jamk.fi

MDM-järjestelmien tekninen vertailu Telia Inmics-Nebula Oy:lle

Lasse Kivikäs

Opinnäytetyö
Toukokuu 2019
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Kivikäs, Lasse	Opinnäytetyö, AMK	Toukokuu 2019
	Sivumäärä 67	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
MDM-järjestelmien tekninen vertailu Telia Inmics-Nebula Oy:lle

Tutkinto-ohjelma
Insinööri (AMK), tieto- ja viestintätekniikka

Työn ohjaaja(t)
Saharinen, Karo; Kotikoski, Sampo

Toimeksiantaja(t)
Telia Inmics-Nebula Oy

Tiivistelmä

Opinnäytetyö tehtiin Telia Inmics-Nebula Oy:n pyynnöstä. Yrityksellä on jatkuvaa palvelua asiakkaille tuottava tiimi, jonka pääasiallisena toimenkuvana on koostettu työasemanhallinta. Heidän tavoitteenaan oli ottaa käyttöön uusi asiakkaille tarjottava mobiililaitteille suunnattu MDM-palvelutuote. Tätä varten tarvittiin tekninen selvitys mahdollisista tuotteista. Tavoitteena oli saada aikaan vertailutaulukko, jonka avulla asiakkaille voidaan tarjota parasta mahdollista tuotetta. Yrityksen tiimin kanssa sovittiin yhteisesti vertailtaviksi tuotteiksi Microsoftin Intune sekä Miradoren Miradore Online.

Toteutusta varten luotiin vaatimusmäärittelylista, jossa käsiteltiin laitteiden päivittäiseen hallintaan liittyviä ominaisuuksia sekä tietoturvan näkökannalta oleellisia asioita. Työssä käytettiin yrityksen tarjoamia mobiililaitteita. Sekä Microsoftin Intunen että Miradore Onlinen palveluihin luotiin testiympäristöt, joissa nämä vaatimukset käsiteltiin ja dokumentoitiin.

Tuloksena saatiin koostettua lista, jossa molempien järjestelmien läpi käydyt yhtenevät ominaisuudet on arvosteltu asteikolla 0-5 työn suorittajan kokemuksen pohjalta. Kyseisessä vertailussa Miradore Online koettiin kokonaisuutena selkeämmäksi ja paremmaksi tuotteeksi, kun puhutaan yksinomaan mobiililaitteiden hallinnasta. Tämä perustui ympäristön selkeyteen ja helppokäyttöisyyteen. Microsoftin Intune on hyvä ja monipuolinen tuote, jonka integrointimahdollisuudet ovat erittäin laajat, mutta kokonaisuutena tuote ei yllä Miradore Onlinen tasolle.

Haasteita työn toteuttamiseen loi myös Intunen monimutkaisuus, sillä tuote sulautuu vahvasti Azure Active Directoryyn, joka yhdistää Microsoftin palveluita verkossa.

Avainsanat (asiasanat)
MDM, tietoturva, Microsoft, Miradore, Intune, mobiilitietoturva

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Kivikäs, Lasse	Bachelor's thesis	May 2019
		Language of publication: Finnish
	Number of pages: 67	Permission for web publication: x

Title of publication

Technical review of MDM systems for Telia Inmics-Nebula Oy

Degree programme

Information and communication technology

Supervisor(s)

Saharinen, Karo; Kotikoski, Sampo

Assigned by

Telia Inmics-Nebula Oy

Abstract

Thesis was assigned by the request of Telia Inmics-Nebula Oy. The company has a team that provides continuous service to its customers, and whose main focus is on providing comprehensive workstation management. Their goal was to create a new service product for mobile device management to their customers. For this, a technical review of possible mobile device management products was required. The goal was to create a comparison table that would provide customers with the most suitable product. After a negotiation with the company, Microsoft Intune and Miradore Online were chosen for the review.

For the implementation, a list of requirements was created containing features related to daily device management as well as issues relevant to security. In the technical part, mobile devices provided by the company were used to create a more specific review. The test environments were created for both Microsoft Intune and Miradore Online services for testing the requirements. These were later addressed and documented.

As the result, a compiled list was created. In this list, the matching requirements and properties were evaluated and scored on a scale of 0 to 5. The scoring was based on the tester's own experience of the system. In this comparison, Miradore Online was found a clearer and overall better system when it comes to mobile device management. This was based on the clarity of the system, as well as on being a more user-friendly product overall. Microsoft Intune is a good and versatile product with excellent and wide integration possibilities; however, it does not reach the level of Miradore Online.

The execution was challenging due to the complexity of Intune, since the service merges with other Microsoft products such as Azure Active Directory, which connects multiple Microsoft services under one interface.

Keywords/tags (subjects)

MDM, information security, Microsoft, Miradore, Intune, mobile device security

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

BLE	Bluetooth Low-Energy
DLP	Data Loss Prevention
EMM	Enterprise Mobility Management
EMS	Enterprise Mobility + Security
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MITM	Man-In-The-Middle
MTP	Mobile Threat Prevention
PDA	Personal Digital Assistant
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

1 Johdanto

Työn tarkoituksena oli perehtyä nykypäivän mobiililaitteisiin sekä niiden haavoittuvuuksiin ja niihin kohdistuviin haittaohjelmiin. Työssä tutkittiin myös, miten mobiililaitteiden tietoturvaa voidaan parantaa niin käyttäjätasolla, kuin kolmansien osapuolien tuotteiden avulla. Työssä keskitytään painotetusti yrityksen käytössä oleviin laitteisiin sekä niiden koostettuun hallintaan. Vaikka tietoturva on suurelta osin yksilötasoista, työstä saadut tulokset olivat painotetusti yrityspuolelle. Näiden tulosten avulla on tarkoitus ymmärtää tämän päivän yritysmaailman mobiililaitteiden riskejä, sekä osata varautua niihin tulevaisuudessa. Aiempaa tutkimusta MDM-järjestelmistä ja niiden ominaisuuksista on tehty Suomen tasolla jonkin verran, mutta osa töistä vain sivuaa tätä aihetta. Lisäksi MDM-järjestelmää tuottavia yrityksiä on monia, ja niiden ominaisuudet saattavat erota suurestikin toisistaan. Jo tehdyissä tutkimuksissa on myös käsitelty aihealuetta eri näkökulmista, mutta kasvava ala tarvitsee jatkuvasti lisää uusia tutkimuksia.

Telia Company on valtakunnallinen teleoperaattori ja IT-palveluita tuottava yritys, jonka tytäryhtiö Inmics-Nebula Oy tarjoaa kokonaisvaltaisia ICT-ratkaisuja yrityksille. Inmics Oy oli vuonna 1989 perustettu jyväskyläläinen perheyritys, joka alun perin rakensi, huolsi ja ylläpiri kuluttajien PC:itä. Nebula Oy helsinkiläinen vuonna 1997 perustettu, pääasiassa hosting-palveluja tuottanut IT-alan yritys. Vuonna 2017 ja 2018 Telia osti Inmics Oy:n sekä Nebula Oy:n ja syksyllä 2018 alkoi yritysten fuusio. Muiden ICT-palveluiden ohella Inmics-Nebula Oy tuottaa työasema- sekä mobiililaitehallintaa. Tätä palvelua tuottavalle tiimille tarvittiin tuotevertailu-tyyppinen tutkimus käytettävistä palveluista, joilla mobiililaitteita voidaan koostetusti hallita.

Työn tutkimusmenetelmänä oli soveltava tutkimus. Työssä käytiin läpi yleisellä tasolla mobiililaitteiden tietoturvaa ja niiden haavoittuvuuksia sekä mikä niiden mahdollinen vaikutus saattaa olla yritykselle. Nämä saattavat olla nykypäivänä elintärkeitä asioita yrityksen toimivuuden ja luotettavuuden kannalta. Mobiililaitteilla kuljetettavan datan määrä tänä päivänä on erittäin suuri, jonka lisäksi pilvipalvelut poistavat laitteen fyysisen tallennustilan rajat. Tämä voi tuntua yrityksestä suurelta riskiltä. Mobiililaitteiden painoarvon lisääntyminen työssä ja työelämässä kasvaa koko ajan,

ja jatkuvasti palveluita tuodaan mobiililaitteille työasemilta. Tästä syystä yritysten pitäisi kiinnittää huomiota tähän jatkuvasti enemmän. Aineistoa kerättiin alan kirjoista, aiheeseen liittyvistä julkaistuista tutkimuksista sekä opinnäytetöistä.

Työn teknisen toteutuksen tavoitteena oli luoda lista, jonka pohjalta asiakkaille voidaan tarjota heidän ympäristöönsä sopivinta tuotetta. Tätä varten valittiin yrityksen kanssa kaksi tuotetta, jotka otettiin tekniseen vertailuun. Tätä varten luotiin vaatimusmäärittelylista, johon valittiin sekä yrityksen että palvelua ostavan asiakkaan kannalta oleellisia ominaisuuksia. Molempiin ympäristöihin tehtiin testiympäristö, jossa listan mukaiset asiat käytiin läpi. Lopuksi näistä ominaisuuksista tehtiin yhteenveto ja taulukkomallinen listaus.

2 Mobiililaitteet

2.1 Mobiililaitteen käsite

Tänä päivänä melkein jokainen kantaa mukanaan mobiililaitteita. Käsitteenä mobiililaite kuitenkin kattaa laajan listan erilaisia laitteita jo nyt, ja uusia laitteita tulee markkinoille kovaa tahtia lisää. Ensimmäisenä mobiililaitteesta puhuttaessa tulee mieleen matka-, tai nykypäivänä älypuhelin, joka on yleisin käytössä oleva mobiililaite ja joka on jokaisella meistä mukana joka päivä, kaikkialla. Puhelimesta on tullut ihmiselle melkein elinehto, sillä suuren osan päivittäisistä asioista pystyy jo hoitamaan pelkällä puhelimella liikkumatta paikaltaan mihinkään.

Han ja Cho (2016) kertovat julkaisussaan, miten mobiililaitteet ovat nopeasti syrjäyttäneet tavalliset matkapuhelimet mobiililaitteiden maailmassa. Laitteiden suosio perustuu nopeasti kehittyvään teknologiaan, aina kommunikaattoreista tehokkaisiin ja edistyksellisiin laitteisiin. Vuonna 2008 Apple julkaisi iPhonen, ja samana vuonna julkaistiin muiden valmistajien älypuhelimia varustettuna Googlen Android-käyttöliittymällä. Nokian ollessa markkinajohtajana, se alkoi nopeasti menettämään paikkaansa sekä Applelle että Androidille ja tarkemmin Samsungille. (Han & Cho 2016, 1-2.)

Mobiililaitteeksi voidaan lukea myös esimerkiksi tabletit (Griffin 2017, 2). Tabletti laitteena on tällä hetkellä lähimpänä puhelinta, kun puhutaan mobiililaitteesta, vaikka tabletin käyttötarkoitus ja käyttömahdollisuudet voivat antaa enemmän viitteitä tietokoneesta kuin puhelimesta. Isompi rakenne antaa mahdollisuuden käyttää tehokkaampia osia ja akkuja, sekä luonnollisesti tuo myös isomman näytön laitteelle.

2.2 Käyttöjärjestelmät ja niiden erot

Kuten tietokone, mobiililaitteet vaativat oman käyttöjärjestelmän toimiakseen. Mobiilikäyttöjärjestelmät ovat suunniteltuja juuri älypuhelimille, tableteille, älykelloille sekä muille nykypäivän kannettaville älylaitteille. Fornin ja Meulenin (2017) julkaiseman lehdistötiedotteen mukaan vuonna 2017 ensimmäisellä kvartaalilla maailmassa oli noin 380 miljoonaa älypuhelinta. Samalla tämä tarkoittaa yhtä montaa mobiilikäyttöjärjestelmää. Laskennassa suurin osuus laitteista (86,1 %) oli Googlen Android-pohjaisia käyttöjärjestelmiä. Seuraavana iOS-pohjaiset käyttöjärjestelmät (13,7 %), eli Applen omat tuotteet ja viimeisenä muut käyttöjärjestelmät (0,2 %). Todellisuudessa siis suurin kilpailu käydään Googlen Androidin ja Applen iOS -järjestelmän välillä. (Forni & Meulen 2017.)

Merkittävä ero näillä kahdella käyttöjärjestelmällä on lähdekoodin avonaisuus. Android -käyttöjärjestelmän ydin (kernel), käyttöjärjestelmä ja osa perusohjelmista perustuvat avoimeen lähdekoodiin (eng. open source). Tätä kutsutaan ohjelmistopinoksi. Androidi käyttää ytimenään Linuxia, vaikkakin sitä on muunneltu Googlen toimesta eikä ole virallisesti Linux-jakelu. Tämä on tehnyt Androidista suositun etenkin kehittäjien keskuudessa ja mahdollistanut myös modifioitujen järjestelmien vaihtamisen omaan Android-puhelimeen. (Silberschatz, Galvin & Gagne 2014, luku 2.7.5.3.)

iOS:n ytimenä on Applen oma Core OS, ja sen ohjelmistopino on suljettu, joskin osa sen komponenteista saattaa olla avointa lähdekoodia. Tämä tarkoittaa sitä, että ainoastaan Applella itsellään on pääsy käyttöjärjestelmän muokkaukseen ja kehittämiseen. Apple ei myöskään salli iOS-laitteille kolmansien osapuolien sovelluksia sovelluskaupoista. Tämän on sanottu tekevän laitteista turvallisemman. (Mt. Luku 2.7.5.2.)

2.3 Mobiililaitteiden yhteydet

Mobiililaitteiden tiedon- sekä datansiirto tapahtuu tänä päivänä pääsääntöisesti langattomilla yhteyksillä, vaikkakin myös langallisia yhteyksiä vielä käytetään. Langattomia yhteyksiä on nykypäivänä useita eri tyyppisiä erilaisiin tarkoituksiin.

Matkapuhelinverkot

Matkapuhelimet, joihin työssä viitataan mobiililaitteena, käyttävät matkapuhelinverkkoja tai nykykielessä mobiiliverkkoja datan välittämiseen laitteilta toisille mainitsee Doherty (2016). Nykyaikaisempien 3G-verkkojen suunnittelu alkoi, kun huomattiin tarve tämän tyyppisille verkoille. 3G-verkot veivät matkapuhelinverkkoja eteenpäin etenkin datamäärän ja tärkeänä osana datan salauksen suhteen. Lisäksi puheessa äänenlaadun suhteen tapahtui paranemista ja multimedia tuli mukaan. Suurena tekijänä oli myös 3G-verkon internetmahdollisuus. (Doherty 2016, 56-58.)

Bluetooth

Isaksson (2017) käsittelee opinnäytetyössään Bluetoothia, joka on lyhyen etäisyyden radiotaajuus kahden tai useamman laitteen kommunikointiin ja tiedonsiirtoon. Sen kehitys alkoi vuonna 1994 Ruotsissa matkapuhelinyritys Ericssonin toimesta. Sen toimiva taajuusalue on 2400-2480 Mhz. Bluetoothin kantama vaihtelee 5-100 metrin välillä riippuen lähettimen tasosta, joita on kolme erilaista. Bluetooth kehitettiin korvaamaan datakaapelit, joilla tietoa on siirretty ennen. Tällä hetkellä Bluetoothista on käytössä useimmissa mobiililaitteissa versio 4.2. Bluetooth 4.0 -sarja julkaistiin heinäkuussa vuonna 2010, ja se toi mukanaan BLE (Bluetooth Low-Energy) -teknologian. Tämän tarkoituksena on vähentää virrankulutusta oheislaitteissa, kuten esimerkiksi langattomissa kuulokkeissa. (Isaksson 2017, 1.) Bluetooth 5 julkaistiin joulukuussa vuonna 2016 (Isaksson 2017, 1, 3.)

Wi-Fi

Wi-Fi tai WiFi on langattoman lähiverkon (WLAN) teknologia, joka perustuu IEEE 802.11-standardiin. Wi-Fi-yhteyden tarkoituksena on siis siirtää dataa samassa langattomassa verkossa olevien laitteiden kesken. Tämä standardi on tullut vuonna 1997, ja se mahdollisti teoreettisen 1-2 Mbit/s tiedonsiirtonopeuden. Vuonna 1999 julkaistiin 802.11a sekä 802.11b. 802.11a käytti 5.15-5.825 GHz:n taajuusaluetta, ja

sen teoreettinen siirtonopeus on 6-54 Mb/s. Standardin tarkoituksena oli tuottaa nopeaa tiedonsiirtoa lyhyellä matkalla. 802.11b taas toimi 2.4 GHz:n taajuudella, mutta sen teoreettiset siirtonopeudet olivat 1-11 Mb/s. Seuraava merkittävä standardi oli kesäkuussa 2003 julkaistu 802.11g, joka mahdollisti a:n ja b:n hyvät puolet, eli matalammalla 2.4 GHz:n taajuudella teoreettisena nopeutena 54 Mb/s. Viimeisin merkittävä uudistus oli lokakuussa 2009, jolloin julkaistiin 802.11n. Tämän teoreettiset nopeudet olivat sekä 2.4 GHz:n ja 5 GHz:n taajuudella noin 600 Mb/s. (What is WiFi: IEEE 802.11. N.d.)

2.4 Puhelimen elämänkaari

Syyskuussa vuonna 2014 CTA (Consumer Technology Association) julkaisi kirjoituksen, jonka mukaan älypuhelimen käyttöikä on 4,7 vuotta. Vuonna 2018 Kantar Worldpanel:n tekemän tutkimuksen mukaan Yhdysvalloissa kuluttaja vaihtaa puhelimensa keskimäärin 22 kuukauden välein. Varsinkin nykypäivän esimerkiksi akkujen lyhyt käyttöikä sekä akun rakentaminen laitteen sisään helpottavat uuden laitteen hankintaa. (Cases 2018.) Laitteen lyhentyvä käyttöikä on parempi vaihtoehto valmistajille, sillä tuotteita myydään jatkuvasti enemmän. Kuluttajalle tämä voi olla ongelma, sillä uusien laitteiden hinnat kohoavat vuosittain korkeammalle. Toisaalta valmistajat panostavat nykyään enemmän myös hinnaltaan halvempiin, perustason laitteisiin. Yrityksille laitteet ovat erilaisessa merkityksessä, sillä laitteiden tietoturvaan pitää pystyä luottamaan.

3 Haittaohjelmat

3.1 Haittaohjelman käsite

Dohertyn (2016) mukaan haittaohjelma -termi (eng. malware) käsittää yleisesti tietokoneohjelman, jonka tarkoitus on aiheuttaa ei-toivottuja tapahtumia tietokoneissa tai järjestelmissä. Haittaohjelma voidaan esimerkiksi piilottaa useisiin eri tiedostomuotoihin koodina, jonka suorittamisesta tai avaamisesta se aktivoituu ja käynnistää esimerkiksi viruksen. Se voi avata esimerkiksi takaportin, josta krakkeri voi päästä tietokoneen tiedostoihin käsiksi. Virus voi myös itse kerätä tietoa koneelta, tai vasta-

vuoroisesti tuhota tiedostoja (Doherty 2016, 77, 338.) Tätä virusta kutsutaan troijalaiseksi (eng. trojan horse). Myös niiden haittaohjelmia sisältävien tiedostojen levitys suurellekin ihmisjoukolle tänä päivänä on helppoa.

3.2 Mobiililaitteiden haavoittuvuudet

Nykypäivänä mobiililaitteen suosio on niin suuri, että kyberrikoksiin erikoistuneet ihmiset ovat antaneet huomionsa niille (Doherty 2016, 327). Pelkästään langattomia yhteyksiä mobiililaitteissa on jo useita. Ja koska ne käyttävät valtaosin eri teknologioita, on niille myös omat haavoittuvuudet ja heikkoudet.

CVEn vuonna 2018 tekemän tutkimuksen mukaan Android oli haavoittuvaisin mobiilikäyttöjärjestelmä. Android-käyttöjärjestelmästä tunnistettiin CVE:n raportin mukaan 597 haavoittuvuutta. Vuonna 2017 kyseinen luku oli 842, ja Android oli myös silloin haavoittuvaisin mobiilikäyttöjärjestelmä. (CVE 2018a.) Applen iOS-käyttöjärjestelmän haavoittuvuuksia vuonna 2018 oli 125 kappaletta. Vuonna 2017 sama luku oli 387. (Mt.) Tämä tarkoittaa, että haavoittuvuuksia on ollut huomattavan paljon vähemmän iOS-laitteissa kuin Android-laitteissa. Huomioitava asia kuitenkin on, että Android perustuu avoimeen lähdekoodiin, joka avaa paljon enemmän mahdollisuuksia tutkia käyttöjärjestelmän komponentteja sekä niiden toimintaa. Siksi, että Android- ja Apple-tuotteet ovat markkinajohtajia niin yritys- kuin kuluttajapuolella, on yleinen oletus, että rikollisten mielenkiinto olisi pääosin näissä käyttöjärjestelmissä. (CVE 2018b.)

Avoin verkko

Tämän päivän yksi suurista ongelmista on avoimet verkot. Raggon (2016) mukaan avoimen Wi-Fi -yhteyden käyttö julkisissa rakennuksissa ja paikoissa, kuten kahviloissa, lentokentillä ja hotelleissa on suuri riski. Myös useissa julkisissa kulkuvälineissä tänä päivänä avoin Wi-Fi-verkko. Tämä asia on luonnollisesti myös tiedossa toisella puolella, ja näitä avoimia verkkoja hyödynnetään paljon. Yksi tapa kerätä käyttäjien tietoa on käyttää sniffer-tyyppistä ohjelmaa, kuten Wiresharkia. Tällä ohjelmalla voidaan seurata verkkoliikennettä. Jos käyttäjä käyttää avointa Wi-Fi-verkkoa ja esimerkiksi kirjautuu salaamattomalle verkkosivulle

(HTTP), voidaan käyttäjän kirjautumistiedot nähdä puhtaana tekstinä Wireshark -ohjelmassa. (Raggo 2016, 16.)

