Lauri Auerniitty

Mobiililaitehallinnan käyttöönotto Kaisanet Oy:lle

Tradenomi

Tietojenkäsittely

Syksy 2020

KAMK • University of Applied Sciences

KAMK • University of Applied Sciences

Tiivistelmä

Tekijä(t): Auerniitty Lauri

Työn nimi: Mobiililaitehallinnan käyttöönotto Kaisanet Oy:lle

Tutkintonimike: Tradenomi, tietojenkäsittely

Asiasanat: mobiililaitehallinta, Intune, Android, iOS

Tämän opinnäytetyön tarkoituksena oli toteuttaa Microsoft Intune -palvelun käyttöönotto toimeksiantaja Kaisanet Oy:lle. Kaisanet Oy on kokonaisvaltainen tietotekniikan palvelutalo, jolla on toimipisteet Kajaanissa ja Iisalmessa. Microsoft Intune on pilvipohjainen palvelu, jota käytetään mobiililaitteiden ja sovelluksien hallitsemiseen. Microsoft Intune -palvelusta haluttiin selvittää hallintaominaisuuksien toiminallisuus sekä kattavuus, joidenka perusteella tutkittiin, onko Intune Kaisanet Oy:n IT-liiketoiminnalle sopiva palvelutuote. Intunen käyttöönotto toteutettiin kesällä 2020 testiympäristön sisälle, jossa sen toimivuutta kokeiltiin erilaisilla mobiililaitteilla. Käyttöönotossa edettiin Centero Oy:n järjestämillä workshop-päivillä ja testiympäristössä saatujen tuloksien perusteella.

Mobiililaitteiden hallinnantaso voi olla kokonaisvaltaista tai kevyttä riippuen laiteomistajuudesta. Kokonaisvaltaista hallintaa käytetään yrityksen omistamiin laitteisiin, joka mahdollistaa laajempien hallintaominaisuuksien hyödyntämisen laiteella. Laajempia hallintaominaisuuksia voidaan käyttää esimerkiksi laitteen rajoittamiseen tiettyyn työtehtävään. Kevyempää laitehallintaa käytetään loppukäyttäjien henkilökohtaisille laitteille, jotka ovat myös työkäytössä. Loppukäyttäjän henkilökohtaiset tiedot ja sovellukset pysyvät poissa hallintapalvelusta. Mobiililaitehallinnan yhteydessä voidaan käyttää myös muita hallintaratkaisuja, kuten sovellustenhallintaa. Sovellustenhallintaa käytetään tiettyjen sovelluksien ylläpidossa.

Testiympäristön käyttöönoton perusteella Microsoft Intune otettiin käyttöön sekä jatkokehitykseen Kaisanet Oy:n tuotantopuolelle. Työssä kuvatun Intune-käyttöönoton ympärille muodostettiin käyttöohjeistus, testien ja workshop-päivien aikana kerätyn dokumentaation avulla. Käyttöohjeistusta tullaan hyödyntämään tulevaisuuden Intune-käyttöönotoissa. Intune osoittautui laadukkaaksi mobiililaitehallintaratkaisuksi. Microsoftilla on vielä kehitettävää Intunen suhteen hallintakäyttöliittymän käyttökokemuksessa ja raportointiominaisuuksissa.

KAMK • University of Applied Sciences

Abstract

Author(s): Auerniitty Lauri

Title of the Publication: Mobile Device Management Deployment for Kaisanet Oy

Degree Title: Bachelor of Business Administration, Business Information Technology

Keywords: Mobile Device Management, Intune, Android, iOS

The aim of this thesis was to deploy and test Microsoft Intune in a proof-of-concept environment. Microsoft Intune is an enterprise mobility management cloud-service that allows a company to manage mobile devices and applications remotely. The work in the thesis was done for Kaisanet Oy to see if the feature set and the functionality of Microsoft Intune would be a fitting service product for the company. The proof-of-concept deployment was done during summer 2020 that progressed based on the test results from different mobile devices and Intune workshop days provided by Centero Oy. To keep the thesis in focus, the subject area was restricted to cover only Android and iOS device management.

The level of device management differs with company owned and personal devices. Company owned devices are managed with a more robust and comprehensive features, that can for example be used to restrict a device to a single work task. Personal devices that are also used in a work environment can be managed with a lighter level of control. The end user's personal details and software are separated from the managed work area and cannot be controlled by the mobile device management service. Mobile device management can be combined with other solutions, such as mobile application management, which is used to control the specified applications within a device.

The proof-of-concept deployment proved to be a success. Microsoft Intune was taken as a service product to be offered for Kaisanet's clients. Intune was also deployed to Kaisanet's production environment to handle the mobile device management inside the company. The proof-of-concept deployment documentation was used to create instructions for future Intune deployments and maintenance.

Sisällys

1 Johdanto 1

2 Mobiililaitteiden hallinta 3

2.1 MDM – Mobiililaitehallinta 3

2.2 MAM – Sovellustenhallinta 4

2.3 EMM – Yrityksen liikkuvuuden hallinta 4

2.4 UEM – Yhdenmukaistettu päätelaitteiden hallinta 4

2.5 Laitepolitiikkaratkaisut 5

2.5.1 BYOD ja CYOD 6

2.5.2 COBO ja COPE 7

3 Microsoft Intune 8

3.1 Intunen lisensointi 9

3.2 Microsoft Endpoint Manager 9

3.3 Intune-yritysportaali 10

4 Mobiililaitteiden rekisteröinti 12

4.1 Android-profiilit 12

4.1.1 Henkilökohtaiset mobiililaitteet 13

4.1.2 Yrityksen mobiililaitteet 14

4.2 iOS-profiilit 16

4.3 Mobiililaitteiden rekisteröintirajoitukset 17

5 Intunen POC-käyttöönotto 18

5.1 Laite- ja käyttäjäryhmien luonti 18

5.2 Laitteiden ja sovelluksien liittämisen edellytykset 19

5.2.1 Android 20

5.2.2 iOS 21

5.3 Sovellukset 24

5.3.1 Sovelluksien lisääminen ja kohdennus 25

5.3.2 Sovelluksien tietoturvat 26

5.3.3 Sovelluksien muokkaaminen 27

5.4 Laitteet 28

5.4.1 Laitekohtaiset asetuskäytänteet 29

5.4.2 Laitekohtaiset vaatimuskäytänteet 30
5.5 Ympäristön testaus 31

6 Pohdinta 34

7 Yhteenveto 36

Lähteet 37

Symboliluettelo

ADE	Automatic Device Enrollment on Applen palvelu, joka mahdollistaa iOS-laitteiden automaattisen rekisteröinnin mobiililaitehallintaympäristöön [1].
Azure AD	Azure Active Directory on Microsoftin pilvipohjainen hakemisto- ja identiteetinhallintapalvelu [2].
BYOD	Bring Your Own Device on laitepolitiikka, joka sallii työntekijöiden henkilökohtaisten mobiililaitteiden käyttämisen työhön liittyvissä tehtävissä [3].
COBO	Company Owned, Business Only on laitepolitiikka, joka sisällyttää yrityksen omistamat ja vain yrityskäyttöön tarkoitetut laitteet [4].
COPE	Company Owned, Personally Enabled on laitepolitiikka, joka sisällyttää yrityksen omistat laitteet, joita työntekijät voivat käyttää myös henkilökohtaiseen käyttöön [4].
CYOD	Choose Your Own Device on laitepolitiikka, jossa yritys tarjoaa työntekijöilleen listan laitteista, joita voidaan käyttää työympäristössä [3].
EMM	Enterprise Mobilitity Management yhdistää erilaisia työkalu- ja käytänneratkaisuja, kuten mobiililaite- ja sovellushallinnan [5].
KME	Knox Mobile Enrollment on Samsungin palvelu, jonka avulla voidaan rekisteröidä yrityksen omistamia Android-laitteita suoraan mobiililaitehallintaympäristöön, laitteen ensimmäisen käynnistyksen yhteydessä [6].
MAM	Mobile Application Management mahdollistaa yrityksen käyttämien sovelluksien tietojen ja pääsyn rajaamisen [7].
MDM	Mobile Device Management tarkoittaa ohjelmistoa, joka on suunniteltu mobiililaitteiden, kuten älypuhelimien hallintaan ja suojaamiseen [8].
POC	Proof-of-concept menetelmän avulla voidaan selvittää idean tai esimerkiksi ratkaisun toimivuus ja jatkokehittämisen kannattavuus [9].
SCCM	System Center Configuration Manager on Microsoftin ohjelmisto, jolla voidaan hallita keskitetysti erilaisia Windows-pohjaisia alustoja [10].

UEM	Unified Endpoint Management mahdollistaa lähes kaikkien mobiililaitteiden päätepistehallinnan yhden palvelun avulla [11].

1 Johdanto

Mobiililaitehallinnan tärkeys yrityskäytössä on kasvanut maailmalla merkittävästi. Mobiililaitteilla, kuten Windows-kannettavalla tai Android-älypuhelimella, käsitellään henkilökohtaista sekä työelämään liittyvää tietoa. Hallitsemattoman tiedon lisääntyminen kasvattaa tietoturvariskejä, joiden vähentäminen jää yleisesti loppukäyttäjän harteille. Yrityksellä ei ole perinteisesti keinoa esimerkiksi poistaa varastetun laitteen tietoja, jolloin sen päätyminen julkisuuteen tai varkaan käsiin on vain ajan kysymys.

Mobiililaitehallinnan avulla yritys saa mobiililaitteet keskitetysti etävalvontaan. Hallinnassa voidaan seurata, miten kyseisten laitteiden päivitykset ja muut määritykset on tehty. Laitteille voidaan myös pakottaa toimenpiteitä, kuten sovelluksen asentaminen tai vahvan lukituskoodin määrittäminen. Mobiililaitehallinnalla voidaan myös taata, että vain sen hallinnan alla olevat laitteet saavat pääsyn yrityksen tärkeisiin resursseihin, kuten työsähköpostisovellukseen. [12.]

Tässä työssä käydään läpi Microsoft Intune -mobiililaitehallinnan POC (proof-of-concept) käyttöönotto. Intune on täysin pilvipohjainen mobiililaitehallintaratkaisu, joten sen käyttöönoton asennusvaiheelle ei ole tarvetta. Intunen käyttöönotossa päästään siis suoraan järjestelmän erilaisiin määrityksiin, heti lisenssin aktivoimisen jälkeen. Opinnäytetyössä käsitelty käyttöönotto on rajattu älylaitekäyttöjärjestelmiin (Android ja iOS).

Opinnäytetyön toimeksiantaja on harjoittelupaikkani Kaisanet Oy. Kaisanet Oy on kokonaisvaltainen tietotekniikan palvelutalo, jolla on toimipisteet Kajaanissa ja Iisalmessa. Kaisanet palvelee yrityksiä, kuluttajia ja yhteisöjä, sekä on jäsenenä valtakunnallisessa Finnet-liitossa. Kaisanet tuottaa asiakkailleen valokuituun pohjautuvaa tietoliikenneverkkoa, modernien alustojen IT- ja viestintäpalveluita ja käyttötukea. Kaisanet tarjoaa valokuitu- ja kaapeli-TV-verkkoa Kainuun, Ylä-Savon sekä Pohjois-Karjalan alueella. Kaisanetin liikevaihto on noin 20 miljoonaa euroa ja henkilöstöä on n. 90. [13.]

Työssä tutkitaan, miten ja millaisia eri ominaisuuksia Intune-mobiililaitehallinnan kautta voidaan ottaa käyttöön ja kuinka kyseinen järjestelmä voidaan toteuttaa. Työn tavoitteena oli saada ymmärrys siitä, kuinka laajaa ja kattavaa hallintaa järjestelmällä pystytään suorittamaan ja onko se Kaisanet Oy:n IT-liiketoiminnalle sopiva palvelutuote.

Intunen toiminta kokeillaan erilaisten testilaitteiden avulla, jonka aikana käyttöönoton eri prosessivaiheet dokumentoidaan. Näiden ympärille rakennetaan jälkeenpäin sisäinen käyttöohjeistus ja toimintatavat.

2 Mobiililaitteiden hallinta

Mobiilin työympäristön hallintaan kuuluu useita termejä ja käytänteitä, joiden hahmottaminen voi osoittautua hankalaksi. Tässä luvussa tarkastellaan mobiililaitehallintaan liittyviä tekniikoita ja vertaillaan neljää erilaista laitepolitiikkaratkaisuja, jotka määrittelevät yrityksen laitehallintatason. Luvun tarkoituksena on käydä läpi yleisempiä ja tämän opinnäytetyön kannalta merkityksellisiä käsitteitä, joista kuvastuu selkeämpi mobiililaitehallinnan maailma.

Hallinta voidaan purkaa käsitteenä tässä yhteydessä mobiililaitteen ylläpitoon ja sen mukana tuleviin osa-alueisiin. Ylläpitoon kuuluu mobiililaitteen asetuksien, ohjelmien ja tietoturvan määrittäminen. Mobiililaitteille suoritettavan hallinnan merkitys on kasvanut vuosien edetessä, sillä laitteiden määrä ja niiden käyttö yritysympäristössä on lisääntynyt vauhdilla. Vastuu mobiililaitteen ylläpidosta on entistä enemmän loppukäyttäjällä. Hallinnan toteuttaminen kolmannen osapuolen ratkaisulla antaa yrityksen IT-osastolle monimuotoiset työkalut, mobiililaitteiden etähallintaa varten. Mobiililaitteiden etähallintaa tarjoavat ratkaisut voidaan määritellä erilaisten strategioiden alle, kuten MDM, EMM ja UEM, joita avataan tarkemmin seuraavissa luvuissa. [12.]

2.1 MDM – Mobiililaitehallinta

MDM (Mobile Device Management), eli mobiililaitehallinta tarkoittaa ohjelmistoa, joka on suunniteltu mobiililaitteiden, kuten älypuhelimien hallintaan ja suojaamiseen. MDM on yksi osa suurempaa EMM-työkalu- ja käytänneratkaisua. Mobiililaitehallinta toteutetaan rekisteröimällä yrityksen laitteet MDM-palveluun, jonka jälkeen rekisteröityneitä laitteita voidaan seurata, hallita ja turvata palvelusta käsin etänä. [8.]

Mobiililaitehallinta on tärkeä suojauskeino yrityksille, sillä sen tarjoamat käytänteet suojaavat mobiililaitteiden arkaluontoista tietoa eri tahoilta riippumatta siitä, onko kyseinen mobiililaite yrityksen tai työntekijän omistuksessa. Mobiililaitehallinnan avulla pystytään esimerkiksi määrittämään, miten yritystietoihin päästään käsiksi, mitkä sovellukset ovat sopivia työkäyttöön ja minkälainen näytönlukitus jokaisessa laitteessa pitäisi olla. [8.]

2.2 MAM – Sovellustenhallinta

Usein mobiililaitehallinnan yhteydessä käytetty hallintapa. MAM (Mobile Application Management), eli sovellustenhallinta, mahdollistaa yrityksen käyttämien sovelluksien tietojen ja pääsyn rajaamisen, varsinaisen mobiililaitteen hallinnan sijaan. MAM kykenee hallinnoimaan yrityssovelluksia ja niiden sisältämää tietoa. Sovellustenhallintaa voidaan hyödyntää erilaisissa käytännön tilanteissa. Esimerkiksi poistuvan työntekijän omista mobiililaitteista voidaan poistaa pelkästään yritykseen liittyvät sovellukset ja niiden tiedot, koskematta työntekijän henkilökohtaiseen sisältöön. [7.]

