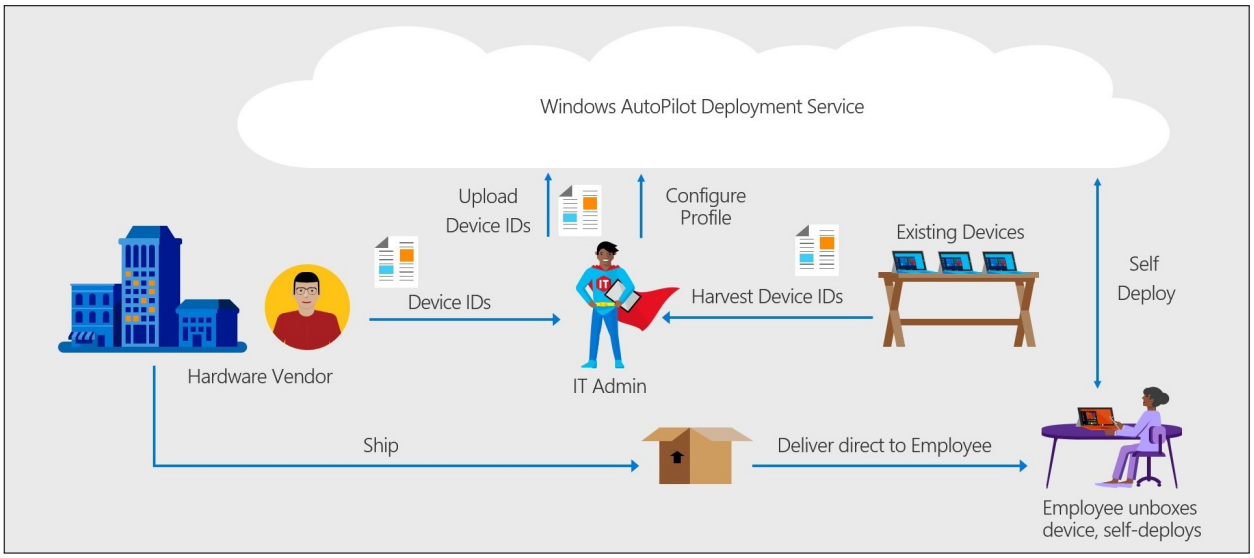
   (b) Maskinen meldes til AD og/eller AAD.[19]

      i Hvis maskinen skal meldes til AD må maskinen (Windows 10 1809) være tilkoblet bedriftsnettet og Intune Connector må være installert hos AD.

   (c) Intune og/eller Group Policy oppdaterer maskinens policies og innstillinger.

   (d) Intune installerer tvungen programvare.

6. Maskinen er klar til bruk.



Figur 6: Autopilot-prosessen

2.5.2 Apple Device Enrollment Program (DEP)

iOS-baserte enheter som leveres gjennom bedriften kan klargjøres ved hjelp av Apple DEP. Dette er kun mulig på helt nye enheter gjennom avtaler direkte med Apple. Når enheten er konfigurert opp imot Intune gjennom Apple DEP vil enheten, ved oppstart, spørre om en identitet (Azure AD Identity) og bli automatisk bli registrert i Intune. Allerede fra første oppstart blir enheten registrert i Intune, og applikasjoner, policies, profiler og sikkerhetsinnstillinger blir tilgjengelig for enheten.[20]

2.5.3 Microsoft Company Portal

For Android- og iOS-enheter som allerede er satt opp uten inngrep fra bedrifter, vil applikasjonen MS Company Portal brukes for registrering i Intune. Applikasjonen finnes i både AppStore for iOS og Google Play butikken for Android. Applikasjonen ber om innloggingsinformasjon og sjekker at identiteten finnes i bedriftens Azure AD. Når brukeren godkjennes blir enheten registrert og Intune begynner klientdrift av enheten. Alle applikasjoner, policies, profiler og sikkerhetsinnstillinger installeres på arbeidsflaten. [21]

2.6 Sikkerhet

Et høyt fokus på sikkerhet vil være viktig for bedriften og deres ansatte, særlig når de beveger bedriften til en skyløsning. Microsoft leverer flere ulike ledd i sikkerheten for å bygge en helhetlig sikkerhetsløsning, dette både på infrastruktur- og brukernivå. Noen av sikkerhetstiltakene vil påvirke enheten som sluttbruker benytter seg av, mens andre vil gå på applikasjonene som blir brukt.

Nedenfor listes sikkerhetsmekanismer som vil benyttes i løsningen. Hvilke regelsett, applikasjoner, dokumenter og hvilken grad av beskyttelse som skal beskyttes, vil være beskrevet mer i detalj i det kommende driftsdokumentet.

2.6.1 Windows Defender

Windows Defender er selve kjernen Microsoft bygger sikkerhet i sine applikasjoner, programvare og tjenester på. Defender kommer installert på alle enheter med Windows 10. Defender fungerer som et antivirus og søker gjennom maskinen for å finne virus, malware og andre trusler. Hvis Defender oppdager en trussel vil den settes i karantene og sluttbrukeren vil få opp et varsel om hva som er hendt. Ved falsk-positiv finnes det mulighet for å reversere tiltakene som Defender har gjort.

Defender varsler som standard direkte til sluttbrukeren, men ved å registrere enheten i Intune vil Defender også kunne kommunisere ut i skyen til Intune (ATA og Defender ATP). Der kan også Defender kunne styres sentralt. Oppdateringer og konfigurasjoner kan endres og klientens helsestatus vil være tilgjengelig i et sanntidsvindu.[22]

2.6.2 Device Guard

Device Guard er Windows 10s teknologi for å kontrollere en datamaskin på tilnærmet samme vis som med mobile enheter. Her kombineres programvare, maskinvare og fastvare for å sikre ansattes maskiner mot kernel-angrep og for å sette restriksjoner til hvilke applikasjoner som kan installeres og kjøres. Restriksjonene kan defineres av bedriften, som eksempel kan de tillate ansatte å laste ned visse filer, men hindre de fra å gjøre endringer på systemkritiske innstillinger. Dette gjør at enheter med Device Guard aktivert vil være herdet mot trusler som knyttes til uforsiktige ansatte og annen brukerfeil.[23]

2.6.3 (Kun E5) Windows Defender Advanced Threat Protection - ATP

Windows Defender ATP overvåker Windows 10 i sanntid. Tjenesten hjelper til med forebyggende sikkerhetstiltak, identifiserer innbrudd, bistår i etterforskningen av angrepsforsøk og anbefaler respons på sikkerhetstrusler.[24]

2.6.4 (Kun E5) Office 365 Advanced Threat Protection - OATP

OATP vil, på brukernivå, forsøke å finne malware og andre trusler i Sharepoint, Teams, OneDrive og Outlook. OATP klarer dette ved å analysere innholdet i dokumenter, eposter, vedlegg og lenker for trusler som malware og falskt innhold. Vanlige trusler som epost-spoofing og phisingforsøk vil oppdages og brukere hindres fra å bli lurt.[25]

2.6.5 Azure Advanced Threat Protection - AATP

Azure ATP er en plattform laget for å analysere nettverkstrafikk og advare mot angrepsforsøk og andre trusler. AATP bruker tidligere nettverkslogger samtidig som den analyserer normal trafikk fra brukere i nettverket, dette for å lære oppførselen til bedriftens brukere og andre enheter i nettverket. Gjennom kunstig intelligens og utnyttelse av Azure-skyens kraft, bygger AATP en omfattende profil på alle de individuelle aktørene i nettverket. Denne oversikten blir over lang tid mer utfyllende og virkelighetsnær. Med basis i dette kan anomalier og suspekt aktivitet oppdages umiddelbart, og bedriften får informasjonen de trenger for å ta nødvendige grep.

AATP leverer informasjon om trusler og uregelmessigheter gjennom et brukervennlig panel som fokuserer på å formidle informasjonen på en enkel og oversiktlig måte. Informasjonen vil fortelle deg hvem, hva, når og hvor, slik at man har full oversikt over den mulige trusselen, og kan ta grep ut ifra situasjonen.[26]

2.6.6 Azure Active Directory Privileged Identity Protection - PIM

Privileged Identity Management (PIM) er til for å hjelpe til med å administrere, kontrollere og overvåke tilgangen til viktige ressurser.[27] Dette er tilgang til ressurser i Azure AD eller ressurser i andre tjenester som Office 365 eller Intune.

PIM inneholder nyttige funksjoner for å tilordne tidsbegrenset tilgang med start- og slutt-dato, skru på varsling for når tilganger er aktivert, kreve godkjenning eller MFA for å aktivere tilganger og revisjonshistorikk av tilganger.

2.6.7 Azure Active Directory Identity Protection - AADIP

AADIP har to viktige sikkerhetsoppdrag. Den første er å beskytte alle identitetene uavhengig av hvilke tilganger eller rettigheter de har. Den andre er å proaktivt hindre at kompromitterte identiteter blir misbrukt.

For å oppdage kompromitterte identiteter benyttes AI og heuristikk. Sammen leter de etter uregelmessigheter og mistenkelige hendelser som indikerer om potensielt kompromitterte identiteter. Hvis noe skulle oppdages genereres en rapport og varsler. Dermed kan man undersøke hendelsen videre og se på anbefalingen til passende tiltak.

I tillegg til å overvåke og rapportere, kan det konfigureres automatiske responser. Slike policies kan oppdage et problem og automatisk utføre en handling når et spesifisert risikonivå er nådd.[28]

2.6.8 Cloud App Security

Cloud App Security er en kritisk del av Microsofts Cloud Security-stack. Det er en omfattende løsning som kan hjelpe bedriften å sikre sky-applikasjoner, samtidig som det gir kontroll gjennom forbedret synlighet av aktiviteter. Det bidrar også til å øke beskyttelsen av kritiske data på tvers av sky-applikasjoner.[29] Cloud App Security håndterer autentifikasjon imot sky-applikasjoner og komuniserer med Azure AD for å bekrefte identiteter, roller og rettigheter.

Cloud App Security integrasjon med Azure Information Protection gir et ekstra beskyttelsesnivå ved å automatisk kryptere filer.[30]

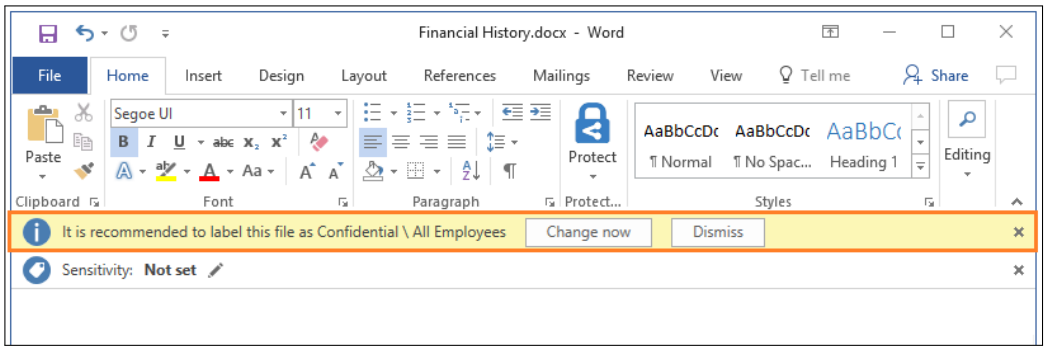
2.6.9 Azure Information Protection - AIP

Informasjon kommer i mange former og media, og noen data er mer hemmelig enn andre. Ofte er data som fødselsnummer, kredittkortnummer og regnskapsdata blant de dataene som trenger mest beskyttelse.

Azure Information Protection lar en klassifisere, merke og beskytte dokumenter og eposter. Klassifiseringene kan være personlig, konfidensiell, intern eller hemmelig. Det er mulig å gjøre dette automatisk ut ifra forhåndsdefinerte regler, manuelt av brukeren selv eller kombinere begge ved å la brukeren få anbefalinger.

Når Azure Information Protection krypterer filer, kan bare programmer som støtter Azure Information Protection vite hvordan du åpner filene. Alle Office 365 programmer støtter AIP. Data som er kryptert er også beskyttet i form av at de kan

spores etter de er delt for å se hvem som har sett på dem og hvor de har vært når de har gjort det.[31]



Figur 7: AIP klassifisering

I figur 7 kan man se at dokumentet anbefales klassifisert som konfidensielt, men er ikke klassifisert enda. Det er også kommet et hengelåsikon for å klassifisere dokumentet.[30]

2.6.10 Conditional Access

Conditional Access samarbeider med Azure AD om å gi muligheten til å begrense tilgang til bedriftens programmer basert på visse forhold. Slike betingelser kan bestemme over hvem (brukere eller gruppe), hva (cloud apps som Word, Outlook, etc.), hvor (steder og nettverk) og igjennom hvilken enhet man må være på for å få tilgang. Dermed kan man for eksempel kreve at maskinen er meldt inn i domenet, maskinen er på bedriftsnettet, maskinen har Windows 10 som OS og at MFA er aktivert.[32]

Sammen med dette får man loggført forsøk og økter i sanntid slik at de kan overvåkes og kontrolleres.

Basert på ulike betingelser kan man utføre handlinger som å blokkere nedlastninger, beskytte nedlastningen med kryptering og autentiseringskontroll, kreve MFA når man ikke er på bedriftsnettverket eller logger inn fra et ukjent system.

2.6.11 Mobile Application Management - MAM

Intune MAM er en pakke med administrasjonsfunksjoner i Intune. Funksjonene tar for seg publikasjon, konfigurasjon, sikring, overvåking og oppdateringer av

apper for brukerne. MAM er til for å beskytte bedriftens data som befinner seg inni en applikasjon. Dette blir gjort gjennom policies (App Protection Policy).

En policy kan være en regel som håndheves hvis brukeren forsøker å flytte bedriftsdata ifra en godkjent applikasjon til en ikke-godkjent applikasjon. Ved å benytte dette kan man fjerne muligheten for å kopiere tekst ifra Word og over i Notepad, eller lagre en kopi av filen på privat Dropbox. Slik kan man forhindre at data kommer på avveie, uavhengig om det er ond hensikt eller ærlig uhell.

Applikasjoner som man vil beskytte med MAM settes til managed. Applikasjoner som Word og OneDrive har ofte bedriftsinformasjon, og er gode eksempler på applikasjoner som bør settes til managed. Hvis det er ønskelig kan man kreve autentisering når en managed applikasjon åpnes, i form av en PIN-kode, passord eller annen MFA.

Slike MAM-policies vil fungere på alle enhetene i løsningen, altså Windows 10, iOS og Android.

Prosjektet kommer til å benytte MAM + Intune MDM, for enheter som er registrert i Intune. Dette åpner for muligheten med å fjerne all bedriftsdata på enhetene som er registrert i Intune, uten å berøre personlig data. Dette kan være ønskelig om enheter er blitt stjålet, på avveie eller ved avsluttet arbeidsforhold.[33]

2.7 Teknisk avgrensning

Vi vil her kort gå gjennom ulike tjenester som ikke implementeres i det nye systemet. Bakgrunnen for at disse ikke implementeres har grobunn i tidsrammene som settes og i relevansen de har til prosjektets mål.

Flere av tjenestene vil anbefales å innføre i et realistisk prosjekt, og vil kunne være nødvendig for å oppfylle krav fra mange bedrifter, men vil ikke være aktuelt å implementere disse i dette prosjektet.

2.7.1 Express Route

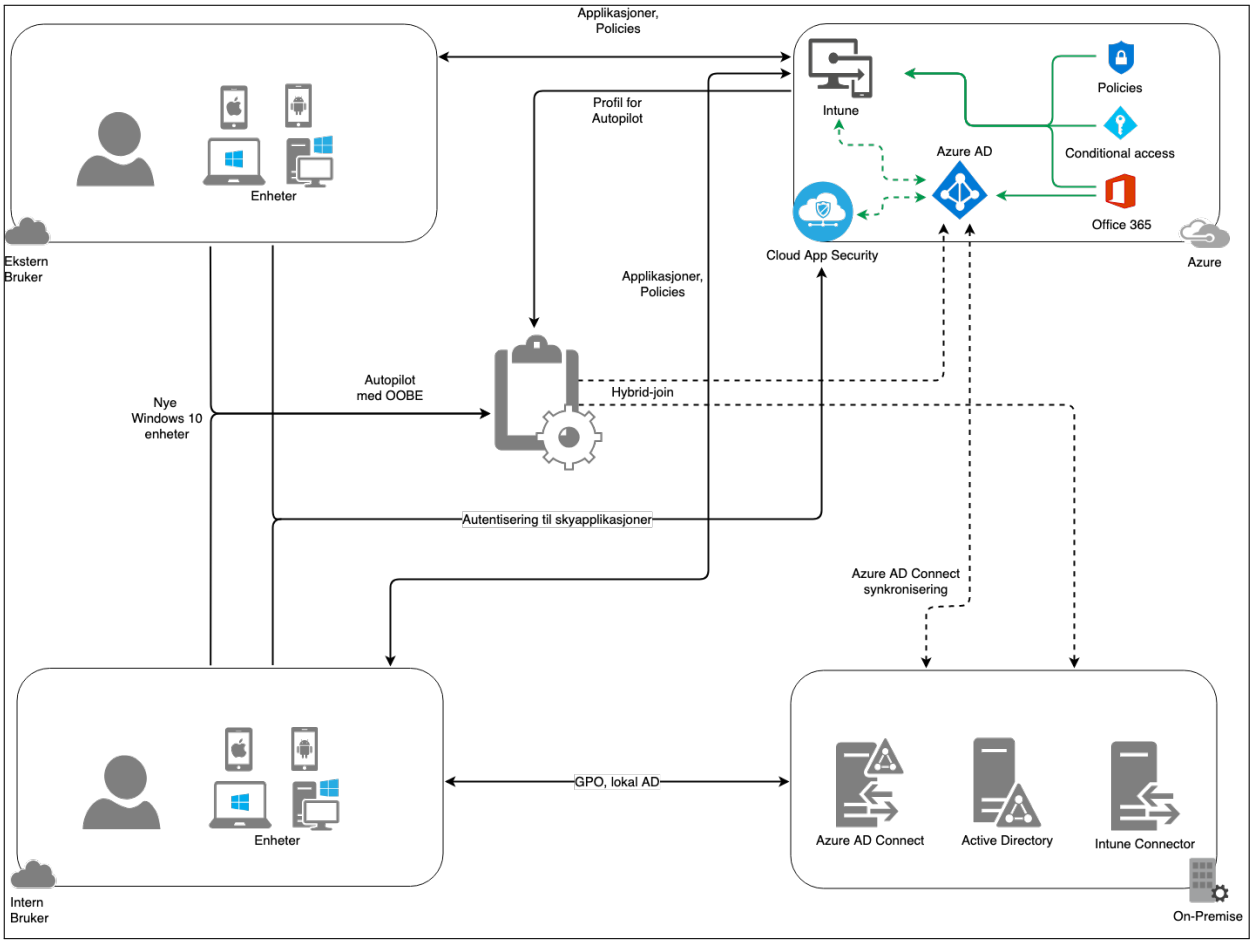
Med ExpressRoute opprettes det en privat tilkobling mellom Azure-datasentre og den lokale infrastrukturen i bedriften. En slik tilkobling unngår trafikk over det offentlige internett gjennom en dedikert kobling mellom bedriften, ISP og Azures datasenter. Med ExpressRoute vil hastighetene og påliteligheten være større, ventetid være redusert og sikkerhet være bedre enn tilkoblinger over det offentlige internett.[34]

2.7.2 Power BI Failover

Power BI er en tjeneste som Microsoft leverer for å sikre HA og hindre tap av data eller ressurser. Failover, som en del av Power BI, kan enkelt beskrives som at Azure har flere instanser av ditt Azure datasenter. Dersom ditt system ligger i Vest-Europa og Power BI er utilgjengelig i regionen, vil det automatisk starte en identisk instans i Nord-Europa som eksempel. Dette vil si at en synkronisert backup av alle komponenter startes i en ny region og din bedrift raskt får tilgang på sine ressurser.[35]

3 Detaljert løsningsbeskrivelse

På figur 8 er løsningen vist grafisk i sin helhet. Her er løsningen delt inn i fire bobler. De fire boblene representerer interne brukere, eksterne brukere, on-prem infrastruktur og infrastruktur i Azure.



Figur 8: Løsningsdiagram

Et av målene med prosjektet skal være å redusere behovet for on-prem infrastruktur. Den nye løsningen vil bestå av en Windows Server 2016 som kjører det lokale Active Directory. På denne tjeneren vil det også installeres programvare for Azure AD Connect og Intune Connector. Disse vil gjøre det mulig for den lokale tjeneren å kommunisere med tjenestene i Azure med samme navn.

Azure AD Connect knyttes til Azure AD og sørger for at identiteter synkroniseres mellom de to katalogtjenestene. Hvis Autopilot skal kunne registrere en ny maskin

i begge katalogtjenestene, AAD og AD, må Intune Connector være installert.

Lokale brukere er koblet på det lokale bedriftsnettverket, det samme nettverket som lokal AD er tilkoblet. Dermed kan Group Policy benyttes for å gi disse maskinene egne regler. Maskinene vil også ha tilgang til ressurser som bare finnes i lokal AD, som printere.

I Azure vil infrastrukturen bygges opp av Azure Active Directory, Intune, Office 365, sikkerhetsmekanismer og overvåkningsmekanismer. Dette innebærer alle tjenestene som befinner seg i Office 365 pakken slik som OneDrive, SharePoint og Teams. Både de eksterne og lokale brukerne vil kunne melde sine enheter inn i Intune. Gjennom Intune vil det dermed være mulig å sende ut både applikasjoner og policies til enhetene, uansett om de måtte være interne eller eksterne.

Hvis en bruker ønsker å benytte seg av en tjenestene som befinner seg i skyen må brukeren autentisere seg. Autentiseringen foregår gjennom Cloud App Security. Cloud App Security kommuniserer med Azure AD for å bekrefte roller, identiteter og rettigheter, og gjennom denne komminikasjonen kan Cloud App Security autentisere brukere imot sky-applikasjoner.

For nye Windows 10 enheter skal det benyttes Autopilot for å sette de opp med riktige innstillinger, policies og programvare. De skal bli meldt inn i både det lokale AD og i Azure AD. Dette kalles hybrid-join og krever at maskinen er koblet til bedriftsnettverket ved første oppstart. Før maskinen startes må den registreres og få tilegnet en Autopilot-profil, begge utføres i Intune.

4 Begrensninger

Tjenestene som følger med i Office 365 har standard-verdier satt og øvre grenser for deler av tjenestene de skal levere. I tabell 2 finner vi en oversikt over noen av de mest essensielle faktorene det er verdt å kjenne til. Dette er på ingen måte en fullverdig tabell, da den kun inneholder høyst relevant informasjon. Microsoft tilbyr en svært detaljert oversikt på sine nettsider, som en kan besøke ved behov.[36, 37, 38]

Tabell 2: Begrensninger

Beskrivelse	Grense	Kommentar
Exchange Online		
Maks postboks størrelse	50 GB	E3 og E5 lisenser
Maks meldinger i postboks	1 000 000	
Maks størrelse på melding	150 MB	Inkluderer vedlegg og gjelder for inboud, outbound og internal
Maks størrelse på vedlegg	150 MB	
Maks lengde på emne	255 tegn	
Maks antall mottakere av melding	500 stk	Gjelder for mottaker, kopi og blindkopi
Bevaringstid på slettede elementer	Ingen grense	
Bevaringstid på elementer slettet fra “Deleted Items” mappen	30 dager	14 dager er satt som standard
OneDrive for Business		
Maks filstørrelse	15 GB	
Maks lengde på filnavn	260 tegn	I praksis vil maks være 256 tegn
Maks antall elementer som kan synkroniseres per bibliotek	30 000 000	Ytelsesproblemer kan oppstå når antallet overskriver 300 000
Maks størrelse for å generere miniatyrbilder	100 MB	Miniatyrbilde vil ikke genereres for bilder som overskrider grensen
Maks størrelse for å generere forhåndsvisninger	100 MB	Forhåndsvisning vil ikke være tilgjengelig for pdf-filer som overskrider grensen

Fortsetter på neste side

Tabell 2 – fortsettelse ifra forrige side

Dato	Ver.	Beskrivelse
SharePoint Online		
Maks filstørrelse	15 GB	
Maks gruppestørrelse	5 000 stk	
Maks antall grupper en bruker kan være med i	5 000 stk	
Maks antall grupper	10 000 stk	
Maks antall elementer som kan synkroniseres per bibliotek	30 000 000	Ytelsesproblemer kan oppstå når antallet overskriver 300 000

*Det sendes ut varsler fra systemet før disse grensene er nådd.

*Disse verdiene er innhentet og oppdatert per 14.02.2019. De kan uten forvarsel bli endret av Microsoft i fremtiden.

5 Veien videre

Prosjektets bakgrunn har vi sett er sammensatt, men den nye strategien med cloud first står sterkt. Ved å velge denne løsningen vil bedriften sitte igjen med en betydelig reduksjon av den lokale serverparken. Løsningen går ut på å bare sitte igjen med én on-prem server og hele den resterende infrastrukturen vil befinne seg i skyen, som strategien tilsier.

Azure forplikter seg til at infrastruktur hos dem vil ha en oppetid på 99,9%. Ved å samle så mye infrastruktur som mulig hos Azure vil dette bli en kjerne som lett kan administreres, alt på ett sted. Den nye løsningen har også flere prosesser som kan automatiseres gjennom Intune, prosesser som enhetsregistrering med oppsett og konto suspensjon ved mistanke om misbruk.

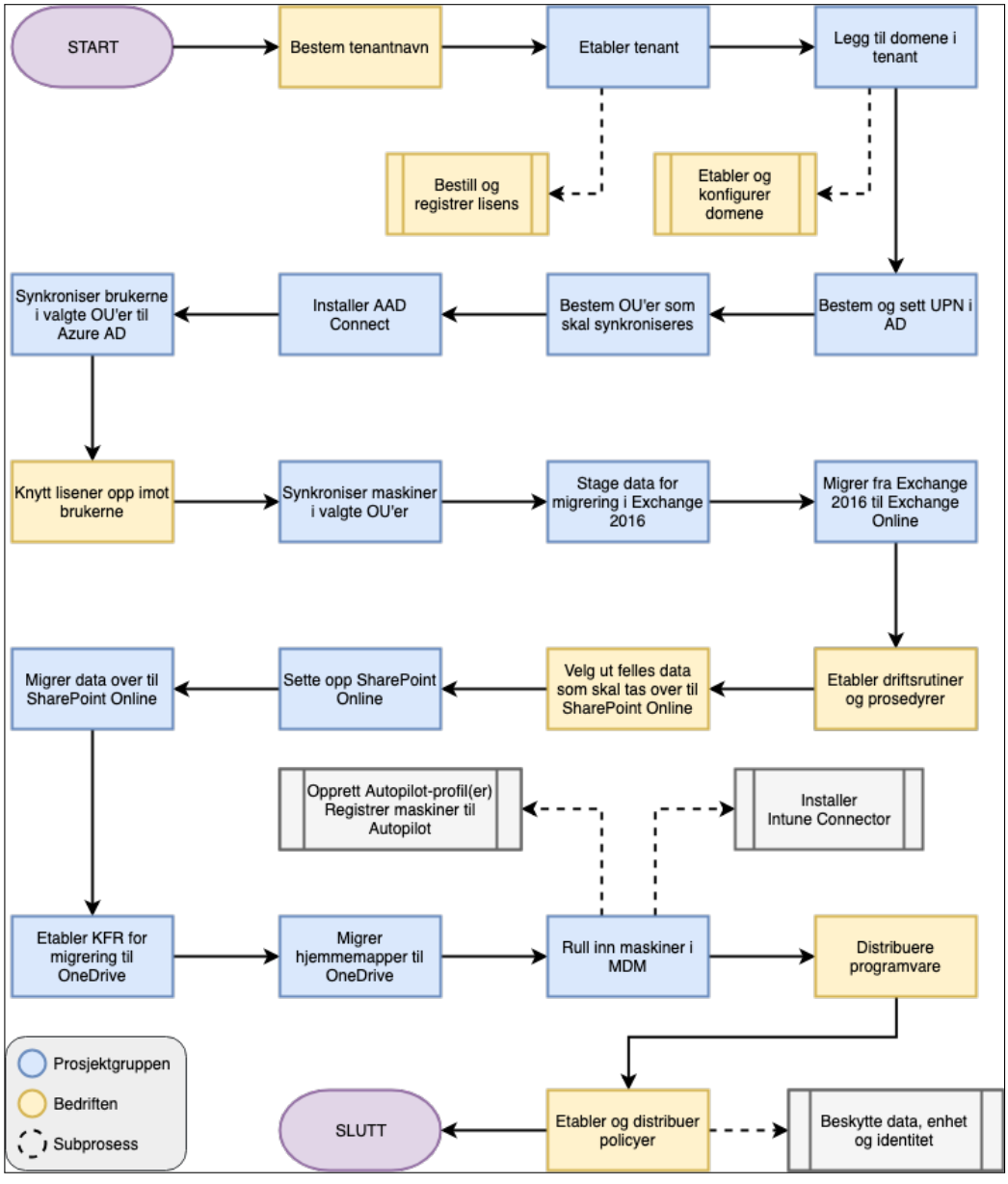
Ved at ansatte oppfordres til og tar i bruk OneDrive og SharePoint vil dette kunne føre til at skygge-IT reduseres betraktelig.

Denne løsningen i skyen vil dessuten gjøre tjenestene og data tilgjengelig uansett lokasjon, slik at ansatte kan jobbe på egne enheter utenfor bedriftens lokalnett. Dette uten at bedriften trenger å bekymre seg for at bedriftsdata kommer på avveie.

Løsningen som presenteres vil bli en betydelig modernisering av den nåværende arbeidsflaten. Programvaren ansatte interagerer med vil være oppdatert og brukerorientert, slik at fornying oppfattes positivt og dermed moderne. Verktøyene for drift vil også oppleve en lignende modernisering, og se at oppgaver forenkles og kan automatiseres gjennom det nye systemet.

5.1 Flytdiagram

For oppsettet og migreringen av den nye løsningen er det utarbeidet et flytdiagram for prosessen. Her er det satt opp prosesser med subprosesser. Flytdiagrammet er vist i figur 9.



Figur 9: Flytdiagram

Ordforklaringer

Tabell 3: Ordforklaringer

Ord	Forklaring
AAD	Azure Active Directory. Skybasert katalogtjeneste levert av Microsoft.
AADIP	Azure Active Directory Identity Protection. Sikkerhetsfunksjon i Azure Active Directory.
AATP	Azure Advanced Threat Protection. Sikkerhetsfunksjon som utnytter skyen.
AD	Active Directory er en katalogtjeneste for Windows-domener levert av Microsoft.
AI	Artificial Intelligence. Forkortelse for kunstig intelligens.
AID	Azure Identity Protection. Sikkerhetsinnstilling for beskyttelse av identieter.
AIP	Azure Information Protection. Sikkerhetsfuksjon i Azure.
ATP	Advanced Threat Protection. Sikkerhetsfunksjon i Windows Defender.
Azure (cloud)	Skyløsning levert av Microsoft.[39]
Azure ID	Måten brukere identifiserer seg gjennom skyen, en kombinasjon av e-postadresse og passord.
BYOD	Bring your own device er en policy som tillater ansatte å bruke personlige maskiner på jobb og lar disse få tilgang på bedriftens arbeidsverktøy og informasjon.
DEP	Device Enrollment Program. Apples metode for klargjøring av bedriftsenheter.
Exchange	Mailtjenerprogramvare. Installeres på Windows Server maskiner. Levert av Microsoft.
ExpressRoute	En direkte og privat kobling mellom infrastruktur og Azure skyen.
HA	High Availability. Høy oppetid på tjenester. Altså at de er tilgjengelig til enhver tid.
Heuristikk	Forsøk på å finne den beste og raskeste måten å løse problemer.
HTTPS	Hypertext Transfer Protocol Secure. Sikkerhetsorientert versjon av kommunikasjonsprotokollen til internett.

Fortsetter på neste side

Tabell 3 – fortsettelse ifra forrige side

Ord	Forklaring
Image	System Image. En fil som inneholder en kopi av et operativsystem. Brukes for å starte installasjonen av OS under første oppstart eller ved reinstallasjon.
In-house	At en bedrift bruker egne ressurser/ansatte framfor innkjøp av eksterne.
Intranett	Internt nettverk for en bedrift, hvor kun ansatte har tilgang.
Intune	Administrasjonsverktøy for datamaskiner og mobile enheter.
ISP	Internet Service Provider. En internettleverandør som for eksempel Telenor og Get.
Kernel	Viktig del av operativsystemet som virker som en kobling mellom maskinvaren og applikasjoner.
KFR	Know-Folder-Redirect. Synkronisering av lokale fil-mapper til OneDrive.
M365 E	Microsoft 365 Enterprise er programvareabonnement for arbeidshverdagen levert av Microsoft. Abonnementet inkluderer blant annet operativsystem til datamaskiner, samarbeidsverktøy, produktivitetsverktøy, sikkerhetsverktøy og administrasjonsverktøy. Det kommer i to varianter E3 og E5. Der E5 er den mest omfattende varianten, med de nyeste og mest avanserte verktøyene for sikkerhet, samarbeid og beskyttelse mot trusler. (advanced threat protection, security and collaboration tools)[40]
Mailbox	Alt av innhold koblet til en epostadresse. Kan inkludere eposter, kalender, kontakter med mer.
Maleware	Skadelig programvare. Eksempler på slike er trojanere, virus og ransomware
MAM	Mobile Application Management. Pakke med administrasjonsfunksjoner i Intune.
Maskinvare-hash	Attributter som lar deg identifisere en enhet. For eksempel serienummer, produsent, modellnummer med mer.
MDM	Mobile Device Management. Administrasjon av mobile enheter.
MFA	Flerfaktorautentisering (Multi-factor authentication) er en metode for tilgangskontroll hvor en bruker må oppgi flere separate bevis for sin identitet. Ofte brukes noe en vet, noe en har og/eller noe man er. Hvis bevisene godkjennes gis det adgang.

Fortsetter på neste side

Tabell 3 – fortsettelse ifra forrige side

Ord	Forklaring
OATP	Office 365 Advanced Threat Protection. Sikkerhetsfunksjon i Office 365.
Office 365	Programvareabonnement for arbeidsverktøy som Word, Excel osv. Leveres av Microsoft
On-Prem	On-premise er når infrastruktur står i bedriftens lokaler.
OOBE	Forkortelse for "out of the box experience". Førsteinntrykket og opplevelsen en bruker har når en tar i bruk et produkt for første gang.
OS	Forkortelse for operativsystem. Eksempler på slike er Windows 10 og macOS.
OU	Organistational Unit. Brukes til organisering av grupper med brukere. Brukes for eksempel til å skille mellom avdelinger i en bedrift.
Passord-hash	Unik verdi som lar systemer identifisere en brukers passord uten at passordet lagres i klartekst.
Password Writeback	Valgbar funksjon som synkroniserer passordendringer i Azure AD ned til lokal AD.
PIM	Privileged Identity Manament. Sikkerhetsfunksjon i Azure Active Directory.
Power BI	Tjeneste levert av Microsoft for Azure-instanser. Forsøker å sikre høy oppetid.
SCCM	System Center Configuration Manager er programvare for administrasjon av grupper av datamaskiner som kjører samme eller ulikt operativsystem levert av Microsoft.
Seamless SSO	Seamless Single Sign-On. Påloggingsmetodikk med fokus på brukervennlighet.
SharePoint	Web-basert samarbeidsplattform som integrerer med Office-programmer som Word, Excel osv. Leveres av Microsoft.
Skygge-IT	Beskriver systemer og filer IT-ansvarlige i en bedrift ikke kan gjøre rede for. Eksempler på dette vil være bedriftsdokumenter lagret i en personlig Dropbox eller på en ekstern harddisk ikke eid av bedriften. IT-ansvarlige vil ikke kunne holde oversikt over, endre, slette eller på annet vis administrere slike dokumenter.

Fortsetter på neste side

Tabell 3 – fortsettelse ifra forrige side

Ord	Forklaring
Teams	Samarbeidsverktøy som integrerer chat, møter, notatskriving og deling av filer i en og samme programvare. Leveres av Microsoft.
Tenantnavn	Navnet på Azureidentiteten til din bedrift.
TLS	Forkortelse for Transport Layer Security. Krypteringsprotokoll for sikring av dataoverføring mellom enheter.
UPN	User Principal Name, innloggingsnavnet til et domene. For eksempel bruker@domene.no.

Referanser

[1] Microsoft. *[MS-MDM]: Mobile Device Management Protocol*. 2019. URL: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-mdm/33769a92-ac31-47ef-ae7b-dc8501f7104f (sjekket 21.02.2019).

[2] Statcounter. *Mobile Operating System Market Share Norway*. 2019. URL: http://gs.statcounter.com/os-market-share/mobile/norway (sjekket 18.02.2019).

[3] Microsoft. *Enroll iOS devices in Intune*. 2018. URL: https://docs.microsoft.com/en-us/intune/ios-enroll (sjekket 21.02.2019).

[4] Microsoft. *Enroll your Android device in Intune*. 2017. URL: https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android (sjekket 21.02.2019).

[5] Microsoft. *What is Azure Active Directory?* 2018. URL: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis (sjekket 18.02.2019).

[6] Microsoft. *What is Azure AD Connect?* 2019. URL: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect (sjekket 18.02.2019).

[7] Microsoft. *What is password writeback?* 2019. URL: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback (sjekket 21.02.2019).

[8] Microsoft. *Integrate on-premises Active Directory domains with Azure Active Directory*. 2016. URL: https://docs.microsoft.com/nb-no/azure/architecture/reference-architectures/identity/azure-ad (sjekket 21.02.2019).

[9] Microsoft. *Azure Active Directory Seamless Single Sign-On*. 2018. URL: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso (sjekket 18.02.2019).

[10] Microsoft. *What is Microsoft Intune?* 2018. URL: https://docs.microsoft.com/nb-no/intune/what-is-intune (sjekket 18.02.2019).

[11] Microsoft. *Import Configuration Manager data to Microsoft Intune*. 2017. URL: https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/migrate-import-data (sjekket 18.02.2019).

[12] Microsoft. *Hva er Office 365?* 2019. URL: https://www.office.com/ (sjekket 21.02.2019).

[13] Stephen Rose. *Migrate Your Files to OneDrive Easily with Known Folder Move*. 2018. URL: https://techcommunity.microsoft.com/t5/

Microsoft-OneDrive-Blog/Migrate-Your-Files-to-OneDrive-Easily-with-Known-Folder-Move/ba-p/207076 (sjekket 18.02.2019).

[14] Microsoft. *What is SharePoint?* 2019. URL: https://support.office.com/en-us/article/what-is-sharepoint-97b915e6-651b-43b2-827d-fb25777f446f (sjekket 18.02.2019).

[15] Tom Warren. *Microsoft Teams launches to take on Slack in the workplace*. 2016. URL: https://www.theverge.com/2016/11/2/13497992/microsoft-teams-slack-competitor-features (sjekket 18.02.2019).

[16] Microsoft. *Overview of Windows Autopilot*. 2019. URL: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot (sjekket 18.02.2019).

[17] Microsoft. *Configure Autopilot deployment*. 2019. URL: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/configure-autopilot (sjekket 22.02.2019).

[18] Microsoft. *Adding devices to Windows Autopilot - Device Identification*. 2019. URL: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/add-devices#device-identification (sjekket 22.02.2019).

[19] Microsoft. *Deploy hybrid Azure AD-joined devices by using Intune and Windows Autopilot (Preview)*. 2018. URL: https://docs.microsoft.com/nb-no/intune/windows-autopilot-hybrid (sjekket 18.02.2019).

[20] Microsoft. *Automatically enroll iOS devices with Apple's Device Enrollment Program*. 2018. URL: https://docs.microsoft.com/en-us/intune/device-enrollment-program-enroll-ios (sjekket 18.02.2019).

[21] Microsoft. *Use managed devices to access work or school resources*. 2019. URL: https://docs.microsoft.com/en-us/intune-user-help/use-managed-devices-to-get-work-done (sjekket 21.02.2019).

[22] Microsoft. *Enforce compliance for Windows Defender ATP with conditional access in Intune*. 2019. URL: https://docs.microsoft.com/en-us/intune/advanced-threat-protection (sjekket 18.02.2019).

[23] Microsoft. *Device Guard: Windows Defender Application Control and virtualization-based protection of code integrity*. 2018. URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control (sjekket 18.02.2019).

[24] Microsoft. *Windows Defender Advanced Threat Protection*. 2018. URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection (sjekket 18.02.2019).

[25] Microsoft. *Office 365 Advanced Threat Protection*. 2019. URL: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-atp (sjekket 18.02.2019).

[26] Microsoft. *What is Azure Advanced Threat Protection?* 2019. URL: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/what-is-atp (sjekket 18.02.2019).

[27] Microsoft. *What is Azure AD Privileged Identity Management?* 2019. URL: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure (sjekket 18.02.2019).

[28] Microsoft. *What is Azure Active Directory Identity Protection?* 2019. URL: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview (sjekket 18.02.2019).

[29] Microsoft. *Microsoft Cloud App Security overview*. 2019. URL: https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security (sjekket 21.02.2019).

[30] Microsoft. *Tutorial: Automatically apply Azure Information Protection classification labels*. 2019. URL: https://docs.microsoft.com/en-us/cloud-app-security/use-case-information-protection (sjekket 21.02.2019).

[31] Microsoft. *What is Azure Information Protection?* 2019. URL: https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection (sjekket 18.02.2019).

[32] Microsoft. *What is conditional access in Azure Active Directory?* 2019. URL: https://docs.microsoft.com/nb-no/azure/active-directory/conditional-access/overview (sjekket 18.02.2019).

[33] Microsoft. *Frequently asked questions about MAM and app protection*. 2018. URL: https://docs.microsoft.com/en-us/intune/mam-faq (sjekket 18.02.2019).

[34] Microsoft. *ExpressRoute overview*. 2018. URL: https://docs.microsoft.com/nb-no/azure/expressroute/expressroute-introduction (sjekket 21.02.2019).

[35] Microsoft. *What is a Power BI failover?* 2018. URL: https://docs.microsoft.com/en-us/power-bi/service-admin-failover#what-is-a-power-bi-failover (sjekket 21.02.2019).

[36] Microsoft. *Exchange Online Limits*. 2018. URL: https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits (sjekket 14.02.2019).

[37] Microsoft. *Invalid file names and file types in OneDrive, OneDrive for Business, and SharePoint*. 2018. URL: https://support.office.com/en-us/article/invalid-file-names-and-file-types-in-onedrive-

onedrive-for-business-and-sharepoint-64883a5d-228e-48f5-b3d2-eb39e07630fa (sjekket 14.02.2019).

[38] Microsoft. *SharePoint Online Limits*. 2019. URL: https://docs.microsoft.com/en-us/office365/servicedescriptions/sharepoint-online-service-description/sharepoint-online-limits (sjekket 14.02.2019).

[39] Microsoft. *Din visjon. Din sky.* 2019. URL: https://azure.microsoft.com/nb-no/ (sjekket 13.02.2019).

[40] Microsoft. *Discover the Microsoft 365 Enterprise solution that's right for you*. 2018. URL: https://www.microsoft.com/en-us/microsoft-365/compare-all-microsoft-365-plans (sjekket 13.02.2019).

Modern Workspace - Driftsdokument Førstegangsoppsett

v.0.6

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
22.03.2019	0.1	Opprettet dokument. Introduksjon skrevet, opprette tenant skrevet, opprette ny global administrator skrevet, førstegangsoppsett skrevet, administrasjon av tenant skrevet, figurer lagt til
29.03.2019	0.2	Revidert tekst, figurer lagt til, figurer oppdatert, innholdsfortegnelse oppdatert
18.04.2019	0.3	Mindre revisjon av tekst, små endringer i oppsett
19.04.2019	0.4	Revidert tekst i store deler av dokumentet, introduksjon omskrevet
25.04.2019	0.5	Revidert tekst for Opprette tenant, Førstegangsoppsett, Administrasjon av tenant
07.05.2019	0.6	Mindre revisjon av tekst, retting av grammatiske og språklige feil

Innhold

1 Introduksjon

I dette dokumentet vil vi gå gjennom de første stegene som må, eller bør, tas når en begynner sitt oppsett av en Azure-tenant. Vi vil først se på oppsettet av tenant, noe som kreves før en kan påbegynne noen form for konfigurasjon. Videre vil vi gå gjennom opprettelse av globale administratorer og hvordan gi de lisenser.

Dokumentet vil så gå gjennom førstegangsoppsett i Office-portalen, noe som er valgfritt, men anbefalt for å sette grunnregler knyttet til enheter og applikasjoner. Vi avslutter med å forklare hvilke kanaler som benyttes til administrasjon av vår nylagde tenant.

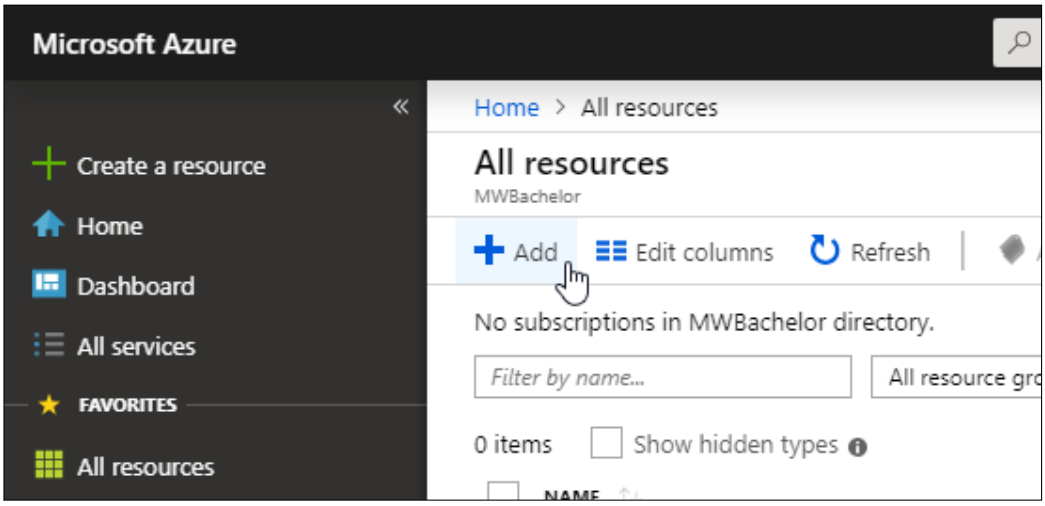
En tenant er en instans i Azure AD som representerer bedriften i sin helhet. Den inneholder og tillater verktøy for administrasjon av brukere, deres enheter og lisenser, applikasjoner og sikkerhet. Dette gjør at en bedrift kan skreddersy sin tenant til IT-behovene de har, slik at ansatte får tilgang på verktøyene de krever i sin arbeidshverdag, bedriftens data er sikker og tilgjengelig og ledelsen har full oversikt over systemet og deres ansatte.

Dokumentet vil gå ut ifra at leser har en viss teknisk kunnskap, og vil ikke nødvendigvis være enkelt for ufaglærte å forstå.

2 Opprette tenant

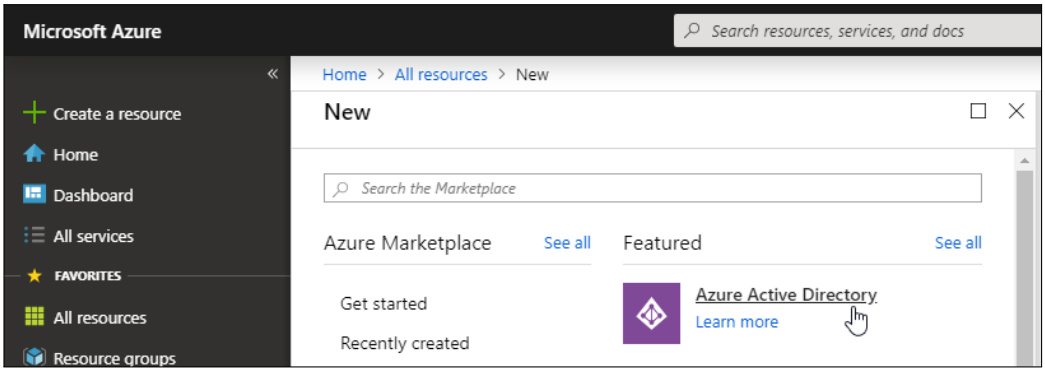
For å kunne gjenspeile bedriften digitalt, må først en tenant oprettes for bedriften. Denne vil inneholde domenet, grupper, brukere, lisenser og alle ressursene som kreves for å administere bedriftens IT-tjenester.

Første steg for å opprette en tenant vil være å logge inn i Azure-portalen og velge "All resources". Her må vi opprette en ny ressurs, noe som gjøres ved å klikke "Add".



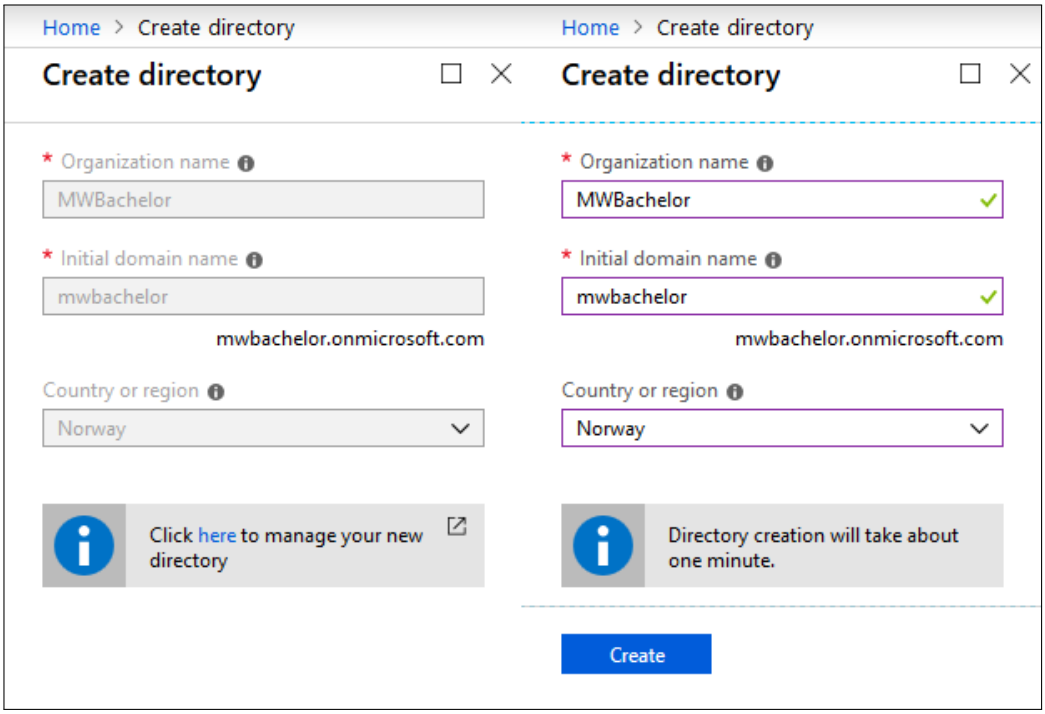
Figur 1: Ny ressurs i Azure

Her kan man søke eller lete etter ressurser under forskjellige kategorier. Under identitet kategorien finner vi den ønskede ressurser, "Azure Active Directory". Velg denne ved å klikke på den.



Figur 2: Velg Azure Active Directory

Organisasjonens navn, ønsket førstegangs-domene og region må oppgis. Trykk så "Create" for å begynne oppretting av tenant. Det vil ta en liten stund før du får mulighet til å administere den nye tenanten, noe som vises gjennom en melding, som vi ser i figur 3. Tenanten er opprettet, og er nå klar til administering.



Figur 3: Valg ved opprettelse av AAD

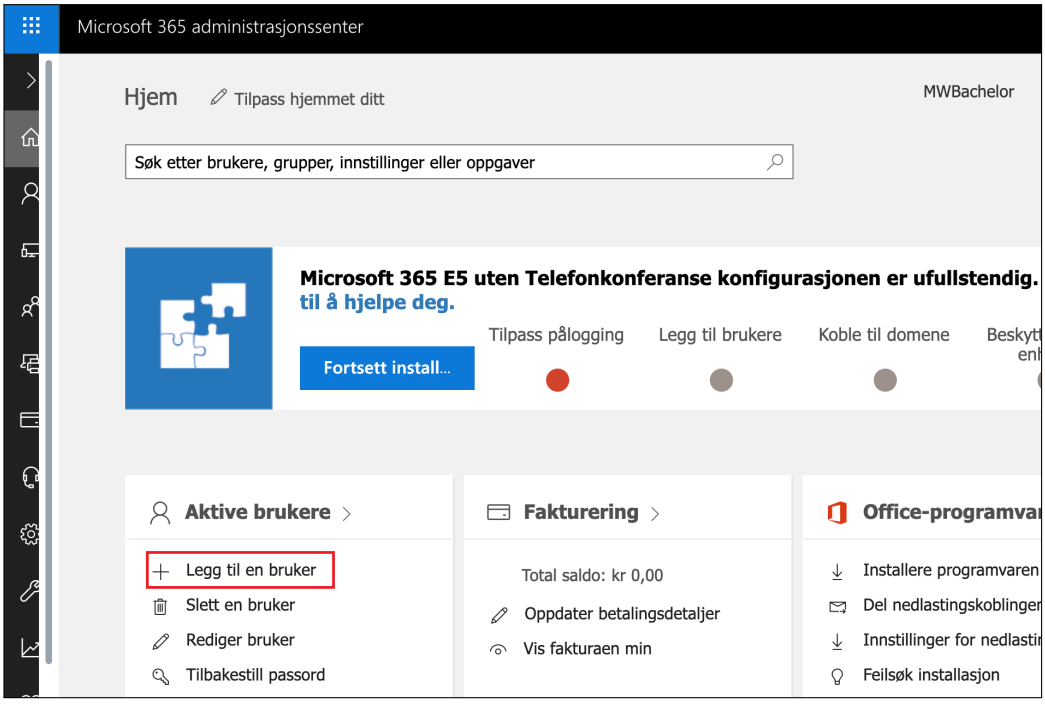
2.1 Begrensninger

Tenant-navnet må bestå av alfanumeriske tegn, spesialtegn er ikke tillat og navnet kan ikke være lengre enn 256 tegn.

3 Opprette global administrator

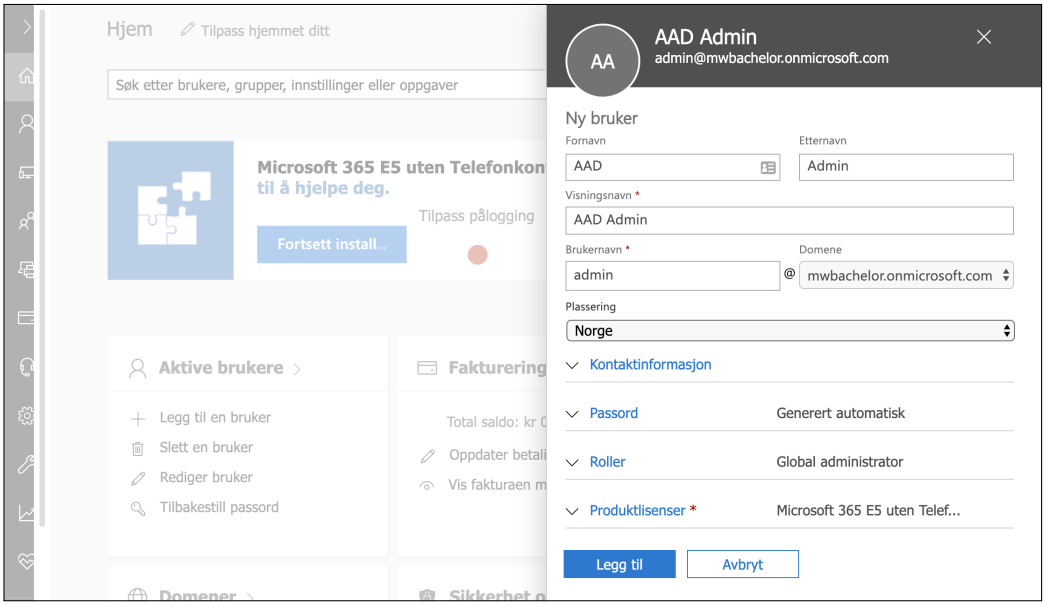
For å kunne administrere tenant via ulike portaler, bør en global administratorbruker opprettes. Denne vil ikke ha de samme restriksjonene som en microsoft-konto utenfor tenant og har fulle rettigheter.

Første steg vil være å trykke på "Legg til bruker" inne i Office-portalen. Denne knappen vil være lokalisert på startsiden, noe vi kan se i figur 4.



Figur 4: Opprett ny bruker

Brukeren får visningsnavnet “AAD Admin” og brukernavnet “admin”. Passord genereres automatisk og må skiftes ved første innlogging. Brukeren får rollen “Global administrator” og blir tilegnet en MS365 E5 lisens.

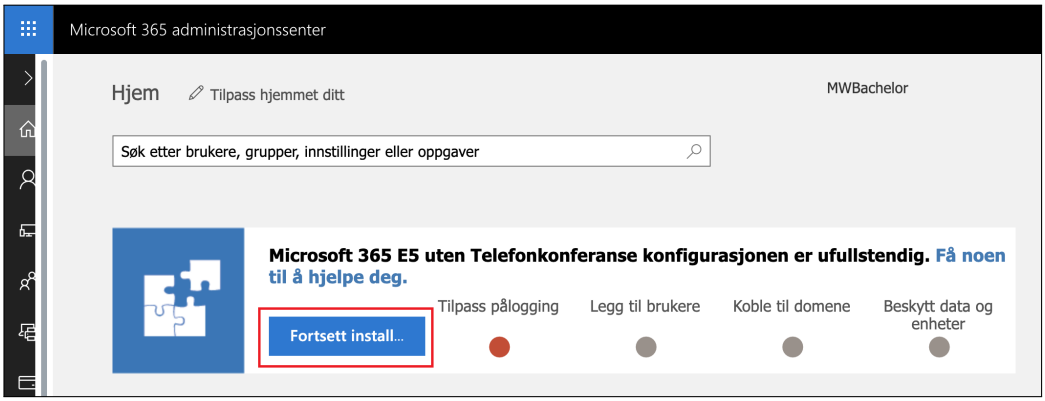


Figur 5: Brukerdetaljer

4 Førstegangsoppsett

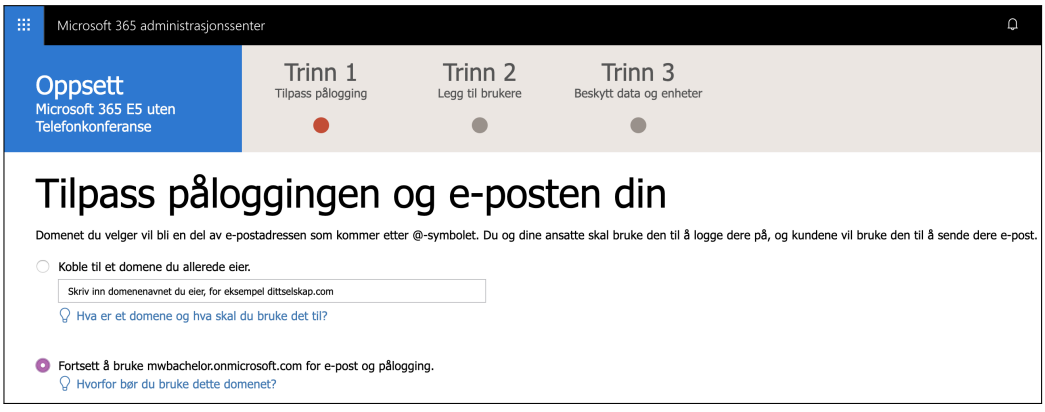
Oppsett i Office-portalen er noe som anbefales alle bedrifter å gjøre, da dette er en enkel veiviser som lar en administrere mange ulike innstillinger tilknyttet Office-programmer, epost, enheter og lisenser.

Første steg for å gjennomføre førstegangsopsett vil være å åpne startsiden til Office-potalen. Her vil det være en beskjed om at Microsoft 365 konfigurasjonen er ufullstendig, som vist i figur 6. Trykk her "Fortsett installasjon".



Figur 6

Dersom bedriften har et eget domene kan dette fylles inn her. Dette kreves ikke, og velger en å fortsette uten eget domene får man et "onmicrosoft"-domene. Dette kan også endres senere, dersom bedriften ønsker et eget domene. Som vi ser i figur 7, velger vi å fortsette å bruke onmicrosoft-domenet.

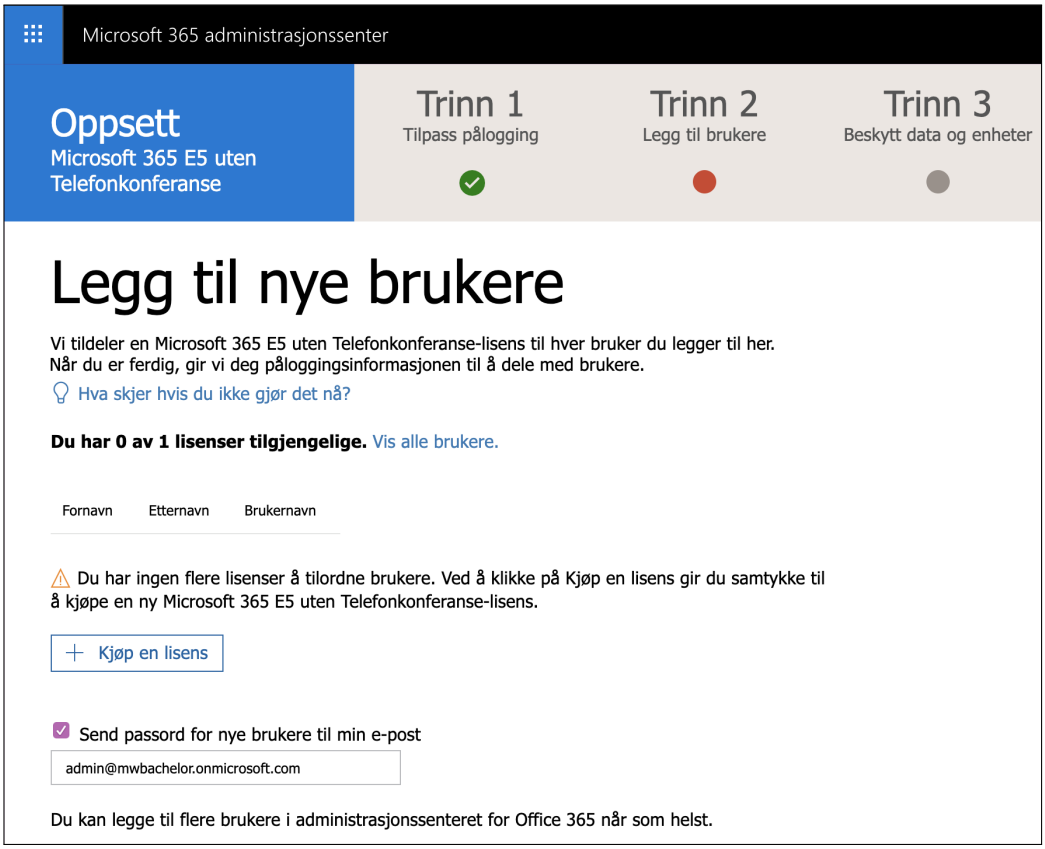


Figur 7

Du vil så få muligheten til å overføre e-postene til de ansatte over i deres nye postbokser. Denne overføringen kan gjøres på et senere tidspunkt dersom bedriften ønsker dette. Vi fortsetter uten å overføre e-postmeldinger, som vist i figur 8.

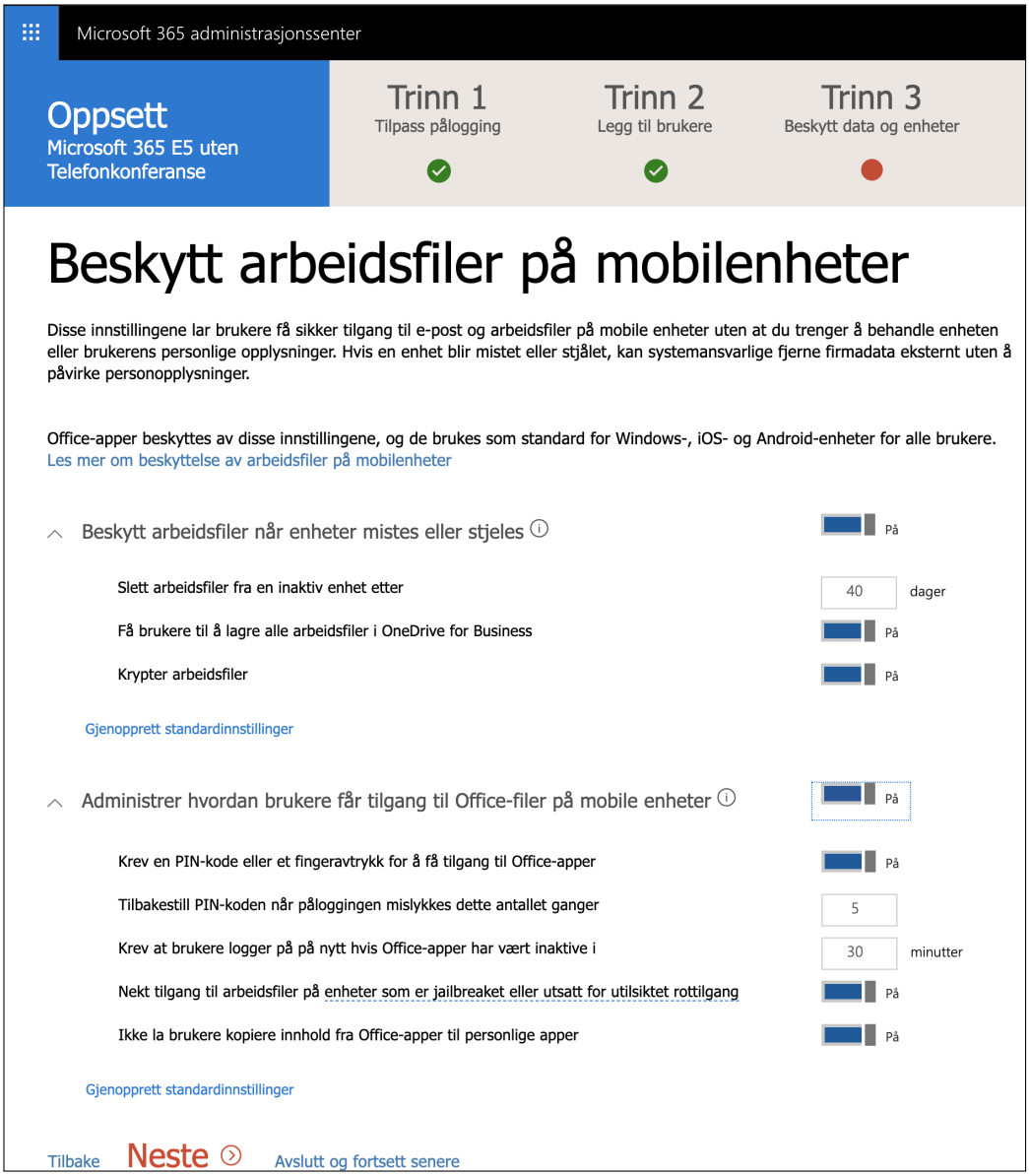
Figur 8

Deretter får en mulighet til å legge til nye brukere og tilegne disse lisenser. Som vist i figur 9, har vi allerede opprettet en bruker og tilegnet lisens, vi legger dermed ikke til noen brukere her. Brukere kan legges til senere, og importering av brukere fra AD kan ikke gjøres via denne veiviseren.



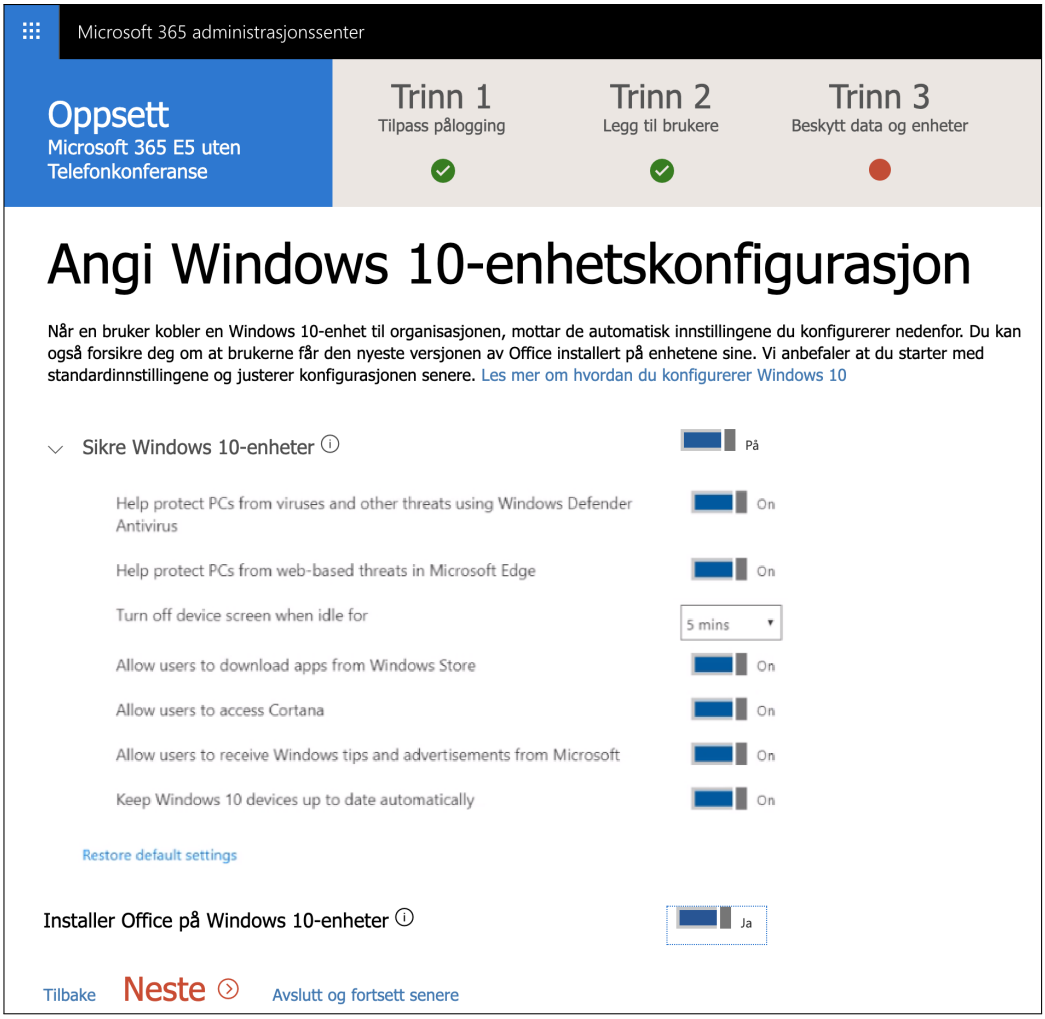
Figur 9

Neste punkt er sikkerhet på mobilenheter. Her kan du konfigurer ut ifra bedriftens behov, og standardinnstillingen vil som regel være et greit utgangspunkt for mange bedrifter. Som vi ser i figur 10, skur vi på beskyttelse av arbeidsfiler ved mistet eller stjålet enhet og administrasjon av tilgang på Office-filer på mobile enheter.



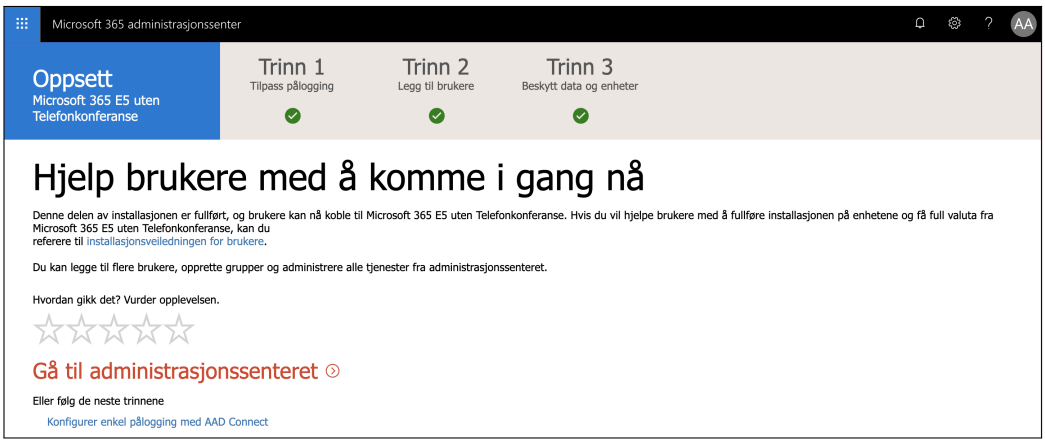
Figur 10

Neste steg er konfigurasjon av Windows 10-enheter. Her kan en konfigurere sikkerhetsinnstillinger ut ifra bedriftens behov. Som vist i figur 11, skur vi på sikring av Windows 10-enheter på, og lar underinnstillinger stå som standard. Vi skrur også på automatisk nedlasting av Office, slik at brukerne slipper å gjøre dette selv på nye maskiner.



Figur 11

Førstegangsoppsettet er nå ferdig, og det er nå dannet et godt utgangspunkt for videre administrasjon. Veiviseren avslutter med en lenke til administrasjonssenteret, som vist i figur 12.



Figur 12

5 Administrasjon av tenant

Brukere og brukergrupper administreres gjennom Azure Active Directory. Enheter og enhetsgrupper administreres gjennom Intune. Begge disse er å finne flere steder. Videre vil noen alternativer for drift listes og vurderes.

5.1 Microsoft 365 Administrasjonssenter

Portal laget for M365-businesskunder som ønsker en brukervennlig administrasjonskanal som ikke har for mange alternativer. Her kan en enkel opprette brukere, kjøpe og tilegne lisenser til brukerne, og administrere bruk av Office-programmer. Her er det store fliser med få undermenyer, som gjør at en får rask tilgang på det som er viktigst for disse brukerne. Portalen var opprinnelig bygd for drifting av Office 365, men har kontinuerlig fått mer funksjonalitet.

Du kan nå administrasjonssenteret gjennom disse URL-ene:

- `https://portal.office.com/adminportal`
- `https://admin.microsoft.com`

5.2 Azure

En portal som inneholder alle verktøyene en trenger for administrasjon av tenant, brukere og enheter. Her finnes også alle andre tjenester som virtuelle maskiner, SQL-instanser og andre ressurser som Microsoft tilbyr i sin skyplattform, Azure. Dette er en portal rik på verktøy og muligheter, men er dermed også mindre oversiktlig enn Microsoft 365 Administrasjonssenter. Siden portalen er rik på verktøy og ressurser er den et viktig punkt for administrasjon, så det er lurt å gjøre seg komfortabel med navigasjon i den.

Du kan nå Azure-portalen gjennom disse URL-ene:

- `https://portal.azure.com`

5.3 Microsoft 365 Device Management

Dette er en forenklet versjon av Azure-portalen. Her er ligger det blandt annet verktøy for administrering av enheter, Intune, sikkerhetspolicies, Azure Active

Directory og klientapplikasjoner. Denne portalen vil bli brukt mest videre i prosjektet, da denne portalen har alt som trengs og egner seg best.

Du kan nå Device Management-portalen gjennom disse URL-ene:

- `https://devicemanagement.microsoft.com`

Modern Workspace - Driftsdokument
AD Connect

v.0.4

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
23.04.2019	0.1	Opprettet dokumentet, lagt inn kilder og figurer for endring av UPN
24.04.2019	0.2	Skrevet introduksjon, lagt til figurer for installasjon av ad-connect, SSO og noe SSPR. Skrevet tekst for AD-Connect og SSO
25.04.2019	0.3	Lagt til figurer og tekst for hele SSPR
04.05.2019	0.4	Mindre revisjon, retting av grammatiske- og andre språkfeil

Innhold

1 Introduksjon

Dagens bedrifter benytter en rekke applikasjoner, noen i sky og noen on-prem. For at samme person skal kunne benytte sin digitale identitet både lokalt og i sky, trengs en hybrid identitet[1]. En slik hybrid identitet kan oppnås ved at alle lokale brukere også eksisterer i skyen. For dette blir AD-Connect tatt i bruk.

AD-Connect benyttes for å synkronisere brukerobjektene i lokal AD ut til Azure AD. Hvis en bruker endrer sitt passord i skyen skal dette passordet bli synkronisert tilbake til lokal AD. Slik sikres høy integritet i både lokal AD og Azure AD.

Dokumentet vil gå ut ifra at leser har en viss teknisk kunnskap, og vil ikke nødvendigvis være enkelt å forstå for ufaglærte.

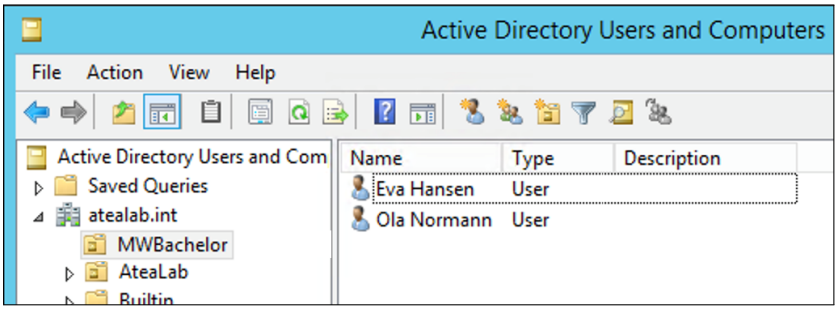
2 Installasjon av AD Connect

2.1 Prerequisites

I dette scenariet er det bare en OU og alle under OU-er som skal synkroniseres til AzureAD. Før dette kan gjennomføres må noen saker være på plass[2]:

- En Azure AD må eksistere
- Domenet som skal benyttes i Azure AD må være verifisert
- Lokal AD og AD Connect må kjøre på Windows Server 2008 R2 eller nyere
- AD Connect krever at serveren har en GUI installert

Det lokale domenet som skal synkroniseres til sky er “atealab.int” og OU-en “MWBachelor” inneholder brukerne. Bare denne OU-en ønskes synkronisert.



Figur 1

Ved å liste ut brukerkontoene i et powershellvindu er det mulig å se at brukernes UserPrincipalName (UPN) inneholder "@atealab.int". Dette er ikke et verifisert domene i vår Azure AD og dermed må brukernes UPN skiftes til "@MWBachelor.onmicrosoft.com".

Listing 1: Brukeres UPN

```
$oupath = "OU=MWBachelor,DC=atealab,DC=int"
Get-ADUser -Filter * -SearchBase $oupath
```

```
DistinguishedName : CN=Eva Hansen,OU=MWBachelor,DC=atealab,DC=int
GivenName         : Eva
Name              : Eva Hansen
ObjectClass       : user
ObjectGUID        : 02cc00ed-c245-462f-8af2-524058ad7433
SamAccountName    : evah
SID               : S-1-5-21-4229914207-3099773454-213119197-1732
Surname           : Hansen
UserPrincipalName : evah@atealab.int
```

Figur 2

Powershell benyttes for å søke gjennom alle brukerne i OU-en og endre UPN hos alle brukerne til det nye domenet.

Listing 2: Endre UPN

```
$olds = "atealab.int"
$news = "mwbachelor.onmicrosoft.com"
$ou = "OU=MWBachelor,DC=atealab,DC=int"
Get-ADUser -Filter * -SearchBase $ou | % {
    $newupn = $_.UserPrincipalName.replace($olds, $news)
    $_ | Set-ADUser -UserPrincipalName $newupn
}
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $olds = "atealab.int"
PS C:\Windows\system32> $news = "mwbachelor.onmicrosoft.com"
PS C:\Windows\system32> $ou = "OU=MWBachelor,DC=atealab,DC=int"
PS C:\Windows\system32> Get-ADUser -filter * -SearchBase $ou | foreach{
>> $newupn = $_.userprincipalname.replace($olds,$news)
>> $_ | Set-ADUser -UserPrincipalName $newupn
>> }
>>
PS C:\Windows\system32> _
```

Figur 3

Når kommandoen er ferdig kan det verifiseres at brukerne benytter det nye domenet i sitt UPN.

Listing 3: Brukeres nye UPN

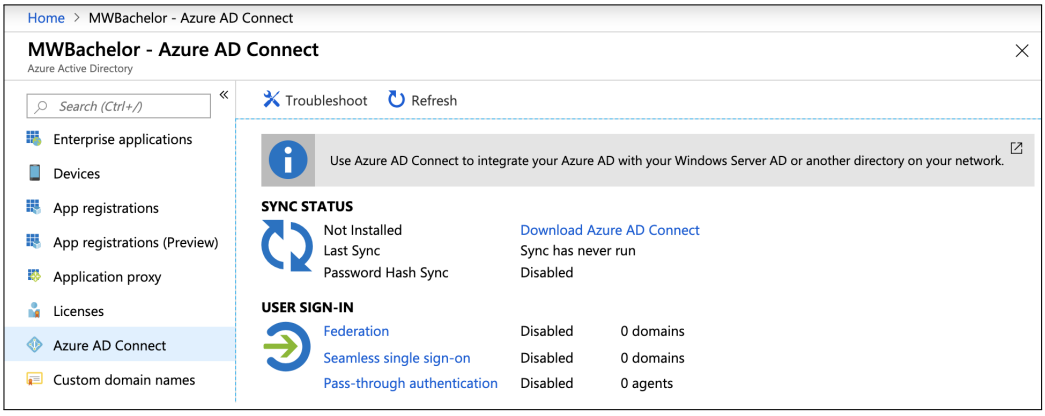
```
$oupath = "OU=MWBachelor,DC=atealab,DC=int"
Get-ADUser -Filter * -SearchBase $oupath
```

```
DistinguishedName : CN=Eva Hansen,OU=MWBachelor,DC=atealab,DC=int
GivenName         : Eva
Name              : Eva Hansen
ObjectClass       : user
ObjectGUID        : 02cc00ed-c245-462f-8af2-524058ad7433
SamAccountName    : evah
SID               : S-1-5-21-4229914207-3099773454-213119197-1732
Surname           : Hansen
UserPrincipalName : evah@mwbachelor.onmicrosoft.com
```

Figur 4

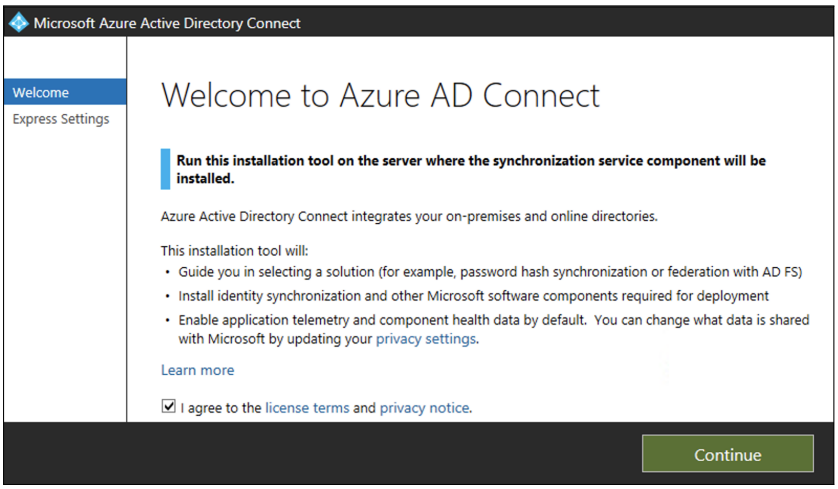
2.2 Installasjonen

I Azure AD er det en meny på venstre side, velg "Azure AD Connect". Her vil det stå status og tidspunkt for siste synkronisering. For å starte installasjonen må agenten lastes ned og installasjonsfilen flyttes til lokal AD server. Agenten lastes ned ved å velge linken med teksten "Download Azure AD Connect".



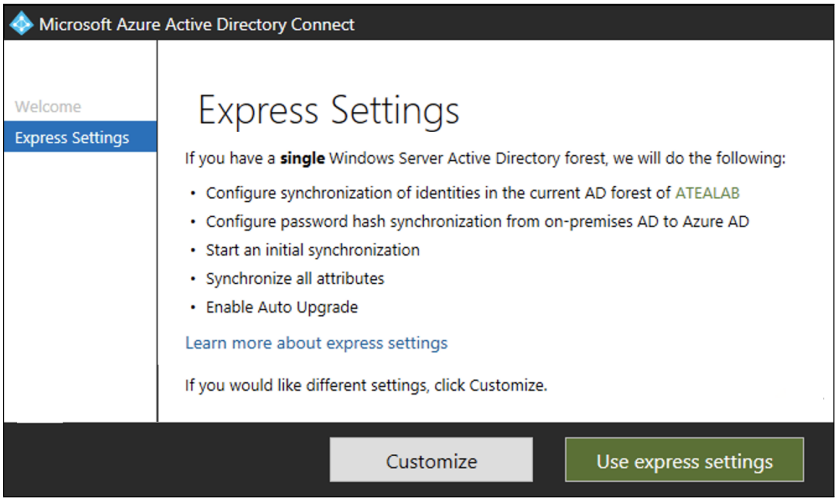
Figur 5

Når installasjonsfilen starter på lokal AD server vil følgende bilde vises. Her må retningslinjene godtas før en kan gå videre.



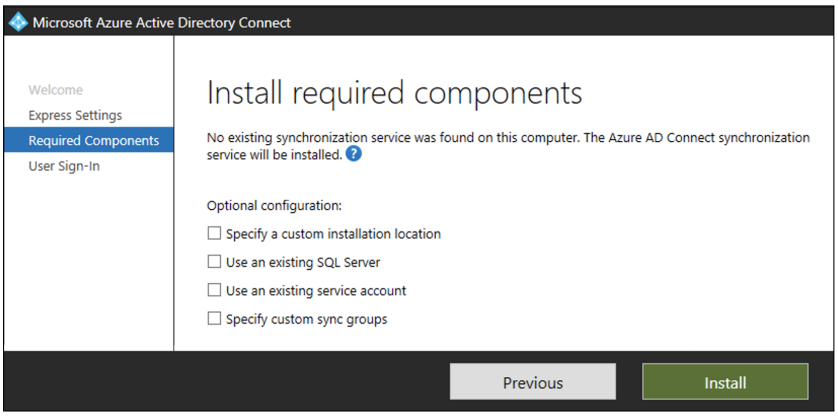
Figur 6

For å få muligheten til å filtrere OU-er i denne veiviseren kjøres en custom installasjon[3]. Flere av valgene vil likevel bli stående som standard.



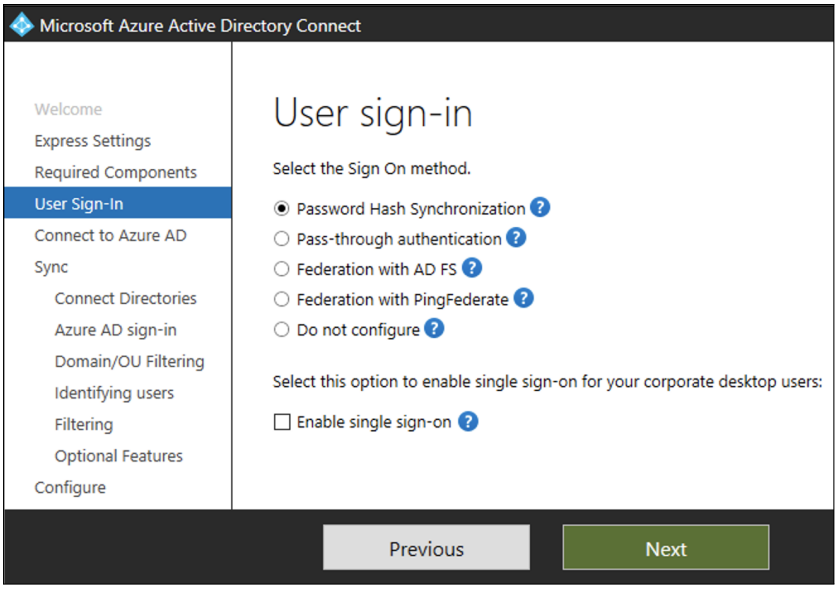
Figur 7

Komponentene som skal installeres bestemmer programvaren selv. Her trengs det ikke å gjøres noe, bare velg “Install”.



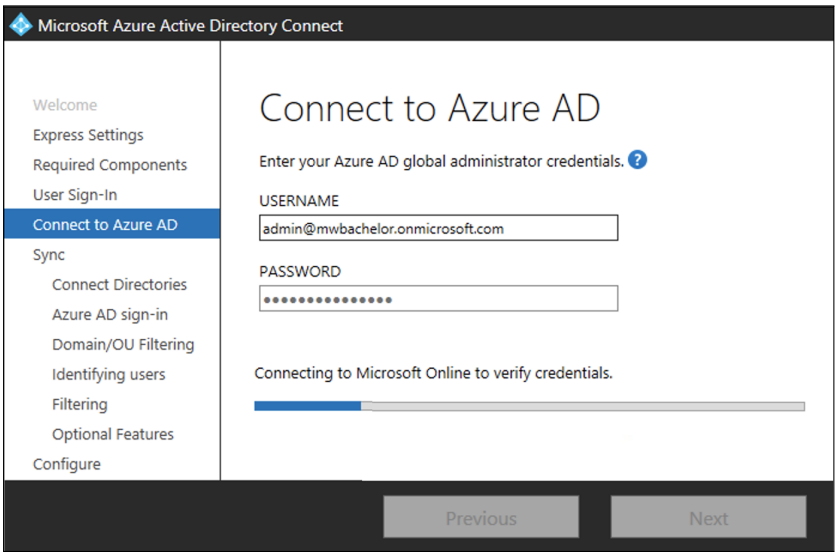
Figur 8

Når komponentene som kreves er installert vil det være mulig å velge mellom ulike innloggingsmetoder. Her velges det “Password Hash Synchronization”. Dette vil si at brukernes passord hashes og denne hashen blir tilgjengelig i skyen. Her vil det også være mulighet å skru på “Single Sign-On”, men dette blir gjort i avsnitt 3. Velg “Next” for å fortsette.



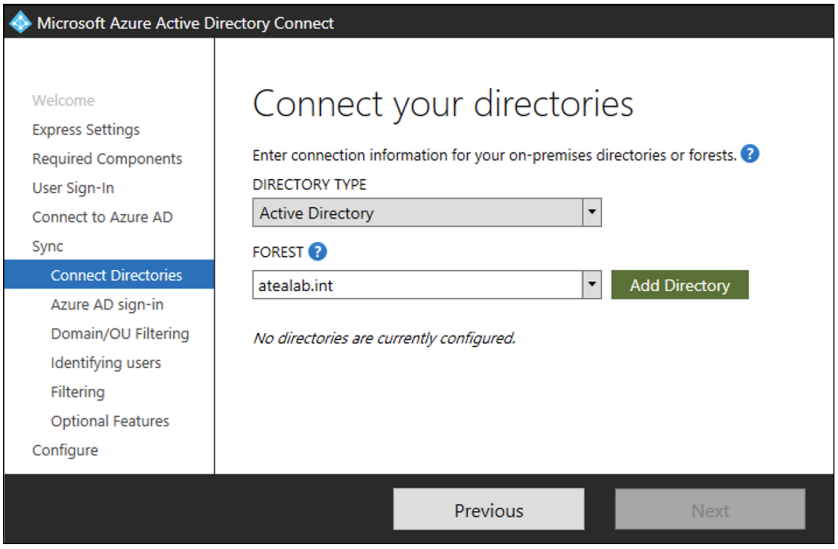
Figur 9

For å få tilgang til Azure AD må det oppgis en konto med globale rettigheter i Azure AD. Velg “Next” for å fortsette og vent på at konto-opplysningene sjekkes.



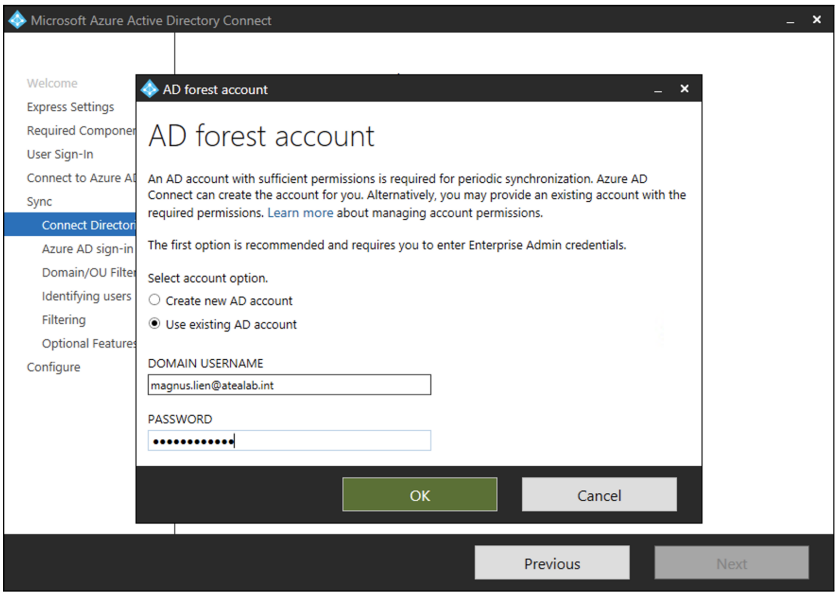
Figur 10

Hvis det lokale domenet har flere skoger må riktig skog oppgis. I dette tilfelle er det bare en skog, denne velges fra nedtrekkslisten og “Add Directory” trykkes.



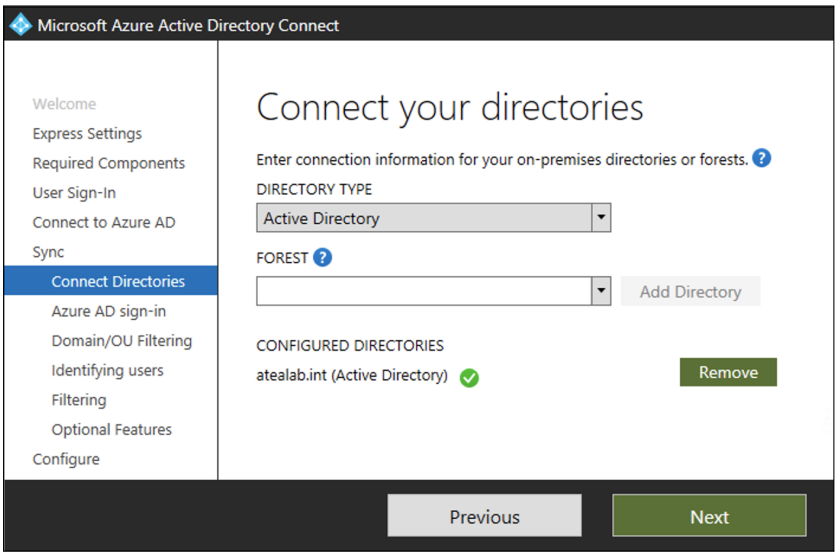
Figur 11

Det må oppgis innloggingsinformasjon for en domeneadminstrator.



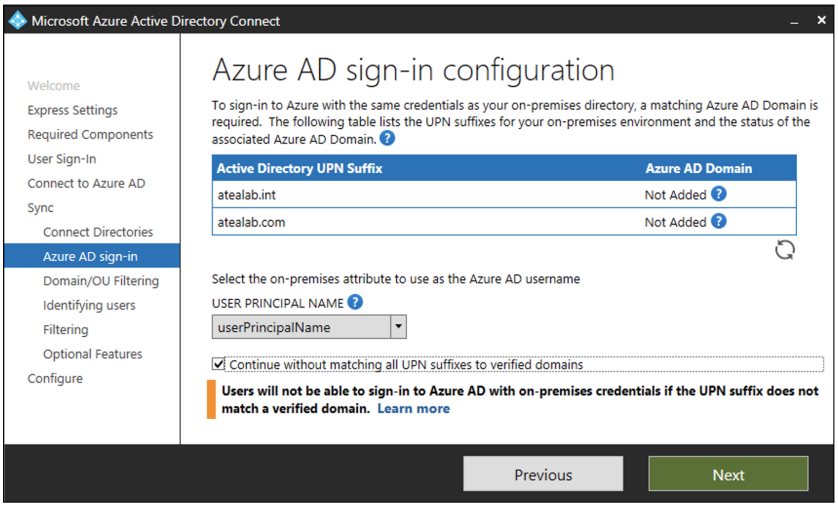
Figur 12

Hvis dette var vellykket vil skogens navn dukke opp med en grønn hake ved seg. Da er det bare å trykke “Next”.



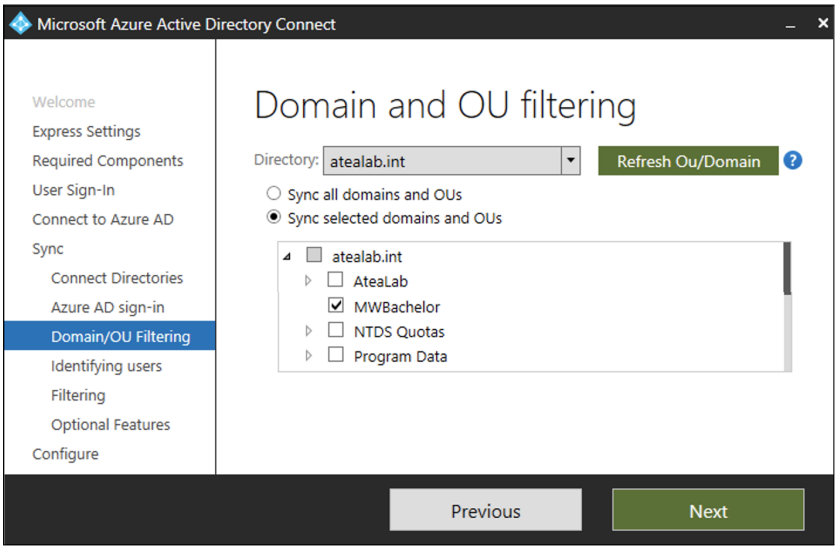
Figur 13

På neste steg vil domene som programvaren finner i det lokale AD dukke opp. For at identitetene skal fungere i skyen, må de ha et domene som er verifisert i Azure AD. I denne listen dukker ikke "mwbachelor.onmicrosoft.com" opp, men det er fordi PowerShell ble brukt for å endre UNP hos brukerne i det lokale domenet. Derfor hukes det av for å fortsette uten å matche UPN imot verifiserte domener.



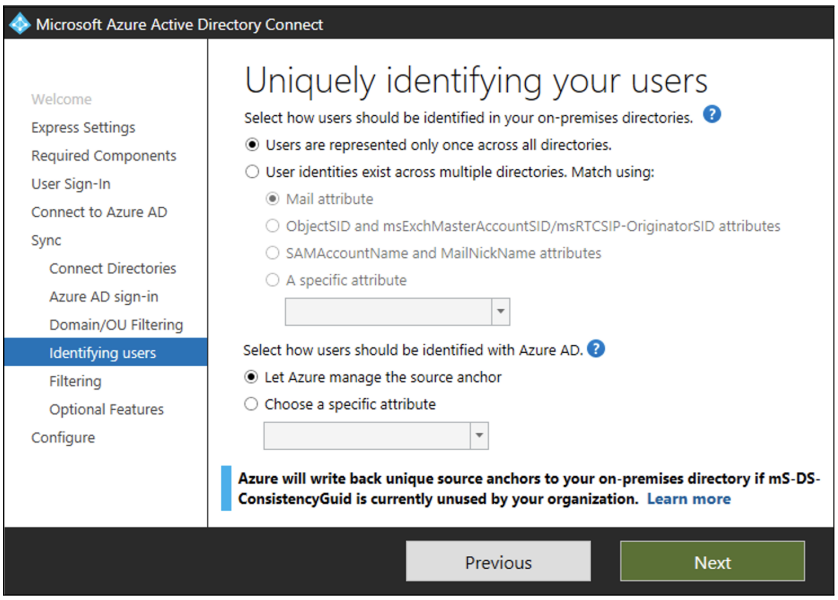
Figur 14

Neste steg tar for seg filtrering av OU-er. Her hukes det bare av for den ene OU-en som ønskes synkronisert. Velg "Next" for å fortsette.



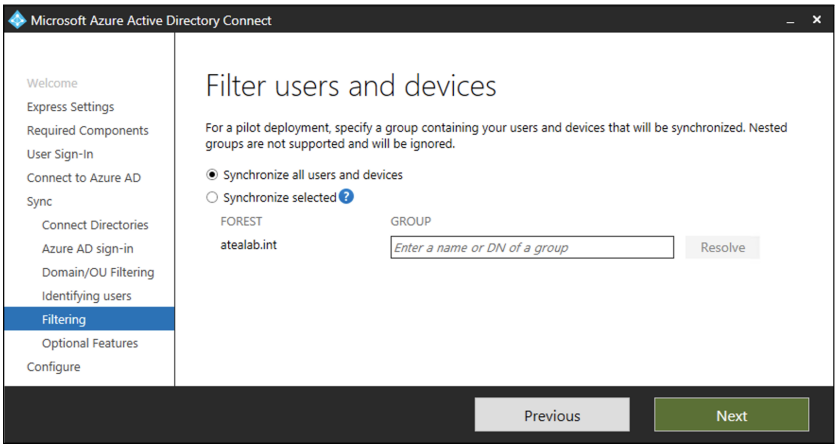
Figur 15

Ved neste steg i veiviseren får alt stå som standard. Her må en passe på at brukerne er unike og ikke forekommer flere ganger.



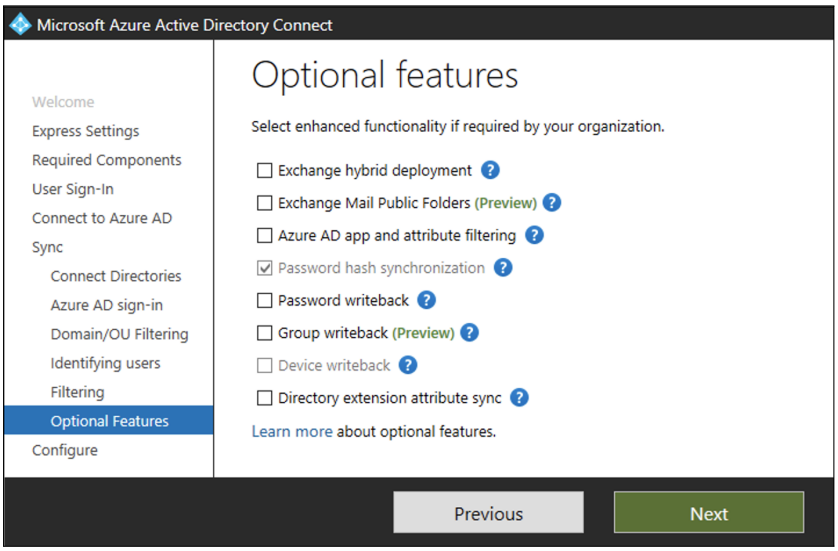
Figur 16

Også ved filtrering av brukere og enheter lar vi valgene stå som standard, dermed vil alle brukere og enheter synkroniseres.



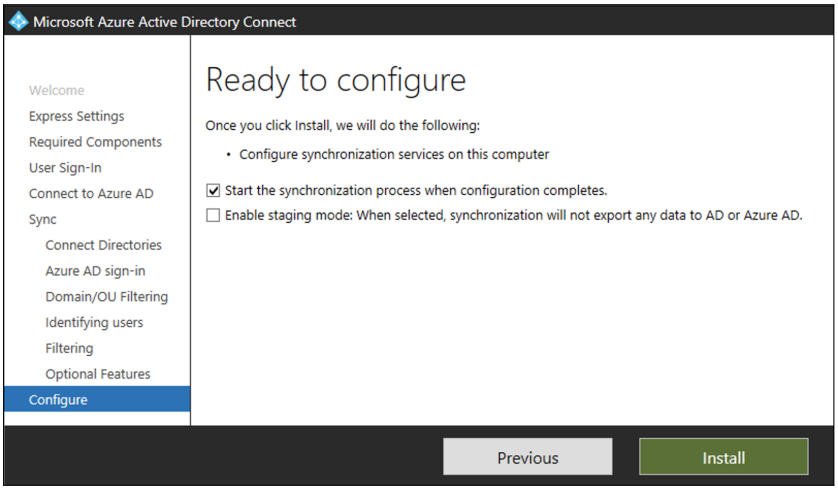
Figur 17

Siste konfigurasjon endres ikke. Men legg merke til “Password writeback” denne vil bli skrudd på i avsnitt 4 Self-service password reset.



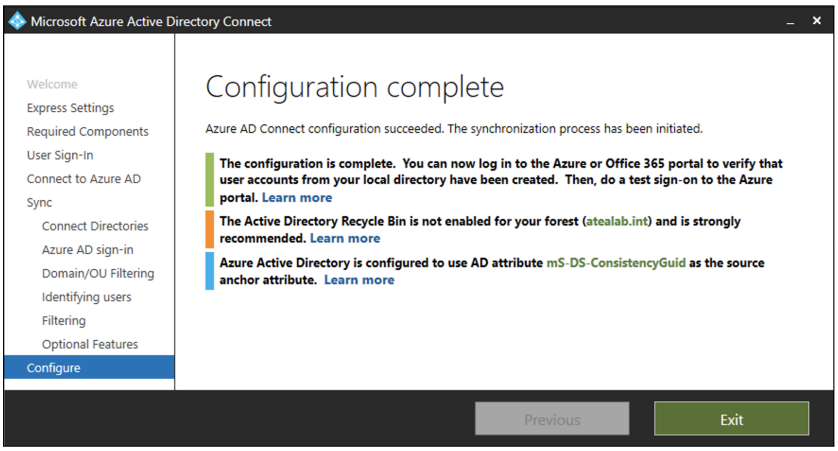
Figur 18

Til slutt hukes det av for å starte synkroniseringen umiddelbart. Avslutt med “Install”.



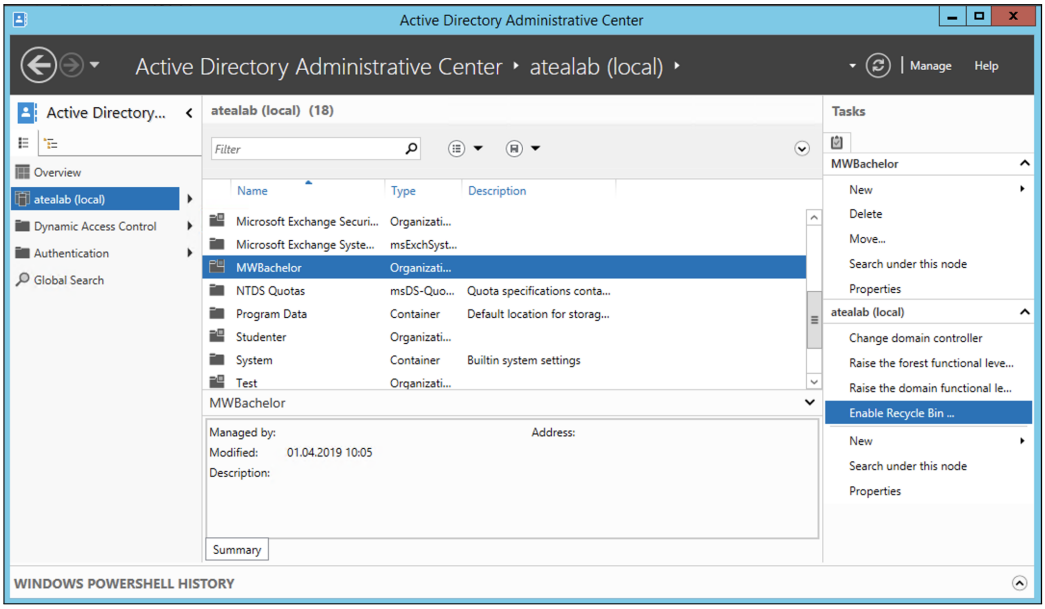
Figur 19

Til slutt vil konfigurasjonen være ferdig, som i figur 20. Her anbefales det å skru på søppelkassen i lokal AD.



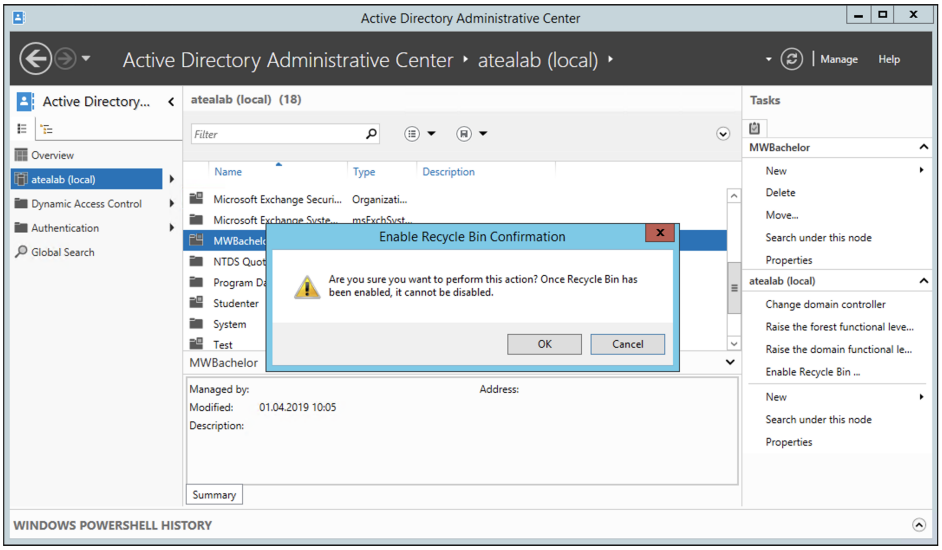
Figur 20

I AD Adminstrative Center klikkes det på det lokale domenet "atealab" i ventre på figur 21. Deretter velges det "Enable Recycle Bin" i menyen til høyre på samme figur.



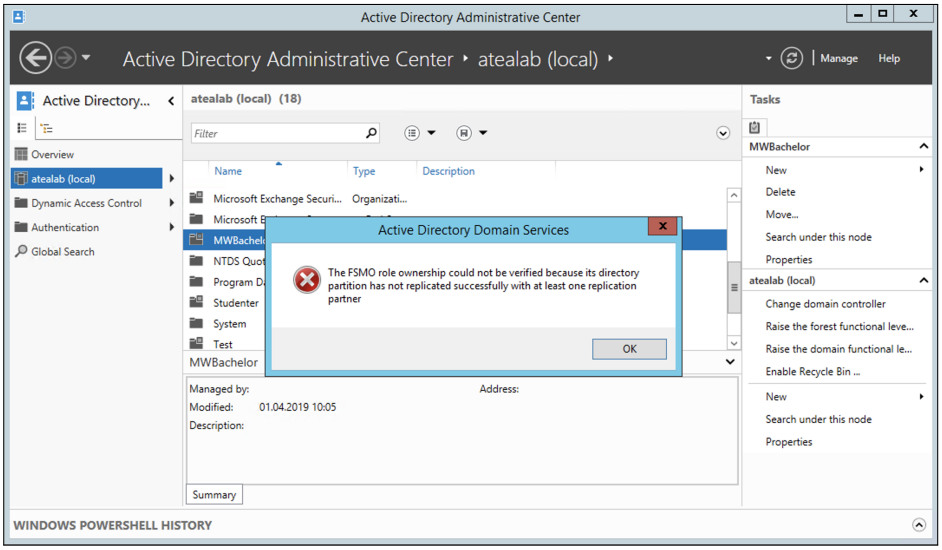
Figur 21

Det vil dukke opp en bekreftelse.



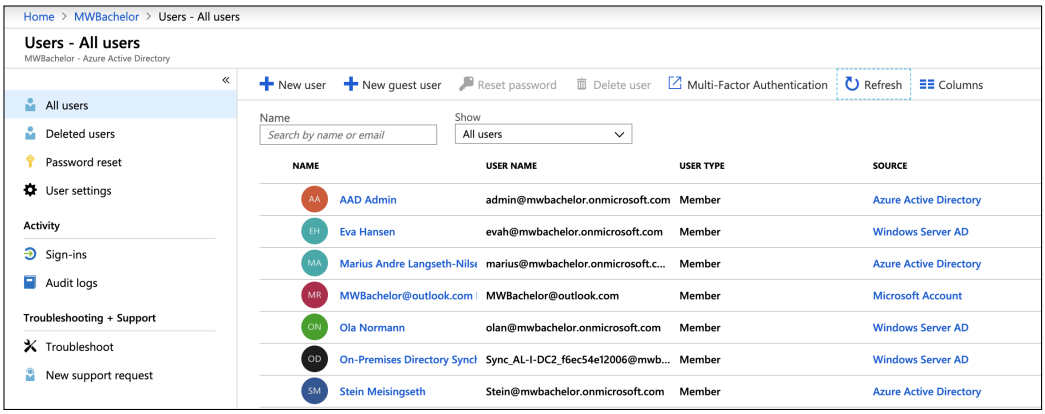
Figur 22

På dette systemet feilet forsøket vårt på aktivering av søppelkurven. Vi opplevde derimot ingen problemer kyttet til den deaktiverte søppelkurven, og den forble derfor deaktivert. Dette kan være et opphav for problemer i andre tilfeller, noe som gjør at det anbefales å utføre feilsøking dersom det skal utføres i en realistisk situasjon.



