MOBIILILAITEHALLINTARATKAISUJEN TESTAUS

Case: Versowood

LAHDEN AMMATTIKORKEAKOULU
Insinööri AMK
Tieto- ja viestintätekniikka
Kevät 2019
Lassi Karppinen

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Karppinen, Lassi	Opinnäytetyö, AMK	Kevät 2019
	Sivumäärä	
	39	

Työn nimi

Mobiililaitehallinta ratkaisujen testaus
Case: Versowood

Tutkinto

Insinööri AMK, Tietotekniikka

Tiivistelmä

Opinnäytetyön tavoitteena oli toteuttaa mobiililaitehallintaratkaisujen testaus ja sopivan ratkaisun löytäminen Versowoodille. Mobiililaitehallintatestaukseen valittiin Miradore, MobileIron, AirWatch sekä Intune. Testaus suoritettiin Versowoodin laitekannasta löytyvillä mobiililaitteilla.

Android käyttöjärjestelmän hallintatapoja ovat device admin, work profile ja fully managed device. iOS-käyttöjärjestelmä voidaan hallintatavaltaan jakaa käyttäjän omistamiin ja yrityksen omistamiin laitteisiin.

Laitehallinta aloitetaan rekisteröimällä laite hallintaan käyttäen laiterekisteröintiohjelmalla, QR-koodilla, NFC:llä, DPC tokenilla tai mobiililaitteeseen asennettavalla agentilla. Kun laite on rekisteröity hallintaan, on siihen mahdollista määrittää asetuksia, jakaa sovelluksia tai tyhjentää laite etänä. Android Enterprise mahdollistaa kaksi eri hallintatapaa, jotka ovat work profile sekä fully managed device. Work profile erottaa työsovellukset erilliseen tilaan, johon hallinta mobiililaitteessa kohdistuu. Fully managed device vastaavasti tarkoittaa täyttä laitteen hallintaa. iOS-laitteissa on myös mahdollista erottaa käyttäjän sekä yrityksen data.

Testaus ei johtanut päätökseen mobiililaitehallintaratkaisun valitsemisesta, mutta antoi työkalut päätökselle, kun sopiva hallintamalli on valmis.

Asiasanat

mobiililaitehallinta, android, iOS

Abstract

Author(s)	Type of publication	Published
Karppinen, Lassi	Bachelor's thesis	Spring 2019
	Number of pages	
	39	

Title of publication

Testing of Mobile Device Management Solutions
Case: Versowood

Name of Degree

Bachelor of Engineering, Information Technology

Abstract

The purpose of this thesis was to test different solutions for mobile device management solutions for Versowood. The solutions to be tested were Miradore, MobileIron, AirWatch and Intune. Testing was done with devices that were in use at Versowood.

Android devices can be managed by device admin, work profile or fully managed device types iOS management types can be categorized as user-owned or company-owned.

Mobile device management starts by enrolling the chosen device by using an enrollment program, QR-code, NFC, DPC token or an agent that can be installed to the mobile device. When the device has been enrolled, it can be configured, and you can distribute applications to it or remotely wipe the device. Android Enterprise enables two types of management, which are work profile and fully managed device. Work profile creates another profile in the mobile device alongside the user's own profile, which can be managed by the administrator. Fully managed device makes the device entirely managed by the administrator. iOS devices can also separate the user's own data and company data.

Testing did not lead to a decision which mobile device management solution would be chosen, but it gave tools for making the decision, when a suitable administrative template would be ready.

Keywords

mobile device management, android, iOS

SISÄLLYS

LYHENTEET

AD	Active Directory
AfW	Android for Work
API	Application Programming Interface
App	Application
BYOD	Bring Your Own Device
COBO	Corporate Owned, Business Only
COPE	Corporate Owned, Personally Enabled
COSU	Corporate Owned, Single Use
DEP	Device Enrollment Program
DPC	Device Policy Controller
EMM	Enterprise Mobility Management
iOS	iPhone Operating System
KME	Knox Mobile Enrollment
MAM	Mobile Application Management
MDM	Mobile Device Management
NFC	Near Field Communication
PIN	Personal identification number
QR	Quick Response
SCCM	System Center Configuration Manager
SWOT	Strengths, Weaknesses, Opportunities, Threats
UEM	Unified Endpoint Management

1 JOHDANTO

Yhä useammat työntekijät hyödyntävät työssään mobiililaitetta, ja tästä johtuen mobiililaitehallinnasta tulee yrityksille yhtä tärkeää kuin työasemien hallinnasta. Mobiililaitehallinnalla voidaan asettaa mobiililaitteeseen yhtiön tarjoamat sovellukset, käyttöön liittyvät asetukset sekä tietoturvaan liittyvät asetukset.

Mobiililaitteisiin kuuluvissa älypuhelimissa yleisimmät käyttöjärjestelmät ovat Googlen Android ja Applen iOS. Koska Androidin koodista suurin osa on vapautettu avoimeksi lähdekoodiksi, on moni älypuhelimien laitevalmistaja valinnut sen käyttöjärjestelmäksi.

Markkinoilla on useita eri mobiililaitehallintaratkaisujen valmistajia. Vaikka eri ratkaisuissa laitehallinta on perustoiminnoiltaan samanlaista, jossa toiminta perustuu käyttöjärjestelmän tarjoamiin toimintoihin, on eri laitehallinta ratkaisuissa useita eroja. Androidin tapauksessa toinen laitehallinta tarjoaa paljon enemmän asetuksia laitehallintaan tai tapoja tehdä laitehallintaan liittyvä toiminto eri tavalla. Tämän takia järjestelmien testaus on hyvä suorittaa ennen sen valintaa.

Tämän työn tavoitteena on testata neljää eri mobiililaitehallinta ratkaisua Versowoodille ja löytää niistä sopiva ratkaisu Versowoodin käyttöön. Pääpainona mobiililaitehallinnalla on Versowoodin älypuhelimet. Laitehallinta testataan valitussa älypuhelimien testiryhmässä, jossa on laitteita eri käyttöjärjestelmillä ja niiden eri versioilla. Testauksen tulokset kirjataan ja arviointia tullaan hyödyntämään sen laitehallinnan valitsemisessa, joka parhaiten sopisi Versowoodin käyttöön.

2 VERSOWOOD

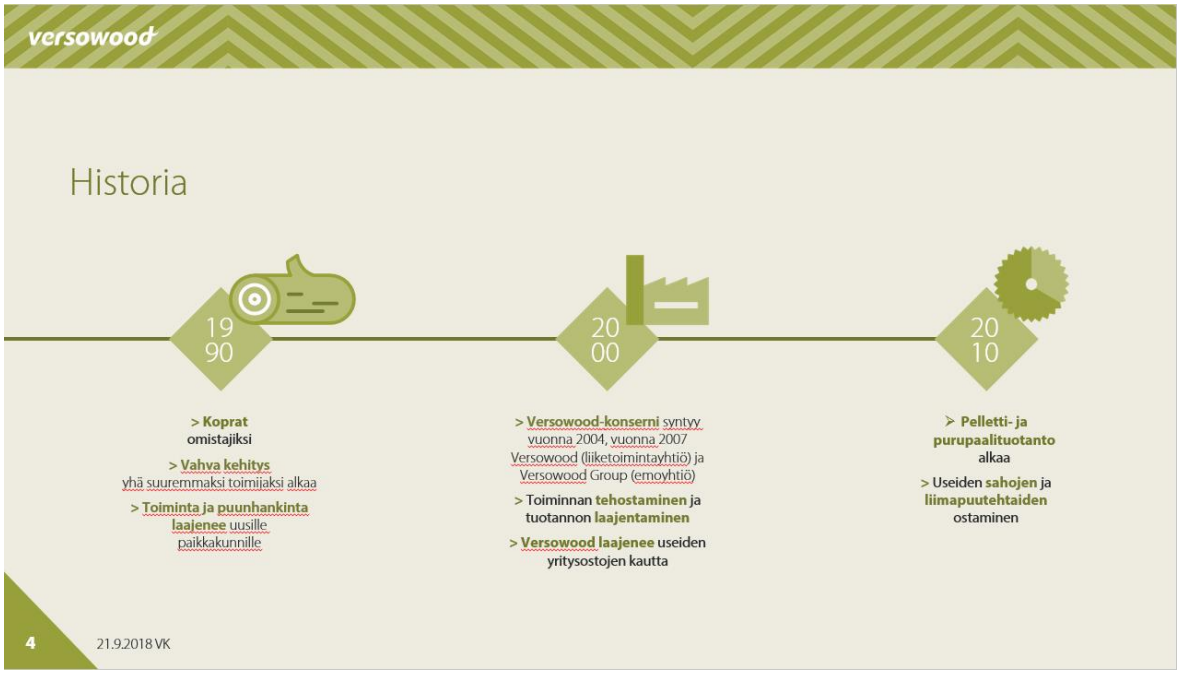
2.1 Historia ja tausta

Versowood on kotimainen perheyritys, joka on samalla Suomen suurin yksityinen sahatavaran tuottaja ja jalostaja. Versowoodin toimitusjohtajana toimii Ville Kopra. Versowood on toiminut vuodesta 1946 (kuvio 1). Toimintaa Versowoodilla on yhdessätoista toimipisteessä, joista yksi sijaitsee Virossa. Pääkonttori sijaitsee Vierumäellä. Versowoodin 370 miljoonan liikevaihdosta 46 prosenttia on kotimaan markkinoilla (kuvio 2). (Versowood 2018b.)

Kuvio 1. Historia (Versowood 2019)

Vuonna 1990 (kuvio 3) Versowoodin omistus siirtyi Kopran perheelle. Tätä ennen oli Versowood ollut Kollin perheen omistuksessa. Aikaisemmin Vierumäen Teollisuutena tunnettu yritys yhtenäisti nimensä Versowoodiksi loppuvuodesta 2004 ja vuoden 2005 alusta asti yritys on tunnettu nimellä Versowood. (Versowood 2018a.)

Kuvio 2. 5 liiketoiminta-aluetta (Versowood 2019)



Kuvio 3. Historia jatkuu (Versowood 2019)

2.2 Mobiililaitehallinta Versowoodilla

Versowoodin laitekannassa olevan AD-toimialueen työasemat, joissa on Windows-käyttöjärjestelmä, hallitaan käyttäen System Center Configuration Manageria, josta käytetään lyhennettä SCCM. Mobiililaitteet, kuten Windows-tabletit, ovat saman hallinnan piirissä, mutta tämä ei kosketa älypuhelimia eikä tabletteja, joissa jokin muu käyttöjärjestelmä kuin

Windows. SCCM:n hallintamahdollisuudet ulottuvat Versowoodin Exchange-sähköpostijärjestelmään kytketyille mobiililaiteille, mutta sen hallintamahdollisuudet ovat nykytilanteessa rajalliset.

Versowoodilla on jo aikaisemmin ollut suunnitteilla lisätä älypuhelimet laitehallintaan, mutta kyseinen mobiililaitehallintaprojekti oli jäänyt saattamatta loppuun. Nyt sitä päätettiin jatkaa, sillä mobiiliympäristön käytön ja laitekannan kasvu, muuttuneet tarpeet sekä kehnot hallintakontrollit vaativat prosessin kehittämistä ja tarkoituksena tähän oli testata neljää eri mobiililaitehallinta ratkaisua, joissa pääpainona olisi älypuhelimien laitehallinta. Älypuhelimissa olisi käyttöjärjestelmänä joko Android tai iOS, sillä Windows Phone on poistuva tuote. Laitekannasta suurin osa on Android-älypuhelimia, joten testauksen pääpaino on kyseisissä laitteissa.

3 MOBIILIYMPÄRISTÖN HALLINNAN OSA-ALUEET

3.1 MAM

Mobile Application Management, josta käytetään lyhennettä MAM, tarkoittaa sovellusten ja datan hallintaa. MAM:eilla yritys ei kontrolloi itse laitetta vaan ainoastaan siinä olevaa dataa. MAM on käytössä BYOD-tapauksissa, joissa käyttäjän oma laite ei ole hallinnassa vaan ainoastaan siinä olevat yrityksen tarjoamat sovellukset kuuluvat hallinnan piiriin. Nämä palvelut kyetään poistamaan mobiililaitteesta ilman, että käyttäjän omaan dataan kosketaan. (Solution Review 2018.)

