jamk.fi

AirWatch-mobiilihallintapalvelun käyttöönotto ja hyödyt

Miika Järvenpää

Opinnäytetyö
Toukokuu 2020
Tekniikan ala
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Järvenpää, Miika	Opinnäytetyö, AMK	Toukokuu 2020
	Sivumäärä 40	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
AirWatch-mobiilihallintapalvelun käyttöönotto ja hyödyt

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Sampo Kotikoski, Jari Hautamäki

Toimeksiantaja(t)
Oppimis- ja ohjauskeskus Valteri, Onerva

Tiivistelmä

Opinnäytetyön toimeksiantajana toimi Oppimis- ja ohjauskeskus Valteri, Onerva, joka tarjoaa palveluja yleisen, tehostetun ja erityisen tuen tarpeisiin. Tavoitteena oli ottaa käyttöön Valterin kouluympäristöön VMwaren AirWatch-tuote, jolla saataisiin kaikki opetukseen käytettävät mobiililaitteet yhden keskitetyn hallintapalvelun alle. Käyttöönoton tarkoituksena oli parantaa yleistä turvallisuutta, mahdollistaa sovelluslisenssien keskittäminen ja vähentää tietojen väärinkäytön riskiä. Kyseinen palvelu oli jo päätetty valmiiksi sekä otettu käyttöön toisessa toimipisteessä.

Toteutus tehtiin pääosin loma-aikana, jolloin palvelun käyttöönotto ei aiheuttanut haittaa opetukselle. Palveluun lisättiin kaikki koululla käytössä olevat Android- ja iOS-mobiililaitteet, lukuun ottamatta puhelimia. Ympäristö konfiguroitiin vaatimusten mukaisesti lisäämään käytännöllisyyttä ja turvallisuutta. Palvelun ominaisuuksia tutkittiin toimintavaatimuksien ja etujen kannalta.

Tuloksena saatiin toimiva mobiilihallinta, jolla voidaan hallita etänä molempia käyttöjärjestelmiä. Palvelun käyttöönotto toi selviä hyötyjä ympäristöön. Maksullisia iOS-sovelluslisenssejä voitiin hankkia ja jakaa keskitetysti sekä siirtää käyttäjältä toiselle ilman, että se on sidoksissa henkilökohtaiseen Apple ID -tiliin. Sovellusten keskitetyn jakamisen avulla opetuksessa käytettäviä sovelluksia voitiin hallita paremmin. Riskiä oppilaiden sekä henkilökunnan salaisten tietojen vuotamisesta saatiin pienennettyä etähallinnan avulla. Käyttöjärjestelmien versioita voitiin seurata ja päivittää etänä. Unohdettujen pääsykoodien tapauksissa ne voidaan nollata ilman fyysistä pääsyä laitteeseen. Tavoitteena oli myös rajoittaa oppilaiden vapaata pääsyä Play-kauppaan, mutta Androidilla sovellusten keskitetty jakaminen ei toiminut halutulla tavalla Play-kaupan estämisen kanssa.

Avainsanat (asiasanat)
AirWatch, MDM, mobiililaitehallinta, Android, iOS

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Järvenpää, Miika	Bachelor's thesis	May 2020
		Language of publication: Finnish
	Number of pages 40	Permission for web publication: x

Title of publication

Deployment and benefits of AirWatch mobile management service

Degree programme

Information and Communications Technology

Supervisor(s)

Sampo Kotikoski, Jari Hautamäki

Assigned by

Valteri Centre for Learning and Consulting, Onerva

Abstract

The thesis was assigned by Valteri Centre for Learning and Consulting, Onerva, a service provider for special education needs. The goal was to implement VMware AirWatch product in Valteri's school environment to connect all mobile devices used for studying into one centralized management service. The purpose of the deployment was to improve general security, enable centralized management of application licenses and reduce the risk of data misuse. This service had already been chosen and put into use at another Valteri school unit.

The implementation was mainly carried out during the holidays, when the deployment of the service did not cause any inconvenience to studying. Except for phones, all Android and iOS mobile devices used at the school were added to the service. The environment was configured as required to increase practicality and safety. Features of the service were examined in terms of operational requirements and benefits.

The result was a functional mobile management that can be used to remotely manage both operating systems. The introduction of the service brought clear benefits to the environment. Paid iOS app licenses could be acquired and distributed centrally and transferred from one user to another without being tied to a personal Apple ID account. Centralized application sharing allowed for better management of applications used in studying. The risk of leaking confidential student and staff information was reduced with remote management tools. Operating system versions could be monitored and updated remotely. In case of forgotten lock screen codes, they can be reset without physical access to the device. The goal was also to restrict students' Play Store usage; however, on Android the centralized application sharing did not work as desired while the Play Store was blocked.

Keywords/tags (subjects)

AirWatch, MDM, mobile device management, Android, iOS

Miscellaneous (Confidential information)

Sisältö

Kuviot

Lyhenteet

APK	Android Package Kit
BYOD	Bring Your Own Device
DEP	Device Enrollment Program
EMM	Enterprise Mobility Management
MAM	Mobile Application Management
MDM	Mobile Device Management
NFC	Near Field Communication
QR	Quick Response
UEM	Unified Endpoint Management

1 Johdanto

1.1 Toimeksiantaja ja tavoitteet

Opinnäytetyön toimeksiantajana oli Oppimis- ja ohjauskeskus Valteri, Onerva, joka toimii Opetushallituksen alaisuudessa ympäri Suomea. Tarjottaviin palveluihin kuuluu konsultointia, koulutusta, oppimateriaaleja, ohjauskäyntejä, tuettua asumista ja verkkovälitteistä opetusta, joiden avulla mahdollisimman monella oppilaalla on mahdollisuus käydä koulua omassa kotikunnassaan ja lähikoulussaan. Valterilla on toimipisteitä Helsingistä Ouluun, joiden yhteydessä toimii Valteri-koulu. Koulu tarjoaa esiopetusta, perusopetusta ja lisäopetusta erityisen tuen piirissä oleville oppilaille. Mobiililaitteet ovat keskeisessä osassa koulun opetuksessa. (Valteri n.d.)

Työn tavoitteena oli tutustua VMware AirWatch -hallintapalveluun ja toteuttaa konfiguraatiot lisäämään turvallisuutta ja helpottamaan ison laitemäärän hallintaa. Lisääntyvä mobiililaitteiden käyttö työskentelyssä asettaa enemmän vaatimuksia mobiilihallinnalle. Työssä käydään läpi teoriaa yleisesti mobiilihallinnan osa-alueista, yleisimmin käytössä olevista käyttöjärjestelmistä ja AirWatchista. Lisäksi työssä toteutettiin palvelun käyttöönotto kouluympäristössä sekä tutkittiin sen ominaisuuksia. Mobiilihallintaratkaisujen toimittajia on useita, jotka tarjoavat eri ominaisuuksilla olevia palveluita. Tämä palvelu oli valittu valmiiksi ja työssä pyrittiin selvittämään, tuoko palvelu lisähyötyä käytännössä.

1.2 Tutkimusmenetelmät ja -kysymys

Tässä työssä mobiilihallinnan tarvetta pyrittiin ymmärtämään tarkemmin ja tutkittiin sen hyötyjä. Tutkittavan palvelun yleisiin käytäntöihin perehdyttiin ja osa-alueita esitettiin. Työssä selvitettiin vaatimusten perusteella palvelun sopivuutta. Käytännön osuudessa keskityttiin täyttämään määriteltyjä vaatimuksia. Tutkittavaa asiaa tarkasteltiin havainnoimalla ja testaamalla sen ominaisuuksia.

Työssä käytettiin konstruktiivista tutkimusmenetelmää. Konstruktiivisella menetelmällä pyritään ratkaisemaan tosielämän ongelma konstruktiolla, joka perustuu teoreettiseen tietämykseen. Se sisältää toteuttamisyrityksen ja käytännön soveltuvuuden testaamisen. Menetelmä edellyttää myös läheistä yhteistyötä ja kokemuksellista oppimista. (Lukka n.d.)

Työssä keskitytään ratkaisemaan toimeksiantajan mobiilihallintastrategian kehittämisvaatimukset. Toimeksiantajalle toteutettiin mobiilihallinta, jota testattiin ja analysoitiin sen sopivuutta käytäntöön. Toteutus tehtiin tiimityönä tutkijan ja toimeksiantajan mobiilihallintavastaavien kanssa. Teoreettista tietämystä on haettu palvelun dokumentoinneista ja tutkimusartikkeleista.

Tutkimuskysymyksenä oli: Voidaanko kouluympäristön mobiililaitehallinta toteuttaa AirWatch-palvelun ominaisuuksilla?

1.3 Kirjallisuuskatsaus

Tutkimusaiheeseen oli saatavilla viittaavia ja sivuavia aineistoja. Aiheeseen liittyvää tietoa löytyi eniten artikkeleista eri verkkosivuilta. Opinnäytetöitä aiheeseen liittyen löytyi eri näkökulmista. Hjort (2015) käsitteli työssään ratkaisuja koulun mobiililaitehallinnan tarpeisiin. Kivikäs (2019) toteutti listan, jonka perusteella yrityksen asiakkaille voidaan tarjota sopivinta tuotetta. Karppinen (2019) testasi mobiilihallintaratkaisuja löytääkseen yritykselle sopivan palvelun käyttöön.

Tämän työn käytännön toteutukseen on käytetty pääosin VMwaren omaa dokumentointia palvelusta. Palveluntuottajan aineistot ovat ajan tasalla sekä luotettavia. Työn tutkimuskysymyksen ratkaisuun ei ollut löydettävissä suoraan verrannollisia tutkimuksia. Kuitenkin edellä mainitut opinnäytetyöt tukivat havaintoja mobiilihallinnan hyödyllisyydestä erilaisissa ympäristöissä. Näistä löytyviä havaintoja ja tuloksia voidaan myös käyttää joustavasti käytännössä, eivätkä ole sidottuna tietynlaisiin toimintatapoihin.

Kirjallisuuskatsaukseen työt tulivat valituksi esimerkeiksi, koska ne ovat suhteellisen uusia töitä aiheesta. Mobiilihallinta on alana kasvava ja nopeasti kehittyvä, jolloin lähdemateriaalina kannattaa suosia tuoreita näkökulmia. Näitä opinnäytetöitä voi hyödyntää vertaisarviointiin. Erilaiset käytännön näkemykset antavat tukea myös omalle työlle. Töiden tuloksista voidaan poimia tyypillisiä käytäntöjä, kuten järjestelmien vertailua ja testausta.

2 Mobiililaitehallinnan tekniikat

2.1 Yleistä

Yrityksissä työntekijöiden mobiililaitteiden käyttö on muuttunut viime vuosina. Henkilökohtaisia laitteita tuodaan ja käytetään enemmän työpaikalla, yrityksen turvallisessa verkossa. Tämä tarjoaa joustavuutta työntekijöille sekä lisää tehokkuutta alhaisemmilla laitekustannuksilla. (Everything You Need to Know about Mobile Device Management (MDM) n.d.)

Kivikäs (2019) toteaa opinnäytetyössään, että mobiilihallintajärjestelmien käyttö yritysmaailmassa on monella tasolla järkevää ja kokonaisvaltainen tietoturva paranee. Laitteen tilaa voidaan seurata ja minimoida riski tietojen vuotamisesta etätyhjennyksellä. Kaikkia käytössä olevia laitteita ei välttämättä ole muistettu tai osattu päivittää, joten tietoturvaa voidaan parantaa seuraamalla ja pitämällä laite ajan tasalla IT-osaston toimesta. (Kivikäs 2019, 20.)

Käytön lisääntymisen mukana tulee uusia näkökohtia turvallisuuteen, liitettävyyteen, yksityisyyteen ja hallintaan. Työntekijöillä on myös erilaisia matkapuhelinpalvelujen tarjoajia, ja heidän laitteissaan on monipuolinen käyttöjärjestelmä. BYOD-käytännön riskit ovat johtaneet mobiililaitteiden hallintaohjelmiin, joita IT-osasto käyttää työntekijöiden kannettavien, älypuhelimien, tablet-laitteiden ja muiden laitteiden valvontaan, hallintaan ja suojaamiseen. Turvallisuus- ja tietosuojamurtojen takia MDM-työkaluista on tullut välttämättömiä nykyaikaisella työpaikalla. Yrityksen liikkuvuuden

hallinta on kehittyvä organisaatiotrendi, joka käsittelee laitteiden käytön liiketoiminnallista ja teknologista taustaa jokapäiväisessä liiketoiminnassa. (Everything You Need to Know about Mobile Device Management (MDM) n.d.)

2.2 Mobiililaitteiden hallinta

Mobile device management eli MDM tarkoittaa tekniikkaa, jolla laitteen elinkaarta hallitaan. MDM-palveluita on saatavilla pilvipalveluina sekä paikallisina sovelluksina. MDM:n avulla mobiililaitteet saadaan määriteltyä ja rajoitettua kaikkiin yritys- ja koulutusympäristölle asetettuihin vaatimuksiin. Nämä palvelut käyttävät etähallintaprotokollaa, eli toimenpiteitä voidaan suorittaa laitteeseen internetin yli. Näitä ovat mm. lukitseminen ja tyhjentäminen, sijainnin selvittäminen, salauksen asettaminen sekä sovellusten asentaminen. Nykyään MDM kattaa ison osan käyttötarkoituksista iOS:ssä ja Androidissa. Käyttämällä iOS-ohjattua tilaa tai Android Enterprise -ominaisuuksia voidaan esimerkiksi lukita laitteita kioskikäyttöön, kuten koulutus- ja myyntipistelaitteisiin. (Madden 2019.)

