Joonas Hänninen

**Mobiililaitteiden hallinta Windows -palvelinympäristössä**

Opinnäytetyö
Kajaanin ammattikorkeakoulu
Koulutusala
Tietojenkäsittelyn koulutusohjelma
Syksy 2014

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

**OPINNÄYTETYÖ**
**TIIVISTELMÄ**

| | |
|---|---|
| Koulutusala<br>Luonnontieteiden ala | Koulutusohjelma<br>Tietojenkäsittelyn koulutusohjelma |
| Tekijä(t)<br>Hänninen, Joonas | |
| Työn nimi<br>Mobiililaitteiden hallinta Windows -palvelinympäristössä | |
| Vaihtoehtoiset ammattiopinnot<br>Järjestelmänylläpito | Toimeksiantaja<br>Haataja, Sirpa |
| Aika<br>Syksy 2014 | Sivumäärä ja liitteet<br>31+2 |


Mobiililaitteet ovat yleistyneet valtavasti muutaman viime vuoden aikana. Organisaatioiden työntekijöiden ei enää tarvitse istua kiinteän työpisteen ääressä. Tämä asettaa uusia haasteita organisaation järjestelmänylläpidolle ja tietoturvalle. Mobiililaitteet pitäisi saada hallittavaksi, kuten perinteiset tietokoneet. On olemassa erilaisia vaihtoehtoja, joita organisaatio voi toteuttaa. Opinnäytetyössä tutustutaan yhteen ratkaisuun ja selvitetään, miten laitteiden hallinta onnistuu.

Selvitettävänä ovat mobiililaitteiden yleistyminen ja tietoturva. Testattava ohjelmisto on Symantec Mobile Management. Tavoitteena on rakentaa toimiva hallintaratkaisu mobiililaitteille Windows -palvelinympäristössä. Asennusprosessi ja konfigurointi kuvataan tarkkaan. Käytännön testaus tehdään käyttämällä kahta erilaista Android-laitetta.

Kohderyhmänä ovat henkilöt ja organisaatiot, jotka ovat kiinnostuneita mobiililaitteiden tietoturvauhkista tai Symantec Mobile Managementista. Tavoitteena on havainnollistaa Symantec Mobile Managementin käyttöönottoa ja tuoda esille erilaisia tietoturvauhkia, joista on hyvä tietää.



| | |
|---|---|
| Kieli | Suomi |
| Asiasanat | Mobiililaitteet, hallinta, symantec mobile management, tietoturva |
| Säilytyspaikka | ☒ Verkkokirjasto Theseus<br>☒ Kajaanin ammattikorkeakoulun kirjasto |

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

**THESIS**
**ABSTRACT**

| School<br>School of Business | Degree Programme<br>Business Information Technology |
|---|---|
| Author(s)<br>Hänninen, Joonas | |
| Title<br>Administrating Mobile Devices in Windows Server Environment | |
| Optional Professional Studies<br>System Administration | Commissioned by<br>Haataja, Sirpa |
| Date<br>Fall 2014 | Total Number of Pages and Appendices<br>31+2 |


Mobile devices have become common very rapidly during the last couple of years. Employees of organizations do not need to sit in front of stationary workstations anymore. This sets new challenges for organization's system administration and information security. Mobile devices should be administrated, like traditional computers. There are different options that organization can implement. The thesis explores one solution and studies how the administration of devices is implemented.

The subjects of the research are the generalization and security of mobile devices. The software for testing is Symantec Mobile Management. The aim is to set up a working administration solution for mobile devices in the Windows server environment. The installation process and configuration are described in detail. The practical testing is done with two different Android devices.

The target groups for this thesis are people and organizations that are interested in security threats of mobile devices or Symantec Mobile Management. The aim is to demonstrate the deployment of Symantec Mobile Management and introduce different security threats that you should be aware of.



| | |
|---|---|
| Language of Thesis | Finnish |
| Keywords | Mobile devices, administration, Symantec mobile management, information security |
| Deposited at | ☒ Electronic library Theseus<br>☒ Library of Kajaani University of Applied Sciences |

SISÄLLYS

1 JOHDANTO 1

2 MOBIILILAITTEIDEN YLEISTYMINEN 2

3 TIETOTURVA 5
3.1 Riskit 5
3.2 WLAN 6
3.3 Puhelinvakoilu 7

4 SYMANTEC MOBILE MANAGEMENT (SMM) TESTAUS 9
4.1 Testausympäristö 9
4.2 Asennus 10
4.2.1 Microsoft SQL Express 2008 R2 11
4.2.2 Symantec Installation Manager (SIM) 12
4.2.3 Symantec Management Platform (SMP) 13
4.2.4 Symantec Mobile Management (SMM) 15
4.3 Konfigurointi 16
4.3.1 Mobile Management Server 16
4.3.2 Android ja Google Cloud Messaging 17
4.3.3 Autentikointi Active Direcorystä 20
4.4 Hallinnan ominaisuudet 21
4.5 Mobile Management Agent App 25

5 POHDINTA 29

LÄHTEET 30

LIITTEET

SYMBOLILUETTELO

| | |
|---|---|
| App | Application software, sovellusohjelmisto |
| FBI | Federal Bureau of Investigation, Yhdysvaltain keskusrikospoliisi |
| GCM | Google Cloud Messaging, palvelimen ja Androidin välillä tietoa välittävä palvelu |
| GPS | Global Positioning System, maailmanlaajuinen paikallistamisjärjestelmä |
| IIS | Internet Information Services, web-palvelinohjelmisto |
| IP | Internet Protocol, protokolla |
| IT | Information Technology, informaatioteknologia |
| NSA | National Security Agency, kansallinen turvallisuusvirasto |
| SIM | Symantec Installation Manager, ohjelmisto, jolla asennetaan ja päivitetään Symantecin tuotteita |
| SMM | Symantec Mobile Management, ohjelmisto, jolla hallitaan mobiililaitteita |
| SMP | Symantec Management Platform, ohjelmisto, joka toimii alustana monille muille Symantecin tuotteille |
| VPN | Virtual Private Network, virtuaalinen erillisverkko |
| WCF | Windows Communication Foundation, viestijärjestelmä palvelusovelluksia varten |
| WLAN | Wireless Local Area Network, langaton lähiverkko |

# 1 JOHDANTO

Mobiililaitteiden yleistymisen myötä yritysten IT-ylläpidot ovat joutuneet kohtaamaan uusia haasteita. Ennen oli hallittavana vain staattiset työpisteet pöytäkoneineen. Nykyisin työnteko on joustavampaa mobliililaitteiden avulla. Mobiililaitteet pyritään saamaan hallintaan, kuten perinteiset tietokoneet. Tähän on olemassa erilaisia ratkaisuja. Työssä testattiin käytännössä ratkaisua nimeltä Symantec Mobile Management.

Mobiililaitteiden hallintaohjelmistot ovat usein osa suurempaa kokonaisuutta, koska yrityksillä on yleensä tarve hallita myös muita laitteita. Symantec Mobile Management on yksi komponentti Symantecin hallintaohjelmistossa. Tämän vuoksi asennusprosessiin kuuluu paljon muutakin.

Tutkimuksessa testattiin Symantec Mobile Managementtia Windows –palvelinympäristössä. Ohjelmiston asennus ja konfigurointi kuvattiin tarkasti. Tämän lisäksi tutkittiin mobiililaitteiden mullistusta yleisesti ja tutustuttiin erilaisiin tietoturvauhkiin. Näin saadaan vähän vihjeitä mobiililaitteiden tulevaisuudesta.

# 2 MOBIILILAITTEIDEN YLEISTYMINEN

Mobiililaitteiden yleistyminen on tapahtunut nopeasti. Internetin käyttäminen liikkeellä ollessa on rutiinia, ja sitä pidetään itsestäänselvyytenä. Taskussa voi kuljettaa valtavan määrän tietoa Wikipedian ja Googlen ansiosta, sosiaalisen median käyttö onnistuu missä vain ja navigointiohjelmistojen avulla ei eksy vieraassa kaupungissa. (Salmenkivi 2012, 54–58.)

Ihmisillä on jatkuvasti käytössä internet-yhteys kehittyneissä maissa. Tähän käytetään kaikkein useimmiten älypuhelinta. Liikepankki Morgan Stanley kertoi vuonna 2011 arvion, että 3G-mobiiliverkon käyttäjiä olisi noin 1 503 miljoonaa. Tämä määrä on hiukan vähemmän kuin perinteisillä kiinteillä koneilla internetiä käyttävien määrä. (Salmenkivi 2012, 58–59.)

YK:n teknologiapaneelien jäsentä, professori Manuel Castellsia kuultiin vuonna 2010 verkkotieteen konferenssissa Royal Societyssä. Hän kertoi, että mobiilien internetkäyttäjien määrä tulisi ohittamaan vuoteen 2014 mennessä pöytäkoneilla internettiä käyttävien määrän. (Salmenkivi 2012, 59.)

Internetanalyytikko ja globaalin teknologiatutkimustiimin vetäjä Mary Meeker kirjoittaa State of Internet -raportissa, että olemme merkittävän teknologiasyklin keskellä. Aiempia syklejä olivat keskusyksikköaika, minitietokone, kotitietokone ja pöytäinternet. Nyt on mobiilin internetin aika. (Salmenkivi 2012, 59.)

Älypuhelinten lisäksi nousussa ovat myös tabletit. Monet tablet-huumaan pyrkineet laitteet ovat jäänet kilpailijoiden varjoon. IPad- ja Android-tabletit ovat saaneet tukevan jalansijan markkinoille. (Salo 2012, 53.)

Vaikka älypuhelinten toimitukset ovat kokonaisuudessaan hurjassa nousussa, suurimmat älypuhelinten toimittajat ovat kokeneet markkinaosuuksissaan laskua. Vuoden 2013 ja 2014 välillä Samsungin markkinaosuus laski 32,4 prosentista 31,2 prosenttiin, kun Applen markkinaosuus puolestaan painui 17,5 prosentista 15,3 prosenttiin. (Lehtiniitty 2014.)

Applen markkinaosuus on ollut laskussa jo pidemmän aikaa, mutta Samsungin markkinaosuus laski ensimmäistä kertaa neljään vuoteen. Myös Nokia on todennäköisesti menettänyt markkinaosuuttaan jonkin verran. Tällä hetkellä nousussa ovat kiinalaiset

valmistajat Huawei ja Lenovo. Kuvassa 1 on taulukko, josta näkee eri älypuhelintoimittajien toimitusmääriä ja markkinaosuuksia vuosilta 2013 ja 2014. (Lehtiniitty 2014.)

Exhibit 1: Global Smartphone Vendor Shipments and Market Share in Q1 2014[1]

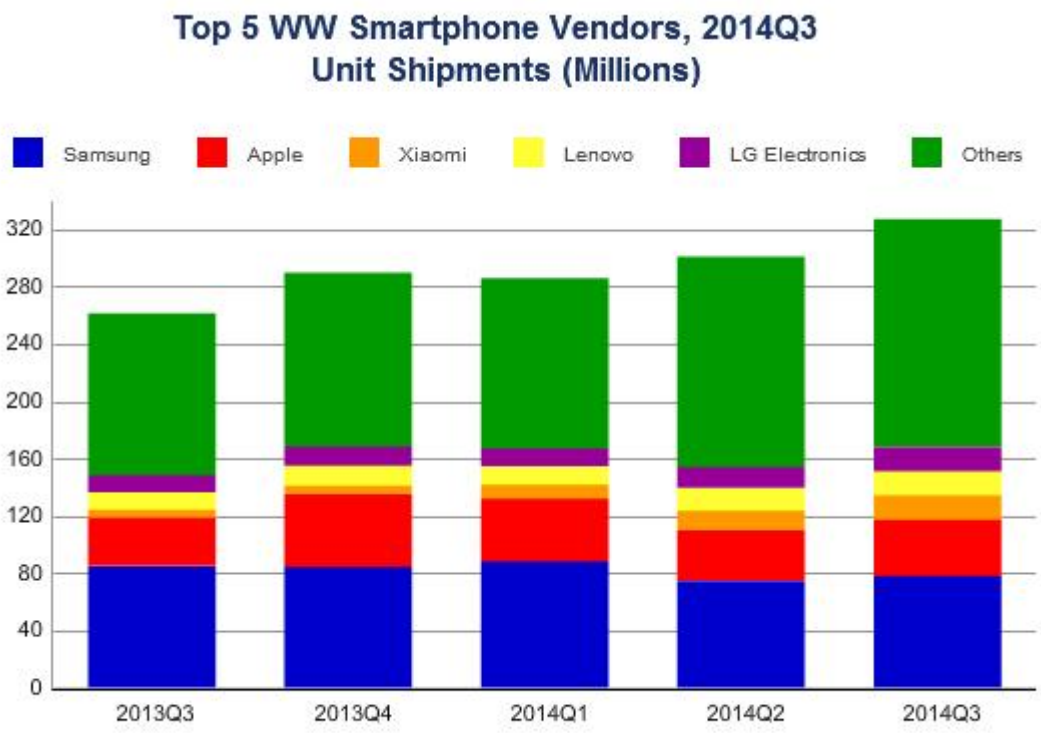
| Global Smartphone Vendor Shipments (Millions of Units) | Q1 '13 | Q1 '14 |
|---|---|---|
| Samsung | 69.4 | 89.0 |
| Apple | 37.4 | 43.7 |
| Huawei | 10.0 | 13.4 |
| Lenovo | 8.4 | 13.3 |
| Others | 88.7 | 125.6 |
| Total | 213.9 | 285.0 |

| Global Smartphone Vendor Marketshare % | Q1 '13 | Q1 '14 |
|---|---|---|
| Samsung | 32.4% | 31.2% |
| Apple | 17.5% | 15.3% |
| Huawei | 4.7% | 4.7% |
| Lenovo | 3.9% | 4.7% |
| Others | 41.5% | 44.1% |
| Total | 100.0% | 100.0% |

| Total Growth Year-over-Year % | 39.1% | 33.2% |
|---|---|---|

Kuva 1. Älypuhelintoimittajien toimitusmäärät ja markkinaosuudet. (Mobiili.fi 2014 a.)

