Janne Enberg

Microsoft System Center 2012 Endpoint Protection

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

11.4.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Janne Enberg Microsoft System Center 2012 Endpoint Protection 37 sivua + 1 liite 11.4.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Kari Järvi Yliopettaja Janne Salonen

Tämä opinnäytetyö käsittelee Microsoft System Center 2012 Endpoint Protection -tietoturvaratkaisun käyttöönottoa testiympäristössä. Opinnäytetyö tehtiin Metropolia Ammattikorkeakoululle. Tavoitteena oli ottaa käyttöön System Center 2012 Endpoint Protection testiympäristössä ja laatia siitä kuvaus. Työ on jaettu kahteen osaan.

Työ on jaettu teoriaosuuteen ja System Center 2012 Endpoint Protectionin käyttöönottoon. Ensimmäisessä osassa käsitellään hieman yleistä teoriaa tietoturvasta ja ohjelmistoista, joita tässä opinnäytetyössä tullaan käyttämään.

Toinen osio opinnäytetyöstä keskittyy System Center 2012 Endpoint Protectionin käyttöönottoon ja sen konfigurointiin. Asennukseen, konfigurointiin ja käyttöönottoon liittyvät osiot käydään läpi kuvien kera, jotta lukijan on helppo seurata työn kulkua. Opinnäytetyössä käydään myös läpi projektissa vaadittava System Center Configuration Manager -ohjelmiston asennus ja konfigurointi. Lopuksi vielä testataan System Center 2012 Endpoint Protectionin toimintaa asiakaskoneessa.

System Center 2012 Endpoint Protection saatiin onnistuneesti otettua käyttöön testijärjestelmässä sekä testattua sen toimintaa käytännössä. Sen käyttöönotosta ja eri toiminnoista saatiin laadittua kattava kuvaus.

Avainsanat	Microsoft, SCEP 2012, Tietoturva, SCCM

Author(s) Title Number of Pages Date	Janne Enberg Microsoft System Center 2012 Endpoint Protection 37 pages + 1 appendix 11 April 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Kari Järvi, Principal Lecturer Janne Salonen, Principal Lecturer

This thesis covers the deployment of Microsoft System Center 2012 Endpoint Protection data security solution. The thesis was made for Metropolia University of Applied Sciences. The aim was to deploy System Center 2012 Endpoint Protection in a test environment and to write a description of it. The thesis has been divided into two parts:

the theoretical part and the deployment of the solution. The theoretical part with general information about information security and the software used in the project.

The second part of this thesis relates to the System Center 2012 Endpoint Protection deployment and configuring the solution. The installation, configuration and deployment sections are introduced with figures in order to better illustrate the processes. The thesis also covers the required System Center Configuration Manager 2012 software installation and configuration. Finally, the testing of the System Center 2012 Endpoint Protection on a client computer is reported.

System Center 2012 Endpoint Protection was successfully installed and thoroughly tested on a test environment. The deployment of the software and its various operations were comprehensively described.

Keywords	Microsoft, SCEP 2012, Tietoturva, SCCM

Sisällys

Lyhenteet

AD	Active Directory on Microsoft Windows -toimialueen käyttäjätietokanta ja hakemistopalvelu.
Client	Asiakasohjelma, jolla otetaan koneelta verkon yli yhteys palvelimeen ja hallinnoidaan palvelimella olevia palveluita.
Domain	Toimialue, jossa toiset käyttäjät ja tietokoneet voivat nähdä toisensa.
Domain Controller	Domain Controller toimii AD-toimialueen ylläpitäjänä. Sen tehtävänä on ylläpitää tietokantaa toimialueen resursseista.
Malware	Haittaohjelma, joka tarkoituksellisesti aiheuttaa haittaa tietokoneessa ja tietojärjestelmässä.
Rootkit	Ohjelmisto, joka tallentuu tietokoneelle, kun hyökkääjä on saanut sen hallintaansa.
Site	Configuration Managerilla hallitava hallinta-alue, joka voi koostua yhdestä tai useammasta IP- tai Active Directory -verkkoalueesta.
SQL	Structured Query Language, relaatiotietokannan kyselykieli.
Virtualisointi	Virtualisointi on tietojenkäsittelyssä tekniikka, joka tarkoittaa fyysisten resurssien muuntamista loogisiksi resursseiksi.
WMI	Windows Management Instrumentation on datan ja operaatioiden hallinta infrastruktuuri Windows-pohjaisissa käyttöjärjestelmissä.

1 Johdanto

Tietoturva on yksi tietotekniikan keskeisimmistä osa-alueista ja se on jatkuvasti vaarassa altistua internetin uhille. Tietoturvaa täytyy jatkuvasti päivittää palomuurien, virustorjuntaohjelmistojen ja eri päivitysten avulla. Ilman tietoturvaa tietoverkot eivät pysyisi kauaa pystyssä. Kun yksityinen käyttäjä voi ehostaa omaa tietoturvaansa esimerkiksi asentamalla virustorjuntaohjelmiston, niin yrityksillä ja isoimmilla tietokoneryhmillä se ei ole niin yksinkertaista. Kyseessä voi olla satoja tietokoneita eri toimipisteissä, joiden tietoturvaa pitäisi jatkuvasti hallita ja päivittää keskitetysti. Muuten tietoturvan ylläpito ja erilaisten ongelmien paikantaminen olisi liian työlästä.

Satojen tietokoneiden tietoturvan hallinta keskitetysti on ainoa järkevä ratkaisu. Microsoft System Center 2012 Endpoint Protection on yksi kehittyneimmistä tietoturvaohjelmistoista, joka tarjoaa tähän ongelmaan ratkaisun. Sen avulla voidaan hallita helposti useita satoja tietokoneita keskitetysti yhdeltä palvelimelta käsin. Endpoint Protection on suoraan integroitu System Center Configuration Manager 2012 kanssa, joten sen asennus ja käyttö on varsin helppoa.

Opinnäytetyö käsittelee yleisesti Microsoftin System Center Configuration Manager 2012:a ja tarkemmin sen alaisuudessa toimivaa System Center 2012 Endpoint Protection -tietoturvaratkaisua. Työssä tutustutaan System Center Configuration Manager 2012 -asennukseen sekä sen konfigurointiin yleisellä tasolla, kun taas Endpoint Protectioniin tutustutaan tarkemmin. Käyttöönotosta, konfiguroinnista ja sovelluksen sisällöstä laaditaan kuvaus. Lopuksi testataan sovelluksen toimivuutta asiakaskoneessa keskitettynä tietoturvana.

Tässä opinnäytetyössä oletetaan, että lukijalla on perustason ymmärrystä palvelimista ja niiden toiminnasta. Työssä ei ole tarkoitus perehtyä SQL-palvelimen toimintaan eikä System Center Configuration Manager 2012:n konfigurointiin kuin niiltä osin, joita vaaditaan Endpoint Protectionin toimivuuden kannalta.

2 Tietoturva

Tämän luvun tarkoituksena on antaa lukijalle hieman perustietoa tietoturvasta ja eri tietoturvariskeistä. Tarkoituksena on myös opastaa lukijaa, kuinka uhkia vastaan tulisi suojautua.

Tietoturvalla tarkoitetaan tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista ulkopuolisilta tahoilta eri ohjelmilla, palomuureilla sekä ohjelma- ja järjestelmiäpäivitysten avulla. Tietoturvallisuuden uhkina pidetään esimerkiksi tietokoneviruksia, huijausyrityksia ja roskapostia. Termillä tarkoitetaan toisen osapuolen luvatonta pääsyä tiedostoihin tai tietoihin.

Kun tietokoneen tai palvelimen kytkee internetiin, se on välittömästi altis internetin uhille. Tämän vuoksi virustentorjuntaohjelmisto ja palomuuri ovat pakollisia laitteille, jotka ovat yhteydessä internetiin tietoturvan takaamiseksi.

Virustorjunnalla tarkoitetaan sellaisia ohjelmia, jotka etsivät ja tuhoavat järjestelmästä haitallisia prosesseja ja niiden tarvitsemia tiedostoja tai ohjelmatiedostoihin tarttunutta haittakoodia. Virustorjunnan tehtävä on työasemien puhdistaminen sekä virustartuntojen leviämisen estäminen toisiin koneisiin tietoverkossa tai massamuistilaitteiden välityksellä.

Palomuuri on tietoverkoissa eristävä järjestelmä, joka suodattaa suojattavan verkon tietoliikennettä haitallisten yhteyksien varalta. Palomuuria käytetään useimmiten suojaamaan käyttäjää avoimesta internetyhteydestä tulevilta hyökkäyksiltä. Palomuureilla on sääntöjä, joiden avulla sisään tai ulos tulevat yhteydet voidaan suodattaa niin, että kaikki muut yhteydet estetään paitsi erikseen määritelty liikenne.

Päivitykset ovat myös yksi turvallisuusriski. Niistä on syytä huolehtia. Monet virukset ja hakkerit hyödyntävät esimerkiksi vanhentuneita ohjelmia tai päivityksiä, joiden avulla he löytävät ohjelmista tai käyttöjärjestelmistä haavoittuvuuksia.

3 Ohjelmisto

Tässä luvussa käydään läpi yleistä teoriaa järjestelmistä ja ohjelmistoista, joita tässä opinnäytetyössä tullaan asentamaan, konfiguroimaan ja käyttämään. Tarkoituksena on antaa lukijalle selkeämpi käsitys käytetystä ohjelmistosta.

3.1 Windows Server 2012

Windows server 2012 on palvelinversio Windows 8 -käyttöjärjestelmästä. Server 2012 on kuudes Windows Server -julkaisu ja se on edistyneempi versio edellisestä Windows Server 2008 R2 -käyttöjärjestelmästä. Windows Server 2012:sta on saatavilla neljä eri versiota: Foundation, Essentials, Standard ja Datacenter. Eri versiot sisältävät rajoitetusti ominaisuuksia. Versioista ja niiden eri ominaisuuksista löytyy kattava taulukko osoitteesta http://www.microsoft.com/en-us/server-cloud/windows-server/buy.aspx. Tässä työssä käytettävä versio on 64-bittinen Windows Server 2012 Datacenter. Metropolia Ammattikorkeakoululta sai ladatuksi kyseisen käyttöjärjestelmän testauskäyttöön ilmaiseksi.

Windows Server 2012 -käyttöjärjestelmään on tullut paljon uudistuksia aiempaan Windows Server 2008 R2 -versioon verrattuna. Käyttöjärjestelmän voi asentaa joko graafisella käyttöliittymällä tai core-asennuksella. Core-asennuksella käyttöjärjestelmä toimii ainoastaan komentorivin avulla. Graafisen käyttöliittymän saa myös pois päältä jälkeenpäin, jos haluaa käyttää komentorivikomentoja. Tässä on esimerkiksi se hyvä puoli, että käyttöjärjestelmästä tulee huomattavasti kevyempi.

Myös Server Manager on täysin uudistettu Windows Server 2012:ssa. Aikaisemmasta Windows Shell -näkymästä on luovuttu ja tilalle on luotu Windows 8 -tyyliin pohjautuva käyttöliittymä. Server Managerilla on helppo hallita ja lisätä uusia rooleja ja ominaisuuksia. Server Managerilla voidaan myös tehdä uusia palvelinryhmiä sekä lisätä muita palvelimia hallittavaksi. [1.]

3.2 System Center Configuration Manager 2012

SCCM eli System Center Configuration Manager 2012 on Microsoftin ohjelmisto, joka on tarkoitettu Windows-pohjaisten työasemien ja laitteiden hallinnointiin. Sen avulla voidaan hallita suuriakin määriä laitteita tietoverkossa. SCCM:llä pystytään esimerkiksi etäasentamaan puuttuvia Microsoft Office -ohjelmia tai ajaa uusimpia Windows-päivityksiä hallinnoitaville tietokoneille. SCCM on myös hyvä ja halpa keskitetty ratkaisu yrityksille, koska sen avulla vikojen etsintä ja ohjelmistojen levitys on vaivatonta. [2.]

Tässä opinnäytetyössä SCCM:n peruskäytön opettelu oli välttämätöntä. System Center 2012 Endpoint Protection hallintapaneelin lisäksi SCCM tuli konfiguroida, ennen kuin pystyttiin siirtymään System Center 2012 Endpoint Protectionin käyttöönottoon.

3.3 System Center 2012 Endpoint Protection

System Center 2012 Endpoint Protection (SCEP 2012) on Microsoftin kehittämä antivirusohjelmisto, joka on aikaisemmin tunnettu nimellä Forefront Endpoint Protection. SCEP 2012 on suunniteltu suojaamaan tietoverkot, palvelimet sekä yksittäiset laitteet keskitetysti viruksia ja verkkohyökkäyksiä vastaan. SCEP 2012 on sovellus, joka on integroitu hallittavaksi SCCM:n kautta.

Muut tietoturvaratkaisut saattavat tarvita oman palvelimen tietoturvan hallinnointia varten. SCEP 2012 -ohjelmistoa taas pystytään hallitsemaan yhdeltä palvelimelta, joten se helpottaa tietoturvan hallinnointia ja samalla vähentää verkonrakenteen monimutkaisuutta. SCEP 2012:n avulla voidaan hallita laajempiakin verkkolaiteryhmiä. Nämä ovat riittäviä syitä, miksi SCEP 2012 voisi olla parempi vaihtoehto kuin monet muut tietoturvaratkaisut. [3.]

SCEP 2012 on nyt täysin integroitu SCCM:n kanssa, joten riittää, että asennetaan vain SCCM -ohjelmisto. SCEP 2012:n clienttien asennus, päivitykset sekä yleisen tietoturvan hallinnointi tapahtuvat siis suoraan SCCM kautta. SCEP 2012 -käyttöliittymä on integroitu myös SCCM-konsoliin, joten erillistä käyttöliittymää ei tarvitse asentaa.

SCEP 2012 tarjoaa mahdollisuuden konfiguroida useita eri hälytyksiä ilmoittamaan kun jossakin laitteessa havaitaan mahdollinen tietoturvauhka. Hälytyksiä voidaan lähettää myös sähköpostitse.

SCEP 2012 on rakennettu käyttämään samaa anti-malware -moottoria kuin Microsoft Security Essentials (MSE). Se tarjoaa reaaliaikaisen suojan, joka monitoroi jatkuvasti tapahtumia tietokoneella ja skannaa uusia ladattuja sekä luotuja tiedostoja. SCEP 2012 client on myös hyvin helppokäyttöinen, ja se on suunniteltu käyttämään mahdollisimman vähän prosessorin tehonkulutusta.

SCEP 2012 clientin asentaminen asiakaskoneelle tarjoaa seuraavat ominaisuudet:

- haittaohjelmien, rootkit -ohjelmien ja vakoiluohjelmien havaitseminen sekä niiden puhdistaminen
- kriittisten haavoittuvuuksien arviointi ja niiden automaattinen määrittely
- integroitu Windowsin palomuurin hallinta
- integroitu Internet Explorer -selaimen tietoturva
- tietoverkon haavoittuvuuksien havaitseminen. [4.]

4 Käyttöönotto

Projekti aloitettiin luomalla testiympäristö, johon kuului palvelin sekä virtuaalikone testausta varten. Testiympäristön luominen aloitettiin pystyttämällä palvelin, joka toimisi myöhemmin SCCM-palvelimena. Ensimmäiseksi asennettiin 64-bittinen Windows Server 2012 -käyttöjärjestelmä sekä Active Directory -ohjauskone (domain controller). Palvelimen nimeksi annettiin ”Server2012DC” ja domainin nimeksi ”Srv2012.local”. Palvelimelta löytyy 8 Gt keskusmuistia, jotta SCCM-palvelin varmasti toimisi sulavasti.

Kun palvelin oli pystytetty, tuli luoda testitietokone, jolle voitaisiin asentaa myöhemmin SCEP 2012 client sekä testata sen toimintaa. Eli testaukseen tarvittiin hallinnoitava asiakaskone, jota hallinnoidaan palvelimelta käsin keskitetysti. Windows Server 2012 mukana tulleen System Managerin avulla asennettiin Hyper-V-virtualisointiohjelma. Hyper-V:llä luotiin virtuaalikone asiakaskoneeksi. Vaikka Hyper-V ei ollut entuudestaan tuttu ohjelma, sen käyttö oli kuitenkin helppoa selkeän graafisen käyttöliittymän

ansiosta. Virtuaalikoneelle asennettiin uusin Windows 8 -käyttöjärjestelmä. Virtuaalikoneelle pystyttiin myös varaamaan haluttu määrä muistia sekä kovalevytilaa.