2.3 Mobiilisovellusten hallinta

Mobile application management eli MAM-tekniikoiden avulla suoraan yksittäisiin sovelluksiin voidaan soveltaa tietoturvaa ja asetuksia. Etuna MAM:n hyödyntämisessä on se, että yritykset voivat suojata yritystietojaan tietoturvakäytännöillä, jotka vaikuttavat vain yrityksen jakamiin sovelluksiin. BYOD-tapauksissa käyttäjä pystyy edelleen käyttämään normaalisti omia sovelluksiaan. Tällä tekniikalla voidaan myös esimerkiksi varmistaa, että sovellus on salattu ja sillä on pääsykoodi, pyyhkiä tai poistaa sovellus etäyhteyden avulla tai estää tietojen vuotaminen estämällä mahdollisuus ottaa kuvakaappauksia tai leikata ja liittää. (Madden 2019.)

2.4 Yrityksen liikkuvuuden hallinta

Enterprise mobility management eli EMM yhdistää MDM:n ja MAM:n. EMM-palveluiden tarjoajat pyrkivät vastaamaan kaikkiin yrityksen liikkuvuuden tarpeisiin.

EMM keskittää kaikkien laitteiden hallinnan, kokoonpanon ja turvallisuuden yrityksessä. Viime aikoina pilvipalveluiden nousun myötä EMM-toimittajat ovat alkaneet tarjoamaan myös identiteetinhallintaominaisuuksia ja integroitumaan muihin tuotteisiin. Yritykset voivat nyt toteuttaa ehdollisen pääsyn käytännöt, joissa käyttäjät voivat käyttää sovelluksia vain, jos heidän laitteensa täyttävät asetetut turvallisuusvaatimukset. Kattava EMM-ratkaisu laitehallinnan lisäksi helpottaa pääsyä yrityksen sisältöihin ja yksinkertaistaa tietoturvaa sekä käyttäjän käyttökokemusta. (Madden 2019.)

2.5 Keskitettyjen päätepisteiden hallinta

Unified endpoint management eli UEM-ratkaisut tarjoavat kokonaisvaltaisen ja käyttäjäkeskeisen lähestymistavan kaikkien päätepisteiden hallintaan yhdistämällä työpöytä- ja PC-järjestelmien perinteisen asiakashallinnan nykyaikaiseen yritystoiminnan liikkuvuuden hallintajärjestelmään (EMM). Kattava UEM-ratkaisu antaa järjestelmänvalvojalle mahdollisuuden hallita käyttäjiä ja tarjota yhdenmukaisen kokemuksen kaikissa päätepisteissä, suojata ja hallita laitteen koko elinkaarta ja tehdä kaiken yhdellä, kattavalla alustalla. Nykyään tekniikan taso yhtenäisessä päätepisteiden hallinnassa on käyttää sekoitusta perinteistä hallintaa ja MDM:ää. (Madden 2019.)

2.6 Tuo oma laite

Bring your own device eli BYOD-järjestelmä tarkoittaa sitä, että työntekijä käyttää henkilökohtaista laitettaan työhön. EMM-alustat antavat yritykselle mahdollisuuden toteuttaa BYOD-strategiaa tinkimättä turvallisuudesta tai työntekijöiden yksityisyydestä tarjoamalla laitteelle erilliset työ- ja henkilötiedot. Tämä erottaminen antaa yritykselle mahdollisuuden hallita ja suojata vain yrityksen tietoja työntekijän omistamassa laitteessa. Laitteen tarpeellisuuden loppuessa IT-osasto pystyy poistamaan vain työhön liittyvät tiedot, jolloin käyttäjän henkilökohtaiset tiedot pysyvät tallessa. (Bring your own device (BYOD) n.d.)

3 Käyttöjärjestelmät

Mobiilikäyttöjärjestelmien kilpailu tapahtuu käytännössä Googlen Androidin ja Apple iOS:n välillä. Android on tällä hetkellä suosituin mobiilikäyttöjärjestelmä maailmanlaajuisesti. Maaliskuussa 2020 Androidin markkinaosuus oli 72,26 % mobiililaitekäyttöjärjestelmistä. Applen iOS on toiseksi suosituin mobiilikäyttöjärjestelmä 27,03 %:n markkinaosuudella. (Mobile Operating System Market Share Worldwide n.d.)

Kuten Applen työpöytäkoneiden Mac OS X-käyttöjärjestelmä, iOS pohjautuu samaan Unix-ytimeen. Syyskuussa 2019 iPadeissa olevaa käyttöjärjestelmää alettiin kutsumaan nimellä iPadOS ja sitä päivitettiin hyötymään enemmän isosta näytöstä (Wuerthele 2019). iOS on ensimmäinen mobiilikäyttöjärjestelmä, joka tukee kapasitiivista kosketusnäyttöä ja useamman sormen kosketusta. Se myös ensimmäisenä älypuhelimen käyttöjärjestelmänä piilotti tiedostojärjestelmän käyttäjältä. iOS on noussut suosituksi helppokäyttöisyyden ja selkeyden vuoksi. (iOS n.d.)

Googlen Android on Linux-ytimeen pohjautuva mobiilikäyttöjärjestelmä. Toisin kuin iOS, Android perustuu avoimeen lähdekoodiin. Androidia pidetään suosittuna sen avoimuuden, kustomoitavuuden ja monipuolisten ominaisuuksien ansiosta. Androidia käyttäviä laitteita on saatavilla edullisesti, mikä lisää niiden houkuttelevuutta. (Android n.d.)

Olennainen ero on myös se, että Androidin avoimempi Play Store -sovelluskauppa mahdollistaa sovelluskehittäjille päätäntävallan oman sovelluksensa julkaisusta, hinnoittelusta ja kohdentamisesta (Android n.d.). iOS:n App Store on tiukempien kriteerien valvonnassa. Apple tarkastaa ja hyväksyy kaikki sovellukset sekä pyytää sovelluskehittäjiltä vuosittaista jäsenmaksua. Sovelluskehittäjä määrittää itse sovelluksensa hinnan, ja Apple palauttaa myyntituloista 70 % kehittäjälle. (iOS n.d.)

4 VMware AirWatch -hallintapalvelu

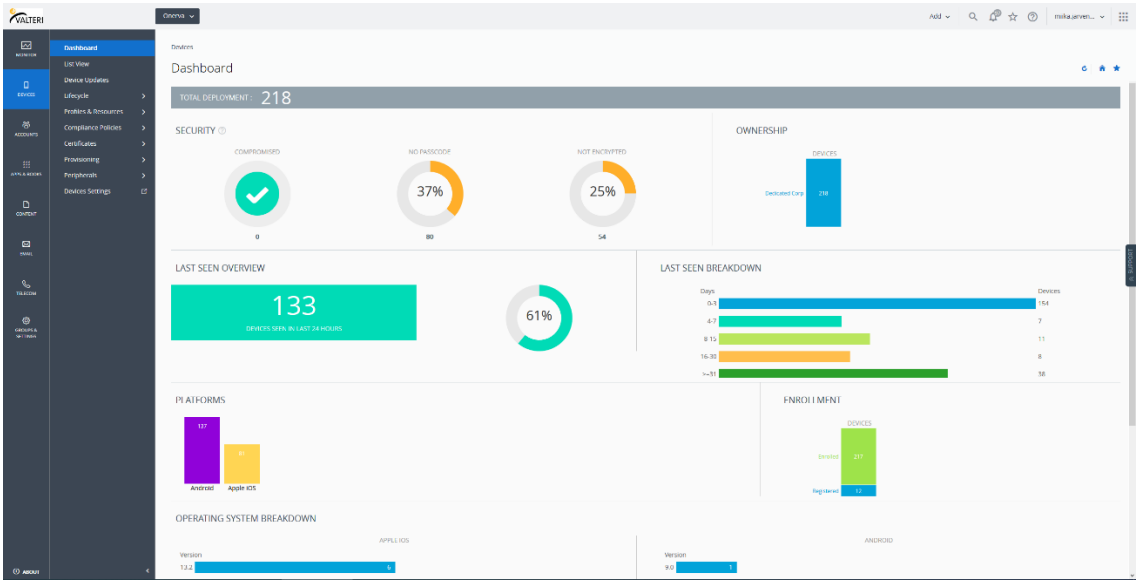
4.1 Yleistä

AirWatch on VMwaren omistama liikkuvuusohjelmistojen toimittaja, jonka teknologioilla yritykset voivat ottaa käyttöön, suojata ja hallita keskitetysti organisaation laitteita sekä tietoja. AirWatchin EMM-tuote on osa VMwaren Workspace ONE -alustaa, jonka tarkoituksena on tarjota käyttäjille keskitetysti hallittava portaali. Se tukee mobiililaitteiden lisäksi Windows 10 ja Mac -tietokoneita. Palvelun asennus voidaan tehdä paikallisesti tai pilvipalveluna ja sitä tarjotaan eri ominaisuuspaketteina. (Rouse n.d.)

AirWatch oli alun perin Wandering WiFi:n MDM-ratkaisu, jonka John Marshall perusti vuonna 2003. Wandering WiFi oli langattoman tietoturvan toimittaja. AirWatchista kasvoi MDM- ja EMM-palveluiden johtaja, jonka VMware osti 1,54 miljardilla dollarilla vuonna 2014. Marshall toimi AirWatchin toimitusjohtajana vuoteen 2016 saakka, jolloin VMware integroi yrityksen täysin. (Mt.)

4.2 Workspace ONE –työtilaympäristö

VMware Workspace ONE on digitaalinen työtilaympäristö (ks. kuvio 1), jonka tavoitteena on toimittaa ja hallita minkä tahansa laitteen sovelluksia. Workspace ONE on rakennettu Workspace ONE UEM -palvelun, entisen AirWatchin, teknologian päälle ja siihen on integroitu VMwaren identiteetin ja pääsynhallinnan ratkaisuja. (What Is Workspace ONE? n.d.)



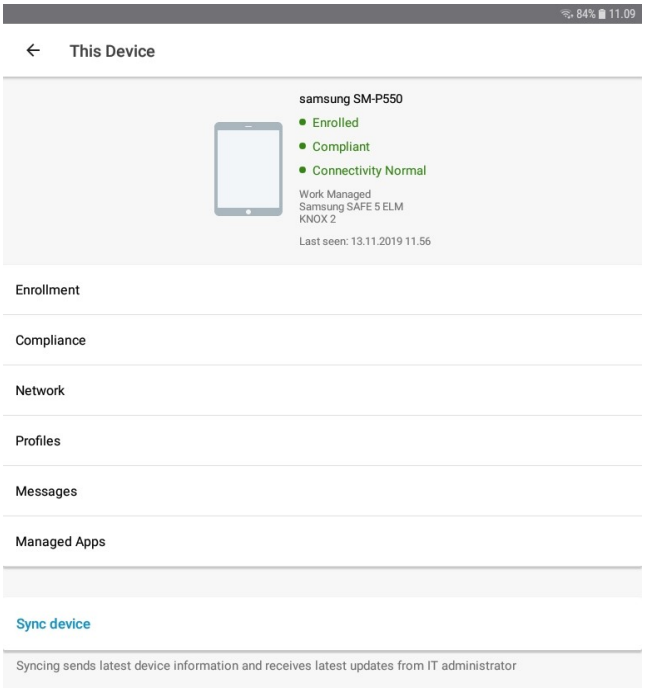
Kuvio 1. Workspace ONE -portaalin Dashboard-välilehti näyttää yleiskatsauksen hallituista laitteista.

4.3 Intelligent Hub -sovellus

Intelligent Hub, entinen AirWatch Agent, on mobiililaitteeseen asentuva sovellus, jonka kautta Workspace ONE käskyttää laitetta. Uudelleenbrändäyksen mukana Intelligent Hub lisää sovelluksen vuorovaikutusta, älykkyyttä ja asiakaskeskeisyyttä. Se tekee muutakin, kuin vain kerää tietoja ja ylläpitää hallintaprofiilia. (Stuart 2019.)

Intelligent Hub tarjoaa pilvipalvelun ylläpitämiä Workspace ONE -sovelluksia Intelligent Hubiin, jotka voidaan lisätä käyttäjille täyden digitaalisen työtilan kokemuksen saamiseksi. Nämä palvelut sisältävät kuluttajakaupasta inspiroidun yrityssovellusluettelon, ihmiset-hakemiston, toiminnalliset ilmoitukset työntekijöille tiedottamiseksi ja mukautetun välilehden selaimen resursseille. (Overview of VMware Workspace ONE Intelligent Hub n.d.)

MDM-rekisteröinnin jälkeen Intelligent Hub näyttää kirjautuneen käyttäjän ja tietoja laitteen tilasta (ks. kuvio 2). Laitteesta voidaan nähdä yhteyden tila hallintaan, asennetut hallintaprofiilit ja avata sovelluskatalogi. Sovelluksessa voidaan myös tehdä unenrollaus eli rekisteröinnin poisto, jos se on sallittu profiileilla.



Kuvio 2. Intelligent Hub -sovelluksen laitenäkymä

4.4 Applen rekisteröintitavat

Device Enrollment Program

Applen Device Enrollment Program -laiterekisteröinti nopeuttaa ja helpottaa laitteiden käyttöönottoa mobiilihallinnassa. DEP-ohjelmalla yrityksien mobiilihallinnan käyttöönotto yksinkertaistuu. Se automatisoi laitteiden MDM-profiilin asentamisen laitteen alkumääritysten aikana sekä lisää laitteet MDM-palvelimelle. Laitteen ei tarvitse käydä fyysisesti järjestelmänvalvojalla, vaan se voidaan antaa suoraan käyttäjän haltuun. DEP-ohjelman käytön edellytyksenä on, että yrityksen tiedot rekisteröidään Applen DEP-ohjelmaan ja se, että laitteet täytyy ostaa suoraan Applelta tai valtuutetuilta jälleenmyyjiltä. (Workspace ONE- \ VMware AirWatch -järjestelmän ja Applelaitteiden rekisteröintiohjelma n.d.)

