PoC-projekt i Microsoft Intune

IT-Teknolog

Erhvervsakademi Aarhus, 4. semester

OPLYSNINGER	
SKREVET AF	Chanett Koldsø
HOLD	ITEK-E22a
AFLEVERINGSDATO	24. maj 2024
PROJEKTPERIODE	18. marts 2024 - 24.maj 2024
PRAKTIKVIRKSOMHED	**NHC A/S** Kejlstrupvej 85, 8600 Silkeborg
KONTAKTPERSONER	**Anders T. Eriksen** Praktikvejleder, Erhvervsakademi Aarhus
	Ømer Hendem Seniorkonsulent & Mentor, NHC A/S
ANSLAG	47.880 anslag // 20 sider

Resumé

Apex Juridisk Rådgivning oplever udfordringer med deres nuværende it-struktur, idet den manuelle administration på deres pc-enheder er ineffektiv og tidskrævende. Projektet sigter mod at implementere Microsoft Intune for at centralisere og automatisere enhedsstyringen, forbedre sikkerheden og effektivisere arbejdsprocesserne med minimal økonomisk investering.

Løsningen omfatter opsætning af automatiseret enhedshåndtering, grundkonfigurationer og sikkerhed i Microsoft Intune samt enhedsmonitorering og skærpede sikkerhedspolitikker i Microsoft Entra ID og Defender. Der arbejdes bl.a. med Security Baselines, Compliancy Policy og Endpoint Security.

Projektet er vigtigt for kunden, da implementeringen muliggør en centraliseret og automatiseret enhedsadministration, hvilket reducerer den manuelle arbejdsbyrde, forbedrer datasikkerheden og sikrer en ensartet enhedskonfiguration, som samlet set bidrager til virksomhedens effektivitet og sikkerhed. Ligeledes er projektet vigtigt for mig karrieremæssigt, da dybdegående viden om opsætning af Microsoft platformene har stor værdi for it-konsulentvirksomheder, som NHC A/S, der arbejder med disse systemer.

Projektet blev udarbejdet hos NHC A/S i Silkeborg, hvor jeg opnåede praktisk erfaring med de berørte platforme og med arbejdsprocesserne, der knytter sig til et sådant implementerings-projekt. Ved hjælp af den agile Kanban-metode blev projektet effektivt udført med tilfredsstillende resultater.

INDHOLDSFORTEGNELSE

1. Introduktion

Apex Juridisk Rådgivning er en juridisk konsulentvirksomhed i Horsens, der grundet stigende vækst står over for udfordringer med deres nuværende it-struktur. Den manuelle administration af deres stationære og bærbare pc-enheder er utilstrækkelig, tidskrævende og økonomisk belastende. Kunden ønsker en løsning, der med minimal økonomisk investering kan effektivisere arbejdsprocesserne og forbedre sikkerheden omkring enhedsopsætning og datasikkerhed.

Da kunden allerede har adgang til Microsoft Intune via eksisterende Microsoft 365 licenser, fokuserer projektet på at implementere Microsoft Intune i et testmiljø, for at demonstrere systemets muligheder for centraliseret enhedsstyring og forbedret sikkerhed. Fokus vil være på opsætning af automatiseret enhedsstyring, forbedring af brugeroplevelsen, skærpelse af sikkerhedspolitikker, automatisk vedligeholdelse og enhedsmonitorering. Til testbrug inddrages en fysisk bærbar samt virtuelle maskiner opsat i Microsoft Azure.

Projektet er inspireret af praktikforløbet hos NHC A/S, hvor jeg blev introduceret for både Microsoft Intune og Microsoft Azure. Projektet har til formål at give mig dybere praktisk erfaring med disse systemer samt praktisk erfaring med arbejdsprocesserne omkring planlægning og opsætning af et implementeringsprojekt.

Projektet strækker sig fra 18. marts 2024 til 24. maj 2024 og er opdelt i følgende moduler: *Analyse, Grundopsætning, Sikkerhed, System- & Integrationstest.* Ressourcer inkluderer ClickUp samt Microsoft-platformene Azure, Intune, Admin Center, Entra og Defender.

Der er i projektet kun fokuseret på implementering af Microsoft Intune på Windows pc'er.

2. Problemformulering

Målet med projektet er at påvise, hvordan et system som Microsoft Intune kan imødekomme kundens behov for effektivisering af arbejdsprocesser gennem centraliseret enhedsstyring samt hvordan systemet kan optimere sikkerheden omkring datasikkerhed og enhedsopsætning.

Projektet vil derfor fokusere på følgende 5 nøglepunkter:

1) Opsætning af centraliseret enhedsstyring
2) Opsætning af automatisk vedligehold af klientenhederne
3) Optimering af sikkerhedspolitikker og adgangstilladelser
4) Optimering af brugeroplevelsen
5) Monitorering af enhederne

2.1 Motivation for projektet

NHC A/S gør brug af dynamiske standardværktøjer i deres implementeringsløsninger og under mit praktikforløb fik jeg en introduktion til Microsoft Azure og Microsoft Intune. Jeg blev under praktikforløbet hurtigt inspireret af systemernes muligheder og i samarbejde med NHC A/S, blev der fundet et projekt, som jeg kunne arbejde med. Projektet udarbejdes selvstændigt på praktikstedet med mulighed for at rådføre sig hos kollegaerne.

Målene med projektet er for mig, at:

- opnå dybere praktisk erfaring med arbejdsprocesserne omkring planlægning og opsætning af implementeringsprojekter
- lære at opsætte testmiljø i Microsoft Azure
- lære og forstå, hvordan Microsoft Intune opsættes
- opnå dybere kendskab til opsætning af sikkerhed - herunder kryptering samt beskyttelse mod phishing, malware m.v.

2.2 Projektomfang

PROJEKTOMFANG	
PROJEKTPERIODE	18. marts 2024 - 24.maj 2024
AFLVERINGSDATO	24. maj 2024, kl. 12.00
OMFANG	Perioden strækker sig over 10 uger, inklusive påskeferie og helligdage
RESSOURCER	Der investeres i Microsoft 365 Business Premium, Microsoft Azure og ClickUp.
RISIKOGRUPPER	Særlige risikogrupper, der især kan forsinke projektet, er sygdom hos datter på 3 år samt helligdage, hvor børnehaven har lukket.
AFGRÆNSNING	Der fokuseres i projektet kun på implementering af Microsoft Intune på Windows pc'er, ligeledes vil "udvidet databeskyttelse og GDPR" ikke være en del af projektet.

3. Metoder & Værktøjer

PROJEKTSTYRING

Projektet blev styret ved hjælp af den agile Kanban-metode, der fremmer et effektivt og visuelt workflow. Værktøjer tæller blokdiagram, Work-Breakdown-Structure diagram og Gantt kort.

CLICKUP

ClickUp er et projektplanlægningsværktøj, der muliggør planlægning og organisering af projekter, hvor der gøres brug af bl.a. Gantt, Kanban Board og Liste-visning. Det bruges i projektet til at visualisere og planlægge arbejdet.
ClickUp Project

MICROSOFT PLATFORME

Microsoft 365 Admin Center et centralt kontrolpanel, hvorfra der i projektet arbejdes med brugeroprettelse og tildeling af licenser.
admin.microsoft.com

Microsoft Intune er en cloud-baseret tjeneste, der tilbyder enhedsadministration, brugerhåndtering og applikationshåndtering samt sikkerhed på tværs af disse services. Tjenesten muliggør let og effektiv håndtering af virtuelle og hybride it-infrastrukturer fra en web-baseret platform, hvor både virtuelle og fysiske enheder, herunder også BYOD-enheder, let kan kobles på Intune via en Microsoft-konto. Alle de nævnte funktioner benyttes i projektet.[1]
intune.microsoft.com

Microsoft Azure er en cloud computing-platform, der bl.a. muliggør opsætning, implementering og administrering af virtuelle miljøer, applikationer og tjenester. Bruges i projektet til oprettelse af virtuelle testmaskiner.
portal.azure.com

Microsoft Entra ID bruges i projektet til opsætning af bl.a. Conditional Access (MFA), Password Protection og monitorering af identitetssikkerhed. Desuden fungerer Tenant ID som bindeled mellem platformene.
entra.microsoft.com

[1] *"What is Intune?" af Microsoft Learn*

Microsoft Defender er en cloud-baseret sikkerhedsplatform, hvor særligt den rekommanderede liste over anbefalede sikkerhedsoptimeringer bruges som guideline til yderligere optimering af sikkerheden for projektet.
security.microsoft.com

Platformene benævnes herefter *Admin Center*, *Intune*, *Azure*, *Entra* og *Defender*.

CHATGPT

ChatGPT er i projektet brugt i forbindelse med at konkretisere og forkorte afsnit.

TESTENHEDER

OVERSIGT OVER TESTENHEDER		
NAVN	**TYPE**	**TPM**
VM-WIN	Azure Cloud VM	Nej
APEX-VM-WIN	Azure Cloud VM	Nej
CK-ASUS	Fysisk enhed	Nej
CHOKO-VM	VM på fysisk enhed	Ja

4. Virksomheden

NHC A/S er en IT-konsulentvirksomhed, hvis målsætning er at styrke deres kunders forretninger med IT-løsninger, der baserer sig på dynamiske standardværktøjer.[2]

NHC A/S blev stiftet i 2008 og består af to kontorer i Silkeborg og København. De beskæftiger 36 ansatte, hvor it-baggrunde bl.a. tæller datateknikere og it-supportere. Virksomheden servicerer godt 400 kunder, hvoraf 350 er kontraktkunder. Virksomheden er delt op i afdelingerne: Service Desk, Technical Service, IT Consulting, IT Operations, Sales & Marketing og Finance & Administration.

Under praktikforløbet hos dem blev jeg tilknyttet Ømer Hendem fra IT Consulting-afdelingen, der håndterer implementeringsprojekter. Her stiftede jeg bekendtskab med Intune og Azure, og det er med afsæt i praktikforløbet og med inspiration herfra, at PoC projektet blev opsat med fokus på implementering af Intune. Ømer Hendem har ligeledes været min nærmeste sparringspartner for projektet. Det daglige projektarbejde udføres selvstændigt på kontoret i Silkeborg med mulighed for at rådføre sig hos kollegaer.

[2] *"Om NHC" af NHC A/S*

5. Intune implementering

5.1 Analyse

5.1.1 Baggrund

Kunden er Apex Juridisk Rådgivning - en juridisk konsulentvirksomhed beliggende i Horsens. Virksomheden blev grundlagt i 2018 og beskæftiger i dag 27 ansatte. I de kommende tre år forventer kunden en stigning i antallet af sager på 13% og planlægger at ansætte tre nye juridiske konsulenter. Grundet vækst oplever kunden udfordringer med deres nuværende it-struktur. En lokal it-administrator vedligeholder enheder, men dette kan medføre inkonsistens i konfigurationer og sikkerhedsopsætning samt risiko for forældet software og potentielle udefrakommende angreb.

Den manuelle opsætning og vedligeholdelse af enhederne kræver betydelige ressourcer, hvilket resulterer i et økonomisk og tidsmæssigt behov for effektivisering. Der er yderligere behov for at forbedre sikkerheden omkring enhedsopsætning og datasikkerhed.

Kunden oplever et stigende behov for:

- effektivisering af arbejdsprocesser
- overskuelighed, struktur og nem vedligeholdelse og administration af enheder
- kontinuerlig sikkerhedsoptimering

Der ønskes et bud på, hvordan man kan effektivisere arbejdsprocesserne, øge sikkerheden og skabe overblik med minimal økonomisk bekostning.

5.1.2 Krav

Der opstilles følgende krav til løsningen:

- Løsningen skal være et centraliseret system tilgængeligt uanset geografi
- Løsningen skal kunne yde automatisering af enhedshåndtering
- Løsningen skal kontinuerligt sikre enhederne gennem opsætning af sikkerhedspolitikker og regler for opdateringer
- Løsningen skal kunne monitorere enhedernes tilstand

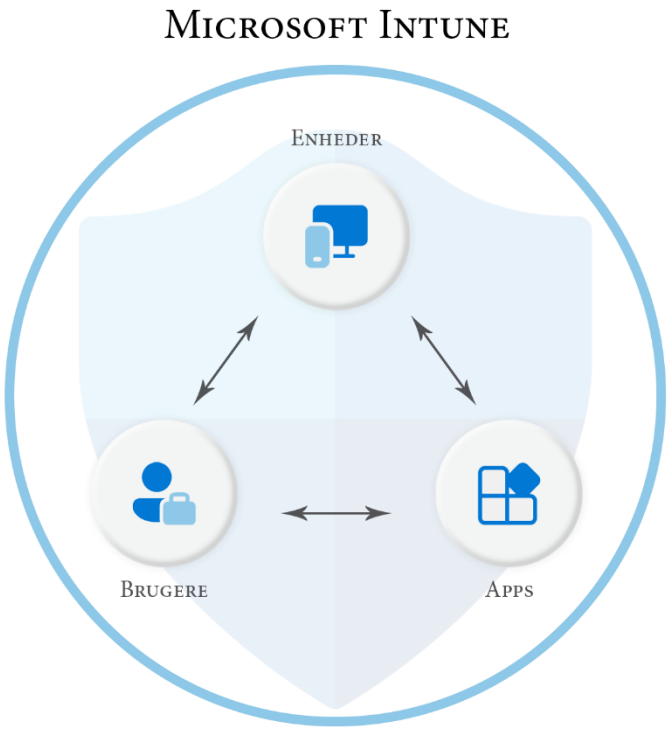
5.1.3 Design

Ved første kundemøde blev det afdækket, at 22 af de 27 medarbejdere allerede havde Microsoft 365 Business Premium licenser. Da Intune kan håndtere de oplistede krav *og* er inkluderet i Premium-licenserne, vil brugen heraf kunne betyde en større økonomisk besparelse for kunden. Dette skyldes at:

1) kunden på nuværende tidspunkt kun skal opgradere fem licenser fra Basic til Premium.
2) tjenester som fx antivirus og firewall er inkluderet i Intune og kan opsiges hos tredjepart.

Ved at udnytte de eksisterende licenser kan udgifterne således holdes nede. På baggrund af de mange betragtninger og med den tilegnede viden om systemet, er det blevet besluttet at projektet udarbejdes med basis i Intune.

Som illustreret i billede 5.1.3-A, kan Intune administrere enheder, applikationer og brugere, hvor hvert segment er tæt forbundet med hinanden. Intune's Endpoint Security omslutter hele systemet. I projektet arbejdes med alle disse elementer.



Billede 5.1.3-A: Intune's tjenester

For at projektet skal blive en succes oprettes testenheder i Azure og indrulles i Intune, brugere og brugergrupper skal oprettes, applikationer opsættes og konfigureres. Hertil opsættes sikkerhed bl.a. autentifikation, autorisation, opdateringspolitik, antivirus, firewall, kryptering, anti-phishing og anti-malware politikker. Sikkerhed og monitorering foretages i Entra, Defender og Intune.

Projektet testes løbende for at vurdere effekten af konfigurationerne. Målet er først og fremmest at opnå en grundlæggende konfiguration af enhedsopsætning og sikkerhed, for derefter at foretage målrettet finpudsning.

Som en del af arbejdsprocessens planlægning, udformes først en liste over opgaver. De blev herefter delt op i modulerne *Grundopsætning*, *Sikkerhed* og *System- & Integrationstest*. Den overordnede opgavefordeling illustreres i blokdiagrammet 5.1.3-B og en detaljeret oversigt over opgaver illustreres i Work-Breakdown-Structure diagrammet 5.1.3-C.

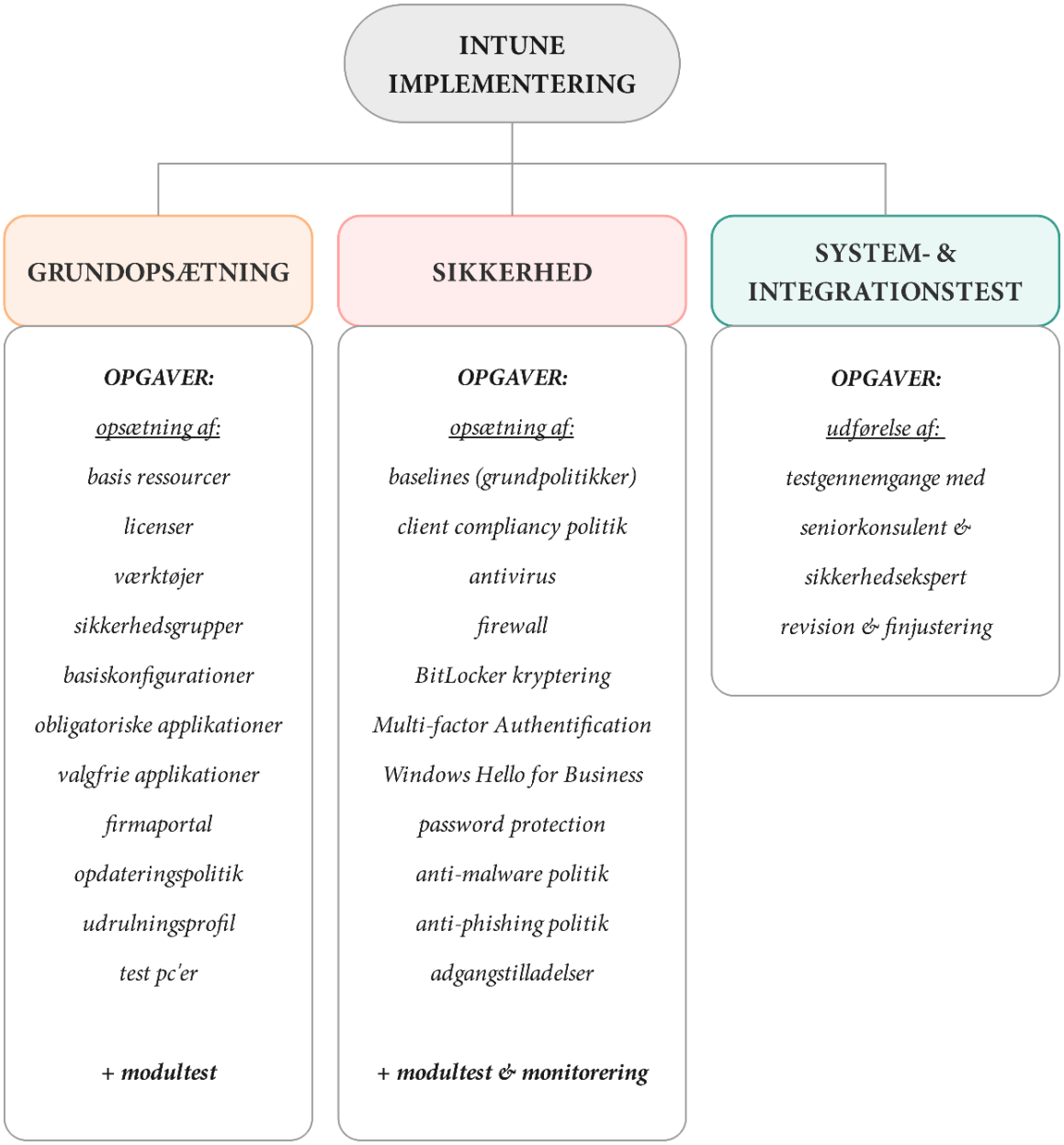


Diagram 5.1.3-B: Bilag 1: Blokdiagram

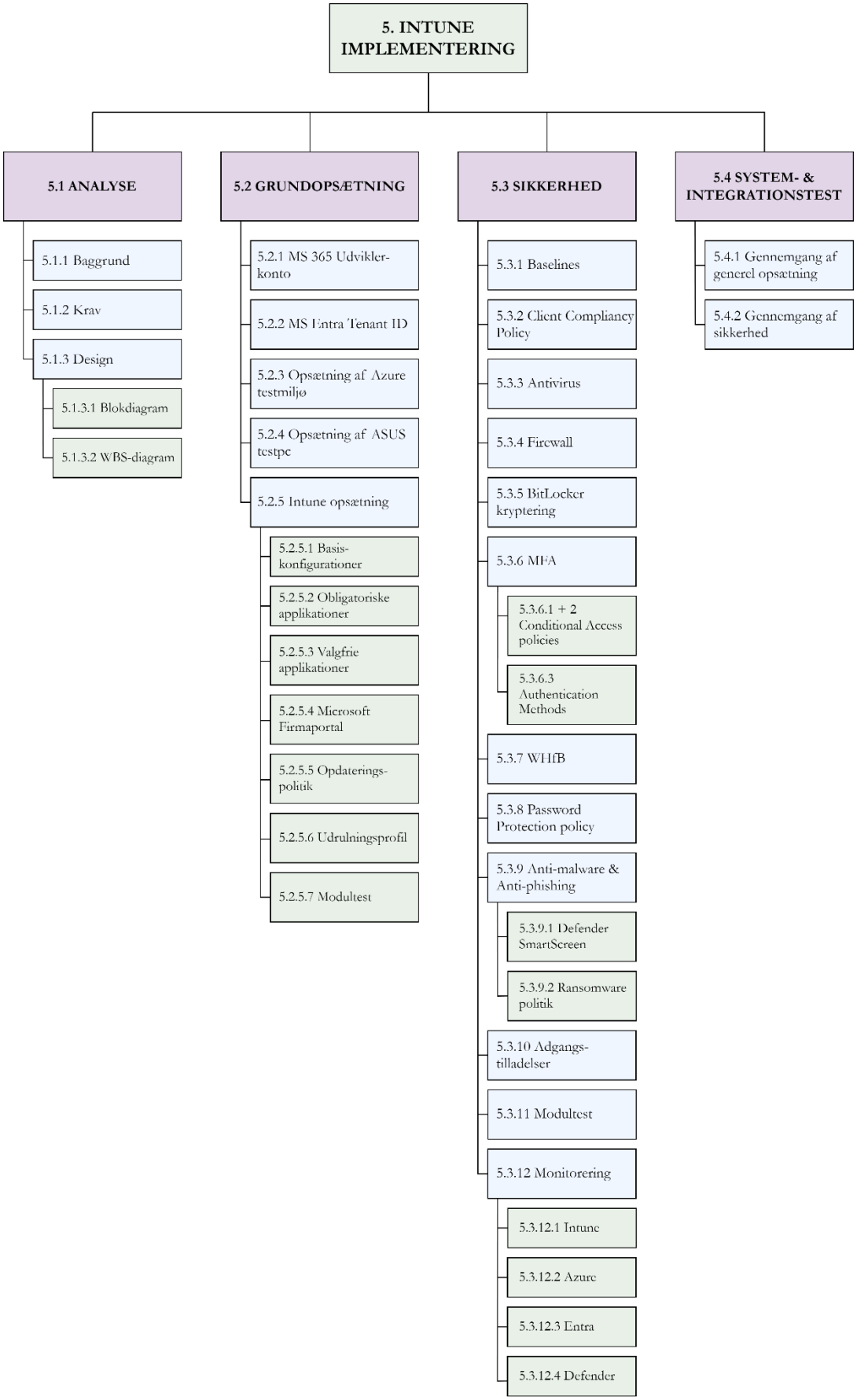
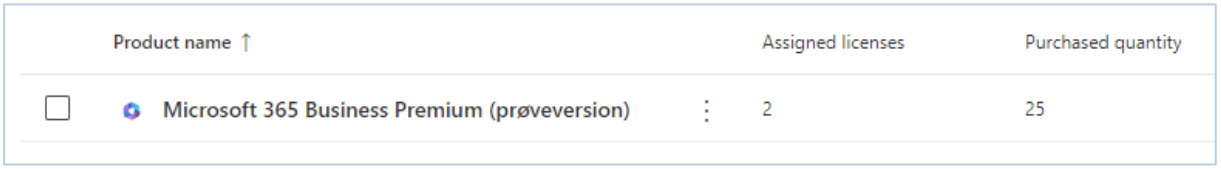


Diagram 5.1.3-C: Bilag 2: WBS-diagram over opgavefordeling

5.2 Grundopsætning

5.2.1 MS 365 udviklerkonto

For at løse projektet var det nødvendigt at oprette en MS 365 udviklerkonto med Global Administrator-rolle (GA). Dette var ikke muligt inden for NHC's domæne, hvilket hindrede adgang til vigtige sikkerhedsfeatures som oprettelse af en Tenant ID i Entra. I stedet blev en udviklerkonto oprettet under eget domæne med licenser til Microsoft 365 Business Premium, som inkluderer Intune, Azure, Entra og Defender. En testbruger blev herefter oprettet og fik tilknyttet en Premium-licens.



Billede 5.2.1-A: 2 af 25 licenser er i brug til testformål, Admin Center

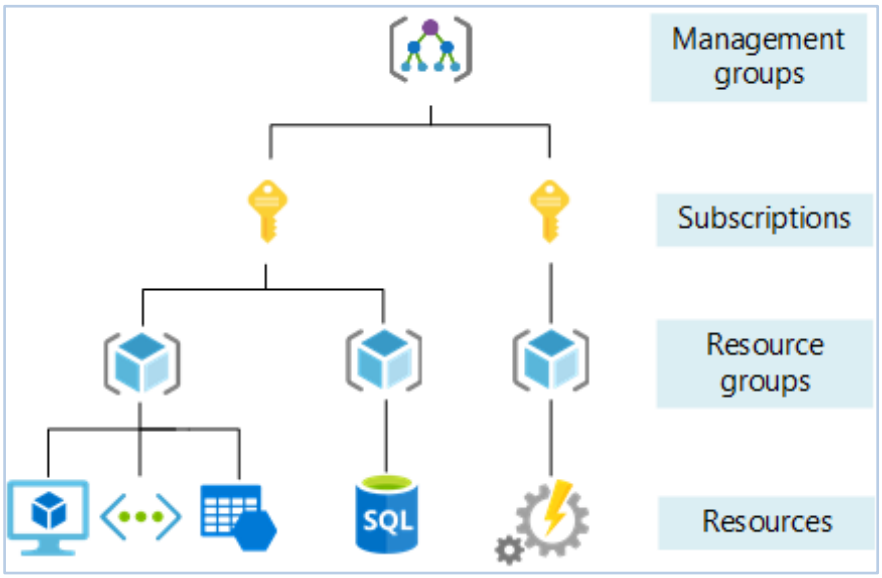
5.2.2 Microsoft Entra ID – Tenant ID

Intune og Azure kan tilgås blot ved login med GA-brugeren, men begge systemer afhænger af en Entra Tenant ID til identitetsstyring, adgangskontrol, enheds- og applikationshåndtering samt monitorering. Efter at have løst problematikken omkring administrator-rettigheder nævnt i afsnit 5.2.1, kunne Entra ID-platformen tilgås, hvor et Tenant ID automatisk blev oprettet.