Koska SCEP 2012 on integroitu SCCM:n kanssa, niin SCCM täytyy asentaa sekä konfiguroida. Seuraavaksi siirrytään aloitustoimenpiteisiin. Ensimmäiseksi tarkastettiin Microsoftin sivuilta tarvittavat komponentit asennusta varten. Jos joitakin komponentteja puuttuu, ne voidaan kätevästi asentaa Windows Server 2012:n mukana tulevan System Manager -ohjelmiston kautta. Komponentit voidaan ladata myös Microsoftin sivuilta.

SCCM tarvitsee myös SQL-palvelimen, jotta kaikki toiminnot toimivisivat. SQL Server 2012 asennettiin samalle palvelimelle, johon myös SCCM tullaan asentamaan. SQL-palvelimen asennuksen jokainen vaihe meni oletusasetuksilla, ja asennus oli hyvin suoraviivaista. SQL Server 2012 ladattiin kokeiluversiona Microsoftin sivuilta. Kun tarvittavat komponentit ja ohjelmistot oli asennettu, voitiin aloittaa varsinainen SCCM:n asennus.

SCCM:n asennuksen sekä konfiguroinnin jälkeen siirryttiin itse SCEP 2012:n käyttöönottoon. SCEP 2012:n käyttöönotosta sekä sen hallinnasta laadittiin tarkka kuvaus kuvien kera.

Taulukko 1. Projektissa käytettävän SCCM-palvelimen sekä virtuaalikoneen tiedot.

	SCCM-palvelin	**Virtuaalikone**
Suoritin	Amd Phenom 9750, 2,40 Ghz	Amd Phenom 9750, 2,40 Ghz
Keskusmuisti	8 Gt	2 Gt
Käyttöjärjestelmä	Windows Server 2012 Datacenter 64-bit	Windows 8 Professional 32-bit

4.1 Laitteistovaatimukset

Ensimmäinen toimenpide ohjelmistojen asennuksessa on tarkistaa tarvittavat laitteistovaatimukset. Laitteistolla on oltava vähintään vähimmäisvaatimukset, jotta asennus varmasti onnistuisi. Seuraavassa taulukossa esitellään laitteistovaatimukset System Center Configuration Manager 2012 ”Site” -järjestelmille, joihin luetaan central administration site, primary site sekä secondary site.

Taulukko 2. Laitteistovaatimukset.

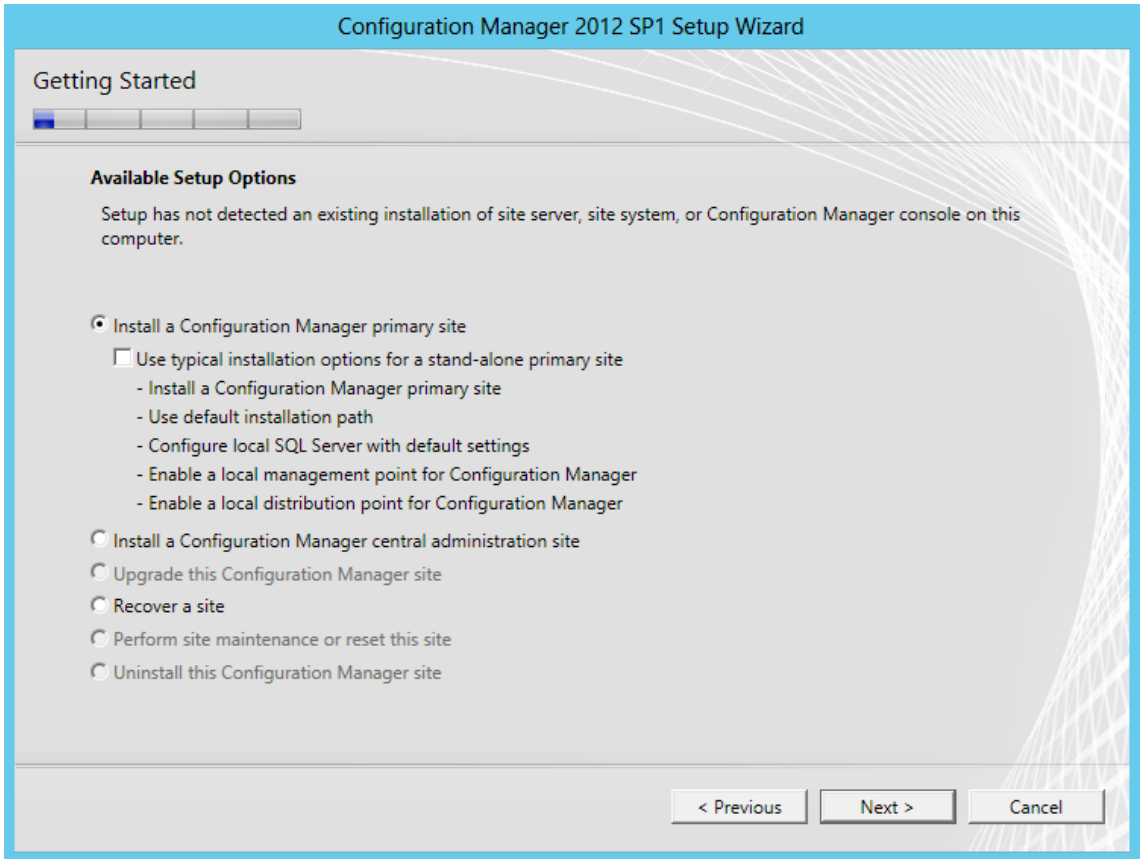
Prosessori	Amd Opteron AMD Athlon 64 Intel Xeon Intel Pentium IV
Prosessorin kellotaajuus	1.4 GHz
Keskusmuisti	2 GB
Vapaa levytila	10 GB

Vähimmäisvaatimukset tukevat kaikkia SCCM:n toiminnallisuuksia yhteensä 100 clientin ympäristössä. Vaatimukset eivät riitä enää, jos asiakaskoneita hallinnoidaan enemmän kuin 100. [5.]

4.2 System Center Configuration Manager 2012:n asennus

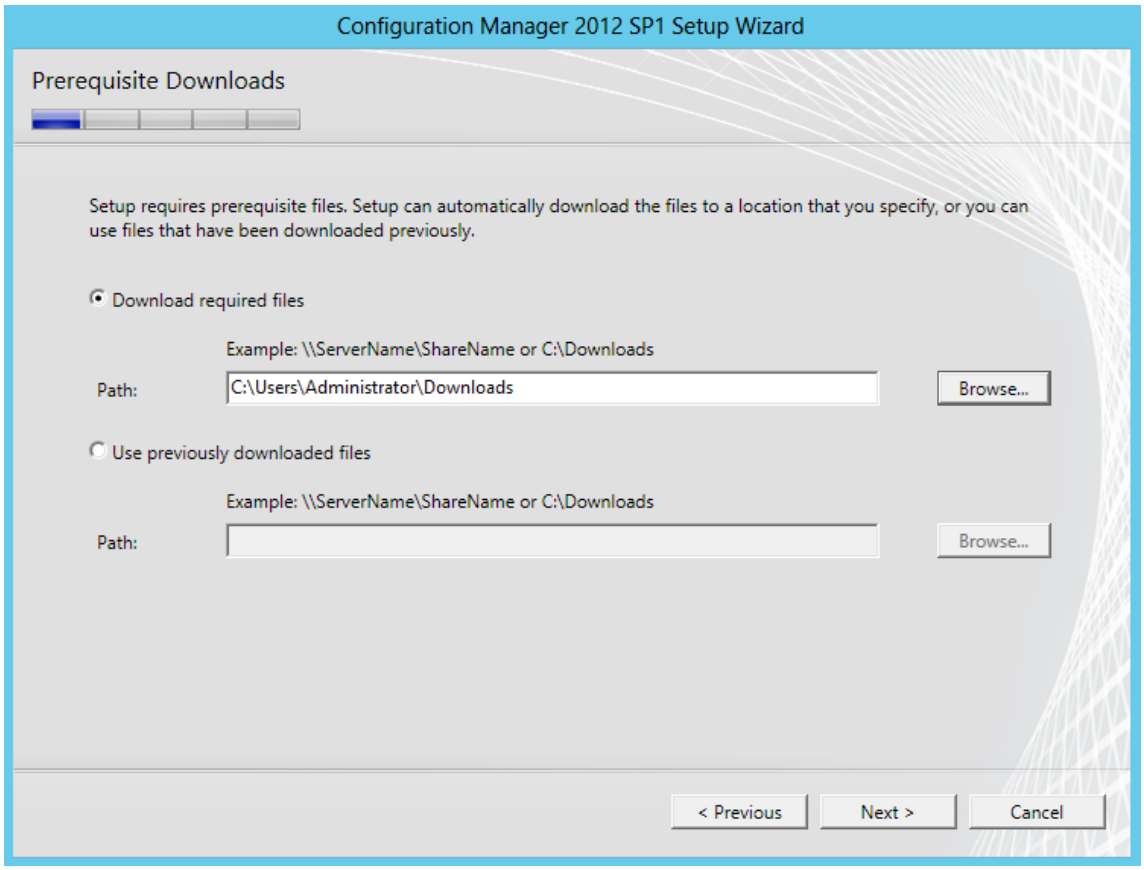
SCCM ladattiin myös Microsoftin sivuilta kokeiluversiona. Kun tiedosto on ladattu ja purettu, asennusvelho voidaan käynnistää ”splash” -asennustiedostosta.

Ensimmäisessä asennusvaiheessa valitaan SCCM-asennuksen tyyppi. Voidaan valita asennetaanko ”primary site” vai ”central administration site”. Central administration site asennetaan yleensä silloin, kun hierarkiassa tulee olemaan myös muita hallittavia ”Site”:jä central administration siten avulla. Tässä työssä valittiin kuitenkin ”Install a Configuration Manager primary site”, koska testiympäristössä tulee olemaan vain yksi hallittava SCCM-palvelin. Use typical installation options for a stand-alone primary site -alavalinta asentaa SCCM:n oletusasetuksilla (kuva 1).



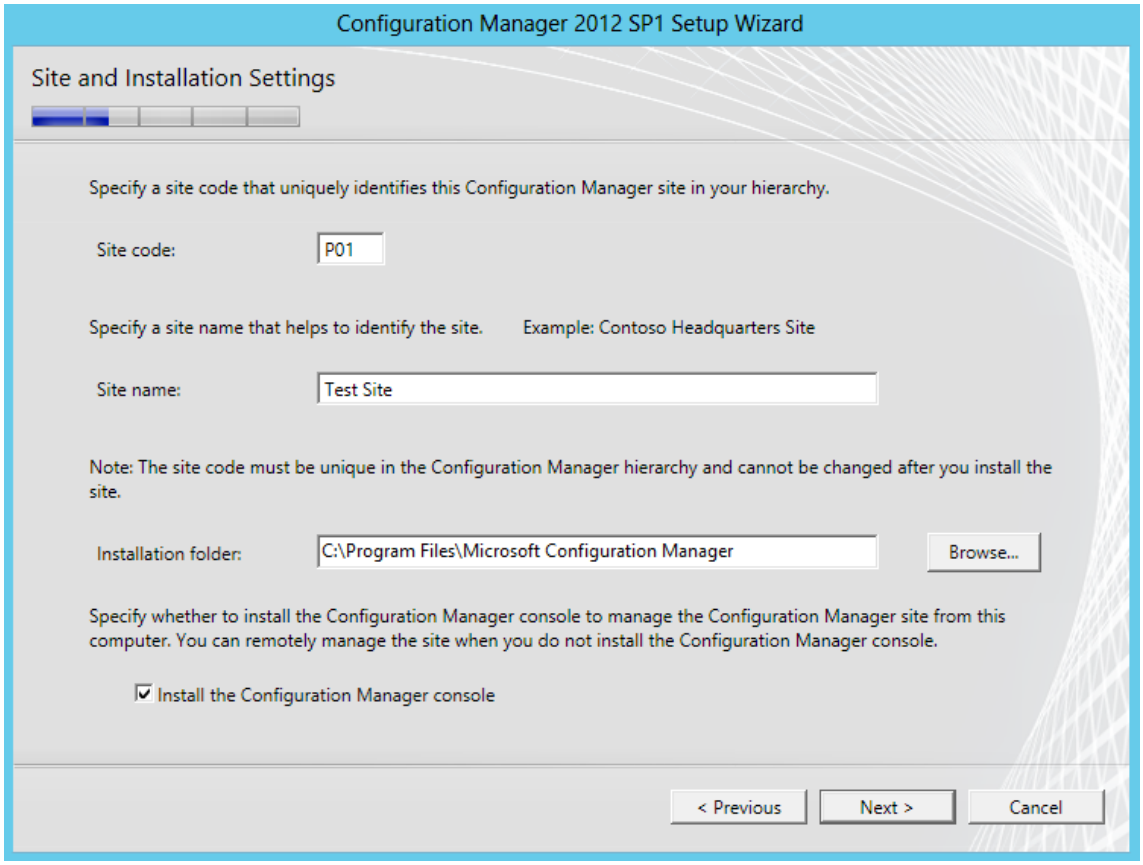
Kuva 1. Valitaan SCCM-asennuksen tyyppi.

Seuraavaksi valitaan hakemisto, johon SCCM lataa tarvittavat tiedostot asennusta varten (kuva 2). Asennustiedostot voidaan ladata joko verkkolevylle tai tietokoneen kovalevylle.



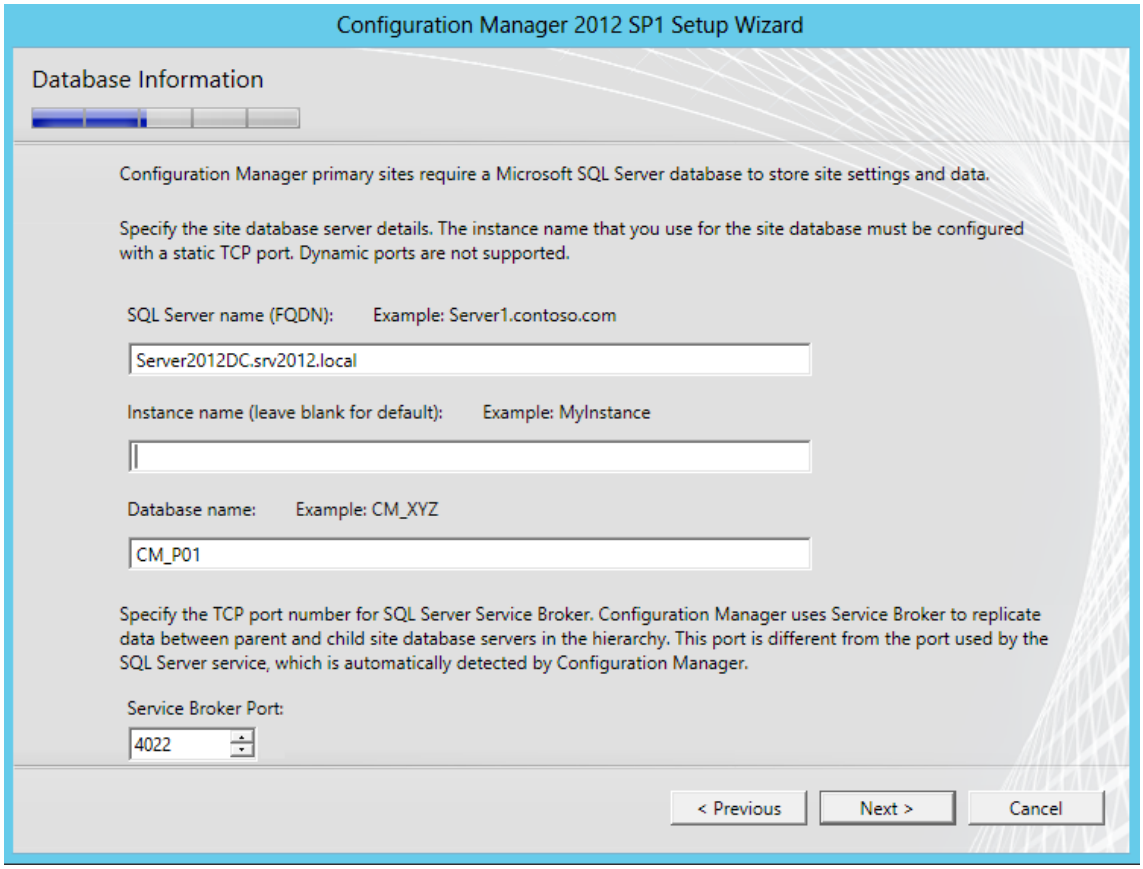
Kuva 2. Määritellään polku, minne SCCM voi ladata tarvittavat asennustiedostot.

