BRUKERHÅNDBOKA

- **Administrasjon av et større nettverk med domenekontroller med PowerShell**

BACHELORPROSJEKT:
Emne: IDRI3001

Semester: 6

Oppgavenummer: 80

Studieretning: ITBAINFODR

FORFATTER:
Cathinka Pedersen

VERSJONSLISTE

Versjon	Dato	Detaljer	Forfatter
1.0	20.05.2019	Ferdigstilt brukerhåndbok	Cathinka Pedersen

INNHOLDSFORTEGNELSE

TABELLISTE

FIGURLISTE

1. INTRODUKSJON

Hensikten med dokumentet er å bidra med informasjon nødvendig for å kunne nyttiggjøre seg produktet, og inneholder følgende informasjon:

Kapittel 2: Nødvendige forhåndskonfigurasjoner før bruk

Kapittel 3: Hvordan man navigerer seg frem til de ulike funksjonelle egenskapene

Kapittel 4: Praktiske fordeler ved bruk av produktet

2. TILPASSE PRODUKTET TIL BRUK I REELT MILJØ

Dette kapittel beskriver kriterier som må være oppfylt for at produktet kan benyttes av en virkelig organisasjon. Beskrivelsene tar utgangspunkt i at bruker kjører skriptet som «Administrator», fra en maskin som er tilkoblet internett, og har operativsystemet *Windows 10* installert (designrapporten beskriver systemkrav for maskiner med andre operativsystem).

2.1. PRIMÆR «DIRECTORY»

For å benytte skriptet i en virkelig organisasjon, må man ha en *AAD*-bruker med rollen «Global Administrator» for en «directory» i *Microsoft Azure*. Videre må den aktuelle «directory» hvis *AAD*-tjeneste man skal administrere, være den primære «directory» for den *AAD*-brukeren man logger seg inn med. Det vil si at dersom *AAD*-brukeren er tilknyttet flere «directory»-er, så må det være den «directory» brukeren kobles til ved pålogging på login.microsoftonline.com, som må være den «directory» brukeren skal administrere (den «directory» brukeren kobles til av «default»). For å utnytte alle produktets egenskaper, må den aktuelle «directory» hvis *Azure Active Directory*-tjeneste skal administreres, inneholde brukere, sikkerhetsgrupper, maskiner og lisenser i forkant.