DEP:n avulla useat organisaatioiden vaatimukset saadaan täytettyä. Käyttäjien ei usein haluta poistavan hallintasovelluksia tai rajoituksia laitteesta. DEP-ohjelma antaa organisaatioiden asentaa laitteisiin kiinteitä hallintaprofiileja, joita käyttäjä ei voi poistaa. Tarpeiden mukaisesti alkuasetuksen määritysvaiheita voidaan ohittaa tai

asettaa pakotetuiksi. DEP helpottaa loppukäyttäjiä automatisoimalla rekisteröinnin jälkeisiä vaiheita. (Mt.)

Apple Configurator

Laitteita voidaan rekisteröidä DEP:iin myös manuaalisesti Apple Configuratorilla, joka on saatavilla Macille. Tällöin ei ole väliä, mistä laite on hankittu, ja laite käyttäytyy niin kuin muutkin rekisteröidyt laitteet. Laitteen manuaalinen rekisteröinti voidaan perua 30 päivän kuluessa, jos laitetta ei ole hankittu valtuutetusti. Laite voidaan aktivoida suoraan käyttöön tai jättää alkuasennukseen käyttäjän käyttöönotettavaksi. Manuaalisen valmistelun vaatimuksena on iOS 11 tai uudempi. (Apple Configurator 2 n.d.)

School Manager

Apple School Manager on kouluille suunnattu verkkopohjainen portaali. Sen avulla Applen mobiililaitteita voidaan ottaa keskitetysti käyttöön ja liittää MDM-palveluun. Järjestelmänvalvojat voivat ostaa ja jakaa sovelluksia MDM-palveluun Applen sovelluskaupasta. School Manager myös integroituu opiskelijatietojärjestelmiin (SIS), SFTP:hen ja Microsoft Azure Active Directory -palvelun nopeuttaakseen tilien luontia. (Mikä on Apple School Manager? n.d.)

4.5 Androidin rekisteröintitavat

4.5.1 Work Managed Device Enrollment

Laitteen omistajan tilassa mobiilihallinta saa oikeuden koko laitteen ohjaukselle. Laite rekisteröidään tehdasasetusten palauttamisen yhteydessä. Tätä tilaa käytetään yleensä yrityksen omistamiin työlaitteisiin hyödyntäen laajempaa käytäntöjen valvontaa. (Work Managed Device Enrollment n.d.)

AirWatch Relay

AirWatch Relay hyödyntää NFC-tekniikkaa ja välittää tietoa yhdestä laitteesta muille laitteille fyysisen kosketuksen kautta. Lapsilaitteiden on oltava tehdasasetustilassa ja

niissä on oltava oletuksena käytössä NFC. Tämä nopeuttaa rekisteröimään suuria määriä laitteita, eikä käyttäjän itse tarvitse suorittaa rekisteröintiä. (Mt.)

AirWatch Identifier

AirWatch Identifier -rekisteröinti yksinkertaistaa liittämisen tunnistetta käyttäen. Määritetty tunniste syötetään laitteen alkuasennuksen aikana, jolloin Intelligent Hubin asennus alkaa. Tämä nopeuttaa suurien laitemäärien asennuksia sekä helpottaa yksittäisen käyttäjän omien laitteiden rekisteröintiä. (Mt.)

QR-koodi

QR-koodin avulla voidaan rekisteröidä niitä laitteita, jotka eivät tue NFC-tekniikkaa. Tehdasasetustilassa olevan laitteen alkuasetuksen aikana luetaan QR-koodi, joka sisältää palvelimen URL-osoitteen ja ryhmätunnuksen tiedot. (Mt.)

Zero Touch

Zero Touch -rekisteröinti lataa automaattisesti Intelligent Hubin ja välittää rekisteröintitiedot palvelimelle alkuasennuksen aikana, kun laite on yhteydessä internetiin. Tätä rekisteröintitapaa tuetaan vain rajoitetulla määrällä matkapuhelinoperaattoreita ja valmistajia sekä vaatii vähintään Android version 8.0. (Mt.)

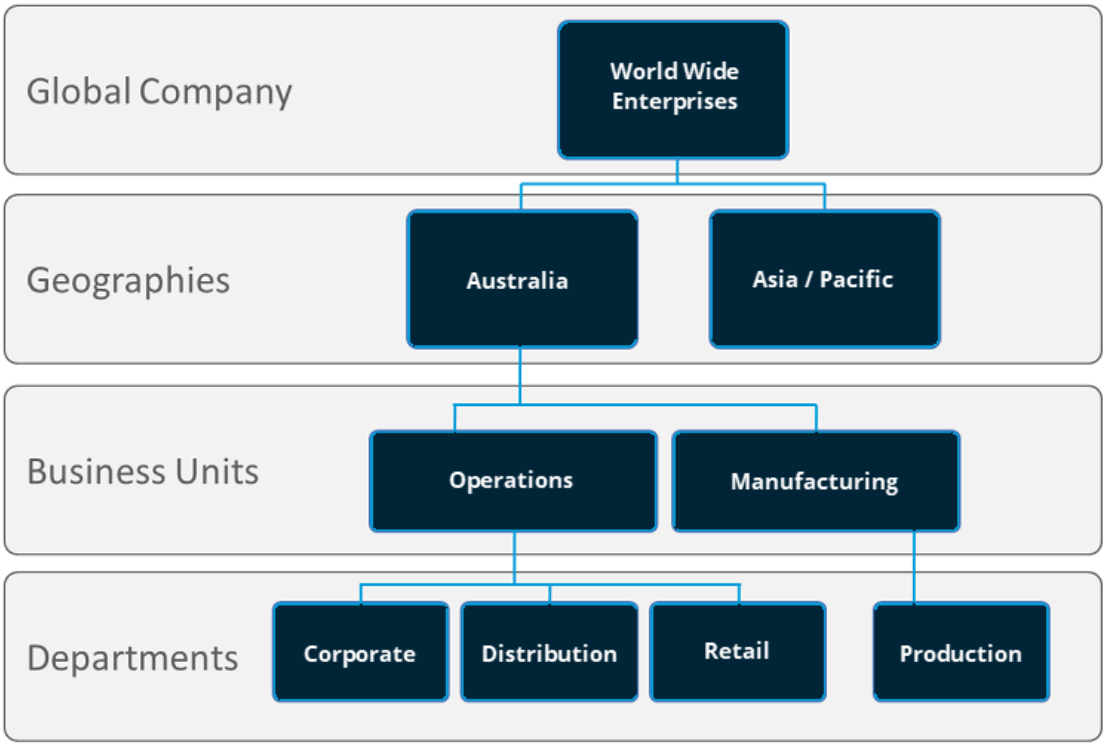
4.5.2 Work Profile Enrollment

Työprofiililla rekisteröityminen luo laitteeseen hallitun työprofiilin, jolla voidaan päästä käyttämään organisaation tietoja ja palveluita. Työprofiili toimii erillään käyttäjän ensisijaisesta profiilista. Organisaatio voi työprofiilin kautta pitää hallinnassa turvallisen pääsyn työsovelluksiin ja tietoihin antaen käyttäjän kuitenkin käyttää henkilökohtaisia sovelluksia ja profiilejaan. (Work profiles n.d.)

Tämä tila sopii BYOD-laitteille, esimerkiksi työntekijän kännyköille, joita käytetään työntekoon. Organisaation on huolehdittava, että henkilökohtaisella laitteella käytettävät työresurssit, kuten sähköpostit ja yhteystiedot, pysyvät tallessa. AirWatchissa rekisteröinti tehdään lataamalla Play-kaupasta Intelligent Hub ja kirjautumalla suoraan siihen käyttäjän tunnuksilla.

4.6 Ryhmät

Organisaatioryhmien avulla voidaan rakentaa yrityksen sisäinen hierarkia tai lajitella laitteet käyttötarkoituksen mukaan (ks. kuvio 3). Lapsiryhmät ovat pääryhmien alle lisättyjä ryhmiä, jotka voivat periä asetuksia pääryhmiltä. (Characteristics of Organization Groups n.d.)



Kuvio 3. Esimerkki organisaation hierarkiasta (Characteristics of Organization Groups n.d.)

Muokattavat älykkäät ryhmät ovat joustavia, joita käytetään käytäntöjen jakeluun. Näiden ryhmien tärkein etu on se, että kerran määritettyjä ryhmiä voidaan käyttää asetuksien ja sisältöjen toimittamisessa helposti uudelleen. Modulaarisuutensa ansiosta niitä voidaan luoda milloin vain. Nämä ryhmät ovat olennainen osa myös sovellusten jakamisessa. Toisin kuin organisaatioryhmillä, älykkäillä ryhmillä edun tai rajoituksen saajat asetetaan yksilöllisemmin. Ryhmän jäsenet voidaan lisätä esimerkiksi omistajuuden, käyttäjäryhmän, käyttöjärjestelmän, mallin tai laitetunnisteen mukaan. Tietty ryhmä voidaan jättää myös käytäntöjen määrittämisen ulkopuolelle. (Smart Groups n.d.)

5 Käyttöönotto

5.1 Yleistä

Tässä työssä toteutettiin AirWatchin käyttöönotto Valterin Jyväskylän toimipisteelle, Onervalle. Palvelu oli valittu jo aikaisemmin sekä otettu käyttöön myös toisella toimipisteellä. Laitteet lisättiin palveluun koulun kesäloman aikaan, jolloin opetus ei häiriintynyt. Palvelun konfigurointi toteutettiin vaatimuksia tavoitellen. Käyttöönoton jälkeen pohdittiin, kuinka hyvin palvelu toteuttaa odotukset ja mitä hyötyjä sillä on.

Palvelulta odotettiin seuraavia toimintoja:

1. Molemmat käytössä olevat käyttöjärjestelmät tuettuja palvelussa
2. Sovellusten keskitetty hyväksyminen ja jakaminen
3. Maksullisten sovelluslisenssien keskitetty hankinta ja omistajuuden vaihtaminen
4. Oppilaan hallittu Google-tili tulee toimia
5. Oppilaiden Play-kaupan vapaan pääsyn rajoittaminen
6. Toimenpiteet hukattujen tai varastettujen laitteiden varalta
7. Pilvipalvelujen käytön rajoittaminen
8. Kovennettu näyttölukitus henkilökunnalle

Työn toteutuksessa käytettiin toimipisteellä olevia mobiililaitteita. Oppilailla oli käytössä pääosin Samsung Tab A -tabletteja ja henkilökunnalla myös lisäksi Applen iPadeja. Tableteissa oli uusin niihin saatavana oleva Android-versio. Ennen Samsung-tablettien lisäämistä ne piti poistaa edellisestä Samsungin MDM-palvelusta. iPadien käyttöjärjestelmät päivitettiin laitteiden valmistelun yhteydessä MacBookilla.

Projekti aloitettiin käymällä läpi molempien käyttöjärjestelmien käyttöönottoprosessia. Testejä tehtiin ja varmistettiin, että testilaitteet saadaan onnistuneesti hallintaan ennen kaikkien laitteiden vastaanottoa. Henkilökunnan käytössä olleista laitteista suurin osa pyrittiin ottamaan käyttöön hyvissä ajoin ennen suurinta palautusaaltoa. Tämä myös siksi, että voitiin vielä varmistaa palvelun käytännön toimivuus.

Käyttäjiä ohjeistettiin ottamaan laitteilta tärkeät tiedot talteen, että nollaukset voitiin tehdä nopeasti ilman varmuuskopioita. Kuitenkin joihinkin laitteisiin varmuuskopiointi täytyi tehdä suuren sovellusmäärän takia tai sen muuten todettiin olevan helpoin ratkaisu. Varmuuskopioitavia laitteita olivat iPadit.

Laitteiden suora varmuuskopiointi lisättyyn laitteeseen palautti sen takaisin tilaan ennen palveluun lisäystä. Palautus toteutettiin ylimääräisen tyhjän laitteen kautta, joka oli jo lisätty DEP:iin. Käyttäjän laitteessa tehtiin varmuuskopio iCloudiin, joka palautettiin tyhjään laitteeseen. Uudessa laitteessa tehtiin uusi varmuuskopio, joka palautettiin takaisin käyttäjän laitteeseen. Tästä syystä varmuuskopiointi vei enemmän aikaa sekä vaati käyttäjältä salasanan syöttämistä useamman kerran.

Käyttäjältä toimenpiteet vaativat sen, että laitteesta tarkistettiin tärkeät tiedot, sovellukset ja tilien toimivuus. Laitteen käyttöönottoon jätön yhteydessä varmistettiin, että iPadeista ”Etsi iPadini” –toiminto oli pois päältä. Tämä asetus ei anna tehdä laitteen käyttöönottoa ilman käyttäjän Apple-tilin salasanaa. Samalla myös otettiin pääsykoodi pois päältä. Tämän jälkeen laitteet voitiin lisätä palveluun, eikä käyttäjältä tarvittu muita toimia käyttöönoton aikana. Kun laite palautettiin käyttäjälle, lisättiin pääsykoodi, tarvittavat tilit ja varmistettiin katalogin toiminta.

Haasteina käyttöönotossa oli varmuuskopioinnin toiminnan selvittäminen, Androidin edellisen hallintasovelluksen ongelmat ja palvelun sopivien asetuksien löytäminen niin, että opiskelu voitiin aloittaa syksyllä ilman ongelmia. Ongelmat havaittiin, kun käyttöönotto aloitettiin. Näihin ei varauduttu etukäteen, koska testauksessa niitä ei tullut vastaan. Vanhempien iPadien käyttöönotto hidastui hiukan, koska niitä ei voitu suoraan itse liittää DEP:iin. Myöhemmin myös ilmeni, ettei Play-kaupan rajoittaminen toiminut odotetulla tavalla. Koska kaikki laitteet kävivät samassa paikassa, tehtiin niistä lisäksi inventaario ja laitelistaa päivitettiin.