Vuoden 2014 aikana kehitys on jatkunut edelleen samansuuntaisena. Suurimmat ja tunnetuimmat teknologiajätit kokevat laskua ja kiinalaiset uudet tulokkaat ovat nousussa. Kiinalaisesta Xiaomista on tullut maailman kolmanneksi suurin älypuhelinvalmistaja. Xiaomi on onnistunut nousemaan Kiinan älypuhelinmarkkinoilla Samsungin ohi ykköseksi. Kuvasta 2 näkee älypuhelinvalmistajien viimeisimpiä toimitusmääriä. (Haikala 2014.)




Kuva 2. Älypuhelinvalmistajien viimeisimpiä toimitusmääriä. (Haikala 2014.)

# 3 TIETOTURVA

Jokin aika sitten verkkorikollisille oli kannattavampaa etsiä uhreja tietokoneiden kautta kuin nykyisin. Nykyisin verkkorikollisten on helpompi etsiä uhreja mobiililaitteiden kautta kuin vielä jokin aika sitten. Tietoturva-asiantuntija Ilari Karisen mukaan mobiililaitteille kohdistuva verkkorikollisuus lisääntyy samalla kun kyseisten laitteiden käyttö lisääntyy. (Paunonen 2014.)

## 3.1 Riskit

Mobiililaitteiden mukana voi kulkea valtava määrä salaista tai henkilökohtaista tietoa. Tällöin laitteen hukkaaminen voi olla suuri riski. Laitteissa ei useimmiten käytetä kunnon suojakoodeja, vaan kuka tahansa saa avattua laitteen lukituksen sormella vetämällä. Suojakoodin ei välttämättä tarvitse olla pitkä. Lyhyt suojakuvio tai suojakoodi on tehokas ja harva taskuvaras vaivautuu murtamaan sen. (Paunonen 2014.)

Mobiililaitteet voivat saada haittaohjelmia ja viruksia aivan kuin tietokoneet. Nämä virukset vaanivat sovelluksissa, joita voi ladata laitteelle erilaisista sovelluskaupoista. On suosittavaa käyttää ainoastaan laitevalmistajan virallista sovelluskauppaa. Tällöin haittaohjelmien riski on huomattavasti pienempi, koska laitevalmistajat yleensä kitkevät epäilyttävät sovellukset kaupoistaan nopeasti. (Paunonen 2014.)

Pelkkään laitevalmistajaan ei kannata luottaa haittaohjelmien torjunnassa. Sovelluksia ladattaessa kannattaa itse tarkistaa, millaisia oikeuksia sovellus laitteeseen haluaa. Eräällä suositulla taskulamppu-sovelluksella oli täydet oikeudet laitteen tietoihin, kuten selaushistoriaan ja puhelutietoihin. Kyseinen sovellus pystyi lähettämään nämä tiedot eteenpäin. Tällaiset sovellukset pystyvät leviämään, koska useat käyttäjät eivät vaivaudu tarkistamaan asentamiensa sovelluksien oikeuksia. (Paunonen 2014.)

On tärkeää, että mobiililaitteet pidetään ajan tasalla samoin kuin tietokoneetkin. Mahdolliset yksittäisten sovelluksien tai käyttöjärjestelmän päivitykset kannattaa ottaa käyttöön mahdollisimman pian. Uusissa versioissa on yleensä korjattu tietoturva-aukkoja. Mikäli käytössä on vanhempi laite johon ei ole päivityksiä saatavilla, erillisen tietoturvaohjelmiston

merkitys korostuu entisestään. Monista tietokoneelta tutuista viruksentorjuntaohjelmistoista on saatavilla myös mobiiliversio. (Paunonen 2014.)

## 3.2 WLAN

Avoimia WLAN-verkkoja käytettäessä kannattaa olla tarkkana. Huijarit voivat luoda oman avoimelta verkolta vaikuttavan verkon kalastellakseen tietoja esimerkiksi kahvilassa tai lentokentällä. Julkisissa tiloissa on hankala tietää, minne tiedot päätyvät avoimen tukiaseman kautta. Avoimien verkkojen käyttö on huomattavasti turvallisempaa, jos käyttää VPN-ohjelmistoa. (Paunonen 2014.)

Jos mobiililaitteella käytetään sähköpostia tai hoidetaan raha-asioita, kannattaa tarkistaa että käytössä on suojattu yhteys. Sivustolla on käytössä suojattu yhteys, jos osoitteen alussa on https. Jos sähköpostia käytetään laitteelle liitetyllä tilillä, kuten Gmaililla, salattu yhteys on käytössä automaattisesti. (Paunonen 2014.)

Lähiverkon langattomuus on suuri hyöty nykyaikaisissa joustavissa työympäristöissä. Tämä mahdollistaa esimerkiksi kämmentietokoneiden ja muiden mobiililaitteiden vaivattoman käytön. WLAN-verkkojen uhkat ovat suurimmilta osin samat kuin perinteisessä lankaverkossa, mutta langattomuus tuo kuitenkin mukanaan uudenlaisia tietoturvaongelmia. (Puska 2005, 18.)

Verkkoa on mahdollista kuunnella tai häiritä ulkopuolelta, koska radioaaltojen etenemistä ei voida rajoittaa rakennuksen sisälle. Radioaaltojen etenemistä on vaikea kontrolloida ja mallintaa. Tähän vaikuttavat monenlaiset asiat kuten ihmiset, kalusteet, kasvillisuus tai sääolosuhteet. Koska radioaaltojen ulottumista halutun alueen ulkopuolelle ei voida välttää, on WLANin suunnittelu hankalaa. (Puska 2005, 21.)

Langaton lähiverkko tuo ylläpitoon uusia haasteita. Langattoman verkon laitteet voidaan varastaa tai joku voi ottaa käyttöön jonkin epävirallisen yhteyspisteen, joka voi vaarantaa tietoturvan. Eräässä esimerkkiskenaariossa rakennuksen ulkopuolelle voidaan sijoittaa yhteyspiste, johon mobiililaitteet ja rakennuksen sisällä olevat työasemat liittyvät. Tämä kyseinen yhteyspiste voidaan määritellä ohjaamaan sisäänkirjautumispyynnöt kohteeseen, joka kerää käyttäjien tunnuksia talteen. (Puska 2005, 22, 68.)

Tällä tavoin voidaan kerätä suuri osa käyttäjien tunnuksista lyhyessä ajassa työajan alkaessa. Kun tunnukset on otettu talteen, yhteyspiste voi palauttaa virheilmoituksen ja uudelleenkirjautumispyynnön. Tällä tavoin käyttäjät luulevat kirjoittaneensa tunnuksensa väärin eivätkä huomaa tilanteessa mitään epäillyttävää. On tärkeää että tietohallinto seuraa laitteiden identiteettiä, jotta tällaisilta tilanteilta vältytään. (Puska 2005, 68.)

## 3.3 Puhelinvakoilu

Viimeaikoina Yhdysvaltain tiedusteluvirasto NSA on ollut suuri puheenaihe. Heillä on käytössään PRISM-vakoilujärjestelmä, joka tuottaa yhden seitsemästä aiheesta, jotka nousevat esiin päivittäisessä turvallisuusraportissa. The Washington Post on saanut käsiinsä dokumentteja, joiden mukaan NSA:lla on pääsy suurimpien Internet-yritysten tietokantoihin. Vakoiltaviin verkkoyhteisöihin kuuluvat muun muassa Google, Gmail, Youtube, Yahoo ja Facebook. (Digitoday 2013 a.)

Tiedot vakoilusta ovat säikäyttäneet ihmisiä ympäri maailmaa, koska suuri osa maailman verkkoliikenteestä kulkee amerikkalaisten tietokanta- ja tietoliikennepalvelimen kautta. NSA:n johtaja James R. Clapper on antanut lausunnon, jossa hän kertoo järjestelmällä kerätyn tiedon olevan tärkeimpiä ulkomaantiedustelun informaatiolähteitä. (Digitoday 2013 a.)

NSA:lla saattaa olla myös pääsy yleisimpien älypuhelinten tietoihin. Muun muassa Apple, Google ja Microsoft ovat luovuttaneet palveluidensa käyttäjien tietoja NSA:lle. Mikäli asia todella on näin, NSA:lla on luja ote suurimmasta osasta älypuhelimista. Microsoft Windows Phone-, Android- ja iOS-käyttöjärjestelmät pitävät hallusaan suurinta osaa älypuhelinmarkkinoista. (Digitoday 2013 b.)

Nokian Lumia-puhelimissa on käytössä Windows Phone-käyttöjärjestelmä, joten myös Nokian puhelinten turvallisuutta alettiin epäillä NSA-paljastusten myötä. Kahden sisäpiirin lähteiden tietojen mukaan Nokian ylin johto tiesi Lumia-puhelinten välittävän käyttäjien tietoja Microsoftille. Asian kiusallisuuden takia yhtiö on ollut asiasta hissukseen. (Sajari 2014.)

Suomen Viestintävirasto on lähettänyt Nokialle useita selvityspyyntöjä ja pyytänyt vakuutusta, että heidän laitteiden käyttäjien ”luottamuksellinen viestintä, paikkatiedot tai

muut yksityiset tiedot eivät paljastu ulkopuolisille ilman käyttäjän suostumusta". Nokia ei pystynyt antamaan vakuutusta, jota Viestintävirasto toivoi. Lopulta Nokia antoi vakuutukset, joissa sen ei tarvinnut vakuuttaa mitään Microsoftin puolesta. (Sajari 2014.)

Nokia korostaa, että kommunikointi ulkomaisten palvelinten kanssa voidaan estää puhelimen asetuksia säätämällä. Tämä ei kuitenkaan välttämättä riitä, koska käyttöjärjestelmä on edelleen yhteydessä ulkomaille. (Sajari 2014.)

Google ja Apple ovat ottaneet käyttöönsä uudet tietoturvakäytännöt. Androidin ja iOS:n uusimmat versiot salaavat käyttäjien tiedot oletuksena. Edes Apple ja Google eivät pääse ohittamaan käyttäjän salausta. (Pitkänen 2014.)

Yhdysvaltain liittovaltion poliisin FBI:n johtaja James Comey on kritisoinut näitä muutoksia. Hänen mielestään uudet tietoturvakäytännöt asettavat käyttäjät lain yläpuolelle. IT-jäteillä pitäisi olla tarvittaessa keino päästä käsiksi käyttäjiensä tietoihin. Näillä tiedoilla voi olla suuri hyöty esimerkiksi terrorismi-iskuja tutkittaessa. (Pitkänen 2014.)

FBI ei enää pysty esimerkiksi kääntymään Applen puoleen, mikäli he tahtovat tietoja jostakin tietystä käyttäjästä. IOS-laitteiden rikosteknilliseen tutkintaan erikoistunut Jonathan Zdziarski kertoo, että uusilla tietoturvakäytännöillä olisi kyse siitä, että yhtiöiden ei tarvitse enää auttaa viranomaisia tietojenluovutuksessa. Viranomaiset pystyvät tarvittaessa ohittamaan iOS-laitteiden suojaukset. (Pitkänen 2014.)

