Antti Öhman

COMODO ONE MSP -OHJELMISTON ESITTELY JA KÄYTTÖÖNOTTO

Tietojenkäsittelyn koulutusohjelma

2017

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

COMODO ONE MSP -OHJELMISTON ESITTELY JA KÄYTTÖÖNOTTO

Öhman, Antti
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Joulukuu 2017
Ohjaaja: Hentunen, Ilmari
Sivumäärä: 47
Liitteitä: 0

Asiasanat: ITSM, etähallinta- ja monitorointi, korjaustenhallinta, pilvilaskenta, Comodo

---

Opinnäytetyön tarkoituksena on esitellä yhdysvaltalaisen Comodo Groupin kehittämää ja ylläpitämää Comodo One -ohjelmistoa, joka on suunniteltu IT-palveluntarjoajille ja sen tarkoituksena on keskittää kaikki mahdolliset IT-palvelut yhdeksi kokonaisuudeksi.

Opinnäytetyössä käydään läpi Comodo Onen käyttöönotto palveluun rekisteröitymisestä sen muokkaamiseen omien tarpeiden mukaan, jotka ovat tässä tapauksessa ITSM, etähallinta- ja monitorointi sekä korjaustenhallinta. Opinnäytetyössä käsitellään asiakkaiden eri laitteiden lisäämistä palveluun yksittäin, jotka ovat tässä tapauksessa Windows-, macOS, Linux- sekä Android-laitteet, sekä Windows-laitteiden lisäämistä palveluun hyödyntäen aktiivihakemistoa. Kerron myös, miten luodaan ITSM-profiileja asiakkaille ja mitä ominaisuuksia ne pitää sisällänsä.

Opinnäytetyössä esittelen myös Comodo RMM Administration -ohjelmaa, jonka avulla pystytään hallitsemaan ja monitoroimaan asiakkaiden laitteita, jotka sijaitsevat palveluntarjoajan ITSM-sovelluksessa.

COMODO ONE MSP SOFTWARE INTRODUCTION AND DEPLOYMENT

Öhman, Antti
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in information technology
December 2017
Supervisor: Hentunen, Ilmari
Number of pages: 47
Appendices: 0

Keywords: ITSM, remote monitoring and management, patch management, cloud computing, Comodo

---

The purpose of this thesis is to present Comodo One software developed and maintained by Comodo Group Inc. It's designed for Managed Service Providers (MSPs) for centralizing all possible IT services into a single entity.

The thesis deals with the introduction of Comodo One from registration of the service to modifying it according to MSP's own needs, in this case ITSM, remote management and monitoring and patch management. The thesis also deals with adding customers different devices to the service one by one, which are in this case Windows, macOS, Linux and Android devices and adding Windows devices to the service using Active Directory. I will also explain how to create ITSM profiles for customers and what features they have.

In this thesis I will also present Comodo RMM Administration Console software which enables to manage, and monitor customers devices located in the ITSM application of the service provider.

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön aiheena on yhdysvaltalaisen Comodo Group Inc:n. Comodo One -ohjelmiston käyttöönotto ja sen ITSM-sovelluksen jakaminen asiakkaiden laitteille sekä sen etähallinta- ja monitorointi-sovelluksen ja korjaustenhallinta-sovelluksen käyttöönotto ja esittely. Kahdesta edellä mainitusta sovelluksesta kerron myös miten käyttöönotto tapahtui, kun ne olivat vielä erillisiä sovelluksia, eikä osana ITSM-sovellusta. Kerron myös opinnäytetyössäni, mitä tarkoittaa ITSM, RMM sekä Patch Management.

Opinnäytetyöllä ei ollut toimeksiantajaa, mutta olen käyttänyt kyseistä ohjelmistoa nykyisessä työssäni, joten tämän opinnäytetyön avulla halusin avata itselleni ja mahdollisesti muille ohjelmistosta kiinnostuneille enemmän sen käyttöönottoa sekä muita ominaisuuksia, joita ohjelmisto tarjoaa.

Lopuksi käyn läpi Comodo Onen huonoja puolia sekä mitä itse jäin kaipaamaan ohjelmistosta verrattuna vastaaviin maksullisiin ohjelmistoihin. Kerron oman näkemykseni läpi käytäviin Comodo One-sovelluksiin muun muassa mitä hyviä sekä huonoja puolia niissä havaitsin ja mitä Comodo mainitsee EULA:ssa käyttäjädatan keräämisestä, kun kyseessä on ilmainen ohjelmisto.

2 ITSM

ITSM (IT Service Management) eli IT-palvelunhallinta tarkoittaa, miten yritys tai palveluntarjoaja hallitsee asiakkaidensa tietojärjestelmiä. ITSM voi sisältää erilaisia toimenpiteitä, kuten esimerkiksi muutoksien suunnittelun ja niiden hallinnan, jotta ne eivät aiheuta liiketoiminnan häiriöitä, korjaavat asioita, kun ne eivät mene oikein tai ne hallinnoivat budjettia, jotta yritys tai organisaatio voi maksaa laskujaan niiden saapumisen yhteydessä. ITSM-termiä käyttävät yritykset ja organisaatiot ajattelevat

tietotekniikkaa keinona tarjota arvokkaita palveluita asiakkailleen eikä keinona hallita tietotekniikkaa. (Rance 2017.)

IT-palveluhallinnan avainprosesseina voidaan pitää palvelujen määrittämistä, muutoksien hallintaa sekä tapahtumien hallintaa. Näistä kolmesta avainprosessista pääavain on palvelujen määrittely, sillä se mahdollistaa sekä asiakkaan että palvelutarjoajan tietävän, mitä he voivat tai eivät voi palvelusta odottaa. Selkeästi määritellyt palvelut kertovat asiakkaille palveluista, mukaan lukien mitä kukin palvelu pitää sisällään ja ei pidä sisällään, niiden kelpoisuuden asiakkaan tarpeisiin, palveluiden rajoitukset, niiden kustannukset, niiden pyytämisen sekä mistä niihin saadaan tarvittavaa apua. Vakiintunut palvelu tunnistaa myös sisäiset prosessit, jotka ovat tarpeen palvelun tarjoamiseksi ja tukemiseksi. (University of California, Santa Cruz 2015.)

Jokaisella asiakaslähtöisellä palvelulla pitäisi olla vähintään korkeatasoinen palvelumääritelmä. Seuraavien viiden kysymyksen vastaukset auttavat määrittämään palvelun:

Asiakasta koskevat kysymykset:

1. Mikä on palvelu ja mistä sen voi hankkia? (palvelun kuvaus)
2. Mistä saa apua ja miten palvelua käytetään? (Apu ja itsepalvelu)
3. Paljonko palvelu maksaa? (Palvelukustannukset ja hinnoittelu)

ITS (sisäistä) koskevat kysymykset

4. Miten ITS tukee kyseisiä palvelua? (Huoltotuki)
5. Miten ITS tulee tarjoamaan kyseisen palvelun? (Palvelun tuottaminen) (University of California, Santa Cruz 2015.)

Muutoksen hallinta auttaa varmistamaan, että asiakasriskiin vaikuttavien muutoksien riski minimoidaan. Muutoksen hallinnan elementtejä ovat

- Vaikutusten arviointi: soveltamisala ja vaikutus
- Testaus- ja takaisinottosuunnitelmat
- Viestintä (University of California, Santa Cruz 2015.)

Tapahtuma IT-palvelunhallinnassa on mikä tahansa tapahtuma, joka aiheuttaa palvelun odottamattoman keskeyttämisen tai vähentämisen. Onnettomuudenhallinnan tavoite on normaalien toimintojen palauttaminen mahdollisimman nopeasti, mahdolli-

simman pienillä häiriöillä asiakkaille. UCSC:ssä, tapahtumien hallinta -ohjelma vaikuttaa yhden vikatiketin hoitamisesta koko järjestelmän huoltokatkoon. (University of California, Santa Cruz 2015.)

Monilla pienyrityksillä on harvoin omaa IT-osastoa vaan IT-palvelujenhallinta ulkoistetaan ulkopuoliselle yritykselle, joka hoitaa pienyritykselle ympäristön kartoittamisen ja sen pohjalta toimittaa pienyritykselle tarvittavan laitteiston, esimerkiksi tietokoneet, näytöt, palvelimet, verkkolaitteet, monitoimilaitteet, tarvittavat ohjelmistot jne. Samalla voidaan laatia laitteille sekä ympäristölle ylläpitosopimus, joka kattaa esimerkiksi asiakkaan ympäristön ylläpidon aina verkkolaitteista asiakkaan käyttämiin liiketoiminnan kannalta tärkeisiin ohjelmistoihin sekä valtakirjan, jossa asiakasyritys vakuuttaa palveluntarjoajan luvan hoitaa heidän yrityksensä tilauksia liittyen esimerkiksi puhelin- ja internetliittymiin. Tämä takaa sen, että pienyrittäjän ei tarvitse huolehtia liikaa alueesta, josta hän ei ymmärrä mitään ja myös sen, että hänen ympäristönsä pysyy ajan tasalla.

Yleensä palveluntarjoaja voi asentaa asiakkaidensa laitteilla ohjelmiston, kuten esimerkiksi Comodo ITSM:n, jonka avulla he voivat hallita asiakkaiden laitteita sekä asiakas voi halutessaan lähettää palveluntarjoajalle tiketin, jossa hän ilmoittaa laitteessansa tai ympäristössään olevan ongelman palveluntarjoajan IT-tuelle, jonka kautta he saavat apua ongelmiinsa. Ohjelmiston avulla palveluntarjoaja voi myös seurata asiakkaan laitteen tilaa ja ilmoittaa asiakkaalle, onko hän havainnut laitteessansa mitään tavallisesta poikkeavaa tai hän voi kertoa, että asiakkaan laite alkaa olemaan jo niin vanha, että se kannattaisi vaihtaa.

3 RMM

Etähallinta ja -monitorointi (Remote Monitoring and Management) on pääte- ja verkonvalvontaohjelmisto tai etähallintaohjelmisto, jonka avulla palveluntarjoajat tai järjestelmänvalvojat voivat seurata ja hallita päätepisteitä, tietokoneita, mobiililaitteita ja verkkoja etäyhteydellä keskitetystä konsolista. RMM-ohjelma asennetaan yleen-

sä ”agenttina” (pieni ohjelmisto jalanjälki) asiakkaan järjestelmiin, työasemiin, palvelimiin, mobiililaitteisiin jne. (Comodo Group Inc. www-sivut 2017a.)

Etähallinta- ja -monitorointiohjelmistojen päätoimintoja ovat:

- Ajantasaiset tiedot käyttäjien ohjelmistojen päivityksistä ja verkkojen tilasta
- Kalustaa palveluntarjoajan viimeisimmän tiedon ja toiminnan avulla
- Heti saatavilla olevat tiketit, kun agentti havaitsee ongelman loppukäyttäjän laitteessa
- Käyttäjien verkon ja laitteen tilan ja terveyden yhdenmukainen valvonta
- Seurata samanaikaisesti useita asiakkaita ja päätepisteitä. (Comodo Group Inc. www-sivut 2017a.)

Etähallinta ja -monitorointiohjelmistojen hyviä puolia ovat muun muassa:

- Ne auttavat havainnollistamaan ongelmia ja ratkaisemaan niitä ennen kuin niistä tulee isoja ja ne aiheuttavat järjestelmän epävakautta
- Ne auttavat pienyrityksiä ottamaan suunnan kohti suuryritystason automaatiota ja monitorointia
- Ne alentavat IT-palveluntarjoajien käyntiä ja niihin liittyviä kustannuksia
- Ne auttavat asiakasyrityksiä hallinnoimaan heidän IT-ongelmia kiinteää hintaa vastaan
- Ne varmistavat verkon vakauden ennakoivan ylläpidon ansiosta
- Ne varmistavat suuremman voittomarginaalin sekä häiritsemättömät palvelut, koska ongelmia esiintyy vähemmän
- Ne kasvattavat asiakastyytyväisyyttä, mikä johtaa asiakasuskollisuuteen
- Ne parantavat tuottavuutta sekä järjestelmänvalvojille, että loppukäyttäjille
- Ne auttavat palveluntarjoajia laajentamaan asiakaskuntaa tarjoamalla asiakkaille 24/7 kattavuutta ja tukea
- Ne tarjoavat loppukäyttäjille parannettua käytettävyyttä ilman häiriöitä palvelun aikana. (Comodo Group Inc. www-sivut 2017a.)

RMM-ohjelmissa on mahdollista avata etäyhteys asiakkaan laitteelle ja suorittaa eri toimenpiteitä. Yksinkertaisin näkymä on, että RMM-sovellus avaa erillisen ikkunan haluttuun laitteeseen, jonka jälkeen voidaan valita työkalu, jota halutaan

käyttää. Yleisimpiä työkaluja ovat tiedostojen siirto laitteelta toiselle sekä etätyöpöytäyhteys.

Tiedostojen siirrossa näkyy yleensä ikkunassa vasemmalla IT-tukihenkilön laite, jolla on otettu yhteys asiakkaan laitteeseen ja oikealla puolestaan asiakkaan laite. Yleensä, jos kyseessä on kahden Windows-laitteen välinen etäyhteys, RMM-ohjelmat avaavat auki molempien laitteiden C: asemat, joista pystytään navigoimaan lähetettävän tiedoston sijaintiin sekä sijaintiin, jonne se halutaan lähettää. Jotkut RMM-ohjelmat mahdollistavat myös tiedostojen siirron asiakkaan laitteelta IT-tukihenkilön laitteelle, esimerkiksi Comodon RMM Administration Console mahdollistaa tämän ominaisuuden.

Etätyöpöytäyhteyden avulla IT-tukihenkilö pääsee näkemään reaaliajassa asiakkaan laitteen työpöydän sekä asiakkaan ilmoittaman ongelman laitteessaan tarkemmin, sillä yleensä kun asiakas ilmoittaa esimerkiksi virheestä, IT-tukihenkilö ei välttämättä saa tarkkaa käsitystä mistä virheestä on kysymys ja mikä on sen aiheuttanut. Yleensä kun IT-tukihenkilö kysyy, että mitä asiakas on tehnyt ennen virhettä, yleisimmät vastaukset ovat joko ”En muista enää tarkalleen…” tai ”En ainakaan mitään väärää, käytin ohjelmaa ihan niin kuin ennenkin…”. Etätyöpöytäyhteyden avulla IT-tukihenkilö pystyy ratkomaan asiakkaan laitteessa olevat ongelmat helposti verrattuna puhelintukeen, mutta puhelintuen hankaluuteen liittyy yleensä asiakkaan pohjatieto liittyen tietotekniikkaan, asiakkaan tietämys omaan laitteeseensa, asiakkaan motivaatio ratkaista ongelmaa puhelinitse IT-tukihenkilön kanssa jne. Tämän takia etätyöpöytäyhteydestä hyötyy molemmat osapuolet, IT-tukihenkilö näkee tilanteen paremmin, jonka jälkeen hän lähtee ratkaisemaan asiakkaan ongelmaa sekä asiakkaan ei tarvitse olla ongelmanratkojana paikan päällä ja mikäli hänellä on tiedossa joitain muita työtehtäviä, joihin hän ei tarvitse laitettaan, asiakas voi sopia IT-tukihenkilön kanssa soitosta hänelle, kun ongelma on ratkaistu sekä selitys ongelman aiheuttajalle ja miten siltä voitaisiin välttyä jatkossa.