Seuraavassa vaiheessa valitaan ”Site”:n koodi, nimi sekä kansio, johon SCCM tullaan asentamaan (kuva 3). ”Site”:lle annettiin koodi ”P01”, nimeksi ”Test site” ja asennuskansio jätettiin oletukseksi. Install the Configuration Manager console -valinnalla asennetaan Configuration Manager -konsoli. Jos ”Site”:ä halutaan hallita etänä, voidaan Configuration Manager -konsoli jättää asentamatta.



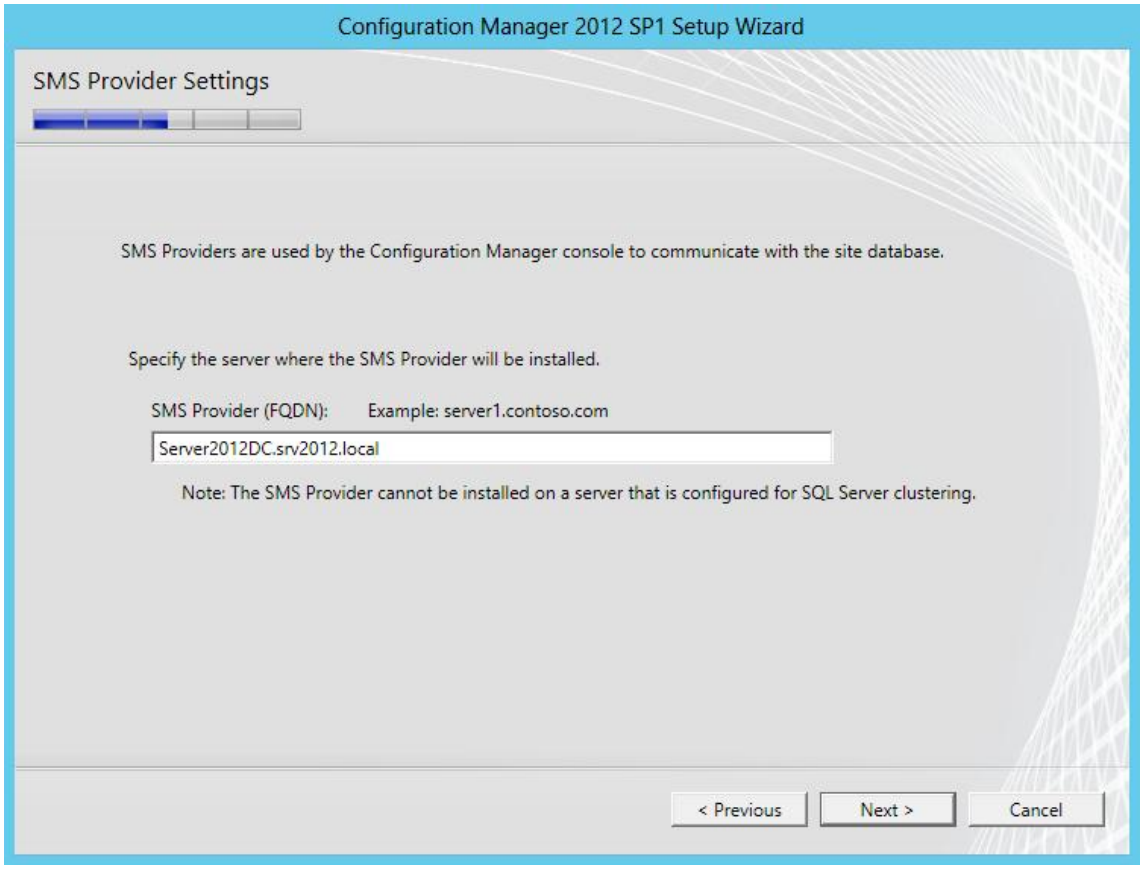
Kuva 3. Valitaan ”Site”:lle tunnus ja nimi sekä SCCM:lle asennuskansio.

Seuraavaksi syötetään SQL-palvelimen nimi sekä annetaan tietokannalle nimi (kuva 4). SQL-palvelimen nimeksi syötettiin ”Server2012DC.srv2012.local”, koska se tulee sijaitsemaan samalla palvelimella kuin domain controller. Tietokannan nimeksi määritettiin ”CM_P01”, Service Broker Port jätettiin oletusarvoksi, eli 4022.



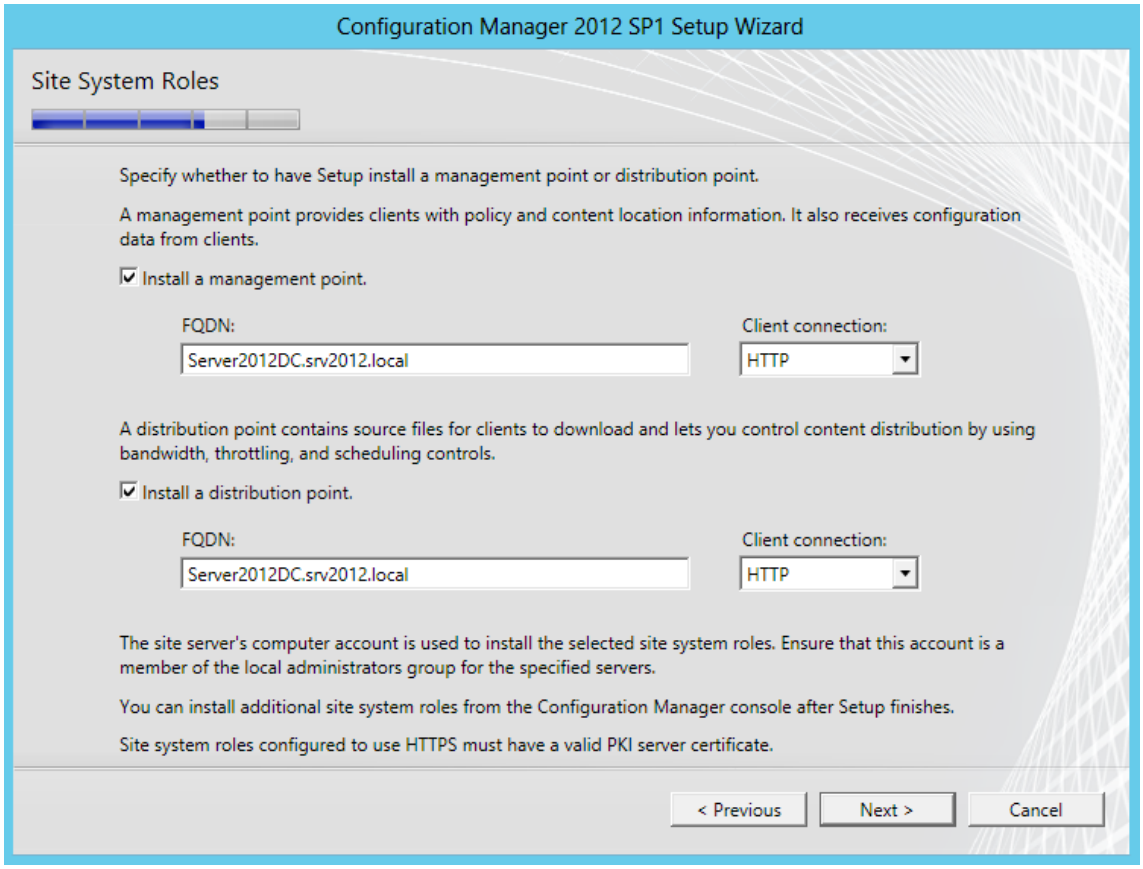
Kuva 4. Määritellään SQL-tietokannan tiedot.

Asennusvelho kysyy seuraavaksi palvelimen nimeä, minne SMS-tarjoaja asennetaan. SMS-tarjoaja on WMI-tarjoaja, joka sallii luku- ja kirjoitusoikeudet SCCM ”Site”:n tietokantaan. Tähän kohtaan annettiin taas palvelimen nimi ”Server2012DC.srv2012.local” (kuva 5).



Kuva 5. SMS-tarjoajan määrittely.

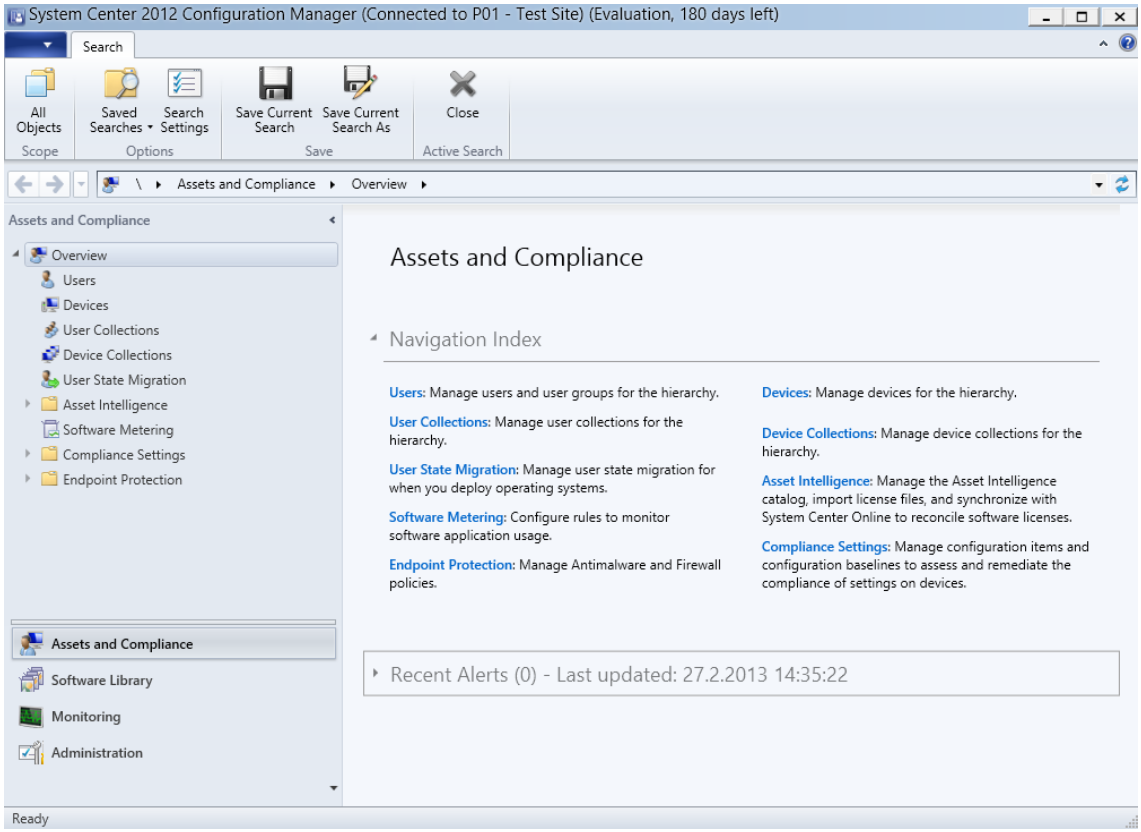
Seuraavassa ikkunassa valitaan asiakaskoneiden yhteydenpitoasetukset. Valitaan Configure the communication method on each site system role, jonka jälkeen päästään muokkaamaan yhteydenpitoasetuksia. Asennetaan hallinta- sekä jakelupisteet palvelimelle, joihin molempiin kohtiin syötettiin jälleen ”Server2012DC.srv2012.local”. Client-yhteydeksi täytyy myös valita joko HTTP tai HTTPS (kuva 6). Tässä työssä valittiin HTTP-yhteys. HTTP on internet-protokolla, jota käytetään tiedonsiirtoon selaimilla sekä WWW-palvelimilla. HTTPS sisältää SSL-salausprotokollan, mutta muuten se on melkein identtinen HTTP-protokollan kanssa. [6.]



Kuva 6. Hallinta- ja jakelupisteiden sekä client-yhteyden määrittelyt.

Lopuksi asennusvelho näyttää yhteenvedon asetuksista sekä käy vielä läpi, puuttuuko joitakin tarvittavia asennuskomponentteja. Kun ollaan tyytyväisiä yhteenvetoon eikä puuttuvia komponentteja löytynyt, suoritetaan asennus loppuun valitsemalla ”Begin Install”.

SCCM on nyt asennettu, ja se on käyttövalmis. Etusivu on suunniteltu mahdollisimman selkeäksi ja helppokäyttöiseksi (kuva 7). Vaikka sovellus näyttää yksinkertaiselta, niin valikoita ja alavalikoita löytyy yllättävän paljon. Vasemmalta alhaalta löytyvät ohjelman keskeisimmät painikkeet, joiden sisältöä käydään seuraavaksi läpi.



Kuva 7. SCCM:n etusivu.

Assets and Compliance -valikko sisältää SCCM:ään liitetyt käyttäjät, laitteet sekä niiden ryhmät. Näiden ryhmittely on tärkeää, jos hallitaan laajempaa tietoverkkoa, joka sisältää satoja laitteita. Ryhmittelyllä selkeytetään hallinnointia. Ohjelmia voidaan asentaa vaikka vain tietylle koneryhmälle tai tietylle käyttäjäryhmälle. Ohjelma huomaa, kun käyttäjä kirjautuu sisään toiselle tietokoneelle, jolloin voidaan asentaa ohjelma myös siihen tietokoneeseen.

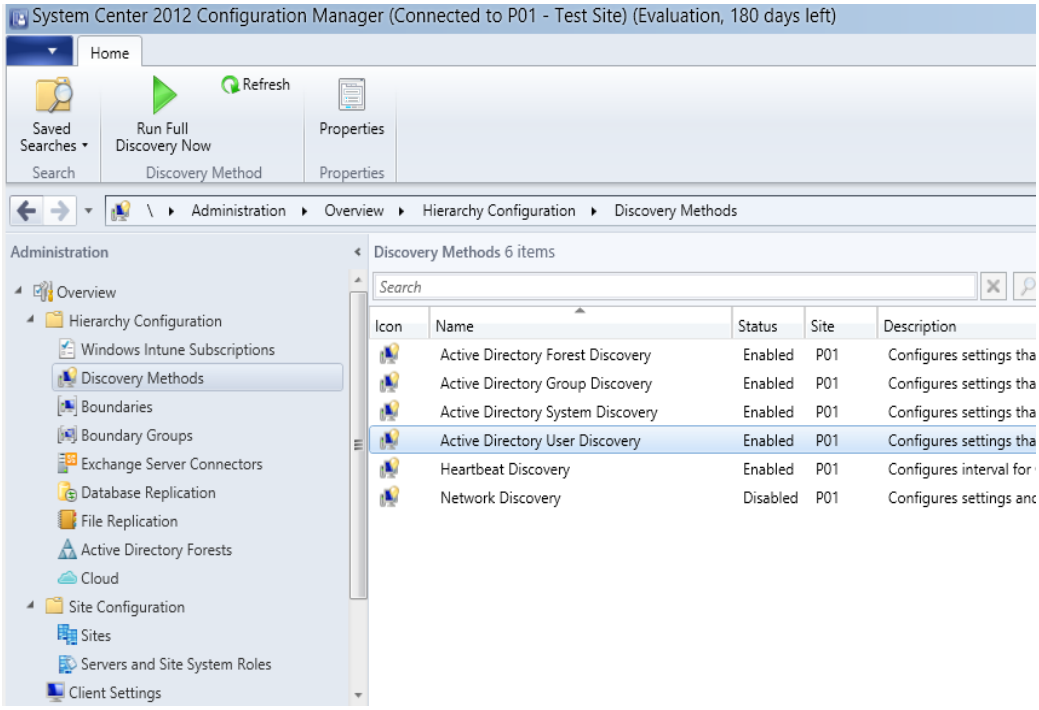
Software Library -valikon avulla voidaan luoda haluttuja ohjelmistopaketteja, ohjelmistopäivityksiä, ajureita sekä käyttöjärjestelmiä. Täällä voidaan luoda esimerkiksi paketti, joka sisältää Microsoft Office 2007 -ohjelmiston tai vaikka ajurit tiettyyn näytönohjaimeen, jotka voidaan sen jälkeen ajaa käyttäjän tietokoneeseen.

Monitoring-valikko sisältää kaikenlaiset hälytykset, tietokannan raportoinnin sekä tämänhetkiset tilat. Valikon alta löytyy myös Endpoint Protection Status, josta voidaan seurata laitteiden tietoturvatilannetta. Endpoint Protection Status -kohtaa esitellään tarkemmin luvussa 5.5.

