ARCADA

Microsoft Enterprise Mobility and Security för medelstora företag

Sebastian Heinonen

Examensarbete
Informations- och Medieteknik
2017

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och Medieteknik
Identifikationsnummer:	5055
Författare:	Sebastian Heinonen
Arbetets namn:	Microsoft Enterprise Mobility and Security för medelstora företag
Handledare (Arcada):	Johnny Biström
Uppdragsgivare:	

Sammandrag:
Trenden inom företagsvärlden ligger inom mobilitet och produktivitet vilket innebär att mycket av arbetet skall kunna skötas varifrån som helst och på alla plattformar. Denna trend ställer ett stort krav på säkerheten samt administreringen. Microsoft Enterprise Mobility and Security (EMS) är en systemhanteringsprodukt utvecklad av Microsoft för att administrera mobila enheter och säkerställa informationssäkerheten. Syftet är att utreda om detta produktpaket är ett lönsamt alternativ för att möta kraven som dagens trend ställer och att granska processen gällande implementering av EMS-systemet. Målet med arbetet är att ha ett klart konfigurerat mobilhanteringssystem med hjälp av EMS och att få svar på om detta är ett relevant system för medelstora företag. Arbetet skall hjälpa medelstora företag och deras IT-administratörer vid planering eller val av ett mobilhanteringssystem. I arbetet granskas vad EMS systemet består av och vilka dessa delars uppgift är. Detta arbete baserar sig på information från nätet samt på tester och validering av ett färdigt EMS-system.

Nyckelord:	EMS, Intune, Azure, O365
Sidantal:	56
Språk:	Svenska
Datum för godkännande:	09.05.2017

DEGREE THESIS	
Arcada	
Degree Programme:	Information and Media Technology
Identification number:	5055
Author:	Sebastian Heinonen
Title:	Microsoft Enterprise Mobility and Security for medium-sized enterprises
Supervisor (Arcada):	Johnny Biström
Commissioned by:	

Abstract:
Today's trend in the corporate world is in mobility and productivity, this because it is expected that employees shall be able to work from anywhere and have access to company data from any device. This trend is quite a challenge considering security and administration. Microsoft Enterprise Mobility and Security(EMS) is a mobile management solution for administrating mobile devices while keeping company data secure. The purpose of this study is to find it if EMS is a suitable product for midsized business to meet the requirements that today's trend generates and to inspect the process of implementing this solution. This study should help corporates and their IT-department when considering or planning new mobile device management solutions. The aim of this study is to configure a complete EMS solution and validate it for corporate enrollment. This research includes the main parts of the EMS system and an overview of every part's key features. The study is based on online material and functional testing of the EMS solution

Keywords:	EMS, Intune, Azure, O365, Molntjänst
Number of pages:	56
Language:	Swedish
Date of acceptance:	09.05.2017

INNEHÅLL

FIGURER

TABELLER

1 INLEDNING

Dagens trend inom informationsteknik ligger i mobilitet vilket innebär att arbetet inte skall vara bundet till bara företagets kontor utan arbetet skall kunna skötas varifrån som helst samt från mobila enheter. Denna trend ställer krav på administreringen samt säkerheten. En del av arbetet måste även vara tillgängligt via arbetstagarens personliga mobil vilket ställer ytterligare krav för att hålla företagets information säker.

Detta arbete kommer att fokusera på ovannämnda krav genom att undersöka om Microsoft Enterprise Mobility & Security (EMS) kunde vara en lämplig lösning för ett medelstort företag. Arbetet kommer också att behandla olika faser av systeminförandet. Microsoft EMS täcker identifiering, säkerhet och administration för mobila enheter (inklusive bärbara datorer).

1.1 Bakgrund

Intresset för att utreda EMS-systemet baserar sig på tidigare erfarenheter av delar av systemet vid ett stort IT-företag och iakttagelser av att flera företag har tagit i bruk EMS. Jag har inte varit med i faserna vid införandet eller planeringen av systemet och vill därför undersöka vilka fördelar ett medelstort företag kunde ha av systemet.

1.2 Syfte och mål

Syftet med arbetet är att undersöka processen av införandet av EMS i ett medelstort företag samt vilka krav och problem detta innebär för administratörerna. Målet för arbetet är att konfigurera och planera ett mobilhanteringssystem med EMS som är färdigt för implementering och att granska arbetsflödet för processen. Det färdiga arbetet förväntas ge svar på frågan: är detta ett relevant system för medelstora företag och vilka typer av företag kunde utnyttja systemet?

Detta arbete kan användas som en referensram för företag och dess IT-administratörer som har tänkt ta i bruk ett nytt mobilhanteringssystem, dock inte som en handbok eller instruktionsbok. Av läsaren förväntas kunskap i administrering av företagets olika IT-system.

1.3 Presentation av företaget

I arbetet utgås från ett företag som är arbetsgivare för 50 personer. Företaget har inte sedan förr en lokal servermiljö eller ordentlig infrastruktur och behöver på grund av detta en mera kontrollerad miljö. Företaget växer och behöver på grund av detta en möjlighet att administrera och säkra sin miljö mot säkerhetsrisker. Som plattform har valts Microsoft's Enterprise Mobility and Security (EMS) för att inte behöva ta i bruk lokala servrar. Företaget använder sig för tillfället endast av bärbara datorer samt mobila enheter (smarttelefon och surfplatta).

Företaget har beställt som tjänst att planera och utföra införandet av Microsofts Enterprise Mobility and Security (EMS). Företaget vill att arbetstagarna skall kunna använda sig av de vanligaste Office-applikationerna och komma åt företagets filer via sina mobila enheter.

1.4 Avgränsning

Tyngdpunkten i arbetet kommer att ligga på Enterprise Mobility and Security och går inte djupare in på andra Microsofts molnbaserade lösningar. Arbetet kommer inte heller att på djupet behandla implementering av tredje parts program i EMS, vilket kunde vara nästa steg för införandet av systemet. I arbetet fokuseras på mobila plattformar i OS och Android, däremot kommer registrering och hantering av bärbara datorer inte att behandlas.

På grund av att företaget inte sedan tidigare har centraliserad användarkontroll kommer både skapandet av användare och grupper att göras direkt i Azure Active Directory (Azure AD). Detta innebär att arbetet inte behandlar kopiering av användare från en lokal servermiljö till den molnbaserade Azure Ad-användarhanteringen.

1.5 Terminologi

AD: Active Directory, Microsofts katalogtjänst för användarhantering

ATA: Advanced Threat Analytics

Azure AD: Identitets- och åtkomsthanteringstjänst för molnbaserade lösningar publicerad av Microsoft (Molnbaserad Active Directory)

BYOD: Bring Your Own Device

EMS: Enterprise Mobility + Security

Intune: Webbaserad systemhanteringsprodukt av Microsoft

MAM: Mobile App management

MDM: Mobile Device Management

O365: Office 365, Microsoft Office paket

OMA-URI: Open Mobile Alliance Uniform Resource Identifier

SaaS: Software as a Service

SSO: Single Sign On, ett och samma användarkonto för flera plattformar

XML: Extensible Markup Language

1.6 Länkar

Azure portal: https://portal.azure.com/

Cloud app Security: https://portal.cloudappsecurity.com/

EMS-registrering: https://signup.microsoft.com/Signup?OfferId=87dd2714-d452-48a0-a809-d2f58c4f68b7&ali=1

IosPSK-generator: http://johnathonb.com/2015/05/intune-ios-psk-mobile-config-generator/

Intune Admin portal: https://manage.microsoft.com/

O365 Admin portal: https://portal.office.com/adminportal/home

2 ENTERPRISE MOBILITY + SECURITY

Detta kapitel innehåller en beskrivning av vad Microsoft Enterprise Mobility + Security (EMS) innebär samt av vad som ingår i produktpaketet.

Microsoft Enterprise Mobility + Security är Microsofts produkt med vilket ett företag kan hantera mobila enheters hela livscykel, d.v.s. införandet, hantering av applikationer, användarkontroll och säkerhet. EMS är inte bara för hantering mobila enheter utan via det kan även Windows och Apples Mac (MAC OS X) datorer administreras. Med hjälp av EMS kan företag även hålla en bättre invertering på sina program samt enheter.

All hantering av systemet sker via molnet. Detta innebär att systemet kan hanteras via alla plattformar med webbläsare samt genom uppkoppling till internet. De mest centrala delarna av systemet ur administrationens synvinkel är Azure Active Directory (Azure AD), Intune, Azure Information Protection och Cloud App Security. Dessa delar presenteras separat i kommande kapitel. (Gilbert 2016).

2.1 Identifikation och åtkomst – Azure AD

Användarhantering och åtkomstkontroll i EMS styrs via Azure AD. Azure AD är multitenant, vilket innebär att flera företag delar på samma server. Azure AD använder sig av Single Sign On (SSO) metoden där användare kan utnyttja samma konto för flera olika SAAS (Software As A Service) program som t.ex. Office365 och Salesforce. De viktigaste egenskaperna som ingår i Azure ad är:

- flerfaktorsautentisering
- enhetsregistrering
- lösenordsbyte som självservice
- gruppadministrering som självservice
- administrering av användarkonton
- rollbaserad åtkomsthantering
- insamling av data över användning av applikationer
- säkerhetsmonitorering.

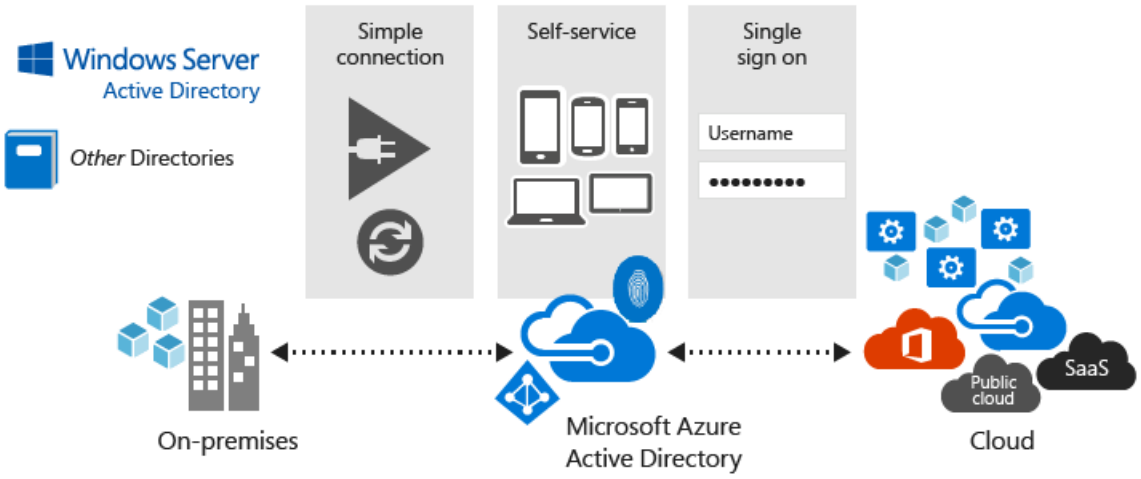
(Collier & Shahan 2016 s.181-184).

Azure AD:s infrastruktur ligger på 28 datacenter runt om i världen och har automatiserad felomkoppling. Detta betyder att om det datacenter går ned där företagets Azure Ad information ligger, så finns det alltid en kopia av företagets data på två andra datacenter som trafiken kopplas till. (Love 2016c).

För tillfället finns det två olika versioner av Azure Ad: Azure AD Premium 1 och Azure AD Premium P2. Båda versionerna innehåller samma basfunktioner men P2 innehåller även följande funktioner: Azure AD Identity Protection och Privileged Identity Management (PIM). Identity Protection innebär att man lättare kan upptäcka sårbarheter när det gäller identiteter inom företaget genom automatisering av rapporter som visar sårbarheter. Identity Protection ger också en möjlighet att kunna undersöka skadliga händelser och få en uppfattning om vad som orsakat skadan.

Privileged Identity Management medför möjlighet att administrera och observera åtkomsten i företagets nätverk. Detta gör det lättare att övervaka användare med administratörsrättigheter och deras inloggningshistoria. Via PIM kan man även ge tillfälliga administratörsrättigheter åt användare för MS online-tjänster såsom Office 365 eller Intune.

Figur 1 visar hur Azure Ad är kopplad till andra system. Samma lösenord fungerar för molnbaserade tjänster (Cloud) och för lokala tjänster som är uppkopplade till standard Active Directory som oftast ligger på en lokal server (On-Premises). (Love 2017b).



Figur 1. Azure AD sammankoppling med lokal infrastruktur (Love 2016c)

2.1.1 Azure Ad och Active directory hybridomgivning

Azure Ad kan integreras med ett företags egna Active directory som ligger på företagets lokala server, detta betyder att användarna mellan Azure AD och Active Directory är synkroniserade med varandra. Servicen som sköter om synkroniseringen heter Azure Ad Connect som består av tre delar: Synkroniseringsservice, Active Directory Federation Services-komponenten (AD FS) och övervakningskomponenten Azure AD Connect Health. Synkroniseringsservicen är ansvarig för att replikera användare, grupper samt objekt i molnet (Azure Ad).

AD FS är en valfri komponent som kan användas för att stöda komplexa hybridmiljöer med lokal AD-infrastruktur. Den används även om instansen använder flera domäner. Azure Ad Connect Health står för övervakning av trafiken mellan Azure AD och Active directory och trafiken kan följas via Azure-portalen. (Mathers 2016)

2.1.2 Azure Ad som fristående service

Azure Ad kan även användas som en fristående service vilket betyder att all användarhantering sker via Azure Ad. I detta fall krävs det ingen lokal infrastruktur av företaget. Detta kan vara en möjlighet för nya företag som inte investerat i lokala servrar och som vill ha hela sin infrastruktur i molnet. Om detta är fallet skapas och hanteras alla använ-

dare och grupper i molnet via Azure Ad. Denna modell kommer att användas i detta arbete. (Shinder 2015).

2.2 Microsoft Intune

Microsoft Intune är en central del som ingår i Microsoft EMS som är en molnbaserad systemhanteringsprodukt för att administrera klienter (Windows, IOS, MAC OS X och Android) oberoende var de befinner sig. Via Intune kan företaget hantera åtkomsten till applikationer, resurser och filer på ett säkert sätt. Intune har en webbkonsol varifrån administratörerna hanterar behövliga operationer. Intune har utöver Adminportalen en portal som är riktad till användare. Portalen som vanliga användare använder sig av heter Intune Company Portal och här kan användaren göra följande saker:

- Registrera/ta i bruk en enhet.
- Följa statusen på sin enhet.
- Byta lösenord/nollställa lösenord.
- Fjärrlåsa sin mobila enhet.
- Ladda ner applikationer som företaget gett ut.
- Kontakta administratörerna för stöd.