# 4 SYMANTEC MOBILE MANAGEMENT (SMM) TESTAUS

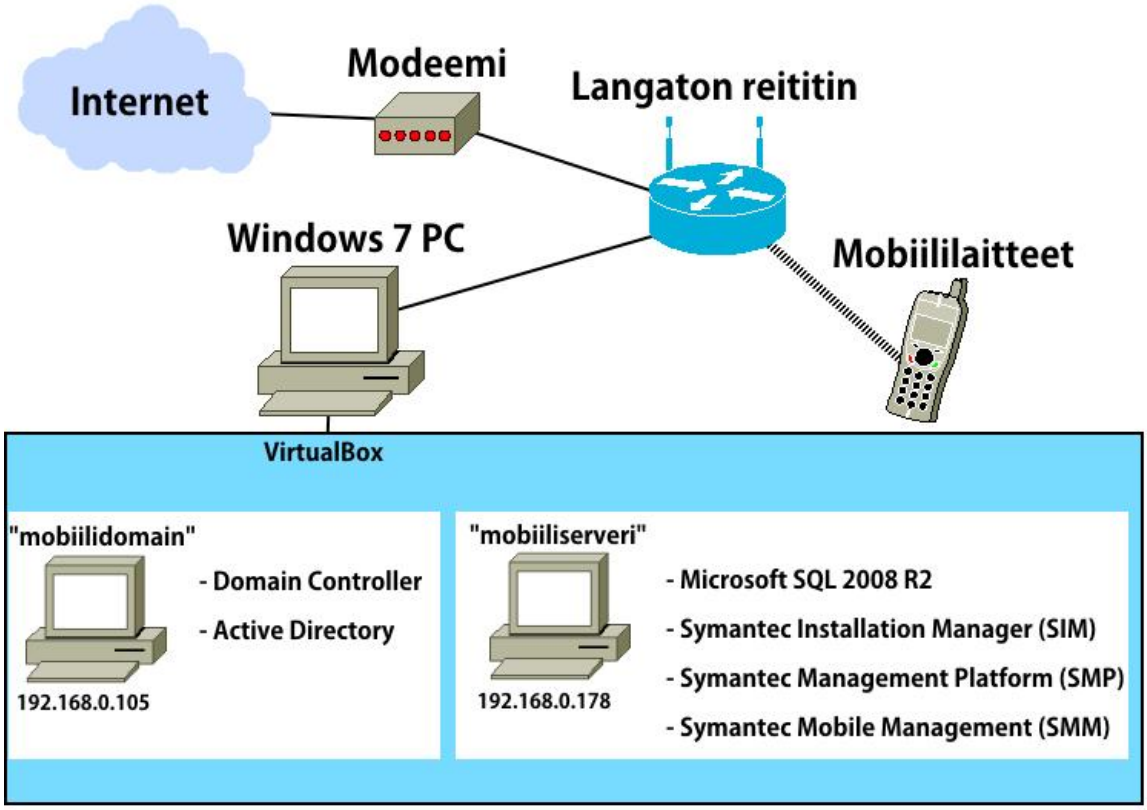
Symantec Corporation on kansainvälinen yritys, joka kehittää tiedonhallintaan ja tietoturvaan liittyviä ohjelmistoja. Yksi heidän tunnetuimpia tuotteita on Norton AntiVirus. Symantecin ratkaisu mobiililaitteiden hallintaan on Symantec Mobile Management.

Kuten yleensä, mobiililaitteiden hallintaohjelmistot ovat usein pieni osa jotain suurempaa kokonaisuutta. Harvoin yrityksissä on tarvetta pelkästään mobiililaitteiden hallintaan. Mikäli käytössä on jokin hallintaohjelmisto, luonnollisinta olisi käyttää kyseisen ohjelmiston tarjoamia mahdollisuuksia myös mobiililaitteisiin. Suurimpiin hallintaohjelmistoihin onkin saatavilla myös mobiililaitteiden hallintatoiminnot. Ne ovat joko erikseen lisättävä komponentti, päivitys tai kuuluvat jo ennestään pakettiin.

Symantec Mobile Management on yksi komponentti valtavassa ohjelmistossa. Se ei pysty toimimaan yksin, vaan vaatii toimiakseen muita Symantecin tuotteita. Seuraavaksi testataan, kuinka mobiililaitteiden hallinta onnistuu Windows-ympäristössä tällä ratkaisulla.

## 4.1 Testausympäristö

Kuvasta 3 näkee testausympäristön havainnollistettuna kaavion avulla. Palvelimet on virtualisoitu VirtualBox -nimisellä virtualisointiohjelmistolla. Mainittava seikka on, että molempien virtuaalikoneiden verkkoasetuksissa on otettu käyttöön "Bridged Adapter". Tämän avulla virtuaalikoneet näkyvät lähiverkossa normaalisti erillisinä laitteina.




Kuva 3. Testausympäristöä kuvaava kaavio.

Symantec Mobile Management tukee laitteita, joissa on Android-, iOS- tai Windows-käyttöjärjestelmä. Testaus tehdään ainoastaan kahdella erilaisella Android-laitteella, koska muuta laitteistoa testausta varten ei ollut.

## 4.2 Asennus

Asennusprosessin aikana asennetaan Symantec Installation Manager (SIM), Symantec Management Platform (SMP) ja Symantec Mobile Management (SMM).

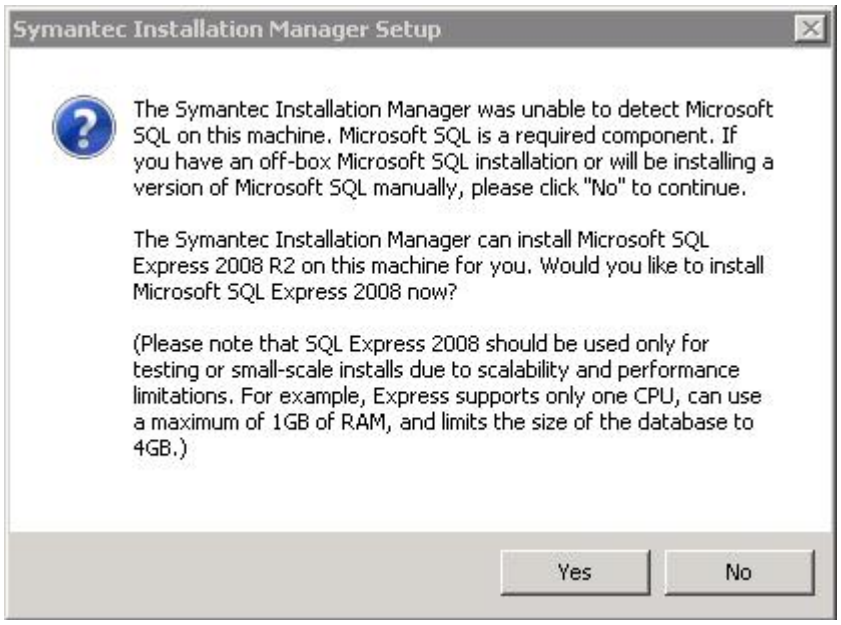
Palvelimina toimii kaksi virtuaalista Windows Server 2008 R2- konetta, joihin on asennettu kaikki saatavat päivitykset. Ensimmäiseen palvelimeen on luotu domain nimeltä "testidomain", jotta saadaan käyttöön active directory. SMM:ssä on mahdollista integroida käyttäjätiedot active directorystä. Tavoitteena oli testata ja nähdä miten hyvin Symantecin ohjelmistot sopivat Windows -palvelinympäristön kanssa yhteen. Tämän palvelimen nimeksi on annettu "mobiilidomain".

Toisen palvelimen nimi on "mobiiliserveri", ja sille asennetaan kaikki mobiililaitteiden hallinnan ohjelmistot. Tämä palvelin ei voi toimia samalla domain controllerina, joten vähintään kaksi erillistä palvelinta on tarpeen. Liitteeseen 2 on merkitty järjestelmävaatimukset.

### 4.2.1 Microsoft SQL Express 2008 R2

SMM:n kokeiluversion saa ladattua maksutta Symantecin sivustoilta, mutta se vaatii rekisteröinnin. Kokeiluversiossa ei tarvitse syöttää avainkoodia, eikä siinä ole rajoitettuja ominaisuuksia. Sitä ei vain saa käyttää tuotantoympäristössä. (Symantec 2014.)

Ladattu tiedosto ei asenna SMM:ää, vaan Symantec Installation managerin. Sitä käytetään lukuisten eri Symantecin tuotteiden asentamiseen. Heti asennuksen alussa asennusohjemisto tutkii, löytyykö palvelimesta tietokantaa. Mikäli tietokantaa ei ole asennettuna, asennusohjelmisto ehdottaa että asennettaisiin Microsoft SQL Express 2008 R2. Tämän ilmoituksen näkee kuvasta 4. Ennen tämän asennusta täytyy olla asennettuna Microsoft.net, joka on saatavilla Microsoftin latauspalvelusta.




Kuva 4. Asennusohjelmisto ehdottaa tietokannan automaattista asennusta.

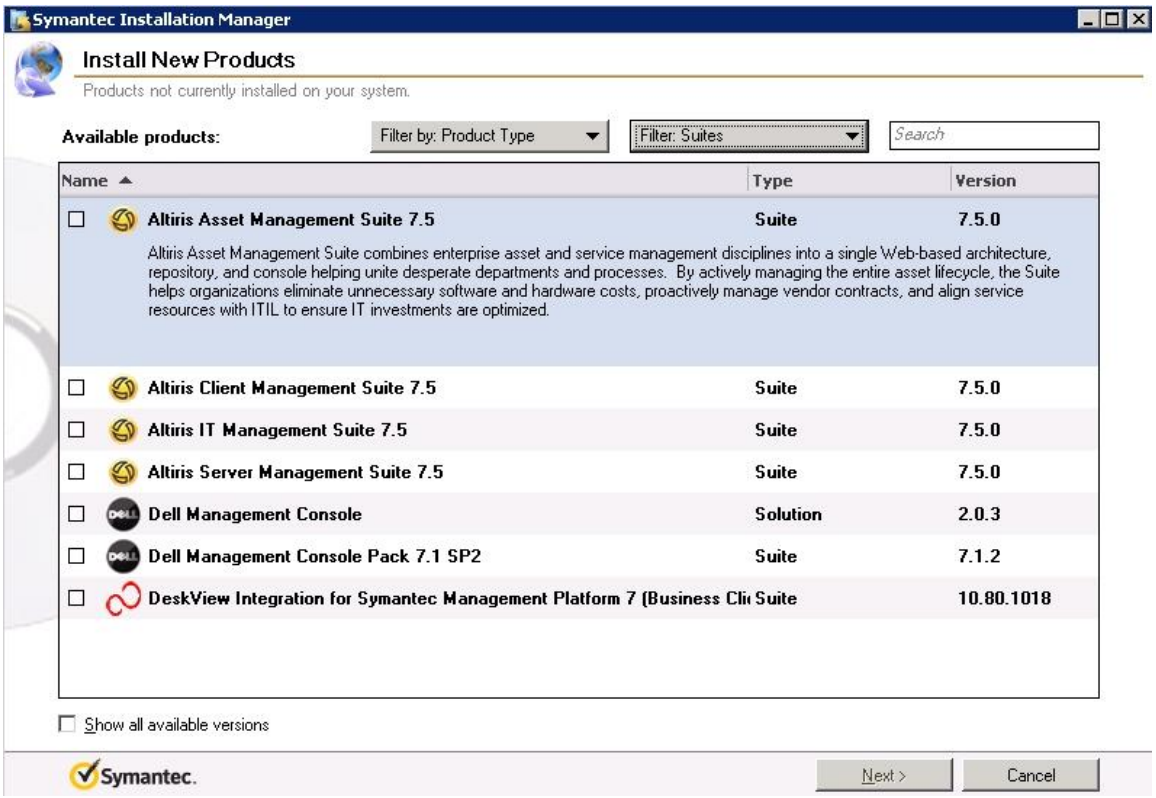
Microsoft SQL Express on ilmaiseksi käytettävä tietokanta, jossa on rajoituksia verrattuna maksullisiin versioihin. Näistä mainittavia ovat 1 GB keskusmuistin käyttö ja tietokannan maksimaalinen koko 4 GB. Nämä ovat pienimuotoiseen testaukseen riittävät.

Tietokannan asennus ei ole niin automaattinen, kuin edellinen ilmoitus antoi ymmärtää. Asennusohjelmisto latasi Microsoft SQL Expressin asennustiedostot ja aloitti asennuksen, mutta varsinainen asennus on tehtävä itse.

Asennuksen aikana ei tarvitse tehdä suuria muutoksia oletusasetuksiin. Kohdassa ”Instance Configuration” annettiin instanssin nimeksi ”symantecsql”. Tätä nimeä tarvitaan, kun erilaisia ohjelmistoja konfiguroidaan käyttämään tietokantaa. (Express Technology 2014.)

### 4.2.2 Symantec Installation Manager (SIM)

Symantec Installation Manager on ohjelmisto, jonka avulla asennetaan lukuisia Symantecin tuotteita. Tietokannan asennuksen jälkeen aloitettiin sen asennus. SIM:n asennuksessa ei tarvinnut tehdä minkäänlaisia säätöjä, vaan koko asennus tapahtui yhtä nappia painamalla. Monimutkaisemmat asennukset tapahtuvat nyt SIM:n avulla. Kuvassa 5 näkyy SIM:n käyttöliittymä.

