jamk

F-Secure Policy Managerin asennus ja käyttöönotto

Joni Hauhtonen

Opinnäytetyö, AMK
Toukokuu 2023
Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hauhtonen, Joni

F-Secure Policy Managerin asennus ja käyttöönotto

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2023, 37 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Opinnäytetyön tavoitteena oli kehittää yrityksen verkkoympäristön tietoturvallisuutta. Parantaakseen yrityksen verkon tietoturvaa, asennettiin verkkoympäristöön F-Secure Policy Manager keskitettyä hallintaa varten ja F-Secure Client Security -virustorjuntaohjelmat verkossa oleville päätelaitteille.

Työn teoriaosuudessa käydään läpi tietoturvan osa-alueita, mikä on virustorjunta, millaisia haittaohjelmia on olemassa ja mitä keskitetty hallinta tarkoittaa. Teoriaosuuden jälkeen tutustutaan F-Secure Policy Managerin kokonaisuuteen. Sen jälkeen suoritetaan asennusvaihe, jossa asennettiin verkkoympäristöön ensin F-Secure Policy Manager Server sekä Console. Policy Manager Serverin ja Consolen asennuksen jälkeen luotiin virustorjuntaohjelman asennuspaketit Policy Manager Consolen avulla ja asennettiin F-Secure Client Security -virustorjuntaohjelmat käyttäjien päätelaitteille. Asennusvaiheen jälkeen, tutustutaan vielä asetuksiin, joilla kovennettiin tietoturvakäytänteitä, jotta verkossa toimiminen olisi turvallisempaa.

Lopputuloksena opinnäytetyössä saatiin asennettua F-Secure Policy Manager palvelimelle sekä F-Secure Client Security -virustorjuntaohjelmat käyttäjien päätelaitteille, jotta saatiin hallittua tietoturvakäytänteitä keskitetysti yhdestä paikasta.

Avainsanat (asiasanat)

Tietoturva, virustorjunta, F-Secure, keskitetty hallinta

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Hauhtonen Joni

Installation of F-Secure Policy Manager

Jyväskylä: JAMK University of Applied Sciences, May 2023, 37 pages

Degree Program in Information and Communication Technology. Bachelor´s thesis.

Language of publication: Finnish

Permission for open access publication: Yes

Abstracts

The purpose of the thesis was to develop information security of the company's network environment. To develop networks information security, there were installed F-Secure Policy Manager for centralized management and F-Secure Client Security antivirus program to networks end users hosts.

At the beginning, there is theory about what are information security, what is antivirus, which kind of malwares there are and what centralized management is. After that, we get familiar with F-Secure Policy Manager. After that comes the installation phase of how to install F-Secure Policy Manager Server and Console. After installation of F-Secure Policy Manager Server and Console, antivirus software was made through Policy Manager Console and F-Secure Client Security antivirus software was installed to end users hosts. After all installation steps, go through available features and how those are used to improve end users' security.

The goal of the thesis was to install F-Secure Policy Manager to server and install F-Secure Client Security antivirus programs to end users hosts, so it was possible to manage information security policies centralized from one place.

Keywords/tags (subjects)

Information security, virus protection, F-Secure, centralized management

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

1 Johdanto

Tämän opinnäytetyön tarkoituksena on tutustua F-Secure Policy Managerin ominaisuuksiin sekä asentaa F-Secure Policy Manager palvelimelle ja F-Secure Client Security -virustorjuntaohjelmistot työasemille. F-Secure Policy Manager on WithSecuren (entinen F-Secure Business Suite) yrityksille tarjolla oleva keskitetyn tietoturvan hallintatyökalu eri käyttöjärjestelmille. Sen avulla voidaan keskitetysti asentaa työasemille virustorjuntaohjelma, asettaa tietosuojakäytänteitä, monitoroida verkossa olevien päätelaitteiden toimintaa sekä tehostaa tietoturvaa usealla tavalla muun muassa hallitsemalla laitteiden palomuureja, tehostaa verkkoselaamisen suojausta ja estää päätelaitteita lukemasta siihen kytkettäviä muita laitteita, esimerkiksi ulkoisia tallennusvälineitä, kuten USB-muistitikkuja tai kiintolevyjä.

Opinnäytetyön tavoitteena on asentaa F-Secure Policy Manager yrityksen verkkoympäristössä toimivalle palvelimelle sekä asentaa käyttäjien päätelaitteille F-Securen tarjoamat Client Security -virustorjuntaohjelmistot ja saada päätelaitteet ottamaan yhteys Policy Manageriin ja pystyä hallitsemaan päätelaitteita keskitetysti Policy Managerilla. Kun päätelaitteille ollaan saatu hallinta, niin voidaan päätelaitteille määritellä ja ottaa käyttöön tietoturvakäytänteitä, jotka tekevät verkon käytöstä turvallisempaa ja näin ollen saadaan parannettua yrityksen tietoturvaa.

F-Secure Policy Managerin avulla myös järjestelmänvalvojien työ helpottuu sekä nopeutuu, kun tarvittavat muutokset voidaan tehdä yhdellä järjestelmänvalvojan laitteella yhtäaikaisesti useammalle loppukäyttäjän päätelaitteelle. F-Secure Policy Managerilla pystyy myös monitoroimaan järjestelmien toimintaa keskitysti ja näkemään, jos virustorjuntaohjelmat ovat havainneet haitallisia tiedostoja päätelaitteilta.

2 Tutkimusasetelma

Opinnäytetyön toimeksiantona oli asentaa yritykselle keskitetyn hallinnan ohjelma ja myös virustorjuntaohjelmat, koska yrityksellä oli tarve päivittää käytössä olevat ohjelmat. Työ on toteutettu yrityksen toiveiden mukaan ja heidän valitsemillaan ohjelmilla. Molemmat ohjelmat ovat WithSecuren tarjoamia, keskitettyä hallintaa varten F-Secure Policy Manager ja virustorjuntaohjelmat F-Secure Client Securityn eri versioilla eri käyttöjärjestelmille. Toimeksiantona oli asentaa F-Secure Policy Manager sekä F-Secure Client Security -

virustorjuntaohjelmat heidän verkkoympäristöön ja käyttäjien päätelaitteille ja niiden avulla kehittää verkon ja käyttäjien tietoturvallisuutta. Toimeksiantajan toiveena oli myös luoda heille erillinen ohjeistus asennusta ja ylläpitoa varten opinnäytetyön lisäksi.

2.1 Tutkimusmenetelmä ja tutkimuskysymys

Tutkimusmenetelmänä toimii palvelun, tuotteen tai produktion kehittäminen. Tällaisessa tilanteessa syvennytään ja keskitytään johonkin käytännössä olevaan ongelmaan sekä kyseisen ongelman ratkaisemiseen. Palvelun, tuotteen tai produktion kehittämisestä tehty opinnäytetyö tulee esiin usein työelämässä kohdatusta tarpeesta ja tavoitteena on kehittää toimintaa käytännön tasolla. Tuloksena voi syntyä esimerkiksi näyttely, tapahtuma tai opas, niinkuin tässäkin opinnäytetyössä. (Opinnäytetyö – Thesis N.d.)

Tässä opinnäytetyössä tutkimuskysymykseksi kehittyi seuraava, “miten F-Secure Policy Manager parantaa yrityksen tietoturvaa?”. Tätä tutkittiin virustorjuntaohjelmien asennuksen jälkeen siten, että virustorjuntaohjelmien toimintaa testattiin muun muassa tekemällä tiedostojen skannauksia, koventamalla tietoturvakäytänteitä ja havaitsemalla Policy Managerin avulla päätelaitteiden tapahtumia ja hälytyksiä, joita saatiin aikaiseksi esimerkiksi eicar -testihaittaohjelmalla.

3 Tietoturva ja sen osa-alueet

3.1 Tietoturva

Tietoturvalla tarkoitetaan hallinnollisia ja teknillisiä toimenpiteitä sekä menetelmiä, joilla tiedot saadaan suojattua erilaisia uhkia vastaan. Usein tietoturvaan yhdistetään niin sanottu CIA-kolmio, havainnollistettu kuviossa 1, joka muodostuu siitä, että on olemassa kolme perusperiaatetta, luottamuksellisuus (eng. confidentiality), eheys (eng. integrity) ja saatavuus (eng. availability) jotka muodostavat tietoturvan. Mikäli jokin edellä mainituista perusperiaatteista pettää, niin silloin tietoturva on vaarantunut. (Kyberturvallisuuskeskus 2020 ja Information Security: The Ultimate Guide N.d.)

Kuvio 1 CIA-kolmio (Oza N.d.)

Luottamuksellisuus

Tiedon luottamuksellisuudella pyritään siihen, että estetään tietojen luvaton käyttö sellaisilta henkilöiltä, joilla ei ole lupaa käsitellä tietoja. Tarkoituksena on pitää esimerkiksi henkilötiedot tai yrityksen salassapidettävät tiedot yksityisinä ja varmistaa, että tiedot ovat nähtävissä vain sellaisilla henkilöillä, jotka tarvitsevat kyseisiä tietoja. (Information Security: The Ultimate Guide N.d.)

Eheys

Tiedon eheys tarkoittaa sitä, että kyseisiä tietoja suojataan luvattomilta muokkauksilta. Tiedon muokkaamisella voidaan tarkoittaa, että sisältöä on lisätty, poistettu tai muokattu joko tahallisesti tai tahattomasti. Tavoitteena on varmistaa, että tieto on luotettavaa ja oikeaa. (Information Security: The Ultimate Guide N.d.)

Saatavuus

Tiedon saatavuudella halutaan varmistaa se, että tiedot ja tietojärjestelmät ovat hyödynnettävissä sillä hetkellä, kun henkilö niitä tarvitsee. Tiedon saatavuus tarkoittaa myös siis sitä, että tietoja ja tietojärjestelmiä ylläpidetään ja kehitetään, jotta saatavuus olisi mahdollisimman korkea ja näin ollen saatavilla juuri silloin, kun tietoja tarvitaan. (Information Security: The Ultimate Guide N.d.)

3.1.1 Kyberturvallisuus

Kyberturvallisuudella tarkoitetaan verkkoympäristössä olevien järjestelmien ja laitteiden suojaamista mahdollisilta uhilta ja hyökkäyksiltä. Suojattaviin järjestelmiin kuuluvat muun muassa tietokoneet, palvelimet ja tietoverkot. Verkkoympäristöä voidaan suojata haitalliselta liikenteeltä palomuurien avulla ja verkossa olevia laitteita ja niiden käyttäjiä suojataan virustorjuntaohjelmien avulla. Kyberturvallisuutta kutsutaan myös tekniseksi tietoturvaksi. (What is Cyber Security N.d.)

3.1.2 Hallinnollinen tietoturva

Hallinnollisella tietoturvalla tarkoitetaan inhimmillisiä tekijöitä, eli yritysmaailmassa tämä tarkoittaa yleensä työntekijöiden tietoturvaosaamista. Sillä voidaan tarkoittaa muun muassa käyttäjätunnusten ja salasanojen käytäntöjä, millainen olisi vahva salasana, tai että et luovuta työssä käyttämiäsi laitteita muille vaan ne ovat henkilökohtaisia. Hallinnollinen tietoturva tarkoittaa myös sitä, että työntekijöille tulee pitää tietoturvakoulutusta, ylläpitää heille koulututettua osaamista, tiedottaa mahdollisista tietoturvapoikkeamista sekä opastaa heitä tekemään sellaisia, jos jotain poikkeavaa havaitaan ja luoda käytänteitä, joita työntekijöiden tulee noudattaa, esimerkkinä salasanakäytänteet (Dosal 2019.)

3.1.3 Fyysinen tietoturva

Fyysinen tietoturvallisuus on myös osa tietoturvaa. Fyysisellä tietoturvalla tarkoitetaan esimerkiksi toimitilojen, niissä sijaitsevien järjestelmien tai laitteiden ja fyysisten dokumentaatioiden suojaamista fyysisiltä uhilta. Fyysisiin uhkiin lukeutuu muun muassa tulipalot, vesivahingot tai varkaudet ja ilkivalta. (Mitä on fyysinen tietoturvallisuus? 2021.)

