Tietoturvan ylläpito

Saatesanat

Tulen kuvaamaan ja kertomaan tietoturva sovelluksen asennuksen ja sen jakamisen työasemille, tietoturva auditointi käyttäen valmista sovellusta sekä merkityksen miksi on tärkeää että on eritelty käyttäjätunnuksen roolin mukaan ja miksi ei tule käyttää liian järeitä tunnuksia laitteiden ylläpitoon.

Tämä merkityksen tulen näyttämän tämän dokumentin Tietoturva demo osiossa, jossa ”ylennän” itseäni normaalisti Active Directory käyttäjästä Domain Administrator tason käyttäjäksi.

Tulen myös kertomaan miten tämä voidaan estää, varsin helpoilla toimenpiteillä toimialueen sekä tietoturvan parannuksilla työasema tasolla.

Virtuaalipalvelimet

Palvelin ympäristö on asennettu Oracle Virtualbox sovelluksen päälle joka on asennettu Windows 10 1909 koneelle.
Fyysisessä koneessa on muistia 24GB ja suorittimena on Intelin i6700k -suoritin, jossa on neljä ydintä. Kiintolevynä Virtualbox palvelimille toimii Kingston merkkinen SSD-levy, jolla kokoa n. 960GB. Itse virtuaalipalvelimet vievät levytilaa n. 181GB

Verkkoalueena toimii 10.0.10.0/24 ja Gateway roolissa toimii Untangle -palomuuri virtuaalipalvelin IP-osoitteella 10.0.10.1

Palvelimet jotka ovat asennettu tähän jarno.local -nimiseen Active Directory toimialueeseen sekä niiden roolit lyhyesti kuvattuna seuraavaksi.

INF-DC01 / 10.0.10.2 / Windows Server 2019 Core
-Domain Controller (FSMO roolien omistaja), DNS-palvelin, DHCP-palvelin, tiedosto palvelin, tulostus -palvelin.

INF-DC02 / 10.0.10.10 / Windows Server 2016 Core
-Domain Controller sekä DNS-palvelin

INF-SEPM01 / 10.0.10.3 / Windows Server 2019 GUI
- Symantec Endpoint Protection Manager-palvelin

INF-SEC01 / 10.0.10.4 / Windows Server 2019 GUI
- Nessus Essentials-palvelin.

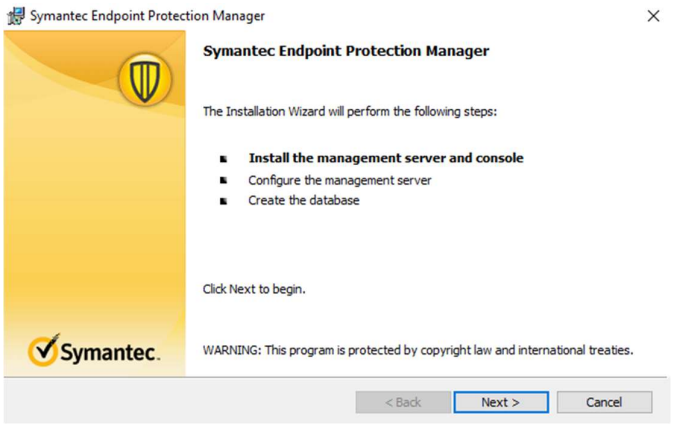
Olen myös asentanut oheiset työasema käyttöjärjestelmäiset virtuaalikoneet, jotka saavat ip -osoitteensa INF-DC01 palvelimet DHCP palvelua käyttäen. Nämä työasemat ovat osana jarno.local toimialuetta.

Windows 10 v1909 Desktop (x64)
Windows 10 v1909 Laptop (x64)
Windows 7 Professional (x64)
Windows XP Professional (x86)

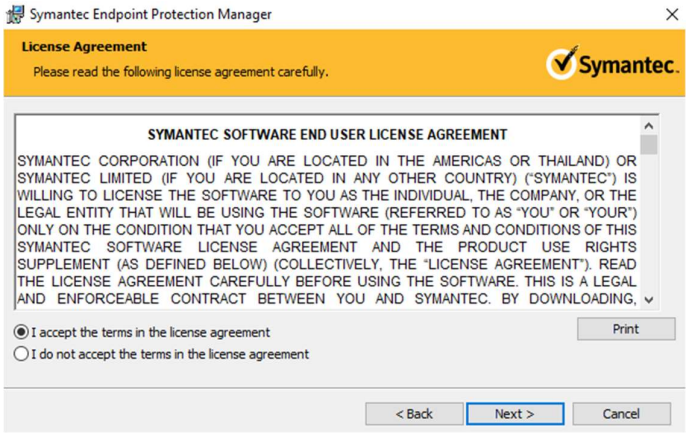
Symantec Endpoint Protection Manager sovelluksen asennus

Seuraavaksi tulen kuvaamaan kuinka tapahtuu Symantec Endpoint Protection Manager (jäljempänä SEPM) palvelimen asennus Windows Server 2019 ympäristöön.
SEPM palvelin tarkoitus on toimia keskitettynä tietoturva sovelluksen hallinta ja ylläpito -palvelimena jarno.local toimialueella.
Tällä palvelimella voidaan jakaa tietoturva sovelluksia erilaisilla komponenteilla työasemille ja palvelimille sekä muuttaa sääntöjä keskitetysti, miten tietoturva -sovellus toimii työasemilla ja palvelimilla.

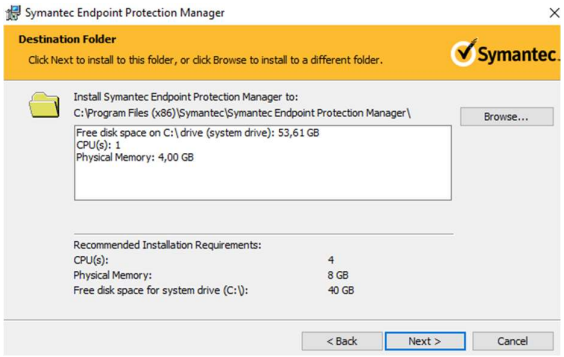
Olen ladannut trial -version jonka tulen asentamaan.



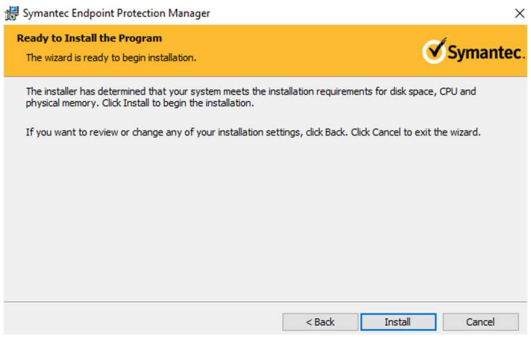
Asennuksen käynnistyksessä tuleen ensimmäiseksi ikkuna joka kertoo mitä tulemme asentamaan ja missäkin järjestyksessä. **Next.**



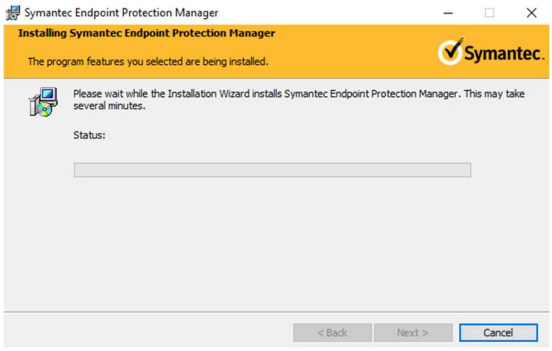
Seuraavaksi luemme tarkasti lisenssi ehdot. **Next.**



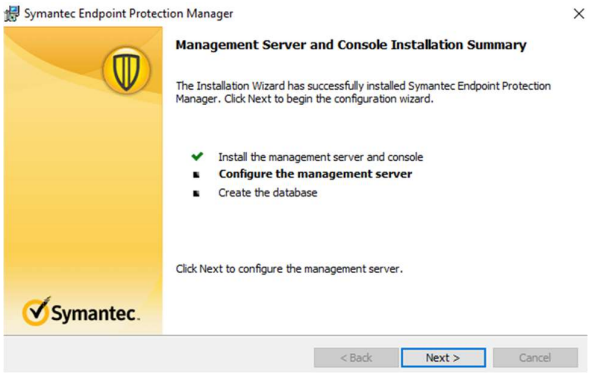
Tämän jälkeen ohjelma ehdottaa asennus kansiota sekä tarkistaa että palvelimella on tarpeeksi resursseja, jotta asennus voidaan suorittaa. Tässä tapauksessa minulla on vain 4GB muistia, vaikka Symantec suosittaa, että olisi 8GB muistia, mutta voimme jatkaa tästä huolimatta asennusta. **Next.**



Seuraavaksi ryhdymme itse asennukseen, kun asennus on varmistanut, että kaikki tarpeellinen resurssi on saatavilla. **Install.**

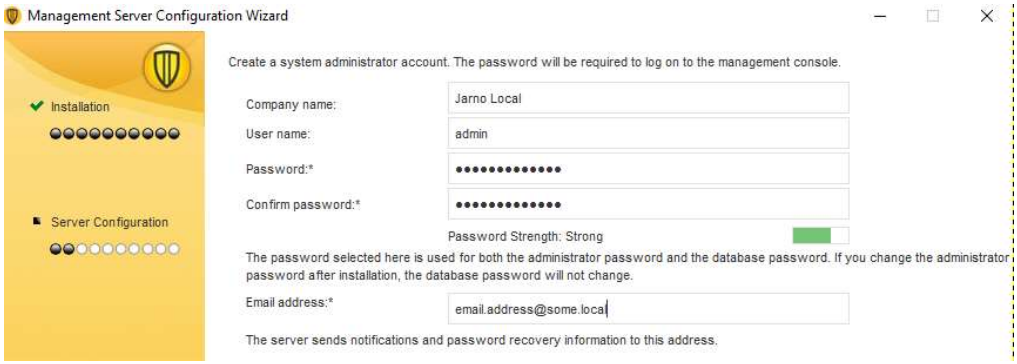


Oheinen asennus dialogi ilmestyy seuraavaksi ja odotamme että se valmistuu.