Et Tenant ID er unikt for domænet og fungerer som bindeled mellem organisationens AD-infrastruktur og de digitale ressourcer på platformene. Med forbindelsen på plads synkroniseres platformene - således vil brugere oprettet i Admin Center automatisk figurer i Intune, ligesom virtuelle maskiner, oprettet i Azure også automatisk figurerer under Devices i Intune, når der logges ind med en Microsoft domæne-bruger. Ligeledes vil enheder og den opsatte sikkerhed kunne administreres og monitoreres i Intune, Entra og Defender.

5.2.3 Opsætning af Azure testmiljø

Azure er bygget op efter en hierarkisk struktur, hvor ressourcer skal oprettes i en bestemt rækkefølge. Hierarkiet i Azure kan illustreres således:

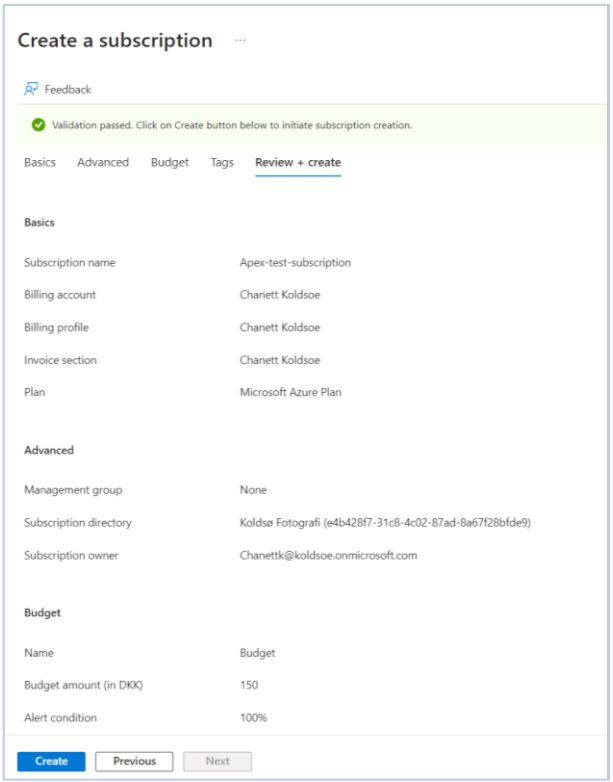


Billede 5.2.3-A: Hierarkisk opbygning i Azure
Kilde: Microsoft Learn

Ved login med GA-brugeren blev adgang til Azure platformen opnået.

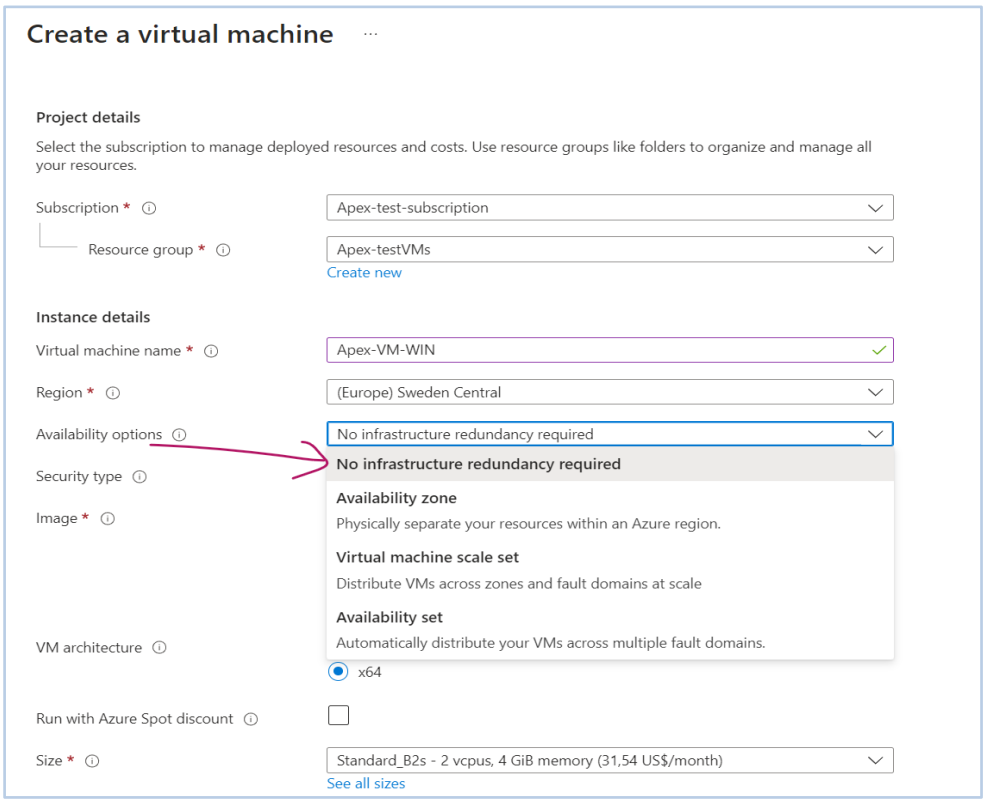
Opsætning af et testmiljø i Azure begyndte med oprettelse af subskriptions. "Pay-as-you-go"-modellen blev valgt og er ideel til projektbaserede formål.

Efterfølgende blev et par ressourcegrupper oprettet og tilknyttet abonnementerne. Herefter blev de virtuelle maskiner opsat.

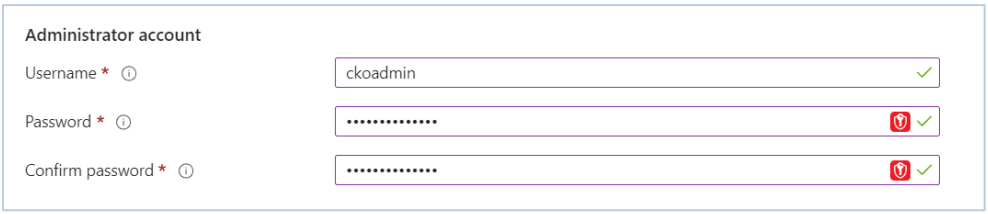


Billede 5.2.3-B: Subscription oprettes

De virtuelle maskiner blev oprettet og konfigureret med de nødvendige specifikationer delvis efter anbefalinger fra Ømer.

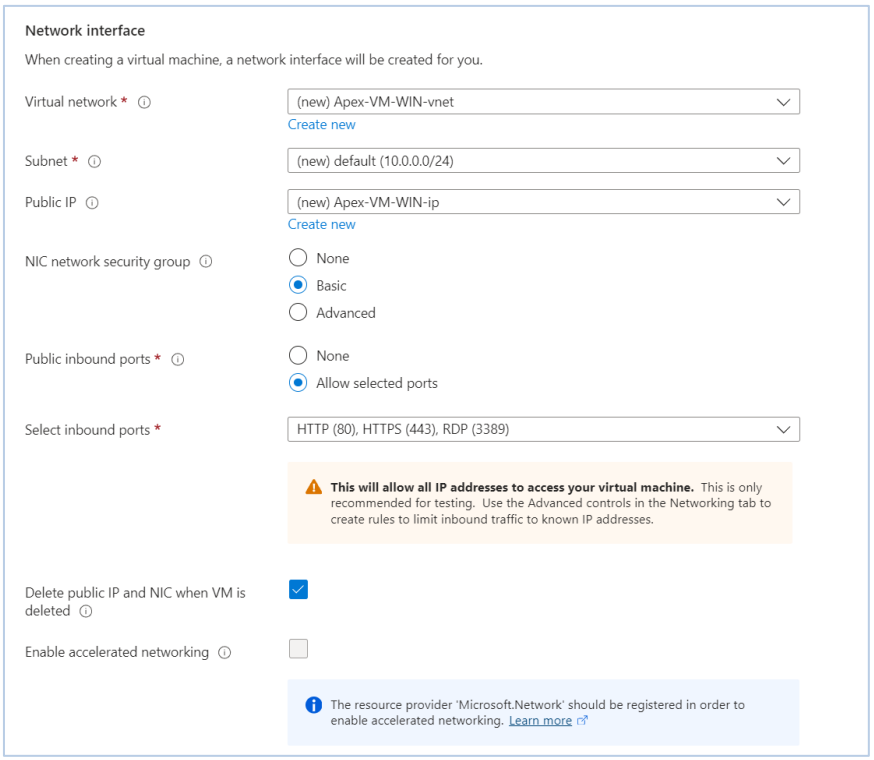


Billede 5.2.3-C: Basics indstillinger sættes, Azure VM

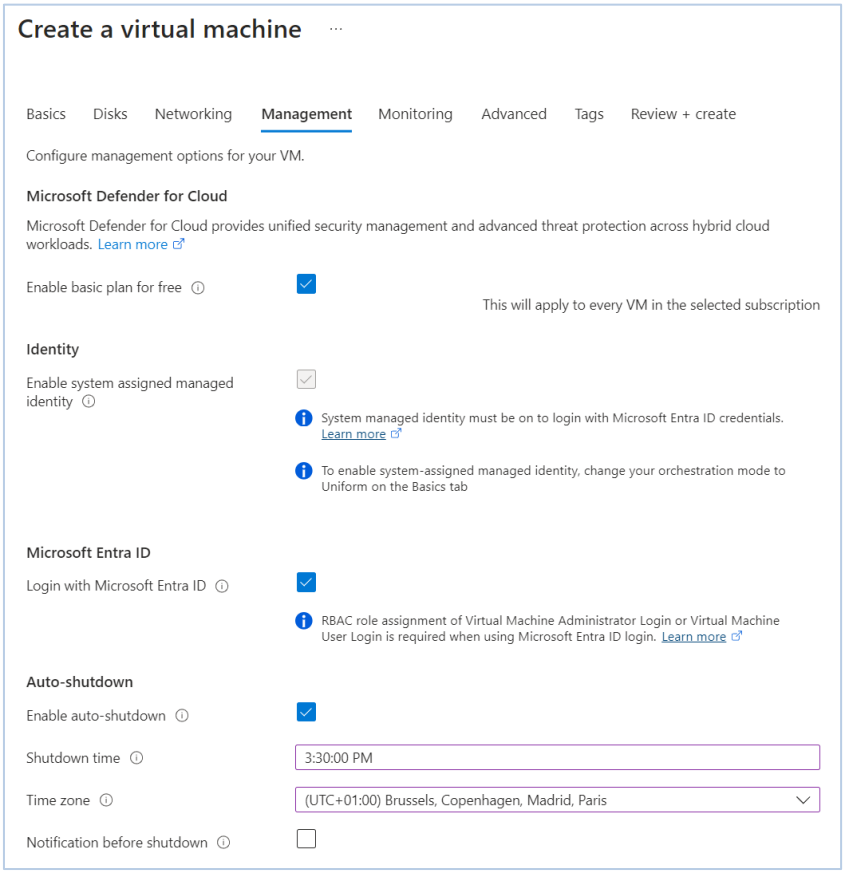


Billede 5.2.3-D: lokal admin opsættes, Azure VM

Sikkerhedsindstillingerne blev sat til standard og redundans fravalgt i dette tilfælde. Sikkerheds-funktioner, som tillader login med Entra ID aktiveres. Entra ID bruges når testmaskiner ind-rulles i Intune ved hjælp af "Entra ID Join". Et tidspunkt for automatisk shutdown sættes.

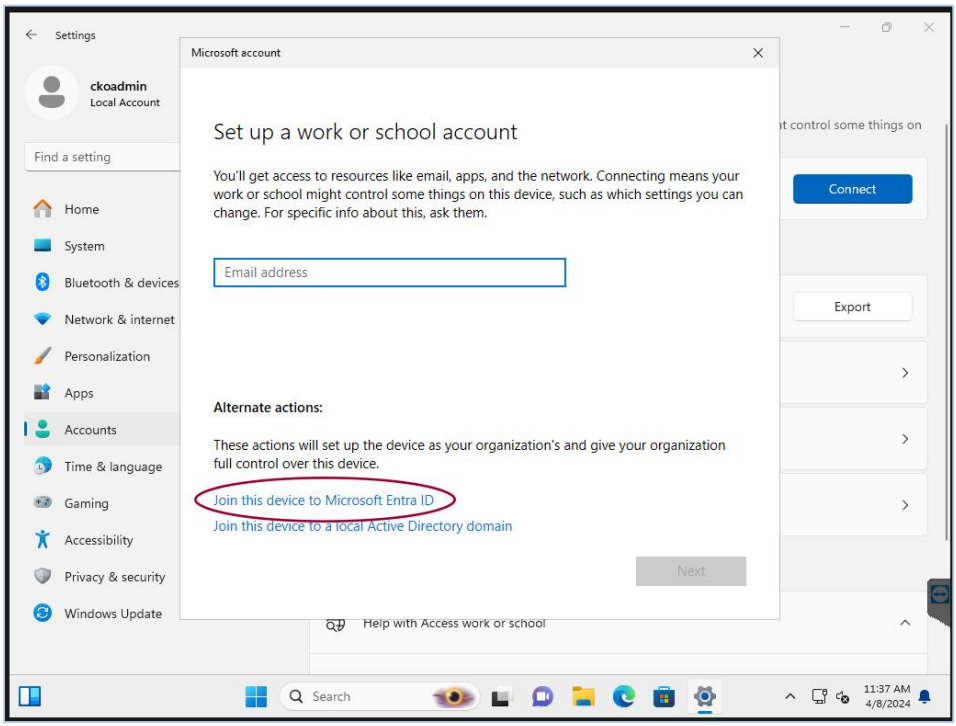


Billede 5.2.3-E: Netværksinterface sættes, Azure VM



Billede 5.2.3-F: Entra ID aktiveres og shutdown sættes, Azure VM

Forbindelsen til testmaskinerne viste sig udfordrende, da brugerskifte via RDP fjernskrivebord lukkede forbindelsen. Dette blev løst ved at installere TeamViewer med Unattended Access, hvilket gjorde det muligt at skifte brugere uden at miste forbindelsen. Herefter blev maskinerne tilsluttet Microsoft Entra ID.



Billede 5.2.3-G: Virtuel pc join

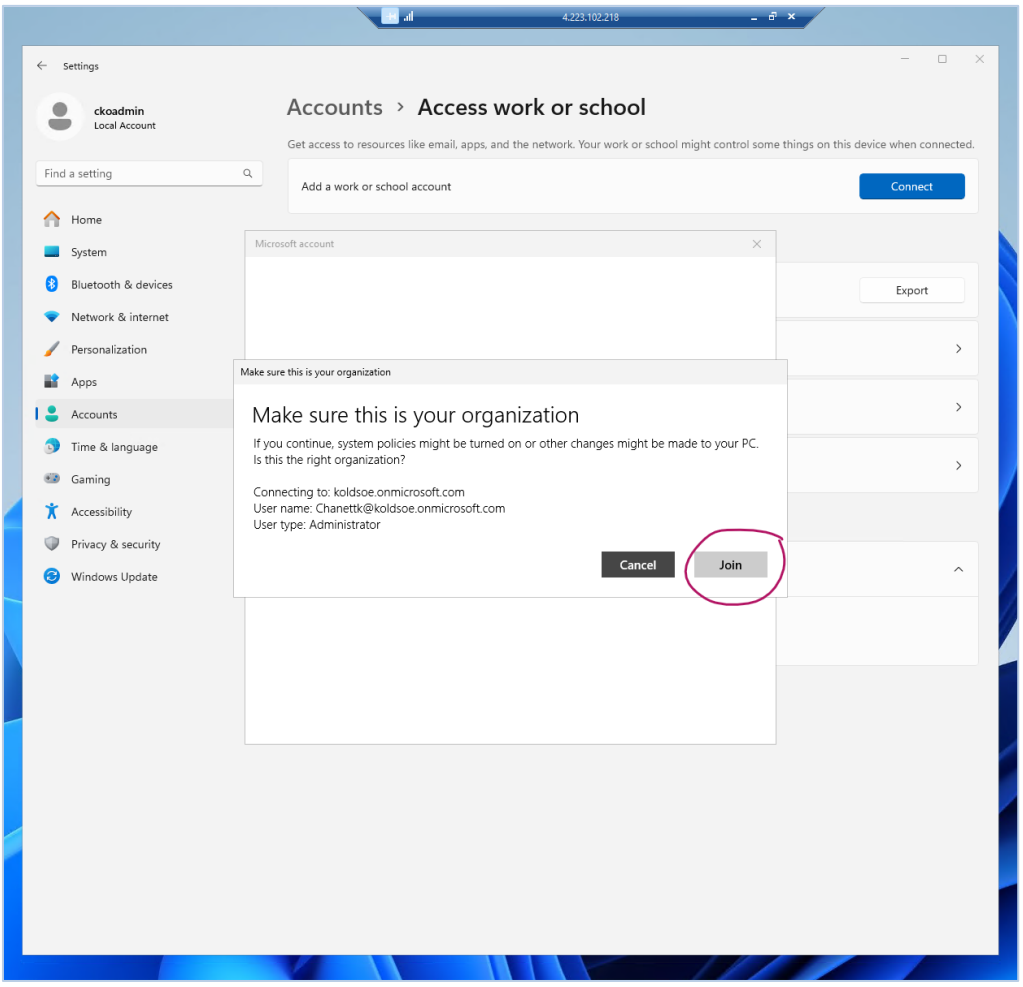
Når enheden er forbundet til domænet, indrulles den automatisk i Intune[3], som påbegynder konfigurationerne, hvorefter man kan logge ind med Microsoft-brugeren.

Processen er uddybet i detaljer i **Bilag 3: Azure opsætning**.

5.2.4 Opsætning af ASUS test pc

Den gamle ASUS formateres til Windows 11 Pro og opsættes med en lokal admin-bruger. Efter konfiguration blev chanettk@koldsoe.onmicrosoft.com kyttet til enheden via Microsoft Entra ID join.

[3] *"Automatic Intune enrollment via Microsoft Entra join" af Microsoft Learn*



Billede 5.2.4-A: Konto tilknyttes med Microsoft Entra ID Join, ASUS

Herefter blev der logget ind med GA-brugeren, hvorefter computeren påbegyndte konfigurationen, der tog 19 minutter. Ved login var Firmaportal, Adobe Acrobat og Office installeret og automatisk login til OneDrive blev observeret i procesbjælken.

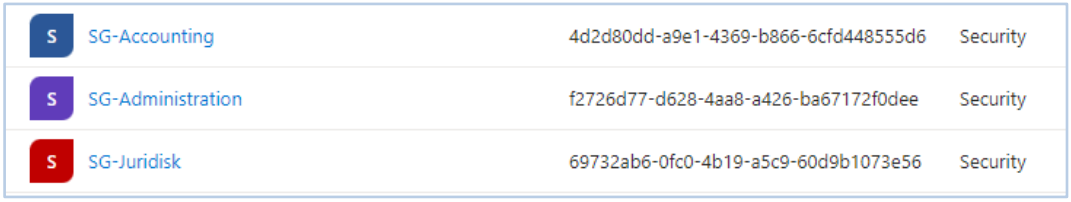
Efter tilknytning fremgik alle enheder i Intune under Devices.

Device name	Managed by	Ownership	Compliance	OS
Apex-VM-WIN	Intune	Corporate	Compliant	Windows
CK-ASUS	Intune	Corporate	Compliant	Windows
VM-WIN	Intune	Corporate	Compliant	Windows

Billede 5.2.4-B: Enhederne figurerer under Intune ► Devices.

5.2.5 Intune opsætning

Adgangen til Intune blev opnået ved login med GA-brugeren. Her blev tre sikkerhedsgrupper oprettet og navngivet **SG-***: **SG-Accounting, SG-Administration** og **SG-Juridisk**. Ved efterfølgende at tilgå *Entra* ▷ *Identity* ▷ *Groups* kunne sikkerhedsgrupperne også findes dér og ligeledes kunne de oprettede testbrugere fra Admin Center findes i både Entra og Intune. Dermed konkluderes korrekt synkronisering mellem de tre platforme.



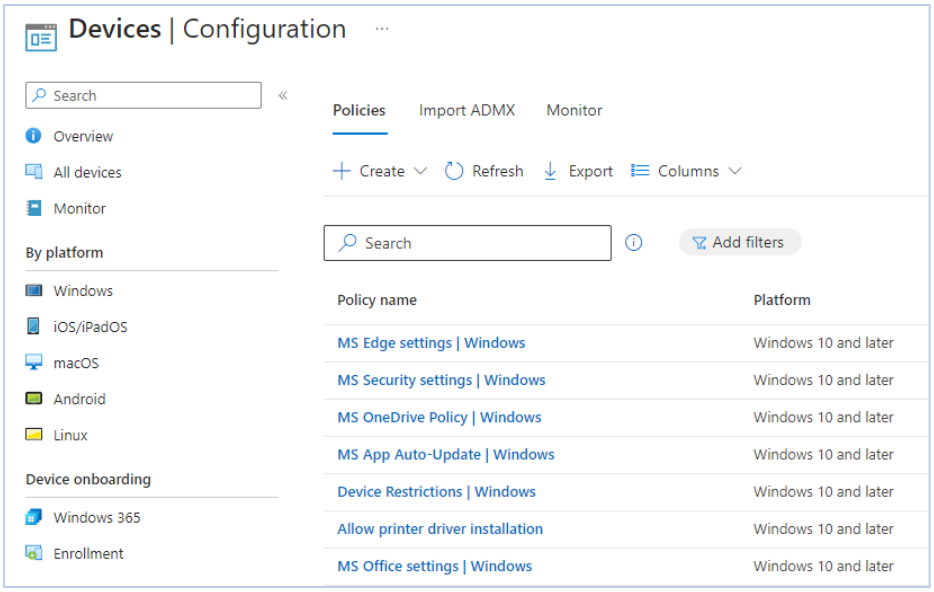
Billede 5.2.5-A: Oversigt over sikkerhedsgrupper i Entra

Sikkerhedsgrupper bør oprettes *inden* konfigurationer påbegyndes, da grupperne bruges til tildeling af konfigurationsprofiler, sikkerhedspolitikker, apps m.v.

5.2.5.1 Basiskonfigurationer

Projektet tager udgangspunkt i enheder med Windows 11. De indbyggede konfigurationer i Windows-operativsystemet behandles ikke i Intune, i stedet foretages sikkerhedsstramninger og justeringer til enhedsadfærd.

Et par generelle konfigurationsprofiler oprettes, men størstedelen af konfigurationerne omhandler adfærd og sikkerhedsstramninger i Microsoft applikationer. Profilerne indeholder segmenter af både brugeroplevelse og sikkerhed, hvorfor rapporten fokuserer på disse to segmenter. Konfigurationsprofilerne kan tilgås fra *Intune* ▷ *Devices* ▷ *Configuration*.



Billede 5.2.5.1-A: Oversigt over konfigurationsprofiler set under Devices ▷ Configuration, Intune

5.2.5.1.1 Sikkerhed

DEVICE RESTRICTIONS | WINDOWS *(Bilag 4)*

Brugere forhindres i at tilføje andre konti end deres godkendte Microsoft-konto til Cloud og Storage units samt forhindrer manuel fjernelse af enheden fra Intune.

MS APP AUTO-UPDATE | WINDOWS *(Bilag 5)*

Automatisk opdatering af Microsoft Store applikationer aktiveres.

MS OFFICE SETTINGS | WINDOWS *(Bilag 6)*

Muligheden for at aktivere/deaktivere Office-opdateringer skjules og automatisk software opdatering aktiveres for Office-applikationer.

MS SECURITY SETTINGS | WINDOWS *(Uddybet i bilag 7)*

Flash player i Office blokeres grundet udfasning i 2020[4] og Office-applikationer blokerer makroer, for at forhindre malware-implementering, da makroer kan udnyttes til netop dette.[5]

5.2.5.1.2 Brugeroplevelse

MS OFFICE SETTINGS | WINDOWS

Opstartsskærm samt demovideo deaktiveres for alle Office-applikationer og Opt-in Wizard. Edge sættes som standard weblink-behandler. Indstillinger i Excel og Word, som filformat og måleenheder fastsættes. Outlook-præferencer som kalenderindstillinger og arbejdstid sættes.

MS EDGE SETTINGS | WINDOWS *(Bilag 8)*

Startskærm for Edge deaktiveres, og browser sign-in med brugerens Microsoft-konto aktiveres. Synkronisering af browserdata mellem browsers gennemtvinges og Google sættes som startside og søgemaskine.

MS ONEDRIVE POLICY | WINDOWS *(Uddybet i bilag 9)*

Opstartsanimation deaktiveres, systemnotifikationer skjules, og mapperne *Desktop*, *Documents* og *Pictures* flyttes til OneDrive i baggrunden. Brugeren logges ind med sin Microsoft-konto.

ALLOW PRINTER DRIVER INSTALLATION *(Bilag 10)*

Brugere tillades at installere printerdrivere uden admin-rettigheder.