Sovellusnäkökulmasta yritys voi esimerkiksi tiukentaa käyttämäänsä sähköpostisovelluksen tietoturvapolitiikkaa mieluisella tavalla. Sähköpostisovellukselle voidaan asettaa jokaista käyttöä varten erillinen lukituskoodi ja estää tekstin tai muiden tiedostojen kopiointi kyseisen sovelluksen ulkopuolella oleville alustoille. [7.]

2.3 EMM – Yrityksen liikkuvuuden hallinta

EMM (Enterprise Mobility Management), eli yrityksen liikkuvuuden hallinta, on erilaisten työkalu- ja käytänneratkaisujen kokonaisuus. EMM yhdistää erilaiset sovellushallintateknologiat, kuten MAM-hallinnan ja MDM-laitehallinnan yhden palvelun alle. EMM-käsite muodostui ICT-alan tutkimus- ja konsultointiyritys Gartnerin toimesta, jolla pyrittiin vähentämään erilaisten ratkaisumuotojen tuomaa hämmennystä. Hallintatapojen yhdistäminen yhden ratkaisun selkeytti olemassa olevaa tuotekantaa. [5.] [14.]

2.4 UEM – Yhdenmukaistettu päätelaitteiden hallinta

UEM (Unified Endpoint Managament), eli yhdenmukaistettu päätelaitteiden hallinta, on EMM-hallinnasta kehittynyt ratkaisumuoto. Nimensä mukaisesti UEM yhdenmukaistaa erilaisten laitteiden, kuten älypuhelimien, tietokoneiden ja IoT-laitteiden päätepistehallinnan yhden ympäristön ympärille. Keskitetyn UEM-ympäristön palveluiden avulla voidaan hallita hyvin laajaa laitekantaa ja vähentää erilaisten työkalujen monimutkaisia integraatioita erilaisten alustojen kanssa. [11.]

2.5 Laitepolitiikkaratkaisut

Mobiililaitehallintaan kuuluu useita, laitepolitiikkaan ja omistajuusmalliin liittyviä termejä. Yrityksen laitepolitiikkasuunnitelma on tärkeä osa mobiililaitehallintaa. Sen avulla tiedetään, minkä tason tietoturvaa, laitehallintaa ja kustannuksia mobiililaitekanta pitää sisällään. Yleisimpiin ratkaisuihin kuuluvat seuraavat mallit: BYOD, CYOD, COPE ja COBO.

IT-konsultti Joel Snyder luettelee Samsung Business Insights -artikkelissaan kolme tärkeää kysymystä, joiden avulla yritys voi määritellä oman menettelytapansa:

- Mobiililaite: mikä se on, kuka valitsee mobiililaitteet ja kuka maksaa mobiililaitteen kulut?
- Hallinta ja tuki: kuka hallitsee mobiililaitetta ja on tukivastaava?
- Integraatio ja sovellukset: kuinka tärkeä mobiililaite on päivittäisessä työkäytössä? [15.]

Mobiililaitekysymyksen avulla selvitetään, tarkoitetaanko mobiililaitteella pelkästään perinteisempää älypuhelin- ja tablettilaitekantaa, vai lasketaanko mukaan myös kannettavat tietokoneet ja muut mahdolliset älylaitteet. Mobiililaitekysymyksellä tarkistetaan myös, mitkä mobiililaitteet päätyvät lopullisen laitepolitiikkamallin alle ja kuka on vastuussa mobiililaitteiden kuluista. Mobiililaiteselvityksen jälkeen yritys voi poissulkea sekä kallistua tiettyihin malleihin. [15.]

Mobiililaitteen hallintaan ja tukeen liittyvällä kysymyksellä halutaan kuvailla, kuka on vastuussa edellä mainituista osa-alueista. Hallintaosuuden määritys voidaan yleisesti peilata suoraan tukeen. Olematon laitehallinta yleensä tarkoittaa vähäistä tukea, kun taas MDM tai EMM-laitehallinnan tuomat, monipuolisemmat rajoitteet yhdistetään myös kattavampaan tukeen. [15.]

Integraatio ja sovellukset -osuudessa käydään läpi, kuinka tärkeä työkalu mobiililaite on työkäytössä. Kuuluuko mobiililaitteen sovellusluetteloon perinteiset, yhteistyötä edistävät sovellukset, vai onko yrityksellä varta vasten mobiililaitteita ja yrityksen verkkoa hyödyntäviä sovelluksia. Lopputulos määrittää, millä tasolla yritys hyödyntää mobiliteettia. [15.]

Samsung Business Insights -artikkelissa todetaan lopuksi, että valitun laitepolitiikkamallin lisäksi on tärkeämpää huomioida sopiva tasapaino menettelytapojen välistä. Yrityksen tavoitteena olisi panostaa jokaiseen osa-alueeseen samantasoisesti ja olla niinkään välittämättä virallisista termeistä. [15.]

2.5.1 BYOD ja CYOD

BYOD (Bring Your Own Device), eli oman laitteen käyttäminen työkäytössä, on yritys- ja koulutusmaailman laitepolitiikka, joka on yleistynyt vuosi vuodelta älylaitemarkkinoiden ja etätyöskentelyn suosion kasvaessa. Nimensä mukaisesti BYOD-laitepolitiikkaan kuuluvat työntekijöiden henkilökohtaiset laitteet, joita käytetään työhön liittyvissä tehtävissä. BYOD tuo mukanaan useita hyötyjä ja huomioon otettavia haasteita. Työntekijät kokevat olevansa tehokkaampia omien laitteiden kanssa, sillä mahdollista oppimiskynnystä uuden mobiililaitteen kanssa ei ole. BYOD on myös kustannustehokas vaihtoehto yritykselle, joka vähentää laite- sekä verkkokuluja tietyissä tilanteissa. [3.]

Suurena riskitekijänä huomioidaan henkilökohtaisten mobiililaitteiden tietoturvallisuuteen liittyvät ongelmat. Yrityksillä on haasteita tasapainottaa BYOD-laitteen tuomaa tehokkuutta ja tietoturvatasoa samanaikaisesti. Yhdysvaltalainen pilvitietoturvayhtiö Bitglass kertoo vuoden 2020 BYOD-tutkimuksessaan, että vastanneiden kesken eniten huolta aiheuttavat henkilökohtaisten laitteiden riskit olivat: tietovuoto (63 %), vaarallisen tiedoston lataus (57 %) ja hävinnyt tai ryöstetty laite (55 %). Tutkimuksessa todettiin, että BYOD-tietoturvariskeistä huolimatta yritykset eivät ota tarpeellisia keinoja yritystietojen turvaamiseksi. Noin puolet kyselyyn vastanneista (51 %) eivät ota kantaa henkilökohtaisen mobiililaitteen tiedostonjakosovelluksista ja hieman alle kolmasosa (30 %) vastanneista ei hallitse tai valvo yrityskäytössä olevia viestintäalustoja. Tärkeä johtopäätös BYOD-tietoturvasta on miettiä, mikä mobiililaitehallintaratkaisu toimisi parhaiten yrityskäytön tarpeisiin, jotta pahimmilta BYOD-tietoturvariskeiltä vältyttäisiin. [16.]

CYOD (Choose Your Own Device), eli valitse oma laitteesi, menettelee BYOD-laitepolitiikan periaatteita, mutta toteutetaan eri tavalla. Yritys tarjoaa työntekijöilleen listan laitteista, jotka noudattavat yrityksen määrittämiä kriteerejä. Työntekijä saa valita itselleen mieluisan laitteen, mutta yritys pystyy hallitsemaan laitteelle asetettavia sovellus- ja asetusmäärityksiä. CYOD-laitteen elinkaari riippuu yrityksen menettelytavoista, laite pysyy työntekijän kanssa työn päättymiseen saakka, tai laite vaihdetaan tietyin väliajoin. CYOD-laitteen omistajuuspolitiikka vaihtelee myös samalla periaatteella. Työntekijä voi esimerkiksi CYOD-elinkaarin päättymisen jälkeen ostaa laitteen itselleen, tai jättää sen yrityksen omistajuuteen. [3.]

Ennalta määritetyn laitelistan avulla yritys tietää, mitkä laitetyypit ja valmistajat ovat työntekijöiden käytössä. Rajoitettu CYOD-laitekanta helpottaa täten yritystä teknisten ongelmien ja tuen antamisessa. Yrityksen käytössä olevat ohjelmistot pystytään myös testaamaan erilaisilla laiteko-

koonpainoilla. Testituloksien perusteella laitelistaan voidaan valita kaikista optimaalisimmat kokoonpanot, mikä voi vähentää ohjelmiin liittyviä ongelmia huomattavasti. Tämän lisäksi yrityksen asettamat sovellus- ja asetusmääritykset vähentävät tietoturvaan liittyviä riskejä. [17.]

2.5.2 COBO ja COPE

COBO (Company Owned Business Only), eli yrityksen omistamat ja vain yrityskäyttöön tarkoitetut laitteet. COBO on käytännössä BYOD-laitepolitiikan vastakohta. Yritys omistaa ja hallitsee mobiililaitteen kaikkia ominaisuuksia. Käyttökokemuksesta on poistettu täysin henkilökohtaiseen laitteeseen sisältyvä joustavuus ja muokattavuus. Yrityksen omistama mobiililaite voi esimerkiksi ajaa vain yhtä sovellusta, jonka avulla suoritetaan tiettyä työtehtävää. [4.]

COBO-laitepolitiikan tiukat määritykset ja hallintamahdollisuudet mahdollistavat mobiililaitteille vahvempaa tietoturvaa sekä toiminnallista tehokkuutta. Työntekijät voivat myös käyttää omia, henkilökohtaisia laitteitaan ilman yrityksen asettamia määrityksiä. COBO-laitepolitiikan yrityskäyttörajauksen takia kyseisiä laitteita käytetään yleensä vain tiettyihin työtehtäviin, eivätkä ne kuulu työntekijöiden jokapäiväiseen työrutiiniin. [4.]

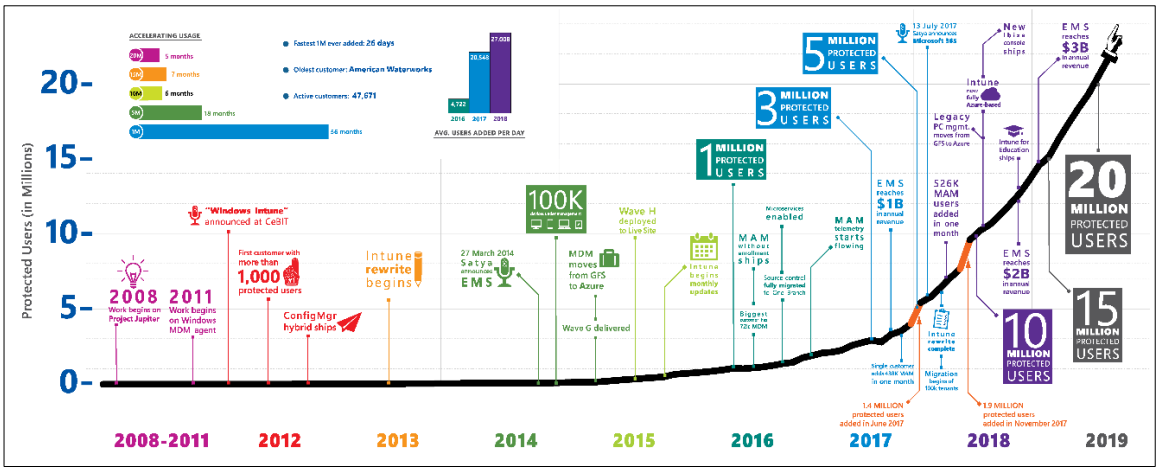
COPE (Company Owned, Personally Enabled), eli yrityksen omistamat laitteet, jotka tarjoavat työntekijöille COBO-laitteista puuttuvaa joustavuutta. COPE nähdään yleisesti BYOD-laitepolitiikan vaihtoehtona, sillä se tarjoaa identtiset hyödyt, poistaen samalla arkaluonteisin tiedon suojaamisen huolet. Työntekijät voivat käyttää COPE-laitetta henkilökohtaiseen sekä työympäristön käyttötarkoitukseen. [4.]

3 Microsoft Intune

Tässä luvussa käydään läpi Microsoft Intune -palvelun perusteet, kuten Intunen lisensointi, ylläpitäjien hallintaympäristö Endpoint Manager ja loppukäyttäjille tarkoitettu yritysportaalisovellus mobiililaitteiden rekisteröintiä varten.

Microsoft Intune on Azure-pilvipalvelussa sijaitseva ohjelmisto, joka mahdollistaa mobiililaite- ja sovellustason hallinnan. Yritysnäkökulmasta Intunea voidaan käyttää työntekijöiden mobiililaitteiden hallintaa varten. Palvelun avulla työntekijöille mahdollistetaan tietoturvallinen pääsy yrityskohtaisiin resursseihin lähes mistä mobiililaitteesta tahansa, riippumatta työtekijän fyysisestä sijainnista. Yrityksen resurssit pysyvät turvassa erilaisten sovellus- ja laiteasetuskäytänteiden avulla. Intune on yhteensopiva Android-, iOS, macOS- sekä Windows 10 -laitteilla. Olemassa oleva työasemien SCCM-hallintaympäristö voidaan kytkeä osaksi Microsoftin Azure-pilvipalvelua, jonka avulla Intune ja SCCM voivat hallita Windows 10 -laitteita yhtäaikaisesti. [18.]

Intune on palveluna kokenut jatkuvaa kasvua, aina mobiilimpaan suuntaan siirtyvän maailman myötä. Microsoftin julkaisemassa taulukossa nähdään käyttäjämäärän ja erilaisten ominaisuuksien nousu Microsoft Intune -palvelun synnyn alusta (kuva 1). Intune on Microsoftin jatkuvassa kehityksessä. Uusien ominaisuuksien kehityksestä ilmoitetaan viikoittain, joista lopulta muodostuu julkaisuvalmis kuukausipäivitys [19].



Kuva 1. Microsoft Intune -statistiikkataulukko tuotteen kehitysvaiheesta vuoteen 2019 saakka [20].

3.1 Intunen lisensointi

Microsoft Intunen tarjoamat käyttölisenssit voidaan jakaa kolmeen erilliseen tuotepakettiin. Ominaisuuksiltaan yksinkertaisin saatavilla oleva lisenssi on standalone, joka mahdollistaa mobiililaitehallinnan, mutta ei sisällä muiden lisenssien tarjoamaa tietoturvaa. Yleisemmin Intune hankitaan osana Microsoft 365 (M365) tai Enterprise Mobility + Security Suite (EMS) -pakettia. Intune on myös saatavilla koulukäyttöön Intune for education -lisenssillä, joka on räätälöity erilaisia koulutustilanteita varten. [20.] [21.]