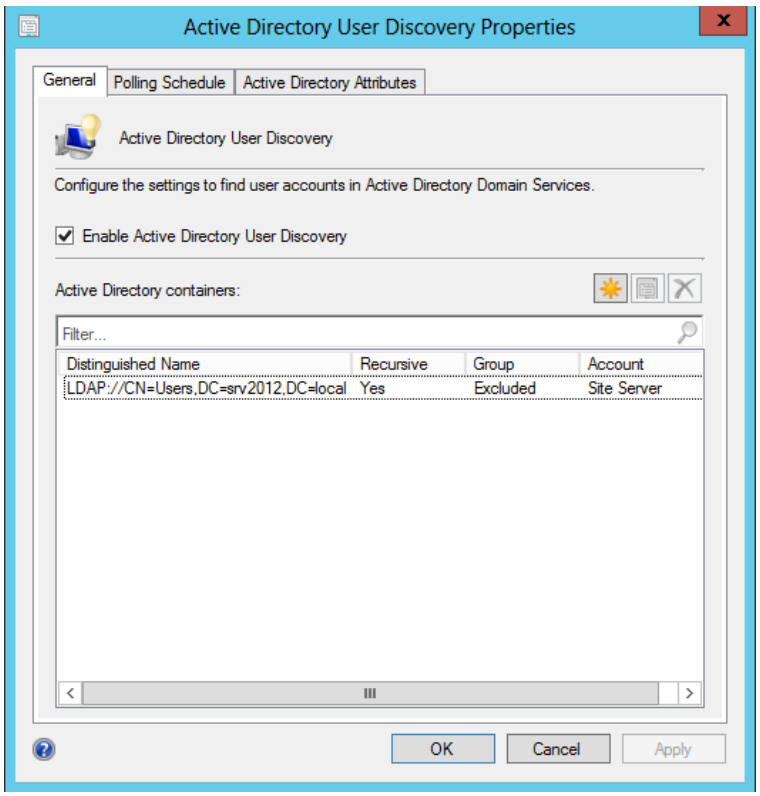
Administrator eli ylläpito pitää sisällään koko järjestelmän hallinnan. Täällä hallitaan rajoja, käyttäjä- ja laitetunnistusmetodeja, palvelimen konfigurointia, jakelupisteitä sekä muita SCCM-palvelimen hallinnan tominnallisuuksia. Seuraavassa luvussa tullaan tutustumaan näihin ominaisuuksiin tarkemmin sekä myös niiden konfigurointiin SCEP 2012 -käyttöönottoa varten. Vaikka SCCM on asennettu, se ei ole vielä täysin käyttövalmis.

4.3 System Center Configuration Manager 2012:n konfigurointi

Peruskonfiguroinnissa lähdetään liikkeelle siitä, että ohjelmiston täytyy löytää Active Directoryn käyttäjät ja laitteet. Tämä asetus löytyy Administration-välilehdeltä, Hierarchy Configuration, Discovery Methods -kohdasta (kuva 8). Täältä voidaan valita eri metodeja, joilla ohjelmisto hakee tarvittavat tiedot Active Directorystä. Ensimmäiseksi valitaan Active Directory User Discovery ja valitaan Properties. Tämän jälkeen sallitaan Active Directory -käyttäjien etsintä valitsemalla Enable Active Directory User Discovery -kohta. Active Directory Containers -kohdasta valitaan polku, josta käyttäjät löytyvät (kuva 9). Sama toiminto suoritetaan myös Forest Discovery, Group Discovery, System Discovery ja Heartbeat Discovery -kohdille. [7.]



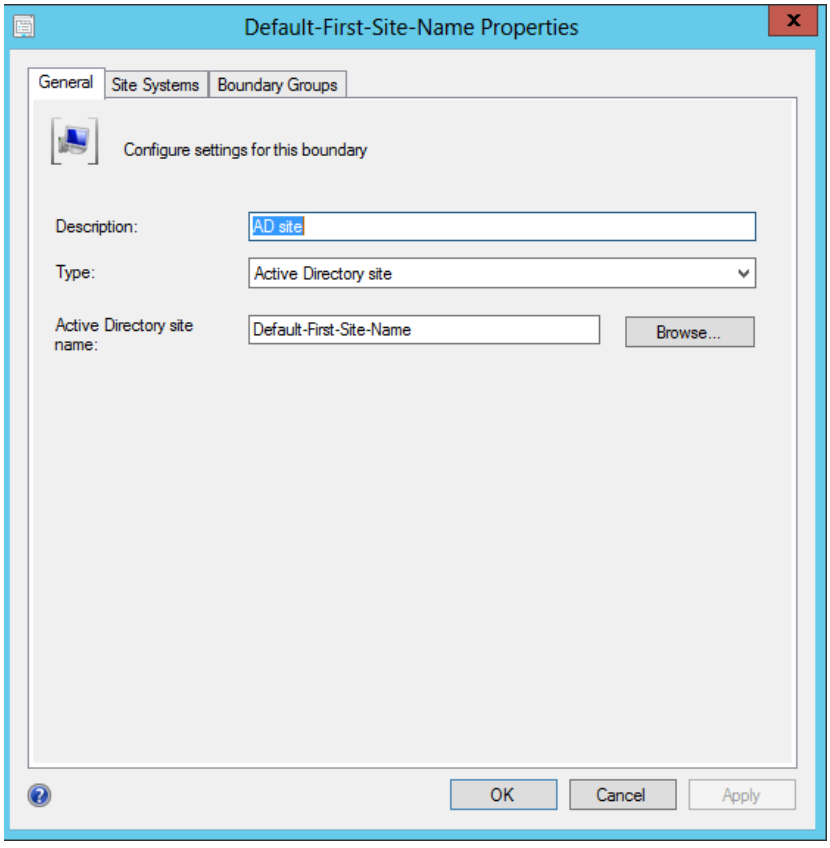
Kuva 8. Discovery Methods -näkymä.



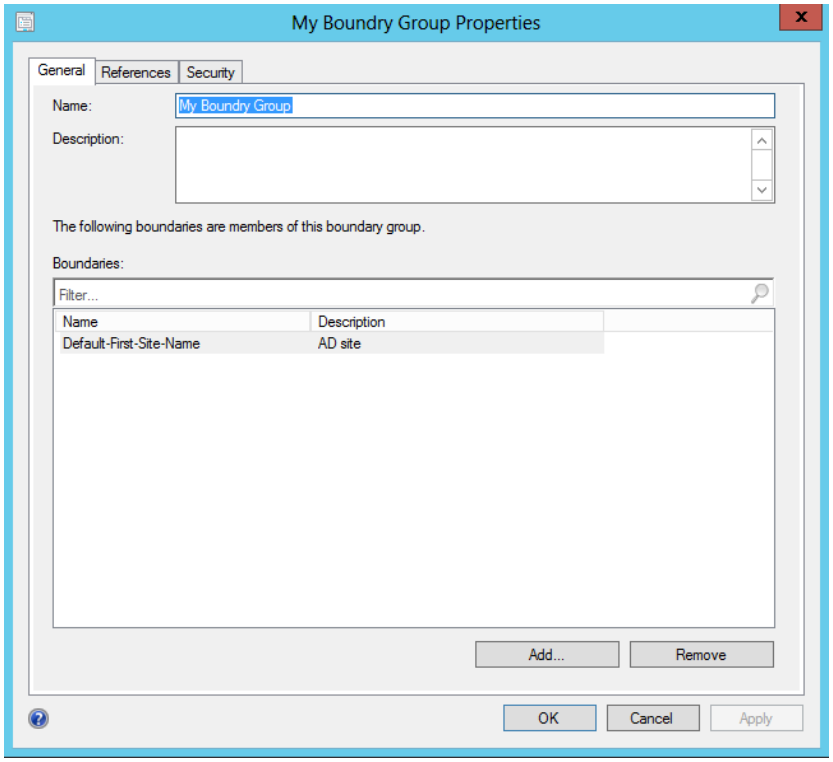
Kuva 9. Active Directory User Discovery -asetukset.

Administrator-välilehdeltä löytyvät myös Boundaries ja Boundary Groups, eli rajat ja rajaryhmät. SCCM:ssä raja on tietoverkkosijainti, joka sisältää yhden tai useamman hallittavan laitteen. Rajat pitää itse käydä asettamassa, jotta ohjelmistojen asennus asiakaskoneisiin toimisi. Boundary voidaan määritellä joko halutulle aliverkon peitteelle, IP-osoitealueelle, Active Directory -alueelle tai IPv6-etuliitteelle. Oletuksena määritellään Boundary, Create boundary -kohdasta Default-First-Site-Name, joka rajataan koko Active Directory alueelle (kuva 10). [8.]

Boundaryn käyttö vaatii ainakin yhden Boundary Groupin. Boundary Group on kokoelma Boundaryitä, jotka sallivat clienttien liittyä ”Site”:lle. Boundary Groupien tehtävä on myös löytää tarvittavat asennettavat ohjelmistot, päivitykset sekä käyttöjärjestelmät. Boundary Groupin luominen tapahtuu Create Boundary Group -kohdasta. Ryhmälle valitaan nimi ja vähintään yksi Boundary (kuva 11). [8.]

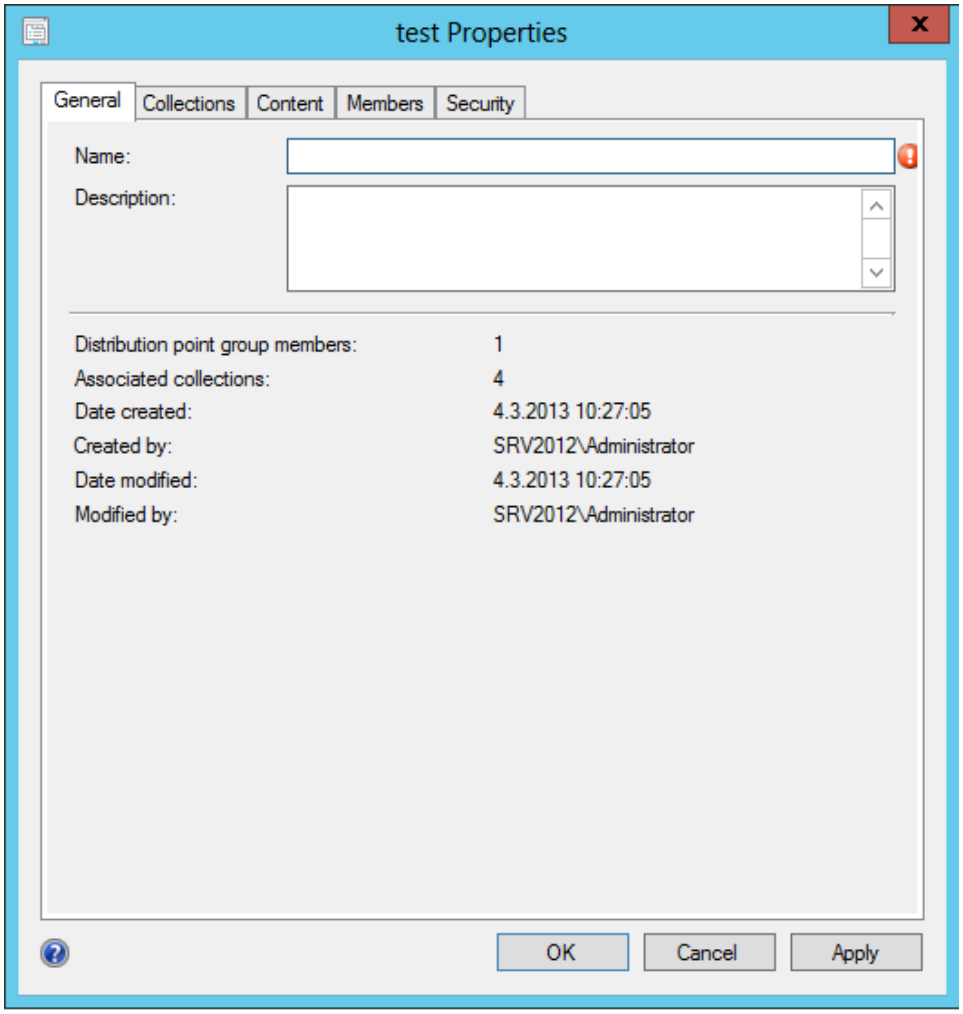


Kuva 10. Default-First-Site-Name -asetukset.



Kuva 11. Boundary Group -asetukset.

Distribution Point sekä Distribution Point Group on myös tärkeä konfiguroida, jotta SCEP 2012 -clientin ja muiden ohjelmistojen jakelu asiakaskoneille on mahdollista. Pääpalvelimelta löytyy oletuksena jo yksi Distribution Point, mutta se ei kuulu mihinkään Distribution Point Groupiin. Distribution Point Group lisätään Administrator-välilehdeltä, Distribution Point Group, Create Distribution Point Group -kohdasta. Members-välilehdeltä valitaan Distribution Point, joka hoitaa jakelun käyttäjille ja laitteille. Collections-välilehdeltä valitaan käyttäjät ja laitteet, jotka kuuluvat tähän Distribution Point Grouppiin (kuva 12). [9.]



Kuva 12. Distribution Point Group -asetukset.

Lopuksi asiakaskoneesta täytää käydä sallimassa palomuuriasetuksista WMI- ja File and Printer Sharing domainverkkoon, mikä mahdollistaa SCEP 2012 -clientin asennuksen asiakaskoneeseen.

5 System Center 2012 Endpoint Protection

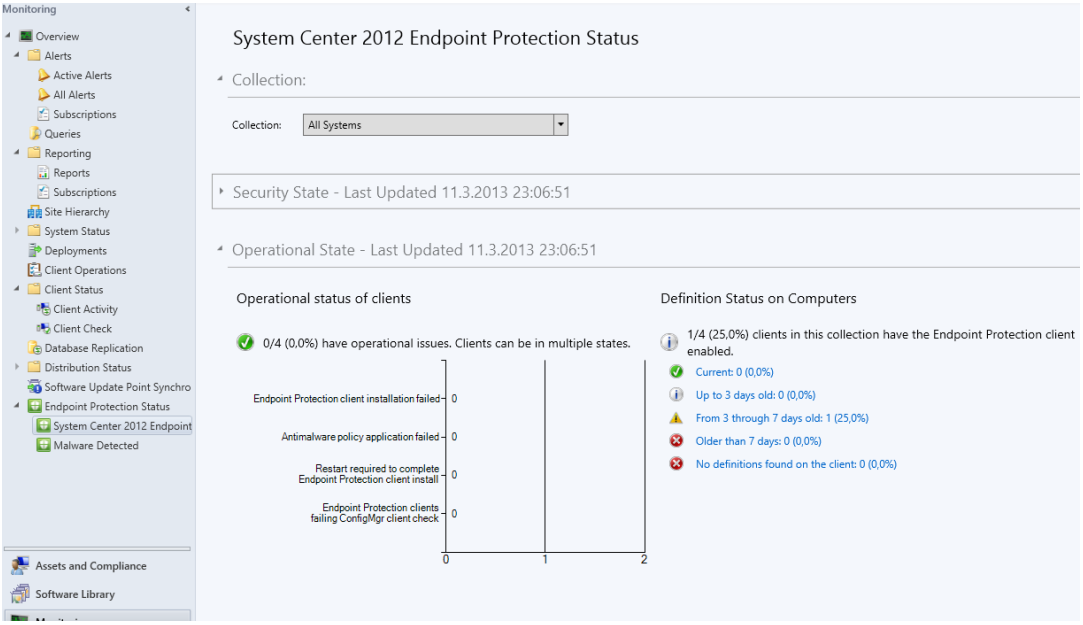
SCCM:n konfiguroinnin jälkeen täytyy käydä asentamassa Endpoint Protection site system -rooli, jonka jälkeen vasta voidaan siirtyä SCEP 2012 -konfigurointiin. SCCM käyttää site system -rooleja tukeakseen sen eri toimintoja ”Site”:llä.

Administrator-kohdasta löytyy Server and Site System Roles, josta voidaan valita Add Site System Roles. Kun asennusikkuna aukeaa, ”Site”:n koodi ja muut tarvittavat

asetukset löytyvät jo oletuksena. Seuraavassa ikkunassa on monia eri rooleja, joita voidaan lisätä, mutta valitaan kuitenkin vain ”Endpoint Protection point”. Loppuasennus on hyvin suoraviivaista, jossa hyväksytään käyttöehdot, jonka jälkeen ohjelma näyttää yhteenvedon asennettavasta Endpoint Protection site system -roolista. SCEP 2012 on nyt asennettu, ja se on käyttövalmis.

5.1 Sovelluksen hallinta

SCEP 2012:n hallinta tapahtuu täysin SCCM:n kautta. Monitoring-välilehdeltä löytyy Endpoint Protection Status eli yleisnäkymä. Täältä voidaan tarkastella suojattujen laitteiden tilat tietoverkossa. Collection-valikosta voidaan valita haluttu kokoelma, jonka eri tiloja halutaan tarkastella. Collectionin alta löytyy myös kaksi valikkoa Security State sekä Operational State (kuva 13).