Fyysistä tietoturvallisuutta voidaan parantaa erilaisilla toimenpiteillä, joilla estetään luvaton pääsy suojattuihin tietojärjestelmiin, laitteisiin ja dokumentaatioihin. Tällaisia toimenpiteitä ovat muun muassa kamera- ja kulunvalvonta. Valvonnan avulla voidaan valvoa, ettei ulkopuolisia henkilöitä päästetä tiloihin, joissa säilytetään sellaista tietoa, mikä ei heille kuulu. (Mitä on fyysinen tietoturvallisuus 2021.)

3.2 Keskitetty hallinta

Yritysympäristöt ovat vuosien saatossa muuttuneet ja yritykset hyödyntävät sekä fyysisiä että virtuaalisia ratkaisuja ympäristöissään muun muassa parantaakseen yrityksen toimintakyvykkyyttä. Tämä on myös tuonut mukanaan haasteita tietoturvan näkökulmasta esimerkiksi siten, että kuinka kaikkia laitteita voidaan hallita mahdollisimman tehokkaasti. Keskitetyllä hallinnalla tarkoitetaan siis sitä, että voidaan hallita koko yrityksen laitteita yhdestä paikasta käyttämällä yhtä siihen tarkoitettua työkalua. Tällaisia työkaluja on tarjolla useampia ja F-Secure Policy Manager, johon tutustutaan tässä opinnäytetyössä, on yksi niistä vaihtoehdoista. Erityisesti isommissa yrityksissä keskittämällä päätelaitteiden hallinta säästetään huomattava määrä aikaa ja resursseja verrattuna siihen, että jokaiselle päätelaitteelle käytäisiin asentamassa ohjelmisto erikseen ja tehdään siihen tarvittavat toimenpiteet. (What is Centralized Management N.d.)

3.3 Virustorjunta

Virustorjuntaohjelma oli alunperin ohjelma, joka luotiin suojaamaan tietokoneita viruksilta, mutta nykyään termi on yleistynyt ja sillä tarkoitetaan ohjelmaa joka on luotu havaitsemaan ja suojaamaan päätelaitteita erilaisilta kyberuhilta ja poistamaan haittaohjelmat. Kyberuhkiin lukeutuvat erilaiset haitalliset ohjelmat, kuten kiristyshaittaohjelmat, vakoiluohjelmat, troijalaiset ja virukset. (Antivirus Software N.d.)

Kun päätelaitteelle asennetaan jokin virustorjuntaohjelma, ne yleisesti toimivat taustalla tehden reaaliaikaisia skannauksia suoritettavista tiedostoista ja ohjelmista ja tarjoavat näin suojaa haittaohjelmia vastaan. Virustorjuntaohjelma käsittelee ja arvioi saamiaan tietoja verkkosivustoista, tiedostoista sekä ohjelmista ja pyrkii löytämään ja poistamaan haitalliset ohjelmat. Virustorjuntaohjelmat käyttävät pääsääntöisesti kolmea erilaista tunnistusta, ”specific

detection”, joka havaitsee tunnetut haittaohjelmat, ”generic detection”, joka havannoi tunnettujen haittaohjelmien sisältämää koodin osia, jotka ovat osana yleistä koodikantaa ja ”heuristic detection”, joka yrittää etsiä uusia tuntemattomia haittaohjelmia havaitsemalla epäilyttäviä tietorakenteita. (Antivirus, N.d.)

3.4 Haittaohjelmat

Haittaohjelma (eng. malware tai malicious software) tarkoittaa haitallista ohjelmaa, jotka pyrkivät tunkeutumaan verkkoympäristöön ja niiden laitteisiin aiheuttaen vahinkoa laitteille. Lähtökohtaisesti kaikkien haittaohjelmien tehtävänä on haitata tietokoneen normaalia toimintaa. Tarkoituksena voi olla esimerkiksi tietojen varastaminen ja tuhoaminen, tietojen lukitseminen tai tietojärjestelmien ja tietokoneiden tuhoaminen. Haittaohjelmia on monenlaisia, muun muassa kiristyshaittaohjelmat, troijalaiset, madot ja virukset. (What is malware? N.d.)

Virus

Virus (eng. virus) on haittaohjelma, joka vaatii jonkin isäntätiedoston toimiakseen. Varsinainen haittaohjelma on upotettu isäntätiedostoon hyödyntäen makroja ja se suorittaa haitallisen koodin, kun tiedostoa käytetään. Virukset leviävät päätelaitteesta toiseen ja niiden tehtävänä on haitata järjestelmien toimintaa. (What is malware? N.d.)

Mato

Mato (eng. worm) on haittaohjelma, joka hyödyntää käyttöjärjestelmien haavoittuvuuksia. Se on itsenäinen ohjelma, joka voi monistaa itseään ja levitä mihin tahansa verkon laitteeseen automaattisesti. Samoin kuten virukset, madot haittaavat järjestelmien toimintaa. (What is malware? N.d.)

Troijalainen

Troijalainen (eng. trojan virus) on haittaohjelma, joka on naamioitu haitattomaksi ohjelmaksi, mutta kun ohjelman lataa, troijalainen virus voi päästä käsiksi järjestelmän tietoihin ja pääsee muokkaamaan tai poistamaan tietoja. Troijalainen poikkeaa madoista ja viruksista siten, ettei se jaa tai monista itseään. (What is malware? N.d.)

Vakoiluohjelma

Vakoiluohjelma (eng. spyware) on haittaohjelma, joka kerää tietoa käyttäjästä ja tietokoneesta. Se toimii yleensä salassa käyttäjältä ja hyödyntää etäkäyttöä raportoiden hyökkääjälle kerätyistä tiedoista. Esimerkiksi Keylogger on eräänlainen vakoiluohjelma, joka tallentaa näppäinpainallukset. (What is malware? N.d.)

Mainosohjelma

Mainosohjelma (eng. adware) on haittaohjelma, joka kerää tietoja tietokoneesi käytöstä ja esittää kohdennettuja mainoksia kohteelle. Adware -haittaohjelmat eivät kuitenkaan aina ole suoraan haitallisia, vaan niiden avulla voidaan ohjata käyttäjä mainoksien avulla sellaisille sivustoille, jotka sisältävät jonkin muun haittaohjelman. (What is malware? N.d.)

Kiristyshaittaohjelma

Kiristyshaittaohjelma (eng. ransomware) on haittaohjelma, joka pääsee käsiksi järjestelmän tietoihin ja salaa tiedot siten, että käyttäjä ei voi käyttää niitä ja hyökkääjä vaatii käyttäjältä lunnaita salauksen purkamista vastaan. (What is malware? N.d.)

Tiedostoton haittaohjelma

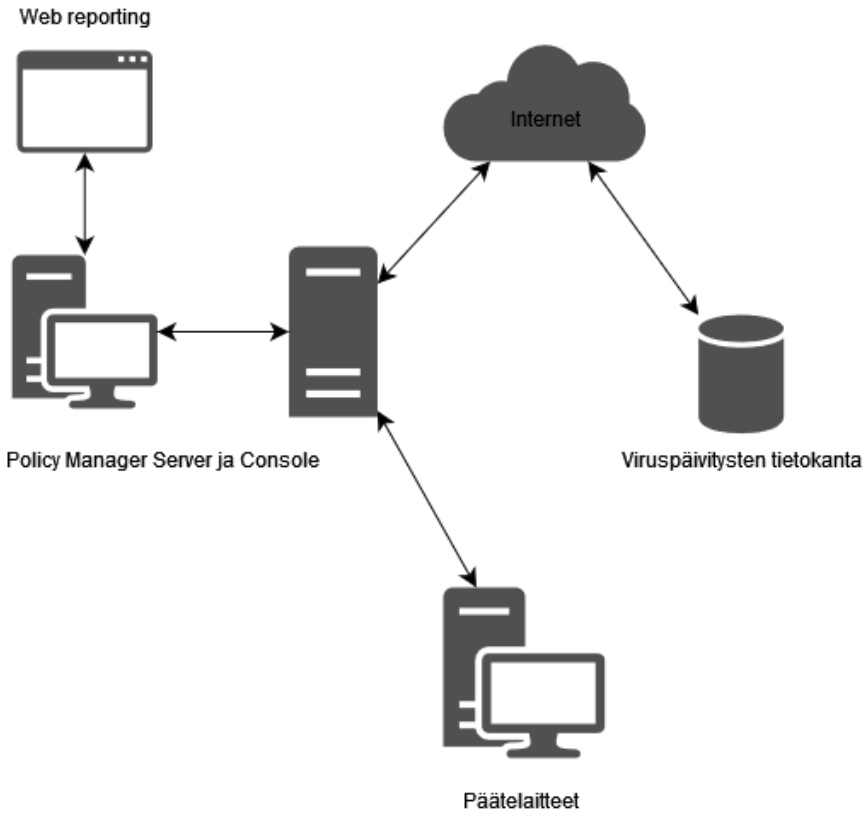
Tiedostoton haittaohjelma (eng. fileless malware) on haittaohjelma, joka toimii tietokoneen RAM-muistissa. Haittaohjelma ei siis sijaitse käyttäjän tietokoneen kiintolevyillä olevissa tiedostoissa ja tekee haittaohjelman löytämisen haastavammaksi, kuin jonkin muun haittaohjelman, joka toimii tiedostojen avulla. (What is malware? N.d.)

4 F-Secure Policy Manager

WithSecure on suomalainen yritys, joka tarjoaa tietoturvaratkaisuja yrityspuolella. Aiemmin WithSecure tunnettiin F-Securena, mutta vuoden 2022 muutoksen myötä, kun F-Secure jakaantui kahtia, yritys- ja kuluttajapuolelle, syntyi WithSecure, joka keskittyy yritystietoturvaliiketoimintaan ja kuluttajapuolesta tuli itsenäinen yhtiö, jonka emoyhtiönä toimii F-Secure Oyj. (About us N.d.)

F-Secure Policy Manager on yksi WithSecuren tarjoamista tuotteista, jolla voidaan mahdollistaa yritysasiakkaille keskitetty hallinta virusten torjuntaan eri käyttöjärjestelmille. Policy Manageria voidaan käyttää tietoturvakäytänteiden asettamiseen ja jakamiseen, virustorjuntaohjelman asennukseen paikallisesti tai etänä sekä monitoroimaan yrityksen järjestelmiä, jotka ovat keskitetyn hallinnan nähtävillä (Policy Manager Administrator's Guide N.d). Tällainen työkalu on hyvin hyödyllinen, koska se mahdollistaa useiden päätelaitteiden tietoturvakäytänteiden hallitsemisen vaikka vain yhdestä paikasta, josta on pääsy palvelimelle, jonne hallinta ollaan asennettu. F-Secure Policy Manager on hyvä vaihtoehto, jos yritykset tarvitsevat keskitetyn hallinnan työkalua, sillä se skaalautuu niin pienemmille kuin isommillekin yrityksille.