(Avraamides 2016).

Intune kan också användas via hybridomgivning, vilket innebär att företaget redan har en utvecklad infrastruktur och enhetshantering i Microsofts Configuration Manager. Om detta är fallet så har företaget oftast redan enhets- och innehållshanteringen på egen server med Configuration Manager, då kan Intune användas för att hantera principer, profiler samt applikationer. (Tillman 2016a).

2.2.1 MDM – Mobile Device Management

Detta avsnitt behandlar MDM. För detta arbete används Intune som verktyg för MDM. Med MDM avses hantering av mobila enheter för att skydda företagets data samt öka produktiviteten. Vanligtvis ingår följande saker i en MDM-lösning:

- Enhetssäkerhet samt konfiguration. I detta ingår till exempel krav på pinkod och konfigurationer som ges ut av företaget.
- Hantering av stulna/borttappade apparater.
- Hantering av applikationer (MAM) – kapitel 2.2.2 beskriver hanteringen av applikationer.
- Resurshantering innebär hantering av åtkomst till företagets resurser, till exempel företagets trådlösa nätverk.
- Inventering och rapportering gällande enheterna.

I MDM-livscykeln, det vill säga mobilenheternas livscykel och hantering, ingår fem stadier börjande från registrering av enhet, konfigurering, säkerhet, kontroll/användning och monitorering. (Della Monica 2016a).

2.2.2 MAM – Mobile Application Management

Detta kapitel beskriver vad MAM (Mobile Application Management) innebär, det vill säga hanteringen av mobila applikationer som är en viktig del av mobilhanteringen.

Distribution och reglering av applikationerna ingår i MAM och all administration av applikationerna sker via Intune-konsolen. Där kan administratörer lägga till olika SAAS-applikationer, till exempel de program som ingår i MS Office-miljön. Med MAM kan man hantera vilka data som kan överföras till utomstående applikationer och därigenom skydda viktiga data (se: Mobile App Security).

Bortsett från andra Intune-regler distribueras inte applikationsregler direkt till enheten. I MAM sköts detta genom att reglerna är associerade med applikationen, reglerna/restriktionerna kopplas på då applikationen laddas ner till enheten.

I MAM kan applikationer regleras på två sätt före distribution i Intune. Första sättet är att använda en så kallad principhanterad applikation som har inbyggd App-SDK. För att använda detta sätt för att publicera en app via Intune måste det läggas till en länk i appen i Intune som för till Ios enhetens Appstore eller Androids Google Play. I detta scenario krävs inga andra åtgärder i Intune för att distribuera appen.

En annan möjlighet för att förbereda en applikation för önskade principer/regler är att använda sig av metoden som kallas ”Wrapped – App”. Dessa applikationer är oftast företagets egna och har inte inbyggd app – SDK. Dessa applikationer packas på nytt i Intune med ett verktyg som heter: ”Intune Wrapping Tool”. I detta arbete kommer inte denna metod att användas utan modellföretaget använder ännu bara färdiga applikationer. (Della Monica 2016b).

2.2.3 Införande av enheter

Då företaget bestämt sig att ta sig i bruk ett gemensamt mobilhanteringssystem är det första steget att få de mobila enheterna uppkopplade till och registrerade i systemet. Ett krav för ett lyckat MDM-system är att införandet skall vara enkelt både för administratörerna och användarna, detta för att få ut alla fördelar av ett MDM-system. Införandet uppdelas ofta i två delar beroende på om det är en företagsägd enhet eller en BYOD-enhet. Vid företagsägda enheter är ett administratörsstyrt införande det vanligaste sättet att ta systemet i bruk, vilket innebär att flera enheter tas i bruk och registreras samtidigt.

Detta arbete fokuserar mera på scenariot att ta i bruk BYOD-enheter. Detta skiljer sig från administratörsstyrt införande genom att användaren själv tar i bruk enheten och registrerar den i MDM-systemet. Denna enhetsregistrering sker vanligtvis med en så kallad ”push-metod” där enheten automatiskt uppmanas att registrera sig i företagets MDM-system då enheten försöker kontakta företagets nätverk eller resurser. Vid registreringen av enheter sker följande:

- Distribuering, åtkomst och hantering av externa samt interna applikationer.
- Säkerhets – och behörighetskonfigurering.
- Skydd mot säkerhetsrisker.

I de flesta fall av enhetsregistrering distribueras enheten med rätt behörighet som antingen från användarens konto (AD/Azure AD) eller från en användargrupp som enheten hör till. Vanligtvis har dessa behörighetsroller redan konfigurerats före registreringen så att enheterna direkt får rätt behörighet för att minimera säkerhetsrisker under registreringen. (Della Monica 2016a).

2.3 Säkerhet och skydd av data

Säkerhet och skydd av data är en viktig del av MDM-livscykeln, i kapitel 2.3 – 2.3.4 beskrivs hur detta är förverkligat i EMS från Microsofts synvinkel.

På vilket sätt sköts säkerheten för mobila enheter och hur skyddas viktig information som är åtkomlig via mobila enheter? Detta är en viktig fråga, speciellt då man utgår från att arbetstagaren sköter arbetsärenden via en personlig telefon eller surfplatta. Enligt Microsoft sker 63 % av attackerna via dålig användarkontroll och via stulna användarnamn och lösenord. I EMS försöker man avvärja dessa attacker med hjälp av identitetsbaserad säkerhet. Användarkontrollen sker via Azure AD som är beskrivet i tidigare kapitel (se Identifikation och Åtkomst) (Microsoft 2016c).

2.3.1 Advanced Threat Analytics – ATA

Advanced Threat Analytics eller ATA är en komponent som ingår i alla EMS-licenser. ATA kan övervaka trafiken över domänkontrollern genom portspegling till en ATA-port som använder en fysisk eller virtuell switch. Det går också att installera ATA Lightway Gateway vilket gör att portspegling inte behövs.

ATA söker information från flera datakällor såsom loggar och händelser för att lära sig användarnas beteende. På detta sätt kan ATA bygga en beteendeprofil på varenda användare i företagets nätverk.

Tekniken i ATA kan identifiera flera misstänksamma aktiviteter i företagets nätverk och fokuserar på den så kallade cyberattackskedjan, vilket innebär igenkännande av följande attacker/förberedande för attacker:

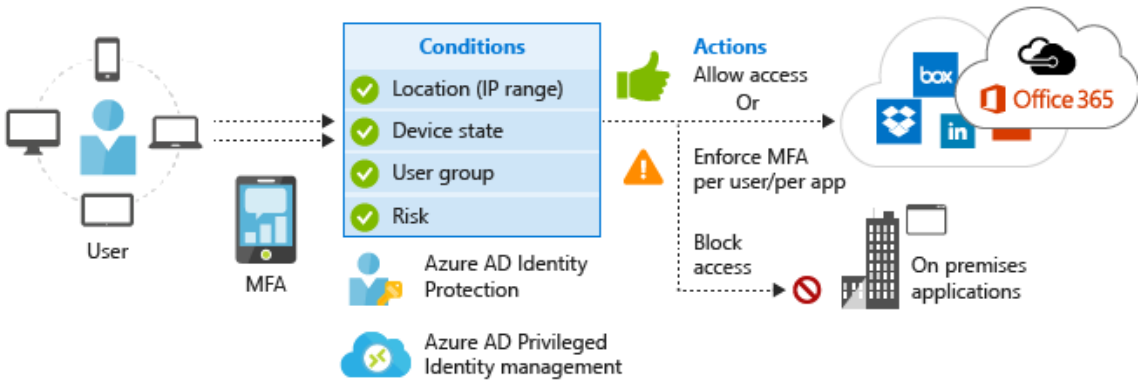
- Rekognosering av företagets miljö. I detta skede kan attackeraren samla in information om vilka tillgångar och enheter det finns i företagets nätverk.
- Identifiering av försök att sprida angreppsyta i företagets nätverk för senare attack.

- Domändominans - i detta skede försöker attackeraren samla in information för senare attack genom att använda olika ingångspunkter, användarnamn och tekniker.

Vanligtvis gäller liknande faser för de flesta attacker och de kan därför kännas igen och förutspås, oavsett vilken typ av företag det är som attackeras. ATA söker efter tre typer av avvikelser i nätverkstrafiken: skadliga attacker, onormalt beteende hos användare samt säkerhetsluckor och säkerhetsrisker. Om ATA upptäcker något avvikande beteende eller attacker fås denna information via ATA-konsolen som kan ge information om vem, vad, när och hur attacken skett. (Karlin 2017a).

2.3.2 Identitets- och användarskydd

Microsoft har en lösning för att skydda identitetsstölder via Azure AD Identity Protection. Funktionsprincipen för Azure Ad Identity Protection bygger på att denna service använder sig av adaptiva algoritmer och heuristik för att upptäcka avvikelser och händelser som tyder på att någons identitet/lösenord har missbrukats. (Vilcinskas 2017).



Figur 2. Funktionsprincipen för Azure AD Identity protections (Vilcinskas 2017)

2.3.3 Applikations- och enhetssäkerhet

Molnbaserade program skyddas i EMS med Cloud App Security. Administratörer kan övervaka användningen av alla molnbaserade program och få rapporter på användningsmönster samt upp-/nedladdningstrafik. Cloud app Security har en databas på över

13000 mobila SaaS-applikationer. En enhet i EMS skannas och ger en riskanalys på applikationen. Applikationen kontrolleras med 60 olika parametrar som granskar t.ex. publicerare, säkerhetsmekanismer och certifikat.

Data lagras inte i Cloud App Security-databaser utan endast metadata över aktivitetsloggar, identifieringsloggar och aviseringar. Cloud Discovery är en del av Cloud App Security som analyserar samt identifierar vilka program som används i företagets molnmiljö. På basis av insamlade loggar i Cloud Discovery kan administratörerna göra en överblicksrapport eller starta kontinuerliga rapporter med Cloud Discoverys logginsamlare. (Cai 2017).

2.3.4 Data- och filsäkerhet – Azure Information Protection

I EMS hanteras datasäkerheten via Azure Information Protection. Via detta system kan företaget styra säkerhetsklasser och filåtkomsten. Administratörer kan styra säkerheten för dokument/filer med grupper, det vill säga, en viss typ av data kan vara sekretessbelagd och dessa typer av dokument styrs med en grupp. Användare kan också markera dokument/filer som sekretessbelagda och sekretessinställningarna används enligt de regler som administratörerna har skapat.

Då användarna gör ett nytt dokument kan de själva också välja vem som har åtkomst till filen. De kan till exempel markera att ett dokument kan användas av ett partnerföretag men inte printas eller skickas vidare. Data och filer krypteras i Azure Information Security, vilket säkerställer att bara behöriga kan modifiera och få åtkomst till filerna.

Systemet ger också möjlighet att följa upp användningen av delat material och sparar loggar över användningen av materialet, t.ex. vid misstanke om missbruk av filer. (Bailey 2017c).

2.4 Prissättning och Licensering

Presentation av prissättning och licensering för EMS (Priserna är angivna i dollar och konverterade till Euro enligt den för tillfället gällande kursen).

EMS-licenserna säljs per användare och prissättningen gäller för användare per månad. För tillfället erbjuder Microsoft två licenser, en grundlicens som heter: Enterprise Mobility + Security E3 som är en grundlicens. Den andra licensen som innehåller alla delar av EMS heter: Enterprise Mobility + Security E5. I tabellen (tabell 1) nedan visas vad som ingår i respektive EMS-licens. (Microsoft.com 2016b)

Tabell 1. Prissättning av EMS (Microsoft 2016b)

EMS	**E3**	**E5**
Azure AD P1	✓	✓
Azure AD P2		✓
Windows Server Client Access License (CAL)	✓	✓
Microsoft Intune	✓	✓
Azure Information Protection Premium P1	✓	✓
Azure Information Protection Premium P2 (Utvidgad klassificering och kryptering av filer)		✓
Microsoft Advanced Threat Analytics	✓	✓
Microsoft Cloud App Security		✓
Pris per användare i månaden	8,13€	13,95€

3 INFÖRANDE AV EMS FÖR FÖRETAGET

Detta kapitel behandlar införandet och konfigurationen av EMS tjänsten för företaget. I kapitlet beaktas de väsentligaste delarna av EMS för att hanteringen av mobila enheter skall kunna inledas.

3.1 Planering av MDM

Planen för införandet av mobilhantering för företaget kommer att göras enligt BYOD-metoden, vilket betyder att användarna själva inför enheterna enligt angivna instruktioner. Från användarnas synvinkel innebär detta att de på sin enhet laddar ner applikationen Company Portal där de följer angivna steg för att registrera sin enhet i Intune.

Administratörens uppgift kommer att vara att säkerställa och följa upp att enheterna registreras i Intune Admin-portalen.

3.1.1 Plan för enhetshantering

Företaget kommer att ta i bruk Intune som fristående service. Detta betyder att all Intune-administrering sker i molnet och att Intune inte är kopplad till Configuration Manager. Denna lösning valdes för att nå en lättare administrering av mobila enheter. På detta sätt kan administreringen ske på alla ställen där det finns på internetuppkoppling. Detta medför igen mera produktivitet för administreringen. Fristående Intune valdes också för att företaget inte hade något mobilhanteringsverktyg från förr och för att administreringsmöjligheterna blir betydligt bredare med enbart Intune. I fristående Intune kan man hantera upp till 50 000 enheter, vilket kommer att räcka till för företaget för en lång tid framåt.

Som de viktigaste fördelarna för fristående Intune kan följande betraktas:

- Stöder Android-, iOS-, Windows 10-, Windows 8- och Windows Phone-plattformar.
- Stöd för Exchange ActiveSync.
- Intune medför enkel administrering via webbaserad konsol.
- Stöd för gruppbaserade principer, vilket gör det enklare att hantera flera typer av enheter samtidigt.
- Stöd för att upptäcka enheter som det har gjorts en ”jailbreak” (upplåsning) eller Root (enhetsrotning) på.
- Stöd för fullständig och selektiv fabriksåterställning.
- I Intune ingår en företagsportal varifrån användarna kan ladda ner företagets interna program och tredjepartsprogram på ett säkert sätt.
- Distribuering av certifikat.
- Stöd för att bara kunna använda vissa browsers på enheten.
- Stöd för att förhindra kopiering från bestämda applikationer.

(Microsoft, 2015d).

3.1.2 Plan för MAM

För att skydda företagets data och hindra läckage av information har det beslutats att text från dokument som tillhör företaget inte kan kopieras till 3:dje parts program. Det skall ändå vara möjligt att kopiera data mellan interna program som används i företaget som Outlook och Word. I det första skedet kommer det bara att tas i bruk principhanterade applikationer på grund av att företaget inte har egna internt skapade applikationer. Första programmet som kommer att ingå i företagets MAM-system kommer att vara Microsoft Word som ingår i produktpaketet Office 365.