Kuva 13. SCEP 2012 -client-tilojen etusivu.

Security State sisältää kaiken informaation koskien valitun kokoelman tietoturvasta. Täältä nähdään esimerkiksi, koska tietoturvapäivityksiä on edellisen kerran ladattu SCEP 2012 -koneille, tai jos jokin SCEP 2012 -client on epäonnistunut päivityksessä.

Operational State taas sisältää tiedot clienttien tiloista. Täältä voidaan tarkastella esimerkiksi, jos clientin asennus asiakaskoneeseen on epäonnistunut, antimalware

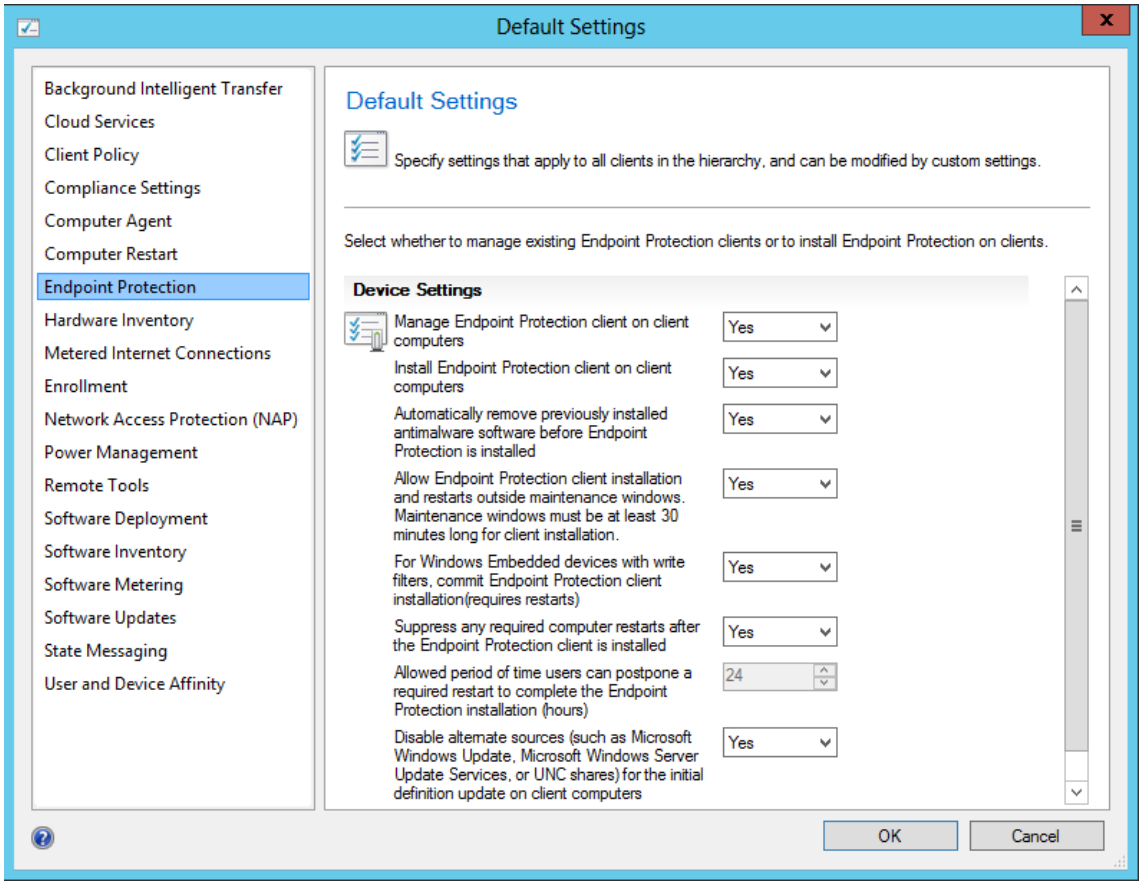
policyn jakaminen clientille on epäonnistunut tai jos tietokoneen uudelleenkäynnistys vaaditaan, jotta SCEP 2012 -client asentuisi. Definition Status on Computers -kohdasta voimme myös nähdä, kuinka moni client on aktiivisena valitussa kokoelmassa.

5.2 Clientin asennus asiakaskoneeseen

SCEP 2012 clientin levitys isoimmillekin ryhmille on hyvin vaivatonta. Tietokoneita voidaan järjestellä eri ryhmiin, esimerkiksi jos joissakin tietokoneissa on jo valmiiksi jokin tietoturvaratkaisu, jota halutaan vielä käyttää. Tässä tapauksessa nämä koneet voidaan siirtää toiseen ryhmään ja jättää SCEP 2012 -client asentamatta niihin. SCEP 2012 -clientin asennuksessa käytetään yleensä SCCM:n omaa client push installation -toimintoa eli puskuasennustoimintaa. Puskuasennus asentaa SCEP 2012 -clientin automaattisesti valitun kokoelman laitteisiin. Jos johonkin kokoelmaan esimerkiksi liittyy uusi tietokone, puskuasennus asentaa SCEP 2012 -clientin siihen. Tässä opinnäytetyössä asennetaan SCEP 2012 -client yhdelle asiakaskoneelle. Seuraavaksi käydään läpi, kuinka SCEP 2012 -clientin puskuasennus tapahtuu.

Ensiksi käydään hieman tarkastelemmassa SCEP 2012 -clientin puskuasennuksen perusasetuksia. Mennään Administrators-, Client Settings-, Default client settings -kohtaan ja valitaan Properties. Tämän jälkeen aukeaa ikkuna, jossa määritellään kaikki Configuration Manager clientin ja Endpoint Protection clientin asetukset, joita tullaan ajamaan asiakaskoneisiin. Configuration Manager client vaaditaan asiakaskoneella, jotta SCEP 2012 clienttiä pystytään hallitsemaan SCCM-palvelimelta käsin.

Tarkistellaan ensiksi hieman Endpoint Protection -välilehden asetuksia (kuva 14). Täältä löydämme kaiken oleellisen liittyen SCEP 2012 -clienttien asennukseen asiakaskoneille. Voidaan valita, sallitaanko SCEP 2012 -clientin asennus ylipäätään asiakaskoneeseen, poistetaanko kaikki aiemmat tietoturvaohjelmistot asiaskoneelta ennen SCEP 2012:n asennusta ja käynnistetäänkö tietokone uudestaan, kun SCEP 2012 client on asentunut.



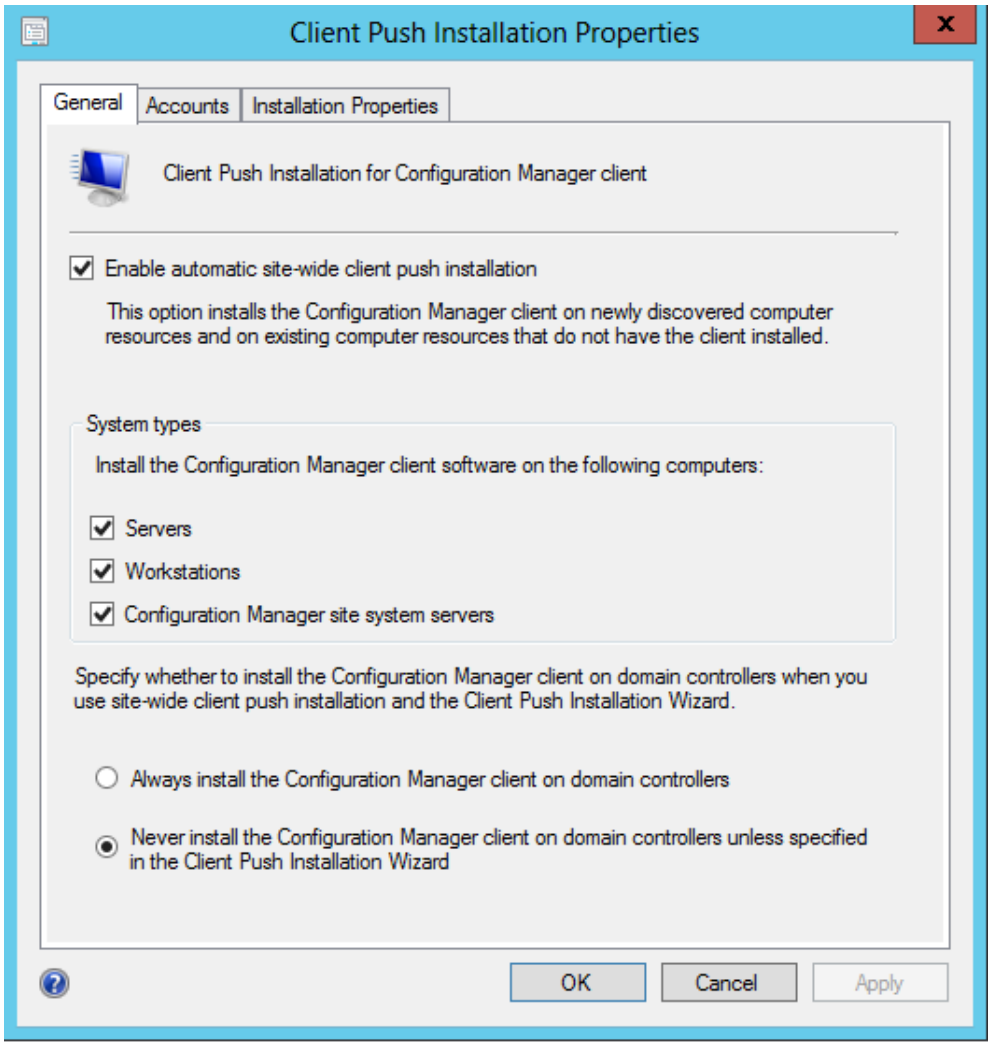
Kuva 14. Client push installation -asetukset.

Client Policy -kohdasta löydämme asetuksen, jolla voidaan automatisoida Configuration Managerin ja SCEP 2012 -clienttien asennukset. Voidaan valita aikaväli, jolloin SCCM tarkastaa kaikki laitteet tietystä määritellystä kokoelmasta läpi, löytyykö niistä Configuration Manager client. Jos Configuration Manager clienttiä ei löydy, niin SCCM asentaa sen automaattisesti. SCCM asentaa myös Configuration Manager -clientin yhteydessä SCEP 2012 -clientin, jos Endpoint Protection -välilehdellä on Install Endpoint Protection client on client computers -kohta valittuna.

Seuraavaksi määritellään Client Push installation -asetuksia. Mennään Sites-välilehdelle, Settings, Client Push Installation. Client Push Installation -asetusikkuna aukeaa, josta löytyy kaksi tärkeää välilehteä, jotka käsittelevät seuraavia asetuksia.

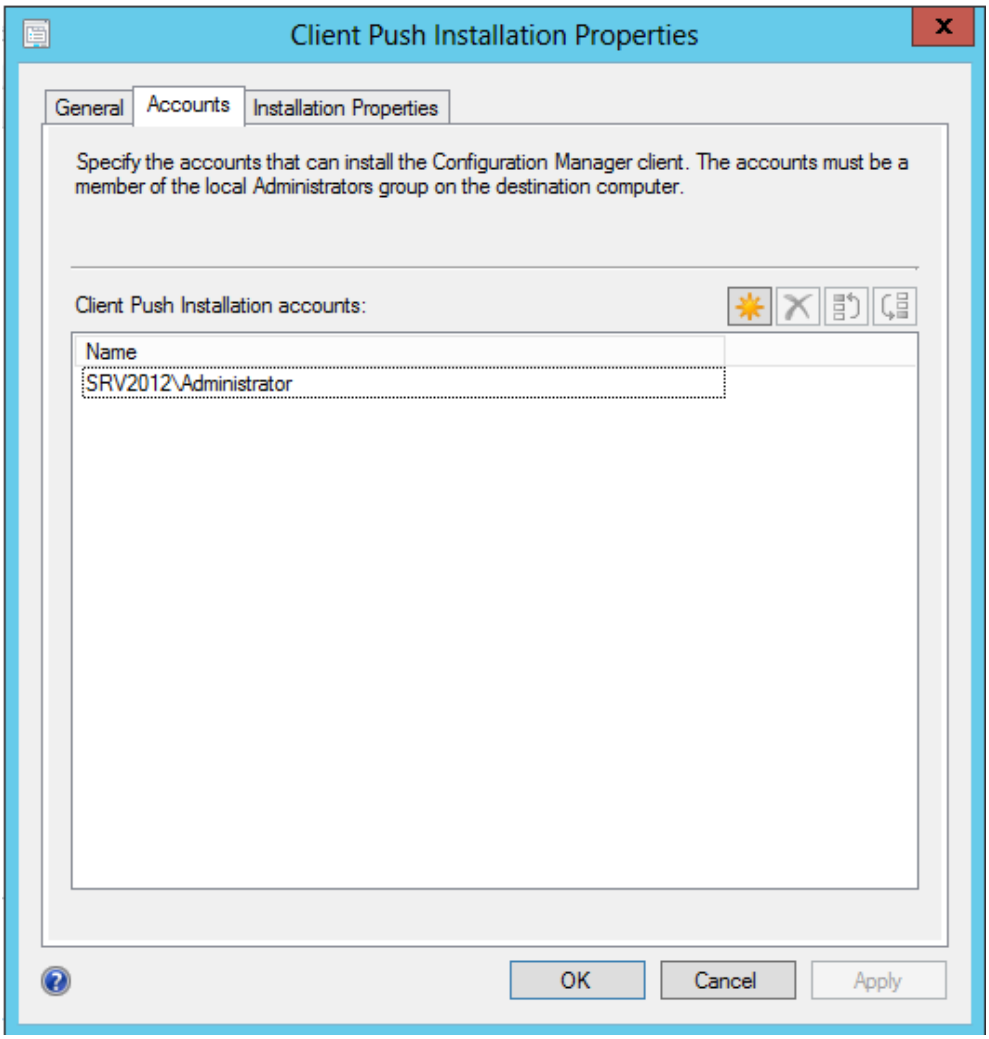
General-välilehdeltä löytyy Enable automatic site-wide client push installation -valinta. Tämä asetus valittuna asennetaan Configuration Manager -client jokaiselle uudelle koneelle, joka havaitaan verkossa. Se asennetaan myös koneelle, jolla ei ole jo ennestään Configuration Manager -clienttiä asennettuna. General-välilehdeltä valitaan

myös asennetaanko Configuration Manager -client palvelimille, tietokoneille vai molemmille. General-välilehdellä voidaan myös määrittää asennetaanko Configuration Manager client domain controllereille (kuva 15).



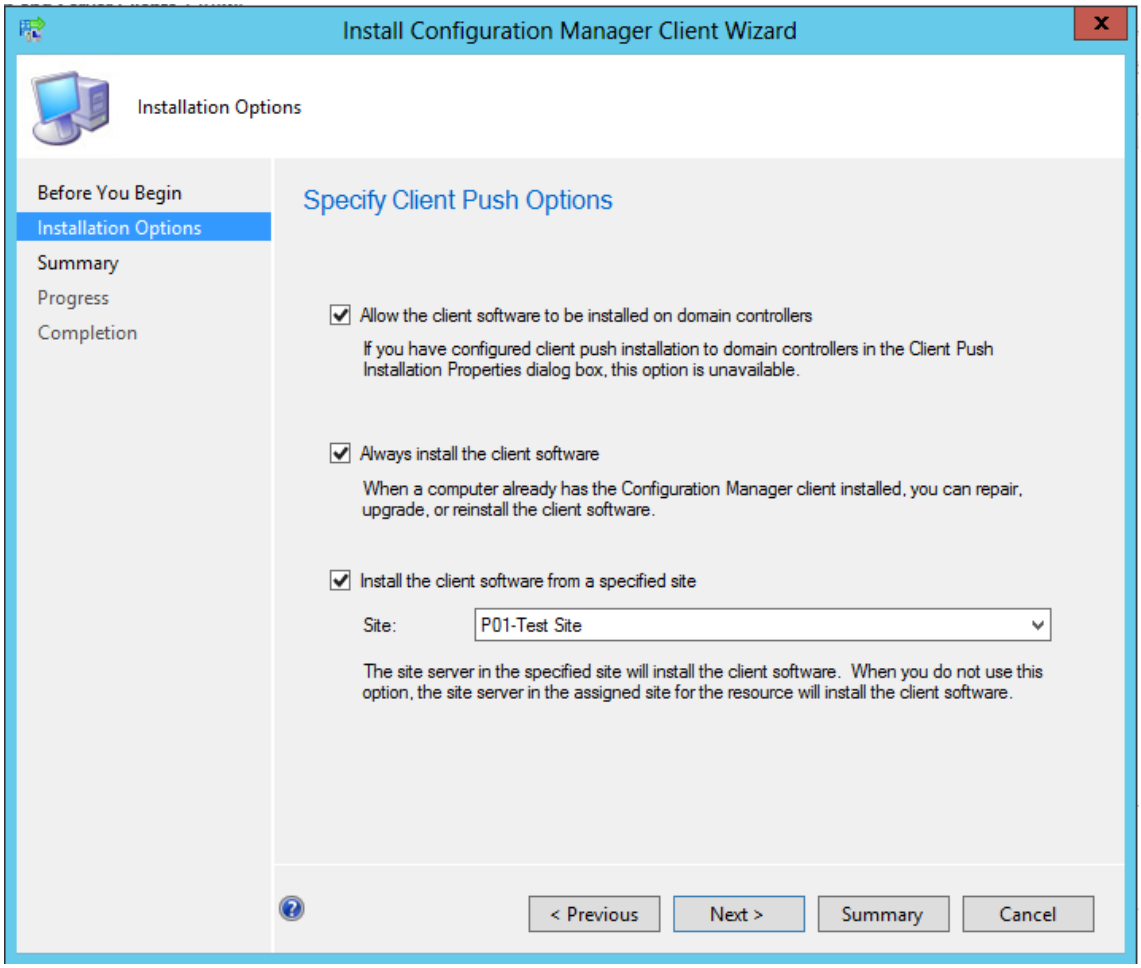
Kuva 15. Puskuasennuksen asetusten General-välilehti.