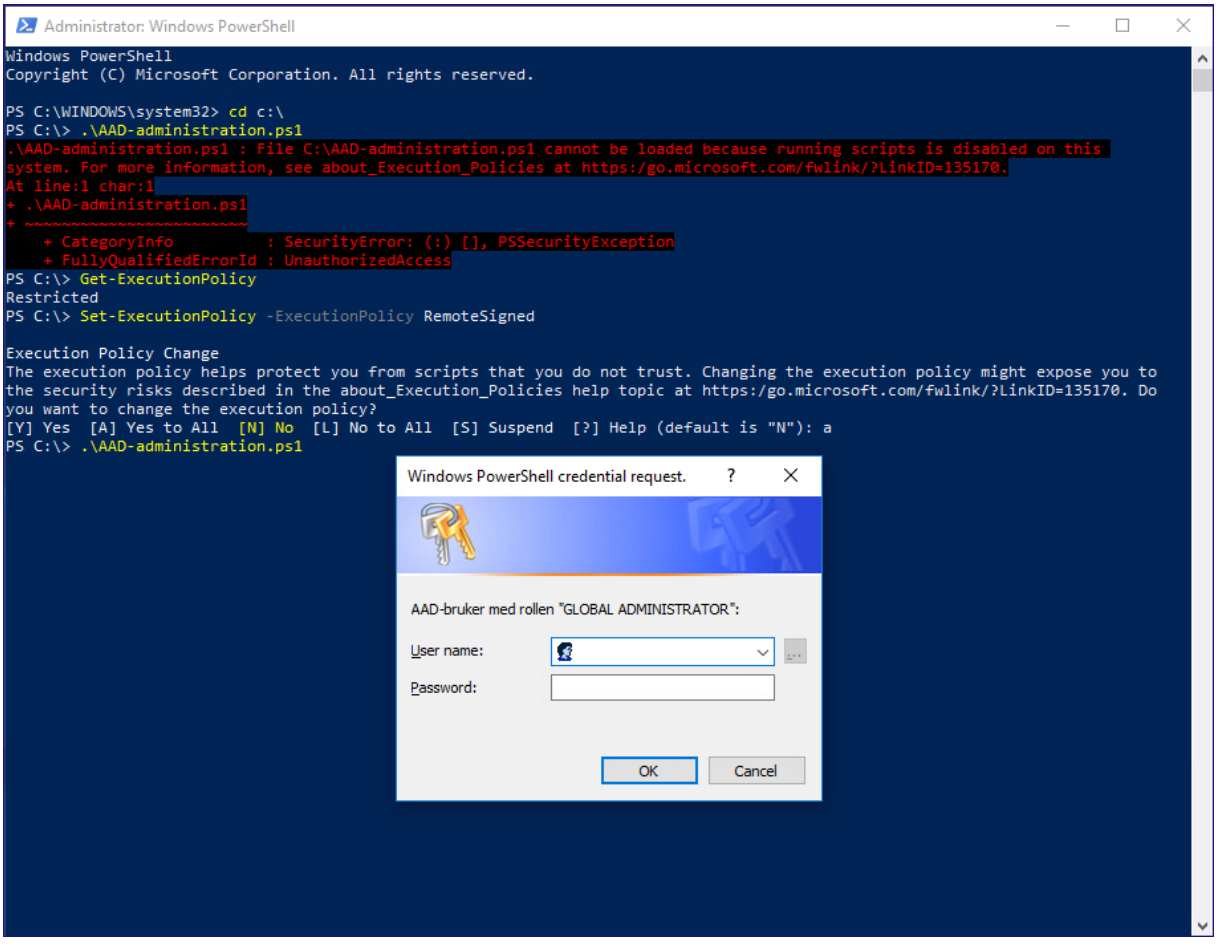
2.2. DOMENENAVN

Skriptet henter ut domenenavn med «.no»-ending. Dersom flere «.no»-domener er tilgjengelig i «directory»-en, eller dersom det ikke finnes noen «.no»-domener i «directory»-en, må det domenenavnet som skal benyttes som utgangspunkt for å opprette *UserPrincipalName* for brukere, hardkodes inn. Dette gjøres på linje *5-9* i funksjonen *createAADUser*, i skriptet.

2.3. EXECUTION POLICY

Maskinen som skriptet kjøres fra, må ha lov til å kjøre skriptet. Klargjør IT-ansvarliges arbeidsstasjon for å kjøre egendefinerte skript ved å:

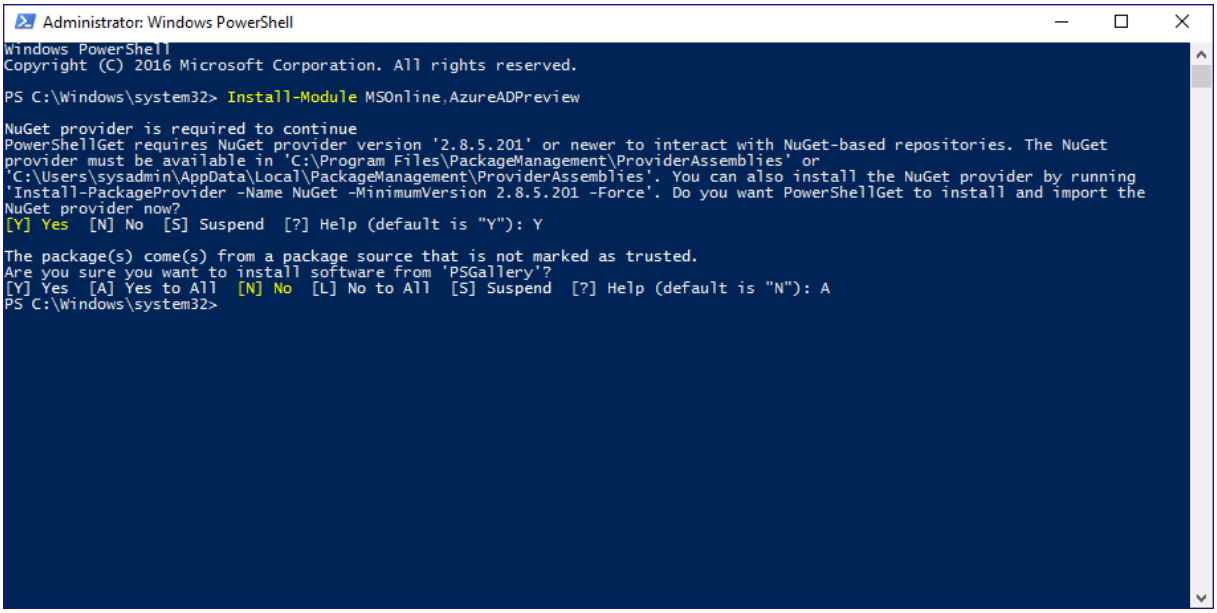
1. Kjøre *Windows PowerShell* som *Administrator*
2. Kjøre følgende kommando: *Set-ExecutionPolicy -ExecutionPolicy RemoteSigned*



Figur 1: *Setter "RemoteSigned", og ser nå at bruker kan kjøre skriptet fra maskinen.*

2.4. MODULER

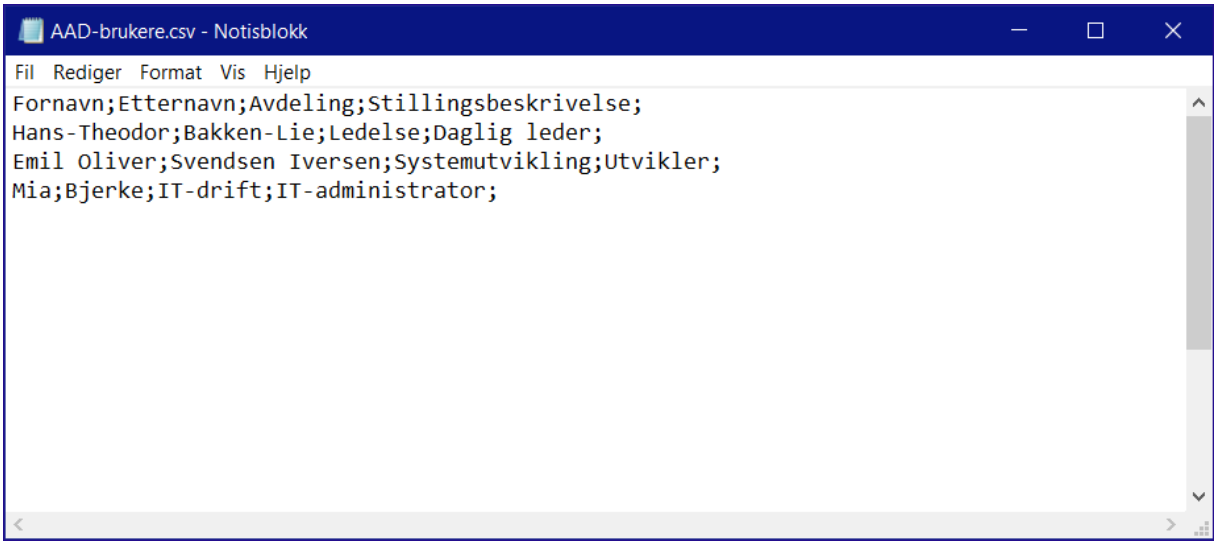
Skriptet benytter «cmdlets» fra to ulike moduler. Disse må installeres på maskinen. For å installere nødvendige moduler, må man også installere *NuGet*. Installerer *NuGet* samtidig med modulene *MSOnline* og *AzureADPreview*:



Figur 2: *Installerer «NuGet», «MSOnline» og «AzureADPreview» for tilgang på nødvendige «cmdlets».*

2.5. OPPRETTE AAD-BRUKERE FRA CSV-FIL

Det å opprette brukere i en bulk-operasjon, krever at man på maskinen har tilgang til en CSV-fil med brukernes informasjon oppført på følgende format:



Figur 3: *Oppretting av flere AAD-brukere i bulk-operasjon.*

3. PRODUKTETS FUNKSJONELLE EGENSKAPER

Produktets egenskaper			
Indeks	**Funksjonalitet**	**Handlingskart**	**Beskrivelse**
Brukeradministrasjon			
1.	Opprette enkel *AAD*-bruker	\Hovedmeny\Brukeradministrasjon\Opprett ny AAD-bruker\Enkel bruker\	**Input:** - Fornavn - Etternavn - Avdeling - Stillingsbeskrivelse **Handlingsforløp:** - Oppretter en enkel bruker i *AAD* - Oppretter sikkerhetsgruppe i AAD med samme navn som avdelingen brukeren tilhører - Bruker plasseres i sikkerhetsgruppe med samme navn avdelingen brukeren tilhører - Brukeren oppføres i filen «C:\OpprettedeAAD-brukere.csv» - Sikkerhetsgruppen oppføres i filen «C:\OpprettedeAAD-sikkerhetsgrupper.csv»
2.	Opprette flere *AAD*-brukere i en bulk-operasjon	\Hovedmeny\Brukeradministrasjon\Opprett ny AAD-bruker\Fra CSV-fil (flere)\	**For hver rad i CSV-filen:** - Oppretter en enkel bruker i *AAD*. - Oppretter sikkerhetsgruppe med samme navn som avdelingen brukeren tilhører - Bruker plasseres i sikkerhetsgruppe med samme navn som avdelingen brukeren tilhører. - Brukeren oppføres i filen «C:\OpprettedeAAD-brukere.csv» - Sikkerhetsgruppen oppføres i filen «C:\OpprettedeAAD-sikkerhetsgrupper.csv»
3.	Nullstille passord for en *AAD*-bruker	\Hovedmeny\Brukeradministrasjon\Nullstill passord for AAD-bruker\Velge fra liste || Velge basert på søk\	Hensiktsmessig når en bruker har glemt passord. – Systemet genererer et midlertidig passord til valgt *AAD*-bruker, som da må velge et varig passord ved neste innlogging. Loggføres i "C:\NyttPassordAAD-bruker.csv"
4.	Midlertidig slette en *AAD*-bruker	\Hovedmeny\Brukeradministrasjon\Slette en AAD-bruker\Velge fra liste || Velge basert på søk\	**Handlingsforløp:** - Brukeren slettes fra ordinær liste med alle *AAD*-brukere.

			- Slettingen loggføres i «C:\SlettedeAAD-brukere.csv».
5.	Oversikt over alle *AAD*-brukere som ikke er midlertidig slettet	\Hovedmeny\Brukeradministrasjon\List ut alle AAD-brukere\	Lister ut alle *AAD*-brukere fra ordinær liste i *AAD*.
6.	Oversikt over en *AAD*-bruker	\Hovedmeny\Brukeradministrasjon\Vis utdypende informasjon om en AAD-bruker\	**Oversikt over:** - Brukerobjektet i sin helhet. - Gruppen(e) vedkommende tilhører. - Maskinen(e) brukeren er registrert som eier av. - Maskinen(e) brukeren er som registrert bruker av. - Lisensen brukeren er tildelt - Tjenestene brukeren har tilgang til
7.	Gjenopprette en midlertidig slettet *AAD*-bruker	\Hovedmeny\Brukeradministrasjon\Gjenopprett slettet AAD-bruker\Velge fra liste || Velge basert på søk\	*AAD*-bruker kan gjenopprettes innen tretti dager etter at slettingen fant sted. Loggføres på «C:\GjenopprettedeAAD-brukere.csv»
Gruppeadministrasjon			
8.	Opprette en ny *AAD*-sikkerhetsgruppe	\Hovedmeny\Gruppeadministrasjon\Opprett ny AAD-sikkerhetsgruppe\	**Input:** - Navn på sikkerhetsgruppe - Beskrivelse av sikkerhetsgruppe **Handlingsforløp:** - Oppretter ny sikkerhetsgruppe i *AAD*. - Loggføres i "C:\OpprettedeAAD-sikkerhetsgrupper.csv".
9.	Endre beskrivelse på en *AAD*-sikkerhetsgruppe	\Hovedmeny\Gruppeadministrasjon\Rediger AAD-sikkerhetsgruppe\Endre beskrivelse på gruppe\Velge gruppe fra liste || Velge gruppe basert på søk\	**Handlingsforløp:** - Sikkerhetsgruppen tildeles ny beskrivelse i *AAD*. - Handlingen loggføres på «C:\NyBeskrivelseAAD-sikkerhetsgruppe.csv».
10.	Legge til en *AAD*-bruker i en *AAD*-sikkerhetsgruppe	\Hovedmeny\Gruppeadministrasjon\Rediger AAD-sikkerhetsgruppe\Legg til en bruker i gruppe\Velge gruppe fra liste || Velge gruppe basert på søk\Velge fra liste || Velge basert på søk\	Valgt *AAD*-bruker legges til i valgt *AAD*-sikkerhetsgruppe.
11.	Fjerne et medlem fra en *AAD*-sikkerhetsgruppe	\Hovedmeny\Gruppeadministrasjon\Rediger AAD-sikkerhetsgruppe\Fjern et medlem fra gruppe\Velge gruppe fra liste || Velge gruppe basert på søk\	Valgt medlem er ikke lenger oppført i valgt *AAD*-sikkerhetsgruppe.
12.	Overføre et medlem fra en *AAD*-sikkerhetsgruppe til en annen	\Hovedmeny\Gruppeadministrasjon\Rediger AAD-sikkerhetsgruppe\Overfør ett medlem fra en gruppe til en annen\Velge gruppe fra liste || Velge gruppe basert på søk\	Overfører valgt medlem i en *AAD*-sikkerhetsgruppe til en annen.