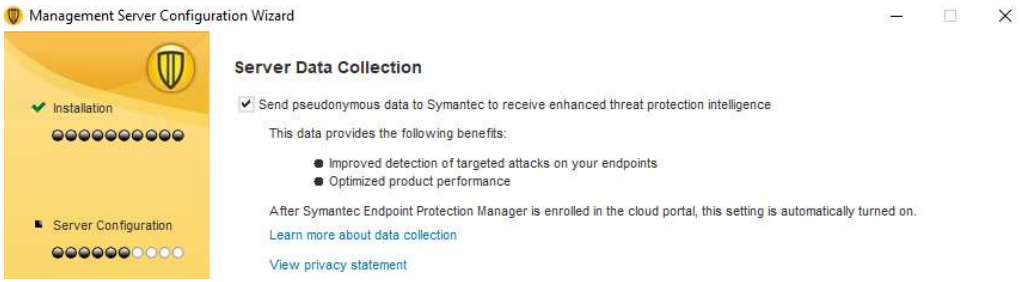
Nyt kun olemme saaneet asennettua palvelimen ja konsolin, niin jatkamme tietokannan asennukseen. **Next.**

Seuraavaksi valitsemme oletuksen, eli meillä on alle 500 työasemaa jota haluamme hallinnoida. Voimme myös määrittää, että luomme oman SQL-tietokannan mutta tässä tapauksessa Symantecin oma sisäänrakennettu tietokanta palvelin riittää meidän asennus tarpeisiin. **Next**

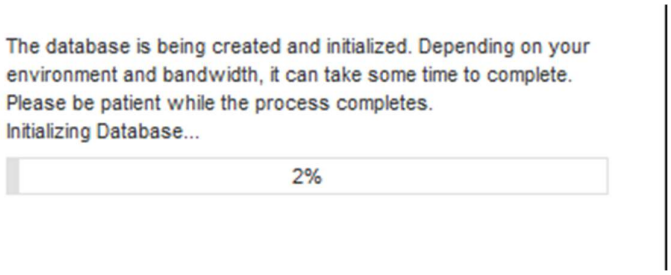


Tämän jälkeen määritämme yrityksen tiedot, sekä pääkäyttäjän tunnuksen sekä salasanan.
Myös tässä kohtaa pitää määrittää sähköpostiosoite mihin voidaan lähettää viestejä järjestelmästä.
Huomio, että tässä tapauksessa olen antanut tähän keksityn sähköpostiosoitteen. **Next.**

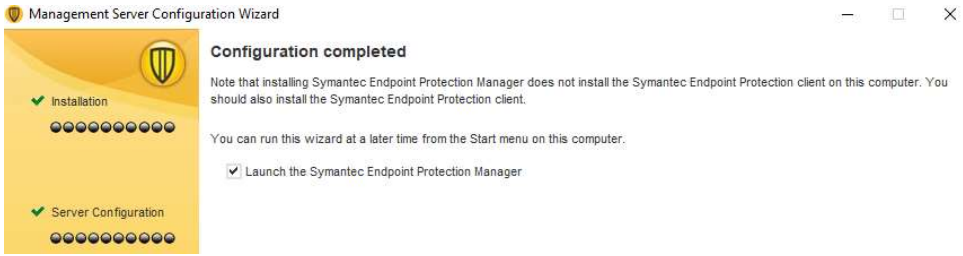
Tässä määritämme seuraavaksi, että Symantec hakee tuoreimmat sovelluspäivityksen sekä virustietokantakuvakset asennuksen aikana. **Next.**



Nyt voimme sallia, että meidän palvelin lähettää pseudonyymisuus tietoa Symantecin palvelimelle. Tämä mahdollisesti voi parantaa myös tietoturvaa yleisellä tasolla. **Next.**

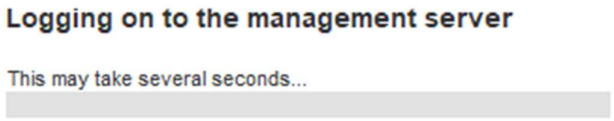


Seuraavaksi tapahtuu itse tietokannan luonti. Tässä voi kestää tovikin, joten tässä välissä voi käydä ottamassa esimerkiksi kupin kahvia tai teetä.

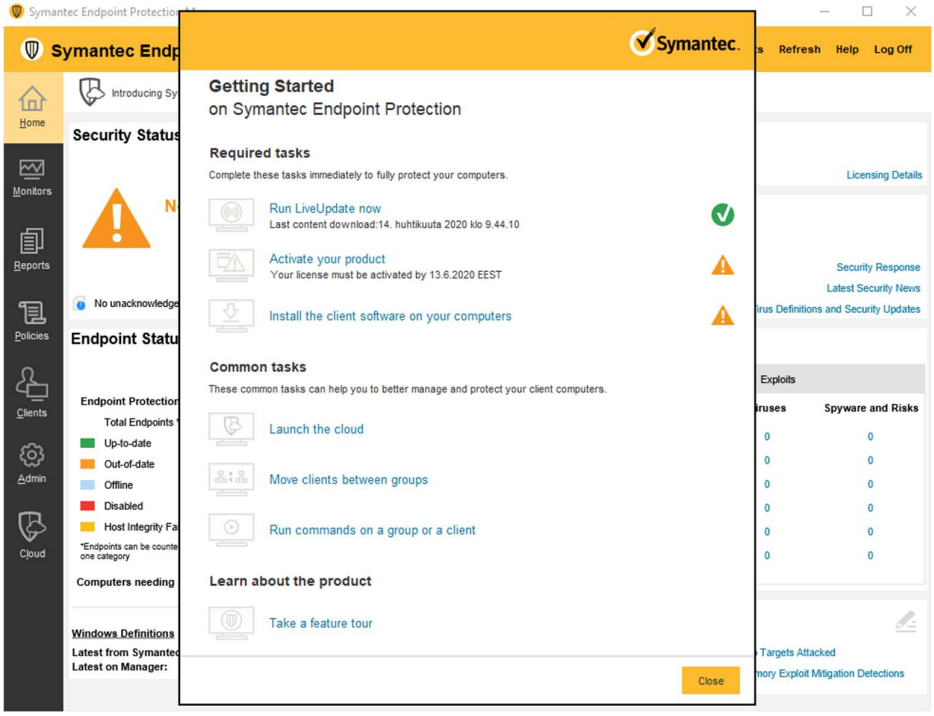


Ja lopuksi kun tietokanta on muodostettu onnistuneesti, voimme asennuksen lopuksi käynnistää Symantec Endpoint Protection Manager sovelluksen. **Finish.**

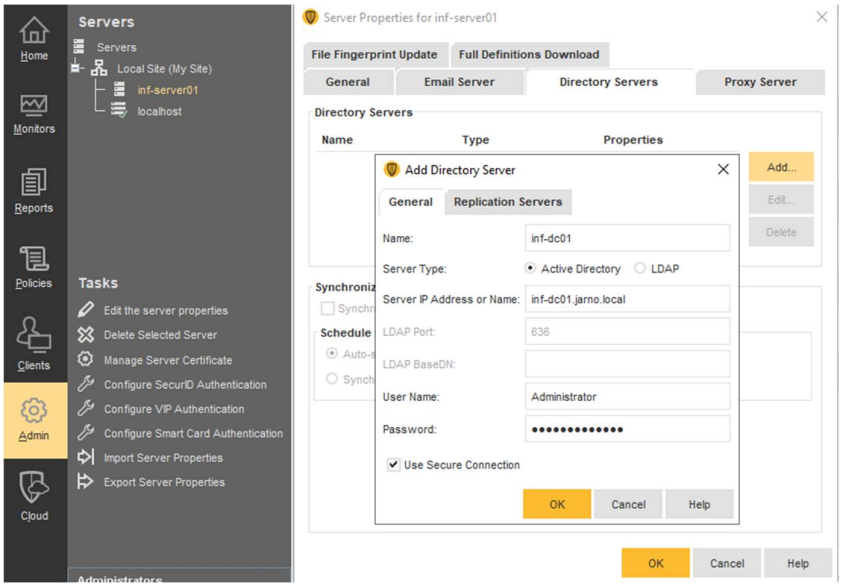
Kun valitsemme että asennuksen jälkeen käynnistetään SEPM sovellus automaattisesti, niin seuraavaksi meitä pitäisi hetken päästä kohdata tällainen ikkuna.
Tähän annamme asennuksen aikana luodut pääkäyttäjä tunnukset. **Log On**



Tämän jälkeen odotamme hetken, kun kirjaudumme sisälle järjestelmään.