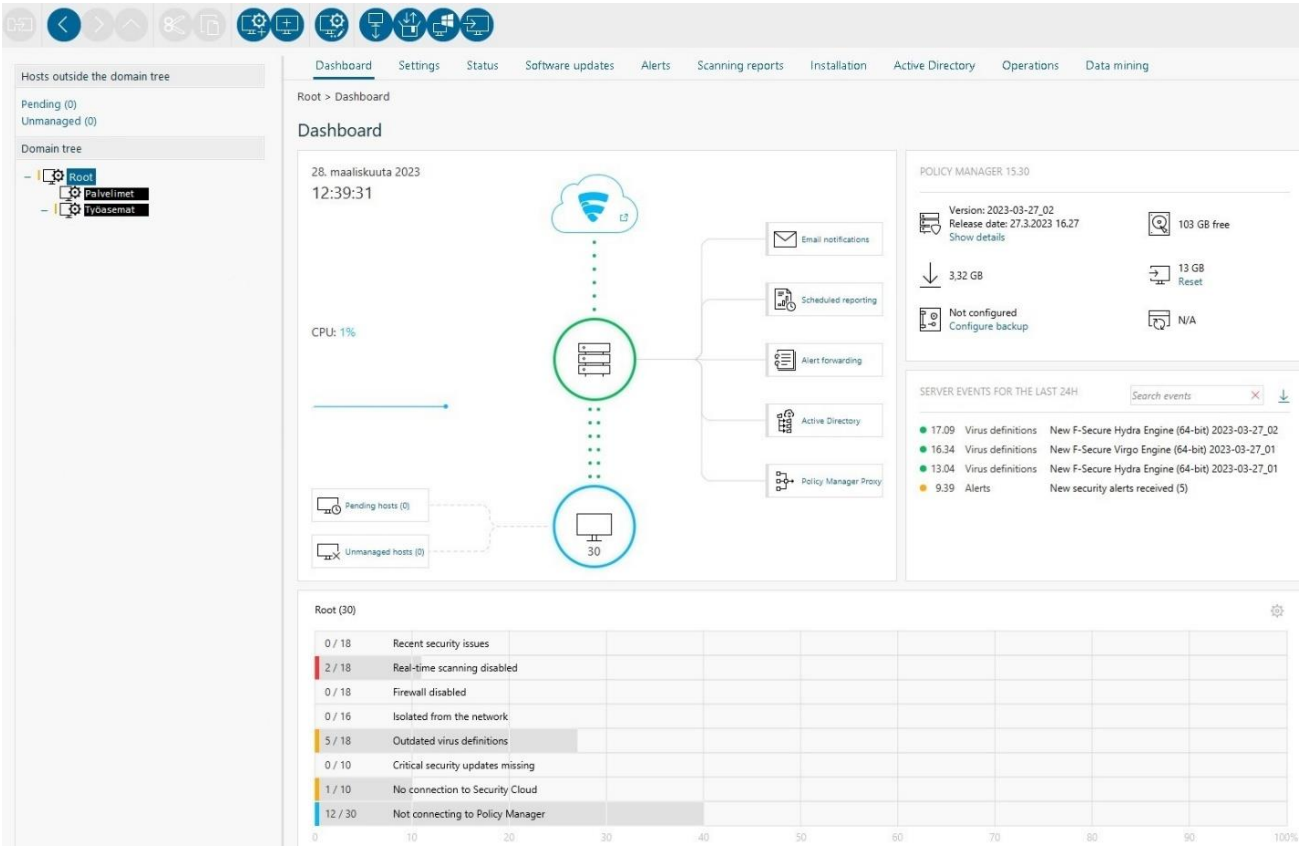
F-Secure Policy Manager koostuu kolmesta eri komponentista. Nämä ovat Policy Manager Console, Policy Manager Server ja Web Reporting. Päätelaitteilla tulee olla asennettuna käyttöjärjestelmälle sopiva Policy Manager Consolella luotu F-Secure Client Security, jotta päätelaite saadaan Policy Managerin hallintaan. Kuviossa 2 on luotu havainnollistava kuva F-Secure Policy Managerin toiminnasta ja komponenttien välisistä suhteista.



Kuvio 2 Kuvituskuva F-Secure Policy Managerin toiminnasta

4.1 Policy Manager Console

Policy Manager Console mahdollistaa keskitetyn hallinnan tietoturvaa varten verkossa oleville päätelaitteille. Policy Manager Consolen kautta voidaan määrittää tietyt tietoturvakäytänteet yksittäisille päätelaitteille tai luoda useamman päätelaitteen ryhmiä ja määrittää luodulle ryhmälle omat tietoturvakäytänteet. Jotta päätelaite saadaan Policy Manager Consolen hallintaan ja muokkaamaan sen tietoturvakäytänteitä, päätelaite tarvitsee käyttöjärjestelmälleen sopivan F-Secure Client Security -virustorjuntaohjelman. Virustorjuntaohjelman asennuspaketti luodaan Policy Manager Consolen kautta ja kun tällä asennuspaketilla asennetaan virustorjuntaohjelma käyttäjän laitteelle, se näkyy Policy Managerissa ja sitä voidaan hallita Policy Manager Consolen kautta sen jälkeen. Käytänteet määritellään Policy Manager Consolella ja ne jaetaan eteenpäin päätelaitteille Policy Manager Serverin kautta. Policy Manager Console on Java-pohjainen sovellus ja sitä voidaan käyttää Windows ja Linux -käyttöjärjestelmillä. Policy Manager Console toimii hallintatyökaluna Policy Manager Serverille. (Policy Manager Administrator's Guide N.d.). Kuviossa 3 on perusnäkymä Policy Manager Console -hallintaohjelmasta.



Kuvio 3 F-Secure Policy Manager Consolen perusnäkymä

4.2 Policy Manager Server

Policy Manager Server on arkisto sekä tietoturvakäytänteille että asennuspaketeille. Policy Manager Serverin tehtävänä on myös vastaanottaa hallittujen päätelaitteiden tila ja hälytykset. Tietoliikenne Policy Manager Serverin ja hallittujen päätelaitteiden välillä on suojattu HTTPS:n avulla, mutta HTTP-protokollan kautta käsitellään ei-arkaluontoiset tiedot, kuten virusten tunnistus tietokannan päivitykset. F-Secure Policy Manager on asennettavissa Windows- ja Linux-käyttöjärjestelmille. (Policy Manager Administrator's Guide N.d.)

4.3 Web reporting

Web reporting on verkon selaimella toimiva graafinen raportointialusta, joka on osana Policy Manager Serveriä. Tämän avulla voidaan luoda raportteja, jotka sisältävät yksityiskohtaisia tietoja keskitetyn hallinnan verkkoympäristöstä. Näihin tietoihin lukeutuvat muun muassa verkkoympäristön tapahtumat ja hälytykset. Web reporting -ominaisuuden avulla voidaan myös havaita mahdolliset suojaamattomat päätelaitteet. Web reporting vaatii tunnistautumista ja käyttämällä Policy Manager Consolen käyttäjätunnusta ja salasanaa, päästään käyttämään web reporting -sivustoa. Se toimii oletuksena Policy Manager Serverin osoitteessa portissa 8081. (Policy Manager Administrator's Guide N.d.)

5 Asennusvaihe

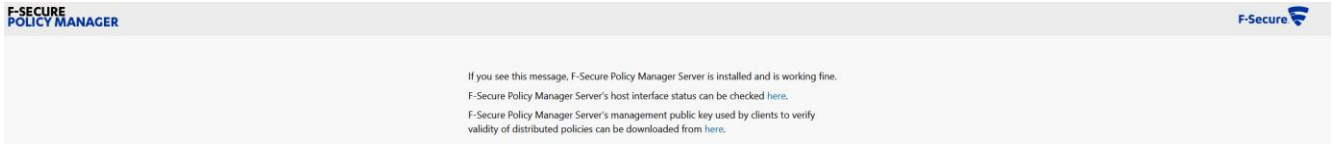
5.1 Policy Manager Serverin ja Consolen asennus

F-Secure Policy Managerin asennus on melko suoraviivainen, siihen löytyy hyvät ohjeet WithSecuren sivuilta ja asennusvaihe on toteutettu seuraamalla WithSecuren ohjetta.

Policy Manageria varten asennettiin palvelimelle uusin Windows Server käyttöjärjestelmä, eli Windows Server 2022. Windows Server 2022 valikoitui palvelimen käyttöjärjestelmäksi sen takia, että se sisältää muutaman ominaisuuden, mitä Linux ei tue, muun muassa Windows käyttöjärjestelmää käyttävien päätelaitteiden haku verkosta automaattisesti. Tätä ei otettu käyttöön vielä tämän opinnäytetyön aikana, mutta jos Policy Managerin toimintaa halutaan edistää eteenpäin, niin se on helpompaa tulevaisuudessa.

WithSecuren sivustolta ladattiin Policy Managerin asennuspaketti, F-Secure Policy Manager 15.30, ja se asennetaan palvelimelle. Kun asennuspaketin suorittaa, voidaan valita halutaanko sekä Policy Manager Server että Policy Manager Console asentaa samalle palvelimelle, vai asennetaanko Policy Manager Console jollekin toiselle päätelaitteelle. Tässä tilanteessa sekä Policy Manager Server että Policy Manager Console asennettiin samalle palvelimelle. Policy Manager Consolen voi siis myös halutessaan asentaa useammalle eri laitteelle, jos on tarve sille, että hallinta on käytettävissä useammalla laitteella. Tämän jälkeen seurasi vaiheet joissa kysyttiin minne polkuun ohjelmisto asennetaan, admin käyttäjä ja sen salasana, ja näiden vaiheiden jälkeen vielä halutut portit ja moduulit. Host -moduulia tarvitaan päätelaitteiden kanssa kommunikointiin, arkaluontoiset tiedot lähetetään HTTPS-protokollalla ja ei-arkaluontoiset HTTP:n kautta. Oletusportteina HTTP käyttää porttia 80 ja HTTPS porttia 443. Administration -moduulia käytetään kommunikoidakseen Policy Manager Consolen kanssa ja oletuksena se hyödyntää HTTPS:n porttia 8080. Asennusvaiheessa voidaan myös valita otetaanko web reporting käyttöön, oletusasetuksena sen portti on 8081. Oletuksena asennuksessa pääsy administrator -moduuliin on vain kyseiseltä koneelta, mille Policy Manager Console asennetaan. Jos Policy Manager Consolea haluaa käyttää joltain toiselta koneelta, täytyy asennusvaiheessa valita asetus, joka sallii pääsyn muilta laitteilta ja asentaa Policy Manager Console myös niihin laitteisiin.

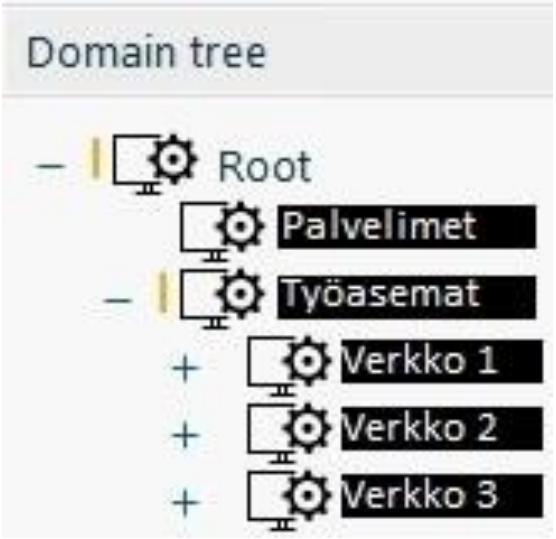
Näiden vaiheiden jälkeen F-Secure Policy Manager Server sekä Console tulisi olla asennettuna ja valmiina käyttöön. Tämän voi tarkastaa menemällä verkossa olevan laitteen selaimella Policy Managerin osoitteeseen ja sivuston tulisi ilmoittaa että Policy Manager Server on asennettu ja toimii, kuten kuviossa 4 näkyy. Tämän jälkeen käynnistä Policy Manager Console, kirjaudu sisään luomallasi tunnuksella ja sitä kautta päästään käsiksi Policy Manager Consoleen hallinnoimaan päätelaitteiden tietoturvakäytänteitä.