13.	Overføre alle medlemmer i en *AAD*-sikkerhetsgruppe til en annen	\Hovedmeny\Gruppeadministrasjon\Rediger AAD-sikkerhetsgruppe\Overfør alle medlemmer i en gruppe til en annen\Velge gruppe fra liste || Velge gruppe basert på søk\	Overfører alle medlemmer i en *AAD*-sikkerhetsgruppe til en annen.
14.	Oversikt over alle medlemmer i en *AAD*-sikkerhetsgruppe	\Hovedmeny\Gruppeadministrasjon\List ut medlemmer i AAD-sikkerhetsgruppe\Velg gruppe fra liste || Velg gruppe basert på søk\	Alle medlemmer i valgt *AAD*-sikkerhetsgruppe listes ut.
15.	Slette en *AAD*-sikkerhetsgruppe	\Hovedmeny\Gruppeadministrasjon\Slett AAD-sikkerhetsgruppe\Velge gruppe fra liste || Velge gruppe basert på søk\	Valgt *AAD*-sikkerhetsgruppe slettes permanent.
16.	Oversikt over alle *AAD*-sikkerhetsgrupper	\Hovedmeny\Gruppeadministrasjon\List ut alle AAD-sikkerhetsgrupper\	Lister ut alle sikkerhetsgrupper oppført i *AAD*.
17.	Oversikt over en *AAD*-sikkerhetsgruppe	\Hovedmeny\Gruppeadministrasjon\Vis utdypende informasjon om en AAD-sikkerhetsgruppe\Velge gruppe fra liste || Velge gruppe basert på søk\	**Lister ut:** - Gruppeobjektet i sin helhet - Lisenser tildelt gruppen - *AAD*-sikkerhetsgrupper valgt sikkerhetsgruppe er medlem av - *AAD*-brukere medlem av sikkerhetsgruppen - *AAD*-sikkerhetsgrupper medlem av valgt sikkerhetsgruppe - Maskiner medlem av valgt sikkerhetsgruppe
Maskinadministrasjon			
18.	Endre det navnet en maskin er oppført med i *AAD*	\Hovedmeny\Maskinadministrasjon\Endre AAD-maskin\Endre navn på AAD-maskin\Velge fra utlisting av alle AAD-maskiner || Velge fra utlisting basert på søk\	**Handlingsforløp:** - Maskinen oppføres med nytt navn i *AAD* - Handlingen loggføres på «C:\NyttNavnAAD-maskin.csv»
19.	Legge til en *AAD*-bruker som eier av en *AAD*-maskin	\Hovedmeny\Maskinadministrasjon\Endre AAD-maskin\Endre registrert eier av AAD-maskin\Legg til eier av AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	Legger til valgt *AAD*-bruker som eier av valgt *AAD*-maskin.
20.	Bytte ut en *AAD*-bruker med en annen, som eier av en *AAD*-maskin	\Hovedmeny\Maskinadministrasjon\Endre AAD-maskin\ Endre registrert eier av AAD-maskin\Bytt ut en eier av AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	Bytter ut en *AAD*-bruker med en annen, som eier av valgt *AAD*-maskin.
21.	Fjerne en *AAD*-bruker som eier av valgt *AAD*-maskin	\Hovedmeny\Maskinadministrasjon\Endre AAD-maskin\ Endre registrert eier av AAD-maskin\Fjern eier fra AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	Fjerner valgt *AAD*-bruker som eier av valgt *AAD*-maskin.