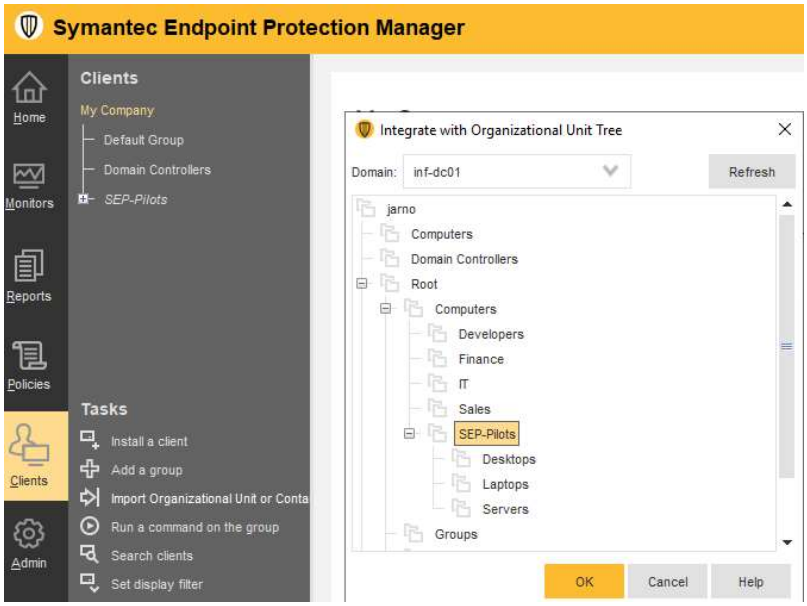


Meille avautuu nyt päänäkymä, jolla voimme hallinnoida SEPM palvelua ja siihen liitettyä työasemia.**Close**
Vasemmalla sivupalkissa on navigointi painikkeet, joilla saamme valittua eri hallinta näkymiä.



Meidän pitää tuota olemassa oleva Active Directory tieto SEPM sovellukseen, jotta voimme hallinnoida koneita Active Directory Organisaatio Yksikkö tasolla. Pääsemme tähän määritykseen vasemmalta Admin -> Servers -> Local Site -> inf-server01 -> Edit server properties -> Directory Servers -> Add

Jossa annamme sitten tiedot toimialueesta, kuten palvelin sekä tunnuksen jolla luomme Active Directorystä tietoa. Tähän voinee käyttää muutakin tunnusta kuin Administrator, riittänee tunnus joka voi lukea vain tietoa, tyyliin Domain Users tason tunnus. **OK**



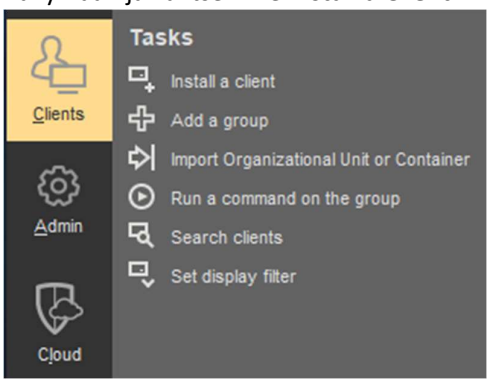
Tämän jälkeen voimme vasemmalta Import Organizational Unit or Container kautta valita domain ->inf-dc01 ja valita jarno -> Root -> Computer -> SEP-Pilots Organisaatio Yksikön jonka jäseniä voimme hallinnoida sekä asentaa SEP tietoturva sovelluksen. **OK.**

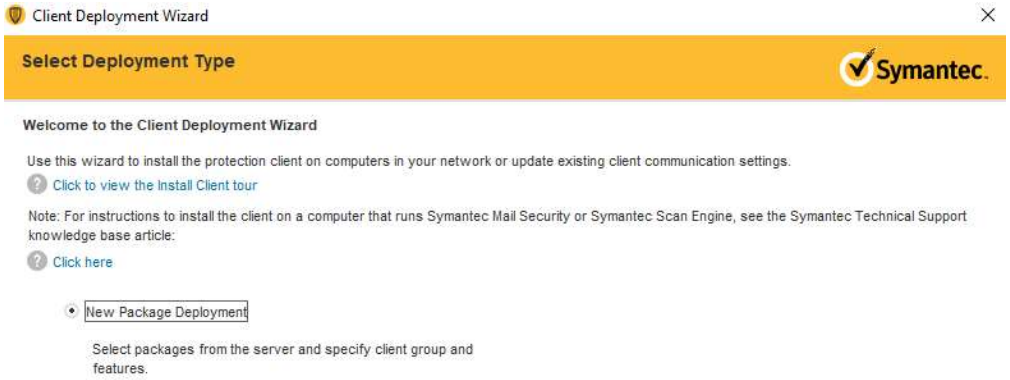
Ja nyt meillä näkyy tämän valitun Organisaatio Yksikkö puu vasemmalle Clients näkymässä.

Tässä vaiheessa olemme siis saaneet asennettua SEPM sovelluksen.
Seuraavassa osiossa luomme asennus paketin ja asennamme sen etänä työasemille SEPM hallinnan kautta.

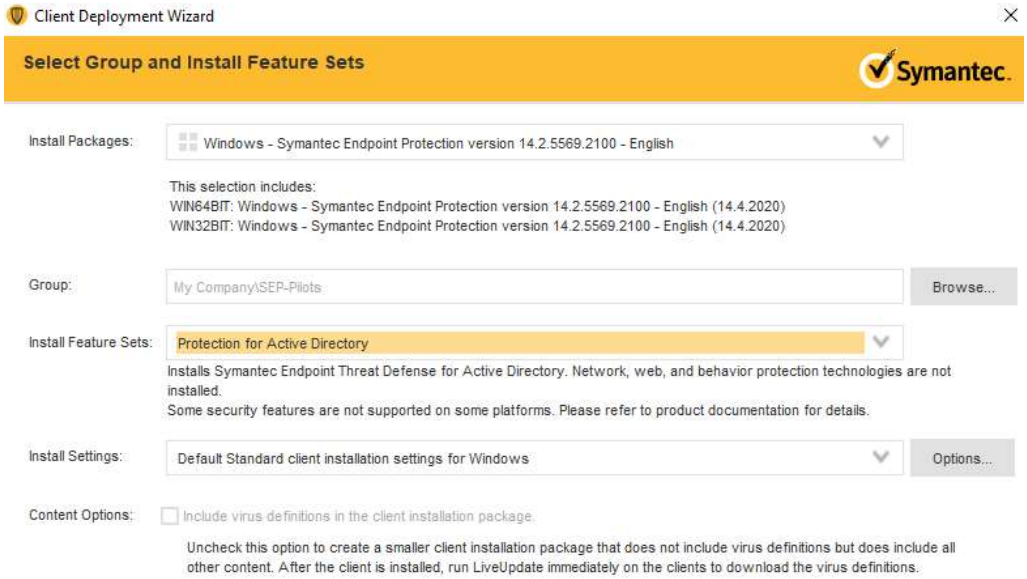
Symantec Endpoint Protection sovelluksen asennus

Avaamme siis SEPM hallinta paneelin, ellei sitä ole jo valmiiksi avattu ja menemme vasemmalta Clients näkymään ja valitsemme **Install a Client.**