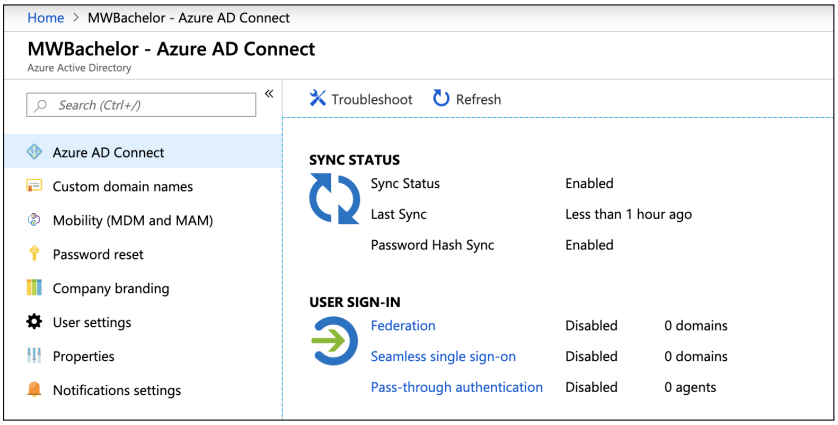
Figur 23

I Azure AD kan vi nå se at det har dukket opp to nye brukere. Dette er de to brukerne som vi kjenner igjen fra lokal AD, noe vi kan være sikre på da disse har kildetypen "Windows Server AD" i figur 24. Det er også dukket opp en "On-Premice Directory Sync"-bruker.



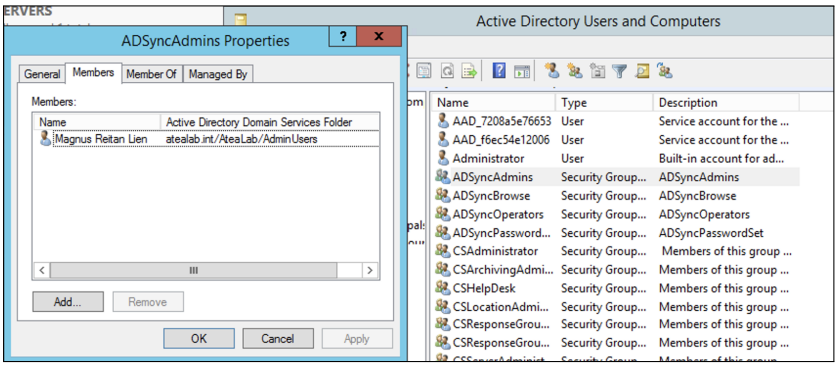
Figur 24

Vi kan også se at statusen og siste synkronisering vil ha oppdatert seg for Azure AD Connect.



Figur 25

I lokal AD er det dukket opp flere grupper som begynner med AD, som ADSyncAdmins. Dette fremkommer i figur 26.

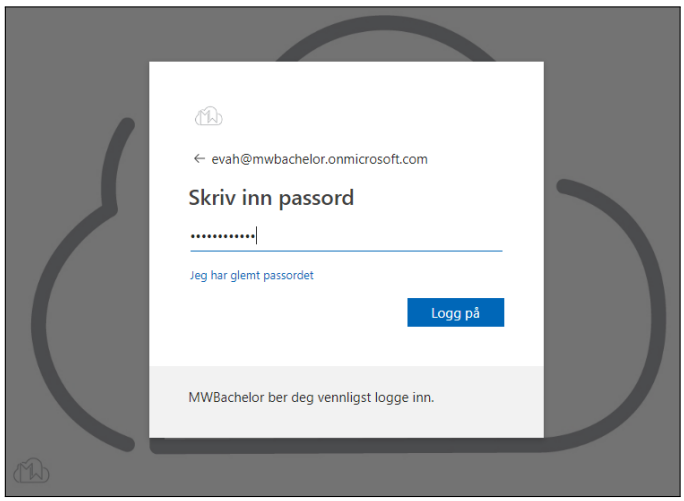


Figur 26

2.3 Test av lokal AD-bruker i sky

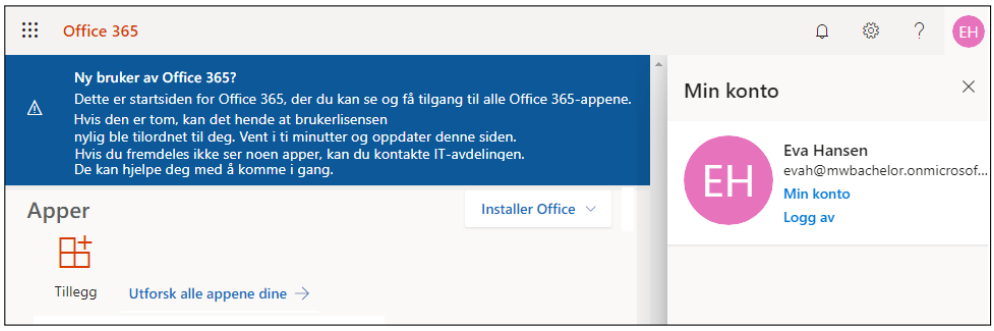
For å teste at brukerne fungerer i skyen vil vi forsøke å logge inn i Office-portalen med en bruker synkronisert fra lokal AD. Verifiser at brukeren får logget inn og har tilgang til de riktige ressursene.

Innloggingen på officeportalen med bruker fra lokal AD.



Figur 27

Bruker får logget inn, men har ingen lisenser knyttet til seg og har dermed ikke tilgang på noen ressurer.



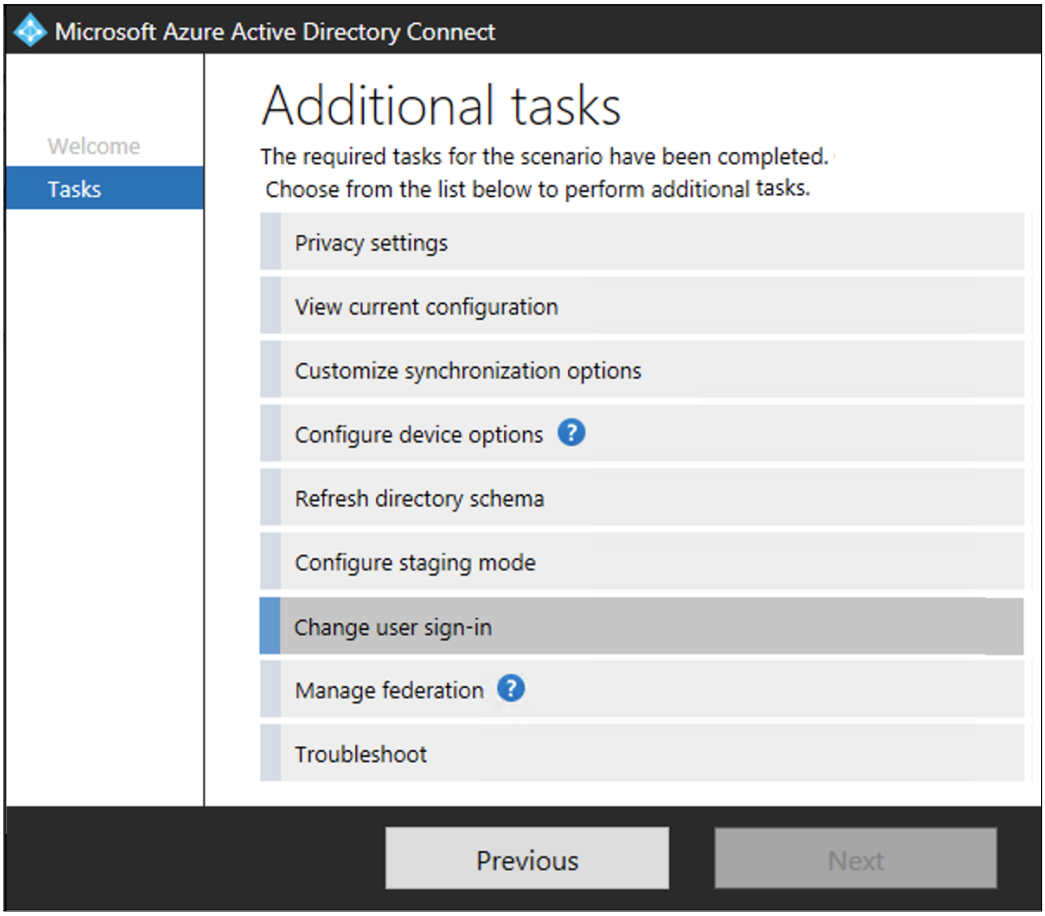
Figur 28

3 Seamless Single Sign-On

Seamless Single Sign-On vil automatisk logge inn brukere som er på bedriftsmaskiner på bedriftsnettverket. På denne måten får brukere kjappere tilgang til skyapplikasjoner.

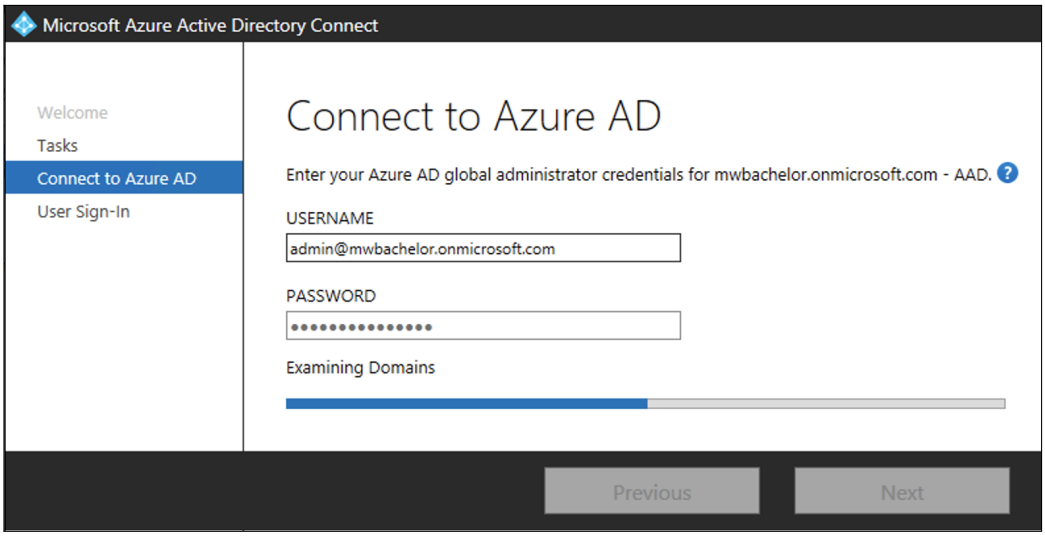
Først må SSO[4] skrus på i Azure AD Connect programvaren. Når dette er utført må SSO rulles ut til brukerne ved hjelp av en "Group Policy" eller en "Group Policy preference" som endrer maskinens intranet sone innstillinger. Denne dokumentasjonen tar for seg utrulling ved bruk av "Group Policy preference". Dette gjør det mulig for sluttbrukeren å endre intranetsone-innstillingen. En group policy ville nektet brukeren å endre denne innstillingen.

Først må SSO skrus på i AD Connect. Åpne programvaren og velg "Change user sign-in"og "Next".



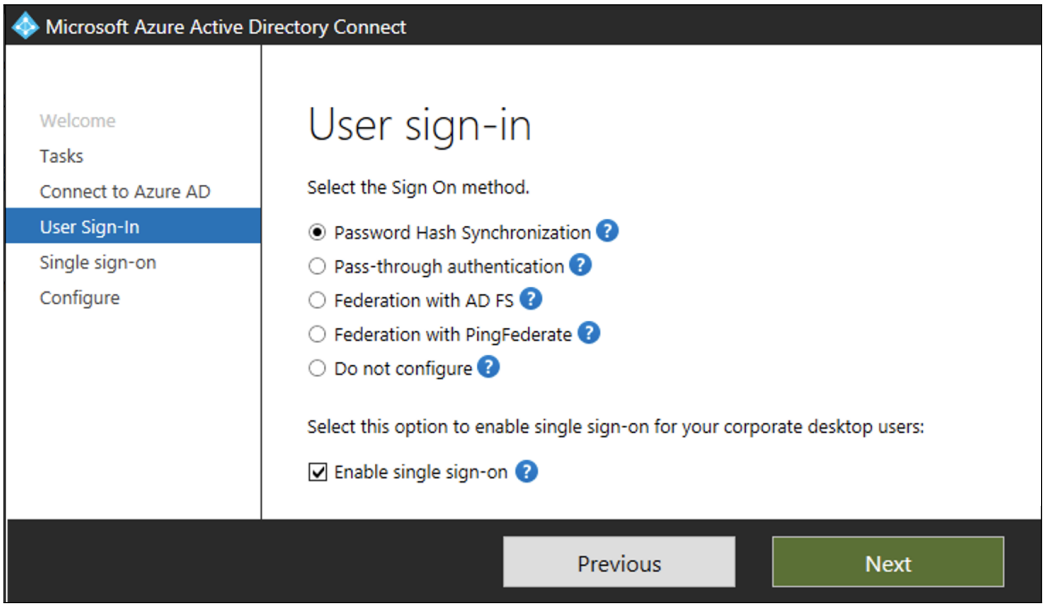
Figur 29

Oppgi kotoinformasjonen til en global administrator i Azure AD.



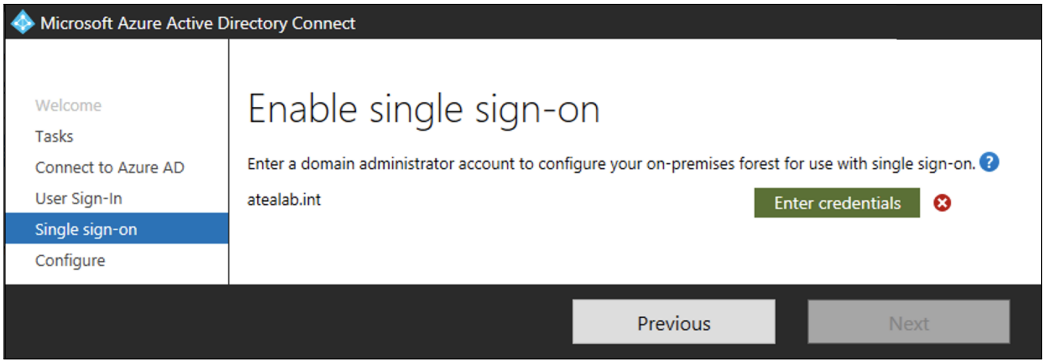
Figur 30

Blant valgene for innlogging hukes det av for “Enable single sign-on”. Trykk så “Nextfor å komme videre.



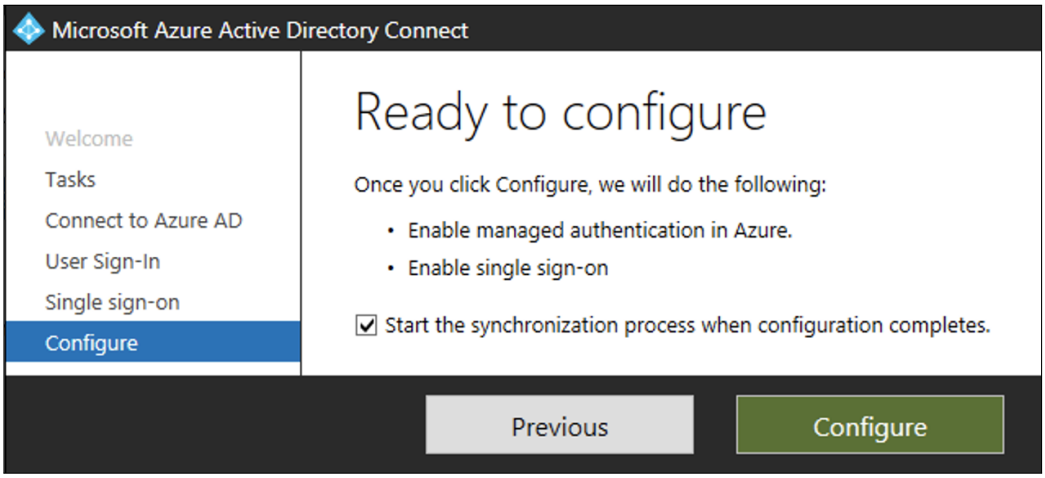
Figur 31

For å kunne endre lokal AD må det oppgis kontoinformasjon til en lokal domeneadminsitrator. Velg først “Enter credentials” og logg inn. Det røde ”X” ikonet skal nå ha skiftet til en grønn hake. Trykk så ”Next” for å komme videre.



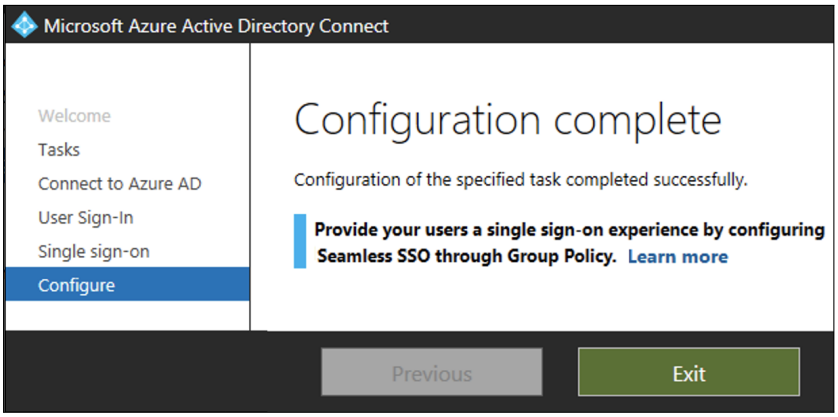
Figur 32

På siste steg hukes det av for å synkroniserer med en gang og “Configure” trykkes.



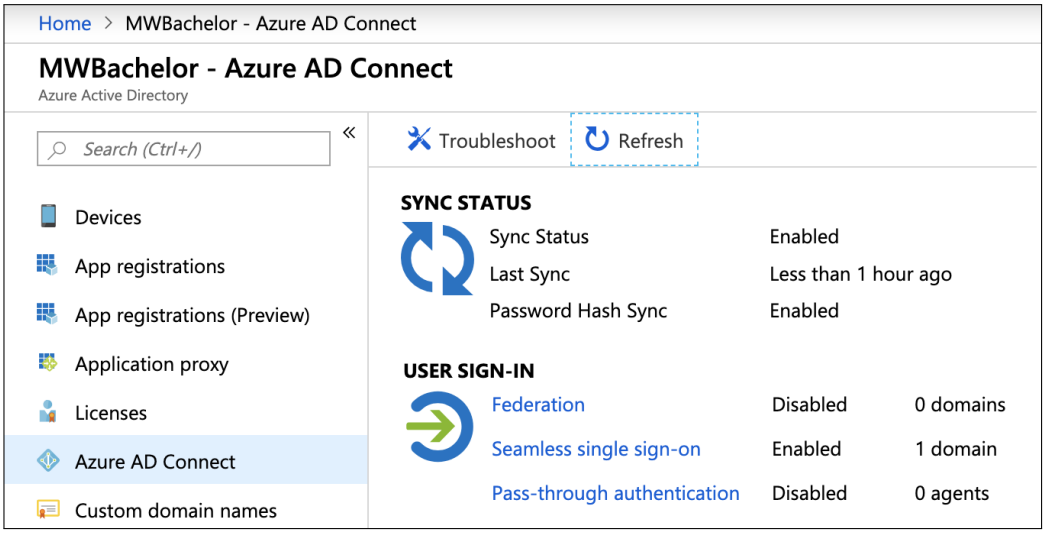
Figur 33

Nå er SSO konfigurert og klar til å gjøres tilgjengelig for sluttbrukerne.



Figur 34

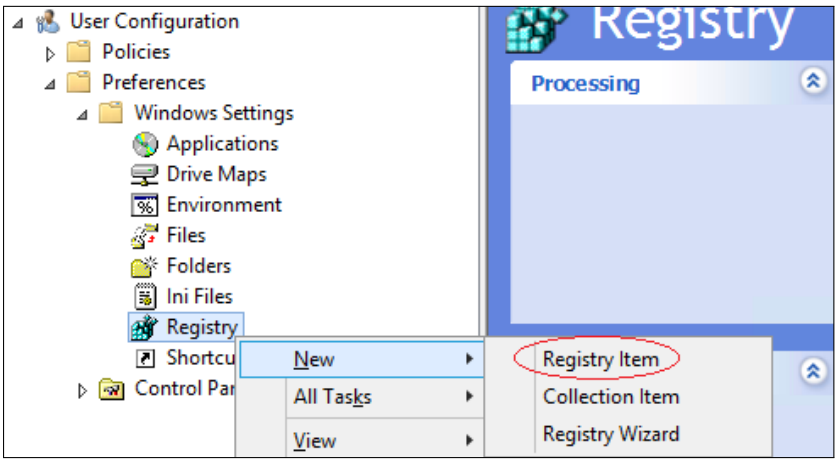
I Azure skal statusen for "Seamless single sign-on"ha blitt endret til "Enabled" for ett domene.



Figur 35

For å gjøre SSO tilgjengelig for sluttbrukerne kan det opprettes en ny GPO eller "Default Domain Policy" kan endres. Sistenevne er det som blir gjort her. Åpne "Group Policy Management Editor" på lokal AD server, høyreklikk på standard policy og velg "Edit".

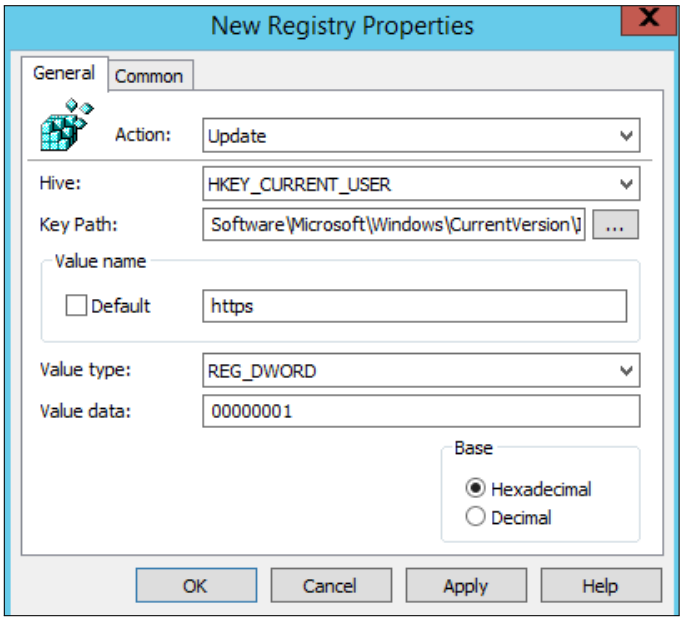
Naviger til "User Configuration", "Preferences" og "Windows Settings". Her er det høyreklikket på "Registry", valgt "New" og "Registry item".



Figur 36

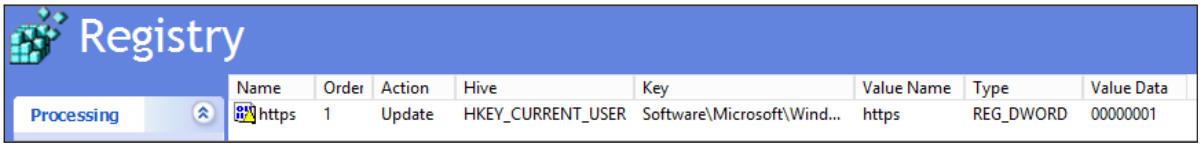
Denne regelen skal ha:

- Key Path: Software\Microsoft\Windows\CurrentVersion\Internet Settings \ZoneMap\Domains\microsoftazuread-sso.com\autologon
- Value name: https
- Value type: REG_DWORD
- Value data: 00000001



Figur 37

Til slutt vil regelen se slik ut som på figur 38.



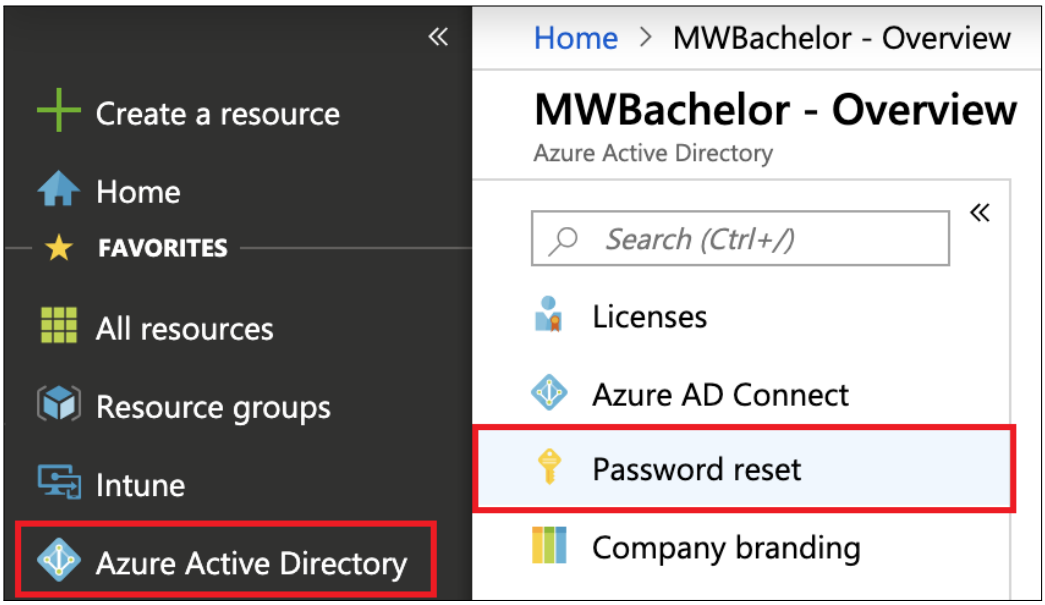
Figur 38

4 Self-service password reset

Brukere glemmer ofte passord eller har andre problemer med å logge inn. En repeterende oppgave for administratorer er å motta slike henvendelser, tilbakestille brukerens passord og sende det nye passordet tilbake til sluttbrukeren. Ved å ta ibruk SSO[5] kan brukeren selv utføre denne prosessen og administrator vil kunne bruke tiden sin på andre henvendelser og oppgaver.

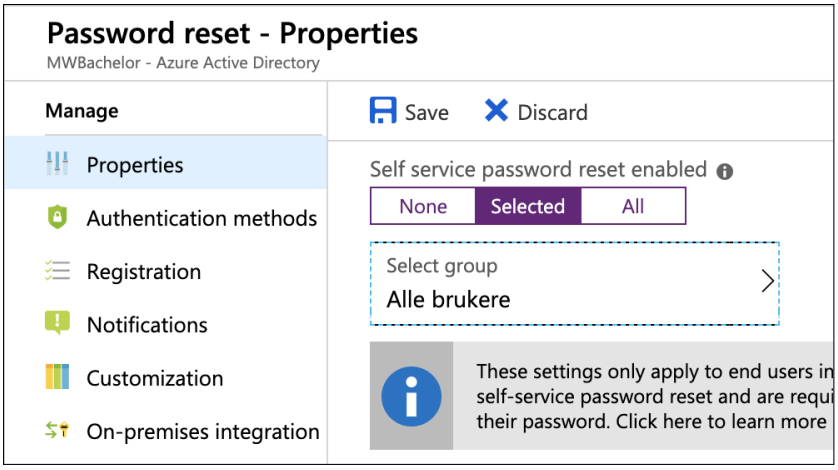
4.1 Oppsett

Password reset skrus på i Azure AD tenanten. Naviger til Azure AD og i menyen på venstre side vil det stå "Password reset", velg denne.



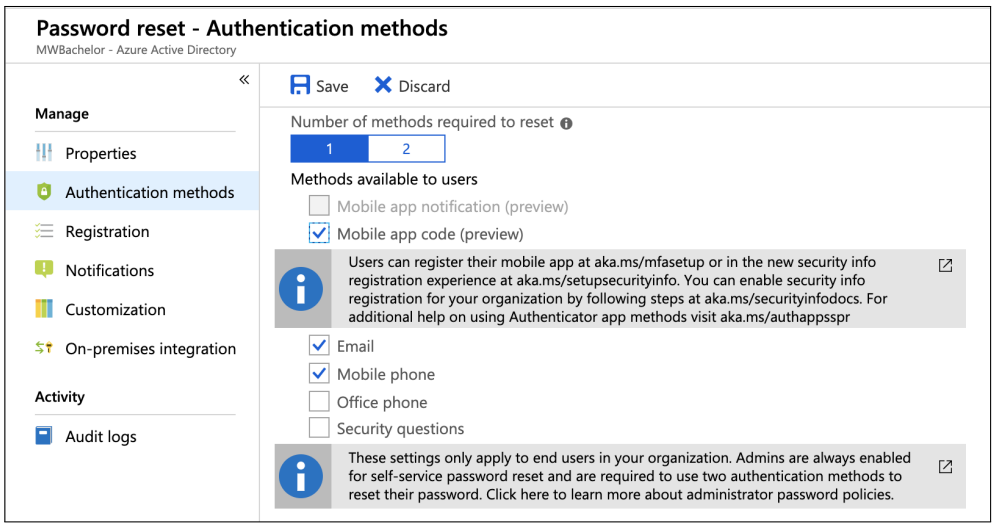
Figur 39

I "Properties" menyen velges det hvem som skal kunne benytte seg av SSPR. Det kan velges mellom ingen, alle eller noen. I dette tilfellet er det valgt noen brukere og spesifisert nærmere med brukergruppen "Alle brukere". Husk her å lagre oppsettet ved å trykke Save". I venstre meny på figur 40 velges nå "Authentication methods".



Figur 40

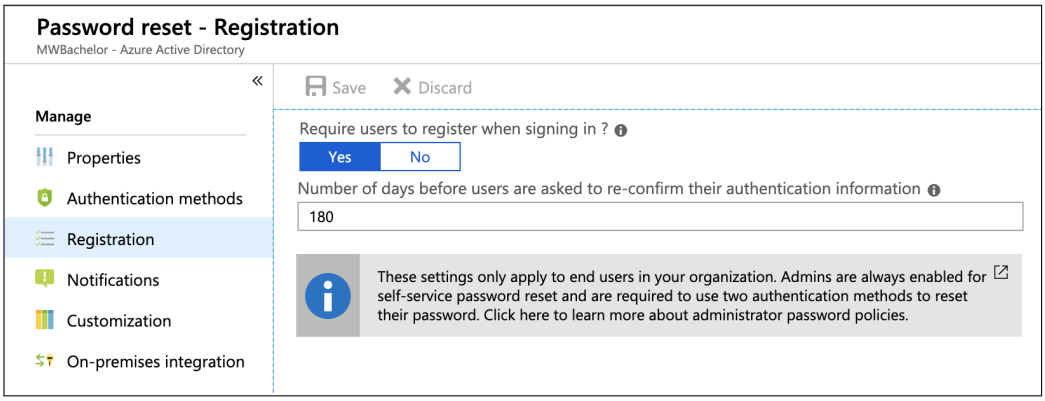
Her velges det hvor mange og hvilke metoder brukerne kan benytte for å autentisere seg seg ved tilbakestilling av passord. I dette tilfellet er det valgt at en metode er nok og brukeren kan velge mellom en mobil app, SMS eller epost. Husk å lagre, og velg videre "Registration" fra menyen på venstre side i figur 41.



Figur 41

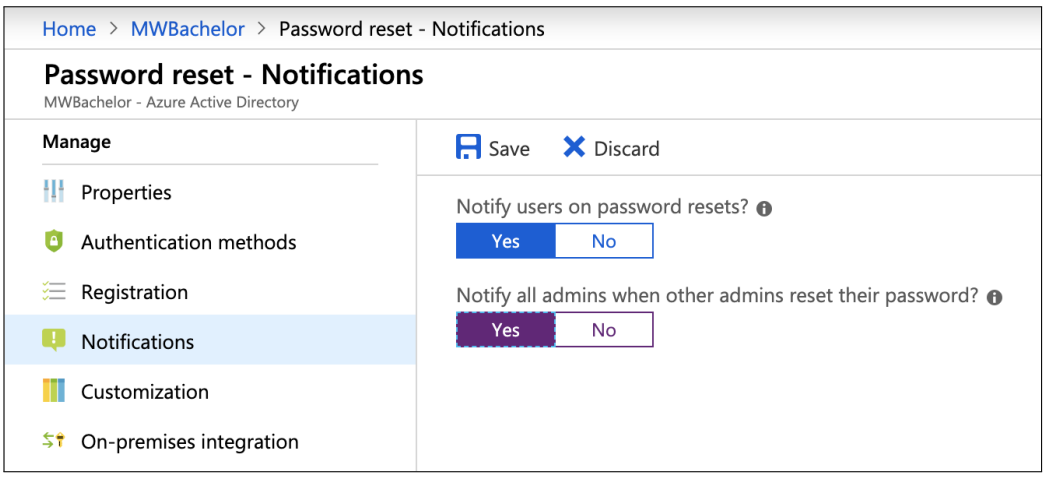
Ved å sette “Require users to register when signing in?” i figur 42, vil brukerne tvinges til å registrere seg for passord-tilbakestilling neste gang de logger inn[6].

Det er også mulig å velge hvor lenge denne registreringen en gyldig. Husk å lagre, og velg videre “Notificatoins” fra menyen på venstre side i figur 42.



Figur 42

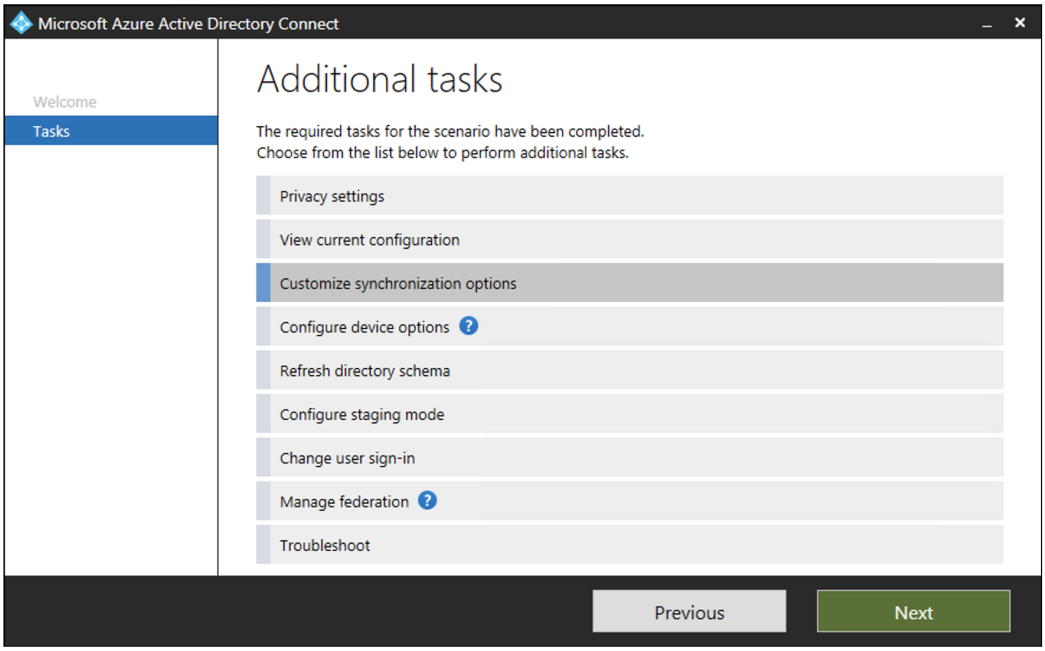
Her er det mulig å tilpasse hvilke varslinger som skal sendes ut ved tilbakestilling av passord. På figur 43 er begge varslene slått på.



Figur 43

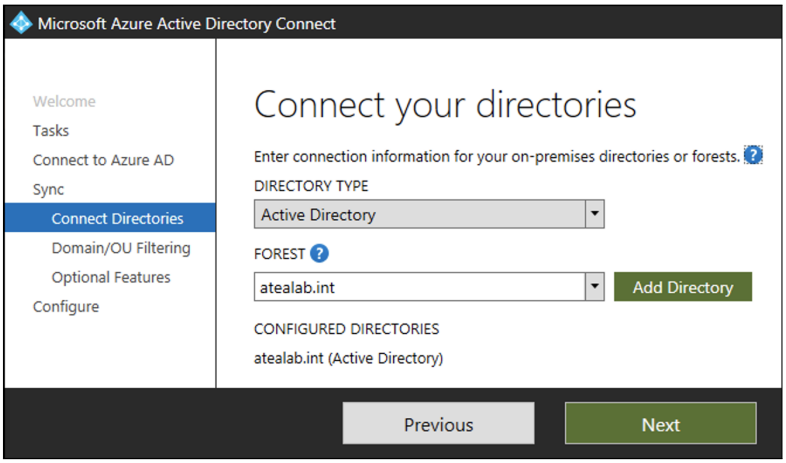
For at passordendringer i skyen skal synkronisere tilbake til det lokal AD må dette skrus på i Azure AD Connect-programvaren på lokal AD server[7].

Åpne AAD Connect, velg der "Customize sync..." og "Next". Om nødvendig må det logges inn med en Azure administrator.



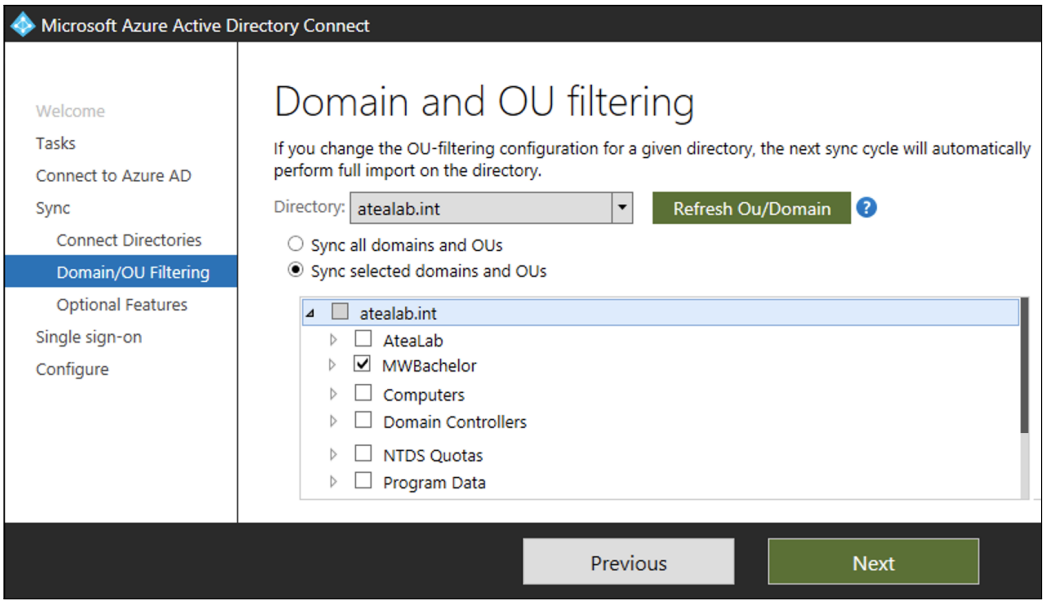
Figur 44

Deretter må det velges hvilket domene som skal konfigureres og administrator må logge inn. Når dette er gjort, velg "Next".



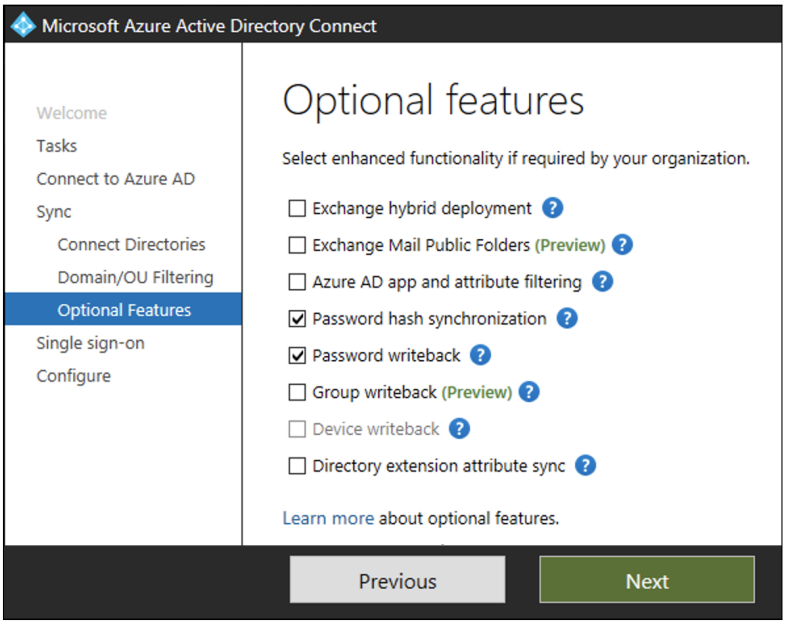
Figur 45

På steget for OU filtrering trengs det ikke gjøres noe, velg “Next”.



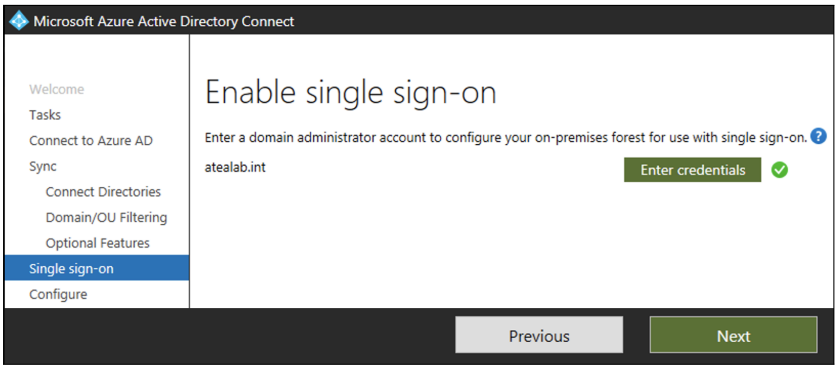
Figur 46

Under “Optional features” hukes det av for “Password writeback” og så velges “Next”.



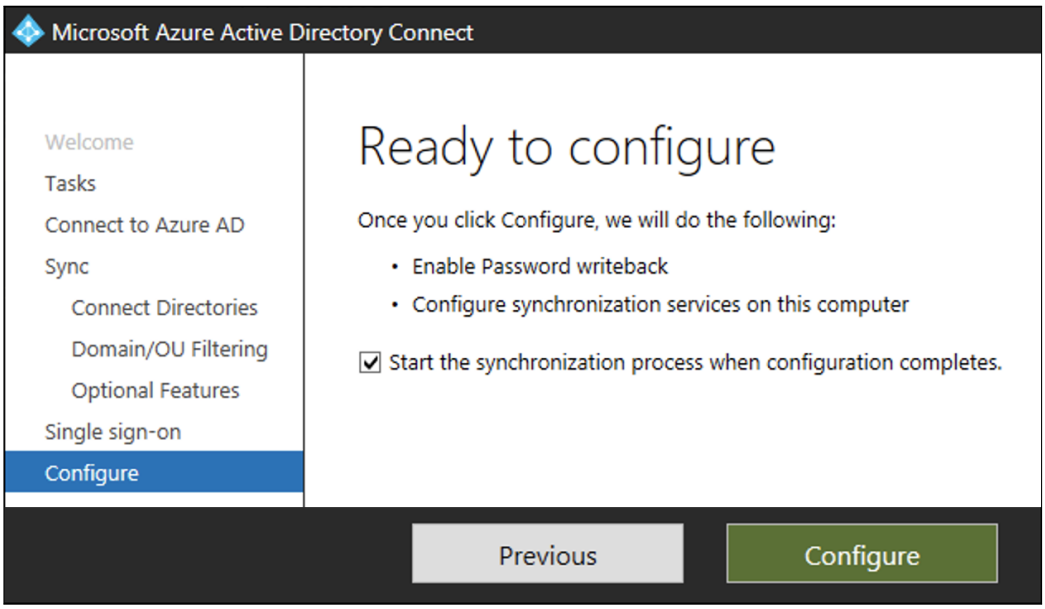
Figur 47

På steget for SSO trengs det ikke gjøres noe, velg her “Next”.



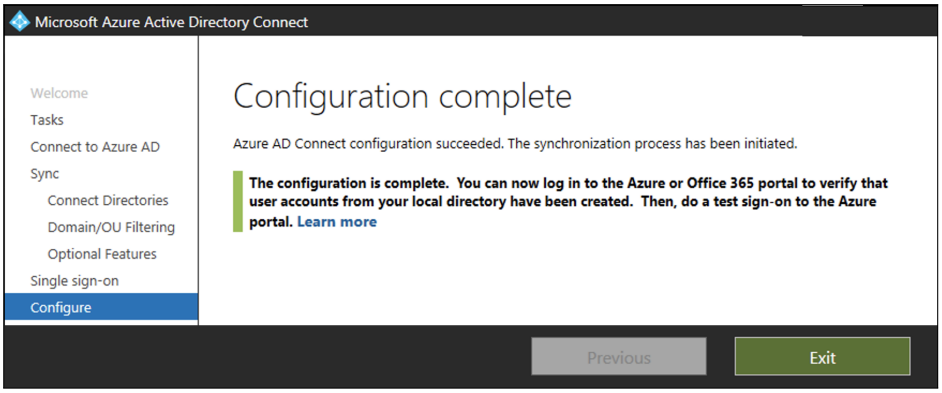
Figur 48

Til slutt vil det dukke opp en oversikt over hvilke endringer som vil konfigureres, forsett med å trykke “Configure”.



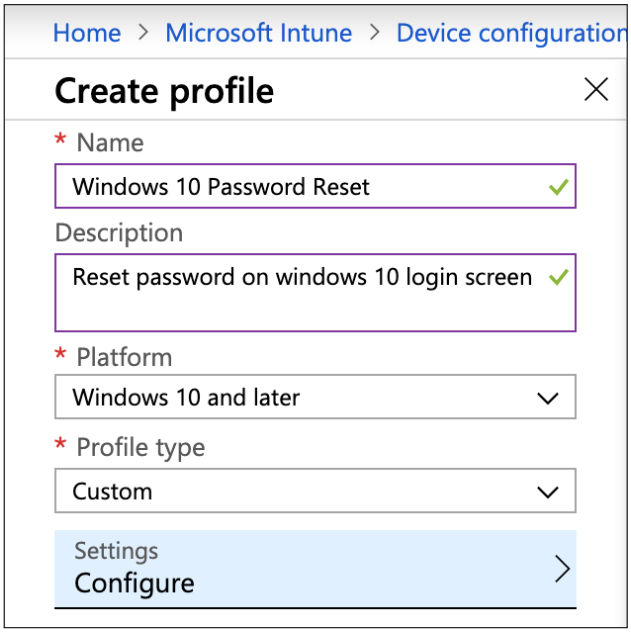
Figur 49

AD Connect er nå satt opp med “Password writeback” og en kan avslutte veiviseren ved å trykke Exit”.



Figur 50

For at tilbakestilling av passord skal fungere på innloggingsskjermen[8] i Windows 10, må det opprettes en enhetskonfigurasjon. Dette utføres ved å navigere til Intune og velge “Device configuration”. Der er det bare å opprette en ny profil. Denne gis et navn og en beskrivelse, “Platform” settes til Windows 10 eller nyere og profilens type skal være “Custom”. En slik profil finnes i figur 51. Trykk på “Configure” under profilens innstillinger.

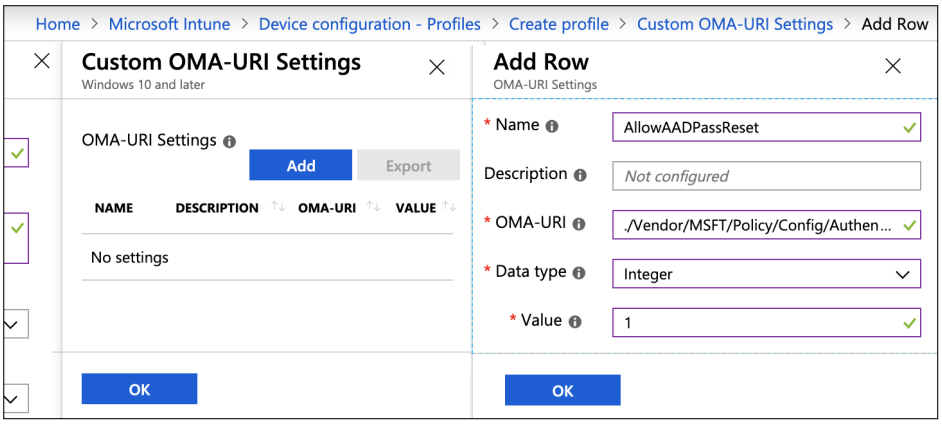


Figur 51

Da vil det dukke opp et vindu som figur 52. Trykk “Add”. I de ulike feltene fylles det ut et navn og følgende:

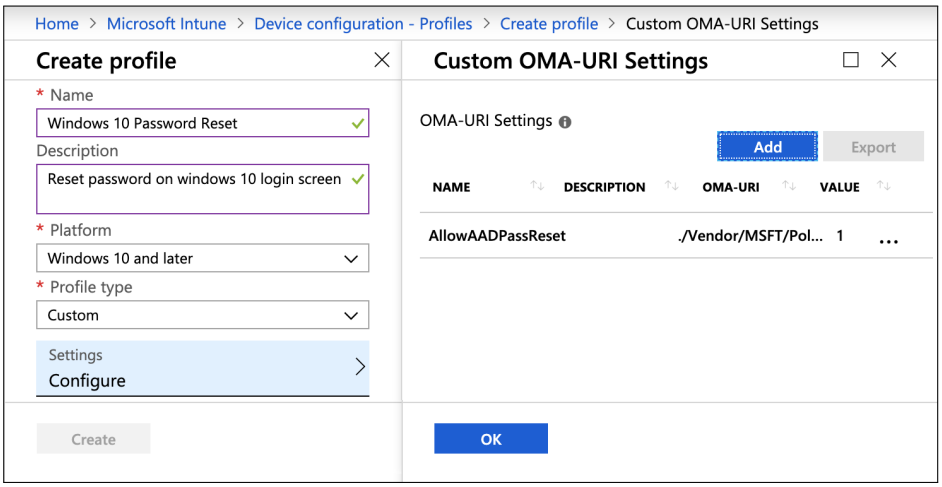
- OMA-URI: ./Vendor/MSFT/Policy/Config/Authentication/AllowAadPasswordReset
- Data type: Integer
- Value: 1

Avslutt med å trykke på knappene som viser “OK”.



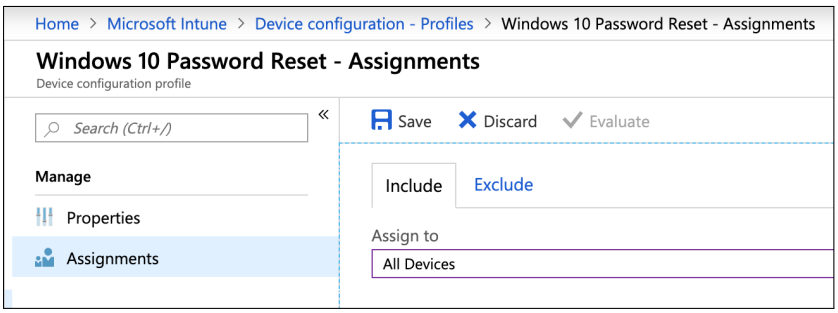
Figur 52

Profilen vil da se ut som på figur 53. Velg “OK” og “Create”.



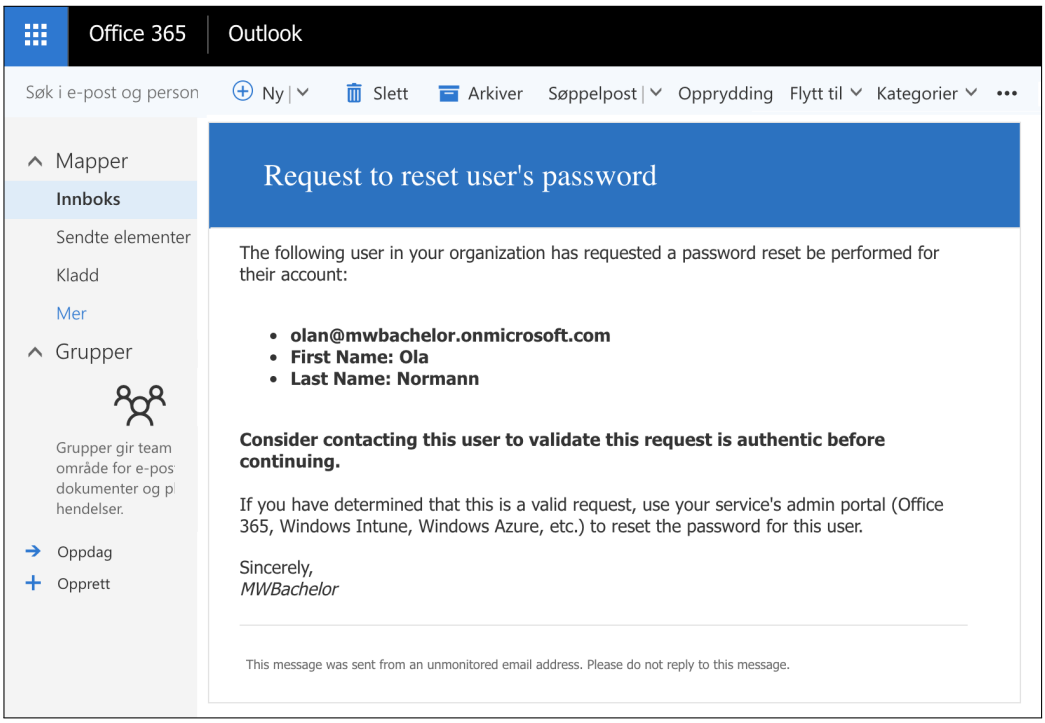
Figur 53

I venstre meny på den nye profilen velges det “Assignments” og profilen tildeles “All Devices”.



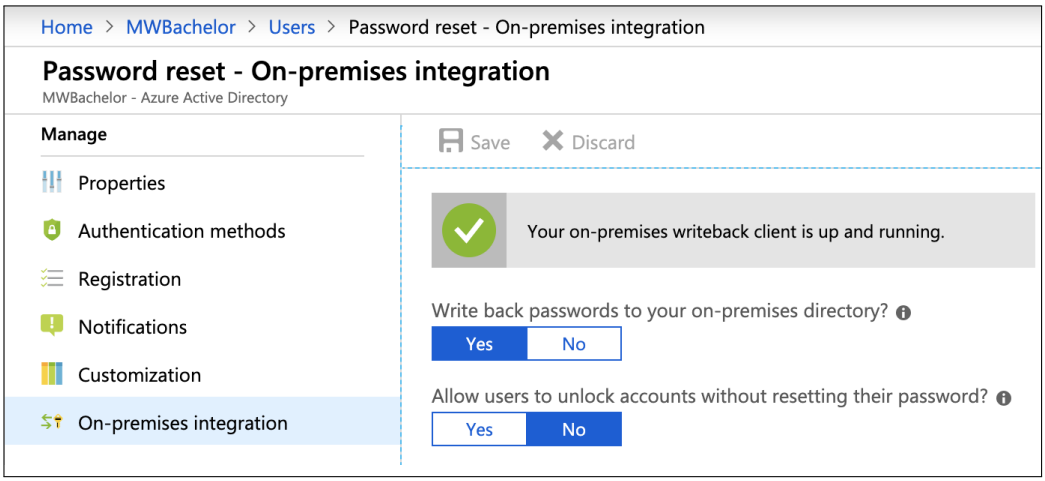
Figur 54

Når en bruker forsøker å tilbakestille sitt passord vil det sendes ut et varsel slik som på figur 55.



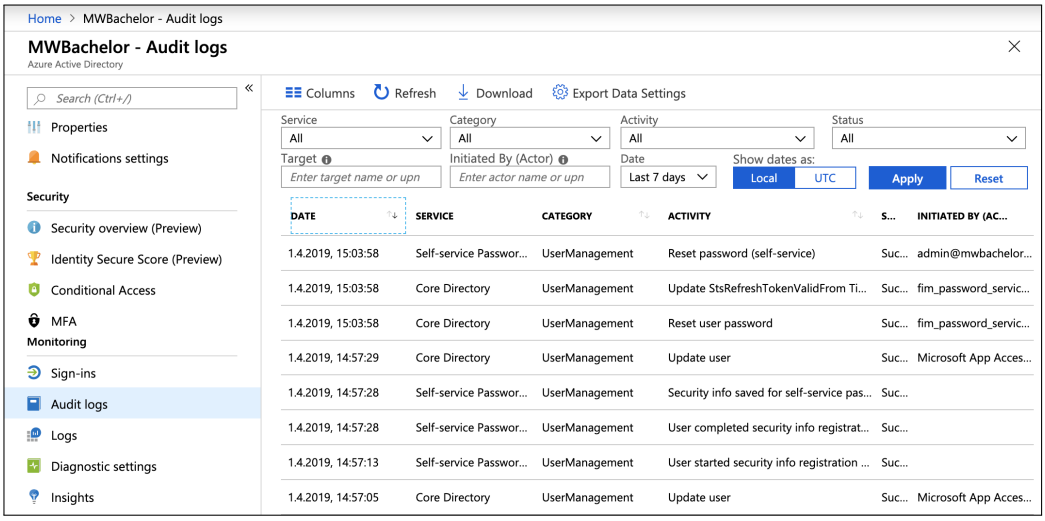
Figur 55

Tilbake i Intune på "On-premises integration" menyen hos "Passord reset" kan det bekreftes at on-prem klienten er oppe og kjører, som på figur 56.



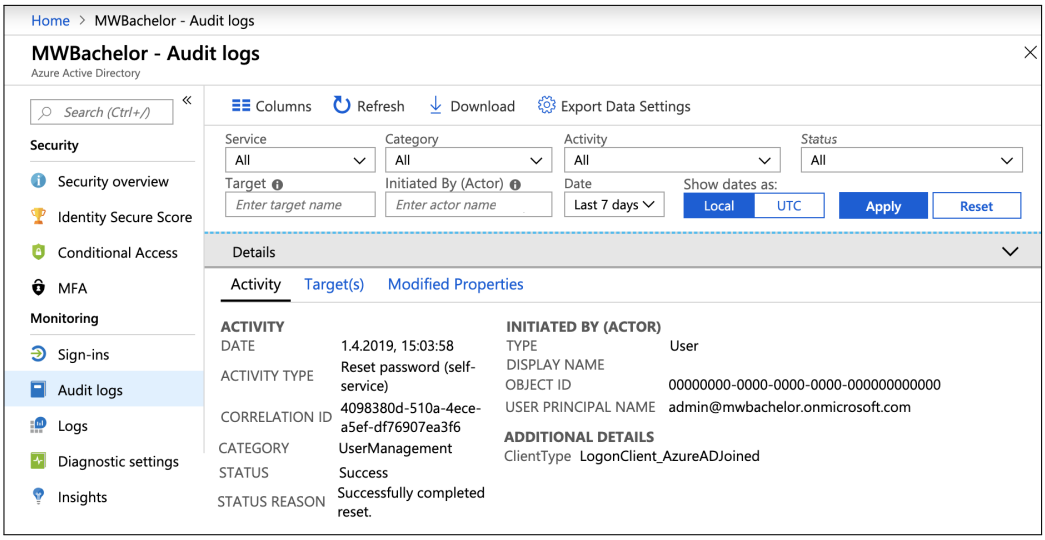
Figur 56

Tilbakestillinger av passord vil loggføres i "Audit logs" i AAD tenanten.



Figur 57

Detaljene for en tilbakestilling av et passord vises i figur 58.



Figur 58

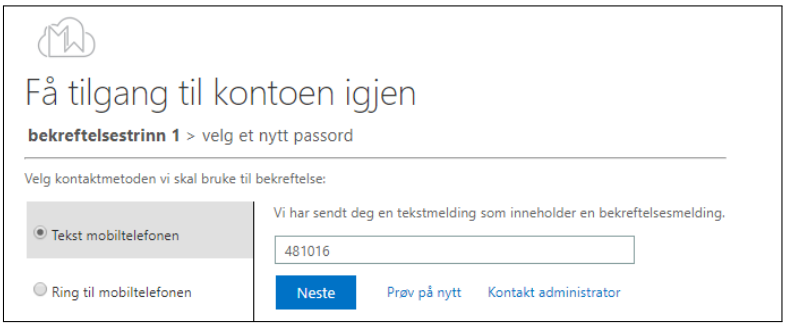
4.2 Test i sky

Hvis en bruker har registrert seg for tilbakestilling av passord vil dette være mulig på `https://aka.ms/sspr`.

Først må brukeren oppgi bruker-ID og en reCAPTCHA, se figur 59.

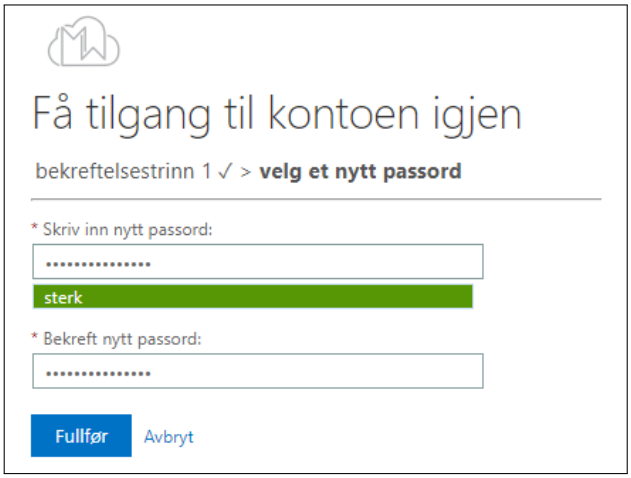
Figur 59

Så må brukeren verifisere seg med registrert metode. SMS benyttes til verifisering i figur 60.



Figur 60

Så får brukeren velge et nytt passord, se figur 61.



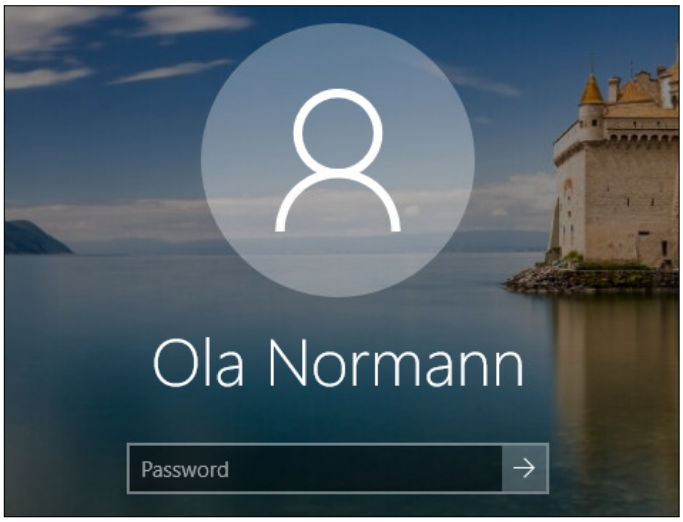
Figur 61

Deretter vil det nye passordet synkroniseres tilbake til lokale AD.

Figur 62

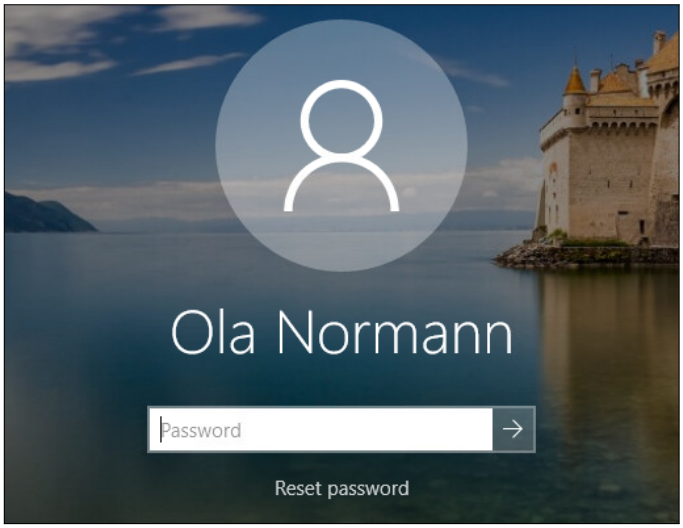
4.3 Test i Windows 10

Før SSPR er aktivert vil innloggingsskjermen se ut som på figur 63.



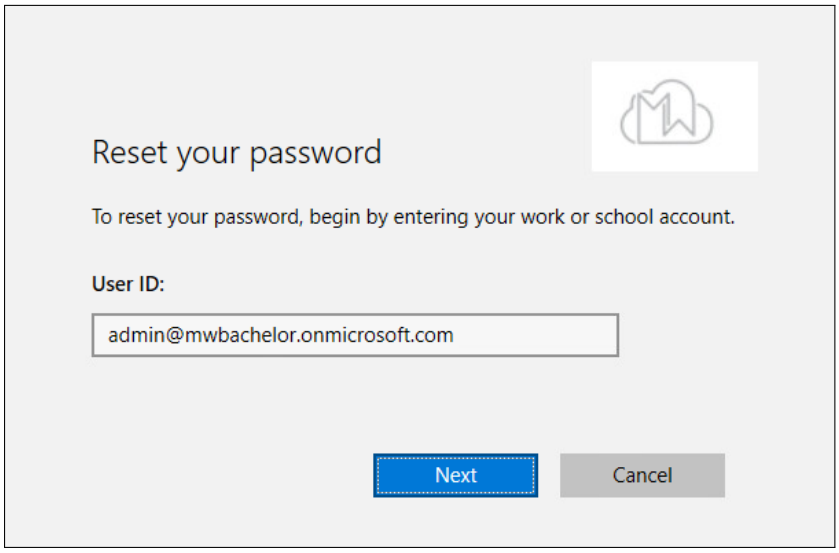
Figur 63

Når maskinen har mottatt den nye enhetskonfigurasjonen med SSPR vil skjermen se ut som på figur 64. Ved å trykke på "Reset password" vil det dukke opp et vindu.



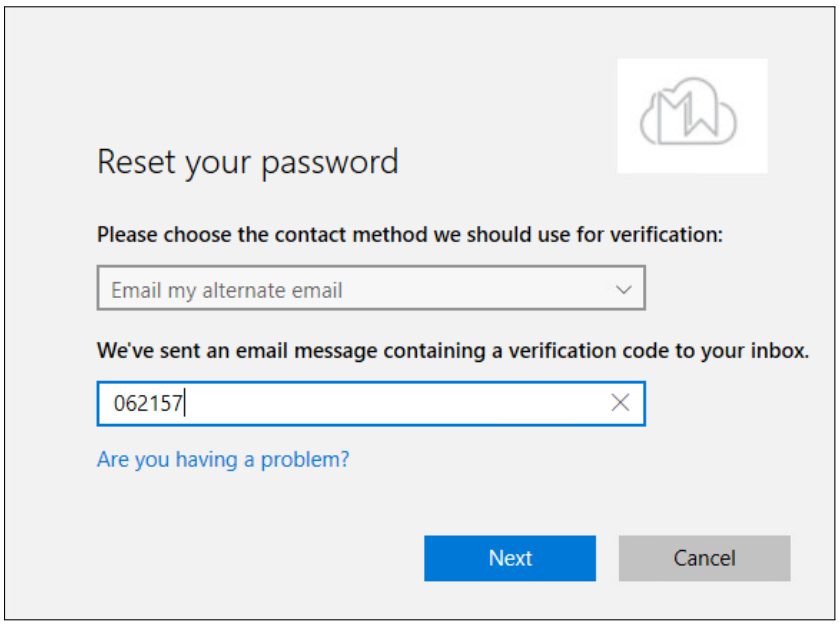
Figur 64

I vinduet på figur 65 må bruker-ID oppgis.



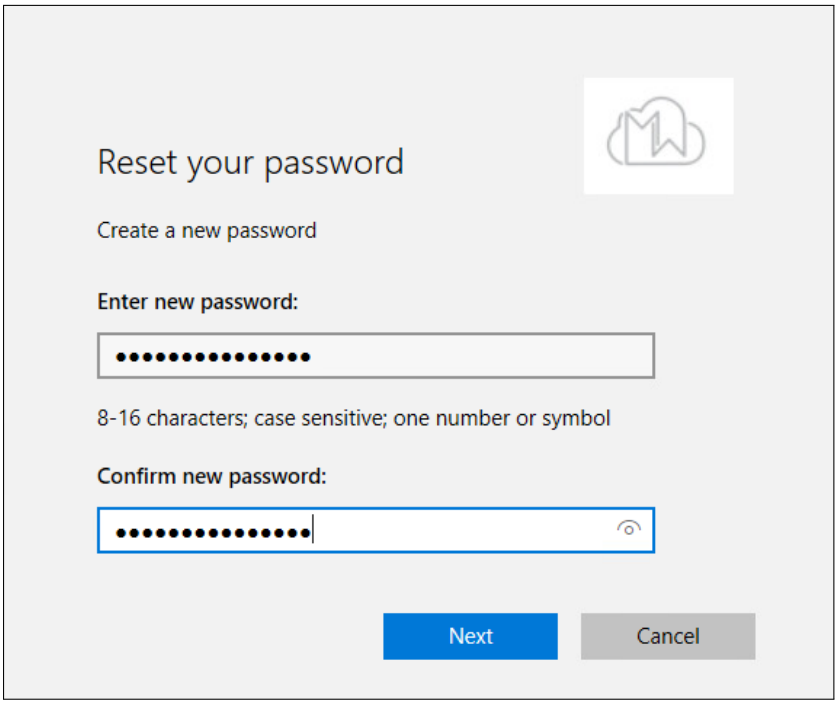
Figur 65

Brukeres må autentisere seg med valgt metode som vist i figur 66.



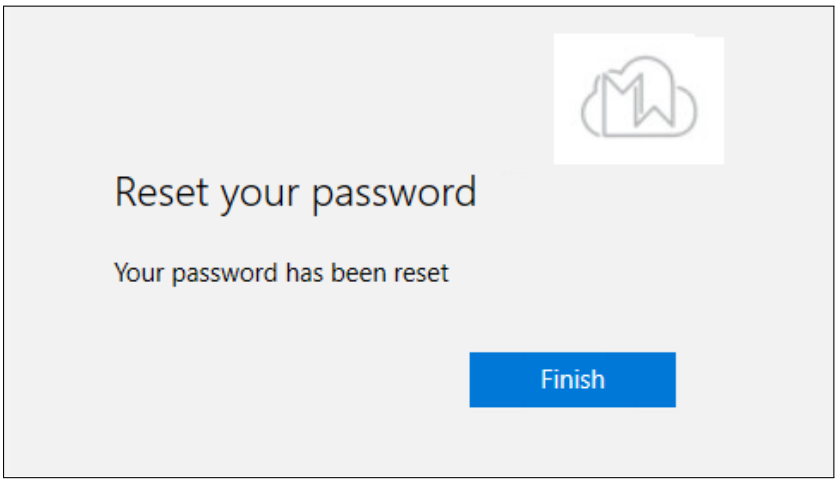
Figur 66

Deretter får brukeren sette nytt passord.



Figur 67

Passordet sendes til lokal AD, en hash genereres og denne sendes til Azure AD. Brukeren vil så få en bekreftelse på at passordet har blitt tilbakestilt.



Figur 68

Referanser

[1] Microsoft. *What is hybrid identity?* 2018. URL: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity (sjekket 01.05.2019).

[2] Microsoft. *Prerequisites for Azure AD Connect*. 2018. URL: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites (sjekket 01.05.2019).

[3] Microsoft. *Custom installation of Azure AD Connect*. 2019. URL: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom (sjekket 01.05.2019).

[4] Microsoft. *Azure Active Directory Seamless Single Sign-On: Quick start*. 2019. URL: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start (sjekket 01.05.2019).

[5] Microsoft. *Tutorial: Complete an Azure AD self-service password reset pilot roll out*. 2018. URL: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-sspr-pilot (sjekket 01.05.2019).

[6] Microsoft. *Use enforced registration*. 2018. URL: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment#use-enforced-registration (sjekket 01.05.2019).

[7] Microsoft. *Tutorial: Enabling password writeback*. 2018. URL: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-writeback (sjekket 01.05.2019).

[8] Microsoft. *Tutorial: Azure AD password reset from the login screen*. 2019. URL: https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-sspr-windows (sjekket 01.05.2019).

Modern Workspace - Driftsdokument
Device Enrollment

v.0.8

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
10.04.2019	0.1	Opprettet dokumentet. Påbegynt iOS enrollment, figurer lagt til
11.04.2019	0.2	Påbegynt Android enrollment, figurer lagt til, innholdsfortegnelse oppdatert
12.04.2019	0.3	Introduksjon skrevet
18.04.2019	0.4	Oppdatert noen figurer for android enrollment og revidert noen figurtekster
23.04.2019	0.5	Revidert Android introduksjon. Skrevet Apple CERT, android enterprise og unenroll/wipe
24.04.2019	0.6	Lagt til Windows 10 enrollment, revidert tekst i første del av dokumentet
25.04.2019	0.7	Revidert tekst for iOS, Android og Windows 10
06.05.2019	0.8	Mindre revisjon av tekst, retting av grammatiske og språklige feil

Innhold

1 Introduksjon

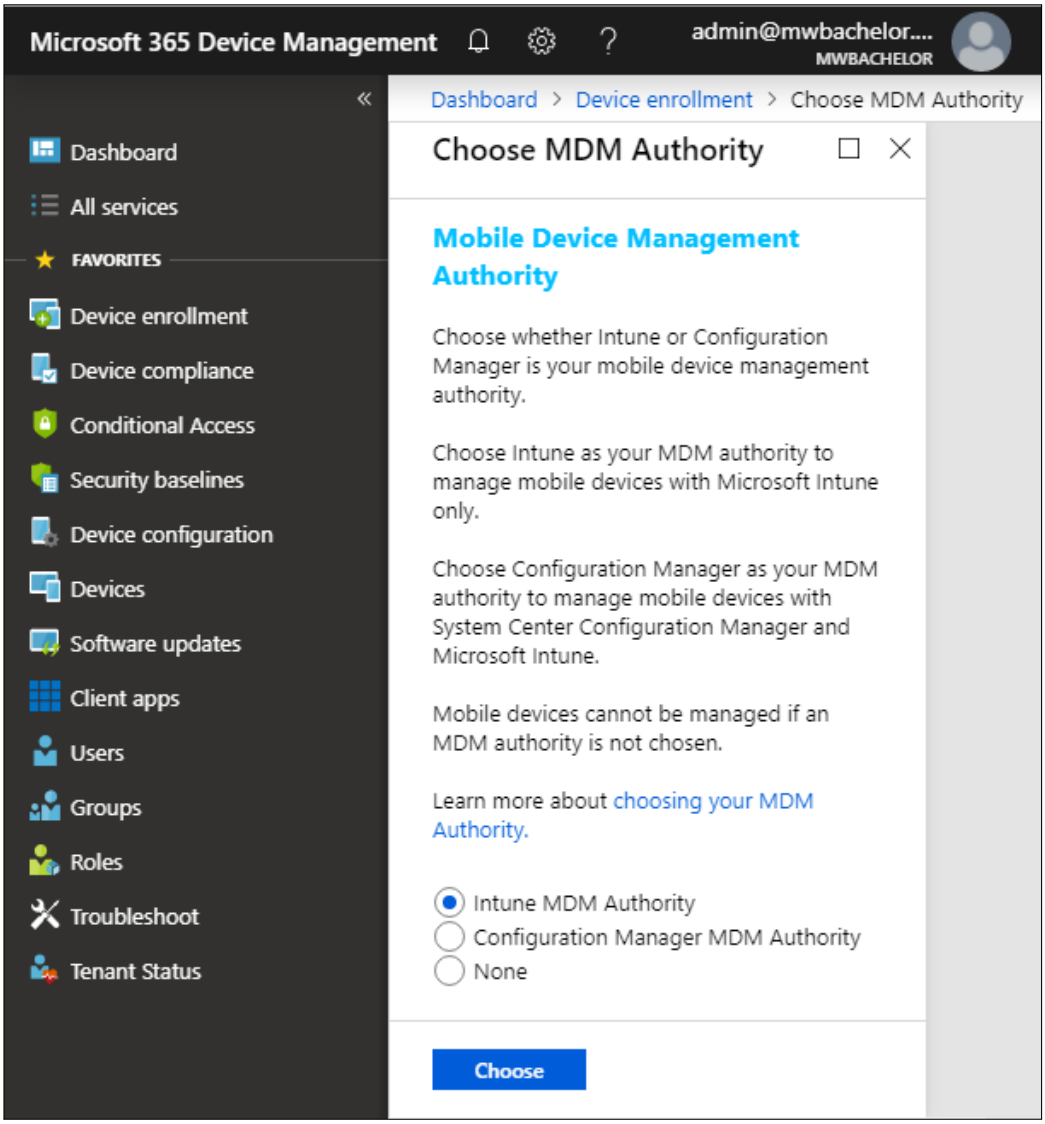
Enhetsregistrering, også kjent som enrollment, lar bedriften administrere brukernes enheter, applikasjoner og hvordan brukere kan behandle bedriftens data. Dette betyr at bedriften kan, blant annet, følge med enhetene, legge inn applikasjoner som brukerne kan benytte, sikre de mot fysiske og digitale trusler, sette krav til hvordan enheten skal benyttes og slette innhold på enheten dersom enheten blir stjålet eller skal pensjoneres.

Det skilles som regel mellom to ulike typer registreringer, personlig og bedriftsregistrering. Ved personlig registrering kan brukerne selv velge enheten de ønsker å jobbe på, og få tilgang på bedriftsdata og applikasjoner på denne. Bedriftseide enheter leveres ferdig oppsatt slik at enheten er registrert allerede før brukeren har åpnet esken den leveres i. Alt brukeren behøver å gjøre for å ta i bruk enheten, er å logge inn med sin bedriftskonto.

Vi vil i dette dokumentet gå gjennom prosessen som gjennomgås for å melde inn enheter i Intune. Alle stegene som tas vil beskrives med tekst og støttende figurer. Dette gjøres slik at leser kan få en grundig innføring i prosessen, samt at en vil få mulighet til å gjenskape våre resultater.

2 Device enrollment - Førstegangsoppsett

Første gangen man navigerer til "Device enrollment" i Intune vil det dukke opp et vindu som det i figur 1. Her velger man hvem som skal ha hovedansvaret for enhetene som registreres. Siden dette miljøet skal administreres ifra Intune i Azure, velges "Intune MDM Authority".



Figur 1: Valg av MDM autoritet

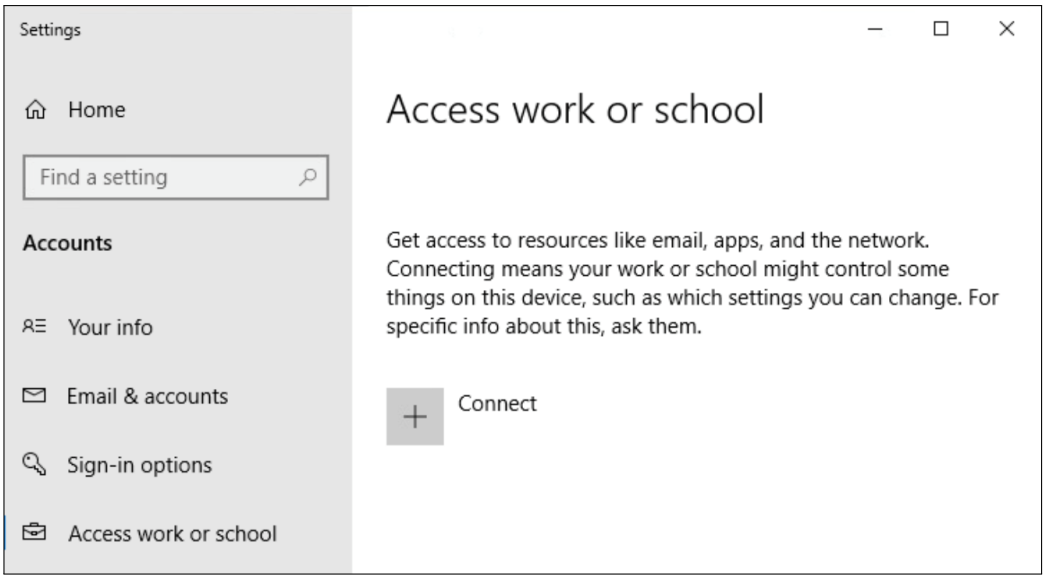
3 Windows 10

Windows 10 kan registreres i Intune på to ulike måter, personlig og bedriftsregistrering. Personlig registrering legger opp for BYOD, slik at brukerne kan ta i bruk sin personlige datamaskin og jobbe med bedriftseide data og applikasjoner på denne. Bedriftsregistrerte enheter låses til bedriften, og vil ikke la brukere fjerne registreringen fra maskinen. Vi vil gå gjennom begge metodene for registrering, men det er verdt å nevne at registrering gjennom autopilot blir beskrevet i "Driftsdokument - Autopilot".

3.1 Enrollment – Personal

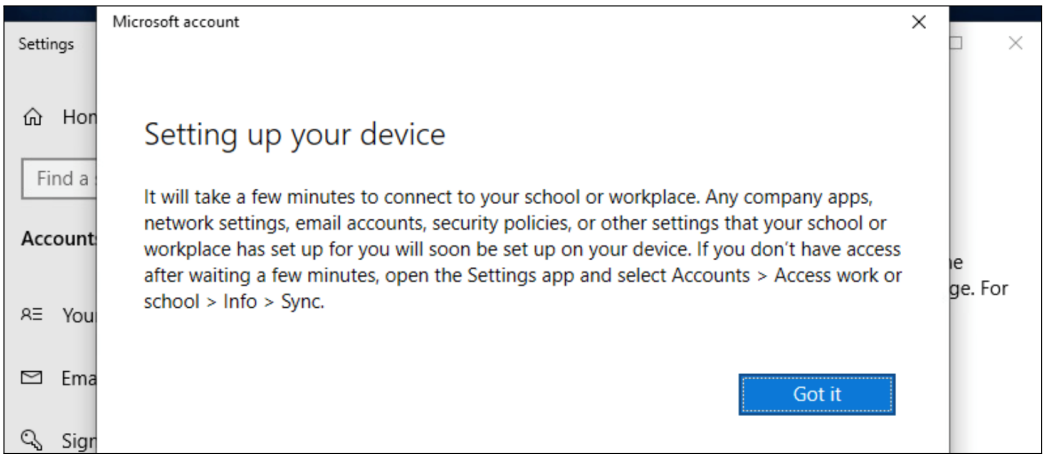
Dersom brukere ønsker å benytte egne maskiner vil dette være mulig gjennom en personlig registrering. Dette gjør at brukerne kan få tilgang på sine bedriftsdata på sin egen maskin, samtidig som brukeren selv kan velge å fjerne registreringen etter eget skjønn.

For å enrolle sin egen PC trenger man bare legge til arbeidskontoen i Windows 10 innstillingene. Åpne maskinens innstillingers "Settings", så naviger til "Accounts" og "Access work or school". Der vil det være en knapp for å legge til en ny arbeidskonto, trykk på "Connect".



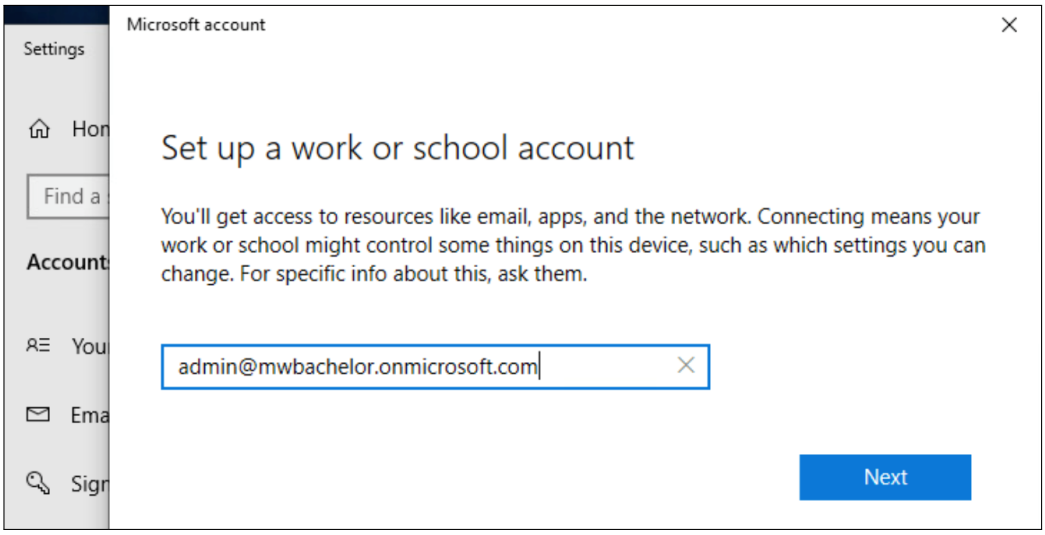
Figur 2

Dette vil starte en veiviser som forteller kort om prosessen. Det kan være lurt å lese for å forstå hva som inngår i en slik registrering. Velg “Got it” for å gå videre.



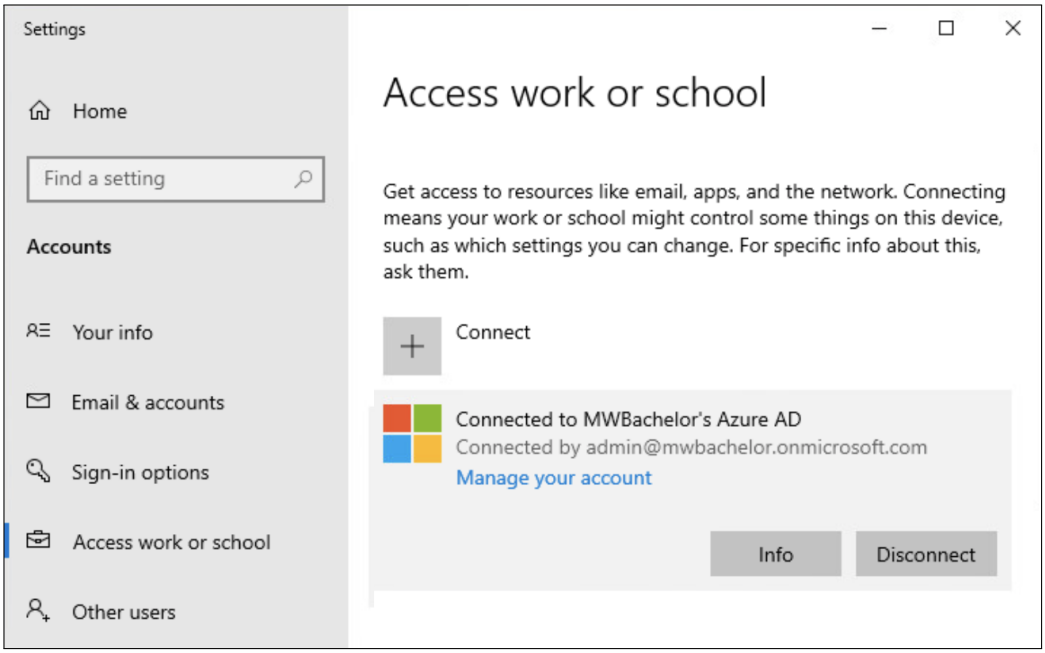
Figur 3

Du vil så måtte oppgi brukernavn og passord for arbeidskontoen. Gå videre ved å trykke på “Next”.



Figur 4

Maskinen vil etter en kort stund være registrert i Intune. Applikasjoner og policies vil nå synkroniseres til maskinen, og bedriftsdata vil nå kunne aksesseres. Med denne måten for registrering har man også muligheten til å koble seg fra Intune ved å trykke "Disconnect", som vi kan se i figur 5.

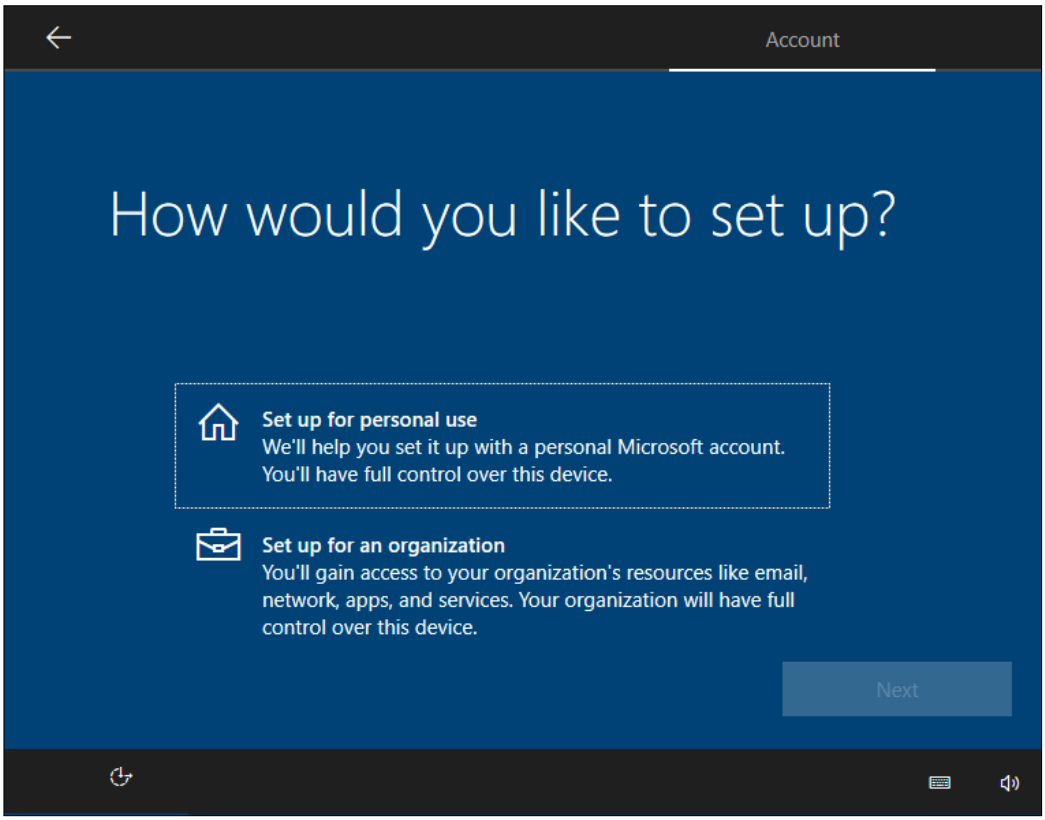


Figur 5

3.2 Enroll – Corporate

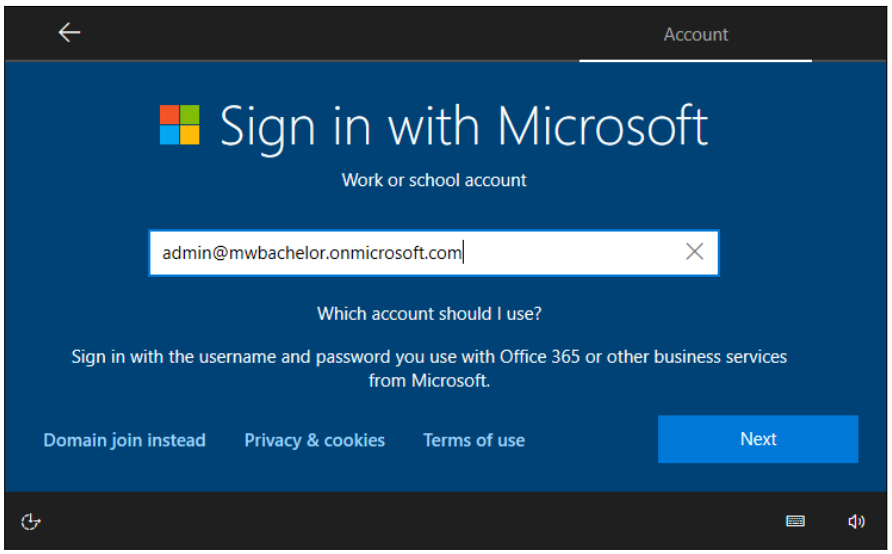
Bedriftsregistrerte enheter vil knyttes opp til Intune før en oppretter en personlig bruker på maskinen. Registreringer gjennom bedrift kan enten gjøres manuelt gjennom OOBE eller ved bruk av Autopilot. Autopilot kan sette opp maskinene til ønsket tilstand uten at de har være innom IT-avdelingen. Autopilot omtales i "Driftsdokument - Autopilot".

For manuelt oppsett av nye enheter vil det bare være å kjøre gjennom OOBE. Ved første valg i OOBE må det velges å sette opp enheten for en organisasjon. Klikk her "Set up for an organization".



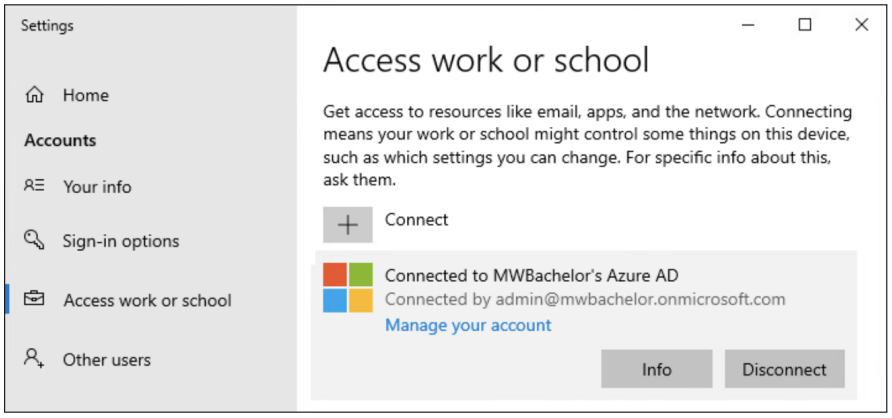
Figur 6

Du vil så bli bedt om å logge inn med din arbeidskonto. Trykk her “Next” for å komme videre.



Figur 7

Resten av OOBE vil inneholde tradisjonelle spørsmål om annonser, sporing og andre Microsoft relaterte spørsmål. Når OOBE er ferdig vil arbeidskontoen være lagt inn i Windows 10 innstillingene, og er å finne i Intune. Dermed vil applikasjoner og policies bli tilgjengelig for enheten. Som vi ser i figur 8, er maskinen koblet opp mot Azure AD.



Figur 8

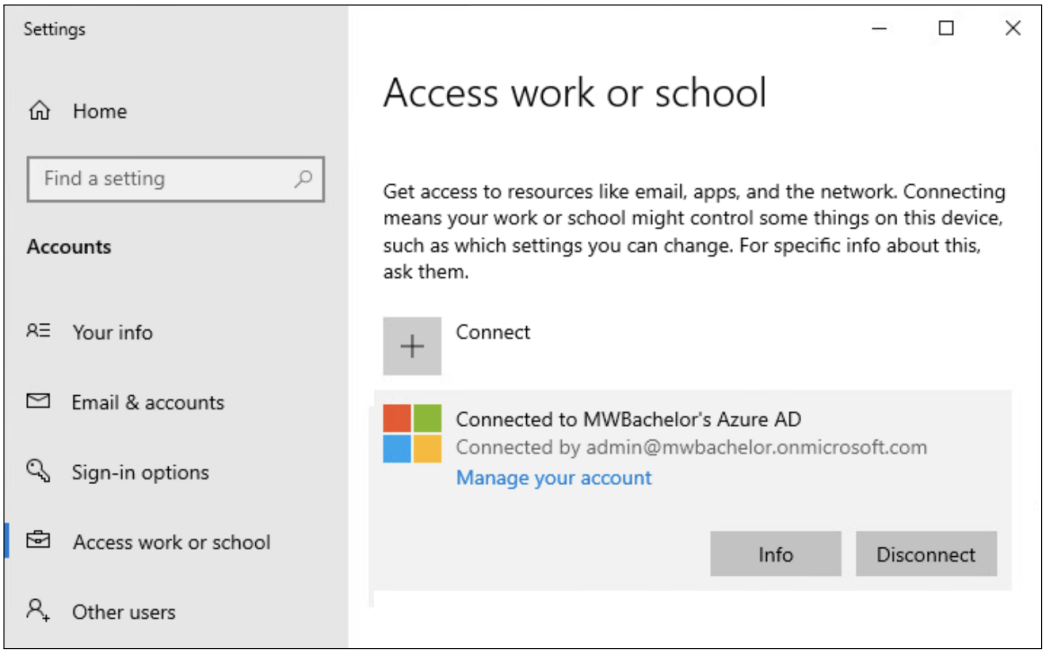
3.3 Unenroll

Dersom en maskin ikke lengre skal administreres av Intune, må den avregisteres, også kjent som "unenroll". Det finnes ulike grunner til å gjøre nettopp dette, som å fjerne gamle maskiner som ikke er i bruk eller dersom en ansatt ikke vil ha sin personlige enhet administrert lengre.

For å unenrolle en maskin som allerede er registrert i Intune, må en navigere til samme sted som en legger til arbeidskontoen. Åpne Windows 10 innstillingene "Settings", velg "Accounts" og "Access work or school". Her vil arbeidskontoen ligge. Ved å klikke på kontoen skal det dukke opp en knapp med teksten "Disconnect". Ved å klikke på denne vil prosessen med å unenrolle enheten starte.

Hvis det ikke er noen slik knapp må eieren av enheten ta kontakt med IT-avdelingen og få de til å fjerne enheten fra Intuneportalen. I Intuneportalen kan administrasjonen fjerne alle enheter fra Intune.

På figur 9 vises en registrert maskin med "Disconnect"-knappen.



Figur 9: Mulighet for å melde maskinen ut

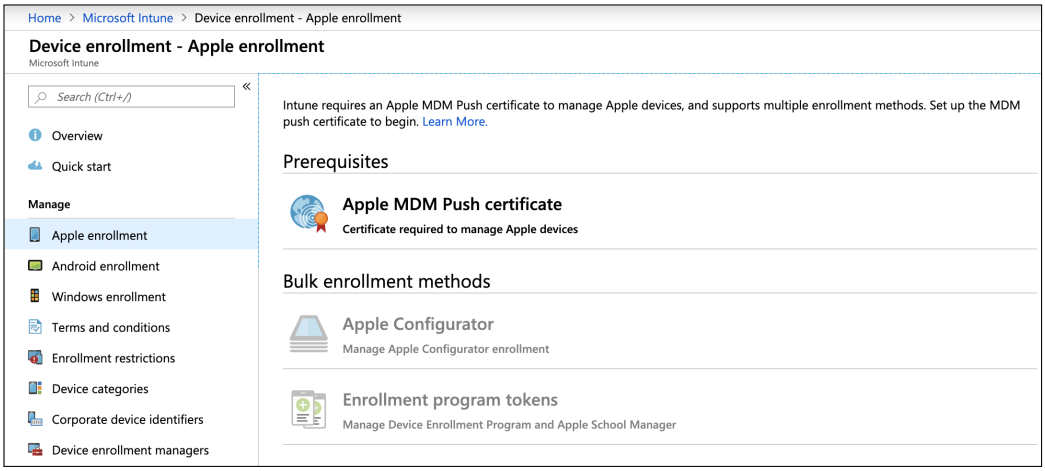
4 iOS

Enrollment for iOS-enheter kan foregå på to ulike måter, automatisk på bedriftsenheter og manuelt på personlige enheter. Automatisk enrollment på iOS-enheter krever at man arbeider gjennom Apple DEP, hvor enheter er koblet opp mot bedriften før den leveres til brukerne. Det vil ikke være mulig for prosjektet å ta for seg en enrollment gjennom Apple DEP, og derfor vil kun personlig enrollment dokumenteres.

4.1 Apple CERT

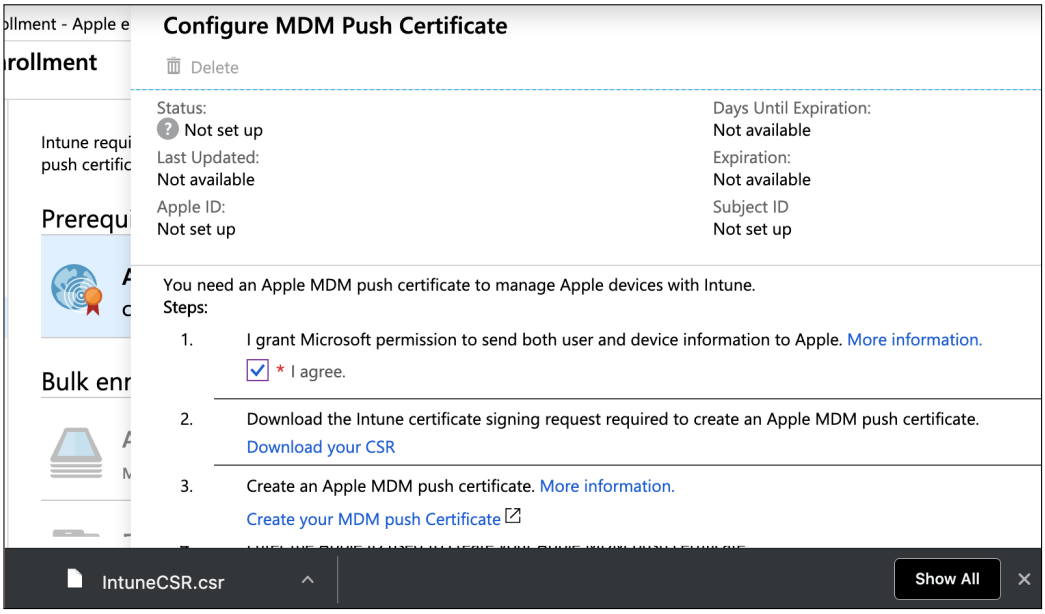
For at Apple-enheter skal kunne administreres av Intune må det opprettes et sertifikat hos Apple[1], som lastes opp til Intune. Dette sertifikatet kan Intune sende videre til enhetene som skal registrere seg.

I Azure-portalen navigeres det til “Intune”, “Device enrollment” og “Apple enrollment”. I figur 10 er to av alternativene utilgjengelige før det er lastet opp et sertifikat. For å starte prosessen velges “Apple MDM Push certificate”.



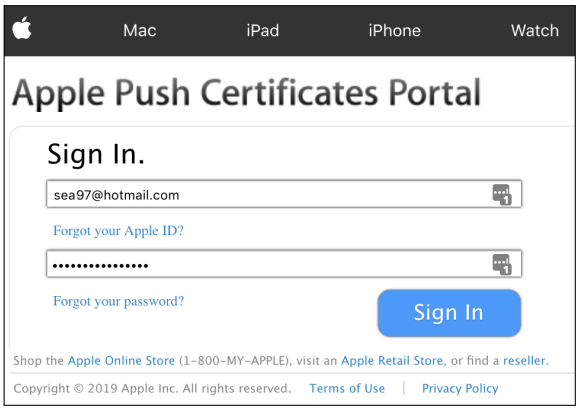
Figur 10

Det vil dukke opp et vindu der mye av informasjonen mangler. Huk av for å godta Microsofts tilganger og last ned Intunes signeringssertifikat, dette behøves senere. Trykk deretter på linken i steg 3, denne går til siden for å opprette et Apple-sertifikat.



Figur 11

Før sertifikatet kan opprettes må det logges inn hos Apple. En kan bruke en hvilken som helst Apple-konto, men det er viktig å huske hvilken Apple ID som benyttes her da den samme kontoen skal oppgis senere.



Figur 12

Etter innlogging vil en dirigeres til Apples "Push Certificate Portal", hvor det

være mulig å opprette et sertifikat. Sertifikatet opprettes ved å trykke på knappen "Create a Certificate", som vist i figur 13.

Figur 13

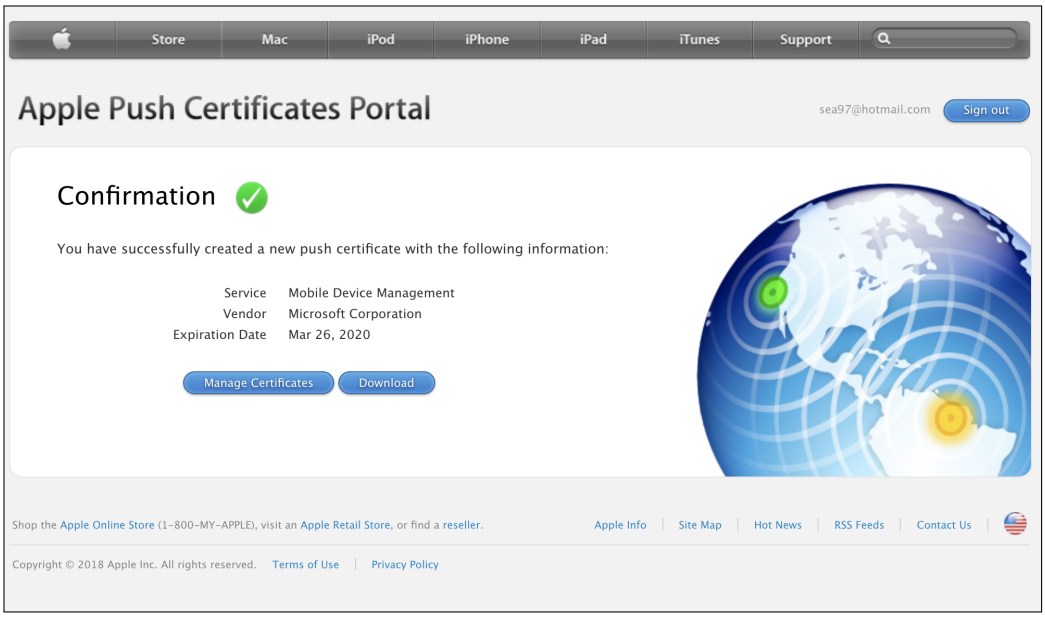
Apples bruksvilkår knyttet til sertifikatet vil så måtte godkjennes. Gå gjennom disse for å sikre at de stemmer overens med vilkårene til bedriften. Huk av for at vilkårene er lest og akseptert, og trykk så på "Accept", som vist i figur 14.

Figur 14

For å kunne opprette sertifikatet må en signatur fra Intune lastes opp til Apple. Dette er signerings-sertifikatet vi lastet ned fra Intune tidligere. Last opp dette ved å trykke “Choose file”, som vist i figur 15. Trykk så på “Upload” for å laste opp signeringen.

Figur 15

Sertifikatet vil så opprettes og dersom alt gikk greit vil du få en bekreftelses-notifikasjon. Som vi ser i figur 16, kan en nå laste ned sertifikatet ved å klikke "Download". Her kan en også administrere andre sertifikater dersom ved å klikke på "Manage Certificates".

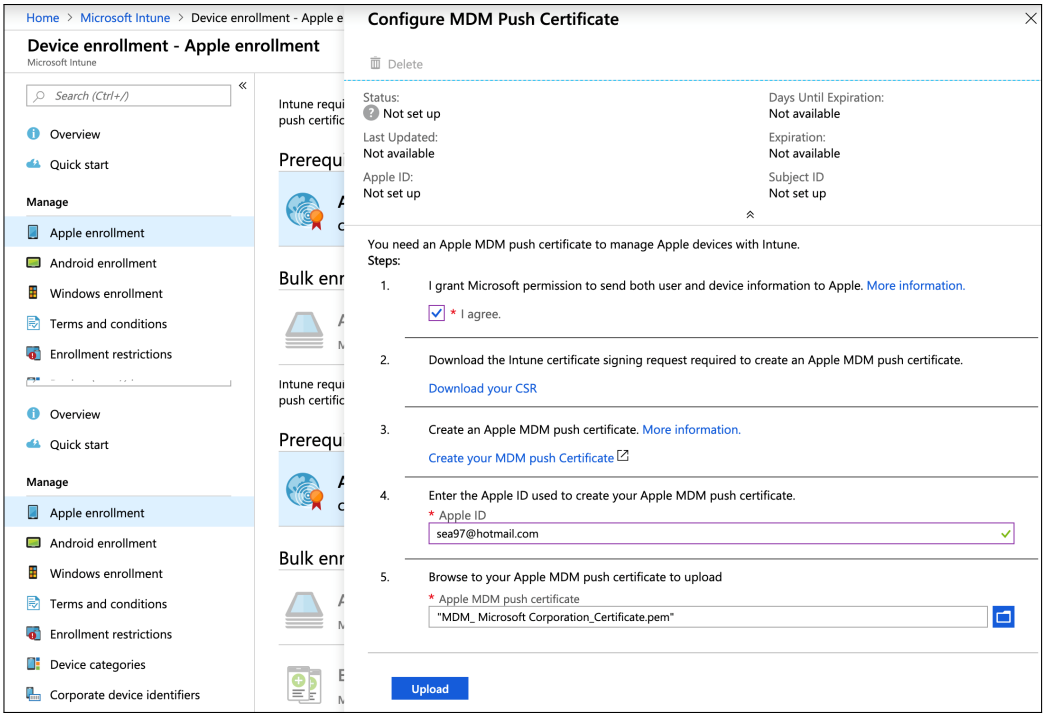


Figur 16

I figur 17 kan vi se en oversikt over alle sertifikatene og detaljer om disse. Vi har et aktivt sertifikat som varer til 2020, som kan fornyes, lastes ned eller tilbaketrekkes.

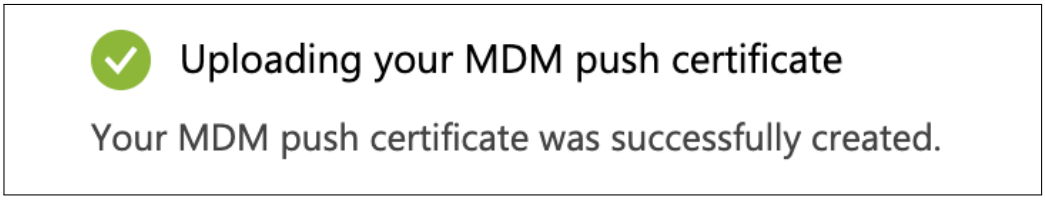
Figur 17

Tilbake i Intune må Apple Push sertifikatet lastes opp. I tillegg må den samme Apple ID-en som ble brukt under opprettelse av sertifikatet skrives inn. Skriv inn Apple-ID under “Apple-ID” og last opp sertifikatet under “Apple MDM push certificate” ved å klikke på mappe-ikonet. Nå kan en trykke på knapp for “Upload”, som vist i figur 18, for å opprette sertifikatet.



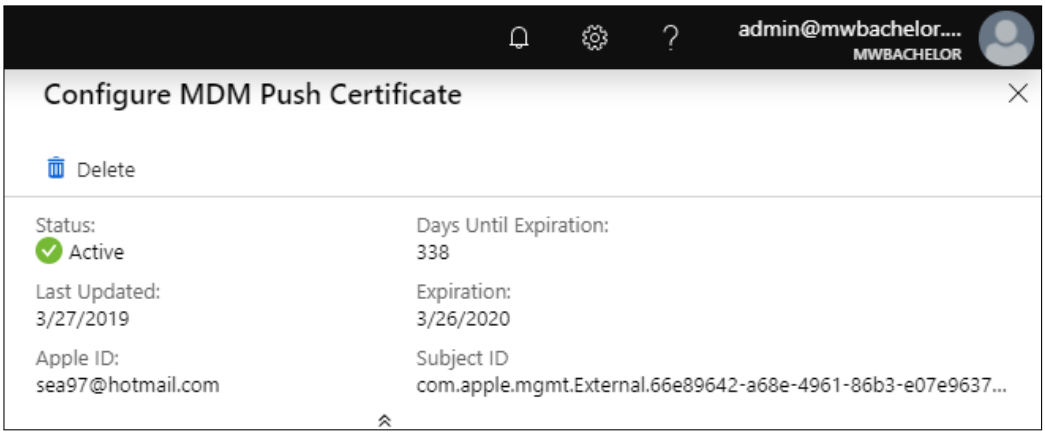
Figur 18

Det vil så dukke opp en notifikasjon som informerer om opplastning av sertifikatet var vellykket eller om noe gikk galt. Som vi ser i figur 19, gikk opplastning feilfritt i vårt tilfelle.



Figur 19

Som vi ser i figur 20, er sertifikatet aktivt. Vi kan også se når det sist ble oppdatert, hvilken Apple-ID som er i bruk og når sertifikatet utgår.

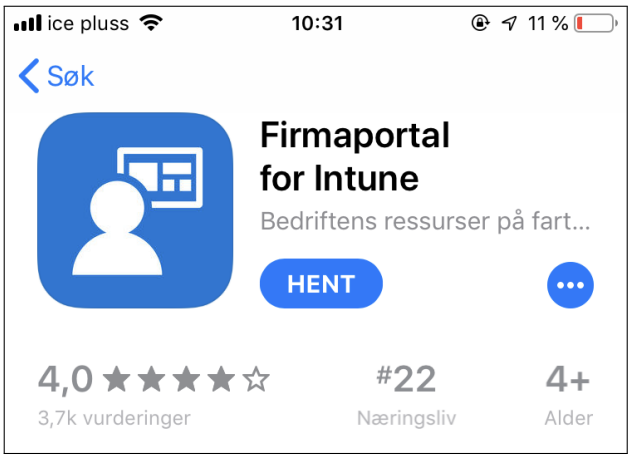


Figur 20

4.2 Enroll – Personal

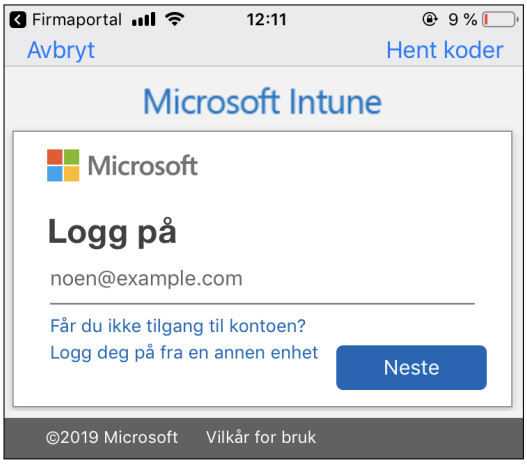
En personlig enrollment til Intune på Apple-enheter krever en del manuelt arbeid for brukeren. Det er anbefalt at brukere slipper denne prosessen, men dersom bedriften ikke har en avtale med Apple og ansatte ønsker iOS-enheter, vil dette være eneste måte å administrere enhetene dere.