22.	Registrere en *AAD*-bruker som bruker av valgt *AAD*-maskin	\Hovedmeny\Maskinadministrasjon\Endre AAD-maskin\Endre registrert bruker av AAD-maskin\Legg til registrert bruker av AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	Legger til valgt *AAD*-bruker som bruker av valgt *AAD*-maskin.
23.	Bytte ut en *AAD*-bruker med en annen, som bruker av valgt *AAD*-maskin	\Hovedmeny\Maskinadministrasjon\Endre AAD-maskin\ Endre registrert bruker av AAD-maskin\Bytt ut en registrert bruker av AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	Bytter ut valgt *AAD*-bruker med en annen, som bruker av valgt *AAD*-maskin.
24.	Fjerne en *AAD*-bruker som bruker av en *AAD*-maskin	\Hovedmeny\Maskinadministrasjon\Endre AAD-maskin\ Endre registrert bruker av AAD-maskin\Fjern en registrert bruker av AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	Fjerner valgt *AAD*-bruker som bruker av valgt *AAD*-maskin.
25.	Fjerne en maskin fra *AAD*	\Hovedmeny\Maskinadministrasjon\Slett AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	**Handlingsforløp:** - Maskinens slettes fra *AAD*. - Handlingen loggføres på «C:\SlettedeAAD-maskiner.csv»
26.	Oversikt over alle maskiner oppført i *AAD*	\Hovedmeny\Maskinadministrasjon\List ut alle AAD-maskiner\	Lister ut alle maskiner oppført i *AAD*.
27.	Oversikt over en *AAD*-maskin	\Hovedmeny\Maskinadministrasjon\Vis utdypende informasjon om en AAD-maskin\Velg fra utlisting av alle AAD-maskiner || Velg fra utlisting basert på søk\	**Lister ut:** - Maskinobjektet i sin helhet. - *AAD*-brukere som er registrert som eier av valgt *AAD*-maskin - *AAD*-brukere som er registrert som bruker av valgt *AAD*-maskin
Lisensadministrasjon			
28.	Oversikt over alle lisenser i *AAD*	\Hovedmeny\Lisensadministrasjon\Alle lisenser\	**Oversikt over:** - Alle lisenser tilknyttet *AAD*. - Alle tjenester tilknyttet hver lisens
29.	Oversikt over alle *AAD*-brukere som er tildelt en spesifikk lisens	\Hovedmeny\Lisensadministrasjon\Brukere og lisenser\Brukere som har lisens\	Lister ut alle *AAD*-brukere som er tildelt valgt lisens.
30.	Oversikt over alle *AAD*-brukere som mangler en spesifikk lisens	\Hovedmeny\Lisensadministrasjon\Brukere og lisenser\Brukere som mangler lisens\	Lister ut alle *AAD*-brukere som mangler valgt lisens.
31.	Tildele en lisens til en *AAD*-bruker direkte	\Hovedmeny\Lisensadministrasjon\Brukere og lisenser\Tildel lisens til bruker\Direkte\	Tildeler valgt lisens direkte til valgt *AAD*-bruker.
32.	Tildele en lisens til en *AAD*-bruker indirekte	\Hovedmeny\Lisensadministrasjon\Brukere og lisenser\Tildel lisens til bruker\Indirekte (arv)\	Plasserer valgt *AAD*-bruker i valgt *AAD*-sikkerhetsgruppe, som har lisensen.

33.	Oversikt over alle *AAD*-sikkerhetsgrupper som er tildelt en spesifikk lisens	\Hovedmeny\Lisensadministrasjon\Grupper og lisenser\Grupper som har lisens\	Lister ut alle *AAD*-sikkerhetsgrupper som er tildelt valgt lisens.
34.	Oversikt over alle *AAD*-sikkerhetsgrupper som mangler en spesifikk lisens	\Hovedmeny\Lisensadministrasjon\Grupper og lisenser\Grupper som mangler lisens\	Lister ut alle *AAD*-sikkerhetsgrupper som mangler valgt lisens.
35.	Oversikt over en spesifikk lisens	\Hovedmeny\Lisensadministrasjon\Utdypende informasjon om en lisens\	**Lister ut:** - Lisensobjektet i sin helhet - Tjenester som inngår - *AAD*-brukere som er tildelt lisensen - *AAD*-sikkerhetsgrupper som er tildelt lisensen