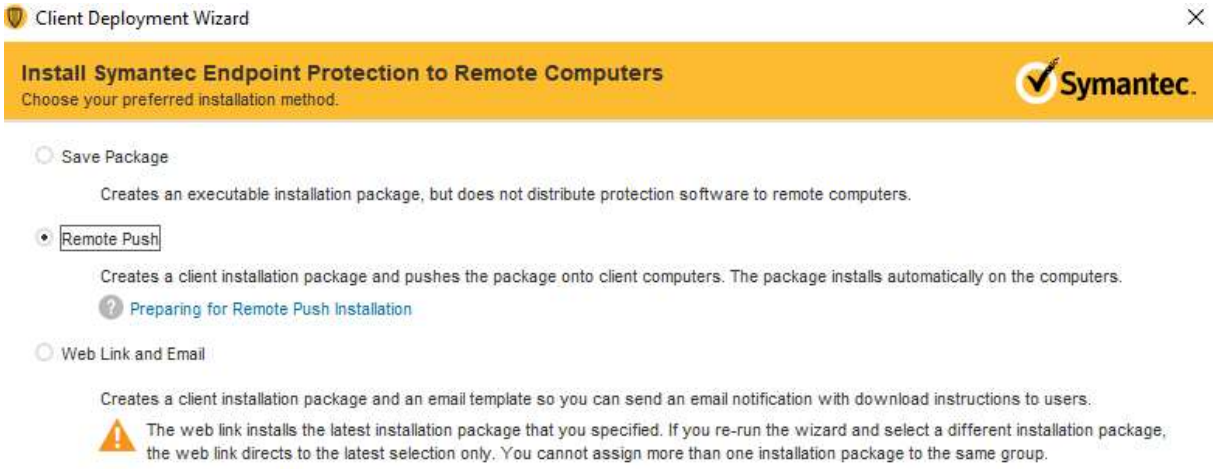




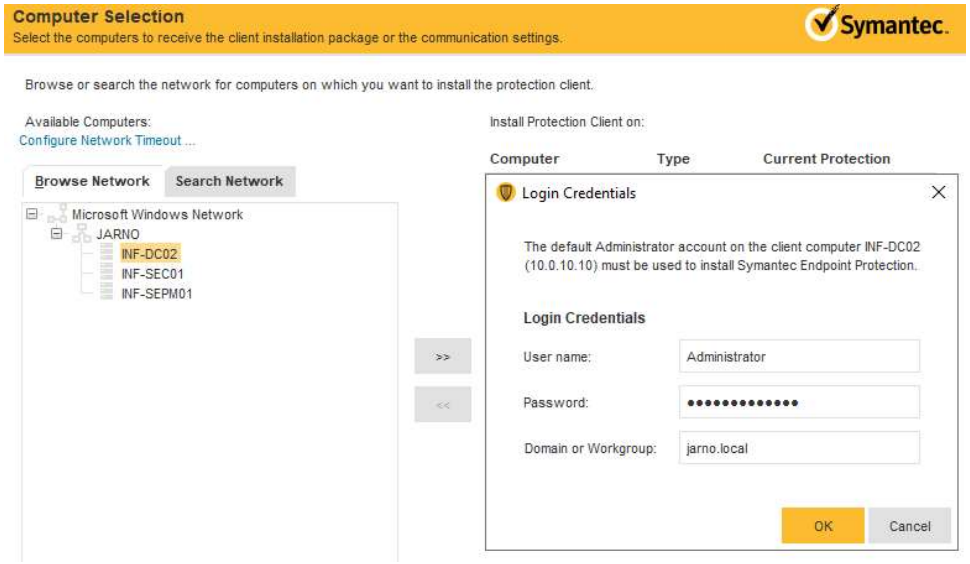
Tämän jälkeen meille avautuu määritys velho, jossa ensimmäiseksi valitsemme New Package Deployment (oletus) **Next.**



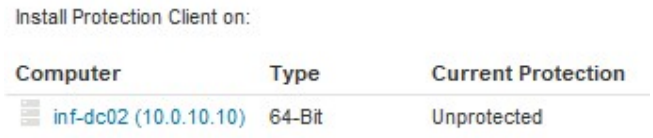
Seuraavaksi voimme määrittää ominaisuuksia, mutta tässä tapauksessa menemme valinnalla Protection for Active Directory sekä Default Standard client installation settings for Windows. **Next.**



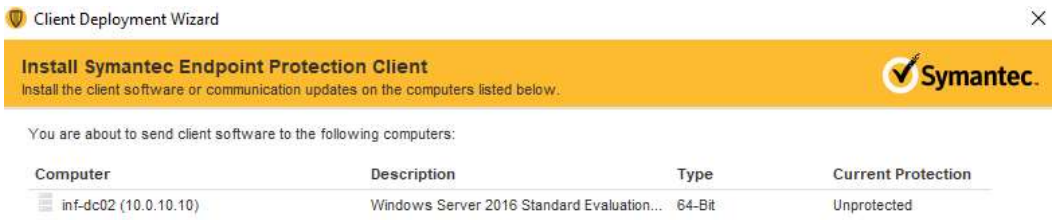
Nyt vielä määritämme tavan jolla asennamme paketin työasemalla, tässä tapauksessa valitsemme etäasennusta varten Remote Push. **Next.**



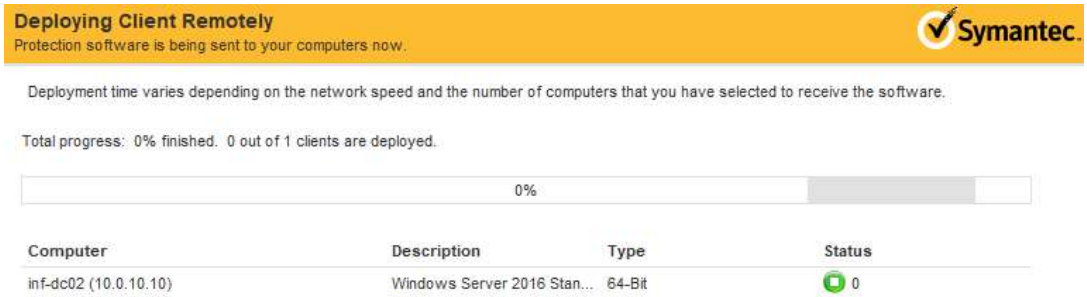
Valitsemme INF-DC02 lisäämme sen asennettavien koneiden joukkoon klikkaamalla kahta hakasulje nappia oikealla. Tämän jälkeen saamme vielä ikkunan jossa kysytään tunnuksia jolla voidaan asennus tehdä tälle palvelimelle. **OK.**



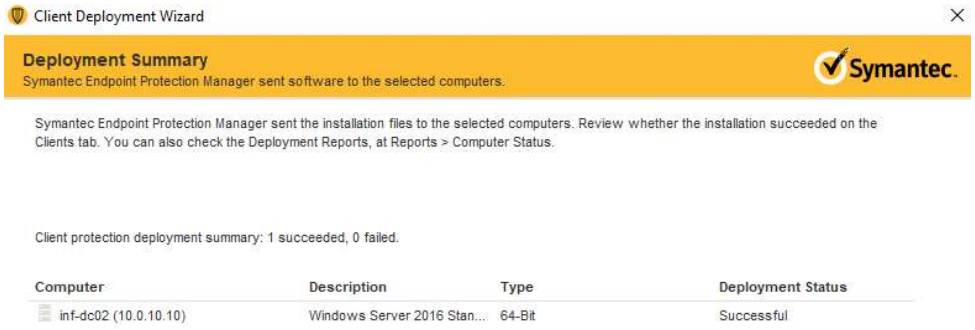
Tämän jälkeen palvelin ilmestyy oikealle ikkunassa ja myös kertoo tiedot palvelimelta (perus) sekä on siellä jo asennettu olemassa olevaa tietoturvasovellusta. **Next.**



Lopuksi saamme vielä vahvistus ikkunan jossa näkyy koneet johon olemme asentamassa SEP-sovellusta. **Send.**



Seuraavaksi tulee ikkuna jossa nähdään, että SEPM palvelin yrittää lähettää ja asentaa SEP sovellusta inf-dc02 palvelimelle.