3.3 Androidin tietoturvahaasteet ja rooting

Doherty (2016) käsittelee kirjassaan Wireless and Mobile Device Security Androidin tietoturvahaasteita. Androidin tietoturvahaasteet liittyvät osakseen Linux-pohjaiseen käyttöjärjestelmään, joka taas pohjautuu avoimeen lähdekoodiin. Kuitenkin kaikilla puhelinvalmistajilla, jotka käyttävät Androidia käyttöjärjestelmänään, on oma prosessinsa sen muokkaukseen, testaukseen sekä paketointiin. Tämä tarkoittaa, että käytännössä Android ei ole sen haavoittuvaisempi haittaohjelmille kuin muutkaan järjestelmät. Tämä on myös riippuvaista loppukäyttäjän omasta toiminnasta laitteen kanssa, kuten esimerkiksi laitteen rootauksesta (eng. rooting). (Doherty 2016, 248-252.)

Rooting-termillä kuvataan Android-laitteen root-tunnuksen käyttöönottoa. Tällä tarkoitetaan korkeinta käyttöoikeutta, jolla on pääsy käyttöjärjestelmän ytimeen ja syvimpään osaan ja sen keskeisiin sovelluksiin. Root-luvan (eng. root-permission) avulla käyttäjä voi ohittaa nämä Androidin asettamat estot. Tämä mahdollistaa esimerkiksi sovellusten lataamisen kolmansilta osapuolilta. Normaalilla käyttöoikeudella ohjelmien lataus onnistuu vain tietyistä sovelluskaupoista kuten Google Play Store tai valmistajan oma sovelluskauppa. Oikein käytettynä ja tekniikkaan perehtynyt ihminen voi saada tästä paljon normaalia enemmän irti, mutta kokemattoman käsissä puhelimen käyttö voi vaarantua. Joissakin Androidin versioissa on myös mahdollista päästä järjestelmän käynnistysjärjestykseen (eng. Boot sequence) käsiksi, jonka kautta voi ladata toisen Android-version puhelimeen. (Mts. 252, 268.)

3.4 iOS:n tietoturvahaasteet ja Jailbraking

Doherty (2016) kertoo, että Applen kehittämän suljetun iOS -käyttöjärjestelmän vahvana etuna on alusta asti ollut se, että Applen omaan App Storeen päätyy vain heidän toimestaan tarkastetut ja hyväksytyt applikaatiot. Tämä on tehnyt rikollisten silmissä iOS:sta vähemmän kiinnostavan. (Doherty 2016, 269.)

Vaikka Applen tapa käsitellä ja hyväksyä itse heidän oman App Storen ohjelmansa on turvallisempi tapa, ei tämä silti takaa täydellistä suojausta haittaohjelmia tai haavoittuvia sovelluksia vastaan. Käytännössä sovelluskehittäjä voi saada mahdollisuuden ladata oman sovelluksensa sovelluskauppaan esimerkiksi varastetulla tunnuksella. Tästä huolimatta iOS-järjestelmä on saatu pidettyä suhteellisen turvallisena. Tähän vaikuttavina tekijöinä ovat olleet muutamat asiat. Yksi syy on kehittäjien pakollinen rekisteröityminen ja digitaalisen sertifikaatin hankkiminen. Toisena syynä on Applen itse testaamat ja hyväksymät sovellukset, mikä tarkoittaa, että kaikki Applen sovelluskauppaan tulleet sovellukset on testattu ja hyväksytty heidän toimestaan. Lisäksi Applen digitaalinen sertifikaatti estää julkaistujen sovellusten muokkaamisen jälkeenpäin, joten päivitetty sovellus vaatii aina uuden jakelun. (Mts. 270.)

Jailbreaking on termi, joka kuvastaa Androidin rooting:ia iOS-laitteelle. Applen laitteet ovat aina tiukasti suojattuja ja rajoitettuja, mikä saattaa olla käyttäjälle liikaa. Tämän vuoksi käyttäjät saattavat rikkoa laitteen suojauksen saadakseen käyttöönsä vähemmän rajoitetun laitteen. Jailbreaking antaa laitteelle juuritason oikeudet (eng. Root privileges). Tämän avulla laitteelle voidaan ladata sovelluksia myös ulkoisista lähteistä. Mutta monet käyttäjät, jotka suorittavat tämän toiminnon, eivät aina ymmärrä laitteen riskien kasvua eivätkä näin ymmärrä suojata laitettaan muilla tavoin. (Mts. 272-273.)

3.5 Haavoittuvuudet ja hyökkäykset

Mobiililaitteille löytyy haavoittuvuustyyppejä paljon. Koivula & Tuomola (2014) kertovat kiristyshaittaohjelmien vakavuudesta. Kiristyshaittaohjelma (eng. ransomware) on yksi 2010-luvun suurimpia haavoittuvuustyyppejä. Kiristyshaittaohjelman toimintaperiaate perustuu haittaohjelmaan, joka lukitsee käyttäjän laitteen ruudun ja näin estää käyttäjää pääsemästä laitteelle käsiksi tai estää pääsy laitteen tiedostoihin. (Koivula & Tuomola 2014, 8.) Näiden avaamiseen tarvitaan purkuavain (eng. Decrypt key), jota vastaan haittaohjelman levittäjä pyytää maksua (Mts. 11). Tämä maksu tapahtuu monesti kryptovaluuttana (mm. BitCoin). Esimerkkinä Trend Micron Mobile App Reputation Service (MARS) analysoi vuonna 2017 yli 468,000 mobiilipohjaista kiristyshaittaohjelman näytettä, joka oli moninkertaisesti enemmän kuin vuonna 2016. Etenkin kolme kiristyshaittaohjelmaa esiintyi ympäri maailmaa: Petya maaliskuussa

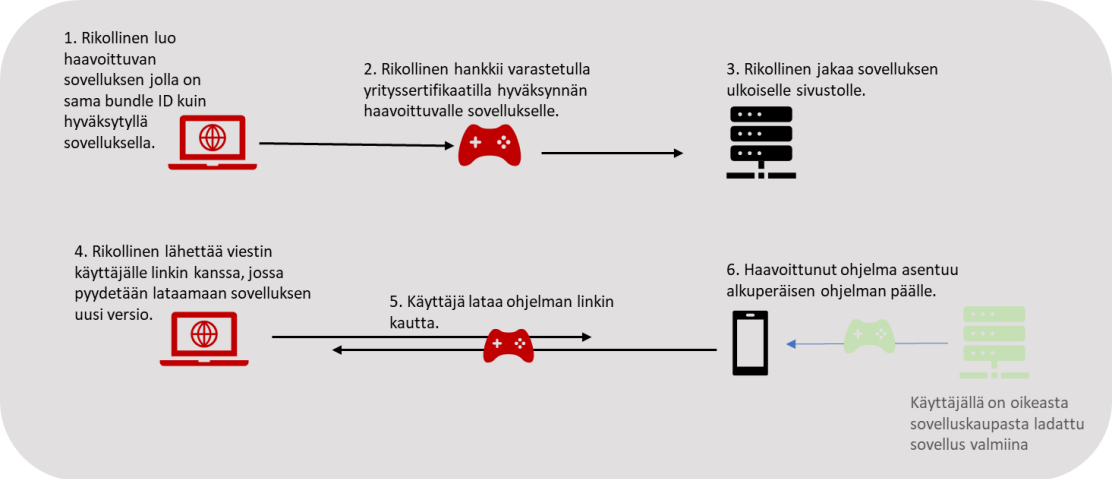
2016, WannaCry toukokuussa 2017 sekä NotPetya kesäkuussa 2017. (2017 Mobile Threat Landscape 2018.)

Monesti viestit on osattu naamioida pelotteleviksi tai uhkaaviksi kuten maksamattomiksi laskuiksi, jotta ihmiset saataisiin avaamaan tiedostot. Myös viestien alkuperäinen lähettäjä pystytään naamioimaan (spoofing) joksikin toiseksi, kuten yleisesti käytössä olevissa toimitusjohtajahuijauksissa tehdään. Näihin monesti käytetään kertakäyttöisiä sähköposteja, jotta riski jäljittämiseen olisi mahdollisimman pieni.

Raggo (2016) mainitsee yhtenä yleisenä hyökkäystyyppinä Man-in-the-Middle-hyökkäyksen (MitM), jossa käyttäjän koneelle kulkeva data reititetään MitM-käyttäjän kautta ilman, että kumpikaan osapuoli tietää tästä. Yksi tapa toteuttaa hyökkäys on, että hyökkääjä pystyttää oman virtuaalisen reitittimen, joka on nimetty samalla tavalla kuin julkisen kohteen reititin (ks. Kuvio 1). Tällä on tarkoitus saada käyttäjä yhdistämään väärään reitittimeen, mutta ei käytännössä huomaa eroa. Tällöin esimerkiksi yrityksen verkkoon kirjautuvat voivat tietämättään antaa pääsyn ulkopuoliselle henkilöille. Samat riskit pätevät myös yritysten avoimiin verkkoihin, kuten vierasverkkoihin. (Raggo 2016, 14.)

Kuvio 1. Havainnollistettu kuva Man-in-the-Middle -hyökkäyksestä

Raggon esittämä toinen esimerkki on sekä Android- että iOS-laitteille suunnattu Masque attack. Tämä hyökkäys ei vaadi laitteelta Roottausta tai Jailbreakia. Tällä menetelmällä uhri houkutellaan lataamaan päivitys jo laitteella olevalle sovellukselle. Koska ohjelmalla on jo yrityksen sertifikaatti ja luotu päivitys käyttää samaa ID:tä, on tämä päivitys oletuksena luotettu. Kuvio 2 havainnollistaa hyökkäyksen kulun. (Mts. 9.)



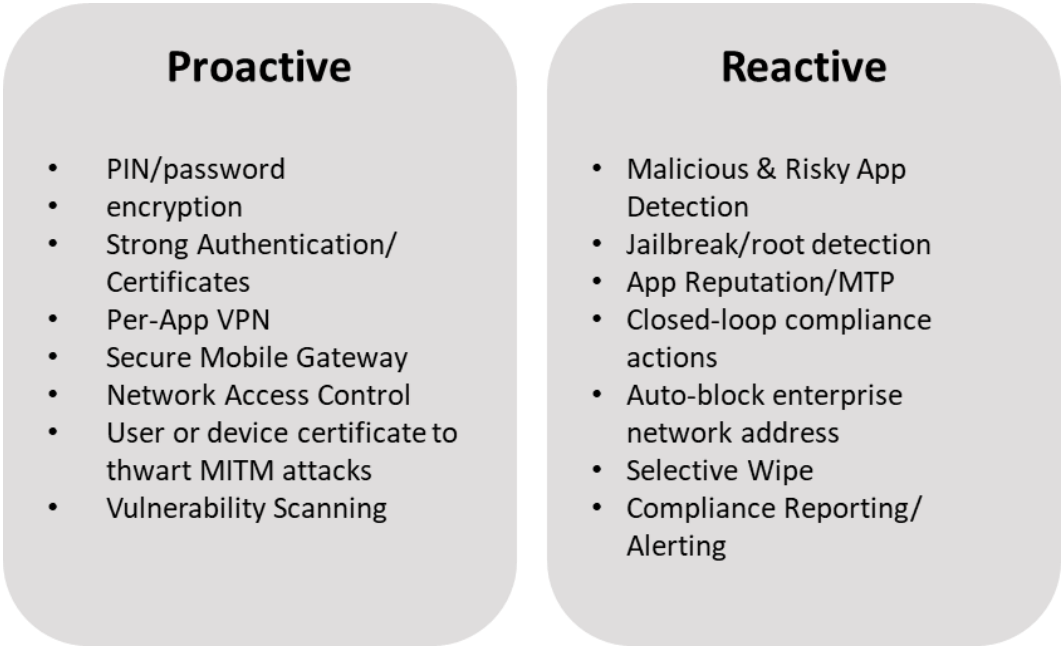
Kuvio 2. Havainnollistettu kuva Masque-hyökkäyksestä

Esimerkkiohjelmana voidaan käyttää sähköpostisovellusta. Tähän ladattu väärä päivitys päivittää ohjelman alkuperäisen version haavoittuneella versiolla, jonka jälkeen käyttäjän sähköpostin data kulkeutuu hyökkääjälle. (Mts. 9-10.)

4 Haittaohjelmien ennaltaehkäisy ja torjunta

4.1 Mobiililaitteiden suojaus

Kirjassa Mobile Data Loss Raggo (2016) mainitsee, että hyvä ja kokonaisvaltainen turvallisuus laitteissa koostuu proaktiivisista, reaktiivisista ja valvovista suojausmetodeista. Proaktiivinen ja reaktiivinen suojaus voidaan jakaa Kuvio 3 mukaisesti:



Kuvio 3. Kuvaus proaktiivisista ja reaktiivisista suojausmetodeista.

Proaktiivinen suojaus

Proaktiivisessa suojauksessa käytetään esimerkkinä liikkumatonta dataa (data-at-rest), sekä dataa, jota siirretään paikasta toiseen (data-in-motion). Mobiililaitteen päällimmäinen suojaus, kuten esimerkiksi PIN-koodi tai salasana, tai laitteen salaus ovat hyviä ja tärkeitä osia laitteen suojausta. Kuitenkin yritysmaailmassa nämä yksinään usein ovat riittämättömiä suojausmenetelmiä. Jotta yrityksen tietoturva on riittävällä tasolla, on kiinnitettävä huolta DLP:hen (Data Loss Prevention). Esimerkkinä, jos yrityksen työntekijä avaa omalla laitteellaan työsähköpostin liitteineen, ei mikään suoraan estä häntä levittämästä tämän liitteen tietoja eteenpäin. Tämän vuoksi yrityksen data pitäisi pitää erillään henkilökohtaisesta datasta. Tämä on nykypäivänä haasteellisempaa, koska monissa mobiililaitteissa saattaa olla esimerkiksi useampi SIM-korttipaikka. Tämä antaa mahdollisuuden käyttää sekä omaa, että mahdollista työliittymää samassa laitteessa. (Mts. 37.).

Doherty (2016) mainitsee kirjassaan proaktiiviseen suojaukseen liittyvistä PIN- ja salasanasuojauksista. Nykypäivänä laitteen suojauksissa käytetään monesti jo biometrisiä suojausmenetelmiä, kuten sormenjälkeä. Monesti loppukäyttäjä saattaa kuitenkin valita helpoimman mahdollisen, kuten 4-numeroisen PIN-koodin. Tämä on käyttäjälle

nopeampi käyttää kuin monimutkainen salasana. Samalla se kuitenkin luo suuremman riskin, jos puhelin joutuu vääriin käsiin. (Doherty 2016, 247.)

Proaktiivista suojaa tiedostoille luo salatut säiliöt (eng. encrypted container). Nämä ovat yksi turvallinen tapa säilöä laitteessa liikkumatonta dataa. Tämä myös estää henkilökohtaisia tiedostoja sotkeutumasta yrityksen tiedostoihin sekä suojaa vahingollisilta tiedoston jakeluilta esimerkiksi pilvipalveluihin. Lisäksi se luo erillisen suojauskerroksen haittaohjelmia vastaan. (Raggo 2016, 37.)

Liikkuvan datan siirtoon turvallinen vaihtoehto on VPN-tunneli tai per-app VPN. Erona näissä kahdessa on perinteisen VPN:n laajuus. Kun VPN saattaa oletuksena sallia dataliikenteen kaikista sovelluksista, luo tämä riskin päästää haavoittunut tai tarttunut ohjelma VPN:n läpi yrityksen verkkoon. Per-App VPN-ratkaisu antaa hallinnoivalle osalle paremman hallittavuuden. Tämän avulla voidaan sallia vain tiettyjen ohjelmien pääsy yrityksen verkkoon, jolloin ei-haluttujen ja mahdollisesti haavoittuvien ohjelmien seulonta helpottuu. (Mts. 37.)

Reaktiivinen suojaus

Reaktiiviset suojausmenetelmät ovat nykyhetkeen ja lähitulevaisuuteen viittaavia suojaustapoja. Tietoturvaloukkauksien havainnoinnissa saattaa mennä jopa vuosia, ennen kuin yritys huomaa ne. Tämä viive aiheuttaa sen, että tietojen väärinkäytön mahdollisuus kasvaa suureksi. Esimerkiksi luottokorttitietojen listoja, terveys- sekä henkilötietoja paljastetaan suurina listoina internetissä ilman, että datavarkautta on edes huomattu. (Mts. 39.)

Reaktiiviseen suojaukseen yritysmaailmassa käytössä saattaa olla EMM (Enterprise Mobility Management), joka muodostaa kokonaisuuden, johon myös MDM kuuluu. EMM:n avulla pystytään automatisoidusti ja nopeammin reagoimaan ja vastaamaan uhkiin. (Mts. 39.)

Käyttöjärjestelmän aukot ja haittaohjelmat ovat suurin osa mobiililaitteiden uhkia, ja mobiililaitteiden kohdalla nämä näkyvät monesti kohdassa 3.3 ja 3.4 kuvatuissa jailbreakatuissa ja rootatuissa iOS- ja Android-laitteissa. Lisäksi sähköpostin ja viestien

kautta lähetetyt ohjelmat, sekä tahallaan että tahattomasti haavoittuvat sovelluskauppoihin jaetut sovellukset luovat riskin. (Mts. 39.)

Ohjelmien pisteytyksien tunnistus, MTP (Mobile Threat Prevention) ja karanteeni suojaavat laitteiden yksityisyyttä, ja yrityksen käyttäessä EMM:ää, voidaan tarvittaessa toteuttaa toiminnallisia tapahtumia laitteille. Näihin lukeutuvia toimintoja ovat laitteen tehdasasetuksiin palautus tai selektiivinen tyhjennys (tyhjennetään vain osa laitteesta). Tämän lisäksi voidaan estää laiteiden pääsy internettiin tai ainoastaan VPN:n yli. (Mts. 39.)

4.2 3. osapuolen tarjoamat sovellukset

Snyder (2018) käsittelee mobiililaitteille suunnattuja antivirus-sovelluksia ja toteaa, että antivirus-käsite on vääristynyt ja anti-malware-käsite on kuvaavampi termi. Tämä käsite on laajempi, sillä se ei rajaa pelkästään viruksiin, vaan käsittää haittaohjelmat kokonaisuutena. Yritysmaailmassa puhutaan kohdassa 4.1 mainitusta EMM-ratkaisuista sekä MDM:stä. (Snyder 2018.)

Jos yrityksen IT on varautunut esimerkiksi MDM-järjestelmällä nykypäivän suurimpaan mobiililaitteita saastuttavaan tapaan, eli haavoittuvien applikaatioiden ja sovelluskauppojen estämiseen, laskee riski saastumiseen jo suuresti. Tämä saattaa myös muuttaa yrityksen tarvetta hankkia erillistä ohjelmistoa suojaamaan laitteita. (Mt.)

Myös monet MDM-järjestelmien palvelut löytyvät myös kolmansien osapuolten sovelluksista, kuten lukitusten määritykset, Wi-Fi-verkkojen rajoitukset ja laitteiden tyhjennykset etänä. Jos yritys ei käytä EMM- tai MDM-järjestelmää ympäristössään, voi kolmannen osapuolen tarjoama ohjelmisto tuoda myös lisäturvaa mobiililaitteille. EMM ja MDM eivät kokonaisuudessaan poista lisäohjelmiston tarvetta. (Mt.)

4.3 MDM

MDM tulee lyhenteestä Mobile Device Management. MDM -järjestelmillä voidaan koostetusti hallita yrityksen sekä työasema- että mobiililaitekokonaisuuksia. Monesti nämä saattavat olla saman ohjelmiston eri osioita. MDM kuitenkin nimensä mukaisesti viittaa juuri mobiililaitteiden hallintaan. MDM-järjestelmiä tuottavat useat eri

IT-alan yritykset. Varsinkin monet suuret ohjelmistoalan yritykset ovat lähteneet tuottamaan omaa järjestelmää. Hallinnalla tarkoitetaan laitteiden yhtenäistä ylläpitoa, kuten ohjelmistojen asennusta koostetusti tai yksilöllisesti järjestelmän kautta. Järjestelmällä voidaan myös poistaa ohjelmia laitteilta, ajaa laitteille päivityksiä tai tyhjentää laitteita. Kaikki tämä voidaan tehdä yhden päätteen kautta ilman, että laitetta tarvitsee erikseen toimittaa esimerkiksi it-osastolle.

MDM-järjestelmien tarve

Yksittäinen henkilö ei todennäköisesti näe tarvetta koostettuun laitehallintaan, mutta yritysmaailmassa sellaisen tarve voi olla suuri. Se, että laitteita voidaan koostetusti hallita yhdestä paikasta, tuo turvallisuutta ja elinkaarihallintaa helpommaksi sekä selkeämmäksi. Elinkaarihallinnalla tarkoitetaan esimerkiksi puhelimen eri vaiheita siitä, kun yritys hankkii laitteen, ottaa laitteen käyttöön, sekä lopuksi poistaa laitteen yrityksen käytöstä. Kun yrityksellä on käytössään joku MDM-järjestelmä, kaikki nämä vaiheet liittyvät siihen jotenkin.