---

[4] *"Flashplayer - End of life" af Adobe.com*

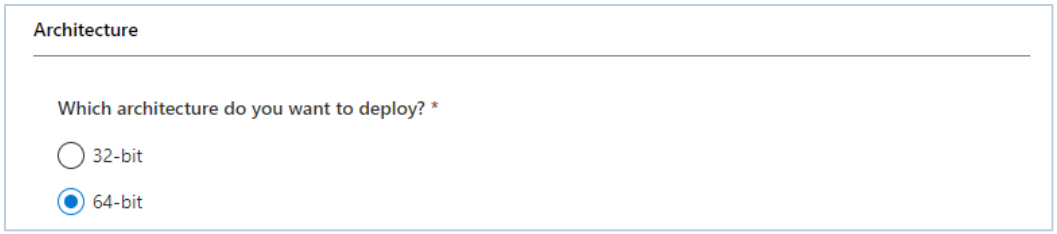
[5] *"Internet macros blocked" af Microsoft Learn*

5.2.5.2 Opsætning af obligatoriske applikationer

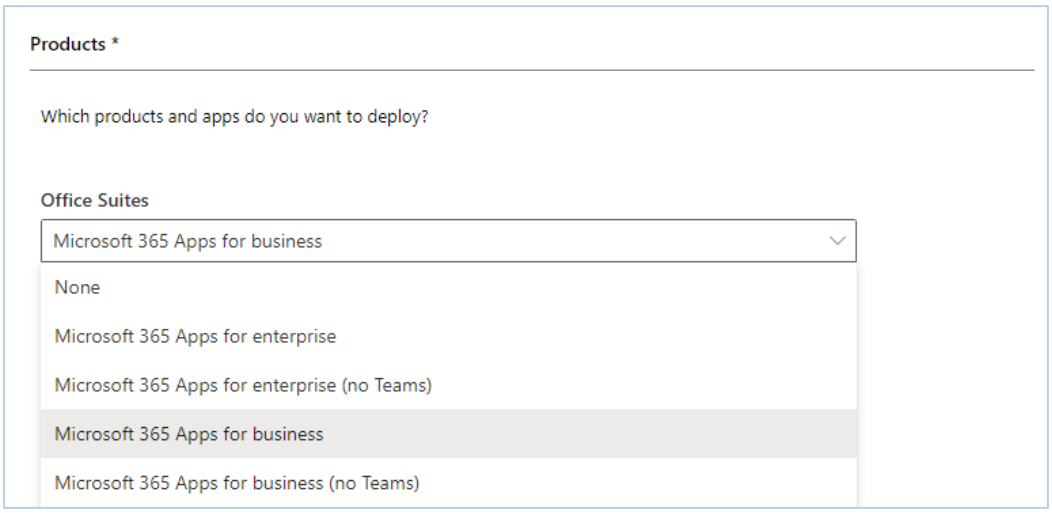
5.2.5.2.1 Microsoft Office 365

Den første opsatte applikation er Office 365-pakken. Ved hjælp af Microsofts pakkegenerator[6] kan administratoren selv oprette en Office-pakke og eksportere indstillingerne som en XML-fil. Denne fil kan derefter uploades til Intune, som installerer pakken med de valgte indstillinger. Applikationerne tilgås fra *Intune* ▷ *Apps* ▷ *Windows*.

Processen illustreres nedenfor:

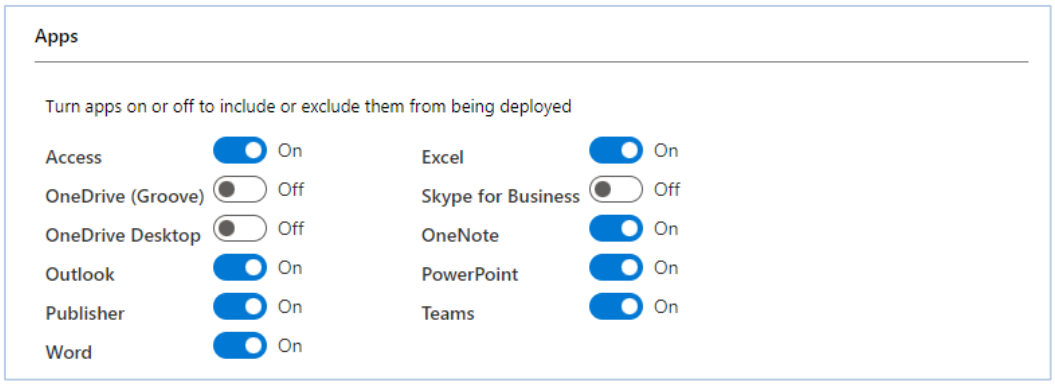


Billede 5.2.5.2.1-A: Systemversion vælges i pakkegenerator

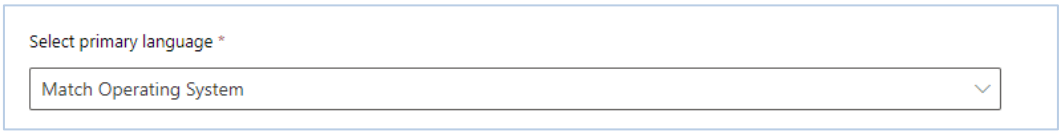


Billede 5.2.5.2.1-B: Office variant vælges i pakkegenerator

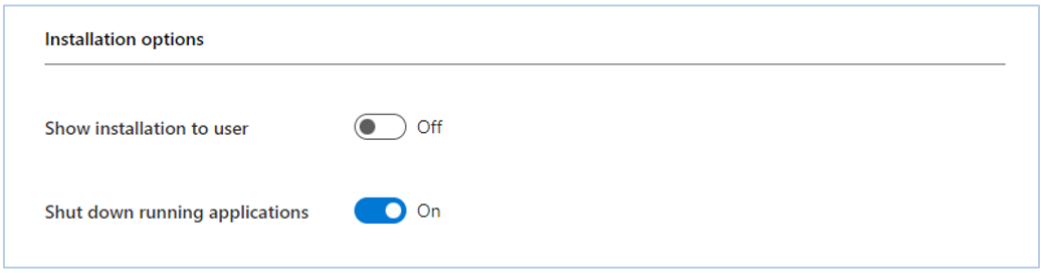
[6] https://config.office.com/deploymentsettings



Billede 5.2.5.2.1-C: Apps tilvælges i pakkegenerator

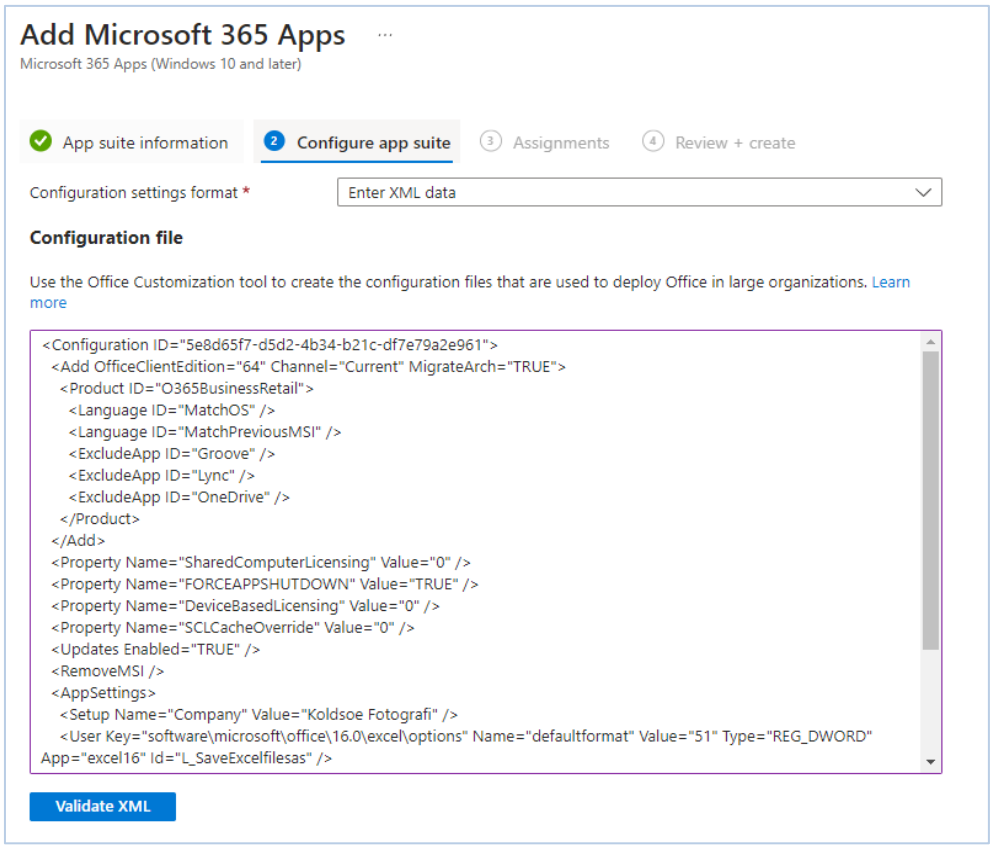


Billede 5.2.5.2.1-D: Sprog opsættes i pakkegenerator



Billede 5.2.5.2.1-E: Installation skjules for brugeren og kørende applikationer lukkes

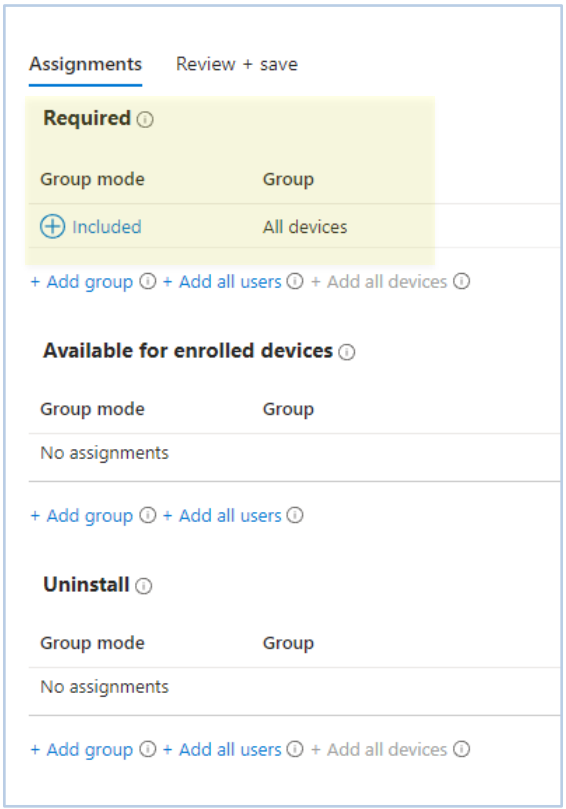
Installationen konfigureres til automatisk at acceptere softwareopdateringer og brugervilkår. Produktet aktiveres og firmanavn opsættes. Derefter eksporteres den som en XML-fil til opsætning af Office 365 i Intune.



Billede 5.2.5.2.1-F: XML indsættes ved konfiguration af Office 365 app

Under *Assignments* specificeres, hvilke brugere og/eller enheder der skal modtage applikationerne, samt om de skal installeres obligatorisk (*Required*) eller være valgfri via Microsoft Firmaportal (*Available for enrolled devices*).

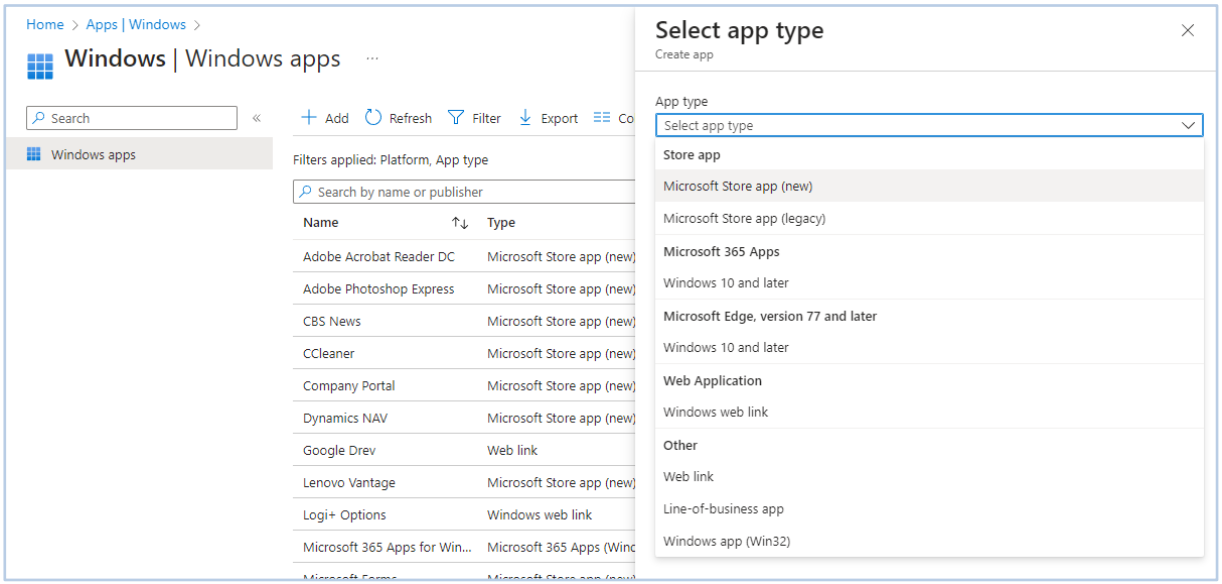
For alle Windows-enheder er installationen obligatorisk. Andre obligatoriske applikationer inkluderer Adobe Acrobat Reader og Microsoft Firmaportal.



Billede 5.2.5.2.1-G: Assignments indstillinger i Intune

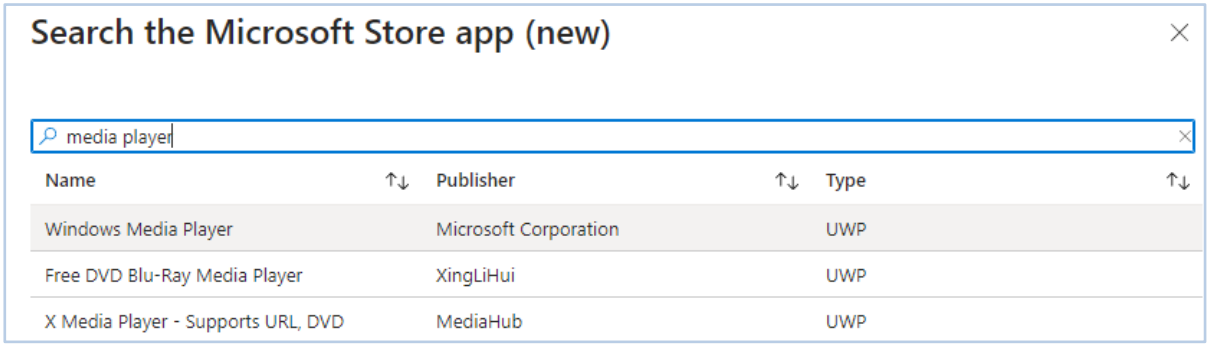
5.2.5.3 Opsætning af valgfrie applikationer

Afsnittet demonstrerer, hvordan en valgfri applikation opsættes i Microsoft Firmaportal. En ny app tilføjes ved at vælge app-type, her vælges Microsoft Store app. Derefter søges der efter en specifik app.

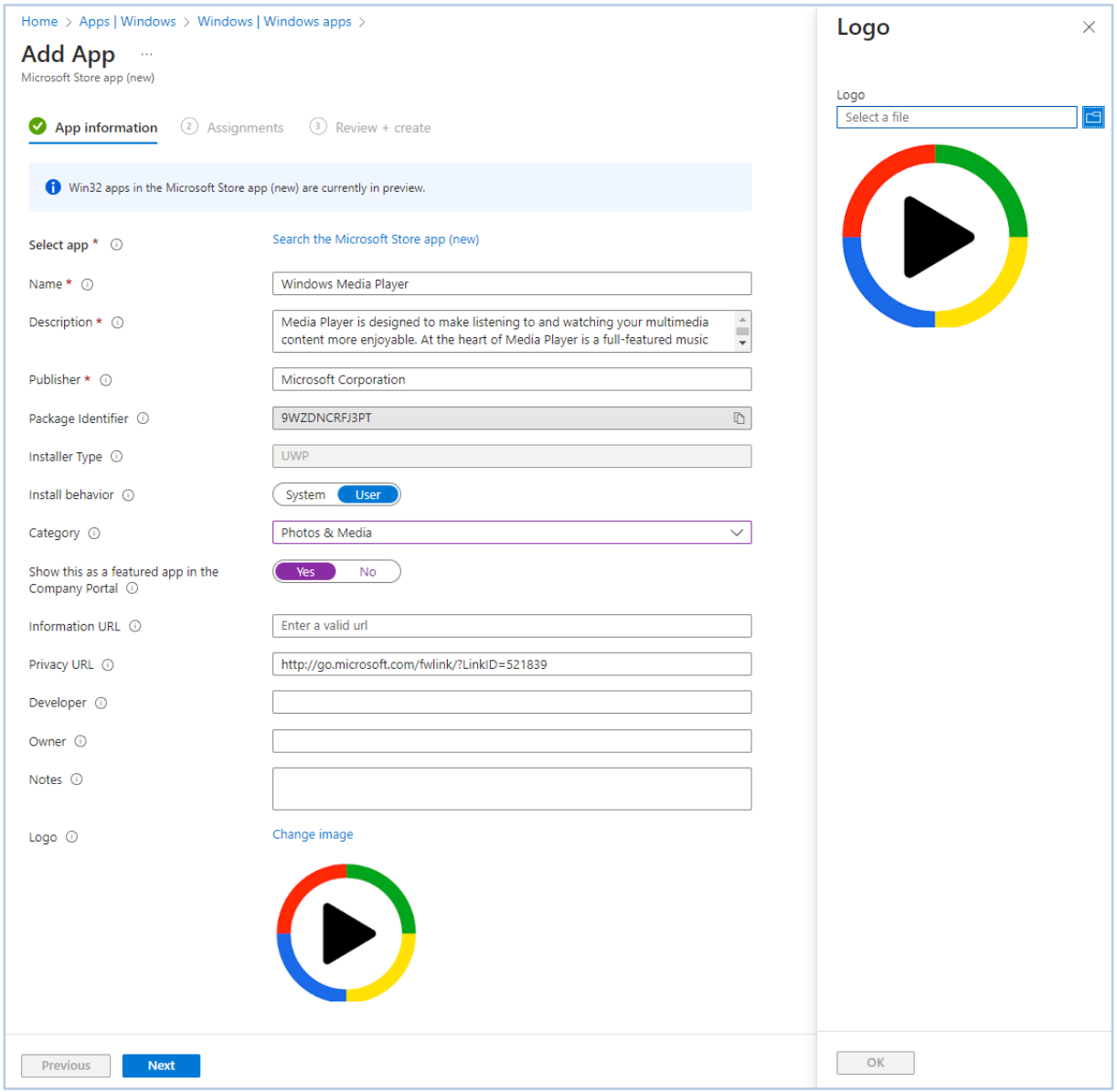


Billede 5.2.5.3-A: Tilføjer ny app ved at vælge app type Microsoft Store app fra listen

Som eksempel vælges her Windows Media Player.



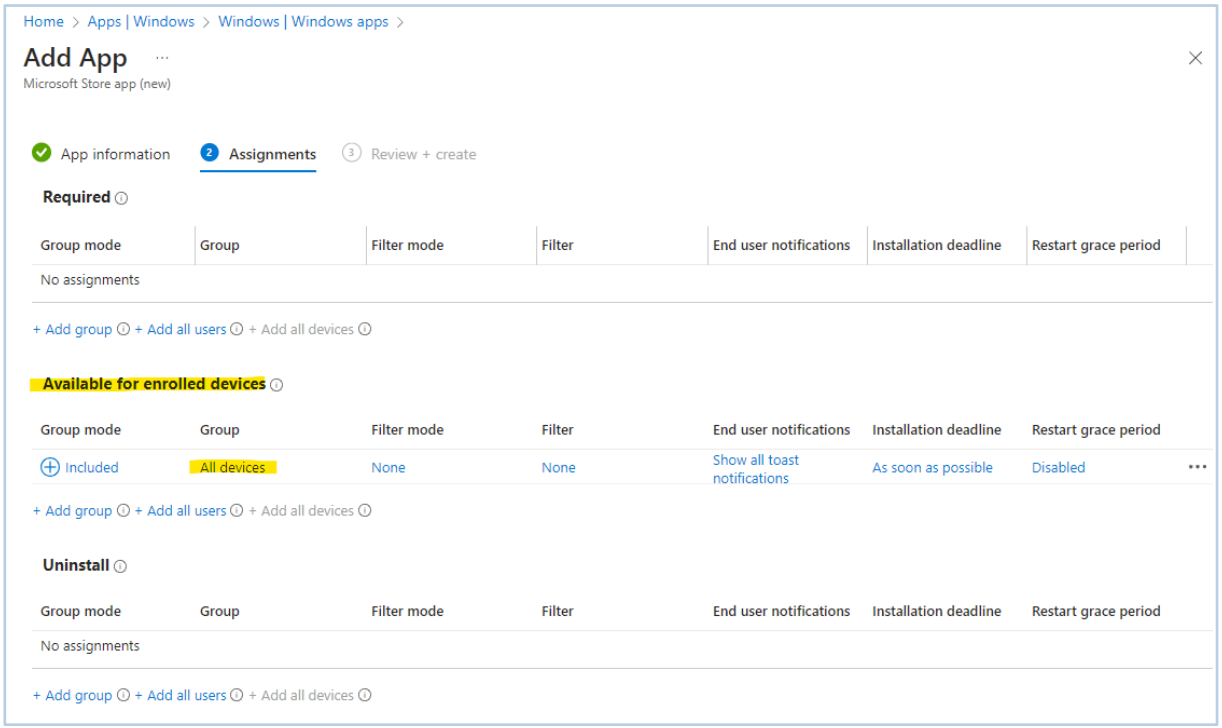
Billede 5.2.5.3-B: App fundet ved søgning



Billede 5.2.5.3-C: App pre-konfiguration, logo uploades manuelt.

Efter valg af app vises en pre-konfiguration, som vist på billede 5.2.5.3-C. Her angives kategori og tilgængelighed i Firmaportalen. Et logo uploades manuelt og bruges som thumbnail i Firmaportalen.

Under *Assignments* angives, hvilke enheder eller grupper app'en skal tildeles, og om den skal være valgfri eller obligatorisk i Firmaportalen.

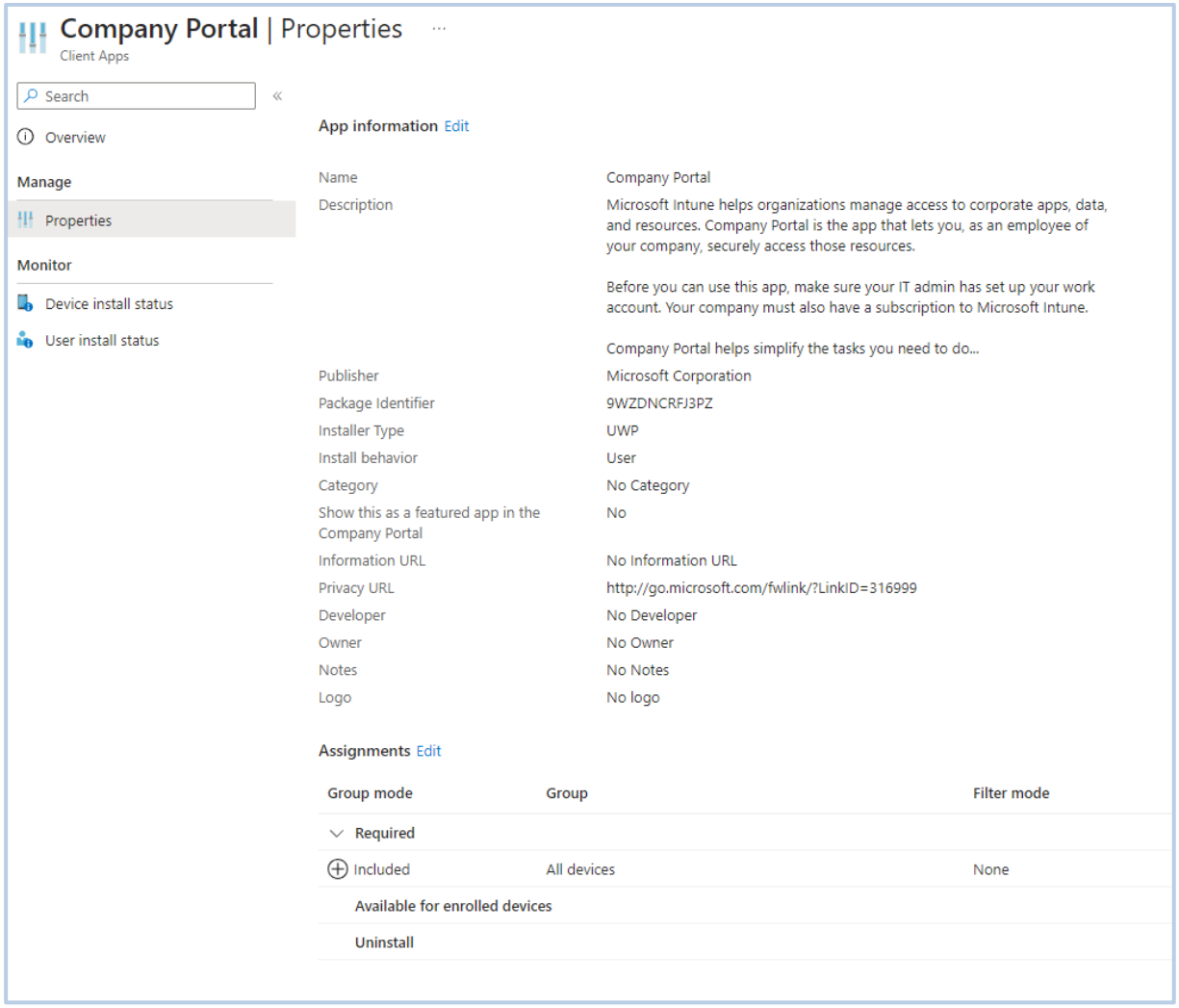


Billede 5.2.5.3-D: App creation ► Assignments

I dette tilfælde gøres den valgfri og tilgængelig i Firmaportal for alle Windows-enheder. Nogle af de opsatte applikationer har tilknyttet særskilte brugergrupper til senere testformål, dokumenteret i afsnit 5.3.10 Adgangstilladelser.

5.2.5.4 Opsætning af Application Manageren "Microsoft Firmaportal"

Projektets fokus på sikkerhedsforbedringer inkluderer begrænsning af brugernes downloadmuligheder fra internettet. Microsoft Firmaportal opsættes med nødvendige applikationer til virksomhedens opgaver som regnskabs- og bookingsystemer, økonomiprogrammer og medieapps. Den konfigureres som en obligatorisk Microsoft Store-app for alle Windows-enheder ved at vælge *Required* og *All Devices* under *Assignments*. Adgang til firmaressourcer afhænger af enhedens overholdelse af virksomhedens Compliancy Policy, detaljeret i test afsnit 5.3.11.1 Compliancy.



Billede 5.2.5.4-A: Konfigurationsprofil for Company Portal, Intune

Administratorens opgave er at sikre, at kun "trusted" applikationer opsættes. Dette opnås bedst ved kun at vælge software fra certificerede partnere såsom Microsoft Store.

5.2.5.5 Opdateringspolitik

Sidste skridt er at opsætte en opdateringspolitik (***bilag 11***), der styrer, hvordan opdateringer modtages og udføres, og som sætter brugerbegrænsninger for at sikre enhedens sikkerhed. Profilen baseres på Microsofts anbefalinger og oprettes under *Devices* ▷ *Windows 10 and later updates*, hvor den tilrettes efter behov med fokus på sikkerhed.