Accounts-välilehdeltä käydään asettamassa käyttäjätunnus, jolla Configuration Manager clientin asentaminen asiakaskoneille tapahtuu (kuva 16). Tämän tunnuksen täytyy kuulua ylläpitäjien ryhmään, jolla on oikeudet asentaa ohjelmia asiakaskoneisiin.



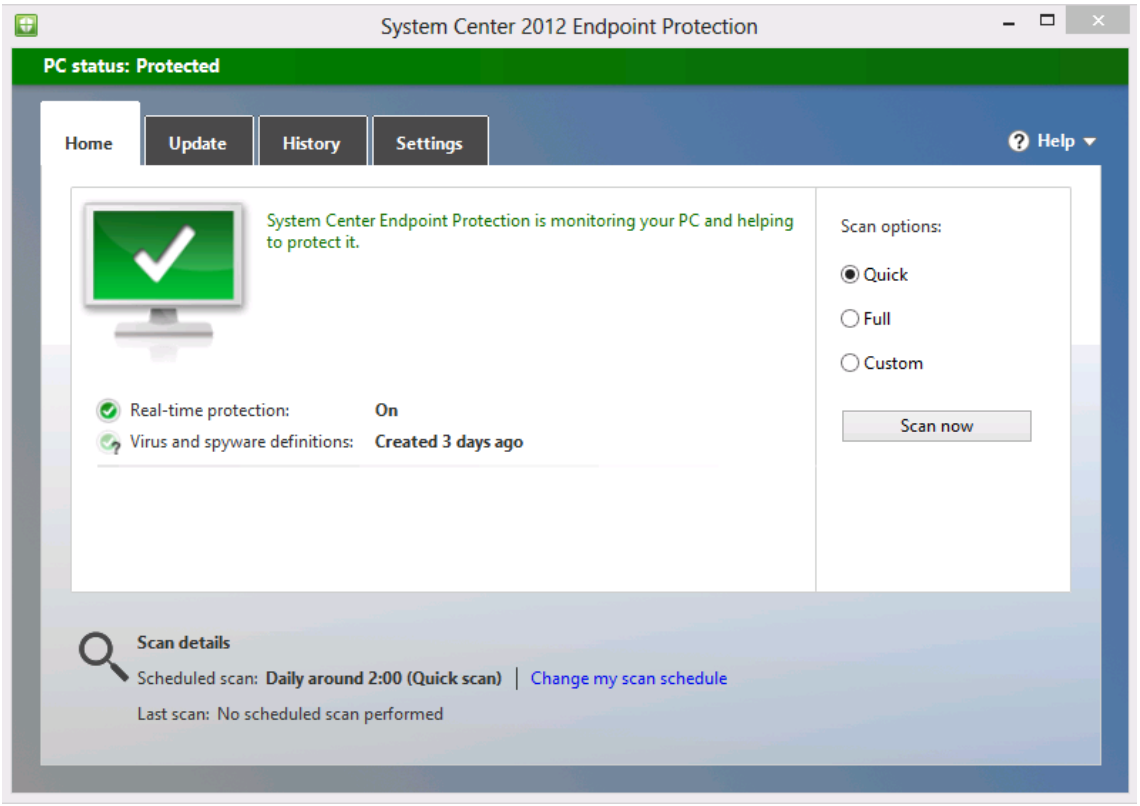
Kuva 16. Puskuasennuksen asetusten Account-välilehti.

Kun puskuasennuksen asetukset ovat valmiit, voidaan Configuration Manager ja SCEP 2012 -clientit asentaa halutulle kokoelmalla. Tämä tapahtuu Assets and Compliance -kohdasta, jossa valitaan haluttu laiteryhmä tai pelkästään yksilöllinen tietokone. Sen jälkeen valitaan Install client. Asennusikkuna aukeaa, jossa valitaan vielä, halutaanko client asentaa domain controllereille, asennataanko client koneelle, jossa on ennestään jo client ja miltä ”Site”:ltä client asennetaan (kuva 17).



Kuva 17. Install Configuration Manager Client -asennusvelho.

Kun halutut asetukset on valittu, voidaan valita Next ja aloittaa asennus asiaskoneeseen. Kun asennus on valmis, asiakaskoneen client pitäisi näkyä SCCM:ssä aktiivi-tilassa. Configuration Manager -client ja SCEP 2012 -client on nyt asennettu asiakaskoneeseen. Kuvassa 18 näkyy yleisnäkymä SCEP 2012 -ohjelmistosta asiakaskoneella.

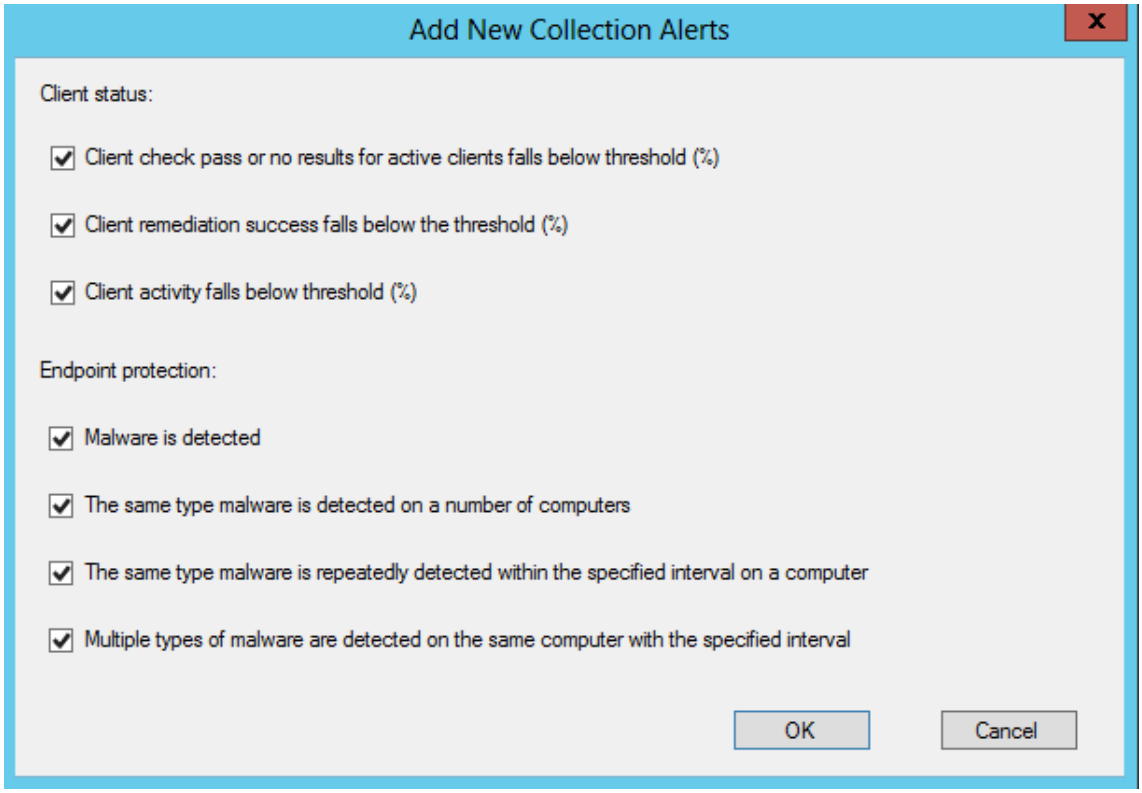


Kuva 18. Yleisnäkymä SCEP 2012 -clientistä asiakaskoneella.

5.3 Hälytykset

Laitekokoelmille voidaan asettaa hälytyksiä, jotka näkyvät Monitoring-välilehdellä Alerts-kohdassa. Kun jossakin tietokoneessa, joka kuuluu tähän kokoelmaan, havaitaan virus, niin hälytys tulee näkyviin Alerts-kohtaan. Hälytykset on tärkeä asettaa esimerkiksi kokoelmille, joille asennetaan SCEP 2012 client. Järjestelmänhallitsijan on hyvä tietää, kun mahdollinen tietoturvauhka tapahtuu.

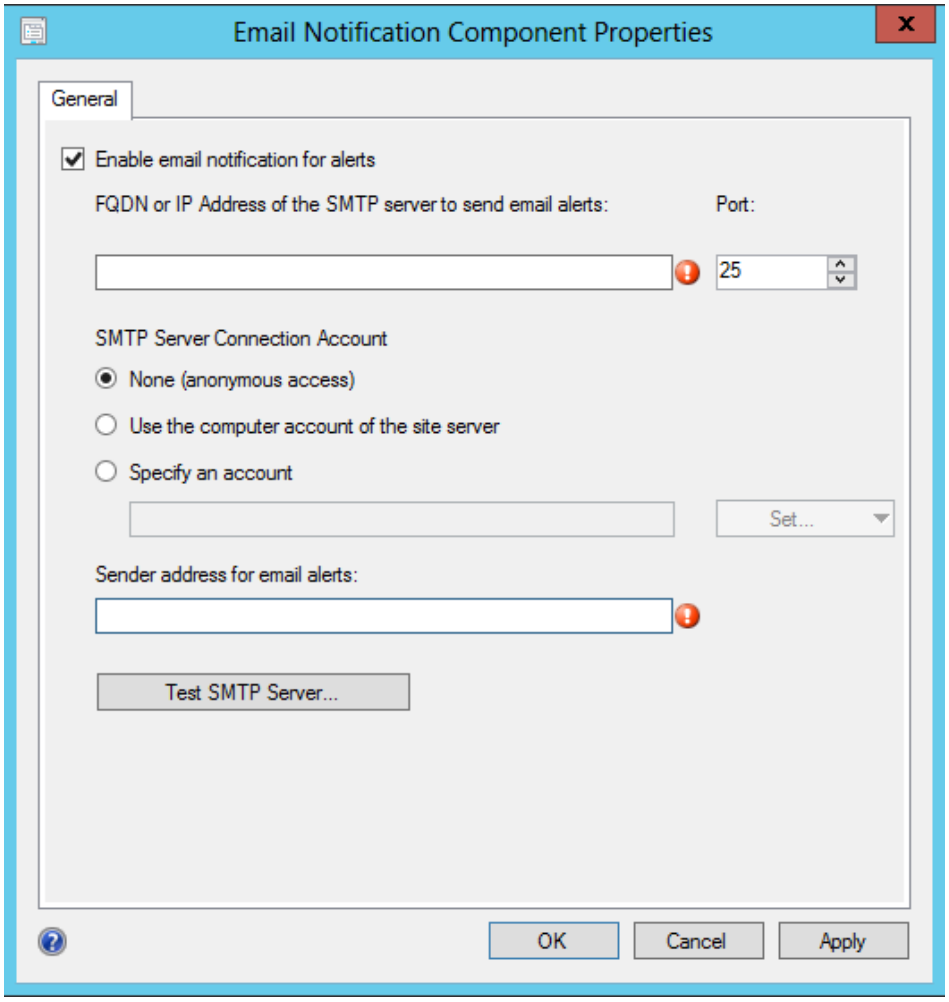
Hälytyksiä voidaan luoda kokoelmille menemällä Assets and Compliance -välilehdelle. Device Collection -kohdasta valitaan haluttu kokoelma, jolle hälytykset konfiguroidaan ja valitaan Properties. Alerts-välilehdessä valitaan View this collection in the Endpoint Protection dashboard. Kyseinen valinta näyttää kokoelman Endpoint Protection monitoroinnissa. Valitaan Add, josta aukeaa uusi ikkuna. Täältä valitaan, mitkä kaikki clienttien tilat ja Endpoint Protection hälytykset tullaan näyttämään. Voidaan valita, miten SCCM näyttää hälytyksen, kun Endpoint Protection havaitsee viruksen (kuva 19).



Kuva 19. Hälytysten määrittely kokoelmalle.

Hälytyksiä voidaan lähettää myös sähköpostitse. Mennään Administrator-välilehdelle, valitaan Settings, Configure Site Components, Email notification. Kuvan 20 asetusikkuna aukeaa, josta voidaan konfiguroida sähköpostihälytykset.

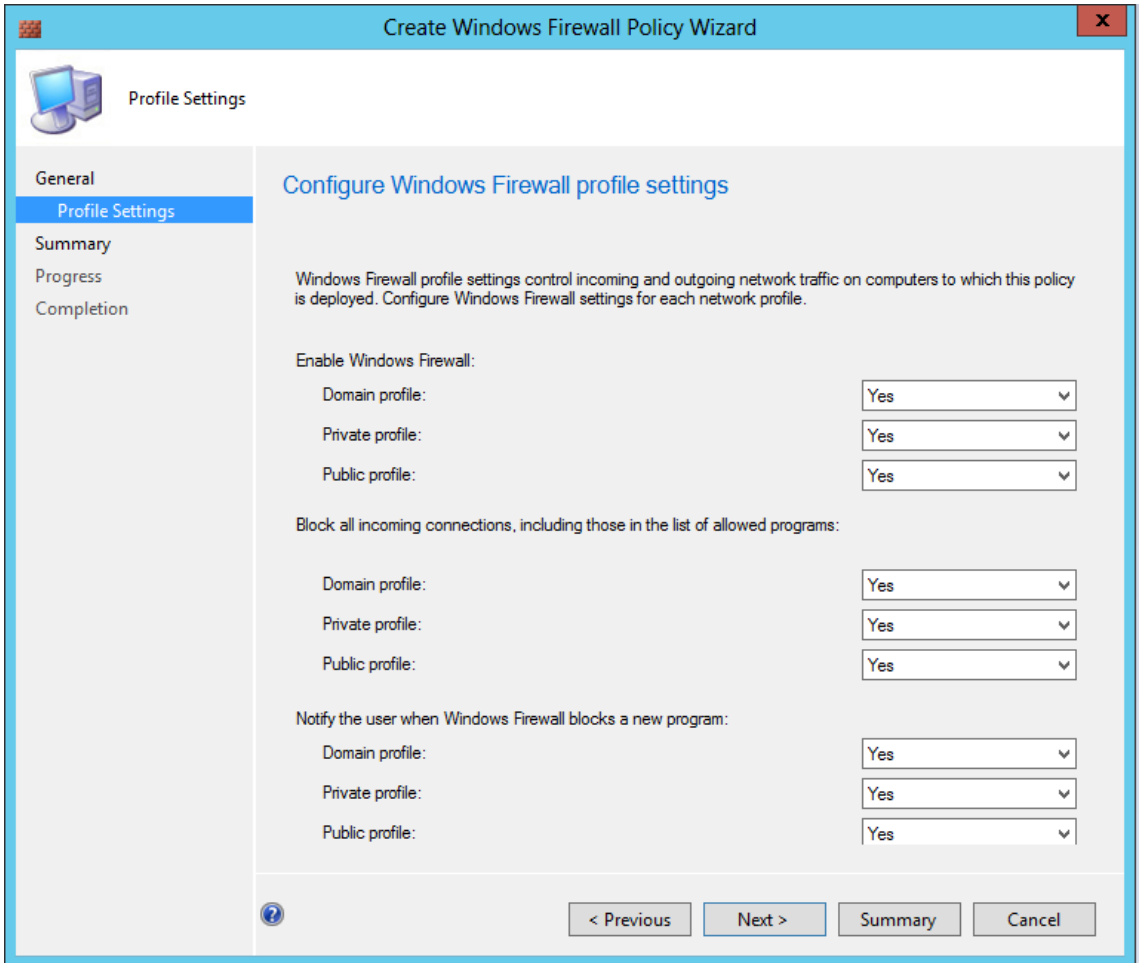
Valitaan Enable email notification for alerts ja annetaan SMTP-palvelimen IP-osoite ja portti. Lähettäjän sähköpostiosoite täytyy myös antaa Sender address for email alerts -kohtaan, jotta sähköpostien lähetykset toimivat.