Planen är att administrationen skall sköta distributionen av första applikationen. I det skede när applikationen publiceras är enheterna då redan registrerade i mobilhanteringssystemet Intune.

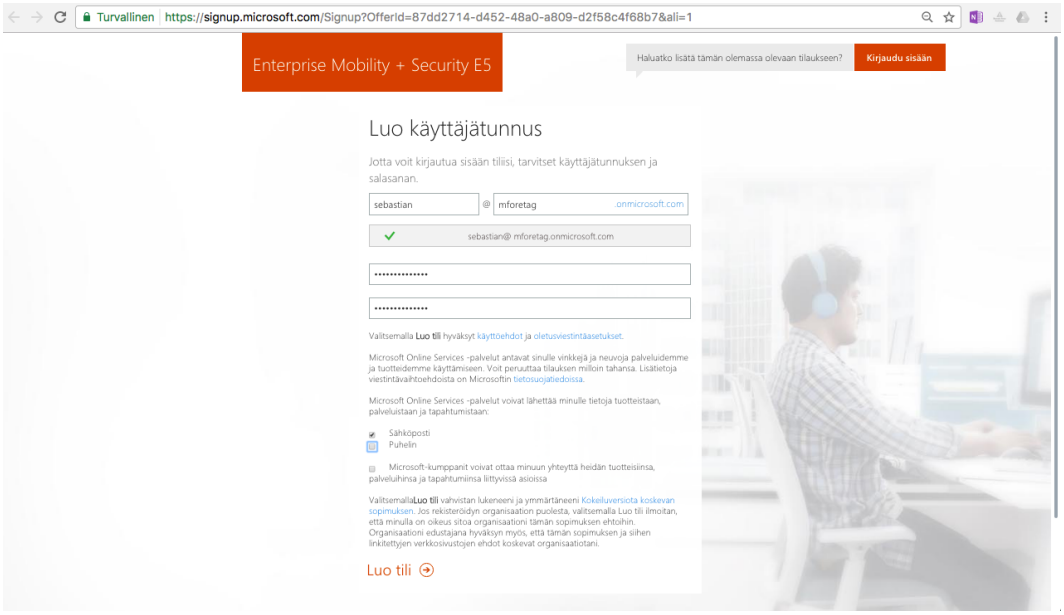
3.2 Skapandet av konto i EMS

Detta kapitel innehåller en beskrivning av de första stegen vid införandet av EMS i företaget. I detta arbete används en gratis 30 dagars utvärderingsversion av EMS, de mest väsentliga funktionerna för ett fungerande mobilhanteringssystem kommer att granskas.

Första skedet av införandet av systemet är att skapa ett EMS konto för företaget och detta görs via EMS-registreringsportalen (se länkar). Där ges uppgifter om var företaget är beläget, beställarens- och företagets namn, telefonnummer, e-post och storleken på företaget.

I nästa steg skapades ett masterkonto för att Administrera EMS. Se figur 5 nedan.
För arbetet aktiverades ett konto som fungerar som masterkonto för administreringen,
I detta fall: admin@Egetforetag.onmicrosoft.com. Nästa steg var att ta i bruk servicen MS Azure för att kunna komma åt Azure-portalen varifrån Azure AD styrs. Det var en överraskning att man separat var tvungen att aktivera en beställning av Azure då Microsoft beskriver att den ingår i EMS (dock inga extra kostnader). Det vore klarare om Azure Ad kunde användas som fristående service. Efter att ha aktiverat Azure subskriptionen och öppnat Azure-portalen är redan nästa steg att lägga till användare i Azure Ad.

(May, 2015). För själva skapandet av kontot för att kunna påbörja användningen tog det ca 20 minuter.

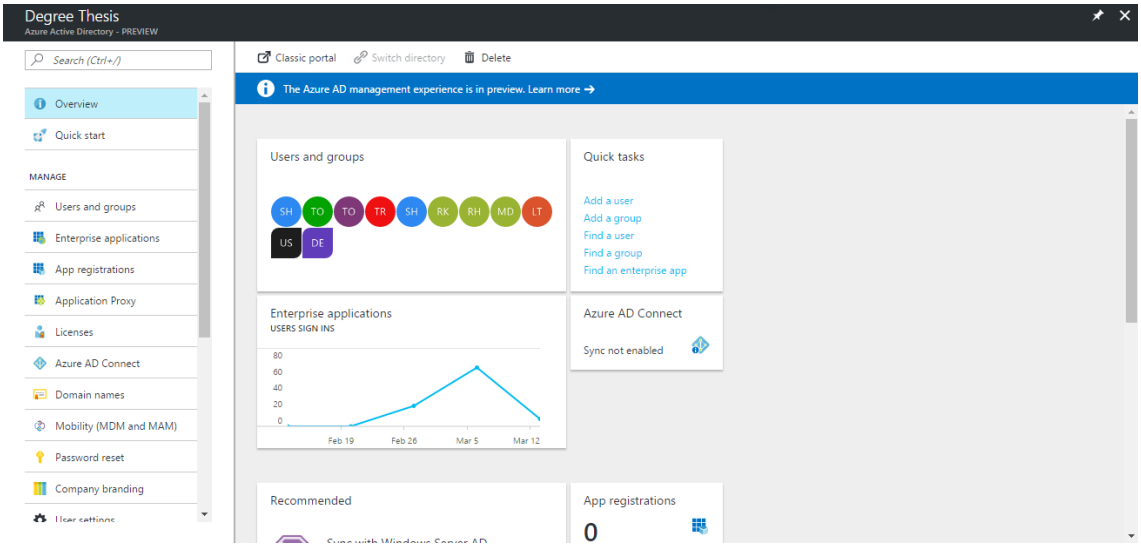


Figur 3. Skapandet av EMS-konto

3.3 Konfiguration av Azure Ad

I detta skede kommer det att föras in användare i Azure Ad för att i nästa steg kunna konfigurera användaren i Intune. Då allt görs direkt i molnet kommer inte en kopiering av användare att göras mellan traditionella AD och Azure Ad.

Då EMS samt Azure är aktiverat är nästa steg att lägga till användare i Azure Ad för användarkontroll. På grund av att företaget ännu inte har haft ett system för användar-kontroll kommer ingen kopiering mellan AD och Azure Ad att göras i detta skede. I figuren nedan visas Azure Ad vyn. Figuren är tagen från Azures nya portal som har tagits i bruk. Den gamla fungerar dock ännu, men i detta arbete kommer det att arbetas med den nya portalen så långt som möjligt.



Figur 4. Azure portalen och Azure Ad huvudvy

3.4 Skapandet av användarkonton i Azure Ad

Införandet av nya användare i Azure Ad sker manuellt då det är fråga om nya användare inom företaget. Såsom tidigare nämnts går det att kopiera från eller synkronisera användare med standard AD, vilket gör att det går att föra in flera användare samtidigt. Att föra in flera användare samtidigt lyckas även när det är fråga om användare från ett partnerföretag med ett eget Azure Ad, men dessa får inte samma privilegier som anställda inom företaget, eftersom de markeras som gästanvändare, Guest User (Love 2017a).

I detta skede stöttes genast på ett problem. Det planerades nämligen att föra in företagets användare via en CSV-fil men detta tycks lyckas bara för partneranvändare, vilket betyder att de borde läggas in manuellt en i taget. Detta vore inte ett problem om företaget skulle ha haft en lokal domänkontroller med Active Directory. Då hade man kunnat aktivera synkronisering mellan Azure Ad och AD. Efter en del undersökande hittades dock en omväg för att lösa problemet med att föra in en användare i taget. Detta sker dock inte via Azure Ad utan via portalen O365 Admin där det finns möjlighet att lägga till flera användare samtidigt via en CSV-fil.

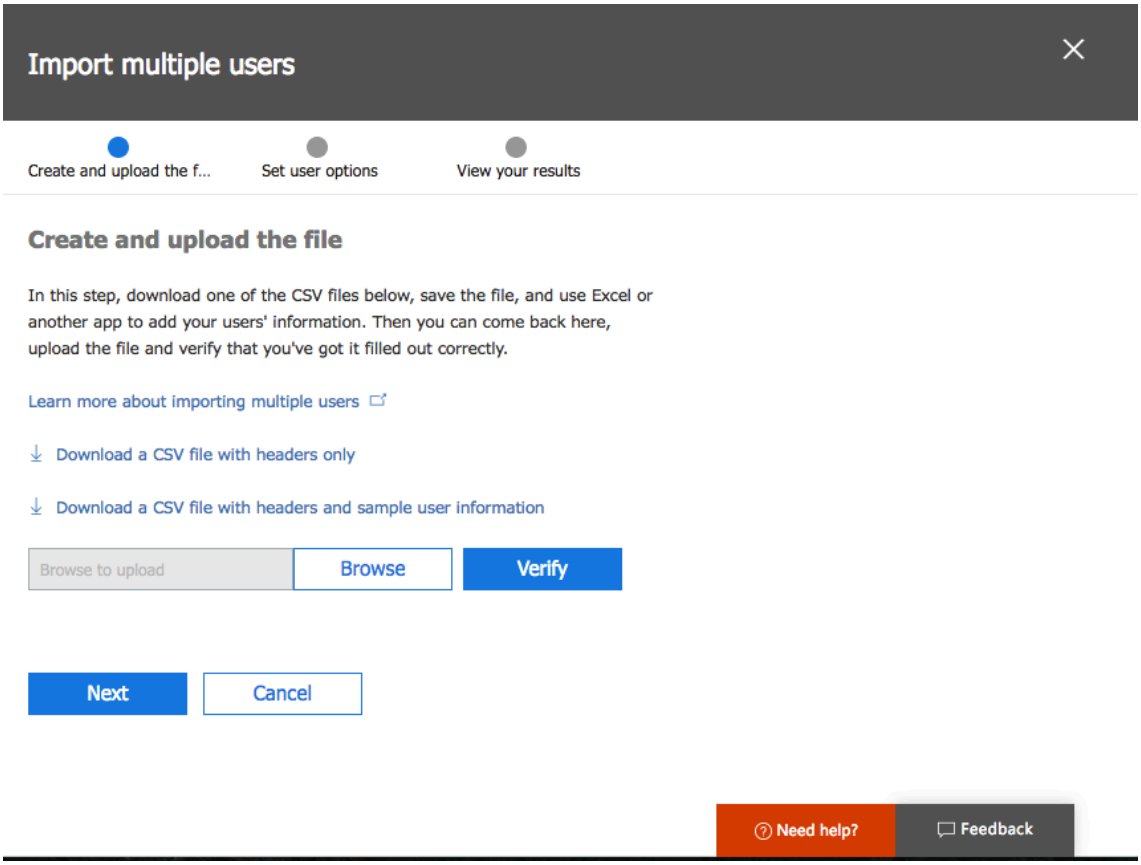
En annan fördel med att föra in användarna på detta sätt är att man i detta skede även kan lägga till en licens för EMS och O365 åt användarna i stället för att lägga till dessa separat en och en (Se figur 7.)

De värden som måste finnas i CSV-filen är inloggningsnamn och visningsnamn. Om information saknas för någon kolumn kan detta markeras tomt med ett mellanslag. CSV-filen skall vara kommaavgränsade och innehålla följande kolumner på engelska:

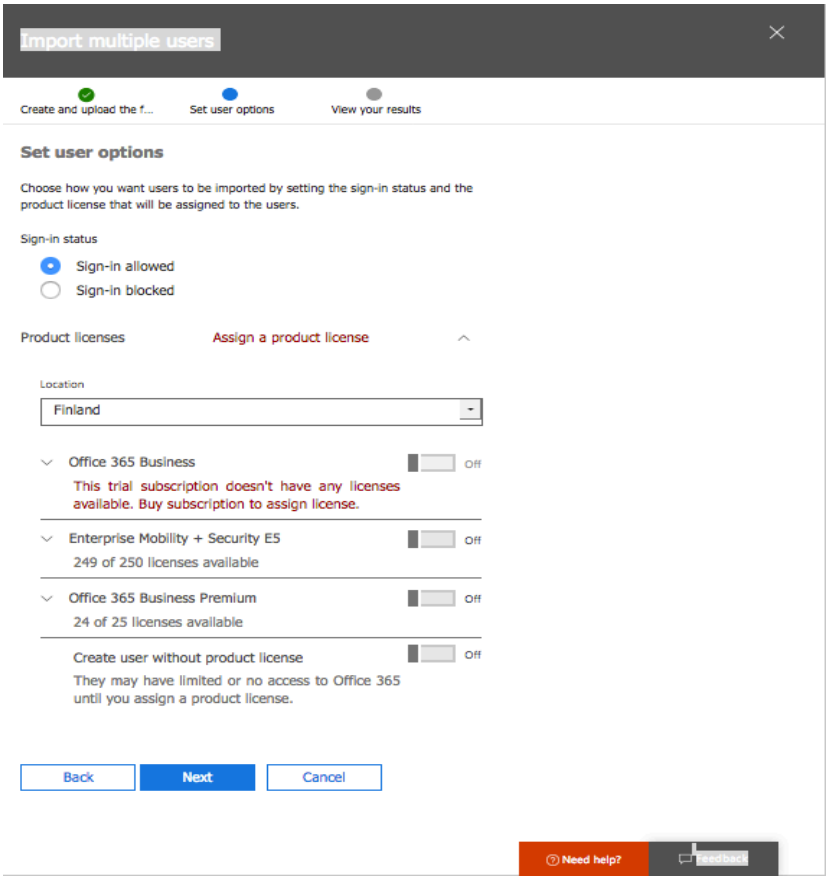
- User Name,
- First Name,
- Last Name,
- Display Name,
- Job Title,
- Department,
- Office Number,
- Office Phone,
- Mobile Phone,
- Fax,
- Address,
- City, State or Province,
- ZIP or Postal Code,
- Country or Region.

För detta arbete aktiverades även en utvärderingsversion av Office 365 som innehåller licens för 25 användare. På basis av detta förs som pilot i första skedet in bara 20 nya användare. Figur 7 och figur 8 presenterar uppladdningen samt beviljandet av licens till de nya användarna.

Efter att de nya användarna förts in via O365-portalen granskades att de också synkroniserades med Azure Ad, vilket bevisar att detta är en fungerande arbetsmetod för införande av flera nya användare samtidigt.