Nøglepunkterne er følgende:

- Kvalitetsopdateringer kan ikke udsættes.
- Funktionsopdateringer kan udsættes med maks. 25 dage.
- Windows 10 enheder opgraderes til Windows 11 OS.
- Windows opdateringer kan ikke pauses, men brugere kan søge efter opdateringer.
- Opdateringer installeres automatisk i ønsket tidsrum.
- Der sættes en deadline for installation.

Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	25
Upgrade Windows 10 devices to Latest Windows 11 release	Yes
Set feature update uninstall period (2 - 60 days)	20
Servicing channel	General Availability channel
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	4 PM
Option to pause Windows updates	Disable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	2
Grace period	2
Auto reboot before deadline	No

Billede 5.2.5.5-A: Bilag 11, opdateringspolitik opsat i Intune

5.2.5.6 Opsætning af udrulningsprofil

Under *Devices* ▷ *Enrollment* ▷ *Enrollment Status Page* opsættes retningslinjerne for, hvordan konfigurationerne skal udrulles.

Basics

Name	All users and all devices
Description	This is the default enrollment status screen configuration applied with the lowest priority to all users and all devices regardless of group membership.

Settings Edit

Show app and profile configuration progress	Yes
Show an error when installation takes longer than specified number of minutes	30
Show custom message when time limit or error occurs	Yes
Error message	Setup could not be completed. Please try again or contact your support person for help.
Turn on log collection and diagnostics page for end users	Yes
Only show page to devices provisioned by out-of-box experience (OOBE)	Yes
Block device use until all apps and profiles are installed	Yes
Allow users to reset device if installation error occurs	Yes
Allow users to use device if installation error occurs	Yes
Only fail selected blocking apps in technician phase	No
Block device use until required apps are installed if they are assigned to the user/device	Adobe Acrobat Reader DC Company Portal Office 365

Assignments

Included groups	All devices

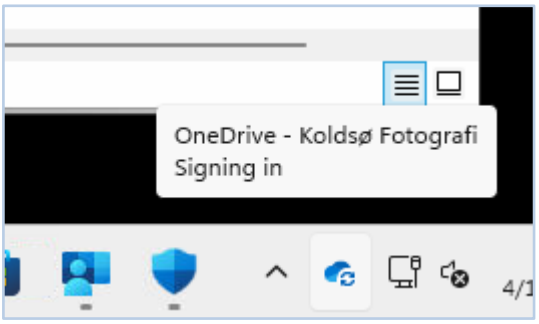
Billede 5.2.5.6-A: Bilag 12, konfiguration for enhedsudrulning i Microsoft Intune

Målet er at konfigurere enheden efter indtastning af Microsoft-konto og først åbne brugeradgang efter konfigurationerne er fuldført. Adobe Acrobat Reader, Firmaportal og Office 365-applikationerne skal være installeret før adgang gives, hvilket sigter mod at forbedre brugeroplevelsen. Andre tidligere oprettede profiler som automatisk login til OneDrive gælder også. Disse retningslinjer styrer enhedskonfigurationer og sikkerhedspolitikker, som beskrevet i afsnit 5.3 Sikkerhed.

5.2.5.7 Test af konfigurationer

5.2.5.7.1 Autologon

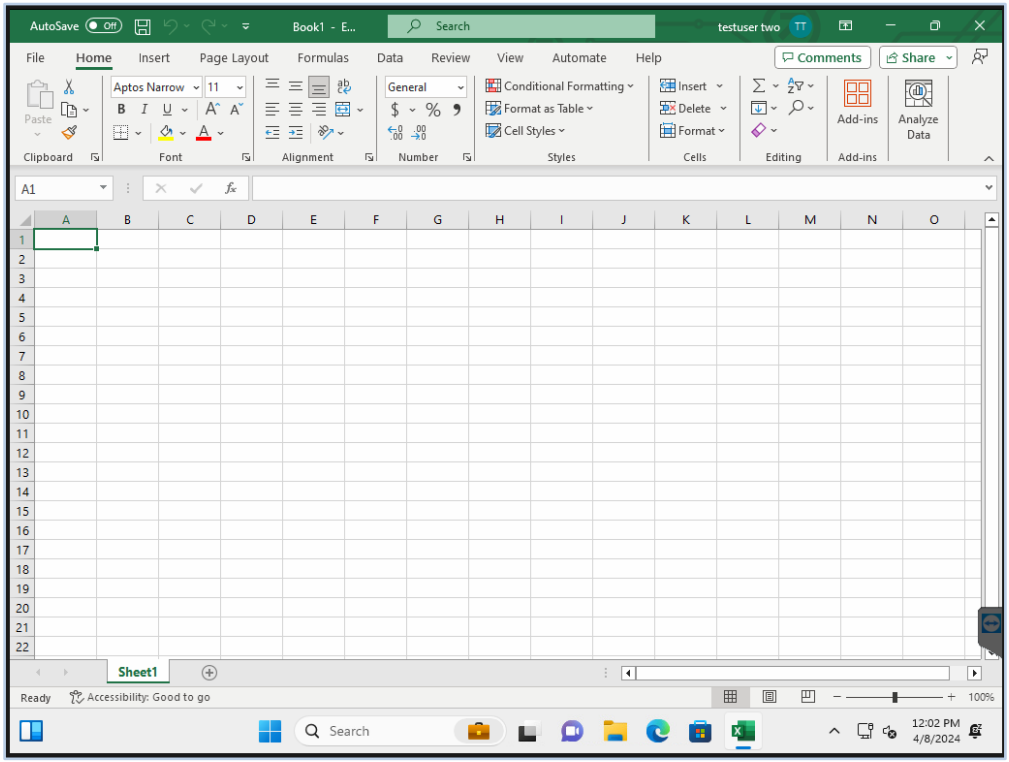
Efter opstart observeres om brugeren logges ind i OneDrive i baggrunden. Som billede 5.2.5.7.1-A demonstrerer logges brugeren ind i OneDrive i baggrunden. Billede 5.2.5.7.2-A demonstrerer hvordan *testuser two* er logget ind i Office applikationerne ved opstart. Dermed konkluderes testen at være succesfuld.



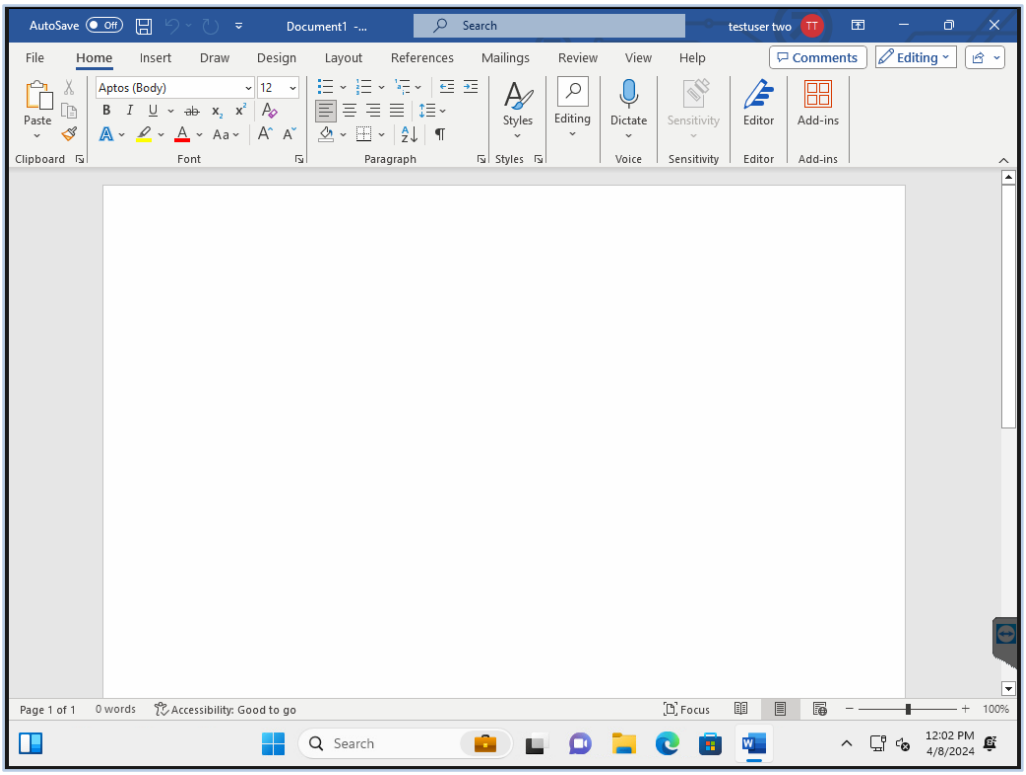
Billede 5.2.5.7.1-A: Autologon tavst i baggrunden

5.2.5.7.2 Applikationsopstart

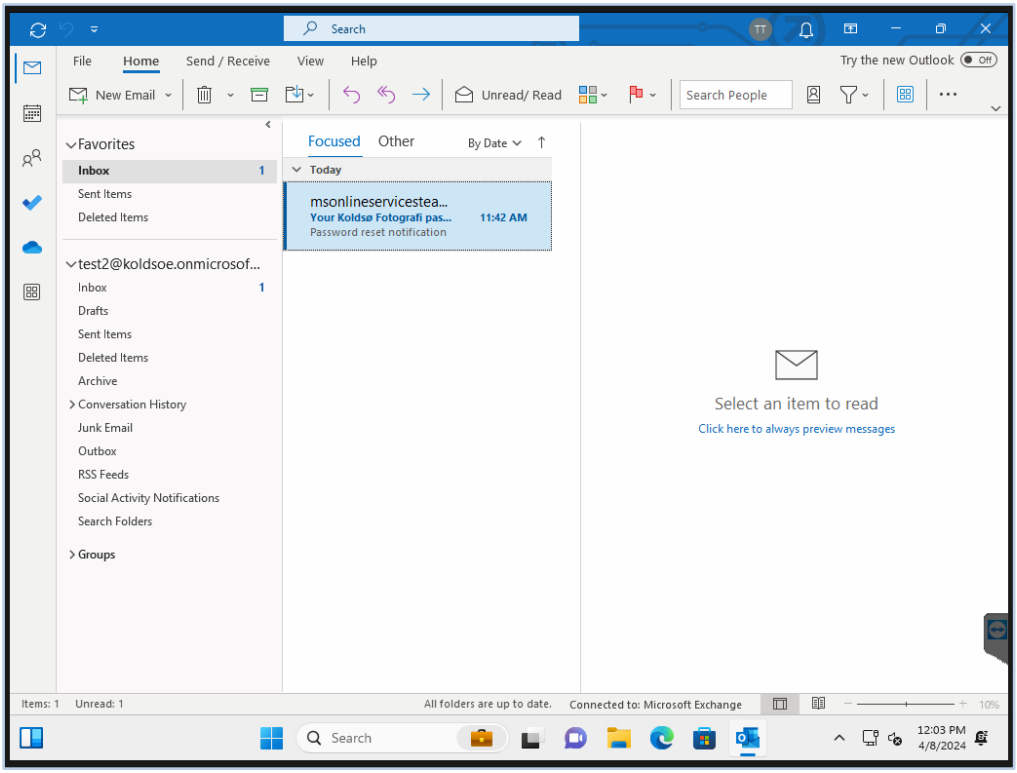
Efter login tilgik jeg programmerne Excel, Word og Outlook for at tjekke, om startskærmen med tips og vejledning for de pågældende applikationer var deaktiveret, som ønsket.



Billede 5.2.5.7.2-A: Startskærm deaktiveret i Excel



Billede 5.2.5.7.2-B: Startskærm deaktiveret i Word

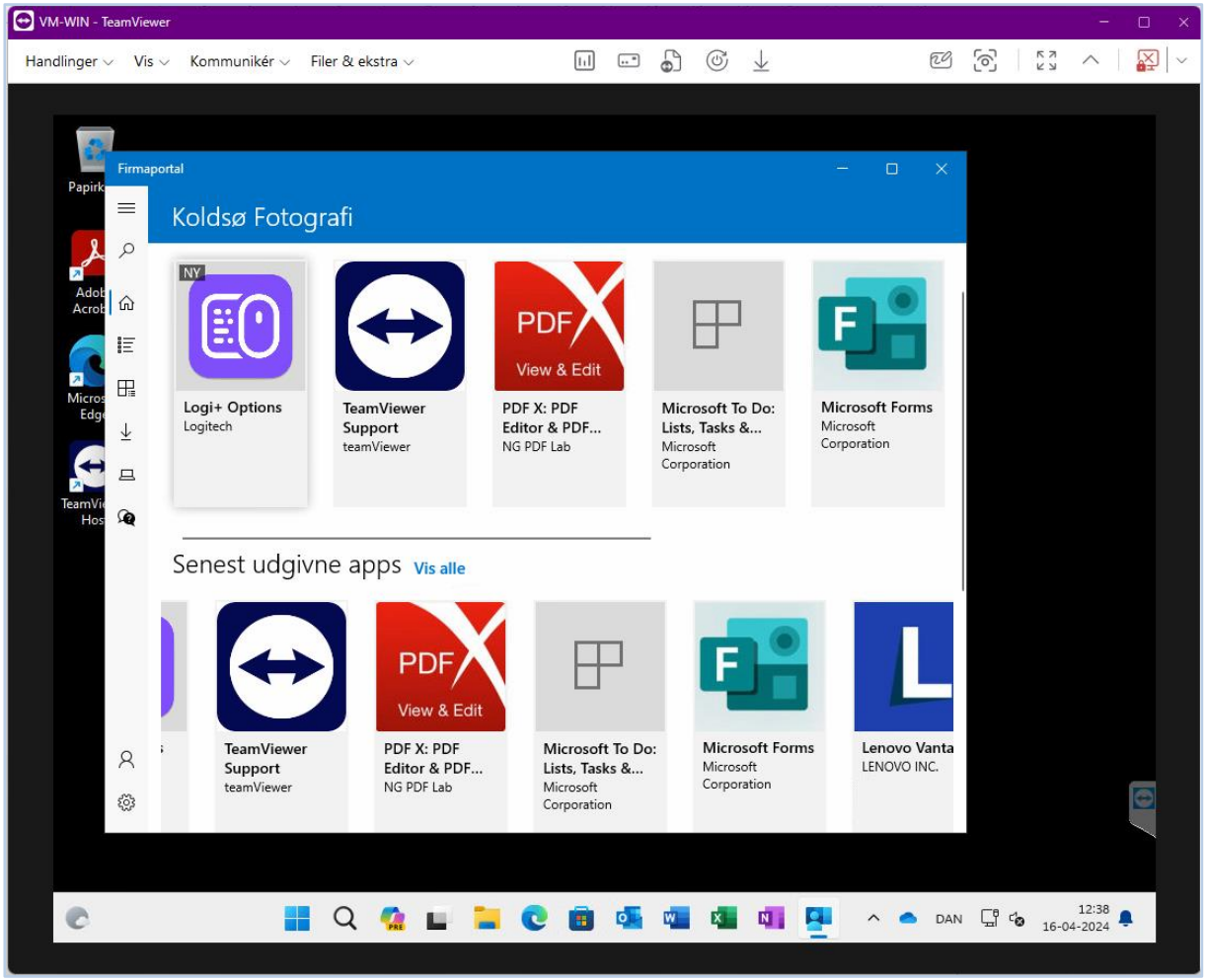


Billede 5.2.5.7.2-C: Startskærm deaktiveret i Outlook

Testen var succesfuld.

5.2.5.7.3 Firmaportal & Apps

Ved login på VM-WIN med testusertwo og tilgang til Firmaportalen kan man se nogle af de på dette tidspunkt tilgængelige applikationer.



Billede 5.2.5.7.3-A: Firmaportal & apps korrekt opsat

Som det ses, kan Firmaportalen og firmaressourcer tilgås, og dermed er applikationerne opsat korrekt.

5.3 Sikkerhed

5.3.1 Baselines

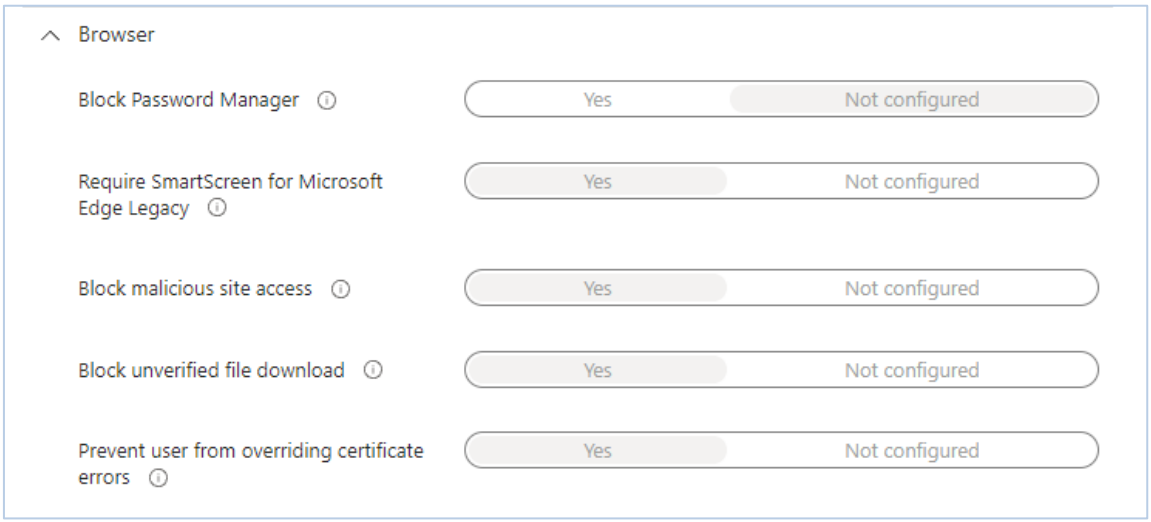
Security Baselines, de første politikker inden for sikkerhedsområdet, er foruddefinerede sikkerhedsindstillinger fra Microsoft. Disse indstillinger implementeres på alle Windows-enheder for at forbedre sikkerheden og mindske risikoen for sikkerhedsbrud.[7]

To baselines er opsat under *Endpoint Security* ▷ *Security baseline* i projektet.

5.3.1.1 Security Baseline for Windows 10 and later

Baselinen ***(bilag 13)*** fastsætter grundreglerne for enhedssikkerhed, datasikring, identitet og adgangsstyring samt applikationskontrol. Intune indeholder specifikke Endpoint Security politikker (firewall, antivirus, BitLocker, SmartScreen) og konfigureres ikke i denne baseline.

Baselinen blokerer adgang til ondsindede sider, forhindrer uverificerede downloads og kræver SmartScreen i Edge Legacy. Justeringer inkluderer deaktivering af stemmeinteraktion og låseskærmsnotifikationer, samt blokering af programinstallationer uden administratorrolle og automatisk opkobling til Wi-Fi hotspots.



Billede 5.3.1.1-A: Browser sektion i Windows 10/11 Baseline

Desuden blokeres muligheden for at være tilkoblet et *domain*-netværk og et *nondomain*-netværk samtidig. Windows Spotlight på startskærmen blokeres, men siden konfigurationen af

[7] *"Security Baselines" af Microsoft Learn*

denne Baseline, tillader en nyere Baseline-version ikke længere blokering af Windows Spotlight på Windows Pro-versioner, som testenhederne er baseret på.

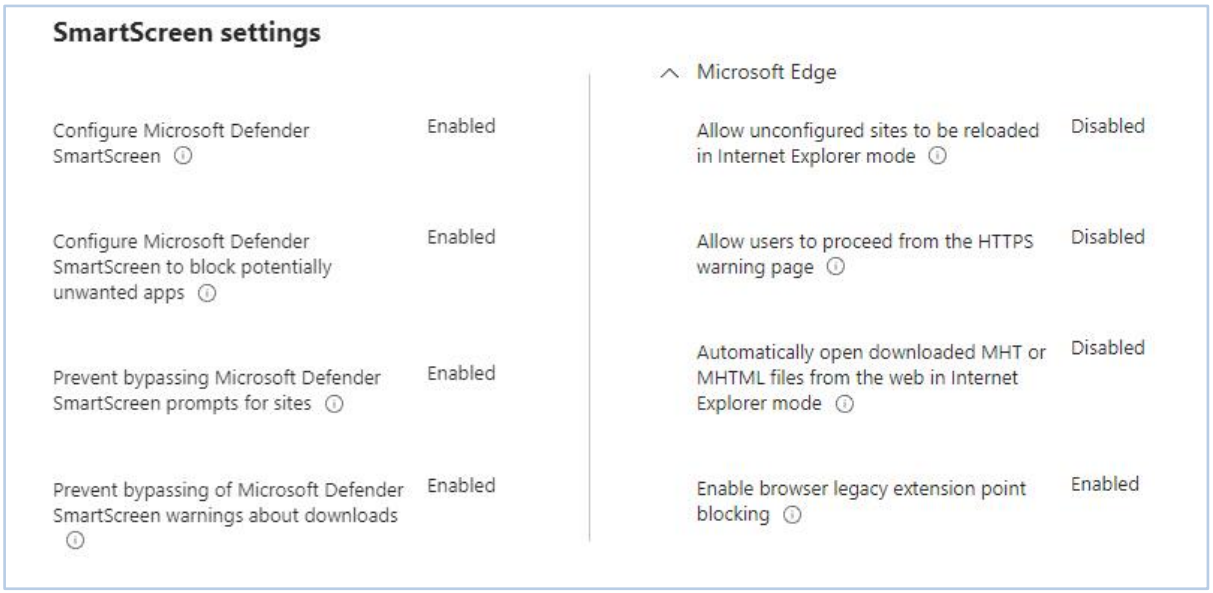
Billede 5.3.1.1-B: Experience sektion i Windows 10/11 Baseline

5.3.1.2 Security Baseline for Microsoft Edge

Baselinen ***(bilag 14)*** har til formål at optimere beskyttelsen af webbrowsing og vil fungere som supplement til den tidligere konfigurerede *MS Edge | Windows* profil.

Hovedpunkter er fx:

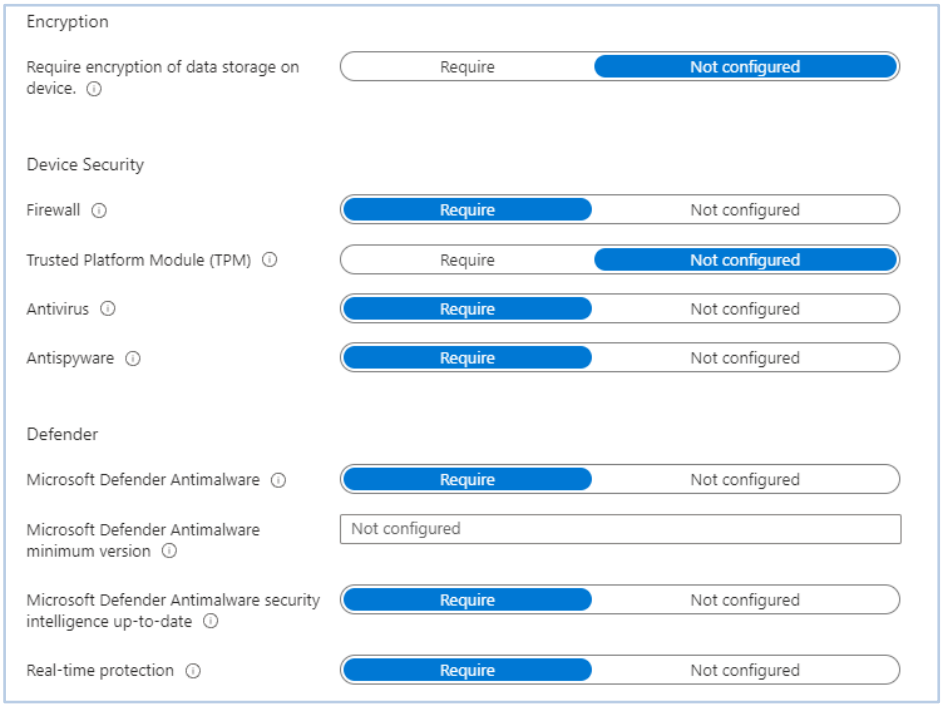
- Bloker brugeren fra at kunne navigere videre fra en HTTPS advarselsside
- Aktivering af Defender SmartScreen funktionalitet ved webbrowsing



Billede 5.3.1.2-A: Udsnit af Baseline for Edge

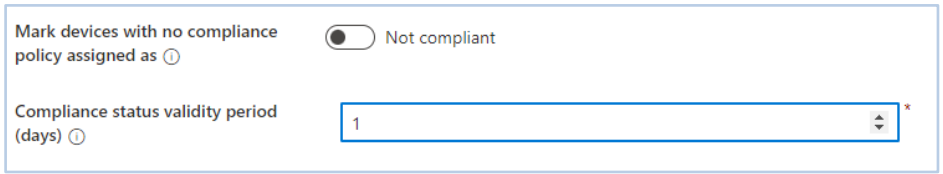
5.3.2 Client Compliancy Policy

Client Compliancy Policy ***(bilag 15)*** fastsætter virksomhedens sikkerhedsstandard og sætter krav til sikkerhedsniveau og overholdelse heraf. *Non-compliant* enheder nægtes adgang til virksomhedsressourcer som applikationer og delingsplatforme. For at blive *compliant* skal enheden opfylde en medium sikkerhedsstandard, opsat under *Devices* ▷ *Compliance*, inklusive aktivering af firewall og antivirus.



Billede 5.3.2-A: Udsnit af Compliancy Policy i Intune

Udover denne politik opsættes Compliance Settings, der dikterer hvordan politikken håndterer enheder.