Haasteet

Diogenes & Gilbert (2015) kertoo kirjassaan, että kun yritys tai organisaatio suunnittelee MDM-järjestelmän käyttöönottoa, pitää huomioida 4 seuraavaa perusasiaa:

- Käyttäjät
- Laitteet
- Sovellukset
- Data

Kun käyttöönottoa suunnitellaan, on otettava huomioon käyttäjä sekä laite, jota hän käyttää. Tämän lisäksi on ajateltava sovelluksia, joita käyttäjä mahdollisesti käyttää tai haluaisi käyttää. Kuitenkin tärkeänä kohtana on pidettävä sitä, miten laitteessa yrityksen data pidetään turvassa. Kun näihin neljään asiaan keskitytään yksilöllisesti, voidaan helpommin havainnoida eri käyttötapauksia. (Diogenes & Gilbert 2015, 2.)

Käyttö yritysmaailmassa

MDM-järjestelmien käyttö yrityksessä on monella tasolla hyvä asia. Kun yrityksen työntekijöiden mobiililaitteet saadaan jonkin yhden järjestelmän alle, niiden kokonaisvaltainen tietoturva paranee. MDM-järjestelmien kautta voidaan esimerkiksi tarkastaa laitteiden tila, onko laite esimerkiksi otettu pois käytöstä. Myös käytöstä poistettu laite voidaan etänä tyhjentää, jotta riski laitteen mahdollisten tietojen vuotamisesta muille minimoituu. MDM-järjestelmän kautta saadaan myös tietoa laitteen versiosta sekä päivityksestä, ja tarvittaessa päivittämättömien laitteiden pakotettu päivitys onnistuu. Tämäkin saattaa olla oleellinen asia tietoturvan näkökannalta, jos laitetta ei ole päivitetty viimeisimpään versioon. Yksittäinen käyttäjä ei välttämättä muista tai osaa päivittää puhelintaan, joten se voidaan siirtää esimerkiksi IT-osaston hoidettavaksi, jolla varmistetaan, että laitteet pysyvät ajan tasalla.

5 MDM-järjestelmien vertailu

5.1 Yleistä

Tässä työssä tehtiin tekninen tutkimus sekä vertailu kahdesta eri MDM-järjestelmästä: Microsoftin Intunesta sekä Miradoresta. Vertailussa käytiin läpi järjestelmien yleisesti teknisiä ominaisuuksia ja piirteitä. MDM-palvelua tuottavan yrityksen näkökulmasta mietittiin muun muassa järjestelmien käytettävyyttä, käyttöympäristöä sekä integrointimahdollisuuksia.

Työssä käytettiin opinnäytetyön tekijän laatimaa vaatimusmäärittelylistaa, jonka pohjalta järjestelmien ominaisuuksia käytiin läpi. Tähän pohjaan sisällytettiin teknisiä vaatimuksia, joita kyseisillä järjestelmillä pitää pystyä toteuttamaan. Vaatimusmäärittelyyn yritettiin kohdentaa asioita, jotka ovat oleellisia yrityksissä, johon tällaisia järjestelmiä voitaisiin ottaa käyttöön.

Työn toteutuksessa käytettiin neljää älypuhelinta, joiden mallit ovat seuraavat: 2 kappaletta Nokia 3, iPhone 5s, sekä Samsung J6. Työssä käytettiin eri valmistajien laitteita, koska eri valmistajilla on omalla tavallaan konfiguroidut käyttöjärjestelmät.

Tästä syystä osa MDM-järjestelmien toiminnoista saattaa toimia eri tavalla eri laitteissa eikä kaikki ominaisuudet välttämättä toimi toivotulla tavalla.
Ennen varsinaista käyttöönoton aloitusta laitteiden tila ja toimivuus varmistettiin. Kaikki laitteet eivät olleet viimeisimmissä Android-versioissa, sillä näiden päivitystä testattiin myös luvun 5.2.3 aikana.

5.2 Yleiset vaatimukset

5.2.1 Vaatimus 1.1: Laitteen käyttöjärjestelmä yhteensopiva hallintajärjestelmän kanssa

Yrityksen käyttöönottaessa mobiililaitehallintaa, on käytettävien laitteiden oltava yhteensopivia valittavina olevien hallintajärjestelmien kanssa. Ilman tätä yhteensopivuutta osa tai koko hallintajärjestelmä voi olla laitteen osalta toimimaton.

Intune

Laitteet kirjattiin (eng. enroll) järjestelmään eri tavoilla, jotta saataisiin dataa siitä, mitkä käyttöönottotyypit ovat tehokkaita sekä tuleeko laitteiden käyttöönotoissa ongelmia jollain tietyllä metodilla. Samsung-laitteen ja toisen Nokia 3-laitteen kirjaus toteutettiin Intunen Android kirjautumispoletilla (eng. Enrollment token). Tätä varten luotiin Corporate-owned dedicated devices välilehden alle uusi profiili OPN Dedicated Devices, joka luo kirjautumispoletin. Poletti sisältää QR-koodin, jonka avulla laitteelle voitiin ensimmäisen käyttöönottokerran yhteydessä lisätä työprofiili (eng. work profile), joka antoi mahdollisuuden lukea koodin ja näin linkittää puhelimen suoraan OPN Corporationiin.

Miradore Online

Sekä Samsung että yksi Nokia 3 asennettiin käyttämällä työprofiilin QR-asennusta. Tämä toimii samalla tavalla kuin Intunessa käytetty kirjautumispoletti, mutta polettia ei tarvinnut Miradore Onlinessa erikseen luoda, vaan löysi valmiina Work managed device provisioning-valikosta. Toinen Nokia 3 kirjattiin järjestelmään suoraan Miradore Online Clientilla. Tämä laite asennettiin ensin valmiiksi, jonka jälkeen siihen ladattiin Google Play Storesta Miradore Online Client, jonka avulla laite rekisteröitiin

järjestelmään. iPhonelle käytettiin sille tarkoitettua kirjausmenetelmää, joka käsitellään liitteessä 2.

5.2.2 Vaatimus 1.2: Laitteella voidaan käyttää työprofiilia tai laitteelle voidaan ladata erillinen client-sovellus

Kun laitteet halutaan hallintajärjestelmän alle, on laitteille löydyttävä joko tähän tarkoitettu luotettavasta lähteestä ladattavissa oleva mobiiliclient, tai vaihtoehtoisesti laitteella pitää olla käytettävissä työprofiiliominaisuus.

Intune

Ennen kuin laitteiden kirjaus Intuneen aloitettiin, kaikille laitteille varmistettiin, että ne ovat yhteensopivia Google Play Storesta/Apple Storesta löytyvän Intune Yritysportaali-applikaation kanssa. Samsung:lle sekä toiselle Nokia 3:lle luotiin työprofiili, ja laite linkittyi suoraan yritykselle, eikä Yritysportaali-applikaatiota tarvittu erikseen.

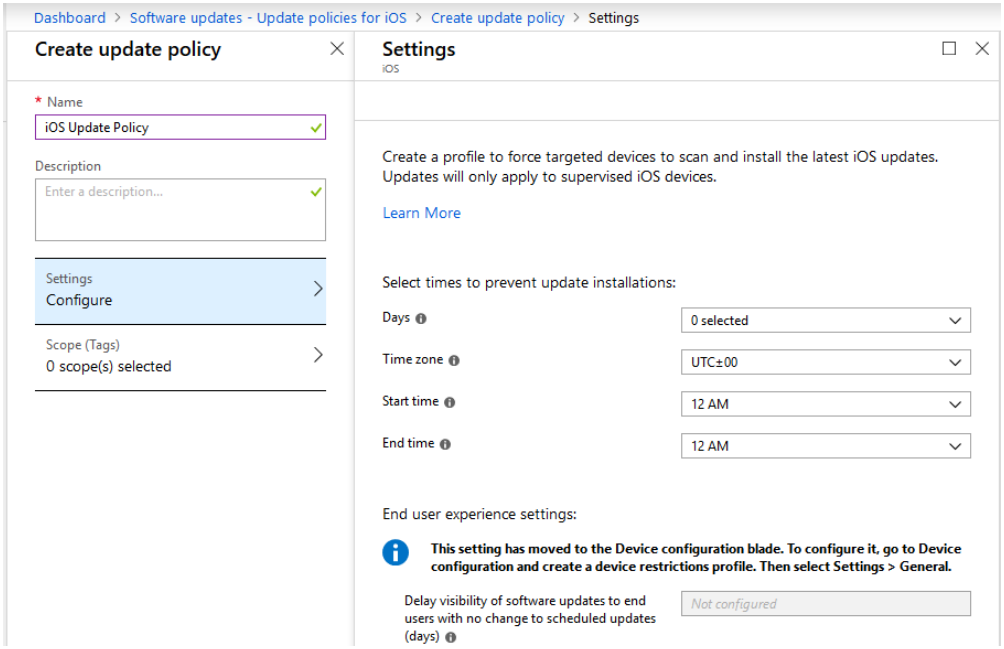
Miradore Online

Alussa varmistettiin, että sekä Google Play Storesta että Applen App Storesta löytyy Miradore Client, joka voitiin ladata laitteille. iPhonen kohdalla jouduttiin kuitenkin toimimaan eri tavalla. Liitteessä 2 kerrotaan, että laitteen kirjaus järjestelmään tapahtui Miradore Onlinen kautta, eikä sovellusta ladata App Storesta erikseen.

5.2.3 Vaatimus 1.3: Laitteen järjestelmäpäivityksiä voidaan hallita hallintajärjestelmästä

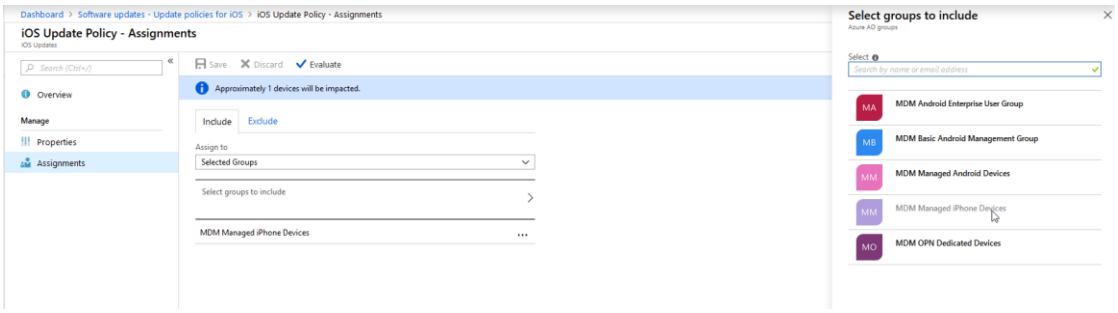
Intune

Intunen hallinnasta löytyvä Software updates osio piti sisällään perustasoisen hallinnan päivityksille. Tätä kautta pystyttiin hallinnoimaan Windows 10-, sekä iOS-laitteiden päivityksiä määrittämällä niille policyjä. Tässä kuitenkin keskityttiin ainoastaan iOS-käyttöjärjestelmän policyihin. Koska Intune ei säilö itse käyttöjärjestelmien päivityksiä, ei niiden hallinnointimahdollisuudet ole täysin vaikutettavissa. Kuitenkin luomalla uuden policyn (ks. Kuvio 4) voitiin määrittää hallituille iOS-laitteille päivitysten mahdolliset aikaikkunat.



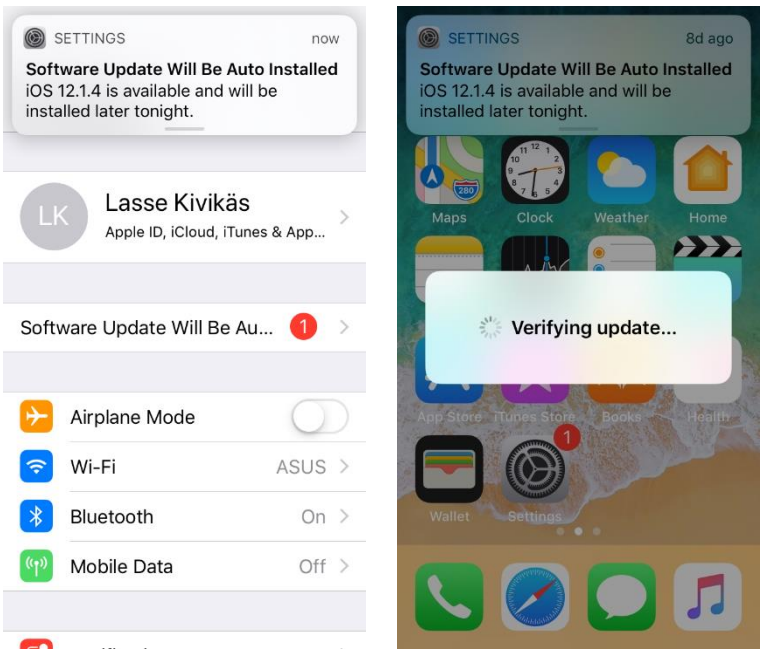
Kuvio 4 iOS-laitteiden päivitysmäärityksen asetukset

Tämän myötä voitiin valita kaikki päivät päiviksi, jolloin päivitysten asennus on estetty. Policyn luonnin jälkeen kohdistettiin policy aiemmin luodulle MDM Managed iPhone Devices -ryhmälle (ks. Kuvio 5).



Kuvio 5. Policyn kohdentaminen iPhone -laitteille

Laite jätettiin päivittämättä, jotta voitaisiin todentaa päivityksen estämisen mahdollisuus. Laite ilmoitti olemassa olevasta päivityksestä päivittäin ja ilmoitti asennuksen käynnistyksen yrityksestä illalla. Noin viikon kuluttua havaittiin, että laite ilmoitti päivityksen asennuksen alkamisesta (ks. Kuvio 6).



Kuvio 6. iPhonen päivitysilmoitus (vas.) sekä päivityksen alkaminen (oik.)

Miradore Online

iOS:n järjestelmäpäivityksien kontrollointi voitiin toteuttaa iOS:n järjestelmäversiosta 11.3 eteenpäin. IOS:n päivityksiä ei voitu täysin estää johtuen siitä, että päivitykset tulevat suoraan Applen toimittamina, eikä Miradore lataa tai hallinnoi päivityksiä. Päivitysten näkyvyyttä voitiin kuitenkin hallita niin, että näkeekö laitteen käyttäjä päivityksiä. Tarvittaessa näitä voitiin myös siirtää 1-90 päivää eteenpäin. Näiden ominaisuuksien käyttö kuitenkin vaati valvotun (eng. supervised) laitteen käytön. Tätä ei voitu toteuttaa testiympäristössä, sillä vaati oikean yrityksen rekisteröinnin. Samsungin laitteelle oli saatavilla KNOX:n kautta restrictions-osion Administration-välilehdellä Ovar-the-Air system upgrades -vaihtoehto. Tämän tarkoituksena olisi estää päivitysten asennus laitteelle. Tämä toiminto otettiin laitteelle käyttöön, mutta laite oli viimeisimmässä Android-versiossa valmiiksi, eikä toimintoa päästy testaamaan täysin. Tavallisessa Android-profiilin luonnissa päivityksiin ei voitu vaikuttaa.

5.2.4 Vaatimus 1.4: Laite voidaan uudelleen käynnistää etänä

Laitteen uudelleenkäynnistys voidaan vaatia tekemään tietyissä tilanteissa, joissa esimerkiksi laite on jäänyt tilaan, jossa näyttö ei reagoi kosketukseen. Tällöin voi olla myös tilanne, että laitteen fyysiset näppäimet, kuten virtanäppäin ei reagoi.

Intune

Intune tarjosi uudelleenkäynnistysmahdollisuuden etänä, jonka avulla kirjattu laite voitiin käynnistää etänä tarpeen vaatiessa. Tämä ominaisuus tarjosi vaihtoehdon ylittää käyttäjävaltuudet ja käynnistää laite ilman käyttäjän erillistä hyväksyntää. Tämä voi jossain tapauksissa olla myös tietoturvaa lisäävä ominaisuus.
Hallintaympäristöön kirjattujen laitteiden kohdalla tätä toimintoa kokeillessa ei saatu laitteita uudelleenkäynnistystilaan. Oletettavana on, että toiminto on toimiva, mutta koska järjestelmä ei anna lokitietoa ongelmasta, on ongelmanselvitys haasteellinen.

Miradore Online

Miradore tarjosi myös etänä toteutettavan uudelleenkäynnistyksen laitteille. Molemmat työprofiililla kirjatut Samsung ja Nokia 3 onnistuivat etäuudelleenkäynnistyksessä. Miradore lokitti hyvin prosessin etenemisen laitteen lokissa tapahtuman eri vaiheissa (queued, in progress, completed). iPhonella laitteen uudelleenkäynnistys ei onnistunut. Failed-ilmoitus ei kuitenkaan antanut enempää tietoa, miksei toiminut. Clientillä lisätyn Nokia 3:n kohdalla uudelleenkäynnistys-vaihtoehto oli poissa käytöstä, ja Miradore Online ilmoitti, että ominaisuus on sallittu vain työprofiilin omaaville laitteille.

5.3 Sovellusvaatimukset

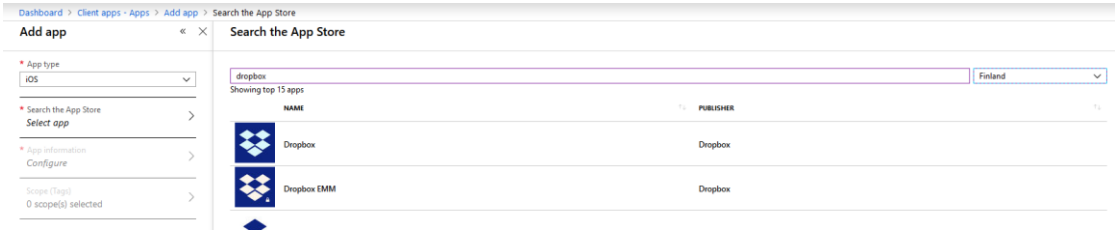
5.3.1 Vaatimus 2.1: Laitteelle voidaan jaella sovelluksia hallintajärjestelmän kautta

Yritys voi vaatia, että työlaitteilla ei käytetä henkilökohtaisia käyttäjätilejä, jotka antavat mahdollisuuden muun muassa Google Play Storen käyttöön ja sovellusten lataa-

miseen. Kuitenkin sovelluksia voidaan sovelluskaupoista tarvita. Tästä syystä hallintajärjestelmästä pitää löytyä mahdollisuus jaella sovelluskaupoista löytyviä tarvittavia sovelluksia käyttäjien laitteille.

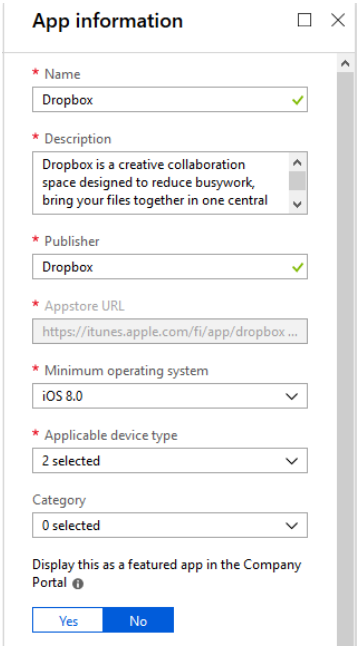
Intune

Sovellusten jako sovelluskaupoista pystyttiin toteuttamaan Intunen portaalista suoraan. Sekä Apple Store että Google Play Store olivat integroituna Intuneen, joten sovellusten hyväksymistä ei tarvinnut tehdä Storen portaalista. Sen sijaan ohjelmat pystyttiin hyväksymään suoraan Intunen sisältä sovellusta hakemalla (ks. Kuvio 7).



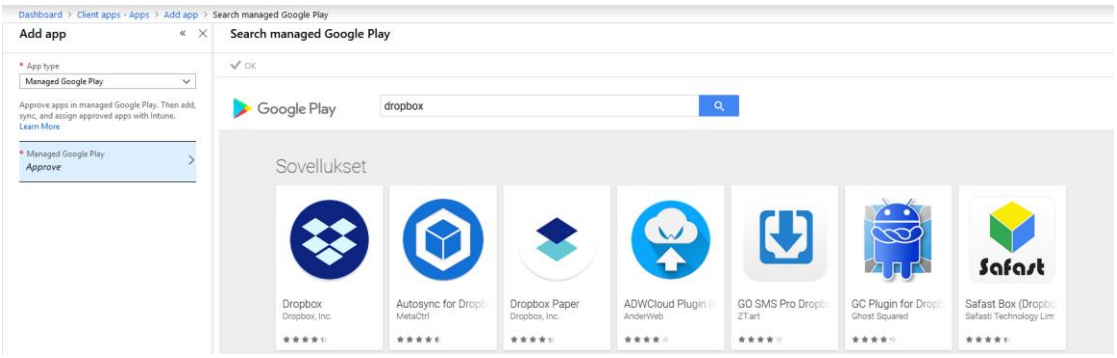
Kuvio 7. Sovelluksen haku Apple Storen valikosta Intunessa

Valitun ohjelman tiedot sekä App Storen tuoma latauslinkki löytyi App Information -valikosta (ks. Kuvio 8).