Yrityksen sähköposti on esimerkki MAM-käytännöstä. Sähköpostiin liittyvät kopiointi- ja liittämistoiminnot kyetään rajoittamaan tai poistamaan toiminnasta turvaten yrityksen data. (Solution Review 2018.)

3.2 MDM

Mobile Device Management, josta käytetään lyhennettä MDM, tarkoittaa mobiililaitteenhallintaa. MDM:llä yritys kykenee hallitsemaan koko laitetta eikä vain siinä olevaa dataa. Laitehallinnassa kyetään asettamaan laitteeseen yrityksen asettamat tietoturva-asetukset, asentamaan laitteeseen tarvittavat sovellukset ja tarvittaessa lukita tai tyhjentää mobiililaite. (Computerworld 2017.)

MDM voidaan myös luokitella kahteen eri tapaan hallita laitetta. On yrityksen omistamat työntekijälle tarjotut laitteet, jotka ovat täysin toiminnaltaan työtehtävään määritelty tai täysin hallinnoitu, joka saattaa rajoittaa mobiililaitteen käyttöä työntekijän omalla ajalla. Toinen tapa on BYOD (Bring Your Own Device), jossa työntekijä voi tuoda oman henkilökohtaisesti omistamansa mobiililaitteensa ja kyetä silti käyttämään yrityksen palveluja. BYOD-tavassa yrityksellä on mahdollisuus kontrolloida mobiililaitteessa vain yrityksen dataa ja sovelluksia. (Mobilock 2018.)

3.3 EMM

Enterprise Mobile Management, josta käytetään lyhennettä EMM, tarkoittaa tapaa hallita laitetta sekä siinä olevaa dataa. MDM tuo mahdollisuuden laitehallintaan ja MAM sovellusten hallintaan. Yhdistämällä MDM ja MAM saadaan käytettävä termi EMM. (Mobilock 2018.)

Opinnäytetyötä aloittaessa termi, jota käytettiin, oli MDM. Nykyään käytetään termiä EMM, joka on kattavampi termi kuvaamaan yritysten mobiililaitehallintaa. Useat

mobiililaitehallintaratkaisut ovatkin lisänneet vähintään Windows 10 – käyttöjärjestelmän hallinta mahdollisuudet omaan tuotteeseensa.

3.4 UEM

Unified Endpoint Management, josta käytetään lyhennettä UEM, tarkoittaa muidenkin kuin älypuhelimien hallintaa. UEM laajentaa hallinnan älypuhelimista työasemiin, riippumatta niiden käyttöjärjestelmistä. (Mobilock 2018.)

Alun perin mobiililaitehallintaan erikoistuneet ratkaisut ovatkin laajentaneet hallinnan työasemiin. Testatuissa hallintaratkaisuissa oli mahdollisuus Windows 10 -työasemien hallintaan.

4 KÄYTTÖJÄRJESTELMÄT

4.1 Android

Android on Linuxin ytimeen perustuva avoimen lähdekoodin ohjelmisto. Android julkaistiin vuonna 2003 ja vaikka se olikin alun perin suunniteltu käyttöjärjestelmäksi digitaalikameroilla, sen kehittäjä Andy Rubin alkoi kehittämään Android-käyttöjärjestelmää käytettäväksi älypuhelimissa. Vuonna 2005 Google osti Androidin, ja kolme vuotta myöhemmin Android nähtiinkin älypuhelin markkinoilla, ei älypuhelimena vaan älypuhelimen käyttöjärjestelmänä. (Looper 2018.)

Ensimmäinen Android-käyttöjärjestelmän puhelimen julkaisi HTC ja puhelin oli nimeltään T-Mobile G1, joka myös tunnettiin nimellä HTC Dream. Käyttöjärjestelmänä toimi silloin Android 1.0. (Callaham 2018.) Vaikka käyttöjärjestelmä olikin minimaalinen nykyajan standardeihin verrattuna, sisälsi käyttöjärjestelmä jo uusimmistakin Android-älypuhelimista löytyvät sovellukset (App), kuten Gmail, Maps ja Youtube integroituna käyttöjärjestelmään. (Raphael 2018a.) Google Play kauppa -sovellus oli myös osana puhelimen käyttöjärjestelmää, vaikkakin Play-kauppa kulki vielä nimellä Market. Kaupan ideana oli keskitetty paikka, josta puhelimeen saatavat sovellukset olisivat ladattavissa. (Looper 2018.)

Vuonna 2009 tuli markkinoille Android 1.5, joka oli koodinimeltään Cupcake. Tästä eteenpäin Android-käyttöjärjestelmät olivat saaneet versionumeron rinnalle nimen, joka oli nimetty karkin tai jälkiruoan mukaan (Callaham 2018). Suurimmat muutokset käyttöjärjestelmässä olivat älypuhelimen näytöllä oleva näppäimistö sekä mahdollisuus sovelluskehittäjille luoda sovelluksilleen widget eli pienoisohjelma. (Looper 2018.)

Androidin kehitystyö jatkuu edelleen, ja nyt on kymmenen vuotta siitä, kun ensimmäinen Android-käyttöjärjestelmä tuli markkinoille. Uusin Android 9.0 on koodinimeltään Pie. (Raphael 2018.)

4.2 iOS

Vuonna 2007 Apple esitteli ensimmäisen kosketusnäyttöihin sopivan käyttöjärjestelmän nimeltään OS 1.0. Samana vuonna julkaistu ensimmäinen iPhone sisälsi tämän käyttöjärjestelmän. Vuonna 2010 käyttöjärjestelmän sai uuden nimen, iOS. (Finder 2018.)

Käyttöjärjestelmä hyödyntää monikosketusominaisuutta, jossa sormen liikkeillä voidaan suorittaa erinäisiä toimintoja, kuten liikuttamalla kahta sormea lähemmäksi toisiaan lähentääksesi ruutu näkymää tai viemällä sormi laidasta laitaan vaihtaaksesi sivua (Lifewire 2018b).

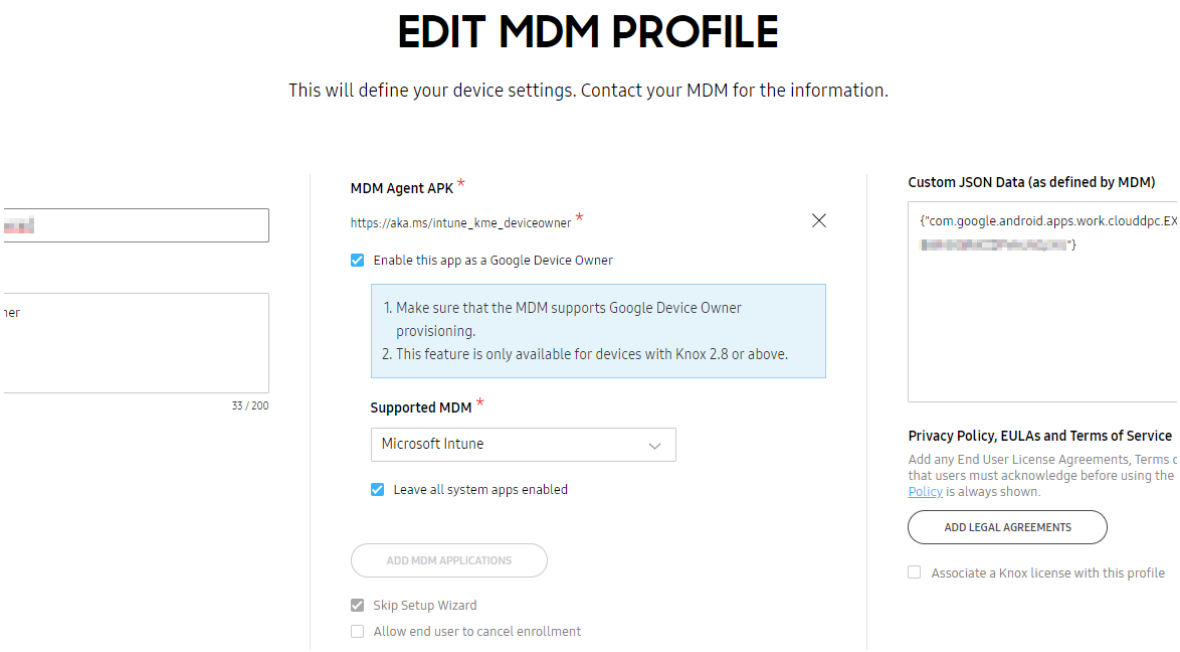
iOS-käyttöjärjestelmässä jokainen sovellus on erillään suljetussa tilassa. Tällä on tarkoitus tuoda tietoturvaa estäen sovellusten vaikutuksen keskenään. Vaikka yksi sovellus olisikin saastunut, ei saastunut sovellus pääse saastuttamaan muita sovelluksia. Tapauksia varten, joissa sovellusten halutaan keskustelevan keskenään, on iOS:ssä toiminto, jolla tämä voidaan mahdollistaa tapauskohtaisesti. (Lifewire 2018b.)

Sovellusten jakeluun iOS käyttää App Store -nimistä sovellusta, jossa kaikki käyttöjärjestelmälle ladattavat sovellukset löytyvät keskitetysti. Apple pitää kauppaa tiukasti hallinnassaan ja päivittää aika ajoin säännöksiä kaupan sovelluksille. Säännökset ovat johtaneet siihen, että sovelluksia poistetaan kaupasta. Tähän ryhmään kuuluvat vanhat sovellukset, jotka eivät ole yhteensopivia uusimman käyttöjärjestelmän kanssa, tai sovellukset, jotka tarjoavat työkaluja toiminnoille, joita käyttöjärjestelmä ei tarvitse. (Lifewire 2018a.)

5 MOBIILILAITEHALLINTAAN REKISTERÖITYMISEN AUTOMATISOINTI

5.1 Knox Mobile Enrollment

Samsung Knox Mobile Enrollment automatisoi mobiililaitteen rekisteröitymisen hallintajärjestelmään. Toimiakseen KME vaatii Samsungin valmistaman laitteen, josta löytyy Knox. Uusin Knox versio on 2.9, joka mahdollistaa älypuhelimen käyttöönoton device owner -hallintaan. Tämän lisäksi KME vaatii järjestelmänvalvojalta rekisteröinnin Knox Mobile Enrollment -ohjelmaan ja Samsung-laitteiden valtuutetun jälleenmyyjän, joka on samaisessa ohjelmassa mukana. (SamsungKnox 2018.) Mobiililaitteita pystyy myös lisäämään KME-portaalin jälkikäteen. Tarvitsee vain antaa valtuutetulle jälleenmyyjälle mobiililaitteen IMEI-koodin. Jälleenmyyjän hyväksyttyä puhelimen portaaliin voi järjestelmänvalvoja määrittää puhelimelle hallintaprofiilin (kuvio 4).



Kuvio 4. KME MDM Profile

KME:n toiminta perustuu siihen, että järjestelmä kykenee tunnistamaan mobiililaitteen ja mobiililaitteen käyttöönotossa aloittamaan rekisteröitymisen valittuun hallintajärjestelmään. Vaikka puhelimeen tekisi tehdasasetusten palautuksen, aloittaa laite rekisteröitymisprosessin taas puhelimen käynnistyttyä. Näin puhelin voidaan suoraan lähettää käyttäjälle ja rekisteröitymisprosessista tulee automatisoitu. Prosessi on loppukäyttäjälle ohjeistettu eikä vaadi järjestelmänvalvojalta toimenpiteitä. Tämä säästää järjestelmänvalvojalta aikaa tehdä asetuksia manuaalisesti ja mobiililaite voidaan toimittaa käyttäjälle ilman, että mobiililaite koskaan kävisi IT-osastolla.

5.2 Google Zero-touch

Googlen Zero-touchilla voidaan automatisoida mobiililaitteen rekisteröityminen hallintajärjestelmään. Vaatimuksena Googlen Zero-touchille, on mobiililaitteessa oltava vähintään käyttöjärjestelmä 8.0 tai Pixel älypuhelin, jossa on Android 7.0. Lisäksi laitehallintajärjestelmän on tuettava täysin hallittuja laitteita, jotka on hankittava valtuutetulta jälleenmyyjältä. (Android Enterprise 2018b.)