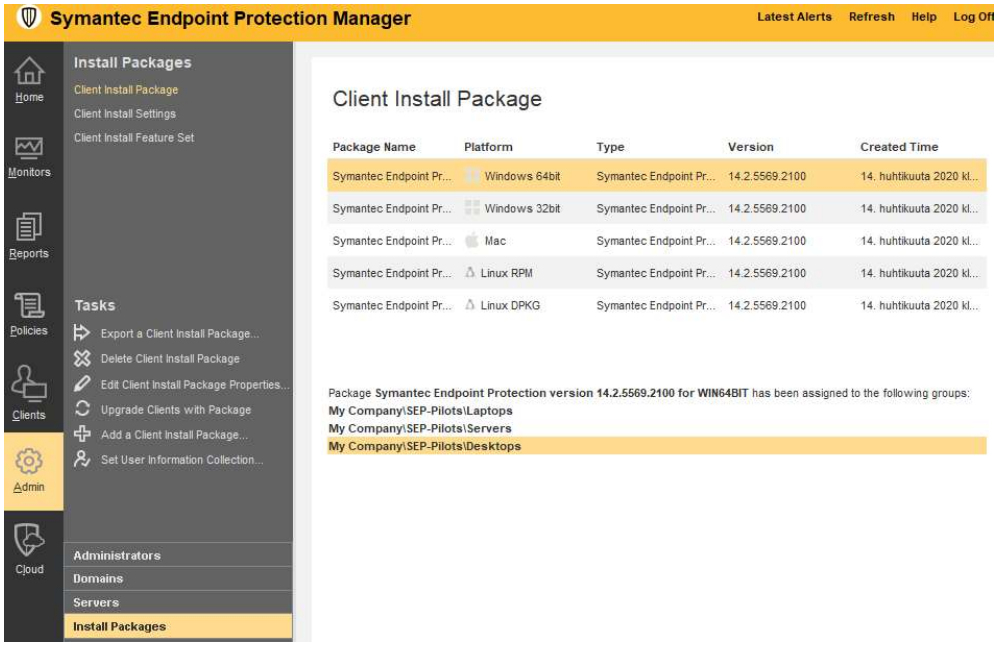


Ja nyt asennuksen jälkeen näemme, että asennus on onnistunut. **Next.**

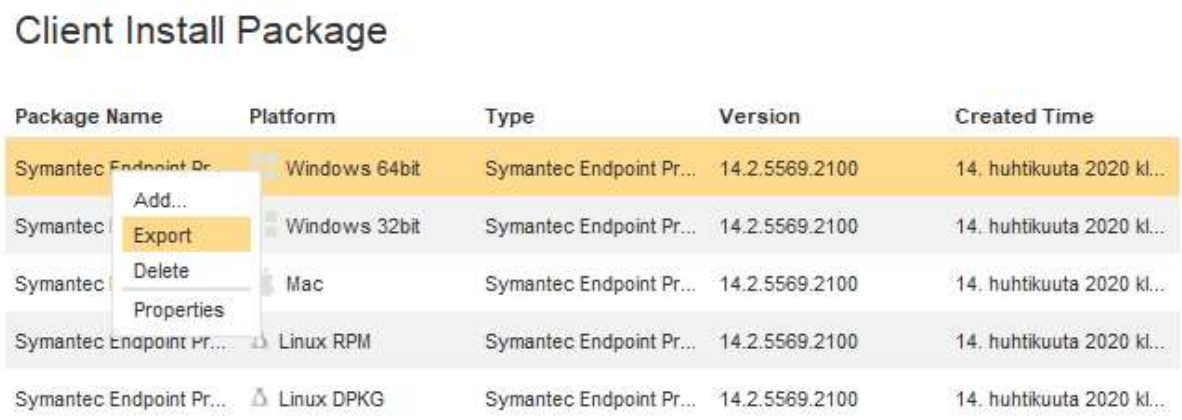
Ja lopuksi tulee vielä vahvistus, että kaikki asennuksen onnistuneet. **Finish.**

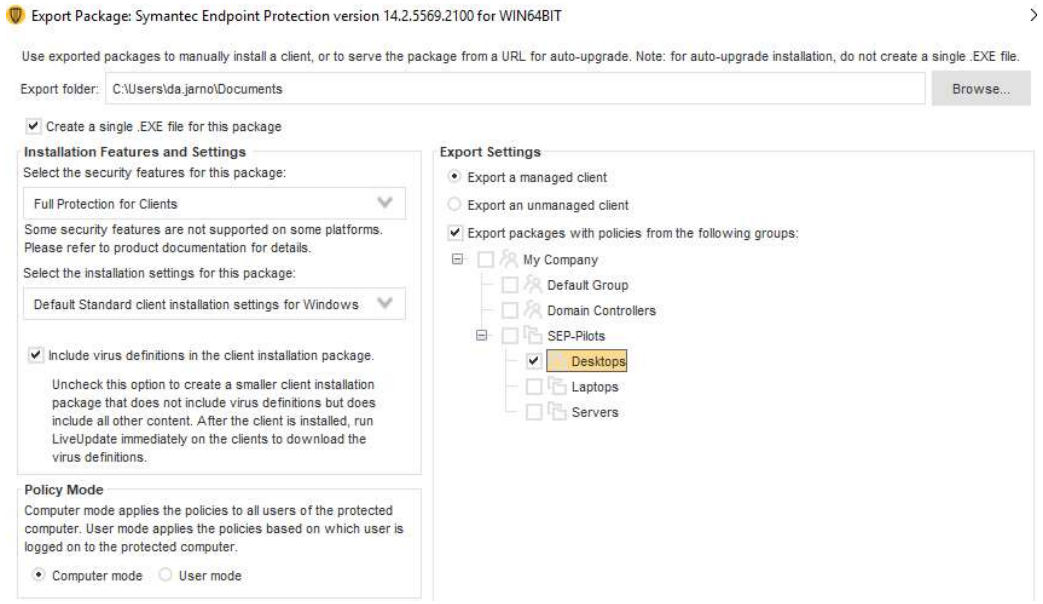
Voimme nyt vielä varmistaa, että asennus on onnistunut, kun tämä palvelin ilmestynyt SEPM hallinnassa Clients näkymään ja palvelin nimen kohdalla on vihreä pallo, joka tarkoittaa, että sillä on myös yhteys meidän SEPM palvelimelle ja voimme sitä hallinnoida.
Tässä tapauksessa inf-dc02 palvelin ilmestyi Default Group kansioon, kun se ei ollut SEP-Pilots Organisaation Yksikön alla, kun se oli Domain Controllers kansiossa Active Directoryssä. Joten jouduin hiiren oikealle ottamaa Move inf-dc02 ja siirtämään sen Domain Controllers (jonka olen myös käsin luonut SEPM hallintaan) kansioon, yhdessä jo toisen Domain Controller koneen kanssa inf-dc01.

Voimme myös luoda ns. manuaalisia asennus paketteja, mikäli emme voi tai halua asentaa Remote Push toimintoa käyttäen.
Tämä tapahtuu menemällä vasemmalla Admin -> Install Packages näkymään

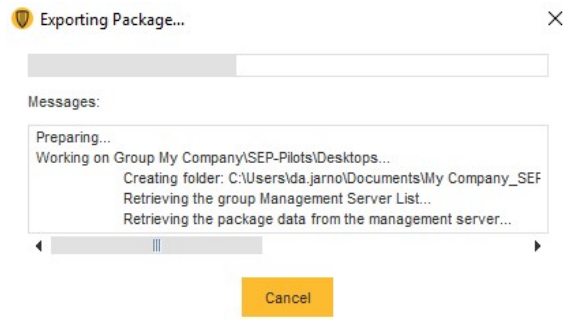


Josta sitten hiiren oikealla valitsemme esimerkiksi ylimmän paketin SEP x64 version ja otamme Export

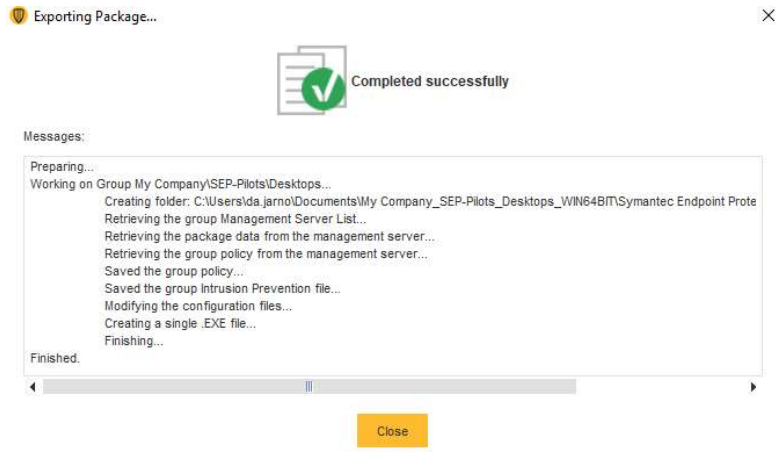




Tässä ensin valitsemme kansion jonne paketin luodaan (Export Folder), sen jälkeen mikä ominaisuus ja asetus asetukset tulee paketilla (Full Protection for Clients), sitten valitsemme mihin kansioon nämä koneet ilmestyvät SEPM hallinnassa, tässä tapauksessa Desktop. Sekä asennus tapana valitsemme Default Standard client installation settings for Windows. Policy Mode: en pidämme oletuksena, eli Computer mode. **Ok.**

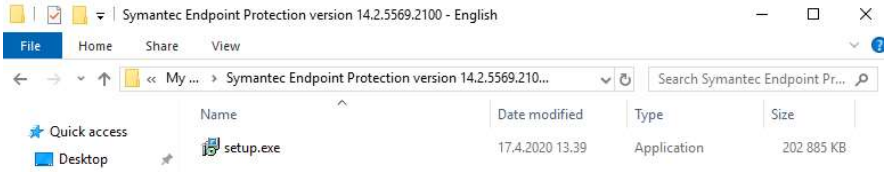


Tämän jälkeen SEPM alkaa luomaan asennuspakettia meidän valitsemilla asetuksilla.