Kuvio 8. Valitun ohjelman tiedot

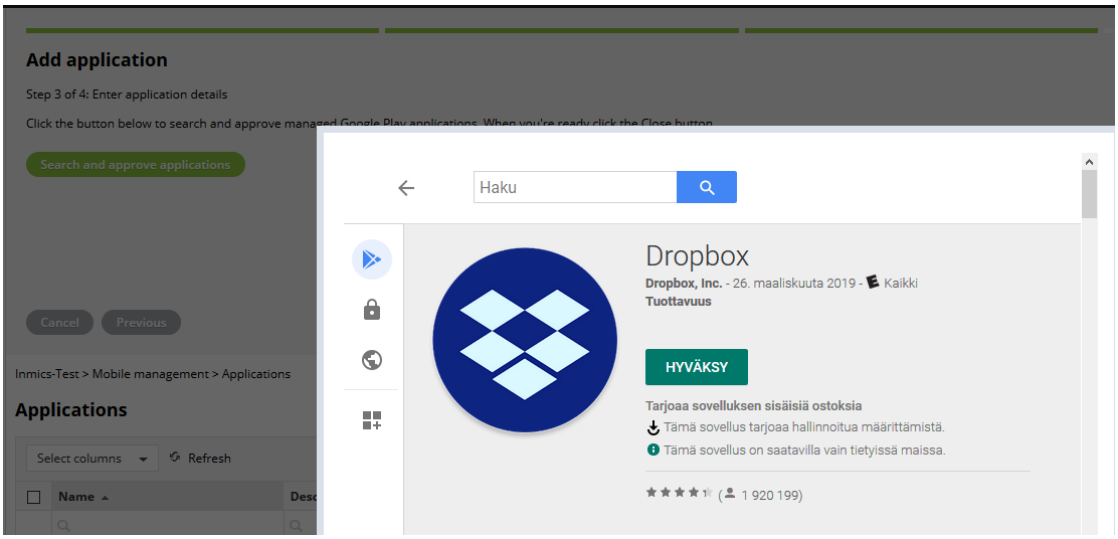
Tämä ominaisuus oli tullut myös Managed Google Playn sovelluksiin, joten erillistä sovelluksen hyväksymistä ei tarvinnut käydä tekemässä Google Playssa vaan tämä avautui Intunessa suoraan ohjelman valitsemisessa (ks. Kuvio 9).



Kuvio 9. Sovelluksen haku Managed Google Playn valikosta Intunessa

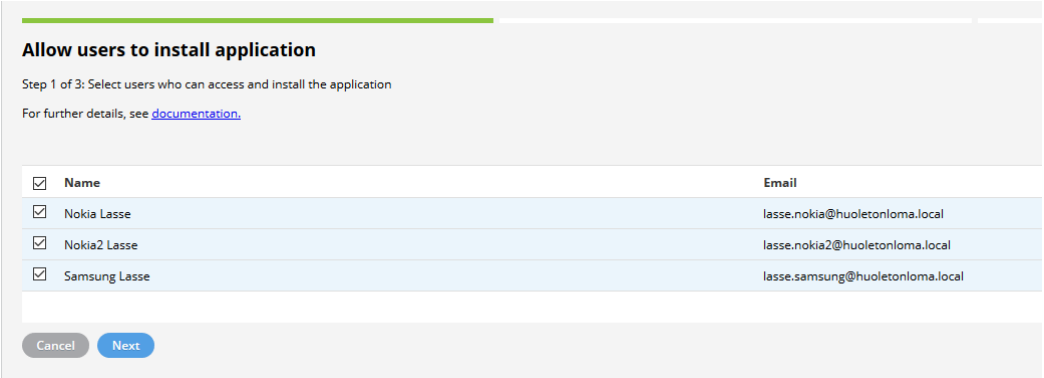
Miradore Online

Miradore Onlinen kautta sovelluksien lisäys voitiin tehdä Androidille Google Play Storen sekä Managed Google Play Storen kautta, tai APK pakettina. Työprofiilia käyttäville laitteille käytettiin Managed Google Playta, jossa hyväksyttiin sovellus Storessa joka tämän jälkeen tuli valittavaksi Miradore Onlinen hallintaan. Tämä ohjelma voitiin jaella nyt laiteille. Esimerkin vuoksi otettiin sovellus Dropbox, joka haettiin Miradore Onlineen (ks. Kuvio 10) Managed Google Play Storesta.



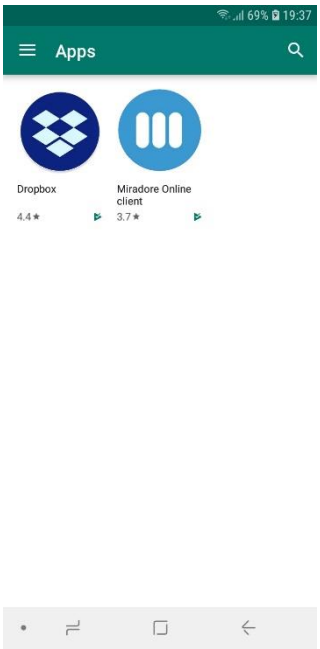
Kuvio 10. Dropbox-sovelluksen haku Miradore Onlinessa

Sovelluksen hyväksynnän jälkeen sovellus laitettiin saataville Android -laitteille. Tämän valittua voitiin päättää mille työprofiilin omaavalle laitteelle sovellus asennetaan (ks. Kuvio 11).



Kuvio 11. Sovelluksen salliminen laitteille

Sallimisen jälkeen laitteiden Managed Google Play Storeen tuli ladattavaksi Dropbox-sovellus (ks. Kuvio 12).



Kuvio 12. Ladattavat sovellukset Managed Google Play Storessa

5.3.2 Vaatimus 2.2: Laitteelle voidaan pakottaa sovelluksia hallintajärjestelmän kautta

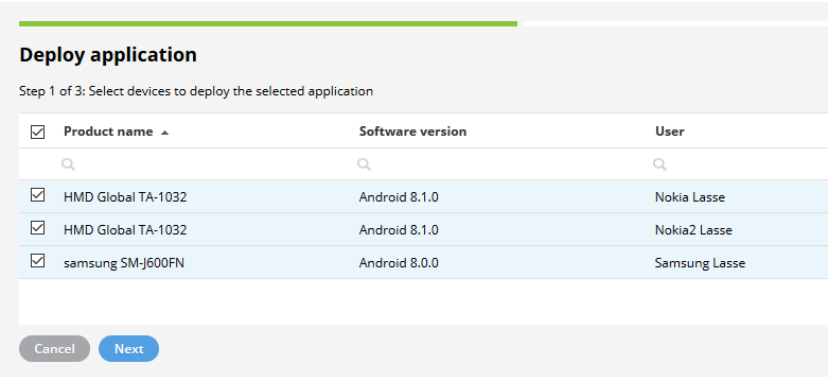
Kuten sovellusten jako, voidaan laitteelle vaadittaessa myös pakottaa ohjelmien asennus. Tällöin lähtökohtaisesti laitteen käyttäjän hyväksyntää kysytä, vaan ohjelman asennus alkaa laitteen taustalla ja käyttäjälle tulee sovelluksen asennuksesta pelkästään ilmoitus.

Intune

Sovellusasennuksen pakotuksessa käytettiin Slack-sovellusta ja sovellus jaeltiin sekä Managed Google Playsta, että Apple Storesta iPhonelle Intunen kautta. Slack-sovellus saatiin pakotettua kolmelle laitteelle neljästä. iPhone ilmoitti uuden sovelluksen asennuksesta, ja vaati Apple ID:n salasanaa, ennen kuin ohjelman asennus alkoi. Intune Company portaalin kautta lisätylle Nokia 3 puhelimelle ei saatu sovellusta pakotettua. Tämän aikana ei havaittu mitään mikä viittaisi virheeseen, mutta ohjelma ei asentunut laitteelle missään vaiheessa.

Miradore Online

Miradore Onlinen hallinnasta voitiin tarvittaessa myös jaella sovellukset ilman että sovelluksen asennuksesta erikseen ilmoitettiin. Tämä toteutettiin järjestelmän ohjelman jakelulla (eng. Deploy application). Sovellusjakelun testaamisessa käytettiin Slack-sovellusta, ja sovellus jaettiin kaikille Android-laitteille (ks. Kuvio 13).



Kuvio 13. Slack-sovelluksen jakelu Android-laitteille

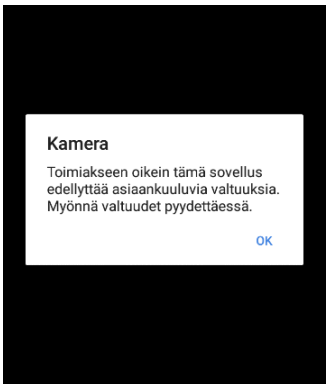
Sovellus saatiin jaeltua kaikille kolmelle Android-laitteelle onnistuneesti. iPhonelle lisättiin myös Slack-sovellus App Storesta, joka jaeltiin laitteelle. Tämän jälkeen laittelle tuli ilmoitus sovelluksen asennuksesta, jonka jälkeen Slack asentui laitteelle.

5.3.3 Vaatimus 2.3: Laitteen sovellusten käyttöä voidaan rajoittaa

Sekä Android- että iOS-laitteiden omia järjestelmässä valmiina olevia sovelluksia voidaan estää, ja täten rajata laitteen kaikkien ominaisuuksien hyödyntämistä. Vaatimusta läpikäydessä estettiin kamerasovellus kaikilta laitteilta, ja tarkastettiin, eroaako työprofiilin kautta lisättyjen laitteiden toiminta yritysportaalin kautta lisättyihin laitteisiin.

Intune

Intunen Device Configuration antaa mahdollisuuden rajoittaa sovelluksia puhelimesta, sekä asettaa estoja sovellusten asentamiselle. Toteutuksen aikana huomattiin, että kameran toiminta saatiin estettyä yritysportaalin kautta lisätyissä laitteissa. Erona iOS-laitteella ja Android-laitteella oli se, että iPhone hävitti kamerasovelluksen käyttäjältä puhelimesta. Yritysportaalilla lisätty Nokia 3 antoi virheilmoituksen (ks. Kuvio 14) kamerasovellusta avatessa. Työprofiilin kautta lisätyissä puhelimissa kameraa ei saatu estettyä. Tähän ei saatu selvyyttä miksi ei, sillä Intune ei antanut lokissa tarkempaa tietoa.

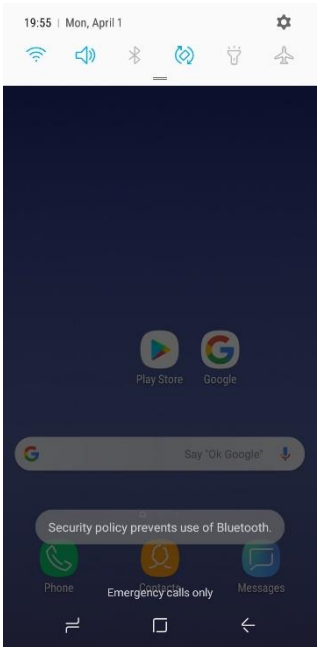


Kuvio 14. Nokia 3:n kamerasovelluksen ilmoitus

Useimmat Decvice restrictions -osion lisäominaisuudet olivat estetty kaikissa Android-pohjaisissa laitteissa, lukuun ottamatta Samsungin KNOX alustaa. Tämä saattaa hankaloittaa erityisesti yritysmaailmassa muiden Android-pohjaisten laitteiden suojaamista Intunen kautta.

Miradore Online

Miradore Onlinessa voitiin konfiguraatioprofiileilla estää tiettyjä toimintoja ja sovelluksia laitteista. Tässä esimerkissä laitteille luotiin profiili, joka esti kameran käytön laitteessa. iPhonelle asetettu esto piilotti kamerasovelluksen laitteesta kokonaan. Samsungin kohdalla kameraa ei laitteella näkynyt, ja lisäksi testattiin myös Bluetoothin käytön estoa, joka saatiin estettyä (ks. Kuvio 15).



Kuvio 15. Ilmoitus Bluetoothin käynnistyksen yrityksestä

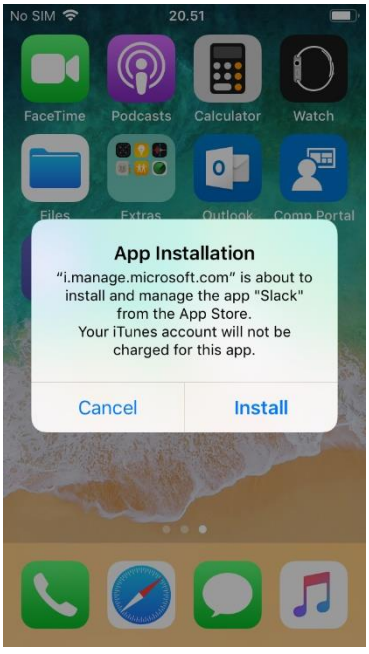
Nokia 3 -laitteilla testattiin sekä kameran käytön estoa, että Bluetoothin käytön estoa, mutta kumpaakaan sovellusta ei saatu estettyä. Lokien mukaan luodut estoprofiilit menivät kuitenkin laitteille onnistuneesti, joten tähän ei saatu selvyyttä miksi profiilit eivät toimineet.

5.3.4 Vaatimus 2.4: Laitteiden sovelluksien poistoa voidaan hallita hallintajärjestelmän kautta

Hallintajärjestelmän kautta laitteelle asennettujen ohjelmien poistaminen pitää olla mahdollista niiden sovellusten osalta, jotka laitteelle on asennettu joko yritysportaalin tai työprofiilin kautta. Poistamisen mahdollisuus riippuu tavasta, jolla ohjelmisto on laitteelle jaeltu. Jos ohjelmisto on jaeltu laitteelle pakotettuna asennuksena, ohjelmaa ei oletuksena pitäisi voida laitteelta itse poistaa. Jos taas sovellus on annettu Yritysportaaliin tai Play Storeen saataville, sekä käyttäjän itse asennettavaksi, pitää käyttäjällä olla mahdollisuus myös poistaa kyseinen sovellus.

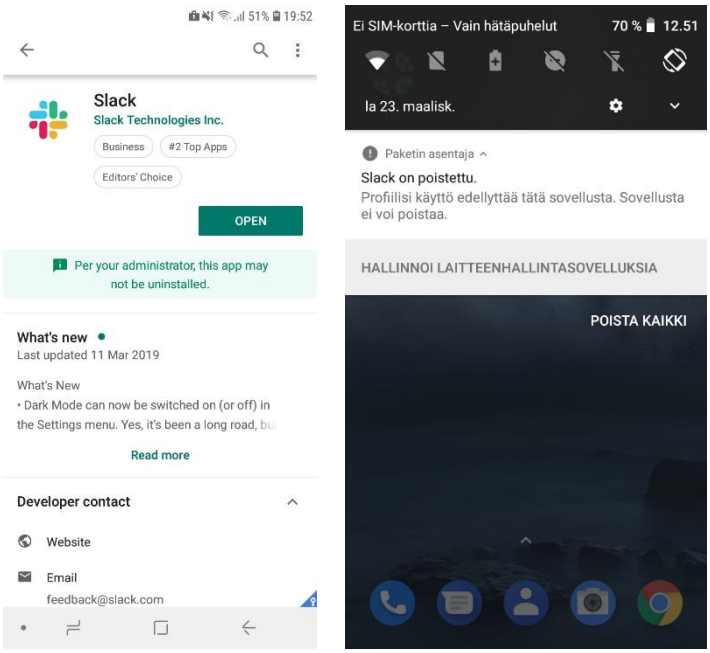
Intune

Tätä vaatimusta testattiin Intunessa sekä laitteelle pakotetulla sovelluksella, että vapaasti asennettavaksi jaetulla sovelluksella. Intunen kautta iPhoneen pakotettu Slack sovellus saatiin käsin poistettua puhelimesta, mutta ohjelma asentui hetken kuluttua takaisin (ks. Kuvio 16).



Kuvio 16. Slack-sovelluksen takasinasennus

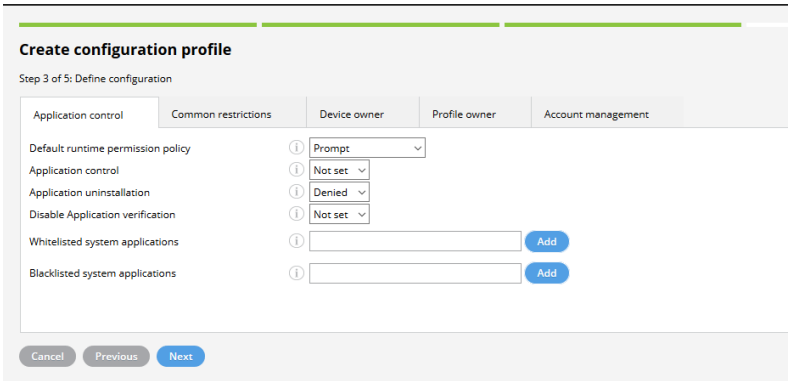
Intunen kautta työprofiilin omaaville Android-puhelimille pakotettua Slack-sovellusta ei saatu poistettua. Vaikka Nokia 3:een asennetut työprofiilin sovellukset tulivat sovelluslistaukseen näkymään, ei järjestelmä antanut poistaa tätä. Samsungin KNOX ei antanut mahdollisuutta poistaa ohjelmia kuin ainoastaan asennetun lähteen kautta, eli tässä tapauksessa Google Play Storen kautta. Molemmat laitteet antoivat Google Play Storessa saman ilmoituksen sovelluksen poiston mahdottomuudesta (ks. Kuvio 17). Yritysportaalia käyttävään Nokia 3:een ei saatu jostain syystä pakotettua eikä jaettua sovelluksia.



Kuvio 17. Play Storen ilmoitus laitteelle pakotetusta ohjelmasta Samsung-laitteella (vas.) ja järjestelmän ilmoitus ohjelman poistamisen mahdottomuudesta Nokia 3:lla (oik.).

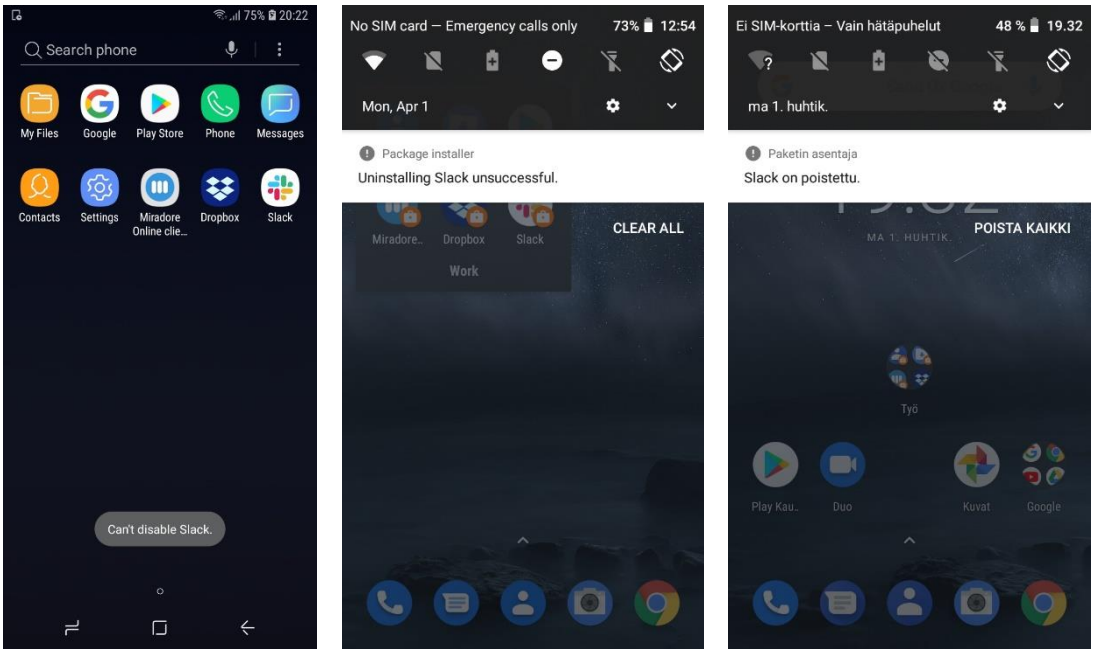
Miradore Online

Miradore Onlinen hallintajärjestelmässä laitteelle sekä asennetut, että jaellut sovellukset voidaan poistaa käyttäjälähtöisesti. Jos laitteelle pakotettujen sovellusten poistoa haluttiin rajoittaa, jouduttiin luomaan konfiguraatioprofiili, joka estää tämän toiminnon (ks. Kuvio 18).



Kuvio 18. Androidin sovellusten poiston estäminen profiililla

Samsungille oleva oma profiilikonfiguraattori mahdollisti myös tämän ominaisuuden käytön, ja kaikkiin Android-laitteisiin esto onnistui (ks. Kuvio 19). Toinen Nokia 3 ilmoitti että poisto on tehty, mutta ohjelma ei kuitenkaan poistunut laitteelta, ja toimi tämänkin jälkeen normaalisti.



Kuvio 19. Android-laitteiden Slack-sovelluksen poiston yritys

iPhonen kohdalla sovelluksen poiston esto vaati laitteen supervised-tilaan, jota ei pystytty käyttämään. Kuitenkin, jos sovellus oli jaeltu laitteelle ja se poistetaan, laite seuraavan synkronoinnin aikana asentaa sovelluksen takaisin.