Kuva 20. Sähköpostihälytysten määrittely.

5.4 Firewall policy

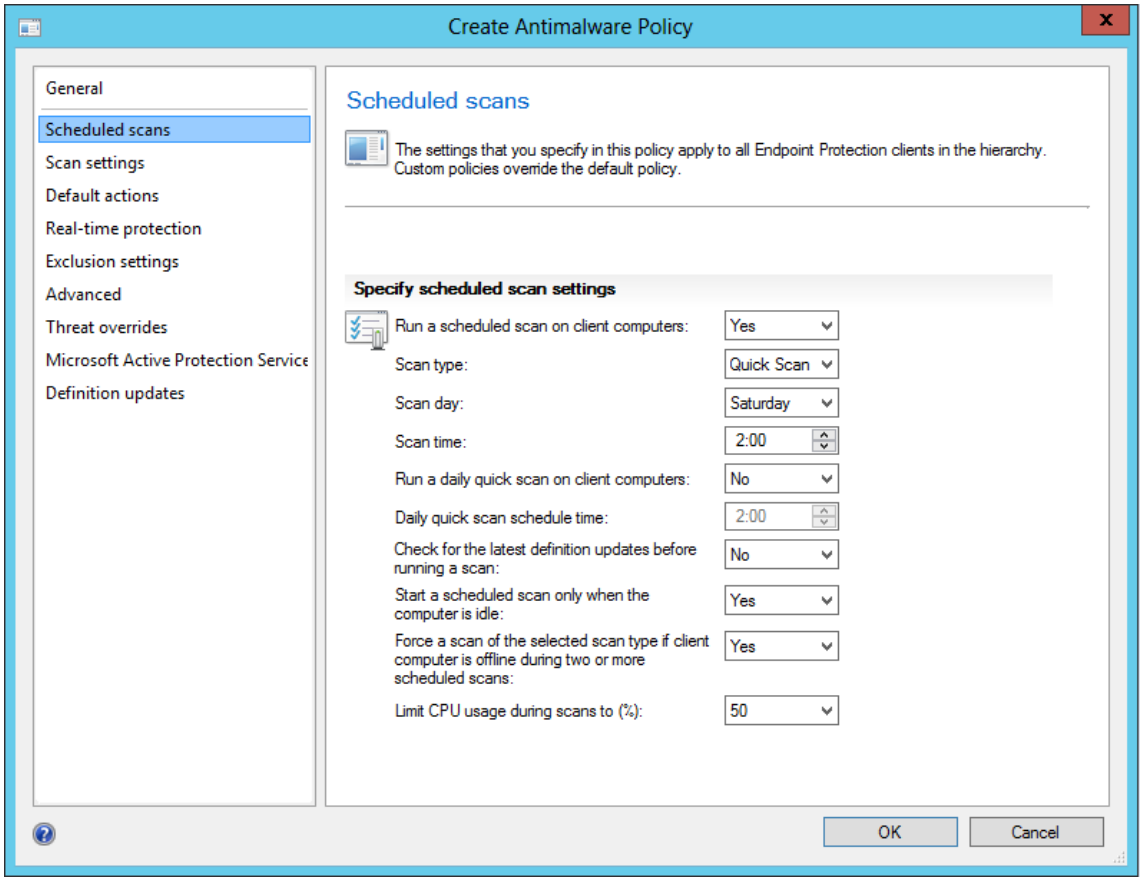
Palomuurin asetuksia voidaan muokata Assets and Compliance-, Windows Firewall policies-, Create Windows Firewall policy -kohdasta. Ikkuna aukeaa, josta määritellään halutut asetukset. Asetuksista voidaan laittaa palomuuri päälle tai pois päältä. Asetuksista muokataan myös, sallitaanko palomuuri toimialueelle, sen ulkopuoliselle turvalliselle verkolle ja julkiselle verkolle. Lopuksi muokataan vielä ilmoituksia palomuurin estämistä ohjelmista (kuva 21).



Kuva 21. Windows Firewall Policy -asetukset.

5.5 Antimalware policy

Seuraavaksi käydään läpi Antimalware Policy -asetuksia. Antimalware policyjä luodaan kohdasta Assets and Compliance, Antimalware policy, Create antimalware policy. Asetusikkuna aukeaa, jossa voidaan määritellä seuraavia asetuksia (kuva 22).



Kuva 22. Antimalware Policy -asetukset.

Scheduled scans -kohdasta voidaan valita, kuinka usein ja milloin tietokoneilla ajetaan virusskannaus. Voidaan myös valita, tarkistaako SCEP 2012 uusimpia päivityksiä ennen kuin se suorittaa virusskannauksen. Jos jotkin tietokoneet eivät ole käynnissä, voidaan virusskannaus pakottaa tehtäväksi, kun tietokone käynnistyy seuraavan kerran. Lopuksi voidaan rajoittaa suoritinkäyttöä skannauksen aikana, jotta virusskannaus ei haittaisi käyttäjän työskentelyä. Tietokoneelle voidaan myös suorittaa manuaalinen virusskannaus, jota esitellään tämän luvun lopussa.

Scan settings -välilehdellä määritellään, mitä kaikkea skannataan. Täältä voidaan valita esimerkiksi skannattavaksi sähköpostit, kovalevyt, ulkoiset massamuistilaitteet, verkon levyasemat tai vaikka vain jokin tietty kansio.

Default actions -kohdasta löytyvät asetukset toimenpiteille, jotka suoritetaan, kun mahdollinen uhka löytyy. On suositeltavaa jättää tämä kohta oletusasetuksille, jolloin SCEP 2012 valitsee järkevimmän toimenpiteen, kun uhka havaitaan.

Enable real-time protection -välilehdellä voidaan muokata reaaliaikaisen suojauksen asetuksia. Reaaliaikainen suojaus skannaa kaikki ulos ja sisään tulevat tiedostot.

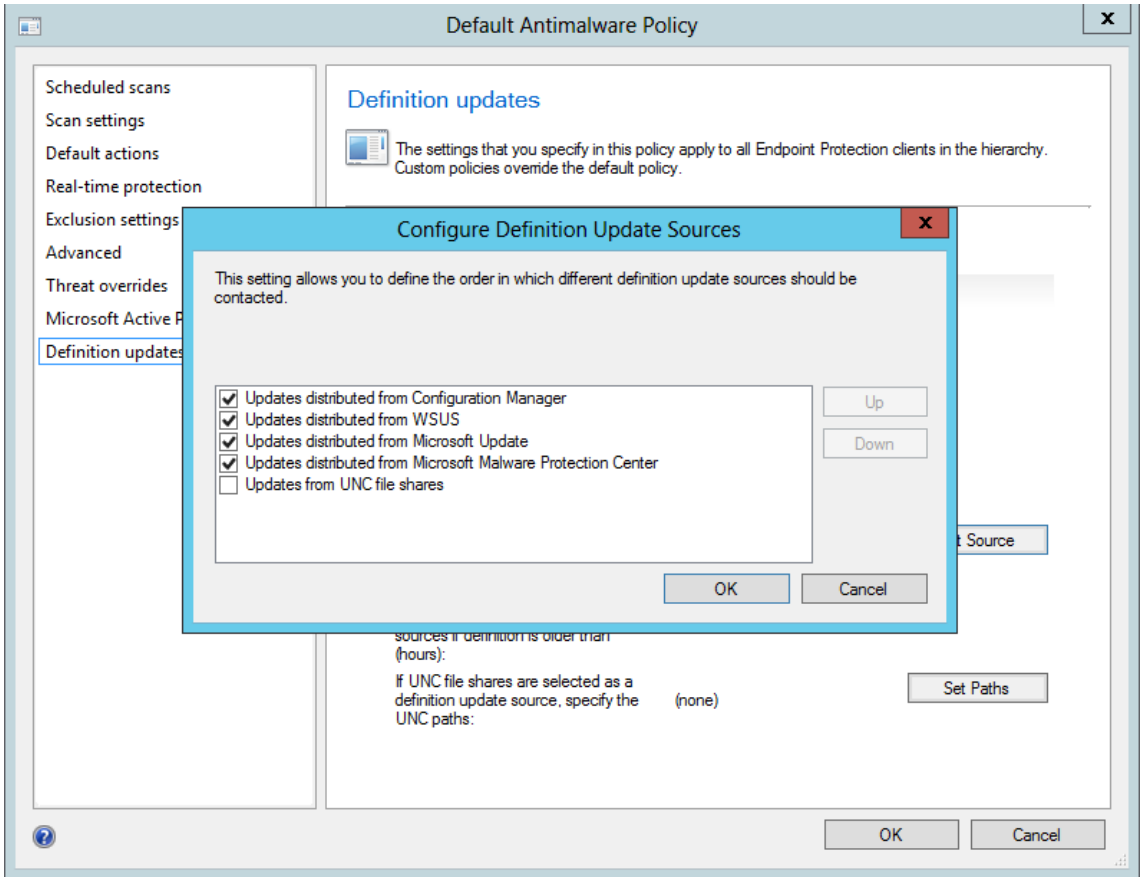
Exclusion settings -välilehdeltä määritellään eri tiedostotyyppien poissulkeminen, kun virusskannauksia suoritetaan. Täältä voidaan sulkea pois esimerkiksi kuvaformaattipäätteet kuten .JPG tai .PNG, mikä nopeuttaa virusskannausta.

Advanced-välilehdeltä löytyy lisäasetuksia tietoturvaan liittyen, kuten mahdollisuus antaa käyttäjälle oikeus poissulkea tiedostoja ja kansioita virusskannauksista. Täällä voidaan myös tehdä järjestelmän palautuspisteitä ennen tietokoneen puhdistamista.

Threat overrides -asetuksissa voidaan muokata suoritettavia toimenpiteitä eri tason tietoturvauhkille, joille on valittuna Recommended actions -asetus. Tietoturvaohjelmistot saattavat luokitella itse tehtyjä ohjelmia haittaohjelmiksi, joten näistä asetuksista voidaan sallia kyseinen ohjelma turvalliseksi.

Microsoft Active Protection Service -välilehdellä valitaan, sallitaanko uhkatilanteessa clientin lähettää tietoa viruksesta Microsoftille.

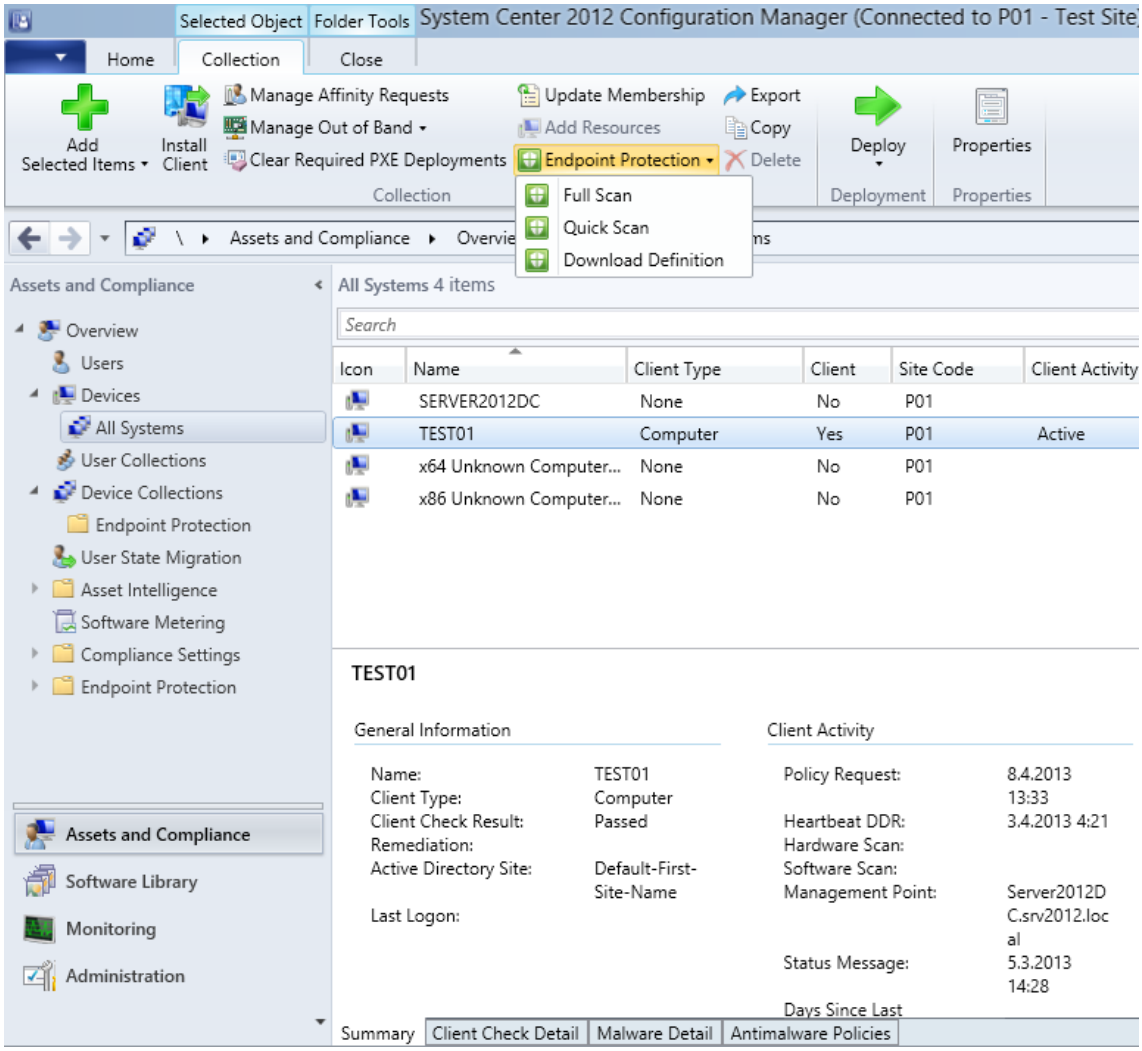
Definition Updates, eli virustietokannan päivitys -välilehdeltä muokataan, kuinka usein SCEP 2012 -client hakee päivityksiä. Päivitysten tarkistus voidaan asettaa esimerkiksi suoritettavaksi muutaman tunnin välein tai päivittäin tiettynä kellonaikana. Asetuksista voidaan valita, mistä päivitykset haetaan (kuva 23). Päivitykset voidaan hakea joko Configuration Managerin kautta, käyttämällä WSUS-, Microsoft Update- tai Microsoft Malware Protection Center -palvelujen avulla. Päivityksiä voidaan ladata myös UNC-tiedostojaolla. WSUS, eli Windows Server Update Services on palvelimella toimiva ohjelmisto, jonka avulla voidaan jakaa päivityksiä tietoverkossa. [10.] UNC, eli Universal Naming Convention on formaatti, jolla määritellään tiedoston tai kansion polku tietoverkossa. [11.]



Kuva 23. SCEP 2012 -clientin päivitysten asetukset.

Kun Firewall- ja Antimalware policyjä on luotu, voidaan jakaa niitä haluttuihin tietokoneisiin tai kokoelmiin. Policyjen jakaminen tapahtuu Assets and Compliance -välilehdeltä, Endpoint Protection -valikon alta. Kun haluttu sääntö on valittuna, voidaan valita Deploy. Avautuvasta ikkunasta valitaan tietokone tai kokoelma, jolle kyseinen Policy halutaan jakaa. Tämän jälkeen valitaan vain OK ja säännöt ajetaan kyseiselle kohteelle.

Tietokoneille ja kokoelmille voidaan myös suorittaa manuaalisesti virusskannauksia. Tämä tapahtuu menemällä halutun kohteen kohdalle Assets and Compliance -välilehdellä ja valitsemalla ylhäältä Endpoint Protection -pudotusvalikko. Täältä voimme valita, suoritetaanko valitulle kohteelle täydellinen vai nopea virusskannaus. Voidaan myös valita Download Definition, jolla tarkistetaan, onko valitulle SCEP 2012 clientille päivityksiä saatavilla (kuva 24).



Kuva 24. SCEP 2012 -clientin manuaalinen virusskannaus.