Etätyöpöytäyhteys mahdollistaa ohjelmien asentamisen etäältä asiakkaan laitteeseen sekä palvelimiin. Vaikka asiakas saa ohjelmiston valmistajalta tarkat ohjeet asennukseen, yleensä hän kokee jollakin tavalla, että hän saa ohjelman asennettua

ainoastaan väärin ja antaa mieluummin tehtävän esimerkiksi IT-palveluita tarjoavalle yritykselle. Hyvä esimerkki on ranskalaisen Dassault Systèmesin SolidWorks-ohjelma, joka on CAD-ohjelma. SolidWorksista pitää asentaa palvelimelle ns. lisenssirooli, josta asiakkaan laitteiden SolidWorks-ohjelma tarkistaa lisenssit ja niiden voimassaolot. Mikäli päivitetään asiakkaan laitteen SolidWorks uudempaan versioon ennen kuin ollaan päivitetty lisenssiroolia palvelimelta, tuotteen aktivointi ei onnistu. Dassault Systèmes on antanut tarkat ohjeet ohjelmistonsa päivittämiseksi uuteen versioon, mutta asiakkaat eivät yleensä halua koskea niin kriittiseen laitteeseen kuin palvelin, joten etätyöpöytäyhteyden avulla IT-tukihenkilö päivittää SolidWorkisin lisenssiroolin helposti, jonka jälkeen hän voi asentaa asiakkaan laitteelle ohjelmasta uuden version.

4 PATCH MANAGEMENT

Korjaustenhallinta on prosessi, jonka avulla voidaan hankkia, testata ja asentaa useita korjaustiedostoja (koodimuunnoksia) olemassa oleviin sovelluksiin ja ohjelmistotyökaluihin, mikä mahdollistaa järjestelmien pysymään ajan tasalla olemassa olevien korjaustiedostojen kanssa ja määrittämään, mitkä korjaustiedostot ovat sopivia. Laitteiden hallinta on helppoa ja yksinkertaista. (Comodo Group Inc. www-sivut 2017b.)

Korjaustenhallinta on käytössä enimmäkseen ohjelmistoyrityksissä osana heidän sisäisiä pyrkimyksiään ratkaista ongelmia eri ohjelmistoversioiden kanssa sekä auttaa analysoimaan olemassa olevia ohjelmia ja havaita mahdollisten turvaominaisuuksien tai muiden päivitysten mahdolliset puutteet. (Comodo Group Inc. www-sivut 2017b.)

Korjaustenhallinta on myös hyvä tapa IT-palveluntarjoajille hallita asiakkaidensa laitteiden päivittämistä. Yleensä asiakkaat pitävät laitteissansa päällä automaattisen päivittämisen, koska he eivät joko tiedä, mistä sen saa otettua pois päältä tai sen takia, että heitä ei kiinnosta mitä päivitykset pitävät sisällänsä, kunhan laite pysyy ajan tasalla. Tämä voi johtaa viallisten päivitysten latautumiseen sekä asentumiseen asiakkaan laitteella, jonka jälkeen syntyy ongelmia. Korjaustenhallinnan avulla IT-tukihenkilö näkee, mitä päivityksiä asiakkaiden laitteisiin on saatavilla ja mitä ne

pitävät sisällänsä. Hän myös näkee mahdolliset vialliset päivitykset, jotka hän voi jättää asentamatta ja odottaa uusia päivityksiä, jotka korjaavat tiedettyjen viallisten päivityksien ongelmat.

Korjauksienhallinnan avulla voidaan myös määritellä, minkä ohjelmistojen päivityksiä halutaan asentaa. Esimerkiksi Comodo Onen ITSM-sovelluksen korjaustenhallinta tunnistaa kaikki ne asiakkaiden laitteilla olevat ohjelmistot, jotka Comodo Group on määrittänyt tietokantaansa. Sovelluksessa voidaan myös rajata tarkemmin päivitettävät ohjelmistot kuten esimerkiksi ohjelmistot, joita asiakas käyttää eniten.

5 COMODO ONE MSP

5.1 Mikä on Comodo One MSP?

Comodo One MSP on yhdysvaltalaisen Comodo Group Inc. luoma IT-hallinta-ohjelmisto, joka koostuu Comodo Groupin omista tuotteista joita palveluntarjoaja tai yritys voi lisätä omaan tiliinsä tarpeen mukaan. Comodo One on SaaS-palvelu (Software as a Service).

Comodo One antaa asiakkailleen mahdollisuuden kasvattaa liiketoimintaansa ja kehittää asiakaskuntaa asettaessaan IT-haasteet ja tekemällä niistä entistä tuottavampia. Tämä on ratkaisu, joka on kehitetty pitämällä mielessä, että useimmilla organisaatioilla on erilainen IT-työprosessi. Comodo One voi jopa hallita MSP-infrastruktuuria, joka voi parantaa voittoa. Voit tarjota jäsenyritysten hallinnoinnit asiakkaillesi ja seurata niiden tehokkuutta etäältä, joka antaa päätepisteturvallisuuden, verkkoturvan, tietojen varmuuskopioinnin, verkonvalvonnan ja suojauksen. (Comodo Group Inc. www-sivut 2017c.)

Comodo Onen sisältävät Comodo Group Inc:n tuotteet ovat

- Comodo ITSM, joka sisältää RMM- ja Patch Management-sovellukset
- Comodo Service Desk

- Comodo Dome Shield
- Comodo Quote Manager
- Arconis Cloud Backup
- Comodo Dome Firewall
- cWatch
- Comodo CRM
- Korugan Central Manager

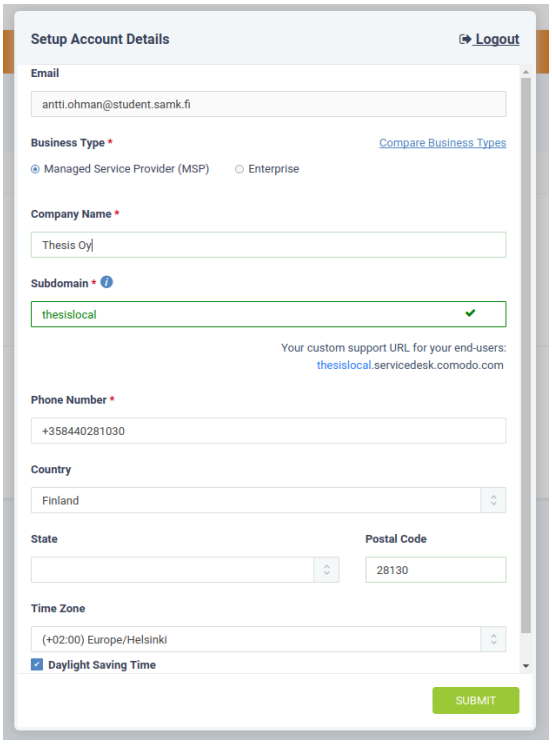
Comodo Onen vanhempi versio sisälsi myös erilliset RMM- ja Patch Management -sovellukset, mutta Comodo Group aikoo tähdätä siihen, että ITSM-sovellus korvaa nämä sovellukset, kuten on käynyt. Opinnäytetyön alkuvaiheessa RMM-sovellus oltiin jo poistettu Comodo Onen omasta kaupasta, mutta Patch Management oli vielä saatavilla, mutta se ei toiminut enää. Kysyttyäni asiaa Comodo Onen HelpDeskiltä, sain vastauksen, jossa he kertoivat, että he aikovat tehdä tuotteestaan mahdollisimman yksinkertaisen ilman montaa ylimääräistä sovellusta.

Comodo Onen tuotteista suurin osa on ilmaisia, mutta muutamat sovellukset ovat maksullisia. Näistä yksi on Arconis Cloud Backup, josta on tarjolla eri paketteja eri maksumetodeilla kuten esimerkiksi 1TB tallennustilaa joko $182,32/KK, $1,990,66/vuosi ennakkoon tai $0,23/GB käytetystä tilasta.

5.2 Comodo One MSP:n käyttöönotto

Comodo One otetaan käyttöön osoitteessa https://one.comodo.com/?s_track=7639&key5sk1=e36e5a585502d1ebbac29f1f96261dd08131dea8&afid=9360&af=9360. Sivustolta löytyy painike, missä lukee ”Get now free” ja sitä klikkaamalla päästään määrittämään yrityksen päätili palveluun. Aluksi eteen ilmestyy keskelle ruutua tekstikenttä, johon käyttäjää pyydetään syöttämään sähköpostinsa, johon haluaa palvelun määrittää. Tämän jälkeen syötetään tilille haluttu salasana ja puhelinnumero, jonka jälkeen Comodo One lähettää tilin luonnissa määritettyyn sähköpostiin varmistuksen, jonka hyväksyttyä päästään jatkamaan tilin määrittämistä.

Seuraavaksi määritetään tilin yksityiskohdat. Yksityiskohdissa määritellään, onko yritys Managed Service Provider (MSP) eli palveluntarjoaja vai Enterprise-tason yritys, yrityksen nimi ja sen aliverkkotunnus, joka tulee näkymään loppukäyttäjien laitteissa ITSM-agentissa muodossa ”aliverkkotunnus”.servicedesk.comodo.com. Yksityiskohdissa määritellään myös, missä maassa yritys sijaitsee sekä postinumero ja aikavyöhyke. Tämän prosessin päätteeksi käyttäjä ohjataan Comodo Onen kirjautumisruutuun, johon syötetään tilin sähköpostiosoite ja salasana. Tämän jälkeen eteen avautuu Comodo One MSP ohjelmiston Dashboardin, joka näyttää yleiskuvan asiakkaiden laitteista, saapuneista tiketeistä sekä pika- ja aputoiminnot (Kuva 1).



Kuva 1 Comodo One tilin luomisen yhteydessä suoritettava tilin yksityiskohtien määritteleminen.

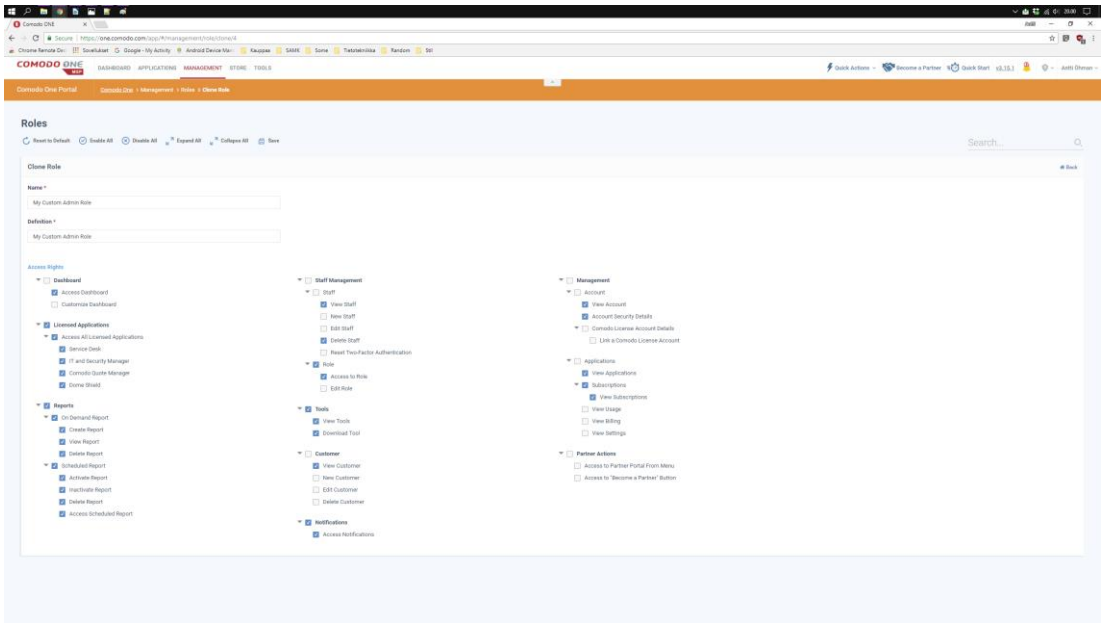
Seuraavaksi kannattaa navigoida Comodo One -kauppaan, josta voidaan ladata haluamia Comodon ohjelmistoja, joilla tullaan hallitsemaan asiakkaiden IT-palveluita. Mikäli tarvitaan ainoastaan esimerkiksi ITSM, RMM ja Patch Managementin, voidaan alkaa suoraan konfiguroimaan näitä sovelluksia, koska ne ovat oletuksena käytössä, mutta jos yritys tarjoaa asiakkailleen esimerkiksi HelpDesk -palveluita, voidaan ladata Comodo One -kaupasta Comodo Service Deskin, jotta yrityksen järjestelmänvalvojat ja teknikot pääsevät seuraamaan asiakkailta saapuvia tikettejä.

Kun tarvittavat ohjelmistot on ladattu, kannattaa seuraavaksi lisätä yrityksen olemassa olevia asiakkaita palveluun, jotta ITSM-ohjelmistossa voidaan lisätä helposti oikeat päätelaitteet oikeaan asiakkaan alle. Asiakkaita voidaan lisätä valitsemalla Dashboardista, ”Management”-välilehden - pudotusvalikosta ”Customer”. ”Customer”-osiosta valitaan ”New Customer” ja syötetään lisättävän asiakkaan tiedot, jotka ovat

- Asiakasyrityksen nimi (Pakollinen)
- Yhteyshenkilön sähköpostiosoite (Pakollinen)
- Asiakasyrityksen osoite (Pakollinen)
- Asiakasyrityksen postinumeron (Pakollinen)
- Kuvaus (Vapaaehtoinen)

Asiakkaat tulevat näkymään automaattisesti ITSM-sovelluksessa lisäyksen jälkeen.

Halutessaan voidaan lisätä yrityksen työntekijöitä ja antaa heille oletusroolit (Admin tai Technician) valitsemalla ”Management”-välilehden pudotusvalikosta ”Staff”. Halutessaan voidaan myös luoda omia rooleja, joihin voidaan määritellä mihin Comodo One toimintoihin roolin omaavalla käyttäjällä on oikeus. Uuden profiilin voi luoda valitsemalla ”Management”-välilehden pudotusvalikosta ”Roles”, josta kloonataan oletusrooli, jonka jälkeen sille annetaan haluamat oikeudet (Kuva 2).