Hallinta tapahtuu nettiportaalista, josta järjestelmänvalvoja voi valita portaaliin kirjatuille laitteille käytössä olevan mobiililaitehallinnan. Rekisteröityminen mobiililaitehallintaan tapahtuu mobiililaitteen käynnistymisen yhteydessä. Toiminta on automatisoitu ohjaten käyttäjää, mikä tekee mobiililaitehallintaan rekisteröitymisestä sujuvaa. (Android Enterprise 2018b.)

5.3 Apple DEP

Apple DEP eli Device Enrollment Program mahdollistaa iOS-mobiililaitteiden automatisoidun rekisteröinnin valittuun mobiililaitehallintaan. Käyttö vaatii rekisteröitymisen Apple laiterekisteröintiohjelmaan, jos yritys ostaa Apple-laitteita suoraan Applelta tai rekisteröintiohjelmaan valtuutetulta jälleenmyyjältä. Mobiililaitteen käyttöjärjestelmän pitää olla iOS 7.x tai uudempi.

Laite voidaan rekisteröidä suoraan oston yhteydessä tai manuaalisesti jälkikäteen käyttäen Apple Configuratoria. Laite rekisteröi itsensä valittuun mobiililaitehallintaan laitteen aktivoinnin yhteydessä. Vaikka laite onnistuttaisiin tyhjentämään, niin mobiililaite aloittaa rekisteröinnin taas, kun laitetta ollaan aktivoimassa. (Apple Inc 2018.)

6 REKISTERÖITYMINEN

6.1 NFC

NFC on lyhenne sanoista Near Field Communication ja nimensä mukaisesti mahdollistaa laitteiden kättelyn sekä tiedonsiirron lyhyeltä kantamalta (Android Authority 2018). Lähimaksaminen on tästä hyvä esimerkki, jossa NFC:tä hyödyntäen kortti tuodaan riittävän lähelle lukijaa, jolloin maksutapahtuma aktivoituu. Maksukortin tilalla voi olla NFC:tä hyödyntävä mobiililaite.

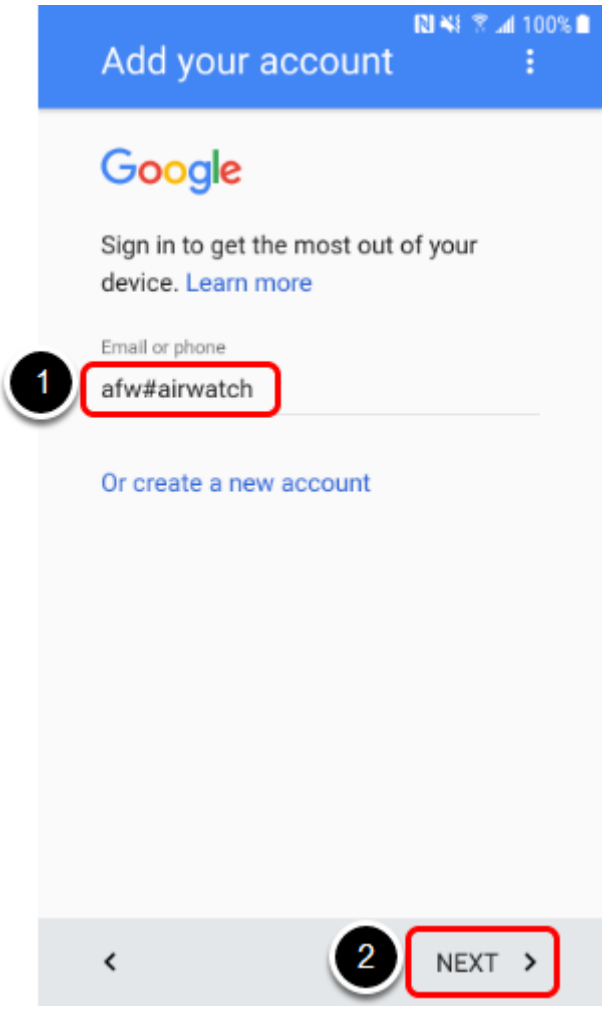
NFC:tä hyödyntävä mobiililaite vaatii laitteelta vähintään Android 5.0 -käyttöjärjestelmän sekä NFC-ominaisuuden. Nämä vaatimukset tekevät NFC:stä yhden käytetyimmistä tavoista rekisteröidä mobiililaitehallintaan. (Miradore 2018b.) Tavat vaihtelevat eri MDM-järjestelmien välillä, mutta pääperiaate on sama.

Jo valmisteltuun mobiililaitteeseen asennetaan laitehallinnan tarjoama NFC-sovellus, johon voidaan laittaa hallinnan vaatimat asetukset. Rekisteröitävä mobiililaite tuodaan asetukset sisältävän mobiililaitteen lähelle ja rekisteröinti alkaa. (Miradore 2018b.)

6.2 DPC token

Android-käyttöjärjestelmän 6.0 ja uudemmat mobiililaitteet voidaan myös ottaa hallintaan DPC tokenin avulla. DPC token hyödyntää Android Enterprisen tapaa ottaa mobiililaitehallintaan ilman siihen erikseen lisättävää henkilökohtaista Google-tiliä. (Bayton 2018a.)

Mobiililaitteen käyttöönottovaiheessa voidaan Google-tilin tilalle laittaa laitehallinnan token (kuvio 5), joka aloittaa laitteen rekisteröitymisen luoden mobiililaitteeseen henkilökohtaisen Google-tilin tilalta yrityksen hallitseman Google-tilin. Google-tilin sähköpostin tilalle kirjoitetaan afw# ja hallinnan oma tunniste. Miradorella token on afw#miradore ja Microsoftin Intunella afw#setup. (Bayton 2018a.)



Kuvio 5. Airwatch indentifier (VMware 2019)

6.3 QR-koodi

QR-koodi on kaksiulotteinen kuviokoodi, joka sisältää informaatiota. Toiminnaltaan QR-koodi on samanlainen kuin esimerkiksi maitopurkista löytyvä viivakoodi. QR-koodin lukemiseen tarvitsee kameran, QR-koodin lukusovelluksen sekä joissain tapauksissa internet-yhteyden. Koska nämä komponentit löytyvät mobiililaitteista, on QR-koodeista tullut yleinen tapa jakaa informaatiota mobiilialustoille. QR-koodi on kaikkien muokattavissa, ja kuka vaan voi tehdä sellaisen internetistä löytyvillä ilmaisilla työkaluilla. (QR code generator 2018.)

Jos mobiililaitteessa on käyttöjärjestelmänä Android 7.0 tai uudempi (taulukko 1), voidaan mobiililaite rekisteröidä laitehallintaan mobiililaitteen aktivointivaiheessa. Uuden tai tehdasasetuksiin palautetun mobiililaitteen ensimmäisen käynnistyksen yhteydessä voi käyttäjä napauttaa mobiililaitteen ruutua kuusi kertaa, joka aktivoi QR-koodin lukijan. (Miradore 2018b.)

Taulukko 1. Tuetut rekisteröintitavat

	QR-koodi	NFC	Token
Android 8	x	x	x
Android 7	x	x	x
Android 6		x	x
Android 5		x	

Tällä QR-koodin lukijalla voidaan lukea mobiililaitehallintaa varten rakennettu QR-koodi. Tästä esimerkkinä on alla oleva koodi, joka on AirWatch MDM ratkaisun tapa rekisteröidä mobiililaite hallintaan (Talvitie 2018).

{

"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":

"com.airwatch.androidagent/com.airwatch.agent.DeviceAdministratorReceiver",

"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":

"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8=\n",

"android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":

"https://awagent.com/mobileenrollment/airwatchagent.apk",

"android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,

"android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": true,

"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

"serverurl": "https://cn1108.awmdm.com",

"gid": "M8226120"

} }

Tämä kyseinen koodi voidaan muuntaa QR-koodiksi generaattorilla ja siitä saadaan QR-koodikuvio (kuvio 6). Tämä kuvio voidaan skannata älypuhelimella, joka aktivoi rekisteröinnin hallintaan.

Kuvio 6. QR-koodi (Talvitie 2018)

6.4 Agentti

Laitehallinnan lisääminen jo käytössä oleviin mobiililaitteisiin onnistuu asentamalla laitteeseen laitehallinnan sovellus eli agentti. Sovelluksen voi ladata käyttöjärjestelmän tarjoamasta kaupasta, kuten esimerkiksi Android-mobiililaitteista löytyvästä PLAY-kaupasta. Agentti on myös mahdollista siirtää mobiililaitteeseen valitulla tiedonsiirrolla ja asentaa suoraan laitteesta. Jos yritys on määrittänyt palveluilleen käyttörajoituksia, niin ilman agentin asennusta ja rekisteröintiä hallintaan ei ole mahdollisuutta käyttää yrityksen palveluja, kuten sähköpostia. (Microsoft 2017.)

Microsoftin Intune tarjoaa agentiksi sovellusta nimeltä Yritysportaali. Yritysportaalin asennuksen jälkeen voi käyttäjä avata sovelluksen, joka ensimmäisenä pyytää käyttäjän kirjautumistiedot. Jos käyttäjän tiedot löytyvät hallinnasta, on hänellä mahdollisuus jatkaa laitteen rekisteröintiä sovelluksen ohjeistuksen mukaan. Koska agentti on usein käytössä BYOD-tapauksissa, ohjeistaa agentti käyttäjää siitä, mitä tullaan hallitsemaan ja mitä järjestelmänvalvoja tulee laitteesta näkemään. Agentin rekisteröitymisvaiheessa agentti asentaa puhelimeen laitehallinnasta määritetyt asetukset, kuten esimerkiksi sen, että laitteessa on oltava PIN-koodi ruudunlukitukselle. Jos ruudunlukitusta ei ole asetettu laitteeseen, on käyttäjän asetettava ruudunlukitus, jotta rekisteröintiprosessi jatkuisi. (Microsoft 2017.)

7 HALLINTATAVAT

7.1 Android device admin

Alkaen Android versiosta 2.2 on device admin ollut tapa hallita mobiililaitetta. Mobiililaitteeseen asennetulle agentille annetaan mobiililaitteeseen täydet käyttöjärjestelmänvalvoja oikeudet. (Microsoft 2018). Näin agentilla on täydet valtuudet hyödyntää Android laitteen ohjelmointirajapintaa, josta on lyhenne API (Bayton 2018b.)

Android 5.0:sta alkaen on Google kutsunut device admin hallintatapaa nimellä Android Legacy. Nimensä mukaisesti on device admin poistuva hallintatapa ja Google on kehittänyt sen tilalle Android fully managed devicen (device owner) ja work profilen (profile owner), joista käytetään yhteisnimeä Android Enterprise. (Android Enterprise 2018a.)

Google on vaiheittain poistanut ohjelmointirajapintoja Androidista (kuvio 7), ja vuodesta 2019:ta sekä Android 9:n myötä poistuu taas osa ohjelmointirajapinnoista. Näiden muutosten myötä laitehallinta on menossa Android Enterprisen hallintatavan käyttämiseen laitehallinnassa. (Android Enterprise 2018a.)