6 Testaus

SCEP 2012 on asennettu ja konfiguroitu. Firewall ja Antimalware policyjä on myös luotu, joten SCEP 2012 on käyttövalmis, ja sitä voidaan alkaa jakaa asiakaskoneisiin. Tätä ennen on kuitenkin hyvä testata sen toimintaa ja varmistaa, että se varmasti toimii halutulla tavalla. Projektissa oli tarkoitus testata, kuinka SCEP 2012 -client havaitsee viruksen ja kuinka se reagoi siihen.

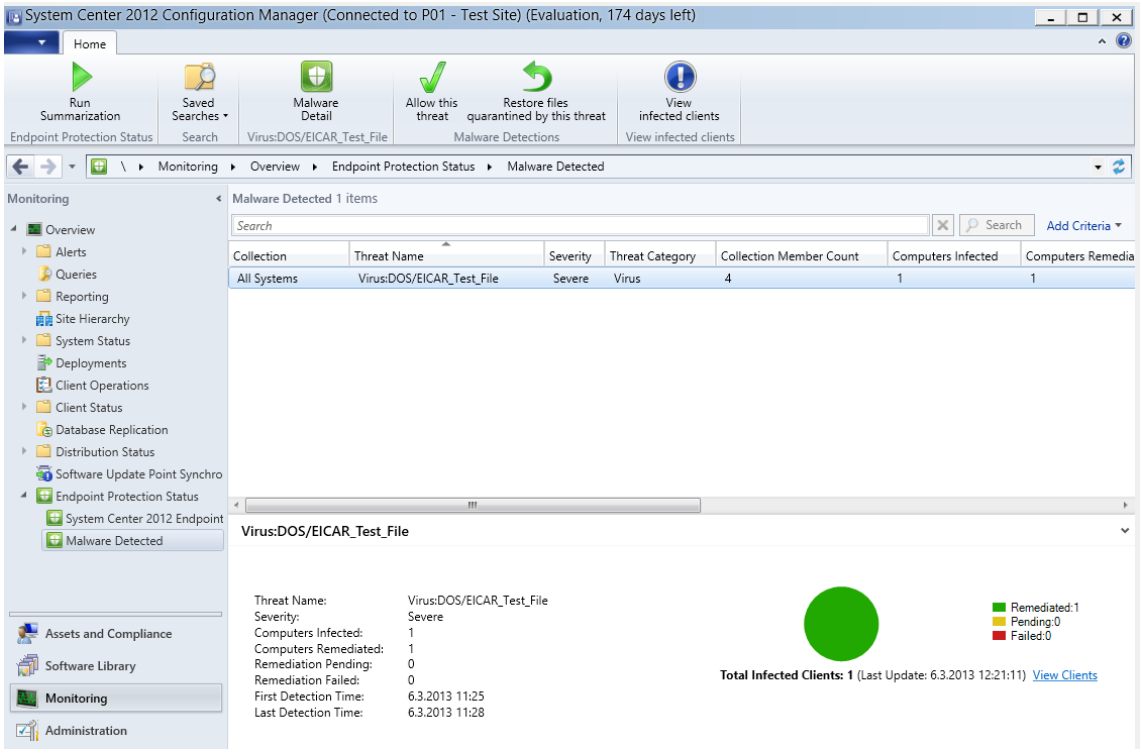
Testauksessa ladataan virus asiakaskoneelle ja katsotaan, kuinka SCEP 2012 client ilmoittaa siitä SCCM-palvelimelle. Testissä käytettiin Eicar-testivirusta. Eicar-testivirus on standardoitu harmiton tiedosto, jolla voidaan testata tietokoneen tietoturvaohjelmistoa. Jos tietoturvaohjelmisto ei havaitse Eicar-tiedostoa, niin voidaan

todeta siinä olevan ongelmia. Eicar-testiviruksen voi ladata osoitteesta http://www.eicar.org/.

Eicar-tiedosto ladattiin .ZIP -päätteisenä tiedostona ja koitettiin avata asiakaskoneella. Eicar-tiedosto yritettiin myös tallentaa asiakaskoneella .COM-päätteisenä. Ohje Eicar-testiviruksen luomiseen löytyy liitteestä 1. SCEP 2012 client onnistui havaitsemaan viruksen ja esti sen (kuva 24).

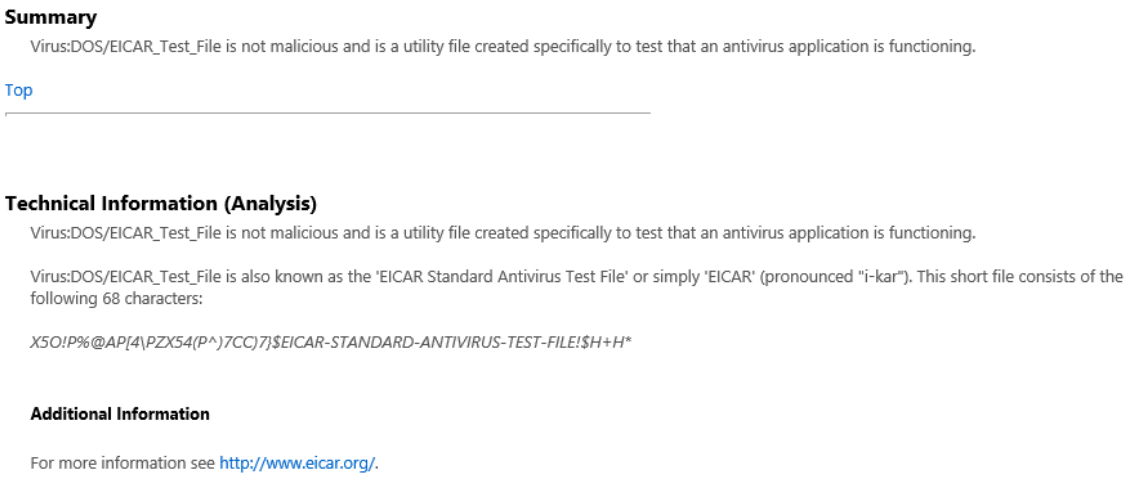
Kuva 25. Kuva SCEP 2012:n ilmoitusviestistä, kun se havaitsee viruksen.

SCEP 2012 client myös esti tallentamasta virusta tietokoneelle. SCEP 2012 client ilmoitti SCCM-palvelimelle onnistuneesti mahdollisesta tietoturvauhkasta. Malware Detected kohdassa näemme, mikä laite on mahdollisesti saanut tartunnan, missä tiedosto sijaitsee, mitä toimenpiteitä sille on suoritettu ja millainen uhka on kyseessä (kuva 24). Tämä helpottaa huomattavasti ylläpitäjän tehtävää löytämään mahdolliset tietoturvauhkat. SCEP 2012 -client havaitsi viruksen, poisti sen ja ilmoitti siitä SCCM-palvelimelle, joten palvelu voidaan todeta toimivaksi tietoturvaratkaisuksi.



Kuva 26. Ilmoitusviesti SCCM-palvelimella havaitusta viruksesta.

Viruksesta voidaan myös tarkastella mahdollisia lisätietoja Microsoftin kattavasta virustietokannasta. Tämä tapahtuu painamalla ylhäältä Malware Detail -painiketta, joka ohjautuu selaimella Microsoftin sivuille kyseisen viruksen tietoihin. Täältä nähdään tarkka kuvaus, minkä tyyppinen virus on kyseessä ja mitä se sisältää (kuva 25).



Kuva 27. Microsoftin kuvaus Eicar-testiviruksesta selaimella.

7 Yhteenveto ja johtopäätökset

Tämä opinnäytetyö tehtiin Metropolia Ammattikorkeakoululle. Työn päätavoite oli laatia käyttöönotto-ohjeet Microsoft System Center 2012 Endpoint Protection -tietoturvaratkaisulle. Työn ensimmäisessä vaiheessa esiteltiin testiympäristö ja ohjelmistot, joita tässä opinnäytetyössä käytettiin. Seuraavaksi käytiin läpi tarvittavien ohjelmien asennus sekä konfigurointi SCEP 2012:ta varten. Toisessa osiossa perehdyttiin myös syvällisemmin työn pääohjelmaan, eli SCEP 2012:n käyttöönottoon, hallintaan ja sisältöön.

Ennen SCEP 2012:n käyttöönottoa laadittiin ohjeet SCCM-asennuksesta, konfiguroinnista sekä käytiin hieman läpi, mitä se pitää sisällään yleisellä tasolla. SCCM:n ensivaikutelma tuntui yksinkertaiselta, mutta ohjelmiston laajuus käy nopeasti ilmi. Ohjelmiston konfigurointi eri tarpeisiin vaatisi varmasti syvempää perehtymistä.

SCEP 2012 vaati hieman harjoittelua ja tutustumista asetuksiin eri käyttötarkoituksia varten. Perehtymisen jälkeen käyttöönotto sujui kuitenkin ongelmitta ja SCEP 2012 client saatiin asennetuksi asiakaskoneelle. Tutustumisen jälkeen SCEP 2012 vaikuttaa hyvinkin selkeältä ja helppokäyttöiseltä, vaikka sen eri asetuksia löytyy laajalti. Lopputestaus myös osoittaa, että SCEP 2012 toimi suunnitellusti asikaskoneella.

SCEP 2012 on varmasti hyvin kätevä tietoturvaratkaisu isoissa organisaatiossa, joissa on monia eri toimipisteitä tai satoja eri laitteita hallittavana keskitetysti. Näin myös SCEP 2012 -clienttien vianetsintä sekä sovellusten asennus asiakaskoneisiin sujuu vaivatta, eikä tarvitse käydä jokaisella asiakaskoneella etsimässä mahdollisia vikoja. Kasvavissa organisaatiossa varmasti kannattaa miettiä SCEP 2012:n käyttöönottoa hyvissä ajoin.

Lähteet

1 What's New in Windows Server 2012. 2012. 2012. Verkkodokumentti. http://technet.microsoft.com/en-US/library/hh831769. Luettu 4.3.2013.

2 System Center 2012 Configuration Manager Overview. 2013. Verkkodokumentti. http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012-overview.aspx. Luettu 6.3.2013.

3 System Center 2012 Endpoint Protection. Verkkodokumentti. http://www.microsoft.com/en-us/server-cloud/system-center/endpoint-protection-2012.aspx. Luettu 7.3.2013.

4 Introduction to Endpoint Protection In Configuration Manager. 2013. Verkkodokumentti. http://technet.microsoft.com/library/hh508781.aspx. Luettu 10.3.2013.

5 Minimum Hardware Requirements for Site Systems. 2013. Verkkodokumentti. http://technet.microsoft.com/en-us/library/gg682077.aspx#BKMK_SupConfigSiteSystemReq. Luettu 5.3.2012.

6 HTTP Secure. 2013. Verkkodokumentti. http://en.wikipedia.org/wiki/HTTP_Secure. Luettu 11.3.2013.

7 Discovery Methods in Configuration Manager. 2013. Verkkodokumentti. http://technet.microsoft.com/en-us/library/gg712308.aspx#BKMK_DiscoveryMethods. Luettu 12.3.2013.

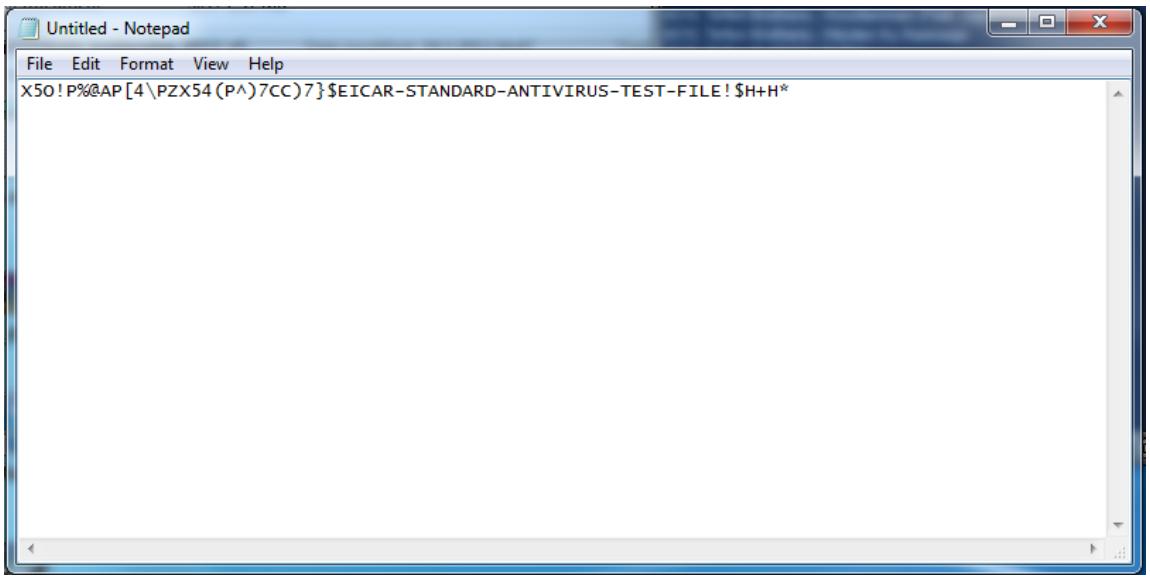
8 Planning for Boundaries and Boundary Groups in Configuration Manager. 2013. Verkkodokumentti. http://technet.microsoft.com/en-us/library/gg712679.aspx. Luettu 12.3.2013.

9 Distribution Point Configurations. 2013. Verkkodokumentti. http://technet.microsoft.com/en-us/library/gg712321.aspx#BKMK_DistributionPointConfigurations. Luettu 13.3.2013.

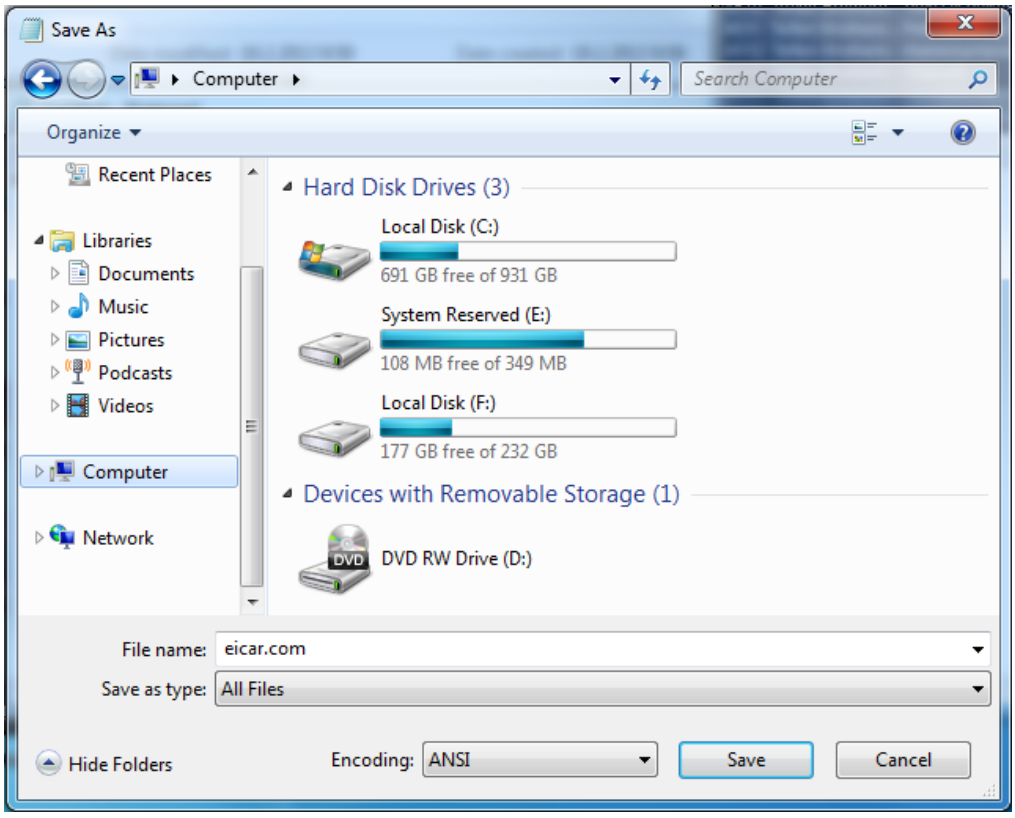
10 Windows Server Update Services. 2013. Verkkodokumentti. http://technet.microsoft.com/fi-fi/windowsserver/bb332157. Luettu 16.3.2013.

11 Universal Naming Convention. 2008. Verkkodokumentti. http://en.wikipedia.org/wiki/Path_%28computing%29. Luettu 16.3.2013.

Eicar-testivirus



Kuva 1. Luodaan notepadilla uusi tiedosto johon kirjoitetaan seuraava skriptikoodi sisällöksi.



Kuva 2. Tiedosto tallennetaan ”eicar.com” nimellä, jolloin tietoturvaohjelmiston pitäisi havaita virus.