Kuva 2 Esimerkki uuden Admin-tyypin roolin määrittämisestä yrityksen MSP-tiliin.

Näiden edellä mainittujen vaiheiden jälkeen voi halutessaan muokata yrityksen MSP-tilin tietoja ”Management”-välilehden pudotusvalikon kohdasta ”Account” tai hallita MSP-tilin ohjelmistoja valitsemalla ”Applications”. Muuten tässä vaiheessa Comodo One MSP -ohjelmisto on valmis käytettäväksi.

6 COMODO ITSM

Comodo ITSM on Comodo Onen oletussovellus, joka on kaikissa Comodo One-tileissä ja sitä ei voida poistaa yrityksen Comodo One -tilistä. Comodo ITSM:n avulla voidaan pitää listaa asiakkaiden laitteista sekä seurata niiden tilaa ja tarvittaessa voidaan asentaa päivityksiä ja määrittää niihin ITSM-profiileja. ITSM-sovellus mahdollistaa myös asiakkaille tikettien lähettämisen palvelutarjoajan sähköpostiin tai Comodo Service Desk -sovellukseen.

Comodo ITSM yksinkertaistaa kaikki IT- ja tietoturvahallintatarpeesi yhdeksi yhtenäiseksi konsoliksi, mikä tehostaa toimintaa ja vähentää riskejä Android-, iOS- ja Windows-laitteilla. Comodo IT- ja tietoturvahallinta tarjoaa yhtenäisen konsolikojelaudan kaikista laitteista ja niiden tilasta. IT-ylläpitäjät voivat helposti toimia ongelmatilanteissa; raportoida nykyisistä riskeistä ja jakaa muutoksia yrityslaajuisesti. ITSM yhdistää tietotekniikan omaisuudenhallinnan ja tuen kattavan profiileihin perustuvan yritysturvallisuuden avulla. Tuotteen päällekkäisyydet ja useat hallintavälineet antavat rajoitetun näkyvyyden ja mahdolliset suojauserot. Nykyään Comodo on integroinut nämä kriittiset komponentit yhdeksi, yhtenäiseksi konsoliksi Advanced Endpoint Protection -ympäristöön. (Comodo Group Inc. www-sivut 2017d.)

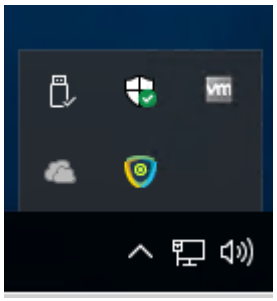
6.1 Asiakkaan laitteen lisäys palveluntarjoajan ITSM-sovellukseen

6.1.1 Windows -laitteet

Kun halutaan lisätä asiakkaan laite palveluntarjoajan Comodo ITSM-sovellukseen, tulee olla palveluntarjoajalla pääsy asiakkaan laitteeseen esimerkiksi käyttämällä TeamVieweriä, ottamalla RDP-yhteys asiakkaan laitteeseen tai olemalla fyysisesti paikalla. Vaihtoehtoisesti laitteen lisäyksessä palvelutarjoajan teknikko tai järjestelmänvalvoja voi lähettää sähköpostitse asiakkaalle ohjeet, miten hän saa laitteensa lisättyä palvelutarjoajansa ITSM-sovellukseen.

Comodo ITSM-sovellukseen voidaan lisätä asiakkaiden Windows-, macOS-, Linux-, Android- ja iOS-laitteita. ITSM-sovellus avataan valitsemalla Dashboardista ”Applications”-välilehden pudotusvalikosta ”IT and Security Manager” ja ”Device Management”, jonka jälkeen eteen avautuu ITSM:n laitelista. Laitelistassa on lueteltuna palvelutarjoajan asiakkaat, jotka ollaan lisätty Comodo Oneen. Ennen kuin lähdetään lisäämään asiakasyrityksen laitteita ITSM-sovellukseen, kannattaa luoda eri ryhmiä laitteille, esim. Servers, Workstations, Mobile Devices jne., jotta laitteiden löytäminen on helpompaa. Uuden ryhmän saa luotua valitsemalla ”Group Management” ja sieltä ”Create Group”, jonka jälkeen annetaan ryhmälle nimi, minkä asiakasyrityksen alle ryhmä luodaan ja vapaaehtoinen kuvaus ryhmästä.

Tämän jälkeen asiakkaan laite lisätään ITSM-sovelluksesta valitsemalla ”Device Management” ja ”Enroll Device”. Tämän jälkeen seuraavaksi valitaan laitteen omistaja, joka on esimerkiksi sähköpostiosoite etunimi.sukunimi@example.com sekä päätetään, näytetäänkö laitteen rekisteröintiohjeet ITSM-palvelussa vai lähetetäänkö ne sähköpostilla valitulle käyttäjälle. Valitsemalla ”Show enrollment instructions” ITSM tuo eteen ohjeet, miten eri laitteet lisätään palveluun. Windows laitteilla kannattaa valita suoraan rekisteröinti linkin kautta, jota klikkaamalla Windows-laitteelle avautuu linkin generoima .msi-asennuspaketti, jonka suorittamisen jälkeen Windows-laite on rekisteröity palveluntarjoajan ITSM-sovellukseen (Kuva 3).



Kuva 3 Windows-laitteen onnistuneen rekisteröinnin jälkeen ITSM näkyy tehtäväpalkin piilotetuissa kuvakkeissa. Kuvaketta klikkaamalla pääsee näkemään palvelutarjoajan palvelinasetukset. ITSM-kuvake on piilotettujen kuvakkeiden toisella rivillä keskellä.

6.1.2 Apple-laitteet

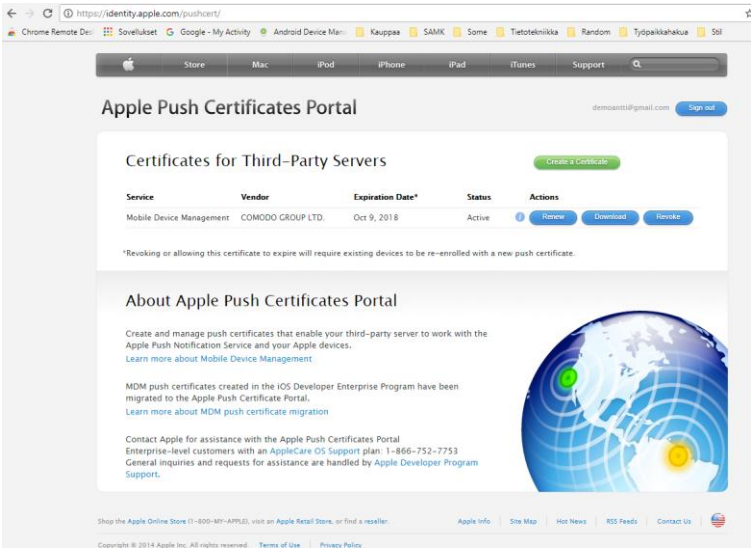
MacOS-laitteiden lisäämistä varten täytyy palvelutarjoajan luoda omaan ITSM-sovellukseen APNs-sertifikaatti (Apple Push Notification).

Apple Push Notification -palvelu on etäilmoitusominaisuuden keskeinen osa. Se on vankka, turvallinen ja tehokas palvelu sovellusten kehittäjille, jotka levittävät tietoja iOS:lle (ja epäsuorasti watchOS:lle), tvOS:lle ja macOS-laitteille. (Apple, Inc www-sivut 2017.)

Kun halutaan luoda palveluntarjoajan ITSM-sovelluksesta asiakasyritykselle APNs-sertifikaatti, tulee navigoida ITSM-sovelluksesta ”Settings”, ”Portal Set-Up” ja ”APNs Certificate”, jonka alta löytyy ohjeet, miten luodaan APNs-sertifikaatti. Ensimmäisenä tulee ladata Comodon allekirjoittama Apple PLIST -tiedosto (Property List), jota tarvitaan APNs-sertifikaatin luomisessa.

PLIST-tiedostot ovat joustavia ja ne ovat käteviä sovellustietojen tallentamiseen. Alun perin Apple määritteli niitä käytettäväksi iPhone-laitteissa ja myöhemmin se levisi muihin Applen-laitteisiin ja sovelluksiin. PLIST-tiedostot ovat itse asiassa XML-tiedostoja, joten voit käyttää yksinkertaista tekstieditoria kääntääksesi niitä. Tämä on kuitenkin hankalaa, sillä jopa yksi merkki väärässä paikassa tekee tiedostosta käyttökelvottoman. (ICanLocalizen www-sivut 2017.)

Kun tiedosto ollaan saatu ladattua työasemalle, pitää seuraavaksi kirjautua Apple Push Certificate Portal -palveluun käyttämällä Apple ID:tä osoitteesta https://identity.apple.com/pushcert/. Kirjautumisen jälkeen valitaan ”Create a Certificate”, jonka jälkeen käyttäjän tulee hyväksyä Applen käyttöehdot. Ehtojen hyväksymisen jälkeen valitaan Comodon .PLIST-tiedosto ja klikataan ”Upload”, jonka jälkeen Apple Push Certificates Portal luo APNs-sertifikaatin ITSM-sovellusta varten ja se on heti ladattavista Apple Push Certificates Portalin etusivulta, josta kyseisen sertifikaatin pystyy myös uusimaan tarvittaessa. Sertifikaatin latauksen jälkeen palataan takaisin Comodon ITSM-sovellukseen ja valitaan APNs Certificate-välilehden alta ”Browse” ja navigoidaan kansioon, johon käyttäjän laitteen käyttämä käyttöjärjestelmä tallentaa ladatut tiedostot, valitaan APNs-sertifikaatti, jonka jälkeen sen pitäisi näkyä palvelussa. Tämän jälkeen Apple-laitteiden lisääminen ITSM-sovellukseen on mahdollista. (Kuva 4).



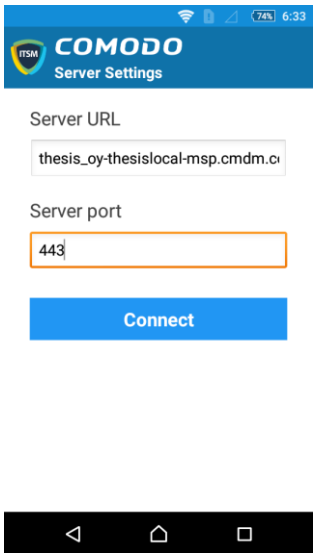
Kuva 4 Apple Push Certificate Portal, jonka etusivulla näkyy luotu Comodon sertifikaatti.

Apple-laitteet lisätään samasta paikkasta kuin Windows-laitteet, mutta valitaan kohta ”For Apple Devices” ja linkki, jonka edellä lukee ”Enroll opening the following link with any browser on your device”. Tämä linkki lataa lisättävälle Apple-laitteelle .profile-tiedoston, joka sisältää asiakasyrityskohtaisen ITSM:n profiilin. Klikkaamalla sitä, avautuu Apple-laitteen ”System Preferences”-ohjelman osio ”Profiles”, josta asennetaan Comodo ITSM-profiili. Asennuksessa laite kysyy, että halutaanko tähän

laitteeseen asentaa profiili nimeltään ”Comodo ITSM”, johon vastataan ”kyllä” ja syötetään kirjautuneen käyttäjän salasana. Hetken kuluttua laite kysyy vielä kerran, että oletko aivan varma profiilin asentamisesta, sillä tämän kyseisen osoitteen admin pystyy etäältä tarkkailemaan tätä Macia, tähän vastataan ”Install”. Tämän jälkeen Apple -laite tulee näkymää palveluntarjoajan ITSM-sovelluksessa. Jos käytössä on Apple -laite, joka käyttää Mac OS X (nyk. macOS) tulee järjestelmänvalvojan asentaa vielä erikseen ITSM-sovellus, jonka saa .profile-linkin alta ITSM-sovelluksesta. Tämän avulla järjestelmänvalvoja näkee vielä asennetut sovellukset, pystyy asentamaan sekä tarkkailemaan macOS -pakettien asennusta, joka ei ole mahdollista ilman ITSM-agenttia.

6.1.3 Android-laitteet

Lisätäkseen Android-laitteen palveluntarjoajan ITSM-palveluun, tulee ladata ensimmäisenä Googlen Play -kaupasta Comodo Client -sovellus, joka on ITSM-sovelluksen agentti Android-laitteille. Android-laitteen voi rekisteröidä Comodo One ITSM -sovelluksen ”Enroll Device” kautta käyttämällä Android-laitteille määriteltyä linkkiä, mutta helpompi tapa on määritellä palveluntarjoajan ITSM-asetukset syöttämällä ne manuaalisesti Comodo Client -ohjelmaan. Manuaaliseen määrittämiseen tarvittava tieto löytyy ITSM-sovelluksesta ”Enroll Devicen” alta, josta löytyy manuaaliseen määrittämiseen tiedot kaikille alustoille. Comodo Client pyytää syöttämään isännän URL-osoitteen sekä portin tiedot. Portti on aina 443, mutta isäntä määräytyy aina palvelutarjoajakohtaisesti esimerkiksi thesis_oy-thesislocal-msp.cmdm.comodo.com. Tietojen syötön jälkeen Comodo Client yhdistää Android-laitteen ITSM-sovellukseen ja se tulee näkyviin ITSM:n laitelistaan (Kuva 5).



Kuva 5 Esimerkki Comodo Clientin manuaalisesta määrityksestä Android-puhelimeen.

6.1.4 Linux-laitteet

Lisätessä Linux-laitteita ITSM-sovellukseen tulee suorittaa Comodo Groupin luoma bash-skripti, jonka saa ”Enroll Devicesta” otsikon ”For Linux Devices” alta olevasta linkistä. Skriptille tulee antaa oikeus suorittamiseen avaamalla Linuxin komentotulkin, navigoimalla sijaintiin johon skripti on tallennettu (oletuksena /home/käyttäjä/Downloads) ja antamalla komento chomd +x {$installation file$}. Tämän jälkeen ajetaan bash-skripti komennolla sudo ./{$installation file$}, jonka päätteeksi skripti kertoo suorittamisen onnistuneen ja Linux-laite näkyy palvelutarjoajan ITSM-sovelluksessa (Kuva 6).

```
[root@CentOS Downloads]# chmod +x itsm_dxfexpcZ_installer.run
[root@CentOS Downloads]# sudo ./itsm_dxfexpcZ_installer.run
Verifying archive integrity... All good.
Uncompressing Linux ITSM Agent  100%
systemd system
dxfexpcZ
Created symlink from /etc/systemd/system/multi-user.target.wants/itsm.service to /etc/systemd/system/itsm.service.
./itsm-linux: /lib64/libcurl.so.4: no version information available (required by ./itsm-linux)
Your device is now enrolled!
Service started
[root@CentOS Downloads]#
```

Kuva 6 Bash -skriptin muuttaminen suoritettavaksi ja sen suoritus Linuxin komentokehotteessa.