5.4 TURVALLISUUSVAATIMUKSET

5.4.1 Vaatimus 3.1: Laitteen toimintoja voidaan seurata hallintajärjestelmän kautta

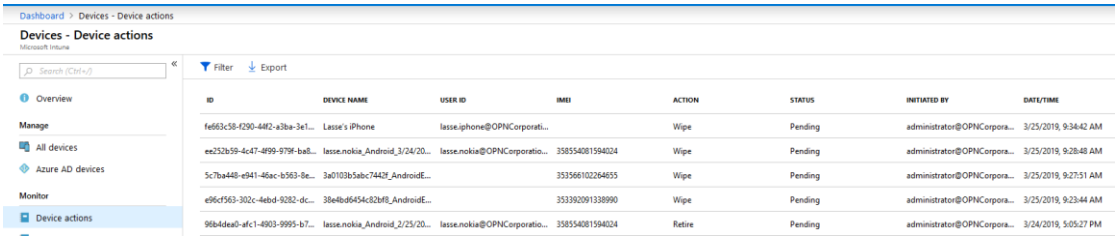
Laitteiden toimintojen perustasoista toimintaa on pystyttävä seuraamaan hallintajärjestelmän kautta. Tämän avulla yritys pystyy seuraamaan laitteidensa tilaa ja mahdollisia virhetiloja, ja reagoimaan niihin mahdollisimman nopeasti ja tehokkaasti.

Intune

Intunen lokitus laitteiden osalta oli yksinkertainen. Intune keräsi laiteosiossa kahta eri lokia. Autidointilokit (eng. Audit logs) ja toimintaloki (eng. Device Actions). Auditointiloki lokitti laitteille järjestelmän kautta tehdyt toiminnot, ja nämä lokit voitiin tarvittaessa exportata järjestelmästä ulos .csv-tiedoston muodossa. Audit loki antoi seuraavat tiedot:

- Tapahtuman päivämäärä ja aika
- Tapahtuman suorittanut käyttäjä
- Ohjelmiston nimi (Intunen tapauksessa Microsoft Intune portal extension)
- Toiminto
- Kohde
- Kategoria
- Status

Device Actions -loki antoi eriteltyjä historiatietoja laitteille ajetuista toiminnoista (ks. Kuvio 20). Tämä piti sisällään myös tietoja, kuten toiminnon suorittajan, toiminnon statuksen sekä ajankohdan.

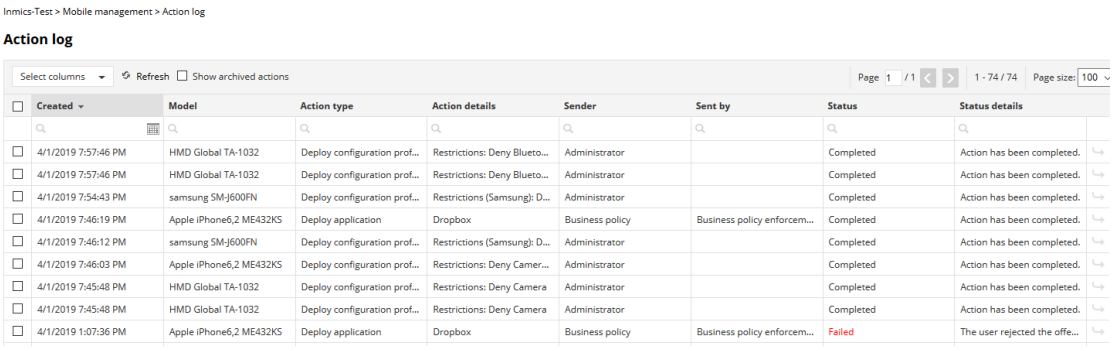


Kuvio 20. Kuva Device Actions -lokista

Miradore Online

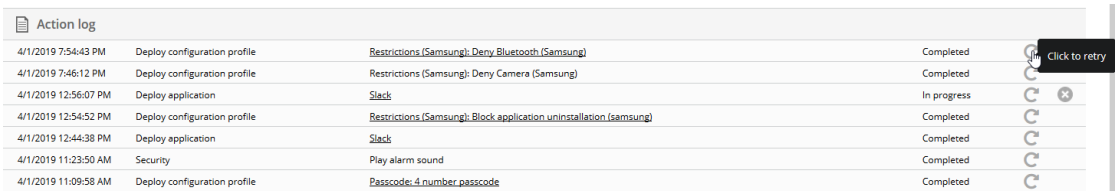
Miradore Onlinen lokitus oli yksinkertaistettu yhteen toimintalokiin (eng. Action log), joka lajitteli laitekohtaiset lokit myös laitehallinnan osioon yksittäisten laitteiden alle. Kuvio 21. Kuva näkyy, kuinka toimintaloki yksilöi kaikki tapahtumat, ja antoi tapahtuman statuksen lisäksi statustiedon (eng. Status detail), joka selvensi tapatumaa. Toimintaloki antoi seuraavat tiedot:

- Tapahtuman ajankohta
- Laitteen mallinimi
- Toiminnon tyyppi
- Toiminnon tiedot
- Toiminnon suorittaja
- Toiminnon lähtöpiste
- Toiminnon tila
- Tilan tiedot
- Käyttäjä



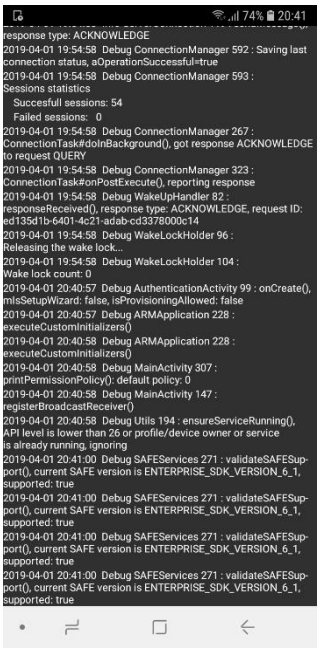
Kuvio 21. Kuva Miradore Onlinen toimintalokista

Laitekohtaiset lokit löytyivät laitteiden alta. Tämä helpotti tietyn laitteen lokien katsomista, ja tätä kautta pystyttiin ajamaan toimintoja uudelleen laitteelle (ks. Kuvio 22).



Kuvio 22. Samsung-laitteen laitekohtainen loki

Lisäksi Android-laitteiden Miradore Online Clientistä löytyi paikallisesti loki, joka päivittyi jatkuvasti (ks. Kuvio 23). Tämän avulla laitteen toimintoja voitiin seurata tarvittaessa myös ilman hallintajärjestelmää.



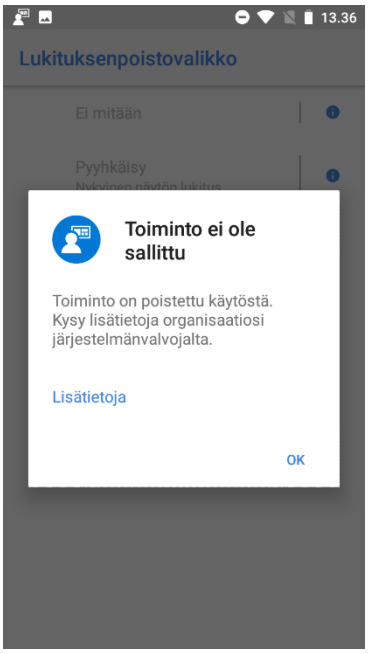
Kuvio 23. Samsung-laitteen paikallinen clientin loki

5.4.2 Vaatimus 3.2: Laitteelle voidaan pakottaa tietyn tasoinen näyttölukitus

Hallintajärjestelmän piirissä oleville laitteelle on pystyttävä pakottamaan tietyn tasoinen näyttölukitus, jolla luodaan lisäturvaa laitteelle. Lisäksi tähän liittyen myös laitteen näytön aikakatkaisun pituuteen on pystyttävä vaikuttamaan. Tämän tavoitteena on vaikeuttaa laitteella olevan datan varastamista ja väärinkäyttöä sen joutuessa vääriin käsiin.

Intune

Intunessa voitiin määrittää näyttölukitus eri osioista. Device Compliance -policyllä voitiin määrittää Intune kysymään laitteelta onko laitteelle asetettu näyttölukitusta. Oletustoimena Intune merkkaisi laitteen järjestelmään ’noncompliant’ -laitteena, jolloin nähtäisiin laitteet, jotka eivät ole toteuttaneet tätä vaatimusta. Vaatimuksen toteutumatta jäämisen estämiseksi voidaan Intune määrittää joko lähettämään sähköposti käyttäjälle ja muille valituille henkilöille, tai lukitsemaan laitteen etänä. Device Configuration -policyllä taas voidaan poistaa asetuksia käytöstä, kuten liian yksinkertaiset salasanat tai salasanattomat vaihtoehdot laitteen asetuksista (ks. Kuvio 24).



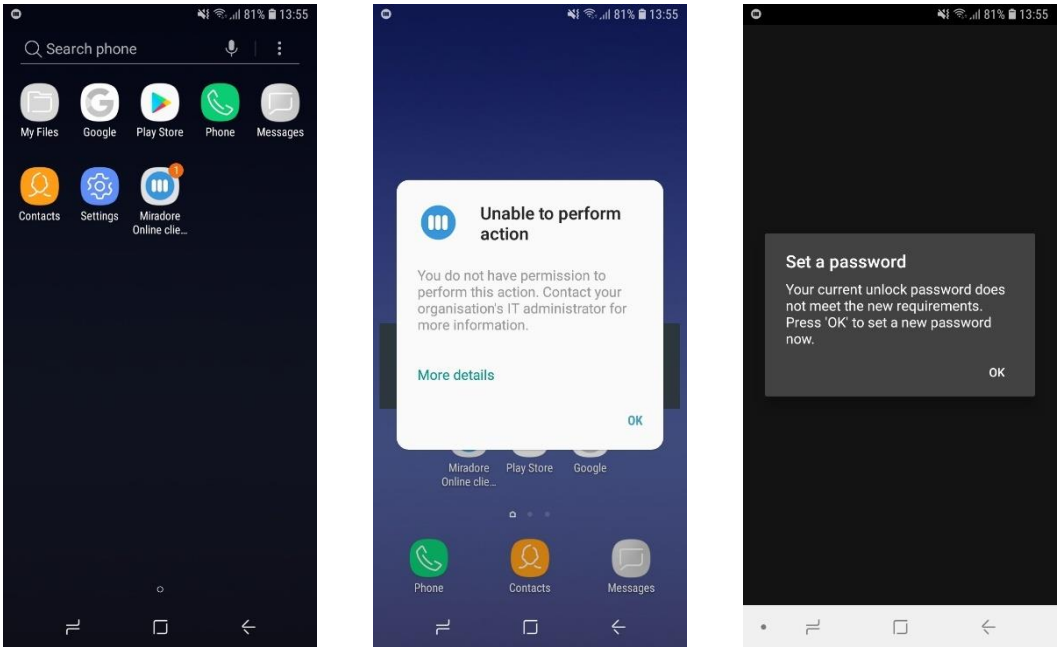
Kuvio 24. Näyttölukituksen tila Nokia 3:ssa

Miradore Online

Miradoren hallintajärjestelmästä voitiin laiteelle pakottaa näyttölukitus määrittämällä konfiguraatioprofiili sitä varten. Näistä profiileista oli luotu valmis pohja järjestelmään, joten sen luomien ei ollut tarpeellista, vaan valmis pohja voitiin jaella suoraan laitteille.

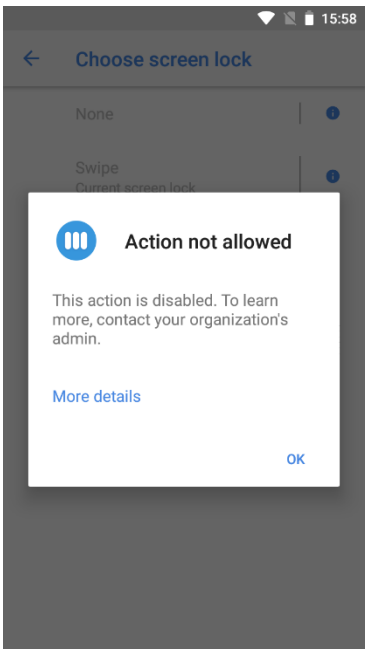
iPhonelle jaeltiin profiili, jossa määritettiin yksinkertainen salasana, jonka vähimmäispituus on 4 merkkiä. Profiilin jakelun jälkeen laitteelle tuli ilmoitus salasanan määrittämisestä, mutta vähintään kuudella merkillä. Tätä kuitenkaan ei voinut estää, vaan ilmoitus tuli joka kerta uudelleen näytölle.

Samsungille järjestelmä ilmoitti salasanamäärityksestä, ja esti tämän jälkeen osan laitteen sovelluksista (ks. Kuvio 25). Salasanan asettamisen jälkeen sovellukset vapautuivat käyttöön.



Kuvio 25. Estetyt sovellukset ja salasanan määritys

Nokia 3 -laitteille kyseistä ilmoitusta ei tullut, mutta kun asetukset tarkastettiin, huomattiin että suojattomat sekä kuviosalaus eivät olleet käytettävissä (ks. Kuvio 26). Ongelmana kuitenkin on, että salasanaa ei vaadittu laitteelta.



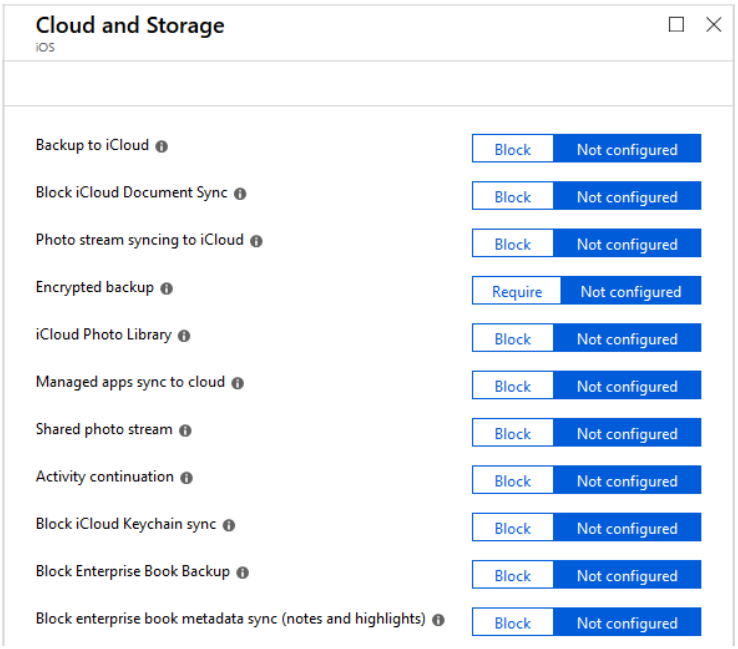
Kuvio 26. Nokia 3:n salasana-asetukset

5.4.3 Vaatimus 3.3: Laitteelle voidaan asettaa rajoituksia pilveen tallentamiselle

Jos yrityksen käytössä on oma verkkoympäristö, voi yritys vaatia estämään muiden pilvipalvelujen käytön työpuhelimissa. Tällä rajataan tietojen leviämistä palveluihin, joita ei yrityksessä tueta. Lisäksi datan seuranta pysyy selkeämpänä ja luotettavampana.

Intune

Riippuen oliko kyseessä iPhone vai Android ja onko laite kirjattu yritysportaalilla vai työprofiililla, vaihteli laitteiden asetukset. Device Configuration tarjosi iPhonelle mahdollisuuden rajoittaa suoraan vain iCloudin käyttöä. Tätä ei kuitenkaan tarvitse rajoittaa kokonaan, vaan Intune tarjoaa laajan mahdollisuuden rajata vain haluttuja osia pois (ks. Kuvio 27).



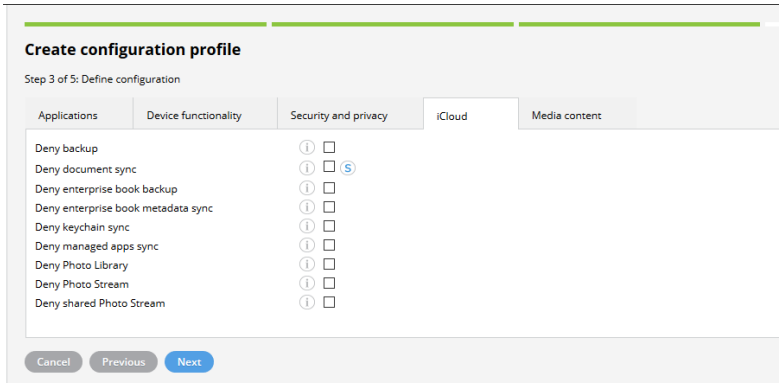
Kuvio 27. iCloudin rajausmahdollisuudet

Asetukset eivät vaatineet supervised-tilaa iPhonelle.

Androidin profiilissa mahdollisuudet olivat rajattu ainoastaan Google Backupiin, jonka lisäksi asetukset olivat saatavilla vain Samsung KNOX-alustalle. Android Enterprise profiilissa ei ollut asetusta pilvitallennuksen rajaukselle. Tämä kuitenkaan ei ole välttämätön kaikissa tilanteissa, sillä työprofiilin omaaviin laitteisiin ei työprofiilin puolelle voida ladata pilvisovelluksia, ellei niitä ole julkaistu yrityksen toimesta ladattavaksi.

Miradore Online

Miradore Onlinen konfiguraatioprofiileilla voitiin rajoittaa eri tasoisesti laitteiden mahdollisuuksia tallentaa tai varmuuskopioida pilvipalveluihin. iOS -käyttöjärjestelmälle tarjottiin mahdollisuus rajata iCloudin käyttöä useilla vaihtoehdoilla (ks. Kuvio 28), tai estää sen käyttö kokonaan.



Kuvio 28. iCloudin rajausmahdollisuudet konfiguraatioprofiilin luonnissa

Androideille suoraa pilveen tallennuksen rajausta ei ollut saatavilla, mutta konfiguraatioprofiileilla voidaan lisätä haluttuja sovelluksia mustalle listalle, jolloin sovelluksia ei pysty itse laitteille asentamaan.

5.4.4 Vaatimus 3.4: Laite voidaan lukita etänä hallintajärjestelmän kautta

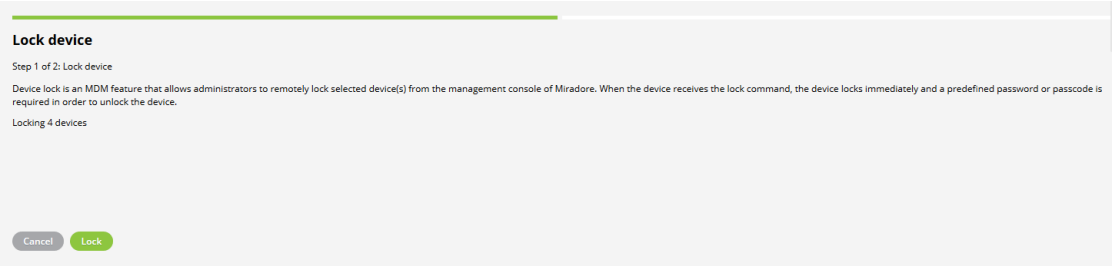
Jos laite onnistutaan varastamaan, tai laite jää käyttäjältä johonkin, jossa ulkopuolinen henkilö voi päästä laitteeseen käsiksi, on laite tällaisia tilanteita varten oltava etänä lukittavissa. Näin laitteella olevan datan väärinkäyttö voidaan minimoida tai estää kokonaan.

Intune

Etälukitus voidaan toteuttaa devices-valikosta. Etälukitusta testattiin kaikille laitteille, ja toteutettiin onnistuneesti kolmelle laitteelle neljästä. Työprofiilin omaava Nokia 3 ei jostain syystä lukittunut, vaikka Intune antoi ilmoituksen onnistuneesta lukituksesta. Syytä tälle ei löydetty.

Miradore Online

Miradore Onlinen hallintajärjestelmästä laitelistauksen puolelta löytyi myös etälukitusmahdollisuus. Miradore Onlinessa voitiin valita kaikki neljä laitetta kerralla lukittavaksi (ks. Kuvio 29).



Kuvio 29. Laitteiden yhteislukitus

Kaikki neljä laitetta saatiin lukittua tällä toiminnolla. Toiminnon suorittamisen ja laitteiden lukittumisen välillä oli sama kaikille.

5.4.5 Vaatimus 3.5: Laitteen työprofiili tai yritysportaali voidaan poistaa tai tyhjentää etänä laitteelta

Tilanteissa, joissa puhelin on kadonnut, tai työntekijä on lopettanut yrityksen palveluksessa mutta pitää laitteen itsellään, tulee vastaan tilanne, jossa yrityksen tiedot saattavat jäädä lopettaneen työntekijän haltuun. Tällöin vaatimuksena on mahdollisuus poistaa laitteelta yrityksen tiedot ilman, että laitteen omiin asetuksiin kosketaan. Tämä tarkoittaa, että kaikki sovellukset ja asetukset, joita on määritetty hallintajärjestelmän toimesta, voidaan myös poistaa etänä ilman käyttäjän hyväksyntää.

Intune

Intunen hallinnasta löytyvällä retire -toiminnolla laitteen yritysprofiili voitiin poistaa. Tämä toiminto löytyi vain yritysportaalia käyttävistä laitteista. Työprofiililla lisätyt laitteet voitiin poistaa suoraan delete -toiminnolla, joka hävitti työprofiilin laitteesta ja poisti samalla laitteen Intune-portaalista.