Første steg vil være å installere Firmaportal for Intune (Company Portal) fra App Store på iOS-enheten. Trykk "Hent" for å starte nedlastingen.



Figur 21

Når nedlastingen er ferdig kan en åpne Firmaportal-applikasjonen. Som vist i figur 22, blir en, inne i applikasjonen, bedt om å logge inn med sin Microsoft-konto. Fyll inn riktig informasjon og logg inn.



Figur 22

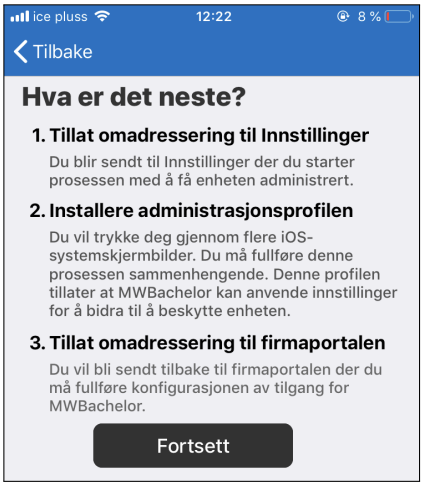
Firmaportalen vil så, som vi ser i figur 23, forklare gjenværende oppgaver for å få registrert enheten i Intune. Her kan vi også se domenet enheten vil registreres i, og det er viktig at dette stemmer overens med det ønskede domenet. Trykk "Start" for å starte registreringen.

Figur 23

Firmaportal-applikasjonen vil så forklare, som vi kan se i figur 24, konsekvensene for registrering i Intune, og hva som vil deles med Intune og ikke. Les gjennom slik at du er innforstått med dataene som vil deles og trykk “Fortsett”.

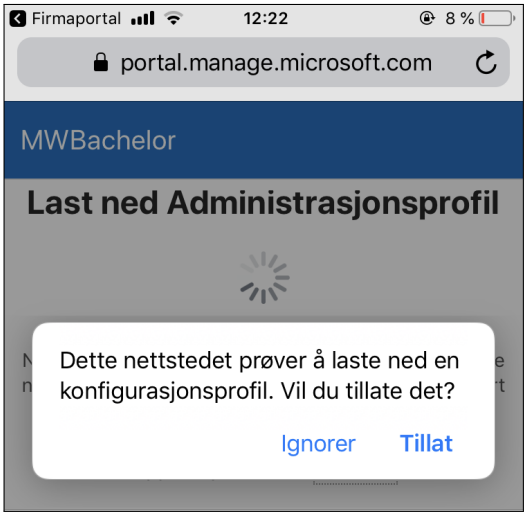
Figur 24

Deretter vil Firmaportal-applikasjonen beskrive stegene i registreringsprosessen. Prosessen starter med å installere en konfigurajsonsprofil på din iOS-enhet. Dette vil skje i systeminnstillingene, før brukeren vil returnere til Firmaportal-applikasjonen. Les nøye gjennom før du trykker “Fortsett”.



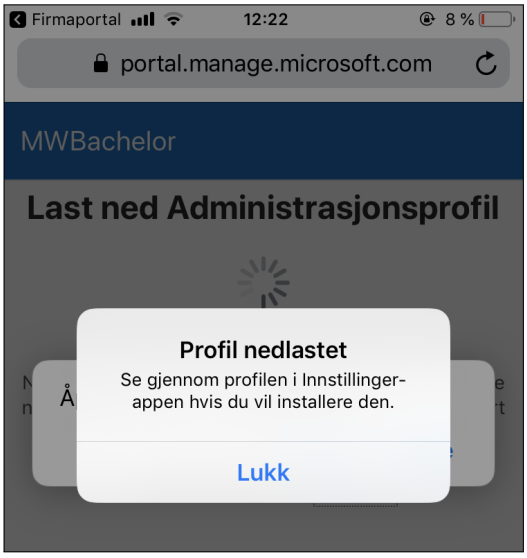
Figur 25

Firmaportal-applikasjonen vil så åpne nettleseren for å laste ned profilen. I nettleseren vil profilen bli forsøkt nedlastet, men det kreves her tillatelse fra brukeren. Trykk “Tillat” for å godkjenne nedlastingen.



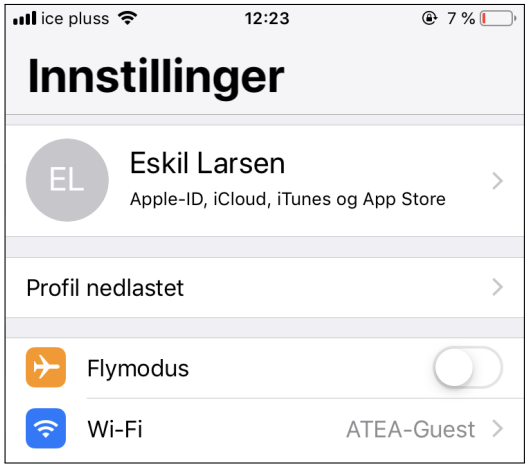
Figur 26

Når profilen er ferdig nedlastet vil det dukke opp et varsel som forklarer at du må bevege deg inn i “Innstillinger” på enheten for å fortsette installasjonen av profilen. Trykk “Lukk” og naviger der inn i “Innstillinger” på enheten.



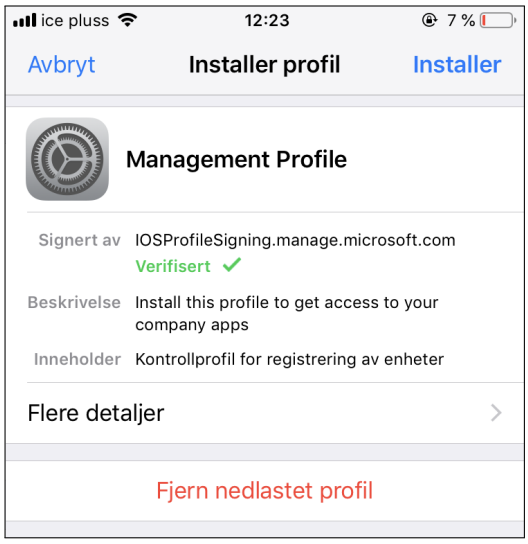
Figur 27

Som vi ser i figur 28, har det dukket opp en melding om at en profil er nedlastet. Profilen krever videre godkjenninger for å kunne installeres. Trykk på denne meldingen, “Profil nedlastet”, for å fortsette installasjonen.



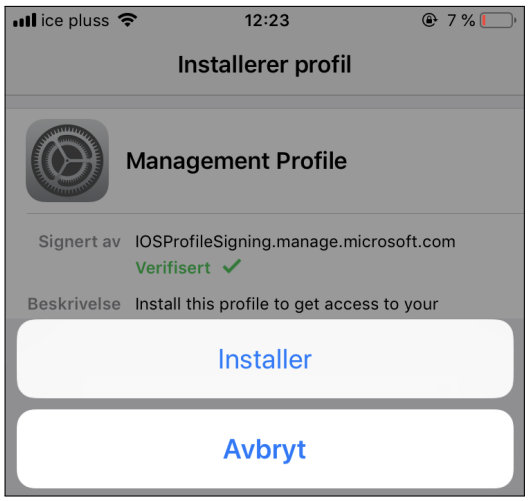
Figur 28

Det vil så komme en detaljert oversikt av profilen, som forklarer at profilen vil ha kontroll over bedriftseide applikasjoner på din enhet. Vi kan også, i figur 29, ser at profilen er signert av Microsoft og at den er verifisert. Pass på at profilen er riktig og klikk “Installer” oppe i høyre hjørne.



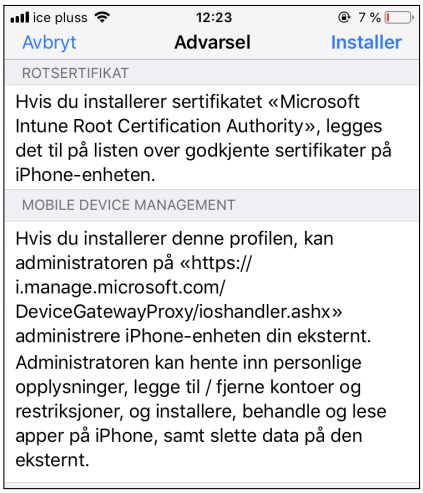
Figur 29

Det vil så dukke opp en liten bekreftelse på at du ønsker å installere profilen. Velg her “Installer” for å fortsette.



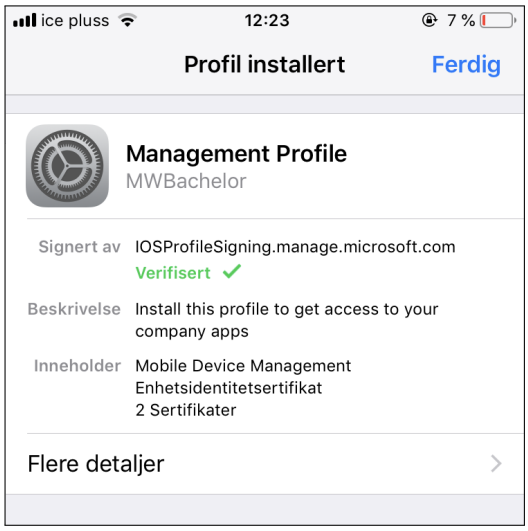
Figur 30

Enheten vil så gi en advarsel som forklarer konsekvensene av installasjonen av profilen. Det vil anbefales at dette gjennomgås slik at du er innforstått med hva som vil skje med enheten. Bekreft installasjon igjen ved å klikke “Installer”.



Figur 31

Profilen er nå ferdig installert. Klikk her “Ferdig” og du returner til Firmaportal-applikasjonen for fullføring av registreringen.

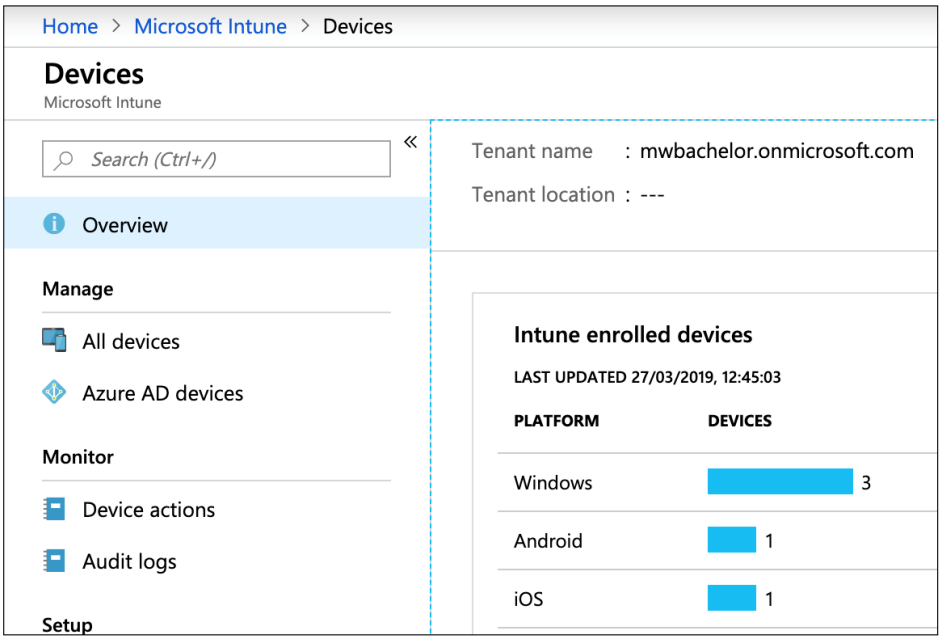


Figur 32

Firmaportal-applikasjonen vil sjekke at profilen er installert og gi feilmelding dersom det er mangler. Som vi ser i figur 33, gikk installasjonen feilfritt i vårt tilfelle. Trykk “Fullført” for å fullføre registreringen.

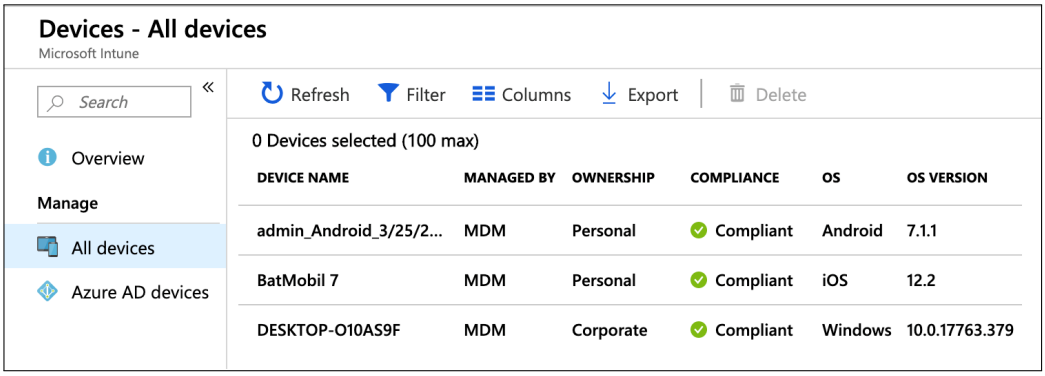
Figur 33

Går vi inn i Intune kan vi nå se at enheten har dukket opp i Intune. I figur 34 ser vi enheter som er registrert, hvorav en av disse er på plattformen iOS.



Figur 34

Som vist i figur 35, ser vi i listen over alle enheter, enheten "BatMobil 7". Vi kan også se at enheten er "Personal", noe som tilsier at enheten er BYOD fremfor en bedriftseid enhet. Vi får også se OS som er iOS, og hvilken versjon av OS enheten kjører på, som er 12.2.

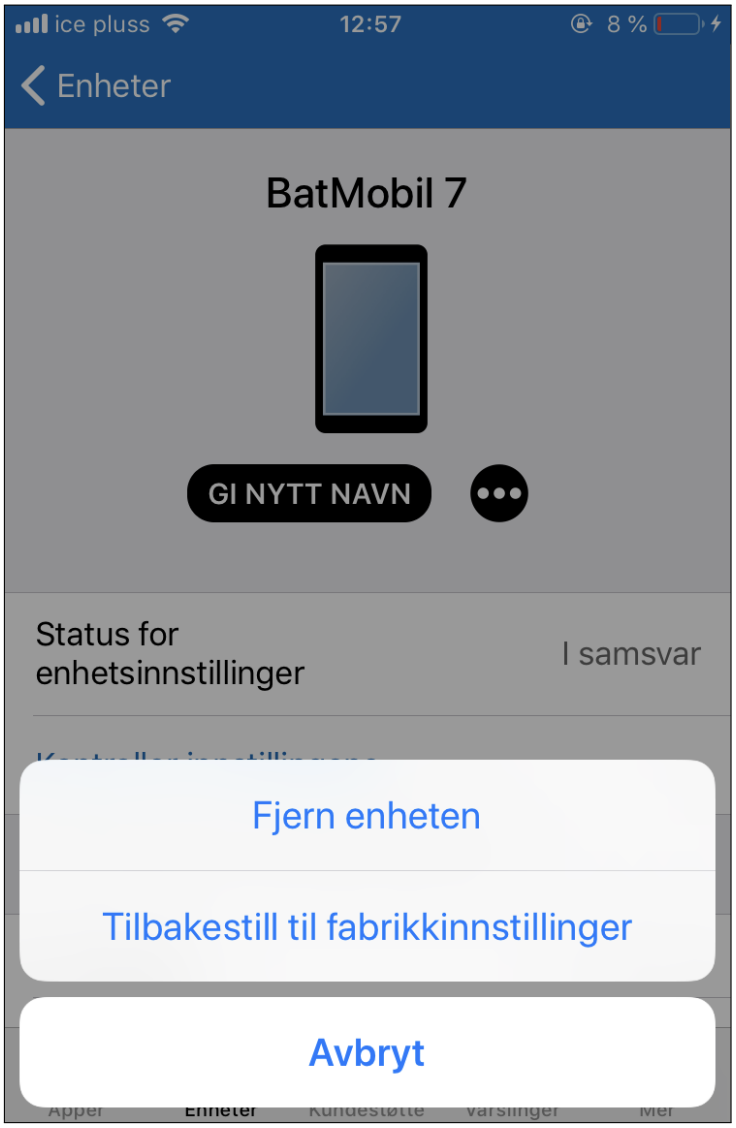


Figur 35

4.3 Unenroll

En bruker kan selv fjerne enheten sin fra Intune-administrasjon. Dette vil blant annet føre til at applikasjonene som er installert gjennom Firmaportalen (Company Portal) blir fjernet og du vil miste tilgang på bedriftsdata.

For å avregistrere enheten er det bare å åpne Firmaportal-applikasjonen og navigere til “Enheter”, klikke på ønsket enhet og deretter de tre prikkene ved “Gi nytt navn”-knappen. Dette åpner en ny meny, her kan enheten fjernes eller fullstendig tilbakestilles til fabrikkinnstillinger. Velg “Fjern enheten”.



Figur 36

Det vil dukke opp et varsel som forteller mer om hva som vil forsvinne fra enheten om den fjernes. Hvis brukeren er innforstått med dette er det bare å bekrefte ved å klikke “Fjern”.

Figur 37

Brukeren vil fremdeles være innlogget i applikasjonen, men enheten administreres ikke lengre av Intune. Vi kan se dette i figur 38, hvor det er kommet et nytt varsel som sier "Denne enheten er ikke administrert.".

Figur 38

Avregistreringen betyr at alle applikasjonene som ble installert via Firmaportal-applikasjonen (Company Portal) blir fjernet når enheten ikke lengre er registrert. Data knyttet til bedriften vil også være utilgjengelig som et resultat av avregistreringen.

5 Android

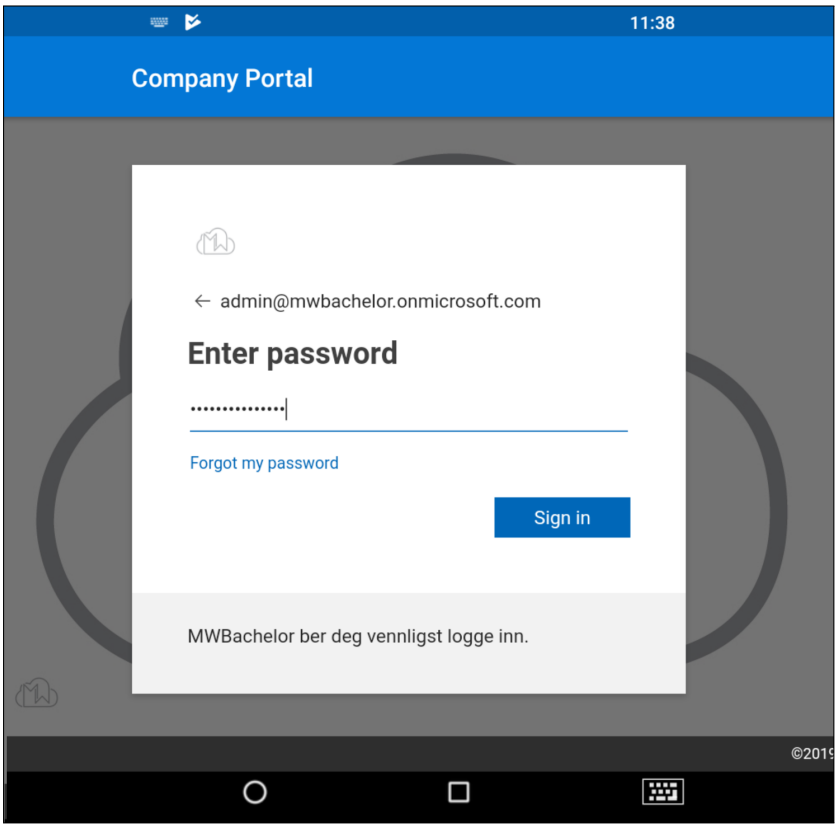
Enrollment av Android-enheter kan foregå på flere måter. Den tradisjonelle måten vil være svært lik prosessen på iOS, mens andre metoder vil være mer strømlinjeformet og enklere for sluttbruker.

Det er viktig å understreke at det ikke lengre anbefales å registrere enheter på den tradisjonelle måten, da det ansees både som en større sikkerhetsrisiko og som inkriminerede på personlig data hos sluttbruker. Dette er fordi den tradisjonelle måten å registrere Android-enheter på, har gitt Intune tilgang til nærmest hele telefonen, også personlig data. En nyere metode å registrere Android-enheter på er ved bruk av såkalte ”Work Profiles”. Denne metoden er sikrere og mindre inkriminerende angående brukers data, og er derfor anbefalt framfor andre metoder tilgjengelig. For å lese om Work Profiles se avsnitt 5.2.

5.1 Enroll – Personal via tradisjonell metode

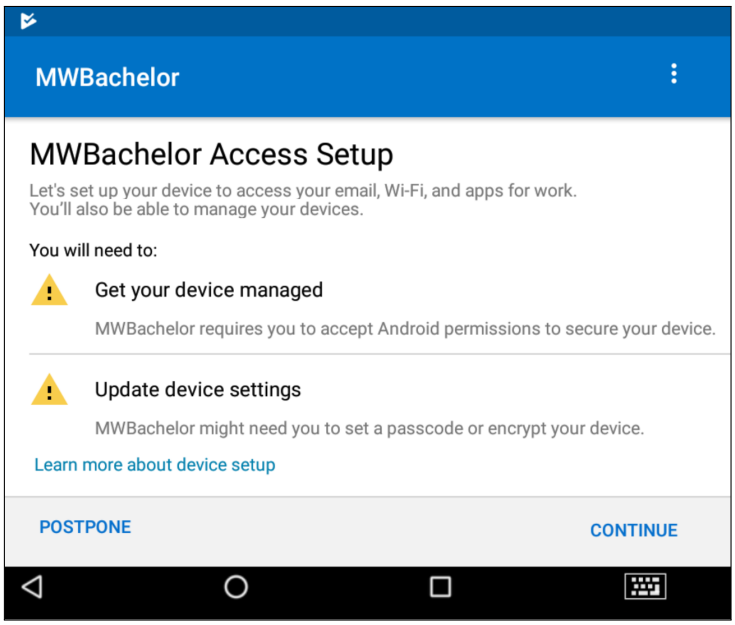
Igjen understrekes det at denne metoden ikke er anbefalt, men vi vil uansett dokumentere metoden da det er en mulighet. Denne metoden gjelder for BYOD-enheter og krever at brukere gjør en del selv for å få enheten registrert.

Første steg vil være å installere Firmaportal-applikasjonen ved navn “Company Portal” i Google Play Store. Når denne er installert kan en åpne applikasjonen. Her vil vi bli møtt av en innloggingside, som vist i figur 39. Fyll inn kontoinformasjonen og logg inn.



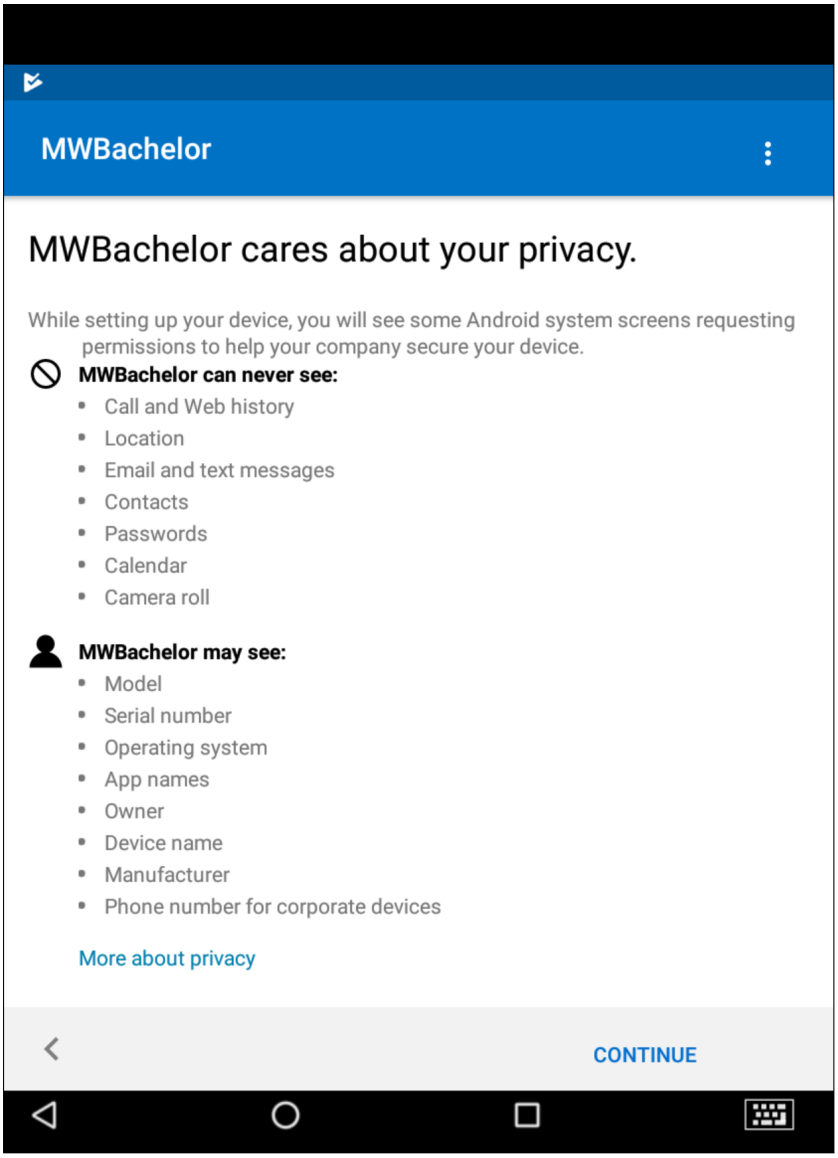
Figur 39

Applikasjonen vil laste inn informasjon om enheten og bruker vil få opp en liste over hva som gjenstår før enheten er registrert i Intune. Gjør deg kjent med punktene på denne listen før du trykker “Continue” for å starte registreringsprosessen.



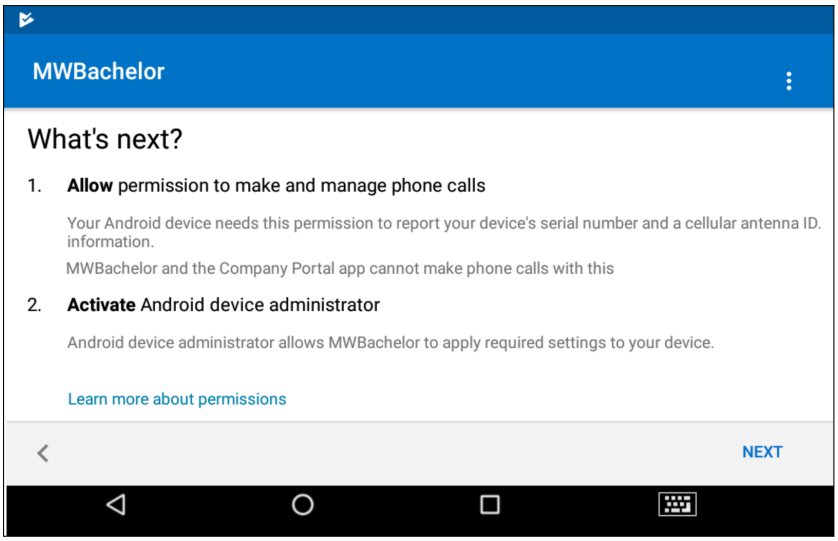
Figur 40

Du vil så bli informert om konsekvensene registrering i Intune vil ha, og hvilke data som deles med Intune. Som vi ser i figur 41, innebærer en slik registrering at Intune kun har tilgang på grunnleggende informasjon om enheten. Når du er innforstått med hvilke data som deles, kan du trykke “Continue” for å fortsette registreringen.



Figur 41

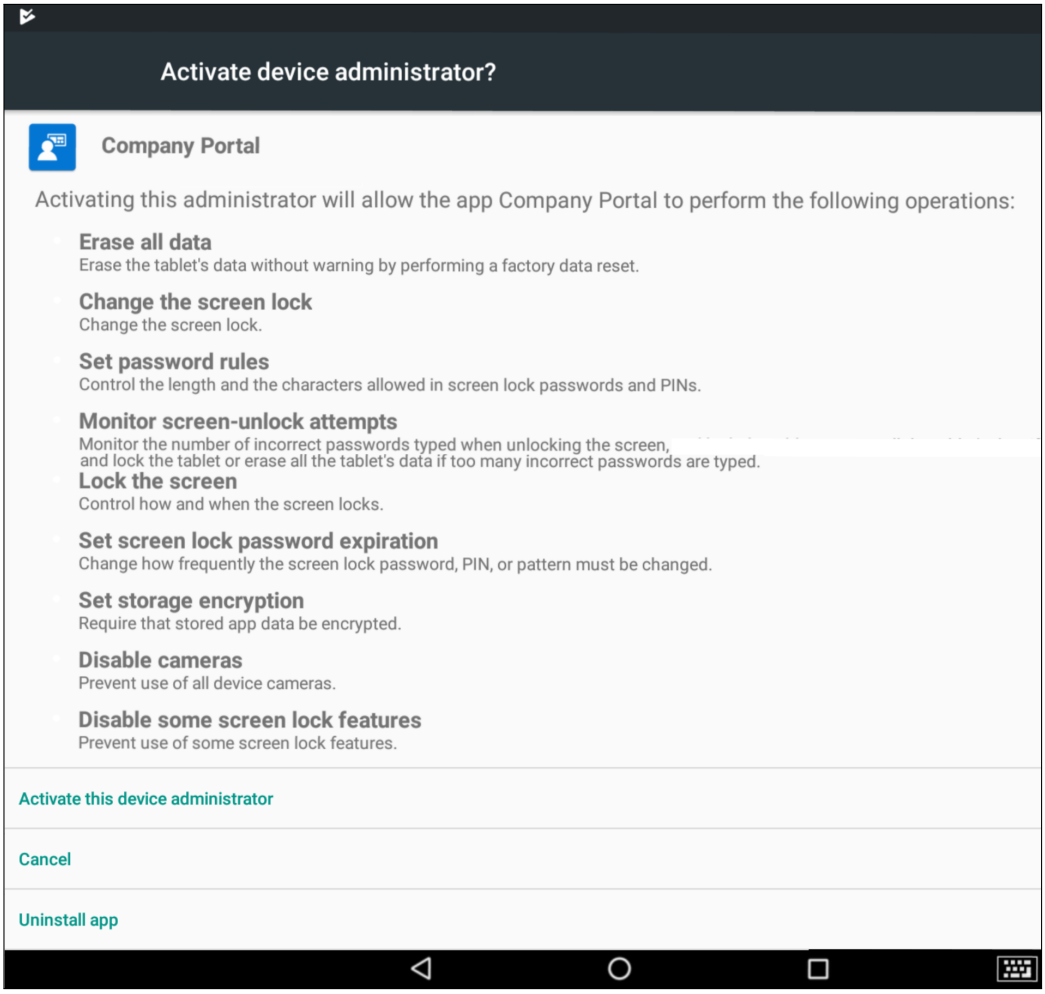
Du vil så bli bedt om å gi ytterligere tilganger, som å gi tilgang på utførelse og adminstrasjon av telefonsamtaler. Dette kreves for, som vi ser i figur 42, at enheten kan sende antenne-ID til Intune og applikasjonen vil ikke ringe eller motta telefonsamtaler på dine vegne. Dette er en av de store svakhetene til denne registreringsmetoden, og en av grunnene til at den ikke lengre anbefales. Trykk "Next" for å komme videre.



Figur 42

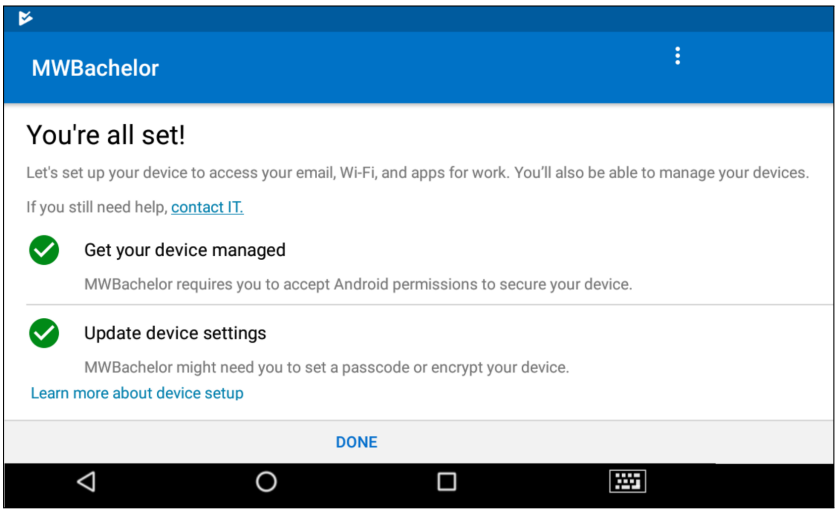
Deretter må enhets-administratortilganger aktiveres på enheten. Dette betyr at applikasjonen kan utføre en hel rekke administrasjonsoppgaver på enheten, som å slette all data, sette passordregler og låse skjermen. Disse rettighetene vises i sin helhet i figur 43.

Trykk deretter "Activate this device administrator" for å gi Firmaportal-applikasjonen tilgangene som kreves.



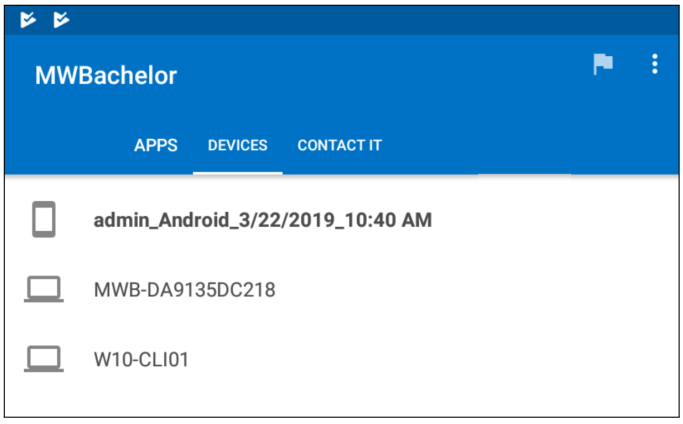
Figur 43

Firmaportal-applikasjonen vil så indikere om alt gikk bra under registreringen. Som vist i figur 44, gikk registreringen feilfritt i vårt tilfelle. Enheten vil nå være administrert av Intune.



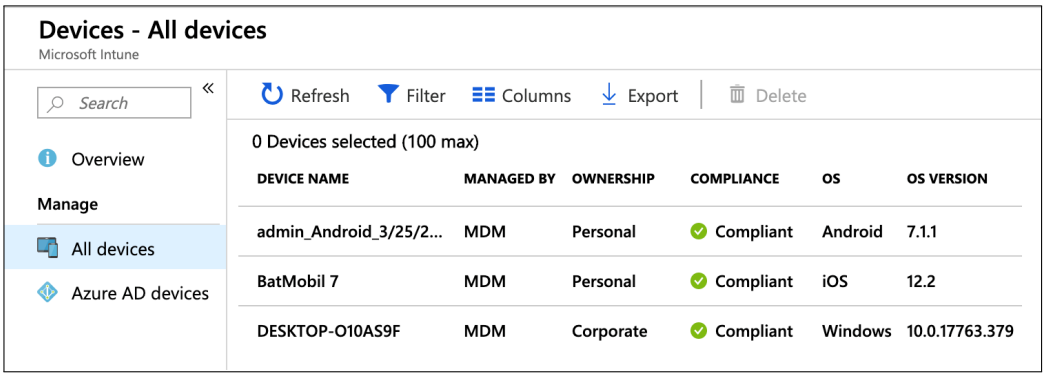
Figur 44

Gjennom selve applikasjonen har brukeren også muligheten til å se en liste over alle enhetene som er registrert på brukeren. Som vi ser i figur 45, er det registrert tre ulike enheter, hvorav to er datamaskiner og den siste er nåværende mobil enhet.



Figur 45

Går vi inn i enhetslisten i Intune, kan vi nå se at det har dukket opp en enhet med OS lik "Android", versjon 7.1.1 og eierskapet "Personal".



Figur 46

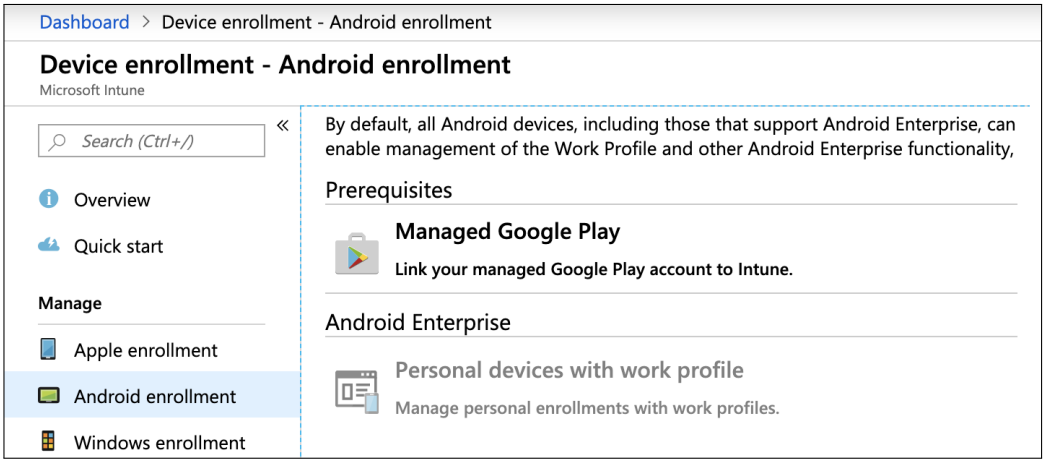
5.2 Enroll – Work Profile

Den tradisjonelle måten å registrere Android-enheter har gitt Intune tilgang til nærmest hele telefonen, også personlig data. Dette anses både som en sikkerhetsrisiko og som inkriminering på personlige data. En nyere metode å registrere Android-enheter er ved bruk av såkalte "Work Profiles"[2]. Dette kan sees på som et eget miljø som installeres inne på Android-enheten, og inne i dette miljøet vil alt som har med bedriften å gjøre legges. Dermed trenger Intune kun tilgang til det spesifikke miljøet og ikke hele enheten, som den tradisjonelle metoden krever. Det gjøre det også mulig å kreve ekstra sikkerhet når noen forsøker å få tilgang på miljøet som inneholder bedriftsdata[3].

For å benytte arbeidsprofiler må en Google-konto kobles til Intune. Denne kontoen burde ikke være noens private konto, opprett om nødvendig en dedikert konto for bedriften.

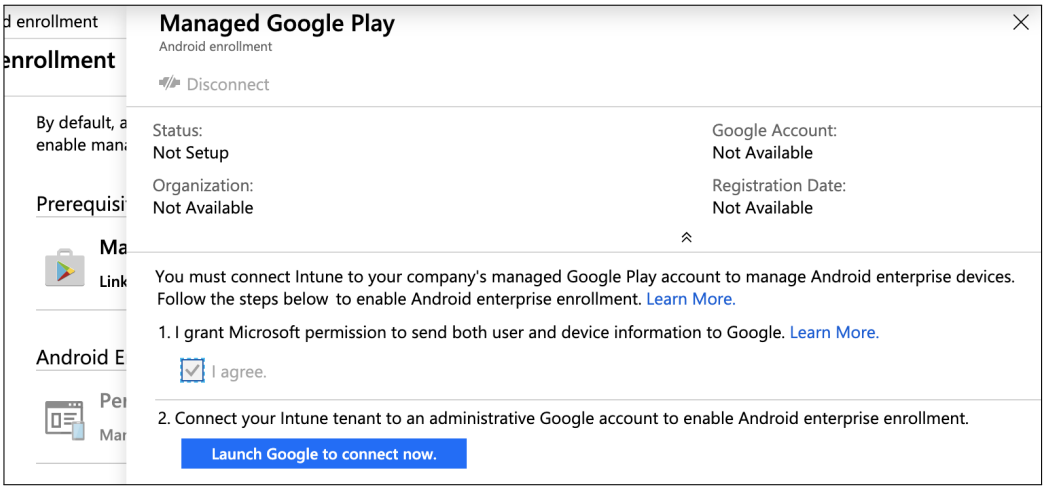
Når arbeidsprofilen er satt opp kan nye enheter registreres på samme måte som i avsnitt 5.1, men sikkerheten for både bedrift og ansatt vil være økt.

Naviger til “Intune”, “Device enrollment” og “Android enrollment”. Her er flere valg utilgjengelige før vi har koblet opp en Google-konto. Trykk på “Managed Google Play” for å starte koblingen mot Intune.



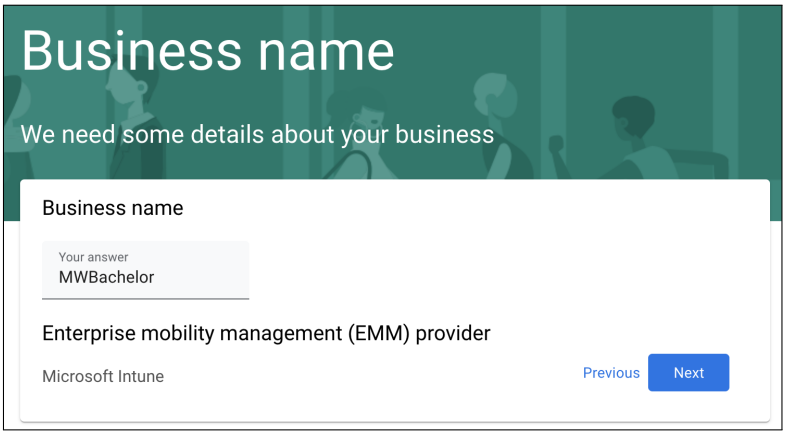
Figur 47

Det vil dukke opp et vindu med informasjon om kobling mellom Google Play og Intune. Som vi ser i figur 48, er det på nåværende tidspunkt ikke koblet opp en konto. Du må også godta at enhetsinformasjon sendes til Google ved å huke av for “I agree”. Trykk så på knappen “Launch Google to connect now”.



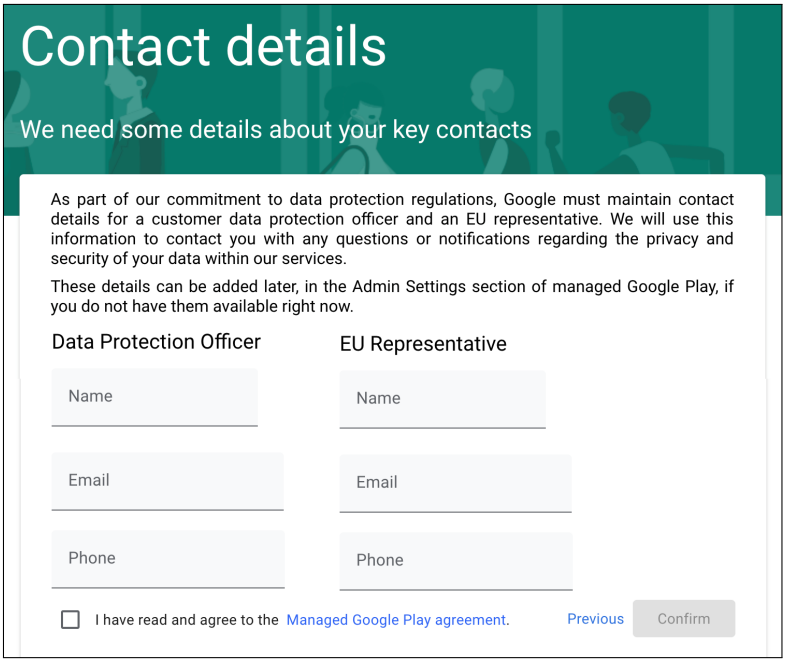
Figur 48

Du vil så bli dirigert til Googles nettside for bedrifter. Her må man logge inn med en Google-konto før en kan starte koblingen mot Intune. Oppgi så bedriftens navn under "Business name" og trykk "Next" for å fortsette.



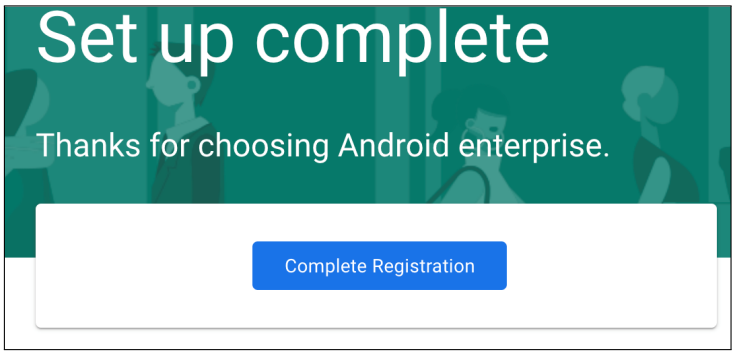
Figur 49

Google vil så be om kontaktdetaljer til ulike personer innenfor firmaet. Disse trenger ikke fylles inn, og kan eventuelt fylles inn på et senere tidspunkt dersom det skulle være behov. La feltene stå tomme, som vist i figur 50 og huk av for at du er enig i retningslinjene til Google. Gå så videre ved å trykke "Confirm".



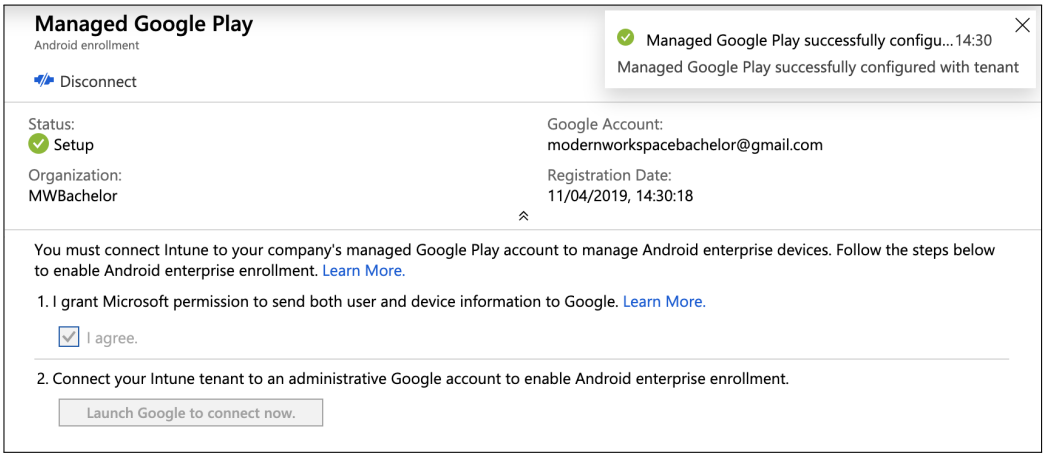
Figur 50

Koblingen vil nå være klar, og det er kun å trykke “Complete Registration” for å fullføre koblingen.



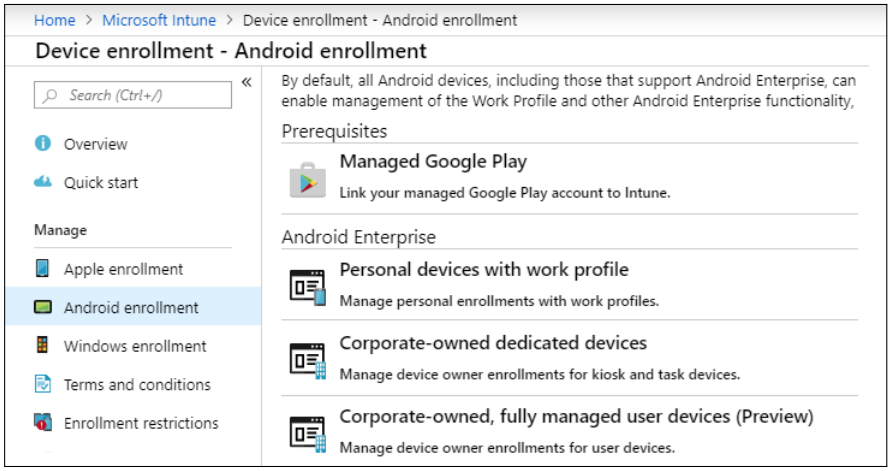
Figur 51

Tilbake i Intune skal statusen nå være grønn og de andre datafeltene bør være utfylt automatisk. Det vil også, som vi ser i figur 52, komme opp en notifikasjon om at “Managed Google Play” har blitt konfigurert.



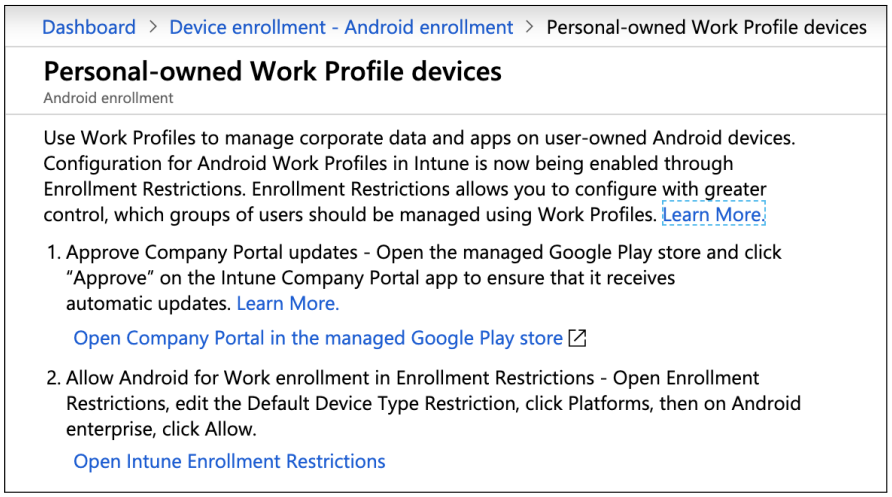
Figur 52

Går vi tilbake til “Android enrollment”, ser vi at alle alternativene nå er tilgjengelige. Velg her “Personal devices with work profile” for å sette opp en profil for registrering av Android-enheter.



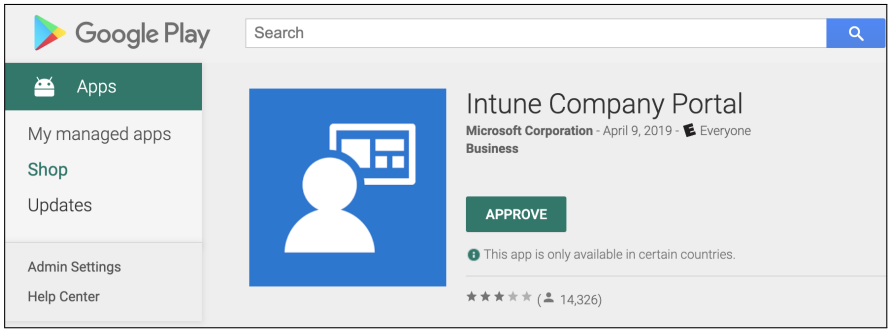
Figur 53

Da vil det dukke opp et vindu som forteller at Firmaportal-appen må godkjennes, og Android med arbeidsprofiler må godkjennes som en registreringsmetode. Trykk så på ”Open Company Portal in the managed Google Play store” for å godkjenne Firmaportal-appen.



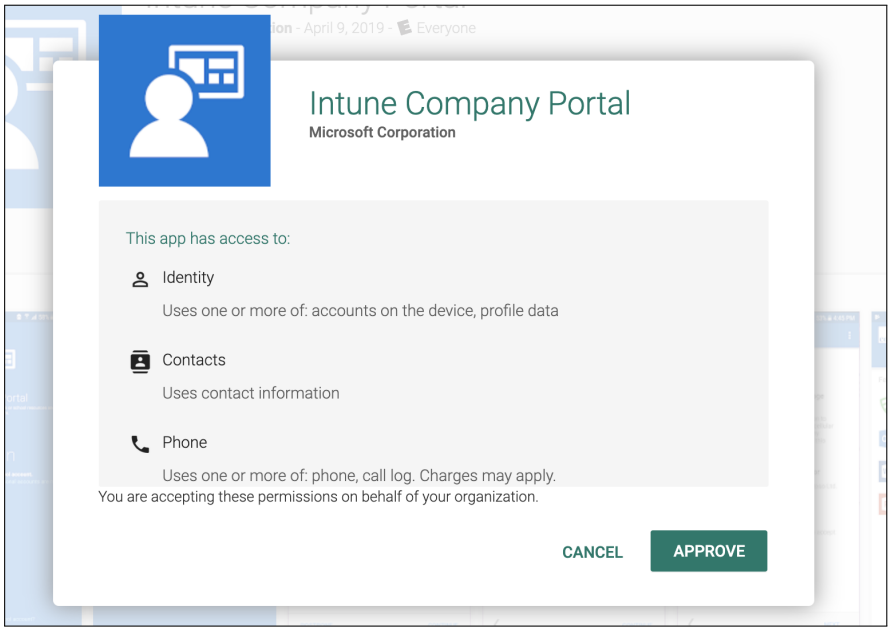
Figur 54

Du vil så bli navigert til bedriftsversjonen av Google Play Store, hvor du må logge inn med samme Google-konto som er koblet opp Intune. Når du er innlogget med riktig konto kan du trykke “Approve” under applikasjonen “Intune Company Portal”.



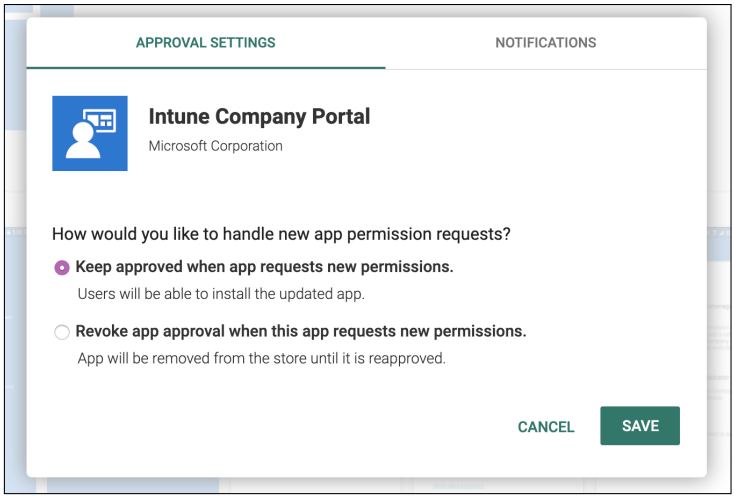
Figur 55

Du vil så måtte godkjenne hvilke ressurser applikasjonen vil få tilgang til på enheter. Les nøye gjennom for å sikre at disse stemmer overens med bedriftens vilkår og trykk “Approve” for å godkjenne applikasjonen.



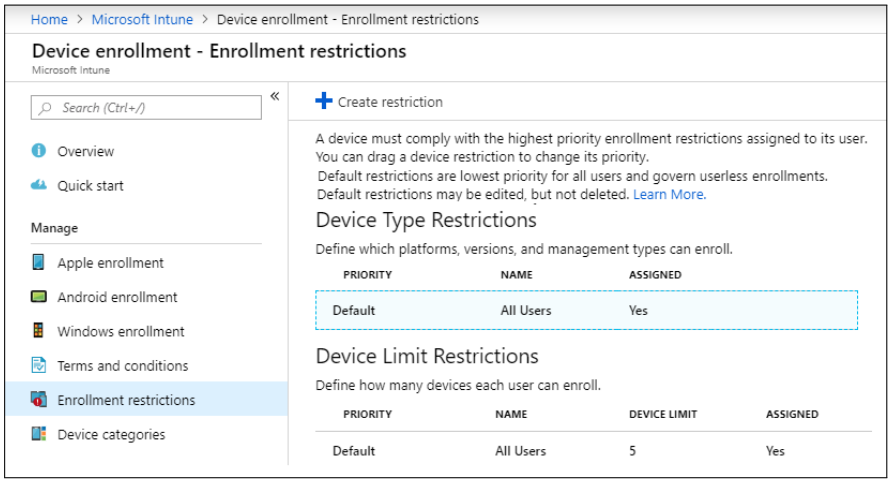
Figur 56

Google Play spør så om krav om tilgang på nye ressurser automatisk skal godkjennes. Dette vil være greit for denne applikasjonen da den er utviklet av Microsoft, men for andre applikasjoner må dette vurderes. Les mer om dette i "Driftsdokument – Applikasjoner". Huk av for "Keep approved when app requests new permissions" og trykk "Save" for å lagre valget.



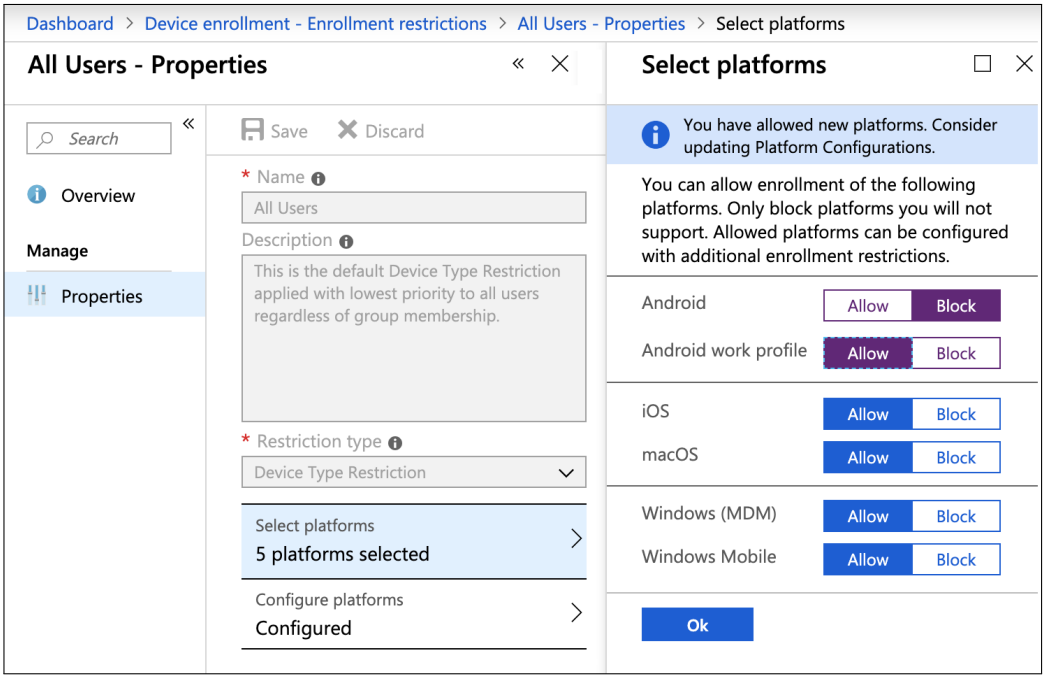
Figur 57

Tilbake i Intune må Android med arbeidsprofiler godkjennes. Dette gjøres i Device restrictions-menyen under "Device enrollment". Velg profilen under "Device Type Restrictions" som vist i figur 58.



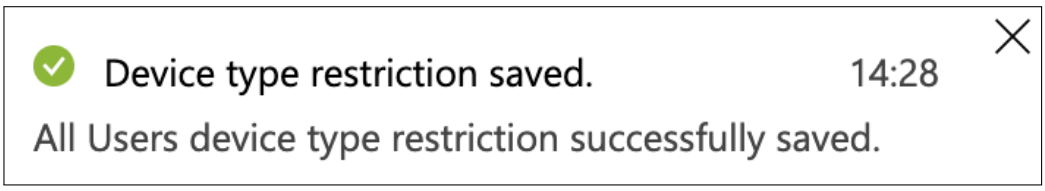
Figur 58

Under innstillingene for plattformer velges “Allow” for Android-enheter med arbeidsprofil, mens den gamle måten å enrolle Android-enheter blokkeres. Velg “OK” og lagre endringene ved å klikke “Save”.



Figur 59

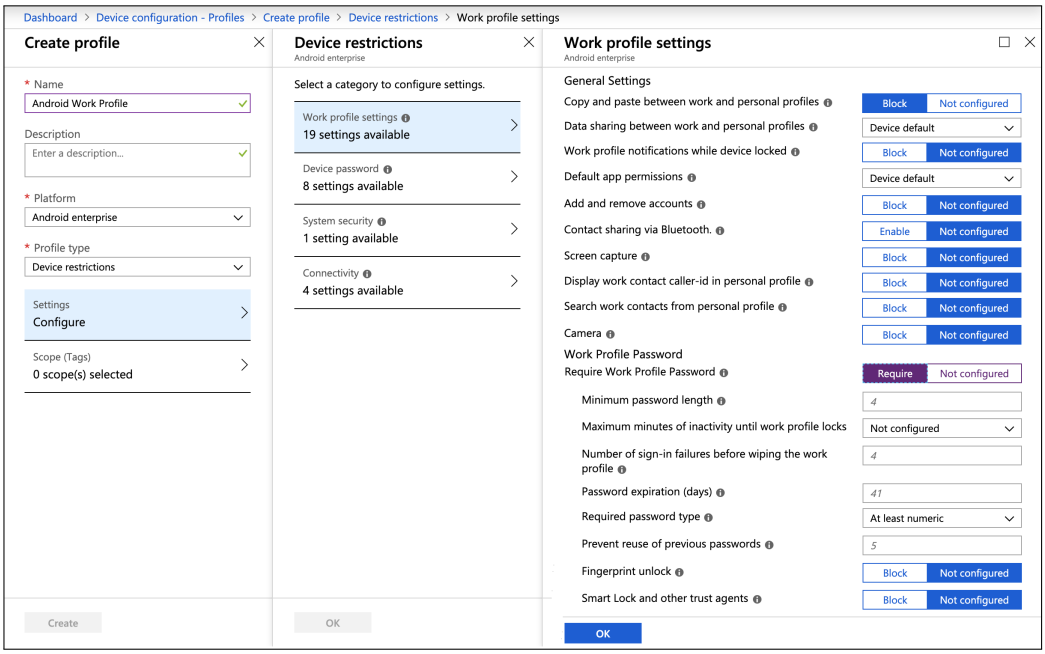
Når profilen er lagret vil det dukke opp et varsel som informerer om at restriksjonene ble lagret. Som vi ser i figur 60, gikk lagringen som ventet i vårt tilfelle.



Figur 60

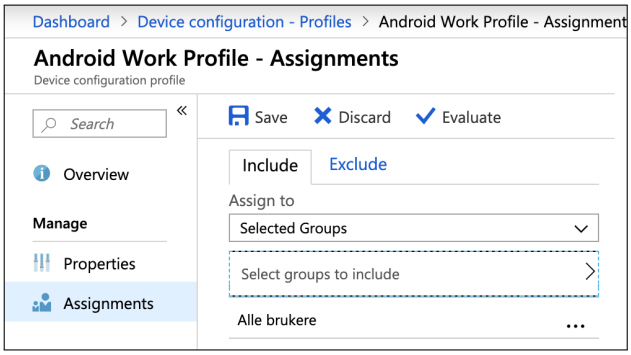
Nå som arbeidsprofiler er tillatt, må det opprettes en profil. Dette gjøres ved å opprette en ny profil i "Device Configuration". Opprett en ny profil, gi den et navn, under plattform velges "Android enterprice" og profiltypen settes til "Device restrictions".

Under instillingene for "Work Profile Settings" er det på figur 61 bare satt krav til at det må opprettes et passord med minst fire tegn.



Figur 61

Når innstillingene er valgt publiseres arbeidsprofilen til alle ved å tildele profilen til alle brukerne. Tilegnelsen kan så lagres ved å klikke "Save".

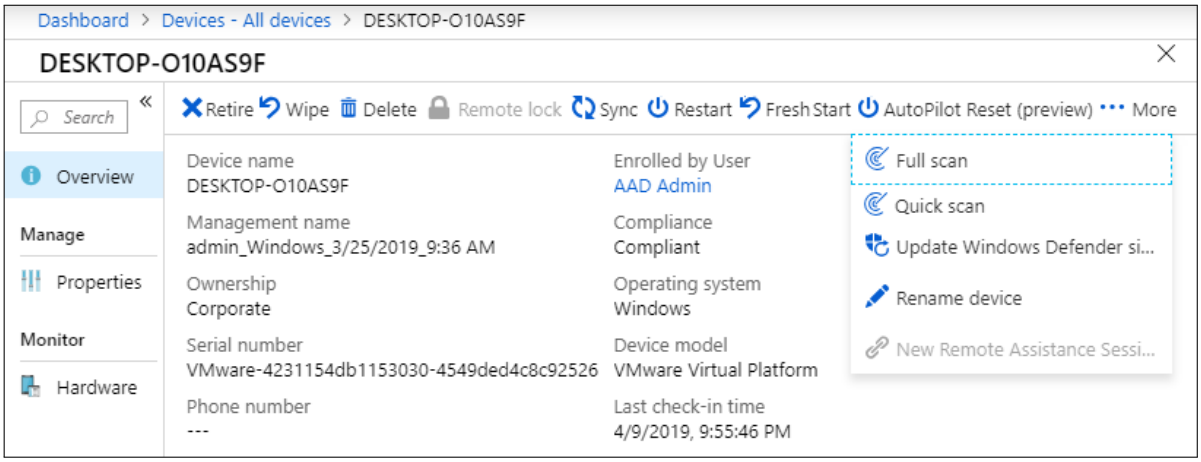


Figur 62

6 Unenrollment i Intune

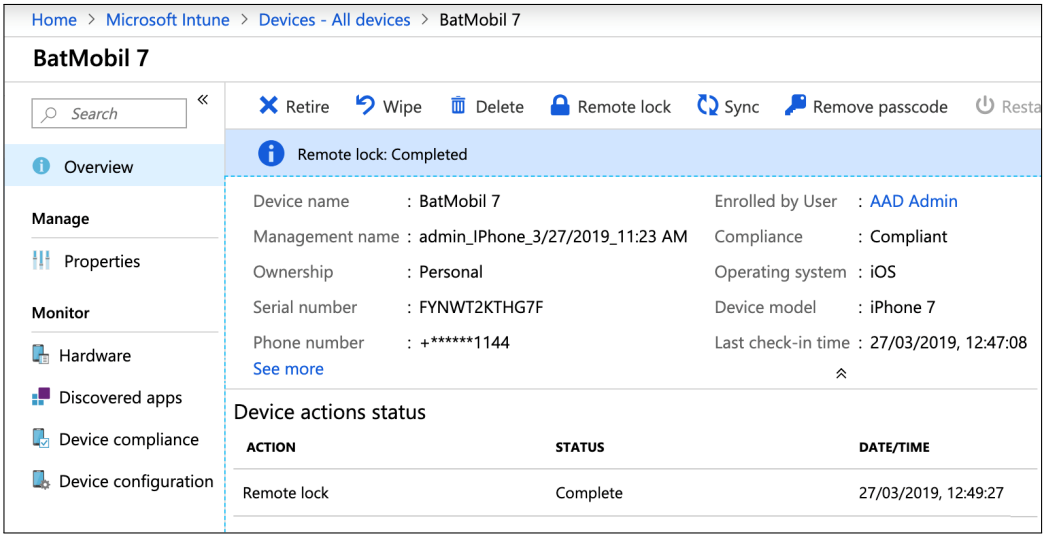
Alle enhetene som er registrert i Intune kan un-enrolles av administrator i Intune. Dette vil fjerne all bedriftsdata på enheten. I tillegg vil det være mulig å utføre en wipe på enheten for å slette *alle* data, både personlig og bedriftseid. For håndholdte enheter vil det være mulig å fjernlåse enheten, slik at enheten må låses opp igjen for å kunne brukes.

Ved å klikke på en enhet i Intune vil det være mulig å un-enrolle (Retire), tilbakestille til fabrikkinstillinger (Wipe), fjernlåse (Remote Lock) og annet som virusscan. Alle mulighetene illustreres i figur 63.



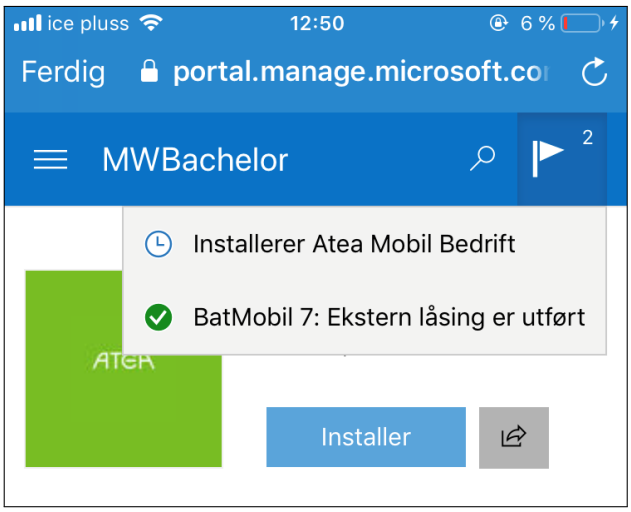
Figur 63

Intune vil loggføre alle handlinger som utføres på enheten under "Device action status". Som vi ser i figur 64, har vi forsøkt å kjøre fjernlåsing av enheten, og den ble gjennomført.



Figur 64

Åpner vi Firmaportal-applikasjonen på enheten som handlingen ble utført på, kan vi se at det er kommet en varsling som beskriver hendelsen. Som vi ser i figur 65, ble en ekstern låsing utført på denne enheten.



Figur 65

Referanser

[1] Microsoft. *Get an Apple MDM push certificate*. 2018. URL: https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get (sjekket 30.04.2019).

[2] Microsoft. *Set up enrollment of Android Enterprise work profile devices*. 2018. URL: https://docs.microsoft.com/en-us/intune/android-work-profile-enroll (sjekket 30.04.2019).

[3] Robin Hobo. *How to Enable Android Enterprise and configure Personal devices with a Work Profile in Microsoft Intune – The ultimate Step-By-Step Guide*. 2019. URL: https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/ (sjekket 30.04.2019).

Modern Workspace - Driftsdokument
Autopilot

v.1.0

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
22.03.2019	0.1	Opprettet avsnitt for standard autopilot
02.04.2019	0.2	Opprettet avsnitt for Enrollment-status-page, oobe-prosessen, og etter oobe
05.04.2019	0.3	Første fulle utkast av standard autopilot klart
11.04.2019	0.4	Lagt inn bilder for hybrid-join og begynt å skrive tekst til de
12.04.2019	0.5	Introduksjon revidert
19.04.2019	0.6	Mindre revisjon av tekst, skrevet videre på tekst for Hybrid-join
22.04.2019	0.7	Skrevet tekst for Intune Connector, OU for autopilot-maskiner, Maskingruppe, Enrollment Status Page, OOBE – Hybrid Join, OOBE – ferdig/etterpå, lagt til nye figurer
23.04.2019	0.8	Revidert bildetekster og lagt til tekst for domenekonfigurasjon
24.04.2019	0.9	Skrevet om ODJ-blob på hybrid-join
05.05.2019	1.0	Mindre revisjon av tekst, retting av grammatiske og språklige feil

Innhold

1 Introduksjon

Windows Autopilot er en prosess som vil sette opp og konfigurere en ny maskin til ønsket tilstand med minst mulig bryderi for systemadministrator og sluttbrukeren. Prosessen kan konfigureres til å melde maskinen inn i Azure AD, lokal AD, installere sikkerhetspolicies og installere utvalgte applikasjoner. Autopilot gjør også at systemadministrator slipper å måtte være i fysisk kontakt med maskinene på noe tidspunkt. Maskinene kan sendes rett fra leverandør til sluttbruker og vil automatisk settes opp når sluttbrukerne skrur dem på.

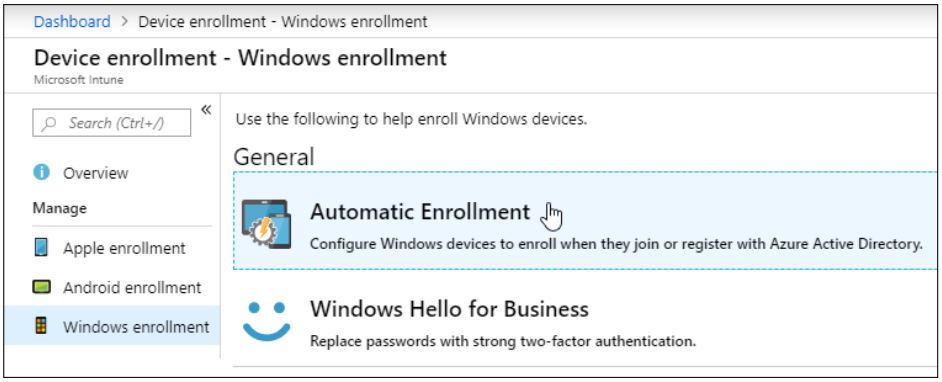
Dette dokumentet skal vise og forklare de forskjellige prosessene involvert i Windows Autopilot. Det vil blant annet ta for seg konfigurasjon av autopilotprofiler, konfigurasjon av brukeropplevelse og hvordan maskiner automatisk kan bli medlem av lokalt domene.

Dokumentet vil gå ut ifra at leser har en viss teknisk kunnskap, og vil ikke nødvendigvis være enkelt å forstå for ufaglærte.

2 Automatic Enrollment

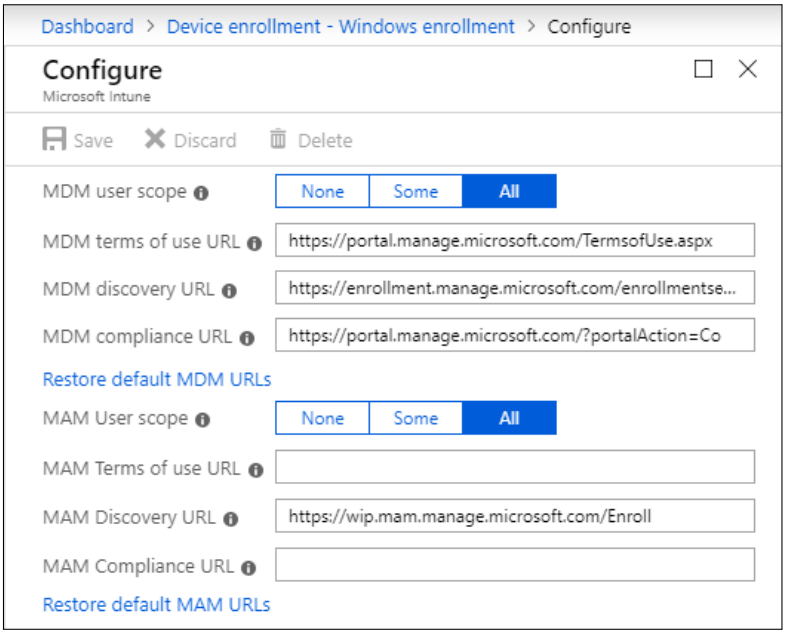
Før vi kan starte med Autopilot må vi forsikre oss om at maskiner kan automatisk registreres til Intune når de blir registrert i AAD.

Gå til Intune, velg Device enrollment", "Windows enrollment"og åpne "Automatic Enrollment"under General".



Figur 1

Bekreft at "MDM user scope" er satt til "All".



Figur 2

3 Autopilot

Vi utfører prosessen på en allerede oppsatt VM med Windows 10 1809. Det skaffes info fra maskinen og før den settes tilbake til fabrikktilstand[1].

3.1 Skaffe hardwareinfo (HWID)

Denne informasjonen kan skaffes direkte fra maskinleverandør, eller ved bruk av skript direkte på en maskin. Følgende kommandoer, i Listing 1, kjøres som administrator i et PowerShell-vindu på VM-en.

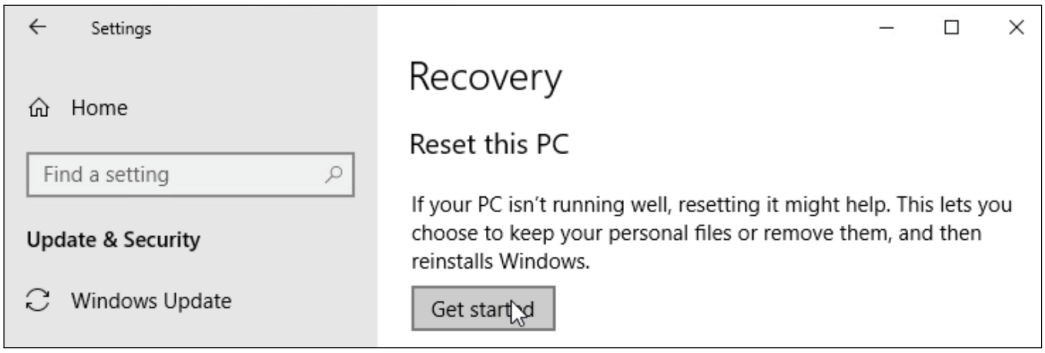
Listing 1: Get HWID

```
1 md c:\HWID
2 Set-Location c:\HWID
3 Set-ExecutionPolicy Unrestricted
4 Install-Script -Name Get-WindowsAutopilotInfo
5 Get-WindowsAutopilotInfo.ps1 -OutputFile
    AutopilotHWID.csv
```

Filen "AutopilotHWID.csv" blir opprettet og denne inneholder alt som trengs for å identifisere maskinen, denne informasjonen vil fra nå av bli forkortet til HWID (Hardware ID). Denne filen må lastes opp til Intune. Dette blir gjort i avsnitt 3.3 Legg til enhet i Intune.

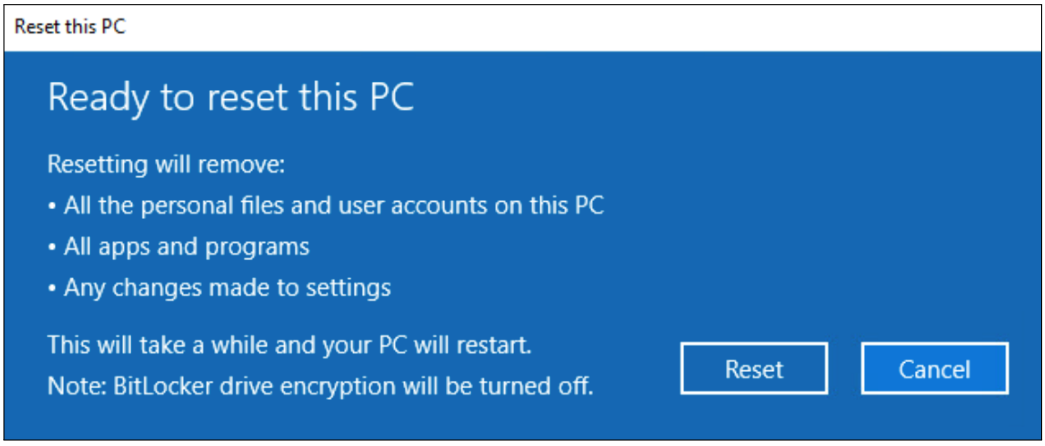
3.2 Reset

Når maskinen kan identifiseres kan den gjenopprettes og stilles tilbake til fabrikk-innstillinger. Dette gjøres via Recovery i Windows-innstillingene på maskinen.



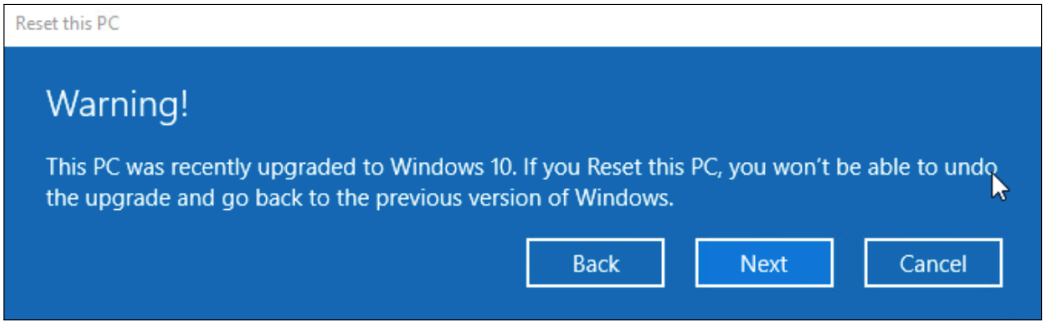
Figur 3

Det vil dukke opp en veiviser som informerer om hvilke konsekvenser en tilbake-stilling vil ha. Klikk her "Reset" for å starte prosessen.



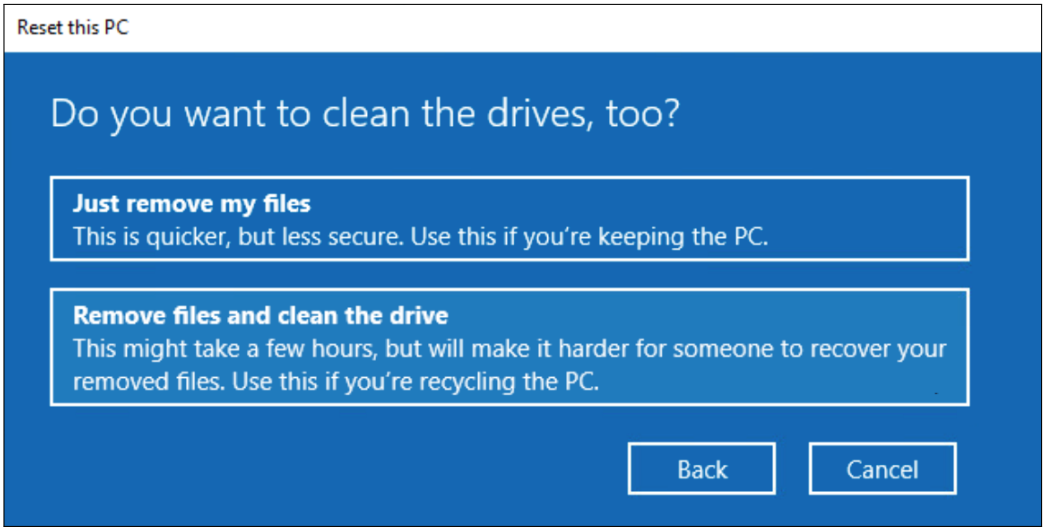
Figur 4

Dersom maskinen nylig oppdaterte Windows-versjon, vil det komme en advarsel om at en ikke kan gjenopprette maskinen til den gamle versjonen. Klikk her "Next" for å komme videre i prosessen.



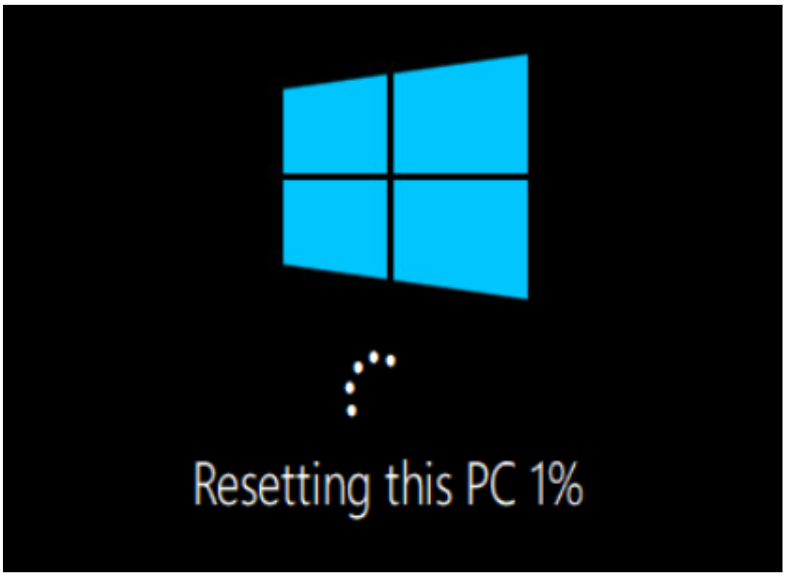
Figur 5

Du vil så bli spurt om du kun ønsker å slette filer fra maskinen eller om du ønsker å fjerne all data. Siden vi ønsker å stille maskinen tilbake til fabrikkinnstillinger velger vi å fjerne alt. Dette gjøres ved å klikke på "Remove files and clean the drive".



Figur 6

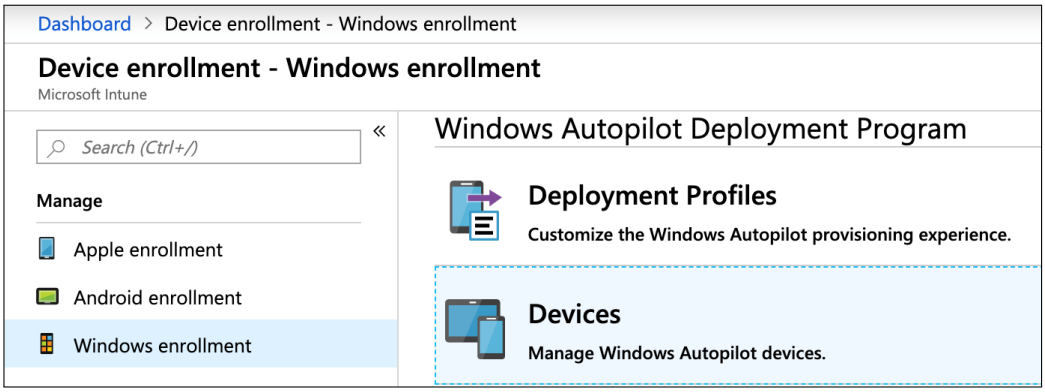
Prosessen vil så starte, og ta en god stund før den er ferdig.



Figur 7

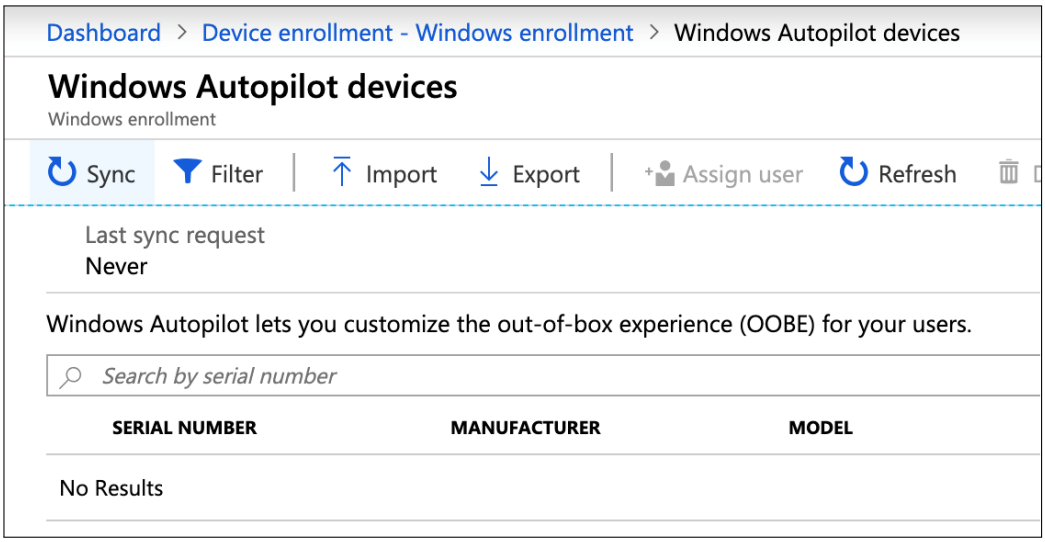
3.3 Legg til enhet i Intune

Når maskinens HWID er klar må denne lastes opp til Intune. Naviger til Intune, derfra velges "Device enrollment", i listen til venstre trykkes det først på "Windows enrollment" og så "Devices" under programmet for Windows Autopilot.



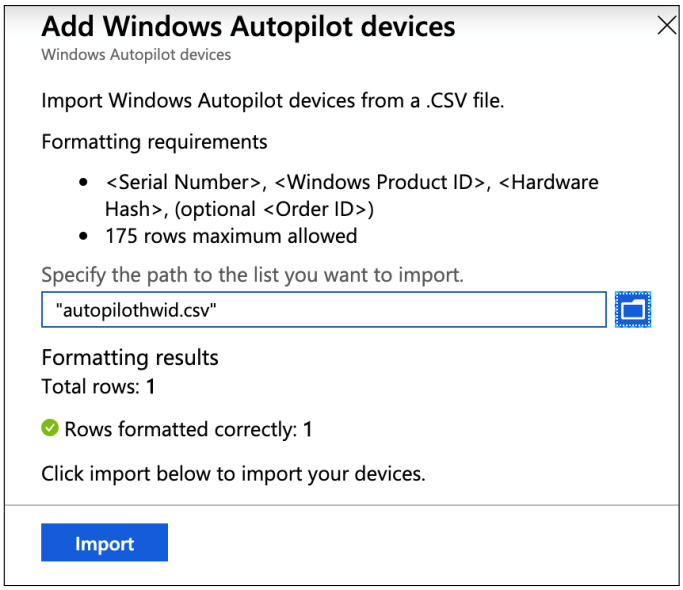
Figur 8

På siden for enheter til autopilot velges det “Import”, og det vil dukke opp et vindu der HWID-filen skal lastes opp.



Figur 9

Last opp filen og trykk på “Import”.

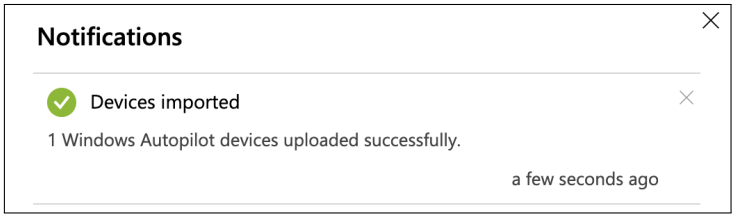


Figur 10

Det vil dukke opp et varsel om at maskinen importeres.

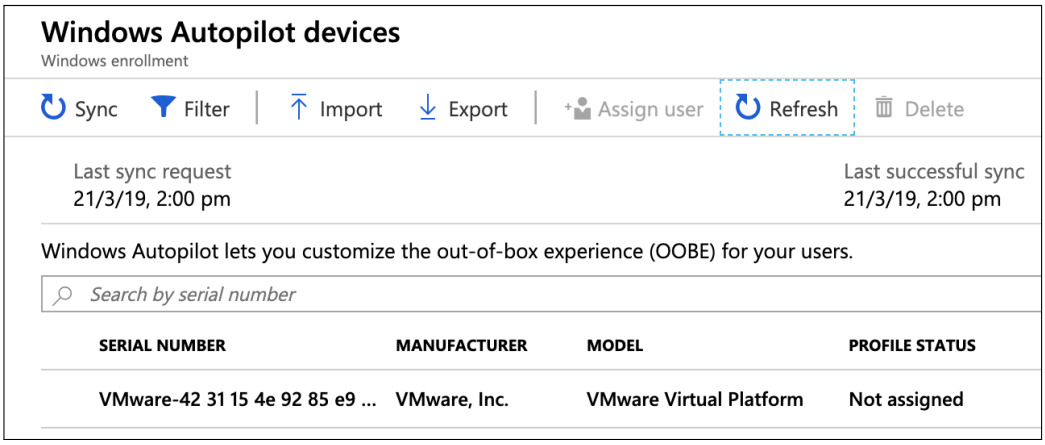
Figur 11

Deretter dukker det opp et varsel som informerer om importeringen var vellykket. Som vi ser i figur 12 gikk importeringen feilfritt.



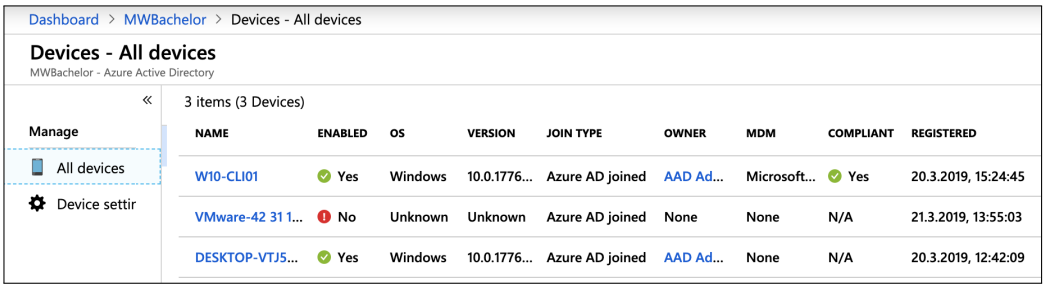
Figur 12

Ved å trykke "Refresh" vil listen oppdateres og maskinen som ble importert skal nå dukke opp. Vi ser at maskinen har profilstatusen "Not assigned", noe som betyr at maskinen ikke har fått tildelt profil.



Figur 13

Som vi ser i figur 14, dukker maskinen også opp i enhetslisten inne i AAD uten noen informasjon annet enn maskin-navn.

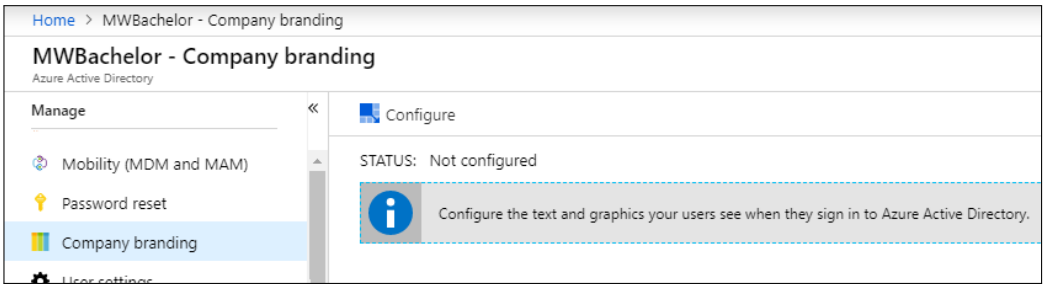


Figur 14

3.4 Company Branding

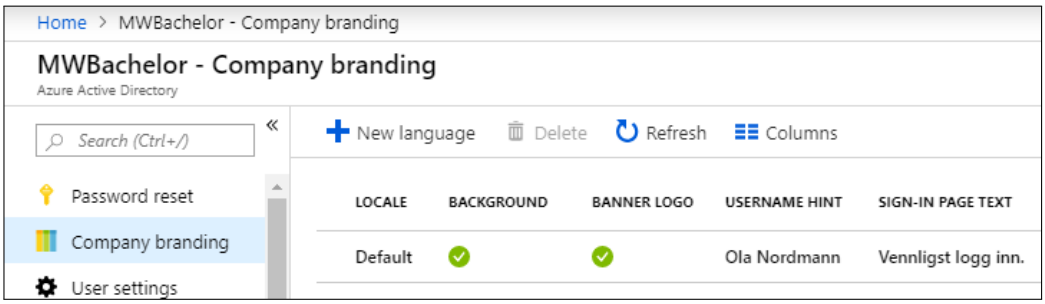
Hvis det er satt opp en Company Branding-profil allerede kan dette avsnittet hoppes over. Men på figur 15 er det tydelig at det ikke finnes noen profil og dette må opprettes. Mer om Company branding finnes i eget driftsdokument.

For å opprette en slik profil navigerer man til Azure Active Directory i Azure. Her er det bare å trykke på meldingen for å opprette en standardprofil. Noen av disse elementene vil vises forskjellige steder under OOBE.



Figur 15

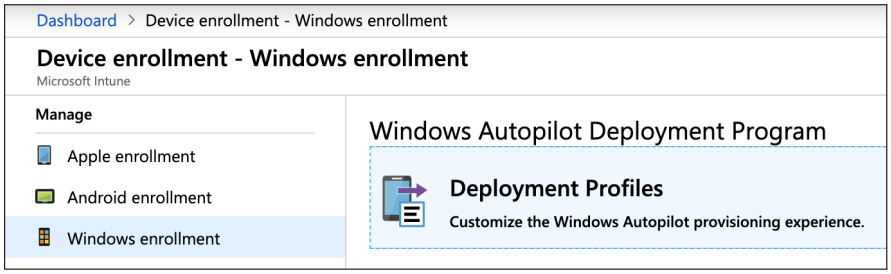
Opprettelse av profil for Company Branding dokumenteres i “Driftsdokument - Company Branding”. Når profilen er opprettet vil det se slik ut som i figur 16.



Figur 16

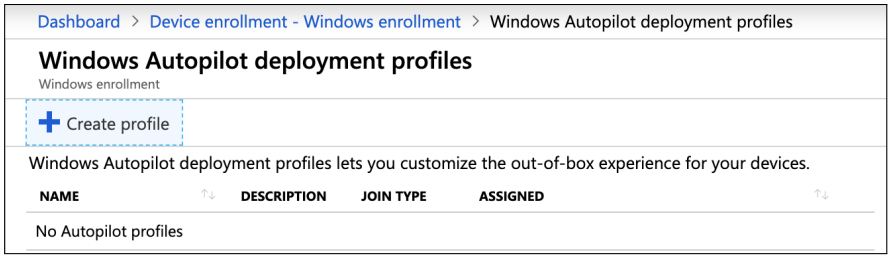
3.5 Opprett Autopilot-profil

Før det kan tildeles en profil til maskinen må det opprettes en profil for autopilot. Naviger til Intune, derfra velges “Device enrollment”, i listen til venstre trykkes det først på “Windows enrollment” og så “Deployment Profiles” under programmet for Windows Autopilot.



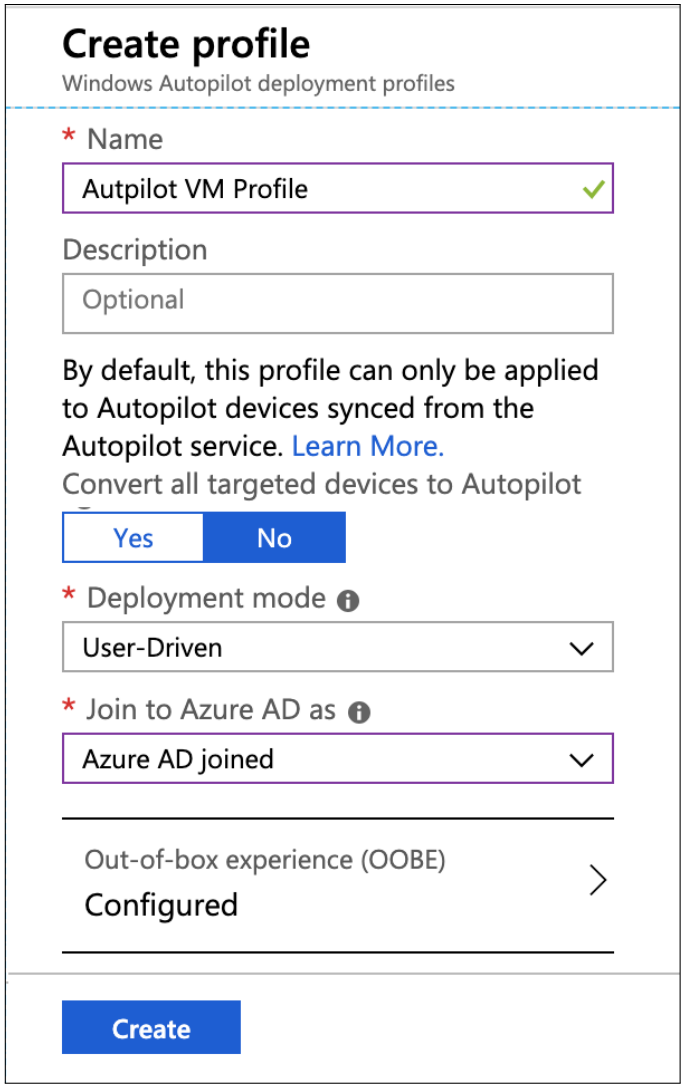
Figur 17

Som vi ser i figur 18, ligger det ingen profiler inne enda. Opprett en ny ved å klikke på “Create profile”.



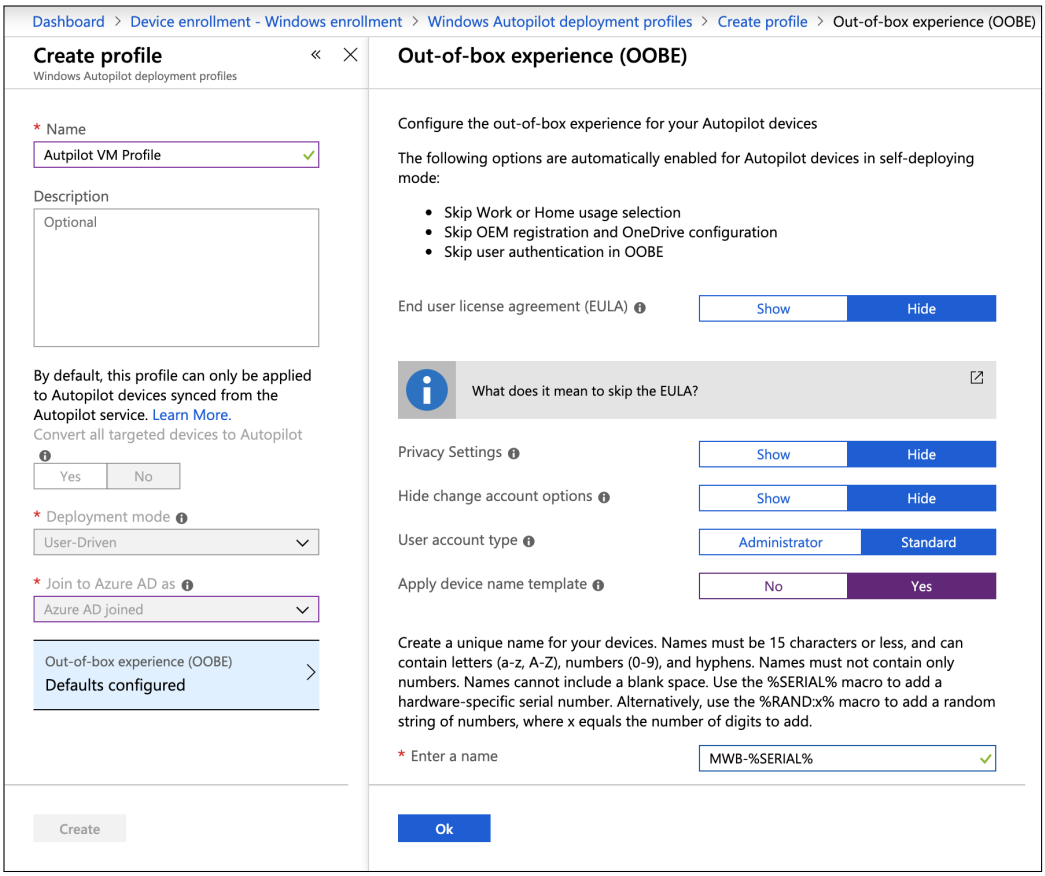
Figur 18

Det dukker så opp et vindu, som vist i figur 19. Her gis profilen et navn og en beskrivelse. “Deployment mode” settes til “User-Driven” og “Join to Azure AD as” settes til AAD-join. For Hybrid Azure AD-join se avsnitt 4 Autopilot - Hybrid-Join.



Figur 19

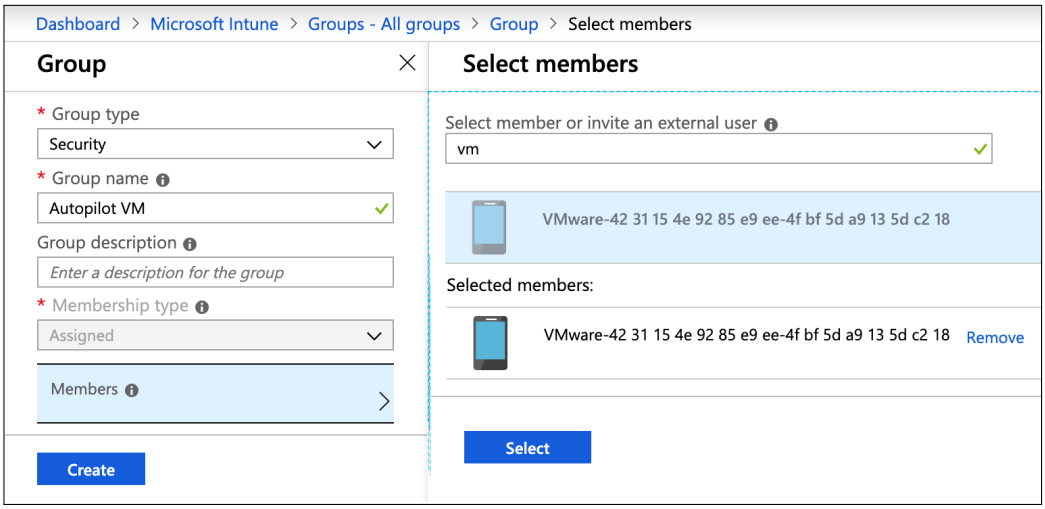
OOBE kan konfigureres helt nedert i profilopprettelsen. Da vil det dukke opp et vindu som i figur 20. Her er det mulig å fjerne administratorkontoen ifra maskinen og ikke vise EULA under OOBE. Nederst i dette vinduet spesifiseres maskinnavnet som maskinen skal ha når den er ferdig konfigurert.



Figur 20

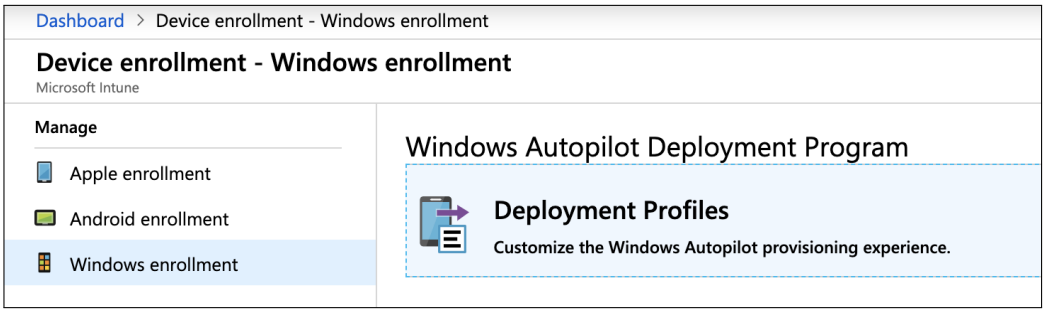
3.6 Tildele profil

Med den nye profilen opprettet kan vi nå tildele profilen til maskinene som skal få OOBE. For å kunne tildele profilen, må vi først opprette en gruppe med maskiner som profilen kan tildeles. Naviger til ”Intune”, Groups”, ”All groups”og trykk New Group”. Som vist i figur 21 legger vi til VM-en vi hentet HWID fra på forhånd.



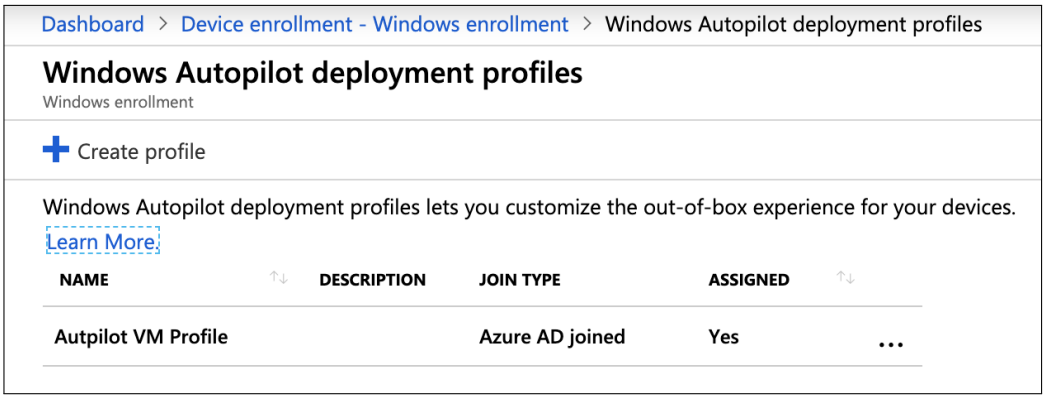
Figur 21

Nå som det er opprettet en gruppe kan vi tildele autopilotprofilen til denne gruppen. Vi navigerer oss til enhetsutrulling for Windows og går til Deployment Profiles”.



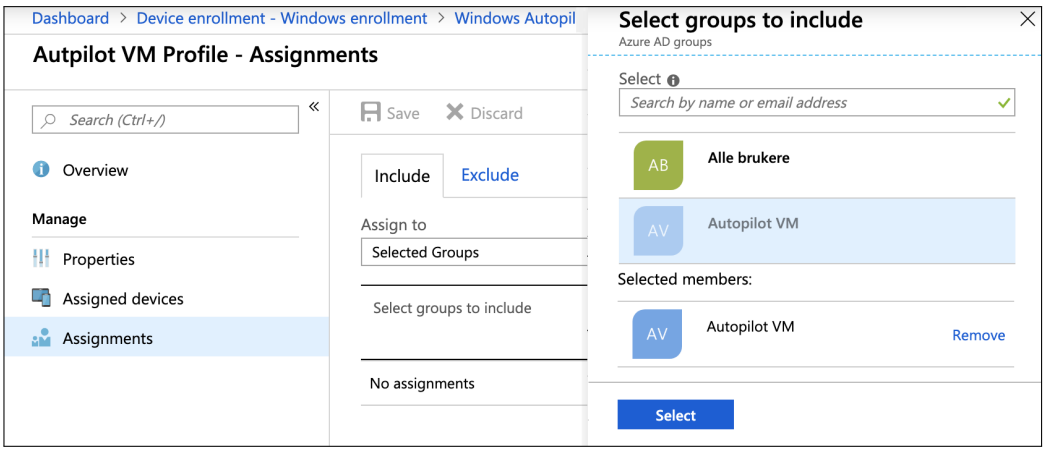
Figur 22

I listen over alle opprettet profiler velger vi vår profil.



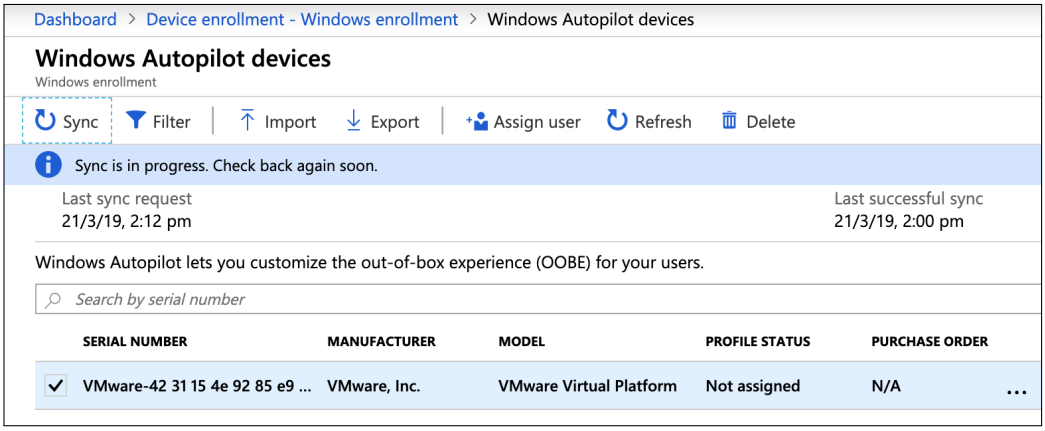
Figur 23

Egenskapene til profilen er allerede konfigurert, så vi velger derfor “Assignments” til venstre og deretter gruppen vår.

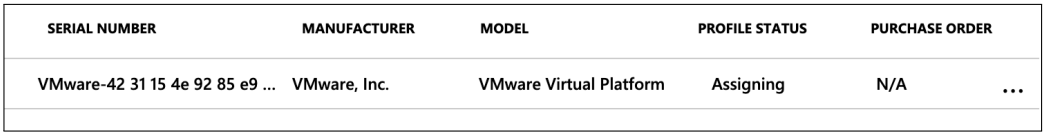


Figur 24

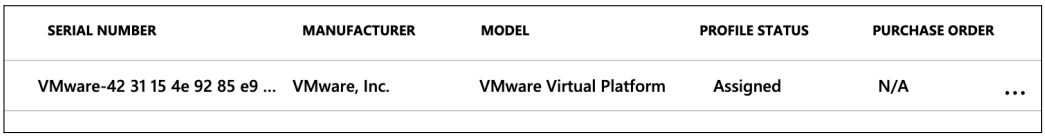
I listen over autopilotenheter vil profilstatusen til enheten endre seg fra “Not assigned”, som vist i figur 25, til “Assigning”, som vist i figur 26. Til slutt endres profilstatusen til “Assigned”, som vi ser i figur 27. Dette tar litt tid.



Figur 25

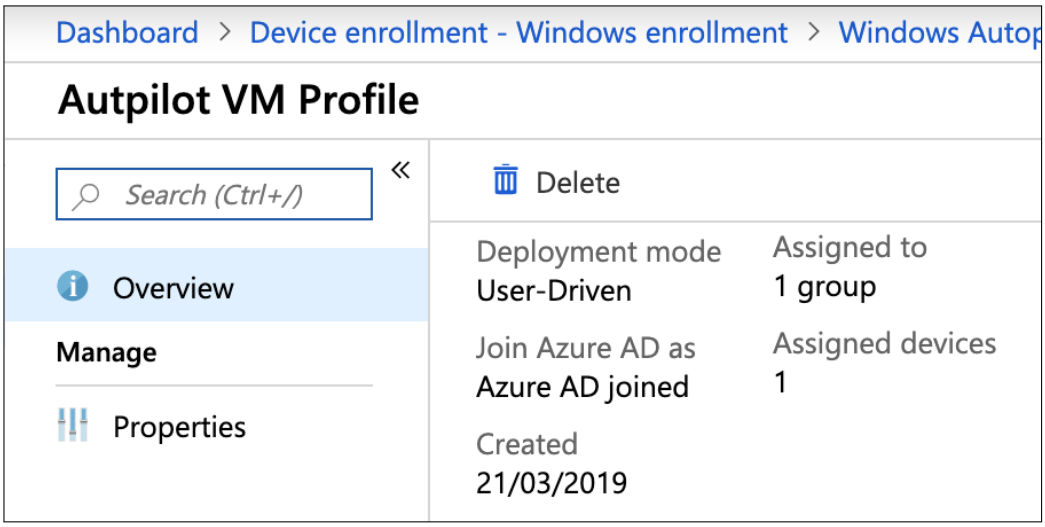


Figur 26



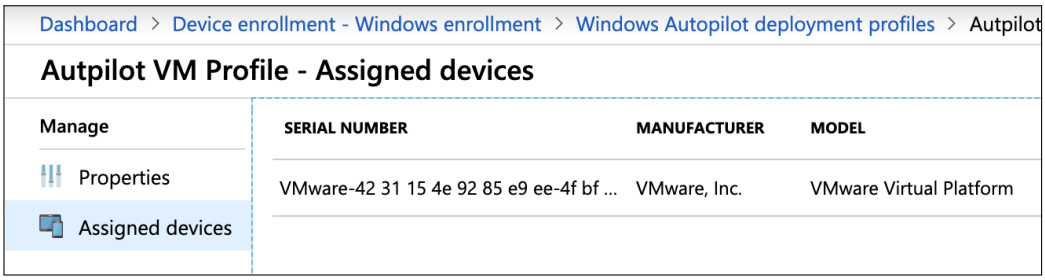
Figur 27

Går vi tilbake til til profilen, som vist i figur 28, kan vi se at den nå er tildelt en gruppe og en enhet.