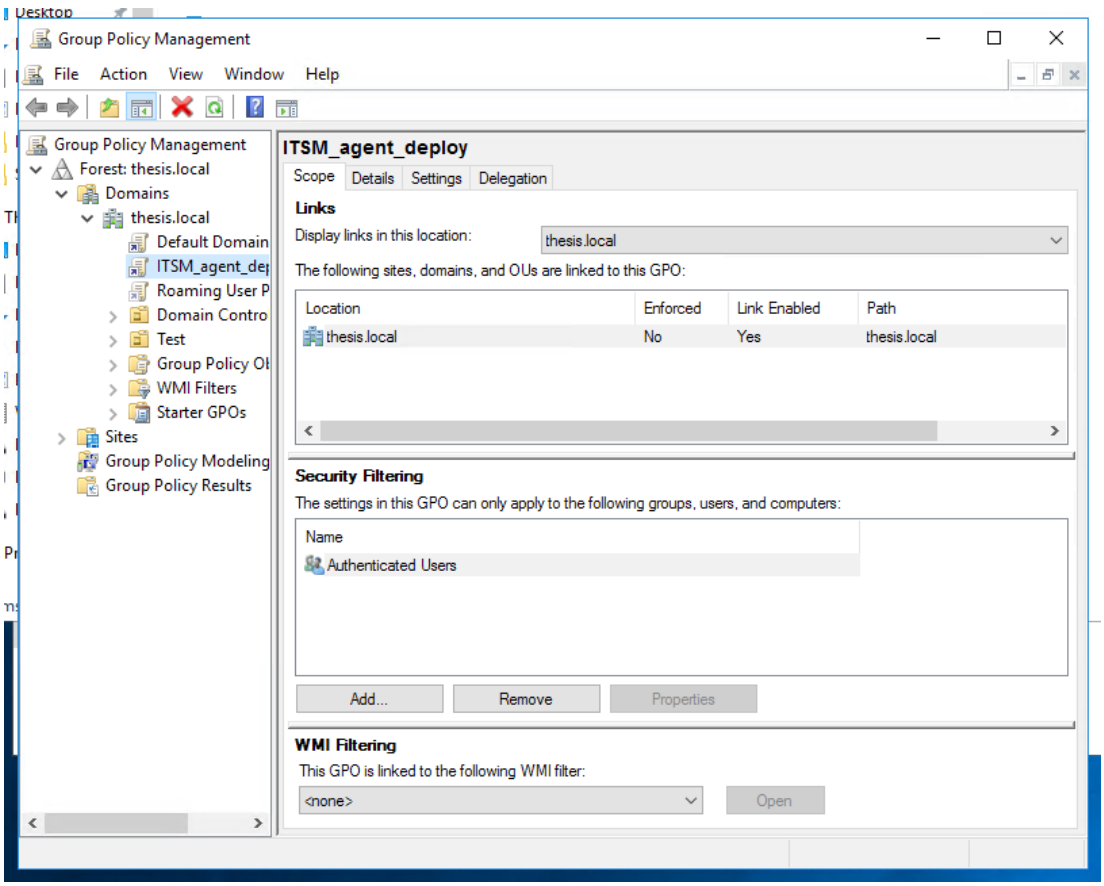
6.2 ITSM-sovelluksen jakaminen käyttäen asiakkaan ympäristön aktiivihakemistoa

Mikäli asiakasyrityksellä on käytössään aktiivihakemisto, ITSM-agentti voidaan jakaa käyttäen toimialueen ryhmäkäytäntöä. Ryhmäkäytännön avulla asiakkaan olemassa olevan ympäristön lisäys käy vaivatta, eikä palvelutarjoajan järjestelmänvalvojien tai asiakkaan yhteyshenkilön tarvitse asentaa ITSM-agenttia yksitellen jokaiseen toimialueen työasemaan. Ryhmäkäytäntöön luotavan ryhmäkäytäntöobjektin avulla varmistetaan myös uusien laitteiden, joita tullaan tulevaisuudessa lisäämään asiakkaan toimialueeseen, saavan myös ITSM-agentin itselleen sekä palveluntarjoajan pääsy uusien laitteiden dataan.

Ensimmäisenä tulee avata ITSM-sovelluksesta ”Devices”-välilehden alta ”Bulk Installation Package”, josta luodaan offline-asennuspaketti, joka tullaan jakamaan toimialueessa. Ensiksi syötetään palveluntarjoajan käyttäjätiedot, johon käy mikä tahansa palveluntarjoajan käyttäjä, mutta ITSM-sovellus asettaa oletukseksi tähän kenttää sen käyttäjän, joka on kirjautunut sisään. Seuraavana syötetään kohde yrityksen nimi esimerkiksi Thesis Oy ja mihin laiteryhmään kyseisen asennuspaketin saavat toimialueen työasemat tai palvelimet tullaan ITSM-sovelluksessa lisäämään. Seuraavana valitaan kohde käyttöjärjestelmä, mutta tässä tapauksessa oletuksena oleva Windows x64 (64-bittinen) tulee säilyttää, ellei haluta asentaa ITSM-agentin lisäksi Comodo Client Securityä eli Comodo Group Incin omaa virustorjuntaohjelmaa. Tässä vaiheessa voidaan myös lisätä omia ITSM-profiileja, mikäli niitä ollaan jo luotu, muuten ITSM-sovellus lisää oletusprofiilin luotavaan offline-pakettiin. Seuraavaksi määritellään uudelleenkäynnistys, josta voidaan valita pakotettu uudelleenkäynnistys 5-30 minuutin kuluttua, uudelleenkäynnistyksen lykkääminen toiseen ajankohtaan tai käyttäjää varoitetaan uudelleenkäynnistyksestä ja hän saa valita, suoritetaanko uudelleenkäynnistys heti vai myöhemmin. Näiden ohella lisätään viesti uudelleenkäynnistyksestä esim. ”Tämä laite käynnistyy uudelleen 10 minuutin päästä. Ole hyvä ja tallenna keskeneräiset työt”, mutta tätäkään ei tarvitse tehdä, jos ei halua, koska ITSM-sovellus on asettanut jo valmiiksi viestin: ”Your device will reboot in x minutes because it’s required by your administrator”. Asiakkaan loppukäyttäjälle voidaan halutessa määrittää viestit, jotka kertovat, jos asennus epäonnistui tai viesti, jossa vahvistetaan asennuksen onnistuneen ja sen ohelle haluama viesti, kuten ”Laitteesi rekisteröinti palveluntarjoaja Thesis Oy:n ITSM-palveluun onnistui”. Kun tarvittavat

asetukset ollaan saatu määriteltyä offline-pakettiin, tallennuksen jälkeen se on ladattavissa ITSM-sovelluksesta.

Seuraavana määritetään asiakkaan toimialueelle ryhmäkäytännön sääntö, joka jakaa sekä asentaa offline-paketissa olevan ITSM-agentin toimialueen nykyisille työasemille ja palvelimille sekä toimialueen tuleville työasemille ja palvelimille. Offline-paketti tulee tallentaa jaettuun kansioon esimerkiksi C:\ITSM_agent. Kansion jako-oikeuksiin kannattaa asettaa määrittelyksi ”Everyone”, mutta halutessaan voidaan luoda oma ryhmä, jolla on jakokansioon oikeus. Päästääkseen muokkaamaan toimialueen ryhmäkäytäntöjä, tulee avata DC-palvelimelta ”Administrative Tools” ja sen alta ”Group Policy Management”. Group Policy Managementista valitaan vasemmalta ”Forest: FQDN” (Fully Qualified Domain Name (esim. thesis.local)), sen alta ”Domains”, ”FQDN”, jonka päältä klikataan hiiren oikealla näppäimellä saadakseen auki pudotusvalikon, josta valitaan ”Create a GPO in this domain, and Link it here...”. Tämän jälkeen annetaan uudelle ryhmäkäytäntöobjektille nimi esim. ITSM_agent_deploy ja klikataan OK, jonka jälkeen uusi objekti ilmestyy Group Policy Managementissa FQDN:n alle. Avataksesi ”Group Policy Management Editorin”, jonka avulla pystyy muokkaamaan ryhmäkäytäntöobjekteja, tulee klikata oikealla hiiren painikkeella haluttua GPO:ta ja valita ”Edit”. Editorin auettua tulee valita ”Computer Configuration” ja sen alta ”Policies”, Software Settings” ja ”Software Installation”, josta valitaan hiiren oikealla painikkeella ”New” ja sen alta ”Package”. Tämän tässä vaiheessa navigoidaan kansioon, minne ollaan tallennettu Comodo ITSM-agentin offline-asennuspaketti ja valitaan ”Open”, jonka jälkeen ”Deploy Software”-ikkunasta määritellään asennuspaketin jakamistapa, joka jätetään oletukseen ”Assigned”. Jos asennuspakettiin ollaan kuitenkin määritelty käytettäväksi Proxy-palvelinta, valitaan ”Advanced”, valinnan jälkeen klikataan ”Ok”. Yleensä uudet ryhmäkäytäntöobjektit tulevat heti aktiivisiksi, mutta se kannattaa varmistaa klikkaamalla GPO:ta hiiren oikealla painikkeella ja tarkistaa onko ”Link Enabled” edessä täppä (Kuva 7).



Kuva 7 Comodo ITSM-agentin jakamiseen määritelty ryhmäkäytäntöobjekti.

Kun ollaan saatu luotua ryhmäkäytäntöobjekti, pitää suorittaa ryhmäkäytännön päivittäminen pakotetusti, jos ei olla erikseen asetettu, että toimialueen jäsenet tarkistavat toimialueen DC-palvelimelta ryhmäkäytännön esimerkiksi 10 minuutin välein, sillä normaalisti aika on 90 minuuttia mahdollisella 0-30 minuutin vasteajalla. Toisin sanoen, jos ei olla tehty muutoksia tarkistusaikaan tai suoritettu pakotettua päivittämistä, Comodo ITSM-agentti ei asennu jäsenkoneille ennen kuin aika on mennyt umpeen. Suorittaakseen ryhmäkäytännön pakotetun päivittämisen, tulee avata toimialueen jäsenkoneella Windowsin oma komentotulkki cmd.exe järjestelmänvalvojana ja suorittaa komento gpupdate /force. Komennon suorittamisen jälkeen tulee suorittaa jäsenkoneen uudelleenkäynnistys, jonka yhteydessä Comodo ITSM -agentti asentuu.

6.3 ITSM-profiilien luominen

Comodo ITSM mahdollistaa palveluntarjoajien luoda ITSM-profiileja eri käyttöjärjestelmille, joista pystyy määrittämään muun muassa monitorointia koskevia hälytyksiä ja toimenpiteitä, automaattitoimintoja, kuten skriptien suorittamista tiettyinä kellonaikoina, päivityksien tarkistamisen ja asentamisen asiakkaan laitteisiin jne. Comodo ITSM:stä löytyy valmiiksi oletusprofiileja, joita voi halutessaan käyttää, mutta suositeltavaa on tehdä omat profiilit, koska oletusprofiilit voivat sisältää toimintoja, joita ei haluta käytettävän asiakkaiden laitteissa, esimerkiksi. tietyt skriptit.

Kun halutaan luoda uusia ITSM-profiileja, tulee ITSM-sovelluksesta valita valikosta ”Configuration Templates” ja sen alta ”Profiles”, josta löytyy ITSM:n oletusprofiilit Windows-, Mac-, Android- sekä iOS-laitteille. Uuden profiilin saa luotua klikkaamalla ”Profiles” välilehdeltä ”Create”, jonka pudotusvalikosta valitaan, mille alustalle profiili luodaan. Tämän jälkeen aletaan määrittämään profiilille osioita, joita ovat **Antivirus** (Windows, Mac), **Updates** (Windows) **File Rating** (Windows), **Firewall** (Windows), **HIPS** (Windows), **Contaiment** (Windows), **VirusScope** (Windows), **Valkyrie** (Windows), **Global Proxy** (Windows), **Clients Proxy** (Windows), **Agent Discovering Settings** (Windows), **UI Settings** (Windows), **Logging Settings** (Windows), **Client Access Control** (Windows), **External Devices Control** (Windows), **Monitoring** (Windows), **Procedures** (Windows), **Remote Access** (Windows), **Certificate** (Android, Mac, iOS), **VPN** (Mac, Android, iOS), **Wi-Fi** (Mac, Android, iOS), **Browser Restrictions** (Android), **Email** (Android, iOS), **ActiveSync Settings** (Android), **Kiosk** (Android), **Network Restrictions** (Android), **Restrictions** (Mac, Android, iOS), **Other Restrictions** (Android), **Air Play** (iOS), **Air Print** (iOS), **APN** (iOS), **Calendar** (iOS), **Cellurar Networks** (iOS), **Contacts** (iOS), **Global Proxy HTTP** (iOS), **LDAP** (iOS), **Passcode** (iOS), **Proxy** (iOS), **Single sign-on** (iOS), S**ubscribed Calendars** (iOS), **Per-App VPN** (iOS), **Web Clip** (iOS) ja **App Lock** (iOS). Osioiden perässä olevien sulkujen sisällä on kerrottu alustat, joita osiot tukevat.

Antivirus osiossa pystytään määrittämään Comodo Internet Securityn -toimintoja asiakkaan laitteella, mikäli se on asennettuna. Antivirus osiosta pystyy säätämään reaaliaikaista skannausta, skannaustyyppejä ja poikkeuksia. Updates osiossa voidaan

määrittää Windows-laitteiden päivityksien tarkistamista ja sitä kautta aikataulua, jonka mukaan Windows-laitteet asentavat saatavilla olevat päivitykset sekä palvelimet, joista ne hakevat päivitykset.

File Rating osiossa voidaan määrittää CSS-luokitusjärjestelmän asetuksia. CCS-luokitusjärjestelmä on pilvipohjainen tiedostonhakupalvelu (FLS), joka varmistaa tiedostojen maineen tietokoneella. Aina kun tiedostoa tarkastellaan ensimmäisen kerran, CCS tarkistaa tiedoston Comodon tietokannasta ja mustista listoista ja myöntää sille luotettavan tilan. Jos sovellus kuuluu Trusted Software Vendors -luettelosta toimivalta tekijältä, se sisältyy laajalle ja jatkuvasti päivitetylle Comodo safelistille tai sovellukselle / tiedostolle myönnetään tilaksi ”luotettu” paikallisessa tiedostoluettelossa. (Comodo Group Inc. www-sivut 2017e).