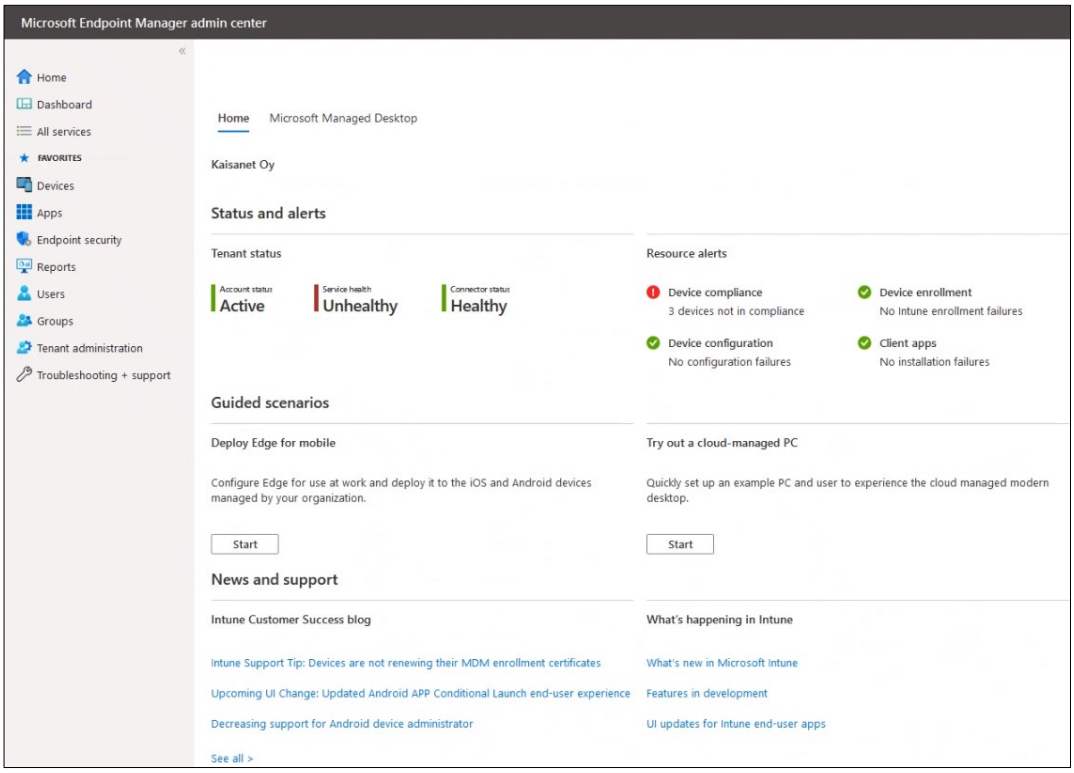
Intune-lisenssit jaetaan pääsääntöisesti käyttäjäpohjaisesti, josta veloitetaan kiinteä kuukausimaksu. Yksi käyttäjälisenssi mahdollistaa mobiililaitehallinnan loppukäyttäjän kaikilla yhteensopivilla laitteilla. Laitekohtainen lisensointi on myös mahdollinen tietyissä käyttötilanteissa, kuten useamman ulkopuolisen henkilön käyttämä infolaite, joka ei tarvitse käyttäjäkohtaista tietoturvaa tai hallintaominaisuuksia. [21.]

Jokaisesta lisenssityypistä on olemassa kolmen kuukauden ilmaiskokeilujakso. POC-käyttöönotossa hyödynnettiin EM+S E5 -kokeilujaksoa, joka sisälsi lisenssin 250 käyttäjälle. Lisenssit määritetään käyttäjille Endpoint Managerin, Azure AD:n tai Powershell-skriptin avulla [21].

3.2 Microsoft Endpoint Manager

Microsoft Endpoint Manager on palvelu, jonka avulla hallitaan useita Microsoftin kehittämiä ratkaisuja, kuten Intune, SCCM ja Azure AD. Endpoint Manager julkistettiin vuoden 2019 lopussa, ja sen tarkoituksena oli yhdistää Intune ja SCCM-tuotepaketti yhden hallintaympäristön alle. [22.]

Microsoft Endpoint Manager -hallintaympäristön kautta voidaan tarkastella ja muokata Intunen erinäisiä komponentteja sekä ylläpitää yrityksen olemassa olevaa laitekantaa. Yleisnäkymän kautta nähdään ympäristön tilanne ja resurssit, jotka saattavat vaatia ylläpitäjän huomiota (kuva 2). Kuvasta 2 näkyy käyttöliittymän vasemmalla puolella oleva välilehtiluettelo, jonka kautta ympäristön eri asetuksiin ja näkymiin pääsee käsiksi. Devices-välilehti avaa esimerkiksi tarkemman laitenäkymän, jonka kautta voidaan hallita mobiililaitteisiin liittyviä määrityksiä.



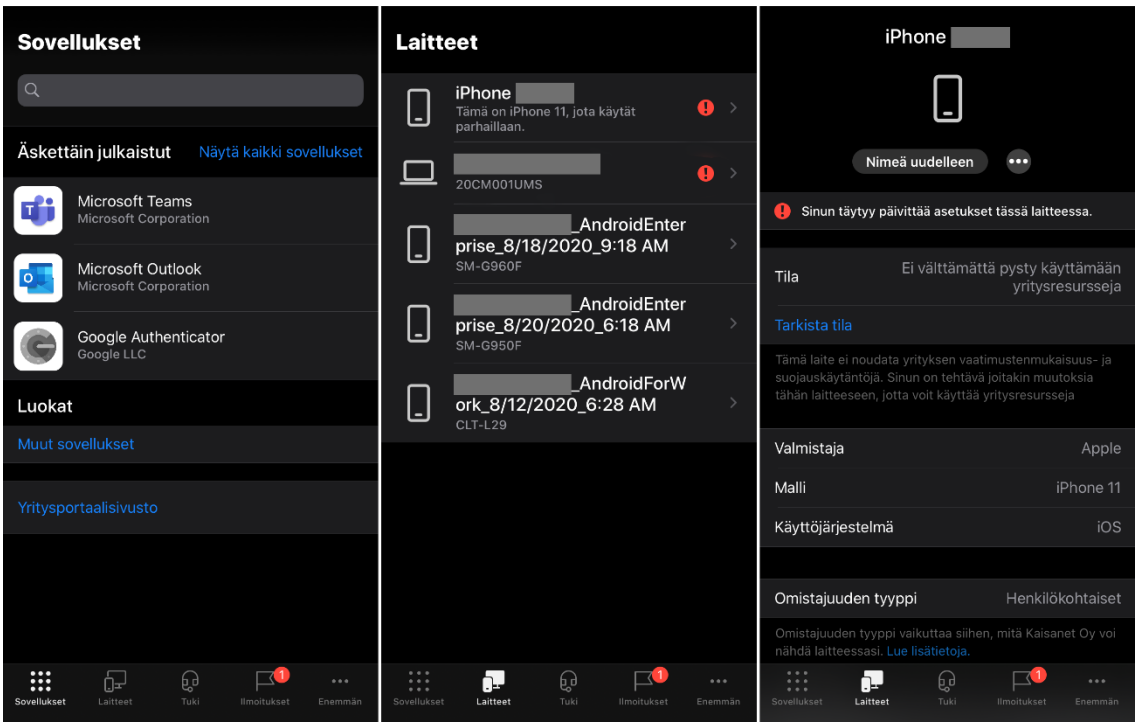
Kuva 2. Endpoint Manager -käyttöliittymän yleisnäkymä. Kuvaa on rajattu jälkikäteen.

3.3 Intune-yritysportaali

Intune-yritysportaali on loppukäyttäjille tarkoitettu itsepalvelusovellus, joka asennetaan mobiililaitteelle. Sovelluksen avulla loppukäyttäjä pystyy suorittamaan erinäisiä toimintoja, kuten rekisteröimään henkilökohtaisen mobiililaitteensa yrityksen Intune-ympäristöön. Yritysportaali ylläpitää myös yhteyden yrityksen ympäristöön ja synkronoi uudet käytänteet sekä sovellukset mobiililaitteelle. Yritysportaaliominaisuuksien saatavuus riippuu osittain yrityksen ylläpitämistä käytänteistä. Loppukäyttäjälle voidaan esimerkiksi antaa mahdollisuus poistaa mobiililaitteensa Intunen hallinnasta yritysportaalin avulla. [23.]

Mobiililaitteen rekisteröimisen jälkeen loppukäyttäjä näkee yritysportaalista yrityksensä julkaisemat sovellukset, loppukäyttäjän omat laitteet sekä yrityksen tukitiedot ja Intune-kohtaiset tukiilmoitukset. Yritysportaalin laiteluettelosta nähdään, noudattaako loppukäyttäjän laitteet Intunessa määriteltyjä käytänteitä. Loppukäyttäjän huomiota vaativat laitteet on merkitty punaisella huutomerkillä (kuva 3). Kuvasarjaa on rajattu jälkikäteen, sekä osa laite- ja käyttäjätiedoista on yliviivattu harmaalla.

Laiteluettelosta pääsee tarkastamaan loppukäyttäjälle rekisteröityjen laitteiden tarkemmat tiedot. Laitenäkymän kautta loppukäyttäjä voi käynnistää manuaalisen synkronoinnin ja tarkastaa, mitkä asetukset täytyy määrittää uudelleen, jotta laite noudattaa yrityksen käytänteitä. Käytänteitä rikkovalta mobiililaitteelta voidaan estää pääsy tiettyihin yritysresursseihin, kunnes rikkeet ovat korjattu.



Kuva 3. iOS kuvankaappaus-sarja Intune-yritysportaalisovelluksesta.

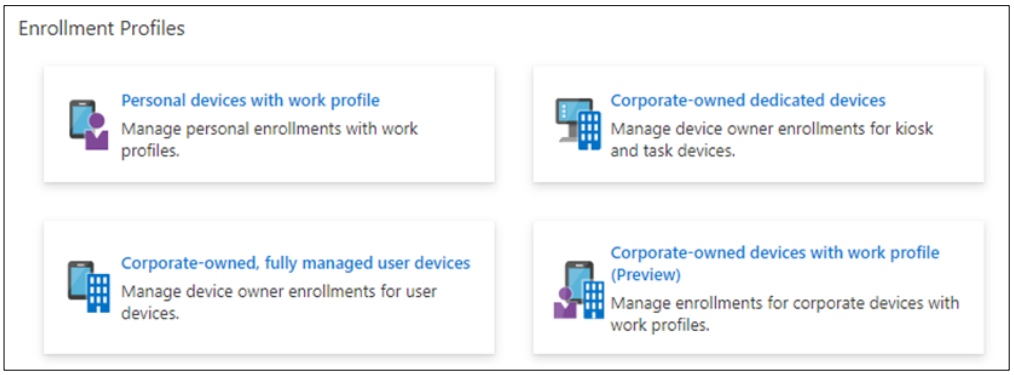
Intune-yritysportaali on myös saatavilla selainpohjaisena palveluna. Selainversion kautta mobiililaitetta ei voida rekisteröidä, mutta sovellusversiosta löydettävät ylläpito-ominaisuudet ovat saatavilla loppukäyttäjälle. Laitteen hallintaprofiilin mukaan loppukäyttäjä voi esimerkiksi etälukita laitteensa tai poistaa sen Intunen hallinnasta. [24.]

4 Mobiililaitteiden rekisteröinti

Mobiililaitteiden rekisteröinti on oleellinen osa mobiililaitehallintaa. Rekisteröintiprosessi antaa mobiililaitteelle MDM-sertifikaatin, jonka avulla hallintaympäristö, tässä tapauksessa Intune, kommunikoi laitteen kanssa [25]. Intune mahdollistaa useita erilaisia rekisteröintitapoja, joiden tarkempi läpikäyminen tässä opinnäytetyössä on rajattu POC-käyttöönoton aikana testattuihin, Intune-rekisteröintiprofiileihin. Luvussa sivutaan myös, miten mobiililaitteiden rekisteröintiä voidaan suoraviivaistaa automatisoimalla Android- tai iOS-laitteen käyttöönotto erilaisten automatisointiratkaisujen avulla.

4.1 Android-profiilit

Intune tarjoaa Android-laitteille neljä erilaista Android Enterprise -rekisteröintiprofiilia, jotka kaikki mahdollistavat eritasoista laitehallintaa (kuva 4). Profiilit voidaan muotoilla seuraaviin ryhmiin: henkilökohtaiset laitteet ja yrityksen omistamat laitteet. Henkilökohtaisten ja yrityksen rekisteröintiprofiilien erot muodostuvat pääasiassa tarjolla olevista hallintaominaisuuksista sekä rekisteröintitavoista.



Kuva 4. Android-rekisteröintiprofiilit Intunessa.

4.1.1 Henkilökohtaiset mobiililaitteet

Intunessa henkilökohtaisten BYOD- tai CYOD-mobiililaitteiden rekisteröinti toteutetaan *Personal devices with work profile* -profiililla. Rekisteröintiprosessi on yksinkertainen, sillä se tapahtuu täysin Intune-yritysportaalin kautta. Henkilökohtaiseen Android-laitteeseen kohdistuu erillinen työprofiili, jonka avulla yrityksen tarjoamat sovellukset ja tietosuojamenetelmät tulevat laitteelle [26]. Työprofiilin hallinnan alla olevat sovellukset tunnistetaan sinisen työsalkkulogon avulla (kuva 5). Työprofiilin kautta loppukäyttäjä voi esimerkiksi käyttää yrityskohtaista Google Play -sovelluskauppaa, josta yrityksen määrittämiä sovelluksia voi käydä lataamassa.

Työprofiili pitää yrityksen ja loppukäyttäjän henkilökohtaiset tiedot erillään toisistaan. Loppukäyttäjän henkilökohtaiset sovellukset ja tiedot eivät siis ole Intunen valvonnassa [26]. Loppukäyttäjä voi myös itse poistaa työprofiilin asetuksien tai yritysportaalin kautta, jolloin kaikki yrityksen sovellukset ja käytänteet poistuvat laitteelta.

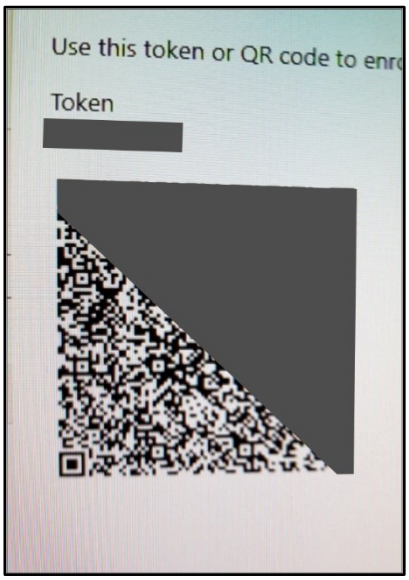
Kuva 5. Henkilökohtaisen Android-laitteen työprofiili-sovellusnäkymä. Työprofiilin jakautuminen riippuu laitevalmistajasta.

Henkilökohtaisen Android-laitteen hallinta on rajallinen muihin rekisteröintiprofiileihin verrattuna. Esimerkiksi automaattiset sovelluspäivitykset voidaan pakottaa vain työprofiilin alla oleviin sovelluksiin [27].