Figur 28

Ser vi på ”Assigned devices”, som vist i figur 29, kan vi bekrefte at VM-en har fått tildelt profilen.

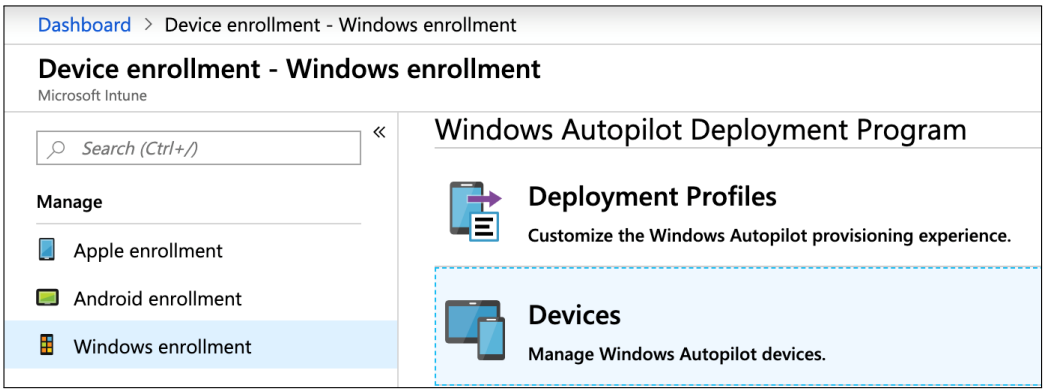


Figur 29

3.7 Tildel bruker (valgfritt)

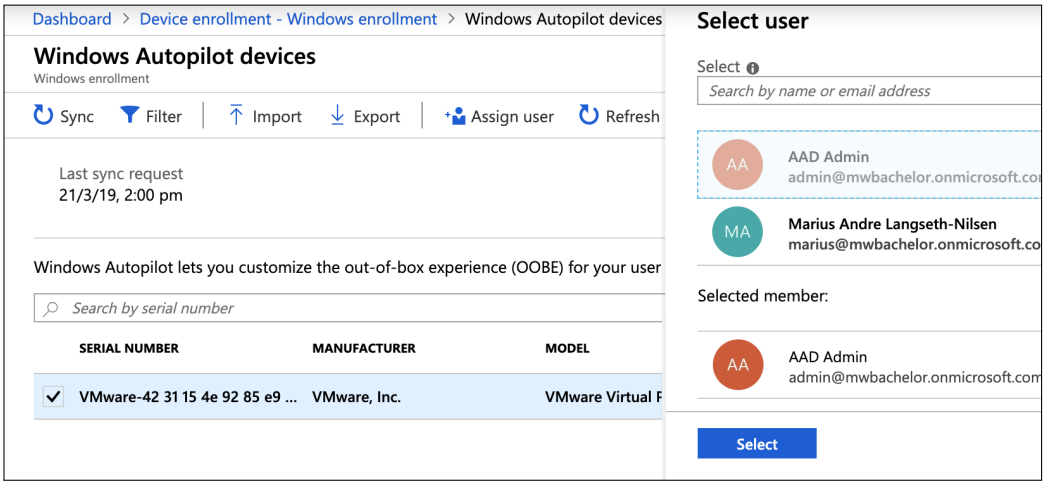
Hvis det allerede er klart hvilken bruker som skal bruke maskinen, kan denne brukeren få tildelt maskinen på forhånd. Da vil maskinen allerede i OOBE-fasen vite hvem som skal logge inn og brukeren trenger bare å oppgi passordet sitt, ikke brukernavn.

Dette gjøres ved å gå til listen over autopilotenheter, velge maskinen, og trykke "Assign user" i samme toppmeny som vi brukte for å importere HWID tidligere.



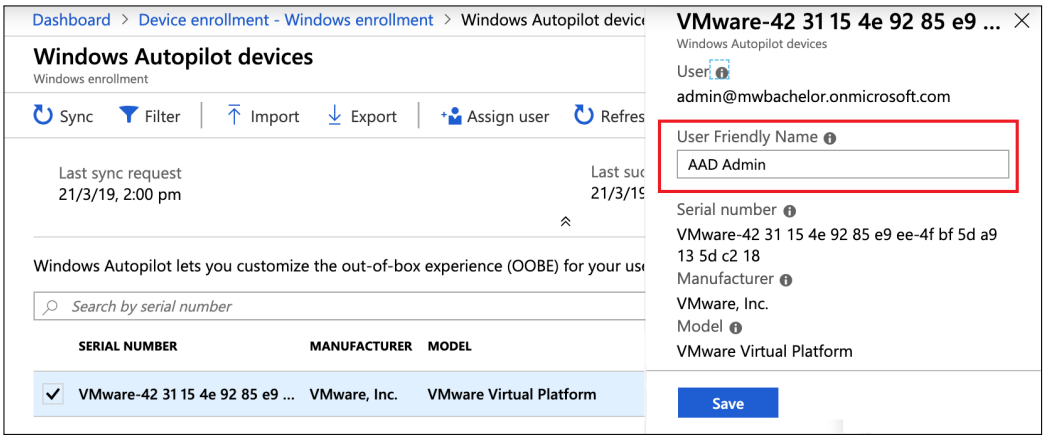
Figur 30

Finn enheten som skal tildeles en bruker, og trykk på "Assign user". Det dukker opp et nytt vindu og her velges den brukeren som skal benytte maskinen ved å finne bruker og trykke "Select".



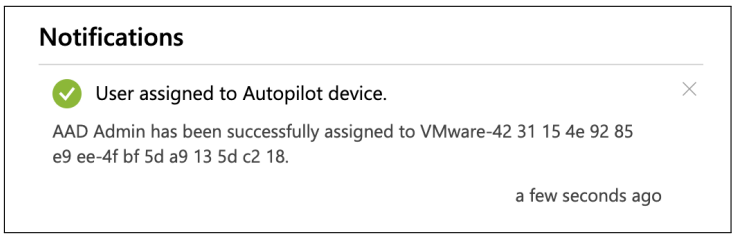
Figur 31

Når brukeren er valgt vil det også være mulig å oppgi et brukervennlig navn som er lett gjenkjennelig. Lagre tildelingen ved å trykke på “Save”.



Figur 32

Det vil så komme opp en notifikasjon som informerer om tildelingen gikk bra eller ikke. Som vist i figur 33, var tildelingen vellykket i vårt tilfelle.

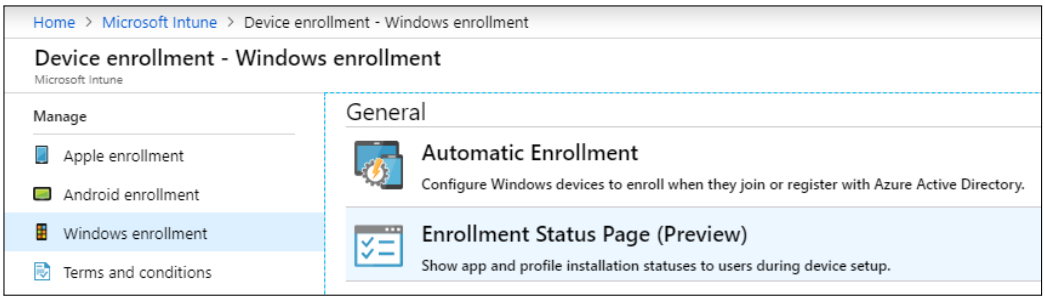


Figur 33

3.8 Enrollment Status Page

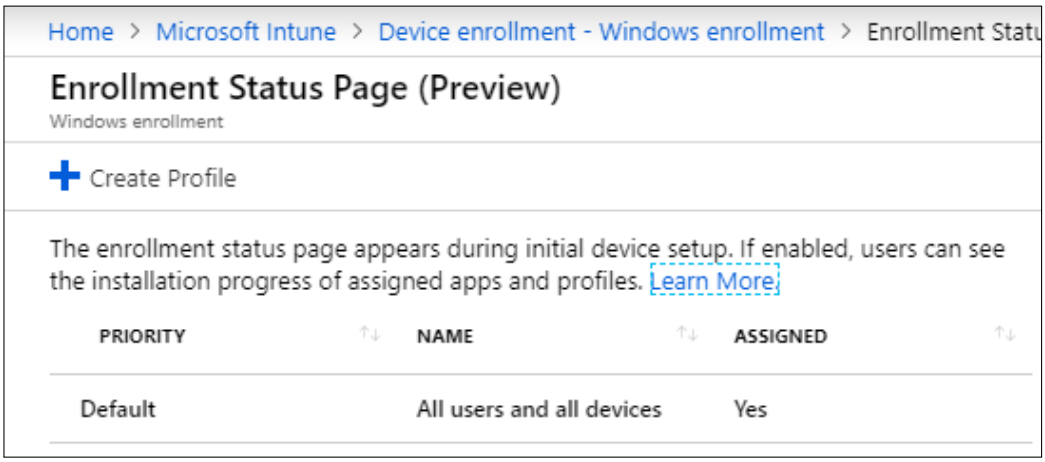
Med å endre profiler for “Enrollment Status Page” kan man videre konfigurere hvordan autopilotprosessen skal oppleves for brukeren. Gjennom disse profilene velger man hva brukeren skal og ikke se under autopilotprosessen. Hvis noen applikasjoner eller profiler er kritiske og må være installert før bruker tar i bruk maskinen, spesifiserer man disse her. Installasjonen vil vente på at disse installeres før brukeren kan nå skrivebordet eller benytte maskinen på noen som helst måte. Andre applikasjoner som ikke er like kritiske før start kan ekskluderes og kan heller installeres i bakgrunnen når autopilotprosessen er ferdig.

Først navigeres det til “Intune”, “Device enrollment”, “Windows enrollment” og det velges “Enrollment Status Page”.



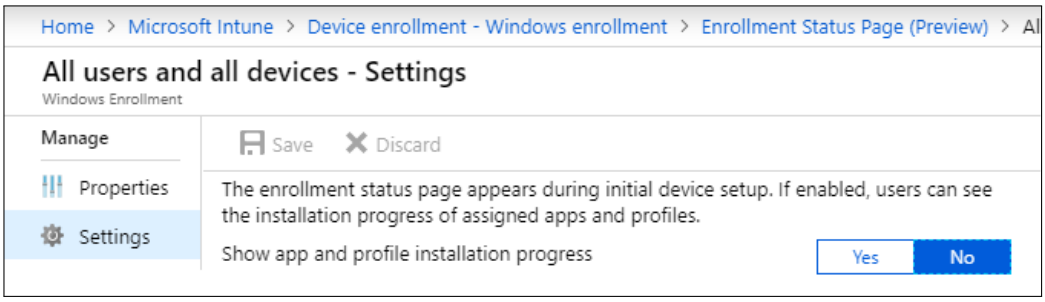
Figur 34

Det eksisterer allerede en standard-profil som benyttes av alle enheter og brukere. Ved å klikke på profilen dukker det opp et nytt vindu.



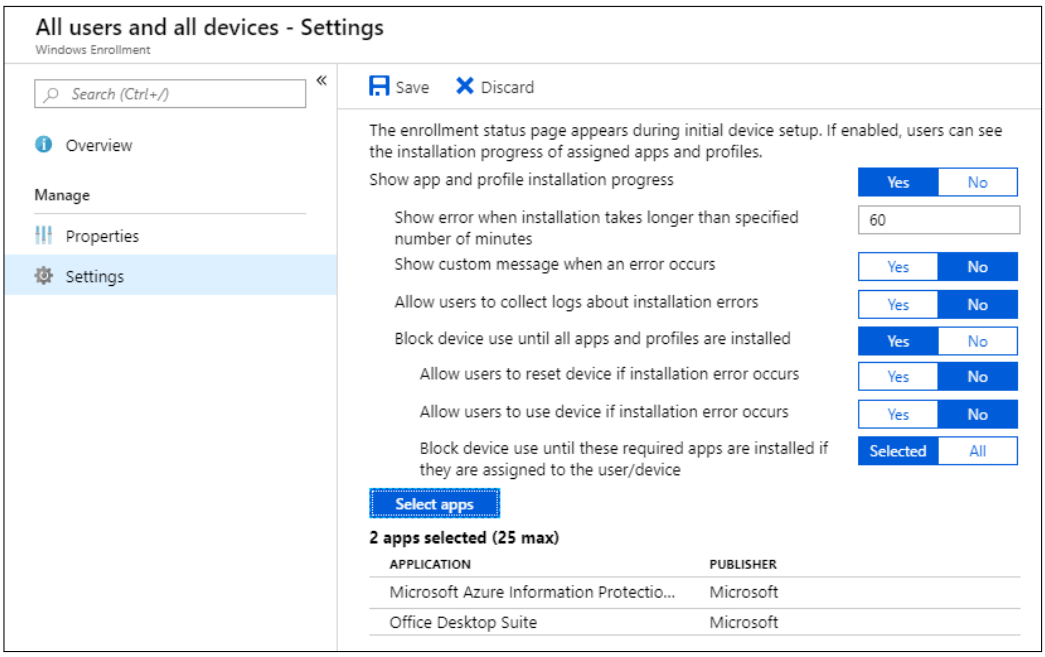
Figur 35

Her velges “Settings” i menyen på venstre side og bryteren skiftes til “Yes”, deretter vil det dukke opp flere konfigurasjonssmuligheter.



Figur 36

Nederst i disse innstillingene er det mulighet for å velge de applikasjonene som skal være installert før brukeren får tilgang til skrivebordet på maskinen. Som vist i figur 37, har vi valgt at AIP-klienten og Office-suiten skal installeres gjennom Autopilot.

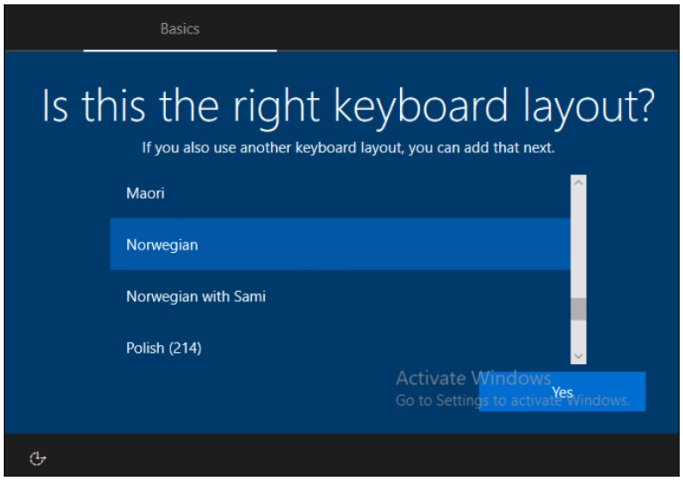


Figur 37

3.9 Out of Box Experience (OOBE)

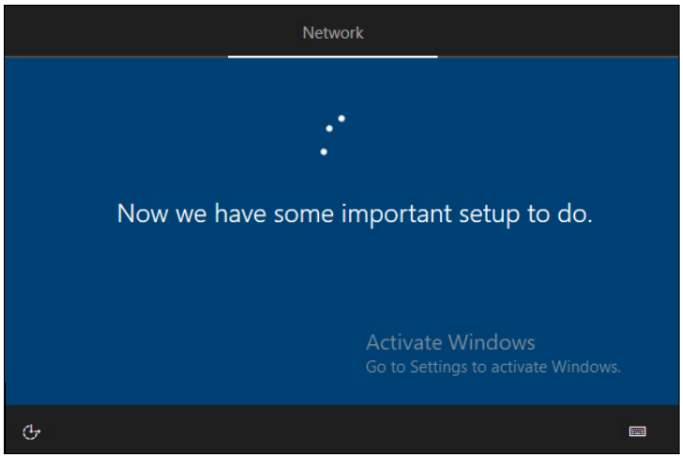
For brukere som får en maskin som innrulleres gjennom autopilot, vil de ha en annen opplevelse når de starter maskinen for første gang sammenlignet med brukere som bruker en personlig enhet. Denne opplevelsen er kjent som "OOBE" og vi vil dokumentere denne raskt.

Når maskinen starter opp vil du få muligheten til å velge tastaturoppsett og språkpakken OS-et vil bruke. Vi velger her norsk tastatur med engelsk språkpakke. Trykk "Yes" for å komme videre.



Figur 38

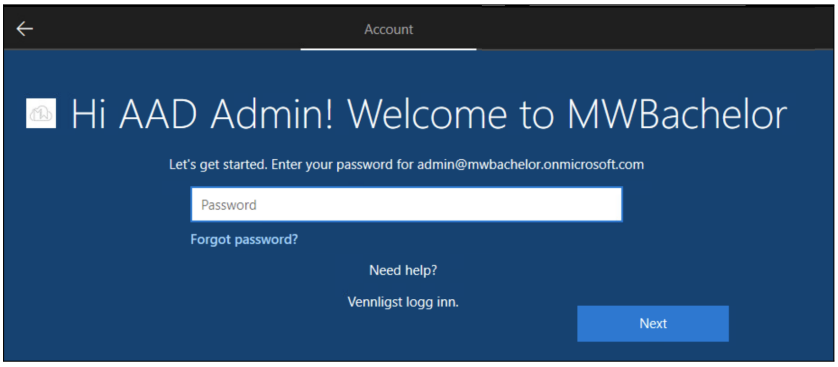
Etter språk og tastaturvalg vil maskinen hente autopilot-profilen. Legg merke til beskjeden om å aktivere Windows nederst til høyre på figur 39.



Figur 39

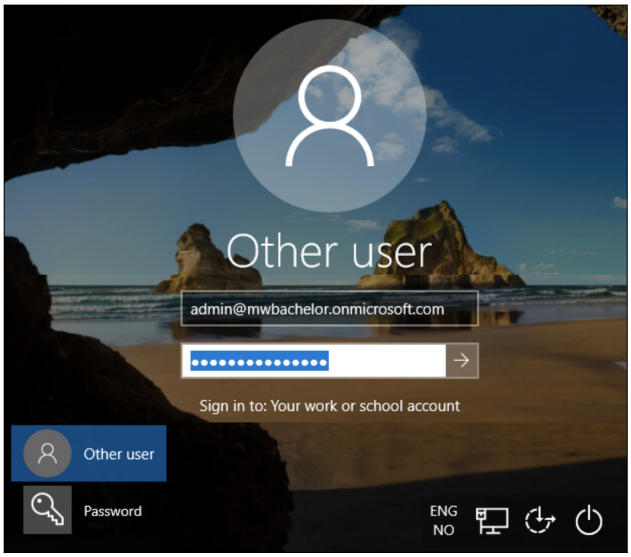
Etter en kort stund kommer vi til en innloggingsskjerm med ferdig utfylt brukernavn. Siden denne maskinen på forhånd fikk tildelt en bruker, ble brukernavnet automatisk lagt inn og visningsnavnet er det samme som vist i figur 40.

Denne brukeren har en E5 lisens og med den følger det med lisens for Windows 10. Dermed er varselet om å aktivere Windows blitt borte. Legg også merke til firkanten før "Hi AAD Admin!", som er logoen som ble lagt inn i Company Branding, i avsnitt 3.4.



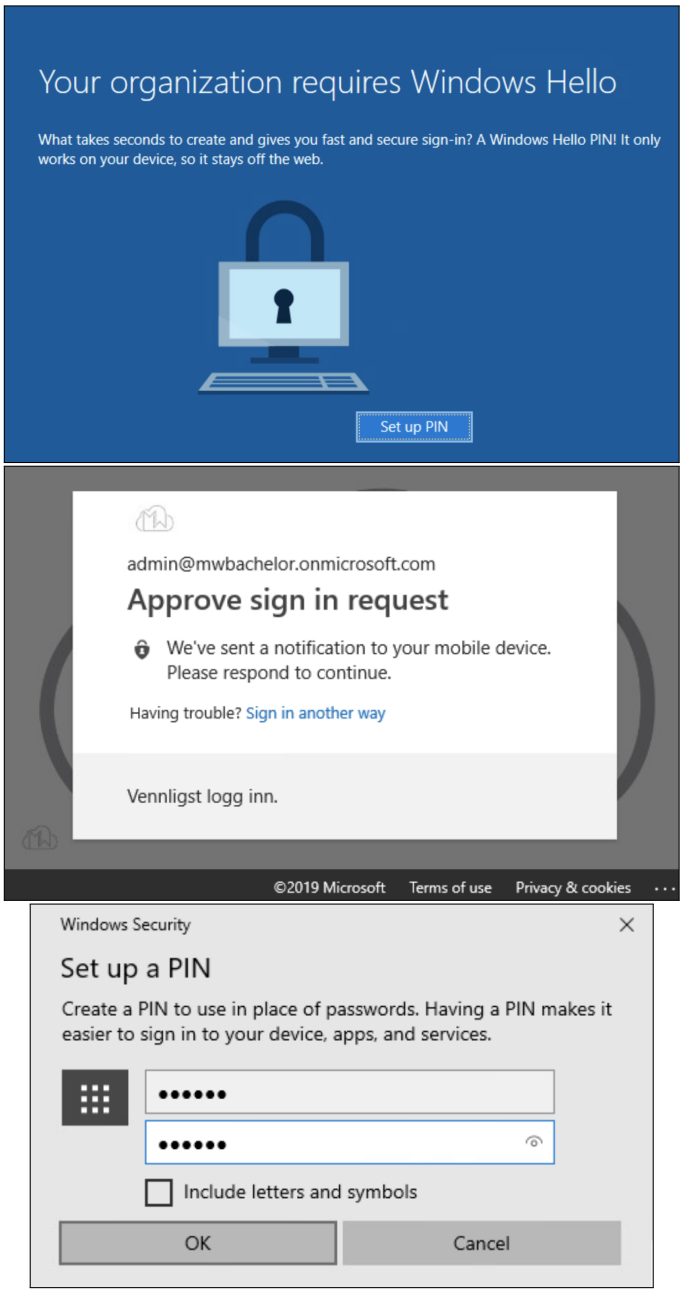
Figur 40

Når passordet skrives inn er det enda noen sekunder med lasting før man presenteres med Windows 10s innloggingsskjerm.



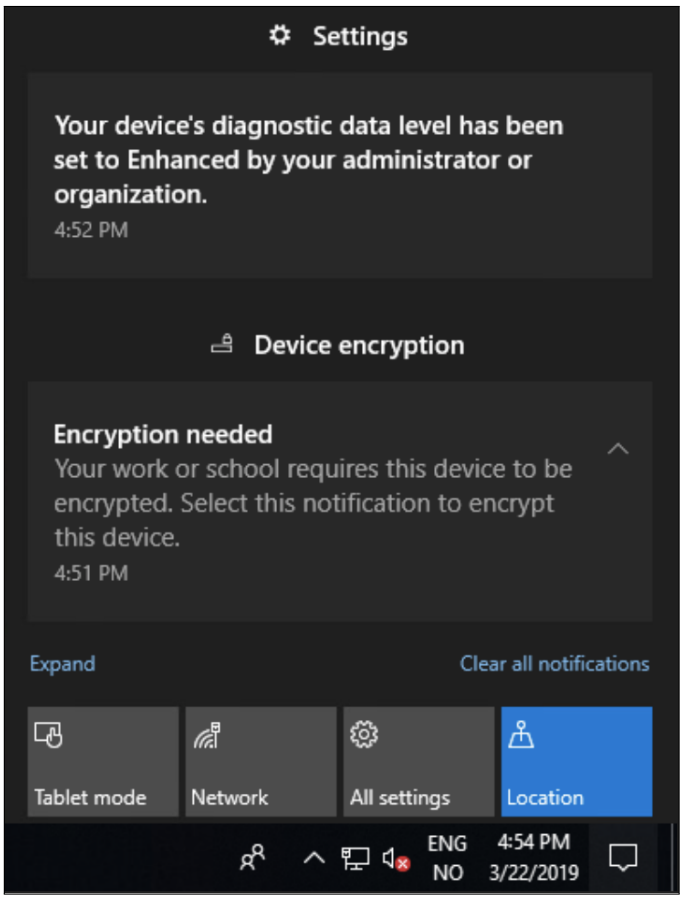
Figur 41

Når brukeren forsøker å logge inn for første gang vil allerede policies som Windows Hello og MFA være tredd i kraft. Dette vil se ut som i figur 42.



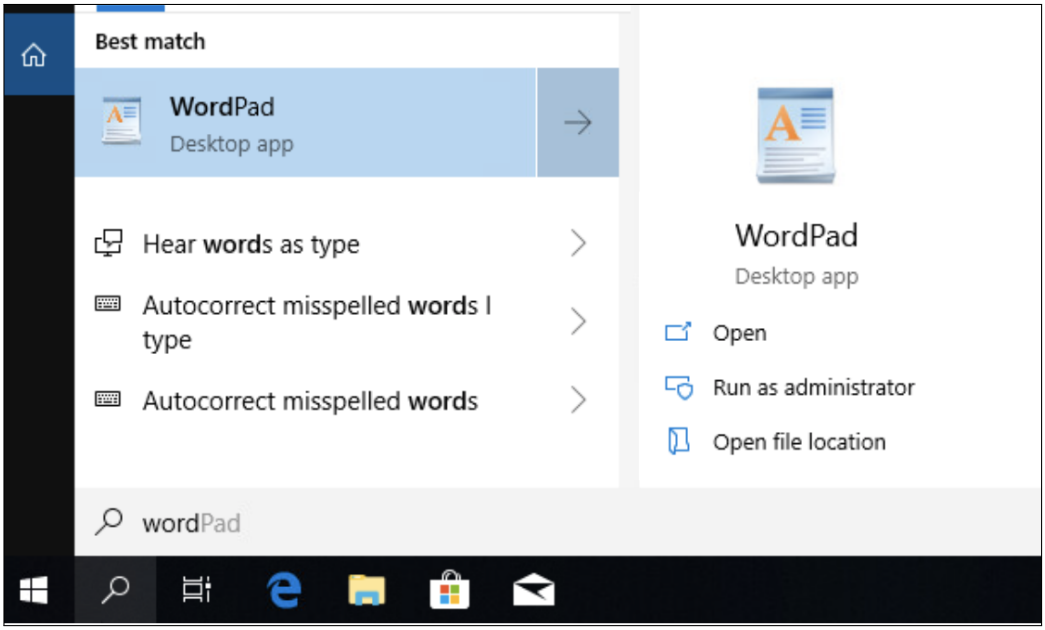
Figur 42

Når en er logget inn dukker det opp et varsel om at maskinen overvåkes og sender diagnostiske data til organisasjonen. Et annet varsel minner på om at en Endpoint Protection-policy krever at BitLocker aktiveres.



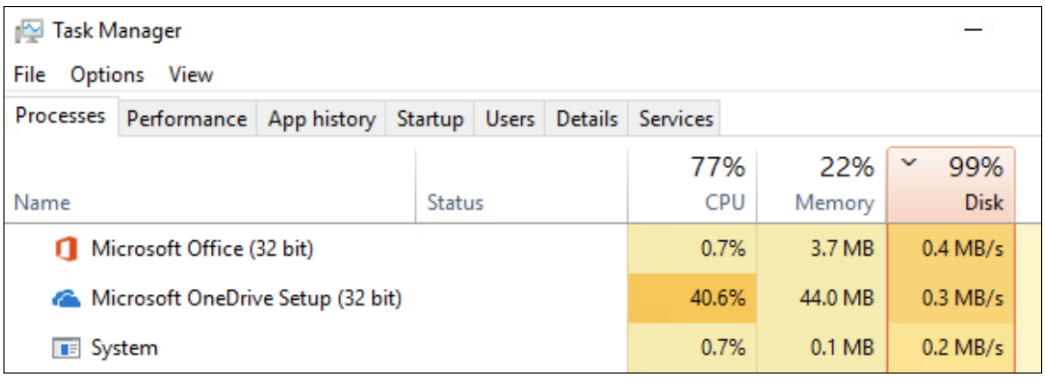
Figur 43

Vi kan se i figur 44 at umiddelbart etter autopilotprosessen, er Office-pakken fortsatt ikke installert enda. Dette illustreres ved at et søk etter “Word” kun vil gi resultatet “WordPad” og ikke “Microsoft Word”.



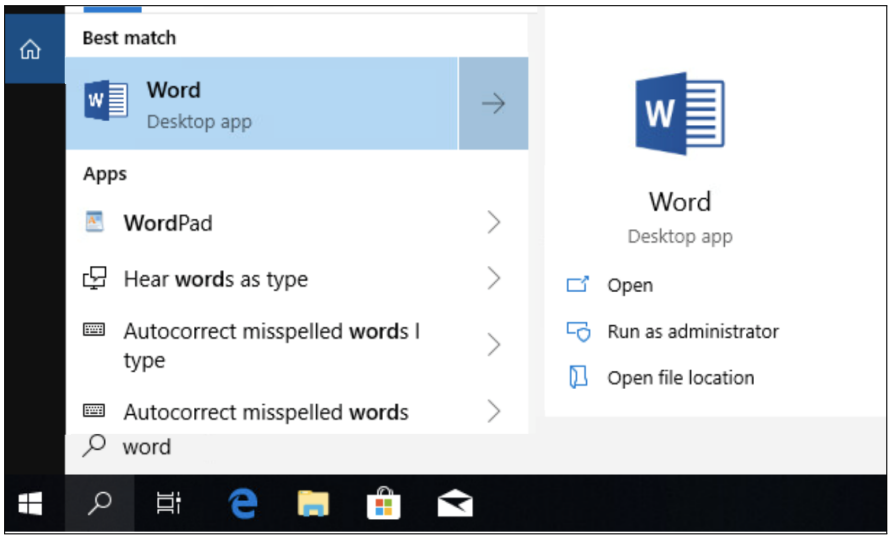
Figur 44

Vi åpner så oppgavebehandling for å se hvilke prosesser som kjører, og her kommer det frem at Office-installasjonen kjører i bakgrunnen.



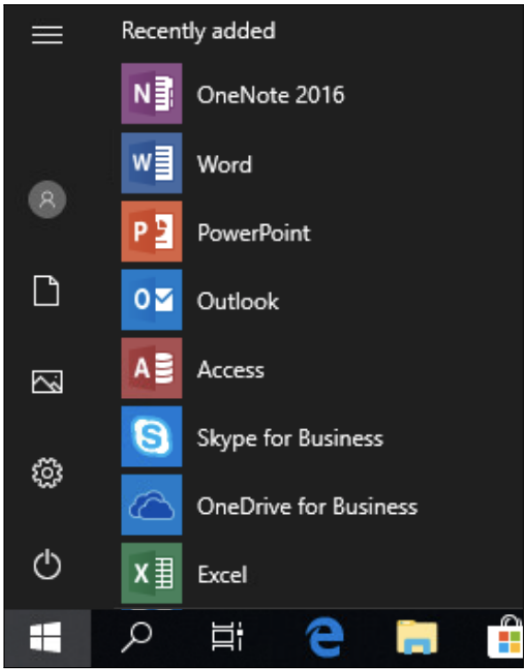
Figur 45

Etter kort tid vil Office-pakken være klar for bruk, og vi kan nå finne Word, som vist i figur 46.



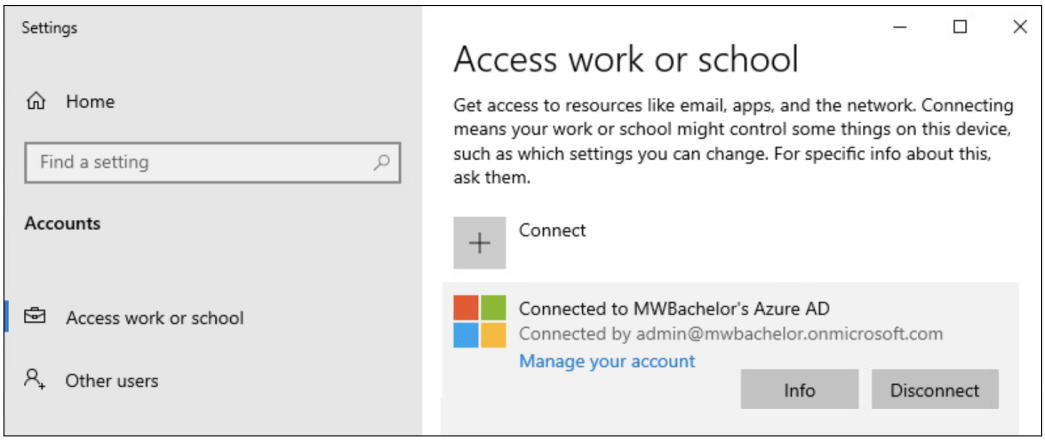
Figur 46

Som vist i figur 47, er resten av Office-pakken også installert på maskinen.



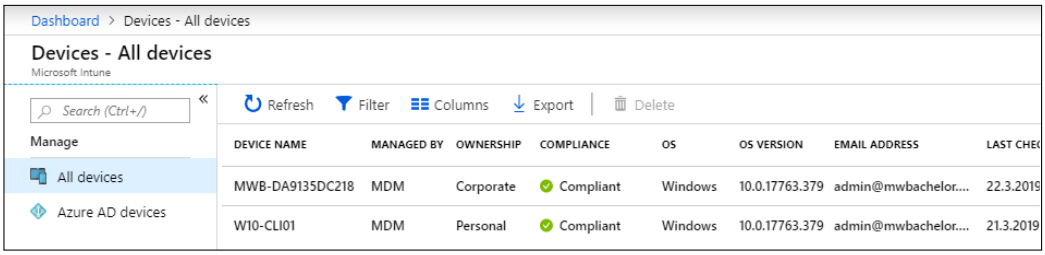
Figur 47

I innstillingene på maskinen kan det verifiseres at maskinen er koblet opp imot Azure AD og benytter Intune som MDM. Det er også ingen lokal administratorkonto. På bildet er det en administrator som er logget inn, og dermed er det mulighet for å fjerne tilknytningen til AAD og Intune. Denne muligheten vil ikke være tilgjengelig for en vanlig bruker, og det vil ikke være mulig for de å trykke "Disconnect".



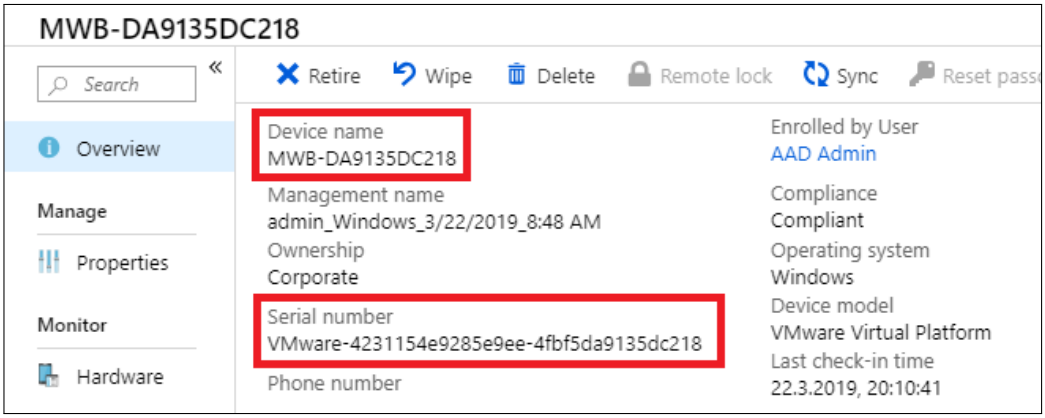
Figur 48

Tilbake i Azure har maskinen dukket opp. Maskinens eierskap er satt til "Corporate" og den har fått navn som følger navnestandarden "MWB-%SERIAL%som spesifisert i autopilotprofilen.



Figur 49

Det kan bekreftes at dette er den samme maskinen ved å klikke på den og sjekke at serienummeret stemmer overens med figur 13. Som vi ser i figur 50, stemmer serienummeret overens med det i figur 13.



Figur 50

4 Autopilot – Hybrid-Join

Autopilotprosessen kan konfigureres til å melde maskinene inn å både Azure AD og lokalt AD. Prosessen med hybrid-join er mye lik andre autopilot prosesser, men det kreves noe mer konfigurasjon for at maskinene skal bli registrert i lokal AD.

Når prosessen er i gang vil Autopilot melder maskinen inn i Intune. Så vil Intune be Intune Connector om å opprette ett maskin objekt i lokal AD. Dette vil generere en ODJ blob (offline domain join). Denne ODJ blob-en sendes tilbake til Intune, som sender den videre til maskinen. Når sluttbruker logger inn, vil maskinen være tilknyttet det lokale domenet[2].

Krav til oppsett av hybrid-join[3]:

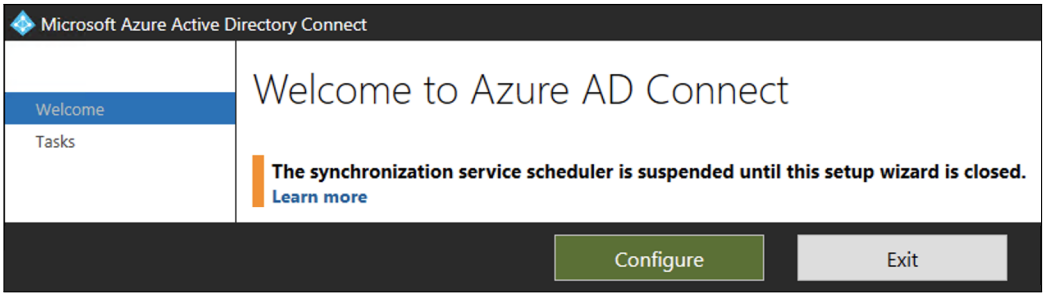
- Windows 10 versjon 1809
- Internett-tilkobling
- Direkte tilgang til Active Directory (VPN ikke tilstrekkelig)

4.1 Azure AD Connect

Før maskiner automatisk kan innmeldes i lokal AD kreves en kobling mellom Azure AD og lokal AD. Denne koblingen skjer gjennom bruk av Azure AD Connect, som er en programvare levert av Microsoft.

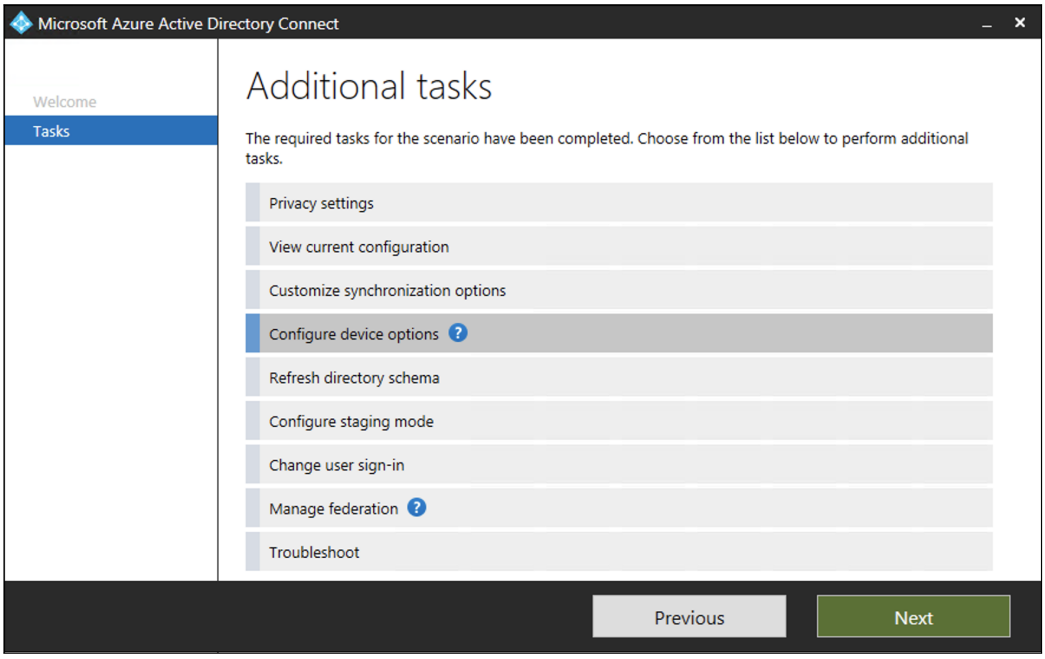
Første steg vil være å hente programvaren fra Azure-portalen. Den kan hentes fra “Azure AD Connect” inne i “Azure Active Directory”. Dette dokumenteres i “Driftsdokument - AD Connect”.

Åpne så programvaren på en maskin innlemmet i det lokale domene eller på den lokale AD-serveren som administrator. Du vil bli møtt av en veiviser, hvor du må trykke “Configure” for å starte prosessen.



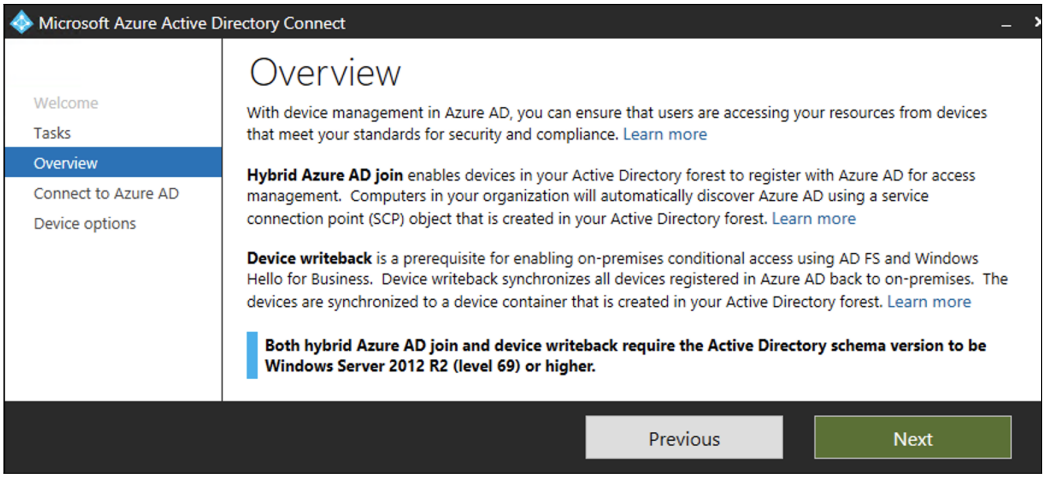
Figur 51

Du vil så bli møtt med en rekke mulige oppgaver som kan gjennomføres. Vi velger her “Configure device options” og trykker så “Next”.



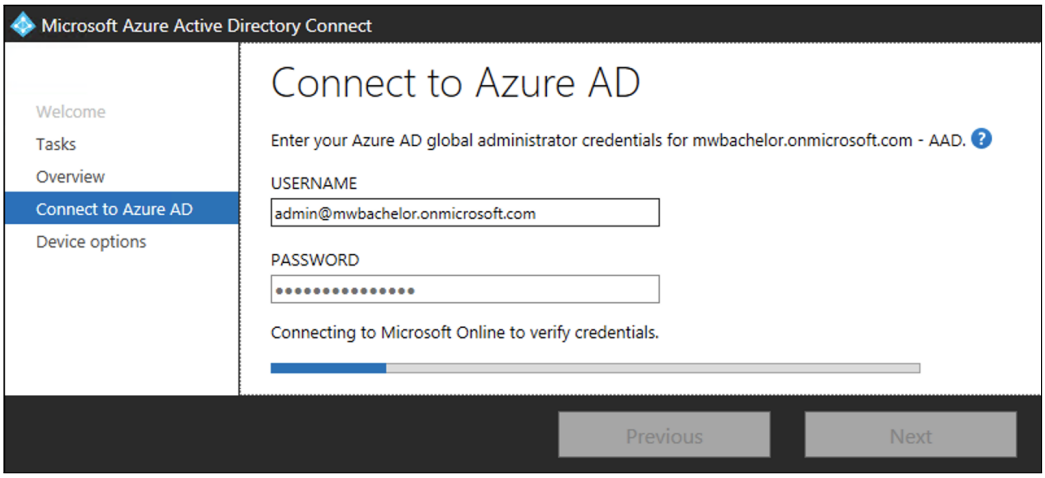
Figur 52

Det vil så komme en beskrivelse av hva som vil foregå, hva Hybrid-join og Device writeback er og gjør. Les nøye gjennom slik at du er sikker på at du ønsker å koble det lokale AD opp mot Azure AD. Trykk "Next" for å komme videre.



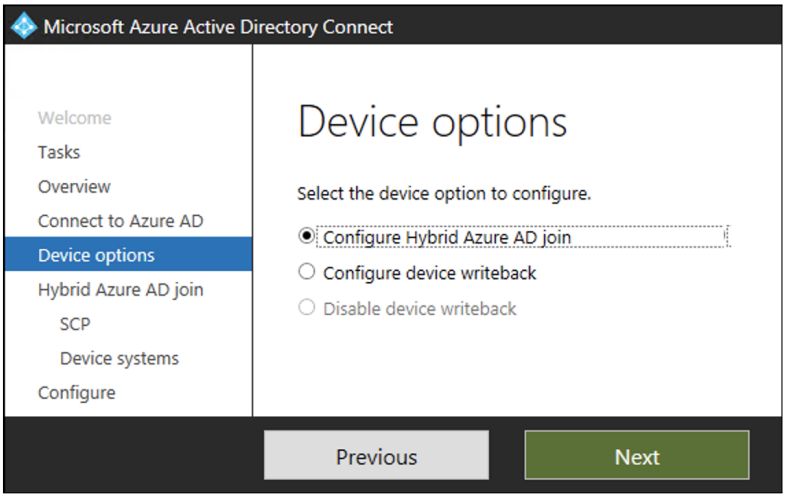
Figur 53

Du vil så bli bedt om å fylle inn brukernavn og passord for en global administrator i din tenant. Etter å ha fylt inn dette kan du trykke "Next".



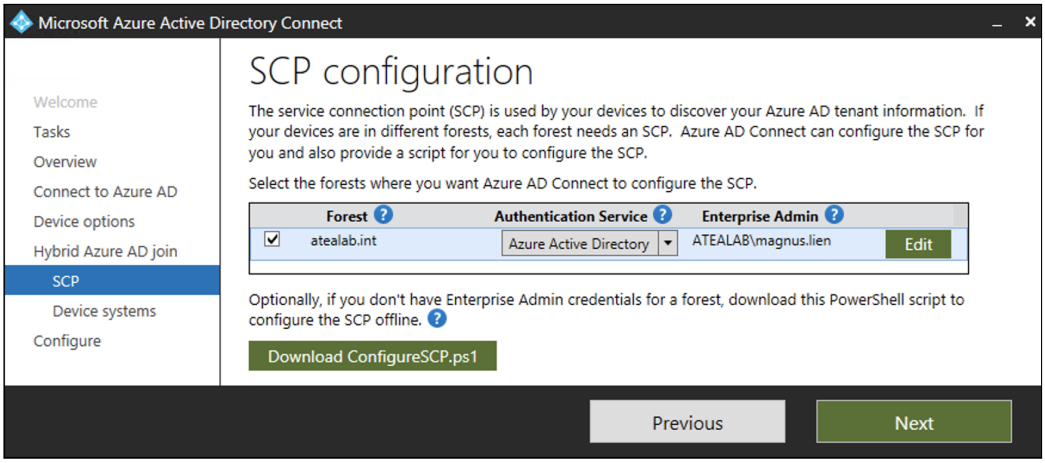
Figur 54

Du vil så få muligheten til å velge hva som skal konfigureres. Her er også muligheten for å skru av Device writeback, noe som er nedtonet da det enda ikke er satt opp. Vi velger å konfigurere Hybrid-join ved å huke av "Configure Hybrid Azure AD join". Trykk så "Next" for å begynne konfigurasjonen.



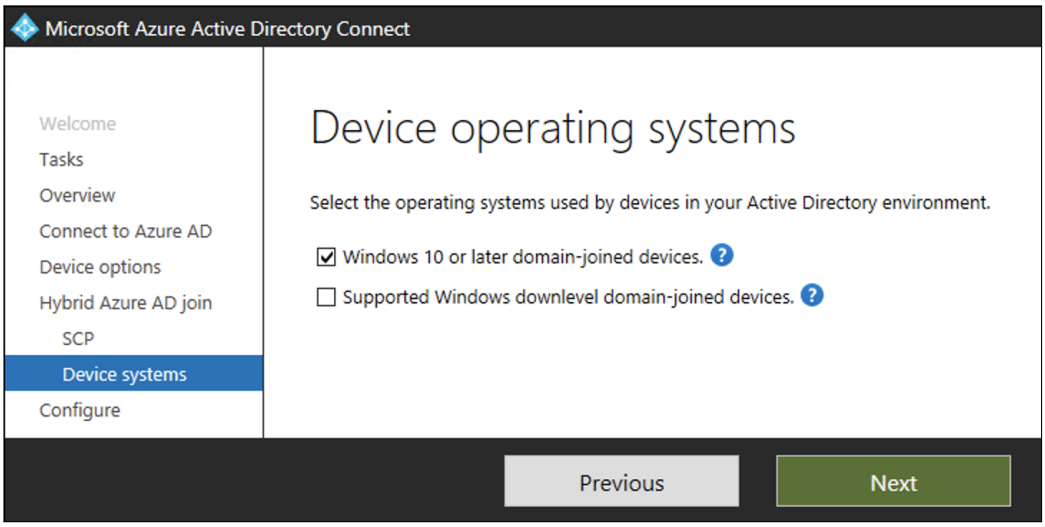
Figur 55

Du vil så måtte konfigurere koblingen som henter informasjon om tenant til enheter, kjent som "Service connection point", SCP. Det må opprettes en egen SCP for hver forest som skal kobles opp mot Azure. Dette steget krever at du logger inn med en Enterprise admin i domenet. Når riktig informasjon er fylt inn, kan du trykke "Next".



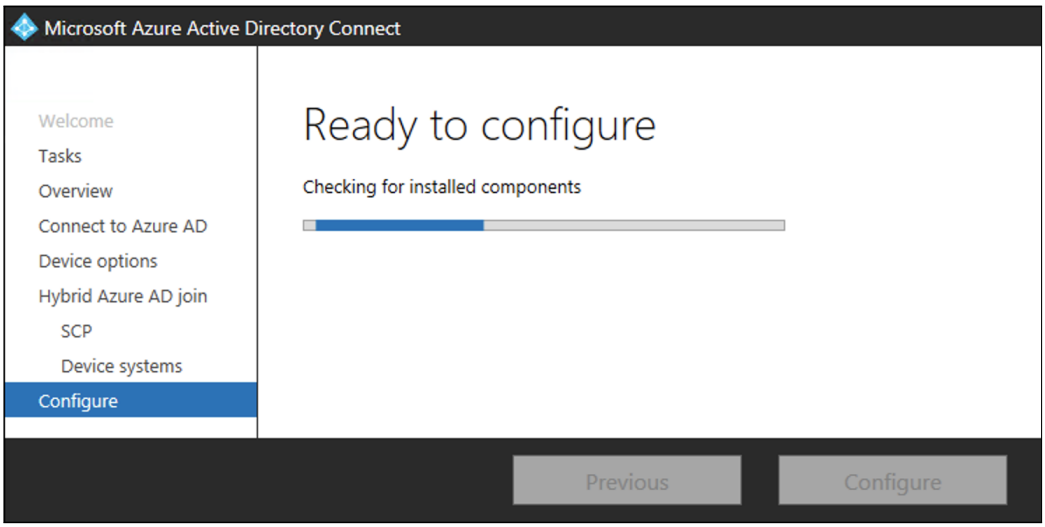
Figur 56

Du vil så måtte velge hvilke OS som blir brukt av enheter i det lokale domenet. Vi velger her å huke av for enheter med Windows 10 og nyere. Trykk så “Next”.



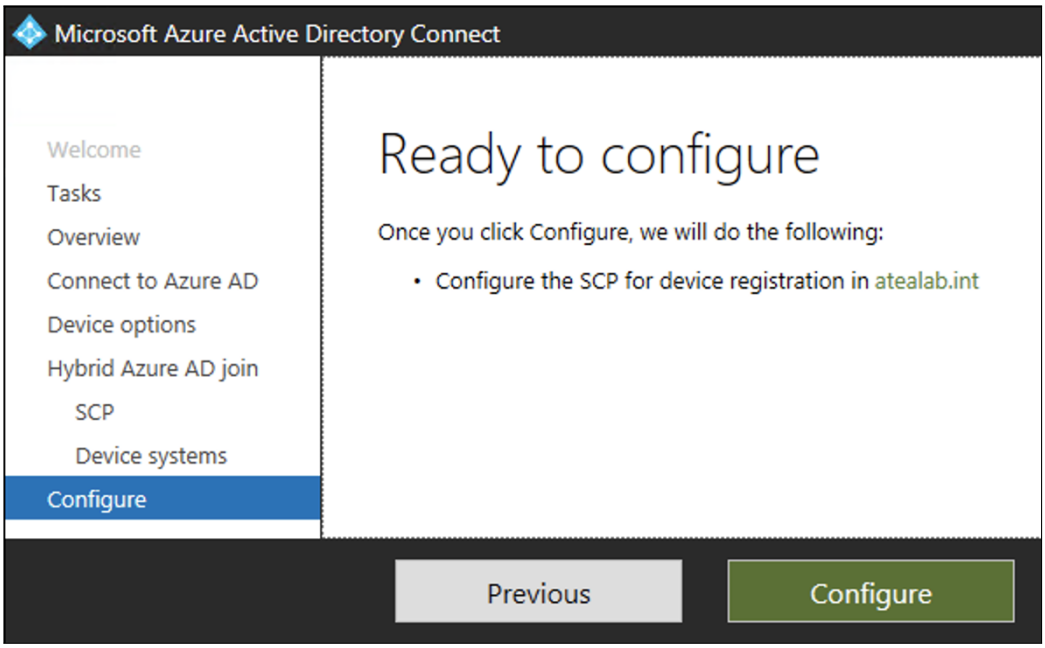
Figur 57

Konfigurasjonsprosessen vil nå sjekkes for mulige feil og klargjøres. Dette vil ta en liten stund.



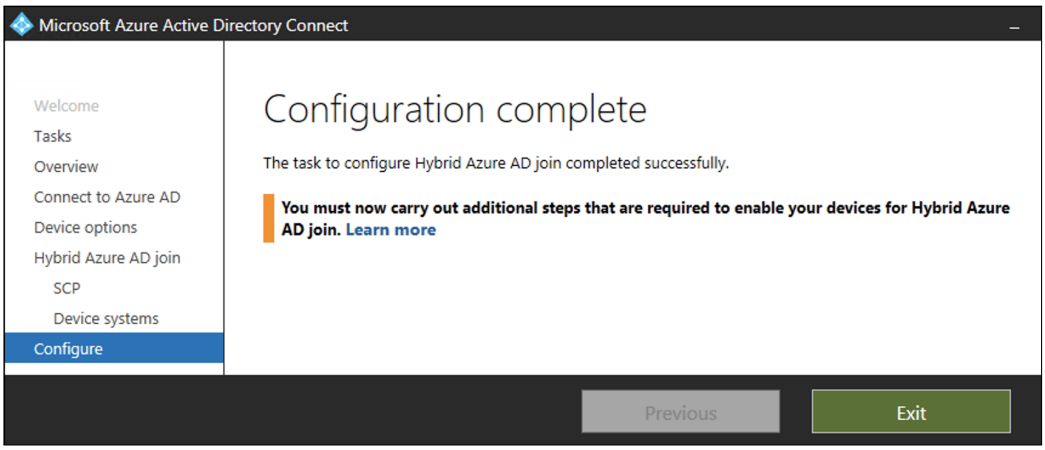
Figur 58

Når prosessen har blitt gjennomgått og godkjent er det bare å velge “Configure” for å starte konfigureringen.



Figur 59

Når konfigurasjonen er over vil vinduet indikere om prosessen var vellykket. Som vist i figur 60, gikk konfigurasjonen uten feil i vårt tilfelle.



Figur 60

4.2 Intune Connector

For å kunne tilby Autopilot til enheter gjennom lokal AD kreves en kobling opp imot Intune. Denne muligheten er i en prøvefase, også kjent som "Preview" per mai 2019. Dette kan medføre at det oppstår feil uten at det finnes en god løsning.

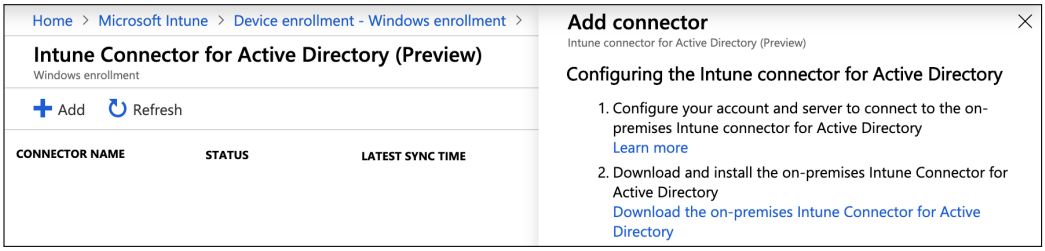
For å sette opp en kobling til Intune kreves:

- Windows Server 2016 eller nyere OS
- Maskinen må være meldt inn i lokalt domene

Første steg vil være å laste ned Intune Connector. Filen hentes fra Intune inne i Azure-portalen. I Azure-portalen velg "Intune", "Device enrollment", "Windows enrollment" og deretter "Intune Connector for Active Directory".

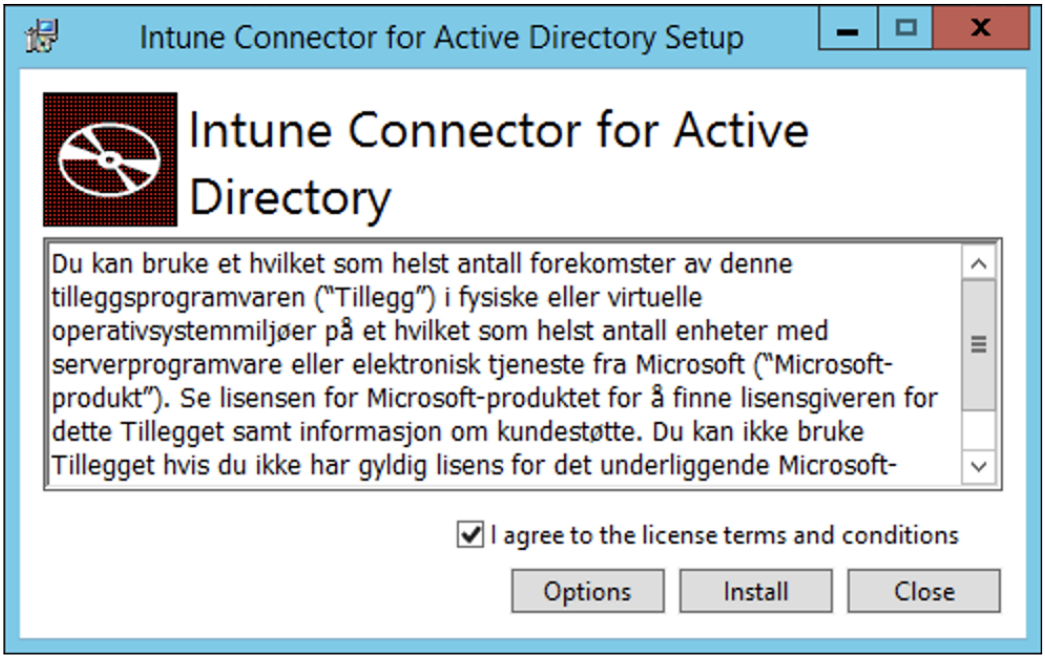
Figur 61

Her inne velger du "Add". Det vil dukke opp et lite vindu med informasjon og lenker. Klikk på lenken som omtaler nedlastning av Intune Connector og vent mens filen lastes ned.



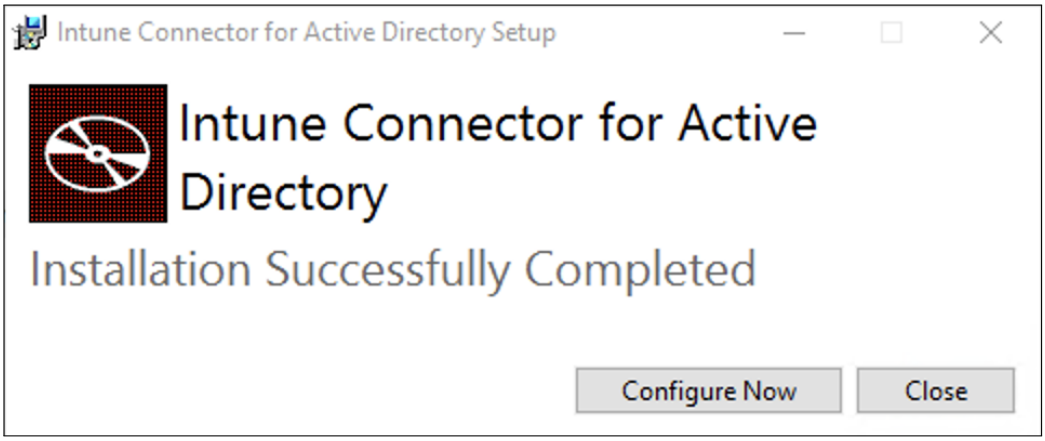
Figur 62

Åpne filen som administrator på maskinen. En veiviser vil starte, godta vilkår før du velger “Install”.



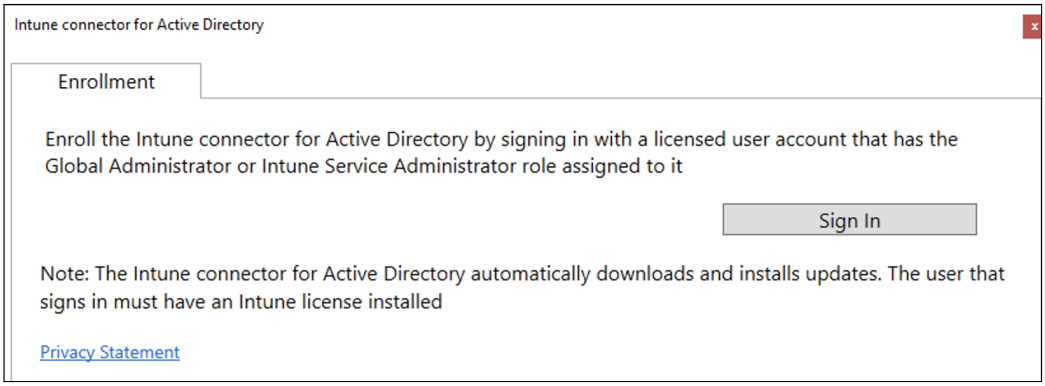
Figur 63

Installasjonen vil ta en kort stund, og det vil dukke opp et vindu som informerer om alt gikk bra eller det oppsto problemer. Som vist i figur 64, var vår installasjon vellykket. Vi kan nå begynne konfigurasjonen av Intune Connector ved å klikke “Configure Now”.



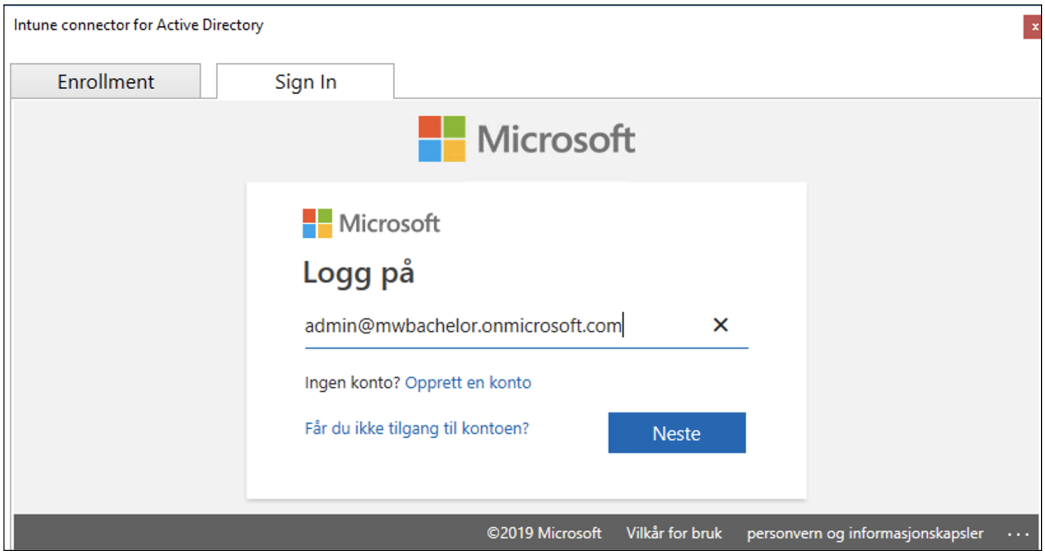
Figur 64

Du vil så måtte logge inn med en bruker som enten er global administrator i tenant, eller en bruker med Intune Service Administrator-rolle. Logg inn ved å klikke på "Sign in".



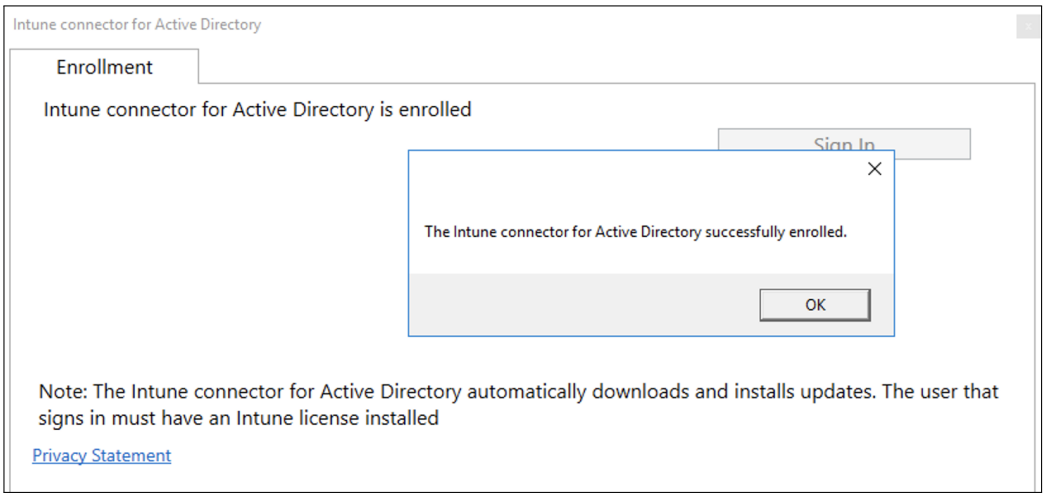
Figur 65

Fyll inn brukernavn og passord, og klikk "Neste".



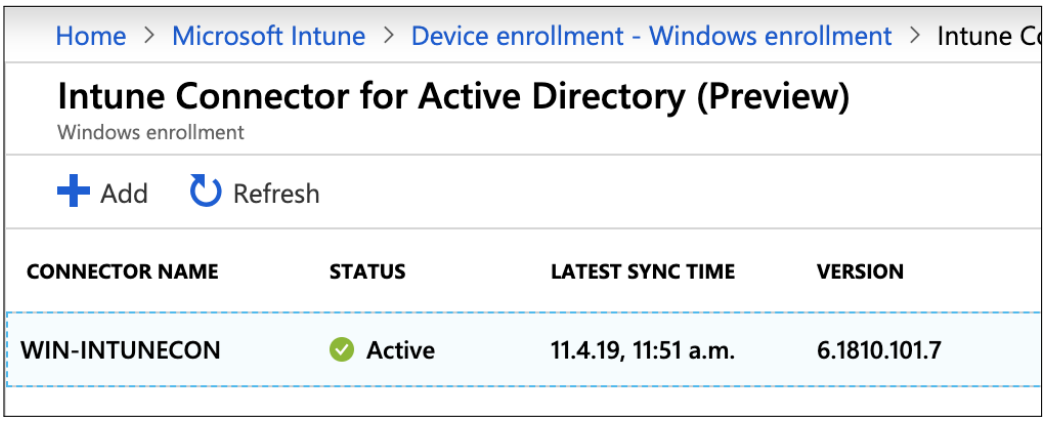
Figur 66

Det vil så komme opp et vindu som informerer om Intune Connector enrollment var vellykket. Som vist i figur 67, var enrollment vellykket i vårt tilfelle.



Figur 67

Åpne deretter Intune for å sjekke om koblingen er aktiv. Som vi ser i figur 68 er koblingen aktiv med “WIN-INTUNECON” som navn.

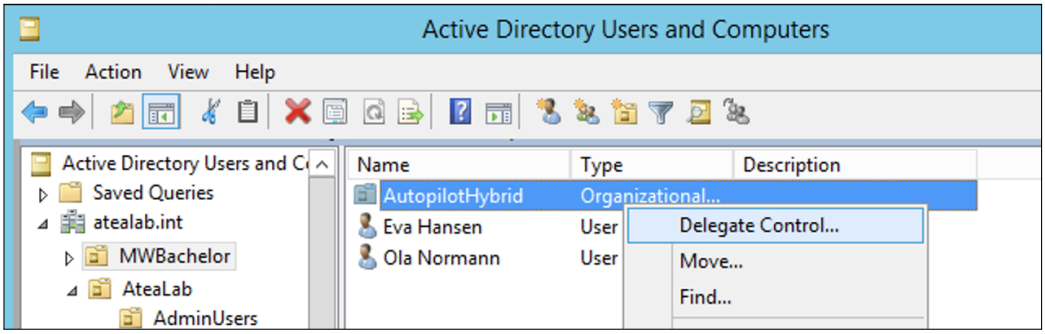


Figur 68

4.3 OU for Autopilot-maskiner

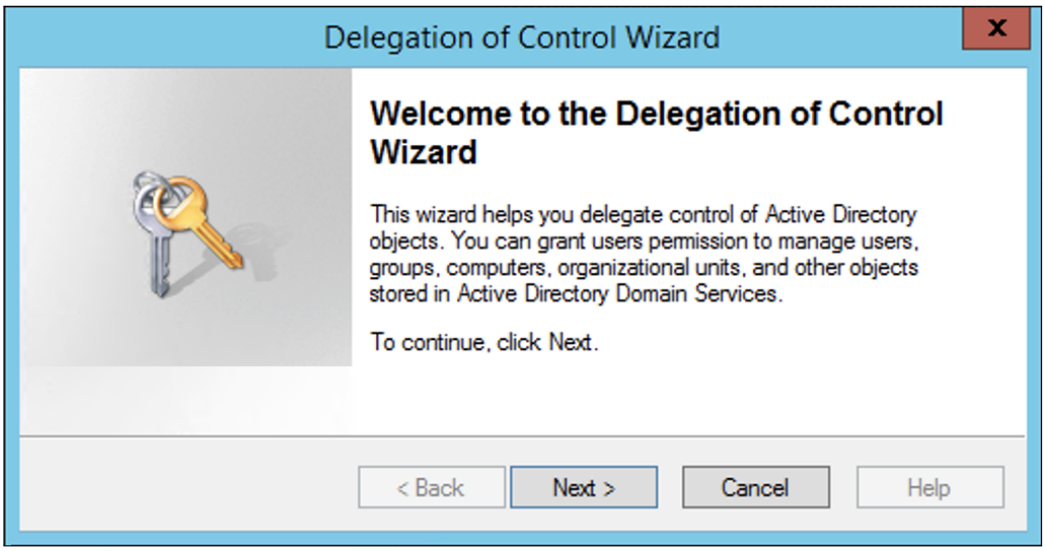
For at koblingen vi opprettet skal kunne la Intune legge til og fjerne enheter fra et OU i lokal AD, må en delegere kontroll over OU. Denne delegeringen foregår på lokal AD-maskin og krever at du er innlogget som administrator.

Første steg vil være å delegere kontroll til koblingen som ble oppsatt under avsnitt 4.2 Intune Connector. Logg inn som administrator på AD-server og naviger til OU som skal kontrolleres av koblingen. Høyreklikk på OU og velg "Delegate Control".



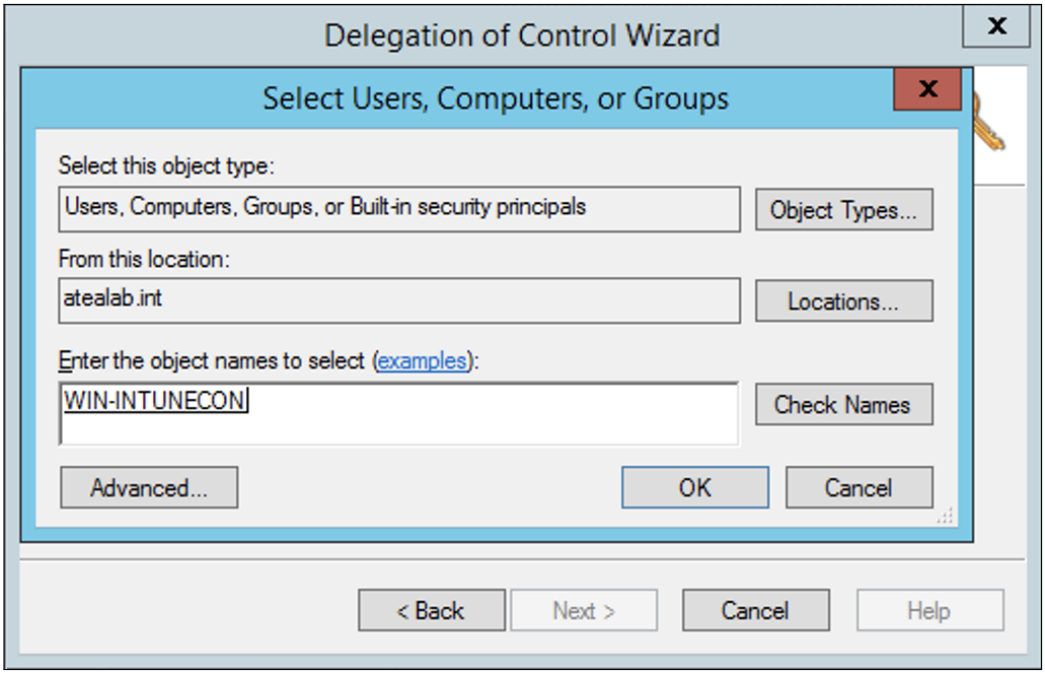
Figur 69

Det vil dukke opp en veiviser som vil la deg konfigurere delegering av kontroll. Velg her "Next" for å begynne delegeringen.



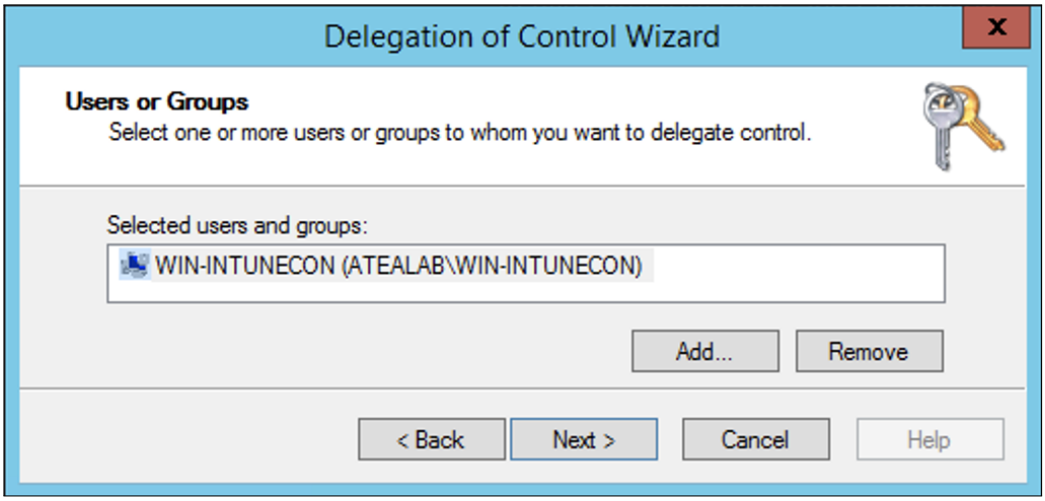
Figur 70

Trykk “Add” på vinduet som dukker opp. Finn deretter koblingen ved å søke etter koblingens navn, i vårt tilfelle “WIN-INTUNECON”. Velg så “OK”



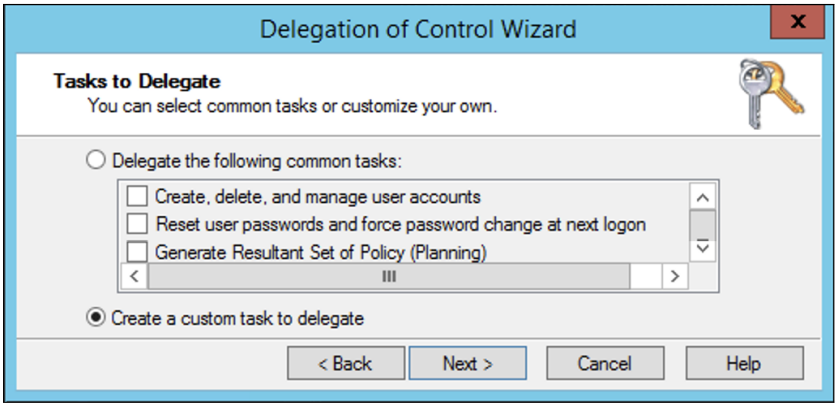
Figur 71

Når koblingen er valgt og vises under “Selected users and groups” kan du trykke “Next”.



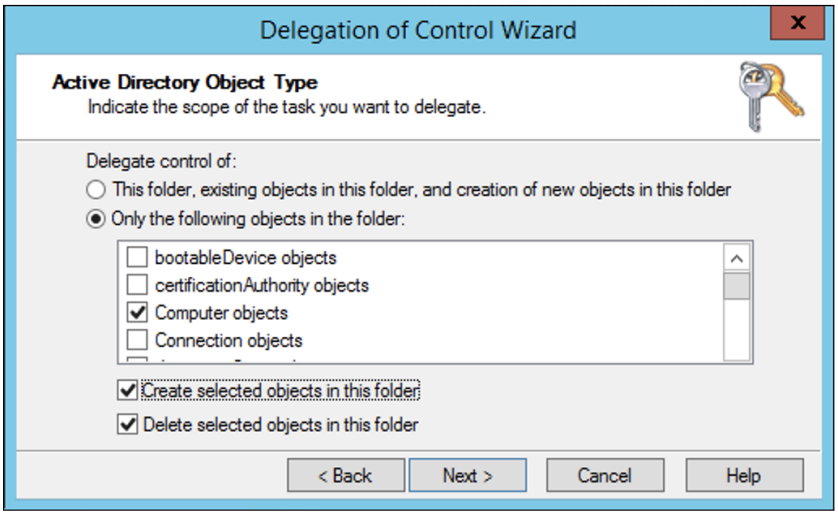
Figur 72

Det vil så komme mulighet for å velge hva slags oppgaver koblingen skal få delegert. Her kan vi velge fra en liste, men vi ønsker å lage en egen oppgave, noe som gjøres ved å huke av for "Create a custom task to delegate". Trykk deretter "Next".



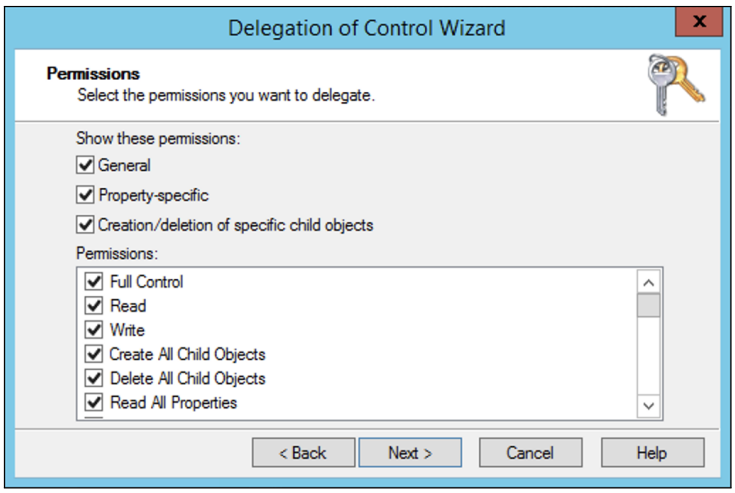
Figur 73

Vi får så muligheten til å delegere kontroll over mappen med nåværende og kommende innhold, eller kun spesifikke objekter. Vi ønsker kun at koblingen skal ha kontroll over maskin-objekter, noe som gjør at vi huker av for "Computer objects" under "Only the following objects in the folder:". Huk også av for "Create selected objects in the folder" og "Delete selected objects in this folder" for at koblingen skal kunne legge til nye og fjerne objekter fra OU. Trykk så "Next".



Figur 74

Tillatelser må så gis til koblingen, hvor vi ønsker å gi den full tilgang i mappen. Huk derfor av alle mulige tillatelser, kjent som “Permissions”, som vist i figur 75, og trykk “Next”.



Figur 75

Et siste vindu vil la deg gå gjennom valgene som ble tatt i løpet av veiviseren. Her anbefales det å gå nøye gjennom for å sikre at koblingen har de rettighetene og tillatelsene som kreves. Når dette er gjort kan veiviseren ferdigstilles ved å klikke “Finish”.

Figur 76

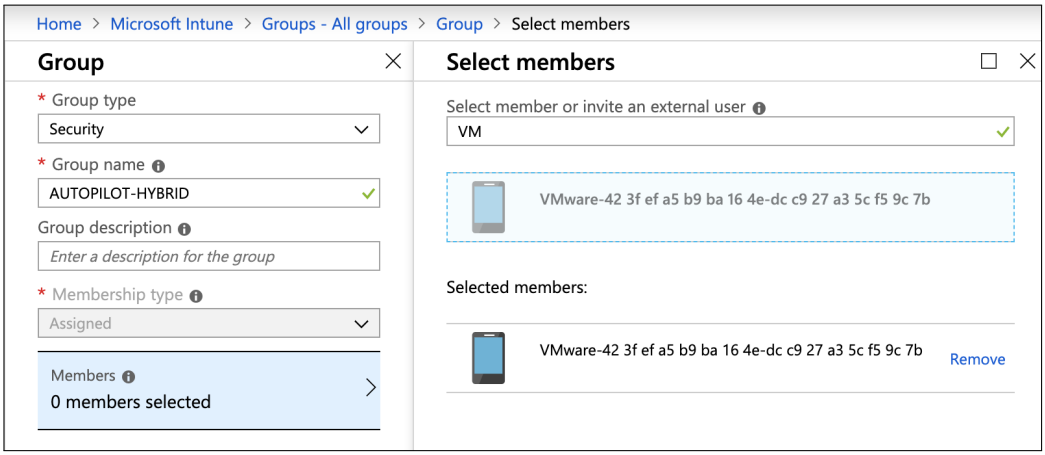
4.4 Maskingruppe

For å kunne opprette en autopilotprofil som kun vil gjelde for maskiner med enrollment gjennom hybrid-join, kreves det at det opprettes en maskingruppe for disse. Denne gruppen må inneholde alle enhetene som skal settes opp via hybrid-join.

Første steg for oppretting av maskingruppe vil være å navigere til punkt for oppretting av grupper i Azure-portalen. Inne i Azure-portalen, velg "Intune" og "Groups". Her inne kan du trykke "New Group".

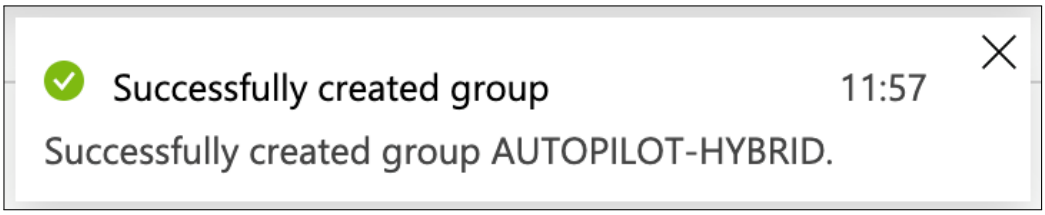
Figur 77

I vinduet som dukker opp må vi fylle inn gruppens navn, type, medlemstype og vi må legge til medlemmer. Informasjonen som skal fylles inn vises i figur 78. Gjennomgå at gruppen har riktig informasjon lagt til og at det er lagt til riktige medlemmer. Når dette er gjort kan du trykke "Create" for å opprette maskingruppen.



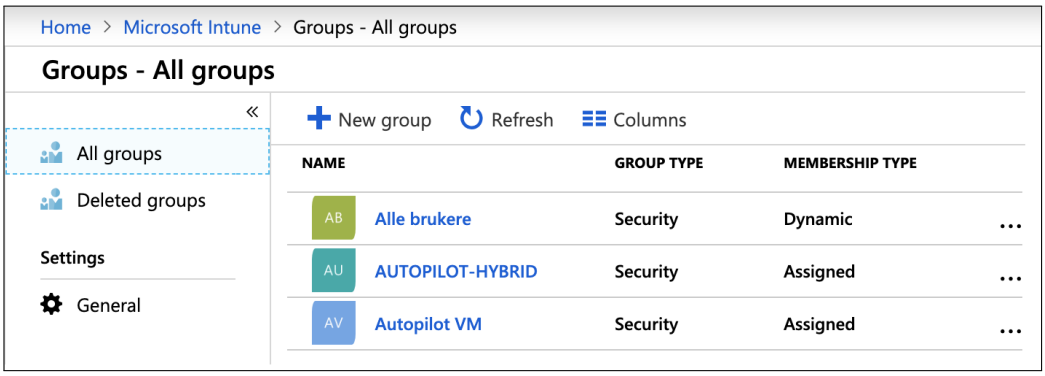
Figur 78

Det vil så komme opp en notifikasjon som informerer om gruppen ble opprettet feilfritt eller om feil oppsto. Som vist i figur 79, ble gruppen opprettet uten feil.



Figur 79

Vi kan så se at gruppen ligger sammen de andre gruppene i Intune.

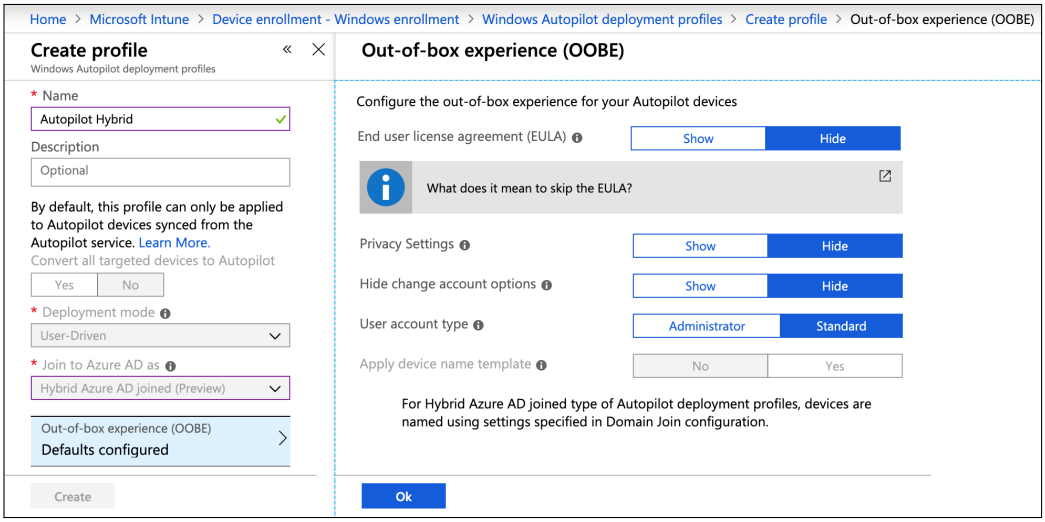


Figur 80

4.5 Hybrid-Join Profil

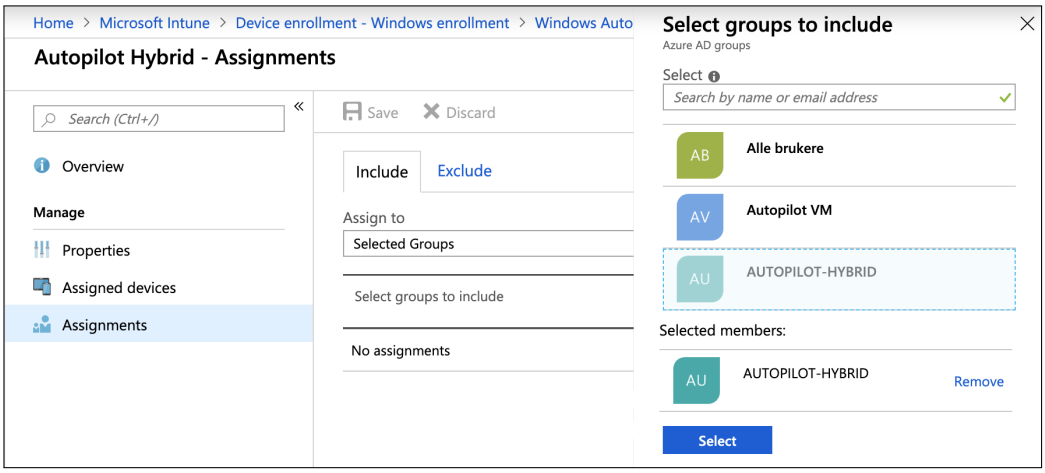
En av de største forskjellene mellom "vanlig" autopilot og autopilot med hybrid-join er selve autopilotprofilen. På figur 81 opprettes det en profil til bruk med hybrid-join. Det er navigert til Intune, lagt "Device enrollment", "Windows enrollment" og "Deployment Profiles". Der er det bare å opprette en ny profil. Her er profilen gitt et passende navn og satt til "User-Driven". I feltet for "Join to Azure AD as" er det valgt "Hybrid Azure AD joined", dette valget er bare mulig å velge i moduset "User-Driven".

Selve OOBE-konfigurasjonen er mye lik figur 20, men med hybrid-join vil det være en "Device configuration"-profil som gir navn til enheten. Dermed er det ikke mulig å sette en navnestandard på slike enheter.



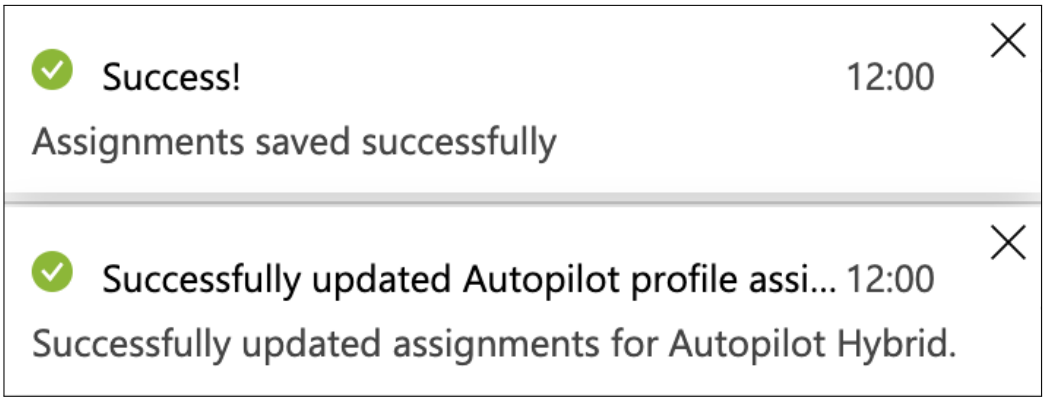
Figur 81

Velg hvilke grupper profilen skal tildeles og lagre tildelingen.



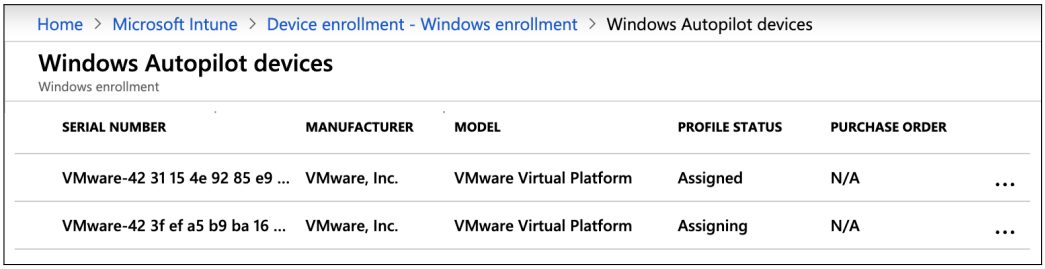
Figur 82

Varselet på figur 83 viser at profilen ble oppdatert og at tildelingen ble lagret.



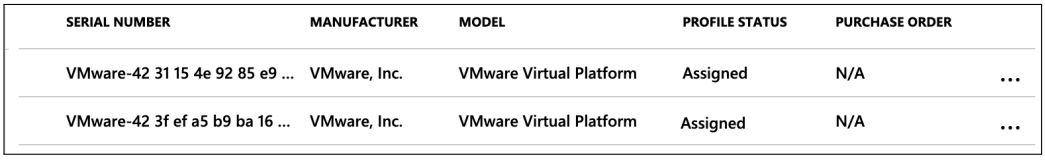
Figur 83

I listen over autopilotenheter må en vente på at "Assigning" går over til "Assigned".



Figur 84

Vi kan se overgangen av profilstatus fra "Assigning" i figur 84, til "Assigned" i figur 85.

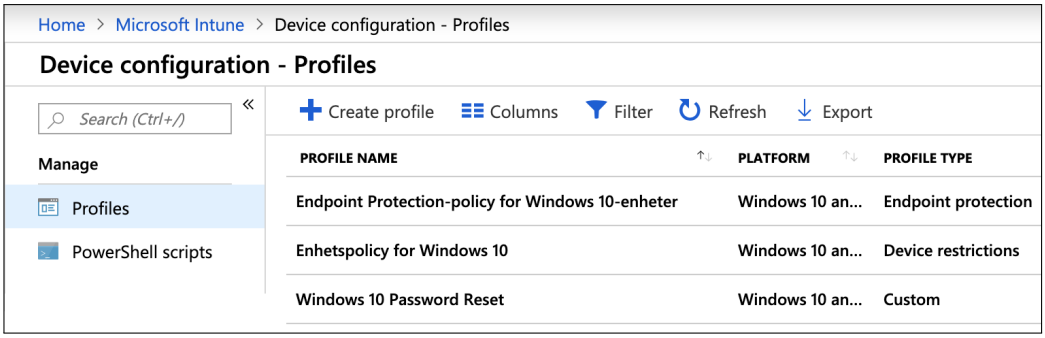


Figur 85

4.6 Domenekonfigurasjon

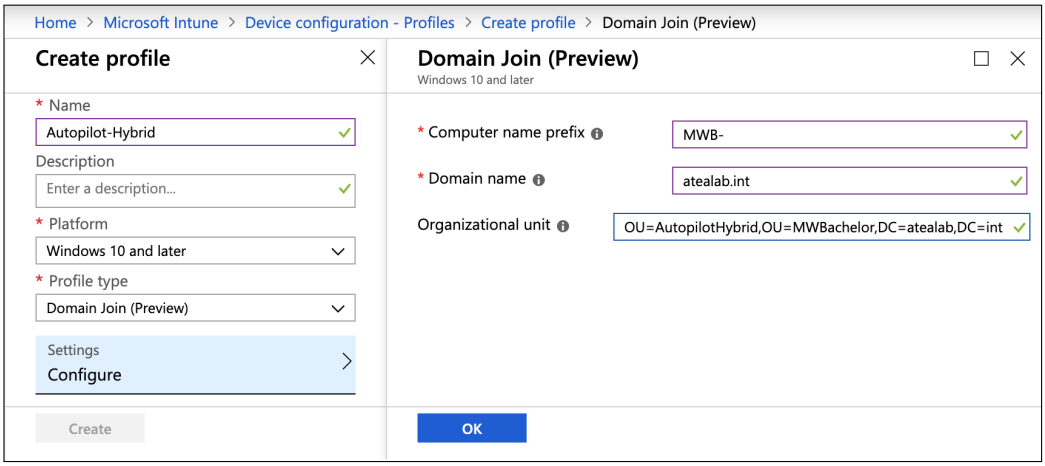
For at Autopilot skal kunne melde maskinene inn i det lokale domenet må det opprettes en profil med domeneinformasjon som domenenavn og OU. Dette utføres med en profil for enhetskonfigurajon av typen “Domain Join”.

Naviger til Device configuration”i Intune og opprett en ny profil.



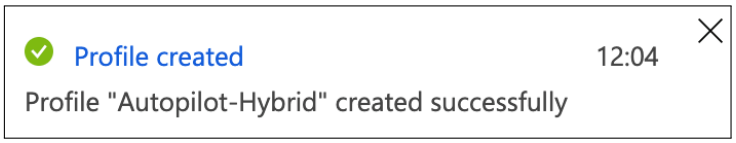
Figur 86

Gi profilen et passende navn og velg at den skal gjelde for Windows 10 og eldre. Profilen skal være av typen “Domain Join”. Under innstillingene til profilen spesifiseres en prefiks for maskinnavnene. I feltet for OU spesifiserer vi den samme OU som maskinen med Intune Connector fikk tilgang til. Avslutt med “OK” og så “Create”.



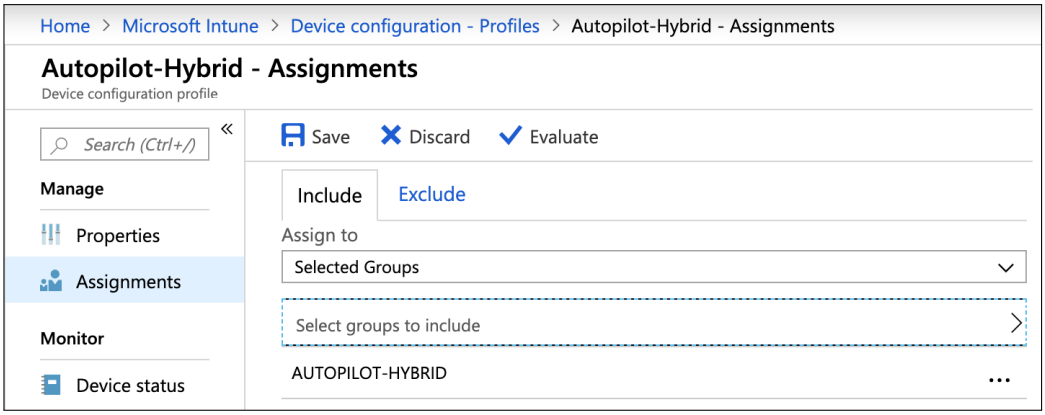
Figur 87

Det vil så dukke opp en notifikasjon som informerer om opprettelse av profil var vellykket. Som vi ser i figur 88, ble profilen opprettet uten feil.



Figur 88

Nå som profilen er ferdig må den tildeles maskinene i gruppen. Dette skjer under ”Assignments”. Vi velger gruppen vi opprettet tidligere, ”AUTOPILOT-HYBRID”, og lagrer ved å trykke Save”.



Figur 89

Det vil så dukke opp en notifikasjon som informerer om tildelingen ble lagret. Som vi ser i figur 88, ble tildelingen lagret uten feil.

Figur 90

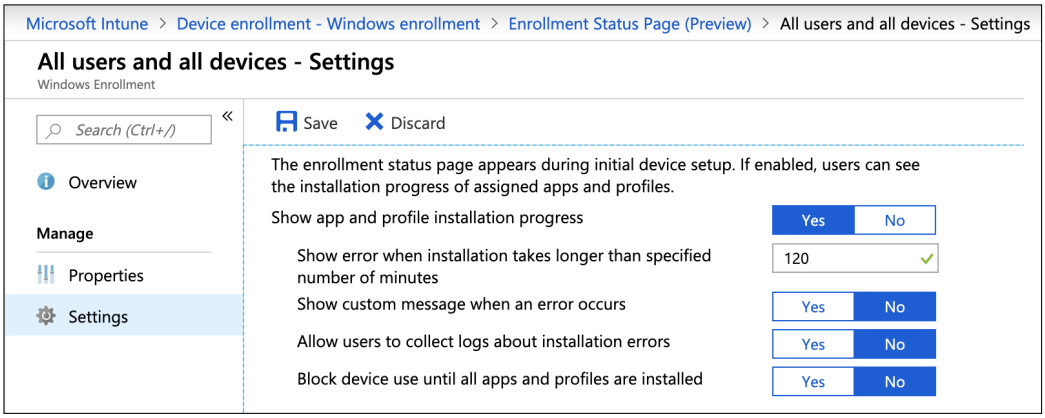
4.7 Enrollment Status Page

For å la brukerne se status og fremgang under oppsett av sin enhet kan en ta i bruk en Enrollment Status Page-profil. Dette vil la brukerne følge med hvor langt i løpet enheten er, og vil være en grei måte å gi brukerne innsikt i hvor lang tid oppsett vil kunne ta.

Første steg vil være å navigere til punkt for "Enrollment Status Page" inne i Azure-portalen. Velg "Intune", "Device enrollment", "Windows enrollment", "Enrollment Status Page (Preview)".

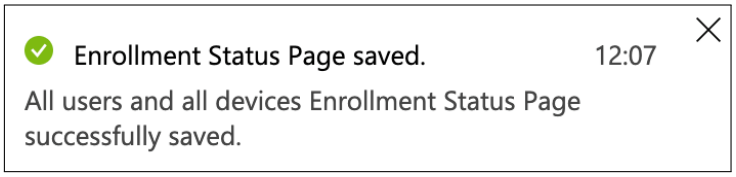
Figur 91

Her kan du velge å lage en ny profil eller redigere standard-profilen. Vi velger å endre standard-profilen. Vi velger her at brukere vil få opp en feilmelding dersom installasjon tar mer enn 120 minutter. Når profilen er konfigurert etter ønske kan en trykke "Save" for å lagre endringer.



Figur 92

Det vil så komme opp en notifikasjon som informerer om endringene ble lagret. Som vist i figur 93, ble endringene lagret uten feil i vårt tilfelle.

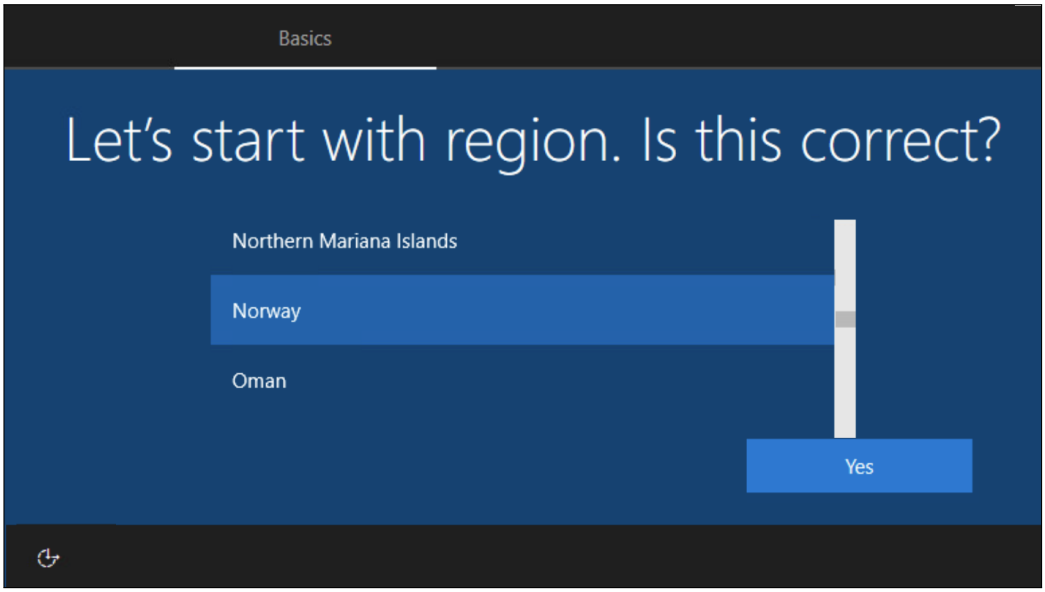


Figur 93

4.8 OOBE - Hybrid Join

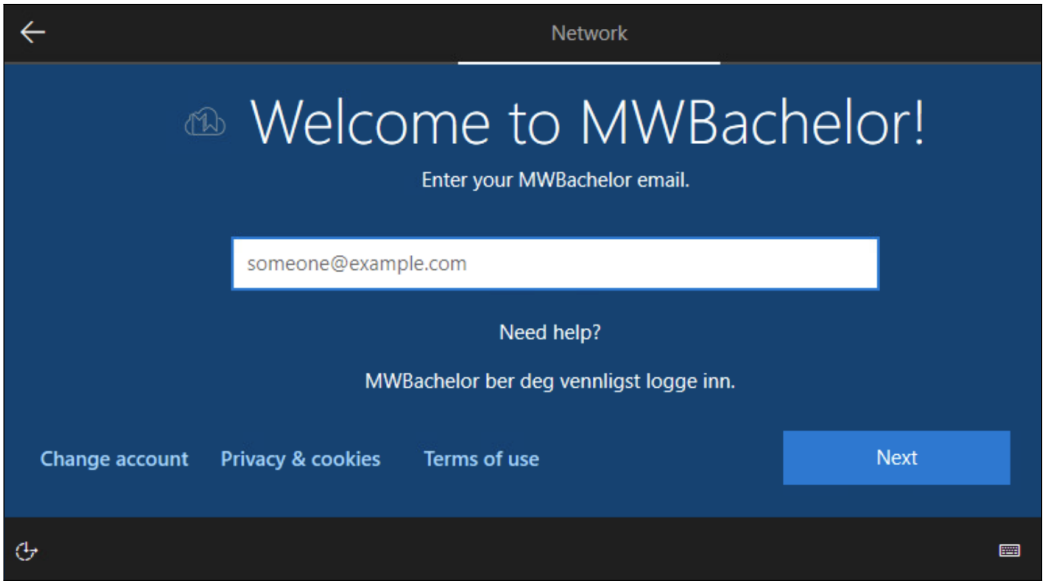
Brukere som får sin autopilot-profil via hybrid-join vil ikke oppleve store forskjeller sammenlignet med de som kun går via Intune. Vi vil uansett gå gjennom førstegangsopplevelsen, da det er visse forskjeller.

Det første brukeren må gjøre er å velge region, språk og tastaturoppsett for sin nye maskin. Dette vil være opp til bruker, men vi velger Norge som region, med engelsk språk og norsk tastatur.



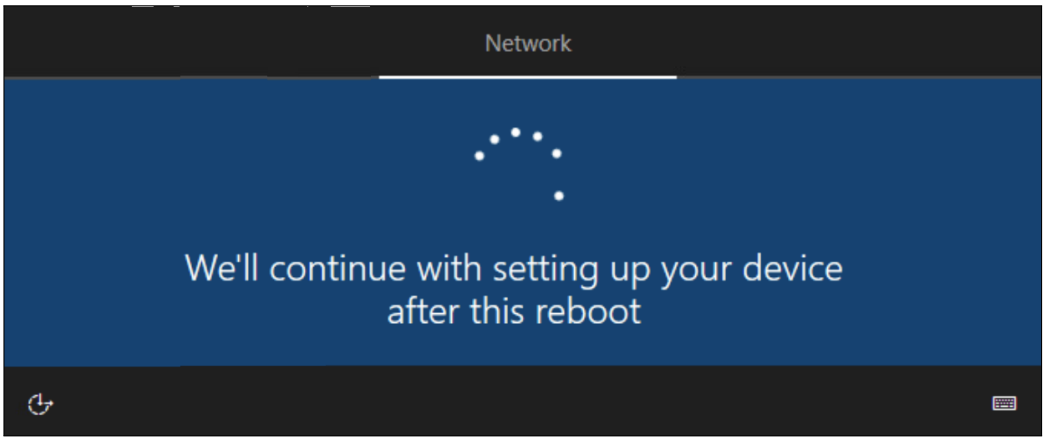
Figur 94

Maskinen vil så bruke en liten stund på å laste inn autopilot-profilen. Det vil deretter dukke opp en mulighet for innlogging til domenet. Bruker må her fylle inn sin innloggingsinformasjon før en trykker “Next”.



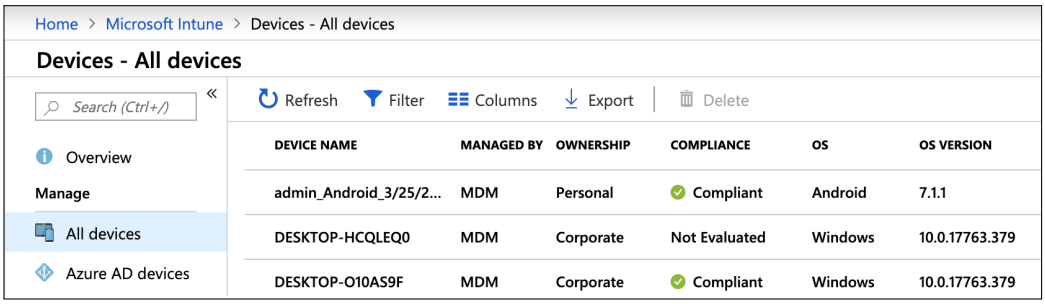
Figur 95

Maskinen vil begynne oppsett fra autopilot-profilen og vil starte på nytt.



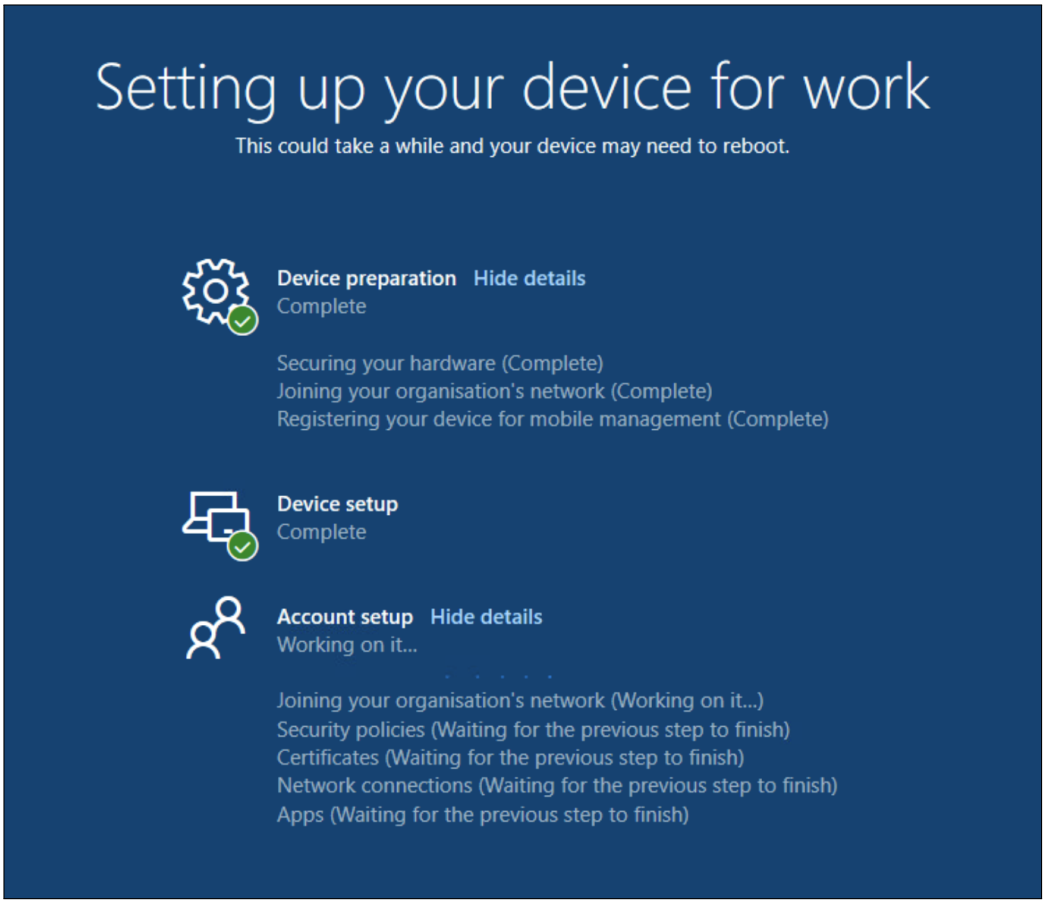
Figur 96

Vi kan nå se at maskinen har dukket opp i Intune som en bedriftseid enhet, men at den fortsatt mangler compliance.