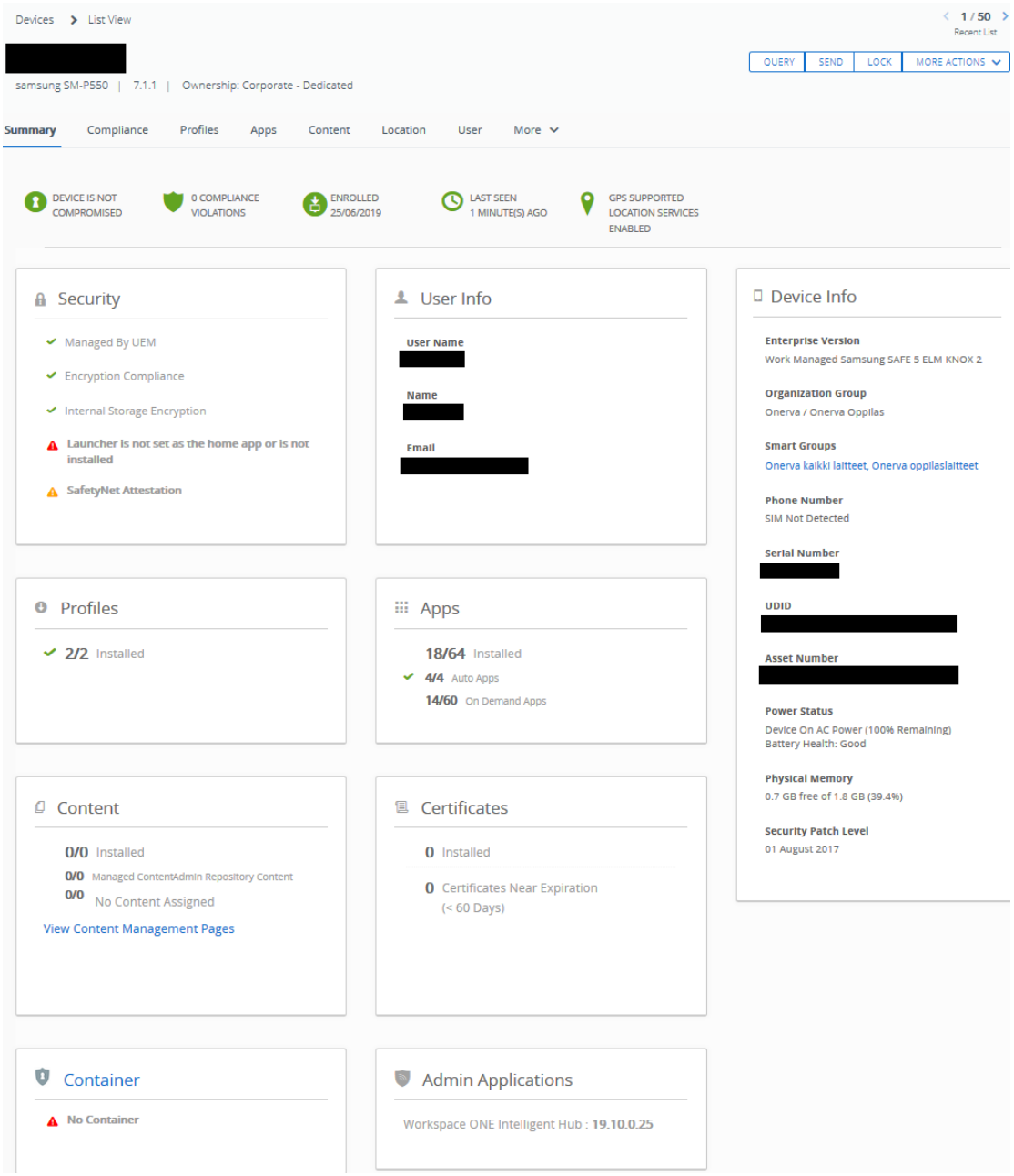
Käyttöönotto saatiin haasteista huolimatta suoritettua hyvin ja aikataulussa pysyttiin. Ongelmien ratkaisemisen ohella aikaa kului suuren laitemäärän lisäämiseen. Suunnitelmat projektissa olivat selkeät ja konfigurointi onnistuttiin tekemään niin, että syk-

syllä laitteet saatiin takaisin käyttöön. Käytännössä palvelusta oli hyötyä organisaation hallinnolle, sekä käyttäjille. Sovellusten hankinta siirtyi pois käyttäjien vastuulta ja hallinto pystyy paremmin hallitsemaan suurta laitemäärää.

5.2 Laitteiden liittäminen palveluun

Android-laitteiden käyttöönotto

Valterin Android-laitteissa käytettiin Work Managed Device -tilaa, koska haluttiin täysi hallinta laitteisiin. Asennukset tehtiin käyttämällä QR-koodia. Tehdasasetusten palautuksen jälkeen, ennen laitteen alkuasetuksia, tabletin näyttöä painellaan 7 kertaa, joka tuo esiin QR-koodinlukijan. Kun koodi luetaan, laite lataa ja asentaa Intelligent Hubin. Sovellus vaatii seuraavaksi laitteen levytilan salaamista. Tämän jälkeen päästään syöttämään käyttäjän kirjautumistiedot ja laite on valmis käytettäväksi. QR-koodiin ei lisätty kirjautumistietoja, koska jokaiselle henkilölle luotiin oma käyttäjätunnus. Workspacesta nähdään tietoja laitteesta lisäyksen jälkeen (ks. kuvio 4).

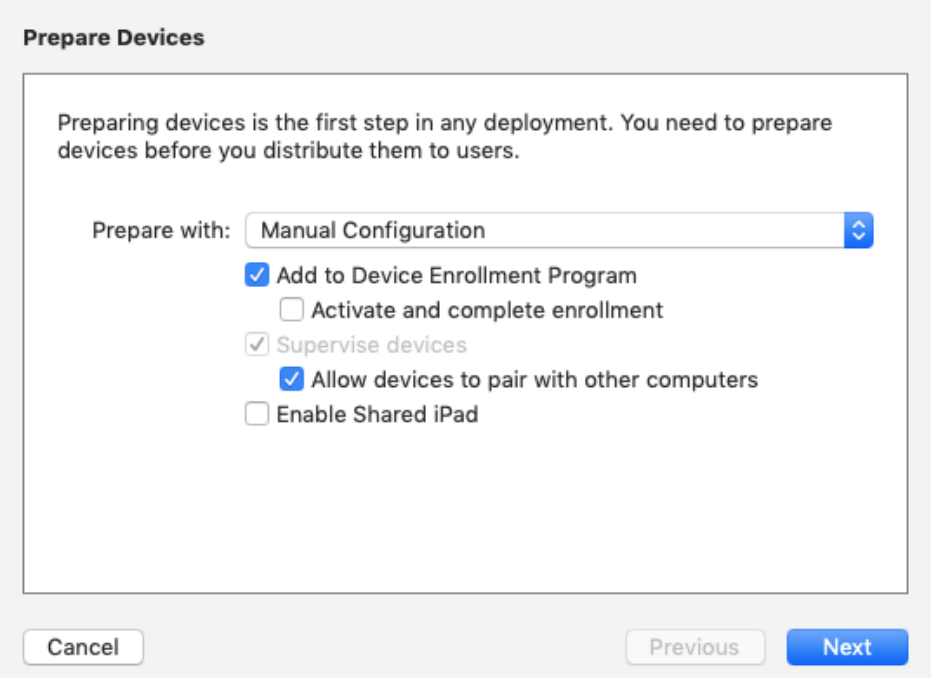


Kuvio 4. Laitenäkymä Samsung tabletista Workspacessa

Samsung-tabletit olivat Samsung SDS IAM & EMM -palvelussa hallittavana ennen AirWatchin käyttöönottoa. Laitteiden poistamisessa ilmeni yhteysongelmia ja edellisen hallintasovelluksen jumittumista. Osa laitteista oli sovelluksen toimimattomuuden vuoksi niin lukossa, ettei niihin voinut puskea päivitettyjä oikeuksia tehdasasetusten palautusta varten. Nämä saatiin kuitenkin tyhjäksi salaamalla laite ja antamalla käynnistyksen yhteydessä väärää pääsykoodia tarpeeksi monta kertaa, jolloin laite tyhjentää itsensä. Yhteysongelmia lukuun ottamatta laitteiden lisääminen palveluun oli yksinkertaista.

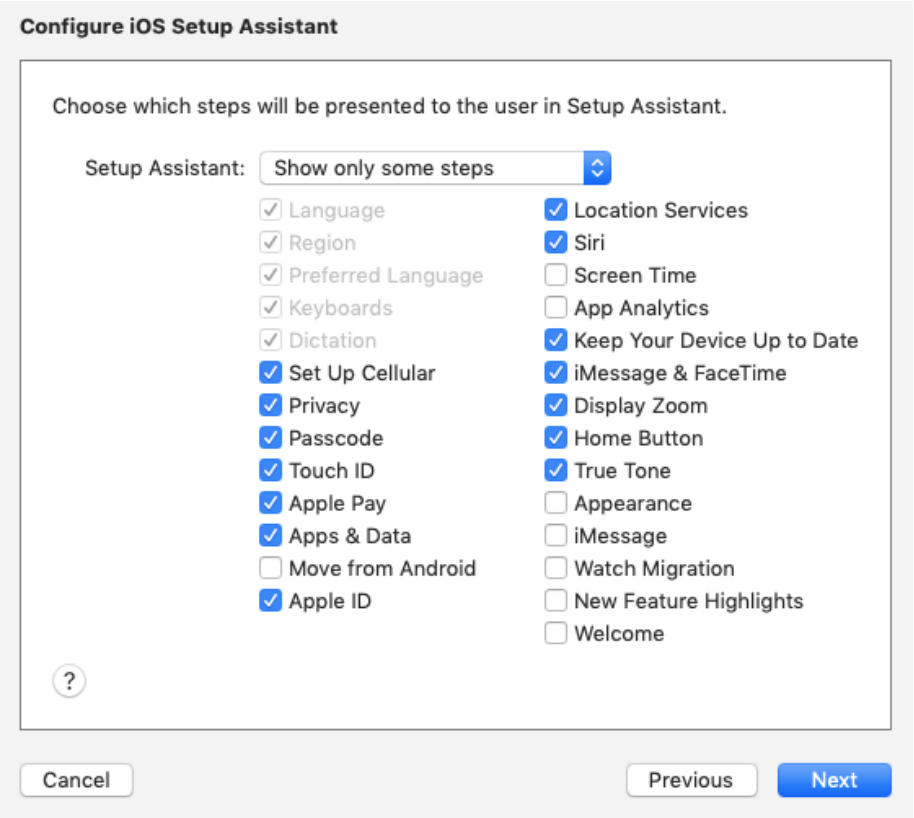
iOS-laitteiden käyttöönotto

Suurin osa iPadeista voitiin lisätä Applen DEP-ohjelmaan manuaalisesti Apple Configuratorilla. Tässä lisätään laitteelle myös organisaatio ja WiFi-profiili. Laitteen valmistelun asetuksista valittuna on DEP-ohjelmaan lisääminen, mutta laitteen rekisteröintiä ei tehdä samalla loppuun (ks. kuvio 5).



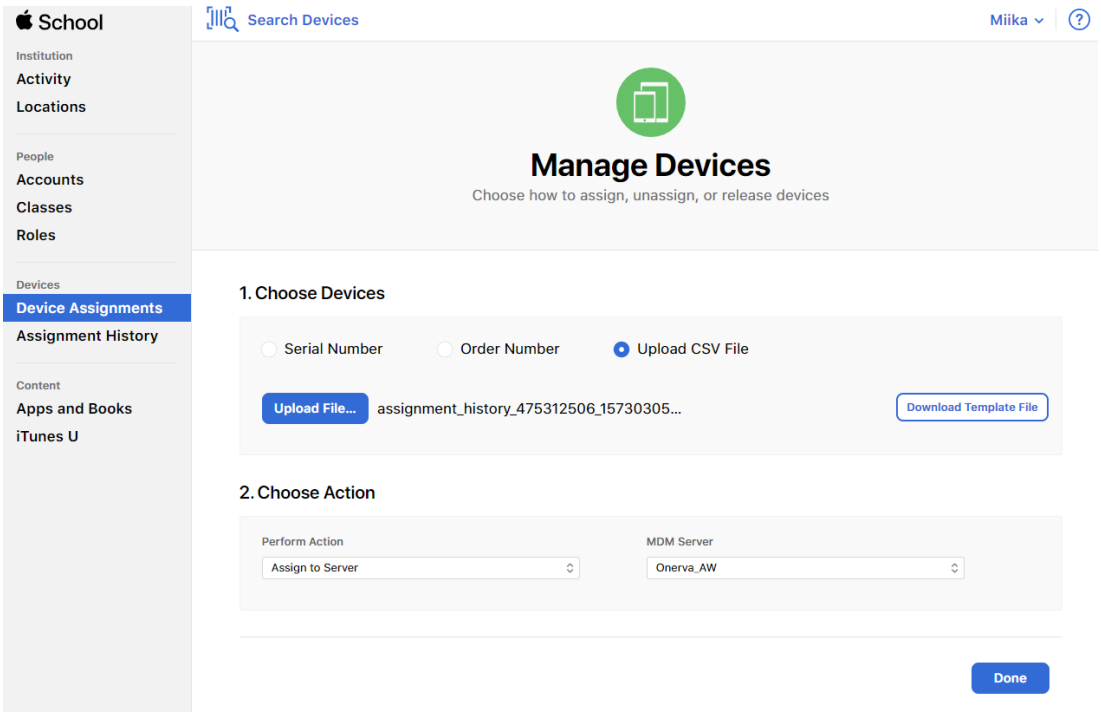
Kuvio 5. Laitteen valmistelu Apple Configuratorilla

Laitteet valmisteltiin käyttäjälle valmiiksi asti, joten asennus voidaan tehdä ajan säästämiseksi pienimmällä määrällä vaiheita (ks. kuvio 6). Tärkeitä oli kuitenkin pitää päällä Apple ID ja Apps & Data, sillä joihinkin laitteisiin palautettiin varmuuskopioita.