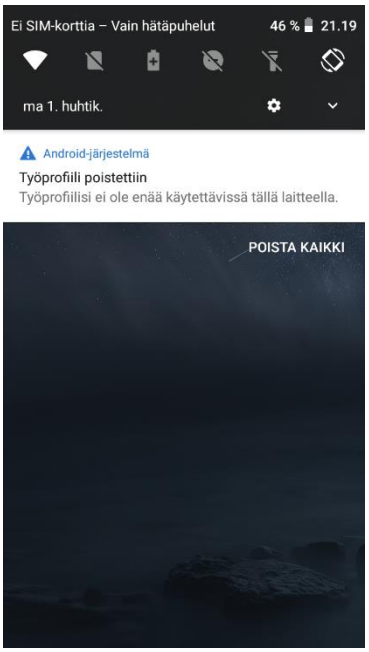
Miradore Online

Miradore Onlinen hallintajärjestelmässä oli mahdollisuus poistaa työprofiili eri tavoilla, riippuen tavasta, jolla laite on kirjattu alun perin järjestelmään. Samsung oli kirjattu järjestelmään QR Setupilla, joka loi puhtaan työprofiilin laitteelle. Tätä profiilia ei voitu poistaa, vaan ainoa vaihtoehto järjestelmän mukaan oli tehdä laitteelle

täysi tyhjennys.

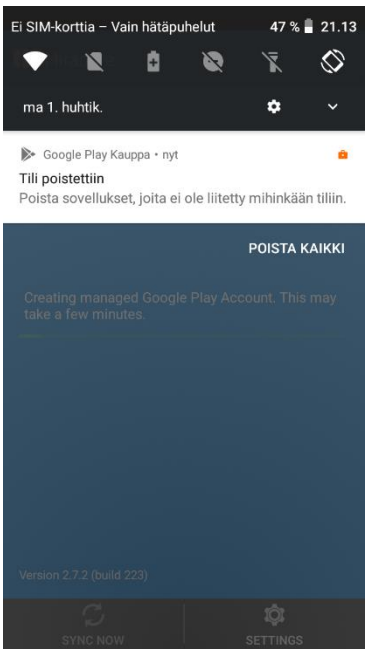
iPhonelle toteutettu unenroll-toiminto poisti hiljaisesti kaikki asennetut sovellukset sekä Miradore clientin, sekä palautti kamerasovelluksen käyttöön.

Toisen Nokia 3:n työprofiili saatiin poistettua unenroll-toiminnolla. Tämän toiminnon suoritettua laite ilmoitti, että työprofiili on poistettu (ks. Kuvio 30).



Kuvio 30. Nokia 3:n työprofiilin poisto

Laitteelta voitiin myös poistaa pelkästään Managed Google Play tili, joka ei poistanut Miradore client -sovellusta laitteelta, vaan pelkästään irrotti tilin laitteesta (ks. Kuvio 31).



Kuvio 31. Tilin poisto Nokia 3:sta

5.4.6 Vaatimus 3.6: Laite voidaan palauttaa tehdasasetuksiin hallintajärjestelmän avulla

Laitteen palautus tehdasasetuksiin tarkoittaa laitteen kokonaisvaltaista tyhjentämistä kaikesta siinä olevasta datasta, sovelluksista ja määritetyistä asetuksista. Tämän on tarkoitus luoda tietoturvaa laitteelle, jos se päätyy varastetuksi tai hukkuu. Näissä tilanteissa on oleellista, että laite saadaan tyhjennettyä vähintään yrityksen omasta datasta.

Intune

Riippumatta laitteen kirjaustavasta Intuneen, pitäisi kaikki laitteet pystyä Intunen järjestelmästä palauttamaan tehdasasetuksiin. Tämä testattiin kaikilla laitteilla Intunen Wipe-ominaisuudella. Toteutuksessa huomattiin, että vain yritysportaalia käyttävät laitteet saatiin palautettua tehdasasetuksille. Nokia 3:n palautus käynnistyi kuitenkin vasta noin 5 minuutin kuluttua. iPhone saatiin palautettua ilman viivettä. Työprofiilia käyttäneistä laitteista saatiin poistettua Wipe-ominaisuutta käyttäen pelkästään työprofiili, mutta laitteen käyttöjärjestelmä jäi entiselleen.

Miradore Online

Laitteiden tehdasasetuksiin palautusta varten Miradore Onlinesta löytyy wipe-ominaisuus, jolla laite saadaan palautettua tehdasasetuksiin. Tehdasasetuksien palautus saatiin toteutettua sekä iPhonelle, että Samsungille. Molemmat laitteet lähtivät suoraan palauttamaan itseään, ilman erillistä ilmoitusta. Nokia 3- puhelimista poistui ainoastaan työprofiili, mutta järjestelmä ei palautunut tehdasasetuksille. Molemmat Nokia 3-laitteet olivat lisätty asennuksen jälkeen työprofiililla, joten toinen laitteista palautettiin käsin alkutilaan. Tälle laitteelle tehtiin QR asennus, jotta voitiin testata tehdasasetusten palauttamista etänä. Lopulta tämä laite saatiin palautettua käyttämällä wipe-ominaisuutta.

6 Tulokset

Asiakasympäristön kartoitusvaiheessa saadaan lähtökohtaisesti tarpeeksi tietoa, jotta yritys osaa tarjota oikeanlaista palvelua asiakkaalle. Asiakkaalla voi olla jo valmiiksi ajateltu palvelu tai tuote, joka halutaan yrityksen käyttöön, mutta monesti palveluita tuottavan yrityksen puolelta osataan sanoa ympäristön koon ja monimuotoisuuden mukaan mikä tuote on toimivin kyseisessä ympäristössä. Luvuissa 6.1-6.2 on käyty läpi molempien käyttöjärjestelmien vaatimukset sekä arvosteltu ne numerolla 0-5 numeron 0 ollessa huonoin ja numeron 5 ollessa paras. Tämä arvostelu on tehty työn suorittajan omalla kokemuksella.

6.1 Microsoft Intune

Taulukko 1:ssä on käyty läpi Microsoft Intunen vaatimukset sekä kommentoitu vaatimuksessa käsiteltävää asiaa.

Taulukko 1. Microsoft Intunen tulokset

Vaatimus	Arvosana	Tarkemmat tiedot
1.1	4 / 5	Kaikkien laitteiden käyttöjärjestelmät olivat yhteensopivia Intunen kanssa. Androidin kirjausprosessia varten piti luoda kirjautumispoletti. Tätä varten piti luoda uusi profiili, jotta poletin sai luotua.
1.2	5 / 5	Intunen mobiilisovellus löytyi sekä Google Play Storesta että App Storesta. Lisäksi Androidille oli saatavilla työprofiili, jonka käyttööotto oli yksinkertaista. Intunessa piti luoda erikseen profiili, jonka avulla voitiin luoda kirjautumispoletti.
1.3	4 / 5	Järjestelmäpäivitysten hallinta siltä osin kuin se oli mahdollista, oli helppoa ja toiminnossa ei ollut liikaa vaiheita tai epäselviä kohtia.
1.4	0 / 5	Arvosanaa ei voitu antaa tälle vaatimukselle, koska ominaisuutta ei saatu testattua.
2.1	5 / 5	Sovellusjakelut Intunesta toimivat kuten odotettiin. Sekä Google Play Storelle että App Storelle olivat integroituna Intuneen, joten siirtymistä näihin palveluihin erikseen ei tarvittu.
2.2	4 / 5	Sovellusjakeluiden pakotus laitteille oli kohtalaisen yksinkertaista. Sovelluksen jakelu tapahtui aina ryhmälle, johon laite kuului, suoraan laitteille jakelua ei voitu tehdä.
2.3	3 / 5	Toiminnon löytäminen Intunesta kesti hetken, sillä ominaisuuden määrittämistä ennen piti luoda laitekonfiguraation puolella konfiguraatioprofiili oikealle alustalle, valita oikea profiilityyppi ja tämän jälkeen vasta valita listassa haluttu sovellus.
2.4	5 / 5	Pakotettuja sovelluksia ei saatu poistettua laitteilta, joten tämä toiminto toimi odotetusti ilman erillisiä toimenpiteitä.
3.1	3 / 5	Lokitus itsessään oli yksinkertainen ja selkeä, mutta esimerkiksi failed-ilmoitukset jäivät ilman seltettä, mikä vaikeuttaa ongelmanselvityksiä.
3.2	4 / 5	Toiminnon käyttö vaati erillisen policyn luonnin, johon kyseinen toiminto piti aktivoida ja tämän jälkeen määrätä oikealle erikseen luodulle laiteryhmälle.
3.3	3 / 5	Androidin puolella toiminnot oli rajattu Samsungin KNOX-alustalle. iCloudin käyttöä voitiin kontrolloida laajalti iPhonelle.
3.4	4 / 5	Toiminnon käyttö oli yksinkertaista ja löytyi helposti Intunen laitteet-osiosta. Tämä kuitenkin voitiin tehdä vain yhdelle laitteelle kerrallaan.
3.5	5 / 5	Laitteen tyhjennys onnistui laitteet-osiosta helposti, eikä käytön suhteen ilmennyt ongelmia.
3.6	4 / 5	Toiminto löytyi laitteet-osiosta, ja tämän käyttö oli nopeaa ja yksinkertaista ilman ongelmia. Yhden laitteen reagointi oli hiukan muita pidempi.
Yht.	**52 / 70**	

Microsoftin Intune on laaja ja vahvapohjainen tuote, joka tarjoaa mobiililaitehallinnan lisäksi myös oman työasemahallinnan. Microsoftin EMS (Enterprise Mobility Security) on vahva lisäturvaa tuova kokonaisuus, johon Intune kuuluu Azure Active Directory Premium- sekä Azure AD Rights Management-palveluiden kanssa. Nämä palvelut mahdollistavat käyttäjien sekä ryhmien hallinnoinnin suoraan pilvestä. Myös MFA:n (Multi Factor Authentication) mahdollisuus palveluissa lisää laitteiden ja järjestelmien välistä tietoturvaa. Lisäksi sen integrointimahdollisuudet muiden yritysten palveluihin ovat erittäin laajat, mikä tekee järjestelmästä hyvän sulauttaa valmiiseen ympäristöön ja palveluihin. Intunen käyttöympäristö järjestelmän hallitsijan näkökulmasta voi vaikuttaa hiukan monimutkaiselta. Järjestelmän All Services listaa kaikki Intunen palvelut, joita on yhteensä kahdeksantoista kappaletta. Palvelut ovat kuitenkin eroteltu selkeästi toisistaan, mutta ominaisuuksiin tutustuminen vie aikaa ja palveluihin pitää jaksaa tutustua huolella. Hyvänä puolena näen järjestelmässä sen yhteentoimivuuden Azure Active Directoryn kanssa, joka näyttää muun muassa samoja käyttäjädatasivuja kuin Intunessa. Kuitenkaan Intunen lokitus ei anna järjestelmän käyttäjälle tarpeeksi dataa virheistä, mikä saattaa hidastaa merkittävästi virheenjäljitystä sekä ongelmanratkaisua. Kuitenkin Microsoftin tekninen foorumi Technet tarjoaa monissa asioissa erittäin paljon tietoa ja tukea.

6.2 Miradore Online

Taulukko 2:ssa on kuvattu Miradore Onlinesta saadut tulokset ja kommentoitu vaatimuksessa käsiteltyjä asioita.

Taulukko 2. Miradore Onlinen tulokset

Vaatimus	Arvosana	Tarkemmat tiedot
1.1	5 / 5	Kaikkien laitteiden järjestelmät olivat yhteensopivia Miradore Onlinen kanssa. Kirjautumispolettia ei tarvinnut erikseen luoda, vaan poletti oli valmiiksi luotuna järestelmässä.
1.2	5 / 5	Miradore onlineen löytyi Google Play Storesta ja App Storesta sovellus, jota pystyttiin käyttämään käyttöönototssa.
1.3	4 / 5	Järjestelmäpäivityksiä voitiin iOS:lle hallinta 11.3 versiosta eteenpäin, eikä päivityksien asennusta voitu täysin estää. Samsungin KNOX-asetuksista voitii käyttää Over-the-Air system upgrades estoa, mutta tämän toimintaa ei saatu työssä todennettua.
1.4	3 / 5	Ominaisuus oli tarjolla ainoastaan työprofiilin omaaville laitteille. Toiminnallisuuden käyttö oli kuitenkin helppoa.
2.1	4 / 5	Toiminnallisuuden käyttö helppoa, mahdollisuus käyttöö Google Play Storea sekä Managed Google Playta erikseen. iOS:lle sovellusten jakelu mahdollista mutta ei suoraa liittymää App Storeen, vaan asennus toimii sovelluksen ID:n avulla.
2.2	4 / 5	Sovellusjakelun pakotus oli helppo toteuttaa laitteille. Mahdollisuutena jaella yksittäisille laitteille, tai tagien perusteella ryhmille. Vaatii kuitenkin jokaiselle laittelle tag-merkinnän, jolla pystytään hakemaan samannimiseksi tagilla merkityt laitteet.
2.3	4 / 5	Konfiguraatioprofiililla voitiin luoda käyttöestoja laitteen sovelluksille. Konfiguraatioprofiilin käyttö oli yksinkertaista ja selkeää, kun vaihtoehdot oli eritelty selvästi. Kaikille laitteille ei saatu pakotusta onnistuneesti tehtyä.
2.4	4 / 5	Poiston esto piti erikseen toteuttaa konfiguraatioprofiililla, ja tämä voitiin toteuttaa kaikille laitteille, paitsi iOS:lle, joka vaati supervised-tilan.
3.1	5 / 5	Miradore Onlinen lokit olivat hyvät ja selkeät. Status-tilan lisätieto helpotti ongelmanratkaisua. Laitteen omista tiedoista löytyi laitteen yksilöity loki. Lisäksi laitteelta itseltään löytyi loki, jota pystyi tarkastelemaan Miradore clientistä.
3.2	5 / 5	Miradoren valmiiksi luoma salasanaprofiili nopeutti toiminnon käyttöä, eikä sitä tarvinut kuin jaella laitteille suoraan. Toimenpide oli myös itse tehtynä helppo ja nopea, sekä käyttöjärjestelmän mukaan antoi paljon vaihtoehtoja.
3.3	2 / 5	Pilveen tallennuksen rajaukset olivat suppeat, vaikka ohjelmien lisäys mustalle listalle olikin mahdollista. iCloudin käyttöä pystyi rajoittamaan jonkin verran.
3.4	5 / 5	Toiminnon käyttö oli yksinkertainen ja toiminnon pystyi ajamaan useille laitteille kerralla.
3.5	4 / 5	Toiminto löytyi muiden tavoin helposti laitevalikosta, jossa voitiin valita halutut laitteet, joille toiminto suoritetaan. Yhtä laitetta lukuunottamatta toiminto toimi odotetusti.
3.6	4 / 5	Wipe-ominaisuuden käyttö jälkeenpäin lisätylle työprofiilille ei toiminut odotetusti, mutta ominaisuus itsessään oli helppokäyttöinen sekä selkeä.
Yht.	**58 (55) / 70**	Sulkuihin merkitty luku on pistekertymä, josta on otettu pois vaatimuksen 1.4 pisteet. Intune-vertailussa ominaisuutta ei voitu arvioida ja täten lopputulokseen annettiin myös vertailukelpoinen pistekertymä.

Miradore saattaa yrityksenä ja tuotteena jonkin verran tuntemattomampi varsinkin ulkomaiden käyttäjille. Kyse on suomalaisesta yrityksestä, joka on tehnyt toimivan ja selkeän tuotteen mobiililaitehallintaan. Miradore Online on myös mahdollista integroida palveluihin, kuten Windows sekä Azure Active Directoryihin. Kuitenkaan suoraa tietoa integroitavista järjestelmistä ei löytynyt. Itse järjestelmä on erittäin selkeäkäyttöinen, ja sen opetteluun meni huomattavasti vähemmän aikaa kuin Intunen opetteluun. Palveluita Miradore Onlinesta löytyy kuitenkin reilusti ainakin mobiililaitteiden hallintaan, ja esimerkiksi käyttäjäkohtaisesti voidaan ottaa MFA käyttöön suoraan saman järjestelmän sisälle. Positiivisena asiana koin järjestelmän selkeämmän lokituksen, joka antoi kaikista lokiin tallennetuista viesteistä jonkinlaisen selityksen, mikä teki ongelmanselvityksestä paljon tehokkaampaa. Myös järjestelmän käyttöönotto tehtiin helpoksi. Ensimmäisellä käyttökerralla sai itse valita järjestelmän osat, joihin haluaa ohjeistetun käyttöönoton. Vaikka käyttöympäristö oli englanninkielinen, suomalaiselle tukea voi tuoda suomenkielinen tukipalvelu ja yhteydenottoa helpottava chat-mahdollisuus.

Vaikka pistemäärät ovat lähellä toisiaan, vaatimusmäärittelylistan pohjalta läpi käytyjen asioiden jälkeen suosittelisin melkein yksinomaan Miradore Onlinen valintaa yritykselle. Intunen vahvuudet näkyvät yksityiskohtaisemmassa lajittelussa ja toiminnoissa, ja niistä teknisesti taitava asiantuntija saa paljon irti. Kuitenkin Miradore Onlinen tarjoaman järjestelmän yksinkertaisuus ja helppokäyttöisyys on vahva etu, kun suunnataan yrityksiin, jossa on paljon laitteita ja käyttö yritetään pitää yksinkertaisena.

7 Pohdinta

Työn tavoitteena oli saada yritykselle vertailulista kahdesta mobiililaitteiden hallintajärjestelmästä, jonka avulla voidaan valita asiakkaan ympäristöön sopivampi vaihtoehto. Tässä tavoitteessa onnistuttiin, ja vaatimusmäärittelylistan pohjalta tehty vertailu kahdesta järjestelmästä saatiin toteutettua. Vertailulistassa käsiteltävien asioiden määrä ja aiheet valittiin henkilökohtaisesti sillä perusteella, mitkä voisivat olla asiakasympäristöissä sekä päivittäisiä että turvallisuutta lisääviä ominaisuuksia. Tutkimuksen luotettavuus perustui työn suorittajan henkilökohtaiseen kokemukseen järjestelmistä, ja ennestään kokemuksen määrä oli suhteellisen pieni. Työtä varten ei

etsitty muita samankaltaisia vertailuja. Tämä johtui siitä, että vertailupohja ei perustunut mihinkään valmiiseen listaan, vaan luotiin itse. Tällöin myös vertailukelpoisen materiaalin löytäminen olisi haastavaa. Järjestelmistä löytyvien ominaisuuksien määrä on hyvin laaja ja vaihteleva, ja kaikkien ominaisuuksien läpikäynti vaatisi suuremmat resurssit sekä laajemman tutkimuspohjan.

Työn suunnitteluvaiheessa pääasiallinen ongelma oli vaatimusmäärittelylistan suunnittelu. Lista haluttiin pitää selkeänä ja tiiviinä, mutta kuitenkin sen verran monipuolisena, että järjestelmien vertailussa saataisiin selviä tuloksia eroista. Järjestelmien läpikäynnissä huomattavia haasteita ei kohdattu. Microsoftin Intune oli alustana tuttu mutta vähän käytetty, ja Miradore Online oli uusi tuote, johon ei ollut kosketuspintaa. Aihepiiri itsessään on uudempi ja sen hyödyntäminen on jäänyt omasta kokemuksesta pieneksi yritysmaailmassa. Toisin kuin työasemien hallinta, mobiililaitteita ei vielä nähdä välttämättä samanlaisena tietokonemaisena laitteena eikä näin ajatella laitteen olevan yhtä suuri riski kuin oma kannettava tietokone töissä.

Työtä voisi laajentaa useaan suuntaan. Useampia järjestelmiä voitaisiin ottaa vertailuun mukaan, jonka avulla voitaisiin tarjota vielä useampaa vaihtoehtoa yrityksille. Lisäksi järjestelmät pitävät sisällään useita ominaisuuksia, joita voisi käsitellä enemmän. Näin saataisiin huomattavasti parempi käsitys järjestelmistä, mitä kaikkea niillä todellisuudessa pystyy tekemään sekä miten niiden käyttöä voitaisiin soveltaa eri tyyppisissä ympäristöissä.

Oma käsitykseni mobiililaitteiden hallintajärjestelmistä on laajentunut työn aikana paljon. Lisäksi käsitys mobiililaitteiden hallinnasta on parantunut ja omakohtainen ymmärrys sen tärkeydestä yritysmaailmassa tänä päivänä on selkeytynyt. Koen että näiden järjestelmien tarve lähitulevaisuudessa kasvaa merkittävästi, sillä esimerkiksi yritysten tarve parantaa tietoturvaa kasvaa jatkuvasti.

Lähteet

2017 Mobile Threat Landscape. 2018. Trend Micron uhkaraportin kooste. Viitattu 16.1.2019. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-mobile-threat-landscape

Bluetooth 5 is now available. 2016. Lehdistötiedote. Viitattu 21.9.2018. https://www.bluetooth.com/news/pressrleases/2016/12/07/bluetooth-5-now-available

Cases, T. 2018. How to extend the lifespan of your smartphone. Viitattu 23.9.2018. https://www.ceotodaymagazine.com/2018/02/how-to-extend-the-lifespan-of-your-smartphone/

CVE Details. 2018a. Apple Iphone OS: Vulnerability Statistics. iPhonen haavoittuvuuksien koostettu raportti. Viitattu 6.1.2019. https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

CVE Details. 2018b. Google Android: Vulnerability Statistics. Androidin haavoittuvuuksien koostettu raportti. Viitattu 6.1.2019. https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Diogenes, Y. & Gilbert, J. 2015. Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices. Washington: Microsoft Press.

Doherty, J. 2016. Wireless and Mobile Device Security. Burlington: Jones & Bartlett Learning.