Firewall osiossa voidaan määrittää Comodo Internet Securityn palomuurin asetuksia, sovelluksiin liittyviä sääntöjä, globaaleja sääntöjä, sääntölistoja, verkkoalueita ja porttiasetuksia. HIPS osiossa säädetään HIPS-asetuksia (host-based intrusion prevention system), HIPS-sääntöjä, sääntölistoja ja suojattuja objekteja. Contaiment säätää Comodo Internet Securityn sandboxin asetuksia, sääntöjä ja baseline-asetuksia.

VirusScope osiossa voidaan määrittää VirusScope-toiminto päälle, jonka tehtävä on monitoroida asiakkaan laitteiden prosesseja ja luoda hälytyksiä, jos ne ryhtyvät toimenpiteisiin, jotka saattavat vaarantaa loppukäyttäjän laitteen yksityisyyttä tai turvallisuutta. (Comodo Group Inc. www-sivut 2017f).

Valkyrie osiossa voidaan määrittää Valkyrie-sovelluksen asetuksia. Valkyrie on pilvipohjainen tiedostojen vertailupalvelu, joka testaa tuntemattomia tiedostoja erilaisilla staattisilla- ja käyttäytymistarkastuksilla, jotta tunnistettaisiin haitalliset tiedostot. Ohjatuissa Windows-laitteista Comodo Client Security pystyy lähettämään tuntemattomia tiedostoja automaattisesti Valkyrieen analysoitavaksi. (Comodo Group Inc. www-sivut 2017g).

Global Proxy osiossa voidaan määrittää välityspalvelimen asetuksia, jonka kautta kyseisen profiili laitteiden sovellukset voivat muodostaa yhteyden ulkoiseen verkkoon, kuten Internetiin. Clients Proxy osiossa voidaan määrittää välityspalvelin, jon-

ka kautta kyseistä sääntöä käyttävien laitteiden Comodo Client Security - ja Comodo Client Communication -yhteyksien tulisi yhdistää ITSM-sovellukseen ja Comodo-palvelimiin. Agent Discovering Settings osiossa voidaan määritellä, kirjaako ITSM-sovellus virustorjunnan tai sandboxin tapahtumia lokitiedostoihin. UI Settings osiossa voidaan määrittää, miten ITSM-agentti tulee näkymään asiakkaiden laitteilla, kuten kieli, näytetäänkö Comodo Message Center-viestejä, näytetäänkö työpöytävimpain (desktop widget). Logging Settings osiossa voidaan määrittää, halutaanko ottaa lokitiedostojen kirjaus käyttöön. Client Access Control osiossa voidaan mahdollistaa salasanasuojattu pääsy Comodo Client Security - ja Comodo Client Community -palveluun hallinnoiduista laitteista.

External Devices Control osiossa voidaan määrittää ei-sallittuja laitteita. Ulkoisten laitteiden hallinta-asetusten avulla järjestelmänvalvojat voivat määrittää luettelon laitteista, jotka pitäisi estää päätepisteissä tämän profiilin avulla. Voit esimerkiksi estää pääsyn USB-tallennuslaitteisiin, USB-liitäntälaitteisiin, Bluetooth -laitteisiin, infrapunalaitteisiin, IDE ATA / ATAPI -ohjaimiin. ITSM estää pääsyn laitteisiin, jotka on kytketty sekä sarja- että rinnakkaisportteihin ja luo lokin yhteystoiminnoistaan. (Comodo Group Inc. www-sivut 2017h.)

Monitoring osiossa voidaan määrittää, mitä ITSM-sovellus monitoroi asiakkaan laitteelta esimerkiksi keskusmuistin käyttö, prosessorin käyttö tai suoritetaanko jokin tietty toimenpide hälytyksen lauetessa esim. suoritetaanko skripti. Procedures osiossa voidaan määrittää, halutaanko asiakkaan työasemilla ajaa skriptejä tiettynä ajan kohtana. Comodo ITSM-sovelluksesta löytyy oletuksena perusskriptejä, joilla on yksinkertaisia toimintoja kuten DNS-välimuistin tyhjennys ja levyvirheiden skannaaminen. Palveluntarjoaja voi itse lisätä omia skriptejä ITSM-sovellukseen, ainoa rajoitus on, että ITSM-sovellus tukee ainoastaan Python-kielellä kirjoitettuja skriptejä. Remote Access osiossa voidaan määrittää, näytetäänkö asiakkaalle etäyhteydenottamisen yhteydessä, että kuka palveluntarjoajan työntekijä on yhteydessä hänen laitteeseensa.

Certificate osion avulla voidaan ladata sertifikaatteja, jotka voidaan valita muihin asetuksiin, kuten "Wi-Fi", "Exchange Active Sync", "VPN" ja niin edelleen. Voit myös rekisteröidä käyttäjä- tai laitevarmenteet Comodo Certificate Manager (CCM) -

sivustolta CCM-tilin aktivoinnin jälkeen paikasta Asetukset > Portaalin asetukset > Varmenteiden aktivointi. (Comodo Group Inc. www-sivut 2017i.)

VPN osiossa voidaan määrittää Mac-, Android- ja iOS-laitteiden VPN asetuksia. Wi-Fi osiossa voidaan määrittää Mac-, Android- ja iOS-laitteiden langattoman verkon asetuksia. Browser Restrictions osiossa voidaan määrittää Android-laitteen Internet-selaimen rajoituksia, kuten sallitaanko pop-upit, JavaScript jne. Email osiossa voidaan määrittää Android- tai iOS-laitteille sähköpostitilejä. ActiveSync Settings osiossa voidaan määrittää käyttäjälle oikeus Exchange-sähköpostitileihin. Kiosk osiossa voidaan määrittää Android-laite kioskitilaan, mikäli laite on Samsung for Enterprise (SAFE)-laite. Network Restrictions osiossa voidaan määrittää Android-laitteiden tietoverkkorajoituksia, kuten esim. sallitaanko ainoastaan hätäpuhelut, sallitaanko verkkovierailu jne.

Restrictions osiossa voidaan määrittää rajoituksia Mac-, Android- ja iOS-laitteille. Other Restrictions osiossa voidaan määrittää muita rajoituksia Android-laitteille, kuten esimerkiksi sallitaanko USB-laitteet, sallitaanko mikrofoni, sallitaanko SD-kortti jne. Air Play osiossa voidaan määrittää iOS-laitteille hyväksytyt laitteet AirPlayn kautta. Air Print osiossa voidaan määrittää iOS-laitteille verkkotulostimia, jotka hyödyntävät AirPrint-protokollaa. APN osiossa voidaan määrittää iOS-laitteille operaattorien tukiasemien asetukset manuaalisesti. Calendar osiossa voidaan määrittää iOS-laitteille esimerkiksi asiakkaan yrityksen kalenteri, joka hyödyntää CalDAVia. Cellurar Networks osiossa voidaan määrittää iOS-laitteiden matkapuhelinliittymäntarjoajan asetukset manuaalisesti. Contacts osiossa voidaan määritellä iOS-laitteisiin kontakteja, jotka hyödyntävät CardDAVia. Subscribed Calendars osiossa voidaan määrittää asiakkaan iOS-laitteille tilattuja kalentereita käyttäen kalenterien URL-osoitteita

Global Proxy HTTP osiossa voidaan määrittää iOS-laitteet käyttämään Global Proxy HTTP ominaisuutta. Määrittämällä tämän asiakkaan mobiililaitteisiin voidaan varmistaa, että internet-yhteys on aina suunnattu uudelleen yhdellä välityspalvelimella. Tämä tarjoaa tietoturvaa, koska kaikki henkilökohtaiset tiedot suodatetaan globaalin HTTP-välityspalvelimen kautta. (ManageEnginen www-sivut 2017.)

LDAP osiossa voidaan määrittää iOS-laitteet osaksi LDAP-ympäristöä. (Lightweight Directory Access Protocol). Passcode osiossa voidaan määrittää iOS-laitteille vaatimuksia liittyen pääsykoodiin, esimerkiksi minimipituus ja pääsykoodin ikä. Proxy osiossa voidaan määrittää iOS-laitteille välityspalvelin, jonka kautta ryhmään kuuluvat laitteet muodostavat yhteyden ulkoverkkoon, esim. Internetiin.

Single sign-on (iOS). Tässä osiossa voidaan määrittää iOS-laitteille tarvittavat asetukset Kerberos autentikointiin ja se on saatavilla niihin iOS-laitteisiin, joissa on iOS 7 tai uudempi versio. (Comodo Group Inc. www-sivut 2017j).

Per-App VPN osiossa voidaan määrittää iOS-laitteille VPN-asetukset sovelluskohtaisesti. Per-App Virtual Private Network (VPN) -toiminto muuttaa pelin etäisillä mobiilipäätteillä. VPN-yhteydet mahdollistavat loppukäyttäjien pääsyn sisäisiin resursseihin missä ja millä tahansa laitteella. Perinteisissä VPN-ratkaisuissa ei kuitenkaan ole älykkyyttä erottamaan henkilökohtaisia ja tuottavia sovelluksia, jotka mahdollistavat kaikkien laitteiden sovellusten käytön. VMware AirWatch per-app VPN luo yhteydet sovellustasolla, eikä laitekohtaisesti. Kun valtuutettu sovellus käynnistyy, VMware Tunnel muodostaa yhteyden saumattomaan ja turvalliseen käyttöön. (VMware, Inc www-sivut).

Web Clip osiossa voidaan määrittää asiakkaiden iOS-laitteille pikakuvakkeita suoraan Internet/Intranet-sivustoille. App Lock osiossa voidaan määritellä asiakkaan iOS-laitteille sovelluksiin rajoituksia. Haittapuolena on, että iOS-profiiliin voi ainoastaan määrittää yhden sovelluksen App Lockiin eli jos haluaa App Lockin moneen sovellukseen, tulee palvelutarjoajan luoda niin monta iOS-profiilia kuin sovelluksia halutaan määrittää App Lockiin.

6.4 ITSM-hälytysten luominen

ITSM-sovelluksessa palvelutarjoaja pystyy luomaan omia hälytyksiä liittyen laitteiden monitorointiin. Kun halutaan luoda hälytyksiä, tulee navigoida ITSM-sovelluksesta valitsemalla vasemmalta ”Configuration Templates” ja sen alta ”Alerts”. Comodon ITSM-sovellus on luonut valmiiksi ”Defaul Alert”-nimisen häly-

tyksen, jonka voi halutessaan kloonata ja muokata tai luoda uuden hälytyksen valitsemalla ”Create Alert”. Uuden hälytyksen luonnissa määritetään hälytykselle nimi, esimerkiksi Thesis Oy MSP alert ja hälytyksen kuvaus, jos sen kokee tarpeelliseksi. Tämän jälkeen itse hälytyksen asetuksia pääsee määrittämään valitsemalla juuri luodusta hälytyksestä ”Alert Settings”, jota klikkaamalla saadaan listaus nykyisistä hälytyksen asetuksista, joita pääsee muokkaamaan klikkaamalla ”Edit”. Hälytyksen asetuksista voidaan määrittää, kuinka monta minuuttia, tuntia tai päivää pitää kulua ennen kuin ITSM-agentti raportoi samoista ongelmista. Vodaan myös määrittää, luodaanko hälytyksestä ilmoitus palveluntarjoajan ITSM-sovellukseen, luodaanko hälytyksestä tiketti Comodo Service Desk -sovellukseen ja liitetäänkö mukaan alkuperäinen tiketti, mikäli uusi vastaa suoritusseurannan ehtoihin sekä suljetaanko tiketti automaattisesti, jos tiedot ylittävät kynnysarvon. Jos valitaan, että hälytykset luodaan tiketteinä Comodo Service Desk -sovellukseen, voidaan vielä määrittää, avataanko tiketit statuksella alhainen, normaali, korkea vai kriittinen sekä meneekö ne huolto-osastoon, myyntiosastoon vai tukiosastoon ja avataanko tiketti. Lisäksi hälytykseen voidaan vielä määrittää laitteen

- Yleistiedot eli merkki, malli, sarjanumero, kirjautunut käyttäjä, toimialue/työryhmä, Mac-osoite, paikallinen IP-osoite, oletusyhdyskäytävän IP-osoite ja laitteen nimipalvelimen osoite
- Suoritustiedot eli suorittimen käyttö, keskusmuistin käyttö, kiintolevyn käyttö, verkon käyttö, järjestelmän nykyinen käynnissä ollut aika ja odottaako laite uudelleenkäynnistämistä
- Liitettävyystiedot eli paikallinen IP-osoite, ulkoinen IP-osoite, oletusyhdyskäytävän IP-osoite, datapakettien lähetys oletusyhdyskäytävään, viimeinen kommunikointi aika ja nimi.

Tämän jälkeen voidaan määritellä vaihtoehtoiset tavat hälytyksien lähettämiseen klikkaamalla ”Additional Recipients”, josta voidaan määrittää, lähetetäänkö hälytykset sähköpostiin vai ei ja mikäli lähetetään, lähetetäänkö samaa laitetta koskeva hälytys aina vai kun hälytys on lauennet esimerkiksi viisi kertaa, lähetetäänkö sähköposti ITSM-sovelluksen järjestelmänvalvojalle eli toisin sanoen yrityksen Comodo Onetilin sähköpostiin vai johonkin muuhun sähköpostiosoitteeseen esimerkiksi jonkun tietyn palvelutarjoajan työntekijän sähköpostiin, joka on vastuussa sen asiakkaan ympäristöstä, jolle hälytys on luotu vai lähetetäänkö hälytys tietyille ITSM-

sovelluksen käyttäjille. Kun ollaan saatu määriteltyä hälytykseen haluamat asetukset, voidaan klikata ”Save” ja ottaa hälytys käyttöön Windows-laitteille suunnatussa ITSM-profiilissa ”Monitoring”-osiossa. Hälytyksiä ei voida määrittää kuin ainoastaan Windows-laitteille.

6.5 Mobiilisovellusten lisääminen ITSM-sovellukseen ja niiden asentaminen asiakkaan mobiililaitteeseen

ITSM-sovelluksessa palveluntarjoajat voivat myös määrittää mobiilisovelluksia Android- ja iOS-laitteiden ITSM-agentteihin, josta asiakkaat näkevät mitä sovelluksia he ainakin tarvitsevat. Kun halutaan lisätä palveluntarjoajan ITSM-sovelluskauppaan sovelluksia, tulee navigoida vasemmalta kohtaan ”Application Store” ja valita joko ”iOS Store” tai ”Android Store”.