4.1.2 Yrityksen mobiililaitteet

Yrityksen omistamia Android-laitteita voidaan rekisteröidä Intunen hallintaan kolmella erilaisella rekisteröintiprofiililla, jotka kaikki tarjoavat eri tason hallintaa. Näiden profiilien rekisteröintiprosessissa täytyy huomioida, että jo yrityskäytössä oleva Android-laite joudutaan palauttamaan tehdasasetuksiin käyttöönottoa varten. Alustamisvaatimuksen takia olemassa olevan mobiililaitekannan tuominen Intune-mobiililaitehallintaan voi osoittautua hankalaksi, jos mobiililaitteille halutaan saada laajempia hallintaominaisuuksia henkilökohtaiseen rekisteröintiprofiiliin verrattuna. Manuaalinen rekisteröinti tehdään oletuksena QR-koodin tai tokenin avulla (kuva 6), joka generoidaan Endpoint Managerissa. Rekisteröintitavaksi voidaan myös määrittää NFC-tunniste, mutta se vaatii erillisen tunnisteen luontia ja muokkaamista. Rekisteröintikoodi kertoo Android-laitteelle, minkä yrityksen ja MDM-palvelun hallintaan laite on tulossa. [28].

Rekisteröintiprofiilien käyttöönotto voidaan aloittaa usealla eri tavalla. Aloitustapa riippuu yleisesti käytössä olevasta Android-käyttöjärjestelmäversiosta. Esimerkiksi Android 7 -versiosta ylöspäin rekisteröintiprosessi aloitetaan näpäyttämällä uuden tai alustetun Android-laitteen aloitusruutua useampaan kertaan, jonka jälkeen QR-koodi ja muut käyttöönottovaiheet voidaan suorittaa. Henkilökohtaisen mobiililaitteen käyttämän Intune-yritysportaalin sijaan yritysrekisteröintiprofiilit asentavat laitteelle Microsoft Intune -sovelluksen. Microsoft Intune -sovelluksen toimintaperiaate on sama kuin yritysportaalissa, mutta on käyttöliittymältään hieman erilainen. [28].



Kuva 6. Täysin hallitun laitteen manuaalinen rekisteröintiprosessi alkaa esimerkiksi QR-koodin skannaamisesta.

Android-rekisteröintiprofiileista rajoitetun versio on *Corporate-owned, fully managed user devices* -profiili. Profiili kattaa yrityksen omistamat COBO-laitteet, joilla on yksittäinen loppukäyttäjä. Täysin yrityksen hallitsemaan Android-laitteeseen pystyy määrittämään ominaisuuksiltaan monipuolisemmat asetukset ja käytänteet BYOD-laitteeseen verrattuna. Loppukäyttäjä esimerkiksi saa asentaa vain ennalta määriteltyjä sovelluksia yrityksen Google Play -kaupasta. [26].

Täysin hallitun Android-laitteen rajoittuneempi versio on *Corporate-owned dedicated devices* -profiili, johon kuuluvat yrityksen omistamat, yksittäiseen käyttötarkoitukseen kuuluvat COBO-laitteet. Dedicated device -termiä käytetään yleisesti kiosk-laitteiden yhteydessä. Kiosk-tyyppisten Android-laitteiden sovellus- ja asetusoikeuksia voidaan rajoittaa esimerkiksi vain yhteen internet-selaimeen sekä tiettyihin internet-sivustoihin. Rajoitettua Android-laitetta voidaan hyötykäyttää mm. suuren yleisön infolaitteena, joka sallii vain tietyn sovelluksen käyttämisen. [26].

Yrityksen COBO-laitteiden rekisteröintiprofiilit mahdollistavat monipuolisen ja tarkan hallinnan, mutta poistavat laitteista täysin henkilökohtaisen käytön mahdollisuudet. *Corporate-owned devices with a work profile* -profiili sisällyttää yrityksen omistamat COPE-laitteet, joiden hallinta on käytännössä yrityksen fully managed -laitteen ja henkilökohtaisen BYOD-laitteen yhdistelmä. Profiili tarjoaa fully managed -tason hallintaa, mutta samalla pitää BYOD-laitteen tavalla työ- ja henkilökohtaiset tiedot erillään toisistaan. [26].

Yrityksen Android-laitteiden manuaalisen rekisteröinnin lisäksi sama voidaan toteuttaa erilaisten automatisointiratkaisujen kautta, kuten Google Zero Touchin ja Samsung KME:n. Automatisointiratkaisujen avulla laitteen esitiedot voidaan tuoda Intuneen, jotta laitteen käynnistyessä rekisteröinti olisi suoraviivaisempaa. Esitietojen avulla mobiililaite tietää jo entuudestaan, minkä yrityksen hallintaan se on tulossa, joten QR-koodin tai muun tunnisteen lukeminen ei ole tarpeellista. Esitiedoilla voidaan esimerkiksi myös määrittää, kenelle työntekijälle laite on tulossa käyttöön. Automatisointiratkaisujen käyttöönottoa varten valtuutetun jälleenmyyjän täytyy kutsua yrityksen käyttämä tili automatisointiratkaisun palveluun. Kutsun jälkeen yritys voi määrittää jälleenmyyjältä ostamansa Android-laitteet automatisointipalvelun kautta. [6.] [29.]

4.2 iOS-profiilit

Henkilökohtaisen iOS-laitteen rekisteröinti toteutuu loppukäyttäjän näkökulmasta samalla periaatteella kuin henkilökohtaisen Android-laitteen rekisteröinti. iOS-laitteelle asennetaan Intune-yritysportaali, jonka kautta laite rekisteröidään Intuneen. Teknisesti iOS-käyttöjärjestelmä menettelee kuitenkin rekisteröintiprofiilin asennuksen eri tavalla. iOS-laitteelle ladataan ja asennetaan erillinen hallintaprofiili, jonka avulla yrityksen tietosuojamenetelmät ja vaatimusmääritelmät tulevat laitteelle. Hallittua Android BYOD -laitetta mukaillen loppukäyttäjän henkilökohtaiset sovellukset ja tiedot pysyvät poissa Intune-laitehallinnasta. [30.]

iOS-laitteiden automatisointi voidaan toteuttaa Intunen kautta Apple Configurator -ohjelmalla tai Automatic Device Enrollment (ADE, entinen DEP) -palvelun kautta. Apple Configurator -ohjelman avulla suuria määriä iOS-laitteita voidaan ennalta määritellä USB-yhteyden kautta Mac-tietokoneella. Määrityksestä voidaan poistaa esimerkiksi nollatun iOS-laitteen käyttöönottovaiheita, joita loppukäyttäjä joutuu menemään käynnistyksen yhteydessä. Apple Configurator -ohjelman käyttäminen ei vaadi kolmatta osapuolta, mutta on iOS-laitteiden automaattisemman käyttöönoton kannalta hitaampi vaihtoehto. [31.]

ADE toimii palveluna samalla periaatteella kuin Android-laitteiden Google Zero Touch ja Samsung KME. ADE-palvelun avulla Intuneen voidaan rekisteröidä suuri määrä Applen valmistamia mobiililaitteita ilman yksittäisiä laitemäärityksiä. ADE-palvelun kautta rekisteröity mobiililaite voidaan antaa suoraan loppukäyttäjällä, sillä tiedot Intune-ympäristöstä ja hallintatasosta ovat laitteessa valmiiksi. ADE-palvelun käyttäminen vaatii Apple Business Manager- tai Apple School Manager -portaalin käyttöä, joiden avulla kolmannelta osapuolelta ostetut Apple-laitteet liitetään Intune-

ympäristön hallintaan. Intunessa voidaan määrittää ADE-rekisteröintiprofiileja, jotka sisältävät Apple-laitteen käynnistyksen yhteydessä tulevat asetukset ja käytänteet. [1.]

4.3 Mobiililaitteiden rekisteröintirajoitukset

Tiettyjen mobiililaitteiden rekisteröinti voidaan estää tarvittaessa kokonaan Intune-hallintaympäristöstä. Rajauksiin voidaan määrittää sallitut käyttöjärjestelmäversiot, laitevalmistajat ja sallittu laitemäärä per työntekijä. Rajoitukset voidaan määrätä koko yrityksen ympäristöön tai rajata vain tiettyihin käyttäjäryhmiin. Rekisteröintirajoituksien hyödyntäminen on kannattavaa esimerkiksi BYOD-skenaarioissa, joissa halutaan varmistaa, ettei työntekijä yritä rekisteröidä erittäin vanhalla Android-käyttöjärjestelmäversiolla. Microsoft huomauttaa dokumentaatiossaan, että rekisteröintirajoituksia ei kuulu laskea tietoturvaominaisuudeksi, vaan enimmäkseen työntekijöiden ohjaamiseksi. Saastunut mobiililaite pystyy ohittamaan rekisteröintirajoitukset. [32.]

5 Intunen POC-käyttöönotto

Intunen POC-käyttöönotto toteutettiin kesällä 2020. Käyttöönotossa edettiin Centero Oy:n järjestämillä Workshop-päivillä, joiden välillä testiympäristössä kokeiltiin erilaisia määrityksiä ja kerättiin mahdollisia kysymyksiä sekä huomioita seuraavaa kertaa varten. Erilaiset käyttöönottovaiheet dokumentoitiin kuvankaappauksien ja kirjallisten muistiinpanojen avulla, joista muodostuisi Intune-käyttöönoton sisäinen ohjeistus. Ohjeistuksen rakentaminen aloitettiin kesän loppupuolella, kun tärkeimmät Intunen osa-alueet oli testattu.

Tässä luvussa on kiteytetty POC-käyttöönoton tärkeimpiä vaiheita, joiden avulla iOS ja Android-mobiililaitteiden hallintaa pystyi toteuttamaan. Luvun loppupuolella käydään läpi käyttöönoton aikana tehtyjä testejä ja ongelmakohtia, jotka huomioitiin testien aikana. Suurin osa luvussa käsitellyistä asioista toimii samalla periaatteella myös Windows 10 -laitteilla, mutta erillisiä huomioita ei mainita opinnäytetyön rajauksen takia.

5.1 Laite- ja käyttäjäryhmien luonti

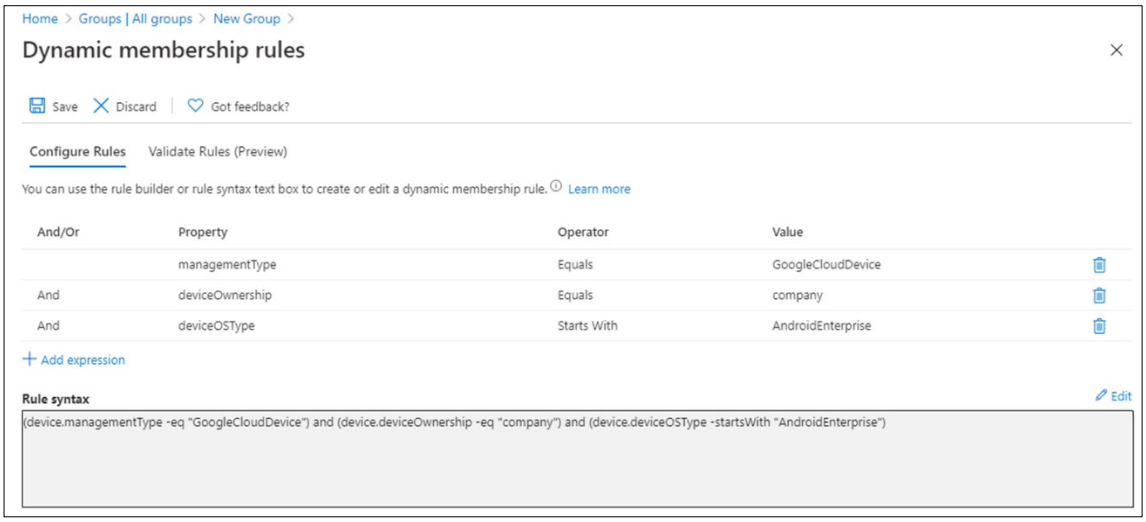
Intune-ympäristön eri laite- ja sovellusmäärityksiä varten tarvitaan varten laite- tai käyttäjäryhmä, johon määritykset voidaan kohdistaa tai tarpeen mukaan poissulkea. Intune-määritykset voidaan myös kohdistaa kaikille yrityksen M365-ympäristössä oleville käyttäjille ja laitteille ilman erillistä ryhmää. [33.]

Ryhmä voi olla tyypiltään määritetty tai dynaaminen. Määritetyssä ryhmässä käyttäjät tai laitteet sijoitetaan manuaalisesti, kun taas dynaamisessa ryhmässä jäsenet liittyvät automaattisesti sääntölausekkeiden perusteella. Laite- ja käyttäjäryhmän käyttäminen riippuu halutusta tavoitteesta. Laiteryhmälle määritetyt asetukset ovat käytössä laitetasolla, ottamatta kantaa laitteen loppukäyttäjistä. Käyttäjäryhmälle määritetyt asetukset sen sijaan liikkuvat käyttäjän mukana eri laitteille. Intune hyödyntää Azure AD -ryhmiä, joten dynaamiset ryhmät vaativat Azure AD Premium -tilauksen [33].

Testiympäristöön tehtiin yksi määritetty käyttäjäryhmä, johon lisättiin käyttöönottotiimin jäsenet. Jokaista rekisteröintiprofiilia varten tehtiin dynaaminen laiteryhmä. Dynaamisen ryhmän sääntölauseke luodaan Rule Builder -työkalulla tai tekstilaatikon avulla, joka mahdollistaa moni-

mutkaisempien sääntölausekkeiden luomisen. Sääntölausekkeet muodostuvat vertailu- ja loogisista operaattoreista, joiden väliin sijoitetaan tässä tapauksessa rekisteröintiprofiileihin liittyvät arvot (kuva 7). Esimerkiksi *Corporate-owned, fully managed user devices* -rekisteröintiprofiilin alla olevat mobiililaitteet ilmestyvät dynaamiseen ryhmään seuraavaan sääntölausekkeen avulla:

(device.managementType -eq "GoogleCloudDevice") and (device.deviceOwnership -eq "company") and (device.deviceOSType -startsWith "AndroidEnterprise")



Kuva 7. Dynaamisen ryhmän sääntönäkymä.

Valmiina oleva sääntölauseke nopeuttaa tulevia Intune-käyttöönottoja, sillä sääntölausekkeet voidaan kopioida suoraan dynaamisen ryhmän lauseketekstilaatikkoon.

5.2 Laitteiden ja sovelluksien liittämisen edellytykset

Jokainen mobiililaitealusta vaatii järjestelmäkohtaisen tilin tai tunnuksen linkittämisen Intune tenanttiin, jotta laitteiden rekisteröinti sekä sovelluksien jakelu sovelluskauppojen kautta olisi mahdollista [34]. Luomis- ja linkitysprosessi vaihteli alustakohtaisesti yksinkertaisesta käyttöönotosta pitempään ja monimutkaisempaan prosessiin.

Intuneen on myös mahdollista integroida ensimmäisen sekä kolmannen osapuolen palveluita, jotka tuovat lisäominaisuuksia ympäristöön. Intune tukee esimerkiksi Teamviewer-etätyöpöytäohjelman integraatiota, jonka avulla etäyhteyden muodostaminen loppukäyttäjän laitteelle on suoraviivaisempaa [35].