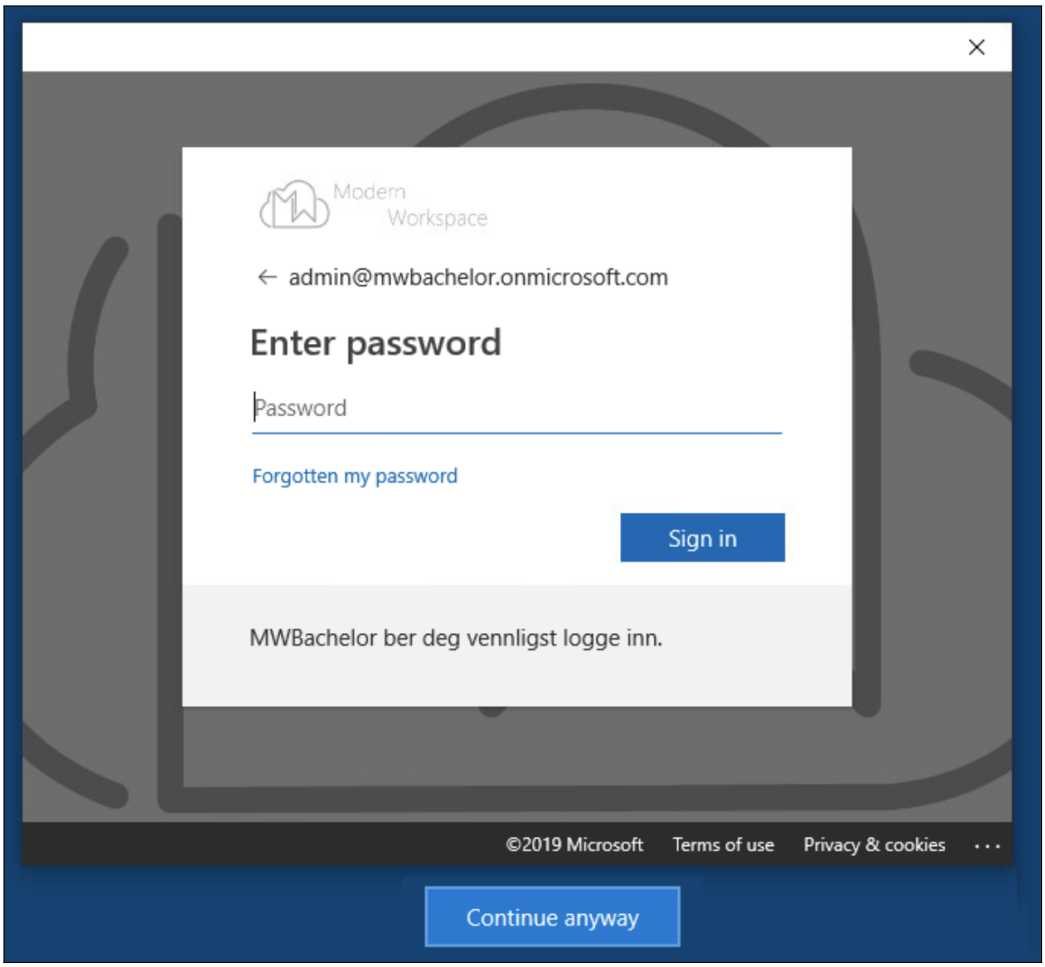
Figur 97

Etter omstarten vil et vindu som forklarer at enheten settes opp dukke opp. Dette vil ta en liten stund.



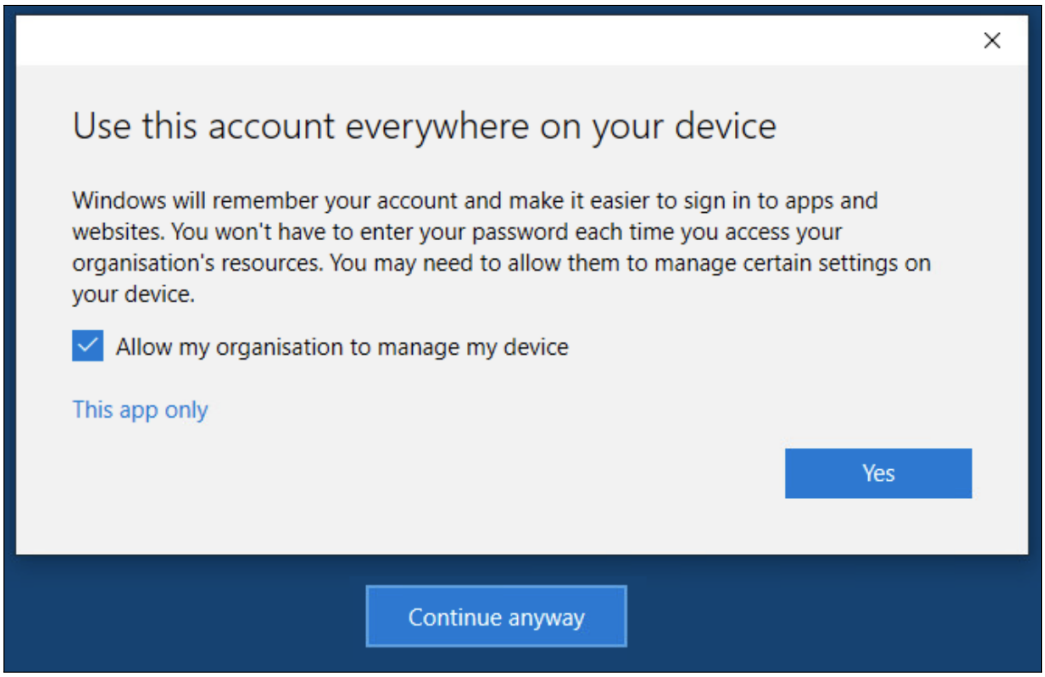
Figur 98

Når maskinen kommer til oppsett av brukerkonto, må bruker logge inn nok en gang. Fyll inn kontoinformasjon og trykk “Sign in”.



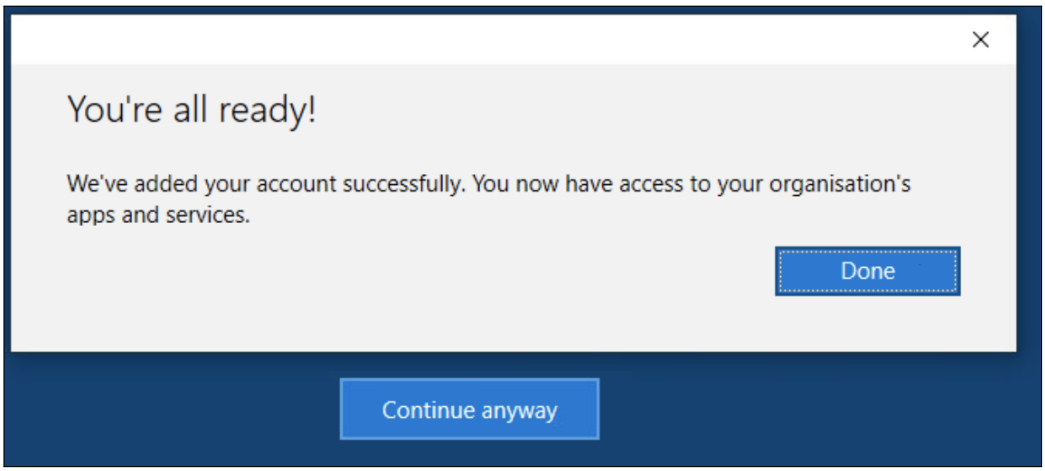
Figur 99

Deretter dukker det opp et vindu som spør om en ønsker å bruke kontoen som innlogging i andre applikasjoner. For å tillate dette må bruker huke av for at bedriften kan administrere enheten.



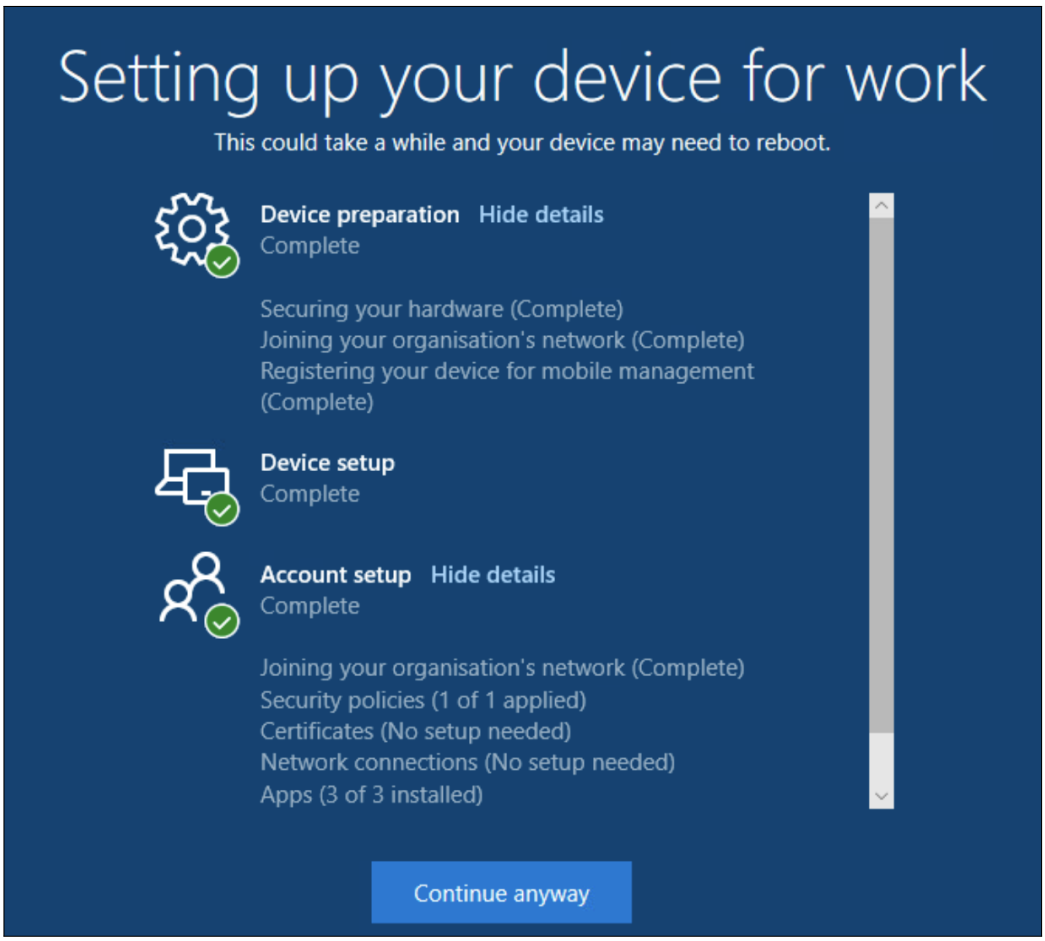
Figur 100

Det vil så dukke opp et vindu som informerer om kontoen ble lagt til. Som vist i figur 101, ble kontoen lagt til og har tilgang på applikasjoner. En kan så trykke "Done".



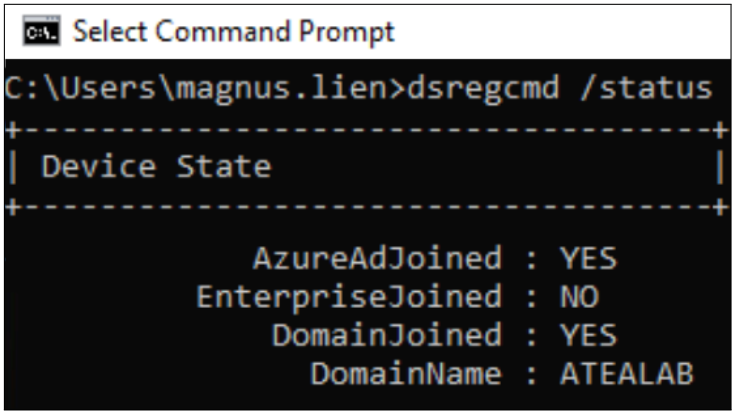
Figur 101

Maskinen vil fortsette sitt oppsett av maskinen en liten stund til før en får mulighet til å fortsette. Når en får en grønn hake på alle tre kategorier er det bare å trykke "Continue Anyway" og enheten er klar for bruk.



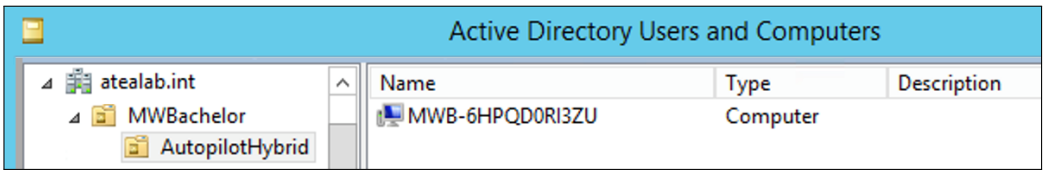
Figur 102

Inne på maskinen kan vi se at den er medlem av både Azure AD og domenet. Som vist i figur 103 har maskinen "YES" bak "AzureADJoined" og "DomainJoined".



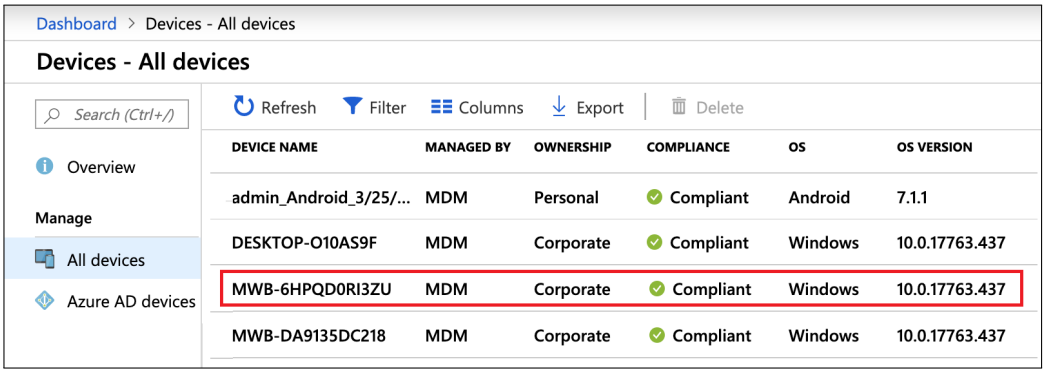
Figur 103

Vi kan også se at enheten er underlagt OU-en som ble opprettet for hybrid-join, med navnestandarden vi satte for slike enheter.



Figur 104

I enhetslisten hos Intune vil maskinen nå være markert som "Compliant" og ha fått navn som følger standarden fra domene-konfigurasjonen.



Figur 105

Referanser

[1] Microsoft. *Demonstrate Autopilot deployment on a VM*. 2019. URL: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/demonstrate-deployment-on-vm (sjekket 02.05.2019).

[2] Microsoft. *Hybrid Azure AD join with Windows Autopilot*. 2018. URL: https://www.petervanderwoude.nl/post/hybrid-azure-ad-join-with-windows-autopilot/ (sjekket 02.05.2019).

[3] Microsoft. *Deploy hybrid Azure AD-joined devices by using Intune and Windows Autopilot (Preview)*. 2018. URL: https://docs.microsoft.com/nb-no/intune/windows-autopilot-hybrid#prerequisites (sjekket 02.05.2019).

Modern Workspace - Driftsdokument
Company Branding

v.0.7

Eskil Uhlving Larsen Magnus Reitan Lien
eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
02.04.2019	0.1	Opprettet dokumentet. Introduksjon skrevet, standard profil skrevet, endre eksisterende profil skrevet, figurer lagt til
05.04.2019	0.2	Profil for spesifikke språk skrevet, azure innlogging skrevet, figurer lagt til
08.04.2019	0.3	Revidert tekst, figurer endret, oppdatert innholdsfortegnelsen
12.04.2019	0.4	Revidert introduksjon, standard profil, endre eksisterende profil og profil for spesifikke språk
16.04.2019	0.5	Mindre revisjon av figurtekster
19.04.2019	0.6	Større revisjon av tekst, ferdigstilt profil for spesifikke språk, lagt til figurer
06.05.2019	0.7	Mindre revisjon av tekst, retting av grammatiske og språklige feil

Innhold

1 Introduksjon

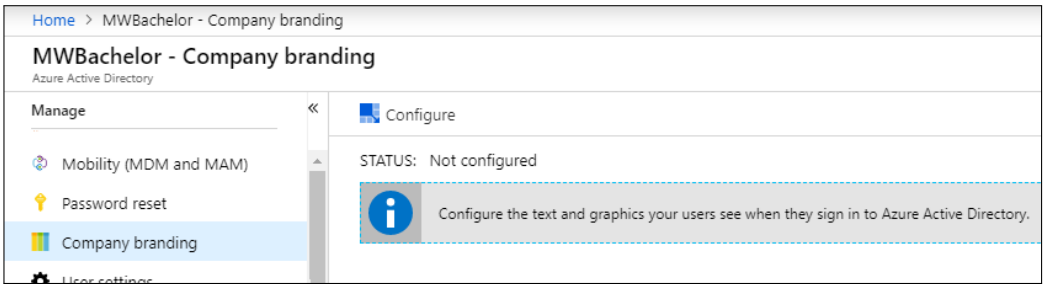
Med Company Branding blir det mulig å legge til bedriftens logo og fargepalett på alle innloggingssidene. Company Branding lar bedriften bygge en merkevare som konsekvent brukes på alle bedriftens sider. Det gis også muligheten til å ta hensyn til forskjellige brukere, ved, for eksempel, å legge til en unik logo brukere som benytter mørkt tema, såkalt "Dark Mode". Videre kan brukere med ulike språkinnstillinger få tilpasset veiledningstekst på innloggingsidene, slik at veiledning foregår på det foretrukne språket.

Dokumentet tar for seg opprettelse av den første profilen, som vil fungere som en standard, redigering av eksisterende profiler og opprettelse av profiler for spesifikke språk. Det vil også gå ut ifra at leser har en viss teknisk kunnskap, og vil derfor ikke nødvendigvis være enkelt å forstå for ufaglærte.

2 Oppsett av standard-profil

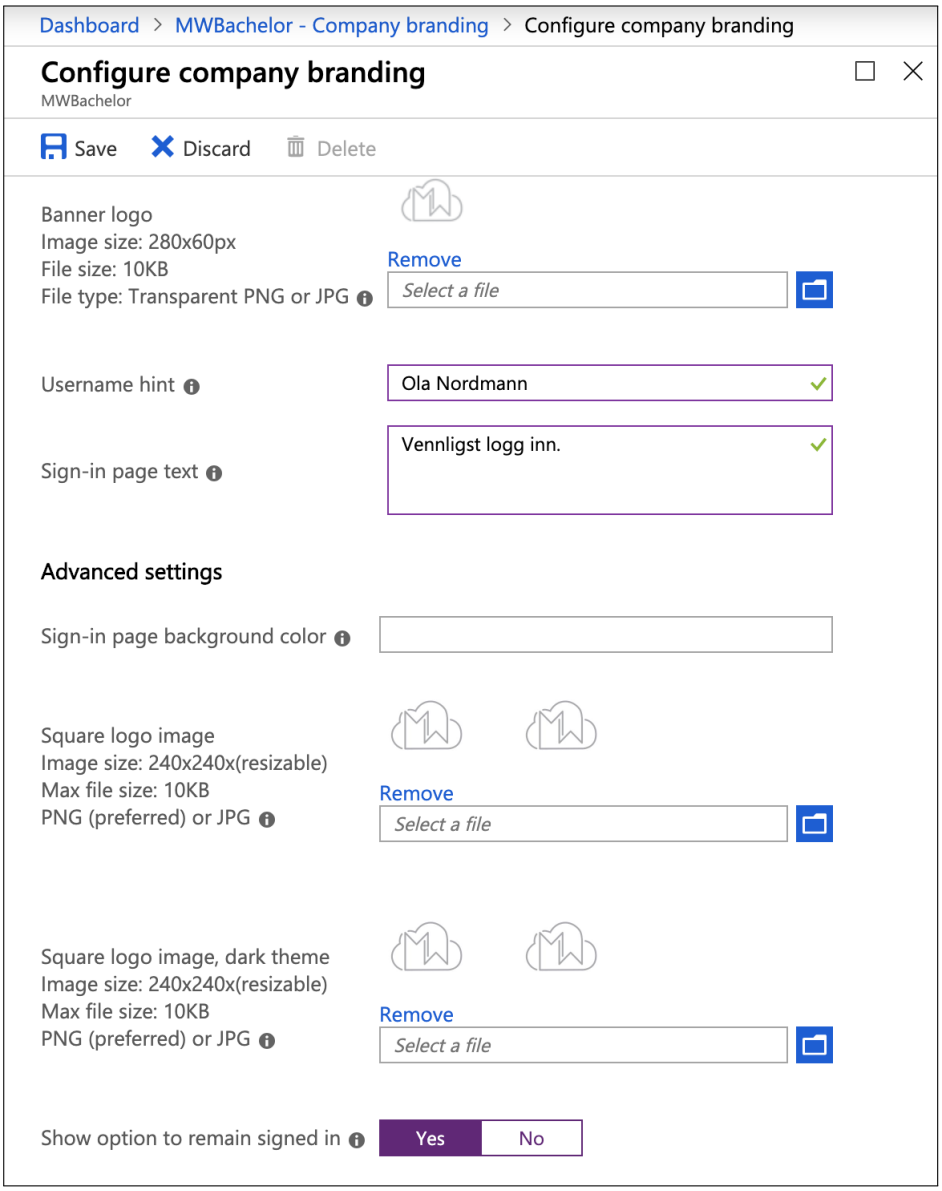
Det første som må gjøres, når det er snakk om Company Branding, er å opprette en standardisert profil. Denne kan både endres og utbygges med nye språk dersom bedriften ser et behov for dette. Company Branding er å finne inne i ”Azure Active Directory”. I menyen til venstre ligger ”Company Branding”under ”Manage”.

For nye tenanter vil det ikke være opprettet noen standard-profil enda og siden se ut som på figur 1. For å opprette den første profilen klikker på “Configure” like over statusen, som vi ser i figur 1.



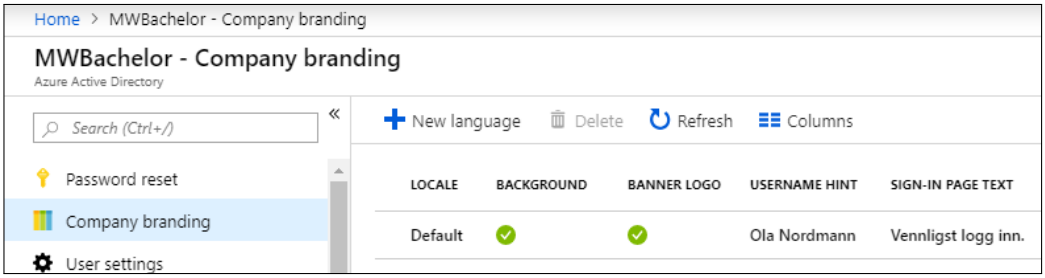
Figur 1: Ingen Company branding

Det vil dukke opp et vindu som i figur 2. Her er det mulig å legge inn elementer som banner, logo, brukernavnhint, velge farge og spesifisere en innloggingstekst. Disse elementene bør følge proporsjonene som vist i "Image size" for å ikke få skjeve eller uklare bilder. De må også være mindre enn maks filstørrelse.



Figur 2: Profilkonfigurasjon

Når profilen er lagret, vil startsiden for Company Branding se ut som på figur 3. Her ser vi at en standardprofil er opprettet, og vi får nå mulighet til å legge til nye språk.

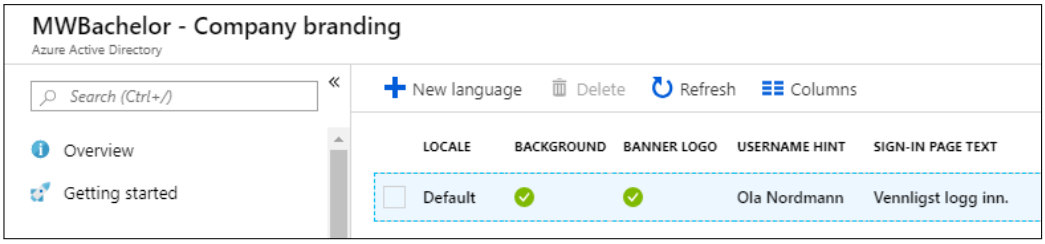


Figur 3: Standardprofilen er ferdig

3 Endre eksisterende profil

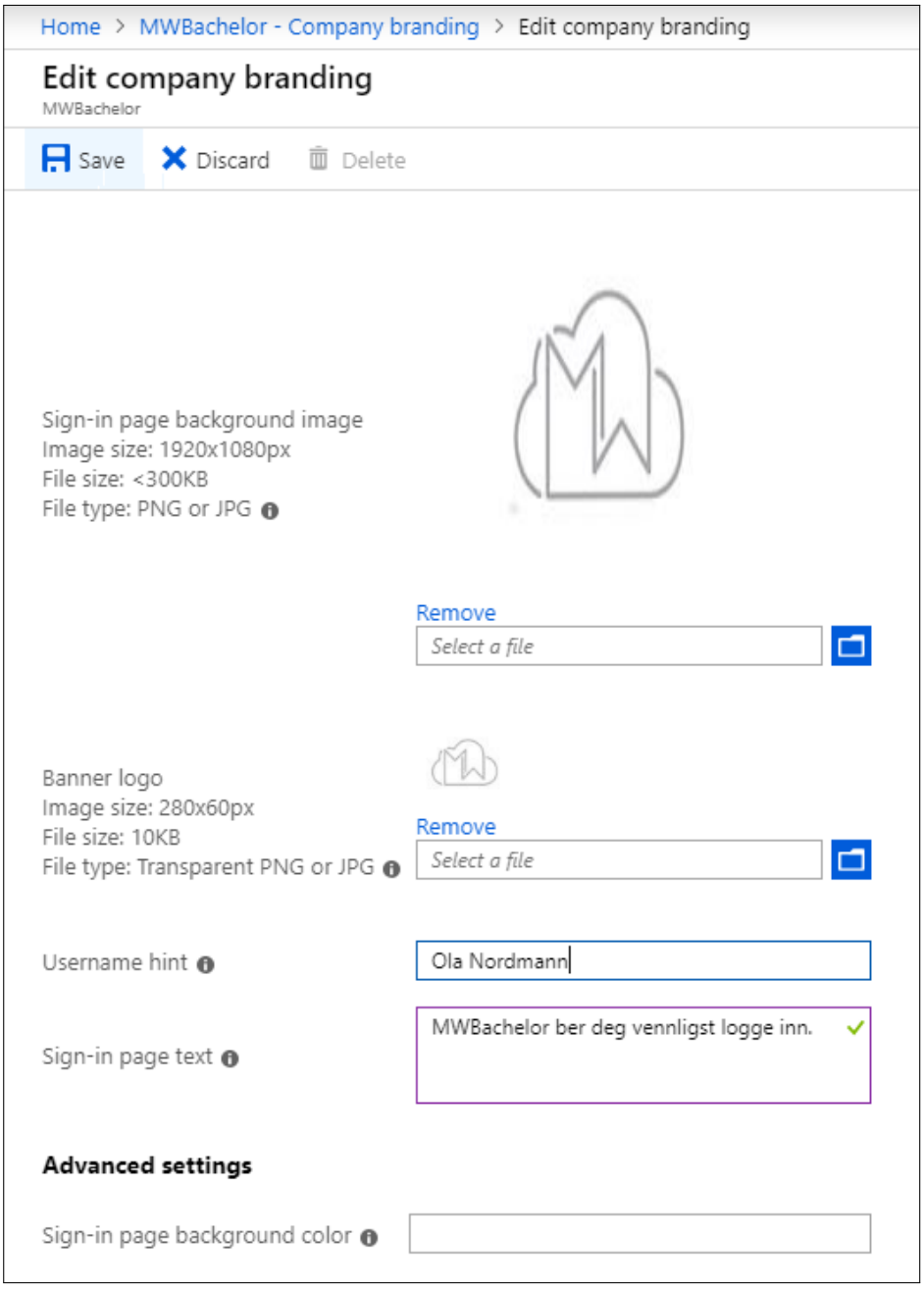
Dersom bedriften skulle endre logo eller rette på småfeil, kan den eksisterende profilen endres. Det trengs ikke å lage en helt ny profil dersom bedriften endrer logo.

For å utføre endringer på profilen må man først finne den eksisterende profilen, som vist i figur 4, og klikke seg inn på denne.



Figur 4: Liste over profiler

På figur 5 er det mulighet å endre innstillingene som logoene, farger og tekster.

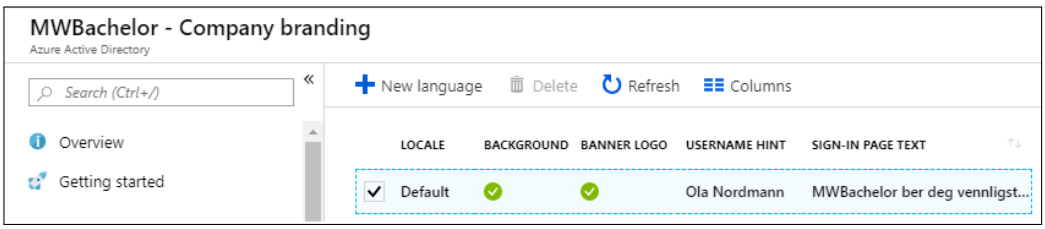


Figur 5: Profilkonfigurasjon

Når innstillingen som skal endres er endret kan en lagre disse ved å trykke “Save”. Det vil så komme opp et varsel som forteller om tenant-branding har blitt oppdatert eller om noe gikk feil. Som vist i figur 6, gikk oppdateringen feilfritt i vårt tilfelle.

Figur 6: Vellykket operasjon

Nå kan vi, som vist i figur 7, se at “Sign-In Page Text” er blitt endret.



Figur 7: Profil ferdig endret

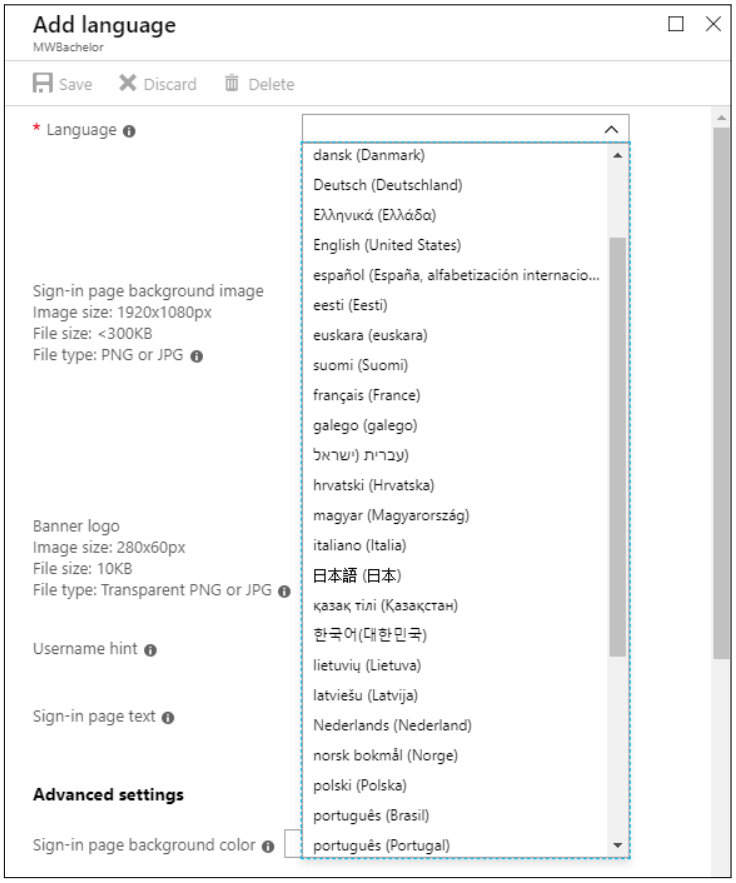
4 Profil for spesifikke språk

Dersom bedriften har internasjonale kontorer, eller ansatte som har behov for et annet språk, kan dette legges til ved siden av standard-profilen. Dersom brukeren benytter et språk uten noen spesifikk profil, vil standardprofilen benyttes. Dette lar bedriften tilrettelegge for internasjonale ansatte som foretrekker sitt morsmål.

Første steg vil være å klikke på "New language" inne i "Company Branding".

Figur 8: Ny språk-profil

Når det opprettes en ny språk-profil vil det være en nedtrekksmeny øverst for å spesifisere hvilket språk denne profilen skal gjelde for. En kan også legge inn en alternativ logo dersom bedriften profileres annerledes i andre landområder.

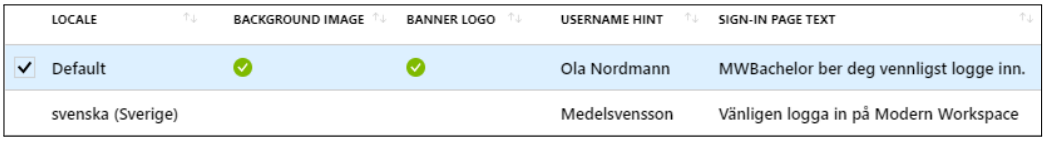


Figur 9: Nedtrekksliste med språkvalg

For å lagre den nye språkprofilen trykker vi “Save”. Det vil så komme en bekreftelse på om profilen ble opprettet eller ikke. I vårt tilfelle ble profilen opprettet uten problem, som vist i figur 10.

Figur 10: Vellykket operasjon

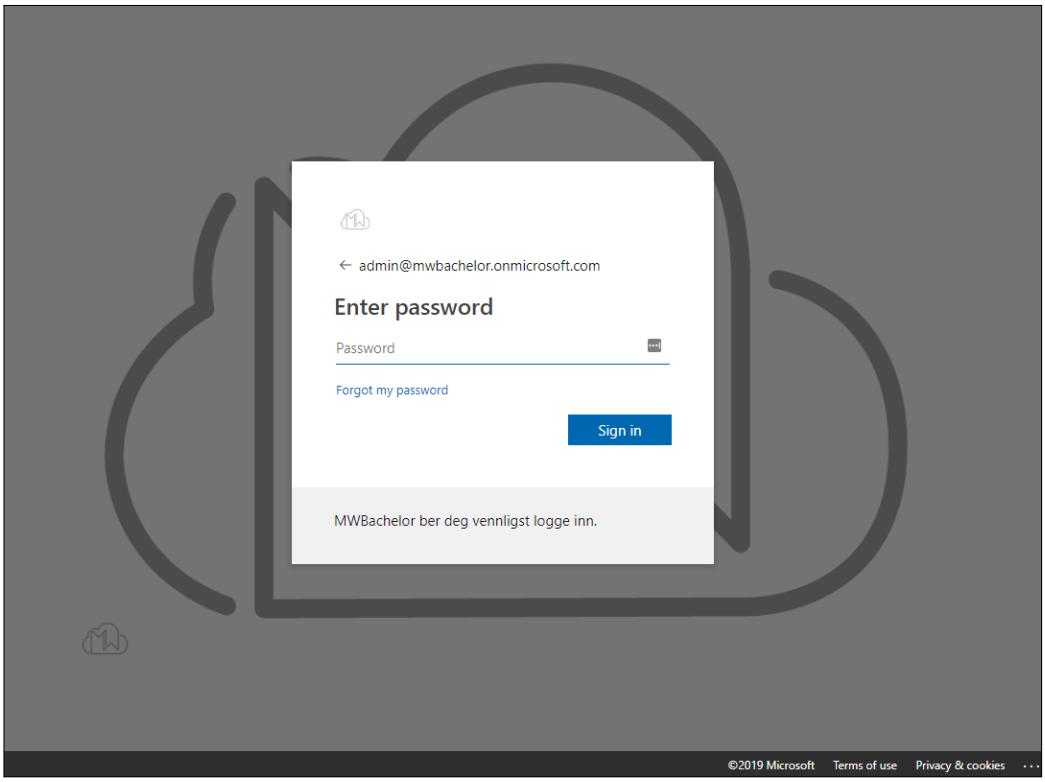
Den nye språkprofilen vil nå vises inne i Company Branding, med det valgte språket som “Locale”.



Figur 11: Liste over profiler

5 Azure innlogging

Company Branding kan sees på ulike steder etter opprettelse av profilen. En av eksemplene som en vil komme over vil være på innloggingsider, som for eksempel Windows 10, Teams og SharePoint. Vi kan også se profilen når vi forsøker å logge inn på Azure-portalen, som vist i figur 12.



Figur 12: Innlogging med Company Branding

Modern Workspace - Driftsdokument Applikasjoner

v.0.8

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
29.03.2019	0.1	Dokument opprettet, introduksjon skrevet, legge til applikasjoner i Intune påbegynt, tildeling av applikasjoner – assignments påbegynt, figurer lagt til
04.04.2019	0.2	Assignments ferdig, ryddet i og lagt til nye figurer
05.04.2019	0.3	Nedlastning av applikasjoner opprettet og ferdigstilt, figurer lagt til, konfigurasjon av policies påbegynt
08.04.2019	0.4	Konfigurasjon av policies ferdigstilt, figurer lagt til, legge til applikasjoner i Intune ferdigstilt, referanser lagt til.
12.04.2019	0.5	Introduksjon revidert
16.04.2019	0.6	Windows 10 – Store App revidert, nye figurer lagt til, referanse lagt til
24.04.2019	0.7	Endret Legge til applikajsoner i Intune – Android, lagt til nye figurer
06.05.2019	0.8	Mindre revisjon av tekst, retting av grammatiske og språklige feil, lagt til referanser

Innhold

1 Introduksjon

I dette dokumentet vil vi gå gjennom utrulling av applikasjoner til brukere. Utrulling av applikasjoner består av fire distinktive steg som bør gjennomgås for at brukerne skal få tilgang på applikasjoner på en sikker og brukervennlig måte. De fire stegene som gjennomgås er:

- **Utrulling av applikasjonen.** Her ser vi på oppsettet som må gjøres i Intune og de ulike applikasjonsbutikkene. Her opprettes en applikasjon, som for eksempel Microsoft Word, i Intune og konfigureres slik at applikasjonen er skreddersydd for bedriften.
- **Tildeling av applikasjonen.** Her forklares oppsettet som må gjøres i Intune for at brukere skal få tilgang på applikasjonen. En såkalt "assignment" brukes for å velge hvilke brukere som skal få tilgang på applikasjonen og hvilke som ikke skal få det.
- **Nedlasting av applikasjonen.** Her gjennomgås stegene som må tas for å få applikasjonen lastet ned på den valgte enheten.
- **Konfigurasjon av policies for applikasjonen.** Her gjennomgås sikkerheten som konfigureres for applikasjonen. Gjennom en policy kan databehandling, sikkerhetskopiering og innloggingskrav konfigureres. Dette gjøres for å sikre at bedriftens data ikke går tapt, blir stjålet eller tukles med.

Dokumentet vil gå ut ifra at leser har en viss teknisk kunnskap, og vil ikke nødvendigvis være enkelt å forstå for ufaglærte.

2 Legge til applikasjoner i Intune

2.1 Android

Når en skal sende ut applikasjoner til Android[1] enheter må din tenant være koblet opp mot Google Play Store, slik at applikasjoner kan godkjennes. Dermed må Managed Google Play settes opp, noe vi beskriver i dokumentet "Driftsdokument - Enrollment". Deretter kan applikasjoner godkjennes inne i work-versjonen av Google Play Store og tilegnes brukere. Vi bruker Microsoft Word i vårt eksempel, men prosessen vil være identisk for alle applikasjoner.

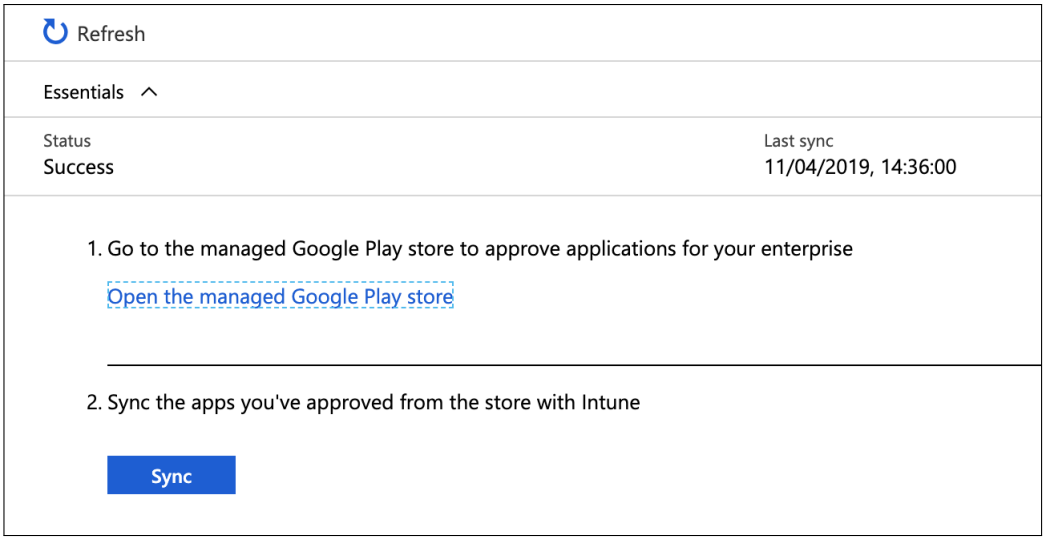
Kravene som settes til å opprette en ny applikasjon for utrulling til Android er:

- Managed Google Play
- Google-brukerkonto

Første steg vil være å navigere til punktet for klientapplikasjoner via Google Play i Azure-portalen. Gå til "Intune", velg "Client apps" og trykk "Managed Google Play".

Figur 1

Her inne kan vi se at Google Play er koblet opp mot Intune da det har skjedd en sync på et tidligere tidspunkt. For å godkjenne applikasjoner må vi trykke på lenken som fører til bedriftsversjonen av Google Play Store ved å trykke på "Open the managed Google Play store". Pass på at du blir ført til en URL som har "/work" i seg, i.e. "https://play.google.com/work".

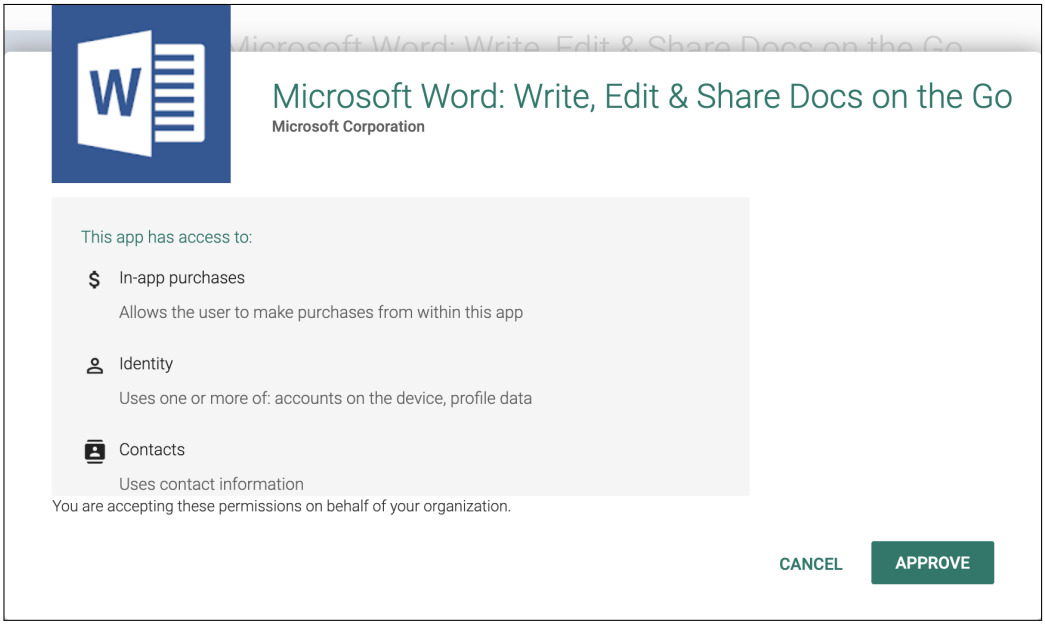


Figur 2

Inne i Google Play kan en søke opp applikasjonen som skal godkjennes for utrulling. Før du kan godkjenne må du være logget inn med den samme Google-kontoen som er koblet opp mot Intune. Trykk her "Approve" for å godkjenne applikasjonen.

Figur 3

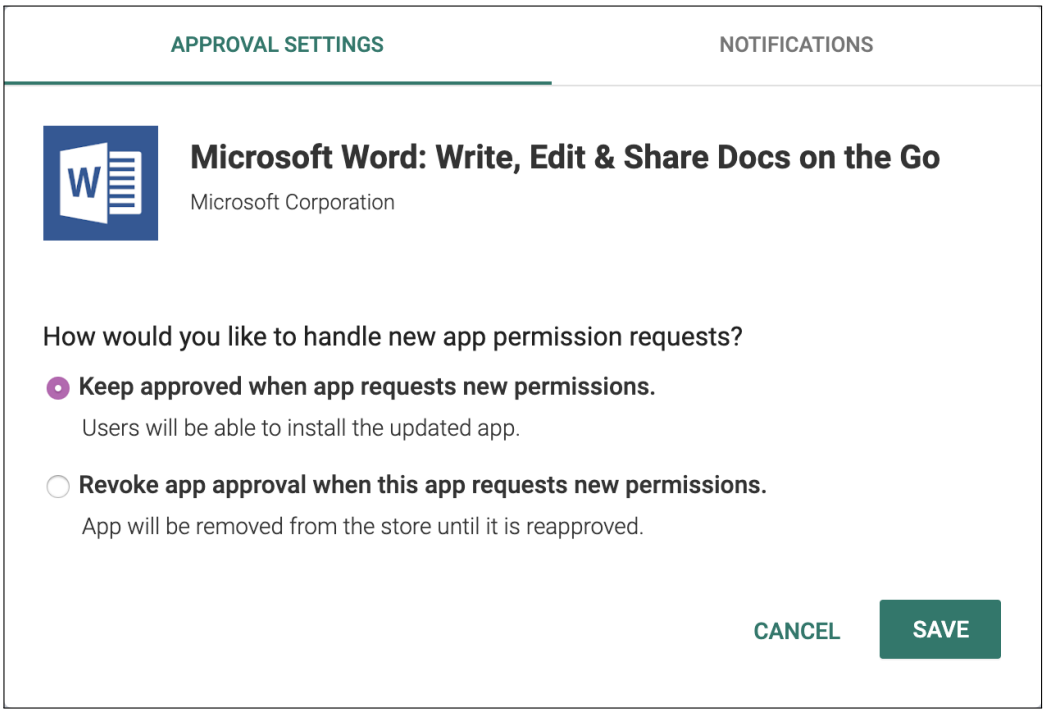
Det vil så dukke opp et vindu som forklarer tilgangene applikasjonen får på enhetene som laster ned den. Les nøye gjennom disse for å sikre at de følger bedriftens krav og vilkår. Trykk “Approve” for å godkjenne applikasjonen.



Figur 4

Det blir så spurt om hva som skal gjøres i tilfeller hvor applikasjoner ber om utvidede tillatelser hos brukere. Her bør en være kritisk til hvilke applikasjoner som automatisk får godkjent kravene, slik at applikasjoner med ondsinnede utviklere ikke automatisk får godkjent tillatelser de ikke bør ha på enhetene til brukerne. Alternativet gjør at applikasjonens nye tillatelser må bli godkjent av en administrator før oppdateringen kan lastes ned av brukere. Det anbefales kun å tillate automatisk godkjenning på applikasjoner fra klarerte utgivere, som Microsoft, Google og Apple.

Vi velger her å automatisk godkjenne nye tillatelser, da applikasjonen leveres av Microsoft. Vi huker derfor av for "Keep approved when app requests new permissions". Vi lagrer så valget vårt ved å trykke "Save".

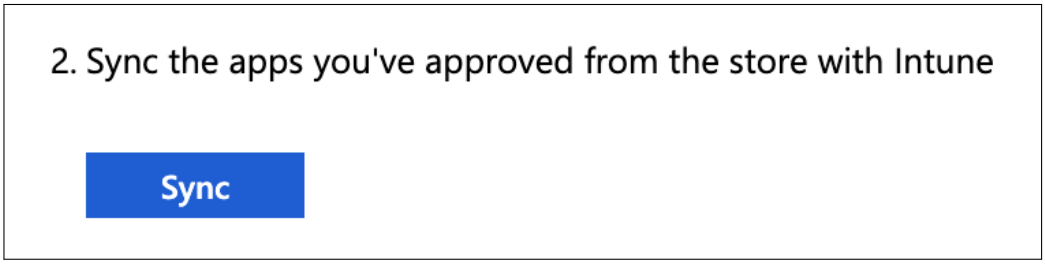


Figur 5

Nå kan vi gå inn i applikasjonen på Google Play og se at det er kommet en liten merknad som sier “Approved” og det er nå mulig å fjerne godkjenningen av applikasjonen ved å trykke “Unapprove”.

Figur 6

For at applikasjonen skal dukke opp i Intune, må vi nå kjøre en synkronisering mellom Google Play og Intune. Dette gjøres ved å trykke “Sync” inne på “Managed Google Play” i Intune.



Figur 7

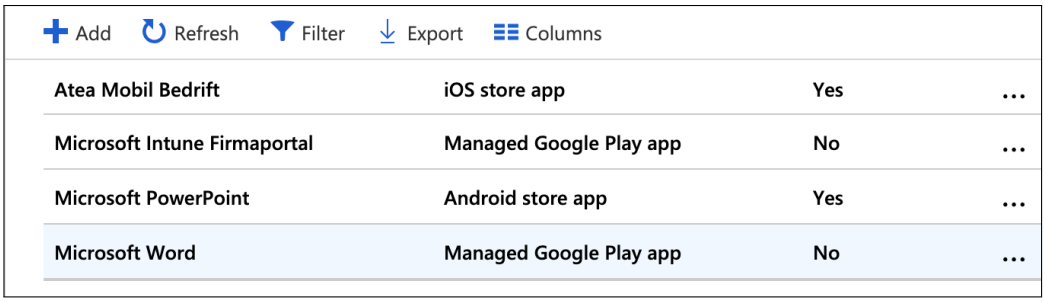
Det vil komme opp en liten notifikasjon som informerer om at synkroniseringen er underveis og vil ta litt tid.

Figur 8

Når synkroniseringen er ferdig kommer en notifikasjon om dette også. Denne vil også informere om noe gikk galt. Som vi ser i figur 9, gikk synkroniseringen feilfritt i vårt tilfelle.

Figur 9

Vi kan nå se at applikasjonen ligger inne i Intune som en "Managed Google Play app". Applikasjonen er nå klar for utrulling.



Figur 10

2.2 iOS

Oppretting av applikasjoner til iOS[2] foregår gjennom Intune i Azure-portalen. Når en konfigurerer en applikasjon vil informasjonen man må produsere være ulik for hver applikasjon. Vi vil bruke applikasjonen Microsoft Word i vårt eksempel, og informasjonen vil kun tilsvare denne applikasjonen.

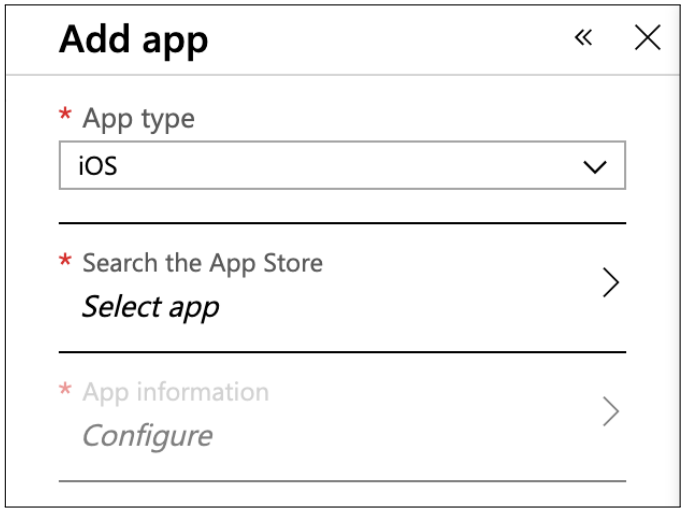
Kravene som settes til å opprette en ny applikasjon for utrulling til iOS er:

- Applikasjonsnavn
- Beskrivelse av applikasjonen
- Utgiver av applikasjonen
- Minimumskrav til iOS-versjon
- Støttede enhetstyper

Første steg vil være å navigere til punktet vi kan legge til nye applikasjoner i Azure-portalen. Gå til "Intune", velg "Client apps" og trykk "Add app".

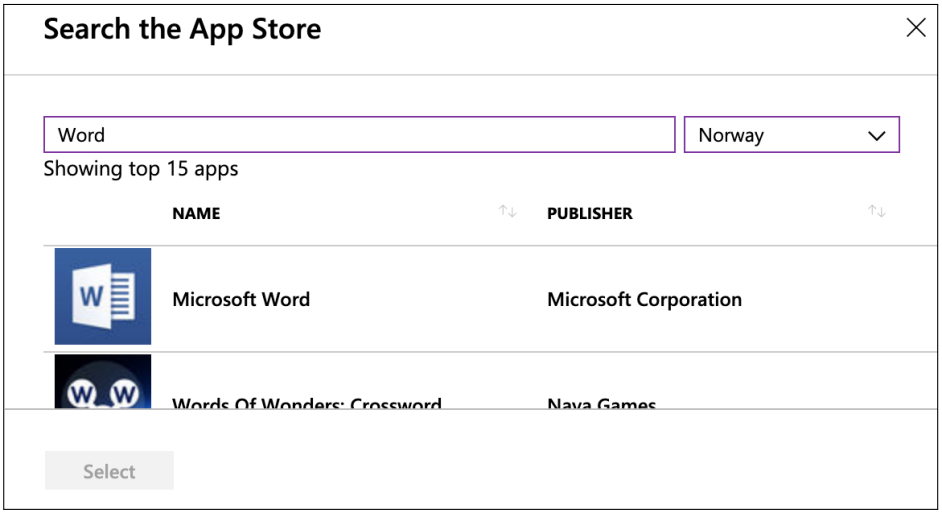
Figur 11

Velg iOS som "App type". Nå kan en søke opp applikasjonen i App Store direkte gjennom Azure-portalen ved å trykke "Select app".



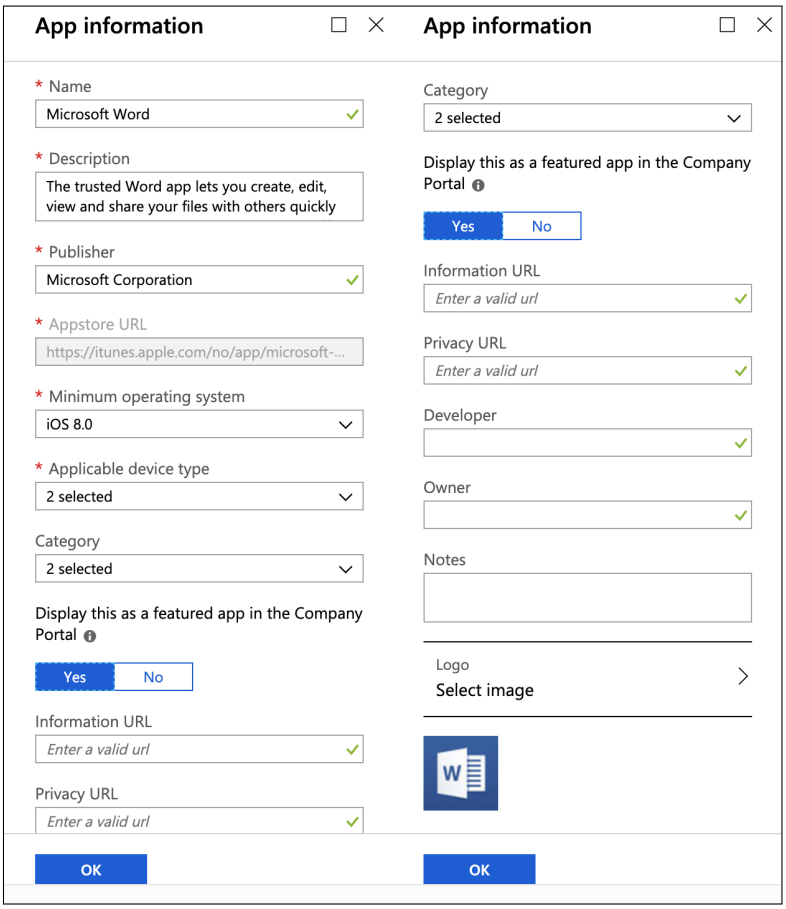
Figur 12

Det vil her være mulig å søke gjennom alle applikasjoner som ligger ute i App Store uten å måtte hente en URL fra internett. Husk å velge riktig land for App Store, da det kan forekomme restriksjoner avhengig av regionen som velges.



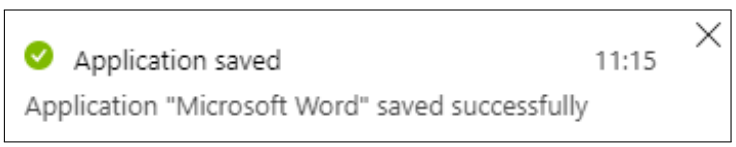
Figur 13

Etter å ha valgt applikasjonen som skal legges til, vil en nå få muligheten til å konfigurere applikasjonen på lik linje med oppsettet for Android. Forskjellen her er at de fleste feltene er ferdigutfylte med informasjon hentet direkte fra App Store. Det er derimot mulig å endre på de fleste parameterne dersom det skulle være behov. Kategorier legges ikke automatisk til, og det er derfor anbefalt å legge inn dette manuelt.



Figur 14

Nå kan en trykke på “Add” og applikasjonen vil legges til i Intune. Det vil komme opp et varsel som informerer om applikasjonen ble lagret eller om noe gikk galt.



Figur 15

2.3 Windows 10

Oppretting av applikasjoner til Windows 10 foregår gjennom Intune i Azure-portalen og Microsofts applikasjonsbutikk. Når en konfigurerer en applikasjon vil informasjonen man må produsere være ulik for hver applikasjon. For Windows 10 er det flere ulike muligheter for utrulling av applikasjoner avhengig av hva slags applikasjon det er og hvor den hentes fra. En "Store app" vil hentes fra Microsoft Store for Business, en "Line-of-business app" er en .msi-fil som lastes opp til Intune, og en "Windows app (Win 32)" er en .exe-fil som også må lastes opp til Intune. Alle metodene er ulike og vil dokumenteres individuelt.

2.3.1 Windows 10 – Store App

Når en applikasjon skal opprettes gjennom Microsoft Store[3, 4] anbefales det at dette foregår gjennom bedriftsbutikken Microsoft drifter. Dersom du går gjennom bedriftsbutikken kreves det ingen innfylling av informasjon ved oppretting av applikasjoner og det gir full oversikt over gjenværende og brukte lisenser. Intune vil også automatisk stoppe tilegninger ved manglede lisenser og frata lisenser fra enheter som har forlatt bedriftens enrollment. Vi vil bruke applikasjonen Company Portal i vårt eksempel.

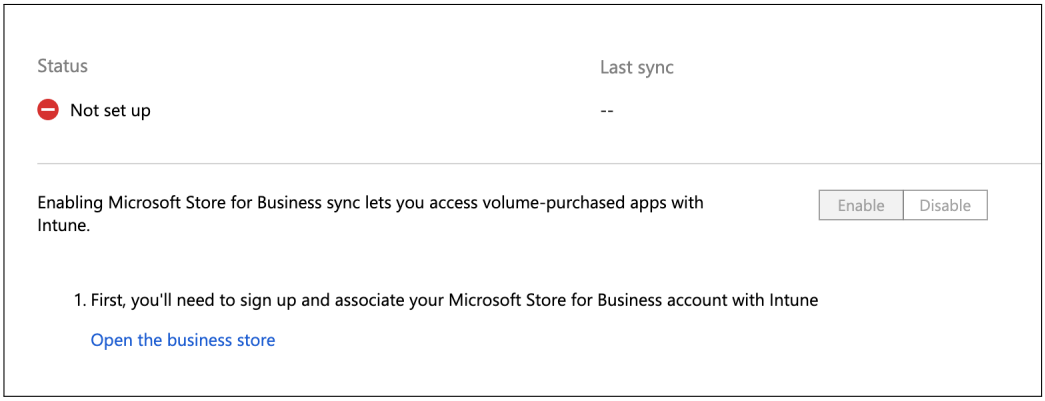
Kravene som settes til å opprette en ny applikasjon for utrulling via Microsoft Store er:

- En Intune-assosiert Microsoft Store for Business brukerkonto

Første steg vil være å navigere til punktet vi kan sette opp Microsoft Store for Business i Azure-portalen. Gå til "Intune", velg "Client apps" og trykk "Microsoft Store for Business".

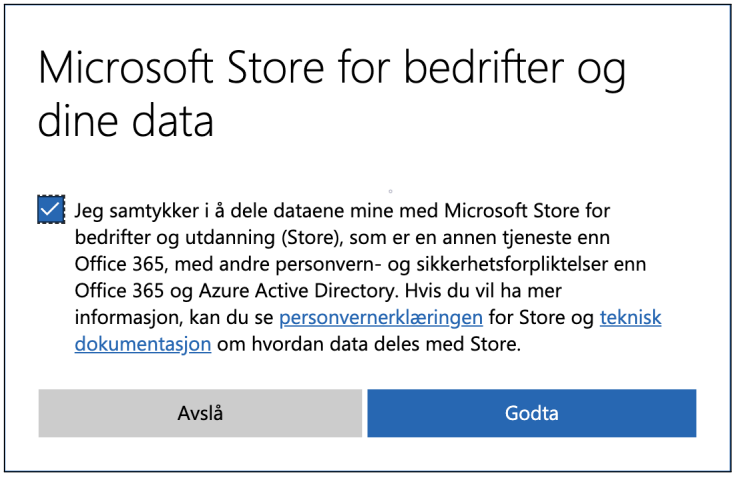
Figur 16

Her inne blir vi nødt til å aktivere synkronisering gjennom Microsoft Store for Business ved å først klikke “Enable”. Deretter må vi åpne Microsoft Store for Business ved å klikke lenken “Open the business store”, som vist i figur 17.



Figur 17

Microsoft vil så be om samtykke angående deling av data med Micosoft Store, som vist i figur 18. Dette må man godta for å bruke Microsoft Store for Business. Det anbefales å gå gjennom personvernerklæringen for å sikre at vilkårene stemmer overens med bedriftens retningslinjer.



Figur 18

Deretter må en navigere til innstillinger for distribusjon inne i Microsoft Store for Business. Gå til "Administrer", velg "Innstillinger" og deretter "Distribuer". Stien vises i figur 19.

Figur 19

Her inne må vi aktivere administrasjonsverktøyet som ønskes å ta i bruk. Vi ønsker å bruke Microsoft Intune, og klikker derfor aktiver bak denne.

Figur 20

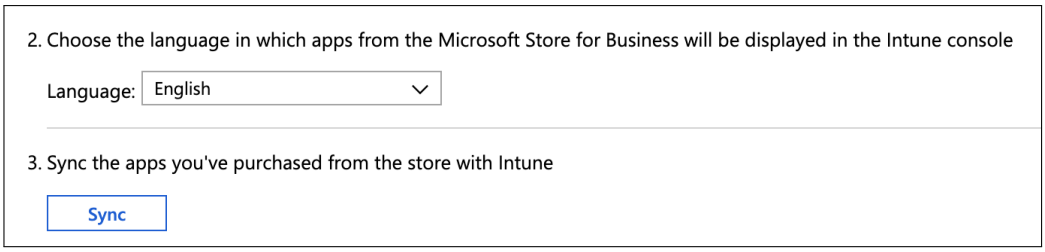
Når Microsoft Intune er aktivert kan en begynne å legge til applikasjoner. Søk opp applikasjonen som skal distribueres inne i "Handle for gruppen min" i Microsoft Store for Business, og velg "Last ned appen".

Figur 21

Det vil nå komme opp en tjenesteavtale som må godtas for å kunne fortsette. Gå gjennom avtalen for å sikre at de stemmer overens med bedriftens egne retningslinjer. Det vil så komme opp en bekreftelse på bestillingen av applikasjonen, som vist i figur 22.

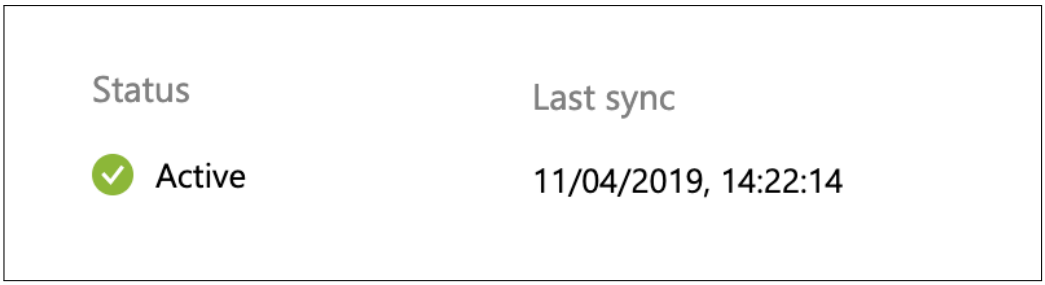
Figur 22

Når applikasjonen er bestilt, kan vi gå tilbake til "Client apps – Microsoft Store for Business" i Azure-portalen. Velg her språket applikasjonene vil bruke, før du synkroniserer Intune med butikken ved å velge "Sync", som vist i figur 23.



Figur 23

Status vil endres til "Active", som vist i figur 24, og applikasjonene er nå synkronisert mellom butikken og Intune. Avslutt så ved å velge "Save". Applikasjonene kan nå tilegnes brukere.



Figur 24

2.3.2 Windows 10 – Line-of-Business app

Når en applikasjon til Windows 10 skal legges til som en "Line-of-Business app" i Intune, vil en selv måtte hente all informasjon om applikasjonen. Informasjonen som legges til i konfigurasjonen vil avhenge av applikasjonen. I dette eksempelet vil vi bruke applikasjonen Azure Information Protection Client.

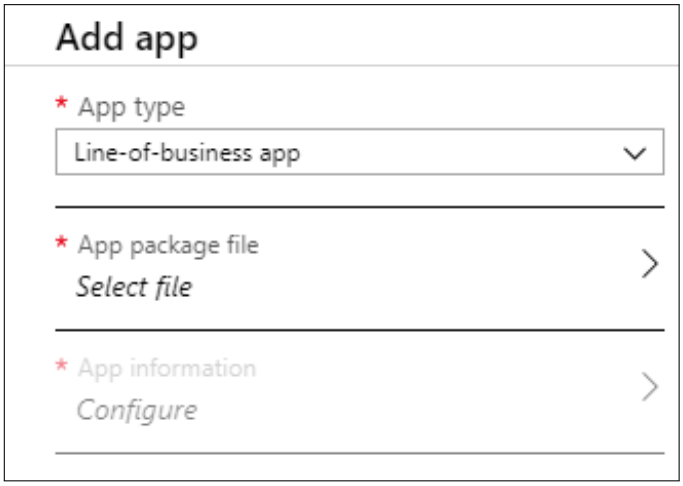
Kravene som settes til å opprette en ny applikasjon for utrulling som Line-of-Business app er:

- Applikasjonsnavn
- Beskrivelse av applikasjonen
- Utgiver av applikasjonen
- Installasjonskontekts
- Applikasjonen i .msi-filformat

Første steg vil være å navigere til punktet vi kan legge til nye applikasjoner i Azure-portalen. Gå til "Intune", velg "Client apps" og trykk "Add app".

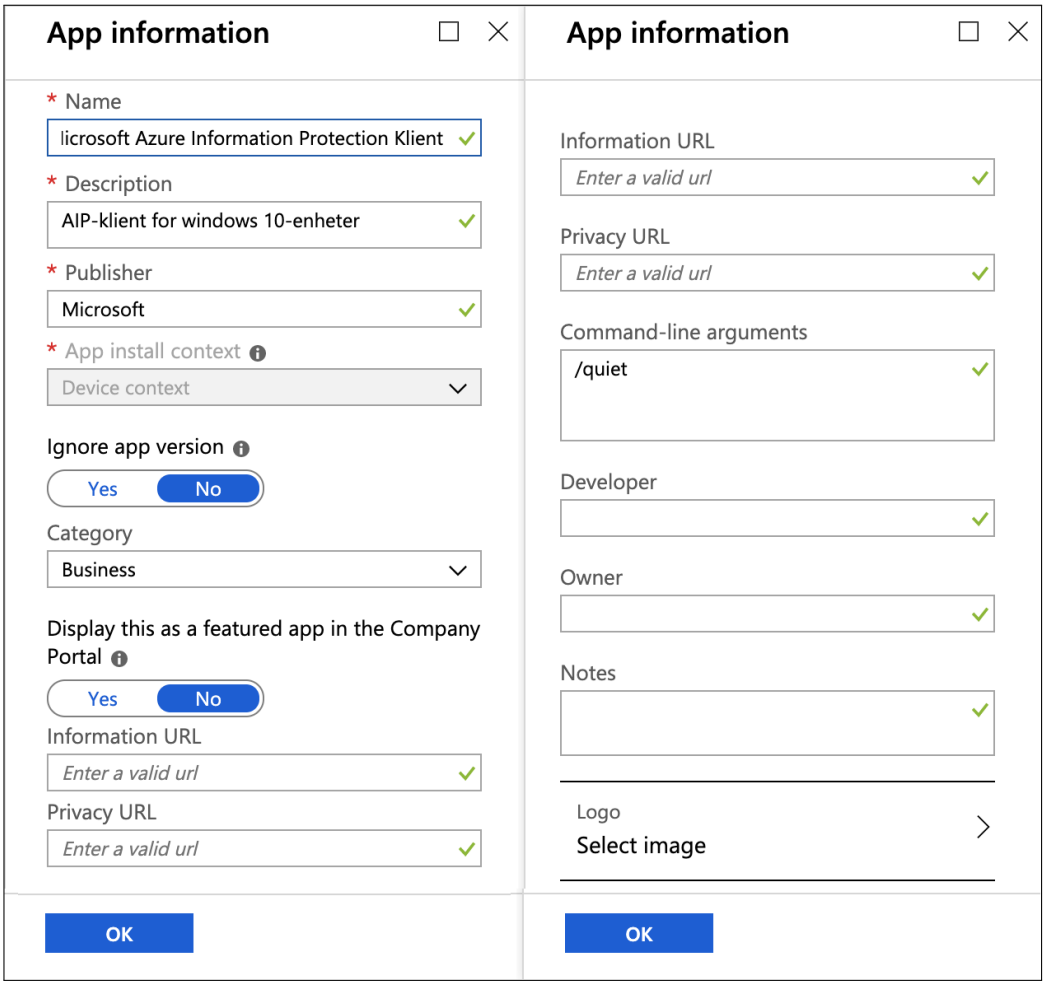
Figur 25

Velg "Line-of-Business app" som "App type". Før konfigurasjon av applikasjonen starter må det legges inn en "App package file" som må være i filformatet .msi.



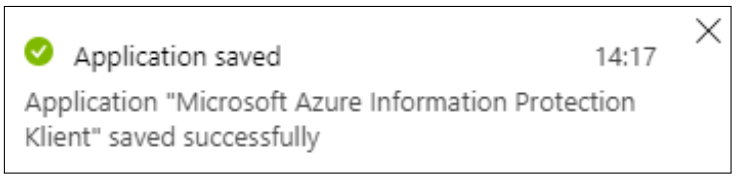
Figur 26

Når filen er lagt til kan en konfigurere applikasjonen under "Configure". Fyll så inn navn, beskrivelse av applikasjonen og utgiveren. Det ble tidligere nevnt at installasjonskontekts kreves, men det er i dette tilfellet ferdig utfylt da applikasjonen ikke er en dual mode app. Her kan en også velge om app-versjon skal ignoreres dersom applikasjonen oppdateres av applikasjonsutgiverer. Kategori og logo er valgfritt, men anbefales for brukervennlighet. Under "Command-line arguments" ser vi også at det er skrevet en kommando i "/quiet". Denne kommandoen sikrer at installasjonen foregår stille i bakgrunnen på brukers datamaskin, noe som sikrer at alle de valgte brukerne får denne applikasjonen uten å måtte laste den ned på egenhånd.



Figur 27

Siste steg vil være være å trykke på “Add” og applikasjonen vil legges til i Intune. Det vil komme opp et varsel som informerer om applikasjonen ble lagret eller om noe gikk galt. Som vist i figur 28, ble applikasjonen lagret uten feil.



Figur 28

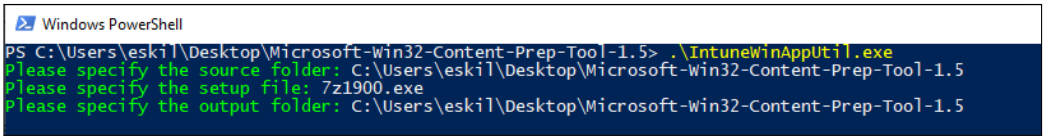
2.3.3 Windows 10 – Windows app (Win 32)

Når en applikasjon til Windows 10 skal legges til som en “Windows app (Win 32)” i Intune[4, 5], vil en selv måtte hente all informasjon om applikasjonen. Informasjonen som legges til i konfigurasjonen vil avhenge av applikasjonen. I dette eksempelet vil vi bruke applikasjonen 7zip.

Kravene som settes til å opprette en ny applikasjon for utrulling som Windows app (Win 32) er:

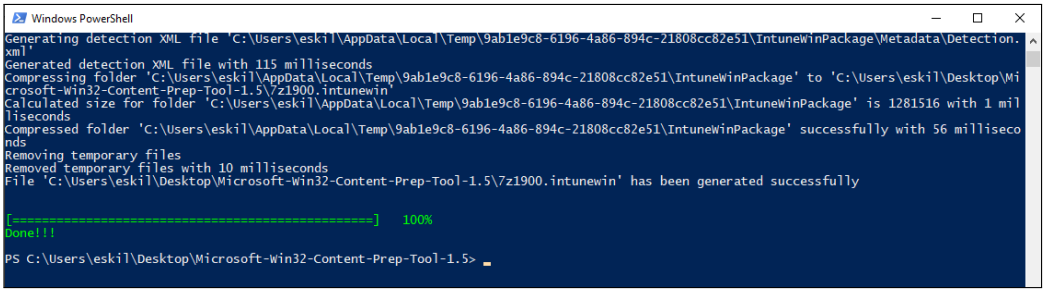
- Applikasjonsnavn
- Beskrivelse av applikasjonen
- Utgiver av applikasjonen
- Installasjonskontekts
- Applikasjonen i .exe-filformat
- Kommando for (av)installasjon
- Regler for oppdagelse
- Krav til OS-versjon
- Krav til OS-arkitektur
- Lastet ned “Win32 Content Prep Tool”

Første steg vil være å klargjøre .exe-applikasjonen ved hjelp av "Win32 Content Prep Tool". Dette er Microsofts egenutviklede verktøy for klargjøring av .exe-applikasjoner, og brukes ved å kjøre kommandoene, som vist i figur 29, i Powershell.



Figur 29

Verktøyet vil gå gjennom prosessen sin, og gi tilbakemelding når den er ferdig eller dersom noe gikk galt underveis. Som vi ser i figur 30, gikk prosessen feilfritt. En vellykket gjennomkjøring vil resultere i at informasjonen i exe-applikasjonen pakkes inn i en fil av typen "intunewin". Denne filen tas med videre.

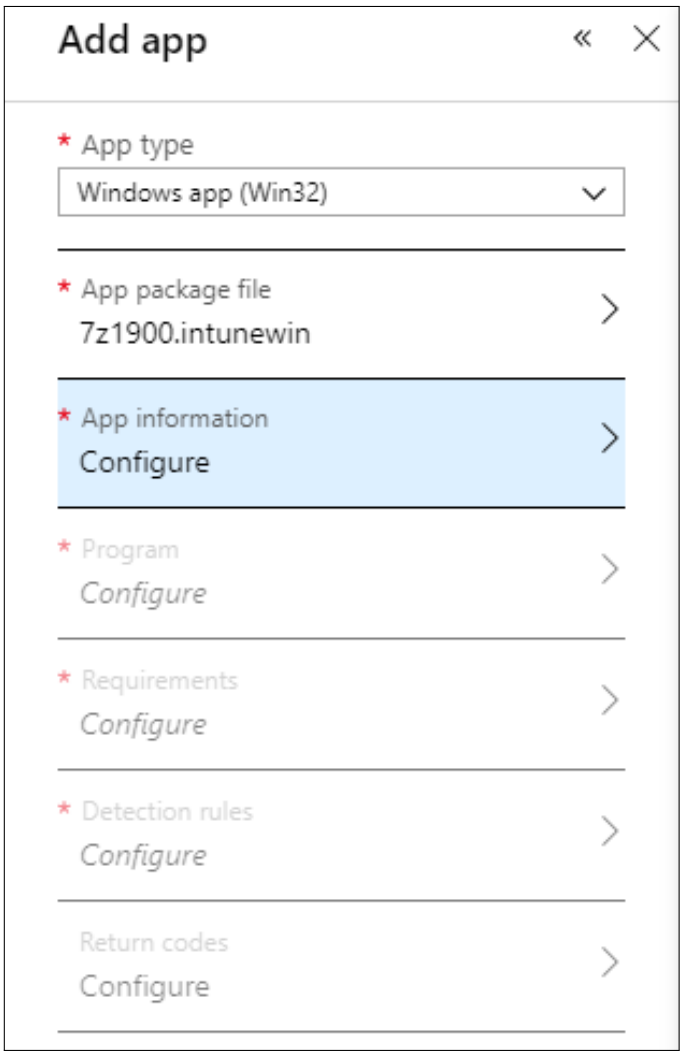


Figur 30

Neste steg vil være å navigere til punktet vi kan legge til nye applikasjoner i Azure-portalen. Gå til "Intune", velg "Client apps" og trykk "Add app".

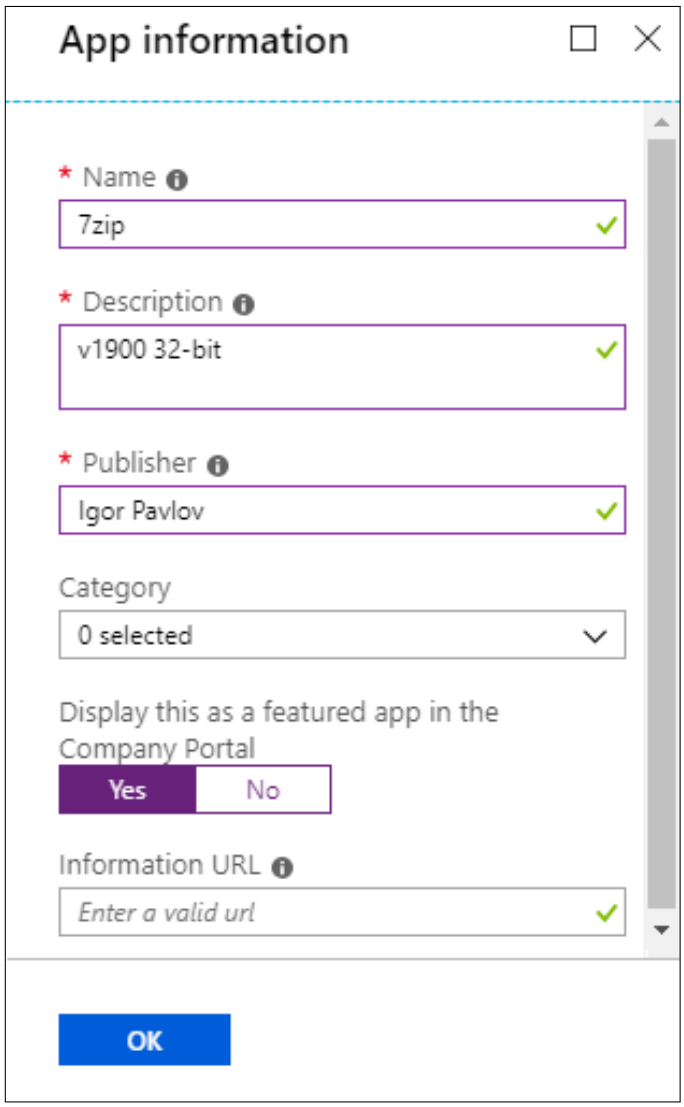
Figur 31

Velg “Windows app (Win 32)” som “App type”. Før konfigurasjon av applikasjonen starter må den klargjorte .exe-applikasjonen legges inn under “App package file”. Filen som legges inn skal være .intunewin-filen fra forrige steg.



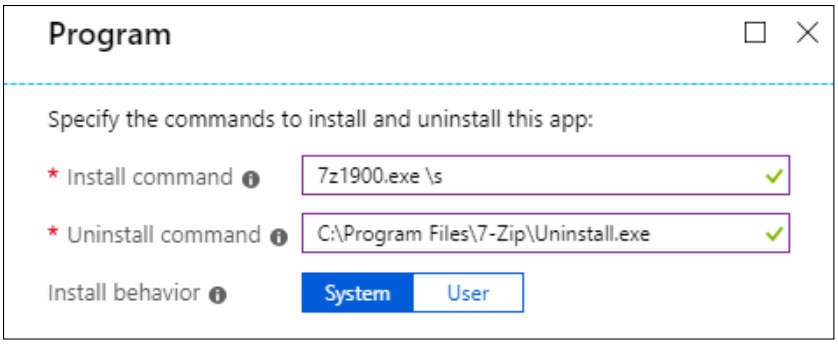
Figur 32

Konfigurer så applikasjonen ved å velge “Configure”. Som vist i figur 33, kan blant annet applikasjonens navn, utgiver og beskrivelse konfigureres. Kategori og logo er valgfritt, men anbefales for brukervennlighet.



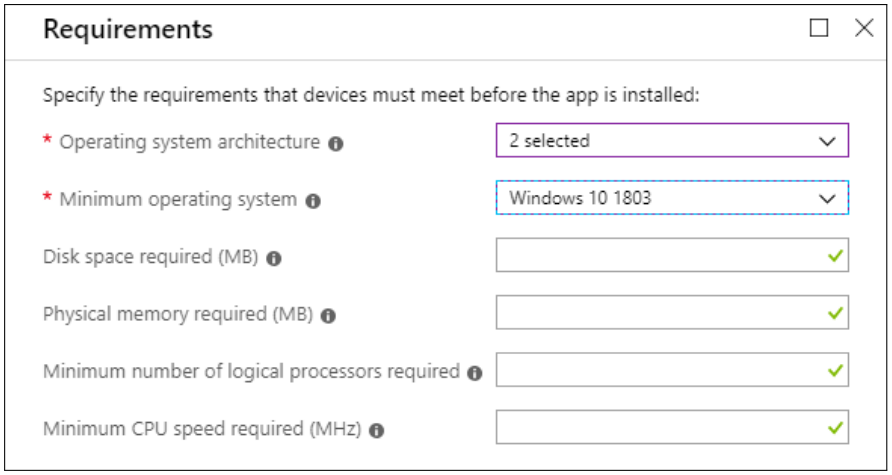
Figur 33

Under "Program" må kommando for installasjon og avinstallasjon legges inn. Dette vil si kommandoen som kjøres for å installere, eller eventuelt avinstallere, applikasjonen på Windows 10-enheter. Kommandoene vil variere fra applikasjon til applikasjon, og vil må sjekkes for hver applikasjon før deployment. Som vist i figur 34, brukes parapeteret \s for å kjøre installasjonen stille i bakgrunnen på enheten.



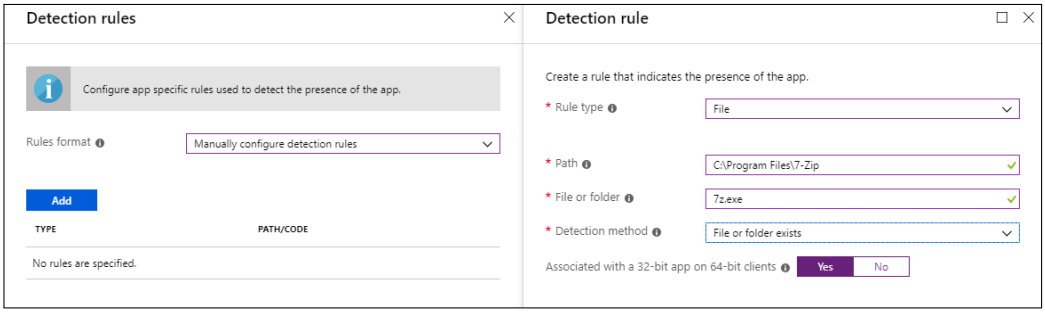
Figur 34

Neste steg er å sette krav til enheten som skal laste ned applikasjonen. Her vil det være mulig å sette minstekrav til RAM, CPU og diskplass dersom applikasjonen krever visse spesifikasjoner for å kjøre. I vårt tilfelle er applikasjonen svært enkel å kjøre, og, som vist i figur 35, er det derfor kun behov for å sette krav til arkitektur (32/64bit) og OS (Windows 10 1803).



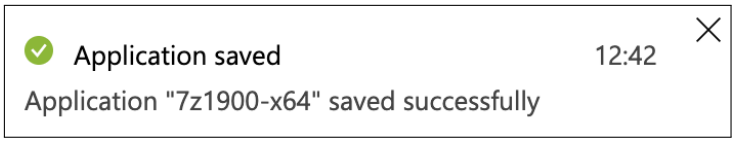
Figur 35

Så må regler settes for at applikasjonen skal oppdages av Intune, noe som gjøres under “Detection rules”. Som vist i figur 36, vil Intune sjekke om mappen til 7zip eller filen 7zip.exe eksisterer på enheten.



Figur 36

Siste steg vil være være å trykke på “Add” og applikasjonen vil legges til i Intune. Det vil komme opp et varsel som informerer om applikasjonen ble lagret eller om noe gikk galt. Som vist i figur 37, ble applikasjonen lagret uten feil.



Figur 37

3 Tildeling av applikasjoner - Assignments

Før en applikasjon kan rulles ut til brukerne må Intune vite hvilke brukere den skal tildele applikasjonen til. Dette gjøres gjennom "Assignments"[6] under den spesifikke applikasjonen som skal rulles ut. Metoden som brukes for å tildele applikasjoner til brukere vil være identisk på tvers av de ulike operativsystemene, og vil derfor kun beskrives en gang. I dette eksempelet vil vi tildele brukere på Android applikasjonen Microsoft Word.

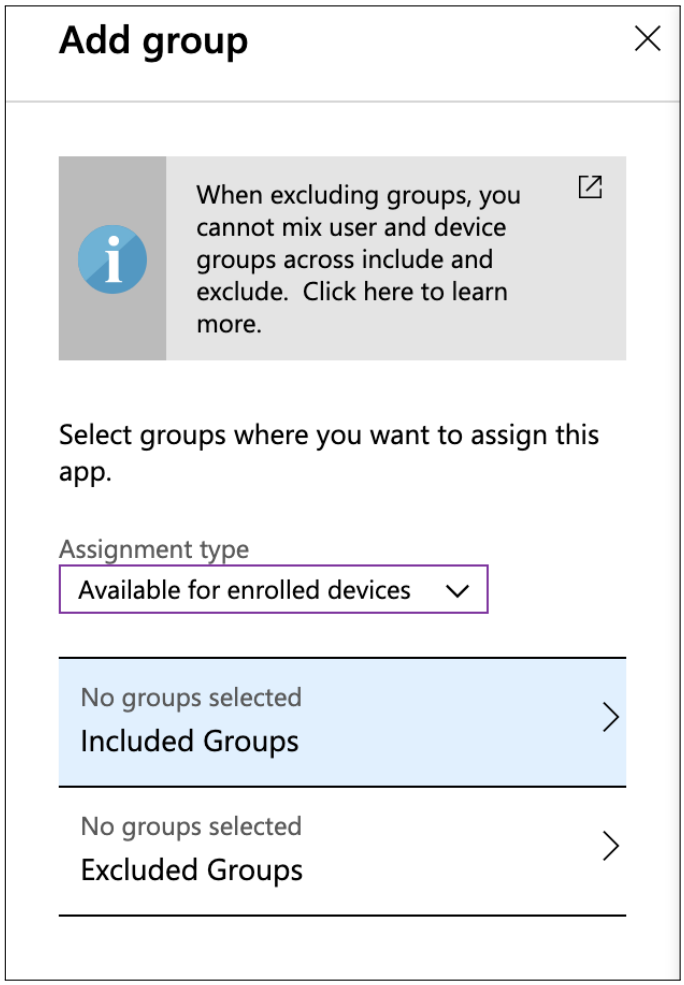
Krav for å opprette en assignment:

- Det er opprettet en applikasjon i Intune

Første steg vil være å navigere seg til "Assignments" inne i applikasjonen som skal tildeles i Intune og trykk "Add group".

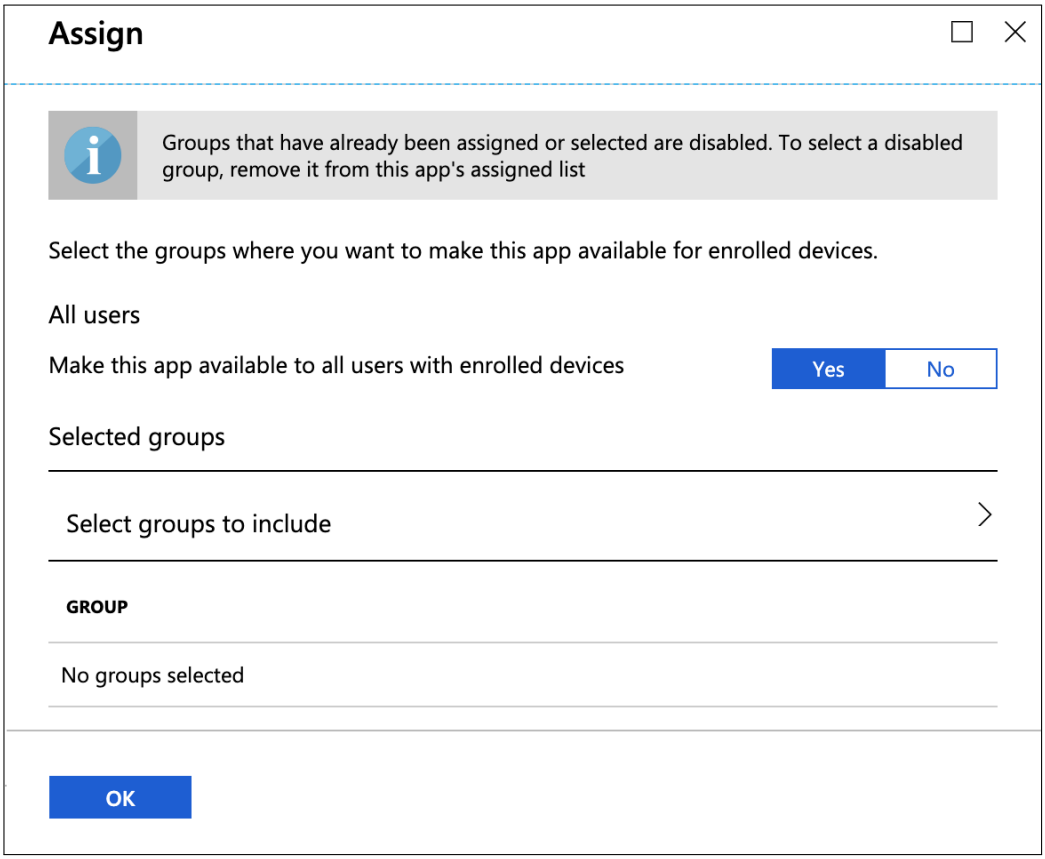
Figur 38

Velg om applikasjonen kun skal være tilgjengelig for enheter den valgte gruppen, eller om applikasjonen er påkrevd.



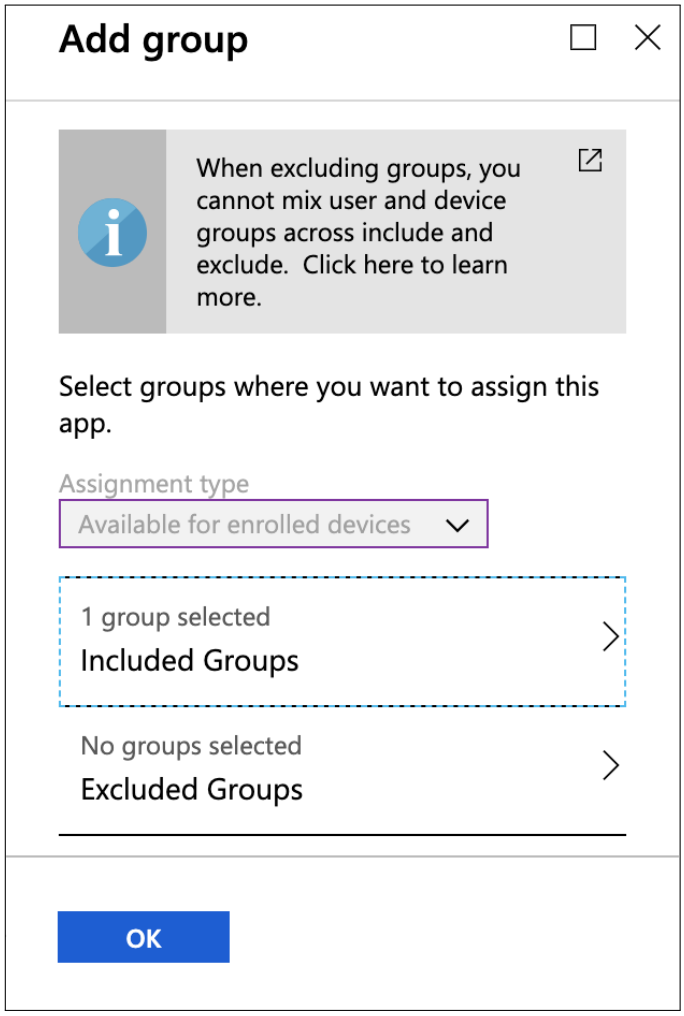
Figur 39

Trykk på “Included Groups” for å velge hvem som skal motta applikasjonen, og velg gruppen som tilsvarer de enheten som skal tildeles applikasjonen. Her kan en også gjøre applikasjonen tilgjengelig for alle brukere med innrullede enheter, noe vi gjør i dette eksempelet. Når du har valgt gruppene som skal inkluderes, trykk “OK”.



Figur 40

Pass på at gruppene som skal inkluderes er med og velg “OK”. Ønsker du å ekskludere visse grupper, kan dette også gjøres her. Dette følger samme prinsipp og framgangsmåte som inklusjon, og vil derfor ikke beskrives.



Figur 41

Siste steg er å lagre tildelingen som gjøres ved å trykke “Save”. Det vil komme opp et varsel som informerer om tildelingen ble lagret eller om den feilet.

Figur 42

4 Nedlastning av applikasjoner

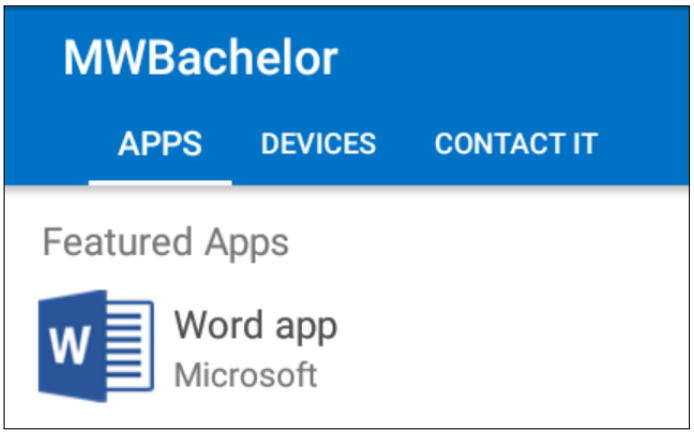
Når brukere har fått tildelt applikasjoner, vil det, avhengig av en rekke parametre, variere hvordan de skal laste de ned. Dersom applikasjonen er påkrevd og den stille rulles ut til brukere, vil applikasjonen enkelt lastes ned i bakgrunnen på enheten uten inngrep fra brukeren. Applikasjoner som tilgjengeliggjøres for brukere, blir synlig for de gjennom en portal, kalt "Microsoft Company Portal", på innrullerte enheter. Denne portalen er tilgjengelig på Windows 10, iOS og Android.

Nedlastning av applikasjoner vil være tilnærmet identisk på alle enheter uavhengig av OS, og vil derfor beskrives kun en gang. Forskjellene vil hovedsakelig ligge i hvilken butikk som brukes til nedlastning av applikasjonen og hva slags brukerkonto som kreves. I dette eksempelet brukes Android som OS og applikasjonen er Microsoft Word.

Krav for nedlastning av applikasjoner:

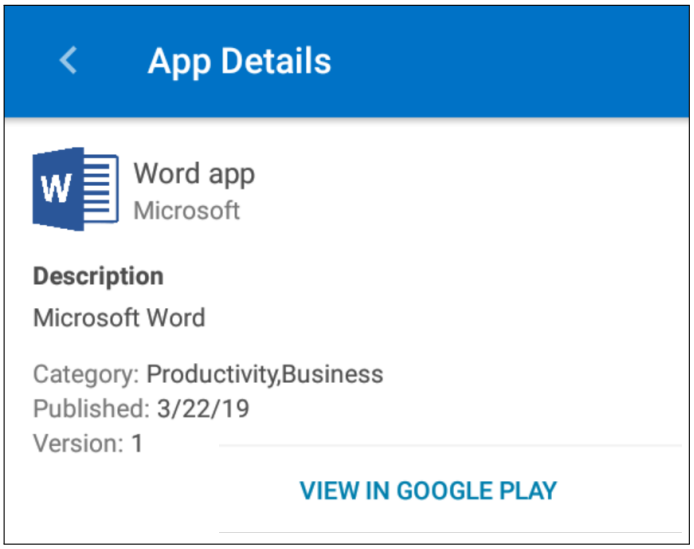
- Applikasjon er opprettet og tildelt til brukere i Intune
- Enhet er innrullert i Intune
- Brukerkonto på Google Play/App Store for mobile enheter
- Microsoft Company Portal er installert

Første steg vil være å navigere seg til applikasjoner inne i Company Portal, og velge applikasjonen som skal lastes ned.



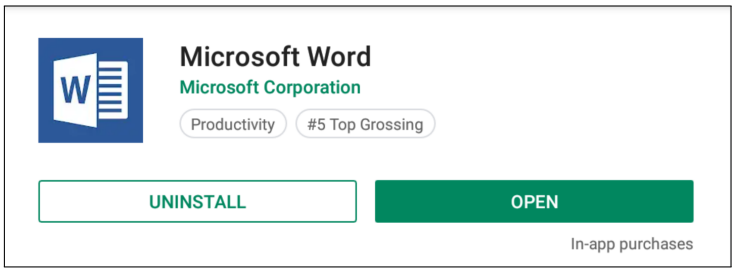
Figur 43

Inne på den valgte applikasjonen får brukeren mer informasjon om applikasjonen og en lenke som fører til applikasjonen i Google Play Store. Her klikker vi på lenken "View in Google Play".



Figur 44

Inne i Google Play er det bare for brukeren å laste ned applikasjonen ved å klikke “Install”, og den vil legges til som en av applikasjonene på enheten. Her må man logge inn med en Google Play-bruker før en får mulighet til å laste ned. Når nedlastningen er ferdig kan en trykke “Open” for å åpne applikasjonen.



Figur 45

5 Konfigurasjon av policies for applikasjoner

Gjennom policies kan en sette sikkerhetsrelaterte restriksjoner for applikasjonene for å hindre misbruk av bedriftsdata. Bedrifter kan selv regulere hvilke restriksjoner de selv ser som nødvendige og ikke, men det er viktig å ikke sette sikkerheten til sides for å gjøre brukernes opplevelse så smidig som mulig.

Policies[7] settes for enheter basert på OS og vil være ulik avhengig av enhet. Vi har derfor valgt å gå gjennom de ulike OS-ene individuelt.

5.1 Android

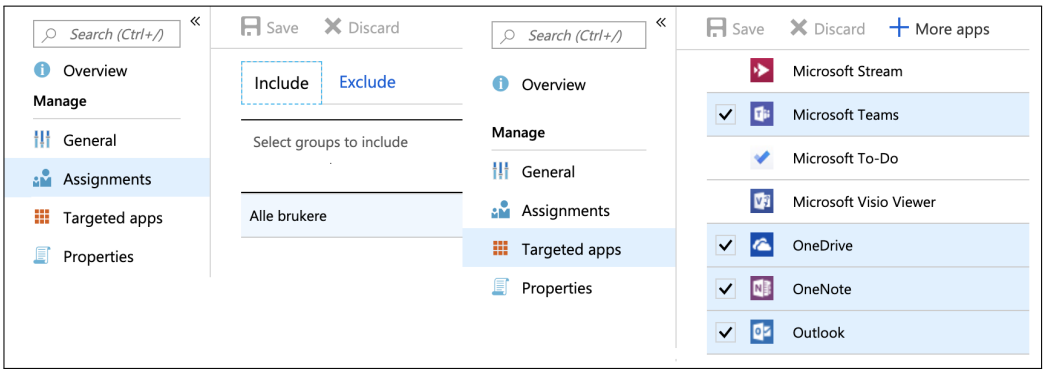
Krav for konfigurasjon av policies for applikasjoner for Android:

- Applikasjonen ligger i Intune

Første steg vil være å navigere seg fram til "App protection policies" inne i Intune og velge Programpolicy for Android".

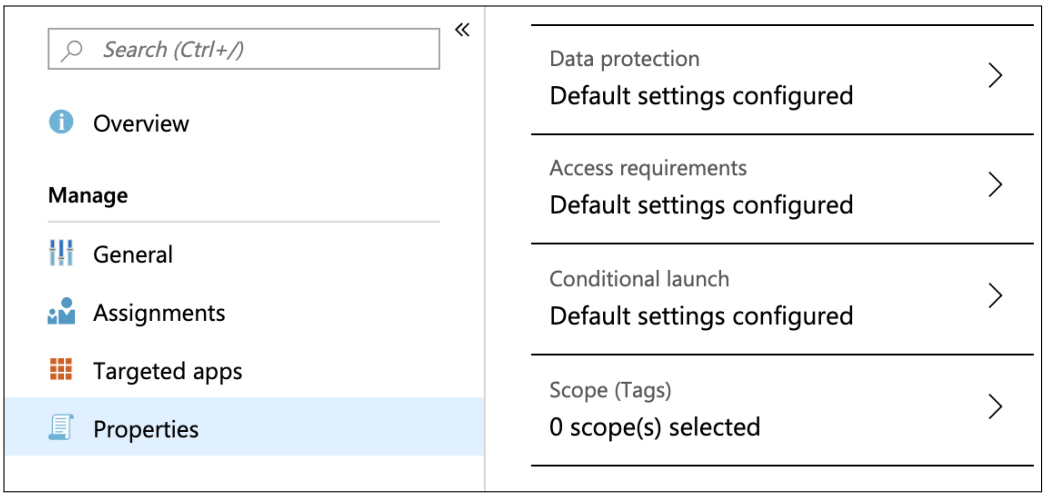
Figur 46

Her inne vil det være flere områder som kan konfigureres, som hvilke applikasjoner, hvilke brukere som blir påvirket og egenskapene for policy. Velg "Assignments" for å tildele policy til valgte brukergrupper og "Targeted apps" for å velge ut applikasjonene som underlegges policy.



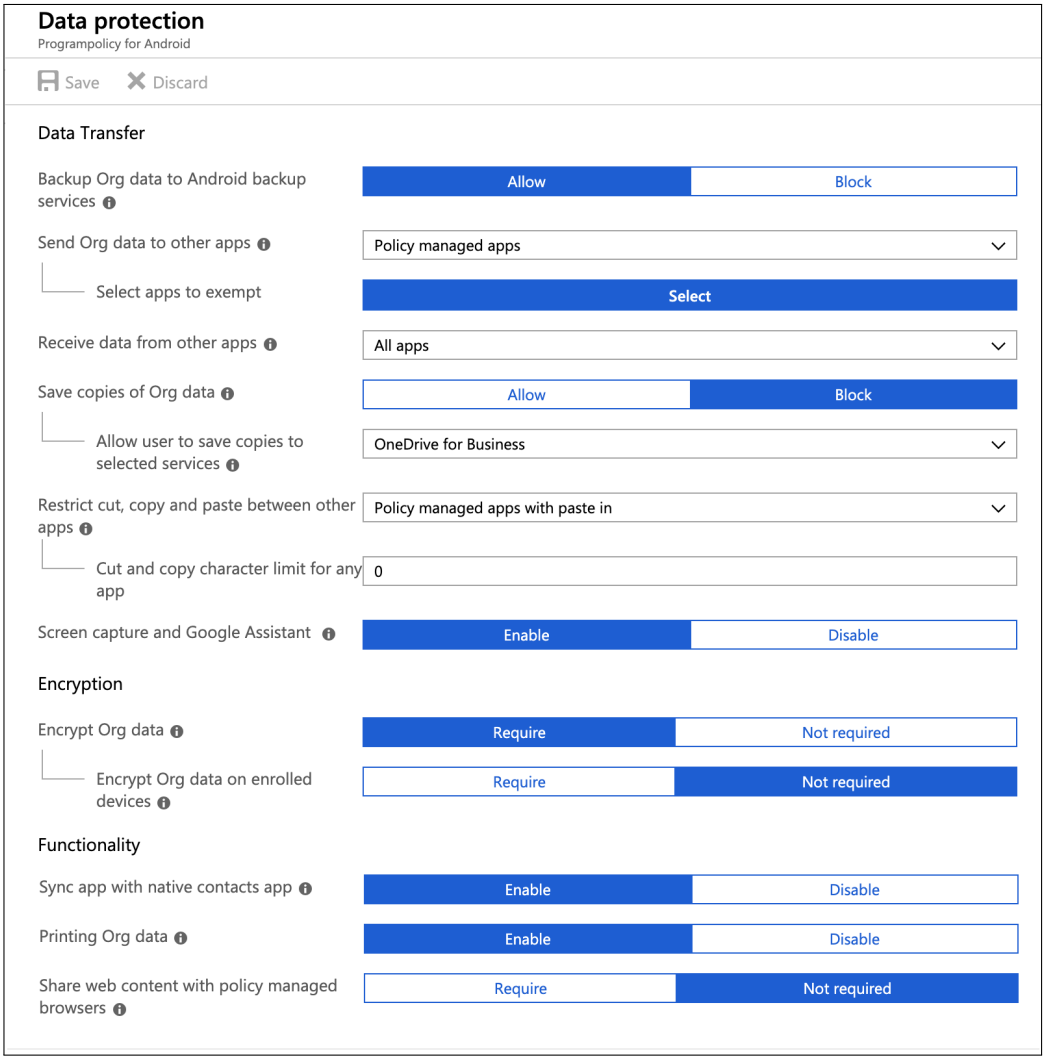
Figur 47

Velg så “Properties” for å få opp egenskapene som skal endres. Her er det viktig å huske at alle endringer som gjøres under “Data protection”, “Access requirements” og “Conditional launch” må lagres individuelt. Det vil ikke komme opp varsler som informerer om endringer blir lagret eller ikke.



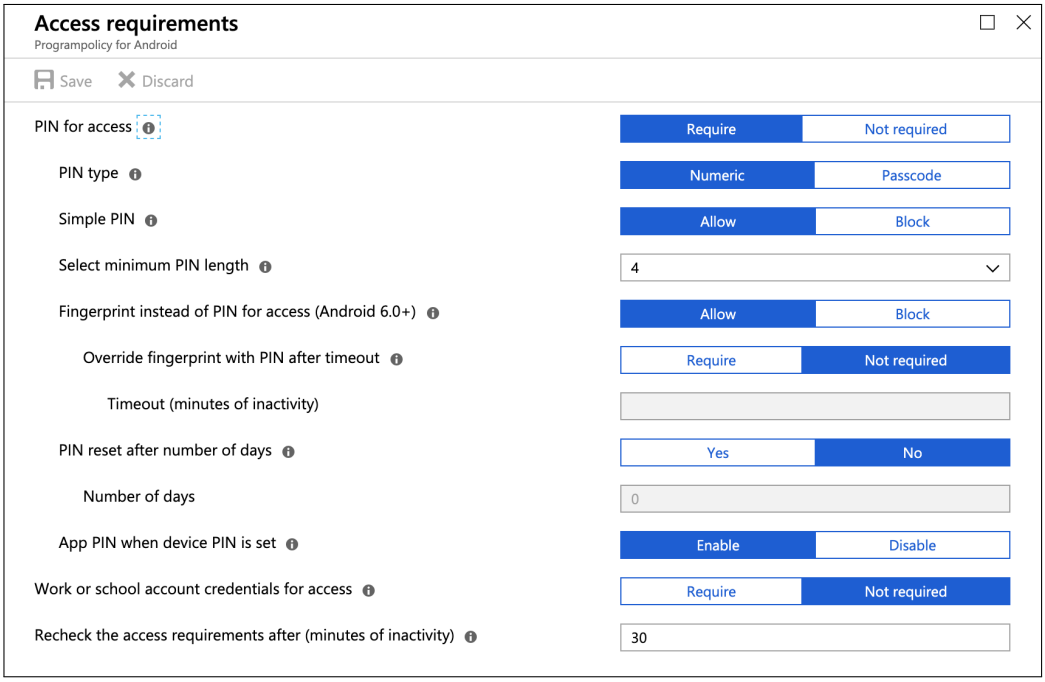
Figur 48

Inne i "Data protection" konfigureres restriksjoner til hvordan bedriftsdata skal behandles innenfor de ulike applikasjonene. Som vist i figur 49, kan blant annet kryptering, sikkerhetskopiering og funksjonalitet konfigureres.



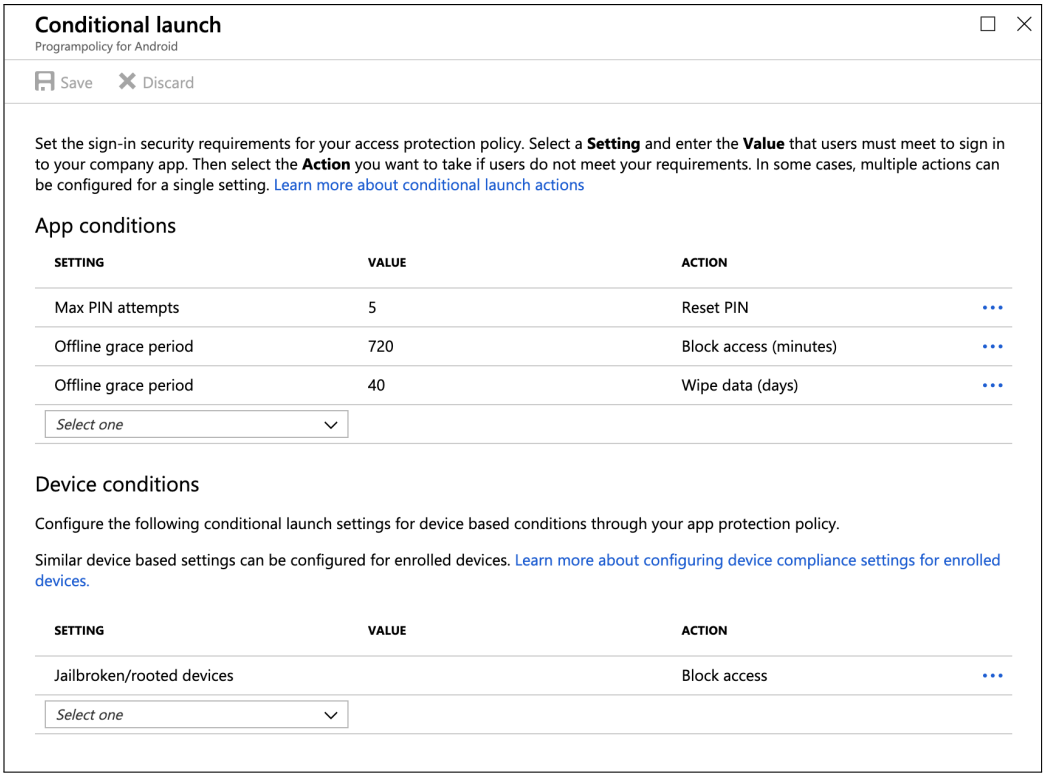
Figur 49

Inne i "Access requirements" konfigureres tilgangskrav på bedriftsinformasjon inne i applikasjonene. Som vist i figur 50, kan blant annet PIN-kode, fingeravtrykk og inaktivitet konfigureres.



Figur 50

Inne i "Conditional Launch" konfigureres tilgangen til applikasjonen. Som vist i figur 51, kan blant annet antall feilskrivinger av PIN-kode, tidsperiode med inaktivitet og enhetstype konfigureres. Konfigurasjonen er todelt i at en handling konfigureres ut ifra det som foregår på enheten. For eksempel må PIN-koden tilbakestilles dersom bruker skriver feil fem ganger.



Figur 51

Siste steg vil være å lagre sikkerhetsprofilen ved å trykke "Save". Det vil ikke gis tilbakemelding som tilsier at profilen ble lagret, så det vil være anbefalt å dobbeltsjekke at endringer blir lagret.

5.2 iOS

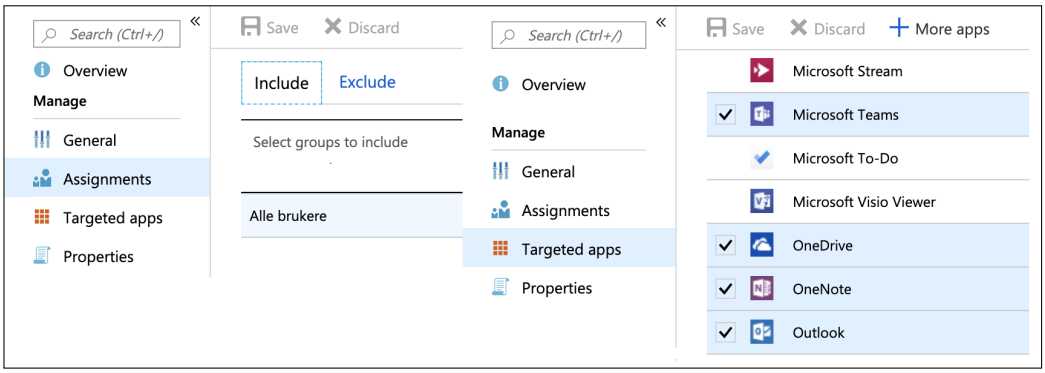
Krav for konfigurasjon av policies for applikasjoner for iOS:

- Applikasjonen ligger i Intune

Første steg vil være å navigere seg fram til "App protection policies" inne i Intune og velge Programpolicy for iOS".