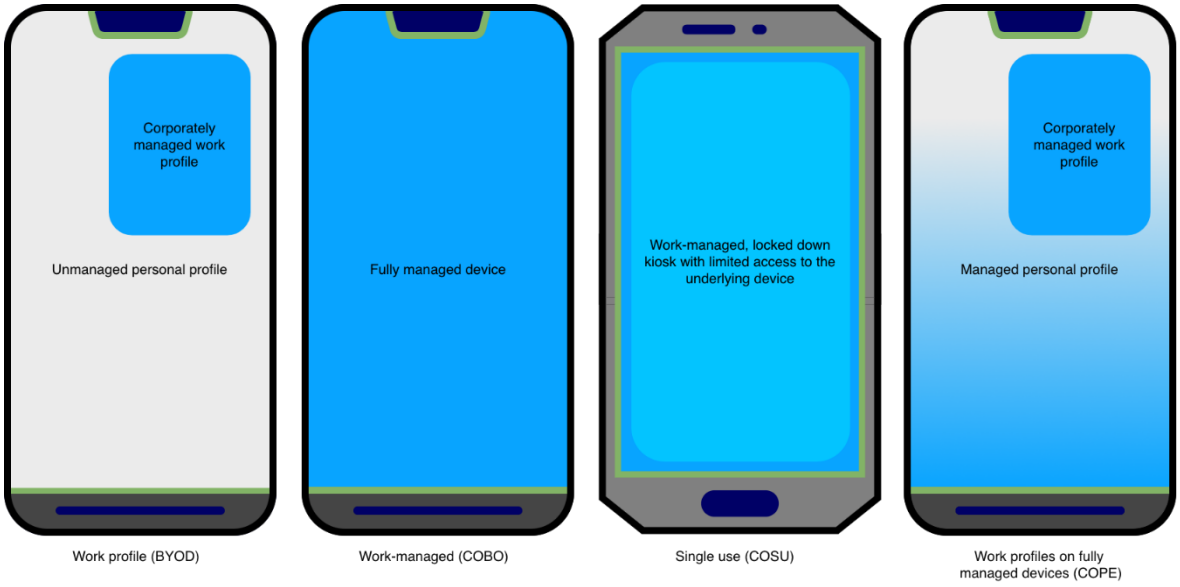
Kuvio 7. Poistuvat ohjelmointirajapinnat (Talvitie 2018)

7.2 Android Enterprise

Android Enterprise, joka aiemmin tunnettiin nimellä Android for Work, tarjoaa kaksi uutta tapaa hallita mobiililaiteitta. Nämä ovat work profile sekä fully managed device. Näistä

fully managed device voidaan jakaa kolmeen eri hallintamuotoon (kuvio 8). (Microsoft 2018.)

Device adminin poistuessa on Android Enterprise jatkossa ainut tapa hallita Android-laitteita. Tästä johtuen testauksen pääpaino uusilla laiteilla on juuri Android Enterprisen hyödyntäminen laitehallinnassa.

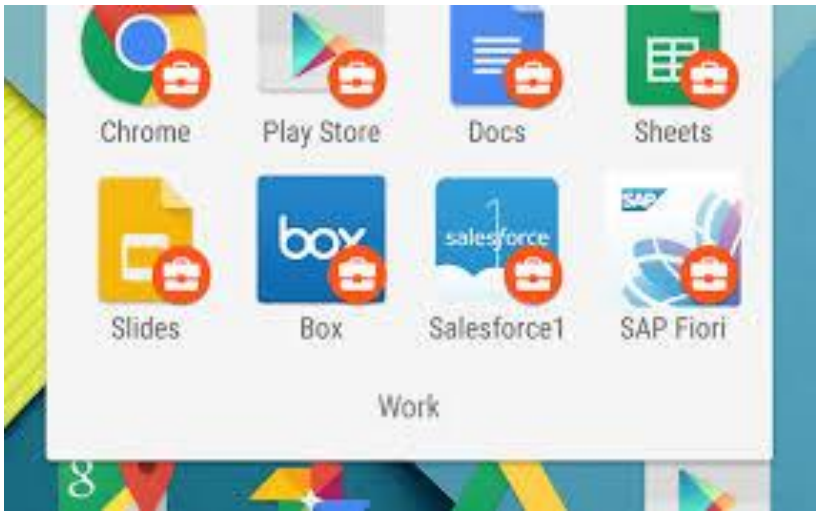


Kuvio 8. Android Enterprise hallinta (Bayton 2018c)

7.2.1 Work profile

Work profile luo mobiililaitteeseen erillisen hiekkalaatikkotilan, jossa hallittavat sovellukset sijaitsevat. Nämä sovellukset ovat tunnistettavissa salkusta (kuvio 9) sovelluksen kuvakkeessa. Hallintapa on sopiva BYOD tapauksissa, joissa työntekijällä on käytössään oma puhelin. Work profilessa laitehallinta toimii vain työprofiilin sovelluksiin ja käyttäjän oma henkilökohtainen puoli puhelimesta jää koskemattomaksi. Järjestelmänvalvoja kykenee estämään tiedonsiirron työprofiilin ja henkilökohtaisen alueen välillä. Kun järjestelmänvalvoja tekee mobiililaitteeseen tyhjennyksen laitehallinnan kautta, tyhjenee vain työprofiilin tiedot ja käyttäjän henkilökohtainen puoli jää koskemattomaksi. (Bayton 2018c.)

Tarvittaessa käyttäjä kykenee ottamaan work profilen pois päältä väliaikaisesti. Work profile saadaan puhelimeen agentin kautta ja ei vaadi laitteen tehdasasetuksiin palauttamista ennen laitteen rekisteröitymistä hallintaan. (Bayton 2018c.)



Kuvio 9. Android work profile (9TO5 2015)

7.2.2 Fully managed Device

Täysin hallinnassa olevat laitteet eroavat siitä, ettei laitteessa ole erillistä käyttäjäpuolta. Tällä tapaa laite saadaan täysin hallintaan ja voidaan hallita täysin jotain tiettyä käyttötarkoitusta varten.

Jotta laite saadaan täysin hallintaan, on sen oltava uusi aktivoimaton laite tai jo käytössä ollut mobiililaite, joka on palautettu tehdasasetuksiin. COBO, COPE sekä COSU ovat kolme eri tyylistä hallintapaa, jotka ovat fully managed device kategoriassa. (Bayton 2018c.)

COBO

COBO on mobiililaite, joka on otettu täysin hallintaan. Sen käyttötarkoitus on määritetty estämään henkilökohtainen käyttö, ja mobiililaite sisältää vain järjestelmänvalvojan siihen asentamat sovellukset. Laitteesta on voitu myös poistaa joitain perussovelluksia, kuten kamera. (Bayton 2018b.)

COPE

COPE-malli sisältää työprofiilin sekä mahdollisesti rajoitetun henkilökohtaisen puolen. Erona pelkkään työprofiiliin on se, että hallinta on mahdollista myös henkilökohtaisella puolella. (Bayton 2018b.)

COSU

COSU-malli luo mobiililaitteesta yhden applikaation laitteen. Tämä kiosk-mallinen laite tarkoittaa mobiililaitetta, joka on käytettävissä hyvin rajoitettuna ja siinä on voitu asettaa toimimaan vain joku tietty erikseen määritetty sovellus. (Bayton 2018b.)

7.3 iOS

Mobiililaitteita, joissa on käyttöjärjestelmänä iOS, voidaan hallita Applen omalla Apple configurator-ohjelmistolla tai käyttäen jotain kolmannen osapuolen MDM tai EMM ratkaisua. Apple configurator vaaditaan silloin, jos halutaan käyttää laitteessa supervised käytäntöä. Supervised käytäntö mahdollistaa laajemman mobiililaitteen hallinnan. (SearchMobileComputing 2012.) Supervised käytäntö myös vaatii sen, että laite on rekisteröity Applen DEP -laiterekisteröintiohjelmaan.

iOS hallinnassa kyetään erottamaan käyttäjän henkilökohtainen ja työnantajan data. iOS hallinnan voikin jakaa kahteen eri tapaan. Käyttäjän omistama laite ja yrityksen omistama laite. Käyttäjän omistama laite tulee hallintaan asettamalla laitteeseen agentti, joka aktivoi laitteen hallinnointi työkalut. Nämä asetukset ovat käyttäjän näkyvillä ja hän on tietoinen mitä toimintoja laitteesta hallitaan. Yrityksen omistamat laitteet on rekisteröity Applen DEP laiterekisteröintiohjelmaan ja niistä on aktivoitu supervised käytäntö. (Apple 2018, 4-11.)

8 MOBIILILAITEHALLINTA JÄRJESTELMIEN TESTAUS

8.1 Testauksen aloitus

Testausta varten käytiin läpi mobiililaitehallinta ratkaisujen tarjontaa yleisesti. Mobiilaitehallinta järjestelmiä oli Versowoodilla tutkittu jo aikaisemmin ja sen pohjalta otettiin yhteyttä neljään Versowoodille jo tuttuun toimittajaan. Heiltä pyydettiin Versowoodin vaatimusmäärittelyyn sopiva mobiililaitehallinta ratkaisu. Vaatimusmäärittelyyn perustuen jokainen toimittaja oli valmis esittelemään mobiililaitehallinta ratkaisunsa.

Jokaisen toimittajan kanssa pidettiin palaveri, jossa he esittelivät mobiililaitehallinta ratkaisunsa. Kaikki neljä eri toimittajaa olivat varteen otettavia vaihtoehtoja, joten päätöksenä valittiin sisäiseen testaukseen Miradore, MobileIron, AirWatch sekä Intune. Jokaiseen ratkaisuun oli saatavissa testiympäristö niiden syvempää tarkastelua varten. Poikkeuksena oli Intune, joka oli Versowoodin käytettävissä jo olemassa olevan lisenssin myötä. AirWatchin ja Intunen tapauksissa oli mahdollisuus toimittajan kanssa käytävään aloituspäivään, jossa käytiin läpi järjestelmän käyttöönotto sekä perustoimintoja. Näissä kahdessa tapauksessa hyödynnettiin mahdollisuus asiantuntijan apuun.

Jokaisen ratkaisun testaukseen varattiin aikaa kaksi viikkoa, testaus tapahtuisi päivittäisen työn ohessa, mutta keskittyen testaukseen. Aikataulun sallimissa rajoissa suoritetun testauksen aikana kirjattiin ylös, kuinka hyvin ratkaisu täytti Versowoodin vaatimusmäärittelyn, testauksen aikana tehdyt havainnot sekä toimintatavat kuinka järjestelmällä toteutettiin mobiilihallintaa. Testausjakson jälkeen pidettiin sisäinen palaveri testatusta ratkaisusta ja yleisesti tulevasta mobiililaitehallinnasta.

8.2 Testauksen valmistelu

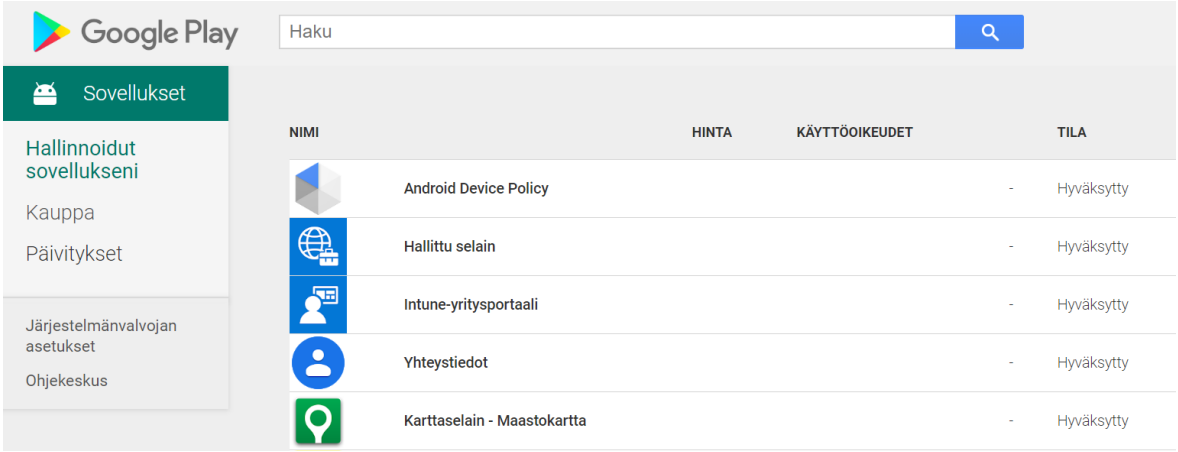
Testausta varten valittiin seitsemän mobiililaitetta, joista kuusi oli Android-käyttöjärjestelmällä ja yksi iOS-käyttöjärjestelmällä (taulukko 2). Mobiililaitteiden testiryhmään valikoitui eri valmistajien laitteita sekä eri versioita käyttöjärjestelmistä. Testiryhmän mobiililaitteet kuvastivat myös sen hetkistä Versowoodin laitekantaa. Laitekanta sisältää vakiolaitteet, joissa käyttäjällä on mahdollisuus valinnanvaraan käyttötarpeidensa mukaan. On myös mahdollista saada käyttöön laite vakiolaitekannan ulkopuolelta, jos perustelu on pätevä.