Billede 5.3.2-B: Compliance settings, Devices ▸ Compliance

5.3.3 Defender Antivirus

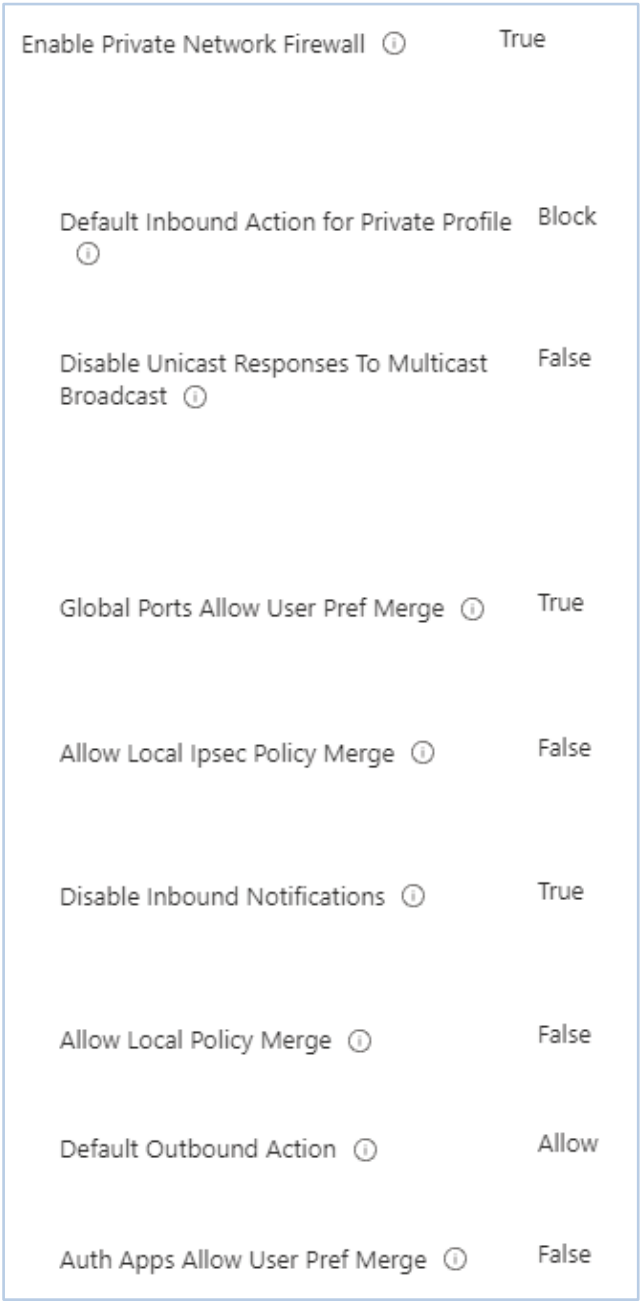
Defender Antivirus-politikken ***(bilag 16)*** er en del af Microsoft Defender-sikkerhedssuiten og forbedrer sikkerheden ved at konfigurere og administrere Microsoft Defender Antivirus-indstillinger på tværs af alle tilknyttede enheder.

Politikken sikrer konsekvent beskyttelse mod malware, vira og andre trusler, samtidig med at den giver administratorer centraliseret kontrol og synlighed over antivirus konfigurationer. I politikken tillades en række scanninger, et tidspunkt for fast scanning opsættes og håndteringen af trusler dikteres.

Billede 5.3.3-A: Udsnit af Antivirus politik

5.3.4 Defender Firewall

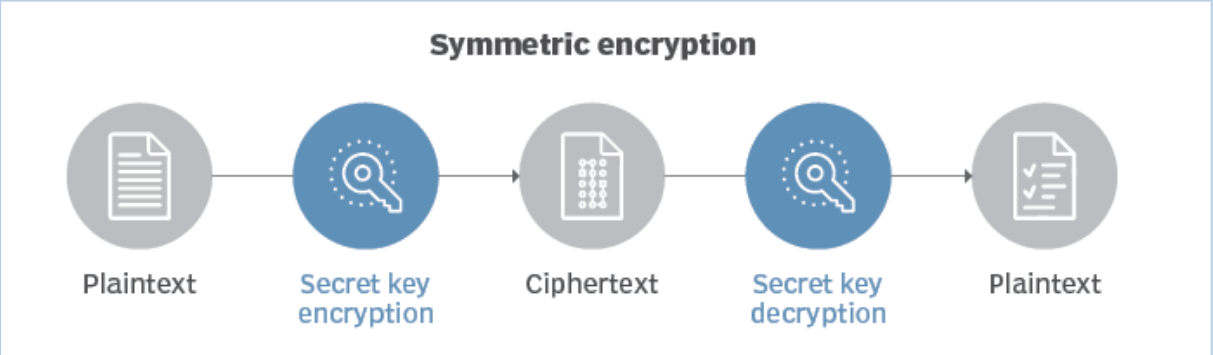
Defender Firewall ***(bilag 17)*** hører også til Microsoft Defender-sikkerhedssuiten og beskytter mod netværkstrusler ved at overvåge og kontrollere trafikken mellem endpoints og internettet samt andre netværk. Politikken består ligesom alt andet i Intune af en række pre-konfigurerede indstillinger, som justeres til behov. Grundlæggende aktiveres firewall for Domain, Public og Private netværk og inbound notifikationer blokeres. Lokale firewall indstillinger ignoreres. Unicast responses til Multicast Broadcast aktiveres. Disse indstillinger gælder for alle tre netværkstyper. Desuden deaktiveres muligheden for at oprette flere FTP-forbindelser.



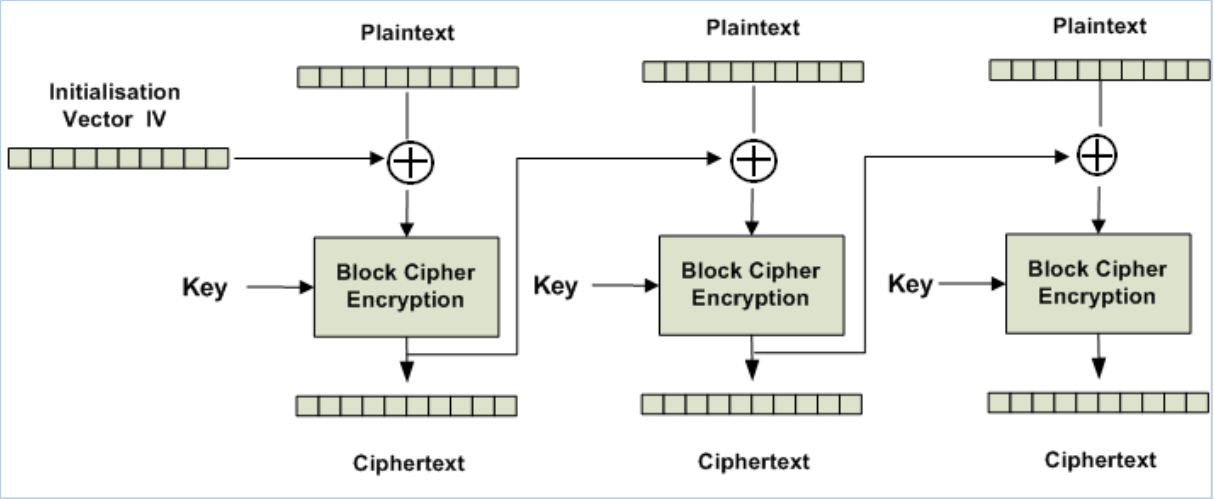
Billede 5.3.4-A: Udsnit af Firewall politik

5.3.5 BitLocker kryptering

BitLocker er en Windows sikkerhedsfeature, der kan kryptere hele drev eller kan begrænses til kun at kryptere brugerdata. BitLocker anvender den symmetriske Advanced Encryption Standard (AES)[8] og kræver en kendt nøgle til både kryptering og dekryptering. AES bruger blokkryptering og splitter data op i mindre blokke af 128 bits, hvortil der krypteres i flere omgange (Cipher-Block Chaining[9]), som illustreret i billede 5.3.5-B.



Billede 5.3.5-A: Eksempel på symmetrisk kryptering. Kilde: TechTarget

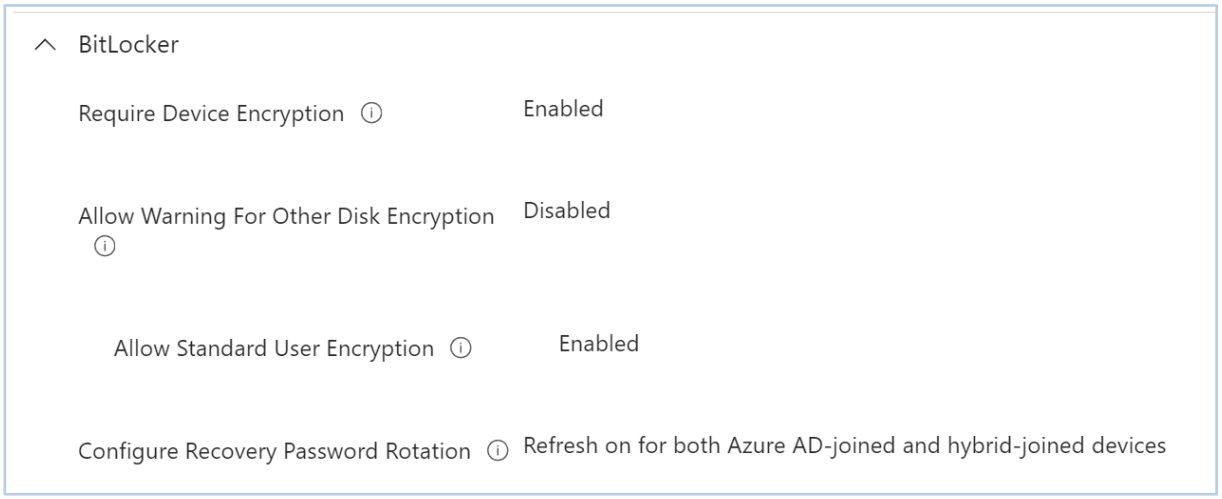


Billede 5.3.5-B: Eksempel på Cipher-Block Chaining (CBC). Kilde: ResearchGate.net

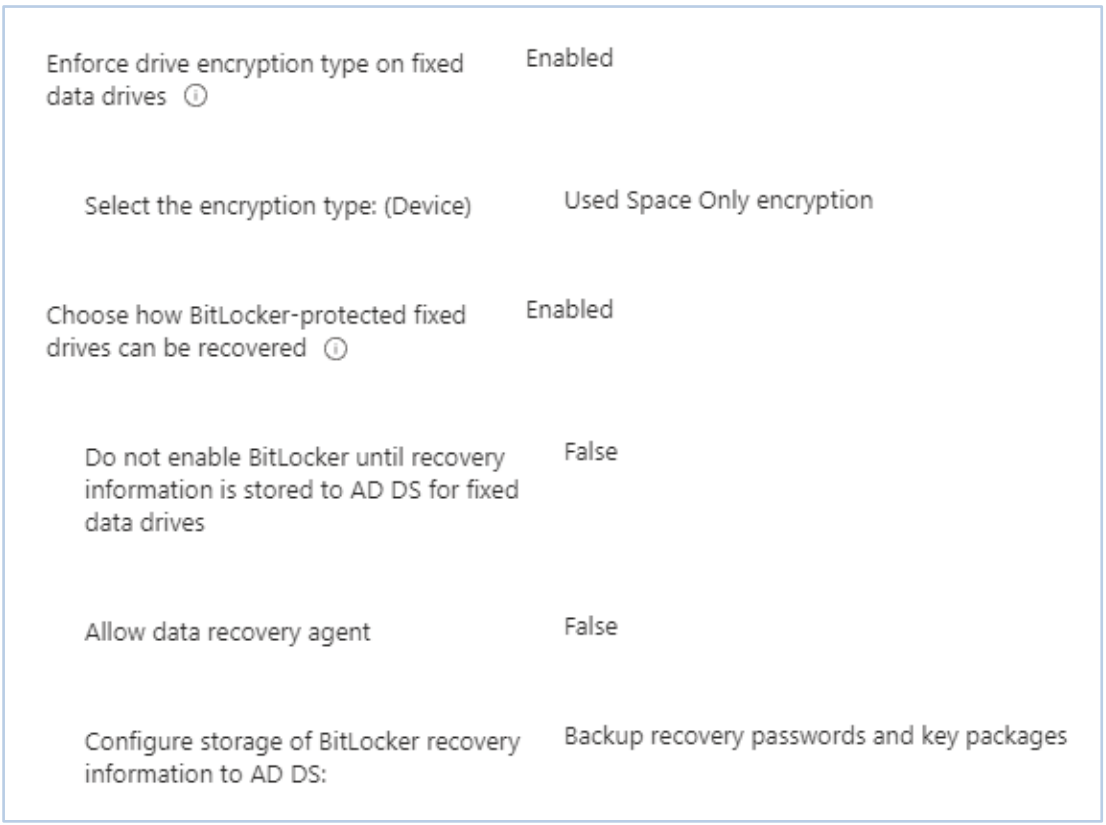
[8] *"Bitlocker" af Microsoft Learn*

[9] *"Cipher-Block Chaining" af ResearchGate.NET*

De følgende screenshots viser, hvordan BitLocker politikken ***(bilag 18)*** er konfigureret i Intune.



Billede 5.3.5-C: Udsnit af BitLocker sikkerhedsprofil - aktiverer BitLocker - Intune



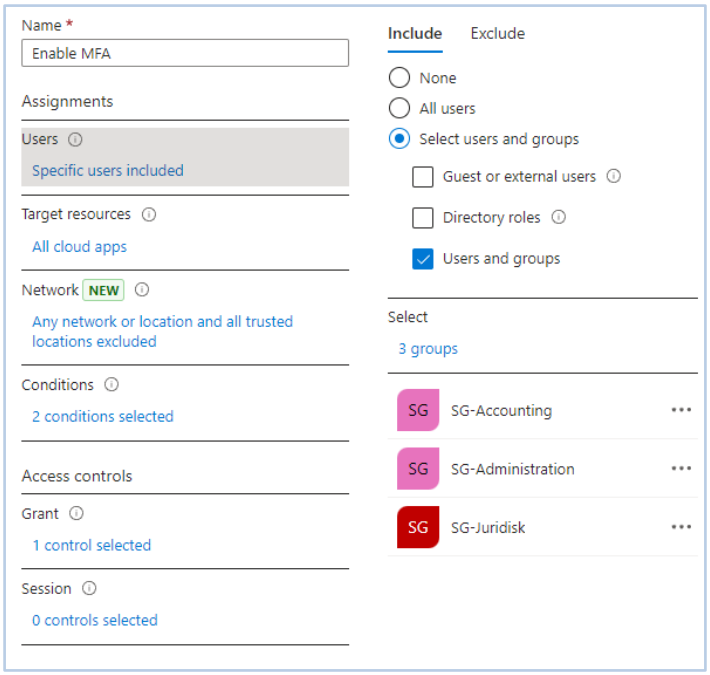
Billede 5.3.5-D: Udsnit af BitLocker sikkerhedsprofil - påtvinger kryptering af brugerdata - Intune

5.3.6 Multi-factor Authentication (MFA)

MFA sikrer mod uautoriseret adgang til brugerkonti ved at kræve ekstra sikkerhedstrin ved login. I projektet konfigureres Entra til at kræve MFA, når en enhed indrulles i Intune. Disse politikker er konfigureret efter anbefaling fra NHC's sikkerhedsrådgiver. Politikkerne opsættes via *Entra ▷ Protection ▷ Conditional Access.*

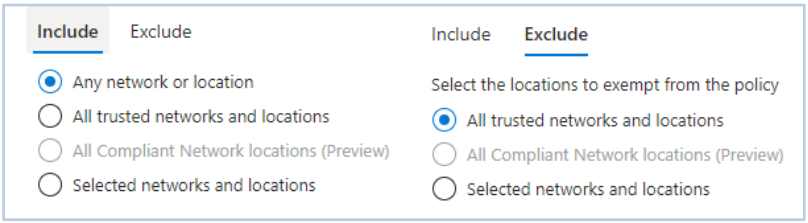
5.3.6.1 Enable MFA Policy[10]

Politikken tildeles de tre sikkerhedsgrupper for domænet og gælder for alle cloud apps. Ved realtime implementering vil GA-brugeren også få tildelt MFA-politikken, men dette er midlertidigt undladt for at undgå udelukkelse i udviklingsfasen.



Billede 5.3.6.1-A: Brugere tildeles MFA politik

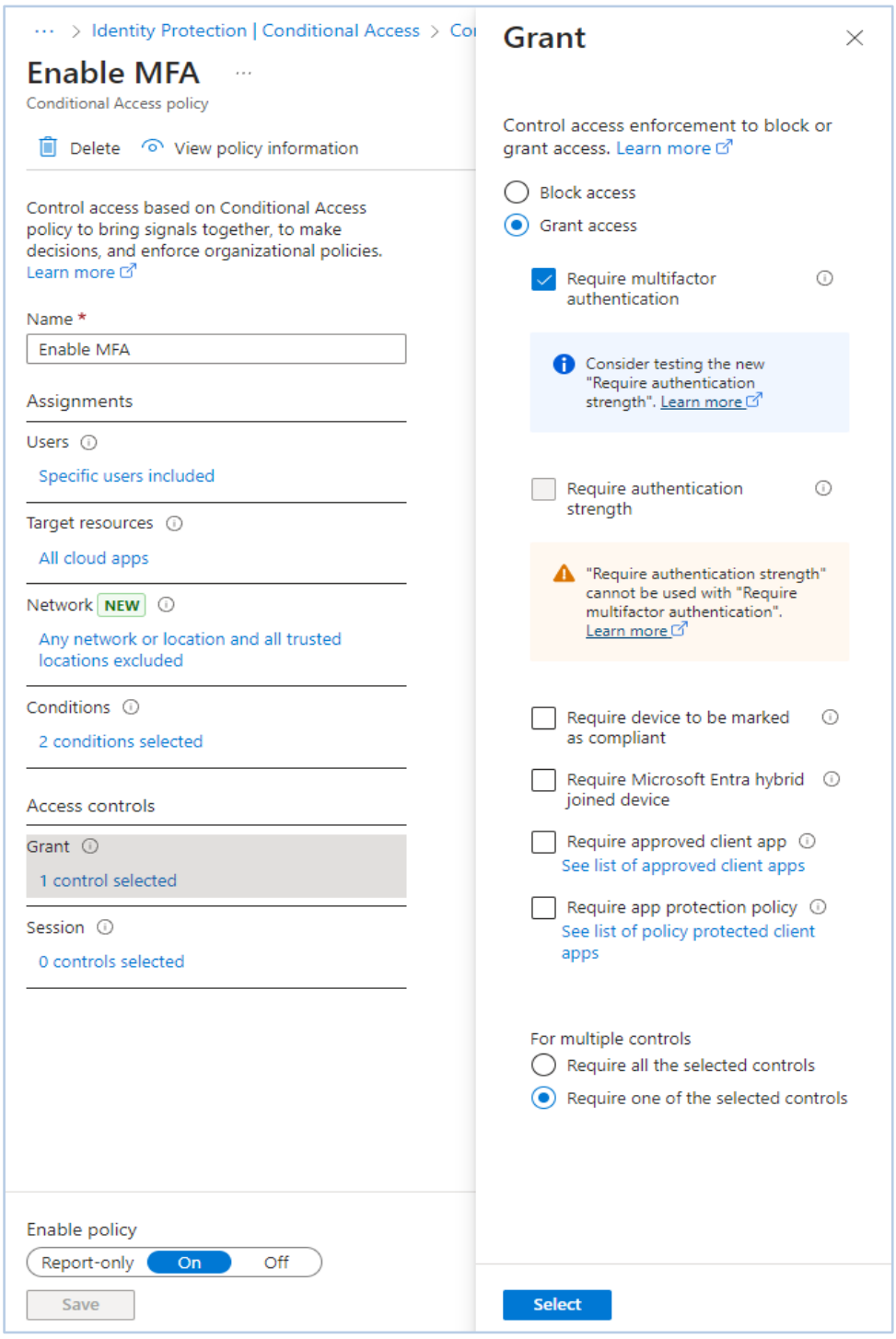
Politikken aktiveres for alle netværk og lokationer undtagen dem, der allerede er markeret som Trusted.



Billede 5.3.6.1-B: Inclusion/Exclusion af netværk

[10] *Konfiguration uddybes i bilag 26: Logbog, s. 123*

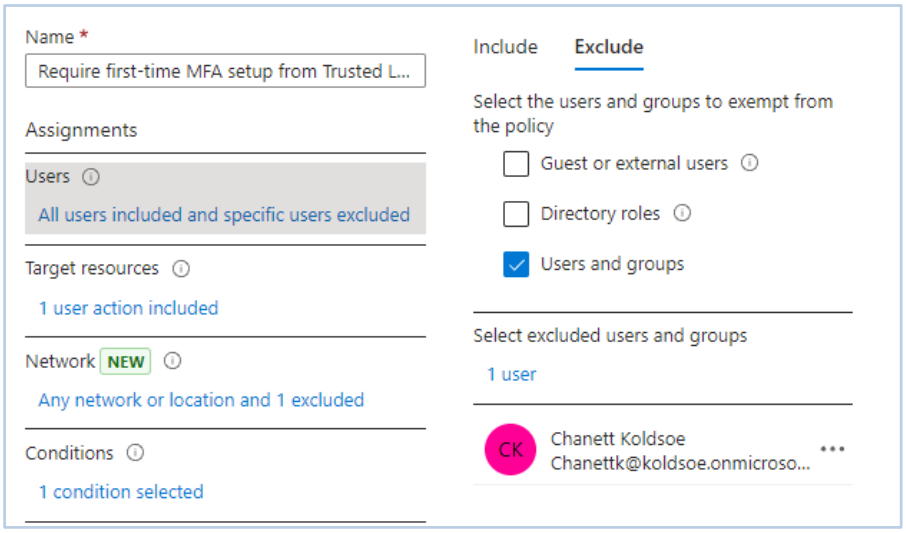
Conditions omfatter netværkskriterier og gælder for fire Client apps, herunder Browser og mobil browser. Adgangstilladelsen kræver MFA.



Billede 5.3.6.1-C: Enable MFA, Entra

5.3.6.2 *Require first-time MFA setup from Trusted Location Policy*[11]

Politikken kræver at førstegangsopsætning af MFA foregår på en geografisk kendt placering. Dette sikrer mod uautoriseret MFA-oprettelse og er et ekstra sikkerhedshensyn. Alle brugere er tilføjet, dog er GA ekskluderet for at undgå potentiel udelukkelse i projektfasen.

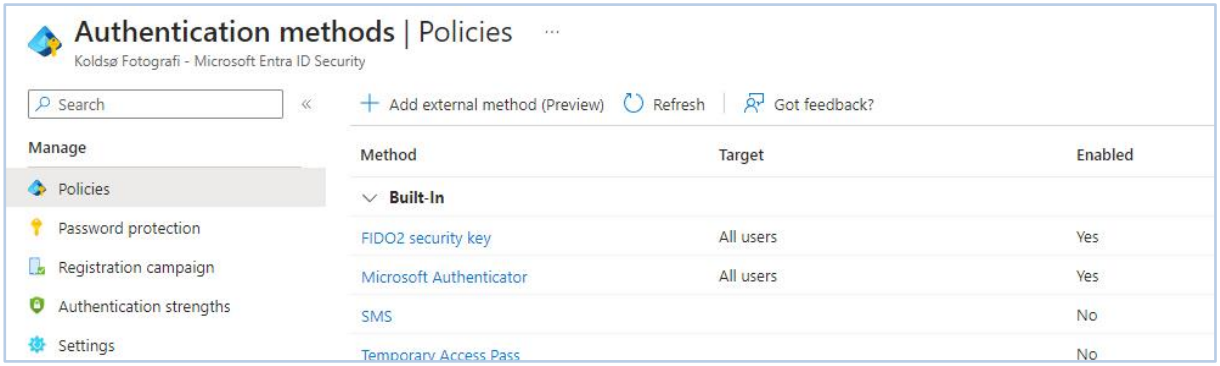


Billede 5.3.6.2-A: GA-bruger ekskluderes fra regel

I projektet er denne politik gemt i *Read-only* tilstand, hvor hændelser logges, men ikke håndhæves. Denne politik vil skulle aktiveres ved endelig implementering.

5.3.6.3 *Authentication Methods*

Microsoft Authenticator og FIDO2 security key aktiveres for alle brugere som godkendt metode ved autentifikationsprocessen. Dette gøres i Entra fra *Protection* ▷ *Authentication Methods.*



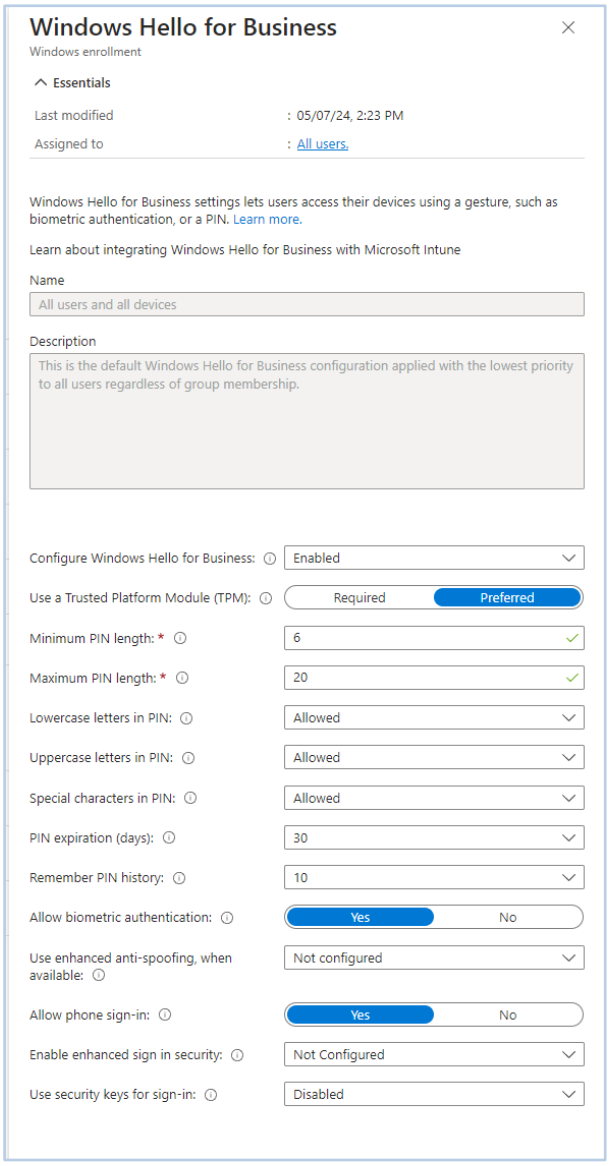
Billede 5.3.6.3-A: FIDO2 & Microsoft Authenticator aktiveret, Entra

[11] *Konfiguration uddybes i Bilag 26: Logbog, s. 136*

5.3.7 Windows Hello for Business

Windows Hello for Business (WHfB) er et sikkerhedsværktøj brugt i projektet til at implementere adgangssikkerhed under enhedsindrulning i Intune. Det tillader brugere at logge ind med biometriske data eller PIN-koder i stedet for adgangskoder eller Authenticator app'en.[12]

I Entra supplerer WHfB MFA-kravet ved at tilføje en ekstra loginmulighed. WHfB er som standard aktiveret i Intune, men konfigureres efter behov under *Devices* ▷ *Enrollment* ▷ *Windows*, hvor krav til PIN-oprettelse og brug af biometri sættes.