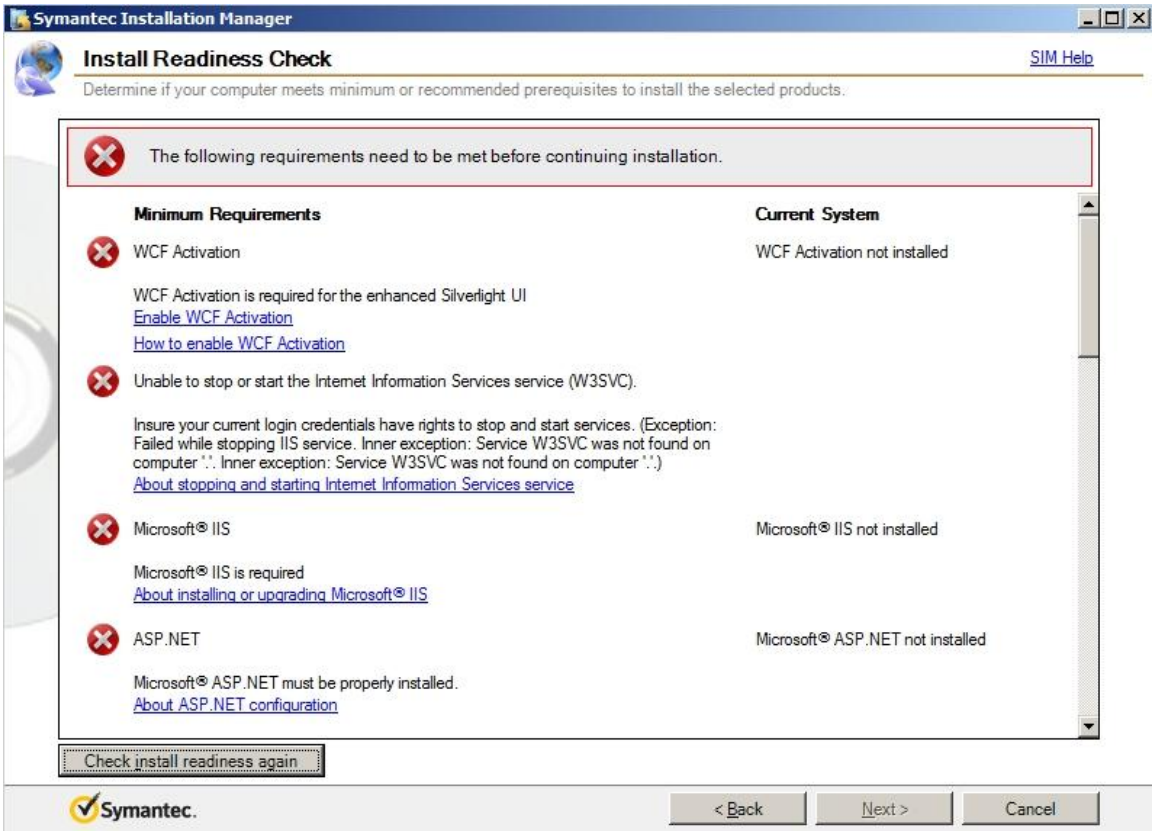



Kuva 5. Symantec Installation Managerin ensimmäinen näkymä.

Heti SIM:n asennuttua alkaa haluttujen tuotteiden asennus. Asennuksen lisäksi SIM:llä on myös mahdollista ohjelmien poisto ja päivittäminen. SIM on yhteydessä Symantecin palveluiden kanssa ja listaa aina uusimmat tuotteet ja päivitykset saataville.

### 4.2.3 Symantec Management Platform (SMP)

Symantec Management Platform on alusta, jonka useat tuotteet vaativat. Yksi näistä tuotteista on Mobile Management. SMP löytyy SIM:n luettelosta valitsemalla suodattimesta "platform". Ennen asennuksen alkua SIM tarkistaa, että palvelimeen on asennettu kaikki tarvittava. Asennus pääsee etenemään vasta kun palvelin läpäisee kaikki tarkistukset. Tämä tarkistusvaihe näkyy kuvassa 6.

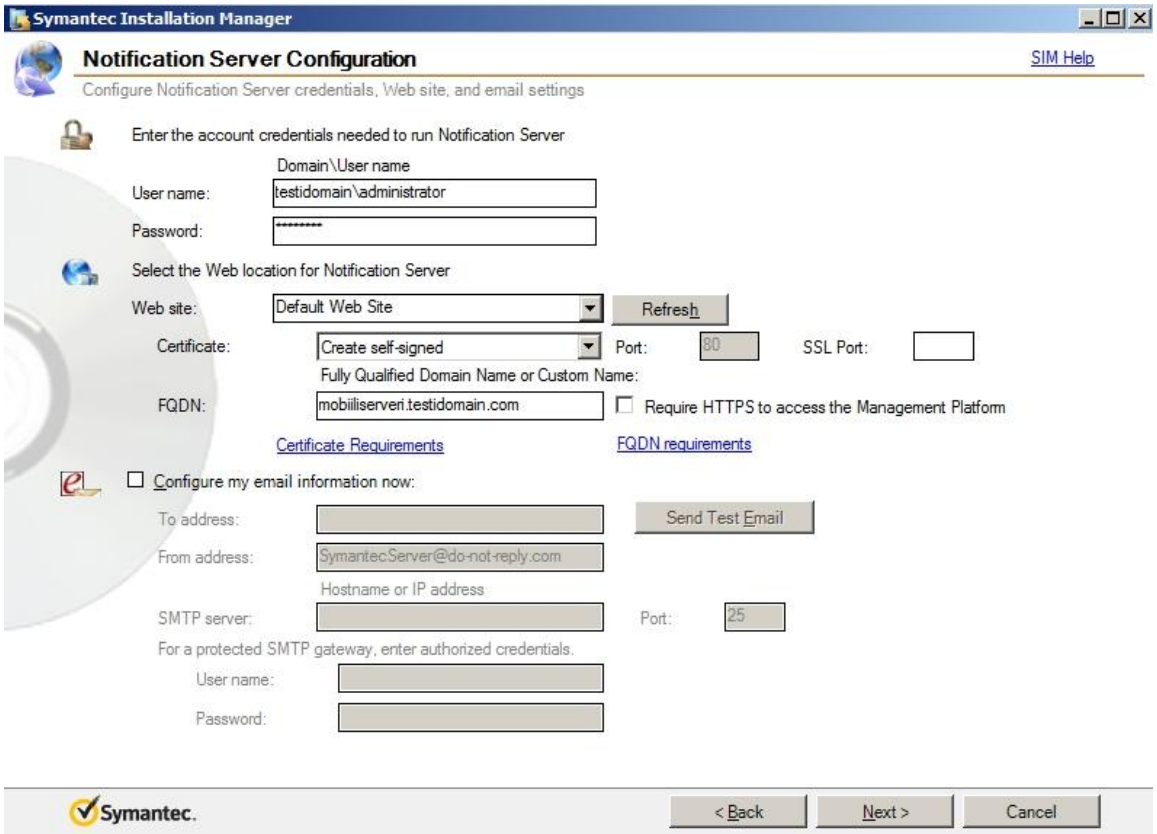



Kuva 6. Palvelimesta tarkistetaan kaikki tarvittava ennen SMP:n asennusta.

Windows Communication Foundationin (WCF) saa aktivoitua helposti klikkaamalla "Enable WCF Activation". WCF on viestijärjestelmä, jonka avulla ohjelmistot välittävät välillään tietoa.

Microsoft IIS on web-palvelinohjelmisto, ja sen saa myös asennettua helposti klikkaamalla "Click to automatically install and configure the required IIS Role Services". Tämä asentaa palvelimelle IIS-roolin ja sen tarvittavat palvelut. IIS:n asennuksen voi tehdä myös itse manuaalisesti. Liitteeseen 1 on listattu IIS:n palvelut, joita tämä toiminto asentaa automaattisesti.

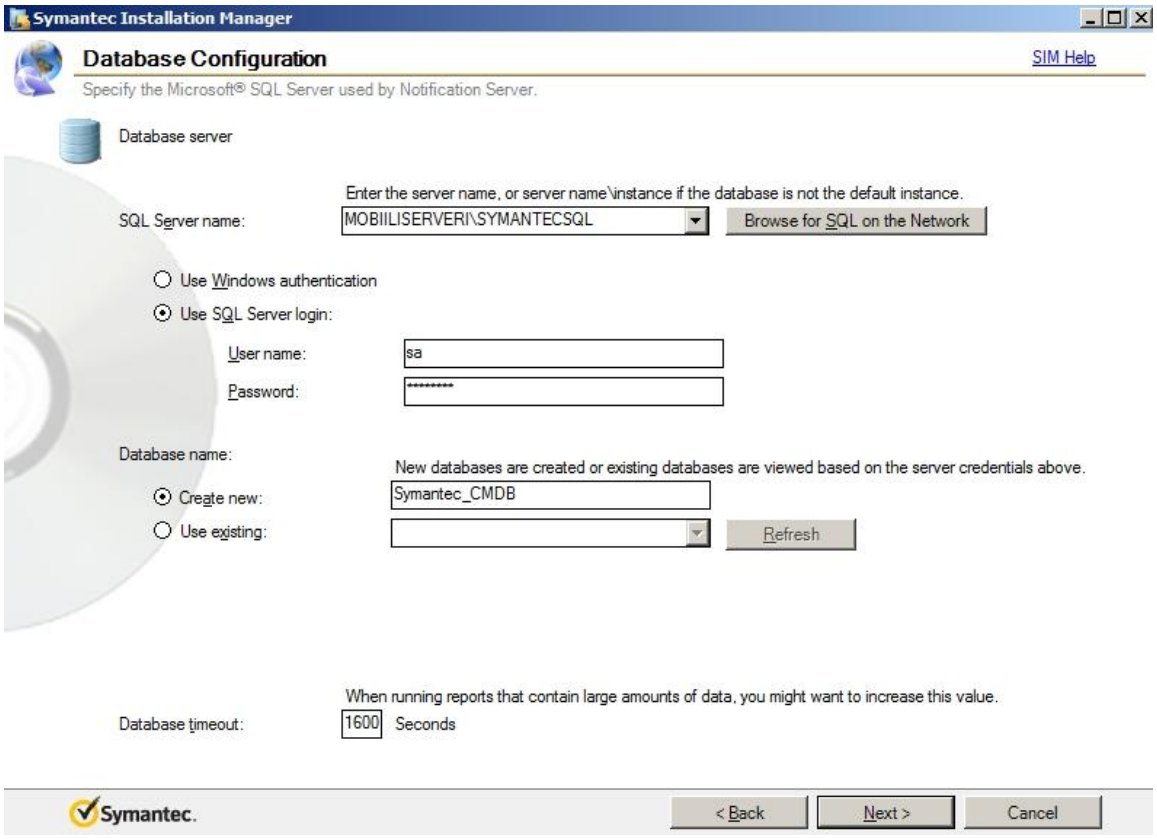
Tarkistuksen jälkeen siirrytään kohtaan "Notification Server Configuration", jossa säädetään palvelulle halutut asetukset. Jos määritetty web site on konfiguroitu väärin, asennusohjelma pystyy konfiguroimaan sen automaattisesti. Sertifikaattiin on mahdollista tuoda jo olemassa oleva sertifikaatti, tai pystytään luomaan asennusvaiheessa oma. Tämä vaihe näkyy kuvassa 7.




Kuva 7. Notification Serverin konfigurointi.

Viimeiseksi konfiguroidaan tietokanta-asetukset. Kohdassa "SQL Server name" täytyy viitata aiemmin tehtyyn instanssin nimeen eli "symantecsql". On mahdollista käyttää joko Windowsin autentikointia tai jotain muuta käyttäjätunnusta, riippuen siitä, miten SQL on konfiguroitu.

Asennushetkellä ei ollut valmista tietokantaa valmiina, joten täytyi luoda uusi. Tämä onnistuu helposti valitsemalla "Create new". Jos halutaan käyttää tietokantaa, joka on jo luotu, se voidaan valita kohdassa "Use existing". Tämän vaiheen jälkeen alkaa SMP:n asennus. Tietokannan konfigurointivaihe näkyy kuvassa 8.




Kuva 8. Tietokannan konfigurointi.