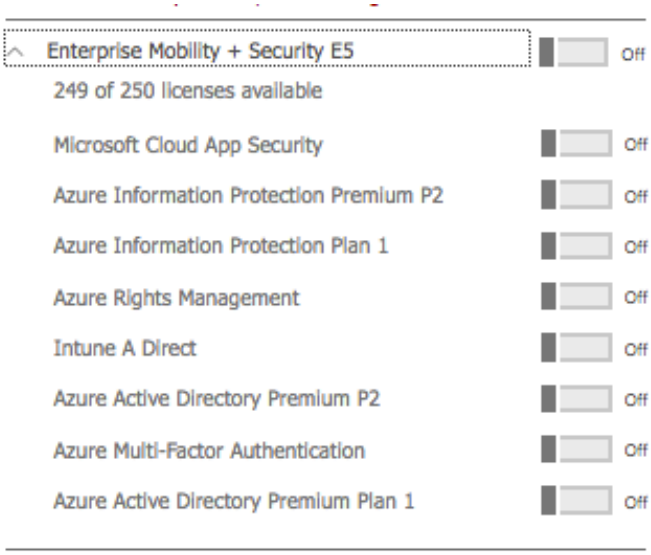


Figur 5. Import av flera användare via O365 admin portalen

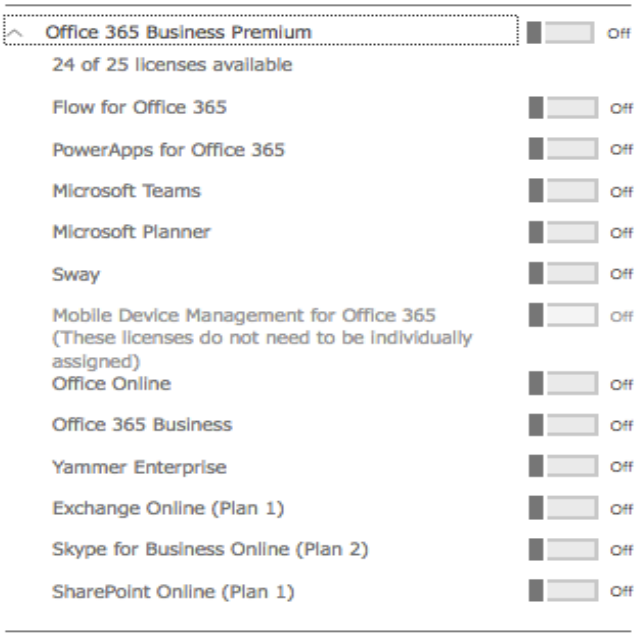


Figur 6. Licensval för nya användare(O365 admin portalen)

I detta skede skulle man även kunna välja bara en del av licenserna. Om det exempelvis finns användare som bara använder Office Online så kan man slopa deras rättigheter att ladda ner hela Office-paketet till sina datorer. Figur 7 och 8 visar vilka licenseringsmöjligheter det finns för användarna när det gäller EMS- och O365-licenser. (Microsoft 2017a)



Figur 7. Licensval för nya användare gällande EMS licenser(O365 admin portal)



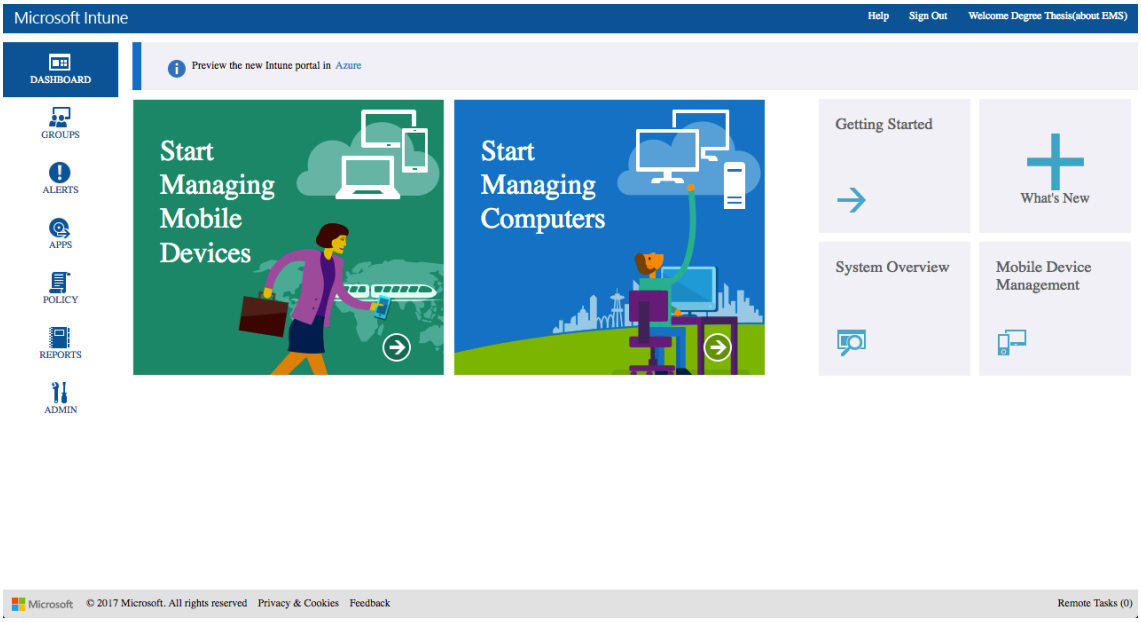
Figur 8. Licensval för nya användare gällande O365 licenser(O365 admin portal)

3.5 Konfiguration av Intune

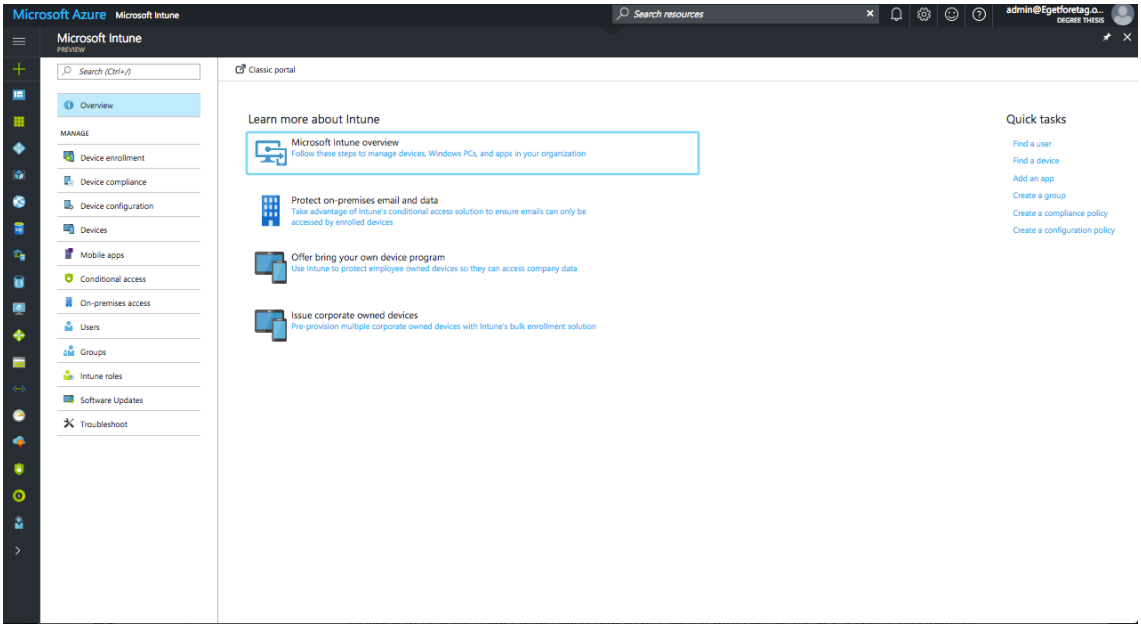
Intune administreras från Intune Admin Portalen (se länkar), eller delvis redan från Azure Intune Preview som fungerar som inbyggd portal i Azure. Figur 9 visar Intune Classic Portal (gamla administreringsportalen). För att kunna börja använda Intune krävs för detta arbete inte något annat än att man väljer Intune som aktiv mobilhanteringsplattform. Ifall användarna inte ännu fått licenser för Intune åtgärdas detta som nästa steg via O365-portalen. Föregående steg har redan tagits i samband med införan-

det av användare. Det krävs dock konfigurering när det gäller hantering av mobila enheter och dessa delar tas upp i kommande kapitel. Intune kommer i framtiden att helt och hållet administreras via Azure-portalen (Figur 10). För tillfället finns inte alla funktioner insatta i den nya portalen, men den kommer att användas i detta arbete för en del av konfigureringarna.

Ifall ett företag har lokal infrastruktur gäller det att beakta följande: för att kunna påbörja hanteringen av företagets enheter som finns i kontorets nätverk (med lokal server) gäller det att konfigurera nätverket för att kunna kommunicera med Intune-klienten. Ifall enheten ligger bakom en proxy server måste servern stöda både http och https på grund av att Intune använder båda protokollen. Proxyändringar kan göras direkt från proxyservern eller styras med hjälp av grupprinciper. (Barnett 2017e)



Figur 9. Intune Classic Portal



Figur 10. Intune Preview inbyggd i Azure-portalen.

3.6 Aktivering av operativsystem i Intune

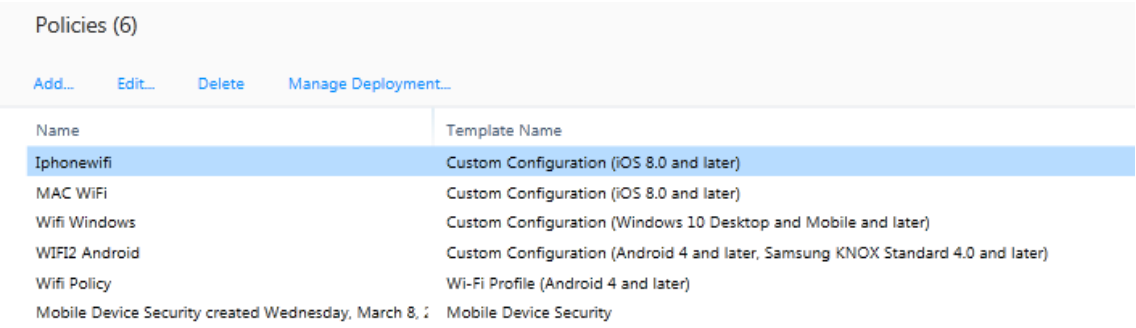
Operativsystemen i detta kapitel aktiveras via Intunes gamla portal.
Aktiveringen av både Windows och Android kräver inte ytterligare konfiguration i Intune för införande av enheter. Det enda som måste göras är att markera dem som aktiva för registrering. (Barnett 2016b& Barnett 2016d)

För att kunna börja hantera Ios-enheter i Intune måste man först ladda ner Apples APN (Apple Push Notification) certifikat och föra in det i systemet. Första steget var att ladda ner en CSR-fil (Certificate Signing Request) som behövs för att kunna ladda ner Apples APN-certifikat. CSR-filen fungerar som en digitalt signerad fil för att få förtroendecertifikatet nerladdat från Apple. CSR-filen laddades ner från Intune och sparades lokalt på en dator. Därefter gjordes en inloggning på Apples Push Certificates portal med företagets Apple konto och där laddades CSR-filen upp, varefter man kunde ladda ner APN-certifikatet. APN-certifikatet måste sedan laddas upp till Intune, vilket kräver att man ännu en gång ger Apple Id för APN-certifikatet (.pem fil). Efter att certifikatet var uppladdat till Intune markerades IoS samt MAC OS X som aktiva operativsystem.
(Barnett. 2016c)

3.7 Intune - principer

Före införandet av enheter valdes som nästa steg att konfigurera olika principer för att skydda företagets data då en enhet registreras.

I Intune kan man använda olika typer av principer för att hantera säkerheten och användbarheten hos mobila enheter. Principerna kan skapas på basis av färdiga mallar eller modifierade versioner av dessa. (Diogenes & Gilbert 2015 s.136 -144). Vid principhanteringen kom det fram ett problem gällande Intune portalens kompabilitet. Tidigare gick det nämligen att använda portalen via en Macbook pro och via Firefox browser (fungerar inte I Chrome). Då det via Intune-portalen skapas en ny profil så öppnas ett nytt fönster där det inte går att välja något och allt är grått. Alla säkerhetsinställningar i Firefox granskades och det säkerställdes att ingenting blockerar pop-up eller liknande. Det testades äldre versioner av Firefox, men det fungerade inte där heller. Detta är ett stort minus på grund av att Microsoft gör reklam för att portalen skall kunna användas i molnet nästan varifrån som helst, men det enda sättet att få detta att fungera var att använda en Windows-dator med Internet Explorer. Detta problem kommer förhoppningsvis att försvinna, eftersom Intune implementeras och har redan delvis implementerats i Azure-portalen. Figur 11 visar de principer som skapats och följande kapitel går igenom själva skapandet av dessa principer.



Figur 11. Lista på skapade principer (Intune Classic portal)

3.7.1 Allmänna villkor

Före skapandet av egentliga principer så skapades allmänna villkor. I Intune kan man skapa villkor för användare där administreringen kan ge en egen förklaring på vad det innebär för användaren att ta i bruk Intune och hur det inverkar på enheten. Som test skapades ett nytt villkor i Intune-portalen som fick benämningen: Terms and Conditions. Det krävdes bara några få steg att skapa detta villkor. Samtidigt valdes de användare som kommer att beröras. På grund av att villkoren kommer att vara desamma för alla användare distribuerades villkoret till alla användare. (Diogenes & Gilbert 2015 s.136)

3.7.2 Konfigurationsprinciper

Konfigurationsprinciper används för att konfigurera enhetens generella inställningar vid registrering. Via denna princip kan man exempelvis ställa krav på pinkod vid upplåsning av telefonen. I detta skede användes en färdig mall som täcker de flesta inställningar för att säkerställa enheten. (Diogenes & Gilbert 2015 s.138-139). Figur 12 visar en överblick över regler som kan väljas vid skapandet av konfigurationsprinciper. Dessa kan dock ändras efter hand.