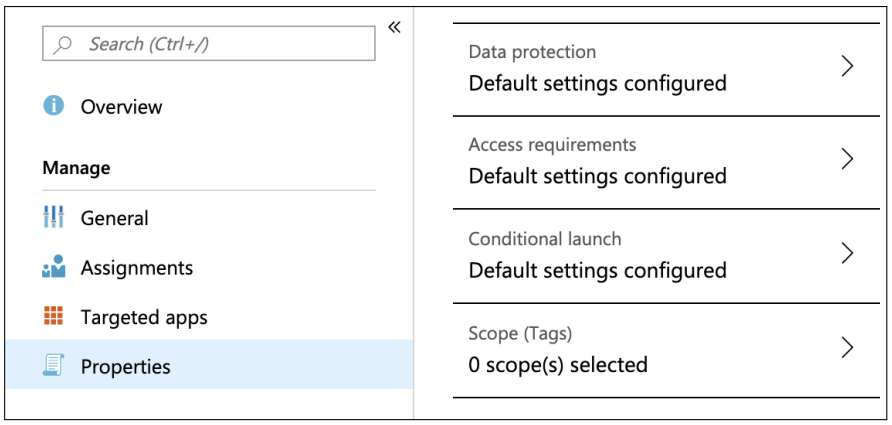
Figur 52

Her inne vil det være flere områder som kan konfigureres, som hvilke applikasjoner, hvilke brukere som blir påvirket og egenskapene for policy. Velg "Assignments" for å tildele policy til valgte brukergrupper og "Targeted apps" for å velge ut applikasjonene som underlegges policy.



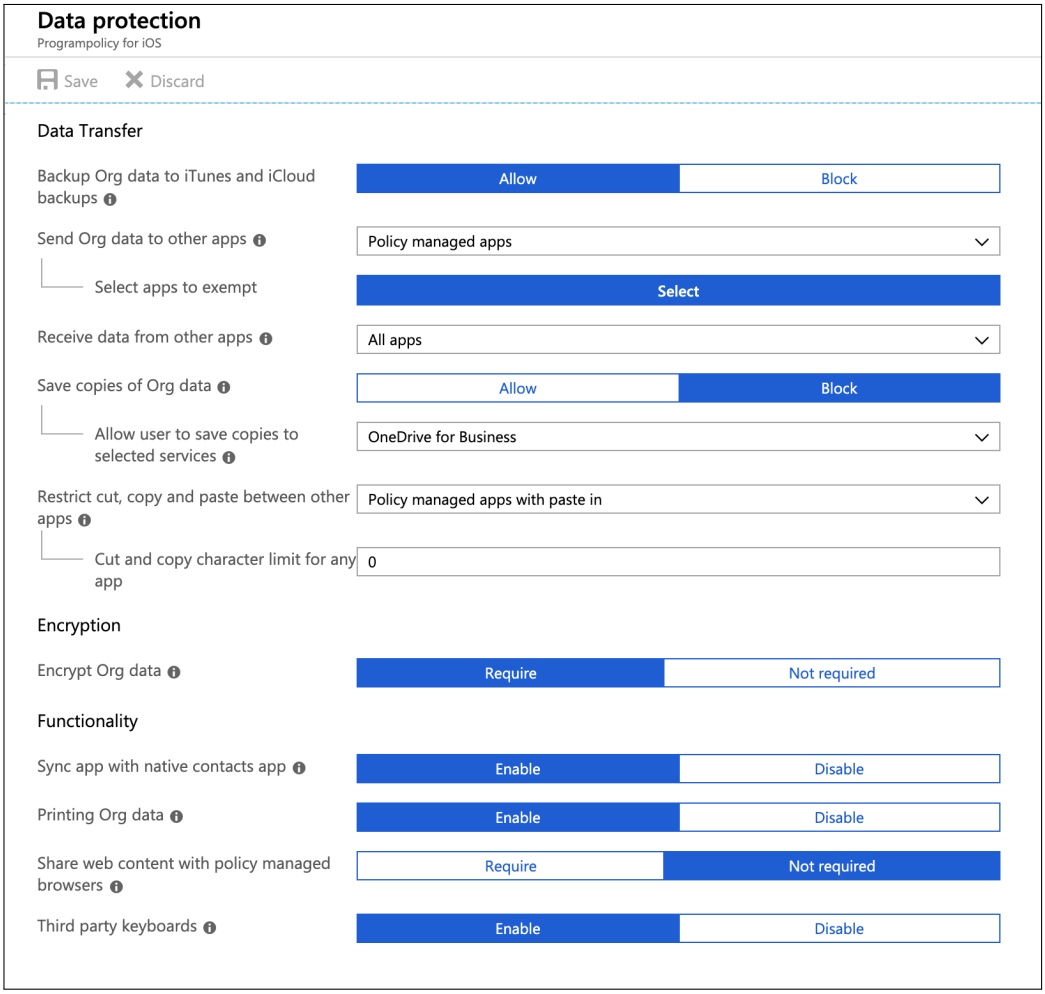
Figur 53

Velg så "Properties" for å få opp egenskapene som skal endres. Her er det viktig å huske at alle endringer som gjøres under "Data protection", "Access requirements" og "Conditional launch" må lagres individuelt. Det vil ikke komme opp varsler som informerer om endringer blir lagret eller ikke.



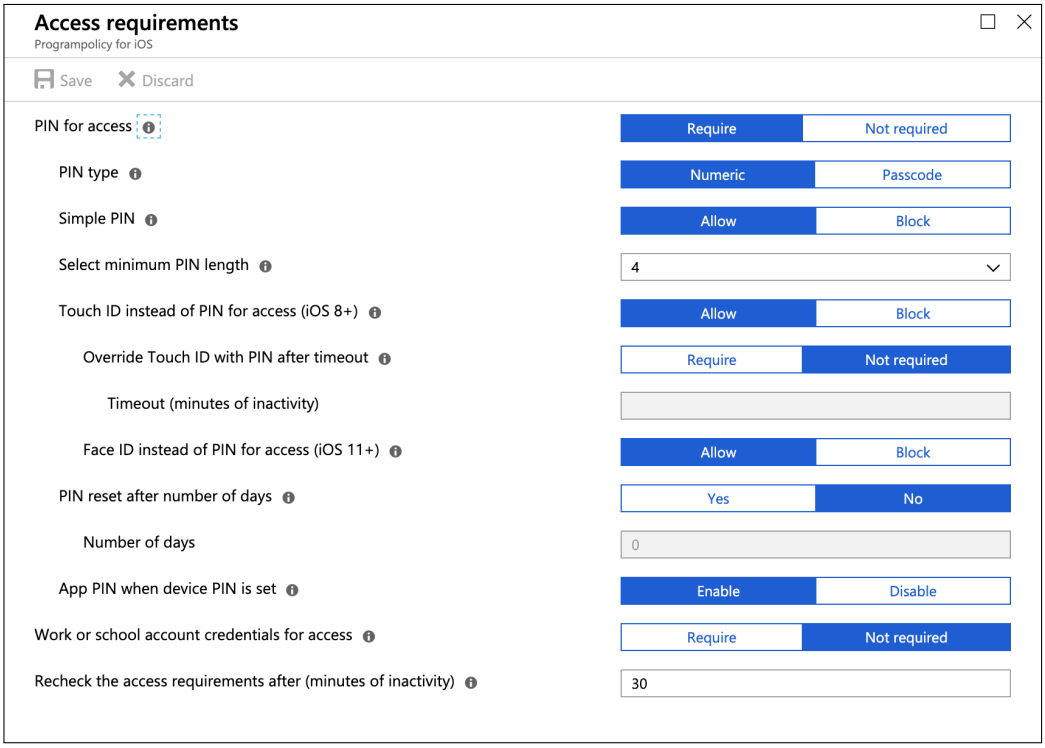
Figur 54

Inne i "Data protection" konfigureres restriksjoner til hvordan bedriftsdata skal behandles innenfor de ulike applikasjonene. Som vist i figur 55, kan blant annet kryptering, sikkerhetskopiering og funksjonalitet konfigureres.



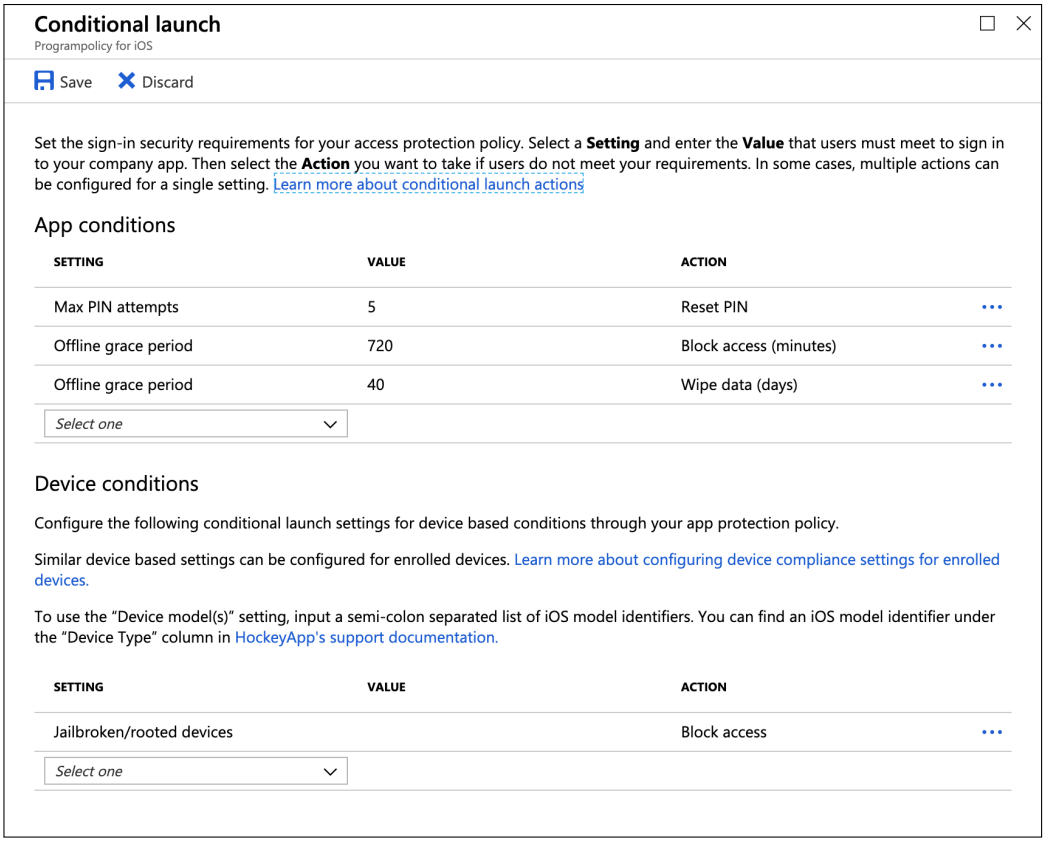
Figur 55

Inne i "Access requirements" konfigureres tilgangskrav på bedriftsinformasjon inne i applikasjonene. Som vist i figur 56, kan blant annet PIN-kode, Touch ID, Face ID og inaktivitet konfigureres.



Figur 56

Inne i "Conditional Launch" konfigureres tilgangen til applikasjonen. Som vist i figur 57, kan blant annet antall feilskrivinger av PIN-kode, tidsperiode med inaktivitet og enhetstype konfigureres. Konfigurasjonen er todelt i at en handling konfigureres ut ifra det som foregår på enheten. For eksempel må PIN-koden tilbakestilles dersom bruker skriver feil fem ganger.



Figur 57

Siden det ikke gis tilbakemelding om hvorvidt endringer lagres, så vil siste steg være å dobbeltsjekke at endringer har blitt lagret og at profilen er konfigurert riktig.

5.3 Windows 10

For Windows 10 er det verdt å nevne at det går et skille mellom enheter som er innrullet og ikke, men siden oppsett er tilnærmet identisk på disse to vil det kun vises fram en gang. Vi bruker innrullerte enheter i dette eksempelet.

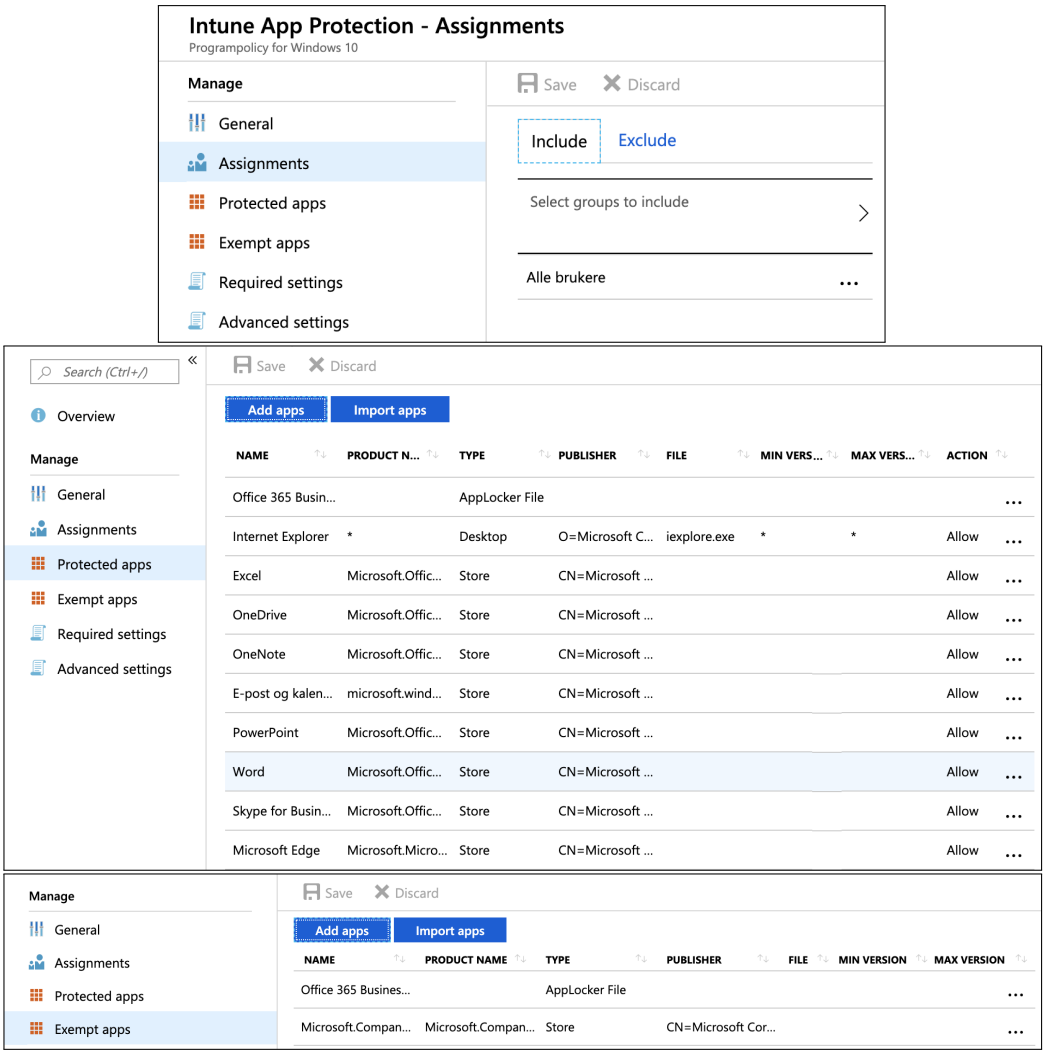
Krav til konfigurasjon av policies på Windows 10-enheter:

- Applikasjonen ligger i Intune

Første steg vil være å navigere seg fram til "App protection policies" inne i Intune og velge Programpolicy for Windows 10".

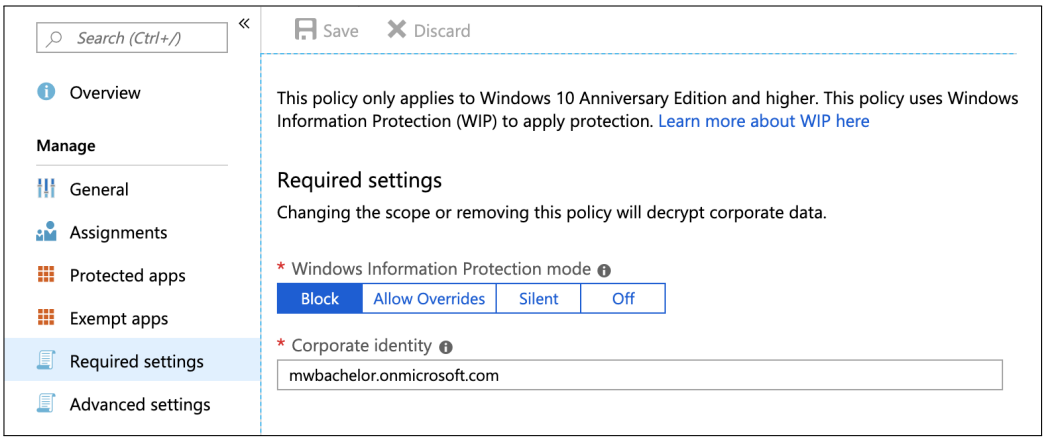
Figur 58

Her inne vil det være flere områder som kan konfigureres, som hvilke applikasjoner, hvilke brukere som blir påvirket og egenskapene for policy. Velg "Assignments" for å tildele policy til valgte brukergrupper og "Protected apps" for å legge til applikasjonene som underlegges policy. Her kan en også legge til applikasjoner som ikke skal underlegges policy, under "Exempt apps". Det er også greit å nevne at alle endringer lagres uten at det gis tilbakemelding til brukeren hvorvidt endringene ble lagret eller ikke.



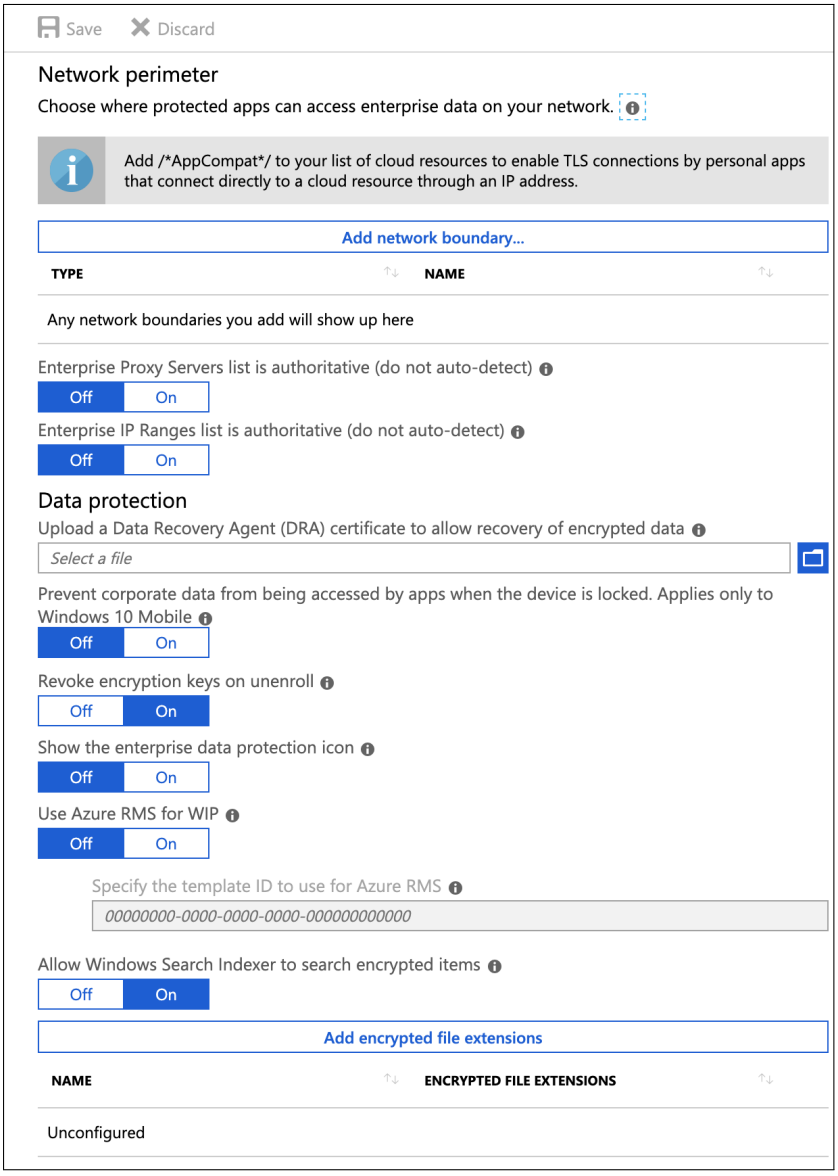
Figur 59

Under “Required settings” kan behandling av bedriftsdata konfigureres. Som vist i figur 60 blokkeres forsøk på å bevege bedriftsdata fra beskyttede applikasjoner. Dette kan endres ut ifra bedriftens behov, slik at brukere for eksempel kan bevege bedriftsdata ut, men får en advarsel eller at det loggføres i Intune.



Figur 60

Inne i "Advanced settings" kan, blant annet, hvilke nettverk brukere må være på for å få tilgang på bedriftsdata, gjenoppretting av kryptert data og fjerning av gjenopprettingsnøkler fra maskiner som ikke lenger er innrullert, konfigureres.



Figur 61

Siden det ikke gis tilbakemelding om hvorvidt endringer lagres, så vil siste steg være å dobbeltsjekke at endringer har blitt lagret og at profilen er konfigurert riktig.

Referanser

[1] Microsoft. *Add Android store apps to Microsoft Intune*. 2018. URL: https://docs.microsoft.com/en-us/intune/store-apps-android (sjekket 06.05.2019).

[2] Microsoft. *Add iOS store apps to Microsoft Intune*. 2018. URL: https://docs.microsoft.com/en-us/intune/store-apps-ios (sjekket 06.05.2019).

[3] Microsoft. *Add Microsoft Store apps to Microsoft Intune*. 2019. URL: https://docs.microsoft.com/en-us/intune/store-apps-windows (sjekket 06.05.2019).

[4] Microsoft. *How to manage volume purchased (or free) apps from the Microsoft Store for Business with Microsoft Intune*. 2019. URL: https://docs.microsoft.com/nb-no/intune/windows-store-for-business (sjekket 06.05.2019).

[5] Microsoft. *Intune Standalone - Win32 app management*. 2019. URL: https://docs.microsoft.com/en-us/intune/apps-win32-app-management (sjekket 06.05.2019).

[6] Microsoft. *Assign apps to groups with Microsoft Intune*. 2019. URL: https://docs.microsoft.com/en-us/intune/apps-deploy (sjekket 06.05.2019).

[7] Microsoft. *What are app protection policies?* 2019. URL: https://docs.microsoft.com/en-us/intune/app-protection-policy (sjekket 06.05.2019).

Modern Workspace - Driftsdokument
Azure Information Protection

v.0.6

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
05.04.2019	0.1	Dokument opprettet
08.04.2019	0.2	Introduksjon skrevet, legge til azure information protection i azure skrevet, aktiver AIP skrevet, standarder skrevet, legge til brukere i policy skrevet, installasjon av klient skrevet, demo skrevet, figurer lagt til
11.04.2019	0.3	Innholdsfortegnelse oppdatert
17.04.2019	0.4	Mindre endringer i dokumentets struktur, oppdatert figurer og revidert noen figurtekster
24.04.2019	0.5	Introduksjon revidert, større revisjoner på tekst i hele dokumentet
05.05.2019	0.6	Mindre revisjon av tekst, fikset grammatiske og språklige feil

Innhold

1 Introduksjon

I dette dokumentet vil det fokuseres på ressursen Azure Information Protection[1]. Ved å benytte Azure Information Protection, heretter forkortet AIP, kan dokumenter og e-poster klassifiseres med etiketter og krypteres. AIP lar organisasjonen sikre dokumenter, slik at de er beskyttet og dermed ubrukelige om de skulle komme på avveie. Denne dokumentasjonen omtaler kun Azure Information Protection og ikke Microsofts nye Sensitivity labels"[2].

AIP opprettes som en ressurs i Azure-portalen. Klassifiseringer består av etiketter, graderinger, klassifiseringer og policies. Det opprettes etiketter for forskjellige graderinger og klassifiseringer. De ulike etikettene kan ha innstillinger omkring kryptering, lengde på offline tilgang, vannmerker og annet. Policies binder etiketter og brukergrupper sammen med et regelsett for hvordan bruken av etikettene skal foregå.

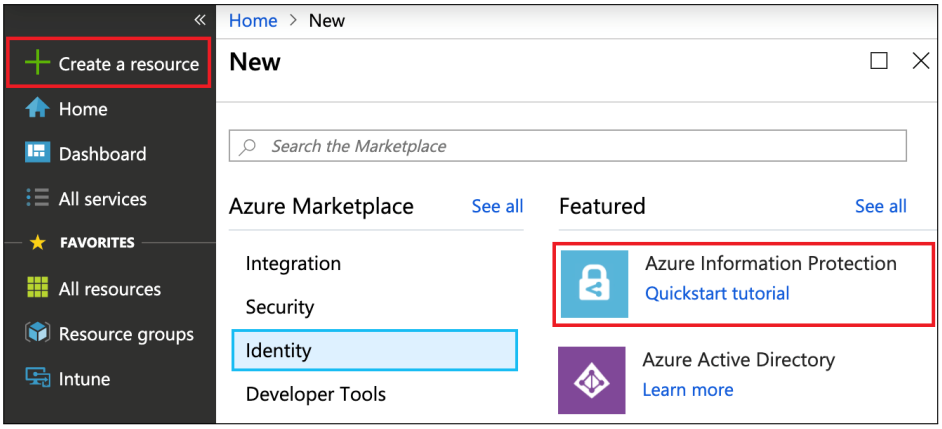
AIP tillater også å automatisk oppdage, gradere og beskytte dokumenter som allerede eksisterer lokalt eller i skyen. For å få denne muligheten må en scanner[3] installeres på en maskin med Windows Server. Vi vil ikke gå gjennom dette i vår dokumentasjon, men det kan være aktuelt å gjennomføre i andre prosjekter.

Dokumentet vil gå ut ifra at leser har en viss teknisk kunnskap, og vil ikke nødvendigvis være enkelt å forstå for ufaglærte.

2 Legge til AIP-ressursen

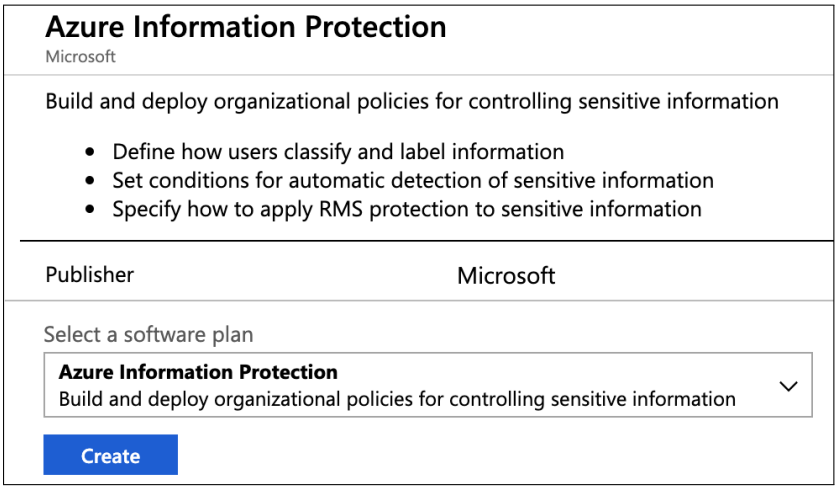
For å bruke Azure Information Protection kreves det at AIP er lagt til som ressurs i Azure-portalen.

AIP legges til på samme måte som andre ressurser i Azure, trykk på "Create a resource", lokaliser tjenesten ved å søke eller bruk kategoriene på venstre side. Trykk på tjenesten for å starte veiviseren.



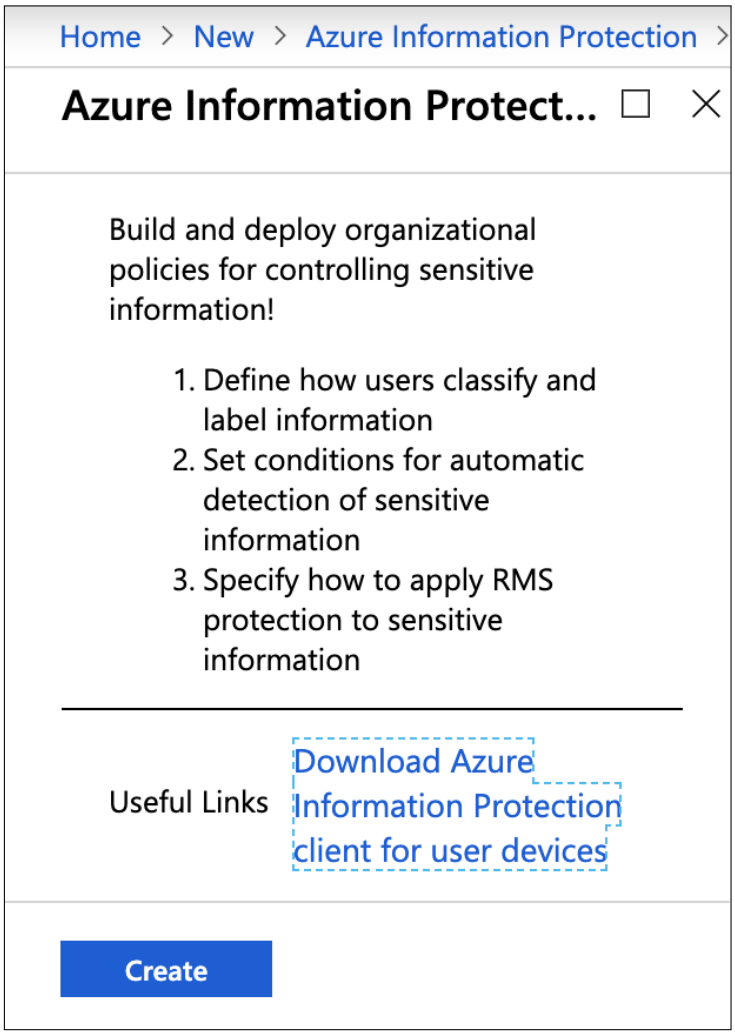
Figur 1

Klikk her på "Create" for å starte oppretting av AIP-ressursen.



Figur 2

Les gjennom informasjonen om AIP slik at du forstår hva ressursen kan tilby. Klikk så “Create” for å opprette AIP-ressursen.

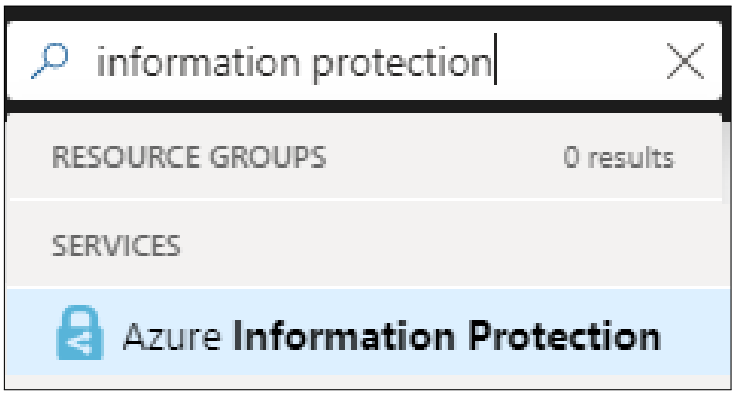


Figur 3

3 Aktiver AIP

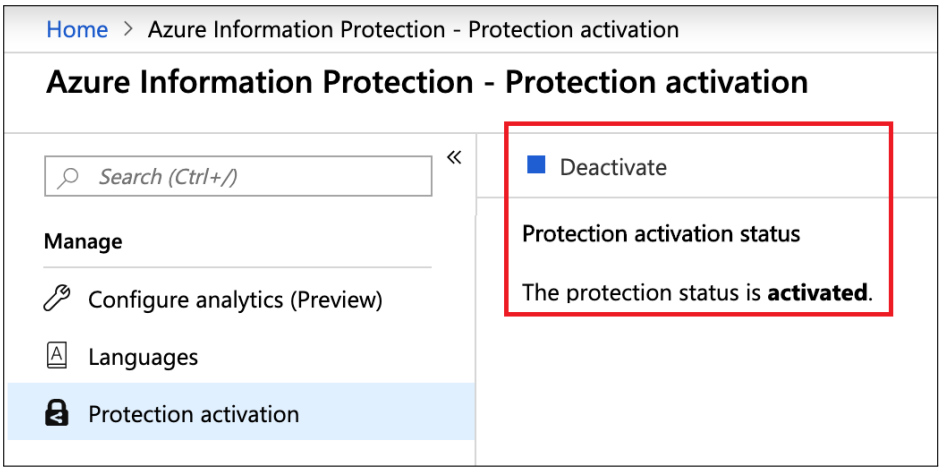
Det vil være lurt å ta en sjekk på at alt gikk fint ved oppretting av ressursen. Dette gjøres ved å sjekke at tjenesten ble aktivert.

For å komme til AIP i Azure er det bare å søke etter "Azure Information Protection" og velge alternativet med hengelåsen som vist i figur 4.



Figur 4

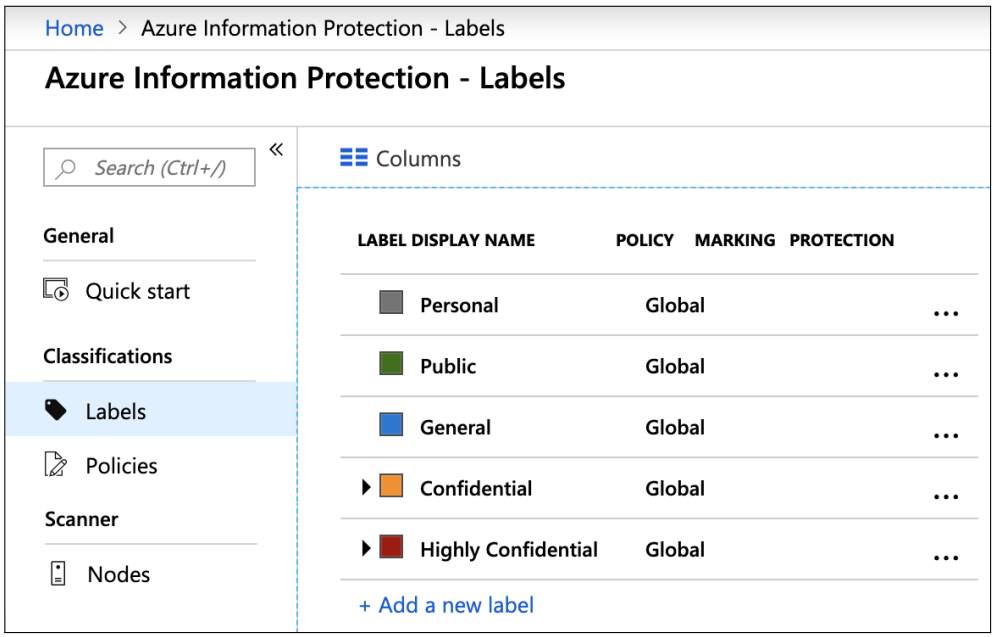
Som vi ser i figur 5, er det en meny på venstre side. I menyen trykker vi på "Protection activation". Her kan vi bekrefte at statusen for beskyttelse er aktivert, noe som vises med teksten "The protection status is activated" og en knapp for deaktivering.



Figur 5

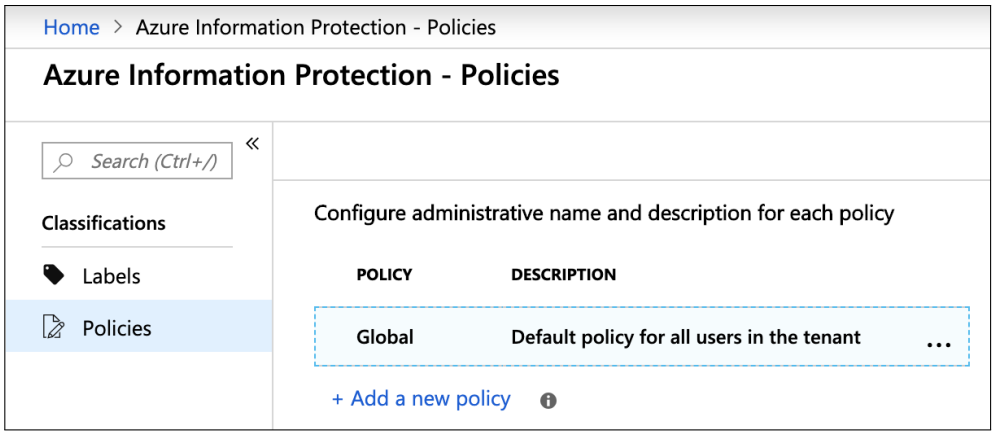
4 Standarder

Når en setter opp AIP vil det automatisk opprettes en standardprofil og flere etiketter. Vi kan se etikettene i figur 6.



Figur 6

Vi kan se standardprofilen i figur 7, men selv om beskrivelsen sier at denne policy gjelder for alle brukere er den ikke tildelt noen automatisk. Tildeling må gjøres manuelt.

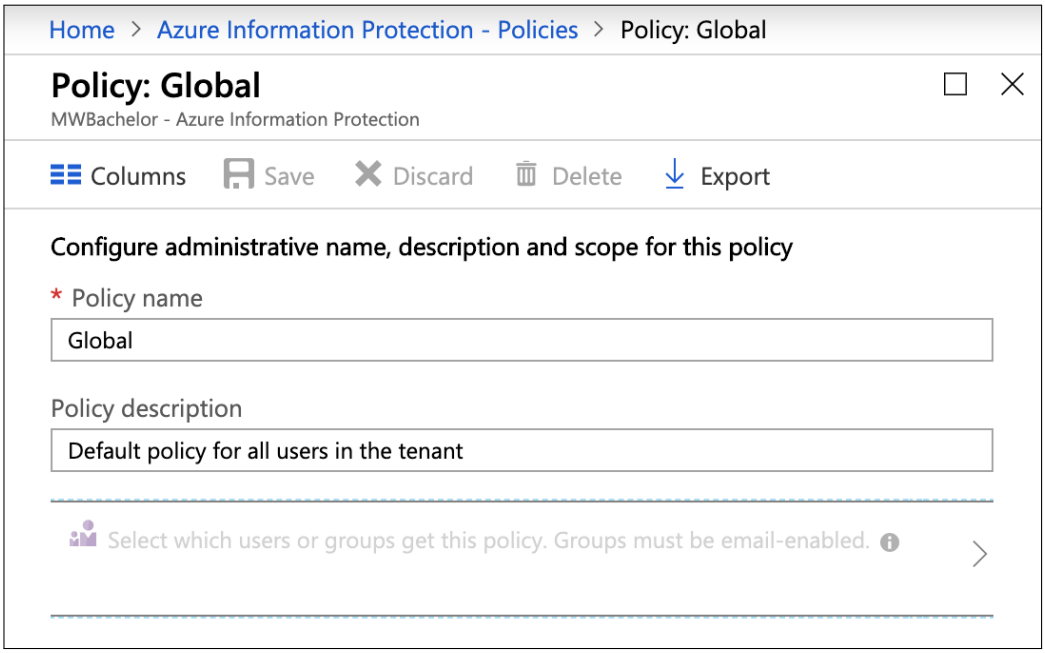


Figur 7

5 Legge til brukere og grupper i policy

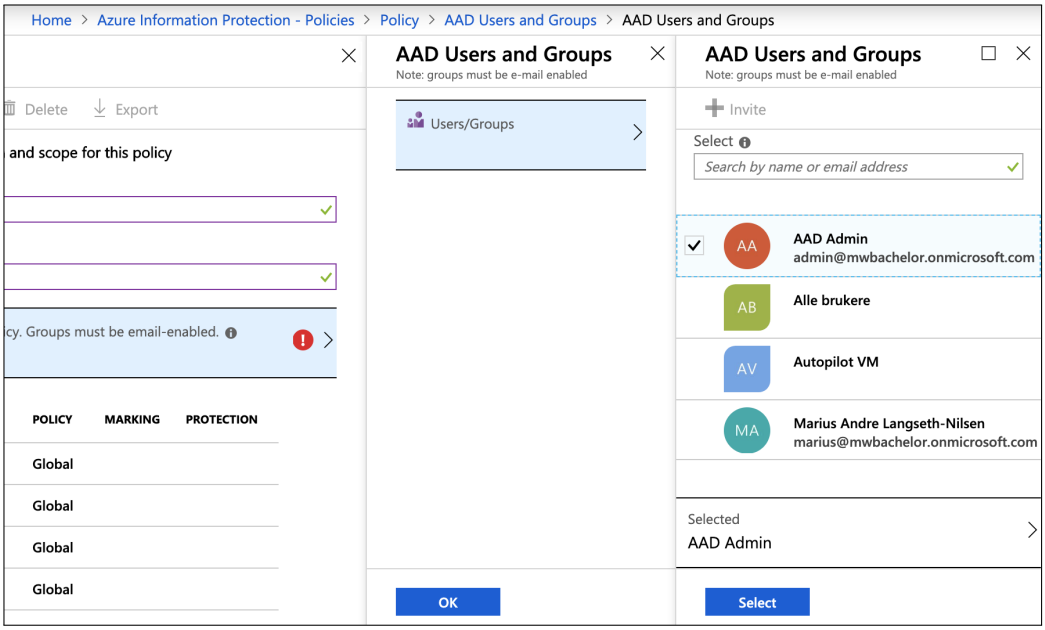
For at en policy skal ha noen innvirkning må den tildeles brukere eller brukergrupper. Disse brukerne blir da underlagt den valgte policy, og gjør at en kan velge hvilke brukere som trenger ulike rettigheter.

Ved å klikke på en policy blir det mulig å redigere den. På figur 8 er den globale policy åpnet, og under navnet og beskrivelsen er det mulighet for å legge brukere eller grupper inn i den.



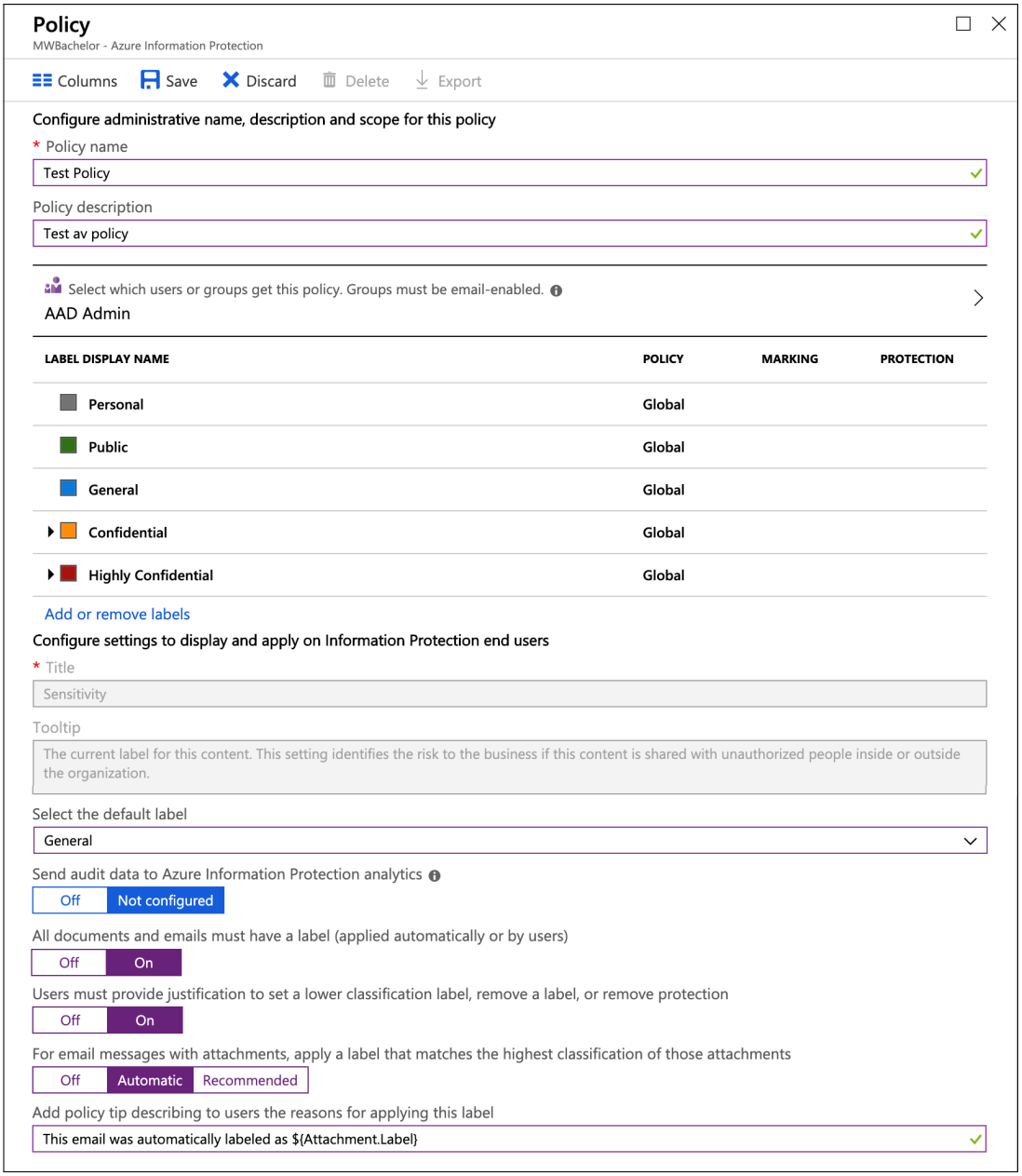
Figur 8: Øverste del av profilen

Vi oppretter en ny profil fremfor å redigere den Globale profilen, da det ikke er mulig å tildele profilen til gruppen “Alle brukere”. Grunnen til dette er at noen av brukerne i AAD ikke var “e-mail enabled”. Derfor ble denne policy gitt til en enkeltbruker, se figur 9.



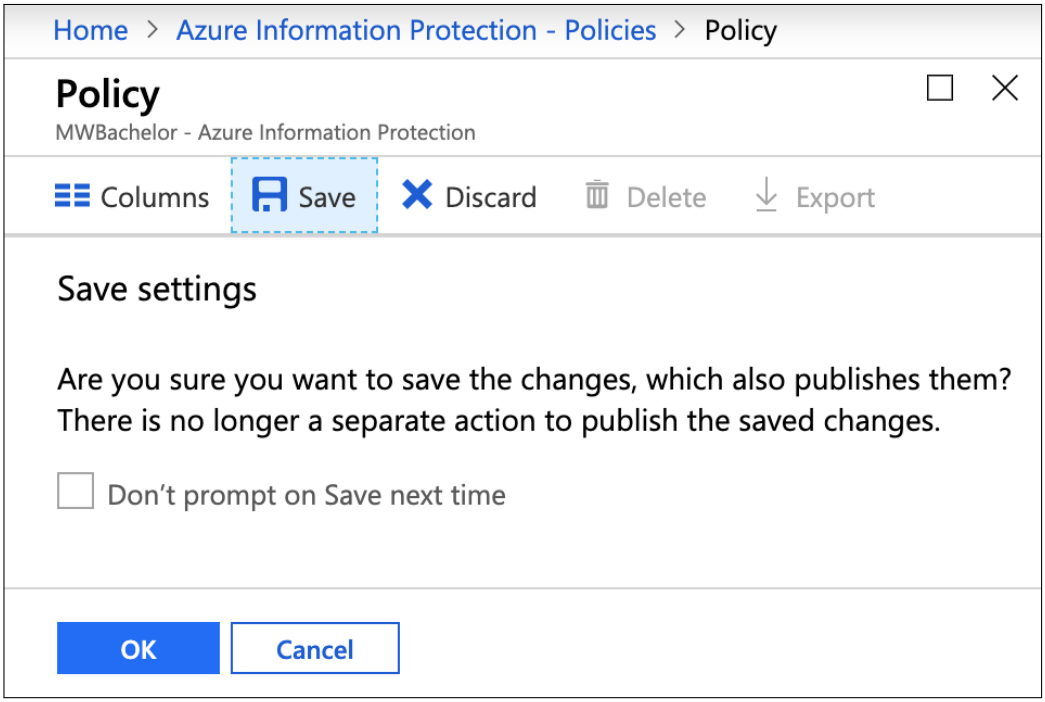
Figur 9: Profilen tildeles bruker

Policy i sin helhet ser vi i figur 10. Valgene som har fått lilla farge er endringer fra standardoppsett. Profilen bestemmer at alle dokumenter skal ha en klassifisering, standard klassifisering er "General", hvis en bruker ønsker å redusere klassifiseringen på det dokument må det oppgis en begrunnelse og all e-post får samme klassifisering som den høyeste klassifiseringen på vedleggene i e-posten.



Figur 10: Hele profilen

Hvis en policy er aktiv og endres vil endringene publiseres når den lagres. Det vil komme et varsel om dette. Varselet må godtas, ellers vil ikke endringene lagres. Trykk “Save” og “OK” for å lagre endringene.

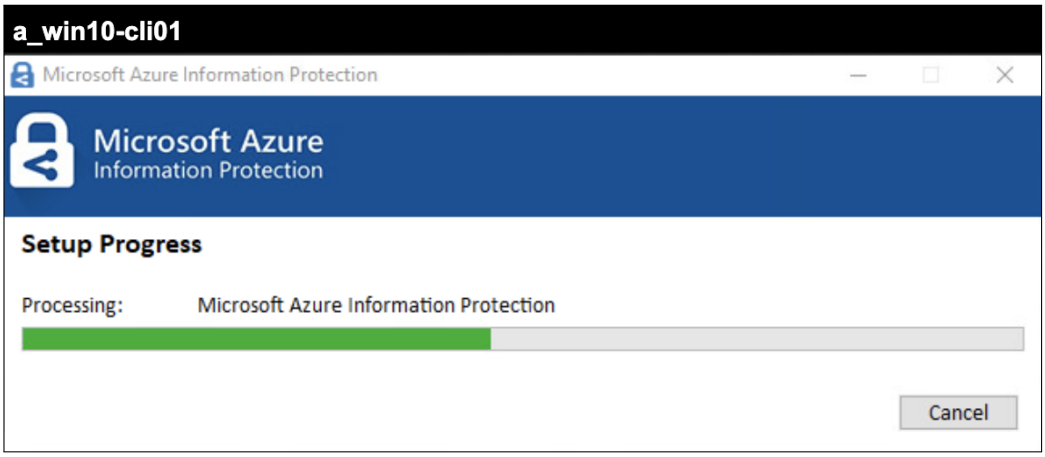


Figur 11: Varsel ved lagring

6 Installasjon av klient

Programvaren for Azure Information Protection må installeres på alle de ansattes klienter for at krypteringen skal fungere. Applikasjonen kan installeres manuelt hos klienter, men det anbefales å publisere applikasjonen og tvangsinstallere den på alle Windows 10-maskiner. Hvordan en publiserer applikasjoner og konfigurerer disse vises i dokumentet "Driftsdokument - Applikasjoner". AIP-applikasjonen er også tilgjengelig for mobile enheter som kjører iOS eller Android.

Figur 12 viser en pågående installasjon av AIP-applikasjonen på en Windows 10-maskin.



Figur 12: Installasjon av klient

7 Demo

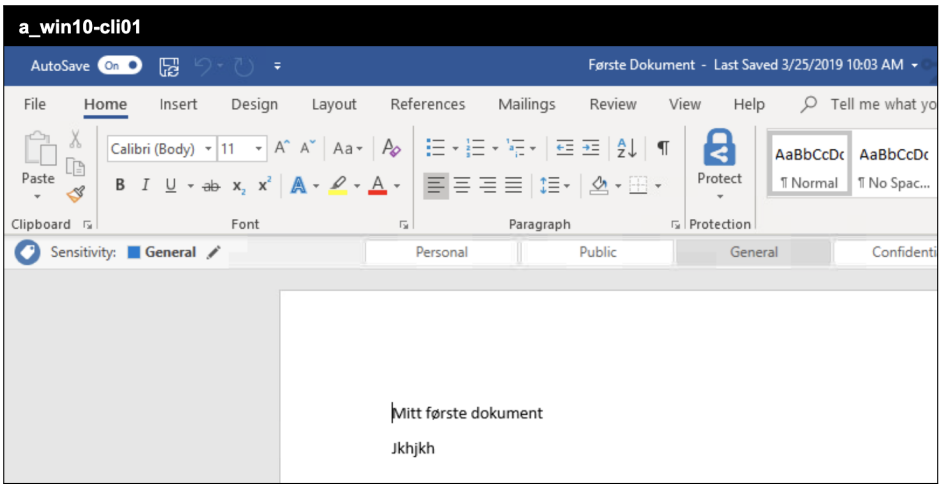
Vi vil her gå kort gjennom hvordan AIP vil se ut og oppleves for brukere, slik at det er tydelig hvilket resultat en skal se etter.

AIP-tillegget vil lastes inn når en starter et av de ulike Office-programmene. Som vist i figur 13, lastes AIP inn under oppstart av Word.

Figur 13

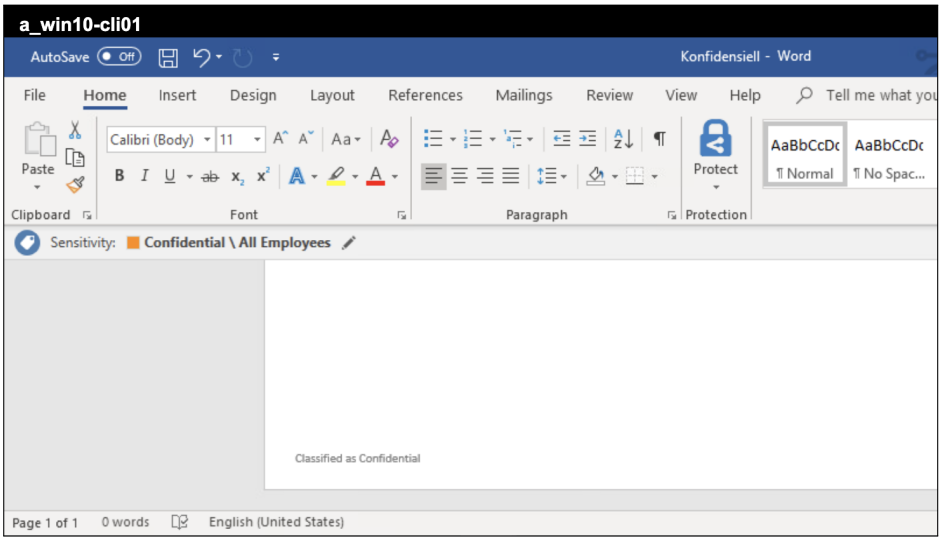
Når dokumenter åpnes vil det nå eksistere en linje øverst i dokumentet med gjeldende klassifisering og mulighet til å endre denne klassifiseringen, som vist i figur 14. I menylinjen har vi nå også fått muligheten til å beskytte dokumenter ved trykke på hengelåsen som leser "Protect". Vi oppretter to ulike dokumenter med ulik klassifisering, i.e "General" og "Confidential".

Dokumentet "Første Dokument" har i figur 14 sensitivtetsgrad "General".



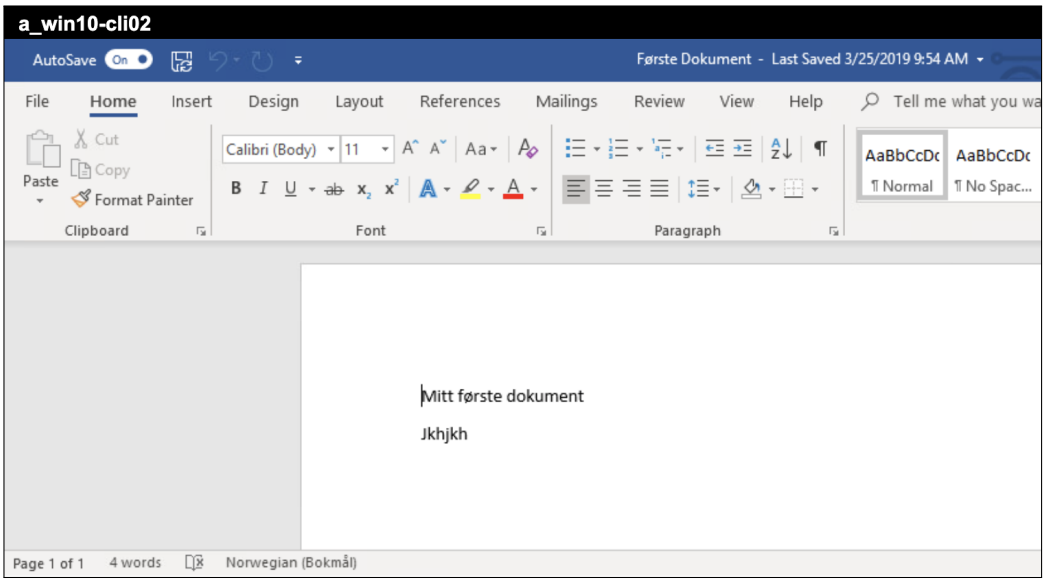
Figur 14

Dokumentet "Konfidensiell" har i figur 15 sensitivitetsgrad "Confidential", det automatisk blir lagt til et vannmerke med klassifiseringen på bunnen av siden.



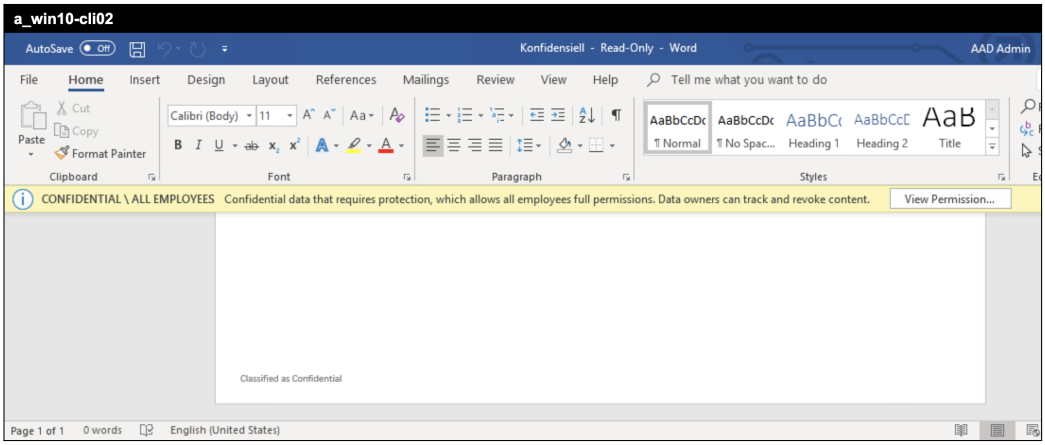
Figur 15

Åpner vi dokumentene på en maskin uten AIP-applikasjonen installert vil dokumentene oppføre seg ulikt avhengig av klassifiseringen. Dokumentet som fikk sensitivetsgrad "General", som vist i figur 16, vil oppføre seg som et vanlig Word-dokument, og vil ikke komme med noen restriksjoner.



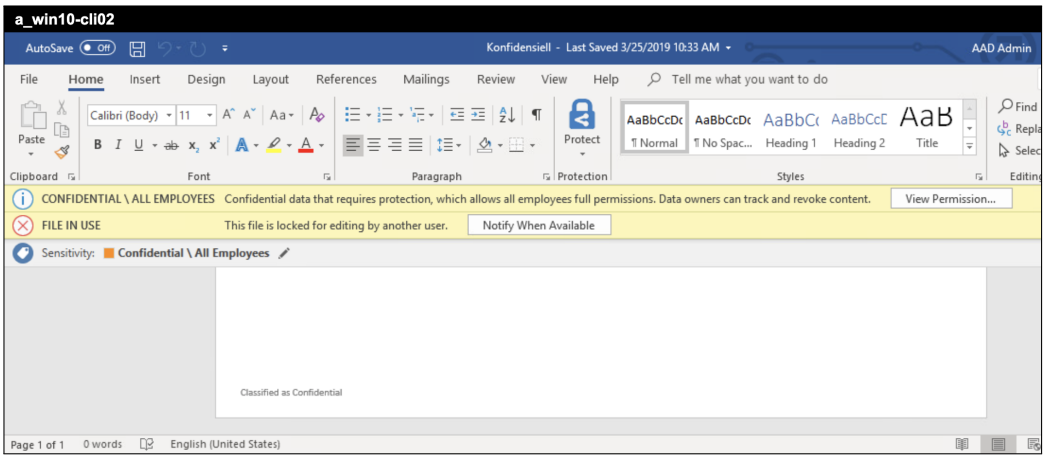
Figur 16

Dokumentet som fikk sensitivitetsgrad "Confidential" oppfører seg derimot annerledes. Siden brukeren ikke har applikasjonen nedlastet får ikke brukeren mulighet til å endre noe i dokumentet, og har kun lesetilgang. Dette vises i figur 17. Vi kan også se dokumentets vannmerke med klassifiseringen nede i venstre hjørne.



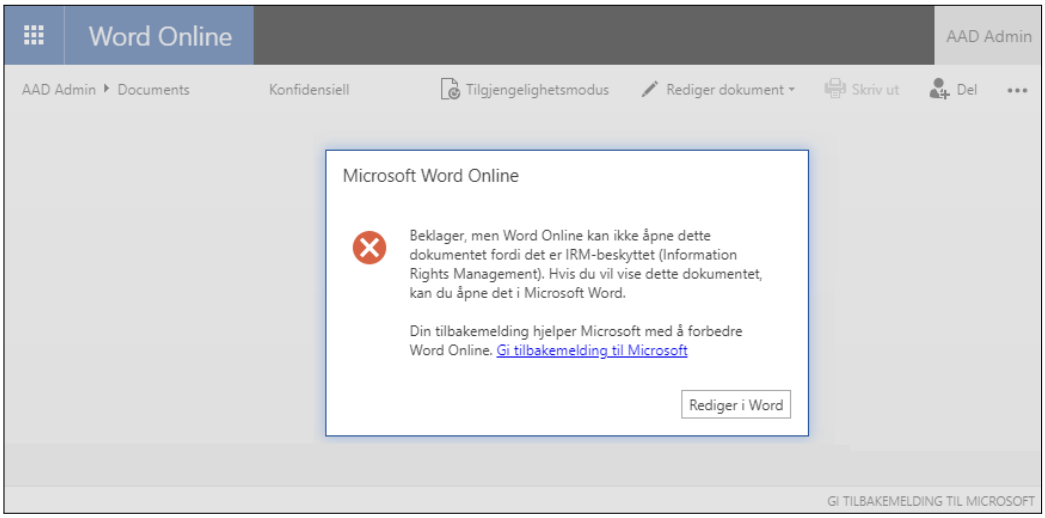
Figur 17

Vi installerer så AIP-applikasjonen, og kan se at det konfidensielle dokumentet nå vil oppføre seg som forventet. Som vi ser i figur 18, har vi nå redigeringsmuligheter, men siden dokumentet er åpent hos en annen bruker, vil AIP låse disse redigeringsmulighetene.



Figur 18

Forsøker vi å på å åpne det konfidensielle dokumentet i web-versjonen av Office 365, resulterer det i en melding om at dokumentet er beskyttet og må åpnes i den lokale versjonen av Word. Denne meldingen vises i figur 19.



Figur 19

Referanser

[1] Microsoft. *What is Azure Information Protection?* 2019. URL: https://docs.microsoft.com/nb-no/azure/information-protection/what-is-information-protection (sjekket 28.04.2019).

[2] Microsoft. *Overview of sensitivity labels*. 2019. URL: https://docs.microsoft.com/nb-no/Office365/SecurityCompliance/sensitivity-labels (sjekket 28.04.2019).

[3] Microsoft. *Deploying the Azure Information Protection scanner to automatically classify and protect files*. 2019. URL: https://docs.microsoft.com/nb-no/azure/information-protection/deploy-aip-scanner (sjekket 28.04.2019).

Modern Workspace - Driftsdokument
Samarbeidsverktøy og lagringsområder

v.0.3

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
17.04.2019	0.1	Dokument opprettet, introduksjon skrevet, teams påbegynt, referanser og figurer lagt til
18.04.2019	0.2	Teams ferdigstilt, SharePoint opprettet og ferdigstilt, tilleggsinformasjon skrevet, figurer og referanser lagt til, innholdsfortegnelse oppdatert
07.05.2019	0.3	Mindre revisjon av tekst, retting av grammatiske og språklige feil

Innhold

1 Introduksjon

I dette dokumentet vil vi fokusere på samarbeidsverktøyene Teams og SharePoint. Vi vil se på oppsett av Teamsites og hvordan en kan organisere ansatte innad i disse for å oppnå et best mulig resultat, i form av godt samarbeid og enkel kommunikasjon.

Teams er et kommunikasjonsverktøy som legger opp til samarbeid i arbeidshverdagen. Teams lar ansatte kommunisere via chat, videosamtaler, møter og konferanser, enten det foregår mellom to eller grupper av ansatte. Brukere settes i relevante grupper, kalt Teams, slik at man enkelt kan få kontakt med de riktige personene og raskt få svar. Teams integrerer også med Office-programmer, SharePoint og OneDrive, slik at ansatte har tilgang på, kan dele og kan samarbeide med andre på egne filer.

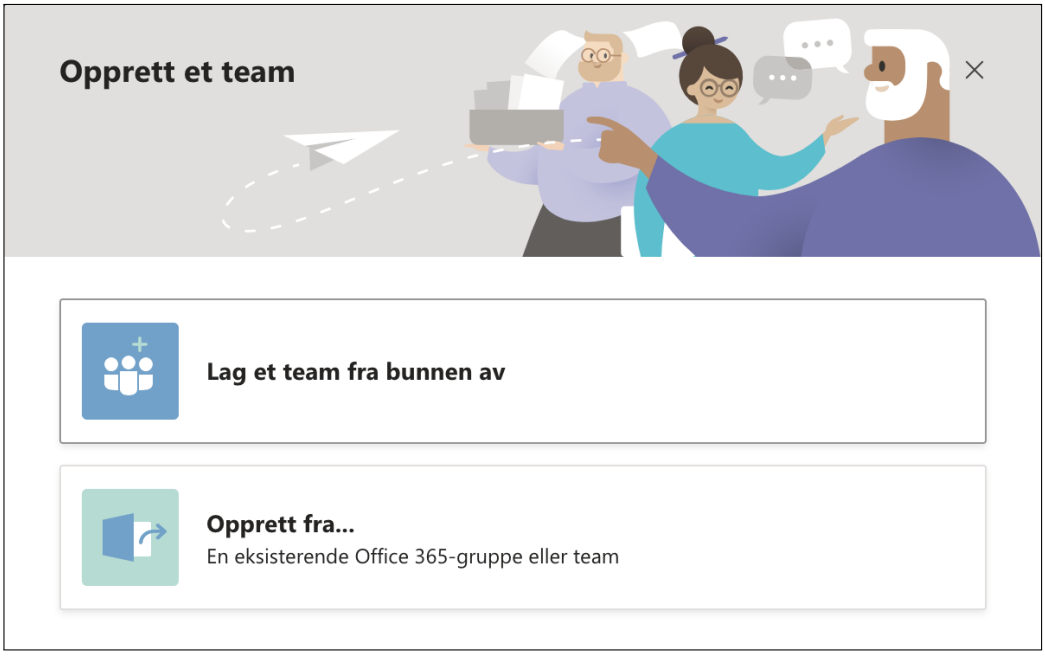
SharePoint er et knutepunkt for lagring og deling av filer mellom ansatte i firmaet. Her kan Teamsites opprettes slik at ansatte får tilgang på filene de trenger, og ikke får tilgang på filer som ikke angår dem. HR-avdelingen vil for eksempel ikke ha behov for å se og redigere driftsavdelingens filer, noe som også gjelder i den omvendte situasjonen. SharePoint integrerer også med Office-programmer, slik at en enkelt kan redigere dokumenter i nettleseren, eller åpne det i det relevante programmet nedlastet på datamaskinen.

2 Teams

2.1 Oppsett av et team

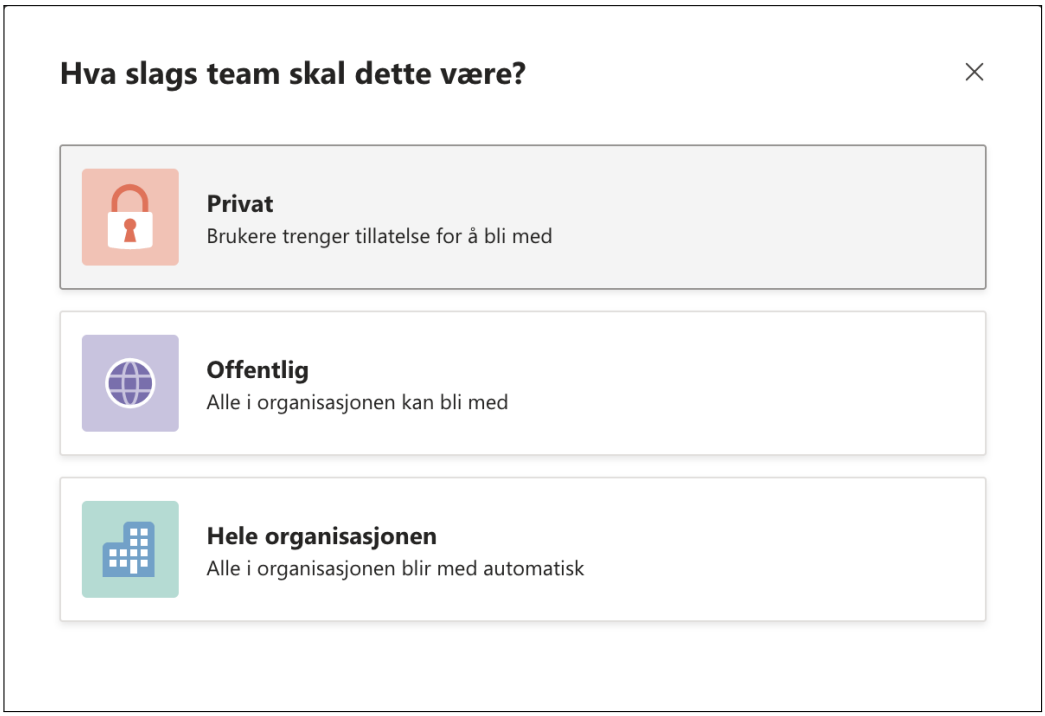
Oppsett av Teams kan gjøres både i selve applikasjonen dersom den er nedlastet på datamaskinen, eller i nettleseren. Vi gjennomgår prosessen via nettleser, men oppsett i applikasjonen vil være tilnærmet identisk.

Første steg vil være å åpne applikasjonen, eller nettsiden til Teams, og logge inn med en global administrator. Du vil så bli bedt om å opprette et team dersom det ikke eksister noen fra før. Som vist i figur 1, får du også muligheten til å opprette et team fra allerede eksisterende grupper. Dette er fordelaktig dersom det er satt opp grupper på forhånd, og det skal opprettes team for disse. Vi oppretter et team fra bunnen av for å vise prosessen.



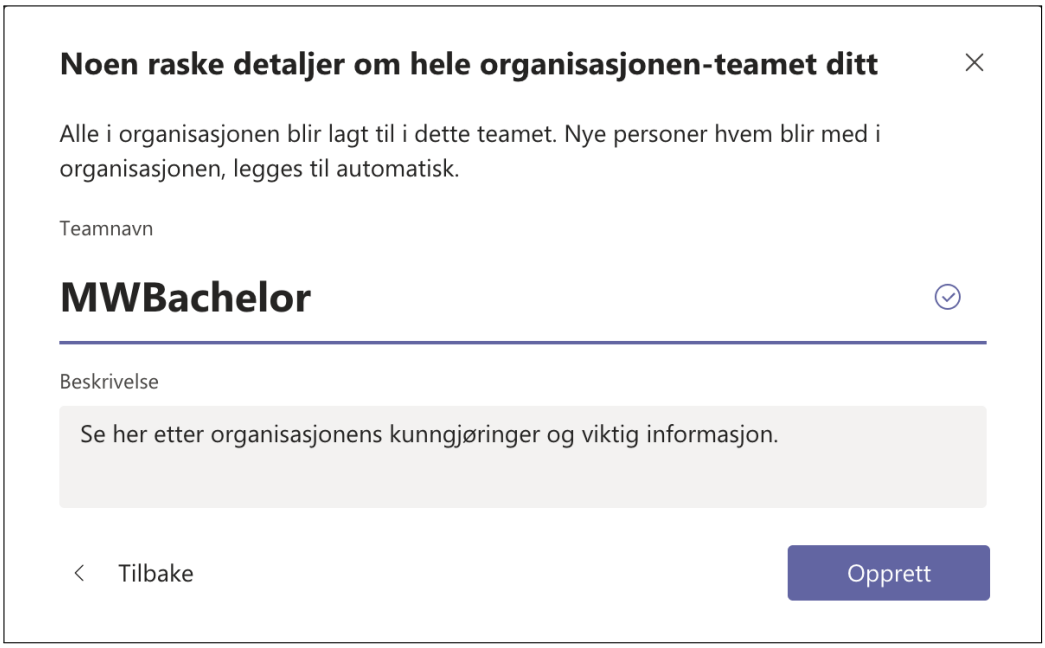
Figur 1

Deretter må en velge hva slags team-type som skal opprettes. Som vist i 2, finnes det tre ulike team-typer, privat, offentlig og hele organisasjonen. Bruksområdene er ulike, og avhengig av hva slags team som skal settes opp, vil det være viktig å velge riktig type, så brukere kun får tilgangene de skal ha og ikke flere. Et privat team vil kreve tillatelse for å kunne bli med, offentlig gir alle muligheten til å bli med i teamet, mens hele organisasjonen vil ta med alle brukerne automatisk. For vårt eksempel vil teamet settes opp for hele organisasjonen.



Figur 2

Til slutt vil en måtte gi teamet et passende navn og en beskrivelse. Når dette er oppgitt er det bare å velge "opprett" og teamet vil være klart.

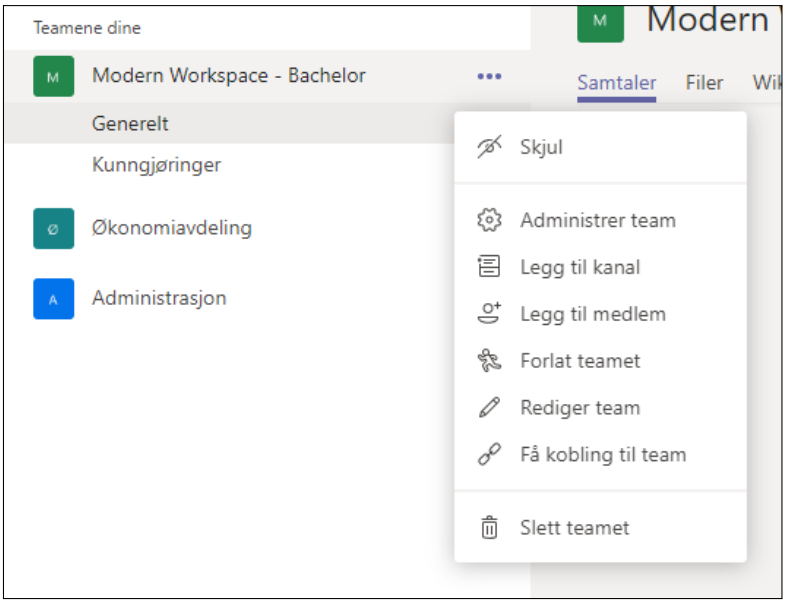


Figur 3

2.2 Legge til kanaler

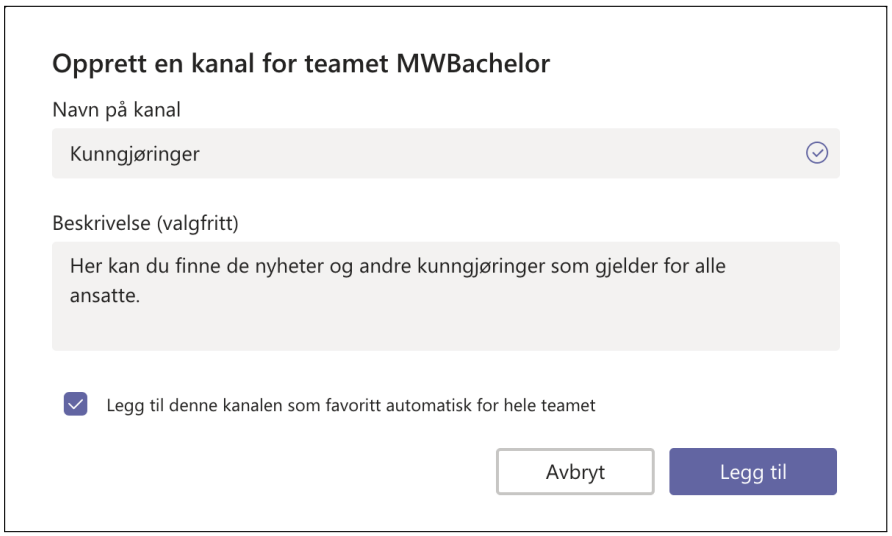
Når en har opprettet et team er det fortsatt en del som må gjøres før verktøyet er optimalisert for bruk. Kanaler er viktig for å kunne samle kommunikasjon rundt ulike tema og hindre uoversiktlige samtaler som går over hverandre. Det er innenfor de ulike kanalene chat, møter, deling av filer og lignende vil foregå. Alle medlemmer av teamet vil ha tilgang på de underliggende kanalene, noe som må tas til betraktning når en konverserer eller deler filer.

Første steg for å legge til en kanal, er å trykke på de tre prikkene bak det aktuelle teamet. Det vil, som vist i figur 4, komme opp en nedtrekksmeny med ulike valg. Velg her "Legg til kanal"



Figur 4

Det vil komme opp et vindu som ber om ulik informasjon angående kanalen. Det kreves et navn, men en beskrivelse av kanalen er valgfri. Når informasjonen er oppgitt kan en trykke "Legg til" og kanalen vil opprettes.

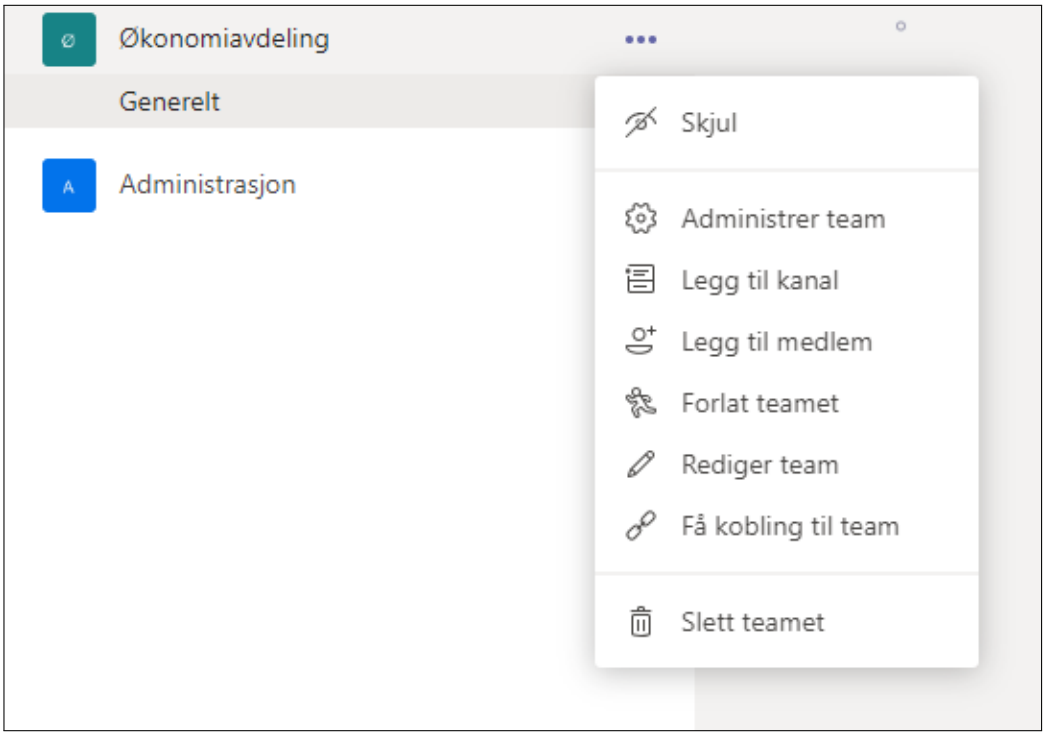


Figur 5

2.3 Legge til brukere

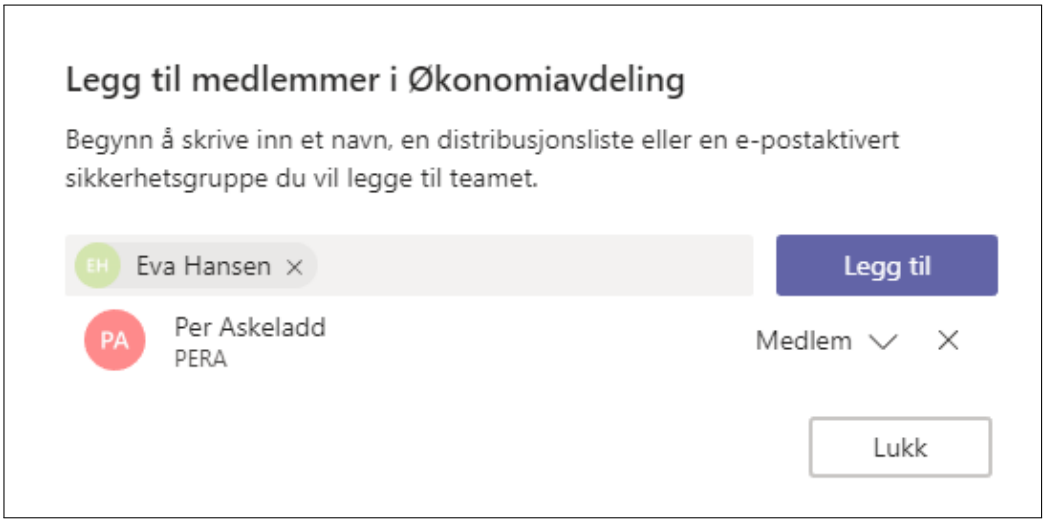
I situasjoner hvor det ikke er ønsket at alle brukere skal få tilgang på kanalene og filene som deles via teams, vil det opprettes private team. Dersom det ikke er satt opp brukergrupper, eller i tilfeller hvor en skal legge til nyansatte kan dette gjøres inne i Teams. Det vil anbefales å ta i bruk grupper slik at en slipper å legge til en og en bruker om gangen, noe som er svært tidskrevende og upraktisk i situasjoner med mange brukere.

Første steg for å legge til en bruker i et team, er å trykke på de tre prikkene bak det aktuelle teamet. Det vil, som vist i figur 6, komme opp en nedtrekksmeny med ulike valg. Velg her "Legg til medlem".



Figur 6

Her inne vil en få muligheten til å legge til enkeltbrukere, eller grupper av brukere. Som nevnt tidligere er det optimalt om det brukes grupper for å slippe unødig arbeid. He kan en søke opp brukerne og gruppene som skal legges til. Når riktig bruker(gruppe) er funnet, kan en trykke "Legg til", og de vil dukke opp med mulighet til å fjerne de fra teamet igjen, som vist i figur 7. Når alle brukerne og gruppene som skal legges til er oppført, kan en trykke "Lukk".

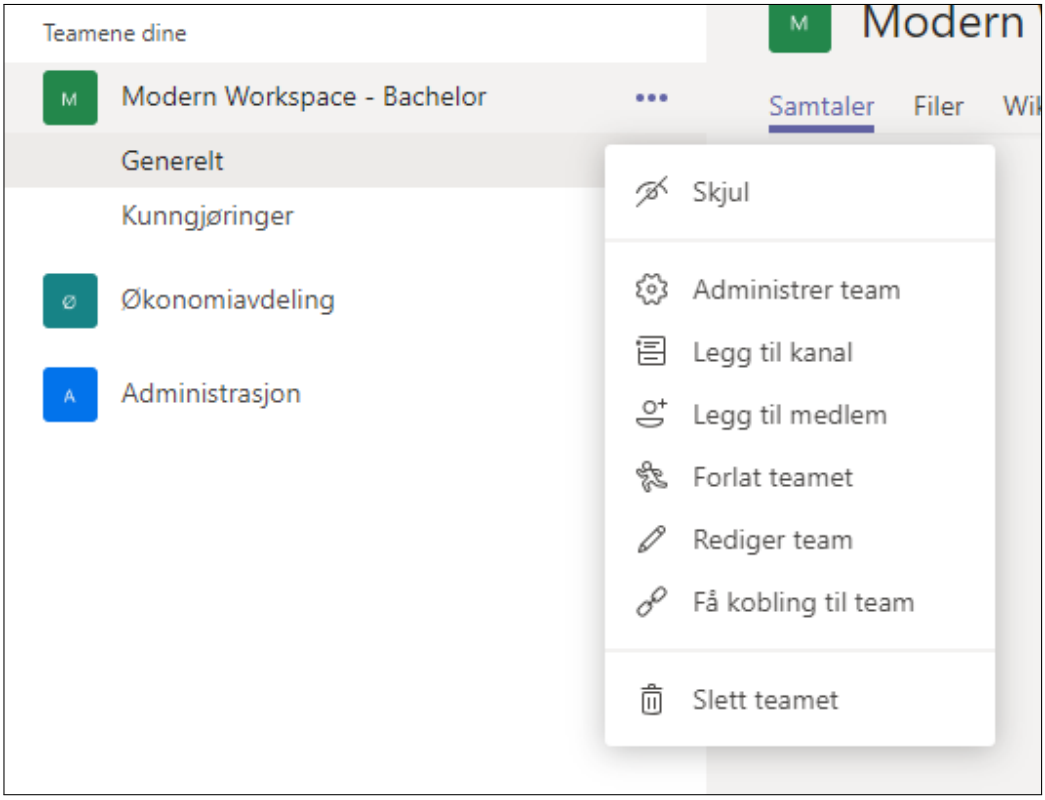


Figur 7

2.4 Administrering av et team

Teams har en rekke funksjoner som kan administreres av eierne av teamet[1]. En kan blant annet kontrollere hvem som kan skrive, om de kan varsle teamet eller kanalen i sin helhet og hva slags innhold som er lov å sende. Teams legger opp til en opplevelse som kan skreddersys avhengig av hva kanalen skal brukes til og av hvem. For eksempel kan et team opprettes for kunngjøringer og nyheter, hvor kun ledelsen kan sende meldinger, slik at viktige meldinger når alle de ansatte uten at de blir begravet under utallige spørsmål og meldinger fra andre ansatte.

Første steg for å administrere et team er å trykke på de tre prikkene bak det aktuelle teamet. Det vil, som vist i figur 8, komme opp en nedtrekksmeny med ulike valg. Velg her "Administrer team".

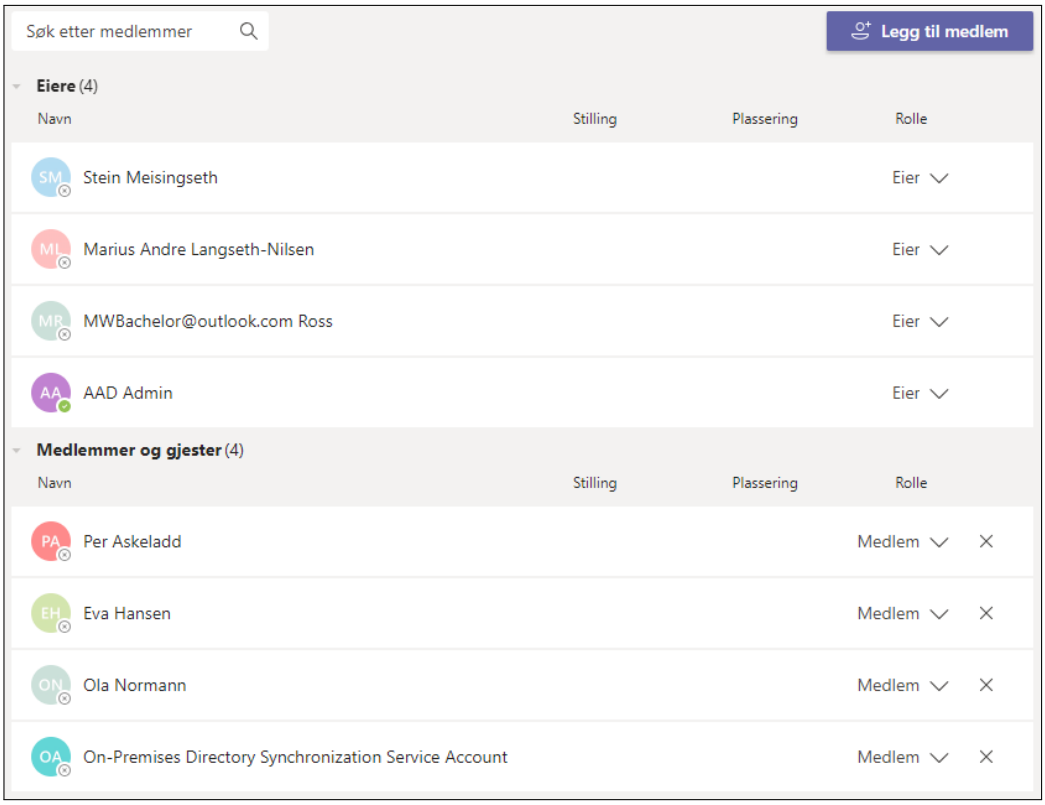


Figur 8

Her vil det være fire faner hvor man kan administrere ulike aspekter av det valgte teamet.

Figur 9

Under “Medlemmer” kan en legge til, fjerne og endre rollen på brukerne i teamet.

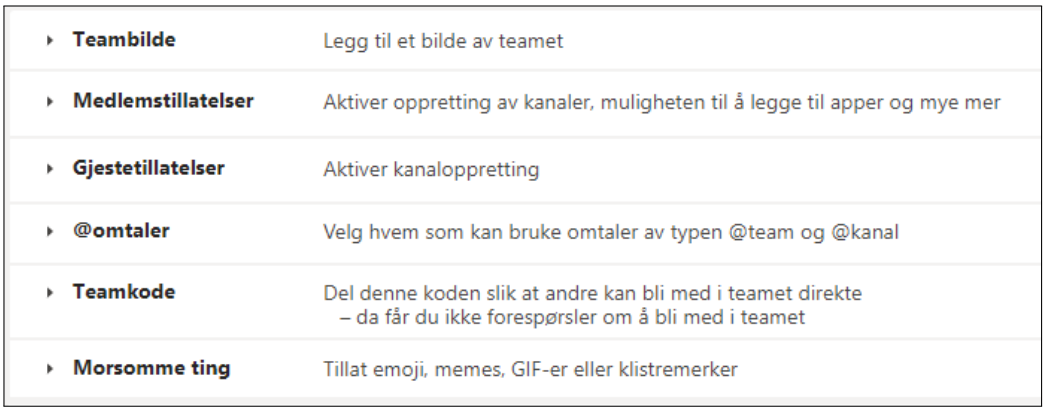


Figur 10

Under “Kanaler” kan en legge til, fjerne og redigere hvordan kanalen vises for brukerne i teamet.

Figur 11

Under “Innstillinger” kan en redigere en rekke innstillinger for teamet. Blant annet kan rettighetene til medlemmer og gjester, hvem som kan varsle og hva slags innhold er lov å dele, redigeres. Som vist i figur 12, er det en rekke nedtrekksmenyer med ulike innstillinger som kan redigeres ut ifra bedriftens behov.



Figur 12

Under “Apper” kan en endre hvilke applikasjoner som skal integreres med teamet. Her kan en fjerne og legge til applikasjoner i teamet. Applikasjoner lar deg utvide funksjonalitet, og åpner dermed for økt produktivitet gjennom tilleggsapplikasjoner som “Trello”.

Figur 13

3 SharePoint

3.1 Oppsett av SharePoint

Oppsett av SharePoint kan anses som overflødig dersom en har opprettet robuste team i Teams. Dette er fordi Teams vil automatisk opprette områder inne på SharePoint som tilsvarer de i Teams. Det er uansett mulig å opprette områder direkte i SharePoint dersom det skulle være behov for dette.

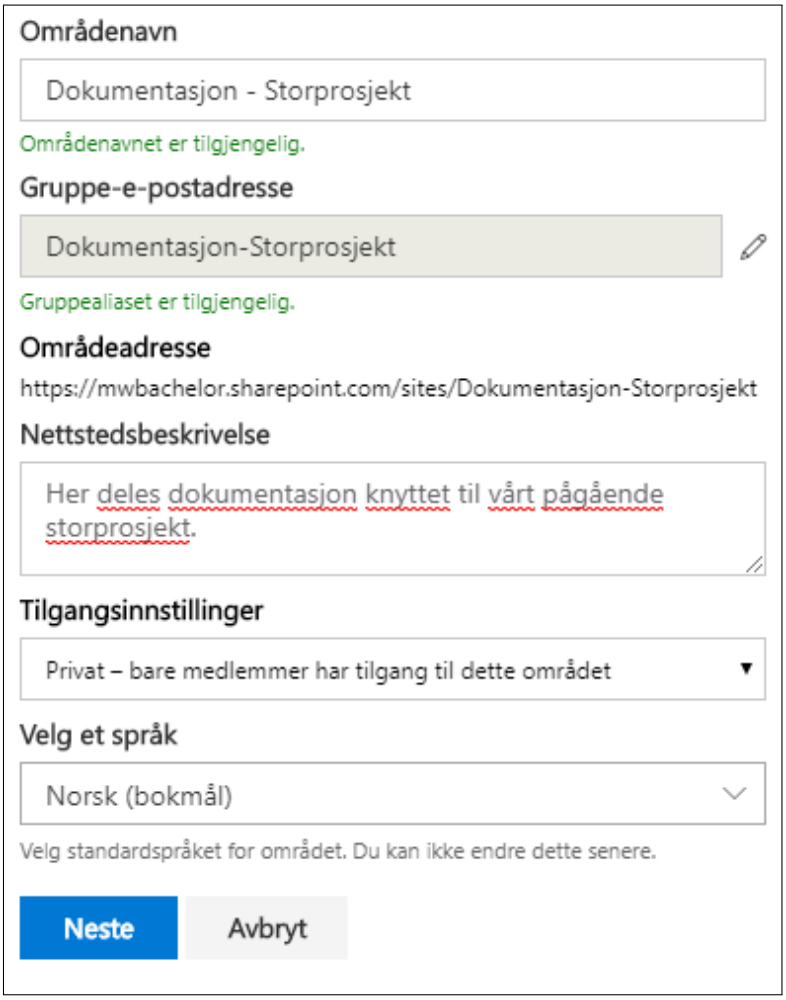
Første steg vil være å trykke på "Opprett område" inne på SharePoint-siden til bedriften.

Figur 14

Det vil så komme opp en veiviser som hjelper til med oppsettet. Her velger man først hva slags område som skal opprettes, enten et "Gruppenettsted" for deling av dokumenter og lignende, eller et "Kommunikasjonsområde" for å holde ansatte oppdatert omkring arrangementer og lignende. Vi velger her et "Gruppenettsted".

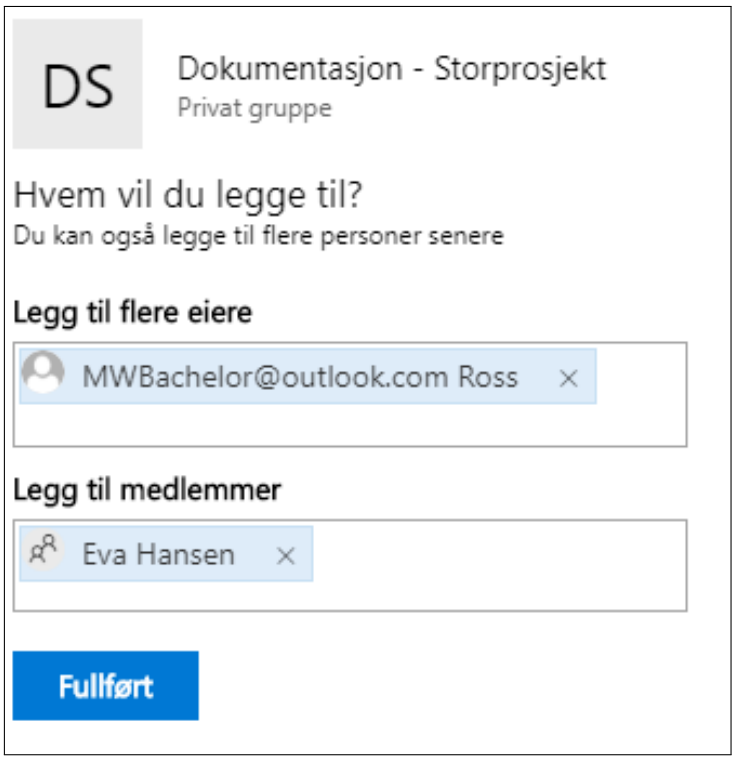
Figur 15

Deretter må en legge til et navn, og man kan også legge til en beskrivelse. SharePoint lar deg kun opprette områder med unike navn, så du vil orienteres om navnet er tilgjengelig og få feilmelding dersom det ikke er det. Her kan en også velge hvem som har tilgang under "Tilgangsinnstillinger" og hvilket språk område vil bruke som standard. Vi velger "Privat" for tilganger og "Norsk (bokmål)" som språk.



Figur 16

Siste steg er å legge til eiere og medlemmer som skal ha tilgang på området. Dette kan gjøres på et senere tidspunkt, og er ikke påkrevd. Trykk så Fullførtfor å fullføre oppsettet.

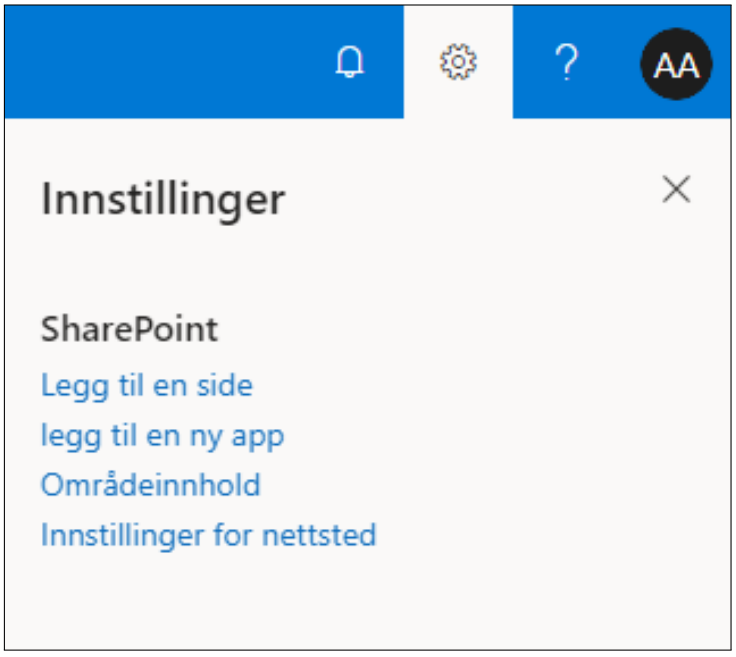


Figur 17

3.2 Administrasjon av SharePoint

Administrering av tilganger, utseende, innhold, deling og mye mer er mulig for SharePoint. På bakgrunn av mengden muligheter for administrasjon av SharePoint, vil vi ikke gå nøye inn på dette, men kun vise til hvor en kan gjøre endringer og kort hvilke muligheter som eksisterer.

Første steg vil være å klikke på tannhjulet øverst i høyre hjørne på SharePoint-nettsiden, som vist i figur 18. Her kan en se både "Områdeinnhold", som lar deg redigere hvordan området skal fremtre, og "Innstillinger for nettsted", som lar deg endre utallige innstillinger for SharePoint-siden. Vi velger "Innstillinger for nettsted".



Figur 18

Her inne finner vi en lang rekke innstillinger som kan redigeres for SharePoint-siden. Det vil være for tidkrevende å gå inn på de individuelle innstillingene, men vi vil endre noen av innstillingene under "Regionale innstillinger" i vårt eksempel.

Figur 19

Under regionale innstillinger kan vi, blant annet, endre tidssone, nasjonale innstillinger og kalendertype. Vi setter “Tidssone” til UTC+1, “Nasjonal innstilling” til Norsk (bokmål) og “Kalender” til Gregoriansk. Dette vil være optimalt for de fleste norske bedrifter. Trykk så “OK” for å lagre innstillingene.

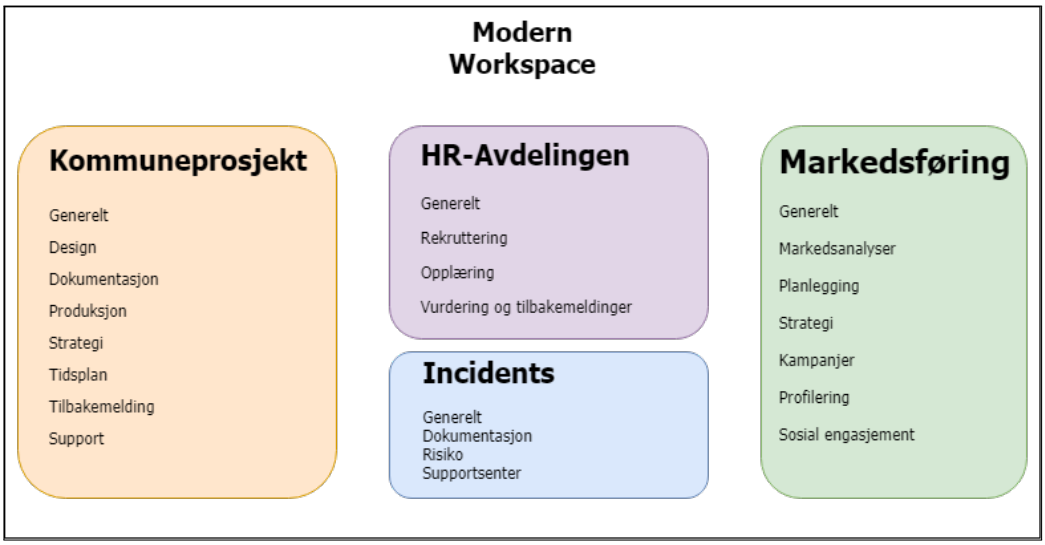
Figur 20

4 Tilleggsinformasjon

På bakgrunn av prosjektets størrelse og tidsplanens restriksjoner, kan vi ikke opprette en Teamsite som gjenspeiler et realistisk scenario. Vi vil derfor illustrere to mulige oppsett for bedriften, hvor en er basert på best-practice og den andre en normal bedriftsstrukturering. Begge vil komme med fordeler og ulemper, og det vil derfor være fornuftig å presentere de begge.

4.1 Best-Practice

Ifølge Microsoft er det "best-practice" å danne team som lar medlemmer krysse over fra deres faste avdelinger, slik at de involveres der det er behov[2]. Dette skal øke samarbeid og tillate ansatte å bruke sin kompetanse på best mulig vis. Illustrasjonen viser teamene som bobler, med kanalene under navnet på teamet.

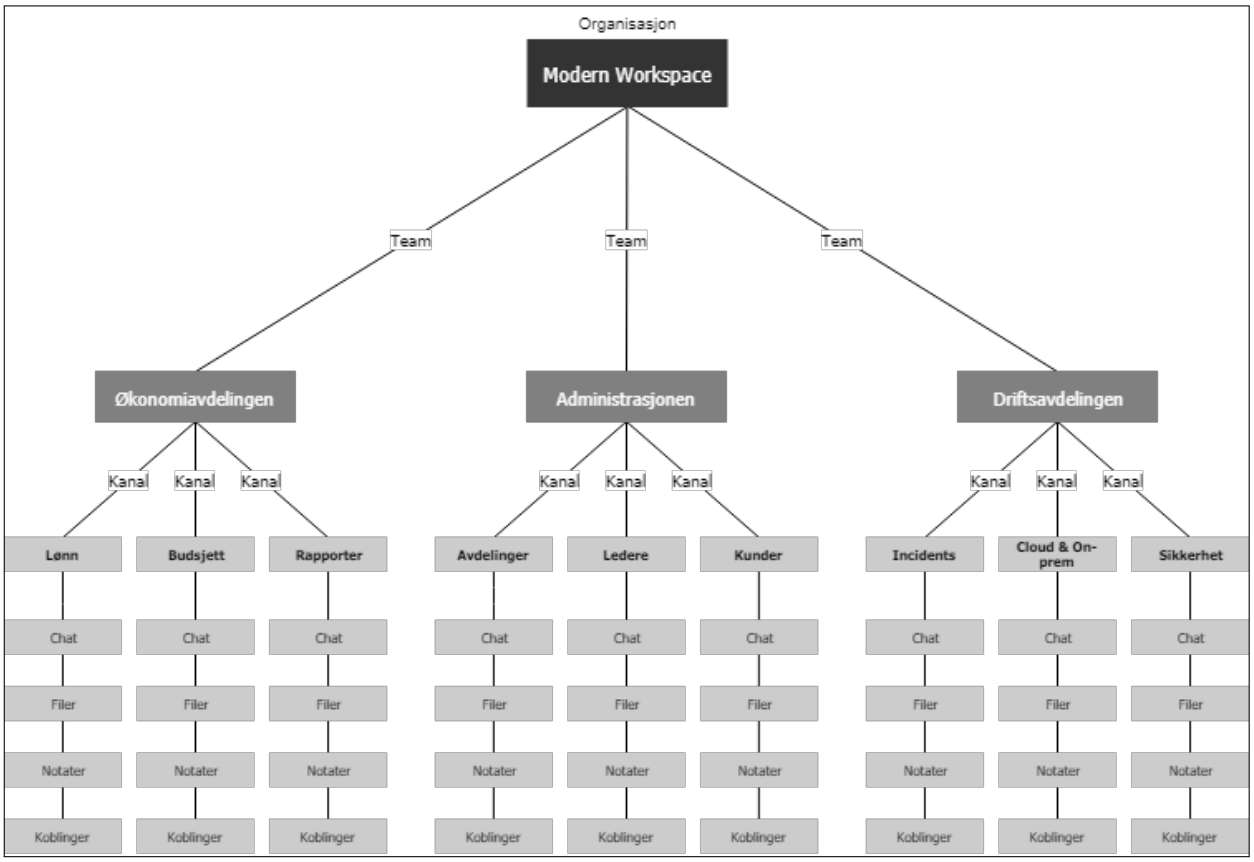


Figur 21

4.2 Organisatorisk orientering

Ifølge Microsoft kan en organisatorisk orientering være en god måte å øke både produktivitet og samarbeid, selv om det ikke alltid er den beste metoden. Her deles bedriftens avdelinger inn i team med underliggende kanaler, slik at driftsavdelingen kun vil finne andre driftere i sitt team, mens administrasjon kun vil se ledere

i sitt team. Ansatte kan kommunisere med medlemmer av andre avdelinger, men ikke innad i teamet deres. Dette gjør oppsettet i Teams oversiktlig og enkelt.



Figur 22

Referanser

[1] Microsoft. *Chat, teams, channels, apps in Microsoft Teams*. 2019. URL: https://docs.microsoft.com/en-us/microsoftteams/deploy-chat-teams-channels-microsoft-teams-landing-page (sjekket 07.05.2019).

[2] Microsoft. *Best practices for organizing teams in Microsoft Teams*. 2017. URL: https://docs.microsoft.com/en-us/microsoftteams/best-practices-organizing (sjekket 30.04.2019).

Modern Workspace - Driftsdokument
Migrering

v.0.5

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
26.04.2019	0.1	Dokument opprettet, lagt til figurer og skrevet tekst for Importere objekter fra SCCM til Intune, startet på epost, SharePoint og OneDrive påbegynt
29.04.2019	0.2	Revidert tekst, Sharepoint tool skrevet, migrering av Exchange til Exchange Online ferdigstilt, OneDrive skrevet
03.05.2019	0.3	Lagt til figur på migrering av Exchange til Exchange Online, skrevet introduksjon
03.05.2019	0.4	Revidert tekst i SharePoint, OneDrive, Importere objekter fra SCCM til Intune og Introduksjon
06.05.2019	0.5	Mindre revisjon av tekst, retting av grammatiske og språklige feil

Innhold

1 Introduksjon

Når en bedrift skal flytte sine systemer ut i skyen, vil det være naturlig at de ønsker å ta med elementer fra det gamle systemet. Ønskene til en bedrift som skal migrere til skyen vil variere fra bedrift til bedrift. Mange vil ønske at brukerne deres deres får tilgang på sin epost og filene lagret på filtjeneren. Å ha løsninger klare, slik at bedriften får riktig funksjonalitet, vil være viktig for å kunne levere et godt produkt.

I dette dokumentet vil vi ser på migrering av elementer fra de lokale tjenerne til skyen og muligheter brukerne har for å få flytte til det nye systemet. Vi starter med å beskrive import av objekter fra SCCM til Intune. Her går vi gjennom prosessen og hvilke krav som må fylles for å oppnå en vellykket importering. Videre dokumenteres migrering av Exchange til Exchange Online kort, slik at det er forståelse for hvordan flytting av post-bokser foregår. Til slutt ser vi på migreringsmuligheter og metoder for å flytte filer til SharePoint og OneDrive, dette slik at bedriften, og brukerne deres, får med viktige filer til skyen.

Dokumentet vil gå ut ifra at leser har en viss teknisk kunnskap, og vil ikke nødvendigvis være enkelt å forstå for ufaglærte.

2 Importere objekter fra SCCM til Intune

For å flytte applikasjoner fra SCCM til Intune, anbefales det å bruke Microsofts selvutviklede verktøy, "Intune Data Importer Tool". Dette verktøyet lar deg velge objekter som skal flyttes til Intune, og vil kjøre en vurdering for hver av disse. Kompatible objekter vil så flyttes ut i Intune, slik at bedriften kan få med det de ønsker når de begynner sin migrering til skyen.

Krav for å kjøre Intune Data Importer Tool[1]:

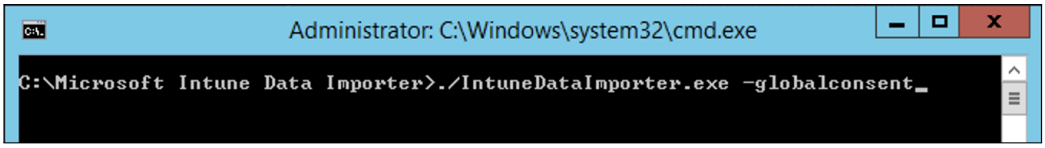
- Domeneinnmeldt maskin med Windows server 2016 eller nyere
- Administratorbruker på lokal maskin
- Global administrator i Intune

Første steg vil være å laste ned verktøyet fra Microsofts GitHub.

`https://github.com/ConfigMgrTools/Intune-Data-Importer/releases`

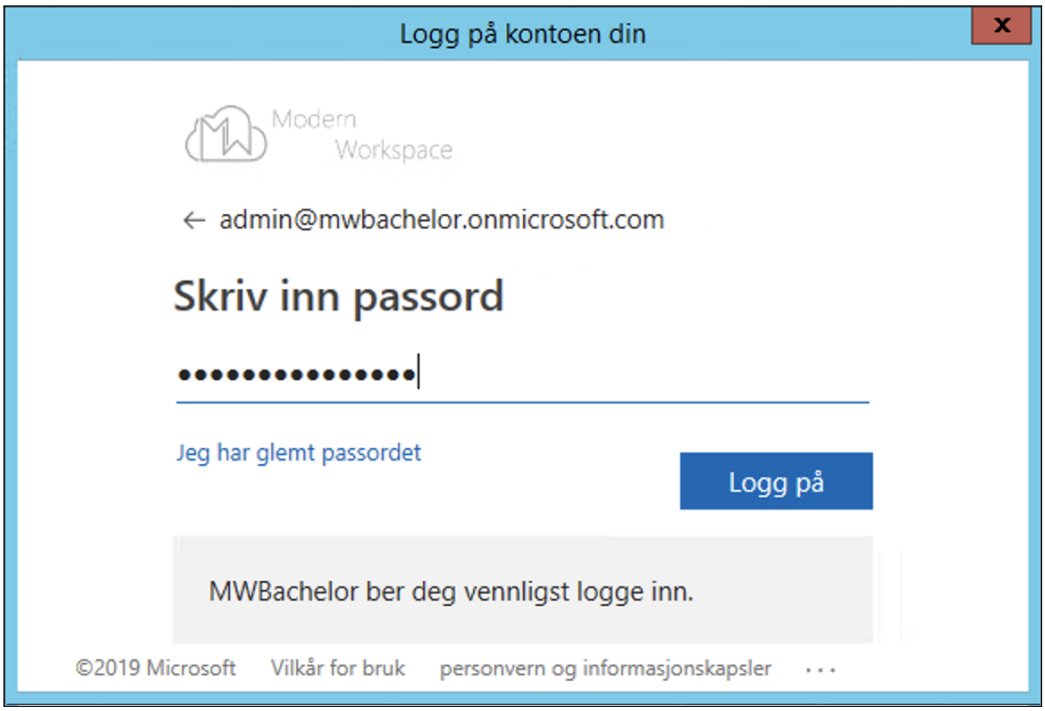
Legg mappen med verktøyet på SCCM-maskinen eller eventuelt en annen maskin innmeldt i det lokale domenet.

Før en kan kjøre verktøyet kreves at det gis tilganger på ressurser i Intune. Dette gjøres ved å åpne et cmd-vindu, som administrator, i mappen verktøyet er lokalisert. Powershell vil også fungere. Bruk så kommandoen "intunedataimporter.exe -GlobalConsent".