### 4.2.4 Symantec Mobile Management (SMM)

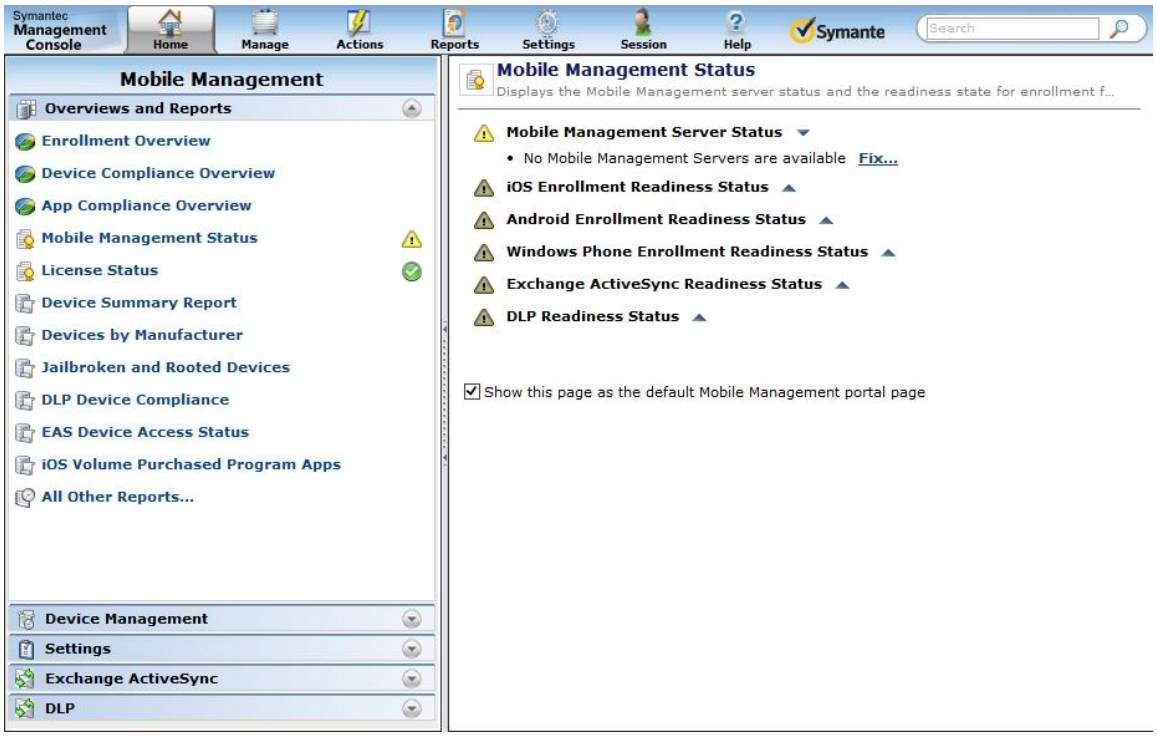
Symantec Mobile Management asennetaan SIM:n avulla. SMM löytyy, kun valitaan filtteristä "Solutions". SIM valitsee automaattisesti asennettavaksi myös Symantec Mobile Frameworkin, jos SMM on valittu. Ennen asennusta alkaa tuttuun tapaan järjestelmän tarkistus. Ainoa asia, joka tarkistetaan, on SSL:n konfiguraatio. Tässä ei pitäisi olla mitään ongelmia, vaikka kaikki olisi asennettu tähän asti oletusasetuksilla.

Tämän jälkeen SMM on asennettu ja se on ainoa komponentti, jonka kokeiluversiossa on aikaraja. SMM toimii kolmenkymmenen päivän ajan, mutta muut jatkavat toimintaansa.

## 4.3 Konfigurointi

Kun kaikki asennukset on tehty, voidaan avata Symantec Management Console, jossa tapahtuu kaikki hallinta ja konfigurointi. Symantec Management Console löytyy palvelimen käynnistysvalikosta.

Mobiililaitteiden hallinnan löytää "Home" -painikkeen alta. Täällä näkee kaikkien eri komponenttien tilan ja pääsee konfiguroimaan erilaisia asetuksia. Tämä näkymä on nähtävissä kuvassa 9.

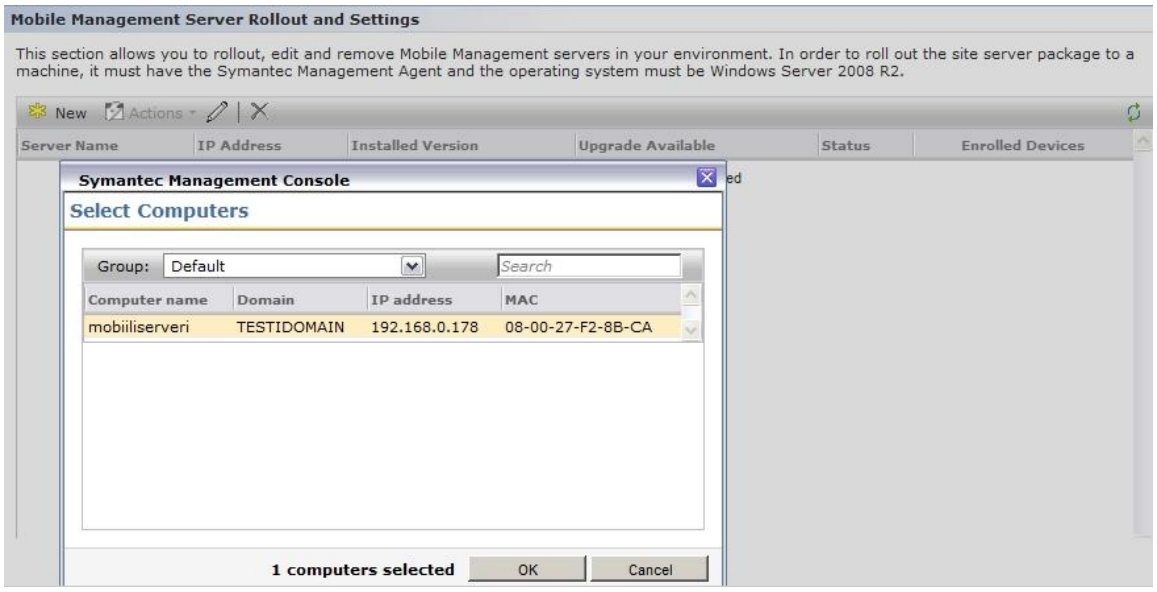



Kuva 9. Mobiililaitteiden hallinnan asetukset.

### 4.3.1 Mobile Management Server

Jotta mobiililaitteiden hallintaa on mahdollista hyödyntää, tätä varten on oltava yksi tai useampi palvelin. Mobiililaitteet ovat näiden palvelimien kanssa yhteydessä. Tällaisen palvelimen lisäys tapahtuu helposti valitsemalla "Mobile Management Status", jossa palvelimen puute ilmoitetaan. Tämän ilmoituksen vieressä on "Fix" -painike, josta aukeaa "Mobile Management Server Settings".

Uuden palvelimen lisäys onnistuu "New" -painikkeella. Tämä aukaisee listan saatavilla olevista palvelimista, joista on mahdollista tehdä mobiililaitteiden hallintapalvelimia. Vaatimuksena palvelimelle on Symantec Management Agent, joka tulee SMP:n mukana. Testiympäristöön riittää yksi palvelin, joten listasta valitaan sama tietokone, johon on asennettu muutkin Symantecin tuotteet. Tämä vaihe näkyy kuvassa 10.



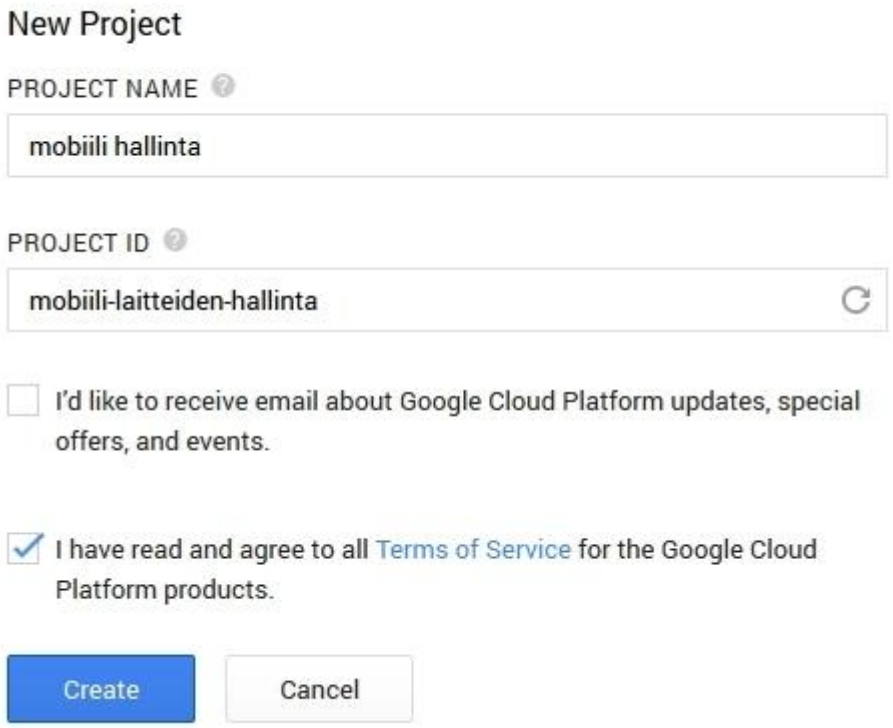

Kuva 10. Mobiililaitteiden hallintapalvelimen lisäys.

Enempää säätöjä ei tarvita, kun haluttu palvelin on valittu. Ruudulla vilisee hetken aikaa komentorivi ikkunoita, kun palvelin asentaa ja käynnistää erilaisia palveluita. Hetken kuluttua mobiililaitteiden hallintapalvelimen lisäys on valmis. Tämä palvelin ei välttämättä näy listoilla ennen kuin sivu ladataan uudestaan.

### 4.3.2 Android ja Google Cloud Messaging

Jotta Android-käyttöjärjestelmää käyttäviä laitteita voidaan hallita, on konfiguroitava GCM (Google Cloud Messaging). Tämä onnistuu samalla tavalla kuin Mobile Management Serverin tapauksessa, eli kohdassa "Mobile Management Status". Androidin kohdalla on laitettava ruksi kohtaan "Enable readiness checks", jotta järjestelmä kertoo tarvittavat toimenpiteet. Tämän jälkeen ilmestyy tuttu "Fix" -painike, josta pääsee tekemään tarvittavat konfiguraatiot.

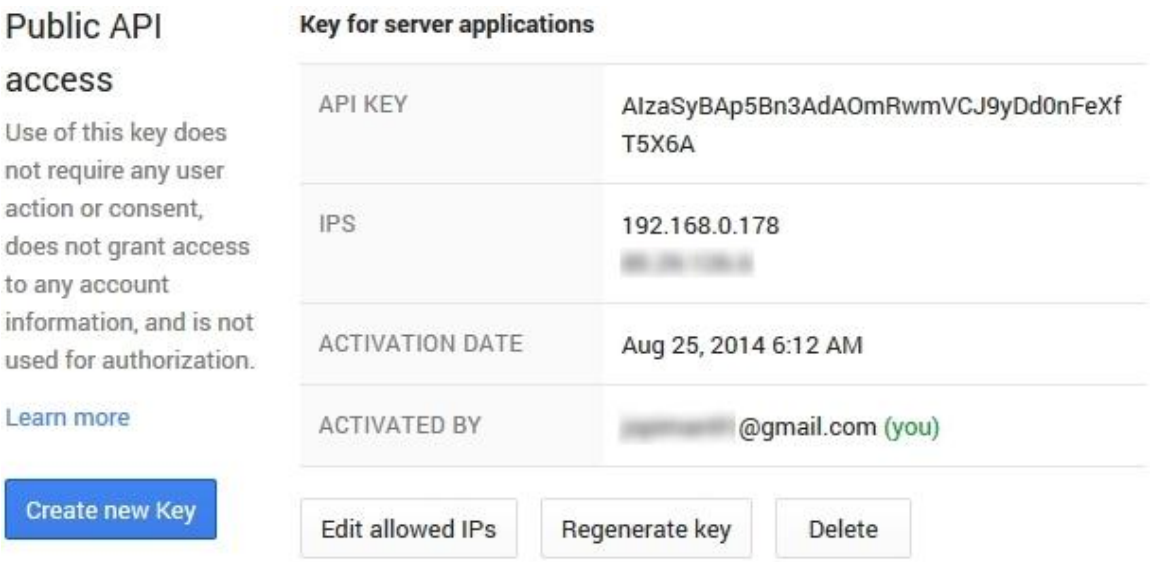
Konfiguraatiota varten tarvitaan Google Project ID ja API Key. Nämä saa Google Developer Console-palvelusta, kun sinne luodaan oma projekti. Tämä palvelu vaatii Google-käyttäjätilin. Ensimmäiseksi projektille on annettava nimi ja Project ID. Näillä tiedoilla ei ole merkitystä. Tämä vaihe näkyy kuvassa 11.




Kuva 11. Google-projektille määritetään nimi ja ID.

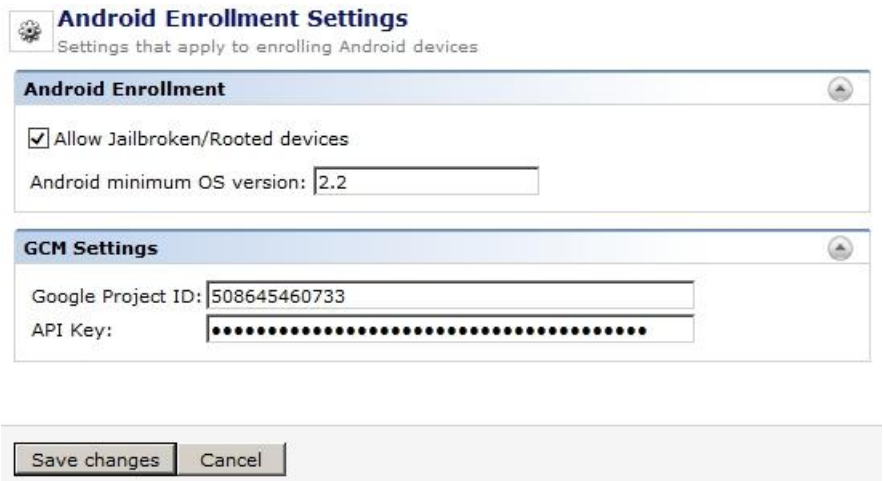
Kun projekti on luotu, tarvittava Google Project ID näkyy heti kohdassa "Project Number". GCM täytyy ottaa käyttöön erikseen. Tämä onnistuu projektin hallintapaneelissa valitsemalla kohdan "APIs & auth" alta "APIs". Tästä avautuu valtava lista erilaisia apeja. Listalta etsitään "Google Cloud Messaging for Android" ja painetaan sen kohdalta off-painiketta, jolloin se otetaan käyttöön.