Ely, C. 2014. The Life Expectancy of Electronics. Viitattu 23.9.2018. https://www.cta.tech/News/Blog/Articles/2014/September/The-Life-Expectancy-of-Electronics.aspx

Forni, A. & Meulen, R. 2017. Gartner says worldwide sales of smartphones grew 9 percent in first quarter of 2017. Gartnerin julkaisema lehdistötiedote. Viitattu 12.9.2019. https://www.gartner.com/en/newsroom/press-releases/2017-05-23-gartner-says-worldwide-sales-of-smartphones-grew-9-percent-in-first-quarter-of-2017

Griffin, P. 2017. Study on Mobile Device Security. Nettijulkaisu. Viitattu 21.4.2019. https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

Isaksson, A. 2017. Bluetooth-sovelluksen kehittäminen androidille. Opinnäytetyö, AMK. Jyväskylän ammattikorkeakoulu, tekniikan ja liikenteen ala, tieto-ja viestintätekniikan koulutusohjelma. Viitattu 21.9.2018. http://urn.fi/URN:NBN:fi:amk-2017112718262

Koivula, P. & Tuomola, J. 2014. Ransomware-haittaohjelmat. Opinnäytetyö, AMK. Turun ammattikorkeakoulu, tietojenkäsittely, yrityksen tietoliikenne ja tietoturva. Viitattu 9.1.2019. http://urn.fi/URN:NBN:fi:amk-2014061012490

Kirby, J. 2017. Apple admitted it's slowing down certain iPhones. Viitattu 23.8.2018. https://www.vox.com/2017/12/22/16807056/apple-slow-iphone-batteries

Niittylahti, J. 2014. WLAN-verkon tietoturva. Opinnäytetyö, AMK. Tampereen ammattikorkeakoulu, tietotekniikka ja tietoverkot, tietotekniikan koulutusohjelma. Viitattu 21.9.2018. http://urn.fi/URN:NBN:fi:amk-2014120819008

Qiwei, H. & Daegon, C. 2016. Characterizing the technological evolution of smartphones: Insigts from performance benchmarks. Vittattu 18.4.2019. https://www.researchgate.net/publication/307090848_Characterizing_the_technological_evolution_of_smartphones_insights_from_performance_benchmarks

Raggo, M. 2016. Mobile Data Loss: Threats and Countermeasures. Waltham: Elsevier.

Silberschatz, A., Galvin, P. & Gagne, G. 2014. Operating System Concepts Essentials. E-Kirja. Vittattu 17.9.2018. http://dusithost.dusit.ac.th/~juthawut_cha/download/Operating_System_Concepts_Essentials_2nd_Edition.pdf

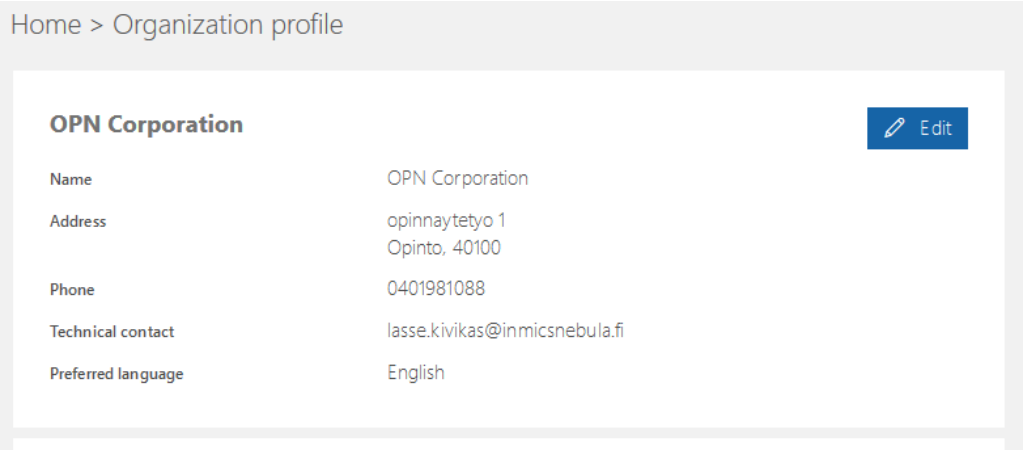
Snyder, J. 2018. Is Installing Anti-Virus Software on Mobile Devices Necessary? Viitattu 16.4.2019. https://insights.samsung.com/2018/01/22/is-installing-anti-virus-software-on-mobile-devices-necessary/

What is WiFi: IEEE 802.11. N.d. Verkkojulkaisu. Viitattu 21.1.2019. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/what-is-wifi.php

Liitteet

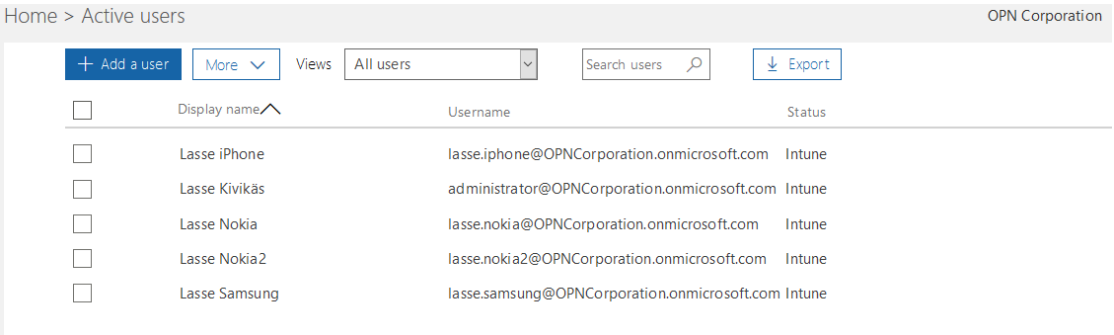
Liite 1. Intunen käyttöönotto

Intune-ympäristöä varten käytettiin Microsoftin omaa testiympäristöä, johon voi rekisteröidä oman testiyrityksen veloituksetta kuukaudeksi käyttöön. Luotiin ympäristö OPN Corporation ja domainia OPNCorporation.onmicrosoft.com. Tänne luotiin administrator-tunnus, jota käytettiin ympäristön konfiguroinnissa ja käyttöönotossa. Ensimmäiseksi käytiin lisäämässä järjestelmään yrityksen osoitetiedot (ks. Kuvio 32).



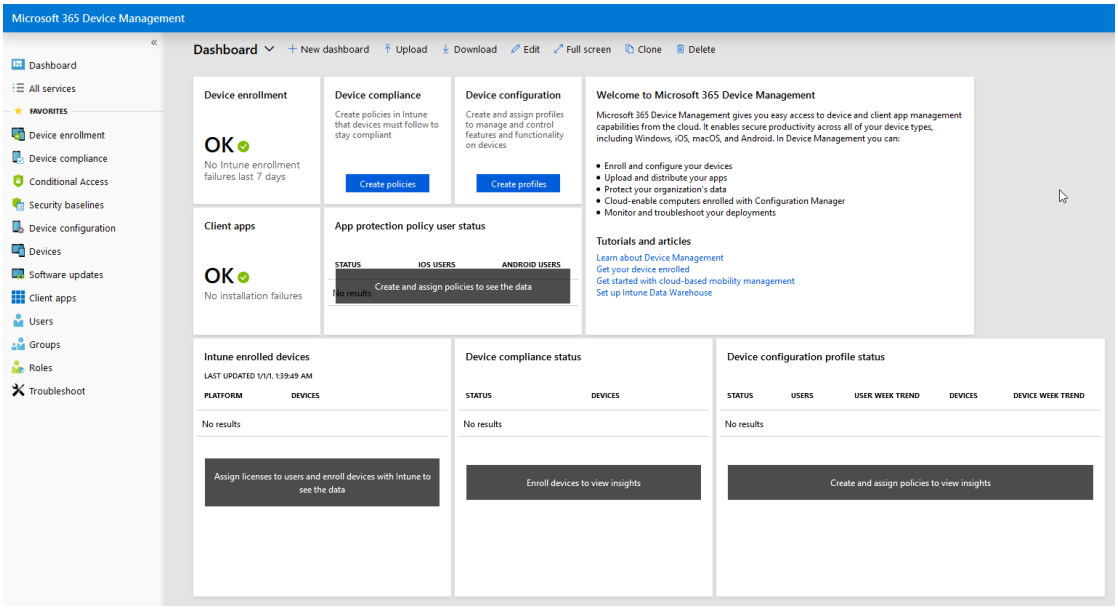
Kuvio 32. Ympäristön tiedot

Lisäksi testiympäristöön lisättiin valmiiksi laitteiden käyttäjät ja nimettiin seuraavan kuvan (ks. Kuvio 33) mukaisesti.



Kuvio 33. Admin Centeriin lisätyt käyttäjät

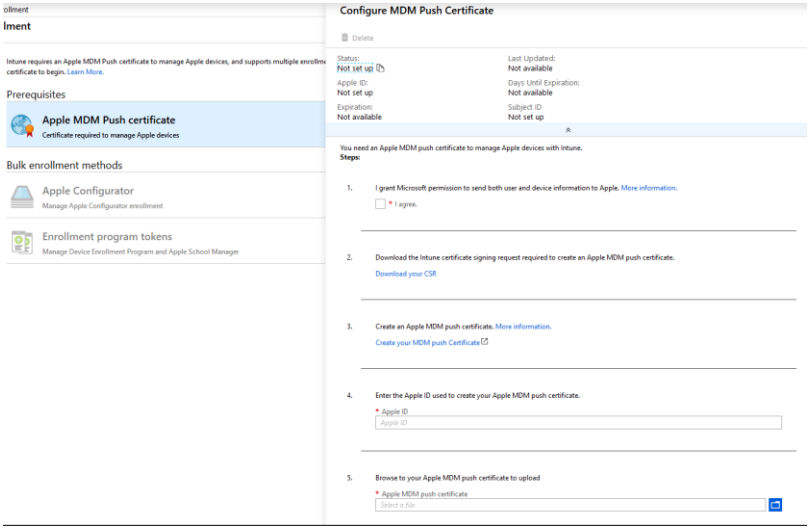
Nämä käyttäjät nimettiin laitteiden perusteella, jotta seuranta myöhemmässä vaiheessa helpottuu. Laitteet myös kirjattiin eri tavoilla, jotta saadaan selville mitkä menetelmät ovat laitteille parhaat. Intune-ympäristö (ks. Kuvio 34) itsessään löytyy valmiiksi Officen portaalista, kun testiympäristö on luotu. Intunen käyttöönotossa käytettiin sen tarjoamaa Quick start osiota, jolla ympäristö saatiin nopeasti käyttövalmiiksi. Tämän avulla pystytään myös seuraamaan käyttöönoton edistymistä.



Kuvio 34. Intunen perusnäkymä ensimmäisessä käynnistyksessä.

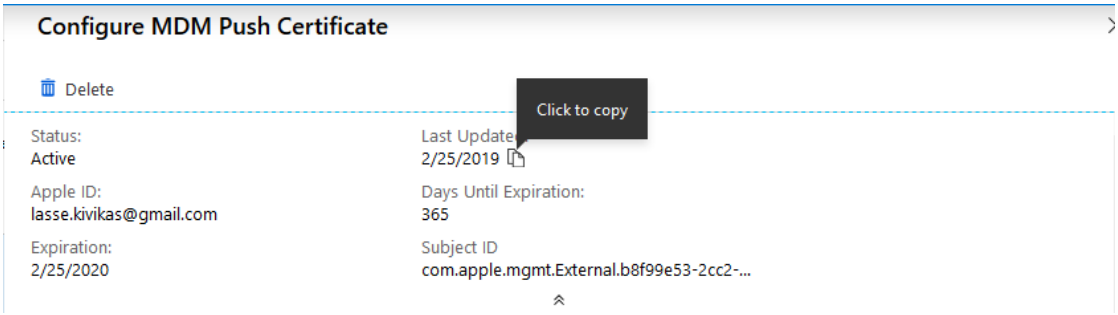
Apple enrollment

Applen iOS-laitteille on oma enrollment-osio. Intune vaatii iOS-laitteilta oman Apple MDM Push sertifikaatin, jota ilman Applen tuotteita ei pystytä lisäämään Intuneen. Intune tarjoaa step-by-step -ohjeet sertifikaatin luomista varten (ks. Kuvio 35). Tämä vaati myös Apple ID:n. Intunesta ladattiin Microsoftin Certificate Signing Request -tiedosto (.csr), joka ladattiin Applen Push Certificate Portaaliin. Tätä vasten Apple antoi oman sertifikaatin (.pem) joka lisättiin Intuneen.



Kuvio 35. Applen Push sertifikaatin konfigurointi

Tämän jälkeen päivitettiin sivu ja sertifikaatin status oli aktiivinen (ks. Kuvio 36). Sertifikaatti on voimassa vuoden kerrallaan. Tämän jälkeen Applen konfiguraattori ja tokenien käyttö mahdollistuu.

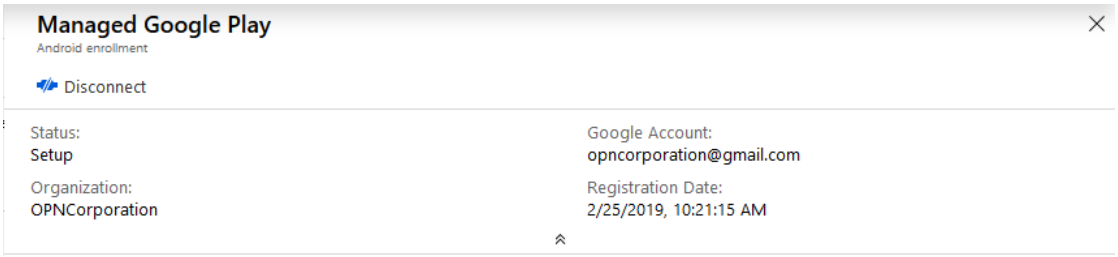


Kuvio 36. Aktivoitu Apple MDM Push-sertifikaatti

Android enrollment

Android-laitteiden enrollment-prosessi tapahtuu Managed Google Play:n kautta. Google Play Work on Google Play:n business-osion puoli, jonka kautta voidaan hallita muun muassa ohjelmistojen hyväksymisiä laitteille. Apple ID-tunnuksen tavoin Google Play Work vaatii käytettävän yrityksen nimen, sekä sille määrätyt data protec-

tion officer ja EU representative. Tähän tarkoitukseen luotiin opncorporation@gmail.com -käyttäjätili. Tietojen täyttämisen jälkeen Managed Google Play oli myös aktiivinen (ks. Kuvio 37) ja Android Enterprise -tuotteet olivat käytettävissä.

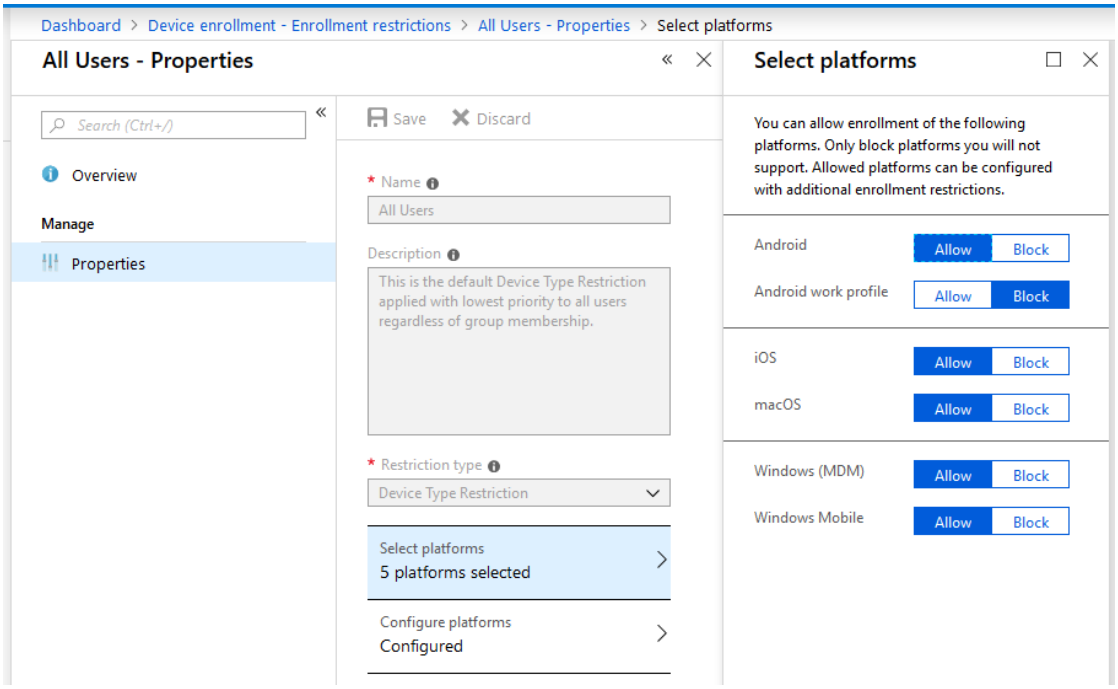


Kuvio 37. Aktivoitu Managed Google Play

Molemmat enrollment-osiot saatiin aktivoitua ilman ongelmia. Google Play Workista testattiin vielä lopuksi, että sovellusten hyväksyntä onnistuu hyväksymällä Intune Company Portal.

Enrollment restrictions

Seuraavaksi Intuneen luotiin Enrollment restrictions (ks. Kuvio 38). Tällä rajataan Intuneen hyväksyttävät käyttöjärjestelmät. Järjestelmistä hyväksyttiin kaikki paitsi Android Work Profile.

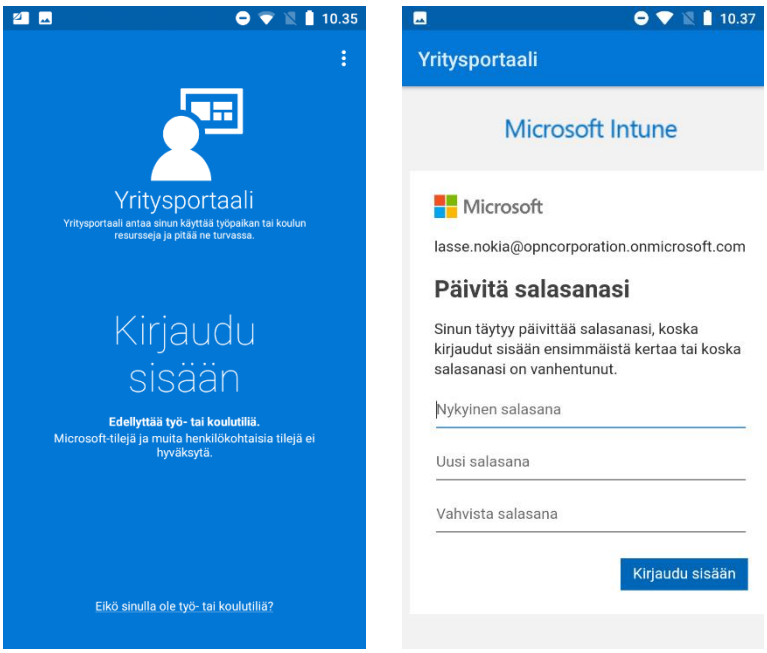


Kuvio 38. Intuneen hyväksytyt käyttöjärjestelmät

Configure platforms -lehdellä voidaan määrittää käyttöjärjestelmien versiot. Näitä versiorajauksia ei testiympäristön laajuuden vuoksi asetettu. Enrollment restrictions on ainoa pakollinen käyttöönotettava rajoite.

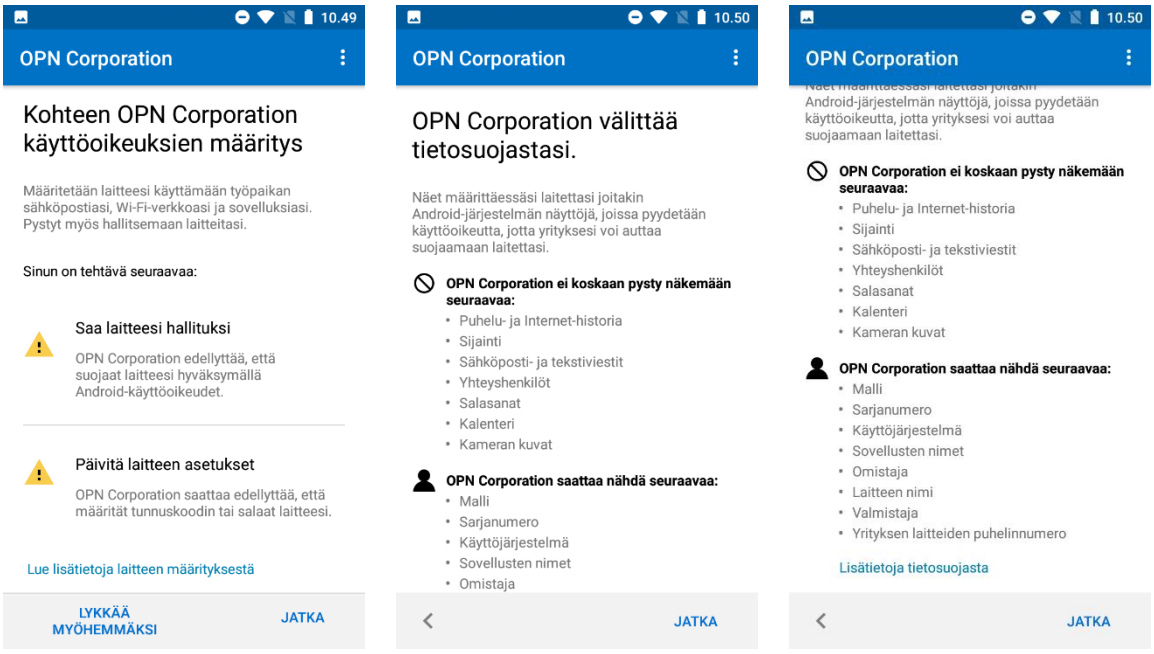
Nokia 3 manual enrollment

Ensimmäinen Nokia 3 puhelin enrollattiin manuaalisesti. Tähän laitteeseen kirjauduin ensin henkilökohtaisilla tunnuksilla, jotta saatiin Intune Company Portal ladattua. Tämän jälkeen kaikki henkilökohtaiset tiedot poistettiin laitteelta. Laitteelta käynnistettiin Intune-yritysportaali (ks. Kuvio 39), johon kirjauduttiin tunnuksella lasse.nokia@opncorporation.onmicrosoft.com. Tämän jälkeen laite pyysi salasanan päivitystä uuteen (Kuvio 39).