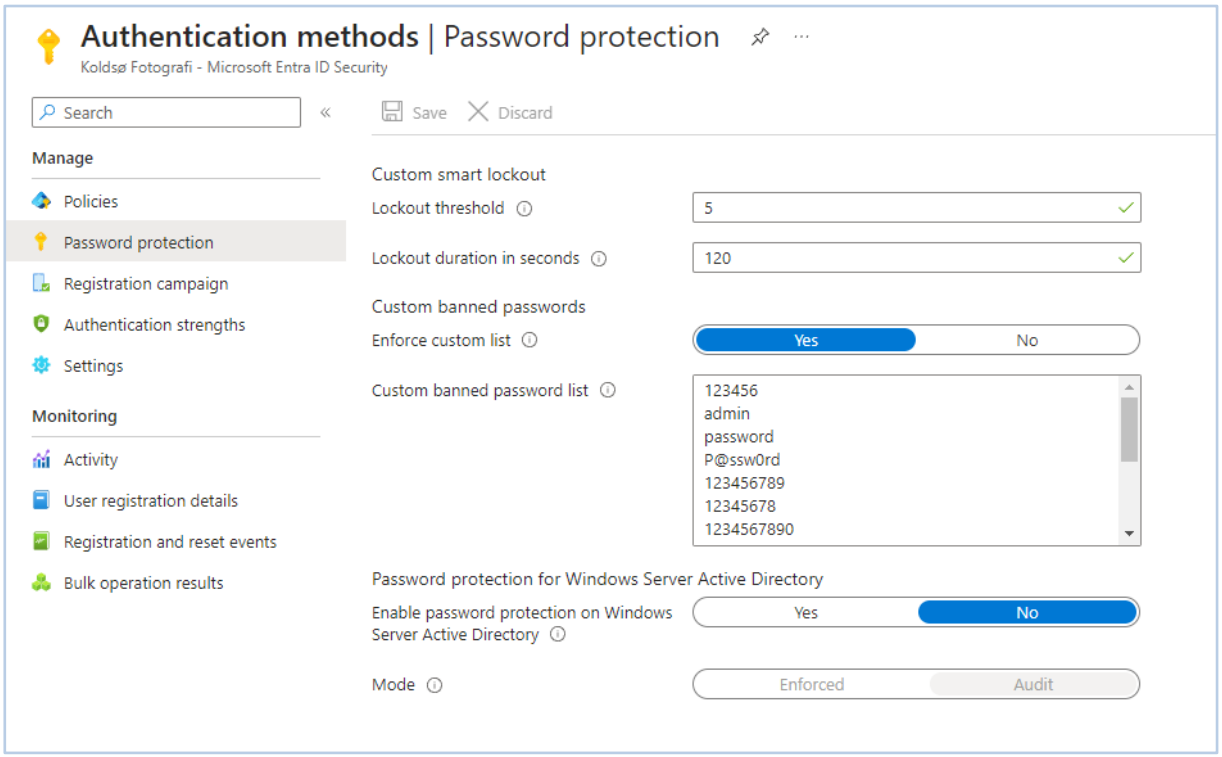


Billede 5.3.7-A: Konfiguration af WHfB, Intune

[12] *"Hello for Business - How it works" af Microsoft Learn*

5.3.8 Password Protection

I Entra opsættes regler for adgangskoder under *Identity ▷ Protection ▷ Password protection.*



Billede 5.3.8-A: Konfiguration af Password Protection, Entra

Blokerede adgangskoder følger NordPass' liste over **Top 200 Most Common Passwords 2019-2022**[13]. Nye brugere får en midlertidig adgangskode, der kræver ændring ved login. Testen af politikken involverede nulstilling af en testbrugers adgangskode og forsøg på at bruge koden "123456", som blev afvist korrekt ifølge konfigurationen.

[13] *"Most common passwords" af Nordpass*

5.3.9 Anti-malware & Anti-phishing

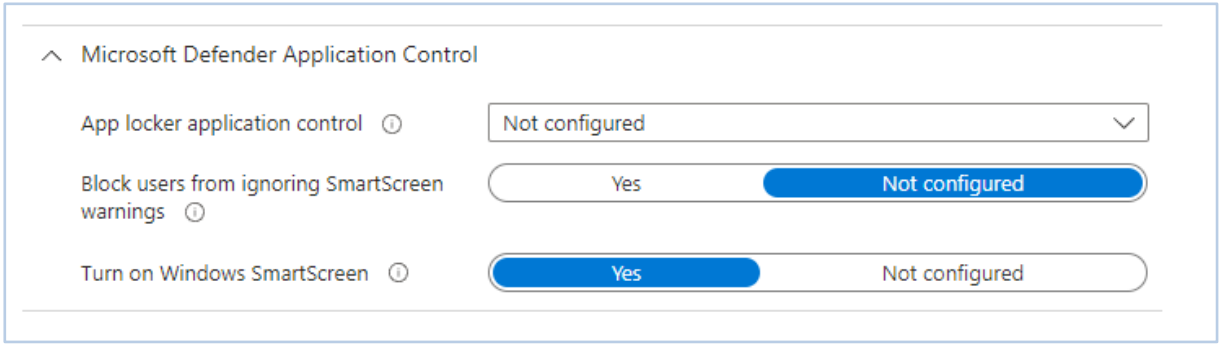
Politikker for anti-malware og anti-phishing sættes i Intune under *Endpoint security* ▷ *Attack surface reduction*.

5.3.9.1 Defender SmartScreen

Defender SmartScreen ***(bilag 19)*** er et "early-warning" system, der kan opsnappe forsøg på phishing eller forsøg på distribuering af malware. Det er integreret direkte i Windows 10/11-operativsystemet og skal blot aktiveres i Intune.

SmartScreens primære funktioner er, at:

- beskytte mod phishing, malware og vildledende reklamer med onde hensigter.
- evaluerer websteders og apps omdømme for at identificere risici.
- blokerer URL'er forbundet med potentielt uønskede applikationer i Microsoft Edge baseret på Chromium.[14]



Billede 5.3.9.1-A: Konfiguration af SmartScreen, Intune

5.3.9.2 Ransomware politik

Microsoft anbefaler aktivering af alle tilgængelige blokeringsregler for maksimal sikkerhed. I billede 5.3.9.2-A oplistes Microsofts anbefalede opsætning af Ransomware politikken ***(bilag 20)***. Block betyder her: *enable the attack surface reduction rule.*[15]

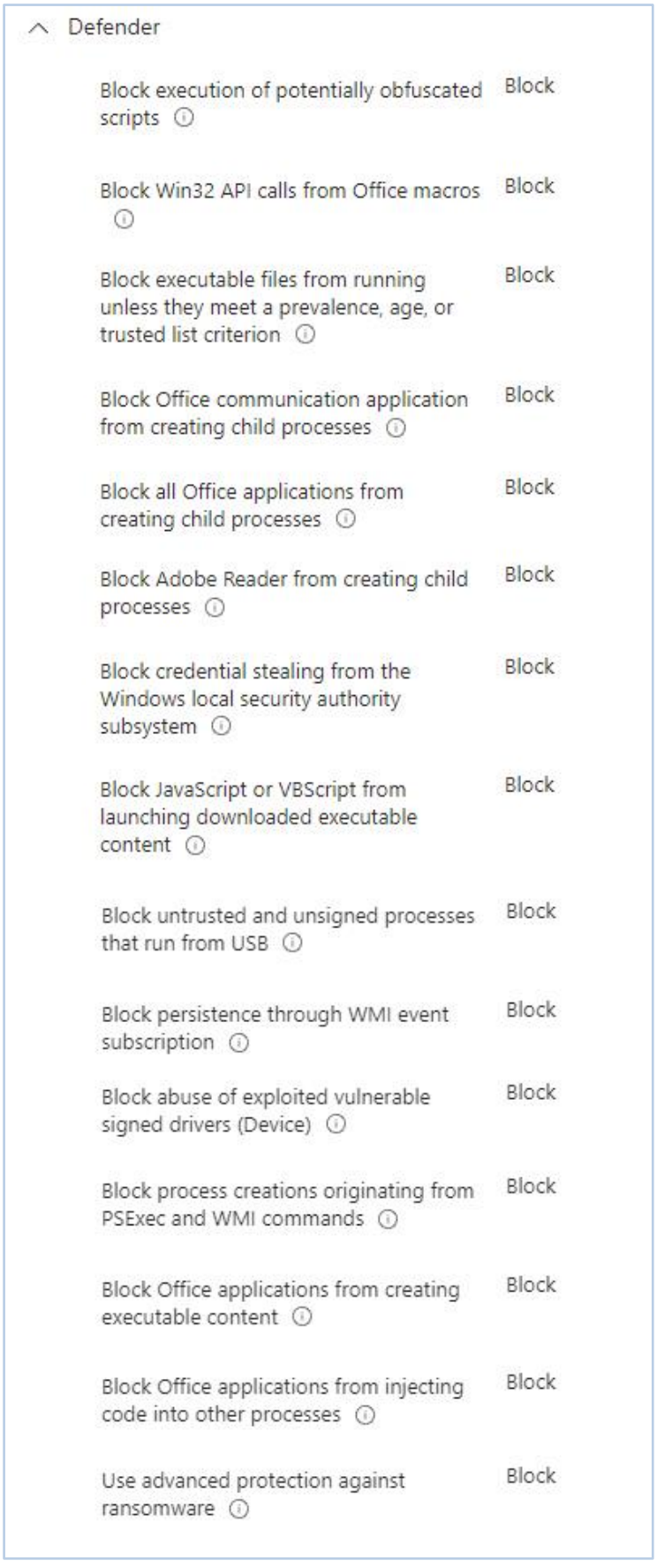
[14] *"Benefits of Microsoft Defender SmartScreen" af learn.microsoft.com*
[15] *"Enable attack surface reduction rules ⇨ Requirements" af learn.microsoft.com*

ASR rule name:	Standard protection rule?	Other rule?
Block abuse of exploited vulnerable signed drivers	Yes	
Block Adobe Reader from creating child processes		Yes
Block all Office applications from creating child processes		Yes
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Yes	
Block executable content from email client and webmail		Yes
Block executable files from running unless they meet a prevalence, age, or trusted list criterion		Yes
Block execution of potentially obfuscated scripts		Yes
Block JavaScript or VBScript from launching downloaded executable content		Yes
Block Office applications from creating executable content		Yes
Block Office applications from injecting code into other processes		Yes
Block Office communication application from creating child processes		Yes
Block persistence through WMI event subscription	Yes	
Block process creations originating from PSExec and WMI commands		Yes
Block untrusted and unsigned processes that run from USB		Yes
Block Webshell creation for Servers		Yes
Block Win32 API calls from Office macros		Yes
Use advanced protection against ransomware		Yes

Billede 5.3.9.2-A: Microsofts anbefalede opsætning af Ransomware regelsæt.

Kilde: "Attack surface reduction rules by type" – learn.microsoft.com

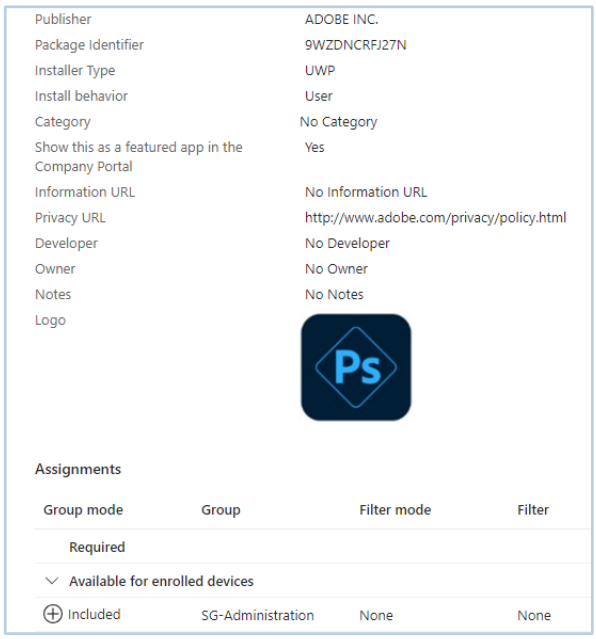
Intune-konfigurationen følger anbefalingerne og aktiverer flere sikkerhedsindstillinger, såsom blokering af manipulerede scripts og aktivering af *styret mappeadgang*. Desuden begrænses kørslen af eksekverbare filer baseret på specifikke kriterier, og Office-kommunikationsapplikationer blokeres fra at oprette underprocesser.



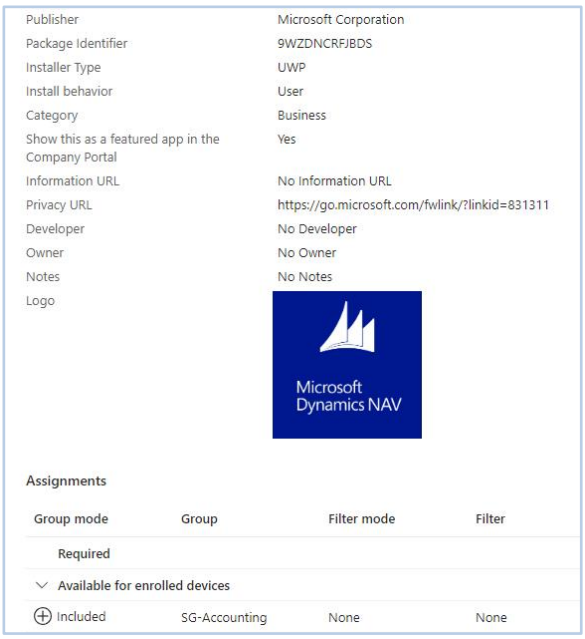
Billede 5.3.9.2-B: udsnit af Ransomware politik, Intune

5.3.10 Adgangstilladelser

For at holde projektets omfang på et realistisk niveau, blev adgangstilladelse kun implementeret, så brugergrupper havde adgang til forskellige applikationer.

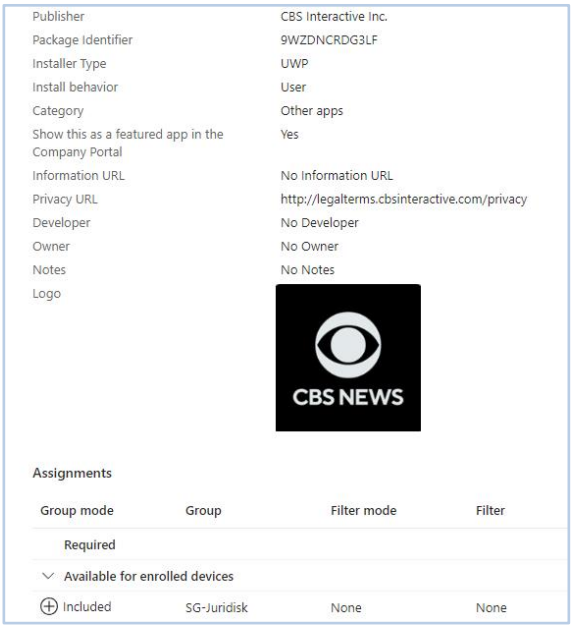


Billede 5.3.10-A: App tilknyttet SG-Administration



Billede 5.3.10-B: App tilknyttet SG-Accounting

Adgang til disse applikationer blev testet i Firmaportal ved login med de forskellige brugere og her bekræftedes det, at kun de fastsatte grupper, havde adgang til de tre applikationer.

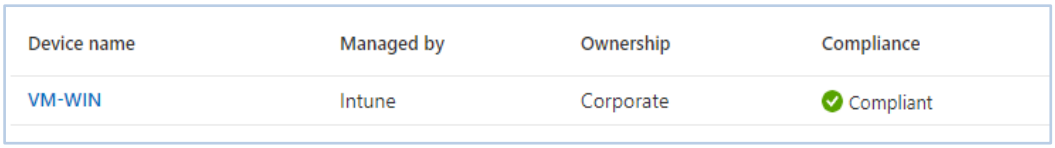


Billede 5.3.10-C: App tilknyttet SG-Juridisk

5.3.11 Test af sikkerhedskonfigurationer

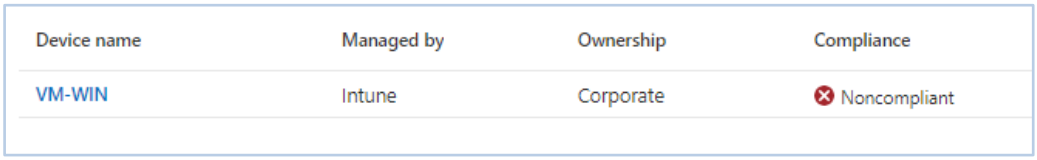
5.3.11.1 Compliancy

Ved første indkøring af testenhederne i Intune stod disse markeret som *Compliant*, fordi der endnu ikke var opsat en Compliancy politik.



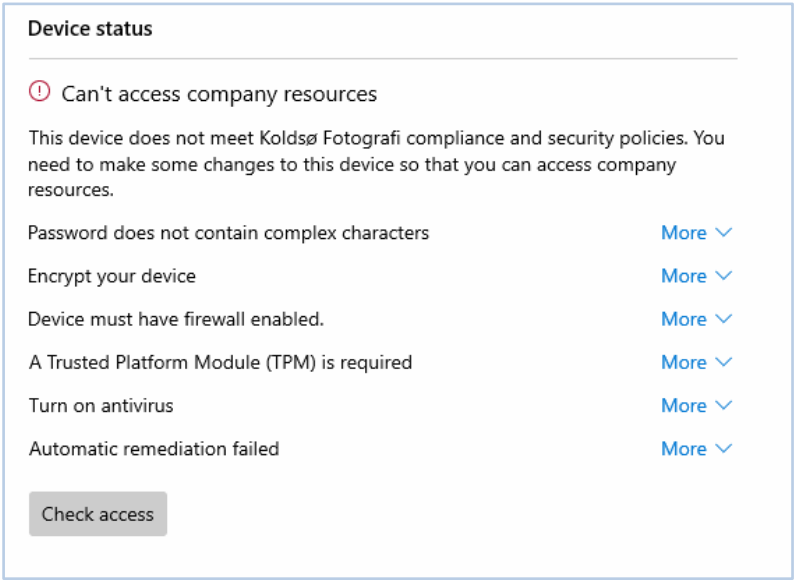
Billede 5.3.11.1-A: Testenhed viser compliant under Intune ► Devices

Efter opsætning af Compliancy politikken og synkronisering af enhederne i Intune, blev enhederne efterfølgende markeret som *Noncompliant*.



Billede 5.3.11.1-B: Efter sync vises en testenhed noncompliant under Intune ► Devices

Dette blev tydeligt i firmaportalen, hvor enhederne efterfølgende ikke havde adgang til firmaressourcer og de manglende opsætninger blev angivet. Dette bekræftede en vellykket implementering af Compliancy politikken.

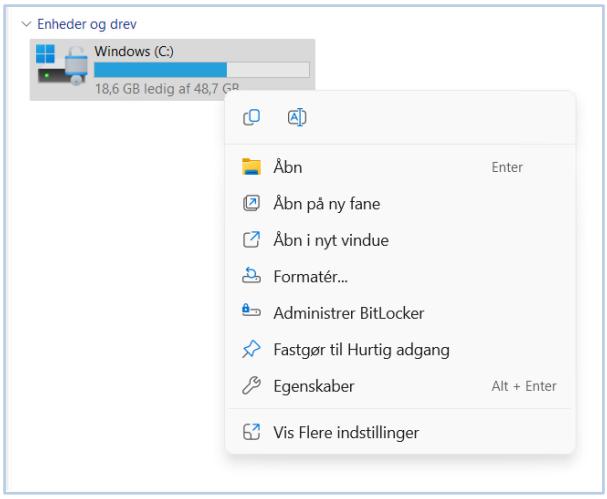


Billede 5.3.11.1-C: Fejlmelding i Firmaportalen, ens for alle testpc'er

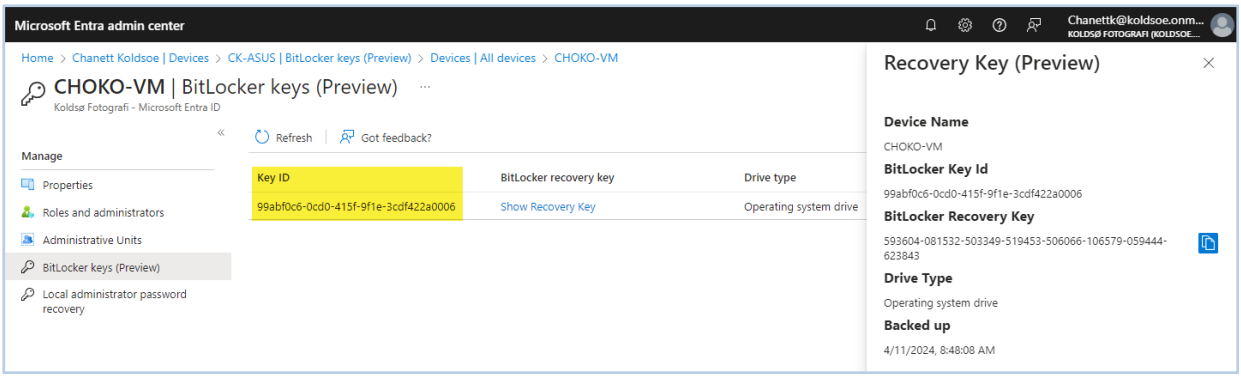
5.3.11.2 BitLocker

Under testen af BitLocker-kryptering på testenhederne blev ingen af dem krypteret, da de manglede den fysiske komponent TPM (Trusted Platform Module). Dette kunne omgås ved at foretage ændringer til konfigurationen med en Local Group Policy[16]. Men da politikken blot skulle bekræftes succesfuld, blev en ekstra virtuel pc, CHOKO-VM, i stedet opsat på en fysisk NHC-enhed med TPM ved brug af Hyper-V og indrullet med en testbruger.

Efter konfigurationen var system disk C:// krypteret på den nye testenhed, og BitLocker-profilen var bevist korrekt opsat. BitLocker Recovery Key blev også bekræftet tilgængelig i Entra, hvilket bekræfter en succesfuld implementering af krypteringspolitikken. Recovery Keys tilgås fra *Entra ▷ Devices ▷ #devicename ▷ BitLocker keys.*



Billede 5.3.11.2-A: BitLocker aktiveret og disk krypteret. Hyper-V: VM-Choko

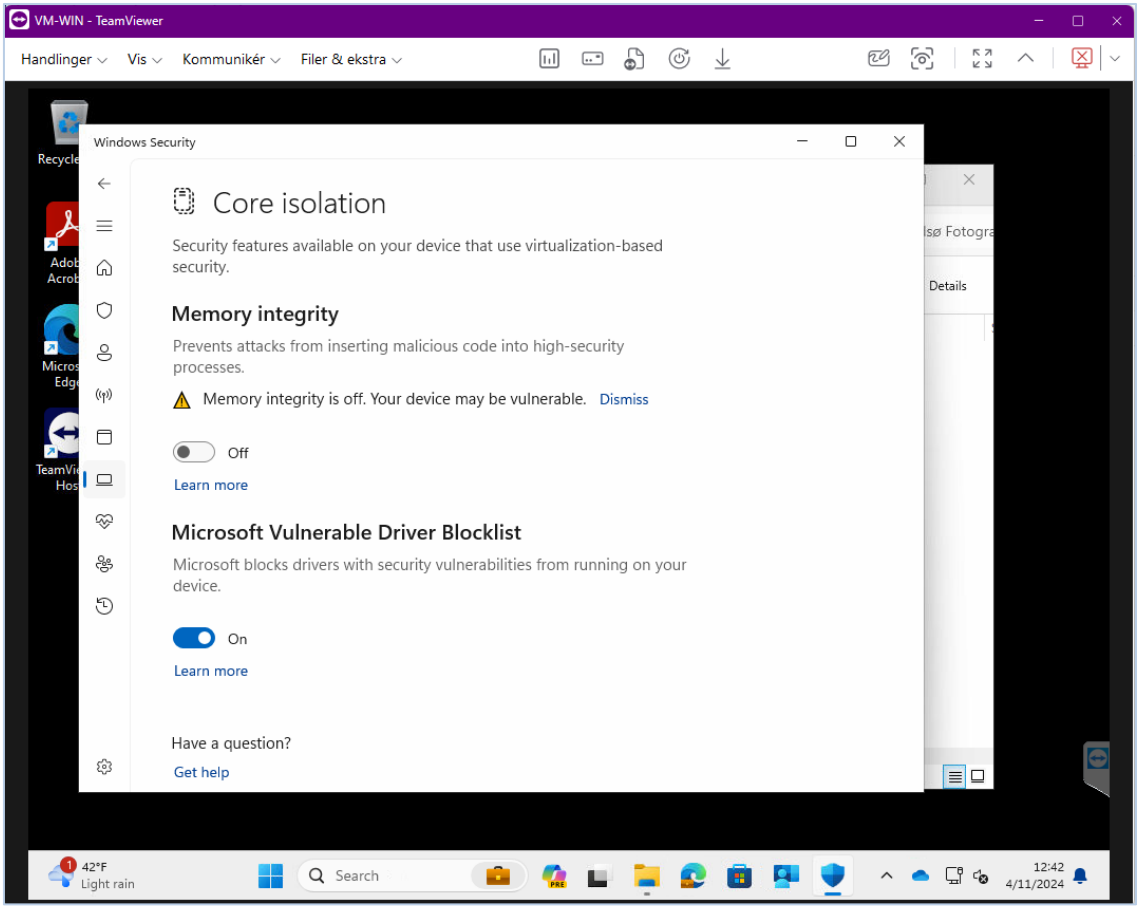


Billede 5.3.11.2-B: BitLocker key lokaliseret i Entra

[16] *"How to use BitLocker with or without TPM" af InfosecInstitute*

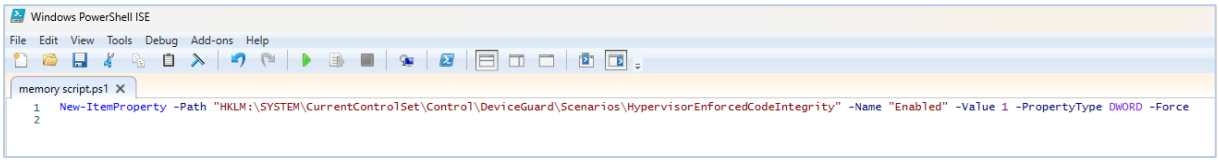
5.3.11.3 Memory Integrity

Ved opstart af VM-WIN fremgik et advarselsikon på Windows Security i proceslinjen. Det fremgik at *Memory Integrity* under *Device Security* var deaktiveret. Memory Integrity er en Virtualization-based security (VBS) Windows feature, der beskytter mod malware angreb på Windows Kernel.[17]



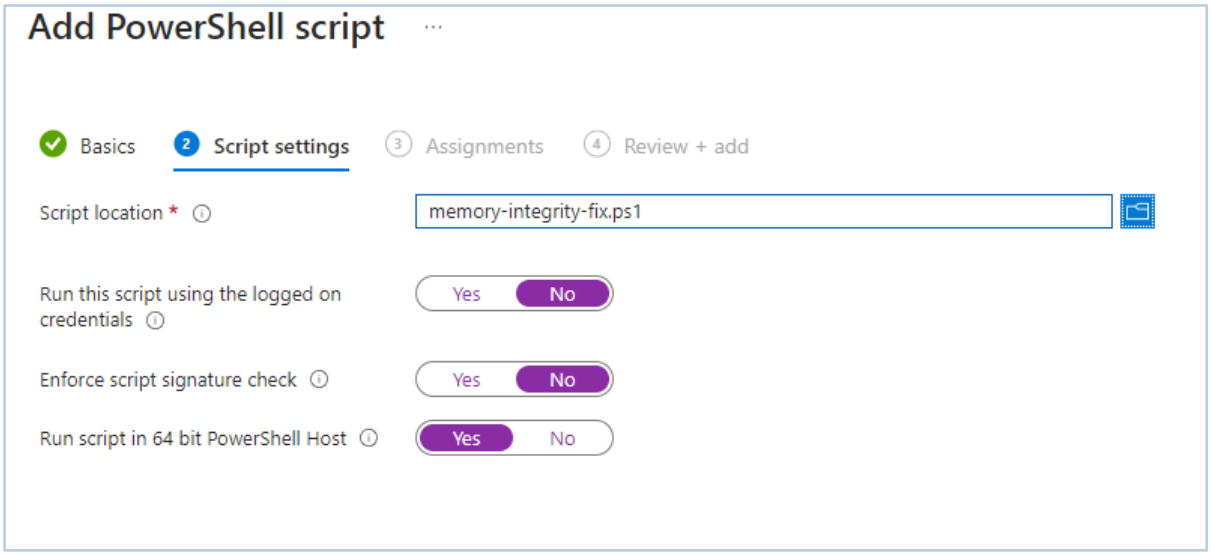
Billede 5.3.11.3-A: Memory Integrity slået fra i Windows Security, VM-WIN

Funktionen kunne aktiveres ved et Powershell script[18]. Konfigurationen blev tilknyttet alle enheder og udrulles til alle brugere.