Tämän jälkeen tarvitaan API Key, jonka saa kun klikkaa Credentials-painiketta. Tästä avautuu uusi näkymä, jossa valitaan "Create new key" kohdan "Public API access" alta. Tämän jälkeen valitaan "Server key" ja syötetään palvelimen IP-osoite. Kun tämä on tehty, saadaan API Key. Tämä näkyy kuvassa 12.




Kuva 12. Google-projektin API Key.

Kun tiedetään Google Project ID ja API Key, palataan takaisin palvelimelle syöttämään nämä tiedot. Tässä vaiheessa on mahdollista hyväksyä rootatut laitteet eli laitteet, joilla on pääkäyttäjän oikeudet. Tämä on hyväksytty, koska testauksessa käytettävät laitteet ovat rootattuja. On määriteltävä myös vanhin hyväksyttävä Android-versio. Tämä on oletuksena 2.2, joka on testauksessa käytettävät laitteet huomioiden sopiva. Tämä vaihe näkyy kuvassa 13.

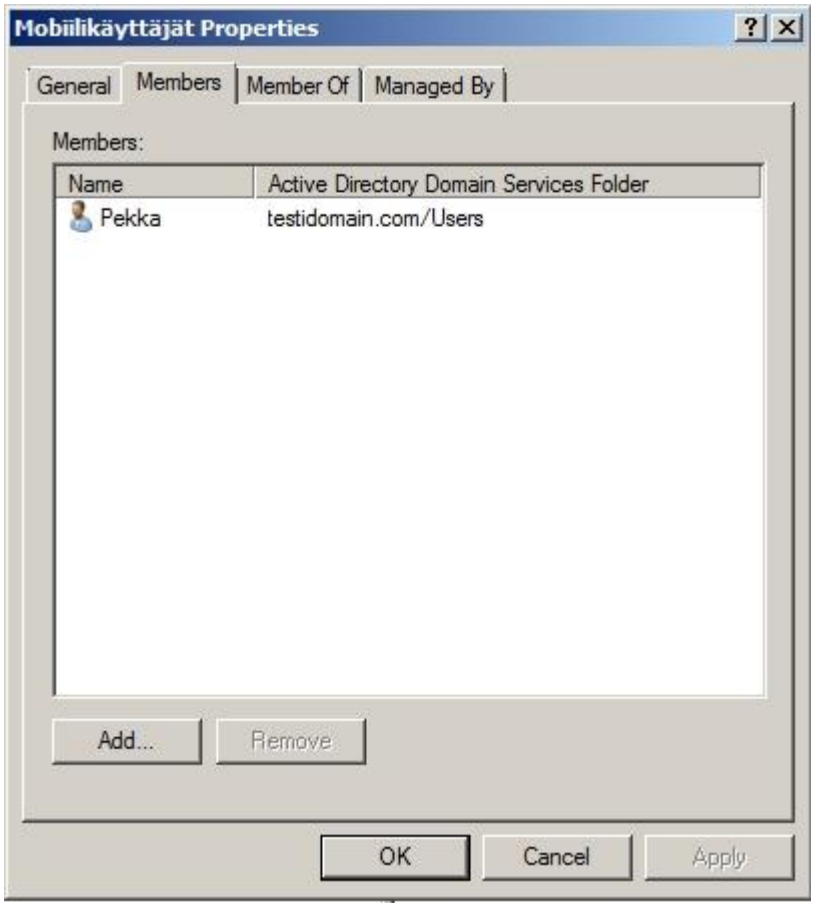



Kuva 13. GCM:n konfiguraatio.

### 4.3.3 Autentikointi Active Direcorystä

Erilliset tunnukset eivät ole tarpeen mobiililaitteella kirjauduttaessa, vaan voidaan käyttää olemassa olevia tunnuksia Windows-ympäristön Active Directorystä. Näin kirjautuminen esimerkiksi organisaation työntekijöille on helpompaa, koska joka paikkaan käy samat tunnukset. Jotta kirjautuminen mobiililaitteella onnistuisi, on tunnusten kuuluttava johonkin tiettyyn määritettyyn ryhmään.

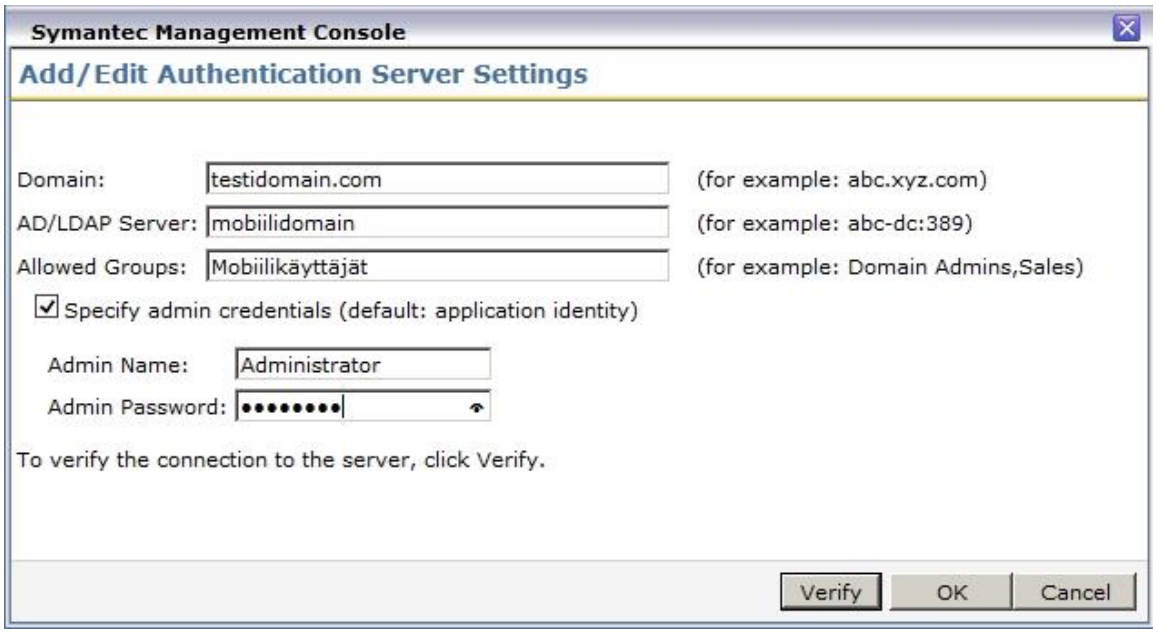
Ennen kuin tämä ominaisuus voidaan konfiguroida, on ensin tehtävä mobiilidomain-palvelimen Active Directoryyn uusi ryhmä. Tämän ryhmän nimeksi annettiin "Mobiilikäyttäjät". Samalla luotiin myös tunnukset nimeltä "Pekka" testausta varten. Nämä tunnukset lisättiin juuri luotuun ryhmään. Tämä ryhmä näkyy kuvassa 14.




Kuva 14. Mobiilikäyttäjät-ryhmään kuuluu hyväksytyt tunnukset.

Kun ryhmä ja testauksessa käytettävät tunnukset on luotu, voidaan palata takaisin mobiiliserveri-palvelimelle tekemään konfiguraatiot loppuun. Autentikoinnin konfiguraation asetukset löytyvät mobiililaitteiden asetuksissa kohdassa "General Enrollment".

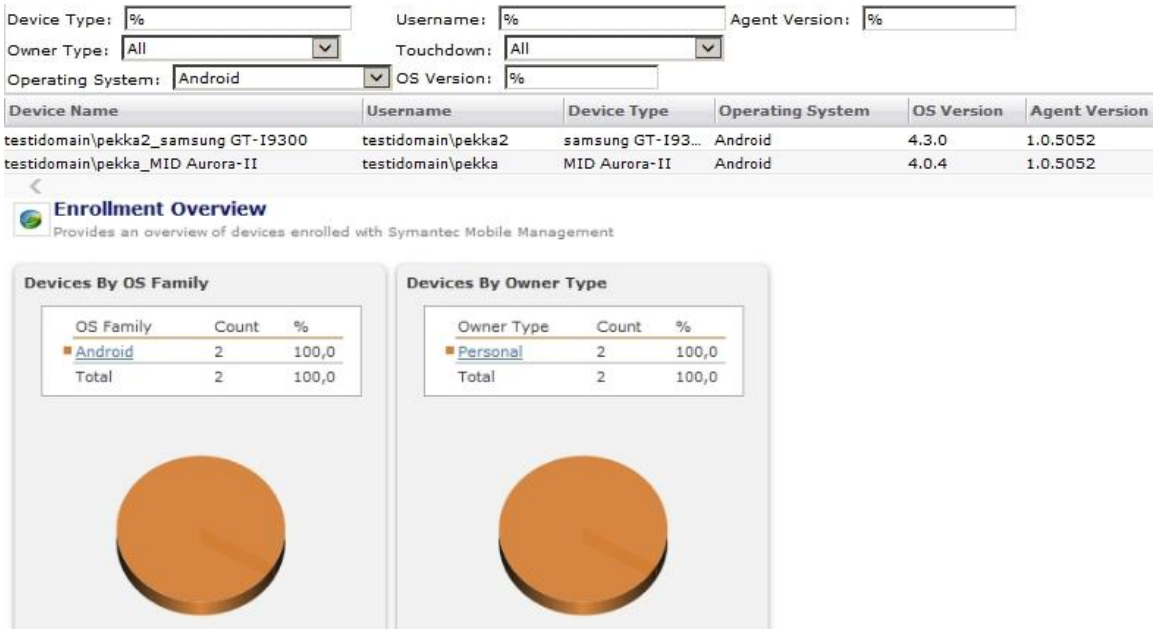
Syötettävät tiedot ovat domainin nimi, Active Directory-palvelimen nimi ja sallittujen ryhmien nimet. Jos sallittuja ryhmiä halutaan lisätä useampi, ne täytyy eritellä pilkulla. Kun tiedot on syötetty, voidaan klikata verify-painiketta, joka testaa yhteyden Active Directoryyn. Tämä vaihe näkyy kuvassa 15.




Kuva 15. Autentikoinnin asetukset.

## 4.4 Hallinnan ominaisuudet

Hallittavia laitteita voi tarkastella monesta erilaisesta näkymästä. Erilaisia kaavioita näkee esimerkiksi eri käyttöjärjestelmien tai valmistajien mukaan. Kaaviosta klikkaamalla avautuu lista kyseiseen ryhmään kuuluvista laitteista. Tämä lista sisältää yksityiskohtaisempaa tietoa kuten laitteen nimi, käyttäjän nimi ja käyttöjärjestelmän versio. Kuvassa 16 on kaavio eri käyttöjärjestelmistä.




Kuva 16. Kaavio laitteiden käyttöjärjestelmistä.

Laitteiden hallinta on joustavaa, sillä se onnistuu mistä tahansa näkymästä jos valittuna on jokin yksittäinen laite. Hiiren oikean puoleisella painikkeella aukenee "Device Management" -valikko, josta löytyy monenlaisia hallintatoimintoja. Tämä valikko näkyy kuvassa 17.


Kuva 17. Laitteiden hallintatoiminnot.

"Set Passcode" -toiminnolla pystyy määrittelemään salasanan, jolla laitteen saa avattua, kun se on lukittu "Lock Device" -toiminnolla. "Clear Passcode" poistaa salasanan käytöstä. Laitteen lukitus on hyödyllinen esimerkiksi tilanteissa, joissa laite on kadonnut tai varastettu.

Jos jonkin laitteen hallinta tahdotaan lopettaa, käytetään "Remove MDM and Reset Agent" -toimintoa. Tämä käytännössä resetoi Mobile Management Agent Apin asetukset. Apilla on yhdistettävä palvelimelle uudestaan, jos laitetta tahdotaan jälleen hallita.

Laitteista pystytään haluttaessa saamaan uusimmat tiedot "Send Inventory" -toiminnolla. Tämä lähettää laitteelle pyynnön lähettää tiedot heti. Kyseisen toiminnon pystyy myös ajastamaan niin, että se toimii automaattisesti.

"Wipe Device" -toiminto poistaa laitteelta kaikki tiedot ja palauttaa laitteen tehdasasetuksiin. Tämä poistaa myös soittohistorian ja kontaktit SIM-kortilta. Kyseessä on siis varsin radikaali toimenpide, joka voi olla hyödyllinen vakavissa varkaustapauksissa.