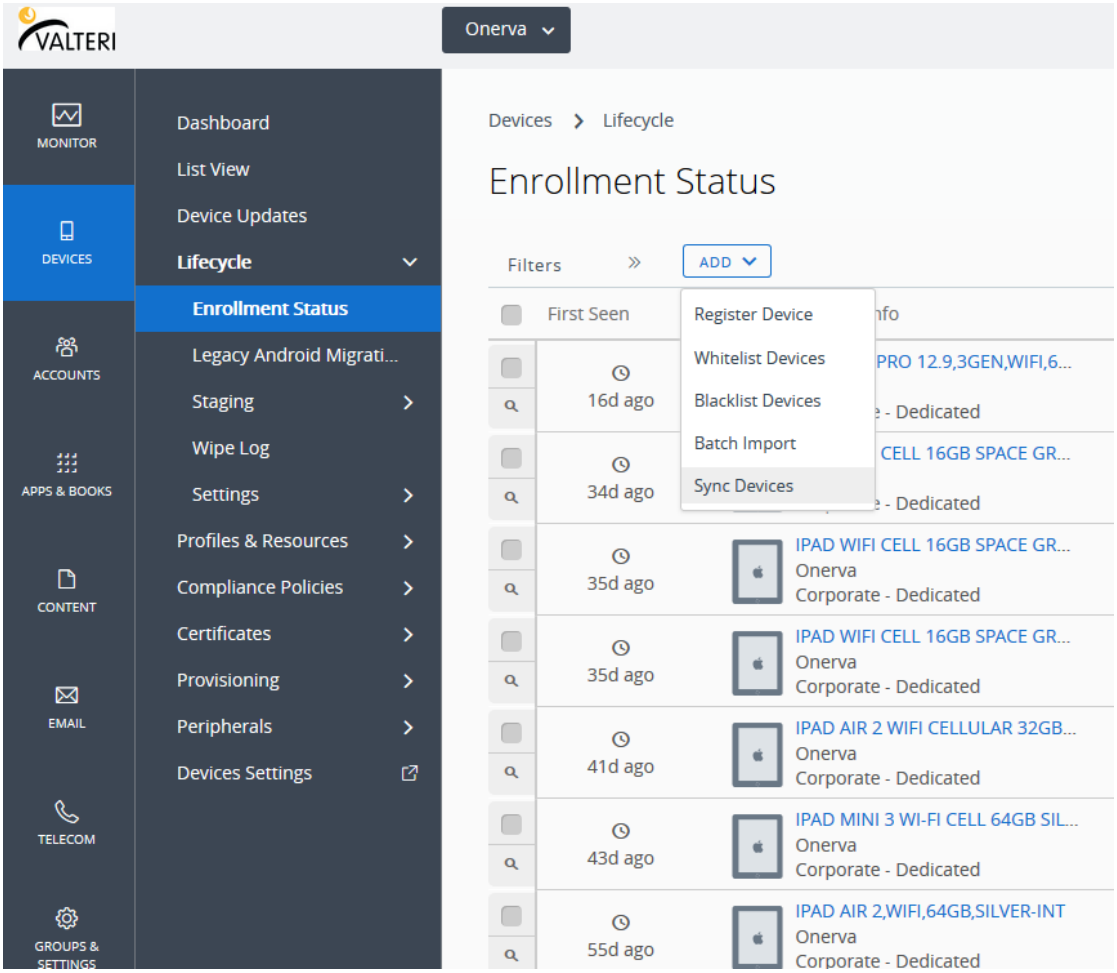
Kuvio 6. Setup Assistant -asetukset

DEP:iin liitetty laite tai lisäystapahtuma tulee näkyviin School Manageriin. Laitteiden hallinta -näkymästä voidaan lisätä laitteita MDM-palvelimelle sekä poistaa tai luovuttaa niitä (ks. kuvio 7). Kun laite luovutetaan, se on kokonaan irti hallinnasta ja voidaan ottaa käyttöön toiseen DEP:iin.



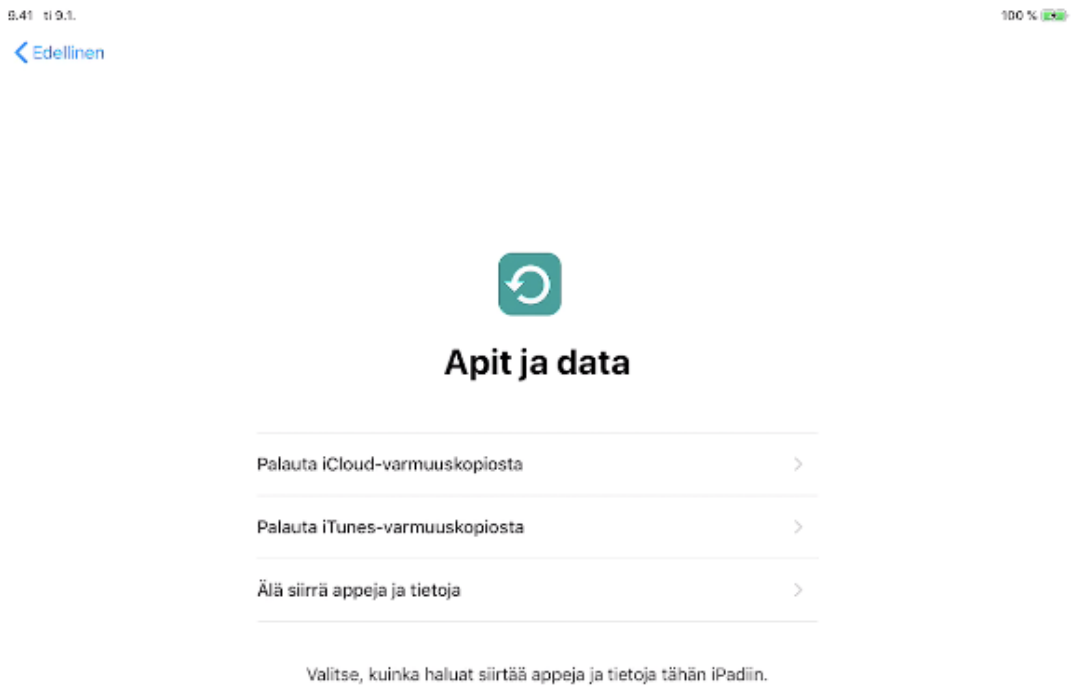
Kuvio 7. Laitteen lisääminen MDM-palvelimelle School Managerissa

Seuraavaksi Workspacesta synkronoidaan laitelista DEP:stä, ja laitteet ilmestyvät Workspacen Lifecycle-sivulle (ks. kuvio 8). Nyt voidaan aloittaa laitteen alkuasennus.



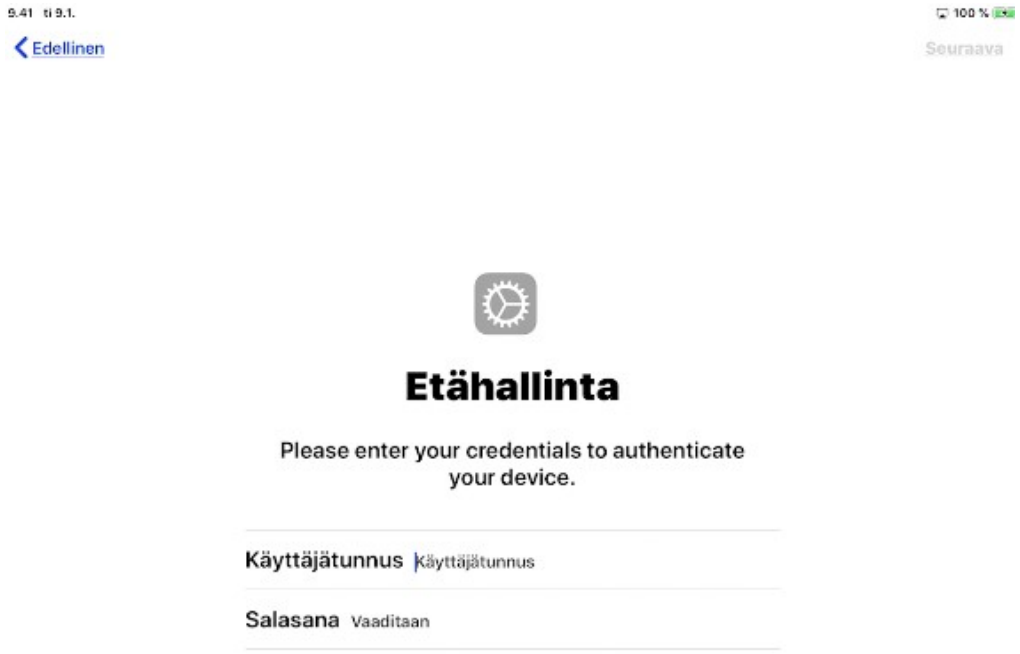
Kuvio 8. Laitteiden hakeminen DEP:stä

Varmuuskopioinnilla saadaan palautettua laitteessa olleet sovellukset, kansiot ja tiedot. Muutamaan laitteeseen todettiin helpommaksi tavaksi suorittaa varmuuskopion palautus kuin, että kaikki sovellukset olisi jouduttu lataamaan uudelleen. Tästä oli apua myös samanlaisten yhteiskäytössä olevien laitteiden käyttöönotossa, joissa oli paljon opetussovelluksia. Näihin kaikkiin voitiin palauttaa kerran tehty varmuuskopio samalla iCloud-tunnuksella. Prosessissa käytettiin yhtä vapaata DEP:iin lisättyä laitetta DEP-aktivoidun varmuuskopion luonnissa. Varmuuskopion palautus laitteelle tehdään alkuasetusten yhteydessä (ks. kuvio 9).



Kuvio 9. iPadien varmuuskopion palautus

Laitteen alkuasennuksen aikana vaaditaan kirjautumista hallintaan (ks. kuvio 10). Tässä vaiheessa kirjaudutaan sisälle Workspaceen luodun käyttäjän tiedoilla. Kirjautumaan pääsevät vain ne käyttäjät, jotka kuuluvat liitettyyn DEP-ohjelman organisaatioon. Katoamistapauksissa laitetta ei voida ottaa uudelleen käyttöön jonkun muun toimesta, vaikka se saataisiin tyhjennettyä.

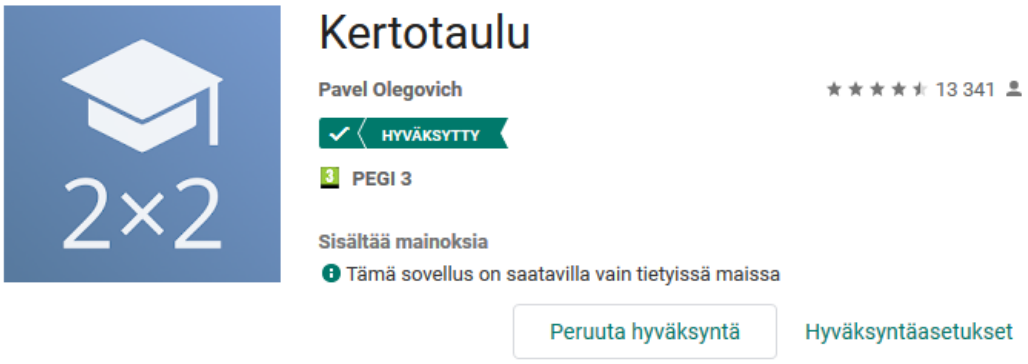


Kuvio 10. Kirjautuminen AirWatchiin käyttäjän tunnuksilla

Osa laitteista oli sen verran vanhoja, ettei niiden käyttöjärjestelmäversio riittänyt manuaaliseen DEP:iin lisäämiseen. Nämä laitteet saatiin liitettyä jälleenmyyjien toimesta.

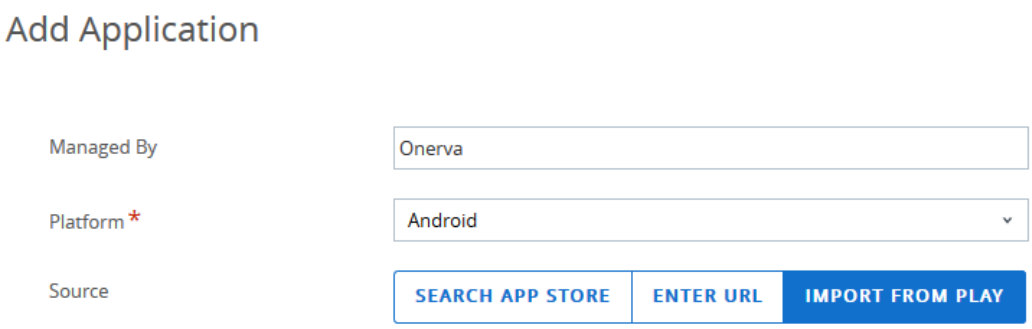
5.3 Sovellusten jakaminen

Haluttiin, että oppilaiden sovelluslatauksia voidaan rajoittaa ja hyväksyä vain opiskeluun käytettäviä sovelluksia. Organisaation sovelluksia hyväksytään hallitun Play-kaupan kautta (ks. kuvio 11). Applen sovellukset haetaan vastaavasti School Managerin kautta.