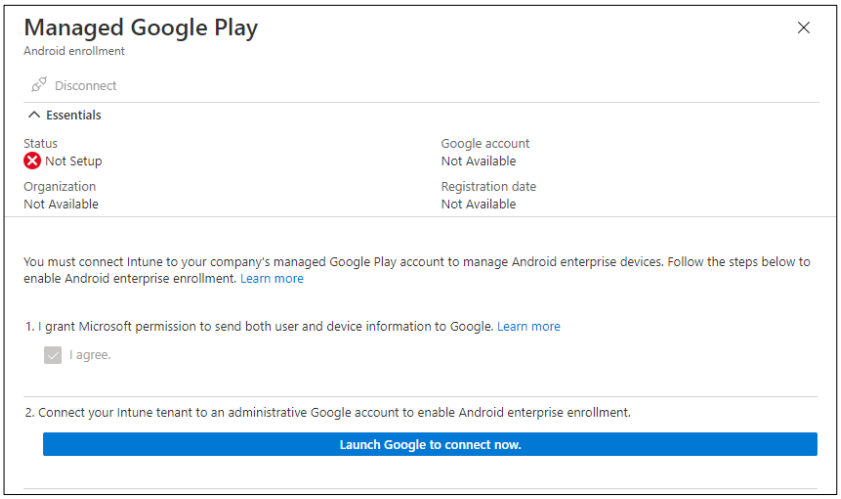
5.2.1 Android

Android Enterprise -hallintaprofiileja ja Google Play -sovelluksia varten tarvitaan Managed Google Play -yritystili. Managed Google Play on Googlen yritystason sovelluskauppa, jonka kautta Intunen hallitsemat Android-laitteet saavat yrityssovelluksensa. Tilin pitäisi olla täysin yritystä varten luotu, jotta jokaisella ympäristöstä vastaavalla asiantuntijalla on oikeus hallita ja julkaista sovelluksia Google Play -hallintaympäristön kautta. Googlen G-Suite-palvelun takana olevaa tiliä ei ole mahdollista käyttää linkittämisen yhteydessä. Mahdollisten yksityisten sovelluksien jakelu vaatii kehittäjätasolla olevaa tiliä. Yksityiseen käyttöön kehitetyt sovellukset täytyy myös olla liitetty saman tilin alle. [36.]

Testiympäristöä varten luotiin uusi Google-yritystili. Yritystilin luomisprosessissa on tärkeää huomioida, että sähköpostiosoitteeksi asetetaan yrityksen verkkotunnuksen alla oleva tili. Yritystilin luomisen jälkeen Google tarjoaa erillisen yritysprofiilin määritystä. Profiilin määritys ei kuitenkaan ole tarpeellinen Intunea varten. [34.]

Vasta luotu yritystili rekisteröidään seuraavaksi Google My Business -palveluun. Google My Business tarjoaa erinäisiä hyötyjä yrityksille, kuten tehokkaamman tilinhallinnan. Tilinhallinnan avulla yritystilille voidaan lisätä esimerkiksi kaikkien Intune-ympäristöstä vastaavien tilit Google Play -sovelluksien hallitsemista varten. Palvelun käyttöönotossa vahvistetaan tili, jota halutaan käyttää rekisteröimiseen. Rekisteröinti vaatii myös yrityksen verkko-osoitteen, yrityksen tiedot ja vähintään toisen tilin, joka nimitetään tilin omistajaksi. [34.]

Rekisteröintivaiheen jälkeen luotu yritystili on valmis Intune-linkitykseen Enroll Devices -osion kautta (kuva 8). Intune avaa erillisen selainikkunan, johon kirjaudutaan yritystilin tunnuksella. Google Play -palvelulle määritetään vielä yrityksen nimi sekä tietosuojavastaavan ja mahdollisen EU-edustajan yhteystiedot. Tietosuojaan liittyvät yhteystiedot voidaan määrittää jälkikäteen tilin asetuksista. Näiden vaiheiden jälkeen Managed Google Play on liitetty onnistuneesta tenanttiin.



Kuva 8. Managed Google Play -tilin määritysikkuna

Managed Google Play -määrityksen aloituksen aikana käytössä oli perus Google-tili, joka oli luotu POC-ympäristöä varten. Workshopin aikana kuitenkin huomattiin, että perustilillä ilmeni käyttöoikeusongelmia, jonka takia Managed Google Play -sovelluskaupan liitäntää ei voitu viimeistellä. Ongelmanselvityksen jälkeen luvun 5.2.1 alussa kerrotut toimenpiteet veivät käyttöönoton loppuun.

5.2.2 iOS

iOS-laitteiden ja sovelluksien liittämisen edellytykset vaativat kaksi erillistä käyttöönottovaihetta. iOS-laitteiden rekisteröinti ja hallinta Intunesta käsin vaatii Apple MDM Push -sertifikaatin ja sovelluksien lisääminen VPP (Volume-Purchased Program Token) -tunnisteen, jolla synkronoidaan Apple Business Manager -portaalista hankittuja sovelluksia. VPP-tunnisteen käyttöönotto ei ole kuitenkaan pakollinen vaihe ilmaisten iOS-sovellusten jakamiseksi. VPP-tunnisteen avulla jaetut sovellukset eivät vaadi loppukäyttäjältä Apple ID -tunnusta niiden asennusta varten. Maksulliset iOS-sovellukset täytyy myös hankkia VPP-tunnisteen kautta.

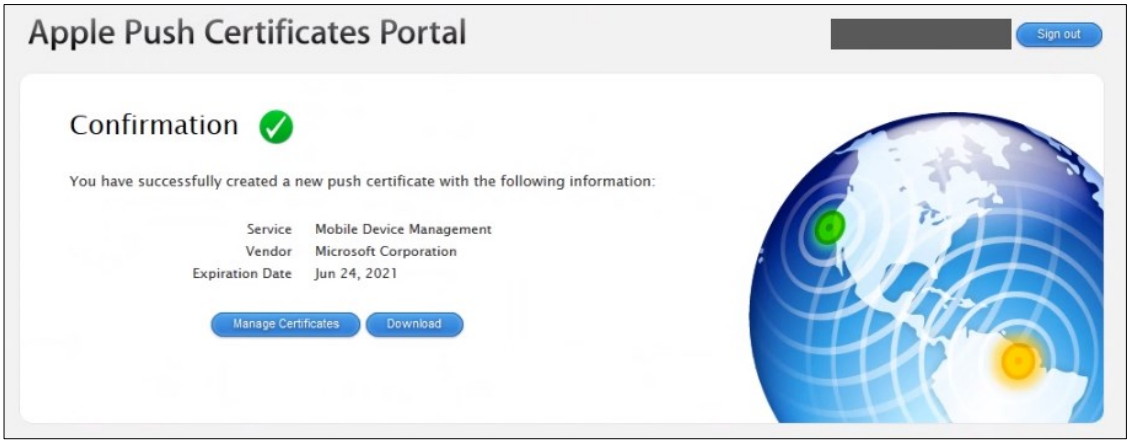
MDM Push -sertifikaatin käyttöönotto oli kahdesta edellä mainitusta vaiheesta suoraviivaisempi. Sertifikaatin konfiguroiminen tehdään Devices-välilehden rekisteröintiosiossa. Intune ohjeistaa sertifikaatin käyttöönottoon viisi erilaista vaihetta, jotka koostuvat käytännössä erilaisten tiedostojen lataamisesta Intunen ja Applen välillä (kuva 10).

Sertifikaatin määrityksessä täytyy ensiksi suostua antamaan Microsoftille lupa lähettää käyttäjä- ja laitetietoja Applelle, jonka jälkeen voidaan ladata CSR (Certificate Signing Request)-tiedosto.

CSR-tiedostoa käytetään luottamussertifikaatin pyytämiseen Apple Push Certificates -portaalista [37].

Seuraavana vaiheena on luoda MDM Push -sertifikaatti. Sertifikaatti tehdään Apple Push Certificates -portaalissa, johon kirjaudutaan käyttöönottoa varten tehdyllä Apple ID -tilillä. Apple Push Certificates -portaalia käytetään Apple Push -sertifikaattien hallinnoimiseen ja uusimiseen erilaisten palveluiden välillä. MDM Push -sertifikaatin voi tehdä millä tahansa Apple ID -tilillä. On kuitenkin hyvä huomioida, että Push-sertifikaatin uusiminen täytyy aina tehdä samalla tunnuksella, jolla käyttöönotto tehtiin ensimmäisen kerran. Uusimisen takia ei ole hyvä idea käyttää henkilökohtaista Apple-tiliä, jos esimerkiksi työntekijä lähtee yrityksestä pois. Apple ID -tilin menettäminen johtaa uuden MDM Push -sertifikaatin luomiseen.

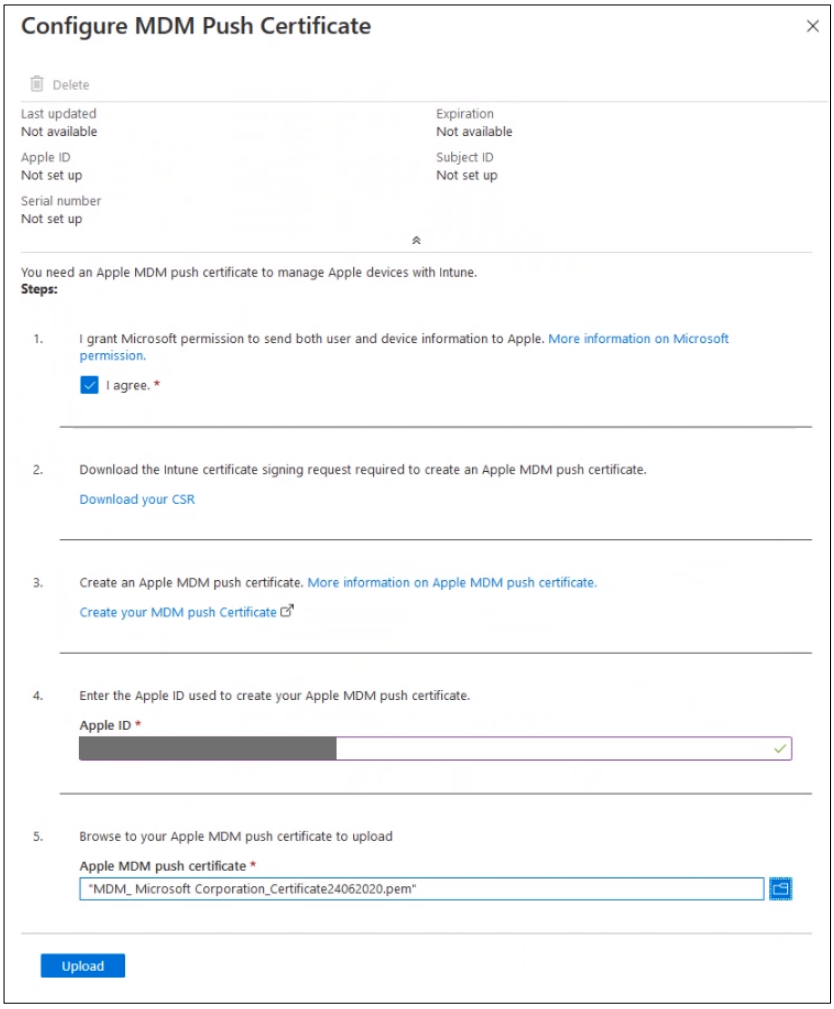
Apple Push Certificates -portaaliin ladataan Endpoint Managerista äskettäin hankittu CSR-tiedosto, jonka jälkeen MDM Push -sertifikaatin luonti on valmis. Apple Push Certificates -portaali ilmoittaa vielä saamansa tiedot vahvistusilmoituksessa, josta MDM Push -sertifikaatin voi ladata (kuva 9).



Kuva 9. Apple MDM Push -sertifikaatti on valmiina ladattavaksi.

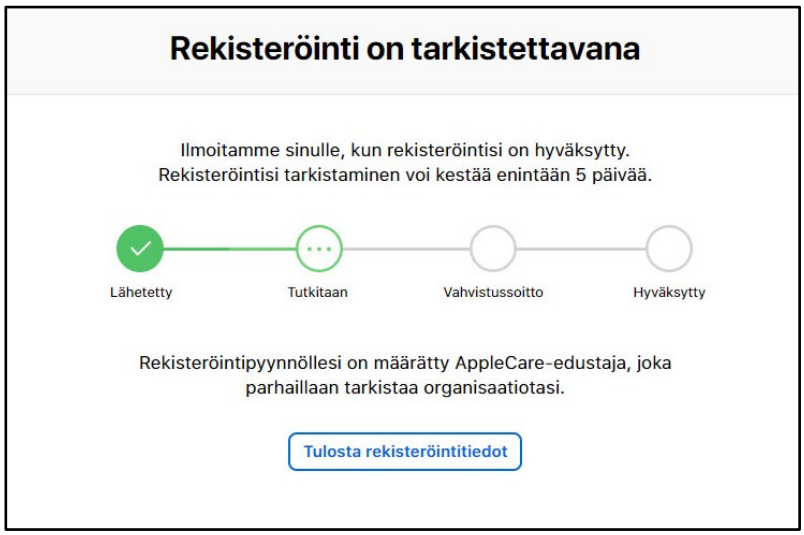
MDM Push -sertifikaatti ladataan portaalista PEM (Privacy Enhanced Mail)-sertifikaattitiedostomuodossa. Apple MDM Push -sertifikaatin käyttöönotosta muodostuvat tiedostot on hyvä tallentaa keskitettyyn paikkaan tulevaisuutta varten. MDM Push -sertifikaatti täytyy uusia kerran vuodessa, jolloin tiedostoon kannattaa nimetä esimerkiksi päivämäärä. CSR-tiedostoa joutuu vain käyttämään ensimmäisen käyttöönoton aikana, jos MDM Push -sertifikaatin uusiminen muistetaan tehdä ajoissa. Muussa tapauksessa myös CSR täytyy uusia. Intune ilmoittaa MDM Push -sertifikaatin vanhenemispäivän ja millä Apple ID -tilillä se on luotu. Varatoimenpiteitä ja dokumentaatiota on kuitenkin hyvä tehdä selkeille asioillekin.

MDM Push -sertifikaatin lataamisen jälkeen käyttöönotossa voidaan siirtyä takaisin Endpoint Managerin MDM Push -määrityksen viimeistelyyn. Määritysikkunan neljänteen kohtaan kirjoitetaan Apple ID -tunnus, jolla MDM Push -sertifikaatti luotiin ja lopuksi valitaan sertifikaattitiedosto (kuva 10). Määrityksien jälkeen MDM Push -sertifikaatin käyttöönotto viimeistellään lataamalla tiedot Intune-ympäristöön.



Kuva 10. Apple MDM Push -sertifikaatin määritysikkuna.

VPP-tunnisteen käyttöönotto aloitetaan Tenant administration -välilehden Connectors and tokens -osiosta, jossa VPP-tunnisteen luominen johdattaa Apple VPP -portaaliin Apple Business -palvelun rekisteröitymistä varten. Rekisteröitymislomakkeeseen annetaan yrityksen, rekisteröijän ja vahvistavan yhteyshenkilön tiedot. Vahvistavan yhteyshenkilön täytyy olla yrityksessä päättävässä asemassa, kuten toimitusjohtaja, joka vahvistaa Apple Business -käyttöönoton AppleCare-edustajalta (kuva 11).