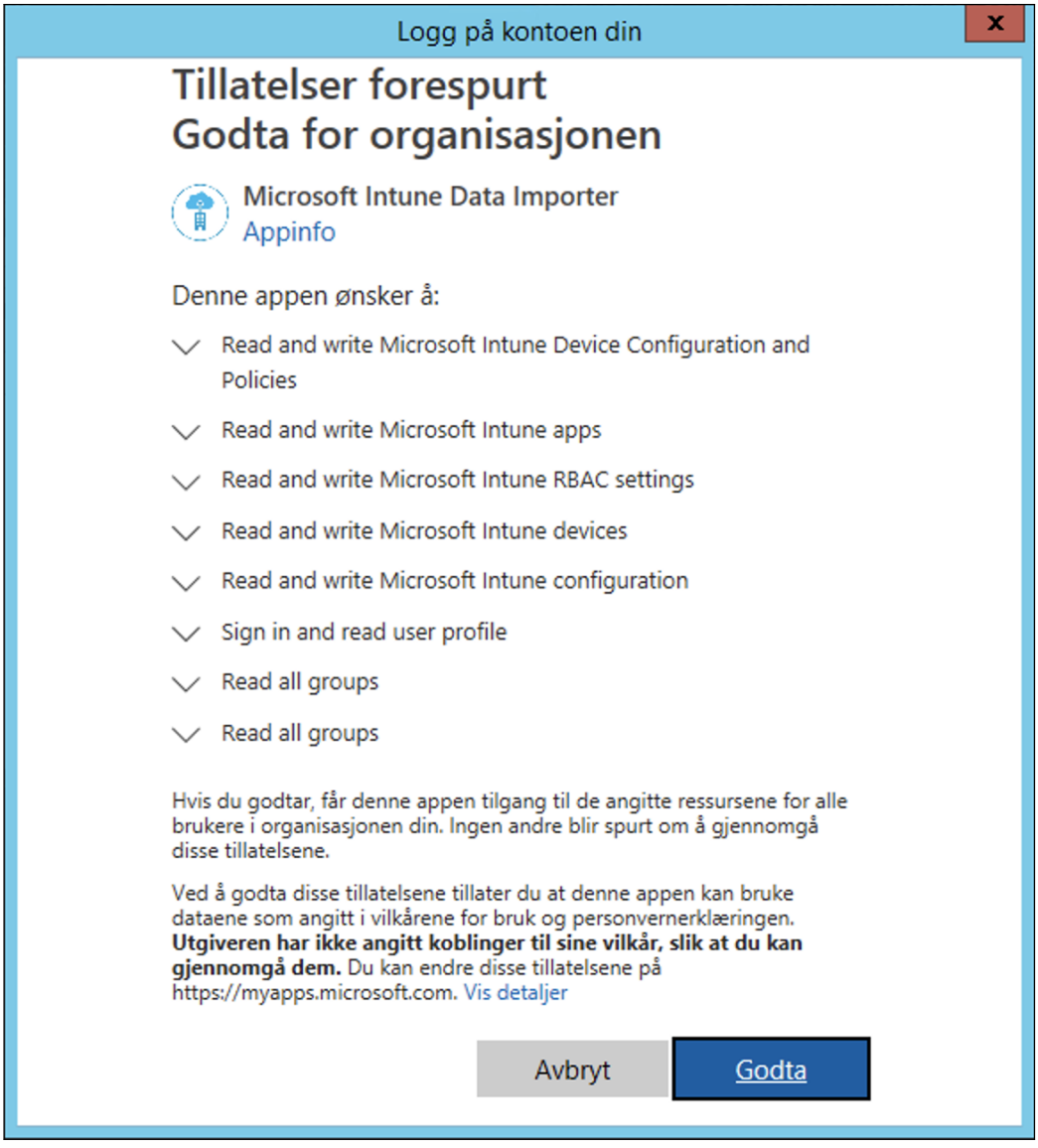
Figur 1

Det vil dukke opp et vindu hvor man må logge inn med en global administrator i Intune. Fyll inn kontoinformasjonen og trykk “Logg på” for å komme videre.



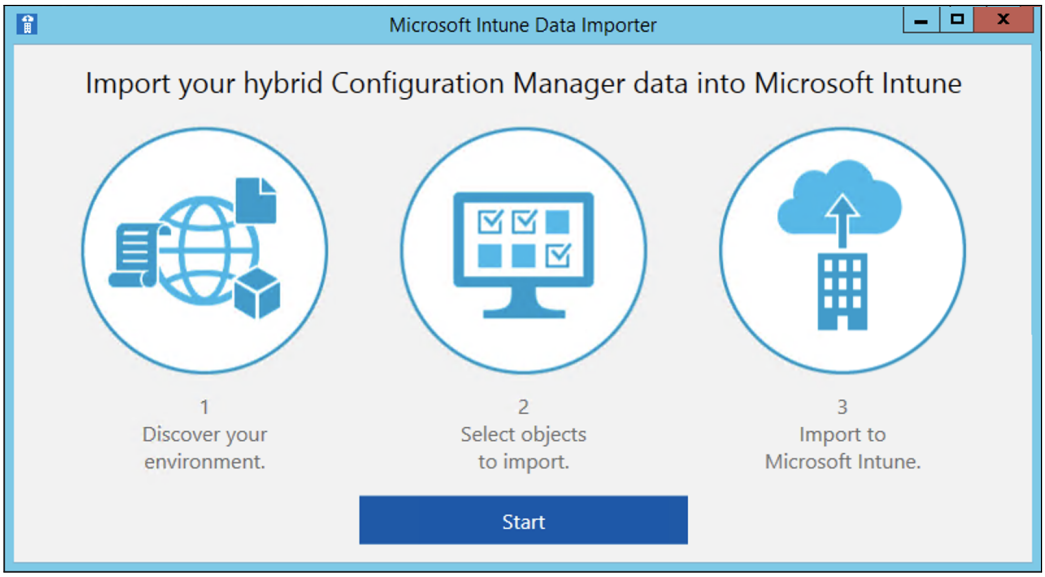
Figur 2

Når du har logget inn vil det dukke opp en oversikt over hvilke ressurser verktøyet vil kunne administrere i Intune. Les gjerne gjennom slik at du vet hva du godtar, og trykk "Godta" for å gi verktøyet rettighetene som kreves.



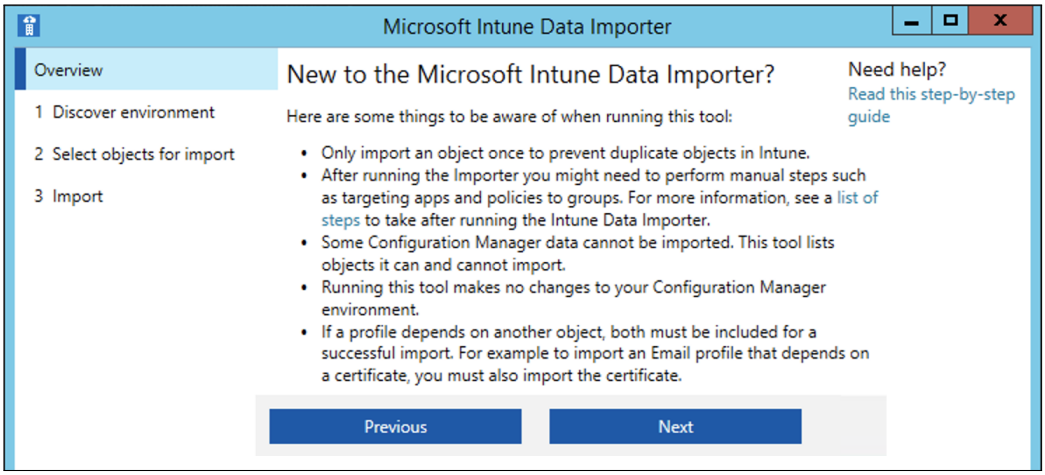
Figur 3

Kjør så selve verktøyet, “Intunedataimporter.exe” som administrator. Det vil dukke opp en veiviser som forklarer prosessen som tas for å importere objekter til Intune. Start verktøyet ved å trykke “Start”.



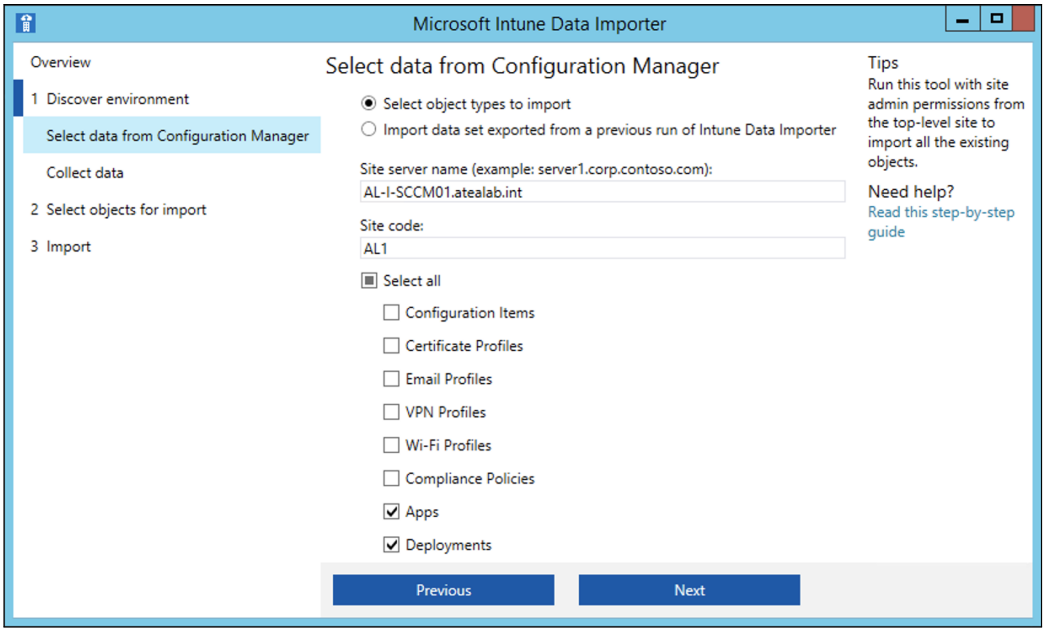
Figur 4

Veiviseren vil så gi noen punkter om hva man bør passe på når en kjører verktøyet, som å kun importere objekter en gang. Det vil være viktig å lese gjennom dette så du forstår hva som bør og ikke bør gjøres. Når du har gått gjennom dette, kan du trykke “Next” for å komme videre i veiviseren.



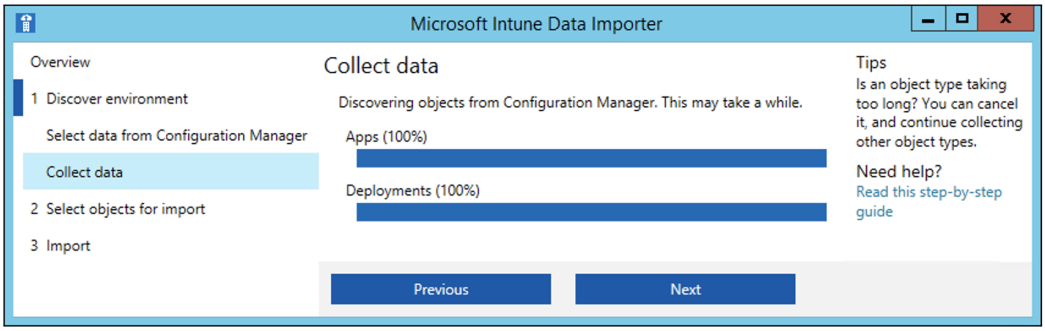
Figur 5

Du vil så måtte velge hvilke objekter som skal importeres, fylle inn server-navn og SCCM-sidens kode. Server-navn og sidekode vil være for SCCM-maskinen en skal migrere objekter fra. Huk så av for objektene som skal migreres. Som vist i figur 6, skal vi kun migrere applikasjoner og distribusjoner. Når alt er fylt inn riktig, og du har valg objekter som skal migreres, kan du trykke “Next”.



Figur 6

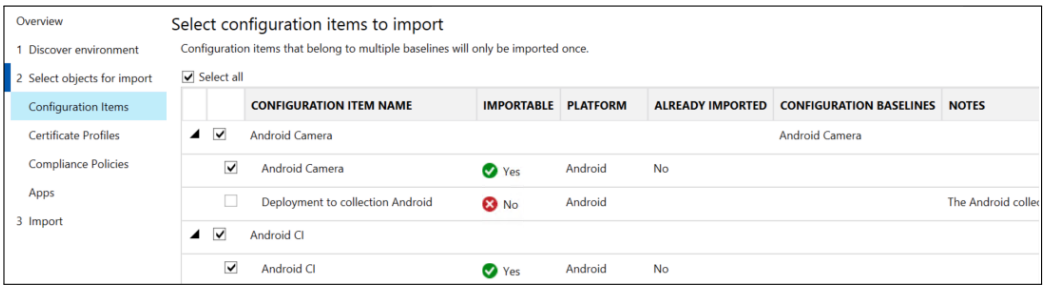
Verktøyet vil så finne objektene som skal migreres. Dette kan ta litt tid avhengig av mengden objekter en skal migrere. Når alle objektene er oppdaget, kan en trykke “Next” for å komme videre.



Figur 7

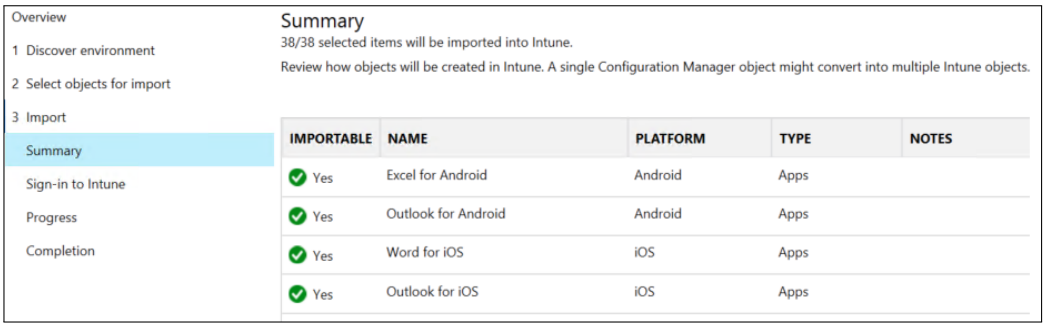
PS: Flere av bildene som følger vil være hentet fra nettet[2, 3] grunnet feil med enten lab-miljø, eller verktøyet, som gjorde at verktøyet ikke ville komme videre. Dette blir gjort da feilsøking ikke gav resultater og på grunn av prosjektets tidsbegrensninger.

Verktøyet vil så vise hvilke objekter som lar seg migrere, og man får her muligheten til å huke av for hvilke objekter som skal migreres. Som vist i figur 8, kan vi blant annet se objektenes navn, om de kan importeres, plattformen de er på og om de er importert tidligere. Objektene vil organiseres ut ifra objekt-type, og det vil derfor være en egen side i veiviseren for de ulike objekttypene. Fjern objektene som ikke er kompatible og de som bedriften enten ikke har behov for eller ikke ønsker å migrere til Intune. Trykk så "Next" for å komme videre.



Figur 8

Deretter får du en oppsummering av objektene som vil importeres til Intune. Her kan en se om de er kompatible, navnet deres, plattformen/OS, objekttype og eventuelle notater. Gå gjennom for å se at de riktige objektene vil bli med, og trykk "Next".

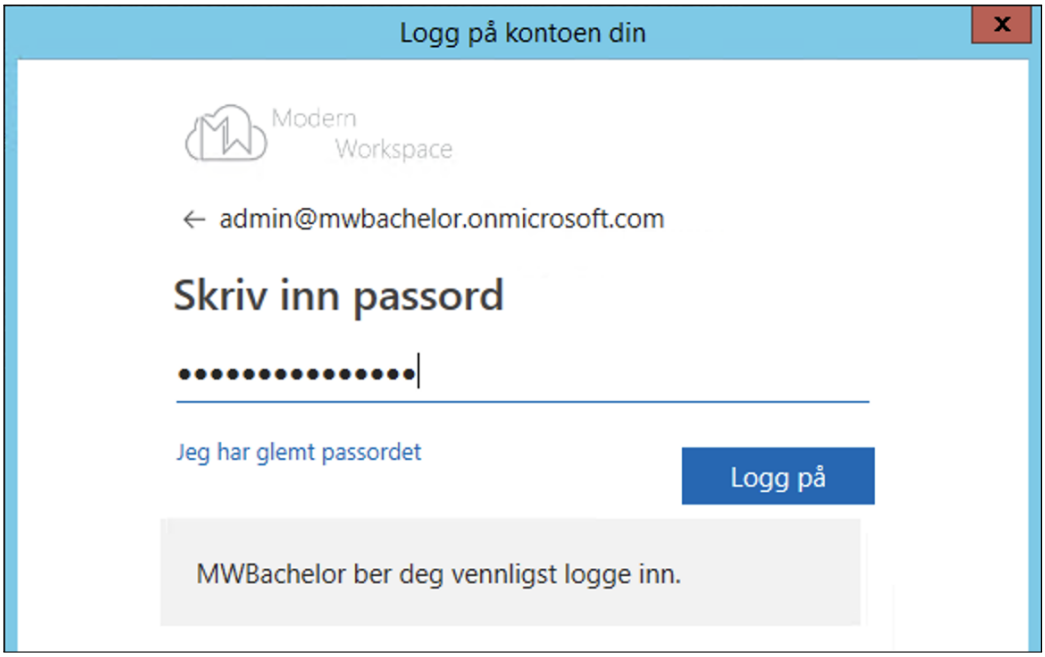


Figur 9

Du må så logge inn med din globale administratorbruker i Intune, slik at objekter kan begynne migreringen. Du kan også eksportere objektene dersom du ønsker å fullføre senere, eller gjøre prosessen på en annen maskin. Trykk her "Sign in to Intune" for å logge på.

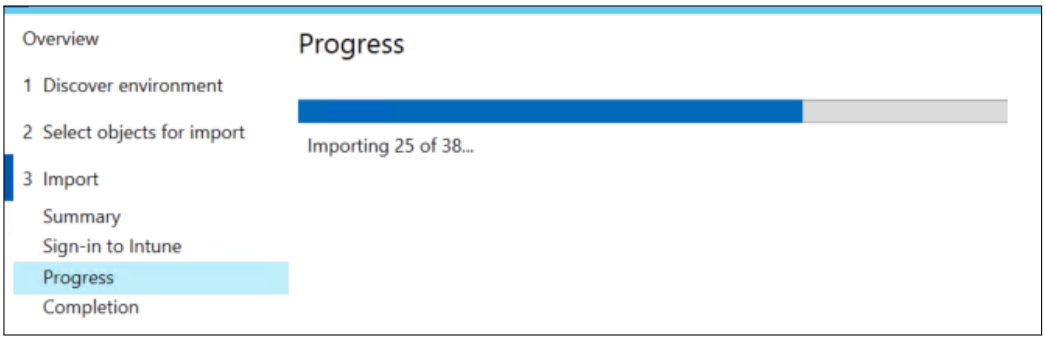
Figur 10

Det vanlige innloggingsvinduet vil dukke opp. Fyll inn kontoinformasjonen og trykk "Logg på".



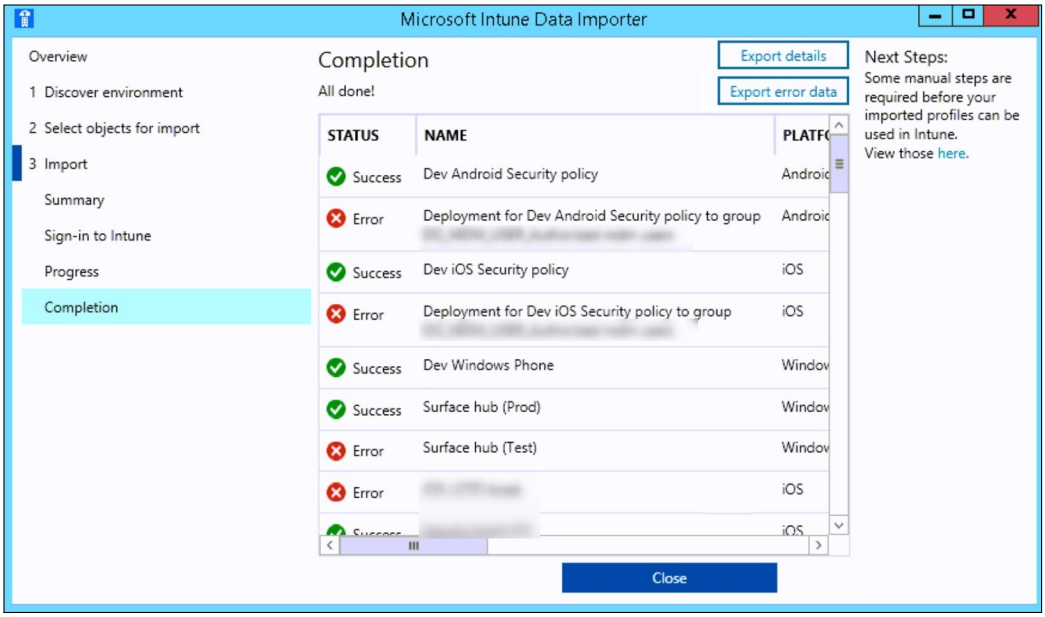
Figur 11

Migreringen vil nå begynne, noe som kan ta litt tid avhengig av mengden objekter som skal flyttes. Som vi ser i figur 12, vil verktøyet vise framgangen underveis. Når framdriftsindikatoren har nådd enden, og alle objektene er importert, kan du trykke “Next”.



Figur 12

Det siste vinduet i veiviseren vil informere om hvilke objekter som ble migrert og eventuelle feil som oppsto under migreringen. Gå gjennom og se etter feil. Eksporter eventuelt alle detaljer eller error data med knappene “Export details” og “Export error data”. Trykk så “Close” for å lukke verktøyet.

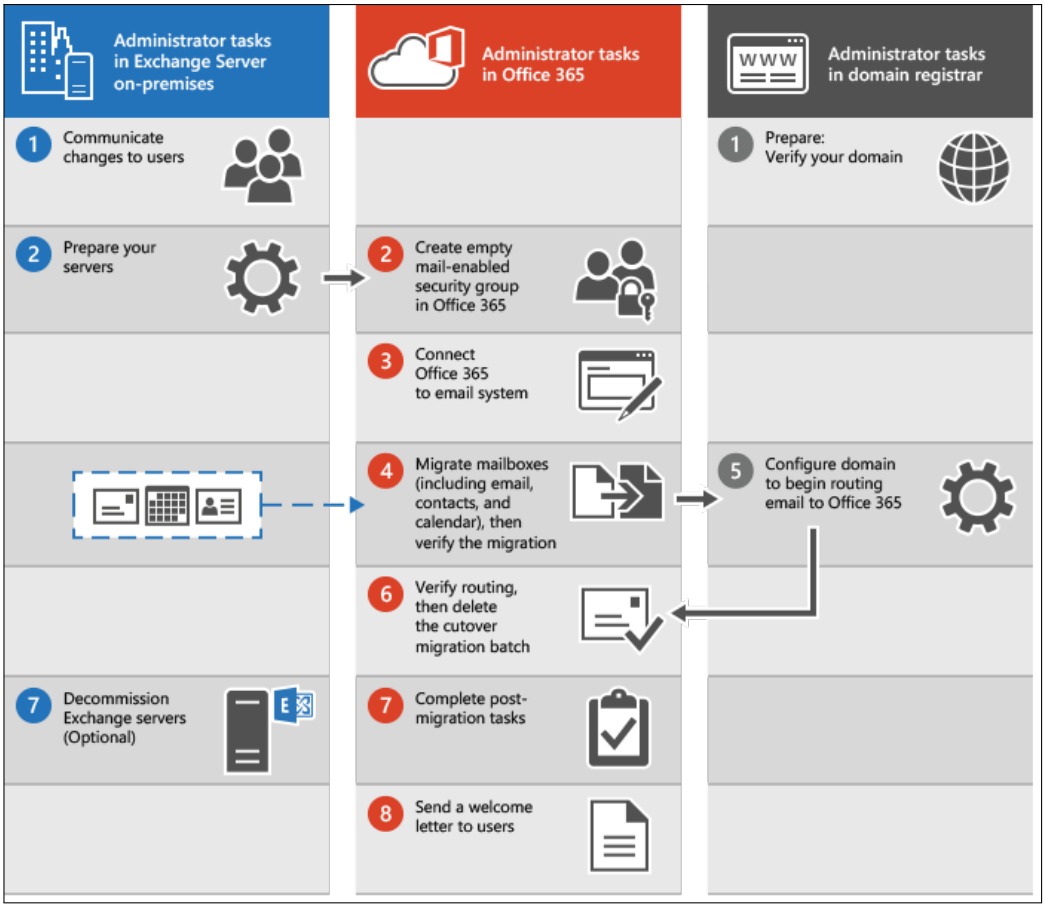


Figur 13

3 Migrering av Exchange til Exchange Online

Migrering av epost-kontoer til Exchange Online gjør at bedriftens ansatte ikke mister e-poster, kalendre, kontakter og andre elementer, samtidig som det tillater enkel og sikker administrasjon via skyen. Det finnes ulike migreringsmetoder som kan benyttes, men den mest relevante for dette prosjektet vil være "Cutover-metoden". Denne metoden lar deg flytte brukernes epost-kontoer til skyen raskt uten at de vil merke overgangen i noen særlig grad. Vi legger ved en figur, utarbeidet av Microsoft, som beskriver prosessen i sin helhet, figur 14.

På bakgrunn av manglende Exchange Server i lab-miljø vil det ikke være mulig å dokumentere en migrering av epost-kontoer til Exchange Online. Migreringsprosessen illustreres i figur 14, og vi vil ikke beskrive prosessen utover instruksjonene gitt i figuren.



Figur 14: Cutover-metoden

4 SharePoint

Det finnes mange metoder å migrere fellesdokumenter fra lokale filområder til SharePointområder. Dokumentasjonen vil omtale to metoder, robocopy og SharePoint Migration Tool. Robocopy benytter kommandoer for å replikere filene i skyen, mens SharePoint Migration Tool er en mer brukervennlig veiviser som hjelper brukeren å ta med seg sine filer til skyen.

4.1 Robocopy

For robocopy trengs:

- En pakke med PnP-cmdlets
- Påloggingsinformasjon for administrator
- Kilde
- Destinasjon

Følgende kommandoer benyttes:

Listing 1: Get HWID

```
1 Install-Module SharePointPnPPowerShellOnline
2 $365Cred = Get-Credential
3 Connect-PnPOnline -Url https://domain.sharepoint.
    com/sites/sitename -credential $365Cred
4 $Source = "filepath"
5 ROBOCOPY /mir /sec $Source " \\domain.sharepoint.
    com\sites\sitename " /MIR
```

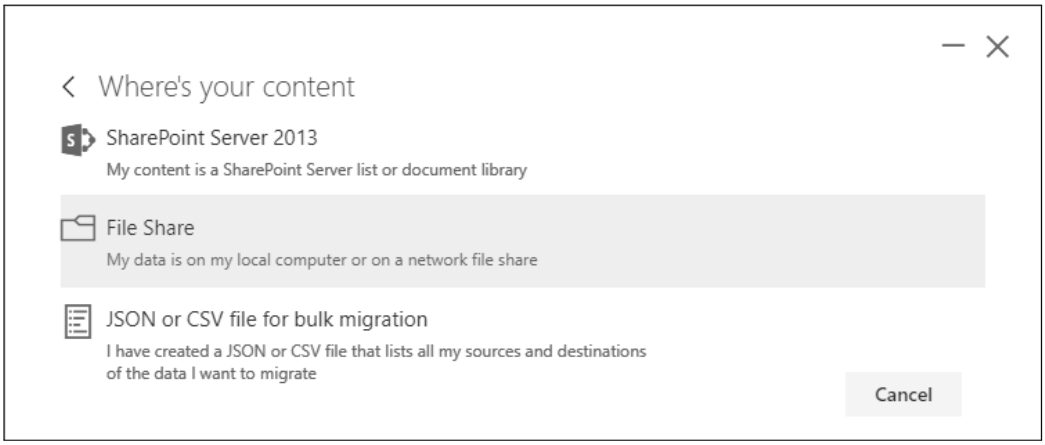
4.2 SharePoint Migration Tool

Microsoft selv har utviklet SPMT[4] for å utføre migrering til SharePoint. Verktøyet har mulighet for å migrere fra flere ulike kilder, som lokal filtjener eller en eldre SharePoint server. Det er anbefalt å gjøre migrering manuelt, men verktøyet kan hjelpe når store mengder filer skal flyttes, eller i situasjoner hvor ting må skje raskt.

Først må verktøyet lastes ned, installeres og åpnes. Så blir administrator bedt om å logge inn. Verktøyet kan lastes ned fra Microsofts nettsider:

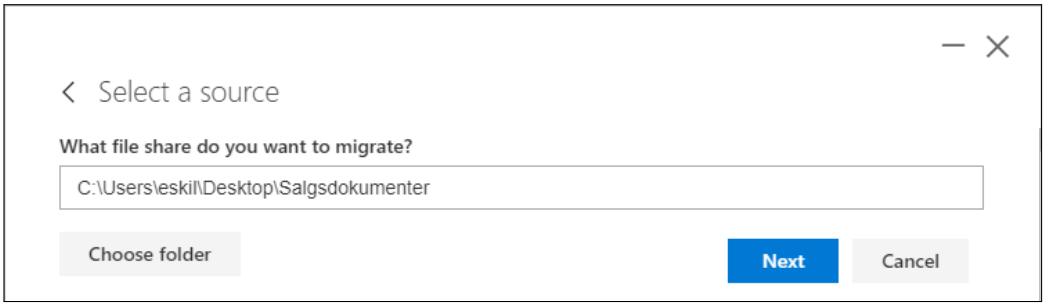
`https://spmtreleasescus.blob.core.windows.net/install/default.htm`

Når en kjører verktøyet vil en veiviser starte. Her får en velge hvor filene som skal migreres ligger. En kan velge mellom å masse-migrere gjennom JSON eller CSV-filer, filer fra lokalt område eller en SharePoint-server. Som vist i figur 15, velger vi å flytte filer fra et lokalt område.



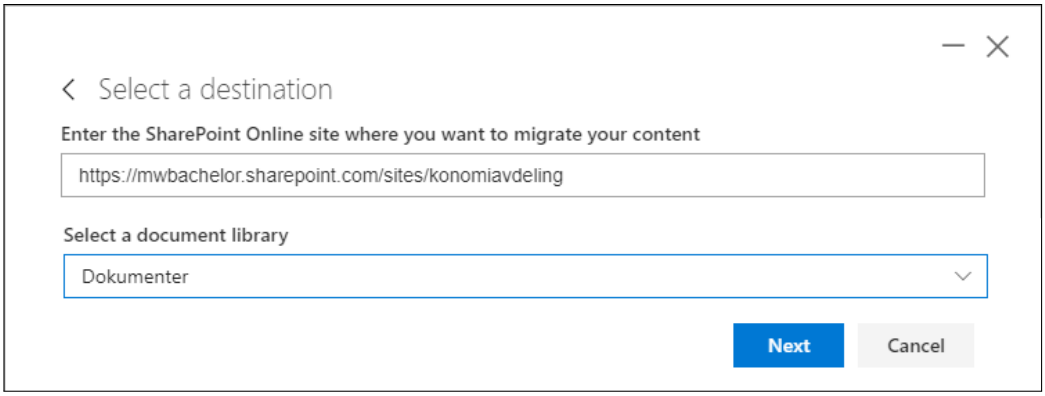
Figur 15

Når du velger lokalt filområde må en velge stien til det lokale filområdet. Filene i dette området vil bli migrert, så det er lurt å passe på at mappen inneholder de ønskede filene. Trykk her "Next" etter å ha funnet riktig filområde.



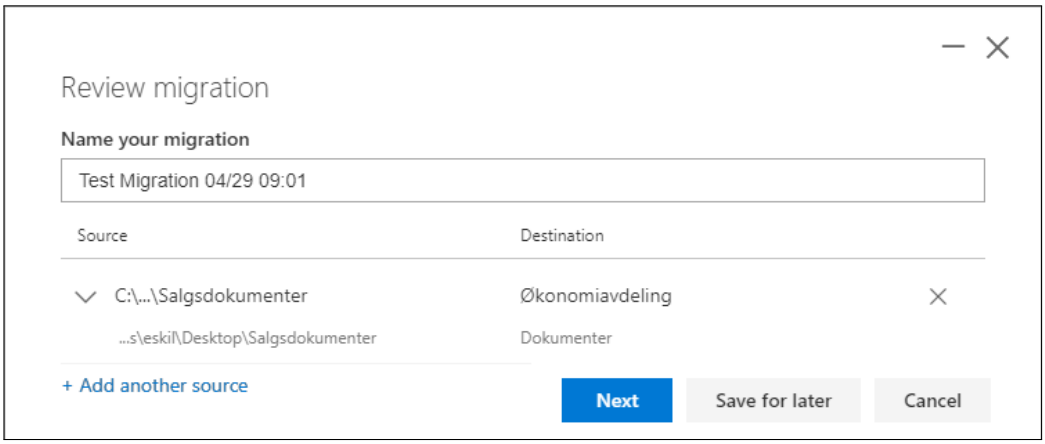
Figur 16

På neste steg skal filenes destinasjon i Sharepoint oppgis. Hvis administrator har tilgang til SharePoint-siden, vil det dukke opp en nedtrekksliste med områder, noe vi ser i figur 17. Her velges det å migrere til biblioteket "Dokumenter". Trykk så "Next" for å komme videre.



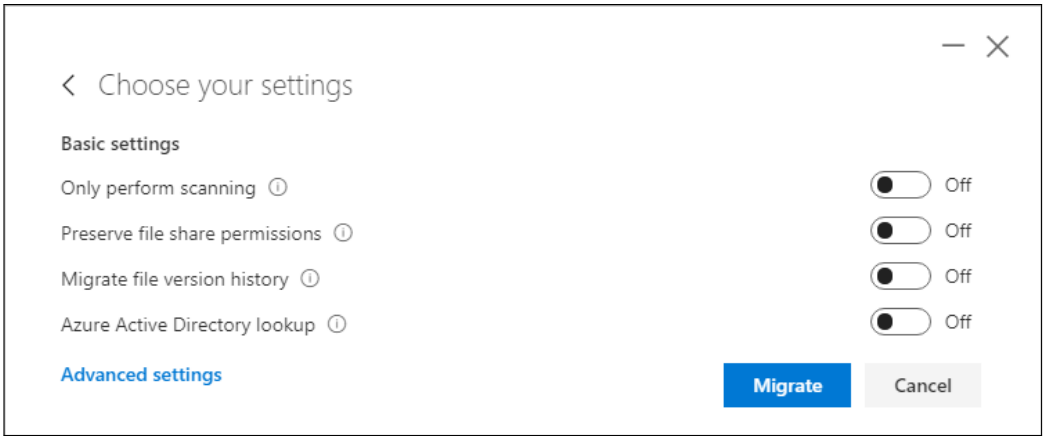
Figur 17

Til slutt vil veiviseren la deg gjennomgå valgene som ble tatt, slik at du får et overblikk over migreringen før du starter prosessen. Her er det lurt å sjekke både at filområde som skal migreres fra er riktig, samt at destinasjonen stemmer overens med ønsket plassering. Som vist i figur 18 kan en også lagre innstillingene hvis ønsker å kjøre migreringen på et senere tidspunkt. Klikk her "Next" for å komme videre.



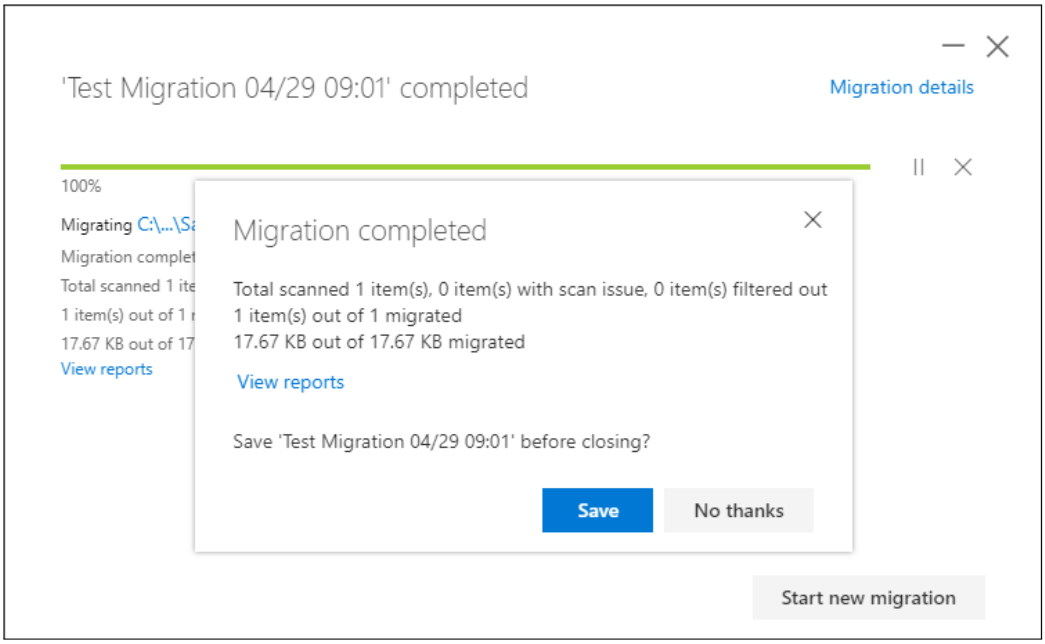
Figur 18

Siste steg før migreringen starter, er å velge innstillinger for selve migreringen. Som vist i figur 19, er de fleste innstillingene avskrudd, men under “Advanced settings” er det huket av for å kjøre migreringen opp til fem (5) ganger for å være sikker på at alle filene migreres riktig. Gå gjennom innstillingene og velg de som passer for situasjonen. Velg “Migrate” for å starte migreringen.



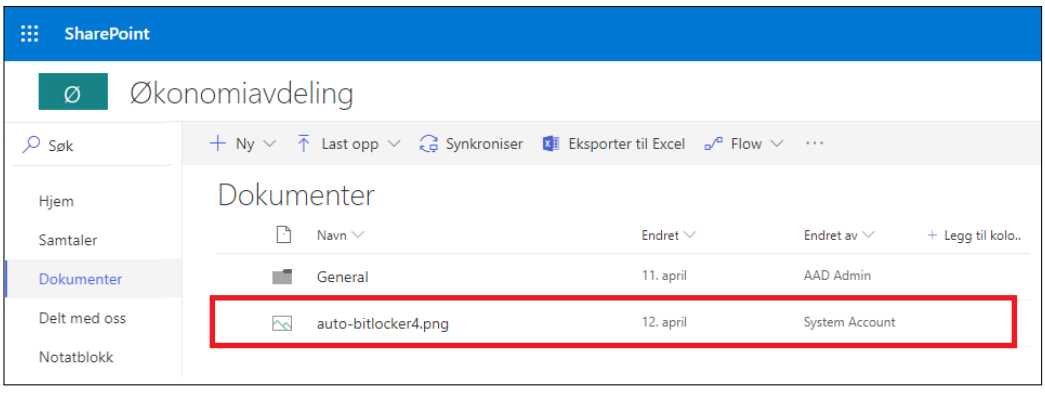
Figur 19

Mens migreringen pågår vil du kunne følge prosessen gjennom en framdriftsindikator. Ved fullføring dukker det opp et statusvindu som informerer om migreringen var vellykket eller ikke, hvor mange filer den migrerte og den totale størrelsen på filene. Som vist i figur 20, gikk migreringen feilfritt i vårt tilfelle.



Figur 20

Ser vi nå i SharePoint, kan vi verifisere at filene ble migrert. Denne migreringen hadde bare en fil og, som vi ser i figur 21, ble bildet lagt i riktig mappe med endring gjort av "System Account".



Figur 21

5 OneDrive

Migrering til OneDrive er en relativt enkel oppgave, som det er anbefalt at brukerne selv gjør. Det finnes metoder for å overføre filer fra en filtjener gjennom script og redirigering av filer, men disse er ikke anbefalt med mindre bedriften krever dette. Brukere kan selv flytte filer til OneDrive enten ved klipp og lim, eller ved kopiering til OneDrive-mappen i filutforskeren. Dette kommer også med fordelen av at brukerne får erfaring med bruk av OneDrive, slik at be blir bedre kjent med lagringstjenesten de vil benytte fremover. Alternativt kan en bruke migreringsverktøyet til SharePoint, SPMT[5], noe som beskrives i avsnitt 4.2, SharePoint Migration Tool.

Referanser

[1] Microsoft. *Import Configuration Manager data to Microsoft Intune*. 2019. URL: https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/migrate-import-data (sjekket 04.05.2019).

[2] Gerry Hampson. *Comanagement and migrating from ConfigMgr hybrid to standalone Intune*. 2017. URL: http://gerryhampsoncm.blogspot.com/2017/10/comanagement-and-migrating-from.html (sjekket 04.05.2019).

[3] Benoit Lecours. *How to Change SCCM MDM Authority to Intune Standalone*. 2018. URL: https://www.systemcenterdudes.com/sccm-mdm-authority-intune-standalone/ (sjekket 04.05.2019).

[4] Microsoft. *Overview of the SharePoint Migration Tool*. 2019. URL: https://docs.microsoft.com/en-us/sharepointmigration/introducing-the-sharepoint-migration-tool (sjekket 04.05.2019).

[5] Microsoft. *Migrate content to OneDrive for Business*. 2019. URL: https://docs.microsoft.com/en-us/sharepointmigration/Migrating-content-to-OneDrive-for-Business (sjekket 04.05.2019).

Modern Workspace - Driftsdokument Enhetssikkerhet

v.0.6

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
24.04.2019	0.1	Dokument opprettet
29.04.2019	0.2	Introduksjon påbegynt, lagt til figurer og påbegynt skriving på aktivering av Windows defender ATP, figurer for testing lagt til
01.05.2019	0.3	Aktivering av Windows Defender ATP ferdigstilt, Detection testing opprettet og ferdigstilt, Demo opprettet og ferdigstilt, lagt inn noen figurer for
02.05.2019	0.4	Endpoint protection opprettet og påbegynt, device restrictions opprettet og påbegynt, conditional access opprettet og påbegynt lagt til nye figurer
03.05.2019	0.5	Endpoint protection ferdigstilt, device restrictions ferdigstilt, conditional access ferdigstillt, introduksjon revidert og ferdigstilt. Flyttet BitLocker dokumetasjonen inn i dette dokumentet
06.05.2019	0.6	Mindre revisjon av tekst, retting av grammatiske og språklige feil

Innhold

1 Introduksjon

Enhetssikkerhet omhandler de innstillingene som skal beskytte individuelle enheter. Dette skjer gjennom konfigurasjon av policies og profiler. Vi deler inn dokumentet i fem ulike deler, som til sammen vil være vårt forslag til oppsett av en helhetlig beskyttelse av enheter. Disse fem delene er:

- **Device Configuration**. Vi går gjennom hvordan Device Configuration profiles fungerer på de ulike operativsystemene og hvilke muligheter som inngår i slike profiler.
- **Endpoint Protection**. Vi går gjennom et mulig oppsett av en Endpoint Protection profil, som vil være et bra utgangspunkt for en bedrift å sikre sine Windows 10-enheter.
- **Conditional Access**. Vi går gjennom mulighetene Conditional Access[1] bringer, hva som kan og ikke kan gjøres, samt resultatet av oppsett av en slik policy.
- **Windows Defender ATP**. Vi går gjennom aktivering, testing og en demonstrasjon av sikkerhetsmekanismen Windows Defender ATP[2]. Vi ser på hvordan mekanismen kan samarbeide med Conditional Access for å blokkere tilgang på bedriftens ressurser når enheten blir rammet av en sikkerhetstrussel.
- **BitLocker**. Vi går gjennom oppsettet som gjøres i Intune for å sette opp kryptering av maskiner om kjører Windows 10. Denne krypteringen gjør at filer, applikasjoner og operativsystem vil være utilgjengelig helt til maskinen dekrypteres ved oppstart.

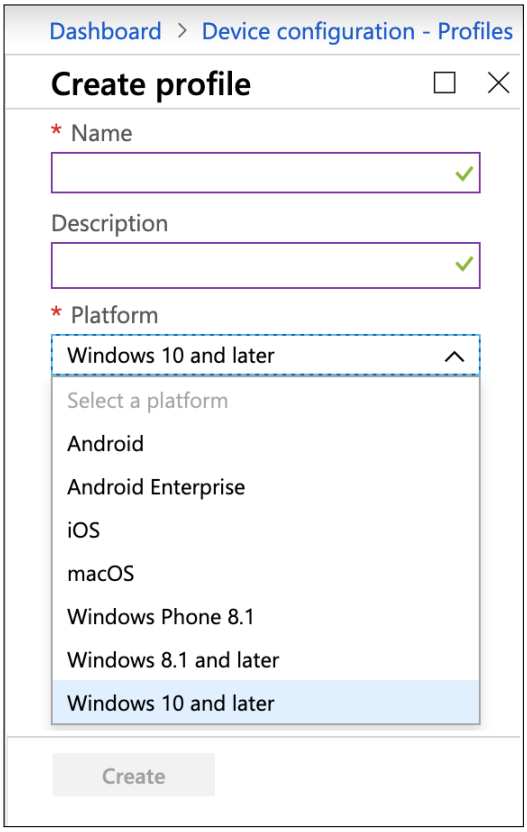
Dokumentet vil gå ut ifra at leser har en viss teknisk kunnskap, og vil ikke nødvendigvis være enkelt for ufaglærte å forstå.

2 Device configuration profile

Konfigurasjonsprofiler lar bedriften konfigurere hvordan enheter vil oppleves, deres sikkerhet og hvordan de oppfører seg i hendene på brukere. Det er et stort antall ulike profiler som kan settes opp, og graden av skreddersøm en bedrift kan oppnå er derfor enorm. Profilene vil være ulike avhengig av plattformen, altså operativsystemet, den settes opp for. Dette vil si at en sikkerhetsprofil for iOS ikke vil være lik den på Android, og de er ikke kompatible med andre OS enn den valgte plattformen.

Profilene bør følge en navnestandard, der "best practice" følger standarden "Operativsystem - profiltype - underkategori", i.e. "Windows 10 - Endpoint protection - Encryption".

På figur 1 kan vi se de ulike plattformene som er tilgjengelig for opprettelse av konfigurasjonsprofiler. Vi ser at alle de største plattformene, som Android, iOS, macOS og Windows 10 støttes, hvor macOS er den eneste vi ikke vil se på i løpet av prosjektet.

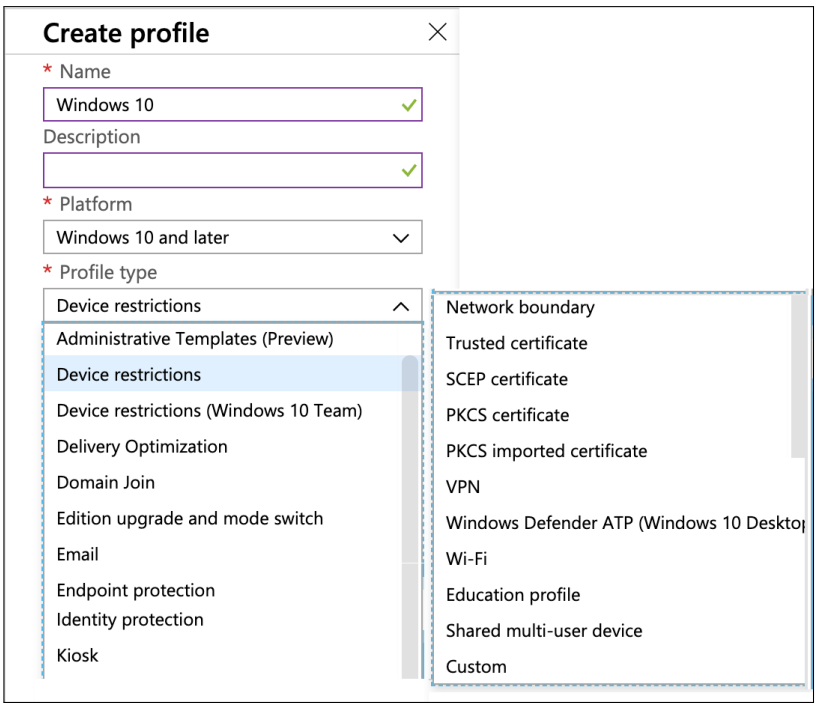


Figur 1

2.1 Windows 10

Konfigurasjonsprofiler for Windows 10 lar bedriften skreddersy hvordan maskiner, registrert i Intune, vil oppleves for brukerne. Her kan en fjerne muligheten til interaksjon med ulike innstillinger for å hindre brukerne fra å endre på innstillinger de ikke vet hva er. En kan også sette opp forhåndsinnstillinger, slik at maskinene ikke trenger konfigurasjon etter innmelding i Intune. Sikkerhet, internett, epost og lignende vil også være mulig å få ferdig oppsatt for brukerne. På bakgrunn av prosjektets restriksjoner i forhold til tid og omfang, vil vi kun gå gjennom enhetsrestriksjoner og Endpoint Protection.

Ser vi på figur 2, under profiltype, er det en rekke konfigurasjonsprofiler som kan settes opp. Flere av disse, som “Device restrictions”, “Endpoint protection” og “Identity protection” vil ha fokus på sikkerhet. Disse konfigureres for å gjøre enheten trygg fra eksterne aktører som ønsker å forårsake skade på bedriften, men også fra egne brukere som ikke vet bedre. Videre i figur 2, ser vi også at en kan konfigurere oppsettet av blant annet WiFi, e-post, VPN og sertifikater. Dette gjør at når brukerne registrerer maskinen sin i Intune, vil de automatisk kunne få koblet seg på bedriftens nettverk, få eposten sin satt opp, få lagt inn sertifikater og satt opp VPN uten at brukerne, eller IT-avdelingen, trenger å gjøre noe.



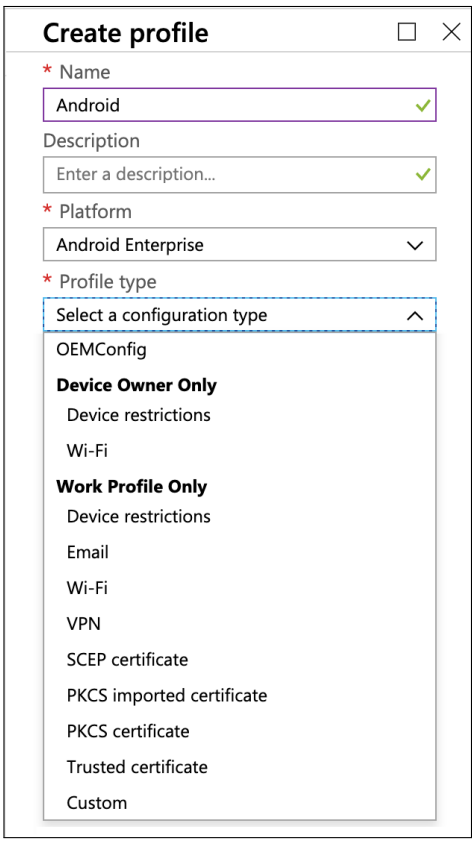
Figur 2

2.2 Android

Konfigurasjonsprofiler for Android lar bedriften skreddersy brukernes opplevelse på deres mobile enhet. Ikke ulikt konfigurasjonsprofiler for Windows 10, kan sikkerhet og opplevelse konfigureres slik at brukeren, og IT-avdelingen, trenger minimalt med egen konfigurasjon.

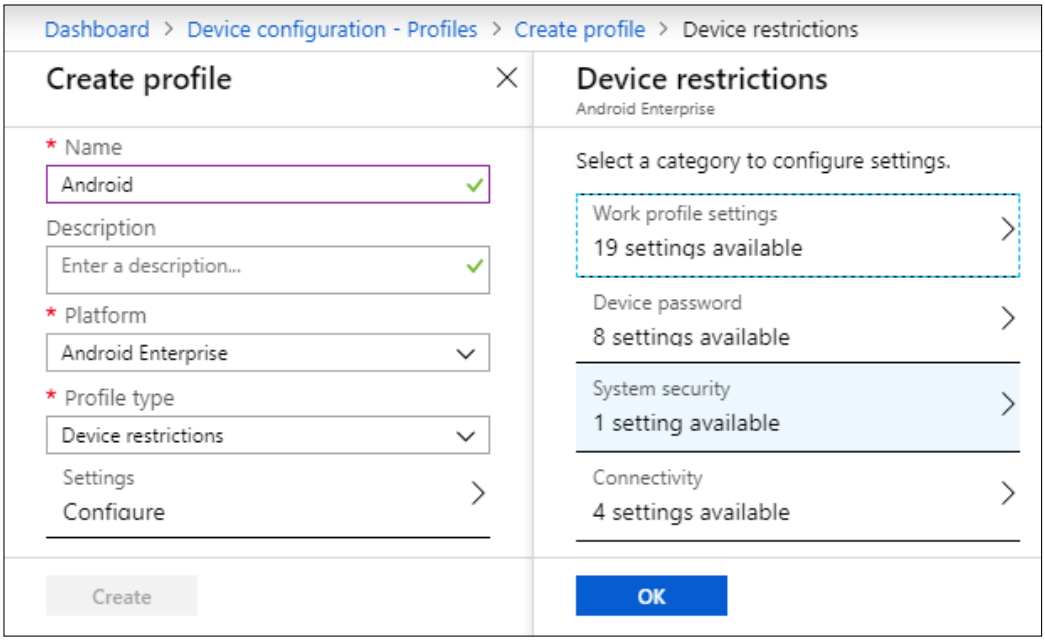
Ser vi på figur 3, får vi en forståelse for mange profiler som kan opprettes for Android-enheter. Profilen "Device restrictions" lar bedriften sette restriksjoner av sikkerhetsgrunner eller for brukervennlighets skyld, slik at enheten er trygg fra ondsinnede eksterne aktører, men også fra egne brukere som ikke er særlig kyndig i teknologiverdenen.

Videre i figur 3, ser vi også at en kan konfigurere innstillinger som WiFi, e-post, VPN. Dette lar bedriften sette opp enheten slik at den er klar for bruk så snart enheten er registrert i Intune. Dette betyr at verken brukeren selv, eller IT-ansvarlig trenger å konfigurere hver enkelt enhet, og at e-post, internett, VPN og lignende er klart etter registrering.



Figur 3

Velger vi å gå inn i enhetsrestriksjoner, som vist i figur 4, ser vi at det er ulike konfigurasjonsmuligheter. Det kan settes opp restriksjoner til enhetens passord, arbeidsprofilen, systemsikkerhet og tilkoblingsmuligheter. Disse vil sammen sikre enheten fra egne brukere og ondsinnede, eksterne, aktører.



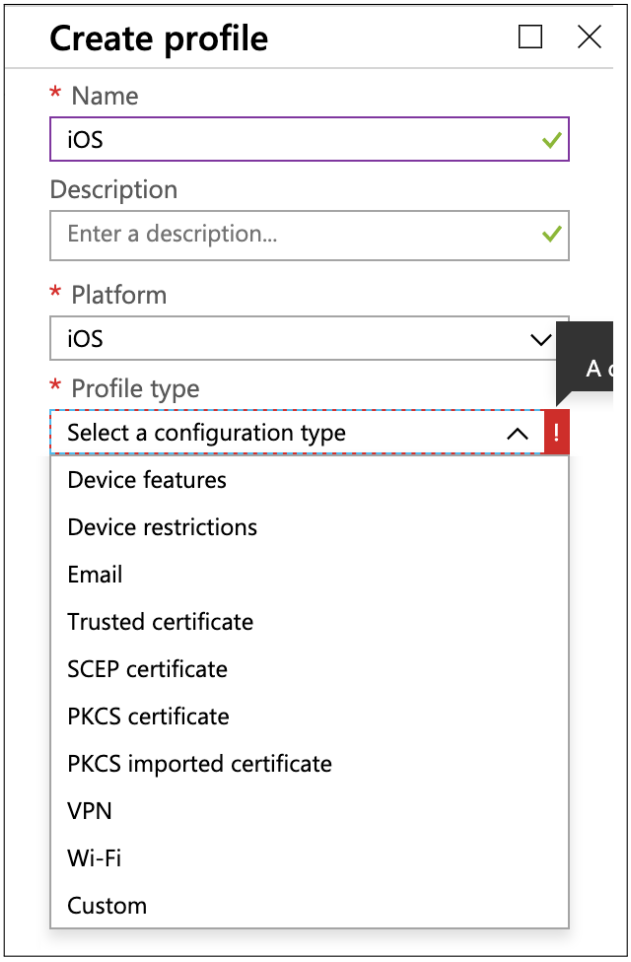
Figur 4

2.3 iOS

Konfigurasjonsprofiler for iOS lar bedriften skreddersy brukernes opplevelse på deres mobile enhet. Ikke ulikt konfigurasjonsprofiler for Windows 10, kan sikkerhet og opplevelse konfigureres slik at brukeren, og IT-avdelingen, trenger minimalt med egen konfigurasjon. Utarbeides en Apple DEP-avtale, kan enhetene være klare allerede før en har åpnet boksen den leveres i.

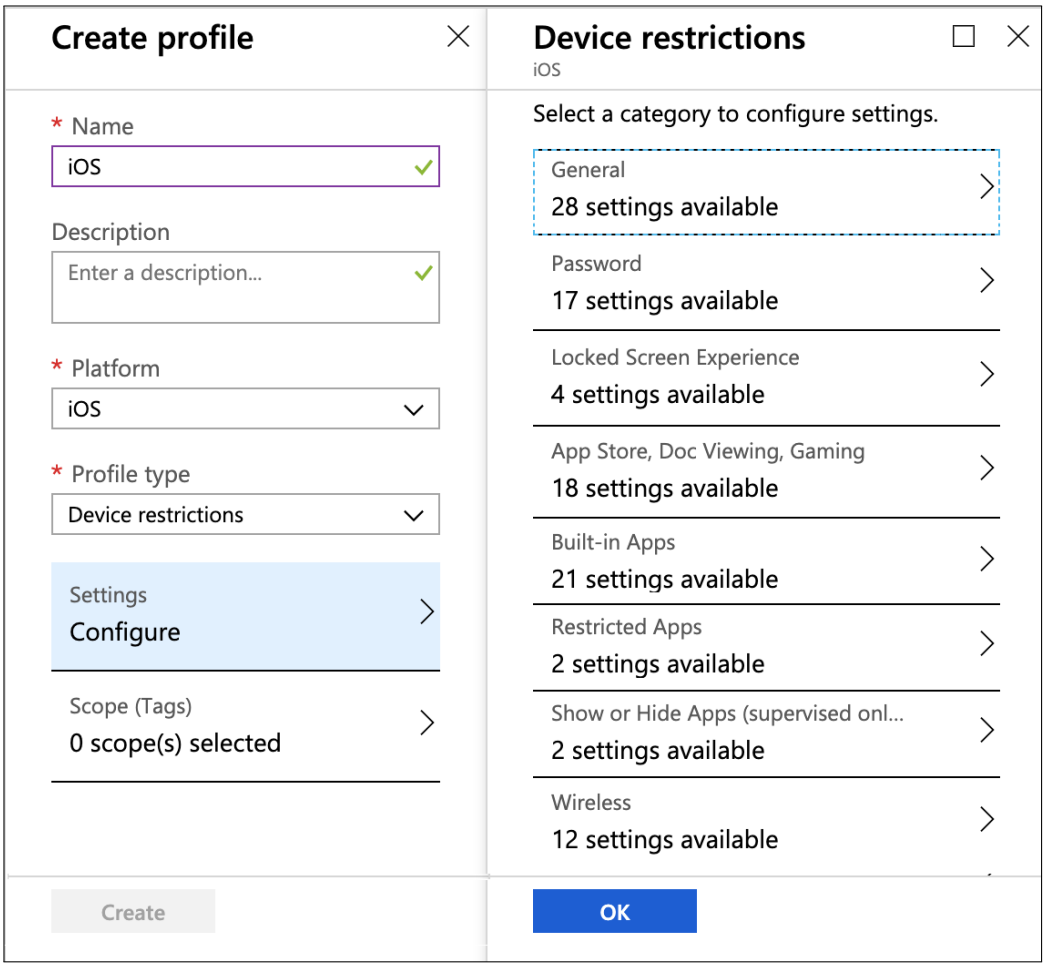
Med figur 5, kan vi forstå omfanget av konfigurasjonsmulighetene en har for iOS-enheter. Profilen for “Device restrictions” vil stå for sikkerhetsinnstillinger, og la bedriften sikre enheten på optimal måte.

Videre i figur 5, ser vi også at en kan konfigurere innstillinger som WiFi, e-post, VPN. Dette lar bedriften sette opp enheten slik at den er klar for bruk så snart enheten er registrert i Intune. Dette betyr at verken brukeren selv, eller IT-ansvarlig trenger å konfigurere hver enkelt enhet, og at e-post, internett, VPN og lignende er klart etter registrering.



Figur 5

Velger vi å gå inn i enhetsrestriksjoner, som vist i figur 6, ser vi at det er ulike konfigurasjonsmuligheter. Det kan settes opp restriksjoner til enhetens passord, arbeidsprofilen, systemsikkerhet og tilkoblingsmuligheter. Disse vil sammen sikre enheten fra egne brukere og ondsinnede, eksterne, aktører.



Figur 6

3 Windows 10 – Endpoint Protection

Endpoint Protection er en av de viktigste delene av sikkerhet på enheter med Windows 10. Innad i en konfigurasjonsprofil for Endpoint Protection er det enorme muligheter for konfigurasjon en bedrift kan gjøre for å sikre de ansattes enheter.

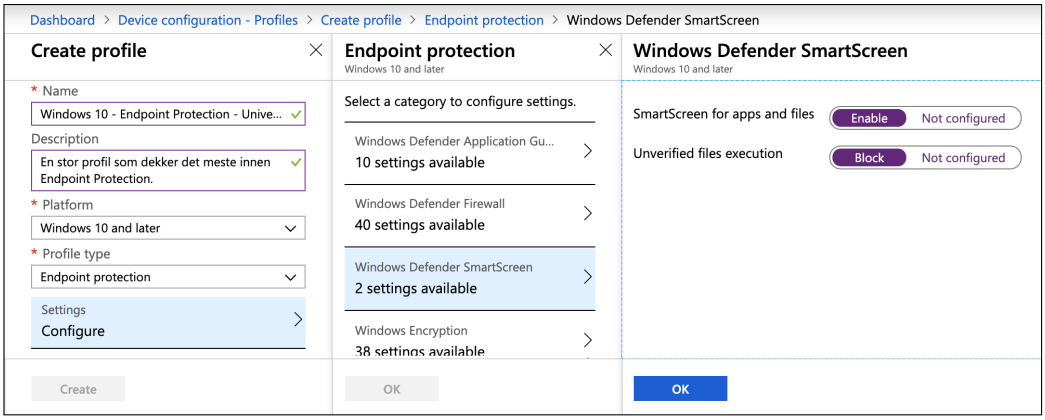
Når en lager en profil for Endpoint Protection anbefales det å lage en profil per underkategori i Endpoint Protection, framfor en stor profil med utallige innstillinger. Grunnen til dette er at det vil gjøre eventuell feilsøking mye enklere, da man raskt kan teste hvilken innstilling som skaper problemer, sammenlignet med en stor profil hvor mange innstillinger kan stå for ulike problemer. En annen grunn er at senere konfigurasjon vil være mye enklere, da en kan åpne den spesifikke profilen som trenger konfigurasjon og slipper å rote gjennom den store profilen.

I vårt eksempel på Endpoint Protection lager vi en stor profil. Dette gjøres grunnet prosjektets tidsrammer og omfang. Vi anbefaler ikke å gjøre dette i en realistisk implementasjonsprosess. Vi vil også understreke at selve oppsettet av profilen må gjenspeile bedriftens behov og ønsker i en realistisk setting. I vårt prosjekt vil vi opprette en profil basert på anbefalinger fra sikkerhtetskyndige personer og andre oppsett funnet på nett.

Første steg vil være å navigere til punkt for oppretting av nye profiler i enhetskonfigurasjon i Azure-portalen. Stien, som vist i figur 7, er “Intune”, “Device configuration”, “Profiles” og “Create Profile”.

Figur 7

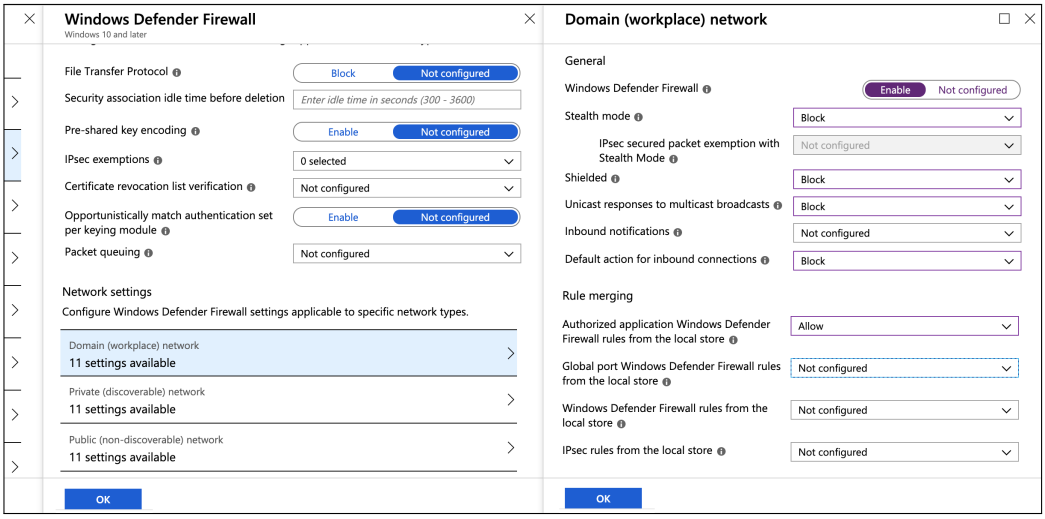
Inne i den nye profilen må vi legge inn et beskrivende navn, og velge plattformen "Windows 10 and later". Under profiltype velges "Endpoint protection". Konfigurasjon av profilen kan nå begynne. Som vist i figur 8, skrur vi på SmartScreen. Dette er funksjon som vil advare brukere når de åpner usikre nettsider i nettleseren og når de forsøker å åpne usikre applikasjoner eller filer.



Figur 8

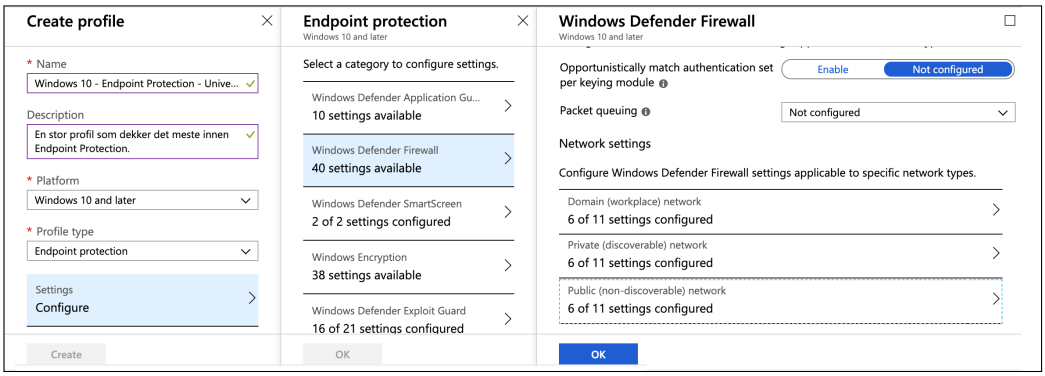
Under innstillingene for Windows Defender gjør vi en rekke endringer, som vist i figur 9. Disse endringene er identiske på alle de ulike nettverkstypene, “Domain (workplace) network”, “Private (discoverable) network” og “Public (non-discoverable network”.

Vi skrur på Windows brannmur og gjør en del annen konfigurasjon, som vises i figur 9. Dette oppsettet vil skru på brannmur på brukernes maskiner og være et godt grunnlag for å kunne opprette brannmurregler og for videre konfigurasjon i profilen.



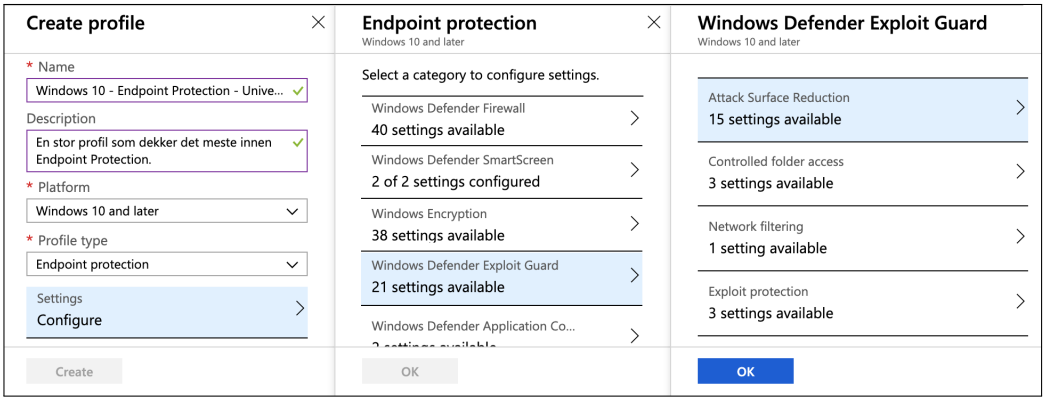
Figur 9

Som vi ser i figur 10, vil de tre nettverkstypene ha konfigurert 6 innstillinger. Disse er de samme innstillingene på tvers av nettverkstypene.



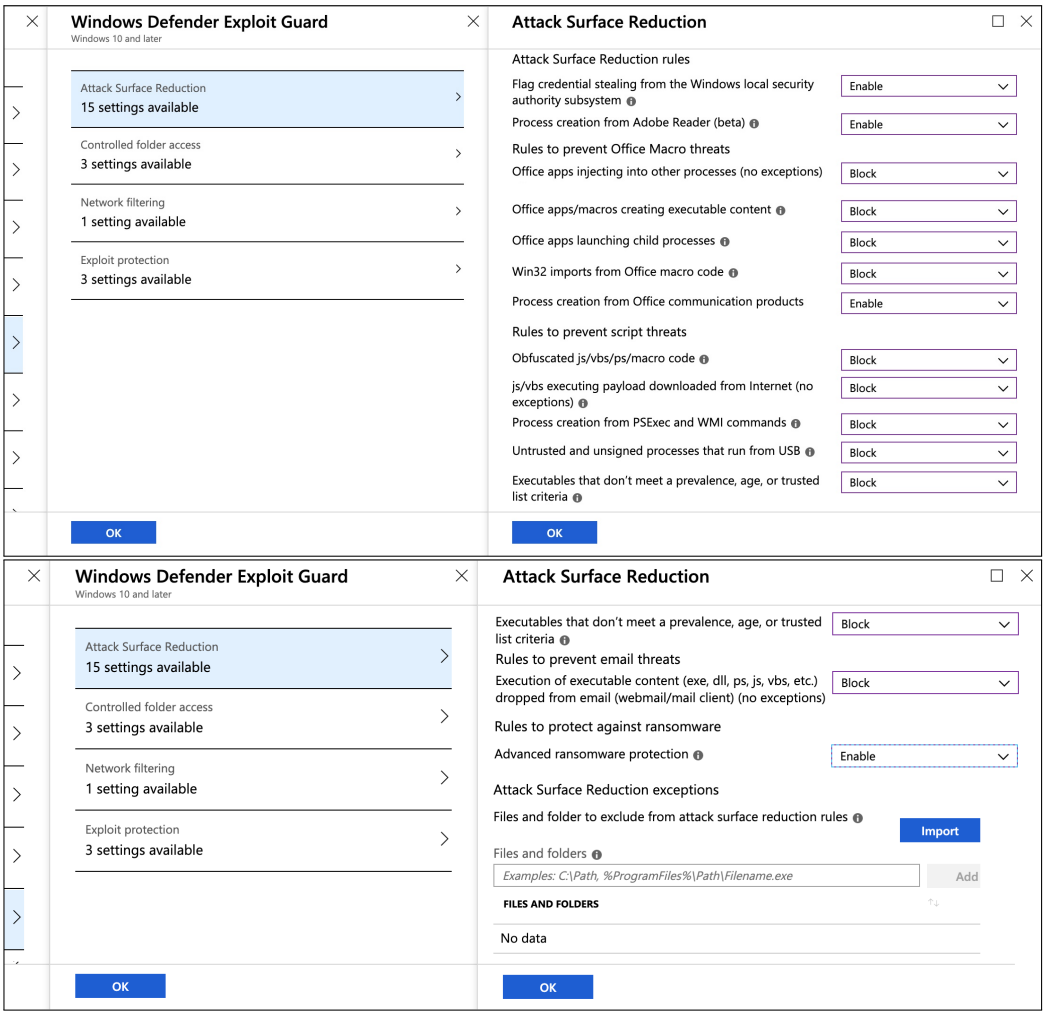
Figur 10

Under “Windows Defender Exploit Guard” finner vi, som vist i figur 11, en rekke underkategorier. Alle disse kategoriene, utenom Exploit protection, krever Windows Defender Antivirus på klientmaskinene for å fungere. Vi vil se på hver underkategori individuelt.



Figur 11

Vi vil først se på Attack Surface Reduction, som vist i figur 12. Attack Surface Reduction er funksjonalitet som vil forhindre angrep på applikasjoner, og da særlig Office-applikasjoner. Disse vil kunne forhindre at en falsk word-fil, sendt via phising mail, vil kunne kjøre makroer, starte underprosesser og lignende. Dette vil i stor grad kunne hindre brukere fra å infisere egen eller flere andre maskiner på nettverket. Her vil en kunne ta en vurdering om en skal starte med blokkering, eller en audit-periode. Ved å velge "audit" på flere av valgene, vil Windows Defender overvåke og lære av bruksmønstret til brukerne. Dette kan gjøres slik at det vil oppstå færrest mulig false positivesnår en skrur på innstillingen.

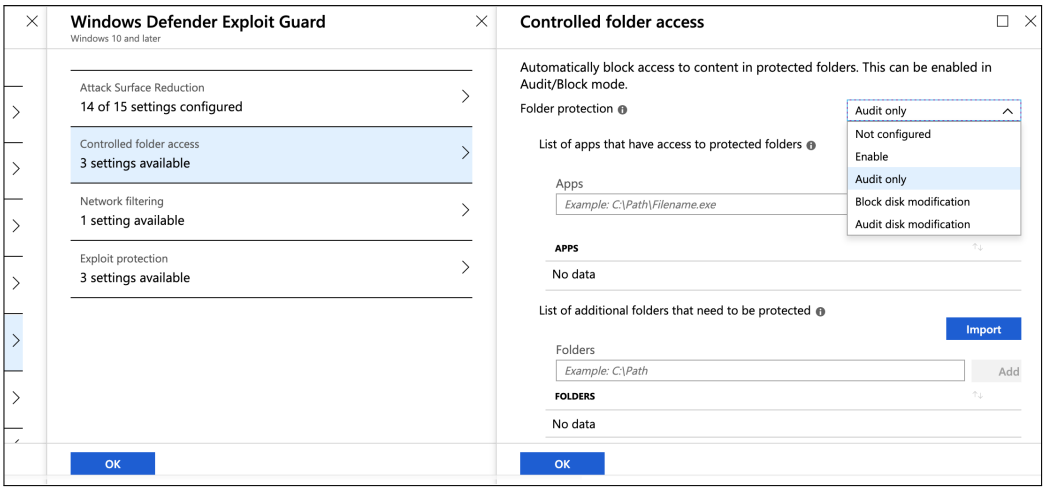


Figur 12

Vi ser så på Controlled folder access, som vist i figur 13. Controlled folder access vil beskytte filer i nøkkelområder på maskinen fra endringer av skadelige eller suspekte applikasjoner, som for eksempel ransomware. Her bør en sette opp funksjonen som audit i en periode, slik at Windows Defender lærer bruksmønsteret til brukeren og forstår hva som er normal bruk og ikke. Etter en slik overvåkningsperiode kan en skru på funksjonaliteten til Controlled folder access ved å endre til "Enable".

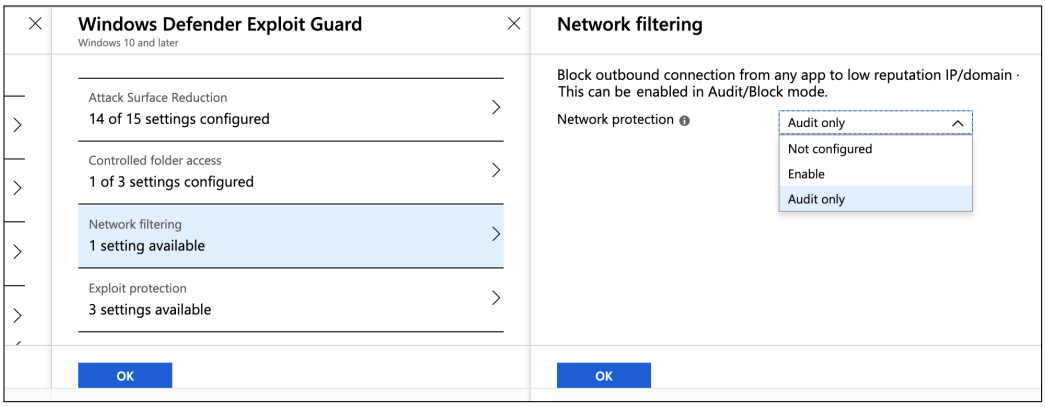
Controlled folder access er en av funksjonene som kunne stoppet angrepet på Norsk Hydro fra tidlig 2019. Hadde Norsk Hydro satt opp Controlled folder access sammen med funksjonalitet i Attack Surface Reduction, er det høyt sannsynlig at angrepet ville blitt blokkert lenge før det kunne gjøre noe skade på maskinene i nettverket. Du kan lese mer om angrepet på Norsk Hydro her:

`https://e24.no/digital/24585520`



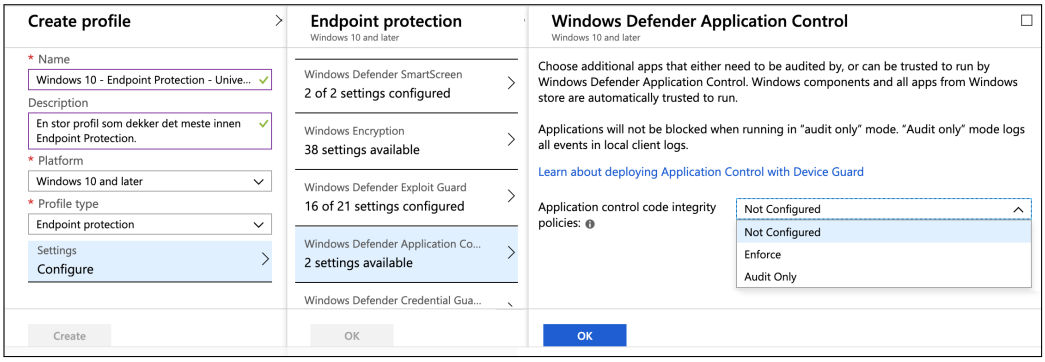
Figur 13

Vi går over til Network filtering, som vist i figur 14. Denne funksjonen utvider SmartScreens funksjonalitet, at slik beskyttelsen inkluderer overvåking av nettverkstrafikk og tilkoblinger på brukernes enheter. Også denne funksjonen kan settes til audit i en periode for å lære bruksmønster, før den settes til "Enable".



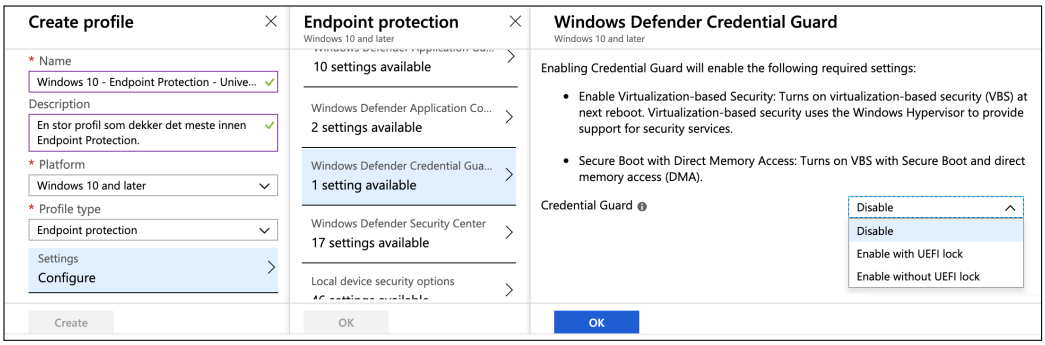
Figur 14

Vi fortsetter til Windows Defender Application Control, som vist i figur 15. Denne funksjonen vil begrense hvilke applikasjoner som kan kjøre kernel-kode. Dette vil hindre en ukjent applikasjon fra å utføre skadelig kode mot operativsystemets kjerne. Application Control kan settes opp i som audit only i en opplæringsperiode, slik at Windows Defender gjenkjenner normalt bruksmønster. Etter opplæringsperioden kan funksjonen aktiveres ved å endre til "Enforce".



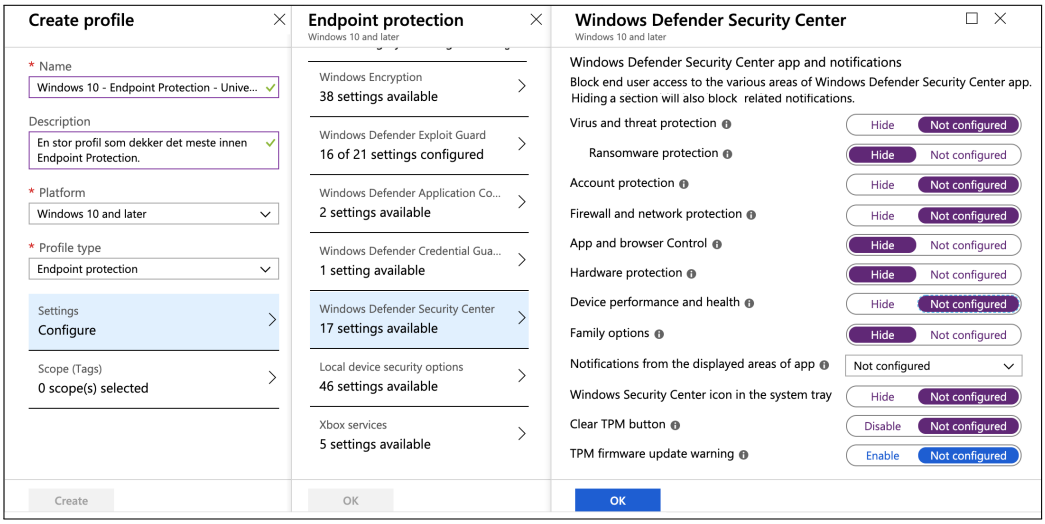
Figur 15

Vi går over til Windows Defender Credential Guard, som vist i figur 16. Denne funksjonen vil hindre uautorisert tilgang på kontoinformasjon gjennom en virtualisert sikkerhetsboks for lagring av legitimasjoner. Dermed må brukere godkjenne dersom en applikasjon ønsker tilgang på en av deres legitimasjoner.



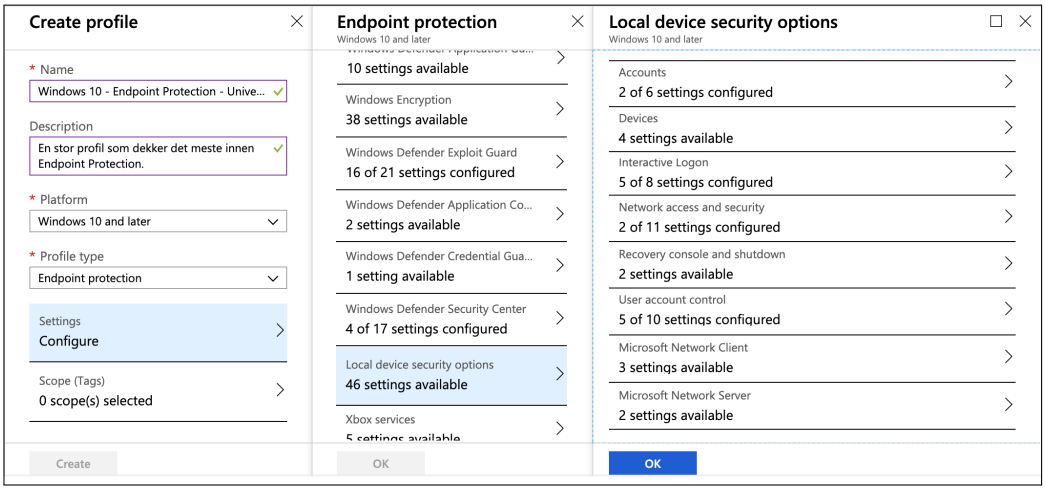
Figur 16

Vi går videre til Windows Defender Security Center, som vist i figur 17. Her kan det konfigureres hva brukeren vil se i sikkerhetssenteret på sin lokale maskin. Dette lar deg fjerne forvirrende og uinteressant funksjonalitet, slik at brukere ikke kan gjøre feil eller bli forvirret av informasjon de ikke forstår.

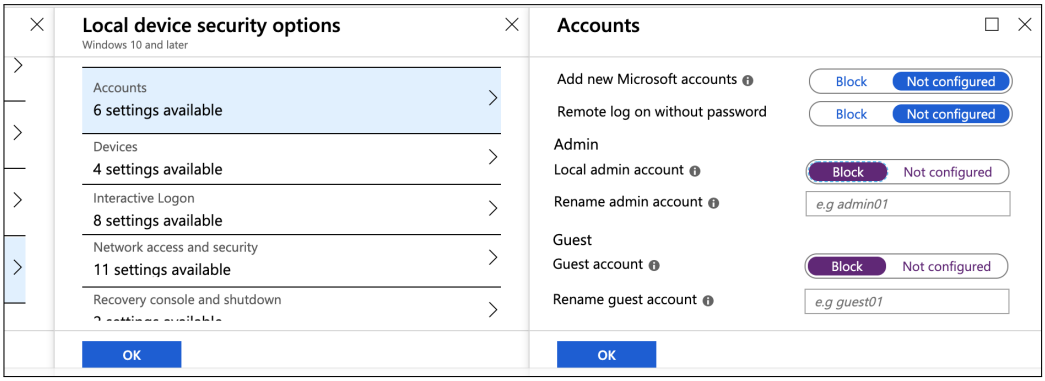


Figur 17

Under Accounts, som vist i figur 18 og figur 19, kan vi fjerne kontotyper. Dette lar oss fjerne muligheten for lokale administratorer og gjestebrukere fra maskinen. Dermed vil kun administratorer i Intune har administratortilganger. Dette hindrer brukere fra å kunne misbruke tilganger og utsette egen, eller andre maskiner på nettverket, for sikkerhetsrisikoer.

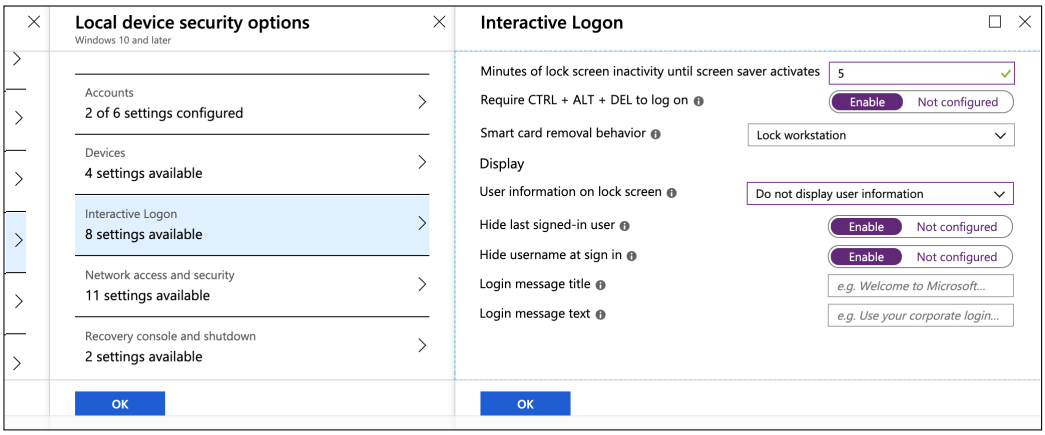


Figur 18



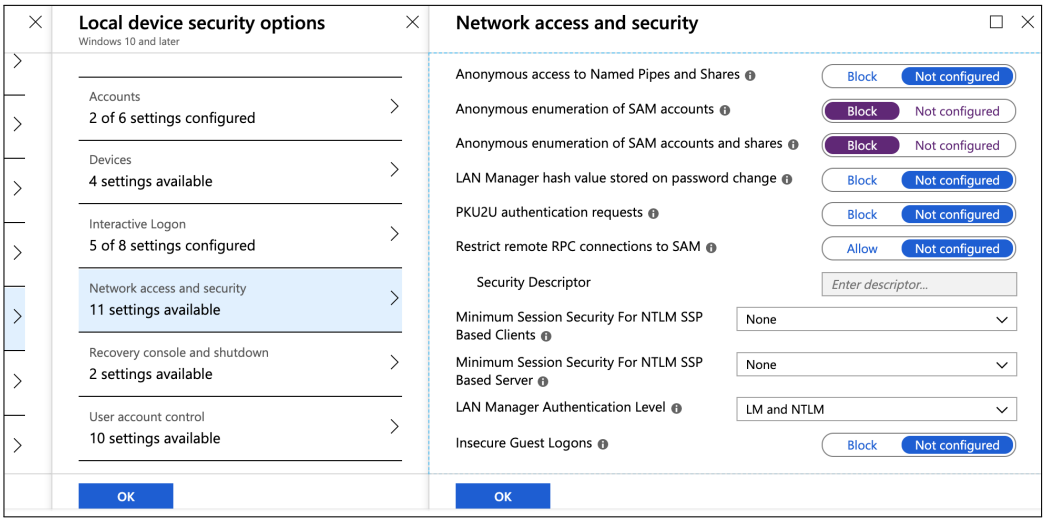
Figur 19

Under Interactive Logon, som vist i figur 20, kan vi konfigurere hvordan innlogging vil oppleves. Av sikkerhetsgrunner fjerner vi at en kan se forrige innlogget bruker, og at brukernavnet vises. Her kan en også endre tekst og lignende ved innlogging.



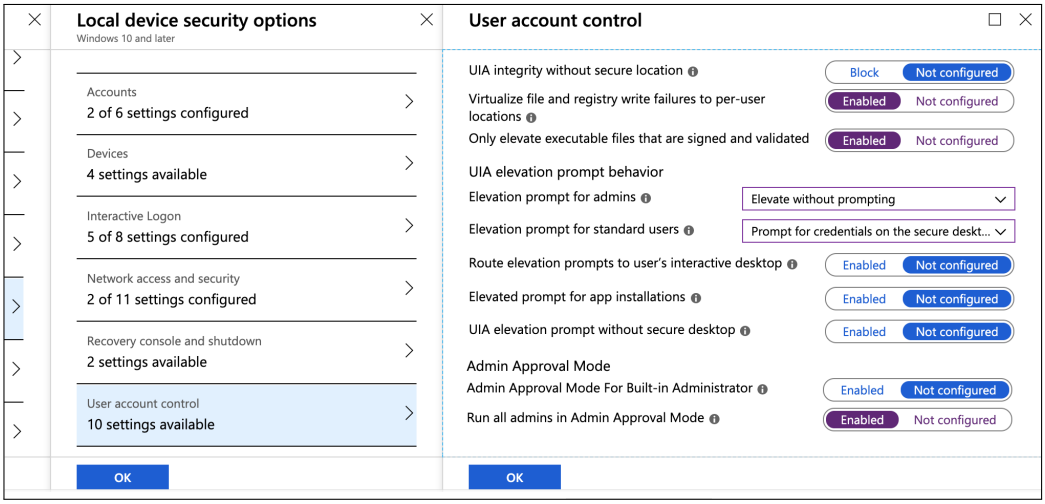
Figur 20

Inne i Network access and security, som vist i figur 21, kan en konfigurere nettverkstilgang og sikkerhet knyttet til nettverk. Her kan en sette krav til nettverkstilkobling og hva som skal blokkeres.



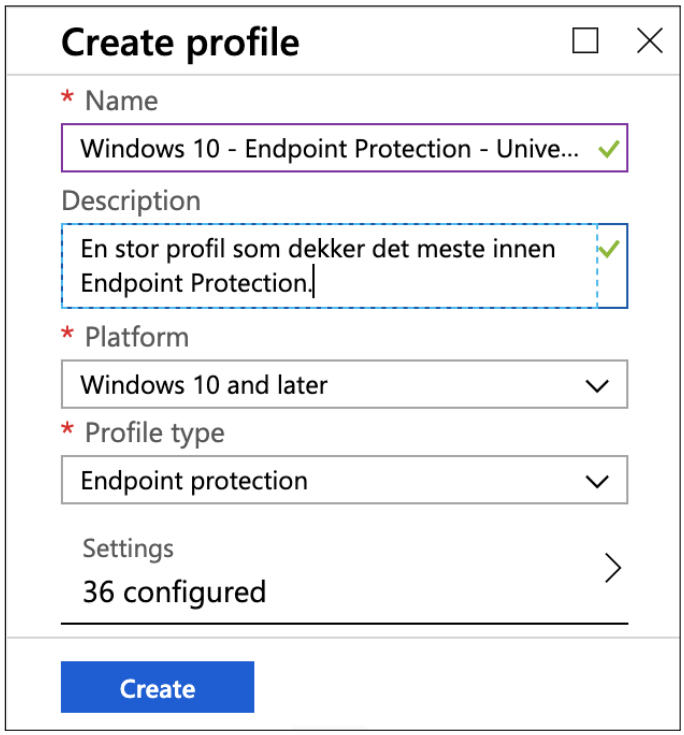
Figur 21

Under User account control, som vist i figur 22, kan en konfigurere hvilke rettigheter brukere har. Her kan en velge hva som krever opphøyde rettigheter og hvordan opplevelsen er når en bruker forsøker å gjøre noe som krever slike rettigheter.



Figur 22

Når profilen er ferdig konfigurert kan en se hvor mange innstillinger som er satt opp, og gå igjennom disse om ønsket. Som vi ser i figur 23, har vi konfigurert 36 innstillinger i denne profilen. Trykk så "Create" for å lagre profilen og klargjøre til tilegnelse.



Figur 23

Det vil så komme en notifikasjon som informerer om opprettelse av profilen var vellykket. Som vi ser i figur 24, ble profilen opprettet uten feil i vårt tilfelle.

Figur 24

Det er viktig å tilegne, eller "Assign", profilen til en bruker/maskin-gruppe for at den skal tiltre. Vi vil ikke gjøre dette for denne profilen, da den vil kunne hindre videre testing på ulike områder inne i klientmaskinen.

4 Windows 10 – Device restrictions

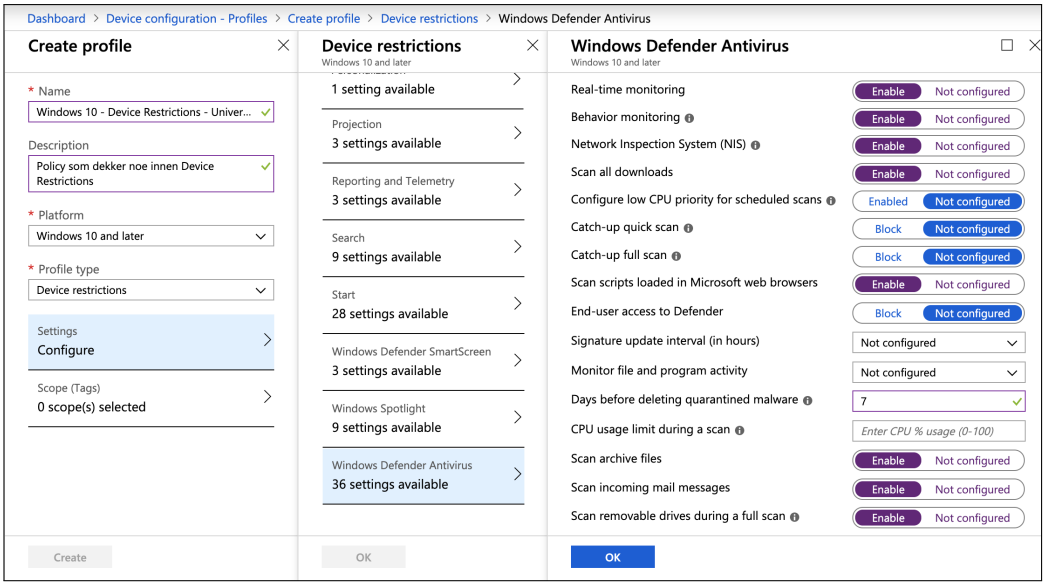
Device Restriction for Windows 10 kan brukes for å tilpasse brukernes maskiner, og hvordan de opplever disse. Bedriften kan avgjøre hvilke muligheter en bruker skal ha på maskinen, og fjerne muligheter som kan stå til forvirring eller som legger opp til brukerfeil. Gjennom Device Restrictions kan en blant annet sette bakgrunnsbilde på maskiner, blokkere mulighet for nettverksdeling og fjerne deler av kontrollpanelet.

Vi vil kun fokusere på konfigurasjon av Windows Defender Antivirus under Device restrictions. Andre restriksjoner kan konfigureres på tilsvarende måte, og hvilke vil være avhengig av bedriftens ønsker og behov.

4.1 Windows Defender Antivirus

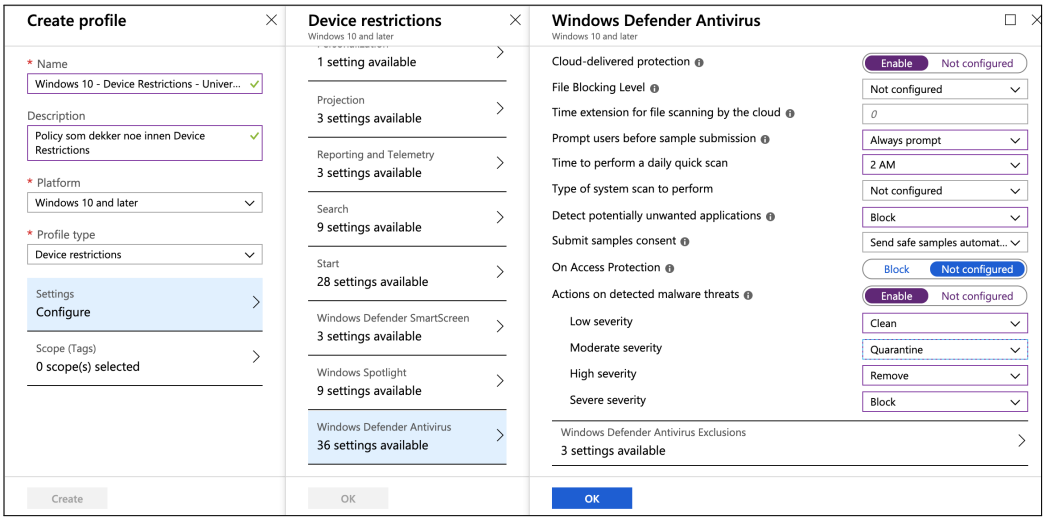
Windows Defender Antivirus selve kjernen for sikkerheten i Windows 10. På egenhånd vil det kunne stoppe store mengder kjente trusler, men i kombinasjon med annen sikkerhetsfunksjonalitet, blir det et svært kraftig verktøy. Deler av Endpoint Protection krever Windows Defender Antivirus for å kunne ta seg av truslene som blir oppdaget, og vil ikke ha noen effekt uten verkøyet. Dermed kan en se på Windows Defender Antivirus som et viktig sikkerhetsverktøy i seg selv, men også som et viktig rammeverk som andre sikkerhetsfunksjoner bygger på.

Inne i Windows Defender Antivirus, som vist i figur 25 og figur 26, kan en konfigurere hvordan antivirusprogrammet skal operere på klientmaskiner. Sanntidsmonitorering, skanning av nedlastinger og mail er blant de mange innstillingen som kan konfigureres. Her er det viktig å forstå bedriftens ønsker og behov, slik at oppsettet er skreddersydd den opplevelsen og det nivået av sikkerhet de er ute etter.



Figur 25

Fortsettelse av figur 25, Windows Defender Antivirus.



Figur 26

Profilen kan så lagres ved å trykke “Create”. Det vil så komme en notifikasjon som informerer om opprettelse av profilen var vellykket.

Det er så viktig å tilegne, eller “Assign”, profilen til en bruker/maskin-gruppe for at den skal tiltre. Vi vil ikke gjøre dette for denne profilen da den vil kunne hindre videre testing på ulike områder inne i klientmaskinen.

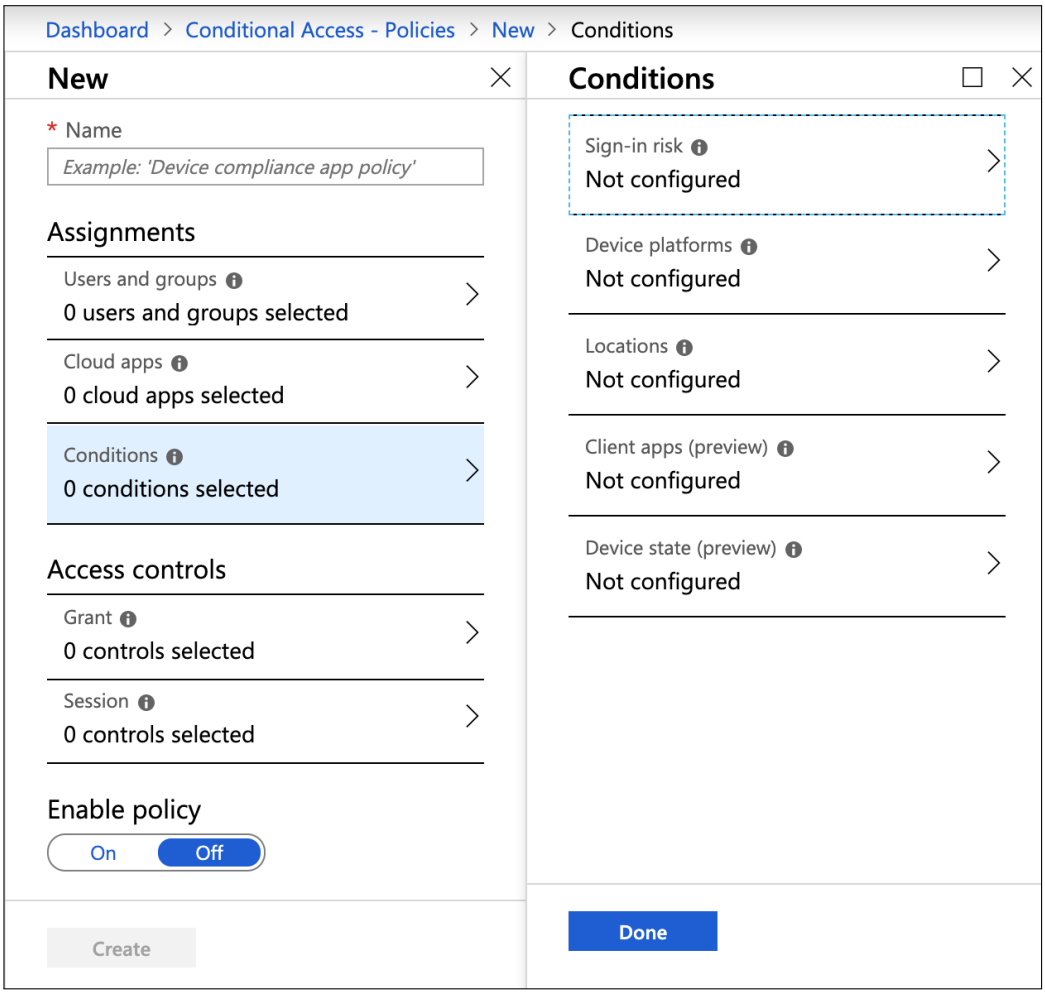
5 Conditional Access

Conditional Access er en funksjonalitet som lar bedriften styre tilganger til applikasjoner, avhengig av valgte betingelser. For eksempel kan Conditional Access blokkere tilgangen til SharePoint, OneDrive, Teams og Exchange dersom en brukers maskin når et visst risikonivå. Conditional Access brukes ofte i sammarbeid med Compliance policies for å blokkere en enhets tilgang dersom den ikke lengre er compliant.

For å opprette en Conditional Access policy må man først navigere til Conditional Access i Azure-portalen. Trykk “Intune”, “Conditional Access”, “Policies” og velg “New Policy”.

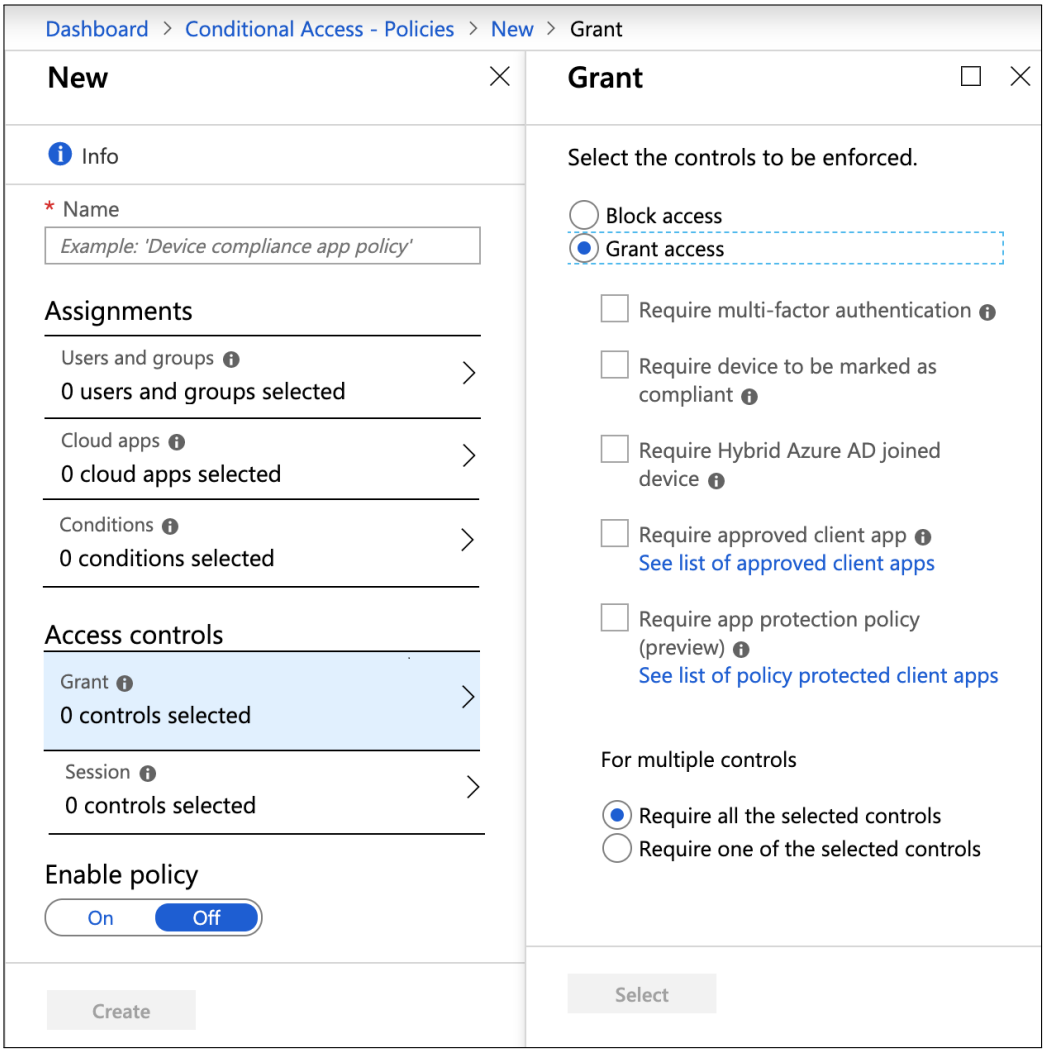
Figur 27

Vi kan nå begynne konfigurasjon av policy. Vi ser først på betingelsene som gjør at Conditional Access skal bryte inn. Som vi ser i figur 28, kan betingelsene baseres på risiko, enhetsplattform, lokasjon, klientapplikasjon og enhetsstatus. Vi vil ikke gå nærmere inn på disse, men vi kan gi et eksempel på en betingelse. En bruker vil kun få tilgang dersom innloggingen forsøkes fra Norge, fra en Windows 10-enhet hvor innloggingsrisikoen anses som lav. Et annet eksempel er hvis de har mange angrepsforsøk fra Kina og Russland, kan bedriften sette som betingelse at dersom innloggingen skjer fra Russland eller Kina, vil brukeren automatisk blokkeres fra sine applikasjoner.



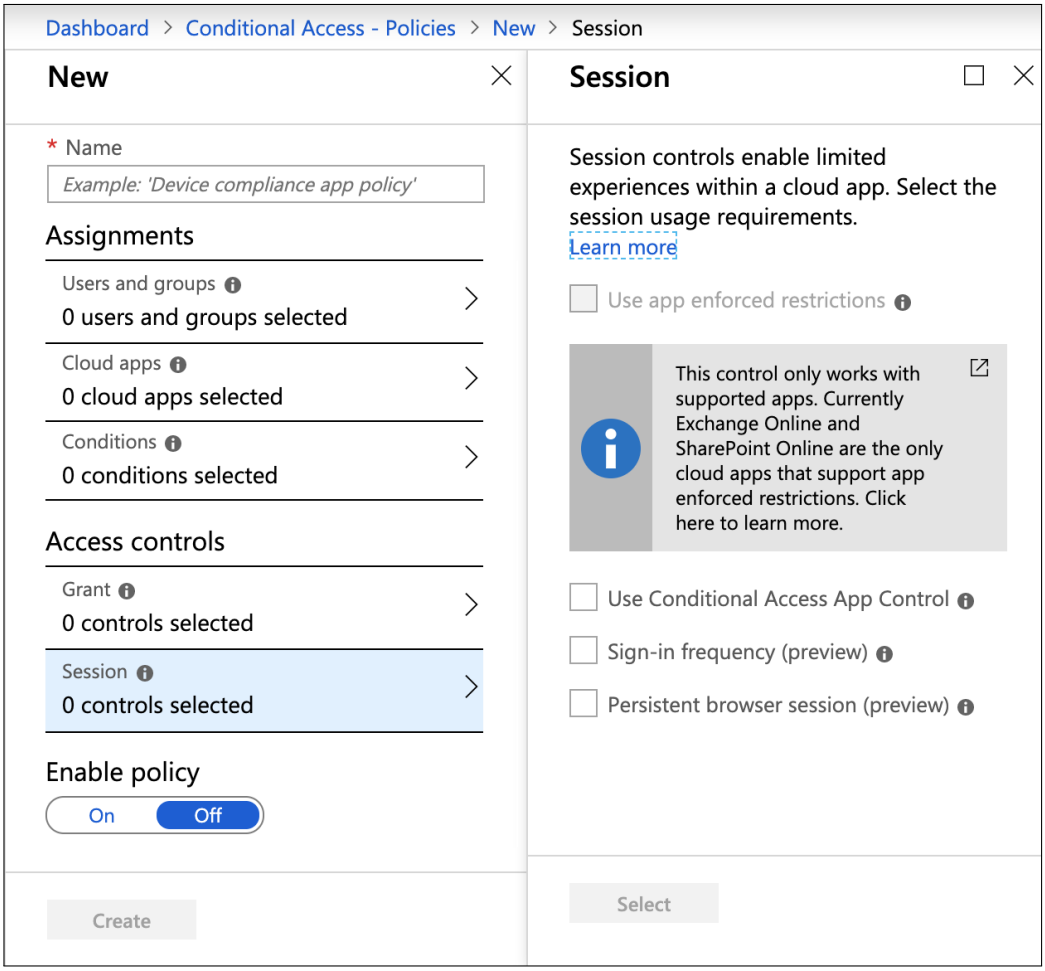
Figur 28

Videre kan vi se på Grant, som avgjør hva som vil skje når betingelsen innfris. Her kan en velge om en vil blokkere, eller gi tilgang. En kan også sette krav om blant annet MFA og compliant enhet, og om kun en av kravene må innfris eller om alle må. Hva som blokkeres eller gis tilgang til bestemmes under “Cloud Apps”.



Figur 29

Under Session, som vist i figur 30, kan en konfigurere en begrensning av tilgangen på en applikasjon. Dette vil si at en kan gi begrenset tilgang i applikasjoner dersom betingelsen innfris, framfor å blokkere eller gi full tilgang.



Figur 30

For å aktivere policy må "Enable policy" være satt til "On". Når dette er gjort kan en opprette policy ved å trykke "Create". Det vil så komme en notifikasjon som informerer om opprettelse av policy var vellykket og om "Enable" er satt til "On" eller "Off".

For mer praktisk bruk av Conditional Access, se avsnitt 6.4.

6 Windows Defender ATP

Windows Defender Advanced Threat Protection, Windows Defender ATP, er en sikkerhetsmekanisme som avslører trusler på maskiner som er registrert i Intune. For å kunne sette opp Windows Defender ATP må en opprette en rekke policies og tilegne disse. Når Windows Defender ATP er satt opp, vil den kunne blokkere tilgangen på bedriftsdata gjennom Conditional Access, og gi administrator mulighet til å overvåke trusler som rammer maskiner innmeldt i Intune.