Kuvio 4 F-Secure Policy Manager asennettu palvelimelle

5.2 Policy domain

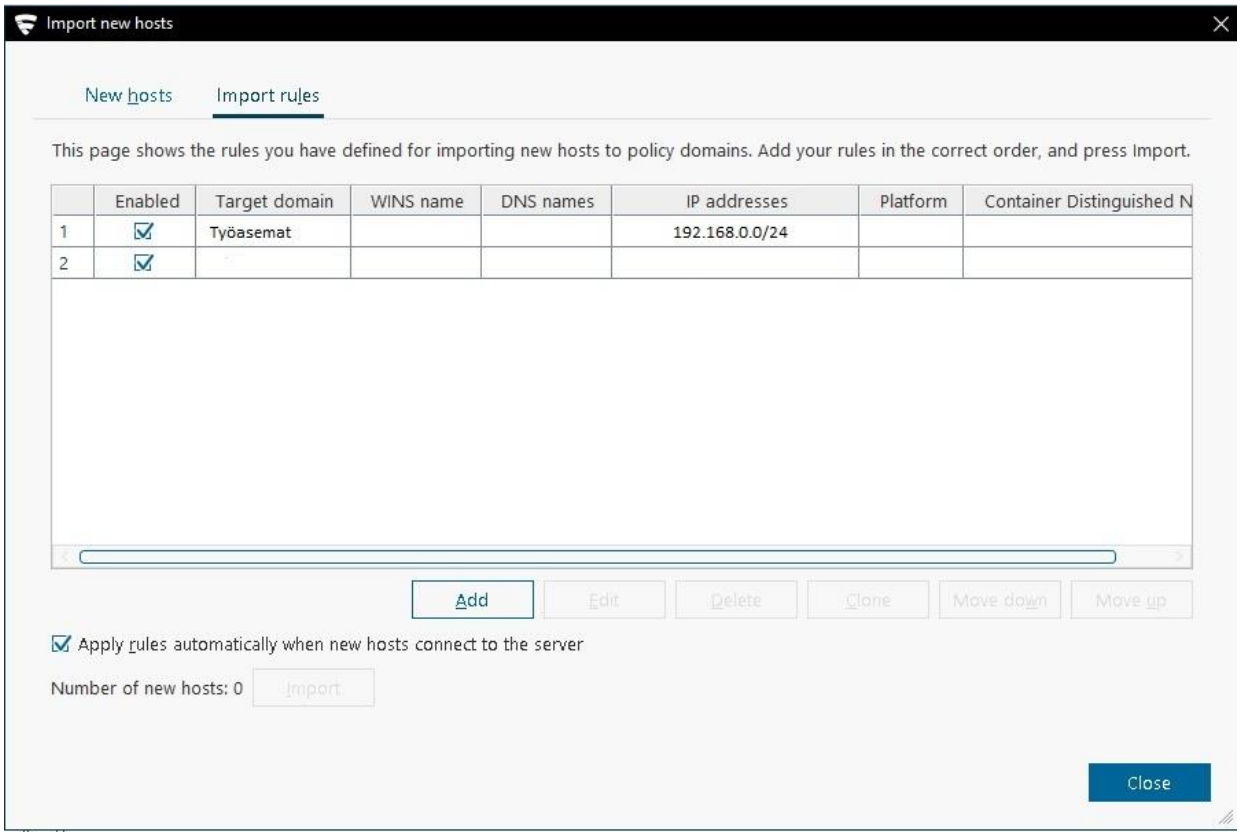
Policy Manager Consolessa voidaan luoda rakenne domain treen alle. Rakenteen avulla voidaan luoda eri ryhmiä verkossa olevia laitteita varten, esimerkiksi käyttäjien tietokoneet ja palvelimet, jotka ovat tuotu hallintaan asentamalla Policy Manager Consolen avulla tehdyllä virustorjuntaohjelmalla, joka on asennettu päätelaitteelle. Näitä luotuja ryhmiä kutsutaan policy domaineiksi. Järjestelmänvalvoja voi luoda jokaiselle policy domainille omat tietoturvakäytänteet tai vaihtoehtoisesti asettaa tietoturvakäytänteet yksitellen laitteille. Tietoturvakäytänteet periytyvät ylimmästä policy domainista sisempään policy domainiin. Esimerkiksi jos ”Root” on korkein ja ”Root” sisälle luodaan policy domain ”Työasemat”, ja kun ”Root”ille määritetään tietoturvakäytänteitä, niin ne periytyvät myös ”Työasemat” policy domainille ja sen sisällä oleviin laitteisiin. Kaikille ryhmille voidaan myös antaa omat käytänteet, jotka koskevat sen policy domainin sisäisiä laitteita. Kuviossa 5 nähdään esimerkki siitä, millaisen rakenteen domain treen alle voidaan luoda.



Kuvio 5 Domain tree ja luodut policy domainit

Policy domaineille voidaan antaa tunnisteita, joiden avulla päätelaitteet sijoitetaan oikean policy domainin alle. Tunnisteiksi voidaan antaa muun muassa päätelaitteen tarkka IP-osoite tai IP-avaruus. Jos tunnisteeksi annetaan esimerkiksi IP-avaruus, niin kaikki päätelaitteet, joille on määritetty IP-osoite annetusta IP-avaruudesta, sijoitetaan policy domainiin, jolle ollaan määritelty tunnisteeksi tämä IP-avaruus. Mikäli tunnisteita ei olla annettu ja päätelaitteelle ollaan asennettu

Policy Manager Consolella luotu Client Security, niin Policy Manager tunnistaa laitteen ja se menee niin kutsuttuun odotustilaan ja päätelaite voidaan sitten manuaalisesti sijoittaa jonkin policy domainin alle. Kuviossa 6 kuvattu tunnisteen lisääminen, jossa IP-avaruudeksi annettu 192.168.0.0/24 ja kaikki sen IP-avaruudessa toimivat päätelaitteet menevät ”Työasemat” policy domainin alle.



Kuvio 6 Tunnisteiden lisääminen policy domainille

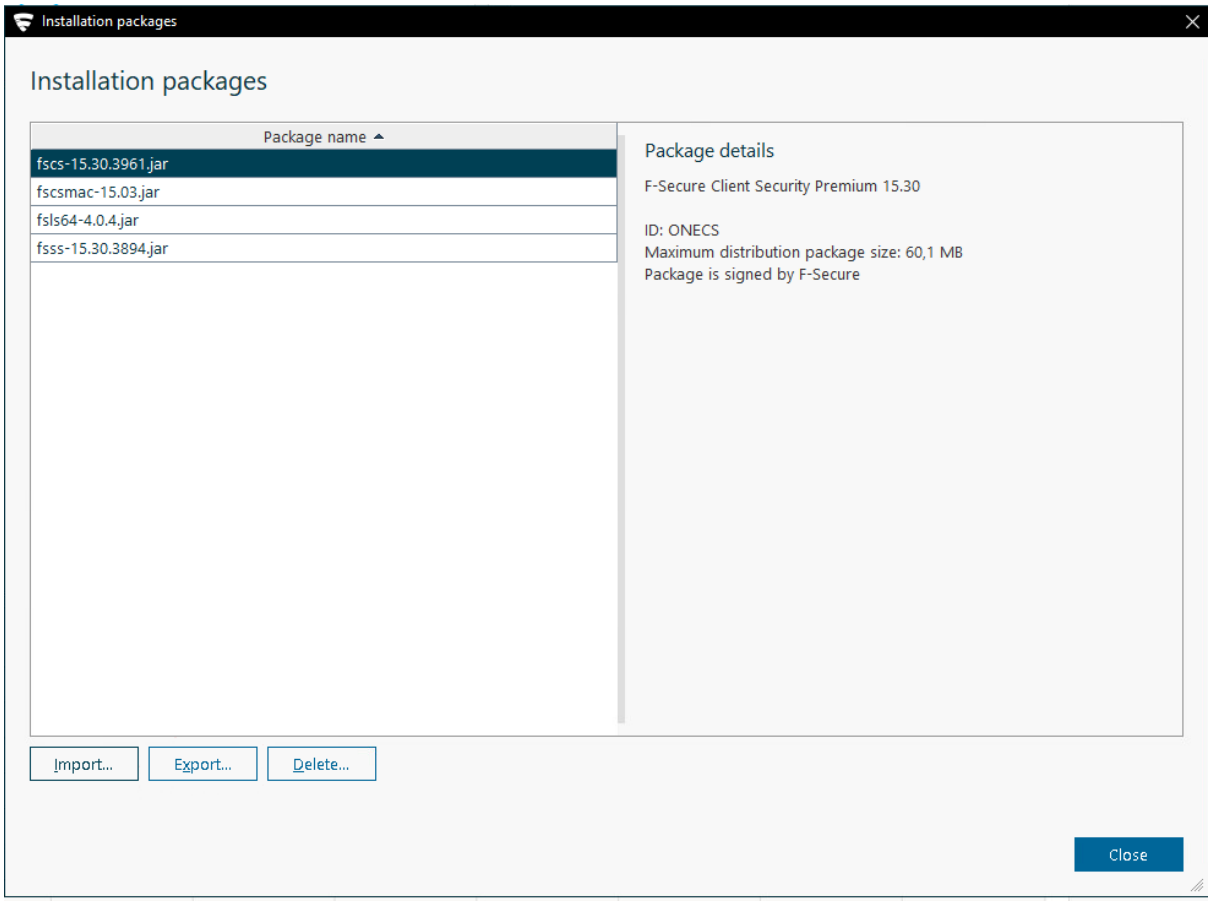
5.3 Virustorjuntaohjelmien asennuspaketit

Yrityksen verkkoympäristössä on käytössä sekä Windows-, Linux- että MacOS-käyttöjärjestelmillä olevia päätelaitteita, joten jokaiselle näistä täytyi ladata oma virustorjuntaohjelma ja luoda niistä asennuspaketit Policy Manager Consolen avulla. Windows -käyttöjärjestelmiä varten F-Secure Client Security 15.30, MacOS -käyttöjärjestelmille Client Security for Mac 15.03 ja Linux -käyttöjärjestelmille Linux Security. Myös palvelimille on mahdollista asentaa Server Security -niminen ohjelmisto, mutta niitä ei vielä tehty tämän toimeksiannon aikana vaan keskityttiin nimenomaan loppukäyttäjien päätelaitteiden virustorjuntaohjelmiin.

5.3.1 Asennuspakettien luonti

Koska yrityksen verkkoympäristössä on käytössä eri käyttöjärjestelmillä olevia päätelaitteita, jokaista käyttöjärjestelmää varten ladataan WithSecuren sivulta niille sopivat .jar -tiedostot. Windowsille Client Security, Linuxille Linux Security ja MacOS:lle Client Security for Mac. Kun kaikki tarvittavat .jar -tiedostot ovat ladattuina palvelimelle, niin niistä täytyy luoda kullekin käyttöjärjestelmälle sopiva ja suoritettava asennustiedosto Policy Manager Consolella, jotta virustorjuntaohjelma saadaan asennettua verkon päätelaitteille.

WithSecuren sivuilta ladatut .jar -päätteiset tiedostot täytyy ensiksi tuoda Policy Manager Consoleen. Tiedostojen tuominen tehdään pakettienhallintatyökalulla ”Installation packages” -kohdasta. ”Installation packages” -ikkuna aukeaa, valitaan ”Import”, jonka jälkeen haetaan .jar-tiedosto palvelimelta ja viedään se pakettienhallintaan. Tämän jälkeen tiedoston tulisi näkyä ”Installation packages” -ikkunassa, kuten kuviossa 7 näkyy.



Kuvio 7 Installation packages -ikkuna

Kun tiedostot saatiin tuotua Policy Manager Consoleen, valitaan se .jar-tiedosto, josta halutaan luoda asennuspaketti ja klikataan ”Export”. Valitaan mihin asennuspaketti tallennetaan ja painetaan taas ”Export”. Tämän jälkeen aukeaa ohjattu asennus F-Secure Client Securitya varten, jossa määritellään lisenssiavain, mitä ominaisuuksia halutaan asentaa, voidaan valita oletuskäytänteet tai jokin luoduista policy domaineista sekä määritetään keskitettyä hallintaa varten Policy Manager Serverin osoite, jotta virustorjuntaohjelman asennettua päätelaite saa yhteyden palvelimelle. Kun ohjattu asennus on suoritettu loppuun, voidaan luotu asennuspaketti viedä päätelaitteelle halutulla tavalla. Liitteessä 1 kuvattu koko F-Secure Client Securityn ohjatun asennuksen vaihe asennuspaketin luontia varten.

5.3.2 Asennuspakettien jako

Virustorjuntaohjelman asennuspaketin jakamista varten on kolme eri vaihtoehtoa. Yksi vaihtoehto on sellainen, että Windowsia käyttäville päätelaitteille voidaan niin sanotusti työntää asennuspaketti joko IP-osoitteen tai tietokoneen host-nimen perusteella. Toinen vaihtoehto on se että, jos päätelaitteilla on jo ennaltaan ollut F-Secure Management Agent, niin asennus olisi mahdollista myös sen avulla. Kolmas, ja myös tässä opinnäytetyössä käytetty vaihtoehto, on asentaa asennuspaketti päätelaitteille paikallisesti. Tässä hyödynnettiin yrityksen verkkoympäristössä olevaa palvelinta, jonne virustorjuntaohjelmien asennuspaketit ladattiin ja loppukäyttäjät pystyivät itse lataamaan omalle käyttöjärjestelmälle sopivan asennuspaketin ja asentamaan virustorjuntaohjelman omalle tietokoneelle. Kun koneelle on asennettu virustorjuntaohjelma, joka on luotu Policy Manager Consolen avulla niin Policy Manager tunnistaa kyseisen laitteen. Kun Policy Manager tunnistaa laitteen, se lisää sen hallinnan alle joko automaattisesti johonkin policy domainiin, jos asennuspakettia luodessa ollaan annettu jokin policy domain tai mikäli laite tunnistetaan jollain tunnisteella tai vaihtoehtoisesti järjestelmänvalvoja määrittää manuaalisesti laitteen jonkun luodun policy domainin alle tai antaa sille yksilöidyt tietoturvakäytänteet.