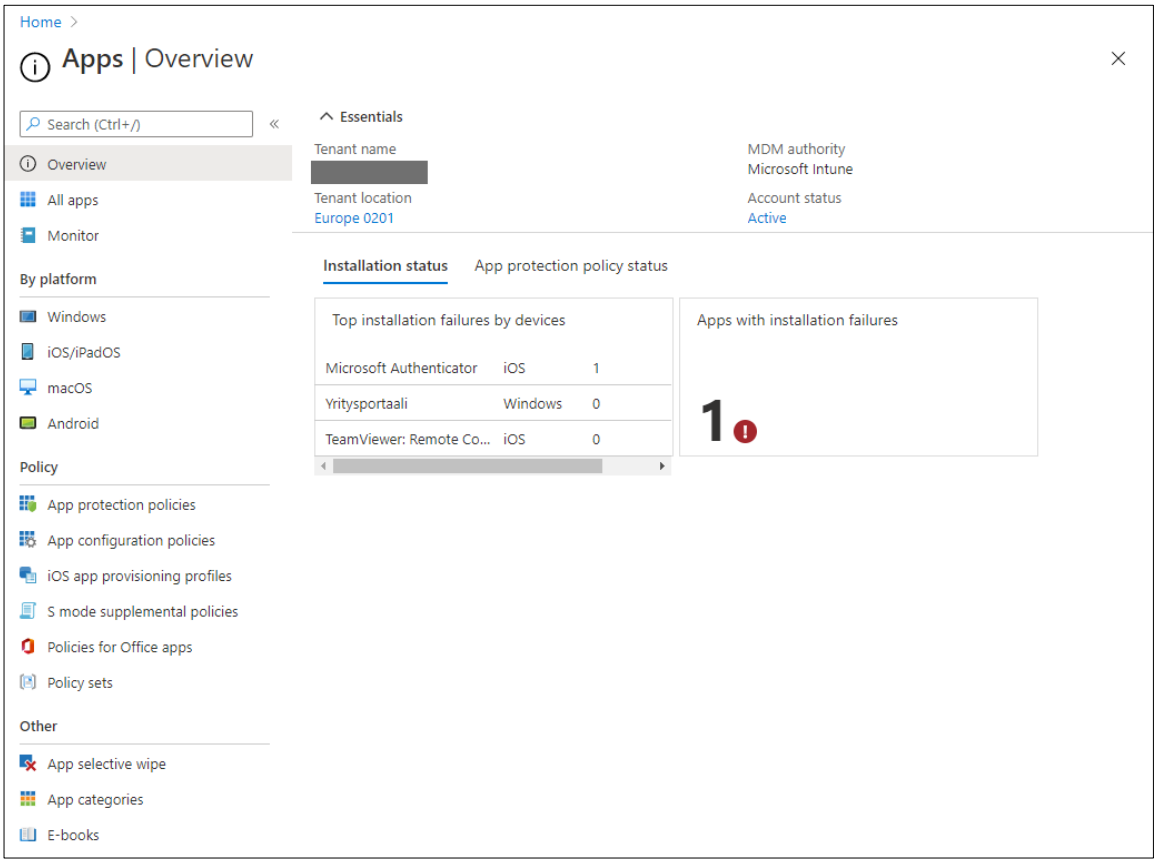
Kuva 11. Apple Business -rekisteröintitietojen syöttämisen jälkeinen ilmoitus.

Rekisteröijä saa käyttöönoton vahvistuksen jälkeen Apple Business -palvelun täydet käyttöoikeudet ja voi delegoida lisää käyttöoikeuksia muille Apple ID -tunnuksille. Apple Business Manager -portaalin Apps and books -osiosta ladataan VPP-tunniste, jotta VPP-käyttöönotto voidaan suorittaa loppuun Endpoint Managerissa. Juuri ladattu VPP-tunniste liitetään Connectors and tokens -osion VPP-linkitykseen. VPP-linkitykselle annetaan vielä nimi ja Apple Business -palvelun pääkäyttäjätunnus, jolla VPP-tunnus ladattiin. VPP-linkityksessä käydään vielä läpi erinäisiä asetuksia, kuten VPP-tilityypin asettaminen, joka on tässä tapauksessa Business. Käyttöönoton jälkeen Intuneen voidaan synkronoida Apple Business Manager -portaalin kautta hankittuja sovelluksia.

5.3 Sovellukset

Endpoint Managerin Apps-valikko pitää sisällään Intunen sovellustason hallintaan liittyvät ominaisuudet. Yleisnäkymästä voidaan tarkistaa, ovatko sovellukset ja sovelluksien tietoturvaan liittyvät APP-käytänteet tulleet hallitulle mobiililaitteelle onnistuneesti (kuva 12).

Käyttöönoton kannalta Apps-valikossa keskityttiin olennaisiin ominaisuuksiin, kuten sovelluksien lisäämiseen ja kohdentamiseen käyttäjä- tai laiteryhmälle. Käyttöönotossa käytiin myös läpi erilaisia sovelluksien käyttökokemusta ja tietoturvaa muokkaavia käytänteitä, jotka muodostaisivat hyvän hallintaperustan sovellustasolla. Sovellustason hallintaa voidaan toteuttaa sovelluskäytäntöjen avulla myös ilman mobiililaitteen rekisteröintiä Intune-ympäristöön.



Kuva 12. Apps-valikon yleisnäkymä.

5.3.1 Sovelluksien lisääminen ja kohdennus

Sovelluskauppojen käyttöönoton jälkeen halutut sovellukset täytyy lisätä Intune-ympäristöön, jotta ne voidaan kohdentaa loppukäyttäjien mobiililaitteille. Sovelluksien lisääminen POC-käyttöönoton aikana tehtiin sovelluskauppojen kautta, jonka jälkeen hankitut sovellukset synkronoidaan Tenant Administration -välilehden Connectors and tokens -valikosta. Sovellukset ilmestyvät synkronoinnin jälkeen Endpoint Managerin sovellusluetteloon, josta sovellukset voidaan lopulta kohdistaa loppukäyttäjille.

Sovelluksen kohdistaminen mobiililaitteelle voidaan tehdä vapaaehtoiseksi tai pakolliseksi. Pakolliseksi määritetty sovellus asentuu heti, kun kohdistetun ryhmän alla oleva loppukäyttäjä rekisteröi mobiililaitteensa Intunen hallintaan. Vapaaehtoiseksi määritetty sovellus on saatavilla loppukäyttäjälle yritysportaalin tai yrityssovelluskaupan kautta. Sovellus voidaan myös määrittää poistettavaksi kohdistettujen käyttäjäryhmien mobiililaitteilta. Testiympäristöön valittiin sovelluksia,

jotka olivat entuudestaan Kaisanetillä käytössä, kuten Microsoft Outlook ja muut käytössä olevat Office-paketin sovellukset.

5.3.2 Sovelluksien tietoturvat

Sovelluksien tietoturvaa voidaan vahvistaa APP (App protection policies) käytäntöjen avulla. APP-käytännöillä määritellään kolme erilaista osa-aluetta: *Data protection, Access requirements* ja *Conditional Launch*. Osa-alueilla voidaan vaikuttaa, miten hallittujen sovelluksien yritystietoihin päästään käsiksi ja miten sitä saadaan jakaa hallittujen sovelluksien sisällä ja ulkopuolella.

Jokaisella mobiililaitealustalle on omat APP-käytänteensä, mutta periaate pysyy samana. APP-hallintaa tukevat sovellukset valitaan valmiiksi olevasta sovelluslistasta, jonka jälkeen jokaisen osa-alueen tarjoamat asetusvaihtoehdot käydään läpi. Sovellukseksi voidaan myös valita itse kehitetty tuote, joka ei ole saatavilla sovelluskaupoista. Sovelluksen täytyy olla integroitu Intune SDK:n kanssa, jotta APP-käytänteitä voi käyttää [38]. Lopuksi APP-käytänteellä kohdistetaan jokin käyttäjäryhmä, jonka laitteille APP synkronoituu.

Testiympäristöä varten tehtiin kaksi oletuskäytäntöä Android- ja iOS-laitteille. Sovelluksiksi valittiin Microsoft Outlook ja Teams. Toimivuuden kokeilun vuoksi käytänteistä muokattiin hyvin rajoittavia, joiden käyttäminen tuotantoympäristössä olisi todennäköisemmin aiheuttanut vastustusta loppukäyttäjien keskuudessa.

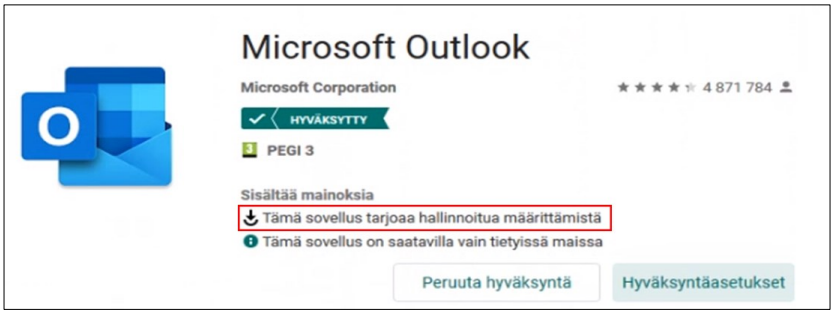
Data protection -osuudessa määritetään, minkälaista suojausta halutaan yritystiedoille, joita Outlook ja Teams tallentaa laitteelle. Oletuskäytänteissä estettiin esimerkiksi sovelluksissa olevien yritystietojen tallentaminen kaikkialle paitsi Microsoftin OneDrive- ja SharePoint-palveluun. Toisena esimerkkinä tiedon siirto muiden ulkopuolisten sovelluksien kautta rajoitettiin vain Intunen hallinnassa oleviin sovelluksiin. Tiedon siirron rajoittaminen estää mm. loppukäyttäjää jakamasta sosiaalisessa mediassa ollutta kuvaa Microsoft Teams -sovellukseen.

Access requirements tarkoittaa asetuksia, jotka vaikuttavat hallittujen sovelluksien pääsyyn. Loppukäyttäjää voidaan esimerkiksi pyytää asettamaan PIN-koodi sovelluskohtaisesti, jos mobiililaitteella ei ole asetettu muuta lukitusta. Oletuskäytännössä sallittiin mm. biometrisen lukituksen käyttäminen PIN-koodin sijaan ja estettiin yksinkertaisen numerokoodin käyttäminen, esimerkiksi neljä peräkkäistä nollaa.

Conditional launch -osiossa määritetään erilaisia ehtoja sovellus- ja laitetasolla. Mitä pitäisi tapahtua, kun loppukäyttäjä on esimerkiksi laittanut sovelluksen PIN-koodin väärin 10 kertaa? Ehdolle valitaan ensiksi asetus sekä arvo ja lopuksi toiminto, joka määrittää, mitä ehdon täyttymisen jälkeen pitäisi tapahtua. Liian monen väärän PIN-koodin syöttämisen seurauksena voitaisiin esimerkiksi nollata PIN tai tyhjentää kyseisen sovelluksen tiedot. Oletuskäytäntöön valittiin PIN-koodin nollaaminen. Oletuskäytännössä estettiin myös esimerkiksi valittujen sovelluksien käyttö rootatulla puhelimella.

5.3.3 Sovelluksien muokkaaminen

Tiettyjä sovelluksia voi muokata ACP (App configuration policies)-käytäntöjen avulla. ACP-käytäntöjen avulla sovelluksen asetuksia voi esiasettaa haluttuun tilaan, joka yksinkertaistaa sovelluksen käyttöönottoa ja vähentää loppukäyttäjän mahdollisia ongelmia. ACP-käytäntöjä tukevat Android-sovellukset voidaan tunnistaa Managed Google Play -sovelluskaupassa seuraavan huomion avulla: *Tämä sovellus tarjoaa hallinnoitua määrittämistä* (kuva 13).



Kuva 13. Android-sovellus, joka tukee ACP-käytäntöä.

Luomisprosessissa valitaan, tuleeko ACP-käytäntö Intuneen rekisteröityneillä mobiililaitteille, vai muokataanko sovellusta laitteelle, joka hyödyntää sovellustason hallintaa ilman Intune-rekisteröintiä. POC-käyttöönoton aikana testattiin kahta Intune-hallittujen laitteille kohdistetun sovelluksen määrittämistä.

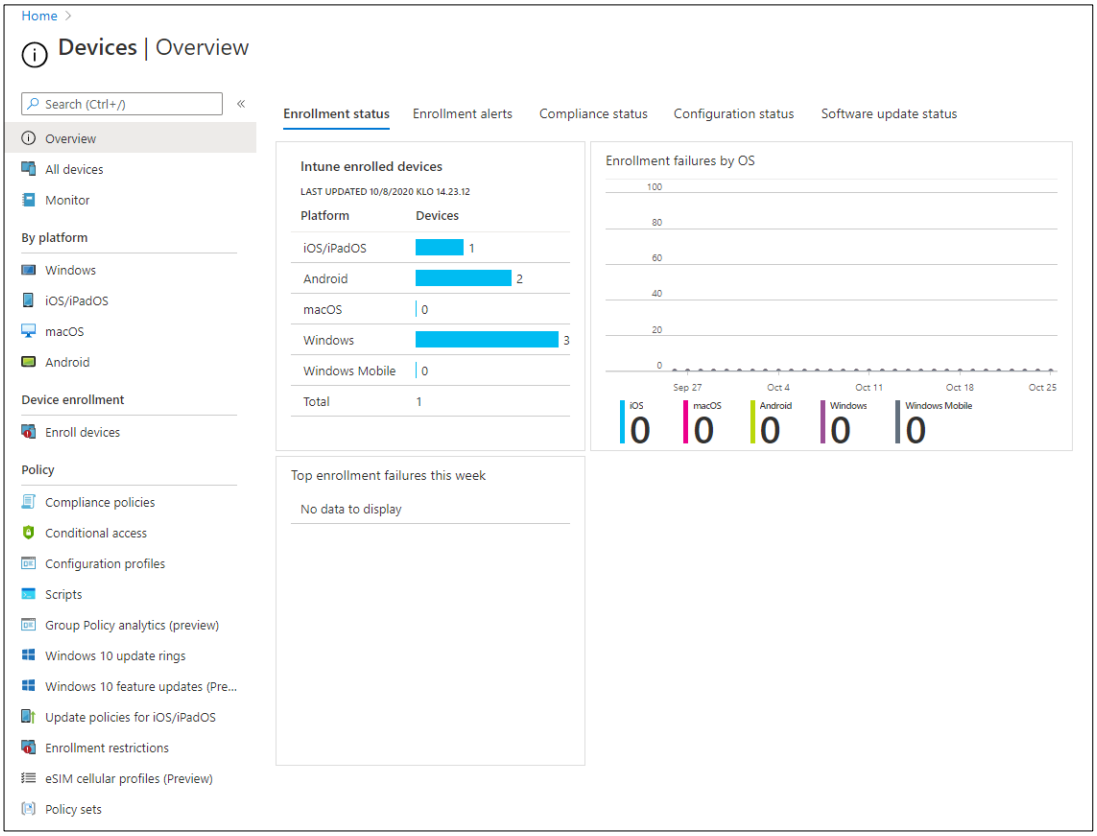
Sovelluksen asetuksien muokkaamisen toteutetaan Intunen configuration designer -editorilla. Vaihtoehtoisesti samat tiedot voidaan syöttää XML-muodossa. Configuration designerin tarjoamat asetukset vaihtelevat sovelluskohtaisesti. Paremmin tuetut sovellukset antoivat graafisen käyttöliittymän tarjolla oleville asetuksille, kun taas esimerkiksi Google Chrome -selaimeen halutut muutokset tehtiin JSON-arvoilla Googlen dokumentaatiota hyväksikäyttäen.

ACP-käytänteiden hyödyntäminen tuli selville mm. rajoitetun hallintaprofiilin alla olevan Android-mobiililaitteen kautta, jolla sai käyttää vain Google Chrome -selainta. ACP-käytännön avulla Chrome-selaimen käyttö rajattiin vain tiettyihin internet-sivustoihin ja pääsy Chromen asetuksiin estettiin.