Ja tämän jälkeen vielä tulee vahvistus, että kaikki on mennyt onnistuneesti läpi ja paketti on luotu. **Close.**

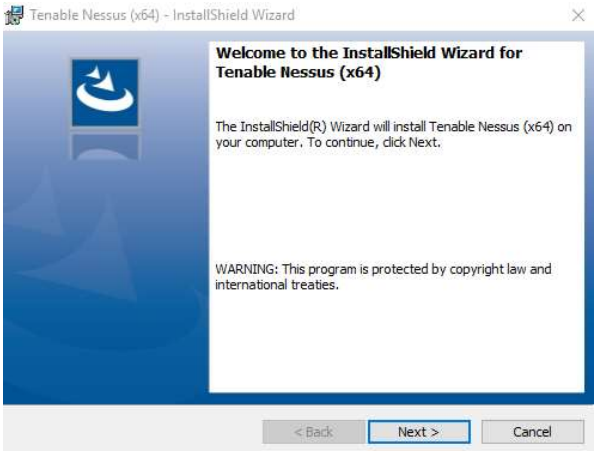
Ja voimme vielä lopuksi tarkistaa SEPM palvelimen kansiosta C:\Users\da.jarno\Documents\My Company_SEP-Pilots_Desktops_WIN64BIT\Symantec Endpoint Protection version 14.2.5569.2100 – English, että sinne on generoitunut asennus paketti.



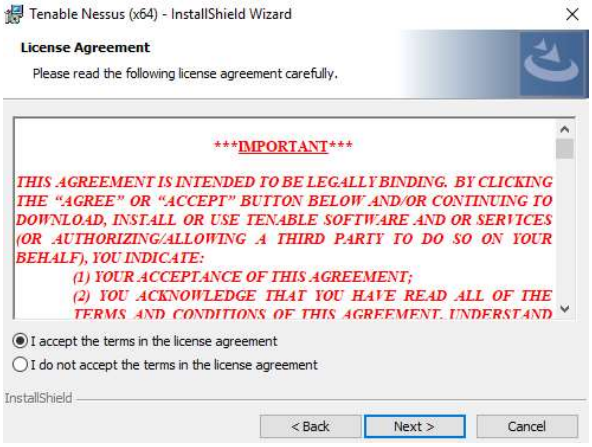
Näin olemme siis asentaneet etänä ja luoneen asennuspaketin SEP asennuksia varten. Seuraavaksi kerron miten voimme auditoida meidän toimialueen tietoturvaa käyttäen Nessus Essentials sovellusta.

Nessus Essentials asennus

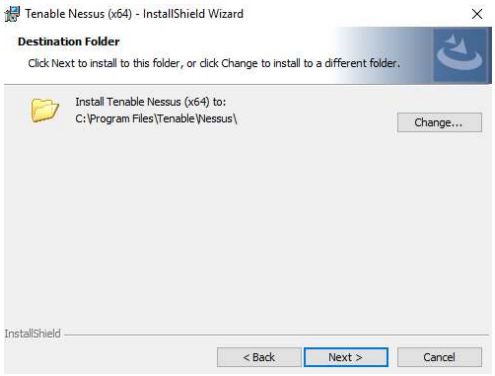
Tulen asentamaan Nessus Essentials tietoturvakartoitus sovelluksen INF-SEC01 Windows Server 2019 palvelimelle. Tällä sovelluksella voimme auditoida toimialueen koneita ja luoda näkemystä olemassa olevasta tietoturvasta ja mahdollista uhista siihen liittyen.
Asennus paketin saa vapaasti ladata https://www.tenable.com/products/nessus/nessus-essentials sivulta, ainoa mitä pitää tehdä on anoa ilmainen aktivointi tunnus asennusta varten.



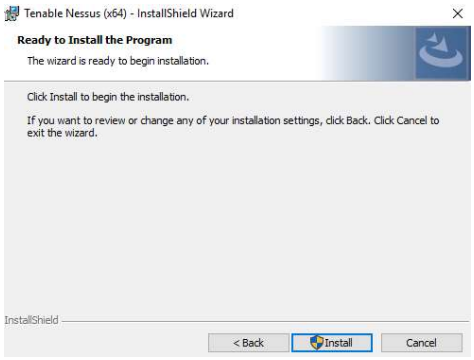
Käynnistämme asennus paketin, jolloin saamme oheisen dialogin. **Next.**



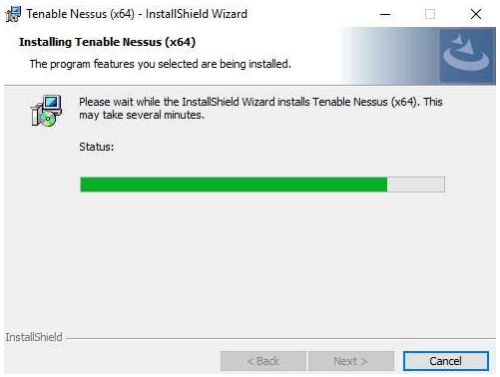
Luomme lisenssi ehdot tarkasti läpi. **Next.**



Valitsemme asennus kansion, menemme oletuksella. **Next.**

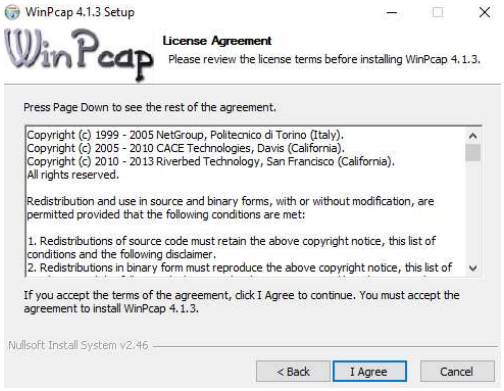


Tämän jälkeen olemme valmis asennukseen. **Install.**

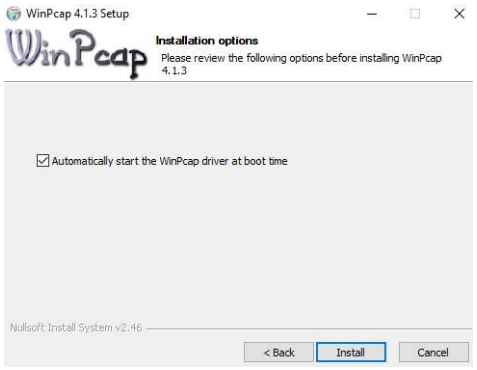


Nyt odotamme, että asennus valmistuu.

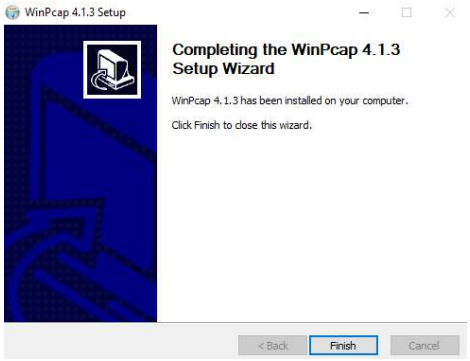
Asennuksen aikana joudumme asentamaan osana Nessusta WinPcap -sovelluksen.
Tämä on osana verkon ja niiden pakettien analysointia varten. **Next.**



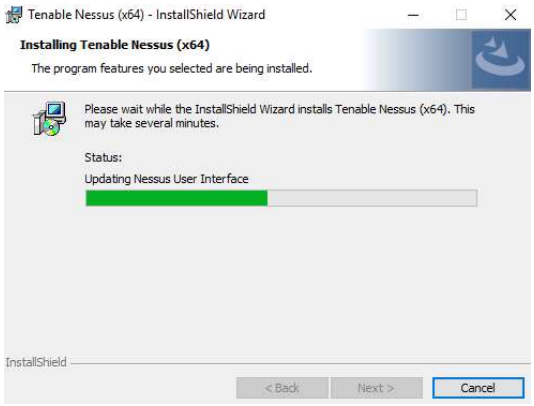
Luomme jälleen tarkasti lisenssiehdot. **I Agree**



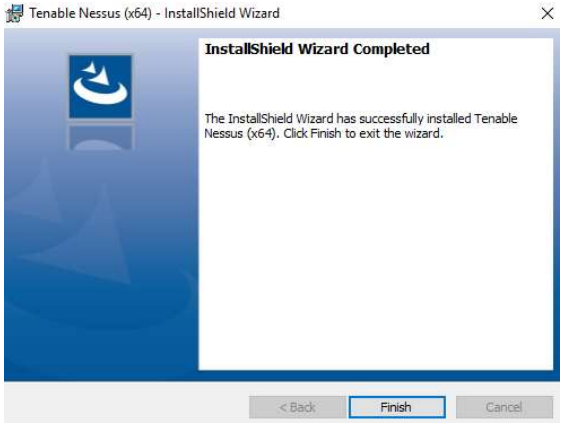
Ja vielä varmistamme, että winPcap käynnistyy palvelimen käynnistyksen aikana. **Install.**



Ja hetken päästä asennus on suoritettu. Nyt voimme jatkaa taas itse Nessus sovelluksen asennusta. **Finish.**

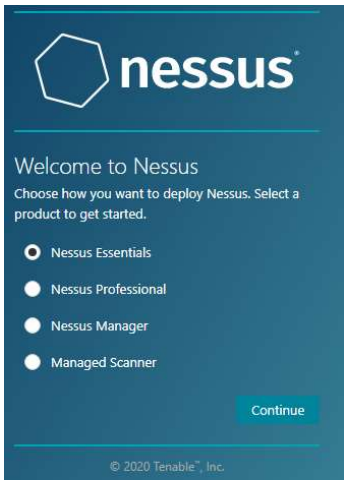


Nyt siis jatkuu taas itse Nessus sovelluksen asennus.