Taulukko 2. Testaukseen käytetyt mobiililaitteet

Valmistaja	Malli	Käyttöjärjestelmä
Samsung	Galaxy A8	Android 8.0
Samsung	X-Cover 4	Android 8.0
Samsung	Galaxy S5 Mini	Android 6.0
Samsung	Galaxy A5	Android 6.0
Huawei	P9	Android 7.0
Sony	Xperia Z5 Compact	Android 7.0
Apple	iPhone SE	iOS 12

Jokaista laitetta kohden luotiin yksi sähköpostillinen AD-käyttäjä. Jokaista Android mobiililaitetta varten luotiin henkilökohtainen Google-tili sekä iOS laitteelle iCloud-tili. Tämän lisäksi luotiin neljä Managed Google Play -tiliä, joiden avulla järjestelmänvalvoja kykenee hallitsemaan niitä sovelluksia, joita Play-kaupasta pystyy lataamaan. Managed Google Play linkitetään mobiililaitehallintaan, jonka avulla laitehallinta kykenee hallitsemaan sovellusjakeluja (kuvio 10), joita ovat automaattisesti laitteeseen asentuvat sovellukset sekä On demand -sovellukset. Managed Google Playn käyttö riippuu hallintatavasta. Puhelimen ollessa täysin hallinnassa, on käytössä vain Managed Google Play ja mobiililaitteeseen asentuu automaattisesti järjestelmänvalvojan asettamat sovellukset. Work Profile sen sijaan käyttää Managed Google Playta vain työprofiilissa, eikä sillä hallita henkilökohtaista Google-tiliä. (Android Enterprise Help 2019.) Mobiililaitteita varten ei avattu liittymiä, vaan hyödynnettiin Versowoodin tarjoamaa langatonta verkkoa.

iOS laitteiden hallinta valituilla hallintajärjestelmillä vaatii Apple ID:n luonnin, jota käytetään Apple Push -sertifikaatin luomiseen. Sertifikaatti on pakollinen, jotta valituilla hallintajärjestelmillä kyetään hallitsemaan iOS-laitteita. Sertifikaatti on vuoden voimassa ennen kuin sertifikaatti on uusittava. (Miradore 2018a.)



Kuvio 10. Managed Google Play

8.3 Testauksen toteutus

Testaus käynnistyi tutustumalla laitehallinnan käyttöliittymään ja käyttöliittymän toimivuus olikin yksi arviointikohde. Tämän jälkeen käytiin läpi ratkaisun soveltuvuus Versowoodin jo olemassa olevien palveluiden integrointiin, kuten jo olemassa oleva AD-ympäristö ja sen hyödyntäminen käyttäjien hallinnassa. Testaus jatkui testilaitteiden rekisteröinnillä testattuun laitehallintaan sen tarjoamilla tavoilla, samalla pohtien hallintatapaa, joka sopisi käyttöönotettavaksi Versowoodille.

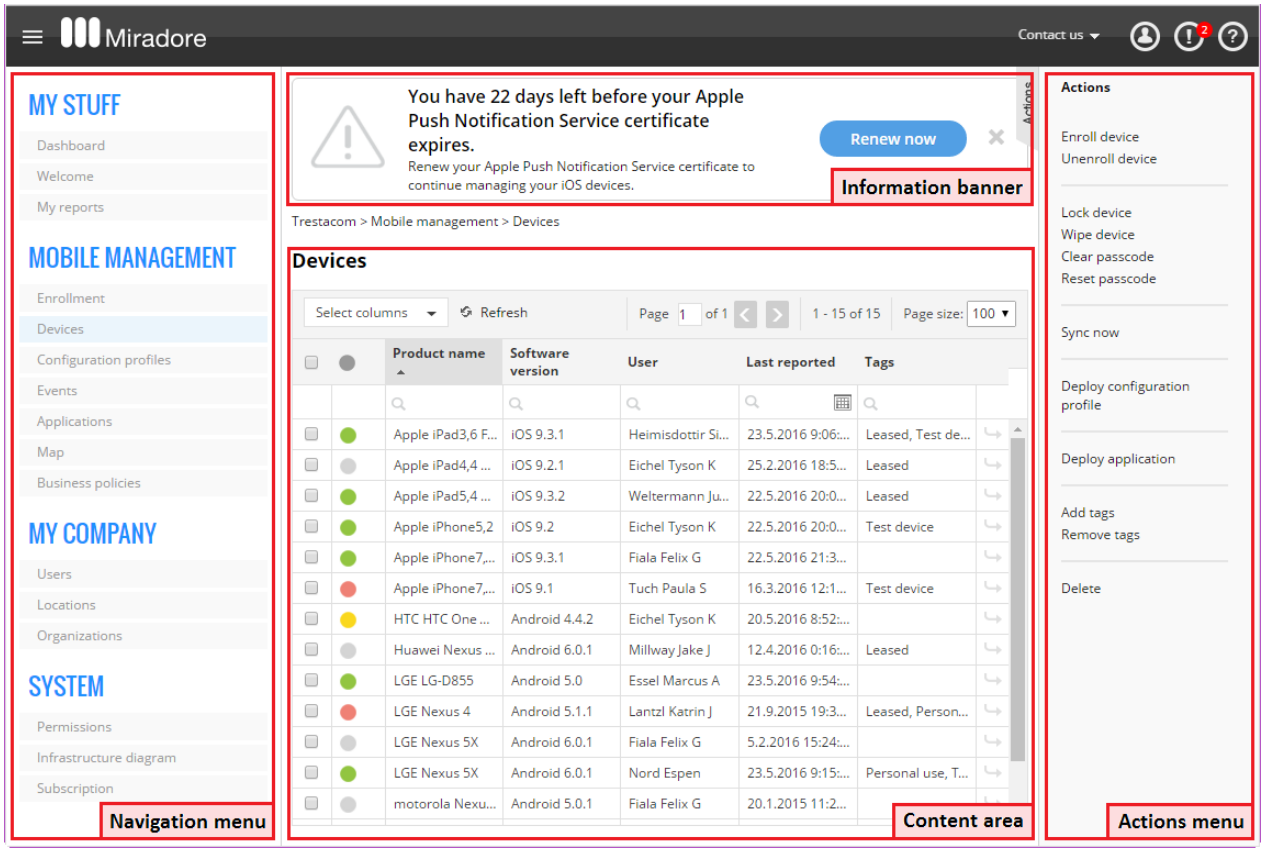
Testauksen ajan pidettiin yhteyttä toimittajaan sekä ongelmatapauksissa laitehallinnan tarjoamaan tukeen. Koska laitehallinta ratkaisut kehittyvät jatkuvasti, niin niiden kehitystä seurattiin, vaikka testaus olikin ratkaisun osalta ohi. Android Enterprisen kehittyessä tulee laitehallinta ratkaisuihin uusia toimintoja niiden kehittyessä mukana.

8.4 Miradore Online

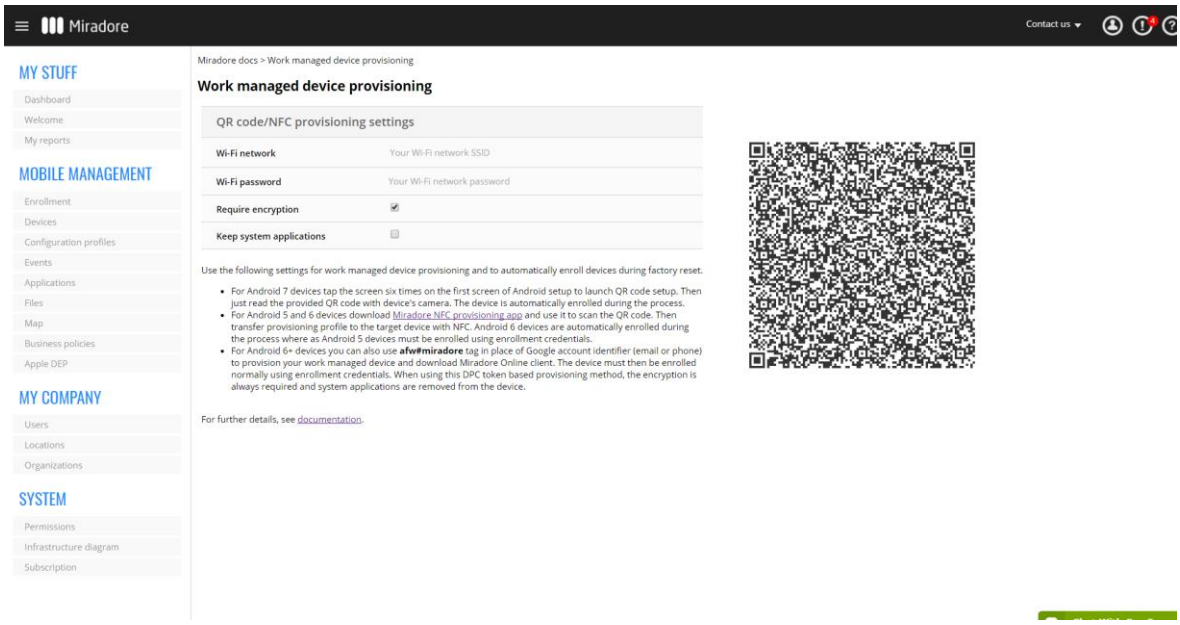
Ensimmäisenä testattavana ratkaisuna oli Miradore Online, joka on pilvipohjainen laitehallintaratkaisu. Sillä on mahdollista hallita Android-, iOS-, Windows-älypuhelimia sekä Windows 10 -työasemia. Miradore Onlinea oli testaus hetkellä mahdollista käyttää kolmella eri lisenssillä. Näistä kolmesta lisenssistä Enterprise kattoi vaatimusmäärittelyn mukaiset toiminnot ja siitä oli saatavilla 14 päivän ilmainen kokeilukäyttö. Käyttöliittymää (kuvio 11) käytettiin internet selaimen avulla.

Miradore Online mahdollisti connectorilla sen, että käyttäjät-valikkoon oli mahdollista saada Versowoodin AD-käyttäjät. Tämä mahdollisti rekisteröitymiskutsujen lähettämisen käyttäjän sähköpostiin. Rekisteröitymiskutsu sisälsi linkin, josta käyttäjä pystyy lataamaan Miradore Online Clientin. Miradore Online Client toimi agenttina, jota kautta mobiililaitteeseen asetetaan hallinnasta asetetut konfiguraatio profiilit. Mobiililaite oli mahdollista

rekisteröidä hallintaan käyttöjärjestelmästä löytyvällä QR-koodilla (kuvio 12), Miradore tokenilla tai käyttäen NFC:tä.



Kuvio 11. Miradore Online käyttöliittymä (Miradore 2018d)



Kuvio 12. Miradore Online QR-koodi (Miradore 2018c)

Testaus hetkellä ei ollut mahdollista käyttää Android mobiililaitteisiin KME rekisteröitymistapaa, mutta kyseinen ominaisuus oli kehityslistalla. Android Enterprisesta oli hyödynnetty work profilen luonti mobiililaitteeseen.

8.5 MobileIron

MobileIron on saatavilla pilvipohjaisena sekä paikallisena ratkaisuna. Testaukseen otettiin maksuton 30 päivää kestävä pilvipohjainen ratkaisu. Tämä on saatavissa MobileIronin kotisivuilta ja ympäristö saatiin käyttökuntoon samana päivänä. Käyttöliittymää käytettiin internet selaimen avulla.

AD-integraatio onnistui Azure-portaaliin. Tätä kautta käyttäjät oli mahdollista saada listattua MobileIron käyttöliittymään. Käyttäjille pystyttiin lähettämään sähköposti, joka sisälsi ohjeet rekisteröitymiseen.

MobileIronissa oli TeamViewer connectori, jolla mahdollistettiin etäyhteyden ottaminen mobiililaitteeseen. Agenttina MobileIron käytti Mobile@Work nimistä sovellusta. MobileIronilla on myös oma sähköpostisovellus nimeltä Email+. Tämän sähköpostisovelluksen asetusten hallinta onnistui MobileIronin kautta.