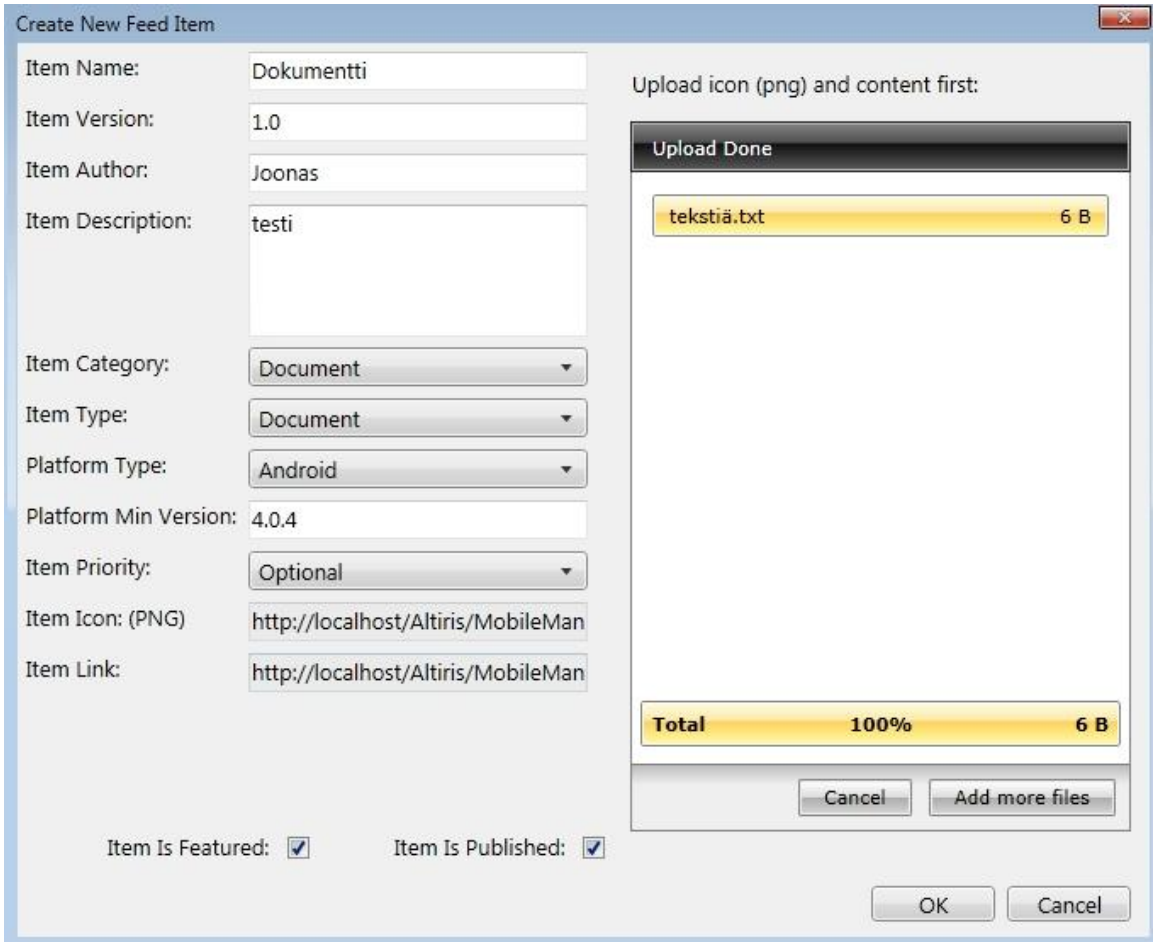
"View Device Information" -toiminto avaa sivun, josta näkee lisää tietoja laitteesta. Täältä on myös mahdollista tarkastella laitteen ja palvelimen välisten toimintojen historiaa. Myös laitteen sijaintitiedot ovat käytössä, jos kyseinen toiminto on otettu käyttöön ja laitteessa on GPS. Näitä tietoja näkyy kuvassa 18.

| | |
|---|---|
| **User:** | testidomain\pekka |
| **Phone Number:** | --- |
| **Device Owner:** | Personal |
| **Device Type:** | MID Aurora-II |
| **OS:** | Android 4.0.4 |
| **MAC Address:** | --- |
| **Device ID:** | 0501000046182AFE18ECA9E9CBED6E42C88B9392 |
| **EAS ID:** | kaiaaadeqgro7aootkplzxxgesglqojj |
| **Agent Name:** | Mobile MGMT |
| **Agent Version:** | 1.0.5052 |
| **Mobile Site Server:** | mobiiliserveri |
| **Enrolled On:** | 30.8.2014 16:58:09 |
| **Last Connected:** | 30.8.2014 16:58:09 |
| **Carrier:** | --- |
| **Registered to GCM/C2DM:** | false |

| | |
|---|---|
| **EULA Accepted:** | true |
| **Managed Device:** | true |
| **Not Jailbroken/Rooted:** | false |
| **Supported OS:** | true |
| **Valid User:** | true |
| **Has Passcode:** | --- |
| **Inventory Up To Date :** | false |
| **No Blacklisted Apps Installed:** | true |
| **All Required Apps Installed:** | true |

Kuva 18. Mobiililaitteen tietoja.

Mobiililaitteiden käyttäjille pystytään toimittamaan appeja, dokumentteja, linkkejä ja muuta mediaa Mobile Libraryn avulla. Näiden tarkastelu onnistuu mobiililaitteella Mobile Management Agent Apissa. Jotta Mobile Libraryä pystyy muokkaamaan, on palvelimella oltava asennettuna Silverlight. Median lisäys näkyy kuvassa 19.




Kuva 19. Mobile Libraryn median lisääminen.

Median kategoriaksi voi valita joko "Application", "Document" tai "Media". Näillä ei ole suurta merkitystä, ne vain vaikuttavat siihen, miten mediat näkyvät mobiililaitteilla. Jos kategoriaksi on valittu "Application", saatavilla on muutama ylimääräinen asetus. Näillä määritellään, poistetaanko laitteelta myös kyseinen appi jos Mobile Management Agent App poistetaan.

Kohdassa "Platform Type" määritellään, mikä käyttöjärjestelmä laitteella on oltava, jotta media on saatavilla. Kaikkien käyttöjärjestelmien valitseminen on myös mahdollista, mutta tällöin kohdassa "Platform Min Version" voi tulla ongelmia, koska eri käyttöjärjestelmissä voi olla aivan erilaiset versionumerot. Vanhinta versionumeroa ei ole pakko määritellää lainkaan, vaan sen voi jättää myös tyhjäksi.

Kohdassa "Item Priority" määritellään, miten tärkeä kyseinen media on. Mediasta voi tehdä vaihtoehtoisen, suositellun tai vaaditun. Vaaditut mediat ovat listan huipulla ja vaihtoehtoiset

pohjalla, kun medioita selataan mobiililaitteilla. Mobiililaitteiden käyttäjät saavat myös ponnahdusikkunoita, jotka ilmoittavat että vaadittu media on saatavilla.

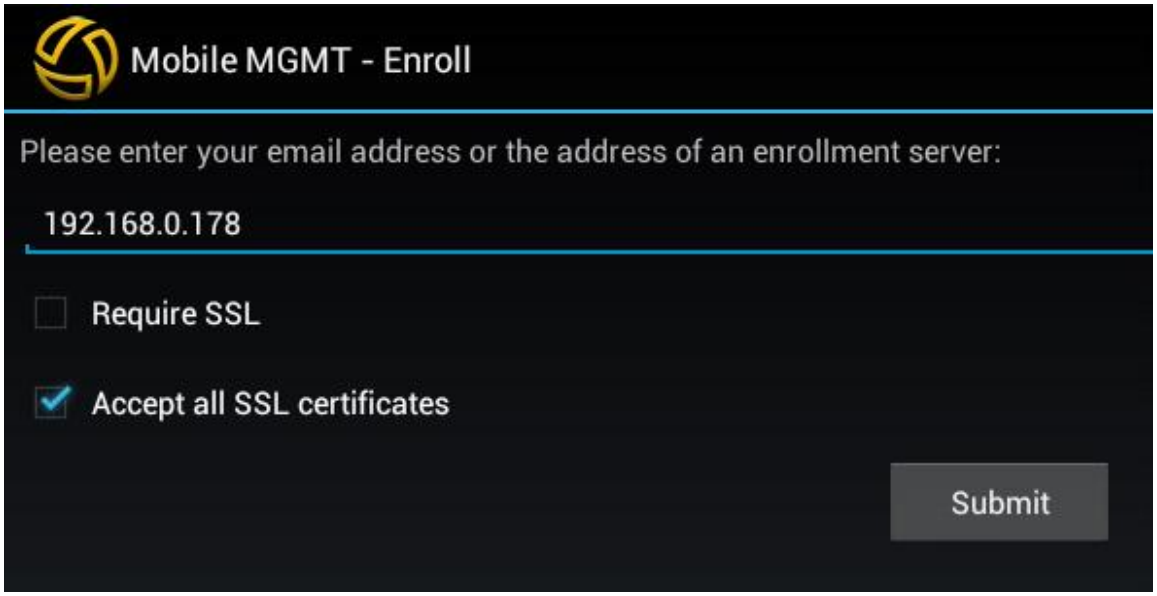
Monimutkaisinta on varsinaisen median lisääminen. Ennen median lisäämistä täytyy ensin lisätä ikoni, joka tulee näkymään median kohdalla mobiililaitteilla. Ikonin formaatin täytyy olla PNG, mutta ohjelmisto ei kerro missään, että sen täytyy olla 57 pikseliä leveä ja korkea. Jos ikoni on väärän kokoinen, se ei tule näkymään median vierellä. Kun ikoni on lisätty, voidaan lisätä haluttu media. Ohjelmisto täyttää kohdat "Item Icon" ja "Item Link" itse kun ikoni ja media lisätään.

## 4.5 Mobile Management Agent App

Kaikille hallittaville laitteille on asennettava Mobile Management Agent App, jonka avulla laitteet ovat yhteydessä palvelimen kanssa. Tämä app on maksuton ja sen saa Android-laitteille Google Play:stä, iOS-laitteille Apple App Store:sta ja Windows-laitteille Windows Phone Marketplace:sta.

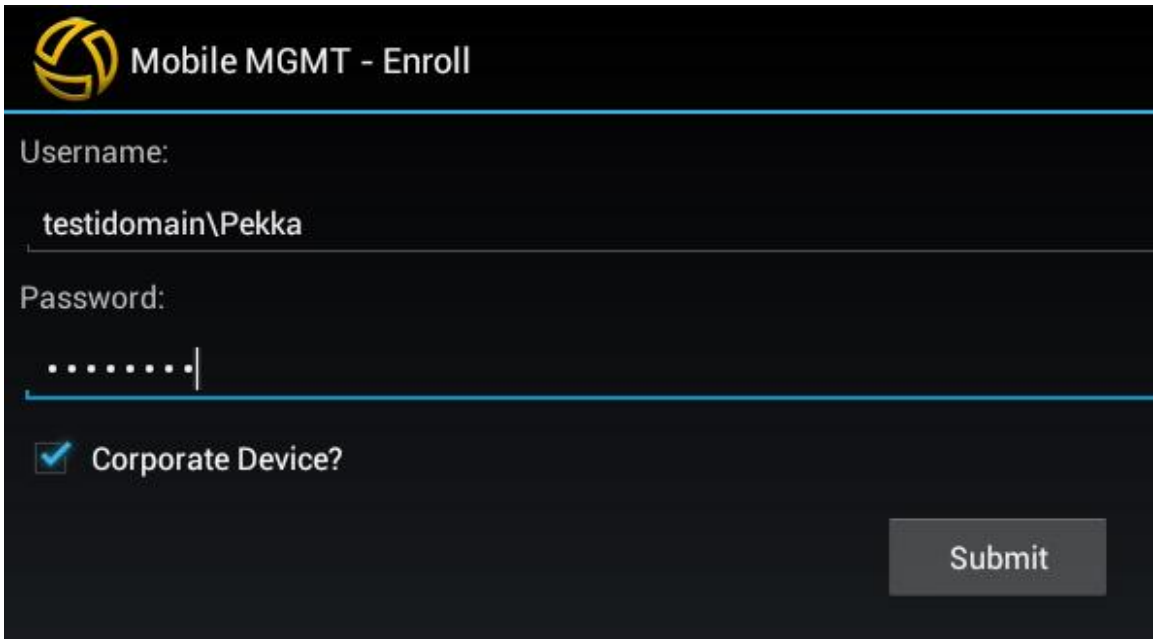
Testaus tehtiin kahdella erilaisella Android-laitteella. Ensimmäinen oli tavallinen Samsung Galaxy S3 -älypuhelin uusimmilla päivityksillä. Toinen oli Ainol Novo 7 Aurora II -tablet-tietokone, johon on asennettu kustomoitu ROM. Tämä ROM perustuu Android-versioon 4.0.4 ja on rootattu. Kyseessä on siis vähemmän yleinen kokoonpano.

Mobile Management Agent App täytyy konfiguroida toimimaan palvelimen kanssa. Ensiksi täytyy antaa palvelimen osoite. Tämä näkyy kuvassa 20.




Kuva 20. Android-laitteella syötetään palvelimen osoite.