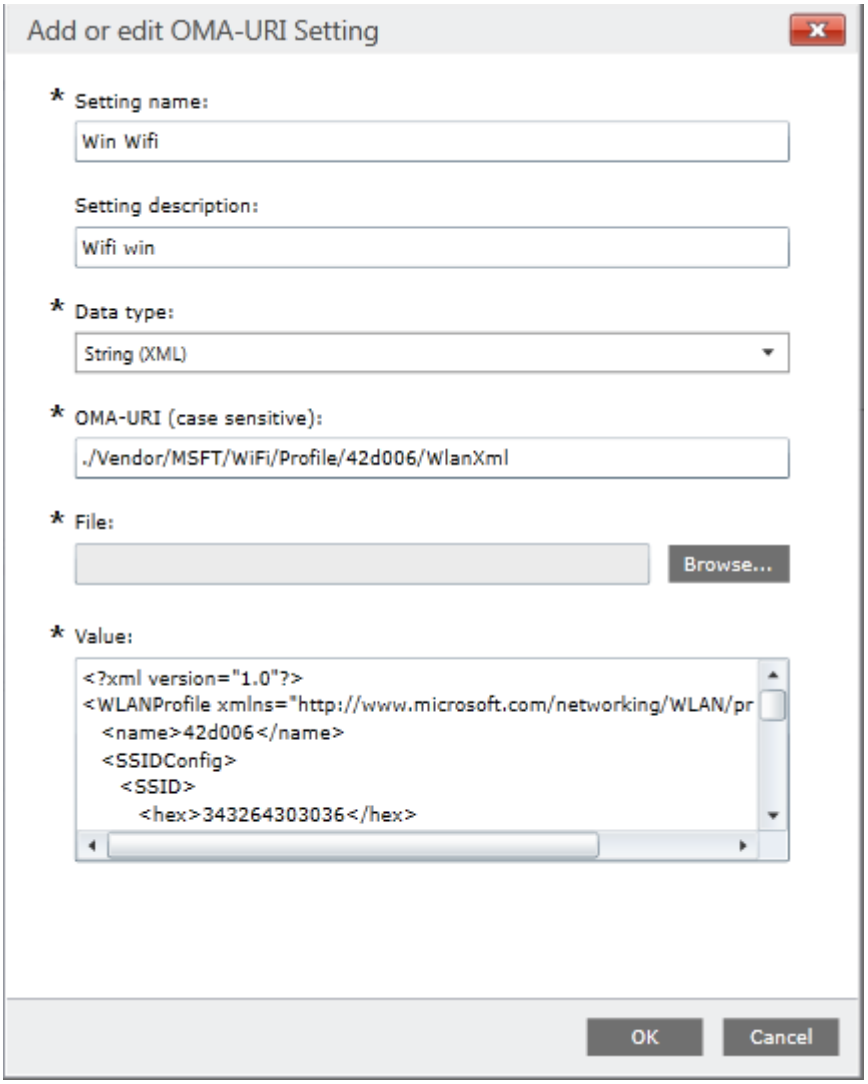
Figur 12. Inställningar för konfigurationsprinciper (Intune Classic Admin Portal)

3.7.3 Resursprincip för Android och Windows

Resursprinciper eller profiler används för att kunna ge åtkomst åt användaren från hans eller hennes enhet till kontorets trådlösa nätverk eller andra lokala resurser. (Stack 2016a).

För konfiguration av denna profil används ett hemmanätverk som fungerar som företagets trådlösa nätverk. Första steget för att skapa en profil som konfigurerar åtkomsten till det trådlösa nätverket är att exportera en XML-fil som innehåller WiFi-profilens information. Denna fil exporteras från en Windows 10 pc som redan är uppkopplad till nätverket i fråga. Som exportmetod valdes att exportera profilen via kommandotolken (CMD.exe). Kommandot som användes för att skapa XML-profilen:
”netsh wlan export profile "42d006" key=clear interface="Wi-Fi" folder="%UserProfile%\Desktop".
Kommandot skapar en XML-fil som innehåller den information som behövs för att skapa en resursprofil för WiFi-nätverk. Denna XML-fil kan användas för att skapa WiFi-profil för Windows och Android, för Ios/Mac OS X-konfiguration se nästa kapitel. (Brink 2017).

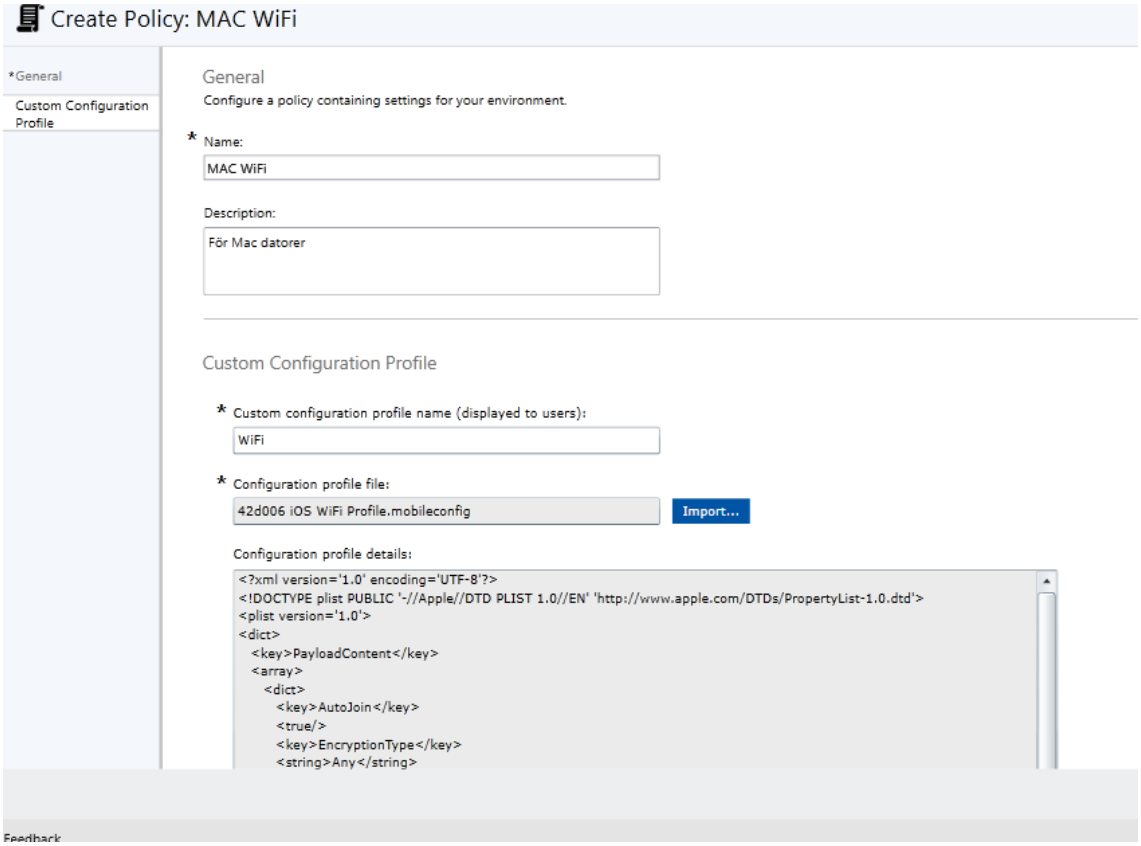
Profilen för både Android och Windows skapades på samma sätt genom att skapa en ny blank profil eller princip. Figur 13 visar konfigurationen av WiFi-profilen för Windows. Här gavs namnet och tilläggsuppgifter för profilen och lades till en **OMA-URI** (Open Mobile Alliance Uniform Resource Identifier) inställning och som typ av data valdes String(XML). Skillnaden mellan Android- och Windows-konfigurationen ligger i OMA-URI för Android:
”./Vendor/MSFT/WiFi/Profile/42d006/Settings”.
För Windows är denna inställning:
“./Vendor/MSFT/WiFi/Profile/42d006/WlanXML”. (Stack 2016b).



Figur 13. Skapande av WiFi-profil för Windows (Intune Admin Portal)

3.7.4 Resurs/Wifi-profil för iOS/MAC OS X

För att skapa en WiFi-princip för iOS måste man skapa en ”Mobileconfig” fil som liknar XML-filen som skapades för Android/Windows. För skapandet kan man använda Apple Configurator som kan laddas ner från App Store och verktyget testades men det fungerade inte som önskat och krävde att man har en iOS-enhet uppkopplad till datorn. Istället valdes att använda en generator tillgänglig via webbplatsen Intune iOS Psk Mobile Config generator (se länkar). Efter skapandet av filen var följande steg att ladda upp den till Intune för att fortsätta konfigurationen. (Stack 2016b). Figur 14 visar konfigurationen av principen för iOS och MAC OS X.

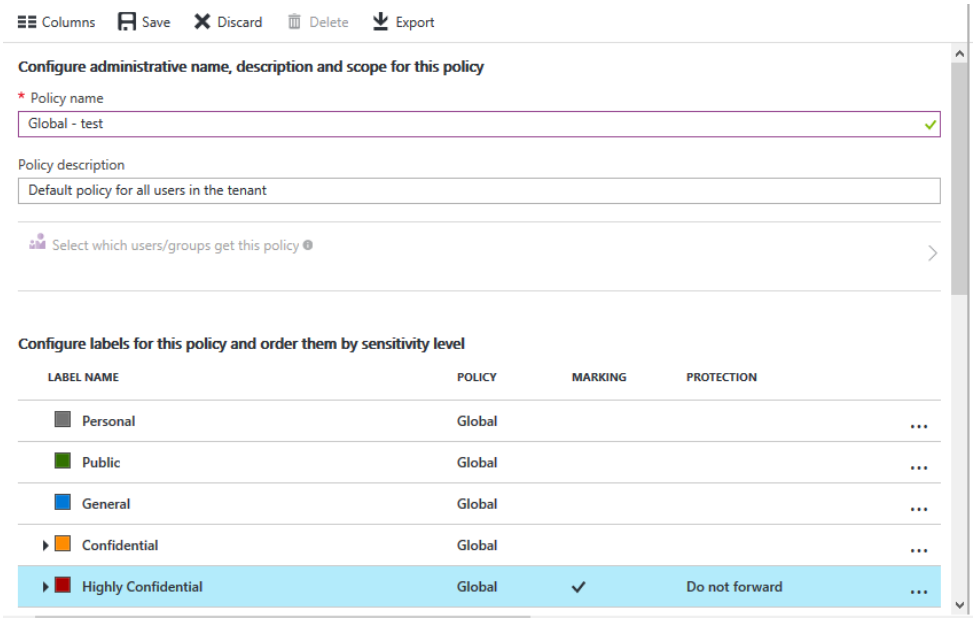


Figur 14. Skapande av WiFi-profil för MAC OS X/iOS (Intune Admin Portal)

3.8 Aktivering av tjänsten Azure Information Protection

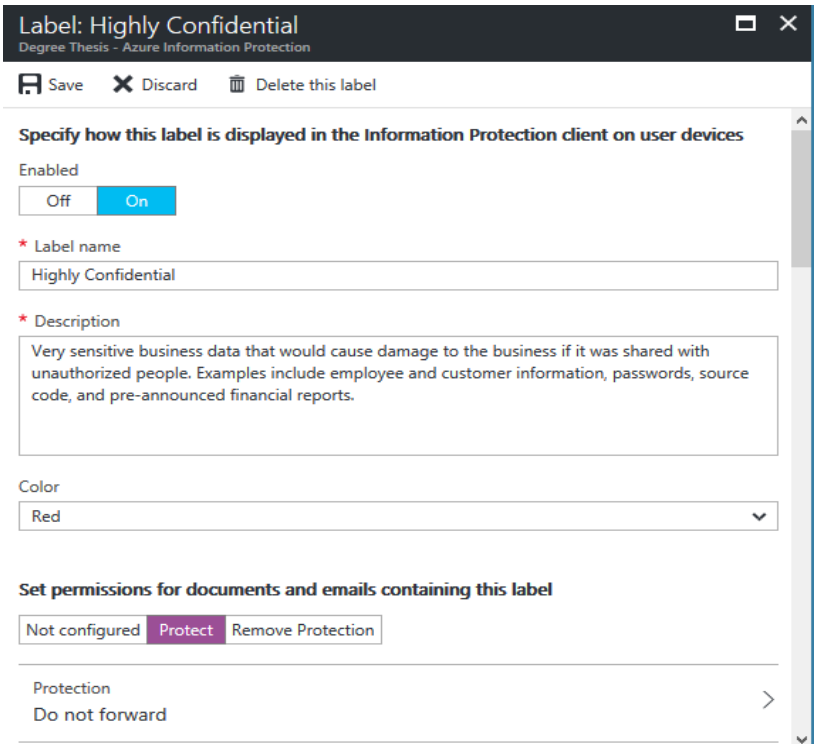
Aktiveringen av tjänsten Azure Information Protection är ganska enkel. Det enda som krävdes för att aktivera tjänsten var att trycka på ”Activate” via kontohanteringssidan för Azure Information Protection.

Nästa steg för att få nytta av tjänsten var att skapa nya regler eller markeringar för dokument och figur 15 visar vilka markeringar som kan appliceras för dokument. (Bailey & Baldwin 2017)

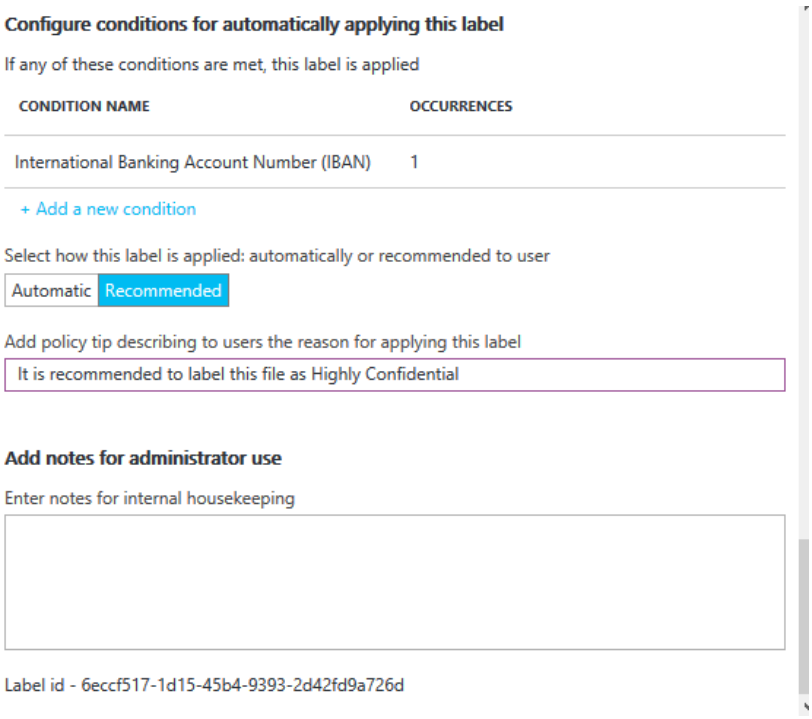


Figur 15. Markeringar som kan appliceras för dokument (Azure information Protection konsol)

Som test gjordes en konfidentiell klass och dokument som klassificeras som konfidentiella får en vattenstämpel. För de konfidentiella dokumenten valdes att de inte kan vidarebefordras via e-post (Figur 16). Denna regel skapades så att den automatiskt appliceras om ett dokument innehåller kontonummer i IBAN-format (figur 17).