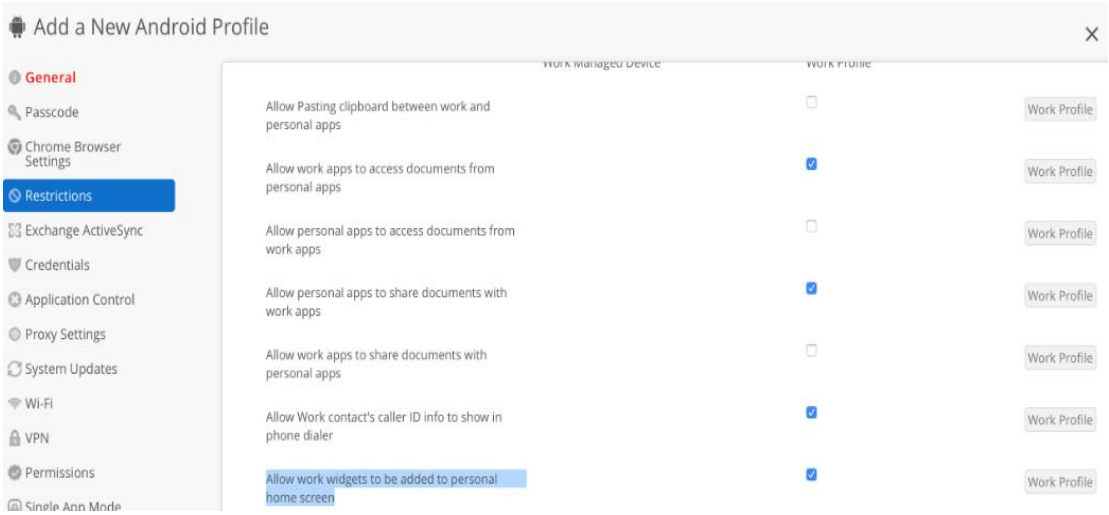
8.6 AirWatch

AirWatch on VMwaren luoma EMM-ratkaisu. Testaus aloitettiin toimittajan asiantuntijan kanssa, ja tähän aloitukseen oli varattu yksi henkilötyöpäivä. Päivän aikana läpi käytiin mobiililaitteiden rekisteröinti, perusasetukset sekä ympäristön pystytyksen, joka oli pilvihallintaratkaisu.

AirWatch integroitui Versowoodin AD-ympäristöön niin, että hallintaan sallitut käyttäjät voitiin hallita suoraan AD-ympäristöstä. AD-ympäristöön luodut ryhmät toimivat apuna sovellusten jaossa. Agenttina AirWatchissa on sovellus nimeltä Workspace ONE. MobileIronin tapaan on AirWatchiin saatavilla myös oma sähköpostisovellus nimeltä Boxer. Kyseisen sähköpostisovelluksen asetukset ovat laajemmin hallittavissa, kuin mobiililaitteiden natiivi sähköpostisovelluksen.

AirWatch sisälsi paljon eri asetuksia, joita muista ratkaisuista ei niiden testaus hetkellä löytynyt. Laitehallinta kyllä kehittyy jatkuvasti ja osa näistä asetuksista löytyy varmasti jo muistakin mobiililaitehallintaratkaisuista. Yhtenä esimerkkinä näistä asetuksista on mahdollisuus käyttää work profilen sovelluksen pienoisohjelmaa eli widgetiä mobiililaitteen henkilökohtaisella puolella (kuvio 13). Tämä ei normaalisti ole mahdollista, sillä work

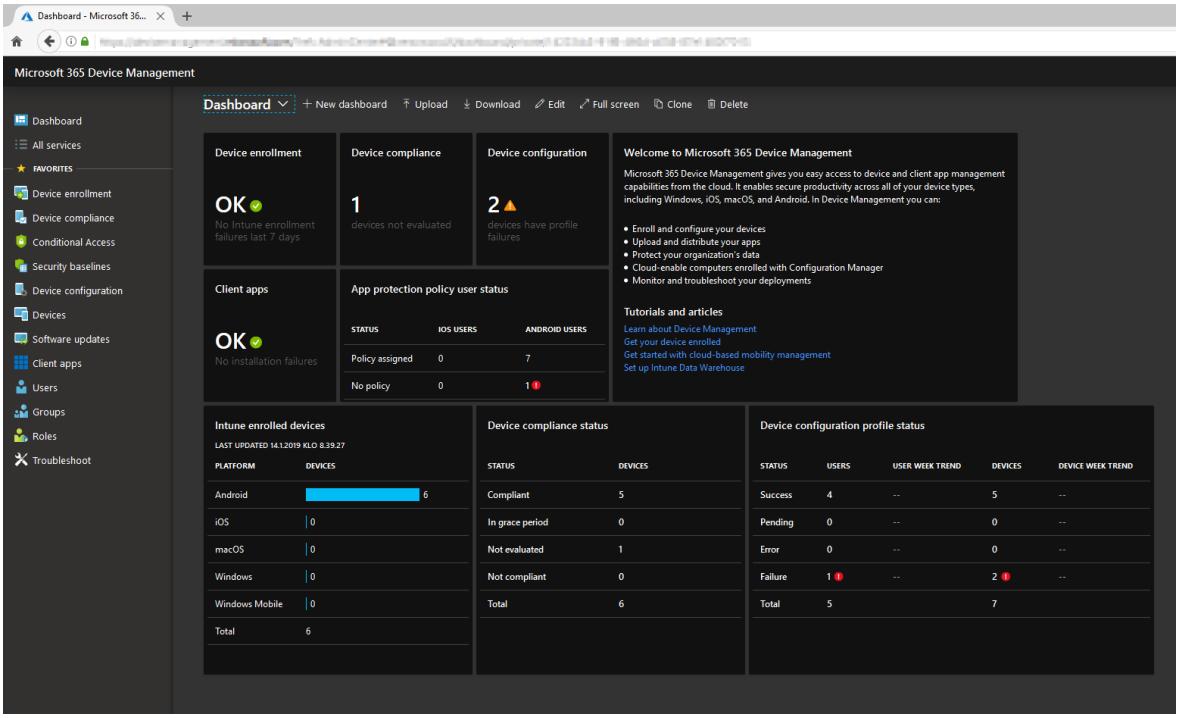
profile ei keskustele henkilökohtaisen puolen kanssa, ilman laitehallinnan sen mahdollistamista.



Kuvio 13. Allow work widgets to be added to personal home screen (Talvitie 2018)

8.7 Intune

Intune (kuvio 14) on Microsoftin kehittämä pilvipohjainen EMM ratkaisu. Intune on käytettävissä Azuren portaalista. Erona muihin ratkaisuihin oli, että Intune on jo olemassa olevan lisenssin kautta Versowoodin käytettävissä ja näin ollen käytössä ei ollut erillinen testiympäristö. Tästä syystä johtuen Intunen testaus ei ollut aikarajoitteinen.

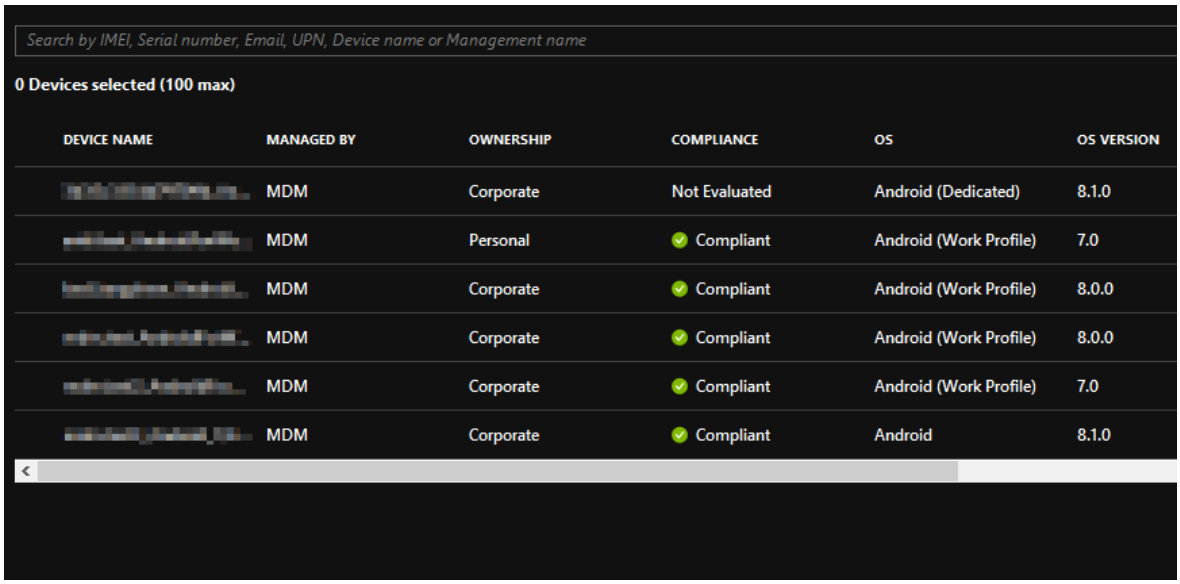


Kuvio 14. Intune Dashboard

Testaus aloitettiin toimittajan asiantuntijan kanssa ja siihen oli varattu yksi henkilötyöpäivä. Päivän aikana läpi käytiin ympäristön aktivointi, mobiililaitteiden rekisteröinnin eri tavat sekä laitehallinnan perustoiminnot.

Intune käyttää käyttäjien hallintaan Azure AD:ta, joten integroinnin suhteen ei tarvinnut tehdä erillisiä toimintoja. Intune onkin yksi sovellus isommassa kokonaisuudessa, joka on Azuren pilviympäristö ja sisältyy Enterprise Mobility + Security lisenssiin.

Intune hyödyntää Android Enterprise hallintatapaa, jossa mobiililaitteeseen tulee work profile (kuvio 15). Rekisteröityminen tapahtuu Yritysportaali-sovelluksella, joka toimii agenttina. Agentti on ladattavissa Googlen Play-kaupasta sekä iOS-laitteisiin Apple-kaupasta. Testaus hetkellä fully managed device vaihtoehdoista oli käytössä COSU, eli laitteesta oli mahdollista tehdä kiosk-laite. Tämä onnistui QR-koodin avulla, joka löytyi käyttöliittymästä.



Kuvio 15. Android (Work Profile)

Microsoftilla on Intunelle oma foorumi, jossa käyttäjät voivat ehdottaa uusia ominaisuuksia sekä antaa jo ehdotetuille ominaisuuksille ääniä. Eniten ääniä saavat ehdotukset otetaan kehityslistalle, jos ehdotus on mahdollista toteuttaa.

8.8 Mobiililaitehallinta järjestelmien vertailu

Testauksen aikana täytettiin ratkaisuehdotusten arviointi taulukkoa, joka sisälsi vaatimusmäärittelyssä mainitut arviointikohteet:

- hallinta käyttöliittymä (taulukko 3)
- Google Android -yritysominaisuudet (taulukko 4)

- tiedonhallinnan ominaisuudet (taulukko 5)
- pääsynhallinnan ominaisuudet (taulukko 6)
- laitteiden käyttöönotto (taulukko 7)
- laitteiden hallinta (taulukko 8)
- laitteiden käytöstä poisto (taulukko 9).

Ratkaisuehdotusten arviointi taulukko työstettiin toimittajille lähetetyn vaatimusmäärittelyn mukaisesti. Tässä vaiheessa alkoi opinnäytetyön tekeminen sekä syvempi tutustuminen mobiilihallintaan. Ratkaisujen testaus suoritettiin siihen sovitulla aikataululla, joten täydellistä ratkaisun läpikäyntiä ei välttämättä ollut mahdollista toteuttaa. Pitää ottaa huomioon, että ratkaisujen jatkuva kehittyminen on voinut muuttaa taulukon sen hetkistä arviointia niiden uusien toimintojen ja ominaisuuksien myötä. On myös otettava huomioon, että useat arviointi kriteerin kohdat löytyvät kaikista ratkaisusta. Tämä johtuu siitä, että ennen testausta oli olettamus, että ratkaisut poikkeaisivat toisistaan paljon enemmän. Testaus opetti, että hallinta menee Androidin ehdoilla. Esimerkkinä tästä on laitteiden tietojen varmuuskopiointi, joka olisi suoritettu mobiililaitehallinnan kautta etänä. Yksikään ratkaisu ei kyennyt suorittamaan kyseistä toimintoa, joka johtui siitä, ettei Androidissa ole sellaista ohjelmointirajapintaa tai se on tarkoituksella estetty.