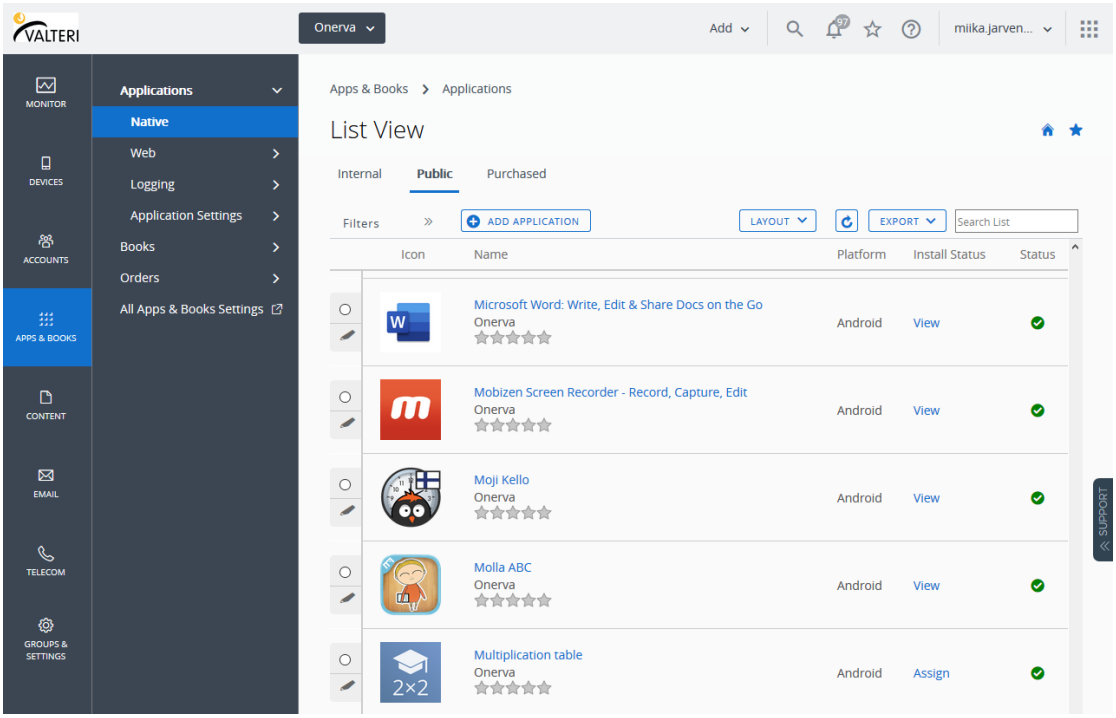
Kuvio 11. Sovellus on hyväksytty hallitusta Play-kaupasta

Sovelluksia voidaan tuoda Lisää sovellus -ruudusta joko nopeasti hakemalla se suoraan integroidusta kaupasta, URL-osoitteella tai tuomalla kaikki hyväksytyt sovellukset kerralla hallitusta Play-kaupasta (ks. kuvio 12).



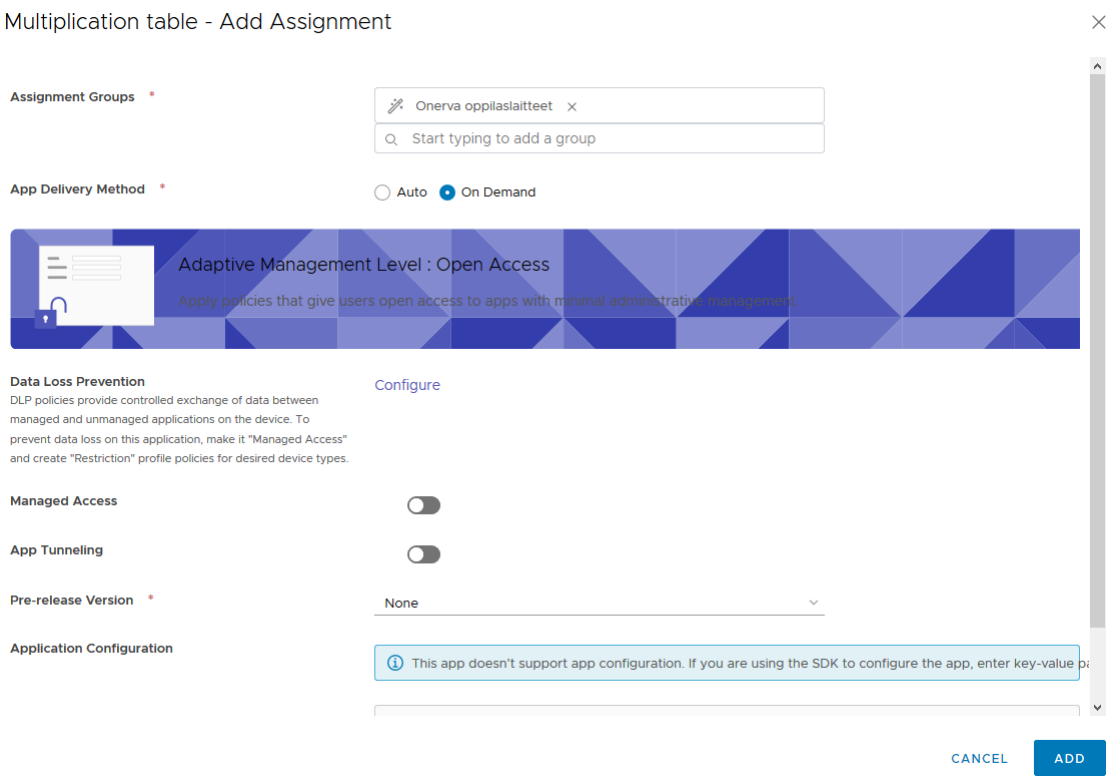
Kuvio 12. Sovelluksen tuominen Workspaceen

Sovellukset välilehdeltä päästään hallitsemaan ja lisäämään sovelluksia. Tänne voidaan tuoda omia APK-paketteja, julkisia sekä ostettuja sovelluksia. Applen kaupasta haetut ilmaiset sekä maksulliset sovellukset tulevat näkyviin Ostetut-välilehdelle, koska ne varataan lisensseillä. Nyt esimerkiksi Kertotaulu-sovellus on tuotu sovelluslistaan, josta voidaan nähdä sovelluksen tila, muokata sen tietoja ja lisätä katalogiin ladattavaksi (ks. kuvio 13).



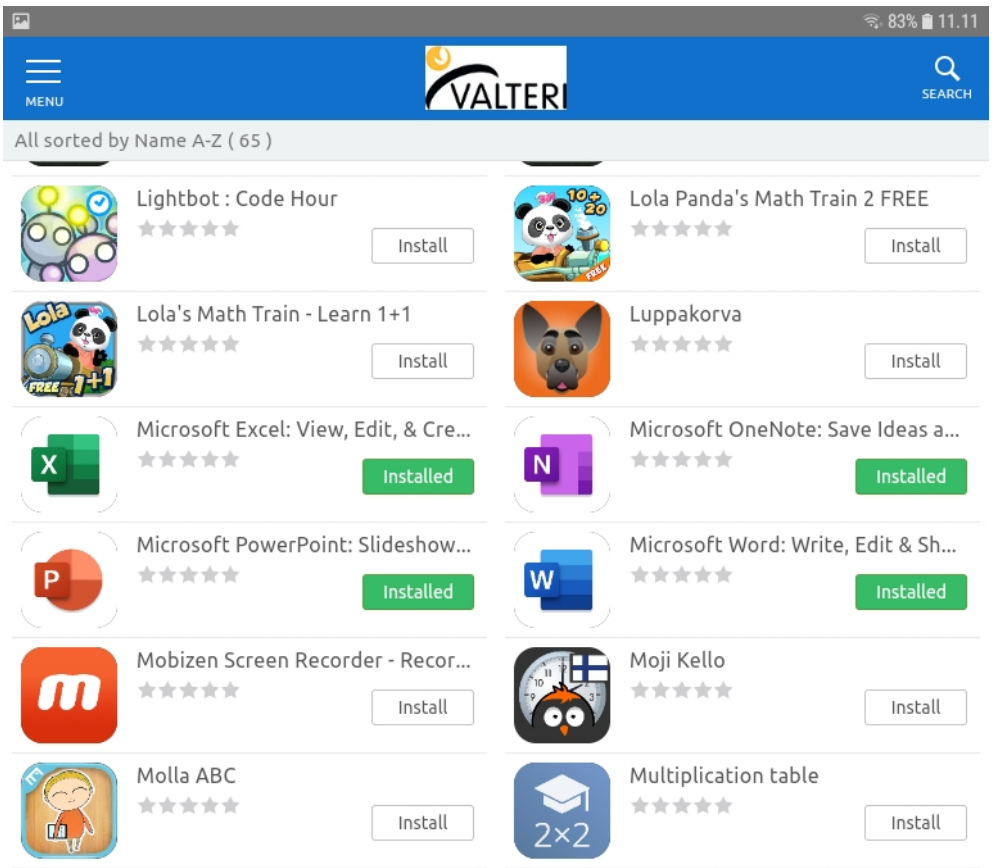
Kuvio 13. Sovelluslista Workspacessa

Kertotaulu-sovellus on lisättynä listaan, mutta sitä ei ole määritetty vielä käyttäjälle. Määrittäminen tapahtuu valitsemalla haluttu ryhmä. Esimerkkinä Kertotaulu-sovelluksen ryhmäksi on valittu oppilaslaitteet, jolloin kaikki oppilaat saavat sovelluksen. Sovellus joko ladataan itse tai se latautuu automaattisesti riippuen siitä, pakotetaanko sen asennus (ks. kuvio 14).



Kuvio 14. Sovelluksen jakamisen asetukset

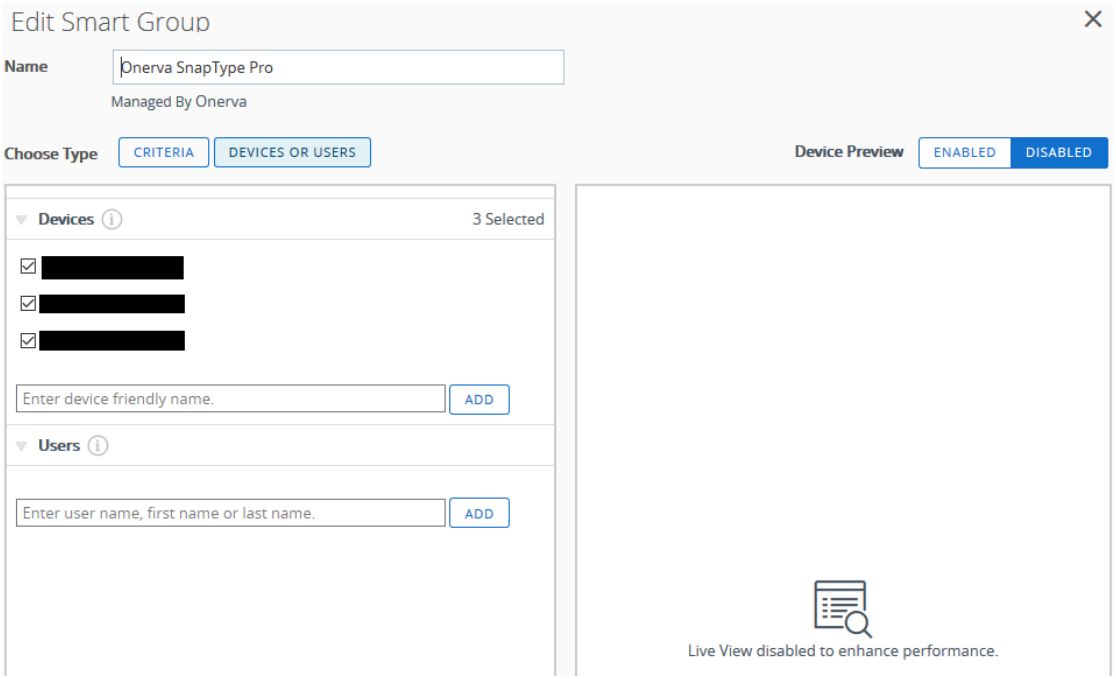
Sovelluksen saajien määrittelyn jälkeen sovellus tulee näkyville katalogiin, jos kyseinen laite tai käyttäjä sisältyy lisättyyn ryhmään (ks. kuvio 15). Katalogiin voidaan lisätä myös sovellusryhmiä, joilla ne voidaan jaotella loogisesti, jolloin suurien sovellusmäärien selaaminen helpottuu. Katalogi tarjoaa myös hakutoiminnon.