Billede 5.3.11.3-B: Script til aktivering af Memory Integrity

[17] *"Enable VBS protection of code integrity" af Microsoft Learn*
[18] *"Enable VBS protection of code integrity" af Microsoft Learn*

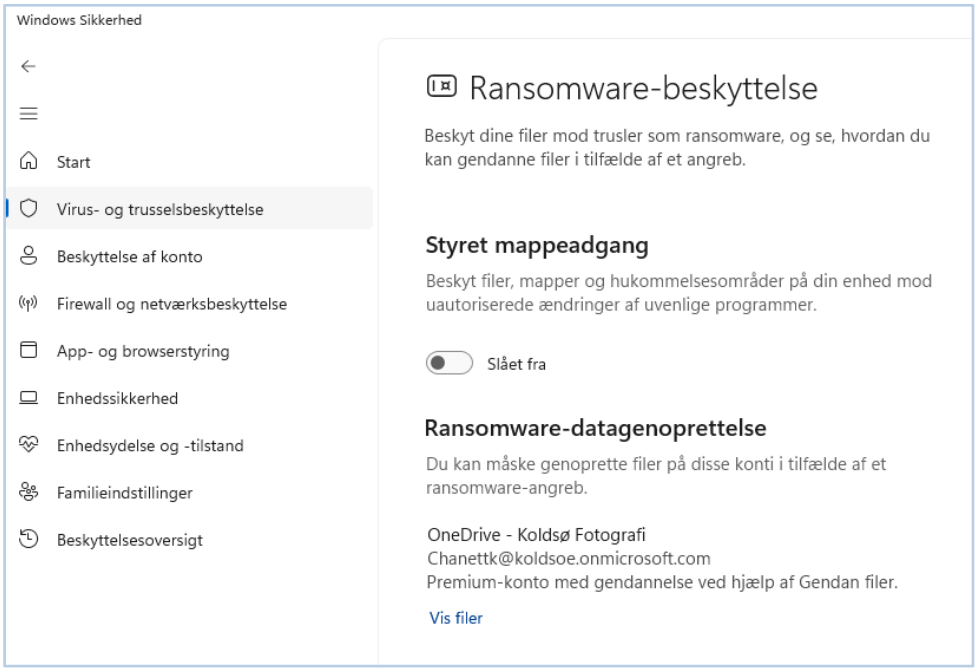


Billede 5.3.11.3-C: Script opsættes i Intune

Efter tilføjelsen af scriptet til *Devices ▷ Scripts & remediations* og synkronisering med Intune var funktionen aktiveret på alle testpc'er.

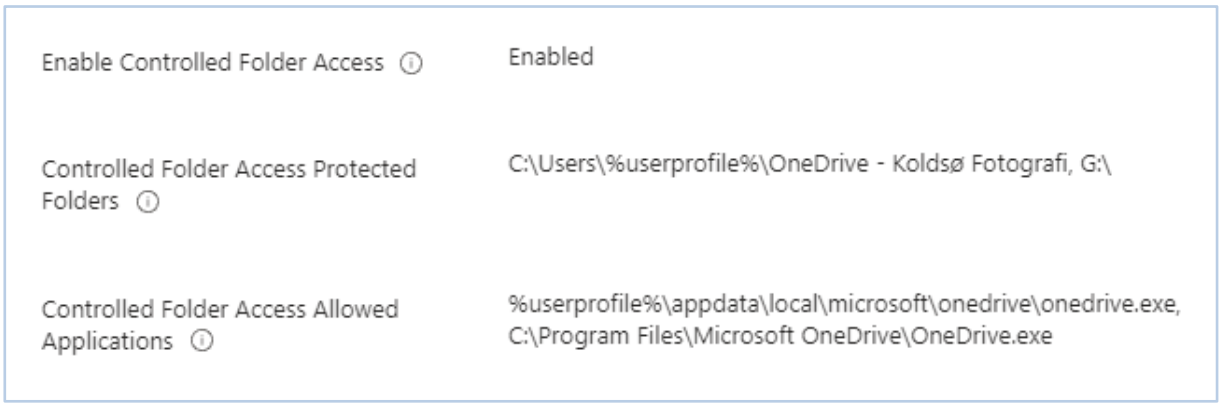
5.3.11.4 Styret mappeadgang

Ved test af Ransomware-politikken (før optimeringen), fandt jeg at *styret mappeadgang* ikke var slået til. Formålet med netop denne opsætning er at forhindre uautoriserede i at kryptere sensitive data.



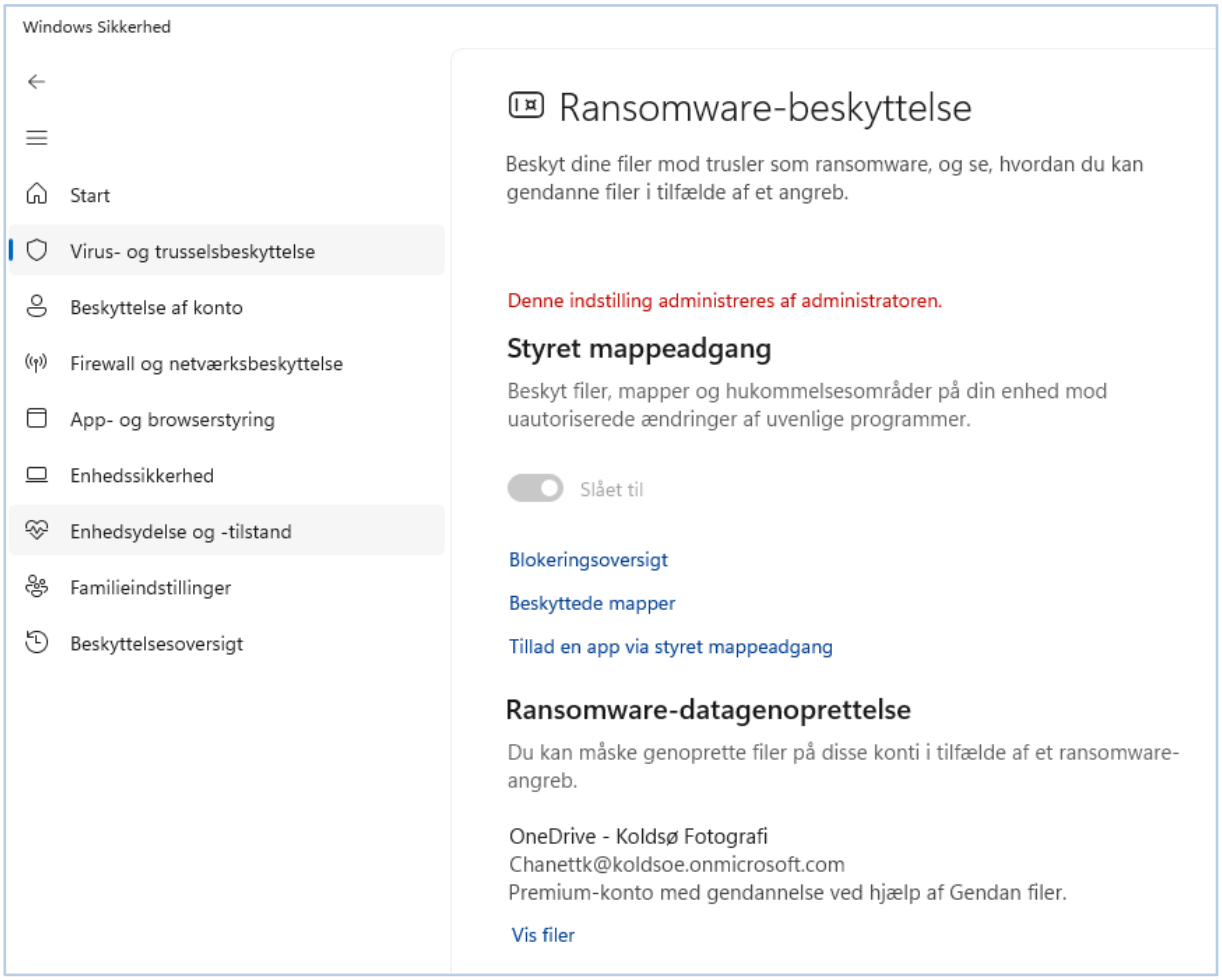
Billede 5.3.11.4-A: Styret mappeadgang slået fra, Windows Security, ASUS test pc

For at rette denne mangel, blev Ransomware-politikken tilgået igen. Her blev "Controlled Folder Access" aktiveret og OneDrive applikation samt OneDrive mappe og G-drev blev valgt, som mål.



Billede 5.3.11.4-B: Styret mappeadgang konfigureres i Ransomware politik, Intune

Ved synkronisering og et par genstart af VMs, var *styret mappeadgang* aktiveret.

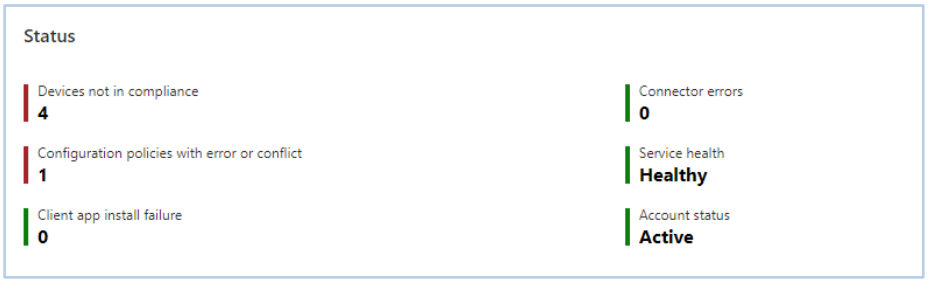


Billede 5.3.11.4-C: Styret mappeadgang er aktiv, ASUS test pc

5.3.12 Monitorering

5.3.12.1 Monitorering i Intune

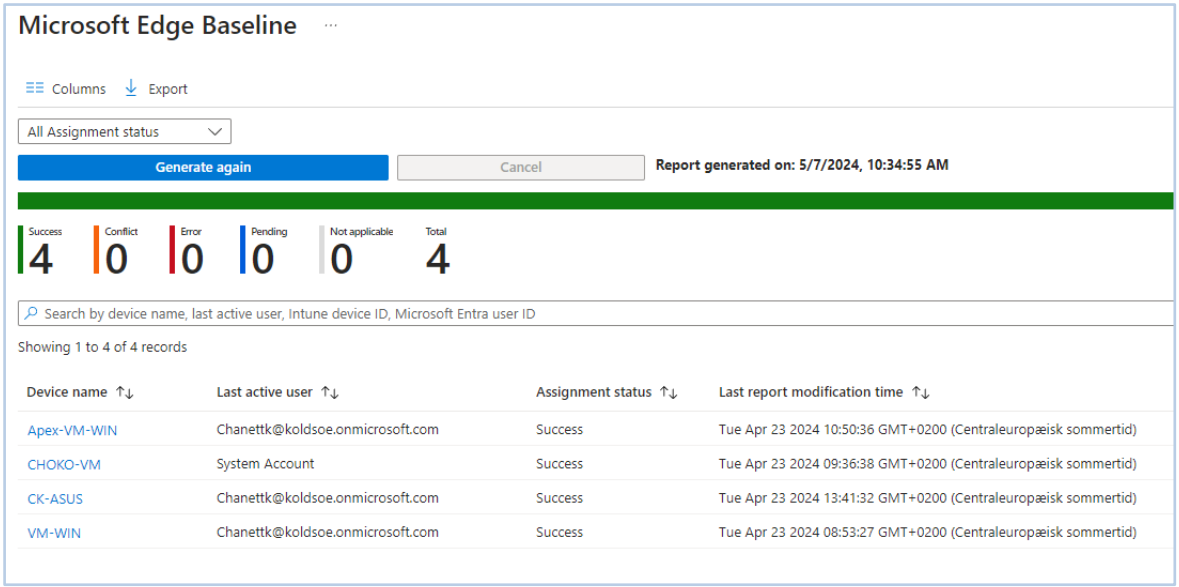
I Intune monitoreres enhedernes compliance og succesraten på udrulning af konfigurationer samt hvorvidt der opstår konflikter mellem konfigurationerne. F.eks. blev der opdaget en konflikt mellem opsætning af Defender Antivirus og Windows Baseline omhandlende scannings-opsætning.



Billede 5.3.12.1-A: Monitorering af status, Intune Dashboard

Device name	Logged in user	Policy compliance status
Apex-VM-WIN	Chanettk@koldsoe.onmicrosoft.com	Compliant
CHOKO-VM	b95b8f40ea3e4bf5ab962657039cbe01...	Compliant
CK-ASUS	Chanettk@koldsoe.onmicrosoft.com	Compliant
VM-WIN	Chanettk@koldsoe.onmicrosoft.com	Compliant

Billede 5.3.12.1-B: Monitorering af Compliance, Intune

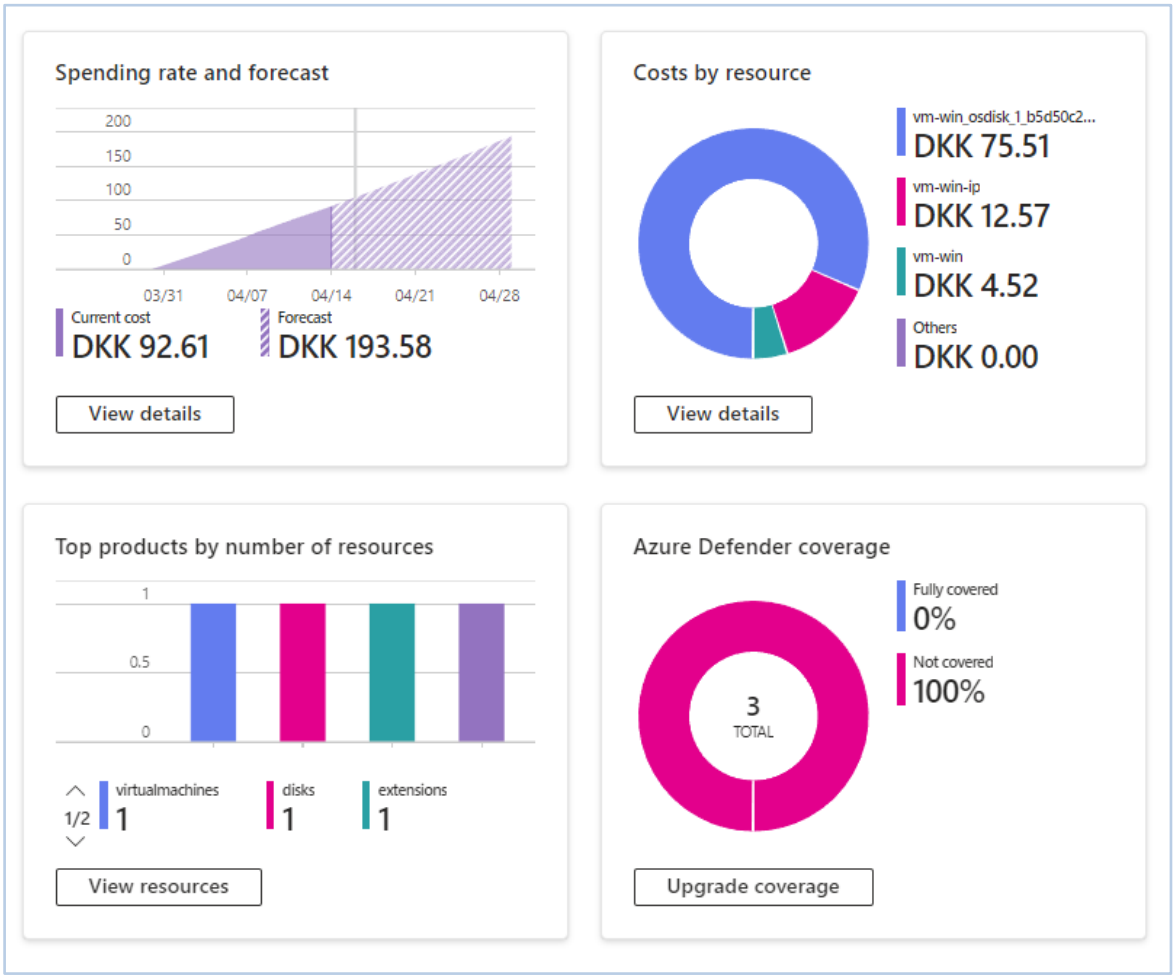


Billede 5.3.12.1-C: Edge Baseline er udrullet korrekt på alle enheder, Intune

De konfliktende Defender-indstillinger blev efterfølgende fjernet fra Baseline, hvorefter konflikten ophørte. Dog figurerer konflikterne fortsat i Intune Dashboard, da de er logget.

5.3.12.2 Monitorering i Azure

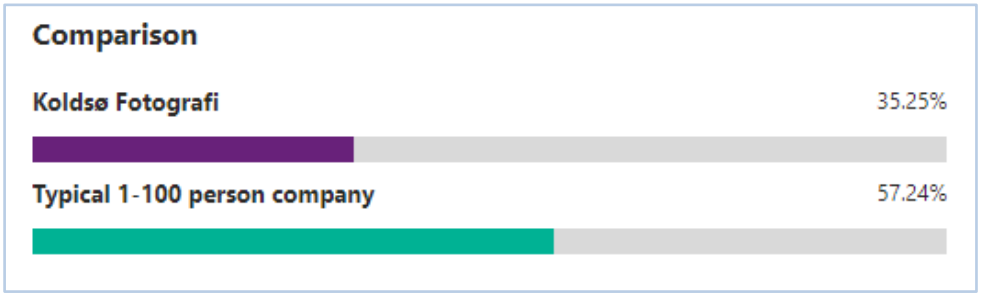
I Azure er det primært det økonomiske ressourceforbrug, der monitoreres i forbindelse med de to kørende testsubscriptions.



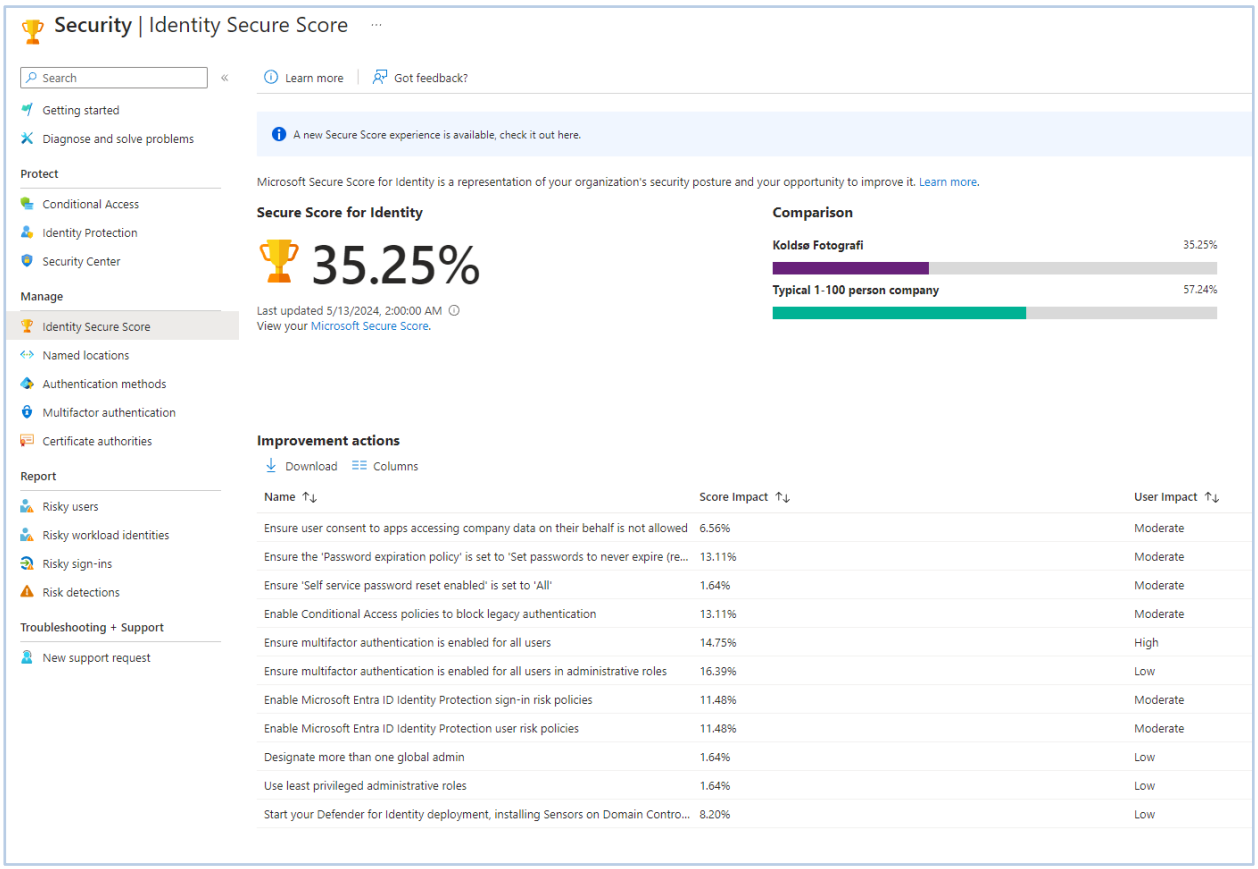
Billede 5.3.12.2-A: Cost analyse i Azure

5.3.12.3 Monitorering i Entra

I Entra monitoreres data vedrørende identitetssikring. Her er der ud fra en realtime implementering behov for forbedring, men set ud fra projektomfanget vurderes niveauet tilstrækkeligt.



Billede 5.3.12.3-A: Secure Score for Identity - projektvirksomhed vs. tilsvarende virksomhed, Entra



Billede 5.3.12.3-B: Overview i Entra

Der er mange ting, man kan monitorere på i Entra og til udbedring findes en rekommanderet liste med sikkerhedstiltag.

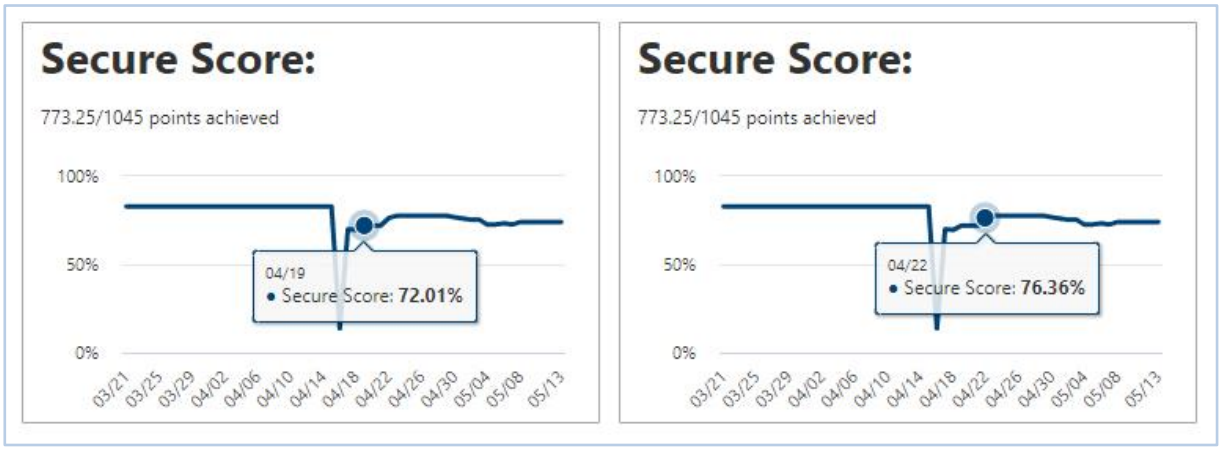
5.3.12.4 Monitorering i Defender

I Defender overvåges sikkerheden omkring identitet, datasikkerhed, applikationer og enheder gennem to statistiske analyser: Exposure Score og Security Score.