Taulukko 3. Hallinta käyttöliittymä

	Miradore	MobileIron	AirWatch	Intune
AD-integraatio	AD-käyttäjät kyetään hakemaan, mutta varsinaista integraatiota ei ole	Hyödyntää Azure AD:ta	Tämä hoidetaan Connectorilla, joten käyttäjien hallinta voidaan hoitaa jo olemassa olevassa AD-ympäristössä	Voidaan hyödyntää jo olemassa olevaa AD-ympäristöä, mutta varsinainen hallinta Azure AD:ssa
Käyttäjien ja/tai laitteiden ryhmittely, ryhmäkäytännöt	Hyödyntää tägejä, jonka avulla voidaan yksilöidä käyttäjä	Hallinnassa kyetään luomaan ryhmiä/rooleja.	Hyödyntää jo olemassa olevaa AD ympäristöä.	Ryhmät luodaan joko AD-ympäristöön tai Azure AD.

		Jaottelee käyttäjän ja laitteen.		

Taulukko 4. Google Android -yritysominaisuudet

	Miradore	MobileIron	AirWatch	Intune
Android Enterprise: Work Profile Work Managed Managed Google Play	Hyödyntää	Hyödyntää	Hyödyntää	Hyödyntää

Taulukko 5. Tiedonhallinnan omaisuudet

	Miradore	MobileIron	AirWatch	Intune
Henkilökohtainen data / Työnantajan data	Android Enterprise Work Profile	Android Enterprise Work Profile	Android Enterprise Work Profile	Android Enterprise Work Profile
Hiekkalaatikko	Kyllä	Kyllä	Kyllä	Kyllä

Taulukko 6. Pääsynhallinnan omaisuudet

	Miradore	MobileIron	AirWatch	Intune
Ehdollisen pääsynhallinnan kontrollointi	Testaus vaiheessa jäänyt selvittämättä	Testaus vaiheessa jäänyt selvittämättä	Testaus vaiheessa jäänyt selvittämättä, mutta on mahdollista toteuttaa. Toiminta nähty niin	Onnistuu. Hyödyntää Authenticator mobiilisovellusta
Vahvan tunnistautumisen (MFA) kontrollointi				

Kertakirjautumisen kontrollointi (SSO)			livenä kuin videolta.	

Taulukko 7. Laitteiden käyttöönotto

	Miradore	MobileIron	AirWatch	Intune
Uuden laitteen hallintaan liittäminen, ilman SIM-korttia	Onnistuu	Onnistuu	Onnistuu	Onnistuu
Olemassa olevien ja käytössä olevien laitteiden liittäminen hallintaan loppukäyttäjän itsensä toimesta	Onnistuu	Onnistuu	Onnistuu	Onnistuu
Sovellusten esiasennus oltava mahdollista automatisoidusti ja keskitetysti	Onnistuu	Onnistuu	Onnistuu	Onnistuu
Käyttäjäkohtaisten sovellusasetusten/käyttäjäprofiilien/käyttäjätilien esimäärittely automatisoidusti ja sovelluskohtaisesti	Onnistuu	Onnistuu	Onnistuu	Onnistuu

Tietojen siirto vanhasta laitteesta uuteen	Ei onnistu	Ei onnistu	Ei onnistu	Ei onnistu

Taulukko 8. Laitteiden hallinta

	Miradore	MobileIron	AirWatch	Intune
Laitteiden asetusten ja rajoitusten hallinta	Riippuu hallintatavasta	Riippuu hallintatavasta	Riippuu hallintatavasta	Riippuu hallintatavasta
Laite-, ohjelmisto-, liittymä-, status- ja käyttäjätietojen inventointi ja raportointi	Kyllä	Kyllä	Kyllä	Kyllä
Laitteiden etäohjaus (etähallinta ja etätuki) ja etälukitus	Etälukitus on sikäli käyttöjärjestelmä ja hallintatapa sen sallii	Etälukitus on sikäli käyttöjärjestelmä ja hallintatapa sen sallii. Mahdollisuus TeamViewer connectorille, jolla etäyhteys mobiililaitteeseen.	Etälukitus on sikäli käyttöjärjestelmä ja hallintatapa sen sallii. Etäyhteys jäi testauksen ulkopuolelle.	Etälukitus on sikäli käyttöjärjestelmä ja hallintatapa sen sallii. Mahdollisuus TeamViewer connectorille, jolla etäyhteys mobiililaitteeseen.
Sovellusjakelut, -päivitykset, -poistot	Onnistuu	Onnistuu	Onnistuu	Onnistuu
Laiteohjelmistojen päivitykset	Riippuu mobiililaitteen käyttöjärjestelmästä	Riippuu mobiililaitteen käyttöjärjestelmästä	Riippuu mobiililaitteen käyttöjärjestelmästä	Riippuu mobiililaitteen käyttöjärjestelmästä

Laitteiden paikallisten tietojen hallintamahdollisuudet tietovaranto- tai sovelluskohtaisesti (organisaation tiedot vs. käyttäjän omat tiedot)	Android Enterprise Work Profile	Android Enterprise Work Profile	Android Enterprise Work Profile	Android Enterprise Work Profile
Laitteiden tietojen varmuuskopiointi ja tietojen palautus, jos mahdollista	Ei ole	Ei ole	Ei ole	Ei ole
Laitteiden etäpaikannus	Riippuu mobiililaitteen käyttöjärjestelmästä	Riippuu mobiililaitteen käyttöjärjestelmästä	Ei ole	Ei ole

Taulukko 9. Laitteiden käytöstä poisto

	Miradore	MobileIron	AirWatch	Intune
Tietojen poisto valikoidusti/sovelluskohtaisesti	Onnistuu. Toiminta hallintatavan mukaan.	Onnistuu. Toiminta hallintatavan mukaan.	Onnistuu. Toiminta hallintatavan mukaan.	Onnistuu. Toiminta hallintatavan mukaan.
Tietojen poisto täysin ja tehdasasetusten palautus	Onnistuu. Toiminta hallintatavan mukaan.	Onnistuu. Toiminta hallintatavan mukaan.	Onnistuu. Toiminta hallintatavan mukaan.	Onnistuu. Toiminta hallintatavan mukaan.

Kuten taulukosta on nähtävissä, on vaatimusmäärittelyn mukaiset arviointikriteerit täyttyneet jokaisella ratkaisulla useassa kohdassa. Kohdat, joissa vaatimusmäärittely ei ole

täyttynyt, ei välttämättä johdu puutteellisesta laitehallintaratkaisusta vaan siitä ettei käyttöjärjestelmä kykene kyseiseen toimintoon.

Vertailutaulukko ei nykyisessä muodossaan suoraan mahdollista päätöksen tekoa ratkaisusta, mutta toimii yhtenä työkaluna päätöstä tehtäessä.

Vertailun perusteella voitaisiin Versowoodille ehdottaa kahta eri vaihtoehtoa. Näistä ensimmäinen on AirWatch, joka tarjoaisi laajan hallintapaketin mobiilihallintaa tarvitsevalla yritykselle. AirWatch jäi ratkaisuista mieleen siinä olevien Android Enterprise toimintojen lukumäärältä, sekä nopeudelle lisätä uusia Androidin toiminnallisuuksia mobiilihallintaansa. Toinen vaihtoehto olisi Microsoftin Intune. Intunen käyttöönotto olisi vaivatonta, koska kyseinen tuote on jo Versowoodin käytettävissä ilman mitään erillistä kustannusta. Intunen integroituminen Versowoodin järjestelmiin toimii myös suurena etuna verrattuna ratkaisuihin, joiden integroituminen koettiin puutteelliseksi. Näiden kahden ratkaisun valintaan vaikuttavat myös testauksen aikana kertyneet kokemukset, toimittajan kanssa tehty yhteistyö sekä ratkaisun tulevaisuuden näkymät.

Miradore Onlinea en voi suositella sen puutteellisen AD-integraation takia. Hyvää Miradore Onlinessa oli sen helppokäyttöinen käyttöönotto sekä selkeä käyttöliittymä aloittelevalle käyttäjällä. MobileIron ei aivan yltänyt testauksessa Airwatchin ja Intunen tasolle käytettävyydessä, jääden täten myös suosittelun ulkopuolelle.

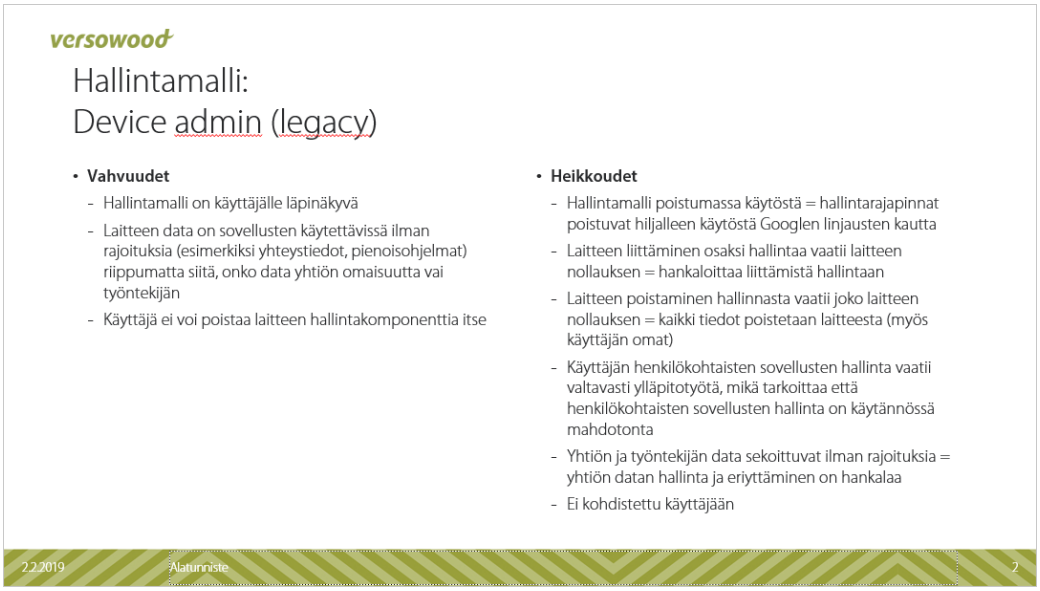
8.9 Testauksen lopputulos

Mobiililaitehallinta ratkaisujen testaus toimi hyvänä oppimisprosessina, miten mobiililaitehallinta toimii ja mihin kaikkiin toimintoihin sillä kyetään. Vaikkakin tiukan aikataulun puitteissa tehty testaus ei valittavasti ollut riittävä täydelliseen ratkaisun läpikäyntiin, oli se oppimisen kannalta kehittävä kokemus. Oppimisprosessi olikin jatkuvaa työn aloituksesta sen lopetukseen. Useamman kuin yhden hallinta ratkaisun testaus oli tärkeää, jotta voitaisiin tehdä päätös sopivasta ratkaisusta, joka mahdollistaisi Versowoodin vaatimuksien mukaisen mobiililaitehallinnan.