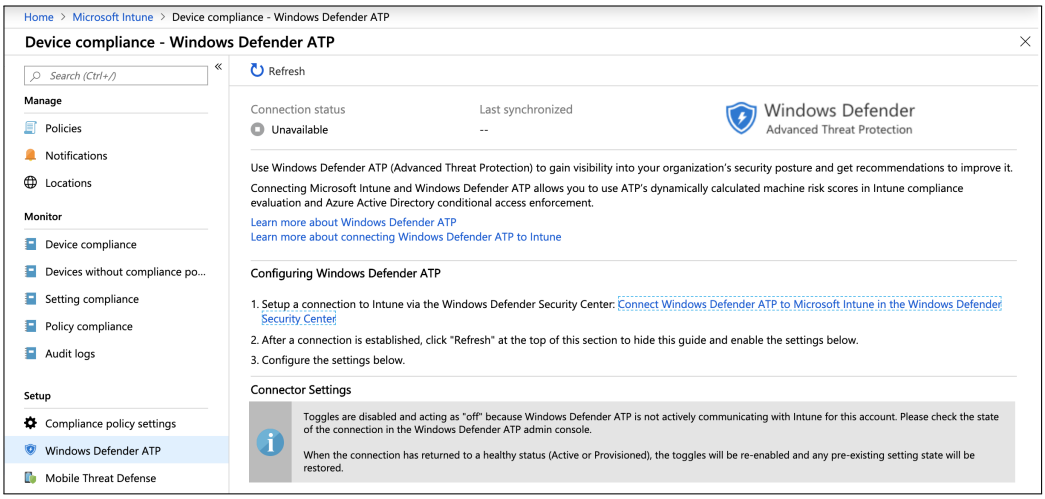
6.1 Aktivering av Windows Defender ATP

Windows Defender ATP er ikke automatisk aktivert i Intune, og krever at en administrator setter dette opp. Oppsettet vil foregå gjennom en veiviser i Microsofts sikkerhetssenter, og ikke direkte i Azure-portalen. Aktiveringen vil opprette en skyinstans og en Windows Defender ATP-konto, og vil avsluttes med onboarding av enheter.

Første steg for å aktivere Windows Defender ATP vil være å navigere til lenken som leder til Microsofts sikkerhetssenter. I Azure-portalen, klikk “Intune”, “Device Compliance” og “Windows Defender ATP”.

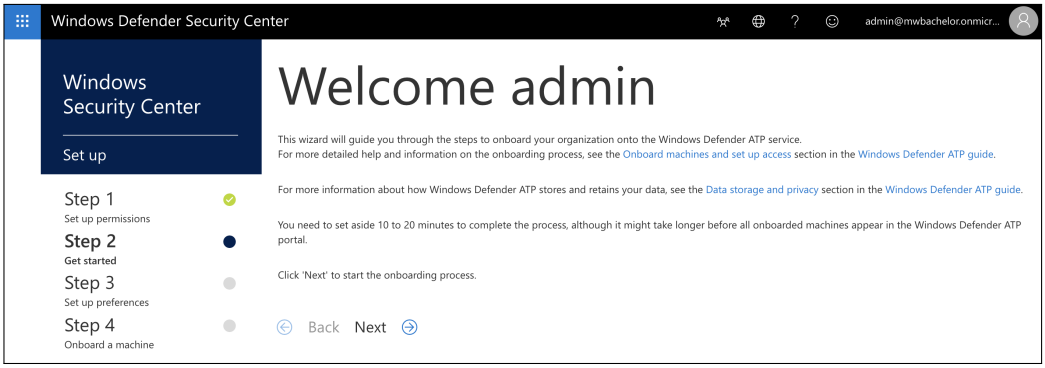
Figur 31

Som vi ser i figur 32, er det ingen kobling opp mot Windows Defender ATP, og det er derfor ikke aktivert enda. For å starte aktiveringen trykk på lenken i teksten "Connect Windows Defender ATP to Microsoft Intune in the Windows Defender Security Center" under første steg.



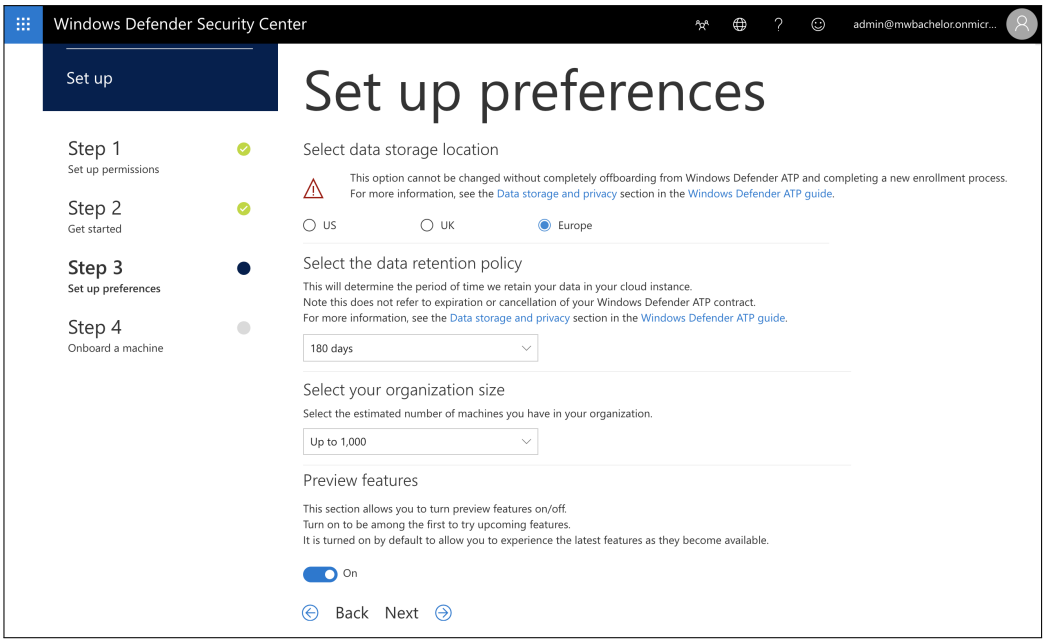
Figur 32

En ny fane vil åpnes med en veiviser i Microsofts sikkerhetssenter. Her får du en kort introduksjon i oppsett av Windows Defender ATP, med lenker til hvor du kan få mer informasjon om prosessen. Det vil være lurt å sette seg inn i hvordan prosessen foregår, og lese informasjonen som er vedlagt. Trykk så "Next" for å starte aktiveringen.



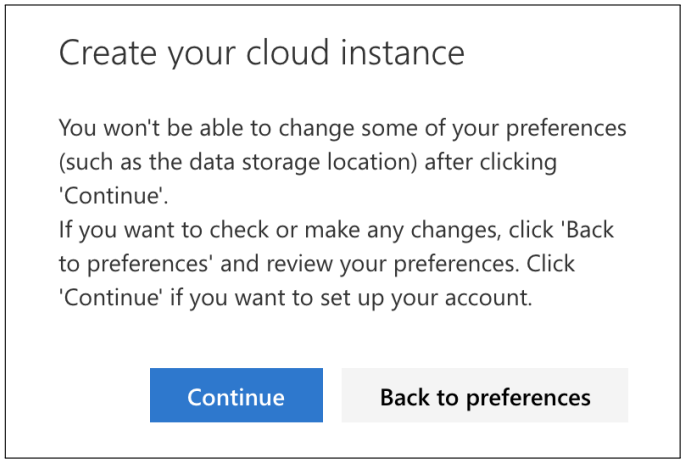
Figur 33

Neste steg i veiviseren vil be om lokasjon på datalagring, hvor lenge data skal lagres, antall maskiner organisasjonen har og om du ønsker å ta i bruk egenskaper som er i testfasen. Valgene som tas her vil være avhengig av bedriften det skal settes opp til, og det vil være viktig å skreddersy oppsettet ut ifra dette. Vi velger her "Europa" som lokasjon for datalagring, "180 days" som lagringsperiode, "Up to 1,000" maskiner innad i organisasjonen og "On" for å ta i bruk egenskaper i testfasen. Trykk så "Next" for å komme videre.



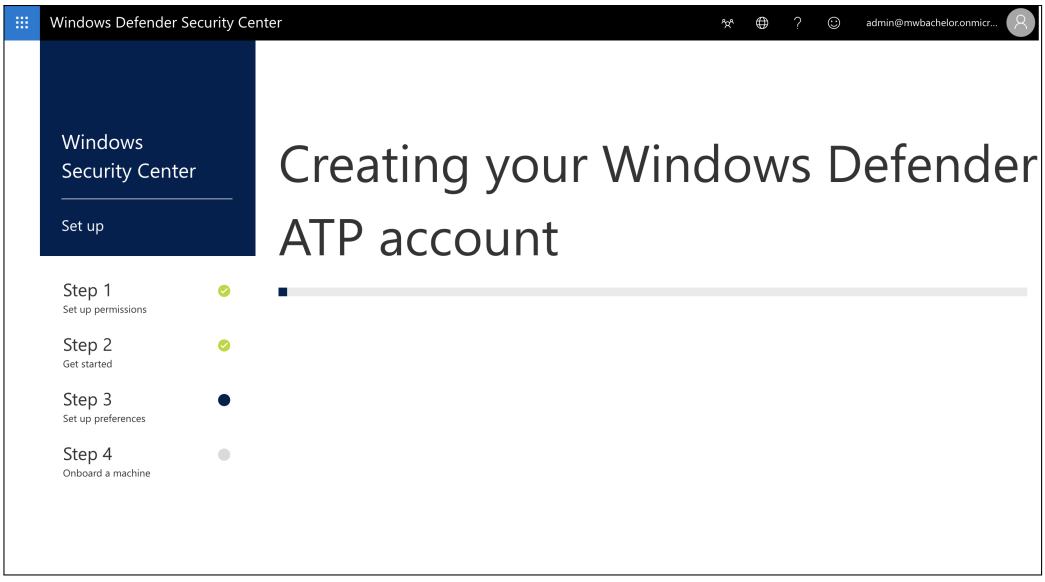
Figur 34

Veiviseren vil så advare om at flere av innstillingene ikke ville kunne endres i etterkant, og anbefale deg å gå gjennom valgene for å sikre at de er de beste for bedriften. Dersom du er usikker, trykk "Back to preferences" og gå gjennom valgene dine en gang til. Trykk så "Continue" for å opprette skyinstansen til Windows Defender ATP.



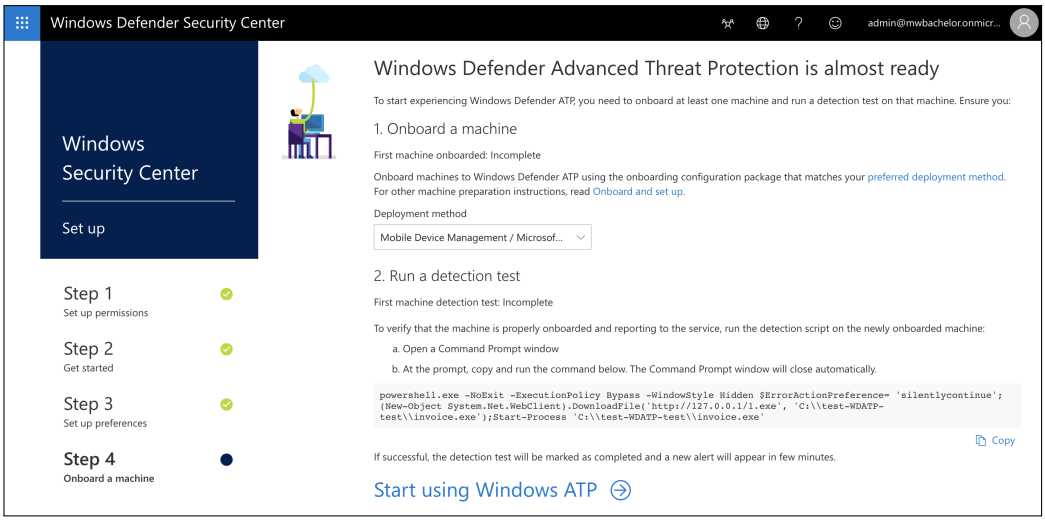
Figur 35

Veiviseren vil så begynne oppsettet av skyinstansen, og den vil lage en Windows Defender ATP-konto for din instans. Dette vil ta en stund, men du kan følge fremgangen i fremdriftslinjen, som vi ser i figur 36.



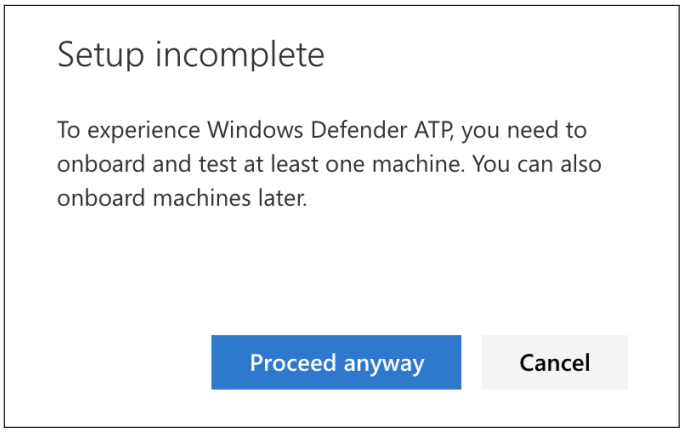
Figur 36

Siste steg i veiviseren vil være onboarding av maskiner. Det er ulike metoder å gjøre dette på, hvor man enten kan kjøre script på maskinene, noe som må gjøres på hver individuell maskin, eller sette opp en policy som automatisk legger til kompatible maskiner. Vi vil sette opp en policy, og vil ikke dokumentere bruk av script. Vi trenger ikke å legge til maskiner enda, og kan avslutte veiviseren uten å ha maskiner oboard. Trykk så "Start using Windows ATP" for å ferdigstille aktiveringen.



Figur 37

Veiviseren vil her advare om at oppsettet ikke vil være ferdig før minst en maskin er oboard. Dette kan, som nevnt tidligere, gjøres etter en har gått gjennom veiviseren. Vi velger derfor "Proceed anyway" for å avslutte aktiveringen.

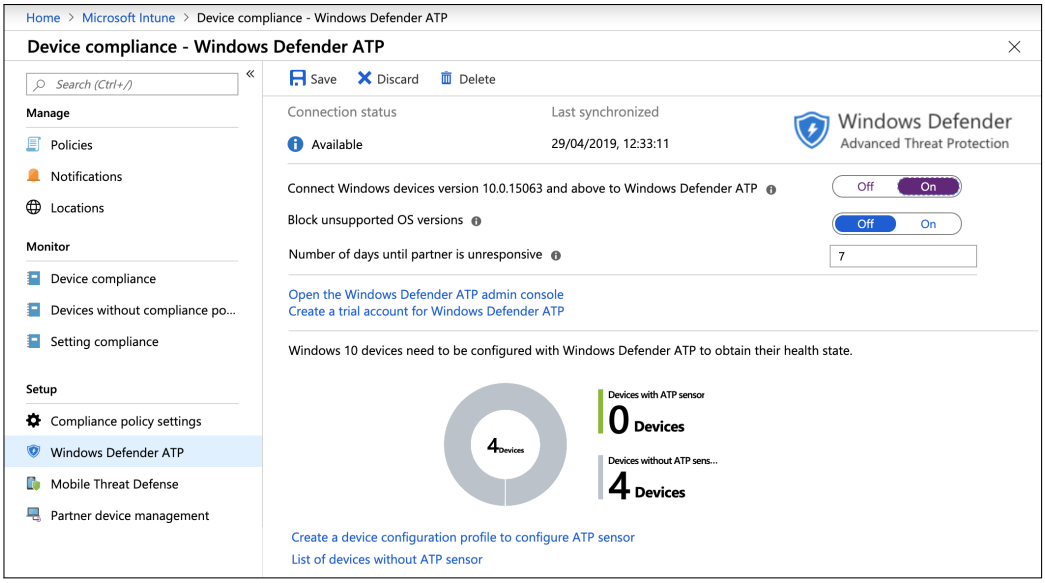


Figur 38

Veiviseren vil så dirigere oss inn i hjem-siden i sikkerhetssenteret. Som vi ser i figur 39, er det ingen aktive maskiner, og for å kunne bruke Windows Defender ATP kreves minst en enhet onboard. For at enheter skal kunne synkroniseres mellom Intune og sikkerhetssenteret må vi aktivetere koblingen mellom disse i sikkerhetssenterets innstillinger og i Intune.

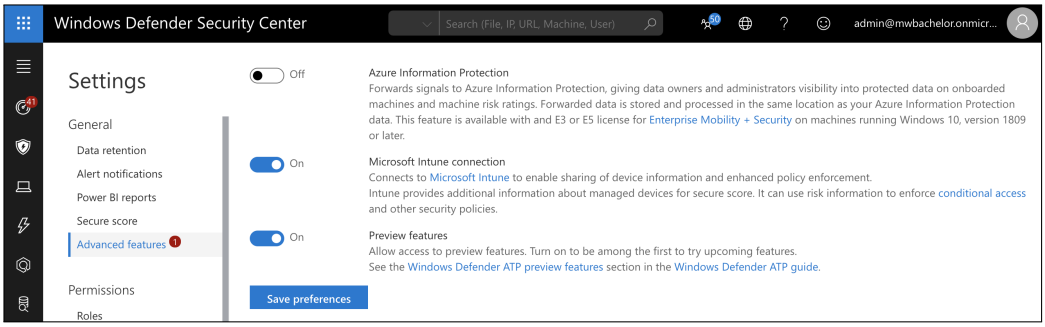
Figur 39

Tilbake i Intune kan vi, i figur 40, se at "Connection status" har blitt endret fra "Unavailable" til "Available". Dette betyr at koblingen ikke er satt opp enda, men at den er klar til å settes opp. Endre her "Connect Windows devices version *x.x.x* and above to Windows Defender ATP" fra "Off" til "On". Trykk så "Save" for å lagre endringen. Koblingen kan nå settes opp i sikkerhetssenteret.



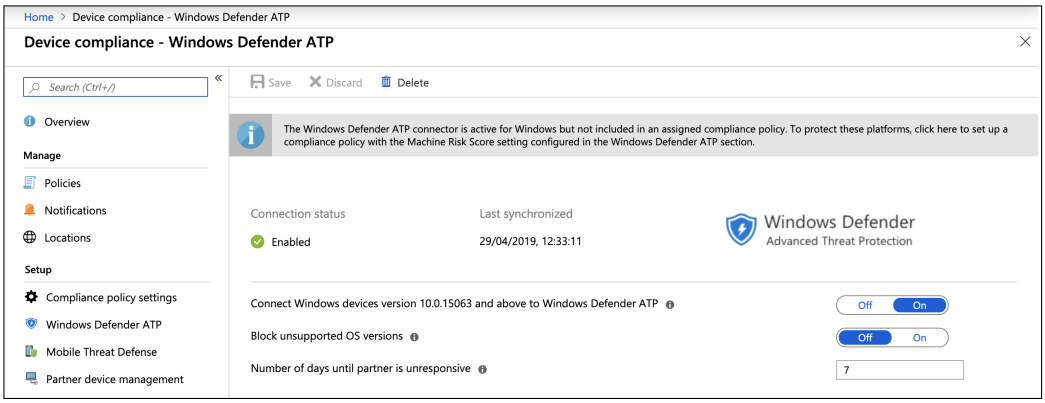
Figur 40

Tilbake i sikkerhetssenteret kan vi åpne innstillinger ved å trykke på tannhjulet på venstre side. Deretter velger vi "Advanced features", som vist i figur 41. Her skrur vi "Microsoft Intune connection" til "On", og så lagrer vi endringen ved å klikke på "Save preferences". Koblingen vil nå være satt opp, og vi kan sjekke om den er aktiv i Intune.



Figur 41

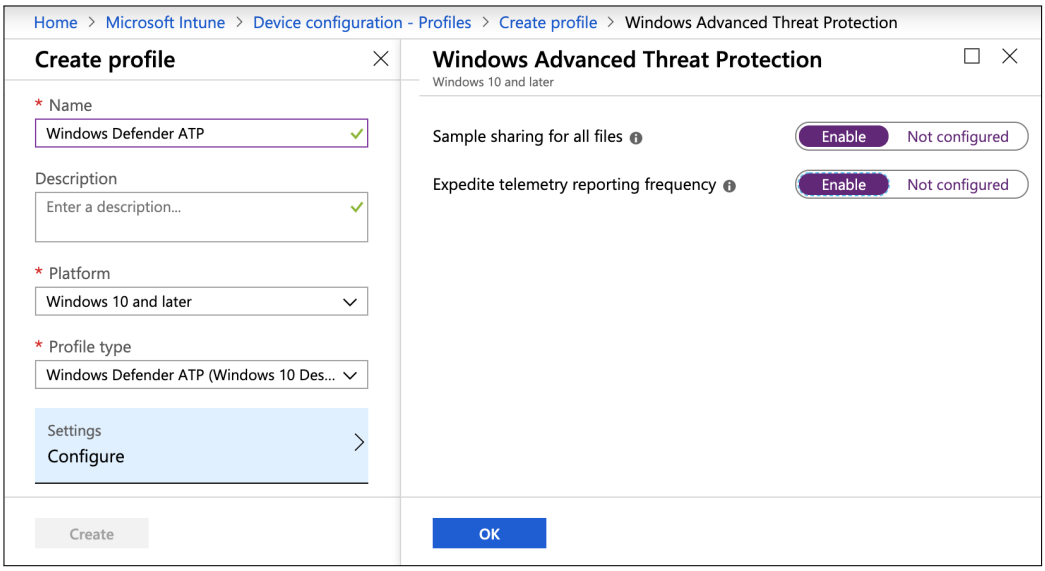
Tilbake i Intune ser vi nå at koblingsstatus har blitt endret til “Enabled”, noe som tilsier at koblingen mellom sikkerhetssenteret og Intune er oppsatt og velfungerende.



Figur 42

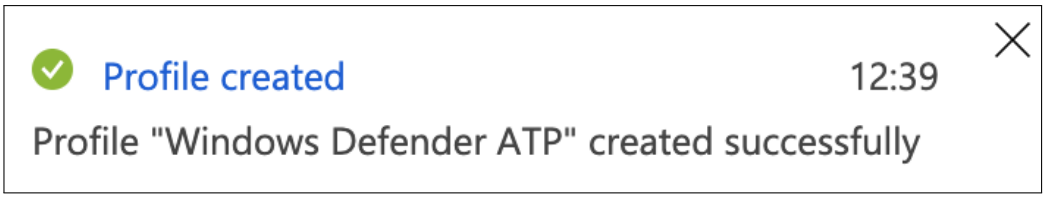
6.2 Onboarding

Nå må vi opprette en profil for onboarding av Windows Defender ATP, slik at klientdata fra ATP blir delt med sikkerhetssenteret. Naviger til enhetskonfigurasjon i Azure-portalen, "Intune", "Device Configuration", "Profiles". Trykk her "Create profile" for å opprette den nye profilen. Gi profilen et passende navn, velg "Windows 10 and later" som plattform og konfigurer innstillingene. Her velges "Windows Advanced Threat Protection" og vi velger å aktivere begge instillingene, som vist i figur 43. Trykk så "Create" for å opprette profilen.



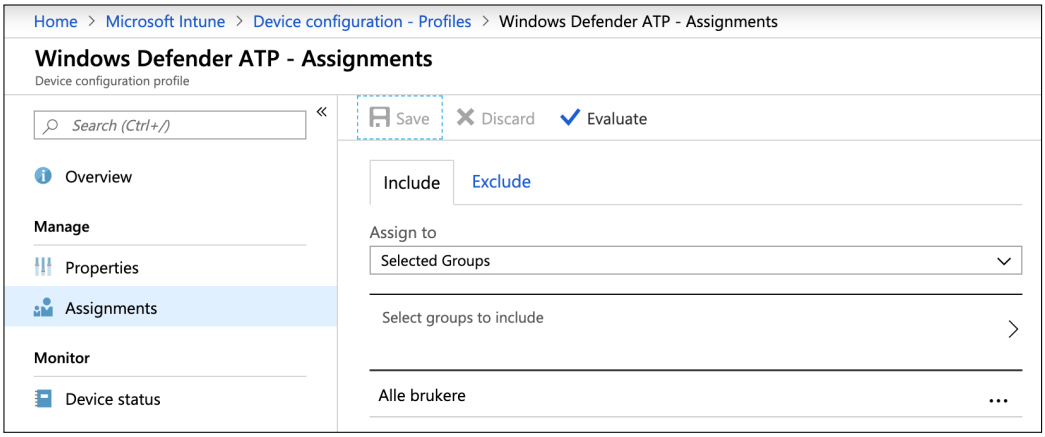
Figur 43

En notifikasjon vil så informere om opprettelse av profilen er vellykket. Som vi ser i figur 43, ble profilen opprettet uten problemet i vårt tilfelle.



Figur 44

Vi må så tilegne profilen til brukere og maskiner. Vi velger å tilegne denne til brukere, men dersom en ønsker å kun overvåke spesfikke maskiner, kan dette også gjøres. Etter å ha valgt brukergruppen/maskinene som profilen skal gjelde for, trykker vi “Save”.



Figur 45

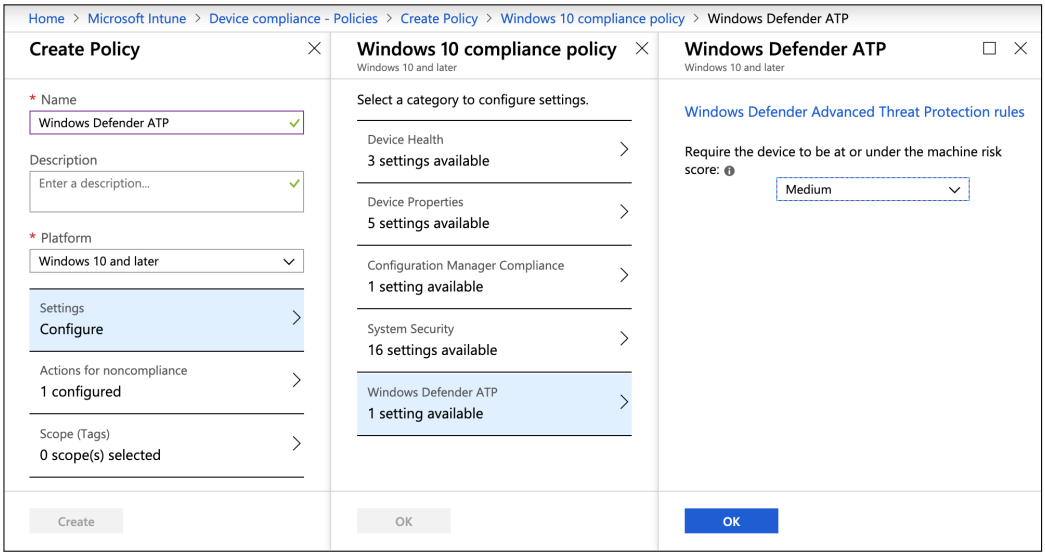
Det vil komme opp en notifikasjon som informerer om tilegningen var vellykket eller ikke. Som vi ser i figur 46, gikk tilegningen bra i vår tilfelle.

Figur 46

6.3 Compliance

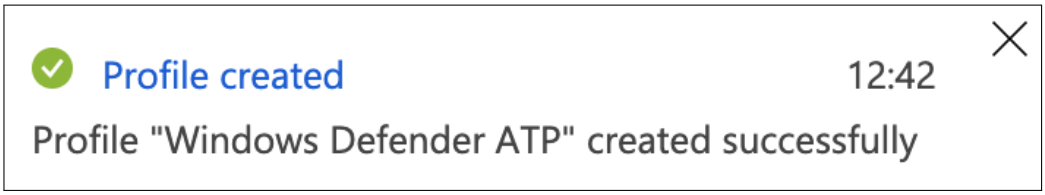
Vi må deretter opprette en policy som sier hvor stor trussel en maskin kan være under før den mister tilgang på bedriftsdata og bedriftsapplikasjoner. Naviger til compliance for enheter i Azure-portalen, “Intune”, “Device compliance”, “Policies”. Velg her “Create new policy” og begynn konfigureringen.

Gi policy et passende navn, velg “Windows 10 and later” som plattform og trykk “Configure” under innstillingene. Under “Windows Defender ATP” settes risikoen maskinen må være under før Conditional Access vil blokkere den fra tilgang på bedriftsdokumenter og bedriftsapplikasjoner. Det vil være opp til bedriften hvilke krav til risiko, om de ønsker å ha lav eller høy toleranse. Vi setter her kravet til “Medium”. Trykk så “Create” for å opprette policy.



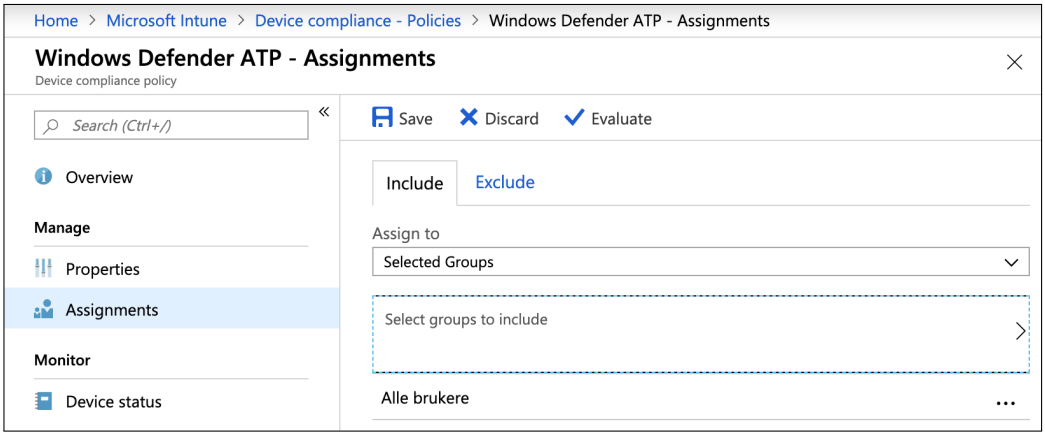
Figur 47

Det vil så komme opp en notifikasjon som indikerer om opprettelse av policy var vellykket. Som vi ser i figur 48, ble policy opprettet feilfritt i vårt tilfelle.



Figur 48

Nå må policy tilegnes brukere eller maskiner for at den skal gjelde. Vi velger å tilegne policy for alle brukere, men det vil være mulig å sette opp for mer spesifiserte grupper. Velg så "Save" for å lagre tilegningen.



Figur 49

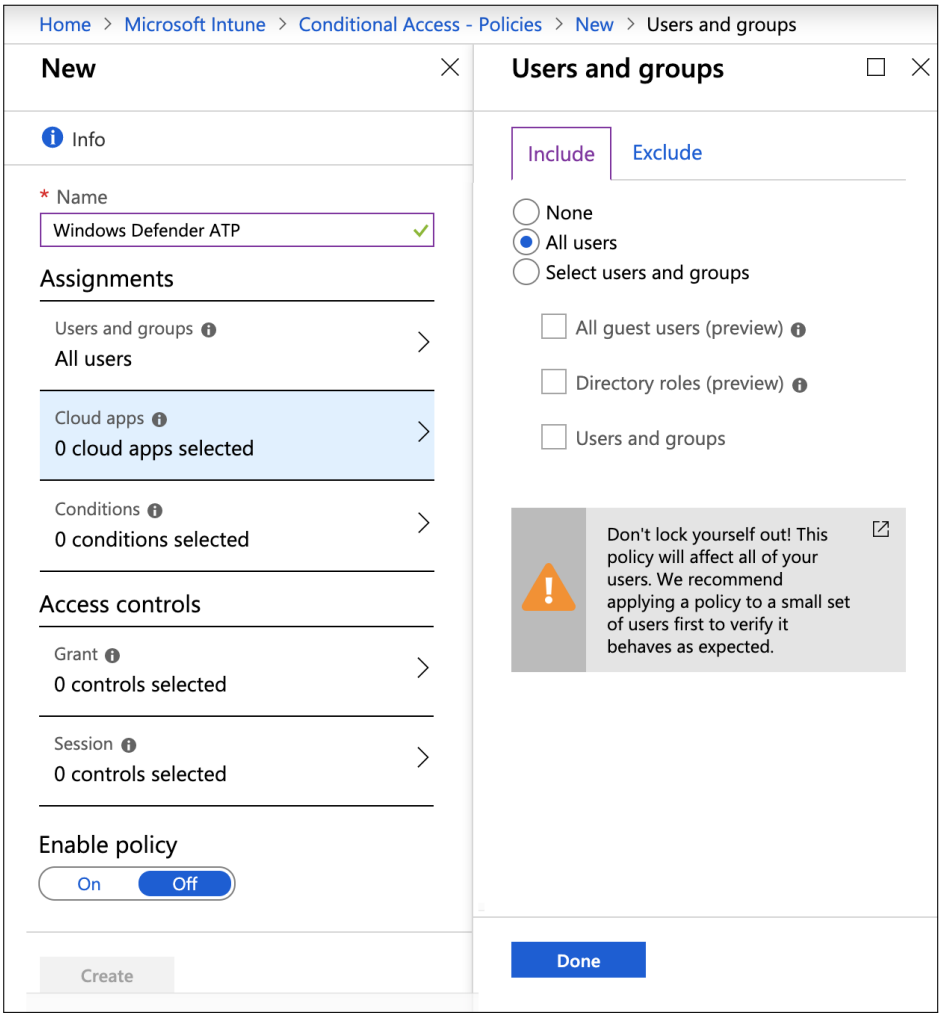
Det vil komme opp en notifikasjon som informerer om tilegningen var vellykket eller ikke. Som vi ser i figur 50, gikk tilegningen bra i vår tilfelle.

Figur 50

6.4 Conditional Access

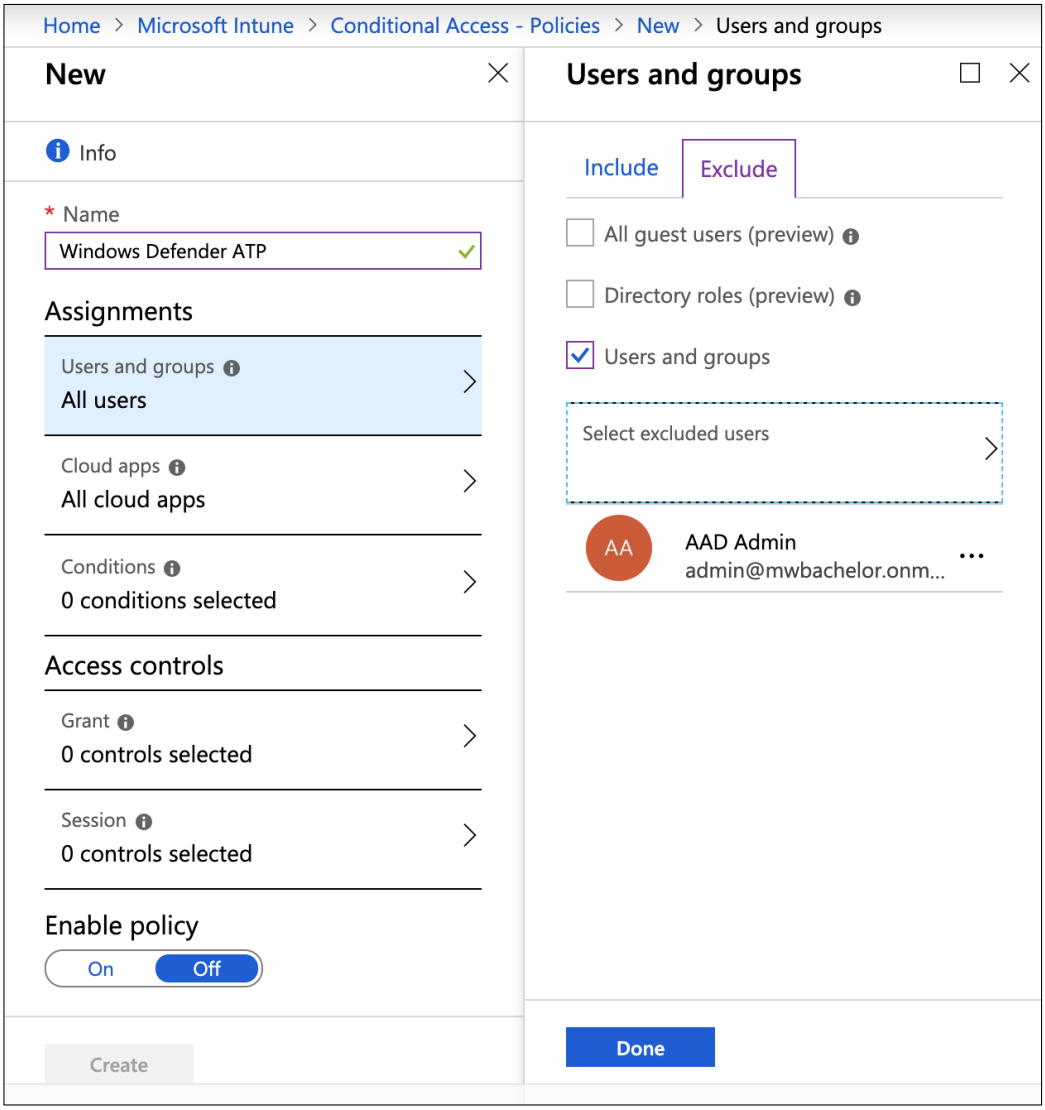
Videre må vi sette opp en policy for Conditional Access. Dette gjøres for at Conditional Access skal kunne forhindre at utsatte maskiner får tilgang på bedriftsdata og bedriftsapplikasjoner. Her er det viktig at man ekskluderer administratorer, slik at de ikke blir låst ute.

Naviger til Conditional Access i Azure-portalen, "Intune", "Conditional Access", "Policies" og velg "Create new policy". Gi policy et passende navn og begynn konfigurering av policy. Vi velger her alle brukere ved å huke av for "All users".



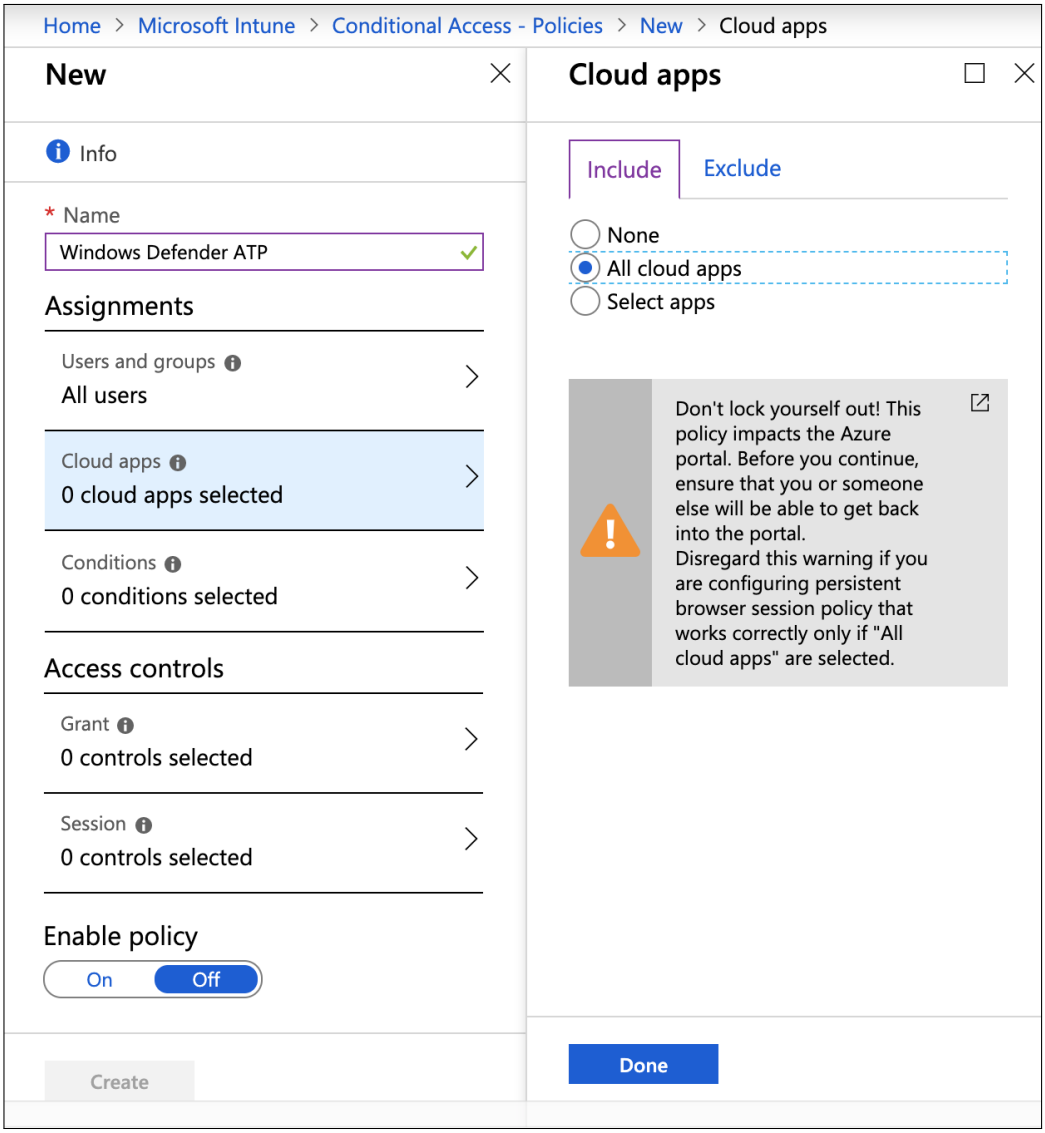
Figur 51

Her ekskluderer vi også vår globale administrator, slik at vi ikke blir låst ut under testing. Huk av for “Users and groups” under “Exclude” og velg brukere som ikke skal låses ute. Velg så “Done”.



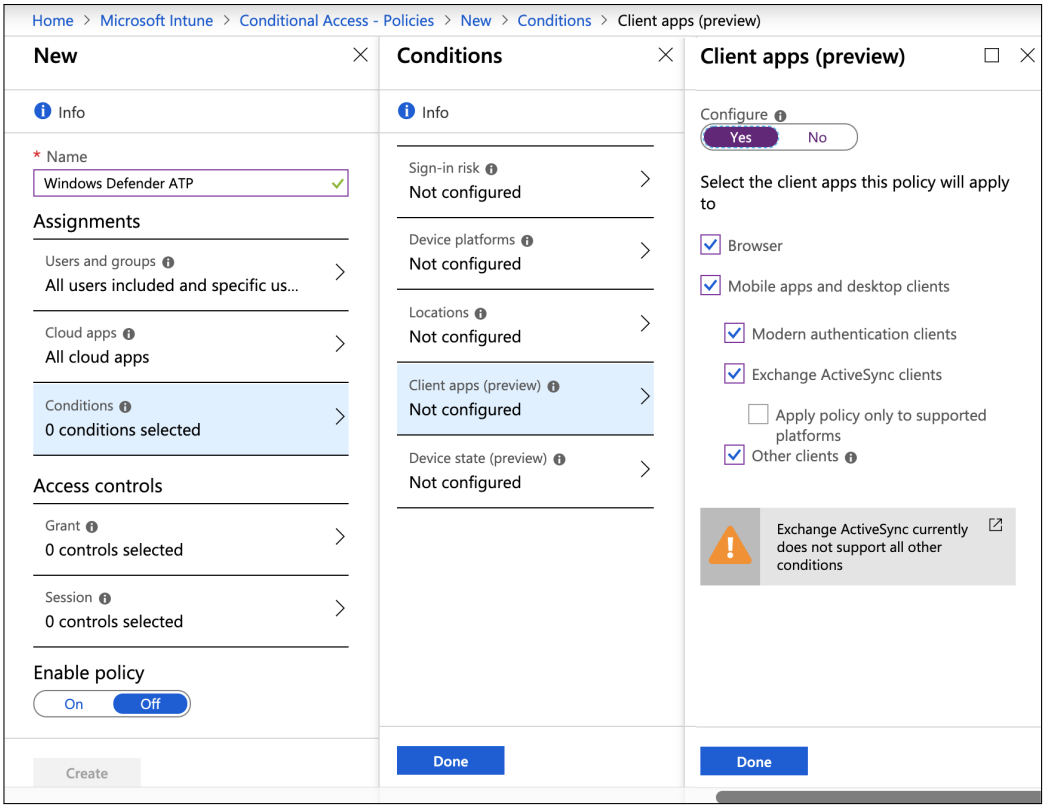
Figur 52

Vi må så velge hvilke applikasjoner brukere skal låses ut av ved risiko. Her kan en enten velge spesifikke applikasjoner, eller velge alle sky-applikasjoner. Vi velger at det skal gjelde for alle sky-applikasjoner ved å huke av for “All cloud apps”.



Figur 53

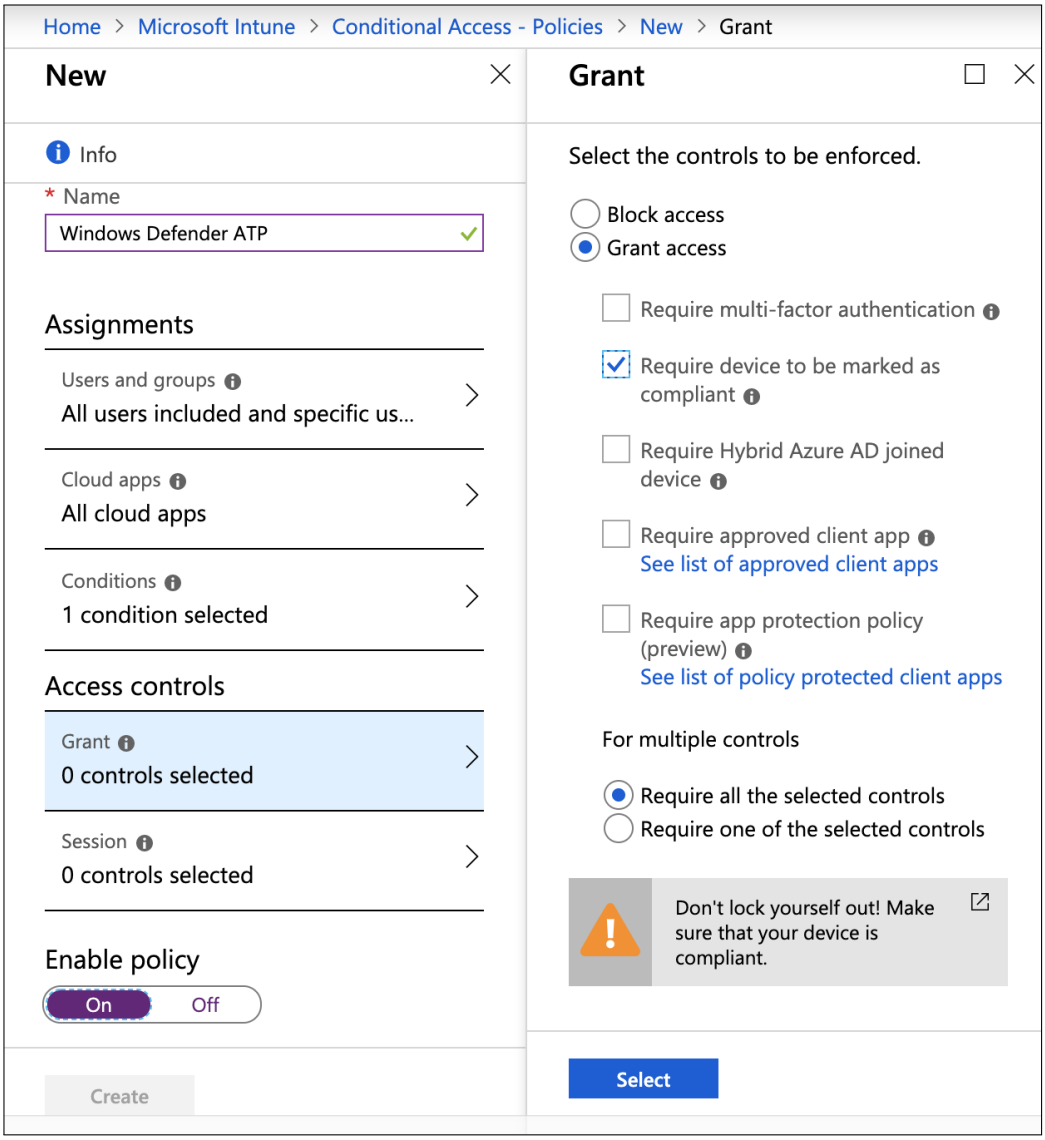
Under “Conditions” velger vi hvilke applikasjoner, nedlastet på klienten, som brukeren skal bli låst ute av ved en risiko på deres maskin. Dette er en såkalt “preview” egenskap, og vil ikke nødvendigvis fungere med alle mulige oppsett. Velg først at det skal konfigureres, så huker vi av for alle typer applikasjoner, som vist i figur 54.



Figur 54

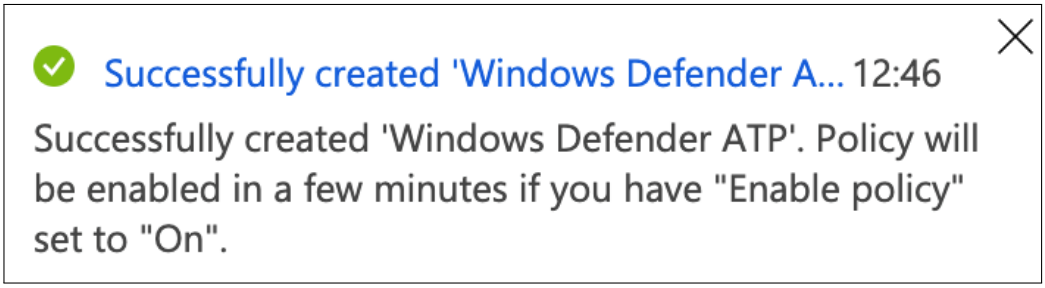
Vi må så velge når Conditional Access skal blokkere brukere ute, altså hva som skal til for at blokkeringen skjer. Under "Access Control" velger vi å huke av for "Grant Access" og under huker vi av for at enheten må være markert som "compliant". Under "For multiple controls" lar vi det stå som standard. Trykk så "Select".

Policy kan nå opprettes, men det er viktig at den aktiveres for at den skal fungere. Dette kan gjøres senere, men vi gjør det under oppsett. Under "Enable policy" velger vi å skru denne til "On", som vist i figur 55.



Figur 55

Det vil så komme en notifikasjon som indikerer om opprettelsen av policy var vellykket. Den vil også informere om at policy vil aktiveres om kort tid dersom “Enable policy” er påskrudd. Som vi ser i figur 56, gikk opprettelse av policy feilfritt.



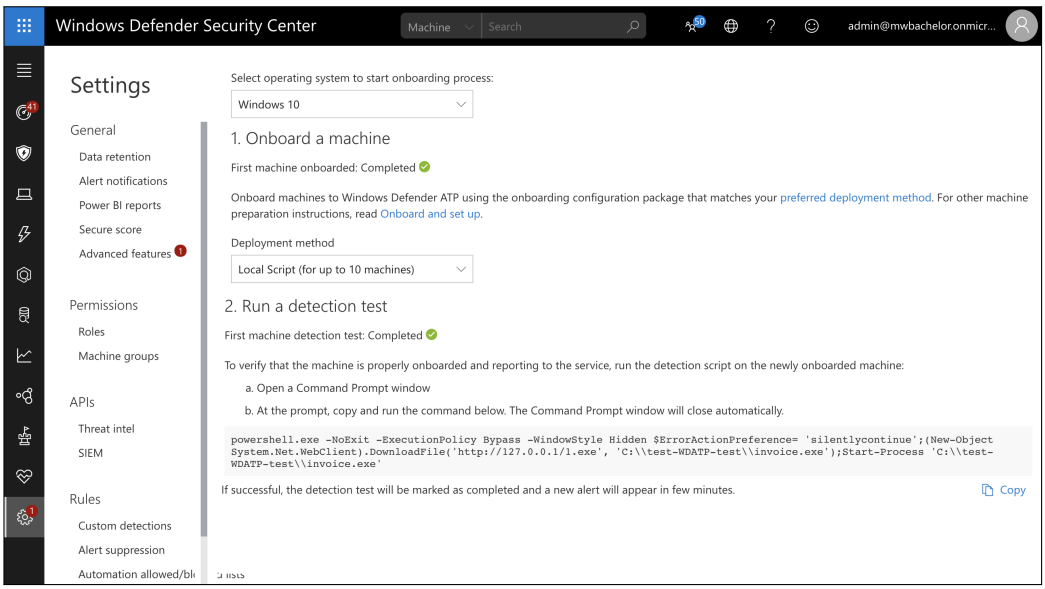
Figur 56

6.5 Detection testing

Etter å ha gjort konfigurasjon av policy og profiler i Intune, kan vi nå kjøre en test for å sjekke om enheter blir onboardet og rapporterer riktig. Denne testen vil ikke måtte kjøres på alle maskiner, kun på en maskin for å teste om måten maskiner skal oppdages fungerer som ventet. Dette vil skje gjennom en powershell-kommando som kjøres på en klientmaskin.

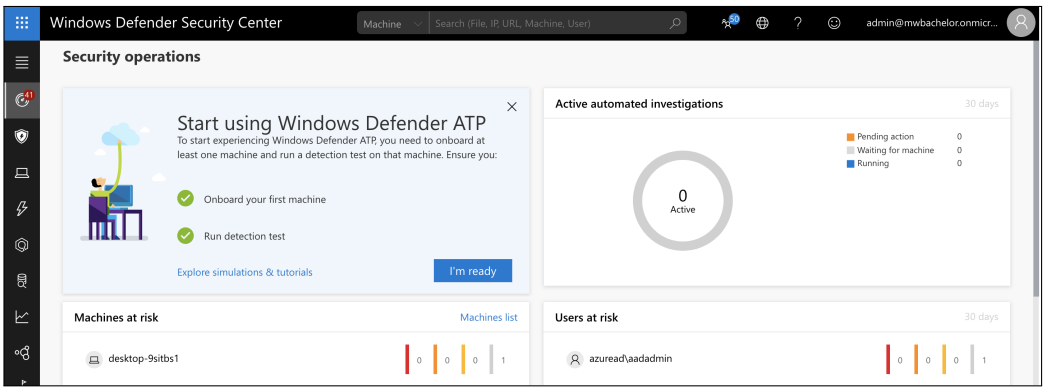
Først må vi hente scriptet i sikkerhetssenteret. Naviger til "Settings", "Machine management" i sikkerhetssenteret. Her kan vi finne innstillingene "Onboarding" og "Offboarding". Velg "Onboarding". Her velges det Windows 10 som OS, "First machine onboarded" vil ha en grønn sjekkboks hvis publiseringen av "Device Configuration" gikk bra.

Under steg to finner vi en powerhell-komando som vil teste at maskinen rapporter korrekt. Kopier komandoen til et komandovindu på en on-boardet maskin. Det skal etter hvert dukke opp en grønn sjekkboks ved steg to, som vi ser i figur 57.



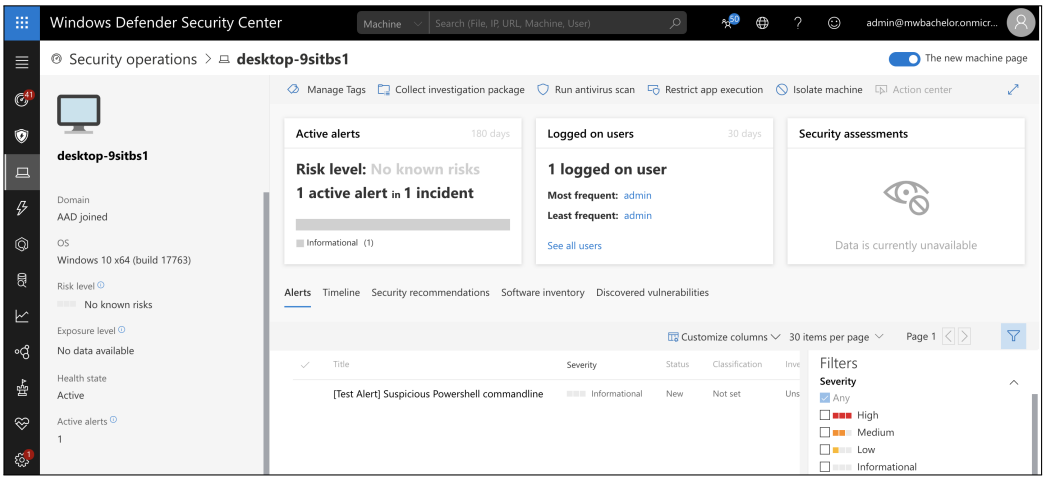
Figur 57

På sikkerhetssenterets dashboard kan vi nå se at detection test er kjørt, og at vi er klare for bruk av ATP. Maskinene vil nå dukke opp i sikkerhetssenteret, og en kan se om de er utsatt for noen risiko eller om det foregår en trussel mot disse.



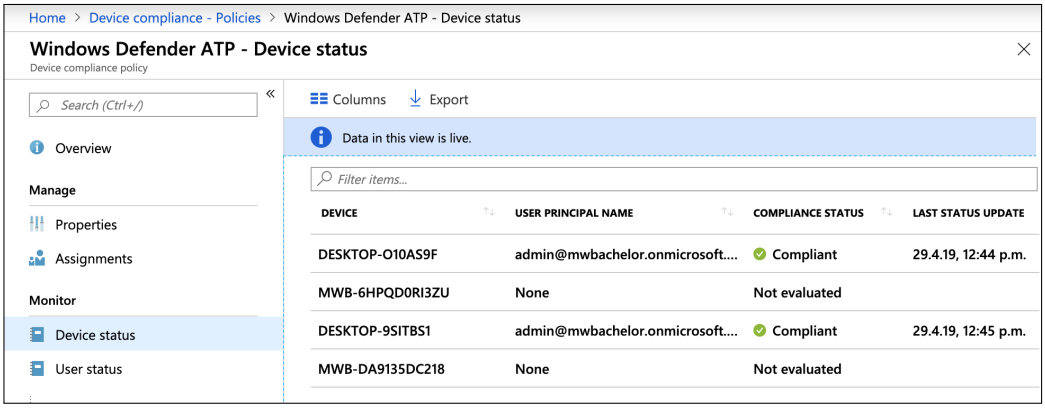
Figur 58

Trykker vi oss inn i maskinen vi kjørte detection test på, kan vi se at det å kjøre kommandoen ble oppdaget som en varsling i sikkerhetssenteret. Varselet, som vi ser i figur 59, beskriver hendelsen som en test, og at det er suspekt bruk av Powershells kommandolinje.



Figur 59

Tilbake i Intune, vil enhetene nå sjekkes for compliance. Som vi ser i figur 60, er to av våre enheter compliant. De resterende enhetene er ikke evaluert enda. Vi kan også se når siste oppdatering ble sendt fra maskinen til Intune og sikkerhetssenteret.

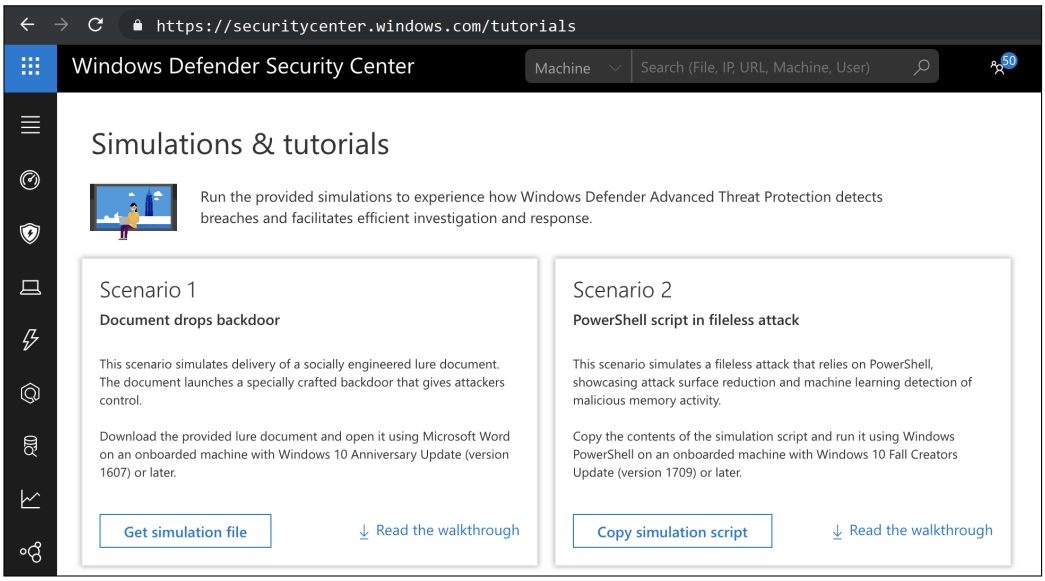


Figur 60

6.6 Demo

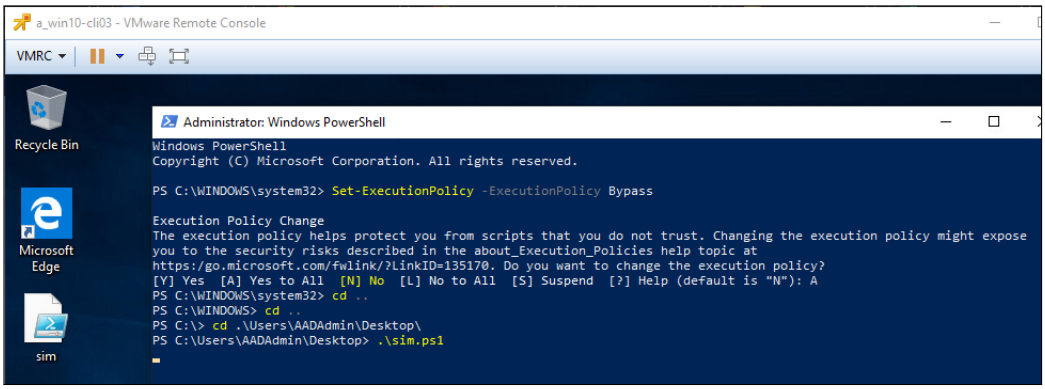
For å teste at Windows Defender ATP fungerer som det skal, kan vi ta i bruk script laget av Microsoft for å trigge en alarm og øke trusselnivået på en klientmaskin. Dersom Windows Defender ATP virker, vil et varsel dukke opp i sikkerhetssenteret og Conditional Access skal blokkere brukeren fra å få tilgang på bedriftens data og applikasjoner.

Naviger til "Simulations & tutorials" inne i sikkerhetssenteret. Velg et scenario, og kopier script ved å trykke "Copy simulation script". Vi velger scenario nummer 2 og kopierer scriptet over til en onboardet maskin.



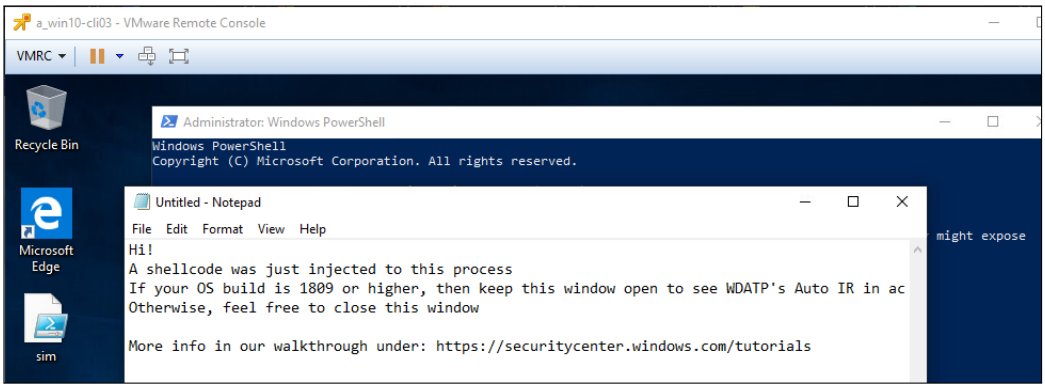
Figur 61

Inne på maskinen skal vi nå kjøre scriptet. Som vi ser i figur 62, lagret vi scriptet som “sim.ps1”, men det kan også limes rett inn i Powershell. Kjør nå scriptet.



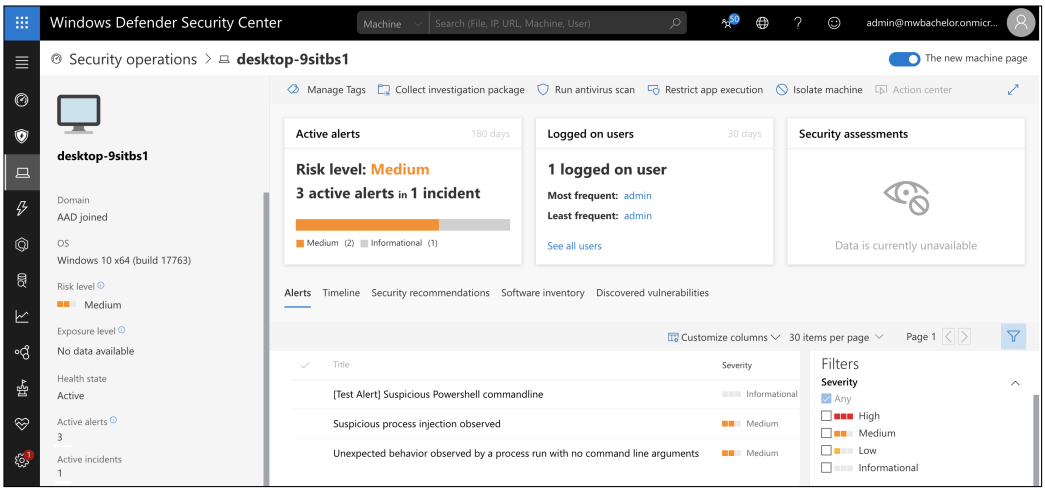
Figur 62

Etter kort tid åpnes en notisblokk med informasjon om hva man skal gjøre avhengig av OS-versjon på maskinen. Siden vi kjører 1809, og txt-filen, som vist i figur 63, ber oss holde vinduet åpent, lar vi vinduet være åpent.



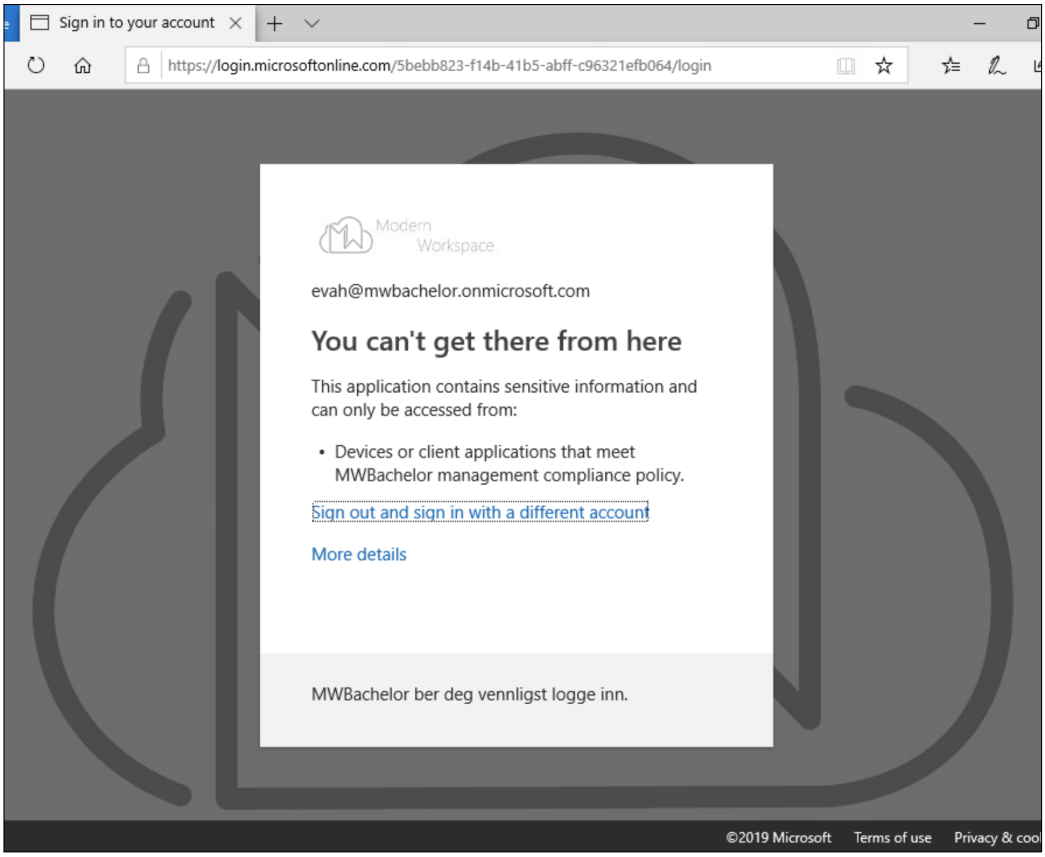
Figur 63

Tilbake i sikkerhetssenteret kan vi nå se at risikonivået er økt til Medium for denne maskinen. Siden vi tidligere spesifiserte at et risikonivå lik medium eller høyere skulle sperre brukere ute, skal brukere nå ha mistet tilgang på bedriftsdata og bedriftsapplikasjoner.



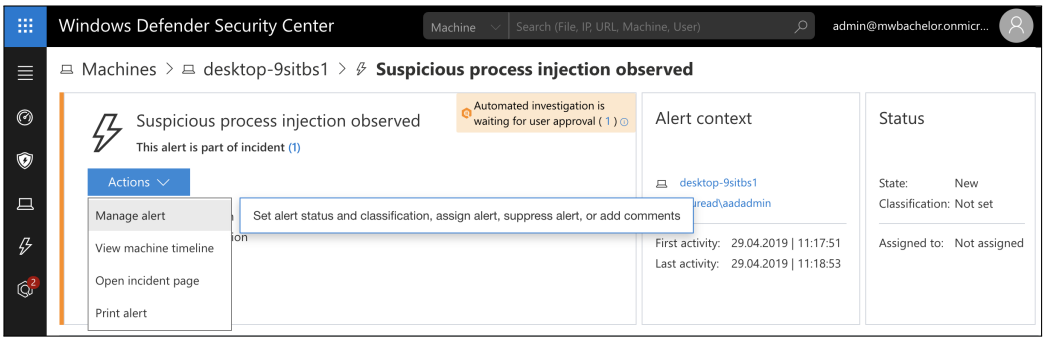
Figur 64

Vi forsøker å logge inn på SharePoint i nettleseren på maskinen som har økt risikonivå, men vi blir ikke sluppet inn. Som vi ser i figur 65, har Conditional Access blokkert vår tilgang på SharePoint på grunn av maskinens risikonivå. Legg også merke til at vi ikke bruker administratorbrukeren, da vi ekskluderte denne fra å miste tilgang.



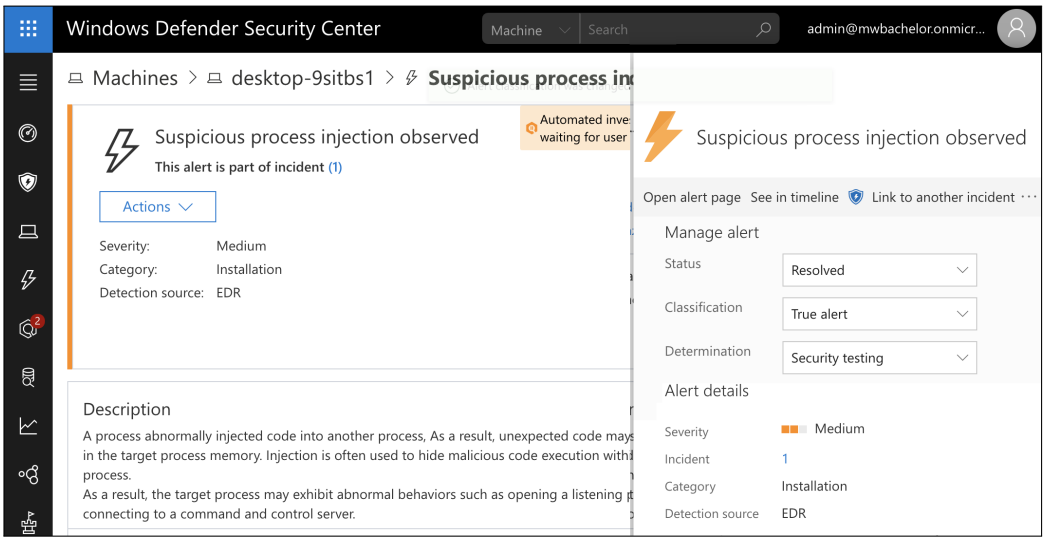
Figur 65

Siden dette er en test, kan vi nå frikjenne maskinen og fjerne varselet i sikkerhetssenteret. Trykker vi på varselet og "Manage alert" under "Actions" kan vi administrere varselet.



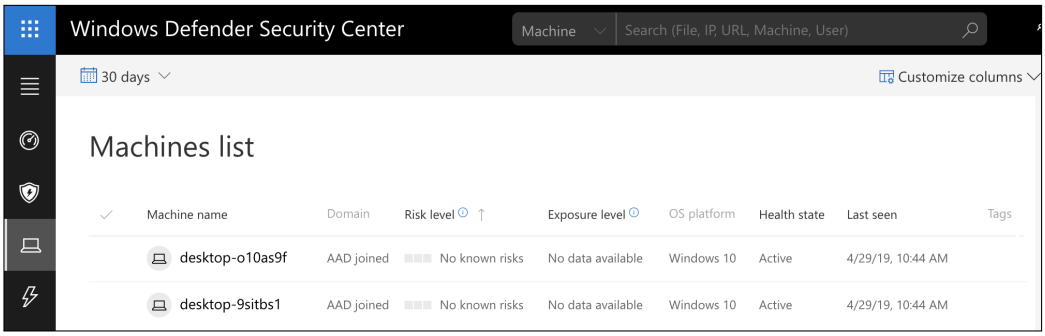
Figur 66

Et vindu åpnet seg, og vi setter statusen til "Resolved", klassifisering til "True alert" og bestemmelsen som "Security Testing". Dersom dette er en realistisk trussel, bør en først fjerne selve trusselen fra maskinen før en setter det som løst i sikkerhetssenteret. Når alle varslene er løst, skal risikonivået gå ned til normalnivå.



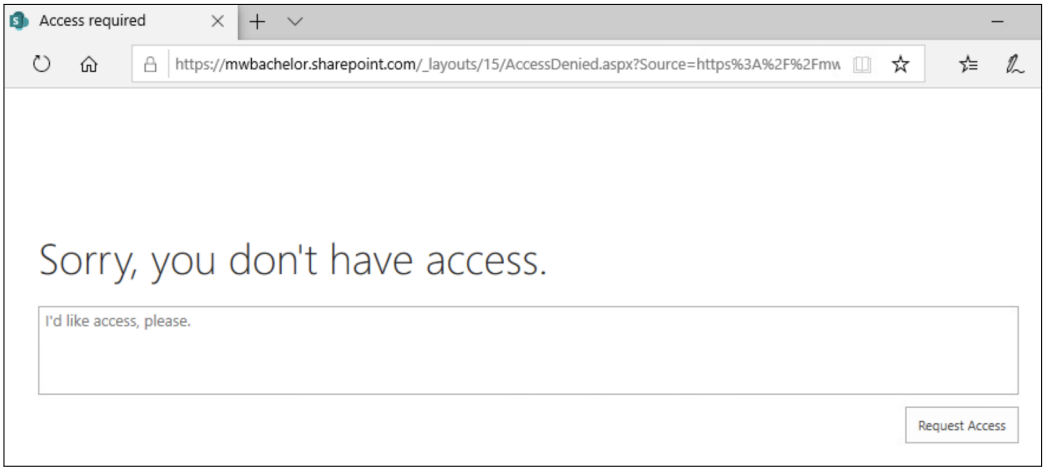
Figur 67

Som vi ser i figur 68, vil maskinen nå ha et normalt risikonivå.



Figur 68

Prøver vi å logge inn på SharePoint på den samme maskinen vil vi nå komme inn. Som vi ser i figur 69, er vi ikke lengre blokkert av Conditional Access, men siden brukeren ikke har lisens til bruk, har den ikke tilgang på SharePoint uansett.

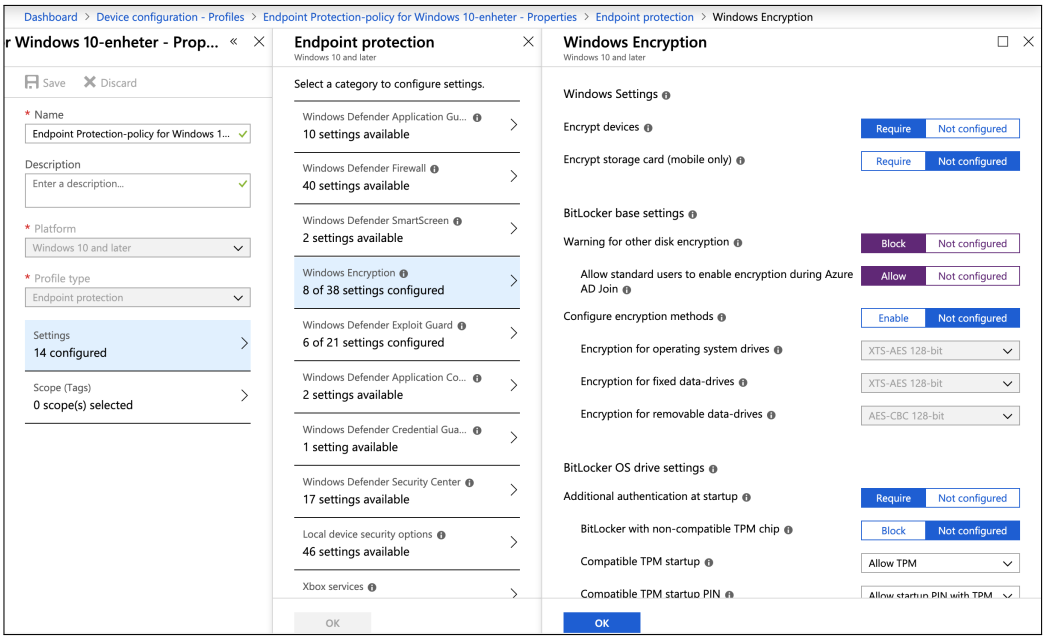


Figur 69

7 BitLocker

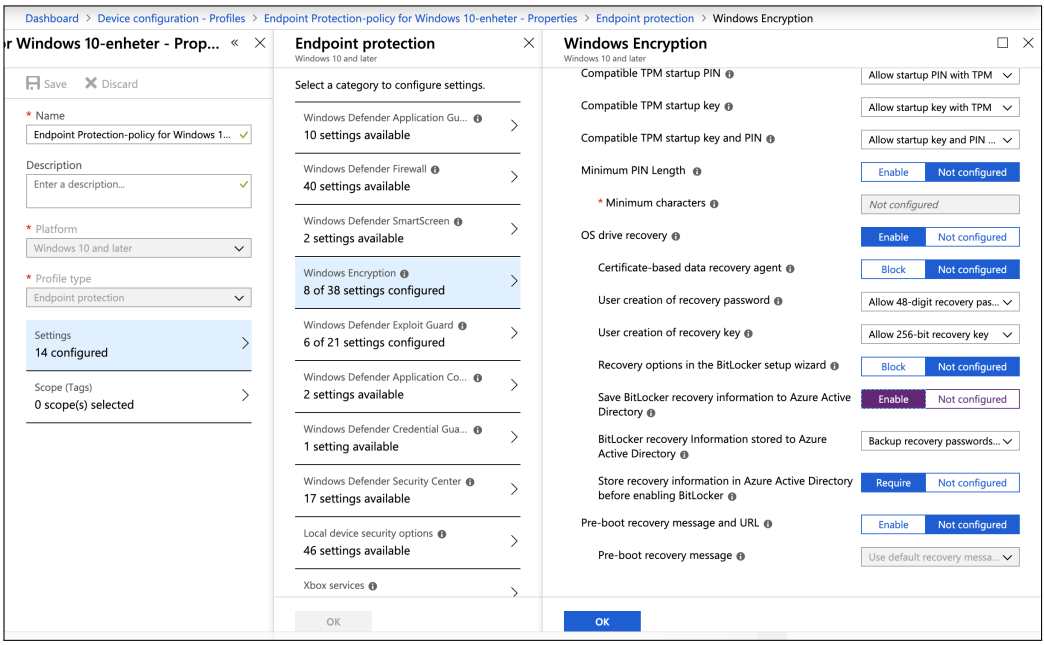
BitLocker er Microsofts eget verktøy for kryptering på Windows-enheter. Krypteringen gjør at data som er lagret på harddisken ikke vil være brukbar for personer uten et passord eller en gjenopprettingsnøkkel. Passordet er noe kun brukeren selv vet og gjenopprettingsnøkkelen er kun tilgjengelig for brukeren gjennom skyen. Dette hindrer bedriftsdata fra å komme på avveie dersom en bruker skulle glemme enheten sin eller få den stjålet.

I vårt tilfelle eksisterte det allerede en policy for Endpoint Protection, men det anbefales å opprette en egen policy for Windows Encryption. Velg "Windows 10" som plattform og "Endpoint protection" som profiltype. Naviger til "Windows Encryption" i profilens innstillinger. Her velges det "Block" for varsling om kryptering, og "Allow" for å la standardbrukere kryptere disken. Med disse innstillingene vil krypteringen automatisk starte stille i bakgrunnen, uten at brukeren merker noe.



Figur 70

Lengre ned i profilen velger vi å lagre gjenopprettingsnøkkelen for BitLocker i Azure AD. Avslutt med å trykke ”OK”, ”OK”og Save”.



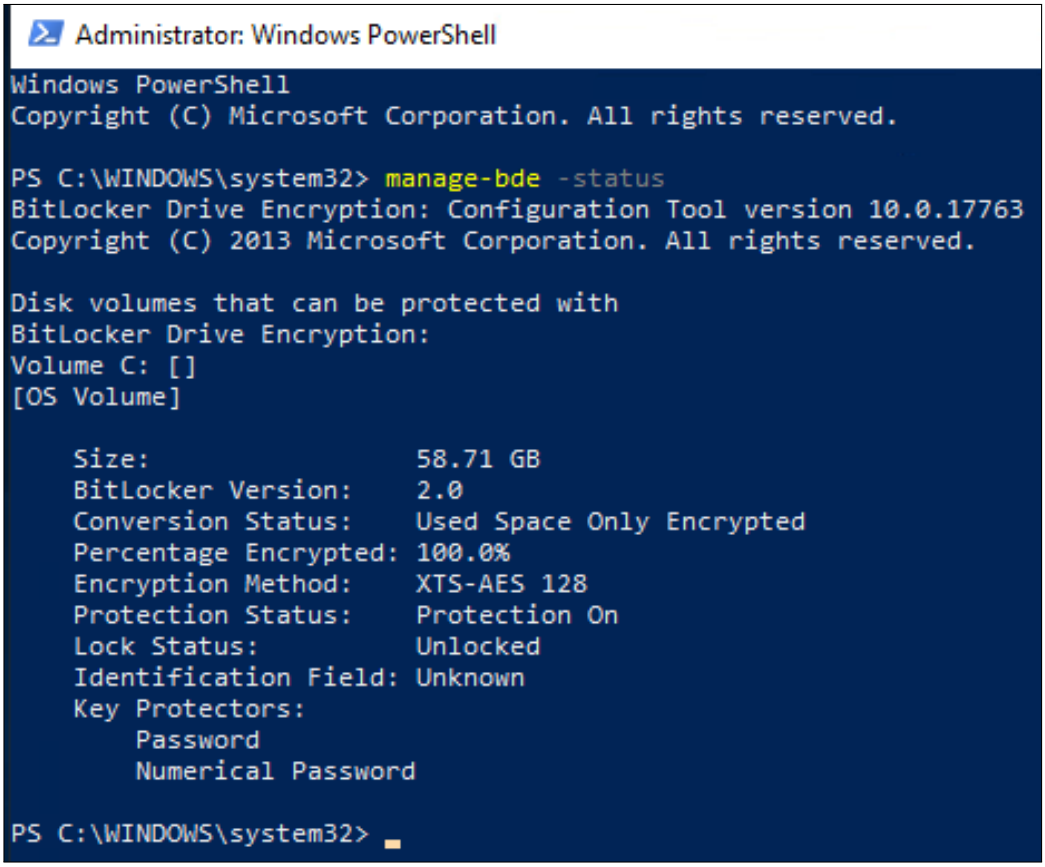
Figur 71

Der vil dukke opp et varsel, som i figur 72, som forteller om noe gikk galt. I dette tilfellet gikk alt bra.

Figur 72

Videre må en tilegne, eller “Assign”, profilen til en bruker/maskin-gruppe for at den skal tiltre.

På en klient som har fått profilen tildelt kjøres kommandoen “manage-bde –status”. Sjekk resultatet og bekreft at “Protection Status” er på og at “Percentage Encrypted” øker. Kjøring av kommandoen kan ses på figur 73.



Figur 73

Referanser

[1] Microsoft. *What's conditional access?* 2018. URL: https://docs.microsoft.com/en-us/intune/conditional-access (sjekket 03.05.2019).

[2] Microsoft. *Enforce compliance for Windows Defender ATP with conditional access in Intune*. 2019. URL: https://docs.microsoft.com/en-us/intune/advanced-threat-protection (sjekket 03.05.2019).

Modern Workspace - Sluttrapport

v.0.4

Eskil Uhlving Larsen Magnus Reitan Lien

eskilul@stud.ntnu.no magnus.r.lien@ntnu.no

20. mai 2019

1 Forord

Informatikk med spesialisering i drift av datasystemer er en studieretning med fokus på et læringsutbytte som bygger kompetansen etterspurt i markedet. Her får studenter bred erfaring innen infrastrukturen som driver dagens IT-verden, og nær kontakt med programvaren og maskinvaren næringslivet avhenger av.

Prosjektets hensikt er å få en helhetlig, teknisk, forståelse for konseptet Modern Workspace. I løpet av prosjektet har prosjektgruppen fått innsikt i hva som inngår i begrepet Modern Workspace. De har bygget en forståelse for at fokuset ligger på personene som skal ta i bruk denne nye arbeidsplassen og ikke nødvendigvis det som anses som avgjørende faktorer i tradisjonelle IT-prosjekt. Gruppen har også fått en forståelse for hva som bygger opp Modern Workspace, med skyapplikasjoner, enhetsadministrasjon, enhetssikkerhet, applikasjonssikkerhet og enhetsregistering, som alt kan konfigureres enkelt i skyen.

Vi i prosjektgruppen ønsker å rette en stor takk til våre veiledere Stein Meisingseth og Marius André Langseth-Nilsen, som har delt sin kompetanse og gitt uvurderlig tilbakemelding i løpet av prosjektets gang. Vi ønsker også å rette en takk til bedriften ATEA for muligheten til å jobbe med prosjektet og for den inkluderende atferden vi opplevde på arbeidsplassen.

Revisjonshistorie

Tabell 1: Revisjonshistorie

Dato	Ver.	Beskrivelse
07.05.2019	0.1	Dokument opprettet, forord skrevet, oppgavebeskrivelse skrevet
08.05.2019	0.2	Skrevet litteratur for prosjektet, maskinvare brukt i prosjektet, arbeidsfordeling, dokumentasjon for prosjektet, det som gikk bra, det som gikk dårlig, hvordan tekniske problemer ble løst og påbegynt måloppnåelse
09.05.2019	0.3	Skrevet måloppnåelse, arbeidsflyt og planlegging, systemets begrensninger, timeregnskap, betraktninger i ettertid og videre arbeid. Mindre revisjon av tekst og retting av grammatiske og språklige feil.
20.05.2019	0.3	Forord ferdigstilt for levering.

Innhold

2 Oppgavebeskrivelse

En bedrift med 500 ansatte jobber i dag på en tradisjonell arbeidsflate. For å få tilgang på applikasjoner og filer må de være på kontoret. Maskinene driftes gjennom SCCM, og er en del av lokal AD. Bedriften har en ny IT-strategi som sier "Cloud first", og de vil designe en ny løsning basert på MS Azure som leveringsplattform. De har derfor kjøpt inn 400 M365 E3-lisenser og 100 M365 E5-lisenser til sine ansatte. De vil bygge hele den digitale arbeidsflaten på M365, men de ønsker også en måte å forflytte seg fra den tradisjonelle plattformen til Azure-skyen.

Prosjektet vil sees på som et implementasjonsprosjekt.

2.1 Presentasjon av oppdragsgiveren

ATEA er et internasjonalt konsern med rundt 7000 ansatte fordelt over 7 land. De sysselsetter 1700 personer i Norge spredt over 24 kontorer, med tilstedeværelse ifra Alta i nord til Kristiansand i sør. ATEA har et mål om å bruke sin kompetanse innen IT til å være med på byggingen av fremtidens samfunn gjennom teknologi. De ønsker også å være bærebjelken private og statlige foretak kan støtte seg til når de utfordres av et stadig økende IT-behov. Prosjektgruppens kontaktperson innen ATEA var Marius André Langseth-Nilsen, som er leder for Modern Workspace-teamet hos ATEA Trondheim.

3 Hvordan ble oppgaven løst

3.1 Litteratur brukt i prosjektet

I situasjoner hvor det har vært behov for faglitteratur har prosjektgruppen, i all hovedsak, funnet dokumentasjon på Microsofts nettsider. Ved feilsøking har dette foregått på tvers av mange ulike nettsider. Prosjektgruppen har også gjennomgått flere videoer produsert av både Microsoft og selvstendige innholdsutviklere. Fysisk faglitteratur, i form av bøker, har ikke blitt brukt i noen faser underveis i prosjektet.

3.2 Maskinvare brukt i prosjektet

Magnus:

- MacBook Pro 13.3” (2016)
- Egenbygd stasjonær datamaskin

Eskil:

- Samsung Series 7 15.6” (2012)
- Egenbygd stasjonær datamaskin

3.3 Programvare brukt i prosjektet

Til rapport- og referatskriving ble disse programmene brukt:

- Microsoft Word (Tekstbehandlingsprogram)
- OverLeaf (Online LaTeX-editor)
- SharePoint (Lagringsområde for fildeling)

Til presentasjon ble disse programmene brukt:

- Microsoft PowerPoint (Bildepresentasjonsprogram)
- Evt videolagingsprog

Til bilderedigering på figurer ble disse programmene brukt:

- Preview (Framvisnings- og redigeringsprogram for bilder på Mac)

- Paint (Bilderedigeringsprogram på Windows)
- Paint 3D (Bilderedigeringsprogram på Windows)

Til diagrammer ble disse programmene brukt:

- Microsoft Project (Programvare for prosjektstyring)
- Draw.io (Diagram- og vektorgrafikkverktøy)

3.4 Arbeidsfordeling

Arbeidsfordelingen underveis i prosjektet har ikke fulgt noen standard, og har endret seg avhengig av dagsorden. Oppgavene ble fordelt uformelt ut ifra gjenværende arbeid på rapporter, og det er dermed ingen egen oversikt over hvem som har gjort hva, utover det timelistene viser.

Gjennomgående for prosjektet er at prosjektgruppen drev selvstendig med orientering rundt fagstoff, ofte tilknyttet forskjellige deler av implementasjonen. Implementeringsfasene og annet oppsett ble gjort i plenum, på storskjerm, for at begge gruppemedlemmene skulle få utbytte av arbeidet. Dette gav prosjektgruppen mulighet til å dele på opparbeidet kunnskap og diskutere løsninger. Bilder ved implementasjonen ble også tatt i plenum. Deretter har prosjektgruppen sammen jobbet med dokumenteringen.

Rapportskriving. Alle dokumentene er skrevet sammen, hvor det ofte er blitt skrevet på ulike deler av dokumentet samtidig. Til slutt har prosjektgruppen gjennomgått dokumentet sammen, og kommet med spørsmål og forslag til mulige endringer. Ingen av dokumentene er skrevet av kun en prosjektdeltaker alene.

Dokumentasjon og billedtakning. All dokumentasjon gjennom hele prosjektet har blitt gjort i plenum på en storskjerm. Dette betyr at begge prosjektdeltakerne har sett og gjennomgått alt som blir omtalt i driftsrapporten. Deler av billedtakningen ble gjort individuelt i situasjoner hvor bilder har blitt i dårlig kvalitet eller måttet tas på nytt av andre grunner.

Diagrammer. Diagrammene ble alle planlagt i plenum, og brorparten av diagrammene ble utarbeidet i samarbeid. Noen av diagrammene ble laget individuelt, men er et resultat av felles planlegging og tilbakemeldinger.

Presentasjon. Presentasjonen ble gjort i fellesskap og er et resultat av samarbeid mellom prosjektdeltakerne.

3.5 Dokumentasjon for prosjektet

Prosjektgruppen ønsket å være oversiktlig og grundig når dokumentasjon ble utarbeidet for prosjektet. Derfor har et sterkt fokus blitt holdt på å holde oversikt over datoer arbeid har blitt utført, skrive timelister og omfattende møtereferater. Innholdet i de ulike rapportene er også utarbeidet for et best mulig resultat. Dette ble gjort ved å finlese alle dokumentene og kvalitetssikre at det som ble skrevet underveis samsvarte med den ønskede ordlyden.

Forstudierapport. Skrevet i Word og lagt over i LaTeX for å få et best mulig resultat. Denne følger IIEs standard-oppsett for en forstudierapport.

Designdokument. Skrevet i Word og lagt over i LaTeX for å få et best mulig resultat. Dokumentet følger IIEs standard-oppsett for et designdokument.

Driftsdokument. Skrevet i Word og lagt over i LaTeX for å få et best mulig resultat. Dokumentet har blitt delt opp i flere ulike driftsdokumenter, dette for å samle ulike tema i et dokument og for å gjøre dokumentet mer oversiktlig. I endelig innlevering er dokumentene satt sammen til et stort dokument.

Timelister. Timelistene er satt opp i Excel på ukesbasis. De er oppdelt slik at en ukesoversikt tar et helt ark, og har notat med hva som blir gjort den dagen. Timelisten har også et ark med totalt antall timer, for å gi en total-oversikt for alle ukene.

Ukesrapporter. Ukesrapportene blir skrevet enten første dag i den følgende uken, eller siste dag i den pågående uken som den omhandler. Her beskrives kort hva som har blitt gjort foregående uke, hva som skal gjøres kommende uke, ting prosjektgruppen er usikre på, eventuelle milepæler som ble oppnådd og notater hvis det er noe som må forklares den uken.

Møtereferater. Prosjektgruppen har hatt sterkt fokus på å skrive grundige referater som gjenspeiler møtets atmosfære og inneholder alt som sies på møtene. Møtereferatene inkluderer hvor det foregikk, hvem som møtte opp, agenda, saker, hvem som var sekretær for møtet og en godkjenning av referatet.

4 Gjennomføring av prosjektet

Prosjektgruppen fikk tildelt et eget møterom hos ATEA for å jobbe med prosjektet. Møterommet Ringrevble reservert alle dager i uken gjennom hele prosjekttiden, bortsett fra tirsdager og noen unntak. Tirsdager var oftest prosjektfrie dager, da prosjektgruppen hadde annet arbeid eller undervisning på disse dagene. Prosjektgruppen arbeidet sammen i tidsrommet mellom 08:30 og 15:30. Utover dette ble det arbeid på eget initiativ hjemmefra.

Som en prosess har prosjektet i all hovedsak etter planen og arbeid har blitt ferdig i umiddelbar nærhet til milepæler satt i tidsplanen. Det har oppstått hindre underveis som har fått konsekvenser for innholdet i driftsdokumentet, noe som vil beskrives nærmere senere i rapporten.

4.1 Arbeidsflyt og planlegging

Prosjektet hadde på forhånd satte rammer knyttet til innlevering og tidsbruk for prosjektet. Tidsrammene var på 500 timer (+/- 5%) per student, med endelig innleveringsdato satt til 20. mai. Med denne informasjonen i minne ble det utformet et GANTT-diagram med datoer og milepæler som skulle stå som en overordnet veiledning for prosjektgruppen. Planleggingen ble gjort på forhånd og prosjektgruppen så aldri et behov for å gjøre endringer på verken den overordnede planen eller diagrammet underveis i prosjektet.

4.1.1 Planlagt tidsforbruk

Task Name	Duration	Start	Finish
MS Modern Workspace	**91 days**	**Thu 10/01/19**	**Thu 16/05/19**
Forstudierapport	**10 days**	**Thu 10/01/19**	**Wed 23/01/19**
Systemkrav/Designrapport	**17 days**	**Thu 24/01/19**	**Fri 15/02/19**
Driftsdokument/Driftsrapport	**56 days**	**Mon 18/02/19**	**Mon 06/05/19**
Sluttrapport	**7 days**	**Tue 07/05/19**	**Wed 15/05/19**
Vurdering av gruppesamarbeid	1 day	Thu 16/05/19	Thu 16/05/19
Innlevering	0 days	Thu 16/05/19	Thu 16/05/19

Figur 1: Planlagt tidsforbruk

- Forstudierapport 10 dager
  - Fra 10. januar til 23. januar.
- Designdokument 17 dager
  - Fra 24. januar til 15. februar.
- Driftsdokumenter 56 dager
  - Fra 18. februar til 06. mai.
- Sluttrapport 7 dager
  - Fra 7. mai til 15. mai.

4.1.2 Faktisk tidsforbruk

- Forstudierapport 11 dager
  - Fra 10. Januar til 24. Januar.
- Designdokument 23 dager
  - Fra 24. Januar til 25. Februar.
- Driftsdokument 52 dager
  - Fra 26. Februar til 07. Mai.
- Sluttrapport 3 dager
  - Fra 07. mai til 09. mai.

4.2 Det som gikk bra

Prosjektgruppen opplevde at både skriveprosessen og resultatet som ble oppnådd i form av forstudierapporten, var en positiv side av prosjektet. Her ble tidsplanen fulgt tett, og resultat som ble oppnådd var noe prosjektdeltakerne var tilfredse med. Tilbakemeldingen som ble gitt gjenspeilte prosjektgruppens tanker, og de var derfor sikre på at dokumentet var av høy kvalitet. Mye av de samme tankene gjaldt også for designdokumentet, men her fikk prosjektgruppen også inntrykk av at innholdet samsvarte med det veilederne ønsket fra et designdokument. Prosjektgruppen er derfor trygge på at designdokumentet er blant de beste dokumentene som ble utarbeidet i løpet av prosjektet.

Samarbeidet mellom prosjektdeltakerne og arbeidsviljen deres, var også en av de positive sidene. Det oppleves som at prosjektgruppen holdt god arbeidsånd underveis i prosjektet og kommuniserte godt. Derfor oppsto det aldri større uenigheter eller friksjon mellom gruppemedlemmene.

Rapporter, timelister og møtereferat fikk god tilbakemelding av veilederne og var viktige ledd i prosjektgruppens dokumentasjonsprosess. Ukesrapportene sammen med gantt-diagramet har vært svært hjelpsomme verktøy for planlegging underveis. De ble benyttet for å holde oversikt over fremdrift, tidsplaner, videre planlagt arbeid og usikkerheter. Usikkerhetene i disse rapportene har vært sentrale for oppbyggingen av agendaer på veiledningsmøtene.

4.3 Det som gikk dårlig

Prosjektgruppen opplevde en del problemer underveis, men disse ble som regel løst. På tross av disse problemene, er det ingen problemer som har fjernet fra helheten i prosjektet, og problematikk har ikke hatt stor innvirkning på det ferdige produktet.

Lisenser til M365 skapte store tidsproblemer for prosjektet. Prosjektgruppen var avhengig av lisenser for å kunne påbegynne arbeide som skulle dokumenteres i driftsdokumentene. På grunn av dette gikk mye tid tapt som kunne blitt brukt til testing og skriving. Prosjektgruppen ble istede nødt til å forsøke å orientere seg rundt prosessen gjennom videoer og lesing. Hadde lisenser kommet tidligere, hadde mer tid kunne blitt brukt på feilsøking, testing og skriving.

NTNU hadde i prosjektperioden problemer med deres SharePoint og dette skapte avbrudd i dokumenteringen for prosjektgruppen. Avbruddene var som oftest korte i varighet, men hyppigheten gjorde dette til et stort irritasjonsmoment. Tekst

skrevet i Word Online måtte kopieres over til lokal maskin og når SharePoint ikke lengre hadde problemer ble tekst flyttet tilbake.

Importering av SCCM-objekter til Intune var en av problemene som ikke lot seg løse underveis. Dette var noe prosjektgruppen satte av en betydelig mengde tid til å forsøke å fikse, uten å oppnå resultater. Selv ikke med hjelp fra dyktige konsulenter fra ATEA lot problemet seg løse, og prosjektgruppen måtte derfor dokumentere prosessen uten å ha fått gjennomgått den selv.

4.4 Hvordan tekniske problemer ble løst

Når et teknisk problem oppsto, ble det først forsøkt å løse problemet ved å gå gjennom oppsettet som ble gjort og sammenligne med dokumentasjonen til Microsoft. Dersom problemet vedvarte forsøkte prosjektgruppen å finne løsninger på nettet, og teste muligheter som ble funnet underveis. Løste ikke problemet seg gjennom disse metodene, ble problemet dokumentert og tatt opp på kommende møte. Tilbakemeldingen gitt på møtet avgjorde om problemet ble løst, eller om fokuset skulle settes på andre områder. Prosjektgruppen fikk også hjelp av ansatte i ATEA dersom problemet innebar lab-miljøet. Slike problemene ble tatt opp med kontaktpersonen innen ATEA og ikke løst av prosjektgruppen da det ikke ingikk i oppgaven.

4.5 Systemets begrensninger

Systemet mangler migrerte postbokser fra Exchange, men studentene kan ikke ta for mye ansvar for dette. Grunnen til at dette mangler er at lab-miljøet ATEA sørget for ikke hadde en Exchange-server, så prosjektgruppen hadde ikke muligheten til å flytte post-bokser. Dokumentasjonen kunne derimot har beskrevet prosessen bedre, men tidsbegrensninger stoppet prosjektgruppen fra å gjøre mer arbeid.

Siden det ikke eksisterte noen Exchange-server i lab-miljøet ble det aldri migrert noen postbokser inn i systemet. Dette bør også ses i sammenheng med at systemet bare er satt opp med en Microsoft 365 E5 lisens. Hvis flere postbokser skulle blitt migrert måtte brukerne av disse postboksene ha hatt sin egen lisens for Exchange Online.

Grunnet problemer med SCCM ble det aldri migrert noen SCCM-objekter til Intune. Dette betyr at systemet mangler migrerte objekter fra SCCM.

Prosjektet har fokusert mye på ny teknologi og såkalte "preview"-funksjoner som fremdeles er i testfasen hos Microsoft. Dermed har det ikke vært noe fokus på støtte for eldre klientmaskiner. På Windows fronten betyr dette at systemet krever Windows 10 1809 eller nyere på klientmaskiner.

Som planlagt i både forstudie og designdokumentet har systemet ikke noen støtte for macOS, men det vil være mulig å utvide systemet med slik funksjonalitet.

4.6 Måloppnåelse

4.6.1 Effektmål

Cloud first strategien realiseres. Med arbeidet gjort i prosjektet har bedriften fått full funksjonalitet i skyen, og det er kun lokal AD som er gjenværende on-prem. Dette betyr at bedriften har tatt store steg mot å kun bruke skyen, og en kan derfor se på målet som nådd.

Bedriften ser en reduksjon i behov for lokal infrastruktur. Prosjektet har fjernet behovet for alle de lokale serverne, og lokal AD kan stenges ned dersom bedriften selv ønsker dette. Målet kan derfor sees på som nådd.

Administrasjon av IT-systemet vil effektiviseres ved blant annet automatisering. Prosjektet har lagt opp til at mye administrasjon vil skje av seg selv. Konfigurasjon kan fortsatt gjøres, og må gjøres manuelt, men det er en stor reduksjon i arbeid som må gjøres av IT-ansvarlige. Dette målet anses derfor som nådd.

Administrasjon av IT-system vil bli mer sentralisert. Prosjektet har gitt bedriften muligheten til å administrere alle systemene gjennom Azure-portalen. Kun lokal AD må administreres adskilt. Målet kan dermed sees på som nådd.

IT-systemets oppetid blir 99.9%. Ved å ta i bruk Microsofts infrastruktur i Azure vil man få deres oppetid som garanteres i tjenestenes SLA-avtaler. Disse avtalene lover en oppe tid på 99.9% og bedre. Prosjektgruppen får ikke testet denne på noen måte, men igjennom prosjektets gang ble det aldri opplevd tilkoblingsproblemer av noen sort. Det er opp til Microsoft om målet er oppnåelig i realiteten, men fra prosjektgruppens ståsted anses målet som nådd.

Ansatte vil oppleve økt tilgjengelighet til data og applikasjoner. Implementasjonen har tatt i bruk skyapplikasjoner som SharePoint, OneDrive og Office 365 og dermed kan ansatte kunne jobbe med sine data og applikasjoner uavhengig av geografisk lokasjon og tidspunkt. Målet anses dermed som nådd.

Muligjør BYOD. Prosjektet har lagt opp til BYOD, og har testet funksjonaliteten. Det ble aldri opplevd noen feil med enheter som ble innmeldt som en BYOD-enhet. Målet anses derfor som nådd.

Bedriften får en moderne arbeidsflate. Gjennom arbeidet gjort i prosjektet er det tydelig at ansatte i bedriften har fått tilgang på en moderne arbeidsflate. De har tilgang på skyapplikasjoner, er beskyttet gjennom policies og kan jobbe uavhengig av lokasjon. Målet kan dermed sees på som nådd.

Eliminere skygge-IT. Gruppen kan ikke sikre at skygge-IT elimineres gjennom det arbeidet som har blitt gjort, men det er lagt opp til at ansatte skal slutte med lokal lagring. Gjennom Teams, SharePoint og OneDrive har bedriften de beste forutsetningene for å hindre skygge-IT. Det vil være opp til bedriftens ansatte om målet er oppnåelig i realiteten, men fra prosjektgruppens ståsted anses målet som nådd.

4.6.2 Resultatmål

Sitte igjen med bare en on-prem server. Per prosjektets slutt er det ikke lengre behov for noen on-prem servere, men på bakgrunn av bedriftens ønsker, er lokal AD fortsatt operasjonell. Målet anses dermed som nådd.

IT-administrasjonen går hovedsakelig via skyen. All administrasjon, sett bort ifra den lokale AD-serveren, kan gjøres via skyen. Målet anses dermed som nådd.

Alle tjenester, applikasjoner og data er flyttet ut i skyen, bare AD er on-prem. Gjennom oppsett av Office-pakken, OneDrive, SharePoint, Exchange Online og Teams er alle applikasjoner, data og tjenester flyttet til skyen. Målet sees dermed på som nådd.

Ansatte har tilgang på tjenester utenfor bedriftens lokaler. Gjennom testing med VPN, og konfigurasjon som skal tillate bruk uavhengig av lokasjon, er prosjektgruppen sikre på at prosjektet har levert et system som støtter dette. Målet anses dermed som nådd.

Mobile enheter, som telefoner og nettbrett, kan administreres (Android og iOS). Gjennom testing med virtualisert og fysisk maskinvare med mobile OS (Android og iOS) og konfigurasjon som tillater administrasjon av slike enheter, er prosjektgruppen trygg på at systemet som har blitt levert kan administrere mobile enheter. Målet sees derfor på som nådd.

4.6.3 Prosessmål

Skape en helhetlig teknisk forståelse for konseptet modern workspace. Gjennom måneder med testing, dokumentasjon og diskusjon, har prosjektgruppen kommet nært på konseptet modern workspace. Konseptet er bredt og det vil ikke være grobunn for å kunne si at prosjektgruppen har kunnet gå dypt inn i de underliggende elementene. Ordlyden i helhetlig forståelse ber derimot ikke om at prosjektgruppen skal ha ekspertkompetanse rundt alle de underliggende elementene, kun en overordnet kompetanse som dekker det helhetlige. En slik kompetanse er prosjektgruppen trygg på at de har opparbeidet seg, og målet er dermed nådd.

Prosjektgruppen skal forstå konseptet og prosessen i migrering av systemer fra on-prem til skytjenester. Gjennom prosjektets gang, har prosjektgruppen jobbet med migrering og implementasjon av nye systemer. Feil som oppsto under migrering gjorde at dette ble en prosess prosjektgruppen har nær kjennskap til. Elementer som ikke lot seg migrere på grunn av manglede server å migrere fra, gjorde derimot at kunnskapen ikke nødvendigvis har nådd det nivået som ble antatt på forhånd. Målet anses dermed som delvis nådd.

Prosjektgruppen får kjennskap til de ulike tjenestene i Office 365. Prosjektet har handlet mye om de ulike produktene og tjenestene i Microsofts tjenesteportfolie og Office 365 har hatt en sentral rolle. Programmer i Office 365 har vært benyttet i flere anledninger som ved oppsett og konfigurasjon av tilleggstjenester og ved testing av sikkerhetsfunksjonalitet og skylagring. Målet anses dermed som nådd.

4.7 Timeregnskap

Denne oversikten over tidsbruk vil kun illustrere hvor mange timer som har blitt brukt på de ulike rapportene og dokumentasjonen til disse. For en oversikt over arbeidets art, vil det være anbefalt å gå gjennom prosjektgruppens timelister. Arbeid med presentasjon vil ikke tas med i regnskapet, men vil visualiseres i timelistene.

Forstudierapporten.

Magnus: 61.75 timer

Eskil: 54 timer

Designdokumentet.

Magnus: 120.75 timer

Eskil: 119.75 timer

Driftsdokumentet.

Magnus: 282.5 timer

Eskil: 298.5 timer

Sluttrapport.

Magnus: 14 timer

Eskil: 14.5 timer

5 Betraktninger i ettertid

Underveis i prosjektarbeidet ble ulike tanker diskutert mellom deltakerne i prosjektgruppen. Disse tankene omhandlet hvordan prosjektet kunne ha utartet seg med andre forutsetninger og hva de ville hatt i minne dersom de skulle gjennom et tilsvarende prosjekt

Migreringen av Exchange til Exchange Online ble utelatt grunnet manglende on-prem SharePoint-server. Dette er noe prosjektgruppen ønsket å teste og få erfaring med da det ble vektlagt, og diskutert, i designdokumentet. Prosjektgruppen så også på en slik migrering som relevant erfaring til arbeidslivet, og de hadde derfor stor interesse av å se nærmere på dette.

Mangelen på fysisk maskinvare er noe prosjektgruppen fikk se konsekvensene av underveis i prosjektet. Mangelen gjorde at gruppen ikke fikk testet automatisering av BitLocker skikkelig, noe prosjektgruppen hadde brukt mye tid på. Det samme gjelder for mobile enheter med Android, noe verken av studentene hadde og ikke fikk testet. Det gunstige ville derfor vært en kombinasjon av fysisk og virtualisert maskinvare tilgjengelig for testing.

Prosjektgruppen hadde tilgang på en Microsoft E5-lisens, og ser at selv om det var tilstrekkelig, ville det vært optimalt med flere lisenser. Testing av funksjonalitet ble på grunn av mengden lisenser begrenset til den globale administratorbrukeren, noe som hindret testing av hos vanlige brukere. Dette hadde vært spennende for å se at policier, profiler, applikasjoner og alt som ble konfigurert fungerte også for brukere uten administratortilganger.

Etter en lengre prat med en seniorkonsulent ansatt hos ATEA, forsto prosjektgruppen at dette burde vært gjort hyppigere og tidligere i prosjektet. Denne praten svarte på mange spørsmål prosjektgruppen hadde og belyste funksjonalitet i Intune de ikke var klar over at eksisterte på forhånd. Prosjektgruppen så derfor at de burde utnyttet kompetansen ATEA stilte til disposisjon bedre i løpet av prosjektet.

6 Videre arbeid

Prosjektets rammer ble satt for å tilpasse arbeidsmengden til den tidsperioden som var satt av for bachelorprosjektet. Prosjektgruppen har noen tanker om ha som burde vært utført og fokusert på dersom prosjektets tidsrammer hadde vært større.

Exchange-migrering er noe prosjektgruppen skulle ønske de hadde mulighet for å jobbe mer med. E-post-migrering er en svært komplisert og omfattende prosess, noe som gjør at det er vanskelig å implementere slikt i en bachelor med et bredere fokus. Prosjektgruppen ser dermed at migrering av e-post vil være et naturlig steg videre for prosjektet.

Fokuset på sikkerheten burde også konfigureres videre i samsvar med bedriftens ønsker og behov. Prosjektets rammer gjorde at elementer som oppdatering og sikkerheten rundt eldre versjoner av Windows ble utelatt. Implementasjonen burde tilpasses videre slik at den også har støtte for eldre versjoner av Windows, Android og iOS. Foruten støtte til eldre OS, ble også arbeid med Device Guard utelatt av tidsmessige årsaker. Dette er en funksjon prosjektgruppen skrev om i designdokumentet, og dermed håpet å få jobbe tettere med.

Støtte av Apple-produkter og bruk av Apple-tjenester er noe prosjektgruppen ser som en naturlig videreføring av prosjektet. Levering av Apple-enheter gjennom Apple DEP er noe bedriften ville hatt stor nytte av, og noe prosjektgruppen gjerne ville jobbet videre med. De ville også satt opp til å støtte administrering av macOS-enheter gjennom Jamf, og kanskje forsøkt å støtte andre Unix-baserte enheter.

Samarbeidsverktøyene Teams og SharePoint ble satt opp, men ikke konfigurert til en realistisk situasjon. Her vil det være naturlig å se på en faktisk bedrift, og hvordan den opererer, for å opprette operasjonelle teams på tvers av avdelinger som gjenspeiler virkeligheten. Konfigurasjonen av SharePoint er gjort ut ifra en fiktiv bedrift, og deres antatte behov. Her vil det vært mye nyttigere og tatt utgangspunkt i en virkelig bedrift med faktiske behov.

På bakgrunn av feil som gjorde at objekter fra SCCM ikke lot se migrere, er dette noe prosjektgruppen gjerne ville sett nærmere på. De ville sett etter alternative metoder for migrering, eller forsøkt en oppdatering av OS på serveren da dette antas å være opprinnelsen for feilen.