5.4 MacOS sertifikaatti

Asentaessa F-Secure Client Security -virustorjuntaohjelmaa MacOS -käyttöjärjestelmää käyttäville päätelaitteille, tuli vastaan ongelma. Päätelaite tuli näkyviin Policy Manager Consolen hallintaan, mutta niiden välillä ei liikkunut tietoja, joten päätelaitteelta jäi aina saamatta uusimmat

tietoturvapäivitykset. Tämän pystyy tarkistamaan siten, että kun menee kyseisellä MacOS-laitteella Policy Manager Serverin osoitteeseen, ja jos sivustoa aukaistaessa tulee varoitus sertifikaatista, niin tällöin se ei toimi oikein.

Ongelma saatiin ratkaistua siten, että haetaan Policy Manager Serveriltä CA-sertifikaatti, viedään se MacOS-laitteelle ja lisätään Policy Manager Serveriltä saatu CA-sertifikaatti MacOS:n järjestelmän keychainiin, jotta laite luottaa yhteyteen.

Joten, ensin täytyy hakea sertifikaatti Policy Manager Serveriltä, ja koska palvelimelle asennettiin Windows Server -käyttöjärjestelmä, saadaan sertifikaatti tuotua palvelimelle seuraavalla komennolla:

> *”c:\Program Files (x86\F-Secure\Management Server\jre\bin\keytool.exe” -keystore “c:\Program Files (x86)\F-Secure\Management Server 5\data\fspms-ca.jks” -alias fspm-ca -exportcert -file fspms-ca.cer -rfc -protected* (Resolving connectivity issues between Client Security for Mac and Policy Manager 2022.)

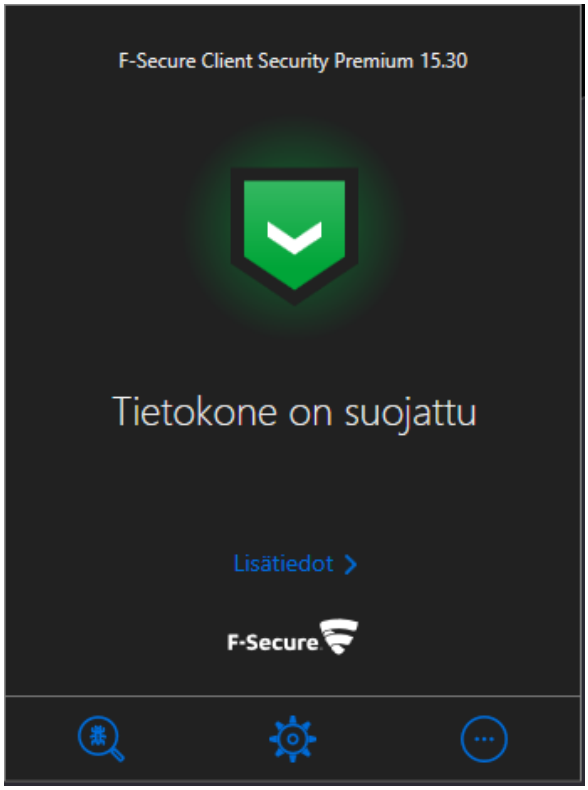
Kun sertifikaatti on saatu palvelimelta, täytyy serfitikaatti ensiksi siirtää Mac-päätelaitteille ja sitten vielä lisätä se käyttöjärjestelmän luotettuihin sertifikaatteihin. Sertifikaatin lisääminen luotettuihin sertifikaatteihin onnistuu seuraavalla komennolla:

> *”sudo security add-trusted-cert -d -r trustRoot -p ssl -k “/Library/Keychains/System.keychain” “tiedostopolku/fpsms-ca.cer”* (Resolving connectivity issues between Client Security for Mac and Policy Manager 2022.)

Sertifikaatin lisäämisen jälkeen tulisi yhteys Policy Manager Serverin ja Mac-päätelaitteiden välillä toimia. Sen voi tarkistaa menemällä Mac-päätelaitteella Policy Manager Serverin osoitteeseen ja yhteyden ollessa luotettava varoitusta sertifikaatista ei pitäisi enää tulla.

6 F-Secure Client Security -virustorjuntaohjelma

F-Secure Client Security on päätelaitteille asennettava virustorjuntaohjelma. Virustorjuntaohjelman tehtävänä on suojata, havaita ja estää haitallisia tiedostoja sekä ohjelmia pääsemästä laitteelle sekä suojata päätelaitetta ohjelmilta, jotka voivat vahingoittaa tietokonetta tai varastaa esimerkiksi henkilökohtaisia tietoja. Tavoitteena on se, että virustorjuntaohjelma onnistuu estämään haitalliset tiedostot tai ohjelmat ennenkuin mitään haitallista on tapahtunut. (WithSecure Client Security for Windows. N.d). Kuviossa 8 on esitettynä F-Secure Client Securityn onnistunut asennus Windows -päätelaitteelle.



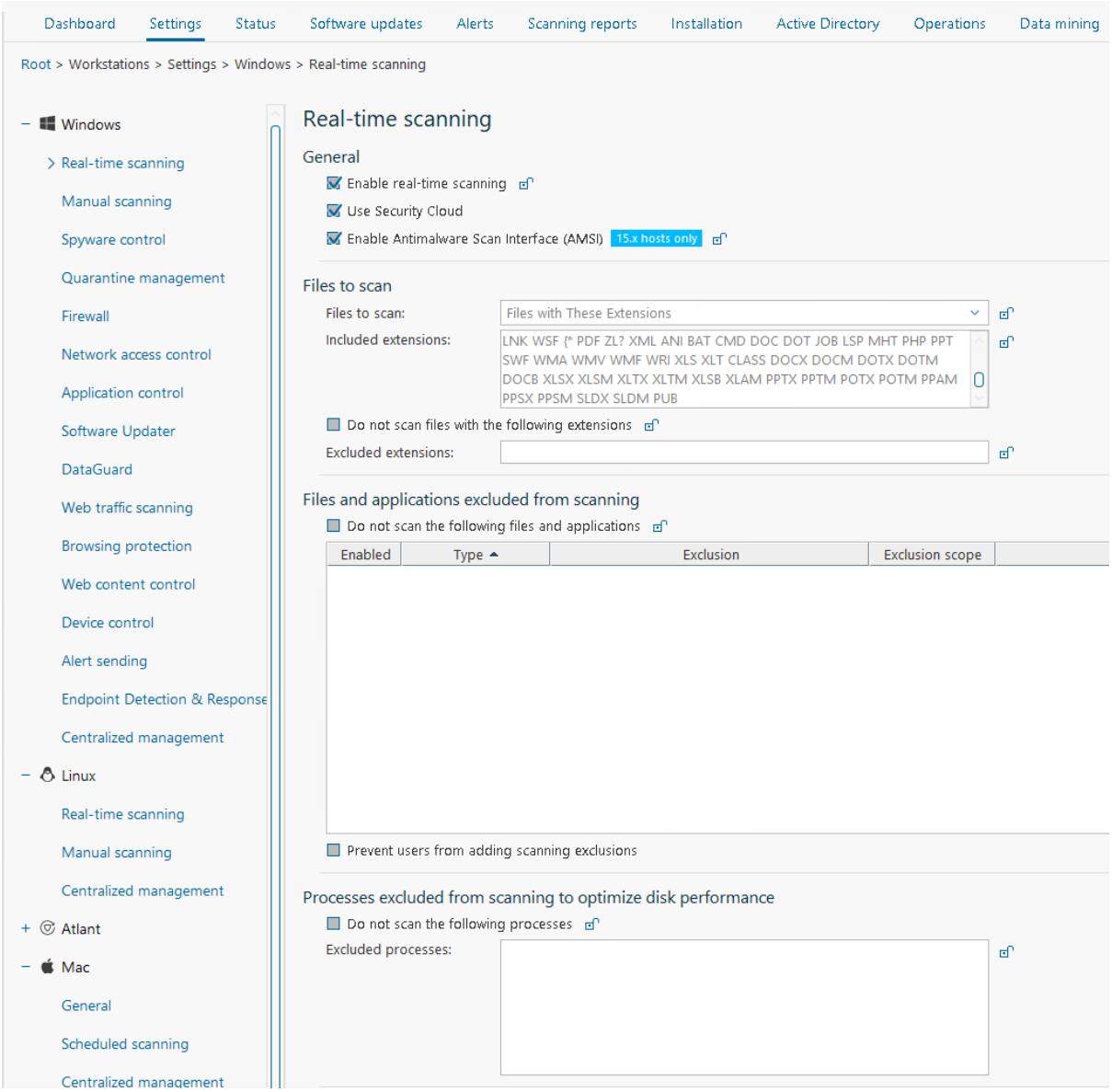
Kuvio 8 F-Secure Client Security

6.1 Asetukset

Kun virustorjuntaohjelmat ovat saatu asennettua ympäristön päätelaitteille, päästään hallinnoimaan ja ottamaan käyttöön sen tarjoamia asetuksia ja tarvittaessa koventamaan niitä. Tämän luvun kappaleissa käydään läpi F-Secure Client Securityn sisältämiä asetuksia yleisellä tasolla, mitä voidaan hallita keskitetysti ja sitä että mikä on minkäkin asetuksen tehtävä. Asetuksia

otetaan käyttöön ja muokataan Policy Manager Consolen kautta. Asetuksia voidaan lukita siten, että käyttäjä ei itse pysty muokkaamaan tai ottamaan niitä pois käytöstä, vaan ainoastaan järjestelmänvalvoja voi muokata tai ottaa pois käytöstä asetuksia Policy Manager Consolella.

Päätelaitteen käyttöjärjestelmästä riippuen saatavilla on hieman eri määrä asetuksia. Windows -käyttöjärjestelmälle on tarjolla kaikki asetukset, Linux- ja Mac -käyttöjärjestelmille saatavilla olevat asetukset ovat hyvin rajalliset verrattuna Windows -käyttöjärjestelmällä oleville, kuten kuviossa 9 näkyy. Lisäksi osa asetuksista on saatavilla vain premium-lisenssillä. Perusversion ja premium-version ominaisuudet ja eroavaisuudet kuvattu kuviossa 10.



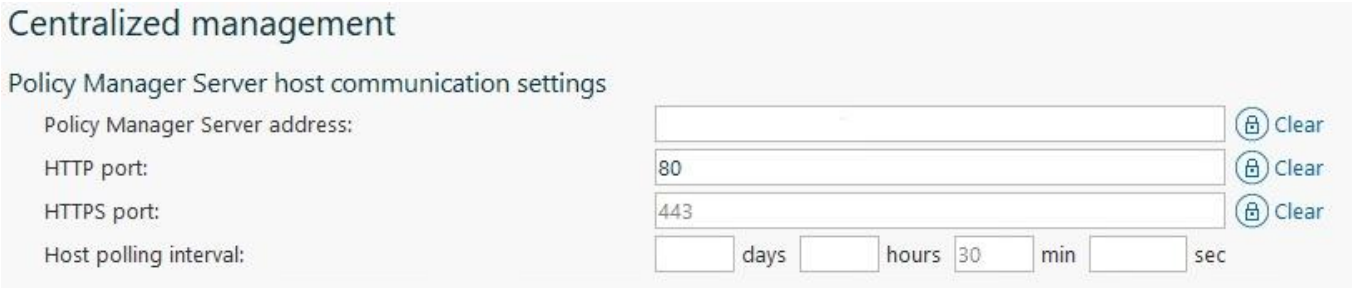
Kuvio 9 Kuva saatavilla olevista asetuksista

Feature	F-Secure Client Security Standard	F-Secure Client Security Premium
Virus & spyware protection	•	•
DeepGuard™	•	•
DataGuard		•
Application control		•
Web traffic scanning	•	•
Firewall	•	•
Browsing protection	•	•
Botnet Blocker	•	•
Device control	•	•
Offload Scanning Agent	•	•
Software Updater		•
Connection control		•
Web content control		•
Rapid Detection & Response	•	•

Kuvio 10 Lisenssien ominaisuuksien vertailu (Release Notes N.d.)