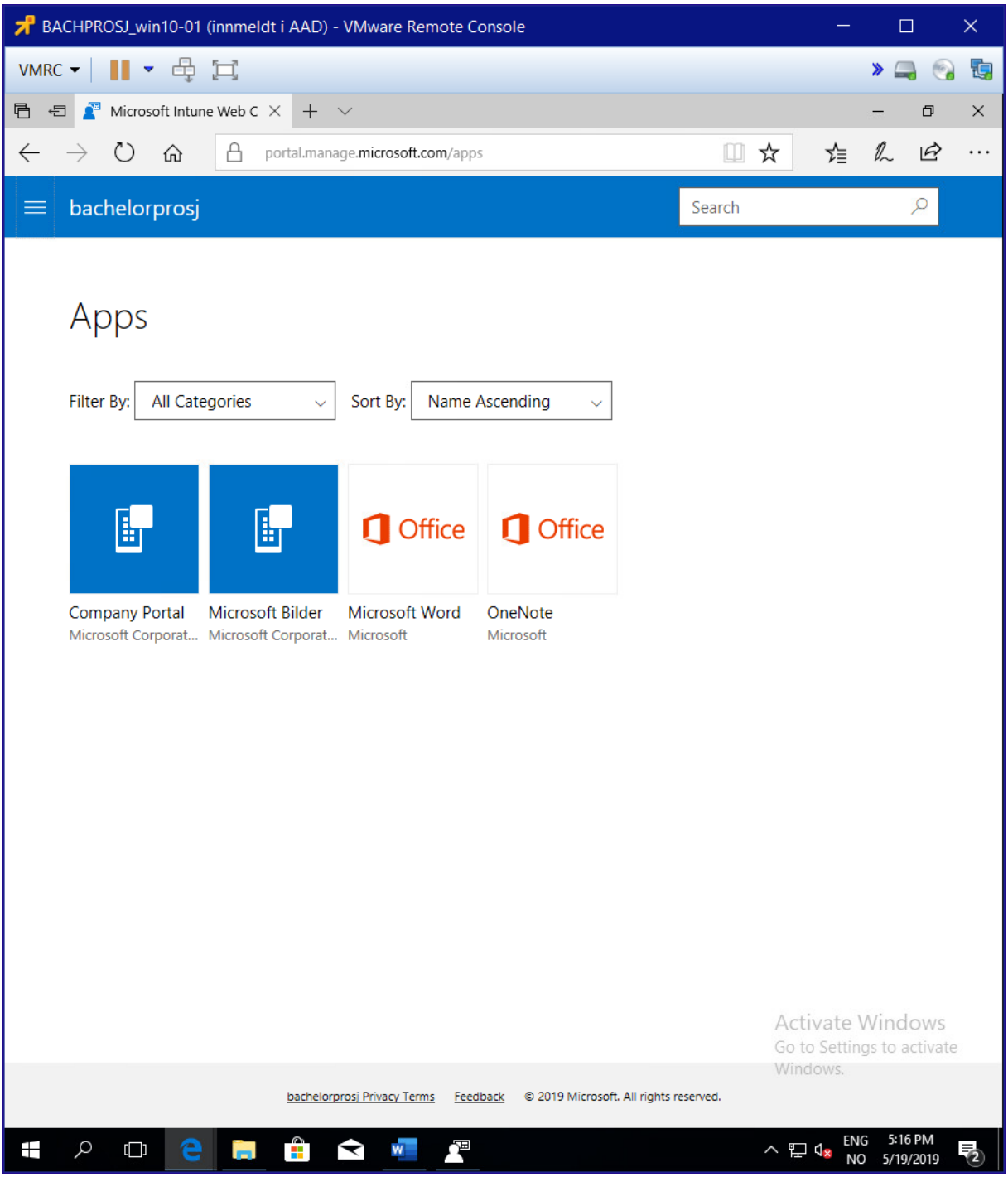
Tabell 1: *Produktets funksjonelle egenskaper.*

4. PRODUKTETS PRAKTISKE NYTTEVERDI

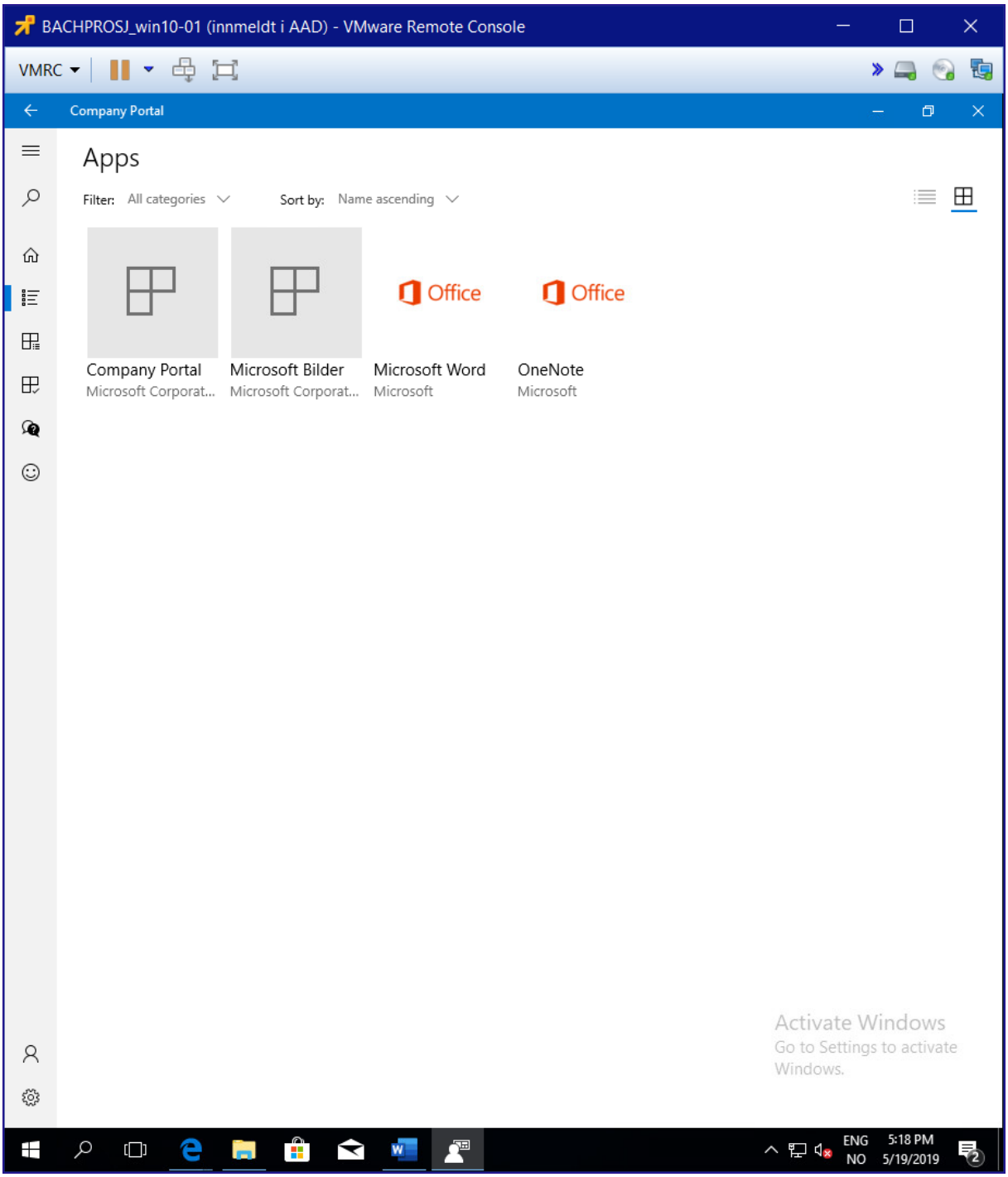
I dette underkapittel viser vi til noen eksempler hvor produktet kan bidra til praktisk nytteverdi for en gitt organisasjon.