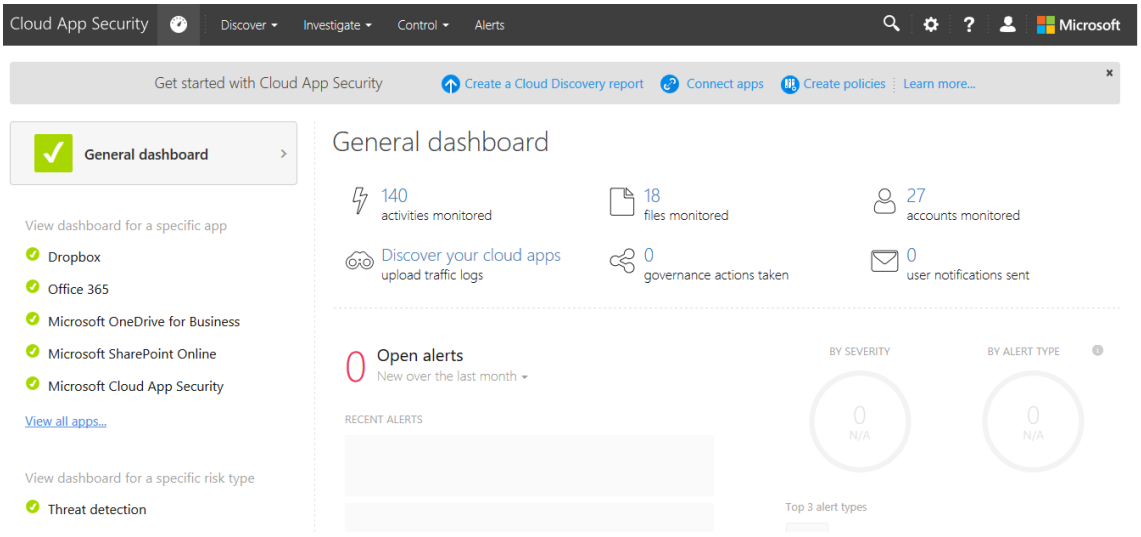
Figur 16. Skapande av ny regel för skydd av dokument(Azure Information Protection portal)



Figur 17. Regel för automatisk användning av stämpel (Azure Information Protection portal)

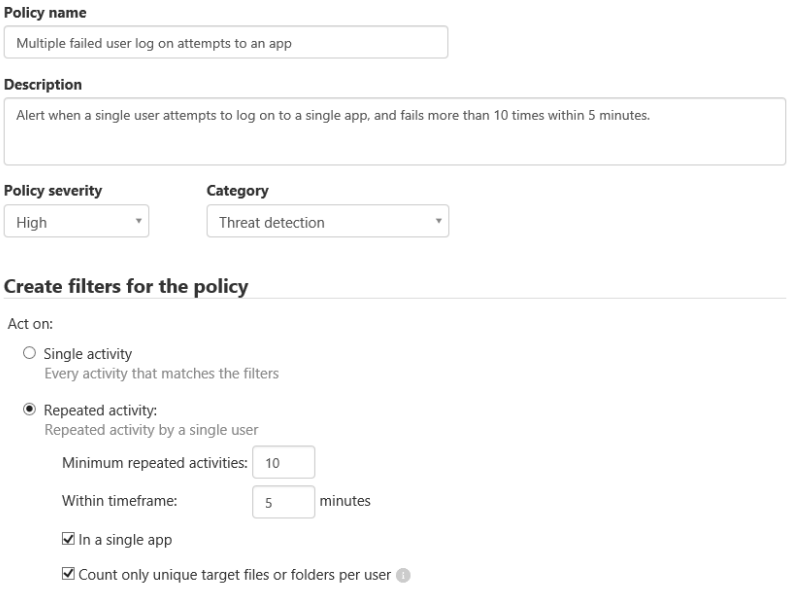
3.9 Cloud App Security-konfiguration

Cloud App Security har redan färdigt inbyggda konfigurationer som innehåller vissa färdiga regler utan extra konfigurering gällande Office familjens program. Som exempel kan nämnas att alla filer som ligger på OneDrive skannas och aktiviteten följs redan automatiskt. Figur 18 nedan visar huvudvyn för Cloud App Security och att aktiviteter redan övervakats utan att det gjorts några konfigurationer. För större helheter med flera användare lönar det sig att skapa automatiska rapporter för att inte behöva gå igenom händelser en för en. (Lloyd 2016).



Figur 18. Huvudvy för Cloud app-portalen

Som test skapades en aktivitetsprincip som meddelar administrationen om någon försökt logga in till någon applikation med fel lösen flera gånger (figur 19).



Figur 19. Skapande av en aktivitetsprincip (Cloud App Security Portal)

4 FÖRBEREDNING OCH PUBLICERING AV APPLIKATION

Det första programmet som valdes för publicering är MS Office-programmet Word. Publicerandet och det förberedande arbetet kommer att göras via Azure portalen. Till skillnad från gamla Intune-portalen så krävs det inte att man manuellt hämtar länken för programmet från plattformens appbutik (detta gäller bland annat MS Office 365-applikationer). Det finns nämligen redan en hel del färdiga applikationer införda i Intune. Detta kom som en överraskning på grund av att ingen uppdatering har gjorts i Microsofts dokumentation som gäller nya funktioner för den nya Intune-portalen inom Azure. Det enda som krävdes för att aktivera programmet var att välja de grupper som man vill distribuera applikationen till och den metod som skall användas för publikation, det vill säga om det är ett program som måste installeras eller om det bara finns tillgängligt. Programaktiveringen måste dock göras separat för varje operativsystem.

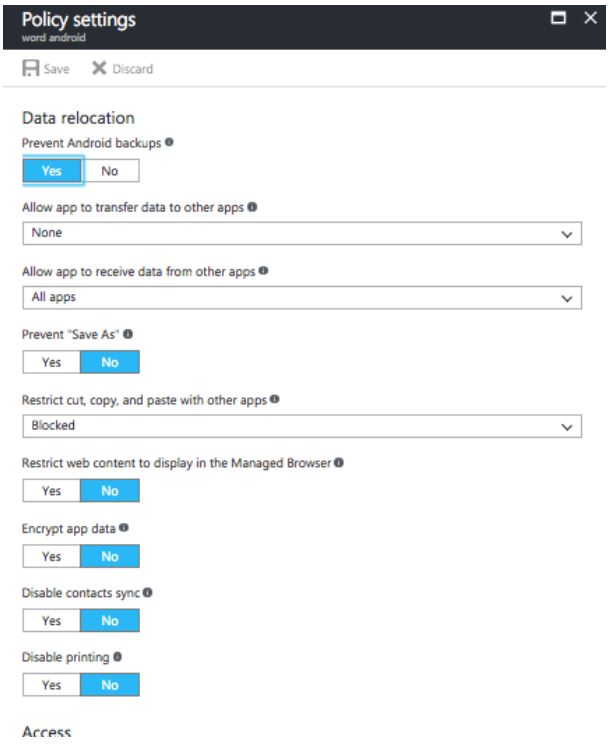
Ifall programmet inte färdigt finns på listan måste applikationen föras in i Intune (Azure Portal) enligt den gamla metoden som används i Intune och detta medför en del ytterligare konfigurationer. För att lägga till applikationen krävs det att man med en länk till plattformens appbutik visar varifrån applikationen kan laddas ner samt företagsspecifik information läggas till för appen. Själva ändringar i appens kod krävs inte. (Della Monica 2016b).

4.1 Skydd av app med App Protection

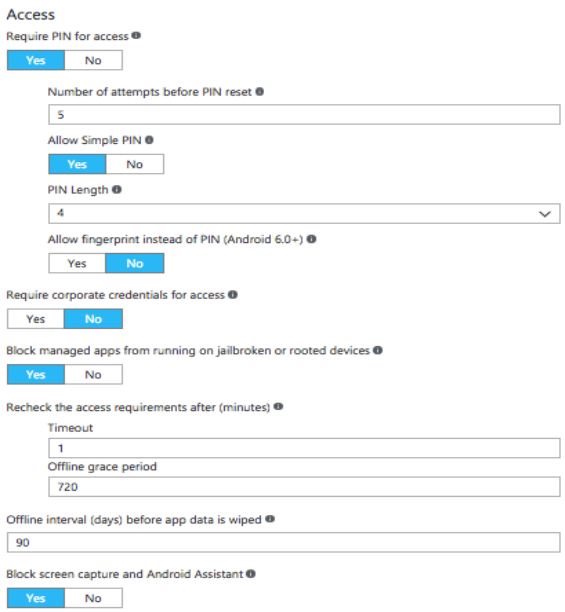
Detta kapitel beskriver vad som gjorts för att skydda programmet MS Word. Reglerna skapades via Azures inbyggda Intune-portal. För att se om dessa regler fungerar som avsett kommer brott mot dessa regler att testas i ett senare skede (se Test av App Protection).

De viktigaste regler som konfigurerades för att skydda programmet var att förhindra möjligheten att kopiera text från appen till utomstående appar. En annan viktig regel konfigurerades gällande åtkomst till programmet. För att kunna komma in i programmet krävs det en pinkod och det maximala antalet fel inloggningsförsök begränsades till fem gånger, varefter användaren måste nollställa sin pinkod. För nollställning av pinkoden

krävs det att användaren loggar in med företagets konto samt lösenord. För fullständig konfiguration av principen för skydd av Word-appen, se figur 20 och figur 21. (Tillman 2016c).



Figur 20.. Skapande av en säkerhetsprincip för Word del 1 (Azure portalens Intune preview)



Figur 21. Skapande av en säkerhetsprincip för Word del 2(Azure portalens Intune preview)

5 TESTER OCH VALIDERING AV SYSTEMET

I detta kapitel testas användbarheten av de viktigaste delarna av ett färdigt EMS-system för företaget. I testerna kommer det att användas en del test från Microsofts valideringsmall för ett färdigt system samt några egna tester gällande säkerhetsregler och införande av enhet. En del tester görs enligt Microsofts valideringstester och en del av testerna har valts för att testa andra viktiga funktioner. (Tillman 2016b)

5.1 Test av enhetsregistrering

Som redan nämnts i planeringen så kommer användarna själva att aktivera sin enhet för Intune enligt givna instruktioner från administrationen. I detta arbete används inte utomstående personer för registrering av enhet på grund av att det mest väsentliga är att själva registreringen lyckas både på enheten samt att den indikeras som registrerad i Intune.

Testerna för enhetsregistrering kommer att göras för både Android- och iOS-operativsystemen. För att detta test skall kunna anses vara lyckat måste enheterna synas som registrerade både på enheten och i Intune Admin-konsolen. En annan aspekt som måste beaktas vid registrering är att enheterna skall få åtkomst till det konfigurerade nätverket. Detta innebär alltså att resursprofilen som skapats tidigare har konfigurerats och distribuerats på rätt sätt.

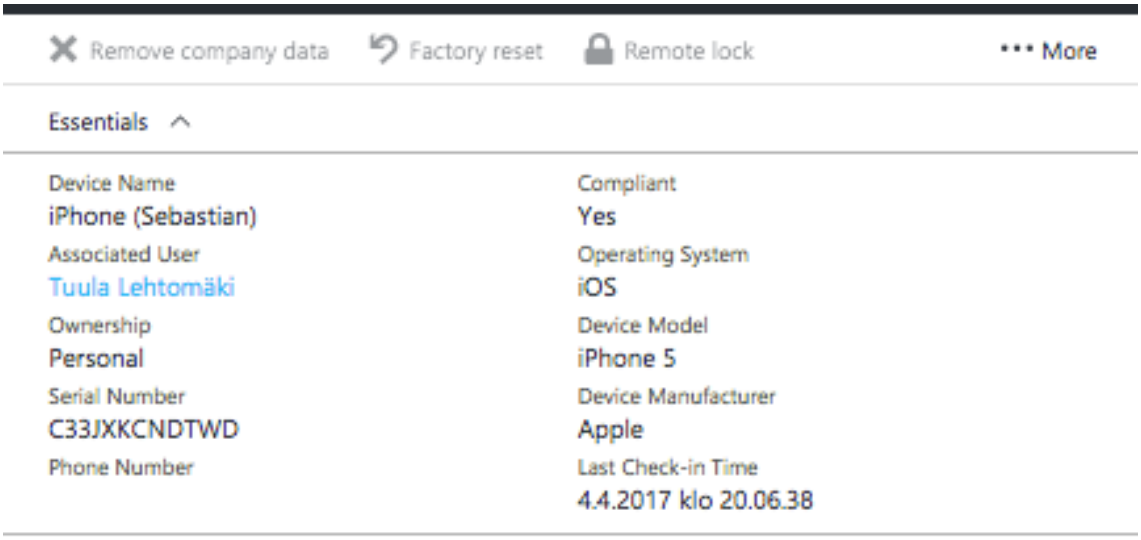
I detta skede kontrolleras också att konfigurationsprinciperna appliceras på enheten och för detta syfte registreras båda enheterna utan pinkod. Då borde Company portal kräva att användaren anger en pinkod som uppfyller kraven. Själva registreringen skiljer sig inte mellan enheterna men båda bör testas på grund av att de aktiverats i Intune på olika sätt.

Efter testregistreringen av enheter skulle följande skede vara att införa systemet stegvis i hela företaget. Då skulle användarna instrueras att på sin enhet gå till antingen Apples AppStore eller Google play store beroende på vilken enhet de använder och därifrån

ladda ner Intune Company portal. Efter nedladdning bör de logga in med sitt företagskonto och följa de instruktioner som Company portal ger för registrering. De kommer även att få en länk för mera instruktioner. För användarna finns det dokumentation och information om Intune för slutanvändare så att de kan läsa vad det innebär att ta i bruk Intune på sina enheter samt hur detta går till. (Barnett 2016b & Barnett 2016c).

5.1.1 Test av IOS-registrering

Som redan beskrivits i föregående kapitel är det första steget för registrering att ladda ner Intune Company portal (företagsportal) från Apples AppStore. Efter nedladdningen gäller det att logga in med företagets konto och följa givna instruktioner. Från en användares synvinkel borde detta skede inte ställa till problem för det krävs bara att man loggar in och godkänner villkoren. Som test gjordes inloggningen samt registreringen på en Apple Iphone med ett vanligt användarkonto. Registreringen krävde att ange en ny pin kod för enheten vilket betyder att konfigurationsprincipen applicerats. Efter att registreringsprocessen var klar anslöt sig enheten direkt till det konfigurerade nätverket vilket indikerar att WiFi-profilen också applicerats korrekt. Registreringen granskades i Intune och som figur 22 visar har registreringen lyckats. (Tillman 2016b).