Molemmissa kaupoissa voidaan asettaa mukautettuja sovelluksia (Enterprise Application) tai sovelluksia Play -kaupasta tai AppStoresta. Lisätessä mukautettuja sovelluksia, palveluntarjoajaa pyydetään antamaan sovelluksen nimi, versio, Bundle -tunnus, kategoria, tuetut laitteet (ainoastaan älypuhelimet, ainoastaan tabletit vai sekä älypuhelimet ja tabletit), onko sovellus pakollinen ja asennetaanko sovellus käyttäjän huomaamatta, mikäli se on sovelluksen osalta mahdollista. Seuraavaksi määritetään lähdetiedosto eli itse sovellus, sovelluksen ikonin ja kuvakaappaukset sovelluksesta ja klikataan ”Save”.

Kun halutaan lisätä palvelutarjoajan sovelluskauppaan sovellus Play-kaupasta tai AppStoresta, tulee klikata ”Add Google Play/AppStore Application”, jonka jälkeen ei tarvitse muuta kuin syöttää sovelluksen nimi ja ITSM-sovellus hakee sen Play-kaupasta/AppStoresta ja määrittää sille version, Bundle-tunnuksen, lisenssityypin, kategorian, tuetut laitetyypit, kuvauksen, jako asetukset, lähdetiedoston, sovelluksen ikonin ja kuvakaappaukset sovelluksesta. Halutessaan voi itse määritellä oman ikonin tai kuvakaappaukset, mutta mikäli ei halua, voi klikata ”Save” ja sovellus tallentuu palvelutarjoajan sovelluskauppaan.

Kun palvelutarjoaja haluaa asiakkaiden asentavan sovelluskaupan sovelluksen, tulee klikata ”Informn Devices Now”, joka lähettää laitteelle ilmoituksen, että asenna nämä seuraavat sovellukset. Asiakkaan näpäyttäessä ilmoitusta, aukeaa eteen välilehti nimeltään ”Applications”, jossa on lista asennettaviksi määrätyistä sovelluksista, jota klikkaamalla asiakas ohjataan Play-kauppaan/AppStoreen, josta hän asentaa sovelluksen laitteeseensa.

7 COMODO RMM

Comodo RMM on Comodo ITSM:n osa, joka tarjoaa etähallinta ja -monitorointi ominaisuuden sovellukseen. Aiemmin Comodo One:ssa oli erillinen RMM-sovellus, mutta nykyään Comodo on integroinut sen ITSM-sovellukseen, mutta vanhoissa Comodo One -tileissä, jotka on luotu ainakin 13.9.2017, voidaan käyttää vanhaa RMM-sovellusta. Comodolla on kaksi ohjelmaa, jolla voidaan ottaa etäyhteyttä asiakkaiden laitteisiin: Comodo Remote Control ja RMM Administration Console.

Comodo tarjoaa palvelutarjoajille RMM-ohjelmiston, joka tunnistaa ja raportoi ongelmat, jolloin asiantuntijat voivat korjata ne. Se auttaa toteuttamaan asioita, kuten aktiivisen ylläpidon, käyttöjärjestelmän päivityksen, virustentorjunta-määrityksen jne. Comodo RMM tarjoaa palveluntarjoajille ajantasaista tietoa käyttäjien ohjelmistojen ja verkkojen tilasta sekä päivityksistä, tarjoaa uusimmat tiedot ja toimintakertomuksen, aiheuttaa välittömän tikettien luomisen, kun tunnistetiedot on identifioitu, auttaa pitämään silmällä käyttäjän verkkoa ja laitteen terveyttä ja seuraamaan useita asiakkaita sekä heidän päätepisteitä. Etuina ovat nopea asennus ja käyttöönotto, reaaliaikainen viestintä, uusin käyttöjärjestelmätuki, panoraamavalvonta, automaatio, laaja raporttien ja lokien nopea tuottaminen jne. (Comodo Group Inc. www-sivut 2017l.)

7.1 RMM-agentin asetaminen asiakkaan laitteeseen

Vanhassa RMM-sovelluksessa laitteen voi lisätä valitsemalla Comodo One Dashboardin valikosta ”Applications” ja sen alta ”RMM”. RMM-sovelluksen auettua

valitaan ”Add Devices”, jonka jälkeen voidaan valita, minkä asiakkaan laitteeseen halutaan RMM-agentti asentaa sekä voidaan päättää, haetaanko tarvittava .msi-asennuspaketti hyödyntäen sivua http://www.joincomodo.com ja koodia, jonka saa sivun linkin alta, vai ladataanko asennus pakketti .exe-asennustiedostona, joka sisältää RMM-agentin lisäksi Patch Management -agentin vai ainoastaan RMM-agentti .msi-asennuspakettina joko 64- vai 32-bittiselle Windowsille. Asennuksen jälkeen palvelutarjoajan työtekijä voi käyttää asiakkaan laitetta tarpeen tulleen etänä.

RMM-sovelluksen ollessa osa ITSM-sovellusta, nykyään RMM-agentin asennus suoritetaan sen kautta. ITSM-sovelluksesta valitaan ”Device List” ja laitelistasta valitaan laite, jolle halutaan asentaa RMM-agentti klikkaamalla laitteen nimeä. Eteen avautuu laitteen tiedot sekä mahdollisia suoritettavia toimenpiteitä, tässä tapauksessa valitaan ”Install or Update Packages” ja sen alta ”Install Additional Comodo Packages”, jonka jälkeen voidaan valita, asennetaanko Comodo Client Security vai RMM Plugin Agent ja mahdolliset asetukset liittyen asiakkaan laitteen uudelleenkäynnistykseen. Valittuaan asennettavaksi RMM Plugin Agent ja asetukset liittyen uudelleenkäynnistykseen, tulee klikata ”Install”, jonka jälkeen ITSM ilmoittaa sovelluksen asennuksen käynnistyneen. Asennuksen prosessia voi seurata valitsemalla ”MSI Installation” ja päivittämällä sivua niin kauan, kunnes ilmestyy ilmoitus onnistuneesta tai epäonnistuneesta asennuksesta.

7.2 Comodo RMM Administration Consolen asentaminen ja esittely

Ottaakseen yhteyden asiakkaan laitteelle etänä, tulee palveluntarjoajan työntekijän asentaa omalle laitteelleen joko Comodo Remote Control tai Comodo RMM Administration Console, joka alun perin on suunniteltu vanhalle RMM-sovellukselle. Suosittelen ladattavaksi RMM Administration Consolen, koska Comodo Remote Control on vielä kehitysvaiheessa, joten se ei välttämättä toimi toivotusti.

Palveluntarjoajan työntekijä voi ladata itselleen kyseiset sovellukset valitsemalla jonkun asiakkaan laitteen ITSM-sovelluksen klikkaamalla ruksin laitteen nimen edessä olevaan laatikkoon, jolloin pystytään valitsemaan ”Enroll Device” vierestä ”Remote Control”, jonka jälkeen voidaan valita, ladataanko uusi Comodo Remote

Control vai vanha RMM-liitännäinen, tässä tapauksessa valitaan jälkimmäinen, jonka jälkeen asennuspaketti latautuu työasemalle, jonka asennuksen suorittamisen jälkeen RMM-liitännäinen on käytettävissä. (Comodo Group Inc. www-sivut. 2017l).

Sovelluksen asennuttua, se löytyy nimellä RMM Administration Console, jonka avaamalla päästään kirjautumaan palvelutarjoajan RMM-sovellukseen. Kirjautumisen jälkeen eteen ilmestyy lista palvelutarjoajan asiakkaista ja laitteista, jotka ovat merkitty asiakkaan omistukseen. Sovellus näyttää laitteista tietoja, jotka ovat laitteen nimi (esim. DC), käyttöjärjestelmä (esim. Windows Server 2016), tyyppi (esim. Server), kirjautunut käyttäjä (esim. THESIS\Administrator), paikallinen IP-osoite (esim. 10.222.232.10), ulkoinen IP-osoite (193.166.150.233), yhteensopivuus (esim. N/A), määritelty monitorointisääntö (esim. Server monitoring policy), kuvaus (esim. Thesis Oy Domain Controller) ja toiminto (esim. Takeover) (Kuva 8).

Laitenäkymää voidaan vaihtaa yläpalkista keskeltä. Voidaan määrätä, että sovellus näyttää kaikki laitteet tilasta riippumatta, offline-tilassa olevat laitteet, ei-yhteensopivat laitteet sekä istunnossa olevat laitteet. Laitenäkymää voidaan päivittää alhaalta keskeltä valitsemalla ”Refresh” sekä laitteilla voidaan määrätä joko työasema tai palvelin monitorointisääntö valitsemalla ”Apply Policy” ja sen alta valitaan, asennetaanko ”Workstation monitoring policy” vai ”Server monitoring policy” sekä valitaan laitteet, jolle jompikumpi sääntö määritetään ja klikataan ”Apply Policy”, jonka jälkeen RMM-sovellus päivittää valituille laitteilla määrätyn säännön. Laitteille voidaan myös suorittaa toimenpiteitä, joita voidaan luoda RMM-sovelluksesta valitsemalla alhaalta keskeltä ”Run Procedure”. Tämän jälkeen valitaan toimenpide, esimerkiksi ”Skannaa levy”, laiteelle, jolla halutaan kyseinen toimenpide suorittaa ja klikataan ”Run Procedure”. Tämän jälkeen RMM-sovellus lähtee suorittamaan toimenpidettä valitulle laitteelle, jonka statusta voidaan seurata Jobs-osiosta.

Sovelluksesta voidaan laitteiden lisäksi tarkkailla meneillä olevia tehtäviä valitsemalla sovelluksen yläpalkista vasemmalta löytyvästä pudotusvalikosta ”Jobs”. Ensimmäisenä eteen avautuu monitori, joka näyttää kaikki tehtävät tilasta riippumatta. Näytettävät tiedot tehtävistä ovat ID (esim. 10670), nimi (esim. Skannaa levy), kuvaus (esim. Työ skannaa kohde laitteiden kiintolevyjen kapasiteetit), aloitusaika (esim. 11:47 PM), tila (esim. Suoritetaan) ja tehtävän suorittaja (esim. by Admini-

strator). Tehtävistä voidaan selata alkavien töiden mukaan, keskeneräisten töiden mukaan ja valmiiden töiden mukaan.

Olemassa olevat toimenpiteet saadaan esiin valitsemalla vasemmasta pudotusvalikosta ”Procedures”. Ensimmäisenä eteen ilmestyy olemassa olevat toimenpiteet, joiden tiedot ovat ID (esim. 4113), nimi (esim. Skannaa levy), kuvaus (esim. Skannaa kohde laitteiden kiintolevyt), yhteensopivuus (esim. Windows) ja omistaja (esim. antti.ohman@student.samk.fi). Uuden toimenpiteen pystyy luomaan valitsemalla RMM-ohjelmasta alhaalta ”Create”, jonka jälkeen annetaan toimenpiteen nimi, kuvaus, alusta (ainoastaan Windows, koska Comodo RMM ei tue muita käyttöjärjestelmiä) sekä toiminnot, joita halutaan suorittaa, tämän jälkeen klikataan ”Save” ja toimenpide on valmis käytettäväksi.

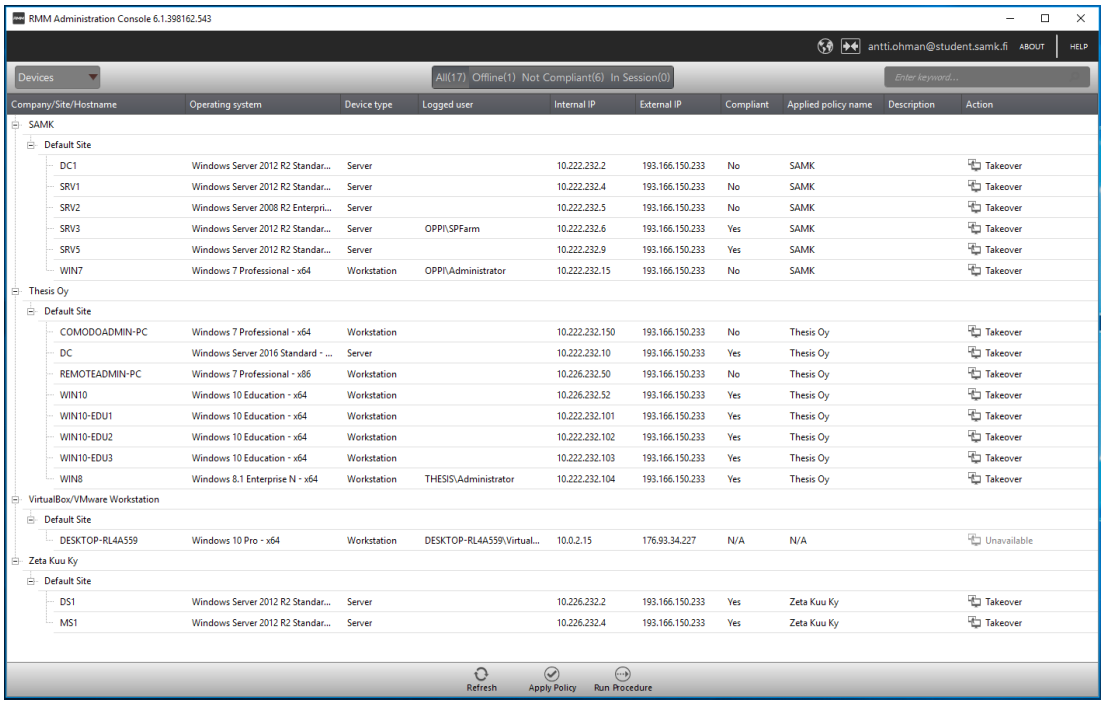
Olemassa olevat säännöt saadaan esiin valitsemalla vasemmasta pudotusvalikosta ”Policies”, jonka jälkeen eteen avautuu Comodo RMM-ohjelmiston oletussäännöt (Workstation Monitoring Process ja Server Monitoring Process). Halutessaan luoda uuden säännön, valitaan Comodo RMM-ohjelmasta alhaalta keskeltä ”Create”, jonka jälkeen säännölle voidaan määrittää seuraavia asetuksia, jotka ovat prosessorin käytön monitorointi (CPU Usage more than x %, For Period more than x min), keskusmuistin käytön monitorointi (RAM Usage more than x %, For Period more than x min), levytilan monitorointi (Free Drive Space less than x GB), verkkoliikenteen monitorointi (Network Usage more than x %, For Period more than x min), levyn terveyden monitorointi (Check Period is x hours), hakkeri monitorointi (Failed Logins equal x times), tiedostokoon monitorointi (File Size more than x MB, File Path is x), kansion koon monitorointi (Folder Size more than x MB, Folder Path is x), vapaan levytilan monitorointi (Free Disk Space less than x GB), levyntilan muuttumisen monitorointi (Consume Rate more than x GB, For Period more than x hours), prosessin monitorointi (Process Name is running x), palvelujen monitorointi (Service Name is running x), tapahtumien monitorointi (EventID is x), TCP-palvelun monitorointi (Hostname is x, Port is open x), Ping monitorointi (Host is down x, Ping Period is x min) ja Webin monitorointi (Content contains x, URL is x). Suluissa kerrotaan, mitkä vaatimukset säännön pitää tavoittaa, ennen kuin se lähettää palveluntarjoajalle tiedon tapahtumasta joko sähköpostiin tai Comodo Service Deskiin.