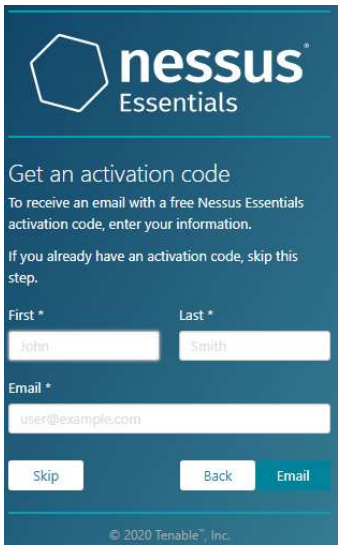


Ja lopuksi asennus on suoritettu onnistuneesti loppuun. **Finish.**

Tämän jälkeen käynnistyy automaattisesti oletus Internet -selain ja avaa osoitteen http://localhost:8834/WelcomeToNessus-Install/welcome jossa voimme jatkaa asennusta.

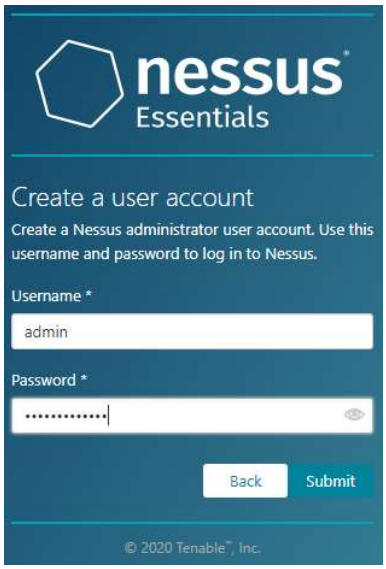


Seuraavaksi valitsemme tuotteen jonka haluamme asentaa. Tässä tapauksessa Nessus Essentials. **Continue**



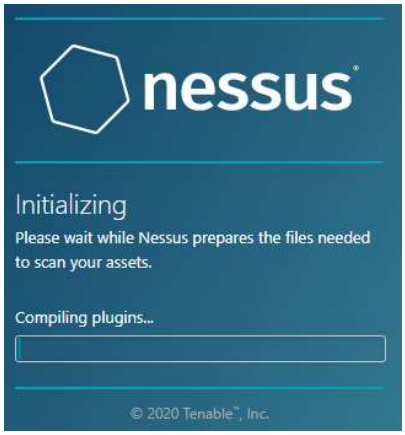
Tässä annamme tiedot jolla luomme ilmaisen aktivointikoodin. Anna tähän sopivat tiedot. **Email**

Kun olemme antaneet tiedot niin syötämme tähän Activation Code kenttään koodin, jonka olemme saaneet sähköpostilla mitä käytimme edellisessä ikkunassa. **Continue.**



Nyt luomme pääkäyttäjän tunnuksen ja salasanan Nessus Essentials hallintaa varten. **Submit.**

Tämän jälkeen asennus käy vielä lataamassa tietoja Nessuksen palvelimelta, kun pluginsit. Tässä menee hetki ja voit taas käydä tässä välissä hakemassa lisää kahvia tai teetä. Myös lounaskin on mahdollista.

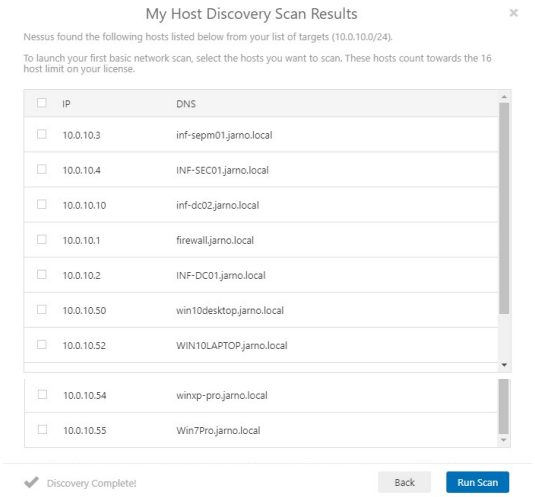


Kun tarvittavat komponentit on saatu ladattua, niin tehdään vielä pluginien rakentaminen. Tässäkin menee se toinen tovinen.
Kun tämä on mennyt läpi, olemme onnistuneesti asentaneet Nessus Essentials sovelluksen.

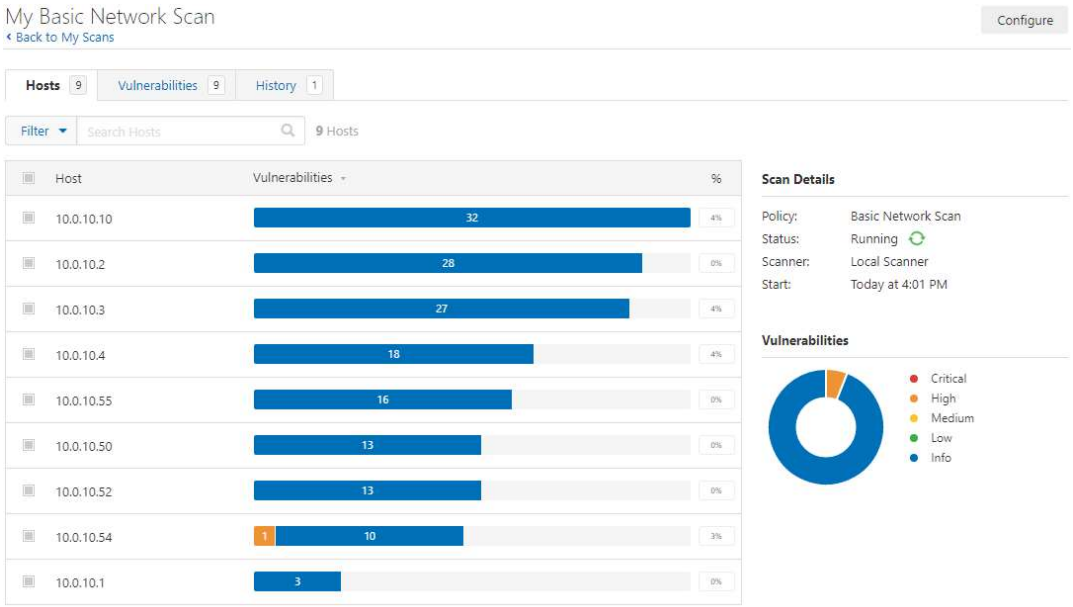
Seuraavaksi aloitamme auditoinnin asennuksen jälkeen.

Nessus Essentials auditointi

Kun nämä komponentit on ladattu ja rakennettu, avautuu tervetuloa ikkuna eteemme. Tähän voimme antaa skannattavien koneiden ip -osoitteet tai vaihtoehtoisesti koko aliverkon mitä halutaan skannata. Tässä tapauksessa annan oman jarno.local toimialueen aliverkon 10.0.10.0/24 **Submit.**

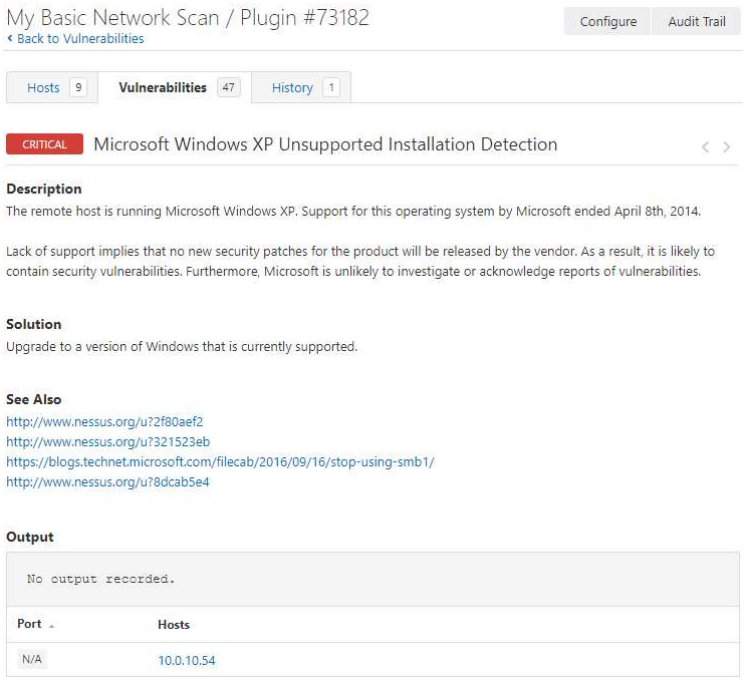


Kun kartoitus on tehty, niin näimme koneet jota tullaan skannaamaan. **Run Scan.**



Tämän jälkeen avautuu Network Scan ikkuna, jossa voi seurata skannauksen edistymistä. Tässä menee tovi, jos toinenkin, riippuen montako konetta käydään läpi.