5.4 Laitteet

Endpoint Managerin Devices-valikko sisältää mobiililaitekohtaiset Intune-ominaisuudet. Yleisnäkymästä nähdään erinäisiä tilanne- ja hälytyskatsauksia, kuten rekisteröityneiden mobiililaitteiden jako eri käyttöjärjestelmien ja rekisteröitymisen onnistumisen perusteella (kuva 14).

Käyttöönoton kannalta Devices-valikon tärkeimmät osiot olivat laiterekisteröitymiseen ja erinäisiin laitekäytänteisiin liittyvät asetukset. Laitekäytäntöjen avulla rekisteröityneen mobiililaitteen ominaisuuksia voidaan hallita rekisteröintiprofiilin perusteella. Laitekäytännöt ovat käytännössä hyvän mobiililaitehallinnan perusta. Testiympäristössä eri rekisteröintiprofiileille tehtiin asetus- ja vaatimuskäytänteitä, jotka muokkaavat ja ylläpitävät hallitun mobiililaitteen asetuksia.



Kuva 14. Devices-valikon yleisnäkymä.

5.4.1 Laitekohtaiset asetuskäytänteet

Intunessa laitekohtaisten asetuskäytäntöjen (Configuration policies) avulla mobiililaitteen erilaisia ominaisuuksia ja asetuksia voidaan ottaa päälle tai pois käytöstä. Intunessa asetuskäytänteet on jaettu erillisiin konfiguraatioprofiileihin, käyttöjärjestelmä- ja rekisteröintiprofiilikohtaisesti. Intune-konfiguraatioprofiili voi käsitellä esimerkiksi langattoman lähiverkon automaattista asettamista tai sähköpostiasetuksien muokkaamista. Mobiililaitteelle kohdistetut asetuskäytänteet tulevat voimaan pakollisesti, joten loppukäyttäjälle ei ole vaikutusvaltaa muuttaa niitä jälkeenpäin.

POC-käyttöönotossa testattiin *Device Restrictions* -konfiguraatioprofiilia Android- ja iOS-laitteille. *Device Restrictions* on yleisen hallinnan kannalta tärkeä Intune-konfiguraatioprofiili, sillä se pitää sisällään erilaisia tietoturvaan vaikuttavia asetuksia ja ominaisuuksia. Henkilökohtaisille sekä täysin hallituille laitteille tehtiin omat *Device Restrictions* -asetuskäytänteet, jotka voisivat olla oletuksena kaikille yrityksen mobiililaitteille.

Henkilökohtaisen Android-laitteen Intune-asetuskäytänteiden vaikutusalue pysyy työprofiilin sisäpuolella, joten huomioonotettavia *Device Restrictions* -asetuksia oli vähemmän täysin hallittuun Android-laitteeseen verrattuna. Työprofiilin käyttämiseen vaadittiin salasana, ja tietojen kopioiminen työprofiilin hallinnassa olevista sovelluksista ulkopuolelle estettiin. Pakotetusti päälle laitettiin myös Managed Google Play -sovelluskaupan *Verify Apps* -ominaisuus, joka skannaa asennettavien sovelluksien turvallisuuden.

Täysin hallitussa Android-laitteessa muokattavien *Device Restrictions* -asetuksien määrä oli huomattavasti suurempi, sillä työprofiilirajausta ei ollut. Täysin hallitulle Android-laitteelle asetettiin esimerkiksi automaattinen käyttöjärjestelmän päivitys ja pakollinen näytönlukituksen salasana. *Corporate-owned dedicated devices* -rekisteröintiprofiilia varten tehtiin vielä erillinen *Devices Restrictions* -asetuskäytäntö, jossa kaikki mahdollinen estettiin ja sallittiin vain yhden sovelluksen automaattinen suorittaminen. Estojen jälkeen mm. USB-tiedonsiirto ja Android-tilapalkin käyttö ei enää ollut mahdollista.

iOS-laitteille tehtiin yksi *Devices restrictions* -asetuskäytäntö, pienemmän testiskenaariomäärän vuoksi. Testeissä käytiin läpi vain loppukäyttäjän rekisteröimä iOS-laite yritysportaalin kautta eli BYOD-skenaario. Asetuskäytäntöön asetettiin mm. pakollinen näytönlukituksen salasana, joka ei henkilökohtaisella iOS-laitteella ollut rajattuna vain työprofiilin kaltaisen ympäristön sisälle.

5.4.2 Laitekohtaiset vaatimuskäytänteet

Intunen laitekohtaisilla vaatimuskäytänteillä (Compliance policies) tarkistetaan mobiililaitteiden asetuksien tilaa. Mobiililaite voi olla *Compliant*- tai *Not Compliant* -tilassa. Intune-vaatimuskäytänteet eivät muuta mobiililaitteen asetuksia ilman loppukäyttäjän päätöstä. Intune-vaatimuskäytänteiden sivuuttaminen laittaa mobiililaitteen *Not Compliant* -tilaan, kun taas asetuksien muuttaminen käytänteiden mukaiseksi antaa mobiililaitteelle *Compliant*-tilan. Compliance-tilatietoa voidaan hyödyntää mm. raportoinnissa, ja sen perusteella voidaan myös estää esimerkiksi hallittujen sovelluksien käytön. Testiympäristön käyttöönotossa rajoittavia Compliance-toimenpiteitä ei kuitenkaan tehty.

Ennen erillisten Intune-vaatimuskäytänteiden luontia on hyvä käydä läpi Endpoint Managerista löytyvät yleisasetukset. Intune-vaatimuskäytänteiden yleisasetukset sisältävät kolme määritettävää kohtaa, jotka kohdistuvat jokaiseen rekisteröityyn mobiililaitteeseen:

- Meneekö ilman vaatimuskäytäntöä oleva mobiililaite *Not Compliant* vai *Compliant*-tilaan?
- Käytetäänkö tehokkaampaa iOS jailbreak -tarkistusta?
- Kuinka pitkän ajanjakson aikana mobiililaitteen täytyy ilmoittaa vaatimuskäytänteiden tila, jotta se pysyy *Compliant*-tilassa?

Intunessa ei yleisesti ilman vaatimuskäytäntöä olevaa mobiililaitetta haluta muiden vaatimuskäytäntöä noudattavien mobiililaitteiden joukkoon, joten *Not Compliant* -raportointi jätettiin päälle. Tehokkaampi iOS jailbreak -tarkistus ei koettu olennaiseksi asetukseksi ainakaan testiympäristössä. Intune mainitsee jailbreak-tarkistuksen vievän myös enemmän virtaa iOS-laitteilta. Vaatimuskäytänneraportoinnin ajanjakso pidettiin 30 päivän oletuksena. Jos mobiililaite on esimerkiksi poissa käytöstä loppukäyttäjän pidemmän loman takia, niin mobiililaite menee *Not Compliant* -tilaan, mutta palautuu *Compliant*-tilaan internet-yhteyden palatessa.

Not Compliant -tila ilmoitetaan loppukäyttäjälle yritysportaali-sovelluksen laiteluettelossa punaisella huutomerkillä. Yritysportaalin tarkemmasta laitenäkymästä loppukäyttäjä näkee, mitkä asetukset pitäisi muuttaa. *Not Compliant* -tilalle voidaan myös määrittää erillisiä toimintoja vaatimuskäytänteen luomisen aikana. Testiympäristöä varten vaatimuskäytännöille luotiin viestipoh-

jat, jotka lähetetään loppukäyttäjälle sähköpostitse. Viestipohjassa on käyttöjärjestelmäkohtaisesti kerrottu, mitkä asetukset loppukäyttäjän pitäisi tarkistaa, jotta mobiililaite menee takaisin *Compliant*-tilaan.

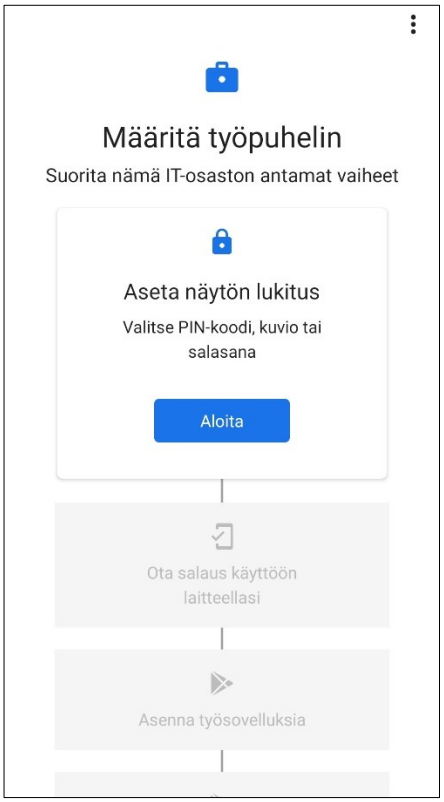
Testiympäristöön luoduille Intune-vaatimuskäytänteille asetettiin samankaltaiset tietoturvavaatimukset, kuten salasanan vaatimisen mobiililaitteen avaamisen yhteydessä. Intune-vaatimuskäytänteen avulla henkilökohtaisten Android-laitteenkin lukitus saatiin parempaan kuntoon, sillä sitä ei voinut pakottaa Intune-asetuskäytänteen avulla.

5.5 Ympäristön testaus

POC-käyttöönoton aikana tehdyt testit suoritettiin Kaisanetin varastolaitteilla. Testilaitekanta koostui useammasta Android-laitteesta ja kahdesta iOS-laitteesta. Android-laitteiden määrän oli tarpeen olla suurempi, jotta jokaista rekisteröintiprofiilia voitaisiin testata ilman jo kokeilussa olevan Android-laitteen nollaamista. iOS ja Android-laitteiden testit koostuivat lähinnä erilaisista sovellus- ja laitekäytänteiden määrityksistä, jonka jälkeen niiden toiminnallisuutta kokeiltiin mobiililaitteilla. Intunen tarjoamia ylläpito-ominaisuuksia käytiin myös testien aikana läpi. Testeistä ilmentyneet ongelmat kerättiin ja selvitettiin Centero Oy:n kanssa eteenpäin, jos niihin ei löydetty ratkaisua.

Laitekohtaisten käytäntöjen testaamisen aikana havaittiin synkronointiin liittyvää ongelmaa. Täysin hallitun Android-laitteen käyttöönotossa pitäisi ilmestyä erilaisia asetusvaatimuksia, jotka loppukäyttäjän täytyy suorittaa (kuva 15). Testilaitteelle ilmestyi kuitenkin vain oletusvaiheet: työsovelluksien asennus ja laitteen rekisteröityminen. Centero Oy:n kanssa pidetyn tilannetarkastuksen yhteydessä syy saatiin kuitenkin selville.

Vaatimuskäytänne oli kohdistettu dynaamiseen laiteryhmään, jonka seuraamuksena Android-testilaite ei voinut saada sille määritettyjä käytäntöjä työpuhelimen määritysvaiheessa. Dynaaminen laiteryhmä osaa liittää laitteen jäseneksi vasta sitten, kun mobiililaitteen käyttöönottovaiheet on suoritettu loppuun. Ongelmanselvityksen kautta tuli selväksi, että dynaamisille ryhmille määritetyt käytänteet synkronoituvat laitteille viiveellä, kun taas valmiiksi määritettyjen ryhmien synkronointi tapahtui nopeammin. Määritetyn käyttäjäryhmän kohdistamisen jälkeen vaatimuskäytänne toimi oikein.

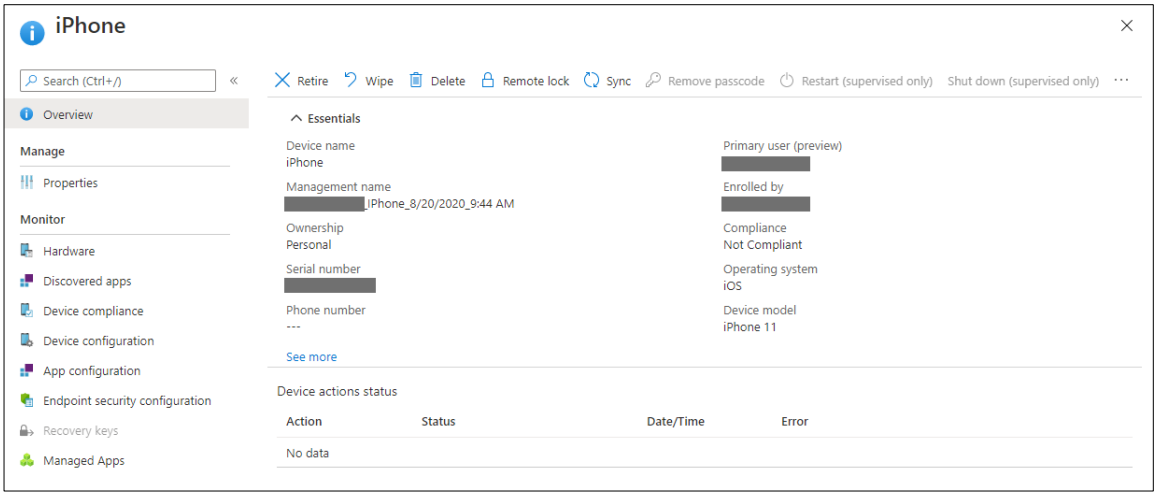


Kuva 15. Täysin hallitun Android-laitteen *Määritä työpuhelin* -käyttöönottovaihe.

Dynaamisten ryhmien synkronointiviiveen takia yritysportaali-sovellus ilmoitti henkilökohtaisen mobiililaitteen rekisteröinnin jälkeen, ettei vaatimuskäytänteitä ole määritetty, vaikka sovellus vaati loppukäyttäjää päivittämään mobiililaitteen asetukset. Synkronointiviiveen kestoksi katsottiin noin viisi minuuttia, jonka jälkeen mobiililaitteelle kohdistetut sovellukset ja käytänteet alkoivat ilmestymään push-ilmoituksina.

Intune-ympäristön testaamisessa havaittiin myös ongelmia yritysportaali-sovelluksen vaatimuskäytännetarkistuksessa. Yritysportaali saattoi ilmoittaa, että juuri rekisteröity testilaite on yhteensopiva yrityksen käytänteiden kanssa, vaikka kaikkia testilaitteen asetuksia ei ollut määritetty niiden mukaisesti. Käytänteiden tila tarkistettiin myös Endpoint Managerin laitekohtaisesta hallintanäkymästä, jossa kaikki määritykset näyttivät vihreää. Ongelmaa lähdettiin ratkomaan uudelleenmäärittämällä käytänteiden ongelmakohtia. Esimerkiksi vaaditun salasanatyypin muuttaminen *Device Default* ja *At least numeric* välillä ja salasanan vähimmäispituuden asettaminen. Henkilökohtaisen iOS-testilaitteen kanssa käytänteiden toimivuus oli Android-testilaitteisiin verrattuna parempi. Vaaditut asetukset, kuten lukituskoodin asettaminen, tulivat suoraan kotinäytön eteen.

Rekisteröityneiden testilaitteiden ylläpito tapahtuu Endpoint Managerin Devices-valikon kautta. Devices-valikon laiteluettelosta valitaan tietty laite, jonka jälkeen saadaan näkyviin laitekohtainen hallintanäkymä. Laitekohtaisessa hallintanäkymässä voidaan seurata käytäntöjen ja hallittujen sovelluksien tilaa sekä suorittaa tiettyjä ylläpitotoimintoja, kuten tehdasasetuksien palauttaminen tai Intune-synkronointi (kuva 16). Ylläpitotoiminnot vaihtelevat rekisteröintiprofiilin ja käyttöjärjestelmän perusteella.