6.1.1 Keskitetty hallinta

Keskitetty hallinta on yksi oleellisimmista asetuksista. Sinne määritetään Policy Manager Serverin tiedot, eli palvelimen osoite, jolle Policy Manager Server on asennettu, ja HTTP- sekä HTTPS-portti, jotka määritettiin myös asennusvaiheessa. Näiden avulla päätelaite saa yhteyden Policy Manager Serverille. Päätelaite ottaa yhteyttä palvelimelle määritetyn ajan välein, mitä voidaan itse säätää, ja saa tätä kautta palvelimelta uusimmat päivitykset ja määritetyt käytänteet. Jos jokin päätelaite ei enää saa yhteyttä palvelimeen, niin sekin saadaan tietoon. Tarvittavat asetukset keskitettyä hallintaa varten kuviossa 11.



Kuvio 11 Keskitetyn hallinnan asetukset

6.1.2 Tiedostojen skannaus

Reaaliaikainen skannaus on jatkuvasti taustalla käynnissä oleva tiedostojen skannaus ja sen tehtävänä on suojata tietokonetta haitallisilta tiedostoilta. Se skannaa tiedostot taustalla haittaohjelmien varalta ennenkuin tiedostoja käsitellään. Jos tarkistuksen aikana havaitaan jokin haitallinen tiedosto tai ohjelma, niin se asetetaan niin kutsuttuun karanteeniin. (Policy Manager Administrator's Guide N.d.)

Myös manuaalinen skannaus on mahdollinen. Manuaalisen skannauksen käyttäjä voi itse suorittaa omalta henkilökohtaiselta päätelaitteelta tai järjestelmänvalvoja voi myös suorittaa skannauksen etänä Policy Manager Consolesta tai luoda ajoitettuja skannauksia päätelaitteelle esimerkiksi viikottain tiettynä ajankohtana. Näissä tapauksissa voidaan määrittää se että, halutaanko skannaus ajaa vain jollekin tietylle tiedostolle tai ohjelmalle vai ajetaanko skannaus kaikille tietokoneen tiedostoille. (Policy Manager Administrator's Guide N.d.)

6.1.3 DeepGuard

DeepGuard on laitekohtainen tunkeutumisen estojärjestelmä (IPS, Intrusion Preventation System), joka monitoroi tiedostoja ja ohjelmia sekä niiden käyttäytymistä. DeepGuardin tehtävä on estää haitallisien muutoksien tekeminen järjestelmään. Se tarkistaa ohjelmien turvallisuuden luotetusta pilvipalvelusaata ja jos sovelluksen turvallisuutta ei voida varmistaa, DeepGuard monitoroi haitallisen sovelluksen käyttäytymistä tarkemmin. (Policy Manager Administrator's Guide N.d.)

DataGuard on DeepGuardin lisäominaisuus, joka auttaa vahvistamaan DeepGuardin tuomaa suojaa valvomalla päätelaitteiden tiettyjä kansioita sovelluksilta, jotka eivät ole luotettavia. Policy

Manager Consolen kautta voidaan määrittää halutut kansiot, joita DataGuard suojaa. Sovellukset, jotka eivät ole luotettavia, pysäytetään, mikäli ne pyrkivät muokkaamaan suojattuja kansioita ja tiedostoja. (Policy Manager Administrator's Guide N.d.)

6.1.4 Palomuuri

Palomuurin tehtävänä on estää päätelaitteen luvaton käyttö internetistä kuten myös mahdolliset hyökkäykset omasta sisäverkosta. F-Securen tarjoamat uudemmat versiot Client Securitystä käyttää Windowsin omaa palomuuria hyödyksi, eikä näin ollen asenna erillisiä ohjelmistoja Client Securityn lisäksi. Tämä muutos on ollut voimassa versiosta 14.00 lähtien eli aikaisemmissa versioissa F-Secure käytti heidän omaa palomuuriaan. Palomuurin asetukset tarjoaa oletuksena kolmea eri vaihtoehtoa, joissa ovat hieman eriävät suojaukset. Oletusvaihtoehdot ovat mobiili, palvelin sekä toimisto. Järjestelmänvalvoja voi määrittää, mitä asetuksia käytetään milläkin päätelaitteella ja näitä voidaan myös koventaa järjestelmänvalvojan toimesta. (Policy Manager Administrator's Guide N.d.)

6.1.5 Verkkoliikenteen suojaus

HTTP-verkkoliikenteen suojaamista käytetään suojana viruksia vastaan HTTP-verkkoliikenteessä. Ominaisuuden avulla suojataan päätelaitetta skannaamalla HTML- ja kuvatiedostoja, suoritettavia tiedostoja ja ladattuja tiedostoja. Asetuksissa voidaan itse määrittää, mitä sisältöä tuntemattomilta sivustoilta halutaan estää. Näihin lukeutuvat muun muassa suoritettavat ohjelmat ja Adobe Flash- ja Microsoft Office -tiedostot. (Policy Manager Administrator's Guide

N.d). Verkkoliikenteen suojaus määrittelee linkkien turvallisuuden kuvion 12 mukaisiin kategorioihin.

Unknown/unrated	• URLs that have not yet been analyzed • URLs that are inaccessible at the time of testing
Safe	• URLs that have been analyzed as safe • URLs where users can knowingly download spyware, riskware, or adware
Suspicious	• URLs that are linked to spamming activities • URLs that are linked to scam-like activities
Malicious	• URLs where the content contains script codes that download or install a malicious file • URLs that belong to drive-by download sites • URLs where the content exploits browser or system vulnerabilities • URLs or content that contain XSS or SQL injections • URLs where the content contains malicious iframes • URLs that belong to phishing sites • URLs that are linked to hacking and other malicious activities • URLs that have been taken down due to malicious behavior

Kuvio 12 Verkkoliikenteen suojauksen kriteerit linkeille (Policy Manager Administrator's Guide N.d.)

Verkkoselauksen suojaamisen tarkoituksena on suojata käyttäjän verkkoselaimien käyttö estämällä pääsy verkkosivustoille, jotka ovat arvioitu haitallisiksi. Haitallisiksi sivustoiksi voidaan luokitella esimerkiksi tunnetut spämmi- tai huijaussivustot. Verkkosisällön hallinnalla voidaan estää verkkosivustoja, jotka sisältävät jotain tietynlaista sisältöä, kuten uhkapelaamista tai muuta, mikä voidaan luokitella haitalliseksi. (Policy Manager Administrator's Guide N.d.)

6.1.6 Ohjelmistojen hallinta

Ohjelmistojen hallinnan avulla voidaan estää sovelluksien asentaminen ja niiden suorittaminen, sekä estää skriptien suorittaminen. Tämän avulla saadaan vähennettyä haitallisia ja luvattomia toimintoja yrityksen verkkoympäristössä. Kyseinen ominaisuus on saatavilla vain versioille 14.00 ja sitä uudemmille. (Policy Manager Administrator's Guide N.d.)

6.1.7 Laitehallinta

Laitehallinnalla voidaan halutessaan estää ulkopuolisten laitteiden käyttö päätelaitteilla. Ulkopuolisiin laitteisiin lukeutuvat muun muassa CD- ja DVD-levyt, USB-massamuistilaitteet (ulkoinen kiintolevy tai muistitikku) tai langattomat Bluetooth-laitteet. Jos laite on estetty laitehallinnalla ja käyttäjä yrittää liittää estetyn laitteen työasemaan, niin sen tehtävänä on estää ulkopuolisen laitteen pääsy järjestelmään. Ulkopuolisia laitteita estetään siitä syystä, että niiden avulla hyökkääjät voivat levittää haittaohjelmia, eikä käyttäjien tulisi muutenkaan kytkeä päätelaitteeseen sellaisia ulkopuolisia laitteita, jotka ovat heille tuntemattomia.

Laitehallinnalla voidaan myös määritellä oikeuksia ulkoisille muistilaitteille. Niille voidaan antaa oikeus olla vain luku -tilassa, niille voidaan antaa kirjoitusoikeudet, eli tiedostoja voidaan kopioida ulkoiselta levyltä koneelle tai niille voidaan antaa myös suoritusoikeudet, jolloin suoritettavia tiedostoja voidaan ajaa ulkoiselta levyltä. (Policy Manager Administrator’s Guide N.d.)

6.1.8 Endpoint Detection and Response

F-Secure Endpoint Detection and Response toimii sensorien avulla, jotka ovat asennettuina päätelaitteille, ja ne ovat osana virustorjuntaohjelmia, versioista Client Security 14.10 ja Server Security 14.00 alkaen. Sensorien tehtävänä on kerätä päätelaitteilta tietoja muun muassa tiedostoista, prosesseista tai järjestelmälokeista. Nykypäivänä on yleistynyt se, että hyökkäykset voivat olla sellaisia, että se ei vaadi erillisiä haittaohjelmia päätelaitteelle. Endpoint Detection and Response tarjoaa suojaa edistyneemmiltä hyökkäyksiltä ja uhilta jo, ennenkuin ne ovat tapahtuneet. (Policy Manager Administrator’s Guide N.d.)

7 Tulokset

Toimeksiantajan tehtävänä oli asentaa yrityksen verkkoympäristöön keskitetyn tietoturvan hallintatyökalu, F-Secure Policy Manager ja virustorjuntaohjelmat, F-Secure Client Security/Linux Security, käyttäjien päätelaitteille ja tuottaa yrityksen järjestelmänvalvojille dokumentaatio ylläpitotehtäviä varten. Annetun työtehtävän aikana oli myös tarkoitus saada kerättyä tietoa ja materiaalia sitä varten, että siitä saa tehtyä opinnäytetyön. Tämä opinnäytetyö voi toimia tukena asennusvaiheessa kenelle tahansa.

Tuloksena saatiin ympäristöön toimiva F-Secure Policy Manager asennettua ja käyttäjien päätelaitteille F-Secure Client Security -virustorjuntaohjelmat asennettua eri käyttöjärjestelmille. F-Secure Policy Manager toimii ympäristössä niinkuin pitääkin ja virustorjuntaohjelmat myös toimivat ja tekevät oman työnsä estääkseen haitallisia tiedostoja pääsemästä päätelaitteille. Policy Managerin avulla voidaan monitoroida verkkoympäristön tapahtumia, voidaan luoda virustorjuntaohjelman asennuspaketit ja sitä kautta saadaan päätelaitteet näkyville Policy Manager Consoleen. Policy Manager Serverin ja Consolen asentaminen onnistui hyvin ja virustorjuntaohjelmien asentaminenkin sujui lähes moitteetta, ainoastaan MacOS -laitteiden kanssa pieniä haasteita, mutta sekin saatiin ratkaistua. Myös asetuksia ja niiden koventamista testattiin, ja niiden avulla voidaan luoda tiukat tietoturvakäytänteet käytössä oleville päätelaitteille. Kaikkia toimintoja ei voida rajoittaa, koska yrityksen verkkoympäristössä tehdään monia asioita, joten käyttäjille itselleen jäi mahdollisuus ottaa näitä käytänteitä väliaikaisesti pois käytöstä. Oleellisinta on kuitenkin se, että järjestelmänvalvojilla on näkymä siitä, mitä verkossa olevilla päätelaitteilla tehdään ja jonkun haitallisen tiedoston havaitessaan, voidaan selvittää onko se ollut tarkoituksellista vai onko kyseessä oikeasti jokin haitallinen tiedosto tai ohjelma.

Opinnäytetyön näkökulma painottuu tietoturvaan ja tutkimuskysymyksenä oli ”Miten F-Secure Policy Manager parantaa yrityksen tietoturvaa?”. F-Secure Policy Managerin avulla saadaan parannettua yrityksen tietoturvaa, koska käyttäjien päätelaitteille asennettiin myös virustorjuntaohjelmat. Virustorjuntaohjelman tehtävänä on turvata käyttäjien turvallinen verkon käyttö muun muassa tarkistamalla ajoittain päätelaitteilla olevat tiedostot ja estämällä haitallisien tiedostojen toiminta.