4.1. MICROSOFT INTUNE

Når maskiner innmeldes eller registreres i *AAD* av en *AAD*-bruker med lisensen *Enterprise Mobility + Security E5*, så rulles maskinen inn i *Microsoft Intune*, samtidig som maskinen oppføres i *AAD*. Her ifra kan man for eksempel sette opp en regel som sier at maskiner med spesifikke *AAD*-brukere registrert som eiere og/eller brukere skal ha tilgang på en eller flere angitte programvarer. Man kan velge hvorvidt disse programvarene skal installeres på aktuell maskin i bakgrunnen, eller brukeren kan ha mulighet å installere disse applikasjonene på eget initiativ. Bakgrunnsinstallasjon er imidlertid kun mulig for *AAD*-innmeldte maskiner.



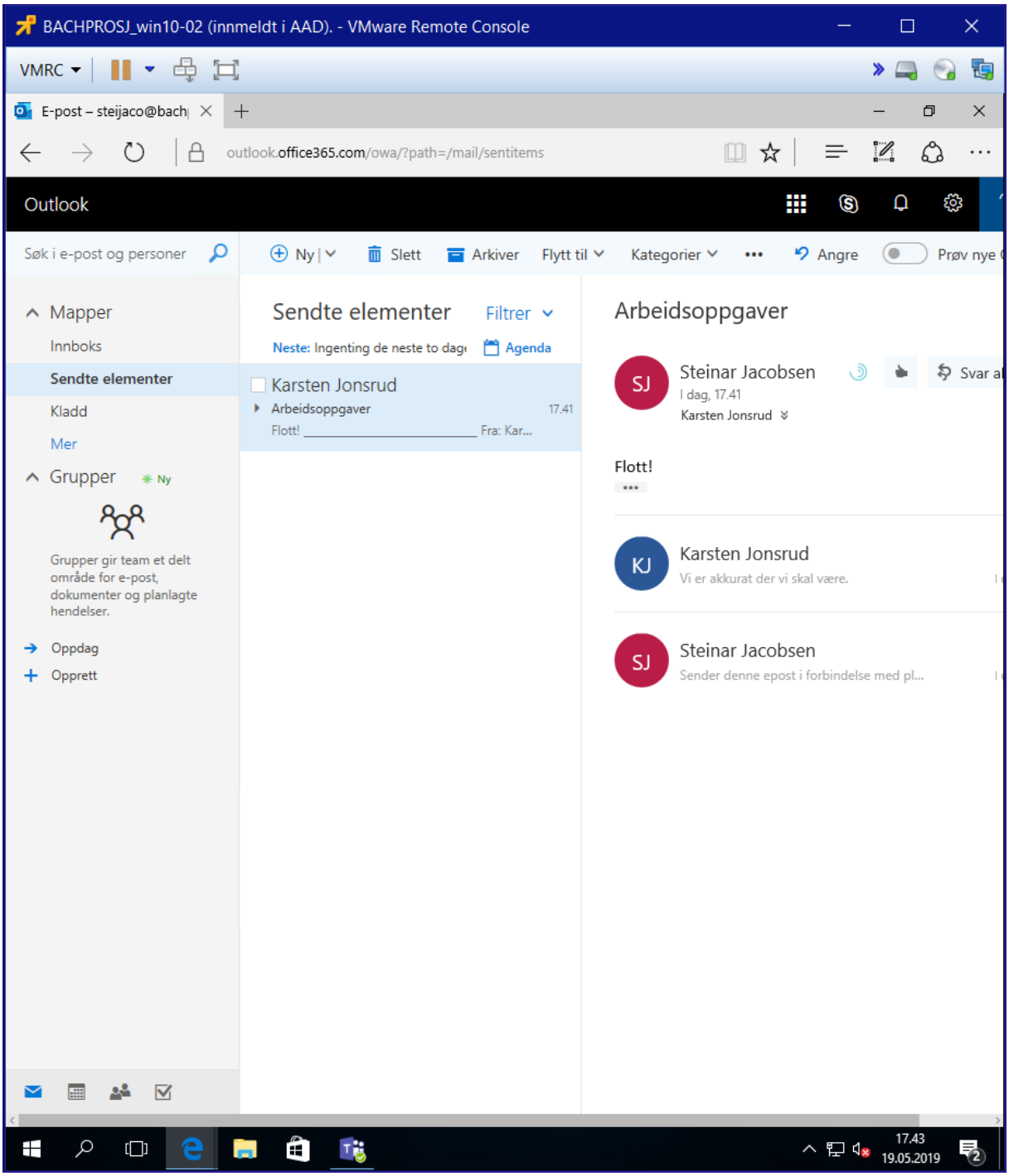
Figur 4: *Fire programmer gjort tilgjengelig for bruker av AAD-maskinen, via Microsoft Intune, fra nettleser.*