Kuvio 15. Jaetut sovellukset ovat ladattavissa katalogista

5.4 Maksulliset sovellukset

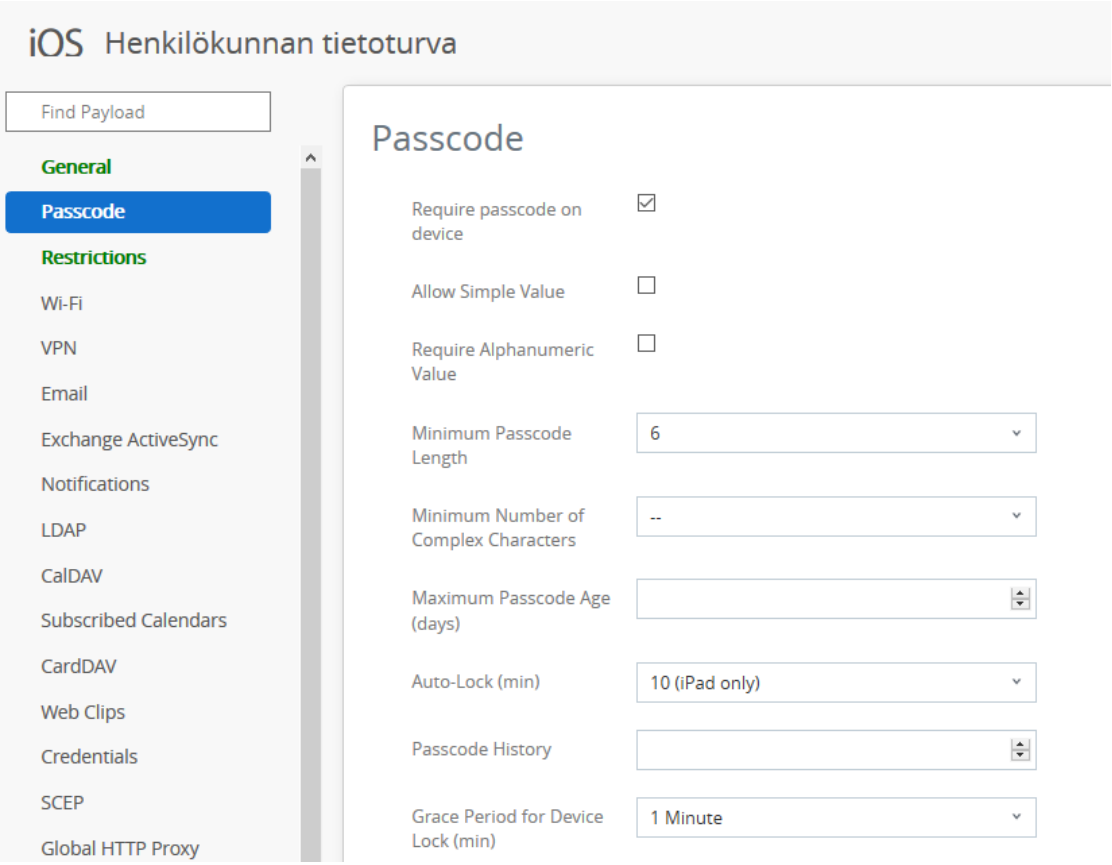
Koululla on käytössä maksullisia opetussovelluksia, joiden ei haluta jäävän henkilökohtaiselle tilille. Keskitetty jakaminen myös helpottaa sovellusten hallitsemista. Maksullisten sovelluslisenssien hakeminen Applen ympäristössä tapahtuu School Managerista samalla tavalla kuin ilmaissovellusten lisääminen. Sovelluksia varten luodaan ryhmä, johon kuuluvat halutut käyttäjät tai laitteet (ks. kuvio 16). Jos käyttäjä ei enää tarvitse kyseistä sovellusta, voidaan käyttäjä vain poistaa ryhmästä ja lisenssi vapautuu uudelleen jaettavaksi. Googlen puolelta vastaavaa maksullisten sovellusten keskitettyä hallintaa ei ole saatavilla.



Kuvio 16. Smart groupin luonti sovellusta varten

5.5 Henkilökunnan pääsykoodit

Henkilökunnan laitteilla voi olla salassa pidettävää tietoa. Laitteita voidaan myös ottaa kotiin tai työmatkalle, joten pääsykoodin vaatiminen on tärkeää. Pääsykoodi asetettiin pakolliseksi ja sen tuli sisältää vähintään kuusi merkkiä. Allow Simple Value -asetuksen pois jättäminen ei salli käyttäjää asettamaan liian monta samaa tai peräkkäistä merkkiä. Pääsykoodin vaihtoaika voidaan tästä myös asettaa, mutta sitä ei pidetty tarpeellisena (ks. kuvio 17).



Kuvio 17. Laitteen pääsykoodin asetukset

5.6 Rajoitukset

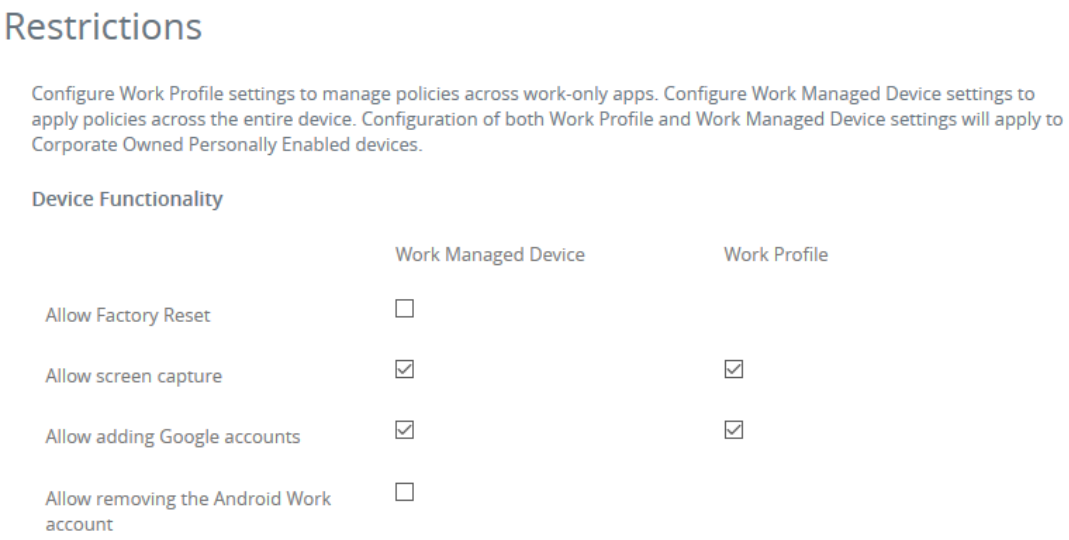
iOS

iOS:llä testattiin pilvipalvelujen estämistä ja se todettiin toimivaksi. Laitteilta voitiin poistaa iCloudiin kirjautuminen, joka esti kokonaan palvelun käytön. iCloudin käytön estoja voitiin määrittää myös tarkemmin, kuten erikseen varmuuskopiointi, tallennustilan käyttö tai kuvien synkronointi. iCloudin käyttöä rajoitettiin yhteiskäytössä olevilta laitteilta.

Android

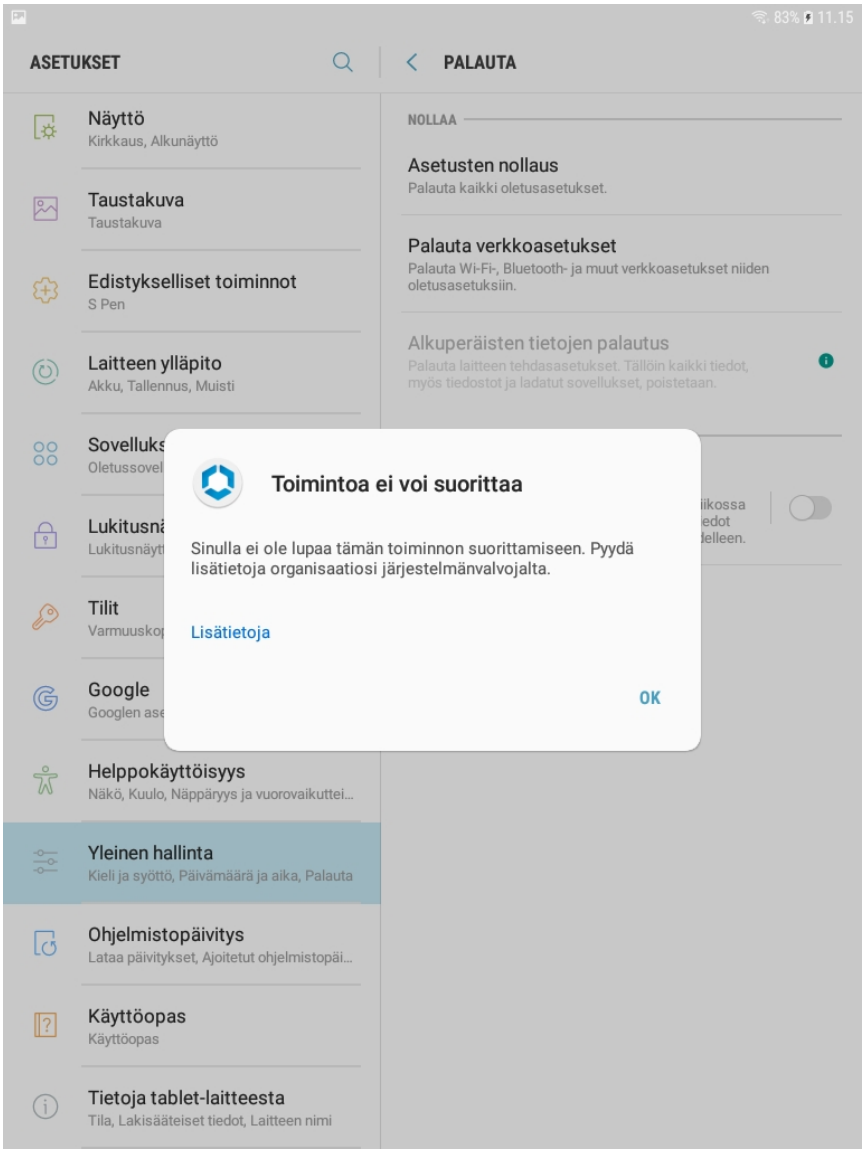
Turvallisuutta lisättiin estämällä sovellusten asentamisen muualta kuin Play-kaupasta, jolloin epävirallisia APK-tiedostoja ei voida asentaa. APK-tiedostojen alkuperästä ei voi olla varma ja ne saattavat sisältää haittaohjelmia. Lisäksi estettiin USB-vianetsintä ja fyysisen massamuistin kiinnittäminen.

Opiskelun kannalta oli tärkeää, että oppilaat saivat lisätä laitteille hallitut Google-tilit Classroomin käyttöä varten. Laitteilta on estetty tehdasasetusten palautus, ettei laite voi päästä katoamaan hallinnasta. Android Work -käyttäjän täytyy myös pysyä laitteessa, ettei hallintaa päästä ohittamaan (ks. kuvio 18).



Kuvio 18. Android-laitteiden rajoitukset

Applen laitteet ovat lisättynä DEP:iin, joten vaikka laite saataisiin nollattua, sitä ei voi ottaa uudelleen käyttöön ilman Workspacen käyttäjän tunnuksia tai poistamatta sitä DEP:stä. Androideilla taas laitteen nollaus poistaa hallintasovelluksen ja katkaisee yhteyden verkkoportaaliin, jolloin laite on niin sanotusti vapaa. Nollauksen esto on tärkeää varsinkin Android-laitteita ajatellen (ks. kuvio 19).



Kuvio 19. Laitteen nollaus ei onnistu laitteen asetuksista

5.7 Play-kaupan rajoittaminen

Toivottiin, että oppilailta saadaan rajoitettua Play-kaupan vapaata käyttöä, mutta tämä ominaisuus ei toiminut odotetulla tavalla Androideilla. Play-kaupan estäminen ja sovellusten jakaminen Workspace ONE:n katalogin kautta ei onnistunut. iOS:llä sovellukset saadaan ladattua katalogista, vaikka App Store olisi kokonaan piilotettuna. Kun Play-kauppa estettiin, sovelluksen lataus ei alkanut, vaikka katalogi näytti, että sovellus olisi asennettu. Laitteen työprofiililla Play-kauppaan ei olisi päässyt ja sovellukset sai ladattua katalogin kautta, mutta oppilaat tarvitsivat omia hallittuja Google-tilejä opiskeluun, joten niiden lisääminen täytyi sallia.

5.8 Laitteen tyhjennys ja lukitus etänä

Salassa pidettävää tietoa ei toivota leviävän ulkopuolisille. Mahdollisia katoamis- tai varkaustapauksia varten on hyvä olla toimenpiteitä, joilla voidaan estää väärinkäyttötilanteet. Tietoturvaa lisätään mahdollistamalla joko laitteen lukitusta tai sen tyhjennystä. Lukitusta olisi hyvä käyttää ensin kadonneille laitteille, joista tiedetään, ettei niitä ole varastettu. Laitteen lukituksen pystyy poistamaan vain Workspacen kautta. Jos laitetta ei syystä tai toisesta löydetä, tai se on varastettu, voidaan se tyhjentää. Tyhjentämällä saadaan pelastettua ainakin mahdollisesti salaisten tietojen vuotamista

6 Tulokset

6.1 Vaatimusten täyttyminen

Melkein kaikki vaatimukset saatiin täytettyä. Ainoastaan Androidin Play-kaupan rajoittaminen ei onnistunut koulun käyttötapauksessa. Tämä ei kuitenkaan ollut kohtalokasta palvelun kannattavuuden kannalta. Muut vaatimukset saatiin täytettyä vaivattomasti ja toimivuus todettiin hyväksi. Sovellusten hankkiminen saatiin pois käyttäjien vastuulta ja vältettiin ylimääräisten lisenssien ostaminen. Turvallisuutta saatiin myös parannettua ja toimenpiteitä voidaan tehdä tarvittaessa, jotta voidaan estää mahdollisia tietovuotoja. Palvelusta havaittiin olevan lisähyötyä koululle ja myös jatkossa voidaan ottaa käyttöön lisätoimintoja.

1. Molemmat käytössä olevat käyttöjärjestelmät tuettuja palvelussa
Haluttiin yksi palvelu, joka tukee kumpaakin käytössä olevaa käyttöjärjestelmää. Androideissa oli käytössä versio 7.1.1 lukuun ottamatta muutamaa poikkeusta ja iOS-laitteita oli versiosta 10 aina uusimpaan asti. Palvelu tuki kaikkia laitteita, mutta versionumerolla oli vaikutusta tuettaviin rajoituksiin. Tarvittavat rajoitukset saatiin tehtyä laitteille.