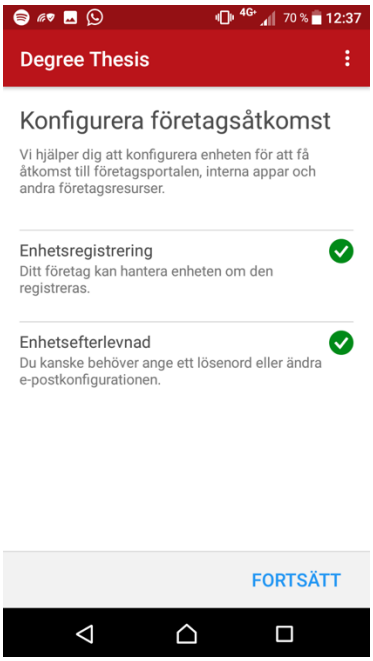


Figur 22. iOS-enheten visas som registrerad i Intune (Azure portalens Intune preview)

5.1.2 Test av Android-registrering

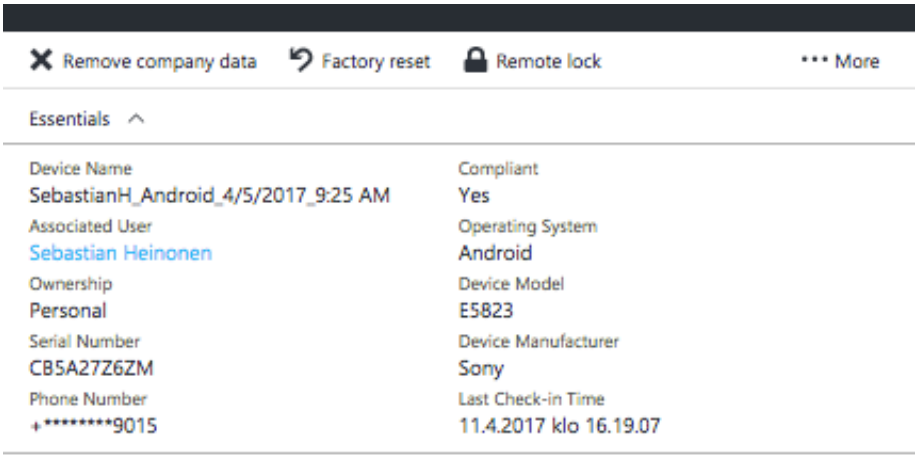
Som redan tidigare nämnts så skiljer sig inte registreringen av Android enheten från iOS-plattformen, på grund av detta tas inte stegen för registreringen av enheten upp på nytt i detta kapitel. För detta test används en enhet med Android 7.0 Nougat.

Vid registreringsskedet krävde företagsportalen att en fyrsiffrig pin kod angavs, vilket här också betyder att konfigurationsprincipen applicerats korrekt på enheten. Till skillnad från iOS-enheten så anslöt sig enheten inte till det konfigurerade trådlösa nätverket genast. Detta problem undersöktes och det kunde bero på att det hade konfigurerats två separata WiFi-profiler som troligtvis var i konflikt med varandra. Efter att den andra WiFi-profilen togs ur bruk via Intune och principerna på enheten synkroniserades manuellt kunde enheten ansluta till det trådlösa nätverket. Figur 23 visar en lyckad registrering av enheten.



Figur 23. Lyckad registrering av Android enhet (Intune Company Portal)

Nästa skede var att för Android-enheten granska att den syns som registrerad enhet i Intune-portalen. Som figur 24 visar har enheten registrerats i Intune utan konflikter. (Tillman 2016b).

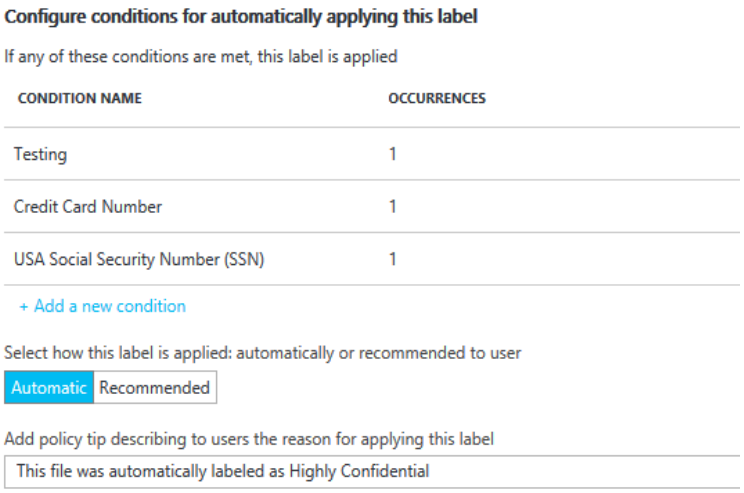


Figur 24. Android enheten syns som registrerad i Intune (Azure portalens Intune preview)

5.2 Tester av säkerhetsregler (Information Protection)

Konfigureringen av en säkerhetsregel gjordes så att dokument innehållande IBAN, kontonummer, personbeteckning skall markeras automatiskt som konfidentiella (figur 25). Detta har inte fungerat på dokument som skapats med matchande triggers. I dessa dokument användes Microsofts angivna teckenserier. (Bailey 2017b).

För att en automatisk stämpel skall appliceras måste dokumentet vara skapat på en Windows-dator som har Azure Information Protection-klienten nedladdad. (Bailey 2017a). Den automatiska appliceringen av säkerhetsregler fungerade inte som avsett, vilket inte var ett önskat resultat. Det granskades att regeln distribuerats och konfigurerats rätt utan några varningar. Reglerna kan appliceras manuellt via Information Protection plug-in in, men detta gav inte heller önskat resultat. (Bailey 2017b).

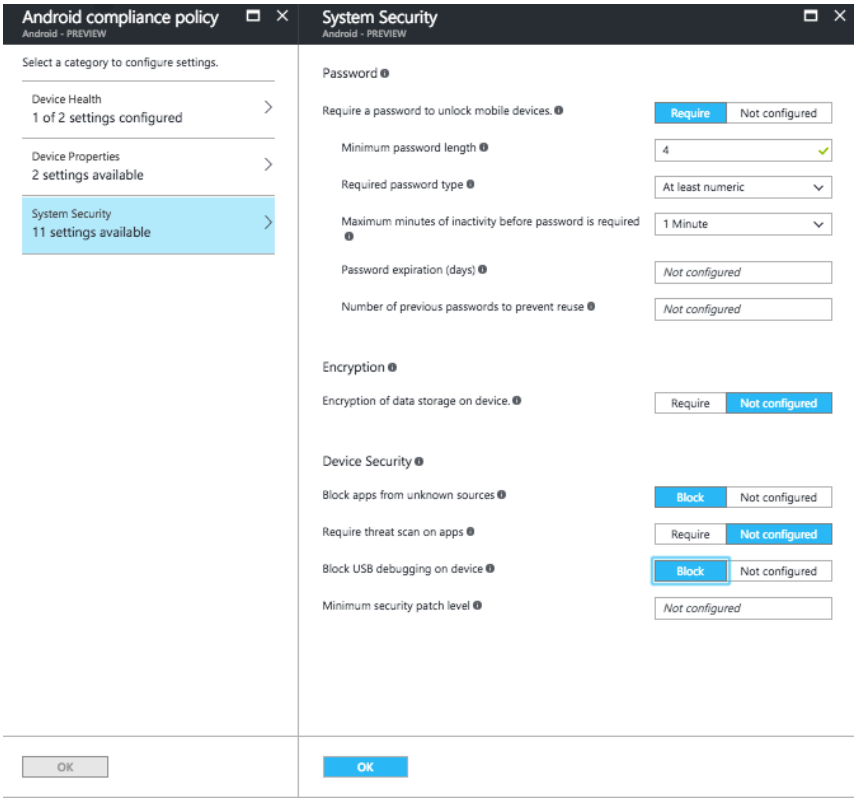


Figur 25. Skapande av en säkerhetsprincip (Information Protection)

5.3 Test av villkorlig åtkomst

Här testas att regler för åtkomst till företagets e-post inte lyckas utan att en enhet anses vara kompatibel eller motsvara angivna regler för en enhets kompabilitet. På figuren nedan visas vilka säkerhetsregler som måste uppfyllas för att en enhet skall anses vara kompatibel för att komma åt företagets e-post. Detta test görs för att se att t.ex. en person inte kan använda vilken som helst enhet för att komma in via O365-portalen till sin e-post. För att komma åt exempelvis O365 Exchange Online så måste enheten uppfylla efterlevnadsprinciper enligt figur 26.

För att skydda O365 Exchange Online-tjänster skapades även en princip för villkorlig åtkomst. Denna regel valdes att gälla alla enheter och användare. Ifall villkoren för åtkomst inte uppfylls ges användarna anvisningar om vad de måste göra för att få åtkomst. (Caserio 2017).



Figur 26. Efterlevnadsprincip (Azure Intune prieview)

För detta test avregistrerades en Android-enhet för att användas som en utomstående enhet. Via Android-telefonen gjordes försök att komma åt e-posten via O365-portalen (se länkar). Inloggning på sidan lyckas men åtkomst till e-posten är blockerad (se figur 27), vilket betyder att regeln eller villkoret för åtkomst fungerar som planerat och som konfigurerat. För åtkomst till e-posten ombeds användaren i detta skede att registrera sin enhet i Intune och ges en länk för installation av Intune Company Portal. Efter detta registrerades enheten på normalt sätt i Intune (se införande av enhet i kapitel 5.1.2) Ett nytt test gjordes efter att enheten registrerats i Intune, då lyckades åtkomsten till Outlook via O365-portalen.

Resultatet för detta test kan anses vara lyckat eftersom alla konfigurerade regler fungerade som planerat.

Figur 27. Försök att läsa e-post via O365-portalen (Android)

5.4 Test av App Protection

Här testas om App Protection-reglerna fungerar som de skall. För detta test gjordes en regel som skall förhindra kopiering från Word till andra program på enheten, detta innebär att ”copy-paste” (klippa och klistra) metoden är inaktiverad (gällande Word-applikationen). Detta test görs både på en Intune-registrerad Apple Iphone med iOS operativsystem och en Android mobiltelefon.

Första testet gjordes på iOS-plattformen. Som test öppnades ett tidigare dokument via Word-applikationen och en del av texten valdes och kopierades (ingen varning i detta skede). Nästa steg var att klistra in den kopierade texten i Apples eget program Notes. Därefter valdes en tom fil och egenskapen ”klistra in” men ingen text infogades (dock ingen varningstext här heller). (Tillman 2016b).

Resultatet av detta test var önskat, d.v.s. ingen text kan kopieras från Word.

Samma test gjordes på en Android-mobiltelefon med samma dokument. Vid kopieringen av texten gav inte systemet någon varning här heller. Vid försöket att klistra in texten i ett utomstående program (här Evernote) gav systemet en text som anmälde att: ”Du kan inte klistra in organisationens data här” se figur 28.

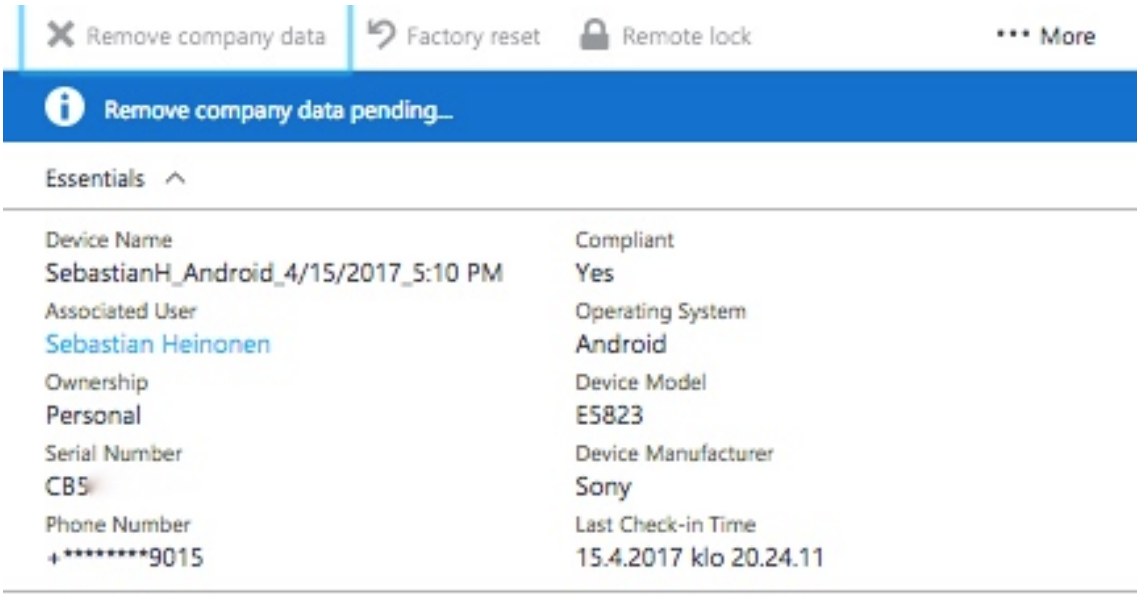
Figur 28. Test av kopiering av text från Word till en utomstående app (Android plattform)

5.5 Test av administrationsmöjligheter

För dessa test används både egna test samt test enligt Microsofts valideringsmall.
Det första testet som skulle göras enligt Microsoft valideringsmall var att söka fram en användare och den enhet som användaren registrerat. Detta lyckas utan problem. Syftet med nästa test var att testa nollställning av pinkod. Detta test misslyckades genast i början, eftersom denna möjlighet inte var aktiverad i Intune admin portalen för alla enheter som registrerats (oberoende av plattform). Det vill säga, det gick inte att välja funktionen för nollställning av pinkoden. Det granskades att administreringen har nödvändiga rättigheter och att enheterna registrerats ordentligt. (Tillman 2016b). Efter flera test och undersökningar kom det fram att när det gäller Android-enheter fungerar inte denna funktion för plattformen Android 7.0 som detta test gjordes för. På iOS enheten fungerar detta också bara delvis, för att på denna plattform går det att tillfälligt ta autentise-

ringen av pinkoden ur bruk, vilket inte kan anses som en säker funktion när det gäller informationssäkerheten. (Barnett 2017a).

Följande test som utfördes var ett test som gällde den s.k. ”Selective Wipe” funktionen, d.v.s. borttagning av företagets data från en registrerad enhet. Detta test görs också via Intune-portalen i Azure (Azure Intune Preview), se figur 29. Testet görs här även på en Android-enhet.



Figur 29. Test av borttagning av företagets data från en Android-plattform (Intune Preview i Azure portalen).

Efter att kommandot för att ta bort företagets data från enheten hade getts gick det ca. fem minuter innan detta syntes på enheten genom meddelandet ”denna enhet hanteras inte mera av företaget”. För att validera att enheten rensats fullständigt testades att öppna Word-appen och granska om tillgång till företagets data via OneDrive ännu lyckas. Vid öppnandet av Word syntes de senaste företagsdokumenten en stund men det gick inte att öppna dem, vid försök att komma åt filerna meddelades: ”Din organisation tycker att du behöver förbättra din säkerhet”. Detta innebär att åtkomst inte tillåts om enheten inte är införd i Intune. Testet visar att ”Wipe” funktionen fungerat som önskat och att testet har lyckats.