Virustorjuntaohjelmien asennuksen jälkeen, niiden toimivuus testattiin siten, että havaitseeko virustorjuntaohjelma haittaohjelmia. Tämä toteutettiin hyödyntämällä eicar-testihaittaohjelmaa ja virustorjunta ohjelma tunnisti haittaohjelman ja siitä tuli hälytys Policy Manager Consolen hallintanäkymään. Testausvaiheessa kokeiltiin myös koventaa tietoturvakäytänteitä, muun muassa estämällä ulkopuolisten massamuistilaitteiden liittämisen koneeseen ja estää käyttäjää tekemästä muutoksia F-Secure Client Securityn asetuksiin. Lisäksi tiedostojen skannaus kokeiltiin suorittaa etänä ja paikallisesti käyttäjän päätelaitteelta, joista saatiin raportit ulos web reporting -sivustolle. Virustorjuntaohjelman toimivuuden kerkesin nähdä myös varsinaisessa käytössä ja sen avulla nähtiin hälytyksiä, joissa oltiin käytetty jotain tuntematonta sovellusta.

Näin ollen toimeksiantajan antamaan tehtävään vastattiin heidän haluamallaan tavalla. Järjestelmänvalvojia varten luotu ylläpito-ohje opastaa heitä, kuinka järjestelmää käytetään ja ylläpidetään. Opinnäytetyötä voi hyödyntää myös siten, että voi tutustua F-Secure Policy Manageriin ja sen toimintaan ja mitä ominaisuuksia F-Secure Client Security -virustorjuntaohjelma sisältää.

8 Pohdinta

Tietoturva on nykypäivänä hyvin oleellinen asia, koska se on lähes jatkuvasti esillä niin yritysmaailmassa kuin tavallisilla kuluttajilla. Usein uutisissa tai sosiaalisessa mediassakin varoitetaan käyttäjiä huijausyrityksistä ja uutisoidaan tapahtuneista hyökkäyksistä ja tietovuodoista. Koska hyökkäyksiä on monenlaisia, tulisi jokaisen yrityksen ja yksilönkin pyrkiä turvaamaan oma toimintansa verkossa, esimerkiksi virustorjuntaohjelmilla ja hankkimalla sekä ylläpitämällä perusymmärrystä tietoturvasta, sillä tänä päivänä melkein kaikki tieto liikkuu verkon välityksellä.

Yrityksen antama toimeksianto oli hyvin selkeä ja suoraviivainen. Toimeksiantona oli asentaa yrityksen verkkoympäristöön F-Secure Policy Manager keskitettyä hallintaa varten ja päätelaitteille F-Securen tarjoama Client Security virustorjuntaohjelma. Ohjelmistojen asentaminen ympäristöön oli yksinkertaista eikä tuottanut isompia haasteita, koska WithSecuren sivuilta löytyvät ohjeet ovat hyvin selkeät ja kattavat. Ainoa haasteellisempi ja enemmän työtä tuotti MacOS:ä käyttävät päätelaitteet, sillä uudemmissa Client Security for Mac versioissa, Client Security ei pääse muokkaamaan MacOS -käyttöjärjestelmän luotettuja sertifikaatteja, vaan tämä täytyi suorittaa manuaalisesti. Tähänkin ongelmaan onneksi löytyi ratkaisu ja MacOS laitteet saatiin myös keskitetyn hallinnan alle. Tehtävä kuitenkin onnistui mielestäni hyvin ja työn päästiin haluttuun lopputulokseen. Itselleni tämän tyylinen konkreettinen työtehtävä oli mieluisa.

Opinnäytetyön kannalta hieman haasteellista on se että, kuinka rajata kyseistä aihetta ja millaisella näkökulmalla lähestytään aiheeseen. Koska aiheena on keskitetyn tietoturvan hallintatyökalu, jolla määritetään tietoturvakäytänteitä ja hallitaan virustorjuntaohjelmaa, niin päädyin tekemään opinnäytetyön tutkien sitä enemmän tietoturvan näkökulmasta ja onnistuin siinä mielestäni hyvin.

Policy Managerin avulla saadaan keskitetty hallinta verkossa oleville laitteille, johon ollaan asennettu virustorjuntaohjelma. Keskitetyllä hallinnalla saadaan näkymä näille laitteille ja Policy Manager Consolella nähdään, jos virustorjuntaohjelma on havainnut jollain päätelaitteella haitallisia tiedostoja, ja toiminut siten määrittämien asetusten mukaan. Verkkoympäristön päätelaitteiden tietoturvakäytänteitä voidaan tarvittaessa koventaa Policy Manager Consolen avulla helposti.

Myöskin järjestelmänvalvojien työtehtävät helpottuu ja ne vievät vähemmän aikaa, koska F-Secure Policy Managerin avulla voidaan hallita laitteiden tietoturvakäytänteitä keskitetysti. Myös päätelaitteiden hälytykset voidaan havaita helposti Policy Manager Consolesta tai Web reporting -sivuston kautta.

Lähteet

About us. N.d. Verkkosivu. Viitattu 2.5.2023. https://investors.f-secure.com/en/about_us/history

Antivirus. N.d. Verkkosivu. Viitattu 28.4.2023. https://www.verizon.com/articles/internet-essentials/antivirus-definition/.

Antivirus Software. N.d. Verkkosivu. Viitattu 11.5.2023. https://www.malwarebytes.com/antivirus.

Dosal, E. 2019. What Are Administrative Security Controls? Verkkosivu. Viitattu 4.5.2023. https://www.compuquip.com/blog/what-are-administrative-security-controls.

Information Security: The Ultimate Guide. N.d. Verkkosivu. Viitattu 6.4.2023. https://www.imperva.com/learn/data-security/information-security-infosec/.

Mitä on fyysinen tietoturvallisuus? 2021. Verkkosivu. Viitatattu 4.5.2023. https://blog.seclion.fi/turvallisuus/fyysinen-tietoturvallisuus.

Opinnäytetyö – Thesis. N.d. Oppimateriaali. Viitattu 10.5.2023. https://oppimateriaalit.jamk.fi/opinnaytetyo/toteutustavat-ja-rakenne/palvelu-tuote-produktio/.

Oza, S. N.d. CIA Triad: Best Practices for Securing Your Org. Verkkosivu. Viitattu 10.4.2023. https://spanning.com/blog/cia-triad-best-practices-securing-your-org/.

Policy Manager Administrator's Guide. N.d. Käyttöohje. Viitattu 6.4.2023. https://help.f-secure.com/data/pdf/fspm-15.30-adminguide-eng.pdf.

Release Notes. N.d. Verkkosivu. Viitattu 13.5.2023. https://help.f-secure.com/product.html?business/releasenotes-business/latest/en/fscs-latest-en.

Resolving connectivity issues between Client Security for Mac and Policy Manager. 2022. Verkkosivu. Viitattu 2.5.2023. https://community.withsecure.com/fi/kb/articles/8933-resolving-connectivity-issues-between-client-security-for-mac-and-policy-manager.

Tietoturva. 2020. Verkkosivu. Viitattu 6.4.2023. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

What is malware? N.d. Verkkosivu. Viitattu 11.5.2023. https://www.cisco.com/site/us/en/products/security/what-is-malware.html.

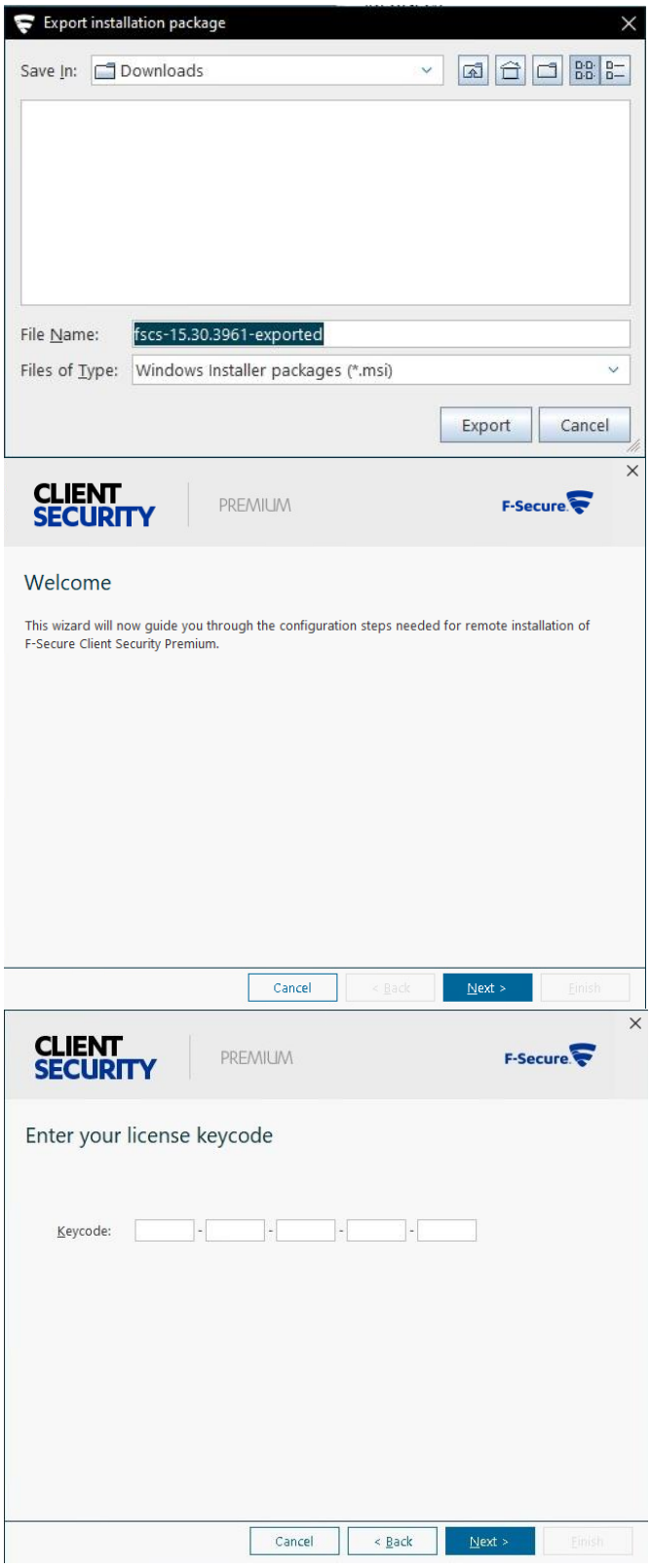
What Is Centralized Management? N.d. Verkkosivu. Viitattu 6.4.2023. https://www.fortinet.com/resources/cyberglossary/centralized-management.