Uuden säännön voi ottaa heti käyttöön valitsemalla ”Apply Policy”, josta valitaan luotu sääntö ja laitteet, jolla halutaan sääntö käyttöön ja klikataan ”Apply Policy”, jonka jälkeen säännön saanet laitteet alkavat noudattamaan säännön monitorointi asetuksia.

Etäyhteys asiakkaan laitteeseen saadaan valitsemalla ”Devices”-välilehti, josta saadaan esiin asiakkaat laitteineen ja valitsemalla halutun asiakkaan laitteen perästä ”Takeover”. Etäistunto avaa uuden ikkunan, josta pystytään valitsemaan, mitä etäyhteystyökaluja halutaan käyttää, jotka ovat Active Connections Manager, Autoruns Manager, Browser Addons Manager, File Transfer, Hardware Monitor Tool, Power Manager, Process Explorer, Remote Desktop, Shell Execute, System Cleaner, System Inventroy ja System Restore. Istunto näyttää myös laitteeseen asennetun agentin tiedot, jotka ovat versio (esim. 6.1.397174.524), isäntänimi (esim. DC), käyttöjärjestelmä (esim. Windows Server 2016 Standard), arkkitehtuuri (esim. x64), laitetyyppi (esim. Server) ja session ID (esim. 257432).

Active Connections Manager mahdollistaa tarkistelemaan sen hetkisiä verkkoyhteyksiä, joita käyttää sovellukset, prosessit ja palvelut. Active Connections Manager yksilöllistää jokaisen yhteyden, josta sovellukset ovat vastuussa sekä tekee pakotetun lopetuksen kaikille sovelluksille asiakkaan laitteissa, jonka se tunnistaa uhkana. Autoruns Manager mahdollistaa käynnistysohjelmien, palveluiden, ajureiden, järjestemäohjelmien jne., jotka ovat latautuneet, automaattisen käynnistyksen asiakkaan laitteella. Browser Addons Manager mahdollistaa asennettujen selaimen lisäosien tarkistamisen ja niiden poistamisen asiakkaan laitteelta. File Transfer mahdollistaa tiedostojen välittämisen palveluntarjoajan työntekijän laitteelta asiakkaan laitteelle. Hardware Monitoring Tool mahdollistaa seurata laitteistoindeksiä tarkistaakseen, onko tietokone ylikuumentunut tai jännite on poissa hyväksyttävästä alueesta estääkseen käyttöjärjestelmän vikoja. Power Manager mahdollistaa asiakkaan laitteen sammuttamisen tai uudelleenkäynnistämisen, jos sitä vaaditaan jonkun kriittisen operaation, kuten Windowsin rekisterin muokkaamisen jälkeen. Process Explorer mahdollistaa nopean tunnistamisen, seurannan ja lopettamisen mahdollisista epävarmoista prosesseista, jotka toimivat päätepisteessä. Process Explorer näyttää kaikki käynnissä olevat prosessit, jopa ne, jotka ovat käynnistäneet haittaohjelmat tietokoneessa ja jotka ovat näkymättömiä tai hyvin syvästi piilotettuja. Remote Desktop mahdollis-

taa asiakkaan laitteen hallinnan etätyöpöytäyhteyden kautta ongelmien selvittämiseksi sekä ratkaisemiseksi. Shell Executella voidaan suorittaa asiakkaan laitteen komentotulkin komentoja. System Cleaner mahdollistaa rekisterin puhdistustoiminnon, joka poistaa vanhentuneet ja ei-toivotut rekisterimerkinnät järjestelmän suorituskyvyn parantamiseksi ja levyjen puhdistamistoimintojen avulla roskapostin tai roskatiedostojen poistamiseksi, jotka käyttävät tilaa asiakkaan laitteessa. System Inventory mahdollistaa tarkastella asiakkaan laitteisto- ja ohjelmistoresursseja. Järjestelmävaraston tarkastus antaa arvokasta tietoa laitteiston yhteensopivuuden määrittämiseksi käyttöjärjestelmien kanssa ja tunnistaa mahdolliset muutokset laitteistossa, joka voi aiheuttaa ongelmia. System Restore mahdollistaa palauttamaan asiakkaan laitteen aikaisemmin luotuun palautuspisteeseen (sisältää järjestelmätiedostot, asennetut ohjelmat, Windowsin rekisterin sekä järjestelmäasetukset) ajassa taaksepäin. Järjestelmänpalauttamisessa voidaan myös tehdä palautuspiste nykyisistä asetuksista asiakkaan laitteesta tulevaa varten.



Kuva 8 RMM Administration Console.

8 COMODO PATCH MANAGEMENT

Comodo Patch Management on Comodo ITSM-sovelluksen osa, joka mahdollistaa korjaustenhallinnan palvelutarjoajan asiakkaiden laitteilla. Niin kuin Comodo RMM, Comodo Patch Management on myös ollut aiemmin oma sovelluksensa, mutta Comodo Group päätti liittää sen osaksi ITSM-sovellusta. Comodo Patch Managementilla pystyy asentamaan käyttöjärjestelmä päivityksiä, mutta ainoastaan Windows-laitteille sekä kolmannen osapuolen päivityksiä asiakkaiden laitteille. Kolmannen osapuolen päivityksiä voi asentaa ainoastaan niille ohjelmille, jotka on kirjattu Comodo Onen tietokantaan.

8.1 Päivitysten hallinta sekä kolmannen osapuolen sovelluksien päivittäminen

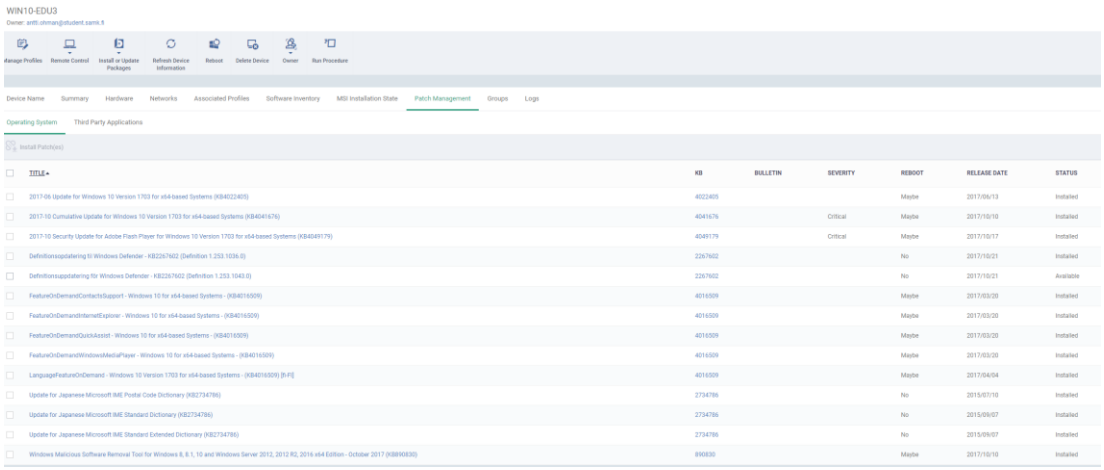
Nykyään Comodo on integroinut vanha Comodo Patch Management -sovelluksen osaksi heidän ITSM-sovellustaan, aivan kuten RMM-sovelluksenkin. Uusille Comodo One -tileille oli vielä tämän opinnäytetyön aloitusvaiheessa mahdollista saada käyttöönsä vanha Comodo Patch Management -sovellus, jonka sai Comodo One -kaupasta ilmaisena. Tämän jälkeen valittiin Comodo One Dashboardista ”Applications”-valikosta ”Patch Management”, josta pystyttiin valitsemaan asiakas, jonka päivityksiä haluttiin hallita ja jakaa. Vanha Patch Management -agentti saatiin asennettua samassa asennusohjelmassa vanhan Comodo RMM-ohjelman kanssa.

ITSM-sovelluksessa ei pysty hallitsemaan käyttöjärjestelmä päivityksiä muuten kuin valitsemalla, asennetaanko vai ei, mutta kolmannen osapuolen sovelluksia pystytään hallitsemaan täysvaltaisesti luomalla ”Procedureja” eli menettelyjä valitsemalla sen ITSM-sovelluksen vasemmasta valikosta ”Configuration Templatesin” alta ja klikkaamalla ”Create” ja valitsemalla pudotusvalikosta ”Create 3rd Party Patch Procedure”. Tämän jälkeen voidaan muuttaa yleisistä asetuksista menettelyn nimeä, kuvausta, sijaintikansiota sekä käytetäänkö siinä hälytyksiä ja mikäli käytetään niin mitä hälytystä (Default Alert, Thesis Oy MSP alert). Tämän jälkeen ”Execution Options”-välilehdestä voidaan valita, suorittaako menettely kaikkien kolmannen osapuolinen sovelluksien päivittämisen, joita laitteille on asennettu vai päivitetäänkö jokin yksittäinen sovellus, kuten esimerkiksi Google Chrome tai Mozilla Firefox. Tämän jälkeen voidaan ”Restart Control”-välilehdeltä määrittää menettelyyn uudelleenkäyn-

nistysasetukset, kuten suoritetaanko pakotettu uudelleenkäynnistys ja minkä ajan päästä, suoritetaanko se korjausten ja päivityksien asennettua, suoritetaanko uudelleenkäynnistystä lainkaan ja asiakas saa itse päättää milloin käynnistää laitteensa uusiksi tai varoitetaan asiakasta uudelleenkäynnistyksestä, jolloin hän saa päättää milloin hän haluaa sen tapahtuvan. Tämän jälkeen voidaan ”Schedule”-välilehdestä määrittää aikataulu korjauksille ja päivityksille, joka pitää ensin luoda ”Profiles”-osiosta. Tämän jälkeen voidaan menettely tallentaa. Menettely voidaan suorittaa valitsemalla laitelistalta asiakkaan laite, jolle halutaan kyseinen menettely suorittaa ja valitsemalla ”Patch Management” -välilehdestä ”Third Party Applications”, jonka alle ilmestyy ne sovellukset, joihin saa päivityksiä, jonka jälkeen voi päättää, asentaako sovellukseen saatavilla olevan päivityksen vai ei. Menettely listaa kaikki sovellukset, joihin on saatavilla päivityksiä, mikäli on luonut menetelmän niin, että se kattaa kaikki sovellukset eikä tiettyjä sovelluksia, esimerkiksi Mozilla Firefox ja Google Chrome.

8.2 Käyttöjärjestelmä päivityksien asentaminen

Käyttöjärjestelmä päivityksiä on saatavilla ainoastaan Windows-laitteille. Käyttöjärjestelmä päivityksiä voidaan asentaa valitsemalla ITSM-sovelluksesta laitelista ja asiakkaan laite, joka halutaan päivittää. Kun laite on avattu, valitaan ”Patch Management”-välilehti ja sieltä ”Operating System”, josta nähdään mitä päivityksiä laitteelle on saatavilla, niiden vakavuusaste, Microsoftin KB-numero (Knowledge Base), tieto siitä vaatiiko päivitys laitteen uudelleenkäynnistyksen, milloin päivitys on julkaistu ja onko se asennettu vai ei. Päivityksiä voidaan asentaa yksitellen tai monta kerrallaan klikkaamalla päivityksen edessä olevaa tarkistuslaatikkoa. Jos halutaan asentaa kaikki saatavilla olevat päivitykset, tulee klikata tarkistuslaatikkoa ”Titlen” vieressä ja kun ollaan valittu asennettavat päivitykset, klikataan ”Install Patches”, jonka jälkeen ITSM-sovellus lähettää asiakkaan laitteen ITSM-agentille komennon, jossa se kertoo, mitä tulee asentaa asiakkaan laitteeseen (Kuva 9).



Kuva 9 Comodo ITSM-sovelluksen Patch Management -välilehti.

9 LOPUKSI

Comodo One on ilmaisohjelmistoksi aika hyvä ottaen huomioon, millaisen skaalan sovelluksia se tarjoaa käytettäväksi ilmaiseksi. Comodo One:ssa on myös valitettavasti huonoja puolia, joista yksi on mielestäni RMM tuki, joka on ainoastaan Windows -laitteille. Mielestäni olisi hyvä ottaa huomioon, että joillakin palvelutarjoajien asiakkailla saattaa olla esimerkiksi Mac-ympäristöjä eli toisin sanoen kerta Comodo RMM ei tue Mac- sekä Linux-laitteita, tulee palvelutarjoajan etsiä toinen korvaava sovellus täyttämään RMM tarpeen kyseisillä alustoilla. Tähän pätevä vaihtoehto mielestäni on TeamViewer. Tietenkin tulee ottaa huomioon, että puhutaan ilmaisohjelmistosta eli pitää myös osata varautua siihen, että puutteellisuuksia saattaa löytyä verrattuna vastaaviin maksullisiin ohjelmistoihin.

Comodo Group pyrkii tekemään Comodo Onesta mahdollisimman yksinkertaisen integroimalla sovelluksia osaksi ITSM-sovellusta. Idea on sinänsä hyvä, koska mielestäni se helpottaa ohjelmiston käyttöönottoa ja tekee muutenkin ohjelmistosta selkeämmän verrattuna siihen, että palvelutarjoajan tulee ladata monta sovellusta saadakseen kokonaisuuden kasaan. Haittana on, että samalla Comodo poistaa vallan mainiosti toimivat sovellukset palvelustaan. Tässä ei ole muuta vikaa paitsi, kun puhutaan ilmaisohjelmistosta, myös puutteellisuuksia löytyy kuten integroidusta Patch Managementista. Kun palvelutarjoajan työntekijä päivittää asiakkaan x laitteet, hän valitsee asennettavat päivitykset ja laittaa prosessin suoriutumaan, mutta hän ei näe

mikä on asennuksen tilanne, esimerkiksi paljonko ollaan prosentteina saatu asentumaan päivityspaketti tai onnistuiko asennus vai eikö ja jos ei niin minkä takia. Kun laitetaan päivityksiä asentumaan, ITSM-sovellus antaa ainoastaan ilmoituksen: ”Patch(es) successfully added to install queue.” Ainoa tapa, jonka keksein tarkistamaan onko asennus suoriutunut, on mennä ITSM-sovelluksessa laiteluetteloon, valita asiakasyritys, jonka laiteita olin päivittänyt, valita laiteryhmä, jossa laite sijaitsee ja päivittää selaimen välilehteä tai toinen tapa on odottaa esimerkiksi 30 minuuttia, jonka jälkeen tarkistetaan, onko asennus onnistunut. Mielestäni olisi hyvä, jos Comodo Group tekisi samanlaisen seurannan kuin MSI-pakettien asennuksessa eli pystytään seuraamaan, onnistuiko asennus ja jos ei niin mistä syystä.