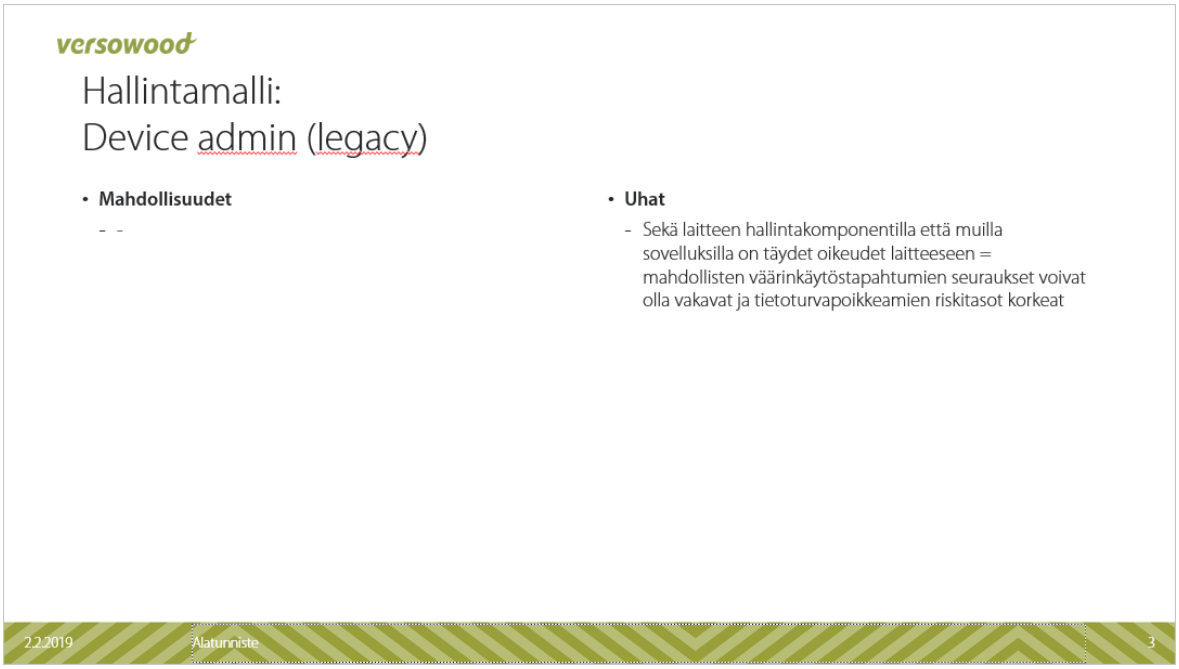
Jokaisesta hallinta ratkaisusta täytettiin arviointi vaatimusmäärittelyyn perustuen, sekä pisteytys Versowoodin oman arviointimallin mukaan. Näillä työkaluilla olisi mahdollista konkretisoida tuleva päätös. Opinnäytetyötä kirjoittaessa ei lopullista päätöstä ollut vielä tehty. Syy tähän on Androidin hallintatavat ja niiden tarkempi tutkiminen, niiden soveltuminen käytettäväksi ja tulevaisuuden hallintamahdollisuuksien selvittäminen. Tarkoituksena on kehittää mobiililaitteiden hallintamalli, jonka pohjalta lopullinen päätös soveltuvasta laitehallinta ratkaisusta on mahdollista tehdä. Hallintamallin päätöksen avuksi on tehty SWOT-analyysi, joka sisältää hallintatavat:

- Device admin (kuvio 16 ja17)
- Work profile (kuvio 18 ja 19)
- Fully managed device (kuvio 20 ja 21).

SWOT-analyysi kertoo jokaisen hallintatavan vahvuudet, heikkoudet, uhat sekä mahdollisuudet. Näistä kategorioista saadaan kiteytetty tieto sopivasta hallintavasta ja SWOT-analyysi toimiikin hallintamallin tukena.



Kuvio 16. Device admin SWOT 1/2



Kuvio 17. Device admin SWOT 2/2

Kuvio 18. Work Profile SWOT 1/2

Kuvio 19. Work Profile SWOT 2/2

Kuvio 20. Work Managed SWOT 1/2

Kuvio 21. Work Managed SWOT 2/2

9 YHTEENVETO

Tämän työn tavoite oli testata mobiiliympäristön laitehallinta ratkaisuja Versowoodille sekä löytää niistä sopiva ratkaisu Versowoodille. Testausta varten yhteyttä otettiin neljään jo Versowoodille tuttuun toimittajaan ja heiltä pyydettiin mobiililaitehallinta ratkaisua Versowoodin lähettämän vaatimusmääritelmän perusteella. Testilaitteina käytettiin Versowoodin omasta laitekannasta löytyviä älypuhelimia. Testilaitteiden käyttöjärjestelminä oli Android sekä iOS.

Mobiililaitehallinta voidaan jakaa kahteen osaan: on käyttäjän omistamat laitteet sekä yrityksen omistamat laitteet. Molempia varten on laitehallinnassa tavat hallita mobiililaitetta. Käyttäjän omistamiin laitteisiin sopii Android Enterprisen tarjoama work profile, joka luo mobiililaitteeseen erillisen tilan työsovelluksia varten. Mikään ei estä käyttämästä work profilea yrityksen omistamissa laitteissa, mutta laitehallinta ei hallitse täysin koko laitetta. Yrityksen omistamiin mobiililaitteisiin sopivampi hallintatapa on Android Enterprisen fully managed device, jossa laitehallinta kykenee hallitsemaan koko laitetta eikä vain osaa siitä. Fully managed device rekisteröinnin pystyy myös automatisoimaan hyödyntäen Samsung Knox Mobile Enrollment ohjelmaa ja Googlen Zero-touch laiterekisteröintiohjelmaa. iOS laitteissa käytetään Applen DEP laiterekisteröintiohjelmaa. iOS laitteista myös aktivoidaan supervised käytäntö, joka mahdollistaa laitteesta enemmän hallittavia asetuksia ja määrityksiä.

Mobiiliympäristön laitehallintaratkaisujen testaus vaiheessa dokumentoitiin vaatimusmäärittelyn täyttyminen ja tavat, jolla mobiililaitehallinta ratkaisu sen kykeni suorittamaan. Hallintajärjestelmät myös pisteytettiin Versowoodin oman arviointimallin mukaan.

Opinnäytetyötä kirjoittaessa ei vielä oltu tehty päätöstä mobiililaitehallinnan valinnasta. Kyse ei ollut siitä millä mobiililaitehallinnalla tultaisiin laitehallinta tekemään, vaan millä hallintatavalla mobiililaitehallinta tultaisiin toteuttamaan. Tulisiko hallinta work profilella, joka olisi hyvä tapa erottaa työsovellukset ja mahdollistaa käyttäjälle oma henkilökohtainen alue mobiililaitteesta, vai olisiko täysin hallittu managed device parempi vaihtoehto hallintatavaksi.

Hallintatapaan vaikuttaa myös mobiililaitteen käyttöjärjestelmän versio ja tästä johtuen kaikkia laitteita ei kyetä hallitsemaan samalla tavalla. Tutkimustyö jatkuu mobiililaitteiden hallintamallin suunnittelulla, jotta mobiililaitehallinnan käyttöönotto Versowoodilla sujuisi hallitusti sekä tuottaisi haluttua lisäarvoa.

Mobiililaitehallinnan merkitys yrityksille kasvaa koko ajan. Yhä useammat työntekijät käyttävät mobiililaitetta työssään ja hyödyntävät mobiililaitteella yrityksen tarjoamia palveluja

tai säilyttävät mobiililaitteessa yrityksen dataa. Mobiililaitehallinnalla voidaan turvata yrityksen data sekä mahdollistaa käyttäjälle yrityksen datan turvallinen käyttö. Mobiililaitehallinta tuo helpotusta laitteiden käyttöönottoon sekä laitteiden käytöstä poistamiseen.

LÄHTEET

9TO5, 2015. Google announces Android for Work w/ Google Play & new features for enterprise users [viitattu 7.1.2019]. Saatavissa: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRjhaiIwITkPLU_ruC4Vd09XW3t2FeaFwYrrspwVxoDrsMSfssuCQ

Android Authority 2018. What is NFC & how does it work? [viitattu 25.12.2018]. Saatavissa: https://www.androidauthority.com/what-is-nfc-270730/

Android Enterprise 2018a. Device admin deprecation [viitattu 7.1.2019]. Saatavissa: https://developers.google.com/android/work/device-admin-deprecation

Android Enterprise 2018b. Zero-touch enrollment for IT admins [viitattu 20.12.2008]. Saatavissa: https://support.google.com/work/android/answer/7514005

Android Enterprise Help 2019. Setup with a third-party EMM provider [viitattu 9.1.2019]. Saatavissa: https://support.google.com/work/android/answer/6174046?hl=en

Apple 2018. Managing Devices & Corporate Data on iOS [viitattu 8.1.2019]. Saatavissa: https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf

Apple Inc 2018. Tietoja Laitteen rekisteröinnistä [viitattu 23.12.2018]. Saatavissa: https://support.apple.com/fi-fi/HT204142

Bayton 2018a. Android Enterprise EMM Token collection [viitattu 25.12.2018]. Saatavissa: https://bayton.org/docs/enterprise-mobility/android/android-enterprise-emm-token-collection/

Bayton 2018b. Android glossary [viitattu 7.1.2019]. Saatavissa: https://bayton.org/docs/enterprise-mobility/android/android-glossary/

Bayton 2018c. What is Android Enterprise and why is it used? [viitattu 7.1.2019]. Saatavissa: https://bayton.org/docs/enterprise-mobility/android/what-is-android-enterprise-and-why-is-it-used/#byod-and-work-profile

Callaham, J 2018. The history of Android OS: its name, origin and more [viitattu 19.12.2018]. Saatavissa: https://www.androidauthority.com/history-android-os-name-789433/

Computerworld 2017. What's the difference between MDM, MAM, EMM and UEM? [viitattu 23.12.2018]. Saatavissa: https://www.computerworld.com/article/3206325/mobile-wireless/whats-the-difference-between-mdm-mam-emm-and-uem.html

Finder 2018. iOS: Everything you need to know about Apple's mobile OS [viitattu 23.12.2018]. Saatavissa: https://www.finder.com/ios-operating-system

Lifewire 2018a. How Many Apps Are In The App Store? [viitattu 23.12.2018]. Saatavissa: https://www.lifewire.com/how-many-apps-in-app-store-2000252

Lifewire 2018b. What Is the iPhone OS (iOS)? [viitattu 23.12.2018]. Saatavissa: https://www.lifewire.com/what-is-ios-1994355

Looper, C 2018. From Android 1.0 to Android 9.0, here's how Google's OS evolved over a decade [viitattu 19.12.2018]. Saatavissa: https://www.digitaltrends.com/mobile/android-version-history/

Microsoft 2017. Enroll your Android device in Intune [viitattu 27.12.2018]. Saatavissa: https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android

Microsoft 2018. Modern Android Management with Microsoft Intune [viitattu 7.12.2019]. Saatavissa: https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Modern-Android-Management-with-Microsoft-Intune/ba-p/250460

Miradore 2018a. About Apple Push Certificate [viitattu 9.1.2019]. Saatavissa: https://onlinesupport.miradore.com/hc/en-us/articles/200730452

Miradore 2018b. How to enroll work managed devices [viitattu 25.12.2018]. Saatavissa: https://onlinesupport.miradore.com/hc/en-us/articles/115001335365-How-to-enroll-work-managed-devices

Miradore 2018c. How to enroll work managed devices [viitattu 10.1.2019]. Saatavissa: https://onlinesupport.miradore.com/hc/article_attachments/115002015405/afw-work-managed-devices-provisioning-2017-03-07.png

Miradore 2018d. What is Miradore Online [viitattu 10.1.2019]. Saatavissa: https://onlinesupport.miradore.com/hc/en-us/article_attachments/204430285/MiradoreOnlineUI.png

Mobilock 2018. What is MDM, EMM or UEM? Let's Understand the Differences [viitattu 23.12.2018]. Saatavissa: https://blog.mobilock.in/what-is-mdm-emm-or-uem-lets-understand-the-differences/

Raphael, J 2018. Android versions: A living history from 1.0 to Pie [viitattu 19.12.2018] Saatavissa: https://www.computerworld.com/article/3235946/android/android-versions-a-living-history-from-1-0-to-today.html

SamsungKnox 2018. Knox Mobile Enrollment User Guide [viitattu 20.12.2008]. Saatavissa: https://docs.samsungknox.com/KME-Getting-Started/Content/about-kme.htm#h2_3

SearchMobileComputing 2012. Apple Configurator [viitattu 8.1.2019]. Saatavissa: https://searchmobilecomputing.techtarget.com/definition/Apple-Configurator

Talvitie, H 2018. Re: Android legacy hallintarajapintojen tippuminen pois. Sähköpostiviesti. Vastaanottaja Karppinen, L. Lähetetty 21.12.2018.

QR code generator 2018. QR Code Basics [viitattu 25.12.2018]. Saatavissa: https://www.qr-code-generator.com/qr-code-marketing/qr-codes-basics/

Solution Review 2018. Understanding the Difference Between MDM, MAM, EMM, and UEM [viitattu 23.12.2018]. Saatavissa: https://solutionsreview.com/mobile-device-management/understanding-the-difference-between-mdm-mam-emm-and-uem/

Versowood 2018a. Historia [viitattu 19.12.2018]. Saatavissa: https://www.versowood.fi/fi/konserni/historia

Versowood 2018b. Puulla on syynsä [viitattu 19.12.2018]. Saatavissa: https://www.versowood.fi/fi

Versowood 2019. Versowood. Powerpoint.

VMware 2019. Managing Android Devices [viitattu 2.2.2019]. Saatavissa: https://techzone.vmware.com/quick-start-tutorial-series-cloud-based-vmware-workspace-one/managing-android-devices