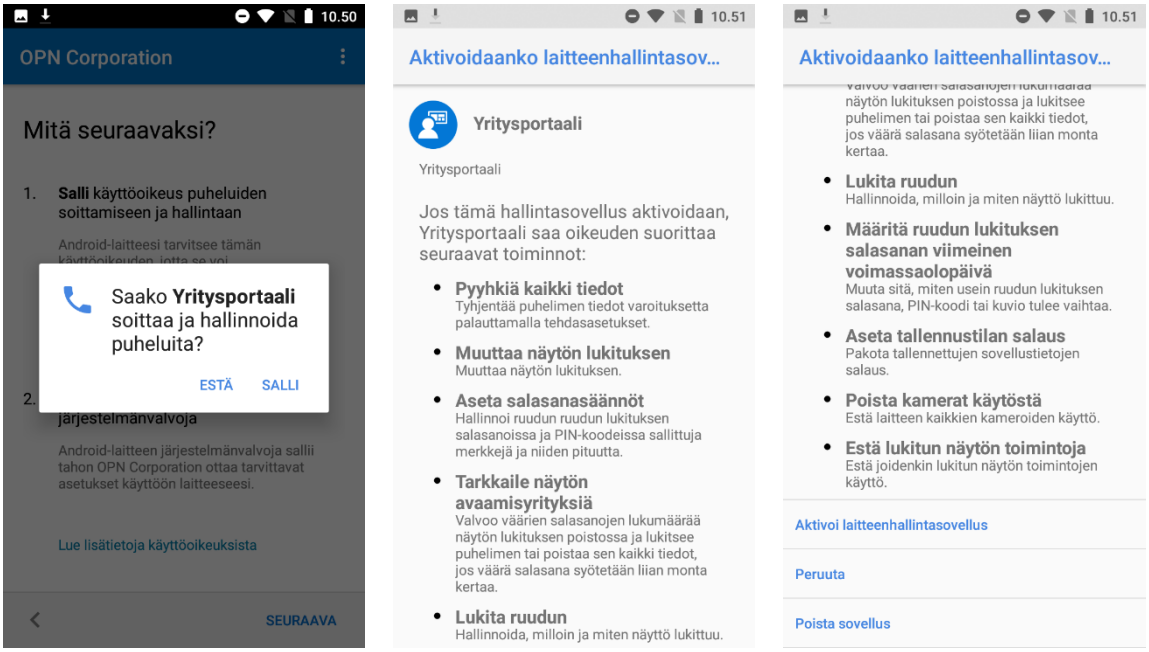
Kuvio 39. Yritysportaalin kirjautumisruutu ja salasanan vaihto ensimmäisellä kirjautumisella.

Salasanan vaihdon jälkeen yritysportaali ilmoitti käyttöoikeuksien määrityksen sekä ilmoitti tietosuoja-asetuksista (ks. Kuvio 40).



Kuvio 40. Käyttöoikeuksien määritys sekä tietosuojailmoitus.

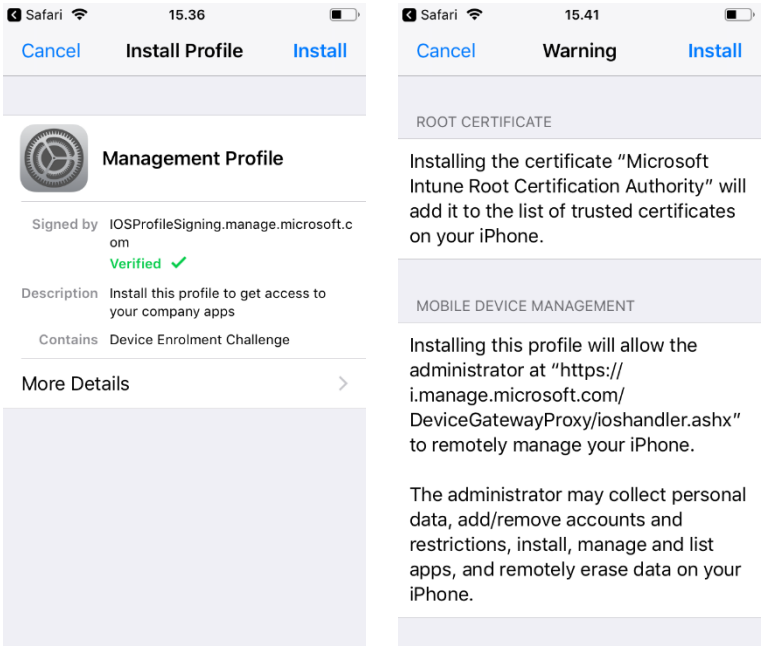
Tämän jälkeen yritysportaali pyysi käyttöoikeuden puheluiden soittoon ja hallinnointiin. Lopuksi yritysportaali edellytti laitteenhallintasovelluksen aktivointia (ks. Kuvio 41), jonka jälkeen ilmoitti onnistuneesta aktivoinnista.



Kuvio 41. Käyttöoikeuksien hyväksyntä ja hallintasovelluksen aktivointi

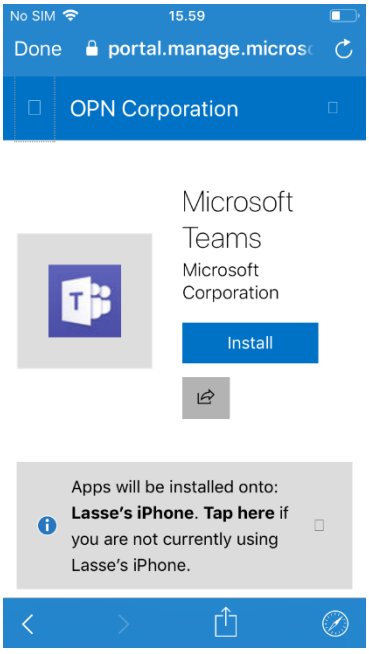
iPhone enrollment

Seuraavaksi tehtiin enrollaus iPhone 5S:llä. Tämän käyttöönotto eteni suoraan yritysportaalista kirjautumalla sisään. Tämän jälkeen portaali pyysi hyväksymään käyttöehdot, jonka jälkeen Management Profile näytti hyväksyttyä. Tämän jälkeen profiili piti asentaa, jossa se varoitti root certifiacten lisäyksestä luotettuihin certifikaatteihin sekä MDM:n ehtoihin (ks. Kuvio 42). Sen jälkeen enrollment iPhonelle oli valmis.



Kuvio 42. Management profile sekä root certificate-varoitus

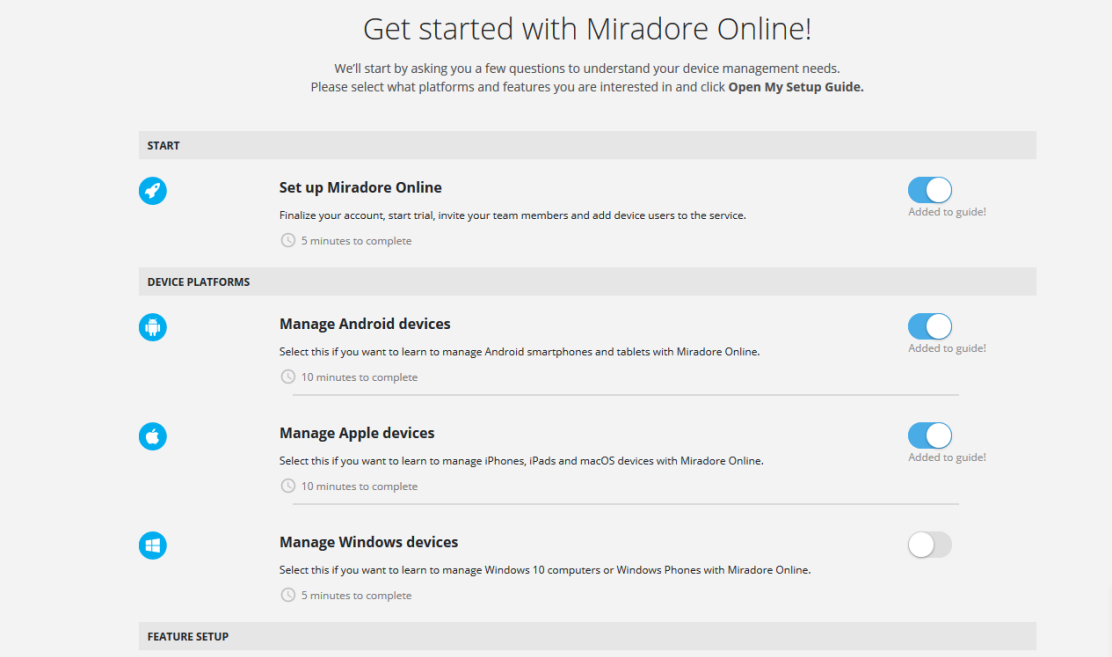
Tämän jälkeen Intunesta lisättiin järjestelmään testin vuoksi Teams-sovellus, jonka näkyminen varmistettiin iPhonen yritysportaalista (ks. Kuvio 43).



Kuvio 43. Teams sovellus Intunessa

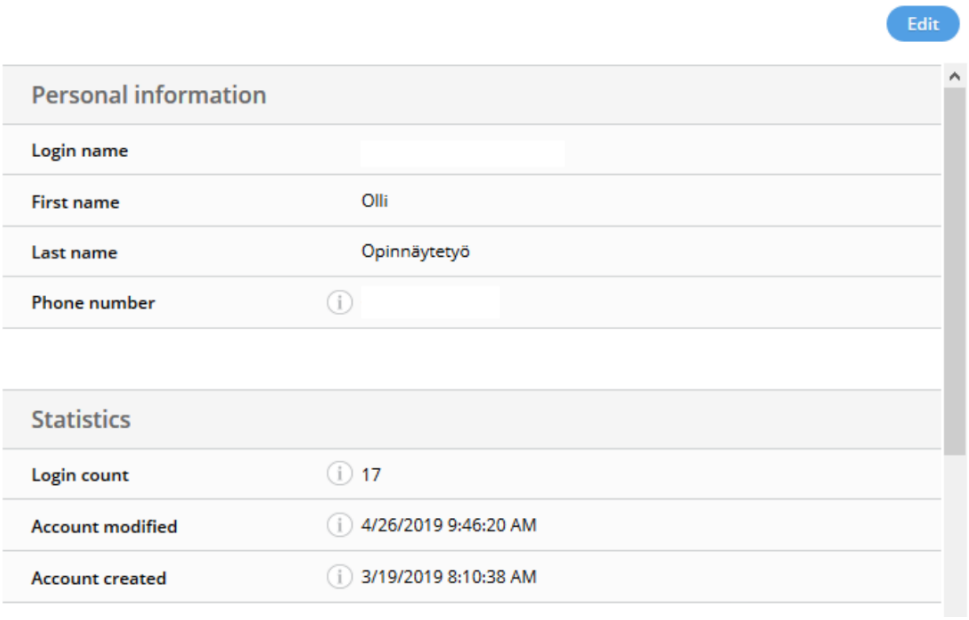
Liite 2. Miradoren käyttöönotto

Miradore Online on verkkoselaimen päällä toimiva järjestelmä, jonka käyttöönotto onnistuu yksinkertaisesti. Ympäristöä ei tarvitse luoda erikseen, vaan ensimmäisen kirjautumisen jälkeen avautui Miradoren aloitussivu, josta voitiin valita tarvittaviin alustoihin ja asetuksiin ohjeet (ks. Kuvio 44). Valintojen jälkeen valituista osista muodostui ohjeistus.



Kuvio 44. Miradoren käyttöönoton ohjeistuksen luonti

Ohjeistusta seuraten käytiin katsomassa ja muokkaamassa henkilökohtaiset tiedot (ks. Kuvio 45).

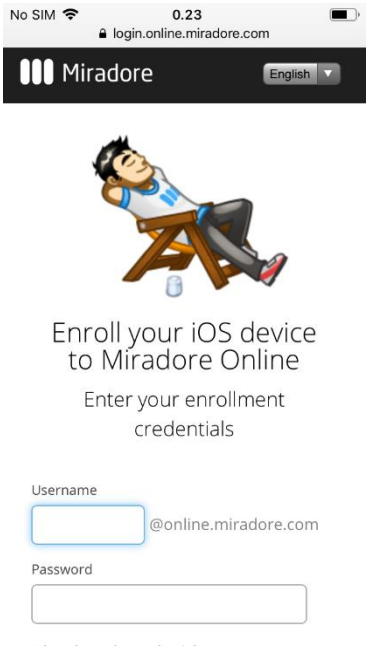


Kuvio 45. Miradoreen täytetyt henkilökohtaiset tiedot

Apple enrollment

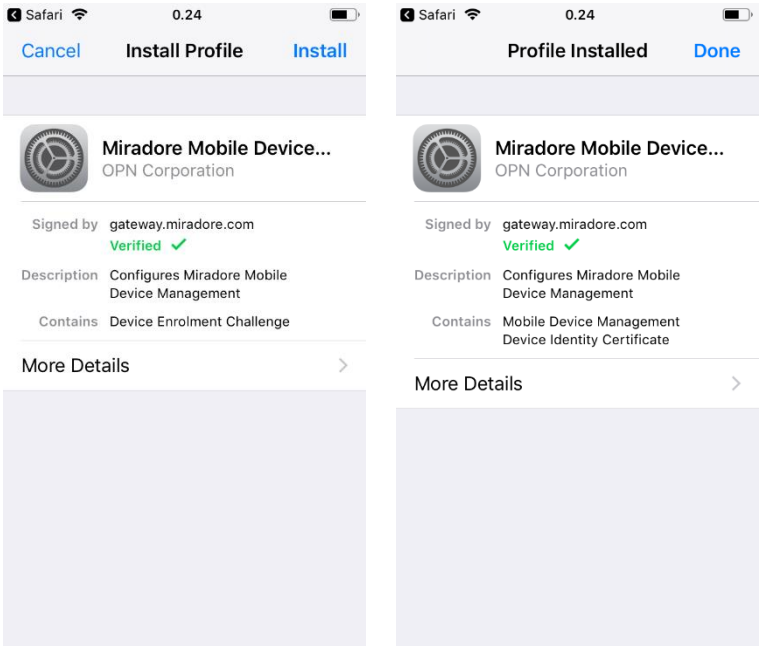
Laitteet kirjattiin Miradoreen samalla järjestyksellä kuin edellisessä vaiheessa. Ainoastaan iPhonen kirjauksessa toteutus oli erilainen. iPhonea varten luotiin Applen Push sertifikaatti kuten Intunen käyttöönotossa. Miradore Onlinessa luotiin ensin Certificate Signing Request (.CSR)-tiedosto, joka ladattiin Applen Push certificate portaaliin. Tätä vasten saatiin. pem-tiedosto, joka lisättiin Miradoreen.

Jotta iPhone saatiin kirjattua järjestelmään, jouduttiin ensin luomaan kutsu, joka lähetettiin käyttäjän sähköpostiin. Sähköposti piti sisällään tunnuksen, jolla aktivoitiin laite Miradoreen (ks. Kuvio 46).



Kuvio 46. Laitteen kirjaus Miradoreen

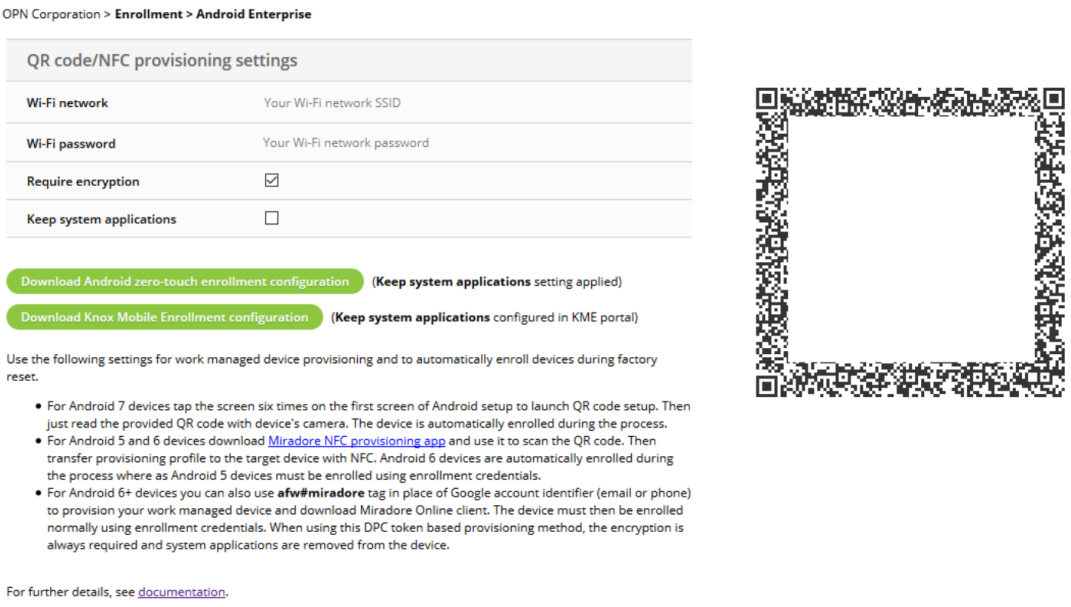
Kun kirjaus oli tehty, iPhone vaati hyväksymään laitteen Device Management -asetuksista Miradoren sertifikaatin ja asentamaan profiilin (ks. Kuvio 47). Hyväksynnän jälkeen Miradoressa käytettiin iOS-alustan valmiiksi luotoa salasanakonfiguraatioprofiilia, (eng. Configuration profile). Tämän avulla laite saatiin yhdistettyä Miradoreen.



Kuvio 47. Miradoren profiilin ja sertifikaatin asennus

Android enrollment

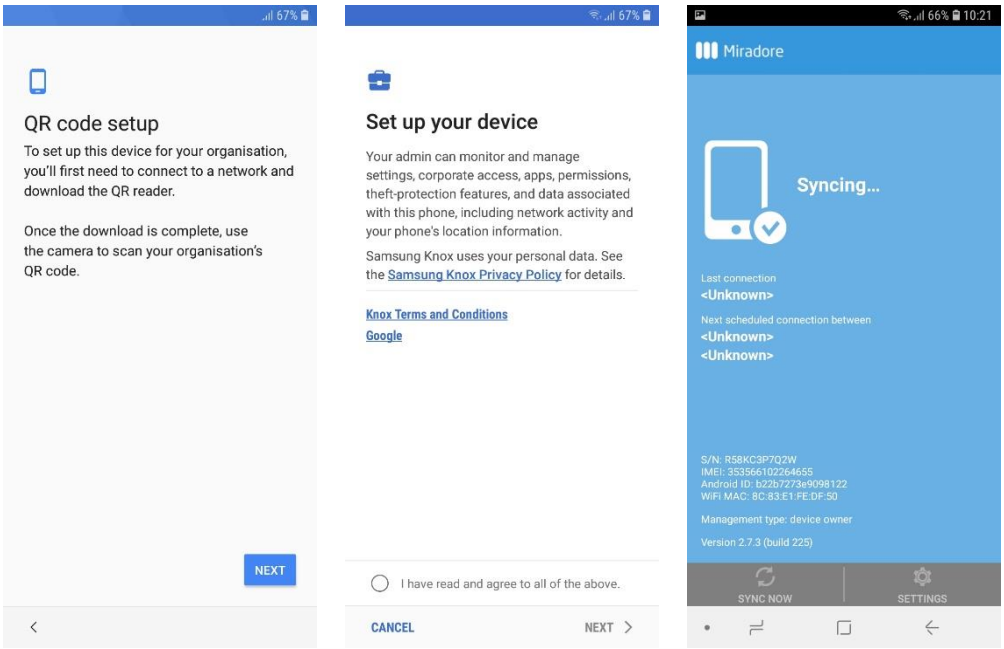
Androidien kirjausta varten ei tarvinnut erikseen aktivoida palveluita. Käyttöä varten mentiin ohjeen mukaan Android client-valikossa Work managed device provisioning-valikkoon, josta löytyi suoraan QR-asennukseen vaadittava token (ks. Kuvio 48).



Kuvio 48. Miradore Onlinen Android-kirjautumispoletti

Samsung enrollment

Samsung asennettiin käyttämällä työprofiilin QR-asennusta, joka tehdään laitteen ensimmäisen käynnistyksen yhteydessä (ks. Kuvio 49). Tämän avulla laitteille saatiin puhdas työprofiili ilman ylimääräisiä sovelluksia. Valinta voitiin tehdä Miradore Onlinen Work managed device provisioning -valikossa. Asennuksen jälkeen laitteella oli käytössä pelkkä työprofiili, ja Miradore client (ks. Kuvio 49). Nokia 3-laitteelle tehtiin identtinen QR-asennus.



Kuvio 49. Samsungin QR-asennus ja laitteen Miradore client