6 SLUTSATS OCH DISKUSSION

Resultatet av arbetet blev som önskat, d.v.s. ett färdigt konfigurerat EMS-system som ett företag kunde ta i bruk för pilotanvändare. Jag hade kanske inte förväntat mig att det skulle bli ett färdigt system som går att använda, eftersom denna produkt är väldigt komplex och innehåller många delar. Trots ett komplext ämnesområde och begränsad erfarenhet lyckades jag få svar på de frågor jag ville gällande EMS-systemet. Nedan beskriver jag vilka iakttagelser jag har gjort och vilka svar jag kommit fram till.

Till en början kan det vara svårt att få en helhetsblick över vad allt EMS innebär och om det verkligen är ett nödvändigt system. Men då man läst in sig på systemet och gått igenom alla delmoment går det lättare att uppfatta vad allt detta system innehåller. För ett mindre företag, som varit utgångspunkt för mitt arbete, anser jag att EMS kunde vara en möjlig lösning för mobilhanteringen. Detta för att även en IT-administratör med mindre erfarenhet kan klara av att ta i bruk systemet och sköta administreringen. Men i detta skede måste det beaktas att alla mindre företag inte har nytta av detta system. För många företag räcker det med vanligt lösenord för att styra åtkomsten till e-posten och andra företagsresurser. Detta är ett system som kan anses vara nödvändigt för företag som behandlar mycket konfidentiellt material som inte får läcka ut till utomstående, som till exempel företag som arbetar med forskning och utvecklande av prototyper. Systemet kan dock anses som en bra lösning för större företag där en större skala av olika användare måste ha åtkomst till företagets data oberoende av enhet eller geologisk position. Då ett företag har större personal ökar även risken att företagets data hamnar i fel händer. För företag med mindre än 100 anställda som inte behandlar mycket konfidentiellt material rekommenderar jag inte ett fullständigt EMS-system. Men om det är fråga om ett företag med minst 100 eller fler användare kan jag rekommendera systemet.

I det första skedet av införandet av EMS blev det snabbt många portaler att hålla koll på och det kan verka förvirrande att inte genast ha koll på vad som behövs var och varför. Men en ny funktion vilket underlättar portalernas mängd var att Microsoft har lagt till möjligheten att administrera Intune via Azure Admin-portalen. För tillfället har inte alla funktioner flyttats till Azure, men övergången kommer att ske stegvis inom den närmaste framtiden. Instruktioner och dokumentering täcker inte den nya Azure-portalens Intune på samma sätt som den klassiska portalen, men de flesta saker går att konfigurera

på samma sätt i nya portalen bara man hittar rätt ställe att göra detta från. Från en Administratörs synvinkel lönar det sig att så långt som möjligt använda sig av den nya portalen för att undvika dubbelt arbete, t.ex. konfigurering av principer replikeras inte mellan dessa portaler. Enda nackdelen med nya portalen när det gäller konfigurationsprinciper är att där måste man skapa dem separat för varje operativsystem medan det i den gamla portalen går att skapa en gemensam princip för alla plattformar.

En av de viktigaste lärdomarna jag fått under arbetets gång gällande EMS systemet är att ge tillräckligt med tid för att identifiera företagets krav och mål för systemet och att satsa på förberedandet och planeringen av systemet. Detta för att i pilotskedet inte behöva göra många konfigurationer på nytt. En annan viktig aspekt att beakta då man planerar ett liknande system för ett företag är att göra utförliga valideringstest för att säkerställa olika fall där företagets data kunde läcka. I testskedet av det system jag konfigurerat kom det ständigt upp nya fall som måste testas. För att minska risken att data går förlorat lönar det sig att göra en färdig stomme för vilka test som skall utföras och vilket resultat som förväntas. Det lönar sig att testa själva systemet i det sista skedet före distribuering till pilotanvändarna.

Efter undersökning och test av hela EMS-produkten har jag kommit fram till följande slutsatser. För ett mindre företag (under 100 personer) får man kanske inte ut all nytta av hela EMS systemet. Då kunde en bättre lösning vara att bara använda delar av hela produktpaketet. För ett mindre företag som inte hanterar mycket konfidentiella data föreslår jag en kombination av bara Intune, Azure AD och en O365-licens. Detta kunde även vara ett lönsamt paket för större företag som inte hanterar konfidentiella data, men som vill ha bättre kontroll över de anställdas enheter och säkerhet. Jag tycker inte att säkerhetsdelen i EMS gav så mycket som Microsoft gjort reklam för. Redan med Intune och Azure Ad kan säkerheten skötas i stor utsträckning gällande informationssäkerheten. Som redan nämnts i testandet av konfigurerade system så fungerade Azure Information Protection inte som önskat och jag ser inte så stor nytta av denna tjänst. Samma gäller för Cloud App Security, för jag testade att bryta mot reglerna för att få en rapport att genereras, men inga varningar eller rapporter dök upp efter flera test. Att bara använda Intune gör det även lättare för administreringen eftersom två komponenter faller bort vid införandet av systemet.

Ovannämnda lösning med bara delar av EMS-produktpaketet kan anses vara en bra lösning för företag utan tidigare infrastruktur och centraliserad användarhantering (som exempel kan nämnas företag som använt Googles gratisprodukter). Detta system kan användas som en helt molnbaserad lösning och då lönar det sig att beakta kostnader för lagringsutrymme i molnet om företaget har mycket data. Från en mindre erfaren administratörs synvinkel skulle detta system vara en god kandidat att beakta vid valet av infrastruktur för företaget. Administreringen är relativt enkel och det går också enkelt att utvidga systemet om företaget växer och det krävs inga ytterligare investeringar i lokala servrar på företaget.

KÄLLOR

Avraamides, L. 2016. *What is Intune*?
Tillgänglig: https://docs.microsoft.com/en-us/intune/understand-explore/introduction-to-microsoft-intune. Hämtad 20.02.2017

Bailey, C. 2017a. *Quick start tutorial for Azure Information Protection*. Tillgänglig:https://docs.microsoft.com/fi-fi/information-protection/get-started/infoprotect-quick-start-tutorial. Hämtad 01.04.2017.

Bailey, C. 2017b. *How to configure conditions for automatic and recommended classification for Azure Information Protection*
Tillgänglig: https://docs.microsoft.com/en-us/information-protection/deploy-use/configure-policy-classification#information-about-the-built-in-conditions. Hämtad 01.04.2017.

Bailey, C. 2017c. *What is Azure Information Protection?* [Homepage of Microsoft], [Online]. Availablehttp://: https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-information-protection.
Hämtad 04.04.2017.

Barnett, N. 2017a. *Help protect your devices with remote lock and passcode reset* [Homepage of Microsoft], [Online]. Tillgänglig: https://docs.microsoft.com/en-us/intune/deploy-use/use-remote-lock-and-passcode-reset-in-microsoft-intune. Hämtad 15.04.2017.

Barnett, N. 2016b. *Konfigurera Android-hantering*.
Tillgänglig: http://docs.microsoft.com/sv-se/intune/deploy-use/set-up-android-management-with-microsoft-intune Hämtad 25.10.2016.

Barnett, N. 2016c. *Konfigurera iOS- och Mac-enhetshantering*. Tillgänglig:
https://docs.microsoft.com/sv-se/intune/deploy-use/set-up-ios-and-mac-management-with-microsoft-intune Hämtad 25.10.2016.

Barnett, N. 2016d. *Set up Windows device management*. Docs.microsoft.com. Tillgänglig: https://docs.microsoft.com/en-us/intune/deploy-use/set-up-windows-device-management-with-microsoft-intune Hämtad 25.10.2016.

Barnett, N. 2017e. *Sign up or sign in to Intune*. Tillgänglig: https://docs.microsoft.com/en-us/intune/get-started/start-with-a-paid-subscription-to-microsoft-intune-step-1. Hämtad 25.10.2016.

Brink, S. 2017, *How to Backup and Restore Wireless Network Profiles in Windows 10* Tillgänglig: https://www.tenforums.com/tutorials/3530-backup-restore-wireless-network-profiles-windows-10-a.html. Hämtad 07.03.2017

Caserio, C 2017. *Protect email access to Exchange Online and new Exchange Online Dedicated with Intune*. Tillgänglig: https://docs.microsoft.com/en-us/intune/deploy-use/restrict-access-to-exchange-online-with-microsoft-intune. Hämtad 05.04.2017

Collier, M & Shahan, R. 2016, *Fundamentals of Azure Second Edition*. E-Bok Redmond, Washington. Microsoft Press Tillgänglig: https://mva.microsoft.com/ebooks?lng=en-US. Hämtad 06.01.2017

Della Monica, A. 2016a. *Understand the MDM lifecycle*. Docs.microsoft.com. Tillgänglig: https://docs.microsoft.com/en-us/enterprise-mobility-security/Solutions/mdm-understand-mdm-lifecycle Hämtad 25.10.2016.

Della Monica, A. 2016b. *Application management options*. [online] Docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/enterprise-mobility-security/Solutions/mdm-application-management-options Hämtad 25.10.2016.

Diogenes, Y & Gilbert, J. 2015, *Enterprise Mobility Suite Managing BYOD and Company-Owned.Devices E-Bok*. Redmond, Washington. Microsoft Press Tillgänglig:https://play.google.com/store/books/details/Yuri_Diogenes_Enterprise_Mobility_Suite_Managing_B?id=U2w0BwAAQBAJ. Hämtad 01.03.2017

Diogenes, Y. 2017. *Protect at the Front Door* [Homepage of Microsoft], [Online]. Tillgänglig: https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/protect-front-door. Hämtad 06.01.2017

Gilbert, J. 2016. *Learn about Enterprise Mobility + Security*. Tillgänglig: https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/learn-about-ems. Hämtad 25.10.2016.

Mathers, B 2016. *Integrera dina lokala identiteter med Azure Active Directory* Tillgänglig: https://docs.microsoft.com/sv-se/azure/active-directory/active-directory-aadconnect. Hämtad 25.10.2016

May, S. 2015. *Get started with the Microsoft Enterprise Mobility Suite (EMS) in Minutes* - Simon May. Simon May. Tillgänglig: http://simon-may.com/get-started-enterprise-mobility-suite-minutes/ Hämtad 25.10.2016.

Karlin, R. 2017a *, What is Advanced Threat Analytics?* [Homepage of Microsoft Technet] Tillgänglig: https://docs.microsoft.com/en-us/advanced-threat-analytics/understand-explore/what-is-ata. Hämtad 24.01.2017.

Lamos, B. 2016. *Authentication Scenarios for Azure AD*. Azure.microsoft.com. Tillgänglig: https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios/ Hämtad 25.10.2016.

Lloyd, C. 2016, *INTRODUCTION TO MICROSOFT CLOUD APP SECURITY*. Tillgänglig: https://oxfordcomputergroup.com/resources/intro-cloud-app-security/. Hämtad 07.03.2017

Love, C. 2017a *Add new users to Azure Active Directory preview*. Tillgänglig: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-users-create-azure-portal
Hämtad 24.01.2017.

Love, C. 2017b. *Azure Active Directory editions* [Homepage of Microsoft] Tillgänglig: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-editions Hämtad 09.11.2016.

Love, C. 2016c. *What is Azure Active Directory?* Azure.microsoft.com. Tillgänglig: https://azure.microsoft.com/sv-se/documentation/articles/active-directory-whatis/ Hämtad 09.11.2016.

Microsoft. 2017a. *Add several users at the same time to Office 365 - Admin Help*. Tillgänglig: https://support.office.com/en-us/article/Add-several-users-at-the-same-time-to-Office-365-Admin-Help-1f5767ed-e717-4f24-969c-6ea9d412ca88?omkt=en-US&ui=en-US&rs=en-US&ad=US&fromAR=1 Hämtad 24.01.2017.

Microsoft. 2016b. *Kattavan mobiliteettiratkaisun hinnoittelu – mobiililaitteiden hallintaohjelmistot | Microsoft*. Tillgänglig: https://www.microsoft.com/fi-fi/server-cloud/enterprise-mobility/pricing.aspx Hämtad 25.10.2016.

Microsoft. 2016c. *Microsoft Identity-Driven Security*. [PDF]. Tillgänglig: http://download.microsoft.com/download/E/C/7/EC78FF06-02BB-4DFD-9EBB-CADB66BB594F/Microsoft_Identity Driven Security_Datasheet_EN_US.pdf Hämtad 25.10.2016

Microsoft. 2015d. *Mobile Device Management Design Considerations Guide V2 Sample*. [PDF] Tillgänglig: https://gallery.technet.microsoft.com/office365/Mobile-Device-Management-7d401582 Hämtad 24.01.2017.

Shinder D. 2015. *Active Directory in the Cloud*. Tillgänglig: http://techgenix.com/active-directory-cloud-part1/. Hämtad 09.11.2016.

Stack, R. 2016a , *Enable access to company resources with Microsoft Intune* Tillgänglig: https://docs.microsoft.com/en-us/intune/deploy-use/enable-access- to-company-resources-with-microsoft-intune. Hämtad 07.03.2017

Stack, R. 2016b. *Use a custom policy to create a Wi-Fi profile with a pre-shared key* Tillgänglig: https://docs.microsoft.com/en-us/intune/deploy-use/pre-shared-key-wi-fi-profile. Hämtad 07.03.2017

Stack, R & Tillman, M. 2016. *Manage settings and features on your devices with Microsoft Intune policies*. Tillgänglig: https://docs.microsoft.com/en-us/intune/deploy-use/manage-settings-and-features-on-your-devices-with-microsoft-intune-policies. Hämtad 07.03.2017

Tillman, M. 2016a. *Choose Intune standalone or hybrid MDM*. [online] Docs.microsoft.com Tillgänglig: https://docs.microsoft.com/en-us/sccm/mdm/understand/choose-between-standalone-intune-and-hybrid-mobile-device-managementHämtad 17.11.2016.

Tillman, M. 2016b. *Intune testing and validation* Tillgänglig: https://docs.microsoft.com/en-us/intune/plan-design/section-9-test-and-validation#functional-validation-testing. Hämtad 17.11.2016.

Tillman, M. 2016c. *How to create and assign app protection policies* [Homepage of Microsoft], [Online]. Tillgänglig: http://: https://docs.microsoft.com/en-us/intune-azure/manage-apps/app-protection-policies. Hämtad 15.03.2017.

Vilcinskas, M. 2017. *Azure Active Directory Identity Protection*. Tillgänglig: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection Hämtad 01.04.2017.