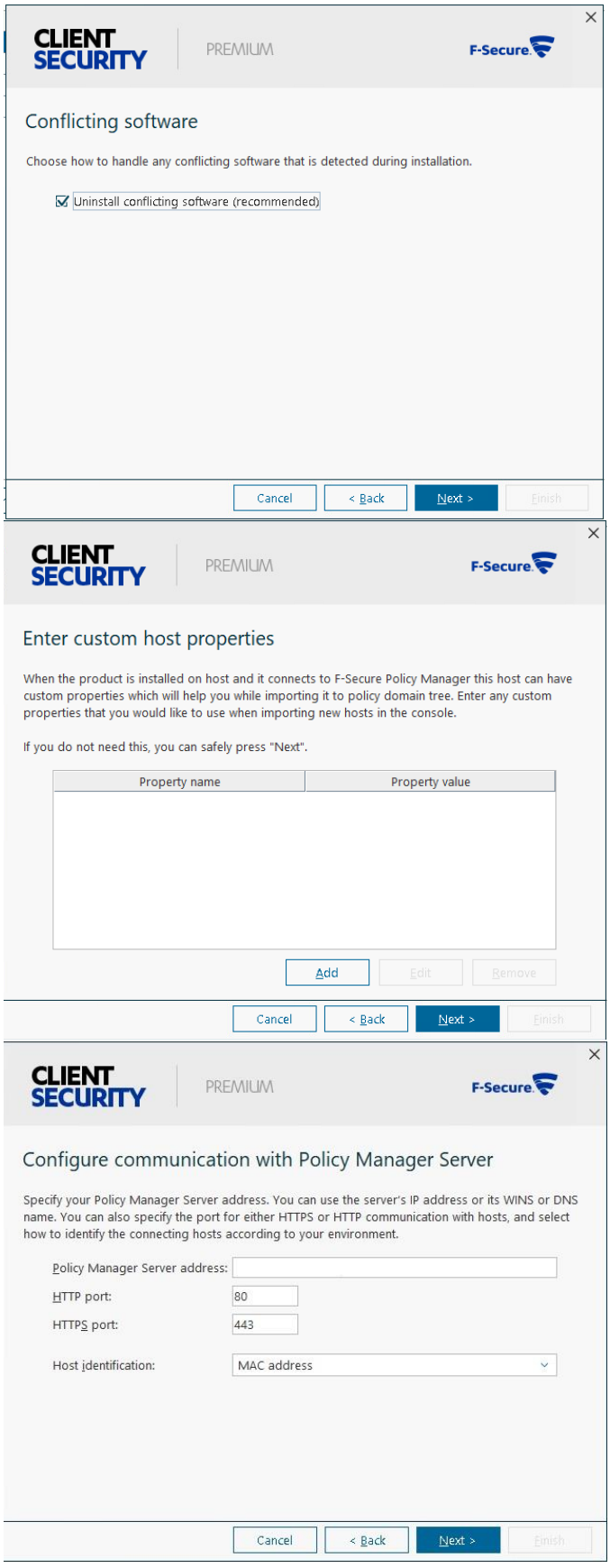
What is Cyber Security? N.d. Verkkosivu. Viitattu 4.5.2023. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

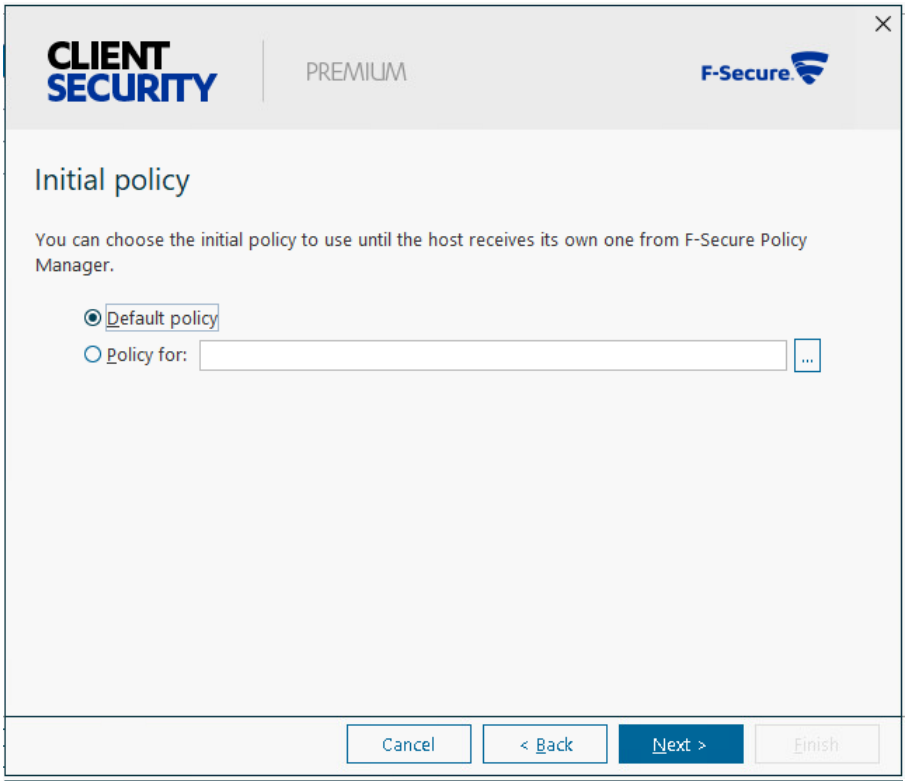
WithSecure Client Security for Windows. N.d. Käyttöohje. Viitattu 28.4.2023. https://help.f-secure.com/data/pdf/wscs_15.30_eng.pdf.

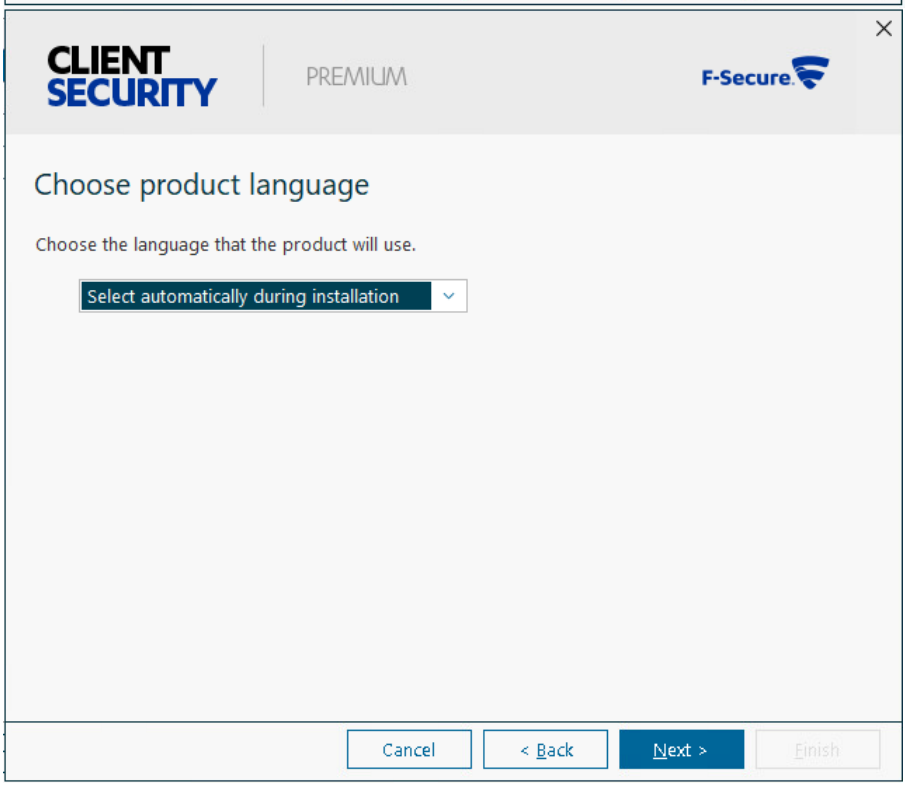
Liitteet

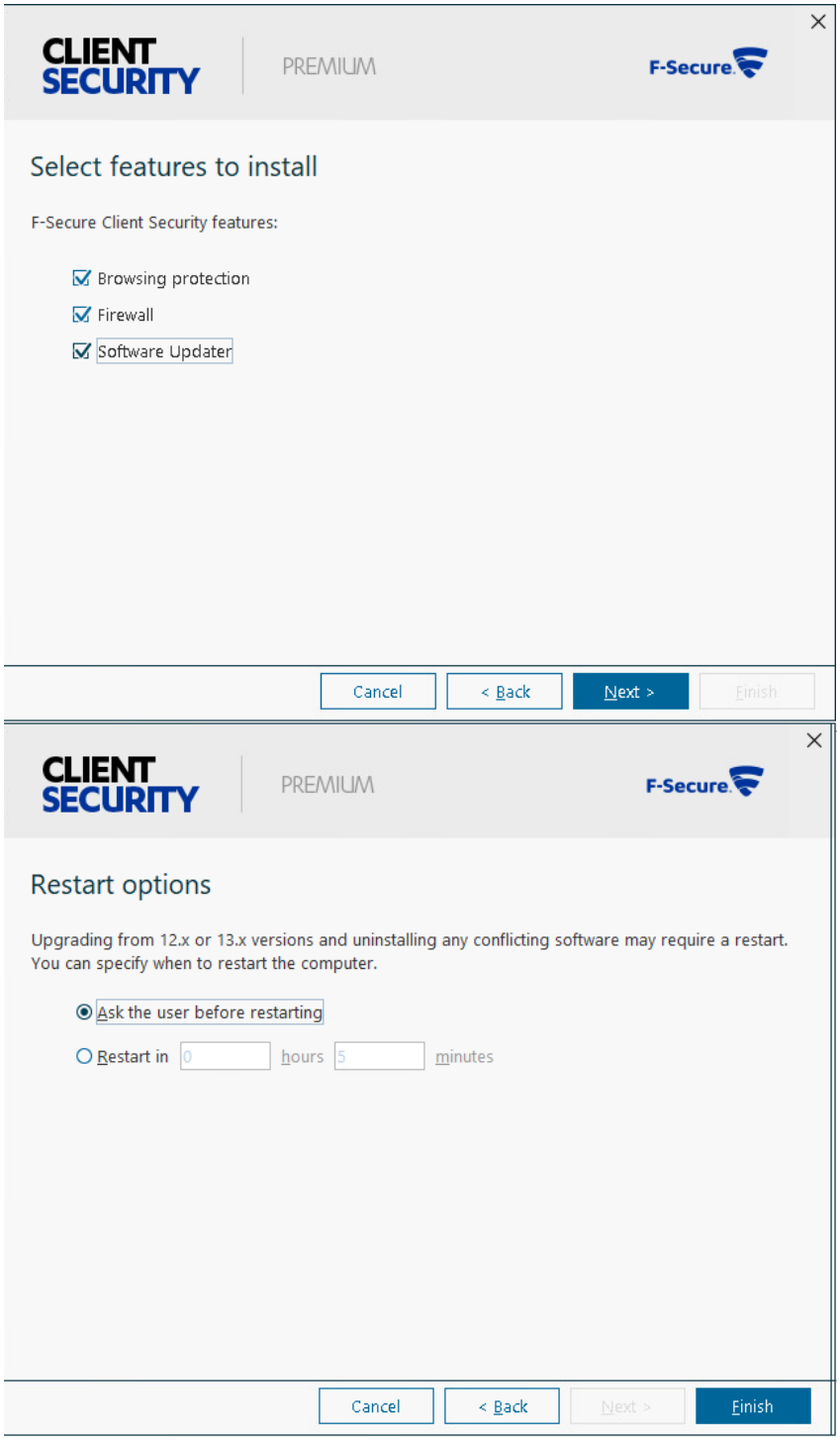
Liite 1. F-Secure Client Securityn ohjattu asennus




CLIENT SECURITY
PREMIUM
F-Secure
Conflicting software
Choose how to handle any conflicting software that is detected during installation.
Uninstall conflicting software (recommended)
Cancel
< Back
Next >
Finish
CLIENT SECURITY
PREMIUM
F-Secure
Enter custom host properties
When the product is installed on host and it connects to F-Secure Policy Manager this host can have custom properties which will help you while importing it to policy domain tree. Enter any custom properties that you would like to use when importing new hosts in the console.
If you do not need this, you can safely press "Next".
Property name
Property value
Add
Edit
Remove
Cancel
< Back
Next >
Finish
CLIENT SECURITY
PREMIUM
F-Secure
Configure communication with Policy Manager Server
Specify your Policy Manager Server address. You can use the server's IP address or its WINS or DNS name. You can also specify the port for either HTTPS or HTTP communication with hosts, and select how to identify the connecting hosts according to your environment.
Policy Manager Server address:
HTTP port:
80
HTTPS port:
443
Host identification:
MAC address
Cancel
< Back
Next >
Finish


CLIENT SECURITY
PREMIUM
F-Secure
Initial policy
You can choose the initial policy to use until the host receives its own one from F-Secure Policy Manager.
Default policy
Policy for:
...
Cancel
< Back
Next >
Finish


CLIENT SECURITY
PREMIUM
F-Secure
Choose product language
Choose the language that the product will use.
Select automatically during installation
Cancel
< Back
Next >
Finish


CLIENT SECURITY
PREMIUM
F-Secure
Select features to install
F-Secure Client Security features:
Browsing protection
Firewall
Software Updater
Cancel
< Back
Next >
Finish
CLIENT SECURITY
PREMIUM
F-Secure
Restart options
Upgrading from 12.x or 13.x versions and uninstalling any conflicting software may require a restart.
You can specify when to restart the computer.
Ask the user before restarting
Restart in 0 hours 5 minutes
Cancel
< Back
Next >
Finish