Exposure Score identificerer enhedernes sårbarheder og guider til udbedring af sikkerhedsrisici. Security Score vurderer virksomhedens sikkerhed inden for applikationer, enheder, identitet og datasikkerhed.

Platformen viser en liste over anbefalede sikkerhedstiltag til risikoforbedring, som er brugt i projektet til at finoptimere sikkerheden. Før optimeringen lå Exposure Score på 32/100 og Secure Score på 72,01%. Efter optimeringen faldt Exposure Score til 15/100, og Secure Score steg til 76,36%.

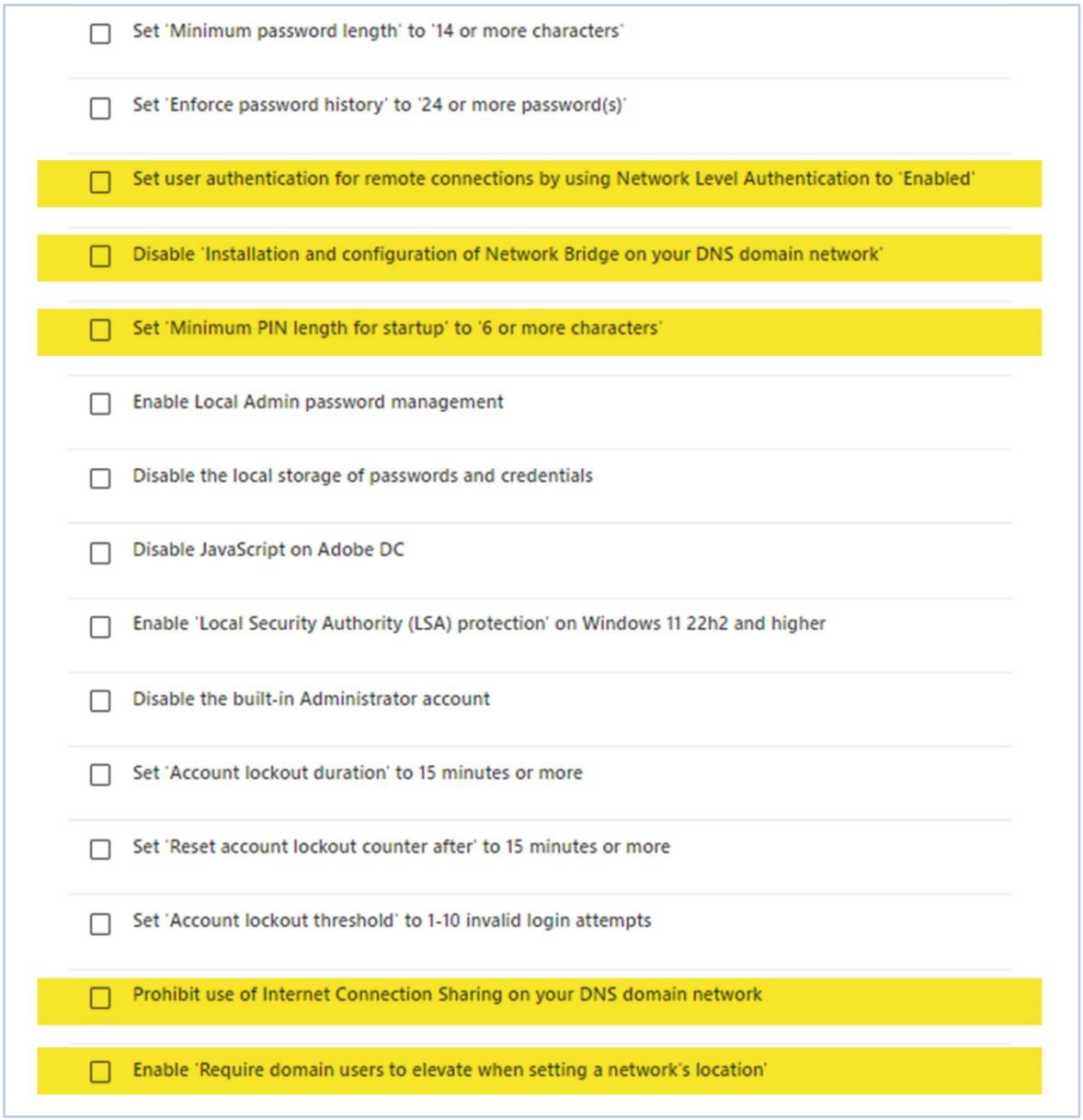
Billede 5.3.12.4-A: Exposure Score før og efter finjustering af sikkerhedsoptimering



Billede 5.3.12.4-B: Secure Score før og efter finjustering af sikkerhedsoptimering

Listen med de udførte tiltag (gul) illustreres nedenfor:

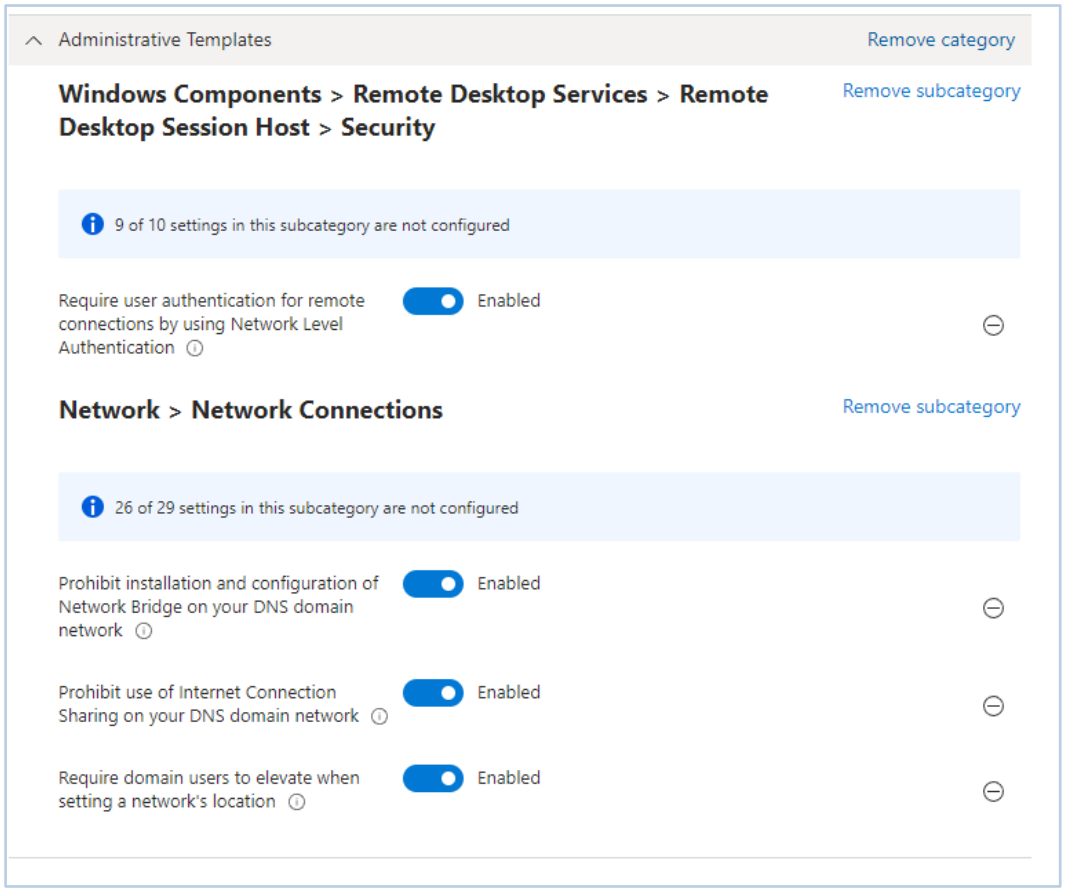
Billede 5.3.12.4-C: Recommendation list del 1, Defender platform



Billede 5.3.12.4-D: Recommendation list del 2, Defender platform

Blandt rettelserne var justeringer til Ransomware politik, antivirus og firewall.[19] Hertil blev konfigurationsprofilen "Network Security Enhancements" omhandlende Network Settings oprettet.

[19] *Se Bilag 26: Logbog, s. 104 + s. 111*



Billede 5.3.12.4-E: Netværksjusteringer opsættes i Intune

På Defender platformen ses også at projektvirksomheden har en Secure Score på 74/100 (pr. 13/05/2024) sammenlignet med tilsvarende virksomheder, der ranker 46,88/100.

Billede 5.3.12.4-F: Secure Score på projektvirksomhed kontra tilsvarende virksomhed

Med udgangspunkt i et tilfredsstillende niveau af sikkerhed for dette PoC-projekt, foretages der ikke yderligere sikkerhedsoptimeringer.

5.4 System- & Integrationstest

5.4.1 Gennemgang af generel opsætning

Ved testgennemgang med seniorkonsulent Ømer Hendem fra NHC A/S, blev følgende justeringer til brugeroplevelsen tilføjet projektopgaverne og efterfølgende opsat som konfigurationsprofiler samt testet:

- Opsætning af standard applikationer til mail, html og PDF ***(se bilag 21)***
- Automatisk fjernelse af Adobe Reader genvej ***(se bilag 22)***
- Deaktivering af "New Outlook" toggle knap ***(se bilag 23)***
- Fastgørelse af applikationsgenveje på proceslinjen ***(se bilag 24)***

Bortset fra disse finjusteringer vurderede han projektet som tilfredsstillende opsat ud fra projektets kriterier.

5.4.2 Gennemgang af sikkerhedskonfigurationer

Ved testgennemgang af sikkerhedskonfigurationer med sikkerhedsspecialist Rasmus E. Kristensen fra NHC A/S, blev det vurderet at sikkerheden særligt omkring Ransomware-politikken var meget stram og kunne give uønskede blokeringer af nødvendigt indhold. Politikken lempes i takt med evt. opstående konflikter.

Yderligere anbefalede han at opsætte en LAPS (Local Admin Password) politik. Først skulle LAPS enables i Entra og herefter kunne politikken konfigureres under *Endpoint security* ▷ *Account Protection* i Intune ***(se bilag 25)***. Politikken forhindrer brugere i at oprette lokale admins. I stedet vil der være oprettet en "lokal admin" bruger i Intune systemet. Har man behov for adgang til en pc, bruges denne lokale admin bruger. Tillige kan sikkerheden sættes således at passwordet udskiftes ugentligt.

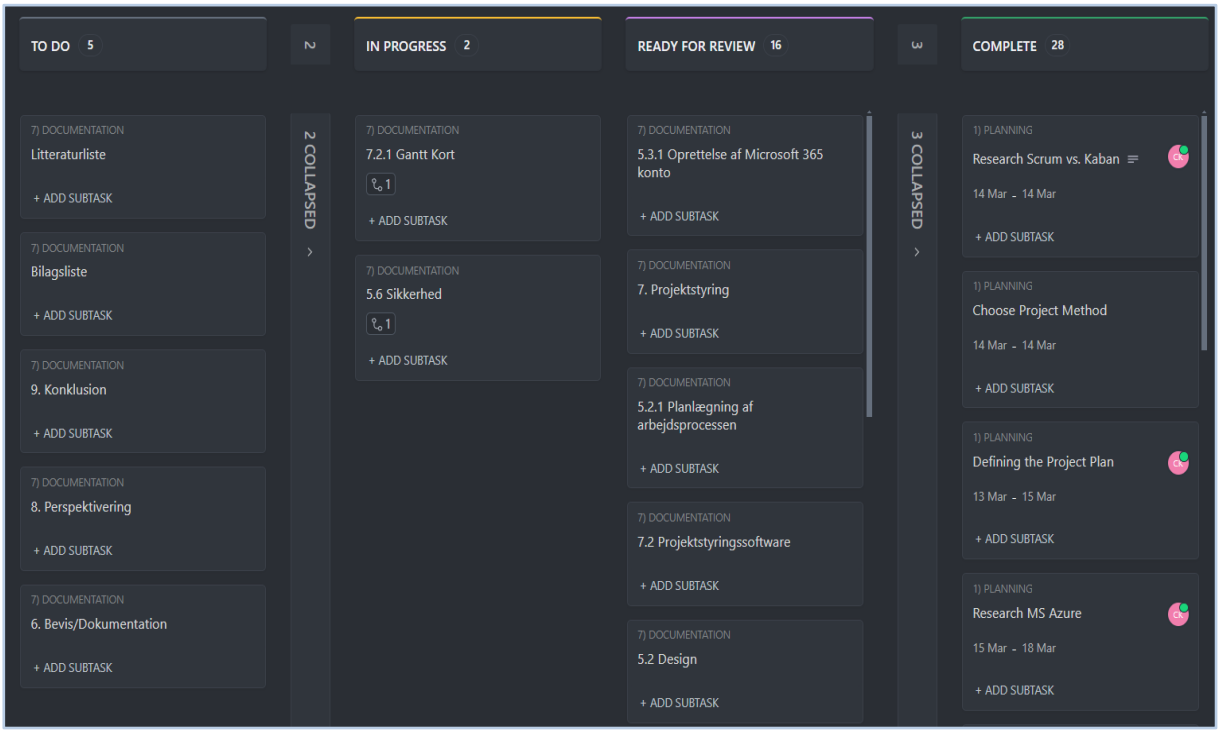
Med disse sikkerhedsoptimeringer vurderede han sikkerheden meget tilfredsstillende ud fra projektets omfang.

6. Projektstyring

Projektet følger den agile[20] projektledelsesmetode Kanban, der vægter indskrænkning og visualisering af opgaverne for at skabe et effektivt workflow. Ifølge Max Rehkopf fra Atlassian, færdiggøres opgaver hurtigere, hvis man begrænser antallet af igangværende opgaver til et minimum - dette kaldes WIP (Work-In-Progress) Limit[21]. Projektets WIP Limit er 2, og dette forsøges så vidt muligt overholdt. WIP udregnes med nedenstående formel:

antal projektmedlemmer * 1,5 (eller 2) = WIP Limit

Valget af metoden skyldes metodens lette implementering uden krav om forudgående erfaring, dens fleksibilitet til at tilpasse sig ændringer på timebasis og dens stærke værktøj til synlig struktur. Opgaverne bør ikke vare mere end 8 timer og er visualiseret som flytbare rubrikker på et Kanban Board i softwaren ClickUp.



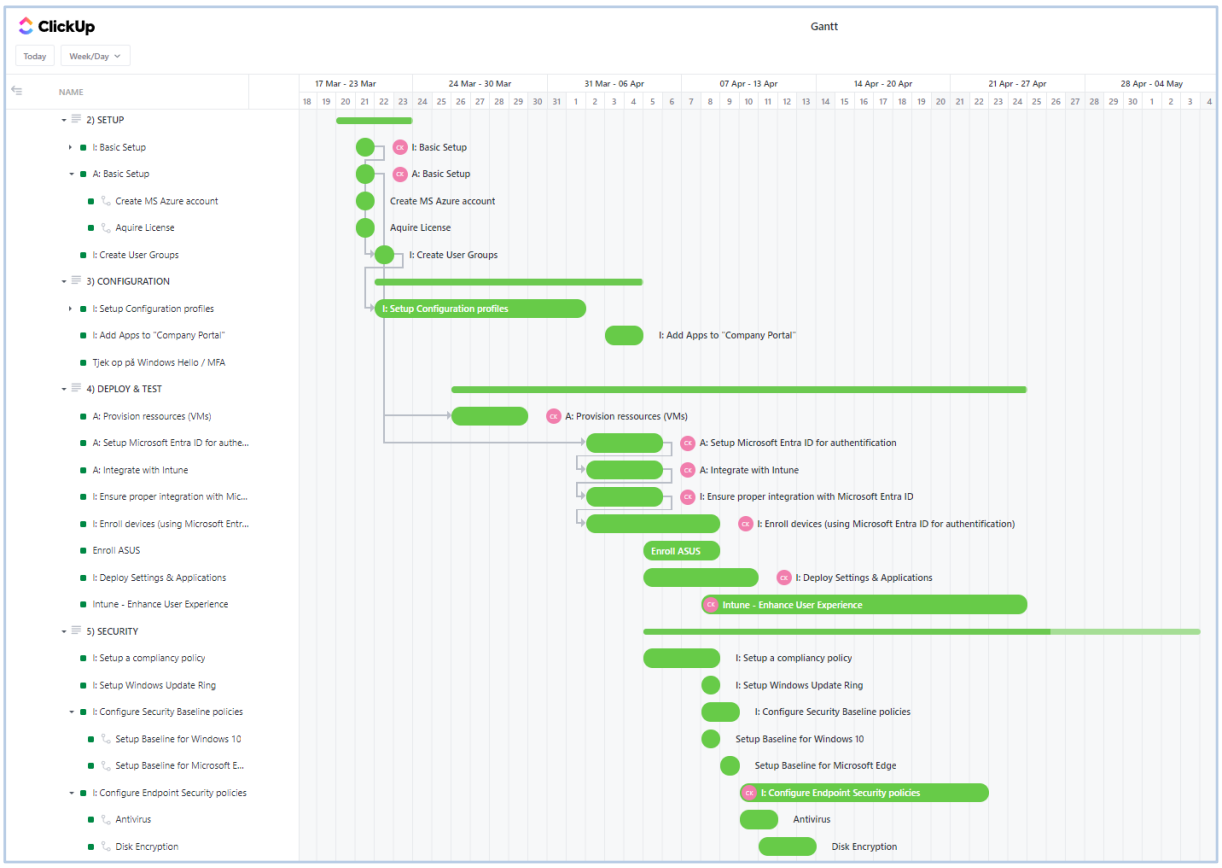
Billede 6-A: Kanban-board i ClickUp

Der benyttes primært visningsværktøjerne *Board View* (Kanban) og *Gantt View* til visualisering af arbejdsopgaverne. Til tidsestimering af hovedopgaverne har jeg rådført mig hos NHC A/S.

[20] *Hvad er agile metoder inden for projektledelse? - Dropbox*

[21] *"WIP-limits" af Atlassian*

Deadlines for de enkelte opgaver blev bestemt og opgaverne blev indsat i Gantt Chart, hvorefter afhængighederne mellem opgaverne blev tilknyttet.

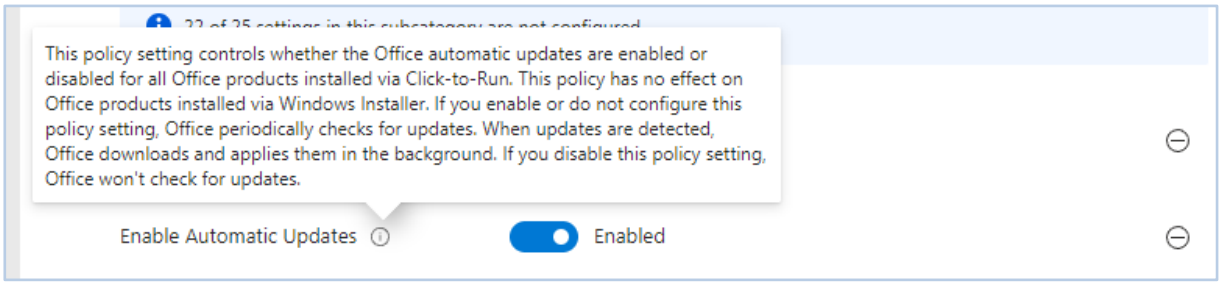


Billede 6-B: Udsnit af Gantt Chart med afhængigheder, ClickUp

7. Perspektivering

Projektarbejdet har givet mig et godt kendskab til arbejdsprocesserne og Kanban-metoden var et værdifuldt redskab til projektstyring, når arbejdsmængden var overvældende. Metoden gav et godt overblik og skabte et flydende workflow.

Under grundopsætningen var dét at finde de rette konfigurationer blandt de 120 områder med underkategorier og individuelle indstillinger meget tidskrævende. Det krævede omhyggelig gennemgang og nærlæsning af dokumentation.



Billede 7-A: Nærlæsning af effekten af den pågældende konfiguration, Intune

Opsætning og test af sikkerhed var dog den mest krævende fase, hvor jeg tilegnede mig ny viden om Intune, Entra og Defender-platformene, herunder om monitorering og konfiguration af WHfB, MFA, kryptering, compliance, baselines, anti-malware og anti-phishing. Projektets omfang begrænsede dog min dybere udforskning af sikkerhedsoptimering.

Processer, tests, resultater og refleksioner omkring projektarbejdet er dokumenteret i ***Bilag 26: Logbog****.*

Projektet har gjort mig i stand til at opsætte Intune fra bunden og jeg har tilladt mig at eksperimentere med konfigurationen, hvilket gav et godt indblik i sammenhængene mellem platformene.

Jeg har lært nye metoder og værktøjer at kende, jeg er blevet mere selvkørende og har opnået forståelse ikke blot for platformene, men også for hvordan man problemløser med udgangspunkt i dokumentationen. Disse kompetencer har særlig stor værdi for NHC A/S, hvor projektet repræsentere et typisk implementeringsscenarie[22], hvilket også har ført til fastansættelse hos NHC A/S fra 1. juni 2024.

[22] *Bilag 27: NHC virksomhedserklæring*

8. Konklusion

Projektets hovedmål var at opsætte et centraliseret system til administration, håndtering, konfiguration og vedligeholdelse af klientenheder på en konsistent og automatiseret måde. Fokus var at sikre en konsistent enhedskonfigurationen og optimere sikkerhedsindstillinger med mulighed for monitorering. Til dette blev Intune implementeret sammen med Azure samt Entra og Defender for udvidet sikkerhedskonfiguration og monitorering.

Løsningen er økonomisk fordelagtig for kunden, som allerede har licenser, der inkluderer disse platforme, og den imødekommer behovet for centraliseret og automatiseret enhedsadministration. Systemet kan tilpasses specifikke behov og desuden indrulle andre enheder som Mac og smartphones, selvom fokus i projektet var på Windows 11-enheder.

Opsætningen inkluderer grundlæggende enhedsadfærd, sikkerhedsindstillinger og brugeroplevelse. Hertil kommer udvidet sikkerhedsoptimering af firewall, antivirus, kryptering, antiphishing og anti-malware samt konfiguration af MFA, Windows Hello for Business, Password Protection og FIDO2/Microsoft Authenticator.

Projektet blev udført selvstændigt hos NHC A/S i Silkeborg, hvor jeg opnåede dybdegående viden om Intune og et bredt kendskab til sikkerhedskonfiguration i Defender og Entra. Ved hjælp af den agile Kanban-metode blev planlægningen og opsætningen effektivt gennemført. Projektet har gjort mig mere selvkørende og jeg er i stand til at arbejde selvstændigt og assistere NHC A/S ved større implementeringsprojekter.

Ud fra de opstillede krav for projektet samt de forskellige udførte tests og systemgennemgange med NHC-repræsentanter, konkluderes det at løsningen lever op til alle projektets krav. Projektet har ligeledes givet mig praktisk erfaring med platforme og arbejdsprocesser, inklusive ekstra erfaring med Entra og Defender, som oprindeligt ikke var en del af projektbeskrivelsen.

9. Kildeliste

DATO	TITEL, UDGIVER & LINK
21-05-2024	"Hvad er Kanban? Den ultimative guide til Kanban" af certificeret projektleder Mark Guldbrandsen https://blivprojektleder.dk/kanban/
21-05-2024	"Hvad er agile metoder inden for projektledelse?" af Dropbox https://experience.dropbox.com/da-dk/resources/agile-methodology
21-05-2024	"Microsoft Entra ID Authentication Methods Explained" by Andy Malone https://youtu.be/iSYcWNpi_6A?si=eP98CKyZWTYTipYV
21-05-2024	"Advanced Encryption Standard (AES)" by TechTarget https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
21-05-2024	"Cryptanalysis of a spatiotemporal chaoticimage/video cryptosystem" by ResearchGate https://www.researchgate.net/publication/215783767_Cryptanalysis_of_a_spatiotemporal_chaotic_imagevideo_cryptosystem#pf5
21-05-2024	"Enroll devices via Microsoft Entra join:" https://learn.microsoft.com/en-us/education/windows/tutorial-school-deployment/enroll-entra-join
21-05-2024	Azure Basics Tutorial af Learnit Training (YouTube) https://www.youtube.com/watch?v=TJOwP5VhvAo

10. Appendix

BILAGSNR.	NAVN	FILTYPE
BILAG 1	Blokdiagram	(PDF)
BILAG 2	WBS-diagram	(PDF)
BILAG 3	Opsætning af Azure testmiljø, uddybet	(PDF)
BILAG 4	Device Restrictions, config	(PDF)
BILAG 5	MS App Auto Update, config	(PDF)
BILAG 6	Office Settings, config	(PDF)
BILAG 7	MS Security Settings, config	(PDF)
BILAG 8	MS Edge Settigs, config	(PDF)
BILAG 9	MS OneDrive Policy (config)	(PDF)
BILAG 10	Allow printer driver installation, config	(PDF)
BILAG 11	Windows Update, config	(PDF)
BILAG 12	Udrulningspolitik, config	(PDF)
BILAG 13	Baseline - SECURITY BASELINE FOR WINDOWS	(PDF)
BILAG 14	Baseline - MICROSOFT EDGE BASELINE	(PDF)
BILAG 15	Client Compliancy Policy	(PDF)
BILAG 16	Defender Antivirus	(PDF)
BILAG 17	Defender Firewall	(PDF)
BILAG 18	BitLocker Encryption Policy	(PDF)
BILAG 19	MS Defender SmartScreen	(PDF)
BILAG 20	Ransomware politik	(PDF)
BILAG 21	Default Application Association - config & test	(PDF)

BILAG 22	Fjernelse af Adobe genvej - config & test	(PDF)
BILAG 23	Disabling "New Outlook" toggle knap - config & test	(PDF)
BILAG 24	Fastgørelse af ikoner til proceslinje - config & test	(PDF)
BILAG 25	LAPS sikkerhedspolitik - config	(PDF)
BILAG 26	Logbog *(147 sider)*	(PDF)
BILAG 27	NHC virksomhedserklæring	(PDF)