ITSM-sovelluksesta en löydä huonoja puolia. Sovelluksen jakaminen yksittäisiin laitteisiin testaamillani alustoilla on toiminut moitteetta, kuten myös sovelluksen jako hyödyntäen aktiivihakemistoa ja ryhmäkäytäntöä. Erityisesti pohdin opinnäytetyötäni tehdessä, kuinka hyvin ITSM jako toimii käyttäen aktiivihakemistoa ja ryhmäkäytäntöä - en sen takia, että se olisi vaikea toteuttaa sillä ohjelmistojen asennus käyttäen ryhmäkäytäntöjä on yksinkertaista luoda, vaan kun kyseessä on ilmaisohjelmisto, joten kaikkeen tulee varautua. Saatuani varmuuden ITSM-sovelluksen jakamisen toimivuudesta käyttäen aktiivihakemistoa ja ryhmäkäytäntöä, tulin tulokseen, että mikäli tulen asentamaan Comodo ITSM:n ympäristöön, joka käyttää aktiivihakemistoa, aion hyödyntää sitä sovelluksen jakamisessa asiakkaan laitteisiin. Määrittelemäni ITSM-profiilit ovat toimineet niin kuin niiden on pitänytkin eri laitteilla. Testasin Windows-, Android- sekä macOS-profiileja ja kaikissa profiileissa toimi määrittämäni ominaisuudet ja rajoitukset.

Comodo RMM on rajoittunut ainoastaan Windows-laitteille, mutta olen positiivisesti yllättynyt, miten monipuolinen sovellus RMM Administration Console on ollakseen ilmainen. Valitettavan todennäköistä on, että Comodo aikoo poistaa myös tämänkin ohjelman tarjonnastaan ja pakottaa käyttäjiensä tottumaan uuteen Comodo Remote Control -sovellukseen. Comodo Remote Control on tässä vaiheessa todella epävakaa ja liian suppea. Comodo Remote Control on täysin riisuttu RDP-sovellus, jossa ei muun muassa ole File Transfer -työkalua, joka on mielestäni todella hyödyllinen työkalu lähettäessä tiedostoja asiakkaan laitteelle sekä toisinpäin. Luulisi, että Comodo Group olisi korvannut tämän työkalun jaetulla työpöydällä tai ”drag and drop”

-ominaisuudella, muta Comodo Remote Controlilla ei pysty lähettämään tiedostoja laitteiden välillä. Ainoat tavat, joita keksein lähettämään tai jakamaan tiedoston on, että palvelutarjoajan työntekijä lataa tiedoston, jonka haluaa lähettää asiakkaalle, esimerkiksi Dropboxiin. Tämän jälkeen hän ottaa asiakkaan laitteeseen etänä kiinni käyttäen Comodo Remote Controlia ja käy lataamassa tiedoston Dropboxistaan asiakkaan laitteeseen. Toinen tapa on lähettää tiedosto asiakkaan sähköpostiin ja ladata se asiakkaan laitteeseen. Tässä vaiheessa on tosin vaikea tietää, aikooko Comodo lisätä File Transferin tai jaetun työpöydän sekä ”drag and drop” -ominaisuuden Remote Control -sovellukseensa vai aikovatko he jättää sen nykyiseen tilaansa.

Vaikka Comodo One on ilmaisohjelmisto, niin jokaisella ohjelmalla on hintansa ja tässä tapauksessa hinta on käyttäjien data. Comodo ei kerää dataa käyttäjien tietämättä eli kun palveluntarjoaja hyväksyy ohjelmiston käyttöehdot, palveluntarjoaja hyväksyy myös sen, että palveluntarjoajasta sekä heidän asiakkaistaan kerätään dataa. Datan keräämisestä Comodo määrittelee tarkemmin EULA:ssa seuraavasti.

Comodo voi kerätä kaikkia tarvittavia tietoja varmistaakseen hyväksyntäsi sopimukseen. Comodo voi kerätä myös ei-henkilökohtaisesti tunnistettavissa olevia tietoja tuotteesi käytöstä, jota Comodo saa käyttää rajoituksetta. Comodo voi seurata ja luoda tuotekäyttöön liittyviä lokeja. Näitä lokeja luodaan ensisijaisesti asiakaspalvelun, sisäisen koulutuksen ja sisämarkkinatutkimuksen parantamiseksi. Comodo saattaa paljastaa nämä lokit ja kaikki muut tiedot lain tai asetuksen noudattamiseksi tai muun valtion pyynnöstä, operoidakseen tuotetta kunnolla ja suojataksemme itseämme ja/tai asiakkaitamme. Datan keräämiseen voi sisältyä:

- Järjestelmätietojen saaminen asiakkaiden laitteista, mukaan lukien laitteiston lämpötilan ja tuulettimien nopeudet sekä sisään kirjautuneen käyttäjän tiedot;
- Listan hakeminen asennetuista ohjelmistoista, selain lisäosista ja aktiivisista tcp/udp-yhteyksistä asiakkaan laitteesta;
- Etätuen istunnon yksityiskohtaisten lokien sekä toiminnallisten lokien lataaminen Comodo One palvelimiin;
- Tapahtumien kerääminen käyttäjätunnelin tietojen analysoimiseksi cWatch-lokijärjestelmästä. Laajennus tietojen keräämiseen cWatchista mahdollistaa sen, että muita tietoja saatetaan myös kerätä jokaisen käyttäjän toiminnasta

> C1 portaalissa saadakseen lajiteltua kerätyn datan käyttäjäkohtaisesti. (Comodo Group Inc 2017).

Comodo, kuten muutkin ohjelmistoja tuottavat yritykset, muuttavat EULAa silloin tällöin. Yleensä käyttäjille lähetetään sähköpostia, jossa kerrotaan sen muuttuneen sekä pyydetään käyttäjää tutustumaan siihen ja hyväksymään tai hylkäämään sen. Comodo ei tätä tee, vaan he katsovat käyttäjän hyväksyneen EULA:n muutokset yksinkertaisesti jatkamalla Comodo Onen käyttöä.

Comodo One on vielä jonkin verran lapsenkengissä, mutta se soveltuu mielestäni hyvin esimerkiksi Pk-yritykselle, joka tarjoajaa asiakkailleen IT-palveluita. Pk-yritys maailmassa monilla on käytössään Windows-ympäristö, joten tämä mahdollistaa muun muassa säästämisen lisensseissä, koska palveluntarjoaja ei välttämättä tarvitse esimerkiksi RMM-tukea Apple-laitteille. Comodo One:ssa ei tarvitse myös miettiä, että kuinka monta laitetta tullaan hallitsemaan verrattuna esimerkiksi Continuumiin, jonka tilauksen yhteydessä annetaan arvio, kuinka monta päätelaitetta hallitaan tai tullaan hallitsemaan sekä Continuum laskuttaa tilauksen ohella myös tietyn summan kuukaudessa työasemista sekä palvelimista, joihin se ollaan asennettu. Tarkkoja summia en saanut selville, sillä Continuum ei näytä hinnastoaan verkkosivuillaan. RMM:n lisäksi Comodo One tarjoaa myös muitakin hyödyllisiä työkaluja ilmaiseksi, kuten esimerkiksi laitteiden monitoroinnin, jonka avulla voidaan esimerkiksi arvioida asiakkaan laitteen ikä ja tämän avulla voidaan saada uusia mahdollisuuksia kauppaan uusista laitteista sekä ohjelmistoista.

Opinnäytetyön aihe oli itselleni ennestään tuttu, koska nykyisessä työssäni käytän Comodo Onea muun muassa asiakkaiden laitteiden hallintaan ja monitorointiin. Käytän eniten opinnäytetyössä käsiteteleministäni sovelluksista RMM-sovellusta etäyhteyden varasuunnitelmana siltä varalta, mikäli TeamViewer on alhaalla tai kollega käyttää sitä ottaakseen etäyhteyden asiakkaan laitteeseen. Comodo Onen RMM-sovellus on myös hyödyllinen asiakkaiden palvelimilla, koska voimme ottaa niihin kiinni ilman, että asiakkaan tarvitsee avata etäyhteyttä tai mikäli TeamViewer on alhaalla tai TeamViewerin Host -ohjelma ei jostain syystä toimi. Vaikka aihe oli ennestään tuttu, opein silti paljon enemmän palvelun käyttöönotosta sekä sen muokkaamisesta yrityksen omien tarpeiden mukaan. Opinnäytetyön ohella sain enemmän

tietoa ITSM-profiileista muun muassa siitä, mitä eri optioita ne pitää sisällään, mitkä optiot ovat käytössä millekin alustalle sekä miten niitä otetaan käyttöön. Opinnäytetyön tekemisessä ei ollut muita ongelmia, kuin ITSM-sovelluksen jakaminen Applen macOS-laitteisiin, koska tässä opinnäytetyössä tutustuin aivan ensimmäistä kertaa sovelluksen jakoon kyseiselle alustalle sekä ettei sovelluksen jako toiminut jostain syystä macOS-virtuaalikoneeseeni, jonka olin asentanut Oraclen VirtualBoxiin. Asennettuani macOS:ssän VMWare Workstation Player 12:sta, sain ITSM-sovelluksen jaon toimimaan ilman ongelmia ja käytin tämän ongelman ratkaisemiseen pari päivää. Toinen asia, johon käytin aikaa, oli vanhan Patch Management -sovelluksen asennuksessa demoympäristöön, koska en ollut tietoinen Comodo Groupin niin sanotusti kuolettaneen koko sovelluksen, myös vanhoista Comodo One-tileistä.

LYHENTEET JA TERMISTÖ

Aktiivihakemisto *Active Directory.* Microsoft Windows -toimialueen käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista.

APNs *Apple Push Notification Service.* Apple Inc:n. luoma alusta ilmoituspalvelulle, joka sallii kolmannen osapuolen sovelluksien kehittäjien lähettää ilmoitusdataa sovelluksiin, jotka ovat asennettuna Apple-laitteisiin.

DC *Domain Controller.* Windows-toimialueen palvelintietokone, joka vastaa suojauksen todennuspyyntöihin (sisäänkirjautuminen, tarkistusoikeudet jne.).

EULA *End User License Agreement.* Sopimus tietokoneohjelmiston oikeuksien haltijan ja ohjelmiston ostajan /käyttäjän välillä.

Forest Kokoelma puita, joilla on yhteinen globaaliluettelo, hakemistomalli, looginen rakenne ja hakemiston kokoonpano.

FQDN *Fully qualified domain name.* Verkkotunnuksen nimi, joka määrittää sen tarkan sijainnin verkkotunnuksen puun hierarkiassa. Joskus käytetään myös termiä *absolute domain name.*

Isäntä Tietokone tai verkkolaite, joka on yhteydessä tietokoneverkkoon. Isäntä vastaa yleensä verkon resursseista, palveluista ja sovelluksista verkon käyttäjille.

ITSM *IT Service Management.* Yleinen termi, joka kuvaa strategista lähestymistapaa organisaatiossa käytettävän IT:n suunnittelun, toimittamisen ja parantamisen kannalta.

Komentotulkki Tekstipohjainen tietokoneohjelma, jolla ohjataan käyttöjärjestelmää.

Korjaustenhallinta *Patch Management.* Prosessi, jonka avulla hankitaan, testataan ja asennetaan korjaustiedostoja olemassa oleviin sovelluksiin ja tietokoneohjelmistoihin.

Liitännäinen	*Plugin.* Tietokoneohjelma, joka toimii vuorovaikutuksessa isäntäsovelluksen, kuten verkkoselaimen tai sähköpostiohjelma kanssa, tarjotakseen tietyn toiminnon tarvittaessa.
MSI-paketti	*Windows Installer Package.* Ohjelmistopaketti ja sovellusohjelmointirajapinta, jota käytetään ohjelmistojen asennukseen, ylläpitoon ja poistamiseen.
MSP	*Managed Service Provider.* Suomennettuna tarkoittaa palveluntarjoajaa, tässä tapauksessa puhutaan IT-palveluntarjoajasta
RMM	*Remote Management and monitoring.* IT-työkalu tai ohjelmisto, joka auttaa palveluntarjoajia monitoroimaan etäältä asiakkaiden tietoverkoja, tietokoneita ja päätelaitteita.
Ryhmäkäytäntö	*Group Policy.* Microsoft Windows NT -käyttöjärjestelmäperheen ominaisuus, joka hallinnoi käyttäjätilejä ja tietokoneita. Se mahdollistaa keskitetyn hallinnan ja konfiguraation käyttöjärjestelmissä, sovelluksissa sekä käyttäjäasetuksissa aktiivihakemisto-ympäristöissä.
Toimialue	*Domain.* Joukko Microsoft Windows -käyttöjärjestelmän sisältäviä tietokoneita, joita voidaan hallita keskitetysti yhdeltä tai useammalta Windows-palvelimelta.

LÄHTEET

Apple Inc. www-sivut. 2017. Viitattu 11.10.2017. https://www.apple.com/

Comodo Group Inc. www-sivut. 2017a. Viitattu 4.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017b. Viitattu 4.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017c. 7.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017d. Viitattu 8.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017e. Viitattu 2.11.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017f. Viitattu 14.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017g. Viitattu 14.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017h. Viitattu 14.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. .2017i. Viitattu 14.10.2017. https://www.comodo.com

Comodo Group Inc. www-sivut. 2017j. Viitattu 14.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017k. Viitattu 14.10.2017. https://www.comodo.com/

Comodo Group Inc. www-sivut. 2017l. Viitattu 19.10.2017. https://www.comodo.com/

Comodo Group Inc. 2017. Data Collection. Teoksessa End User License Agreement Comodo One. Viitattu 10.11.2017. https://one.comodo.com/signup-for-free/eula.pdf

ICanLocalizen www-sivut. 2017. Viitattu 11.10.2017. https://www.icanlocalize.com/site/

ManageEnginen www-sivut. 2017. Viitattu 2.11.2017. https://www.manageengine.com/

Navare, S. 2017. VMware AirWatch 101: Per-App VPN. Viitattu 14.10.2017. https://blogs.vmware.com/euc/2017/04/vmware-airwatch-101-per-app-vpn.html

Rance, S. 2017. ITSM vs. ITIL: What's the Difference?. Viitattu 5.10.2017. http://www.bmc.com/blogs/itsm-or-itil-that-isnt-the-question/

University of California. 2015. Viitattu 5.10.2017. https://www.ucsc.edu/index.html

VIITTEET