2. Sovellusten keskitetty hyväksyminen ja jakaminen

Sovellukset saatiin hyväksyttyä hallittujen kauppojen kautta, Androidilla Google Play-kaupassa ja iOS:llä School Managerissa. Hyväksyttyjä sovelluksia voitiin hyväksymisen jälkeen jakaa halutuille käyttäjille tai laitteille katalogin kautta. Jakaminen todettiin toimivaksi odotetulla tavalla kummassakin käyttöjärjestelmissä. Sovelluksia ei kuitenkaan voitu jakaa suoraan laitteelle ilman ryhmän luontia.

3. Maksullisten sovelluslisenssien keskitetty hankinta ja omistajuuden vaihtaminen

Maksullisten sovellusten keskitetty hankinta puuttuu Androidin Managed Google Play:sta, mutta iOS:llä maksullisia sovelluslisenssejä voitiin hankkia School Managerista ja jakaa käyttäjille samalla tavalla kuin ilmaissovelluksia. Suurin osa sovellushankinnoista tehdäänkin iOS:lle. Sovelluslisenssien omistajuuden vaihdokset onnistuivat älykkäiden ryhmien muokkaamisella ja jatkossa tämä tulee laskemaan kustannuksia sekä helpottamaan sovellusten hallintaa.

4. Oppilaan hallittu Google-tili tulee toimia

Oppilaat tarvitsevat hallittua Google-tiliä opiskeluun, joten se jätettiin sallituksi profiilien rajoituksista. Jos henkilökohtaisia hallittuja tilejä ei olisi tarvittu, olisi Play-kaupan käyttöä voitu rajoittaa tällä asetuksella.

5. Oppilaiden Play-kaupan vapaan pääsyn rajoittaminen

Oppilaiden käyttämiä sovelluksia pyrittiin hallitsemaan paremmin rajoittamalla Play-kauppaa. Tätä ei kuitenkaan saatu toteutettua, koska Play-kaupan estäminen pysäytti myös sovellusasennukset katalogin kautta. Laitehallinnan luoma tili rajoitti kaupan käyttöä, mutta oppilaiden hallituilla tileillä pääsi kauppaan normaalisti.

6. Toimenpiteet hukattujen tai varastettujen laitteiden varalta

Tietoturvaa saatiin parannettua mahdollisissa laitteiden katoamistapauksissa. Laitteita voidaan lukita tai tyhjentää etänä. Tyhjennys poistaa palauttaa laitteen tehdasasetuksiin. DEP-ohjelmassa olevat Applen laitteet kysyvät tyhjennyksen jälkeen organisaation käyttäjätunnuksia, joten kukaan muu ei pääse käyttämään laitteita. Laitteen lukitus vaatii lukituksen poiston hallintapaneelin kautta.

7. Pilvipalvelujen käytön rajoittaminen

Tietojen asettamista pilveen haluttiin pystyä rajoittamaan. iCloudin käyttö voitiin estää kokonaan, eikä silloin kirjautuminen siihen onnistunut. iCloudin osia voitiin myös tarkemmin estää, esimerkiksi pelkästään kuvien synkronointi.

8. Kovennettu näyttölukitus henkilökunnalle

Henkilökunnan laitteille asetettiin profiilien kautta pakollinen, vähintään kuuden merkin mittainen pääsykoodi. Lukitukselle voitiin määrittää muitakin asetuksia, mutta niille ei vielä koettu tarvetta.

6.2 Muut hyödyt

Vaatimusten ohella palvelussa havaittiin muitakin etuja. Käyttöjärjestelmien versioista saadaan tietoa ja ne voidaan tarvittaessa pitää ajan tasalla, jos käyttäjä ei muista sitä tehdä. Johonkin versioon on voinut jäädä tietoturva-aukkoja, joten päivittäminen voi olla tärkeää. Päivittämisestä voidaan palvelun kautta lähettää kehote tai pakottaa se. Laitteista saadaan lisäksi muutakin tietoa, kuten esimerkiksi tapahtumalogeja, asennetut sovellukset ja onko laite vaarantunut. Laitteille saadaan lisättyä ehtoja, joiden täytyttyä tai täyttämättä jääminen laukaisee jonkun toiminnon, esimerkiksi lähettää järjestelmänvalvojalle ilmoituksen. Näitä ehtoja ei testattu, mutta niistä voi olla hyötyä jatkoa ajatellen.

Lisäksi palvelu tarjosi käyttäjiä helpottavia ominaisuuksia. Pääsykoodien nollaus käy helposti etänä ja se todettiin toimivan hyvin nopeasti. Laite kysyy seuraavan kerran näytön lukituksen yhteydessä asettamaan uuden pääsykoodin. Tarpeellisten sovellusten pakotettu asentaminen helpottaa huomattavasti käyttäjää, varsinkin kiireellisessä tilanteessa tarpeelliset sovellukset voidaan saada nopeasti suoraan käyttäjille. Hyötynä oli myös se, että joidenkin yksittäisten sovellusten käyttö voidaan estää kokonaan.

7 Pohdinta

Työn tavoitteena oli perehtyä VMware AirWatch –palveluun ja ottaa se käyttöön kouluympäristöön, ottaen huomioon turvallisuuskysymykset. Palvelu oli valittu ja otettu kokeiluun jo toisessa toimipisteessä. Tavoitteeseen päästiin, eli konfiguroitiin MDM-palvelu, jonka sisälle saatiin molemmat käytössä olevat mobiilikäyttöjärjestelmät. Uudistuksen koettiin tuovan selvää hyötyä käytännössä. Sovellusten hallinta helpottui siirreltävien keskitetysti hankittujen lisenssien ansiosta. Omistetuista sovelluksista pysytään paremmin perillä, eikä laitteita käyttävän henkilökunnan tarvitse itse huolehtia maksullisten sovellusten hankkimisesta.

Ympäristön käyttöönotto oli yksinkertaista. Aikaa toteutuksessa kului eniten laitteiden lisäämiseen suuren laitemäärän ja vähäisten latureiden määrän takia. Muutamaan iPadiin suoritettiin varmuuskopion palautus. Palautus ei onnistunut suoraan DEP:iin lisäämisen jälkeen, koska laite palautui samaan tilaan kuin ennen sitä. Palautus jouduttiin tekemään tyhjään laitteeseen, joka oli jo lisätty hallintaan. Tämän jälkeen tehtiin uusi varmuuskopio uudessa laitteessa ja vasta sitten palautus tehtiin alkuperäiseen laitteeseen. Varmuuskopioiden palauttamisen parantaminen helpottaisi olemassa olevien laitteiden käyttöönottoa, joissa on suuri määrä sovelluksia ja tietoa, tai ne halutaan täysin samanlaisiksi.

Mobiililaitteiden käyttö yrityksissä kasvaa ja hallintajärjestelmät tulevat tarpeelliseksi isommilla laitemäärillä. Hallintajärjestelmien kehitys ja integroinnit yrityksen käyttämiin palveluihin muokkaavat mobiilihallintaa kokonaisvaltaisemmaksi hyödyksi verrattuna pelkkään laitteiden rajoittamiseen käytännöillä. Myös BYOD-käyttötapauksissa sekä työntekijän että yrityksen tietoturvaa parannetaan ja mahdollistetaan turvallinen pääsy yrityksen resursseihin.

Koen, että AirWatch kokonaisuutena on laaja ja suosittu palvelu, joka tarjoaa hallintamahdollisuuksia moneen tarpeeseen. Tässä työssä käytetyt ominaisuudet pääosin liittyivät laitteiden hallintaan, sovelluksiin ja turvallisuuteen. Mobiilihallinta oli aluksi itselleni melko vieras kokonaisuus, mutta se tuli nopeasti tutuksi työtä tehdessä. Työtä tehdessä pysyttiin suunnitelmassa, tutkittiin ominaisuuksia ja opittiin uutta.

Uskon, että työstä on hyötyä tulevaisuudessa oman ammattitaidon kasvattamisessa ja yritysmaailman mobiiliratkaisujen ymmärtämisessä. Työtä voivat hyödyntää myös organisaatiot, jotka suunnittelevat mobiilihallinnan käyttöönottoa.

Lähteet

Android. N.d. Artikkeli itewikin verkkosivuilla. Viitattu 12.2.2020. https://www.itewiki.fi/opas/android/

Apple Configurator 2. N.d. Apple Configurator 2 käyttöopas. Viitattu 5.1.2020. https://support.apple.com/fi-fi/guide/apple-configurator-2/cad99bc2a859/mac

Bring your own device (BYOD). N.d. Artikkeli ManageEnginen verkkosivuilla. Viitattu 24.1.2020. https://www.manageengine.com/mobile-device-management/bring-your-own-device-byod-management.html

Characteristics of Organization Groups. N.d. Dokumentointi VMwaren verkkosivuilla. Viitattu 28.5.2020. https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1903/UEM_Managing_Devices/GUID-AWT-CHARACTERISTICSOFOGS.html

Everything You Need to Know about Mobile Device Management (MDM). N.d. Artikkeli Continuumin verkkosivuilla. Viitattu 4.3.2020. https://www.continuum.net/resources/mspedia/everything-to-know-about-mobile-device-management-mdm

Hjort, P. 2015. Android-tablettien opetuskäyttö – Case Helsingin Juutalainen Yhteiskoulu. Opinnäytetyö, AMK. Metropolia Ammattikorkeakoulu, tekniikan ala, tietotekniikan koulutusohjelma. Viitattu 25.5.2020. http://urn.fi/URN:NBN:fi:amk-2015120419464

iOS. N.d. Artikkeli itewikin verkkosivuilla. Viitattu 12.2.2020. https://www.itewiki.fi/opas/ios/

Karppinen, L. 2019. Mobiililaitehallintaratkaisujen testaus: Case: Versowood. Opinnäytetyö, AMK. Lahden ammattikorkeakoulu, tekniikan ala, tieto- ja viestintätekniikan koulutusohjelma. Viitattu 25.5.2020. http://urn.fi/URN:NBN:fi:amk-201902122264

Kivikäs, L. 2019. MDM-järjestelmien tekninen vertailu Telia Inmics-Nebula Oy:lle. Opinnäytetyö, AMK. Jyväskylän ammattikorkeakoulu, tekniikan ala, tieto- ja viestintätekniikan koulutusohjelma. Viitattu 2.4.2020. http://urn.fi/URN:NBN:fi:amk-2019053113875

Lukka, K. N.d. Konstruktiivinen tutkimusote. Viitattu 24.5.2020. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Madden, J. 2019. What is MDM, MAM, EMM, and UEM, and what's the difference? Viitattu 4.3.2020. https://www.brianmadden.com/opinion/What-is-MDM-MAM-EMM-UEM

Mikä on Apple School Manager? N.d. Apple School Managerin käyttöopas. Viitattu 5.1.2020. https://support.apple.com/fi-fi/guide/apple-school-manager/tes7909096bf/web

Mobile Operating System Market Share Worldwide. N.d. Kaavio Statcounterin verkkosivuilla. Viitattu 3.4.2020. https://gs.statcounter.com/os-market-share/mobile/worldwide

Overview of VMware Workspace ONE Intelligent Hub. N.d. Tuotteen dokumentointi VMwaren verkkosivuilla. Viitattu 8.12.2019. https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Hub_Services_Pointer/GUID-DCFC6D0F-74B4-4681-B1BB-BBDFF4C243EC.html

Rouse, M. N.d. VMware AirWatch. VMworld 2016 konferenssista. Viitattu 23.11.2019. https://searchmobilecomputing.techtarget.com/definition/VMware-AirWatch

Smart Groups. N.d. Dokumentointi VMwaren verkkosivuilla. Viitattu 28.5.2020. https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/UEM_ConsoleBasics/GUID-AWT-SMARTGROUPSOVERVIEW.html

Stuart, G. 2019. AirWatch Agent is now Intelligent Hub, and it's still watching you! Viitattu 8.12.2019. https://vdestination.com/airwatch-agent-is-now-intelligent-hub-and-its-still-watching-you/

Valteri. N.d. Valterin verkkosivut. Viitattu 10.5.2020. https://www.valteri.fi/valteri/

Wuerthele, M. 2019. Apple unveils iPadOS, adding features specifically to iPad. Viitattu 4.3.2020. https://appleinsider.com/articles/19/06/03/apple-supplements-ios-13-with-new-tablet-specific-ipad-os-branch

What Everybody Ought to Know About Android: Introduction, Features & Applications. N.d. Artikkeli ElProCusin verkkosivuilla. Viitattu 4.3.2020. https://www.elprocus.com/what-is-android-introduction-features-applications/

What Is Workspace ONE? N.d. Artikkeli VMwaren verkkosivuilla. Viitattu 6.12.2019. https://techzone.vmware.com/resource/what-workspace-one

Workspace ONE- \ VMware AirWatch -järjestelmän ja Apple-laitteiden rekisteröintiohjelma. N.d. Artikkeli Dellin verkkosivuilla. Viitattu 13.12.2019. https://www.dell.com/support/article/fi-fi/sln306829/workspace-one-vmware-airwatch-j%C3%A4rjestelm%C3%A4n-ja-apple-laitteiden-rekister%C3%B6intiohjelma?lang=fi

Work Managed Device Enrollment. N.d. Dokumentointi VMwaren verkkosivuilla. Viitattu 28.5.2020. https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/VMware-Workspace-ONE-UEM-Android-Documentation/GUID-AWT-AFWENROLLMENT-OVERVIEW.html

Work profiles. N.d. Dokumentointi Android Developers -verkkosivuilla. Viitattu 18.2.2020. https://developer.android.com/work/managed-profiles