Tämän jälkeen suoritetaan kirjautuminen aiemmin luoduilla tunnuksilla. Tässä vaiheessa on myös mahdollista kertoa palvelimelle, onko kyseinen laite yrityksen omistama vai yksityinen. Tämä vaihe näkyy kuvassa 21.




Kuva 21. Mobiililaitteella kirjaudutaan käyttämällä Active Directoryssä olevia tunnuksia.

Kirjautumisen onnistuttua laitteella ilmaantuu heti ilmoitus tarvittavasta toimenpiteestä. Jotta laitteen hallinta onnistuisi, on Mobile Management Agent App lisättävä laitteen

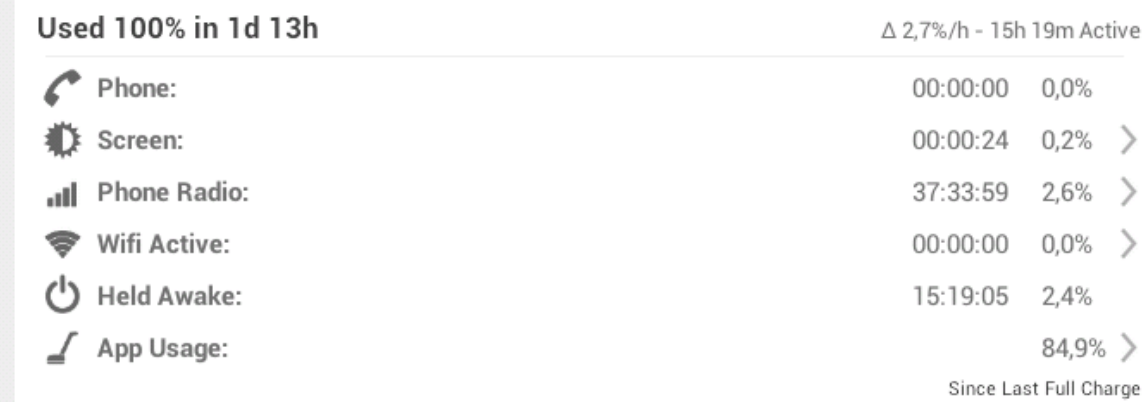
järjestelmänvalvojaksi. Ilmoituksesta painettaessa avautuu ikkuna, joka varoittaa käyttäjää mahdollisista toimenpiteistä, joita voidaan tehdä laitteelle etäältä. Tämä ilmoitus näkyy kuvassa 22.


Kuva 22. Järjestelmänvalvojan käyttöönotto.

Tämän jälkeen Mobile Management Agent App on konfiguroitu ja laittetta pystytään hallitsemaan palvelimelta. Käyttäjät pystyvät halutessaan poistamaan kyseisen apin, mutta ensiksi se pitää poistaa laitteen järjestelmänvalvojista. Apia poistettaessa avautuu ikkuna, jossa on painike järjestelmänvalvojien hallintaan.

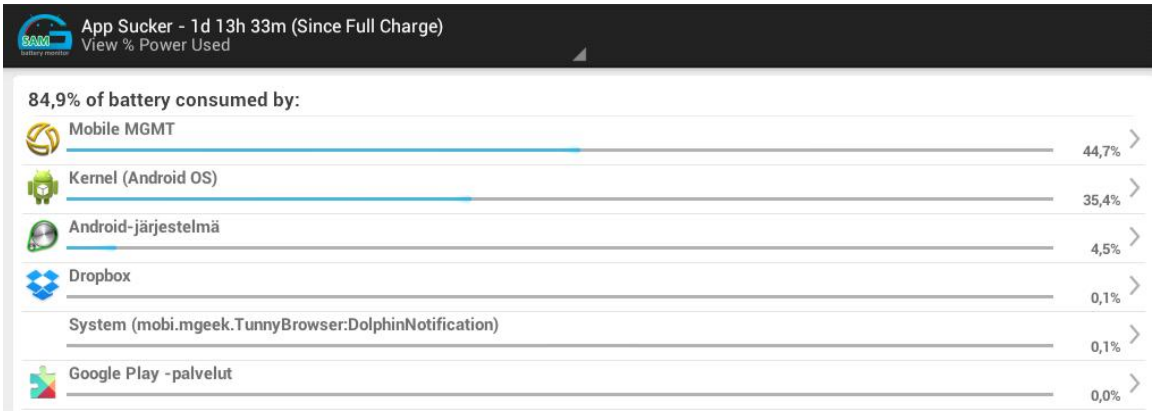
Laitteiden akun kulutuksessa helposti havaittava muutos, kun app on asennettu. Akut tyhjenevät selvästi aiempaa nopeammin. Asiaa tutkittiin Ainol Novo 7 Aurora II -laitteella

apilla nimeltä GSam Battery Monitor. Kyseinen app on ilmainen ja saatavilla Google Play:stä. Kuvassa 23 näkee akun kulutuksen eri osa-alueilta prosentuaalisesti.




Kuva 23. Apit ovat kuluttaneet akkua eniten.

Akun kulutus oli hyvin vähäistä muualla kuin appien osalta. Laitetta ei käytetty testauksen aikana. Siitä pidettiin näyttö pois päältä ja odoteltiin, että akusta loppuu virta. Akussa riitti virtaa noin 37 tunnin ajan. Kuvassa 24 näkee paljonko akkua eri apit kuluttivat. Sama testi tehtiin myös ilman Mobile Management Agent Appia. Akku kesti silloin noin 192 tuntia. Kyseessä on siis huomattavan suuri ero.




Kuva 24. Symantec Mobile Management App kulutti yksin akusta 44,7%.

# 5 POHDINTA

Työssä pyrittiin keräämään mahdollisimman uutta tietoa mobiililaitteiden tämän hetkisestä tilanteesta ja kehityksestä, jotta olisi mahdollista hahmottaa tulevaisuuden näkymiä. Kerätty tilastotieto viittaa siihen, että tulevaisuudessa Android saattaa nousta entistäkin yleisemmäksi älypuhelinmarkkinoilla, samalla kun iOS menettää markkinaosuuttaan. Tämä johtunee kiinalaisten älypuhelinten noususta.

Käytännön osuudessa asennettiin ja testattiin Symantec Mobile Managementtia. Tämän asennusta varten täytyi ensin asentaa Symantec Installation Manager, jonka avulla asennetaan Symantecin ohjelmistoja. Yleensä tällaiset väliin tulevat ohjelmistot koetaan rasittaviksi, mutta SIM oli positiivinen yllätys. Asennus sujui helposti ja monia asioita oli automatisoitu. Projektin aikana julkaistiin pari päivitystä SMM:ään, jotka SIM asensi ongelmitta.

SMM sisältää vaikuttavat toiminnot mobiililaitteiden varkauksia varten. Laittet pystyy lukitsemaan tai niistä voidaan poistaa kaikki tiedot. Mobiililaitteita on jopa mahdollista paikantaa GPS:n avulla. Tämä toiminto oli kuitenkin hiukan piilotettu, kun muut toiminnot olivat yhden painalluksen päässä.

SMM:n heikko puoli oli median ja tiedon jakaminen laitteille. Tämä toiminto on toteutettu hiukan kömpelösti, eikä ohjelmisto anna tarpeeksi ohjeita sen käytöstä. Tähän saattaa joskus tulla muutoksia päivitysten myötä.

Käytännön testaus tehtiin valitettavasti käyttäen vain Android-laitteita. Windows Phonen ja iOS:n hallinnan testaus olisi ollut hyvä lisä, koska näiden konfigurointiprosessit ovat erilaiset.

# LÄHTEET

Digitoday. 2013 a. NSA vakoilee suoraan Microsoftin, Applen, Googlen ja Yahoon keskuspalvelimilla. Saatavilla: http://www.digitoday.fi/tietoturva/2013/06/07/nsa-vakoilee-suoraan-microsoftin-applen-googlen-ja-yahoon-keskuspalvelimilla/20138079/66 (Luettu 25.10.2014)

Digitoday. 2013 b. Nämä tiedot iPhone-, Lumia- ja Android-puhelimet välittävät yhdysvaltoihin. Saatavilla: http://www.digitoday.fi/tietoturva/2013/06/15/nama-tiedot-iphone--lumia--ja-android-puhelimet-valittavat-yhdysvaltoihin/20138379/66 (Luettu 25.10.2014)

Express Technology. 2014. What is Named Instance and Default Instance? Saatavilla: http://www.expresstechnology.com/support/knowledge-base/46-sql-database-server/206-what-is-named-instance-and-default-instance (Luettu 20.3.2014)

Haikala N. 2014. Kiinasta kajahtaa: Xiaomi kiilasi maailman suurimpien älypuhelinvalmistajien kärkikolmikkoon. Mobiili.fi. Saatavilla: http://mobiili.fi/2014/10/30/kiinasta-kajahtaa-xiaomi-kiilasi-maailman-suurimpien-alypuhelinvalmistajien-karkikolmikkoon/ (Luettu 28.10.2014)

Lehtiniitty M. 2014. Samsung sekä Apple ottivat turpaan alypuhelinten markkinaosuuksissa - voittajia ovat nyt muut. Mobiili.fi. Saatavilla: http://mobiili.fi/2014/04/29/samsung-seka-apple-ottivat-turpaan-alypuhelinten-markkinaosuuksissa-voittajia-ovat-nyt-muut (Luettu 28.10.2014)

Paunonen R. 2014. Vaara vaanii älyluuria. Savon Sanomat 28.7.2014, 14

Pitkänen M. 2014. FBI-pomo on huolissaan Android L:n ja iOS 8:n uusista salausominaisuuksista. AfterDawn. Saatavilla: http://fin.afterdawn.com/uutiset/artikkeli.cfm/2014/09/26/fbi-pomo-on-huolissaan-android-l-n-ja-ios-8-n-uusista-salausominaisuuksista?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+afterdawn_uutiset+%28AfterDawn+-+Uutiset%29&utm_content=Google+International (Luettu 20.10.2014)

Puska M. 2005. Langattomat lähiverkot. Helsinki: Talentum Media Oy.

Sajari P. 2014. Nokian Lumia-puhelin vuotaa tietoja ulkomaille. Helsingin Sanomat. Saatavilla: http://www.hs.fi/sunnuntai/a1393046974949 (Luettu 20.10.2014)

Salmenkivi S. 2012. Digitaalitodellisuus. Helsinki: Talentum Media Oy.

Salo I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo Oy.

Symantec. 2014. Symantec Mobile Management. Saatavilla: http://www.symantec.com/mobile-management/trialware (Luettu 20.3.2014)

Symantec. 2011 a. Symantec Management Platform 7.1 SP2 Installation Guide. Saatavilla: http://kbdownload.symantec.com/resources/sites/BUSINESS/content/live/DOCUMENTATION/4000/DOC4798/en_US/SMP_install_gde.pdf?__gda__=1405950909_083286960291734a745160c9805bc6bf (Luettu 21.7.2013)

Symantec. 2011 b. Symantec Mobile Management 7.2 SP3 Implementation Guide. Saatavilla: http://www.symantec.com/business/support/index?page=content&id=DOC6826 (Luettu 21.7.2013)

TARVITTAVAT IIS-ROOLIN PALVELUT

- HTTP Redirection
- Logging Tools
- Tracing
- Basic Authentication
- Windows Authentication
- Digest Authentication
- Client Certificate Mapping Authentication
- IIS Client Certificate Mapping Authentication
- URL Authorization
- IP and Domain Restrictions
- Dynamic Content Compression
- IIS Management Scripts and Tools
- Management Service
- IIS-6 Management Compatibility

SYMANTEC MANAGEMENT PLATFORMIN JA MOBILE MANAGEMENTIN JÄRJESTELMÄVAATIMUKSET

| **Laitteisto** | **Minimaaliset vaatimukset testausta varten** | **Suositukset pienelle yritykselle** | **Suositukset suurelle yritykselle** |
|---|---|---|---|
| CPU | Tuplaydinprosessori | Kaksi tuplaydinprosessoria | Kaksi neliydinprosessoria |
| CPU Nopeus | 1.8 GHz | 2.53 GHz | 2.53 GHz |
| RAM-muisti | 1.5 GB | 4 GB, DDR2 | 8 GB, DDR2 |
| Kovalevy | 15 GB vapaata tilaa | 15 GB vapaata tilaa | 15 GB vapaata tilaa |
| **Ohjelmisto** | | | |
| Käyttöjärjestelmä | Microsoft Windows Server 2008 R2 | Microsoft Windows Server 2008 R2 | Microsoft Windows Server 2008 R2 |
| Tietokanta | Microsoft SQL Server 2005 tai 2008 Express | Microsoft SQL Server 2005 tai 2008 Standard tai Enterprise yli 500:lle hallittavalle laitteelle | Microsoft SQL Server 2005 tai 2008 Enterprise |
| Adobe Flash Player 10 tai uudempi | Jotkin ominaisuudet vaativat Adobe Flash Playerin | | |
| Microsoft Silverlight 3.0 tai uudempi | Jotkin ominaisuudet vaativat Microsoft Silverlightin | | |