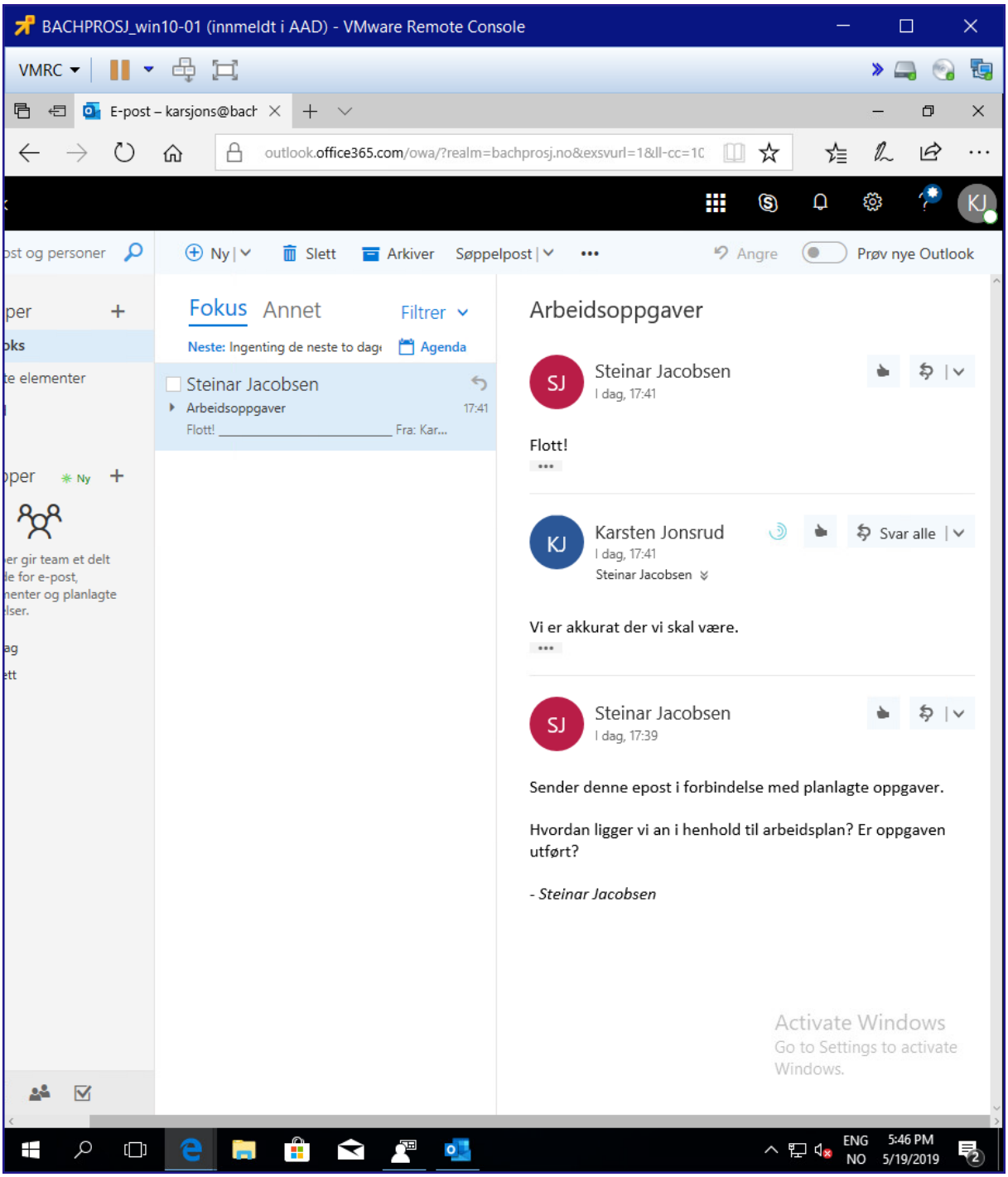
Figur 5: *Fire programmer gjort tilgjengelig for brukerne på AAD-maskinen, via Microsoft Intune, i appen Company Portal.*

4.2. EPOST

Det å tildele spesifikke lisenser til en *AAD*-bruker eller sikkerhetsgruppen *AAD*-brukeren tilhører, gir aktuell bruker tilgang på ulike tjenester. For eksempel, ved å tildele brukeren *Office 365 Business Premium*-lisensen, så har brukerne tilgang på skytjenesten *Outlook*:



Figur 6: *Å tildele O365 Business Premium-lisens til brukere, bidrar til at brukerne får tilgang til hver sin egen epostkonto. Bilde 1/2.*



Figur 7: *Email-korrespondanse mellom to AAD-brukere på bakgrunn av at de er blitt tildelt lisensen O365 Business Premium, bilde 2/2.*

4.3. FJERNER MASKIN FRA AAD

Når man fjerner en maskins kobling til *AAD*, lokalt på maskinen, forblir maskinen oppført i *AAD*. For å fjerne maskinens oppføring fra *AAD*, må man benytte *Windows PowerShell*. Følgende video bekrefter dette: https://youtu.be/TCCH5wSvYd0

4.4. SSO PÅ INNMELDT MASKIN

Når man logger inn på en *AAD*-innmeldt maskin, får man tilgang til adgangskontrollerte applikasjoner, på bakgrunn av identifiseringen man foretok ved innlogging. Følgende video demonstrerer *SSO*: https://youtu.be/hNtev17ETpM