Kuva 16. Mobiililaitteen hallintanäkymä.

Testatut ylläpito-ominaisuudet todettiin toimiviksi. Esimerkiksi tehdasasetuksien palauttaminen Endpoint Managerista käsin täysin hallitulle Android-testilaitteelle tapahtui lähes hetkessä. Jos testilaite oli juuri sammutettuna, niin tehdasasetuksien palauttaminen lähti käyntiin heti internetyhteyden palautuessa. Testilaitteille kokeiltiin myös muita ominaisuuksia, kuten *Retire*, joka poistaa vain yrityskohtaiset tiedot mobiililaitteelta, tai *Sync*, joka synkronoi mobiililaitteelle kaikki uudet ja päivitetyt sovellukset sekä käytänteet.

6 Pohdinta

Intune mahdollistaa mobiililaitteiden monipuolisen ja keskitetyn hallinnan. Kokonaisuudessa POC-käyttöönotto eteni kesän aikana hyvää tahtia ja tarpeelliset testit saatiin tehtyä. POC-käyttöönoton perusteella Intune otettiin käyttöön Kaisanetin tuotantopuolella, josta se pääsee jatkokehitykseen testiympäristön pohjalta. Tehdasasetuksien palauttamista vaativien rekisteröintiprofiilien käyttäminen jää todennäköisesti pieneksi olemassa olevien laitekantojen takia. Henkilökohtaisten mobiililaitteiden hallintaominaisuudet ovat skaalaltaan pienempiä, mutta mahdollistavat silti tärkeitä vaatimuksia, kuten näytönlukituksen asettamisen.

Käyttöönoton ohjeistuksen rakentaminen osoittautui suureksi työksi, sillä Intune on ominaisuuksiltaan valtava. Centeron workshop-päivien ja testien aikana kerätyillä muistiinpanoilla sekä kuvankaappauksilla ohjeistusta saatiin pitkälle, mutta dokumentaation kerääminen olisi ainakin oman panostuksen kannalta voinut olla vielä laajempaa. Tietyt käyttöönoton osa-alueet jouduttiin tarkastamaan uudelleen ohjeistuksen työstämisen aikana. Intunen jatkuvasti kehittyvät ja uudet ominaisuudet aiheuttivat myös muutoksia ohjeistuksessa ja vaativat tietyissä tapauksissa uudelleen testauksia. Jatkuvan kehityksen alla olevan palvelun ohjeistusta joutuu välttämättä päivittämään aika ajoin.

Intune-ympäristöön ylläpitoon liittyviä aihepiirejä ei käsitelty POC-käyttöönoton aikana laitekohtaisen hallintaominaisuuksien lisäksi. Selvitettäväksi työksi jää esimerkiksi Intune-ympäristön käyttöoikeudet ryhmittäin ja miten ne jaotellaan tietoturvan kannalta järkevästi. Ylläpito-osuudelle täytyy myös rakentaa oma ohjeistus.

Intune-ympäristön käyttöönoton monimutkaisuus riippuu hallintaan tulevasta laitekannasta ja sen myötä selvitettävistä asioista. Käyttöönoton ohjeistuksen rakentamisen yhteydessä huomioitiin esivalmistelujen tärkeys, joka tulee ensimmäisenä vaiheena Intune-käyttöönotossa vastaan. Perusteellisen esivalmistelun kautta alkava käyttöönotto tulee etenemään sujuvammin, kun jokaista osa-aluetta ei tarvitse lähteä selvittämään erikseen käyttöönoton aikana.

Microsoftilla on vielä kehitettävää Intunen käyttökokemuksessa, vaikkakin POC-käyttöönotto sujui lähes mutkattomasti ja tärkeimmät ominaisuudet todettiin toimiviksi. Endpoint Manager on käyttöliittymältään ja ominaisuuksiltaan suurimmaksi osaksi laadukkaasti toteutettu, mutta käyttöönoton aikana huomioitiin tiettyjä parannuksen kohteita. Eri osa-alueiden raportointi oli usein

huomattavasti myöhässä verrattuna mobiililaitteiden varsinaiseen sovellus- ja käytännetilaan tai ei päivittynyt laisinkaan.

Endpoint Managerin luettelotaulukkojen järjestämisvaihtoehdot eivät ole myöskään johdonmukaisia. Esimerkiksi sovellusluetteloa voi vain järjestää tiettyjen tietosarakkeiden perusteella. Sovellustyypin perusteella järjestäminen olisi mm. hyödyllinen lisäys, joka täytyy tällä hetkellä tehdä erillisen asetusikkunan kautta.

Mobiililaitteiden keskitetyssä hallinnassa on tärkeää miettiä tietoturvan ja käytettävyyden rajoja. Liian aggressiiviset käytänteet voivat haitata loppukäyttäjän työskentelyä ilman varsinaisia hyötyjä tietoturvan kannalta ja liian kevyet käytänteet päinvastoin. Yksinkertaisemmat oletusvaatimukset, kuten näytönlukituksen vaatiminen on hyvä lähtökohta, jonka pohjalta voi lähteä miettimään yrityksen näkökulmasta tärkeitä kipukohtia. Voidaan esimerkiksi pohtia sovellusten tiukempia käytänteitä, jotta kriittiset yritysresurssit pysyvät paremmin turvassa.

Työn aihepiiri oli aloitusvaiheessa suurimmilta osin tuntematon. Intunea ja mobiililaitehallinnan maailmaa olin ehtinyt aikaisemmin pintaraapaisemaan teoreettiselta puolelta, mutta varsinainen käytännön työ ja sen kautta tarkempi tutkiminen opetti paljon, kehittäen samalla omaa ammatillista osaamista. Dokumentoinnin tärkeys korostui entisestään käyttöönoton aikana. Hyvä dokumentointimateriaali vähentää pyörän uudelleen keksimisen tarvetta ongelman tai muun selvitettävän asian yhteydessä.

7 Yhteenveto

Työn alkuosiossa perehdyttiin mobiililaitteiden etähallinnan yleiskäsitteisiin ja erilaisiin laitepolitiikkaratkaisuihin. Mobiililaitteiden etähallinnan mahdollistavat tuotteet voidaan lajitella näiden käsitteiden alle, jonka kautta hallintaominaisuuksien taso saadaan tietoon. Hallintaominaisuuksiin voi esimerkiksi kuulua mobiililaitteen asetuksien ja sovelluksien määrittäminen. Laitepolitiikkaratkaisujen avulla tiedetään mobiililaitteiden omistajuuden ja hallinnan taso. Henkilökohtaisten mobiililaitteiden kohdalla todettiin tietoturvaan liittyviä riskitekijöitä vähäisen laitesuojaamisen takia. Yrityksen omistamat mobiililaitteet takaavat paremman tietoturvan, mutta rajaavat työntekijöiden käyttökokemusta.

Seuraavana työssä tutustuttiin Microsoft Intune -palvelun perusteisiin ja sen osa-alueisiin. Intunen avulla mobiililaitteita voidaan etähallita sovellus- ja laitetasolla Azure-pilvipalvelusta käsin. Intune on kokenut suurta kasvua lähivuosina maailman siirtyessä mobiilimpaan ympäristöön. Kasvun myötä Intune on jatkuvassa kehityksessä ja saa uusia ominaisuuspäivityksiä kuukausittain.

Mobiililaitteiden etähallinnan toteutuminen vaatii mobiililaitteen rekisteröintiä hallintapalveluun. Mobiililaitteiden rekisteröintitapa riippuu laitteelle halutusta rekisteröintiprofiilista. Henkilökohtaiset mobiililaitteet rekisteröidään Intune-palveluun erikseen ladattavan yritysportaali-sovelluksen kautta, josta loppukäyttäjä saa laitteelle kohdistetut käytänteet ja sovellukset. Yrityksen omistamat eli täysin hallitut mobiililaitteet rekisteröidään QR-koodin tai muun tunnisteen avulla erillisen käyttöönottoprosessin kautta. Täysin hallitun mobiililaitteen rekisteröintiprosessia voidaan myös yksinkertaistaa erilaisten automatisointiratkaisujen avulla.

Työn käytännön osuus koostui Intune-testiympäristön käyttöönoton erinäisistä vaiheista ja ympäristön testaamisesta. Käyttöönoton alkuvaiheessa täytyi tehdä käyttöjärjestelmäkohtaisia edellytystoimenpiteitä, jotta Android- ja iOS-sovelluksien ja laitteiden lisääminen Intune-ympäristöön olisi mahdollista. Edellytystoimenpiteiden jälkeen testiympäristöön tehtiin sovellus- ja laitekohtaisia määrityksiä, joiden toiminnallisuutta kokeiltiin testilaitteistolla. Intunen ylläpito-ominaisuuksien perustoiminnallisuutta käytiin myös läpi.

Intune-testiympäristön käyttöönoton ja suoritettujen testien perusteella palvelu todettiin toimivaksi. Intune otettiin työn jälkeen Kaisanetillä käyttöön ja jatkokehitykseen. Pohdinnassa otettiin huomioon Intunen heikkouksia, kuten raportoinnin hitautta ja puutteellisuutta. Intune oli työn aiheena opettavainen ja toi esille paljon uutta mobiililaitteiden hallinnasta.

Lähteet

[1] Microsoft. Enroll iOS/iPadOS devices - Automated Device Enrollment. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-ios. Haettu 28.10.2020

[2] Microsoft. What is Azure Active Directory? 2020; Saatavilla: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis. Haettu 01.11.2020

[3] Hein D. BYOD vs. CYOD vs. COPE: What's the Difference? 2019; Saatavilla: https://solutionsreview.com/mobile-device-management/byod-vs-cyod-vs-cope-whats-the-difference/. Haettu 14.10.2020

[4] Shahane R. BYOD vs CYOD vs COBO vs COPE - Know the Difference. 2020; Saatavilla: https://blog.scalefusion.com/byod-vs-cyod-vs-cobo-vs-cope/. Haettu 14.10.2020

[5] Continuum. What is Mobile Device Management (MDM)? 2019; Saatavilla: https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm. Haettu 08.10.2020

[6] Microsoft. Automatically enroll Android devices using Samsung's Knox Mobile Enrollment. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/android-samsung-knox-mobile-enroll. Haettu 21.10.2020

[7] Valia H. What is Mobile Application Management (MAM). 2019; Saatavilla: https://www.ilantus.com/blog/what-is-mobile-application-management-and-why-is-it-important/. Haettu 08.10.2020

[8] Smartsheet. All about Mobile Device Management. n.d; Saatavilla: https://www.smartsheet.com/mobile-device-management. Haettu 08.10.2020

[9] Rouse M. What is proof of concept (POC)? 2018; Saatavilla: https://searchcio.techtarget.com/definition/proof-of-concept-POC. Haettu 01.11.2020.

[10] Microsoft. What is Configuration Manager? 2019; Saatavilla: https://docs.microsoft.com/en-us/mem/configmgr/core/understand/introduction. Haettu 01.11.2020.

[11] Hanna T. Understanding the Difference Between MDM, MAM, EMM, and UEM. 2018; Saatavilla: https://solutionsreview.com/mobile-device-management/understanding-the-difference-between-mdm-mam-emm-and-uem/. Haettu 08.10.2020

[12] Triuvare Oy. Miksi mobiililaitteita pitäisi hallita keskitetysti? 2018; Saatavilla: https://materiaalit.triuvare.fi/artikkelit/mobiililaitteita-pitaisi-hallita-keskitetysti. Haettu 08.10.2020

[13] Kaisanet Oy. Kaisanet yleisesittely.

[14] Solutions Review. Gartner Shifts from MDM with their 2014 Magic Quadrant for EMM. 2014; Saatavilla: https://solutionsreview.com/mobile-device-management/2014-gartner-magic-quadrant-for-emm-mobility-management-mdm/. Haettu 08.10.2020

[15] Snyder J. BYOD, CYOD, COPE, COBO — What Do They Really Mean? 2018; Saatavilla: https://insights.samsung.com/2018/05/09/byod-cyod-cope-cobo-what-do-they-really-mean/. Haettu 14.10.2020

[16] Lugo J. Bring Your Own Device: Bitglass' 2020 Personal Device Report. 2020; Saatavilla: https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY20Q3BringYourOwnDevice2.pdf. Haettu 16.10.2020

[17] Jääskeläinen T. BYOD, CYOD ja firman laitepolitiikka. 2016; Saatavilla: https://blogi.mpy.fi/byod-cyod-ja-firman-laitepolitiikka. Haettu 14.10.2020

[18] Microsoft. What is Microsoft Intune. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune. Haettu 11.10.2020

[19] Microsoft. What's new in Microsoft Intune. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/fundamentals/whats-new. Haettu 11.10.2020

[20] Microsoft Endpoint Manager POC [Powerpoint]. n.d; Saatavilla: https://www.microsoft.com/microsoft-365/partners/endpoint-manager-poc. Haettu 21.09.2020

[21] Microsoft. Licenses available for Microsoft Intune. 2019; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses. Haettu 12.10.2020

[22] Microsoft. Microsoft Endpoint Manager overview. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/endpoint-manager-overview. Haettu 12.10.2020

[23] Microsoft. Enroll Android device with Intune Company Portal. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-company-portal. Haettu 21.10.2020

[24] Microsoft. Using the Intune Company Portal website. 2018; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/user-help/using-the-intune-company-portal-website. Haettu 21.10.2020

[25] Microsoft. What is Microsoft Intune device enrollment? 2019; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment. Haettu 21.10.2020

[26] Google. Overview - Android Enterprise. 2020; Saatavilla: https://developers.google.com/android/work/overview. Haettu 21.10.2020

[27] Microsoft. Android Enterprise device settings in Microsoft Intune. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work. Haettu 08.10.2020

[28] Microsoft. Enroll Android Enterprise dedicated, fully managed, or corporate-owned work profile devices in Intune. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/android-dedicated-devices-fully-managed-enroll. Haettu 21.10.2020

[29] Google. Zero-touch enrollment for IT admins. n.d; Saatavilla: https://support.google.com/work/android/answer/7514005?hl=en. Haettu 28.10.2020

[30] Microsoft. Enroll iOS/iPadOS devices in Intune. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll. Haettu 28.10.2020

[31] Microsoft. iOS/iPadOS device enrollment - Apple Configurator. 2018; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios. Haettu 28.10.2020

[32] Microsoft. Set enrollment restrictions in Microsoft Intune. 2018; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set. Haettu 21.10.2020

[33] Microsoft. Add groups to organize users and devices. 2019; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add. Haettu 27.10.2020

[34] Kaisanet Oy. Intune käyttöönotto dokumentaatio.

[35] Microsoft. Remotely Administer devices in Microsoft Intune. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/remote-actions/teamviewer-support. Haettu 27.10.2020

[36] Microsoft. Connect your Intune account to your Managed Google Play account. 2019; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/connect-intune-android-enterprise. Haettu 13.10.2020

[37] Microsoft. Get an Apple MDM Push certificate for Intune. 2018; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get. Haettu 25.10.2020

[38] Microsoft. App protection policies overview. 2020; Saatavilla: https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy. Haettu 26.10.2020