Ja kun skannaus on ohitse, näemme meidän yleiskuvan meidän tietoturvatilanteesta.



Ja kun avaamme Vulnerabilites välilehden, niin voimme nähdä, että ainakin yksi Critical tason tietoturvavaroitus tulee meidän toimialueen Windows XP koneesta.

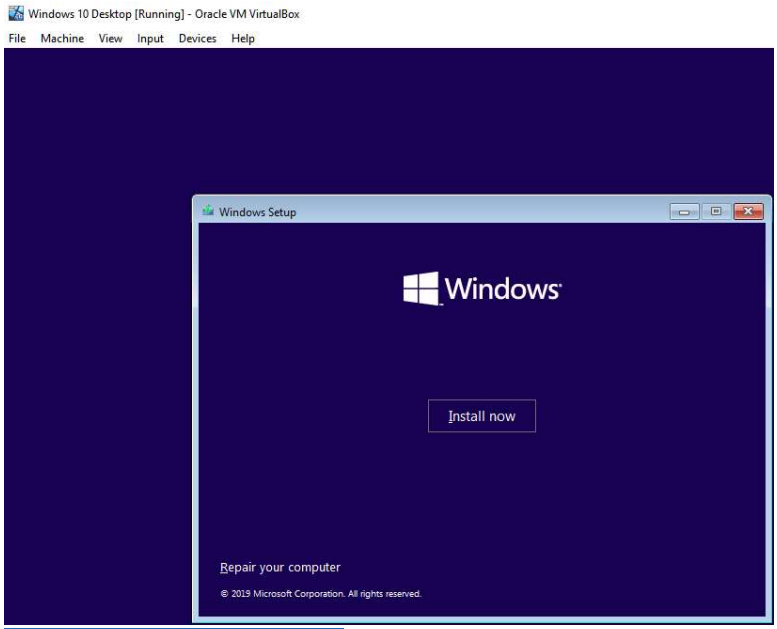
Tietoturva demo: / AD User -> Domain Admin

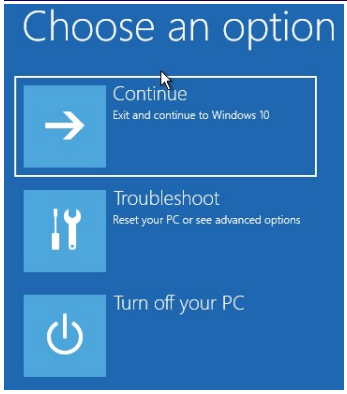
Eli lähtötilanne on se, että meillä Win10Desktop tietokone johon meillä ei ole paikallista Administrator tason tunnusta.
Käytämme kirjautumiseen jarno.nousiainen@jarno.local joka on normaali Domain Users ryhmän jäsen Active Directoryssä.

Eli haluamme aluksi saada tietokoneelle Win10Desktop Administrator tason tunnukset. Tähän voidaan käyttää joko työkalua jolla voimme nollata Win10Desktop Administrator käyttäjän salasanan, tai vaihtoehtoisesti korvata ns. Stickey Keys toiminnon Command Prompt sovelluksella.

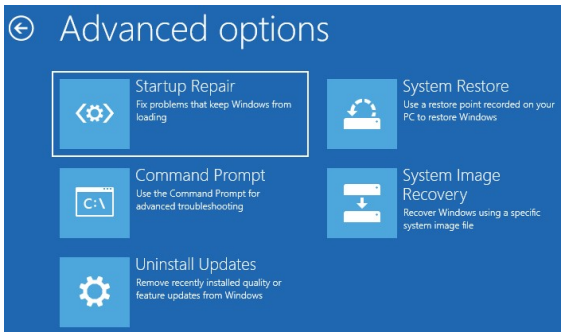
Tämä siksi, kun tämä Stickey Keys voidaan jo käynnistää ennen kirjautumista koneelle ja tämä Stickey Keys suoritetaan System -tason tunnuksella. Tällöin voimme esimerkiksi komennolla ”net user Administrator password!!” resetoida Administrator käyttäjän salasanan ja voimme sitten kirjautua paikallisesti Administrator tunnuksella.

Eli aloitamme käynnistämällä Win10Desktop Windows 10 käynnistys .ISO imagella ja menemällä sieltä Repair your computer toimintoa pitkin tiedostojärjestelmään kiinni.

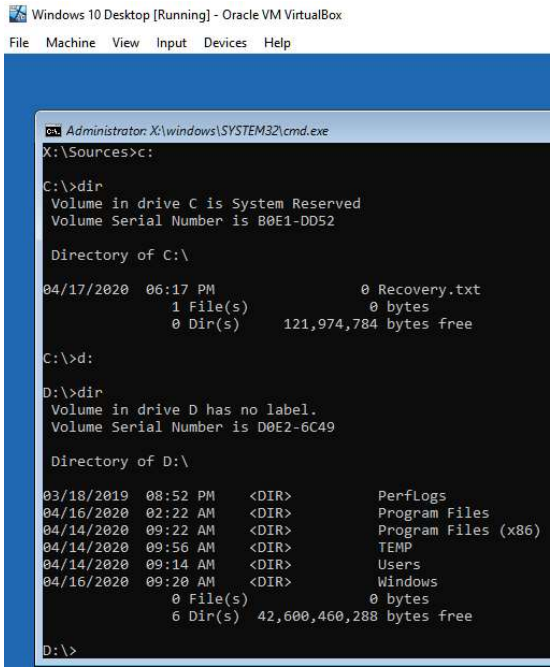




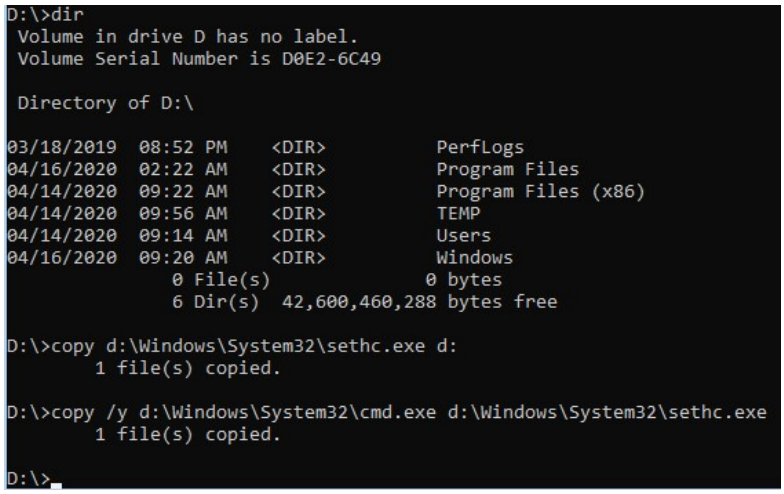
Josta valitsemme Troubleshoot



Seuraavaksi valitsemme Command Prompt, jotta pääsemme tiedostojärjestelmään käsiksi.

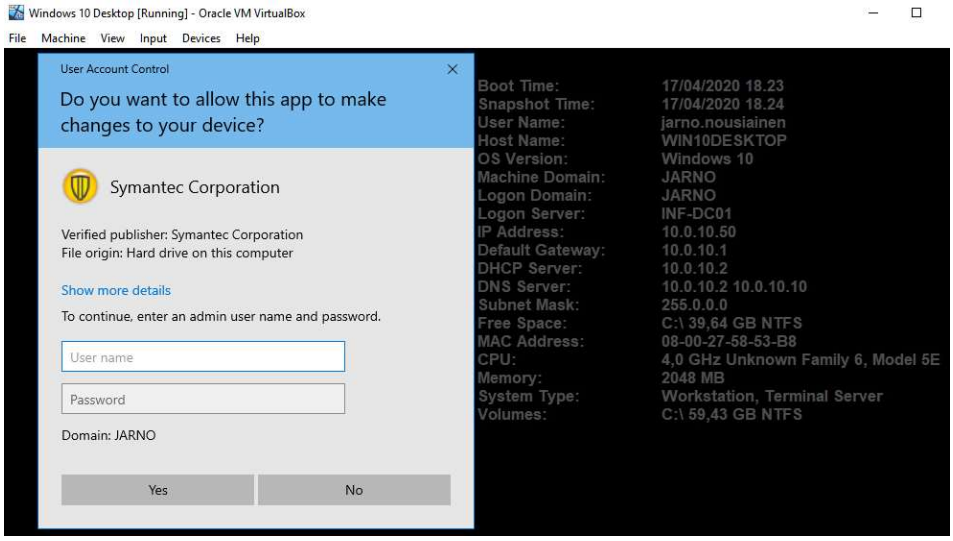


Ja kuten tästä huomaamme, levykirjaimen D:\ alta löytyy Windows asennuksemme



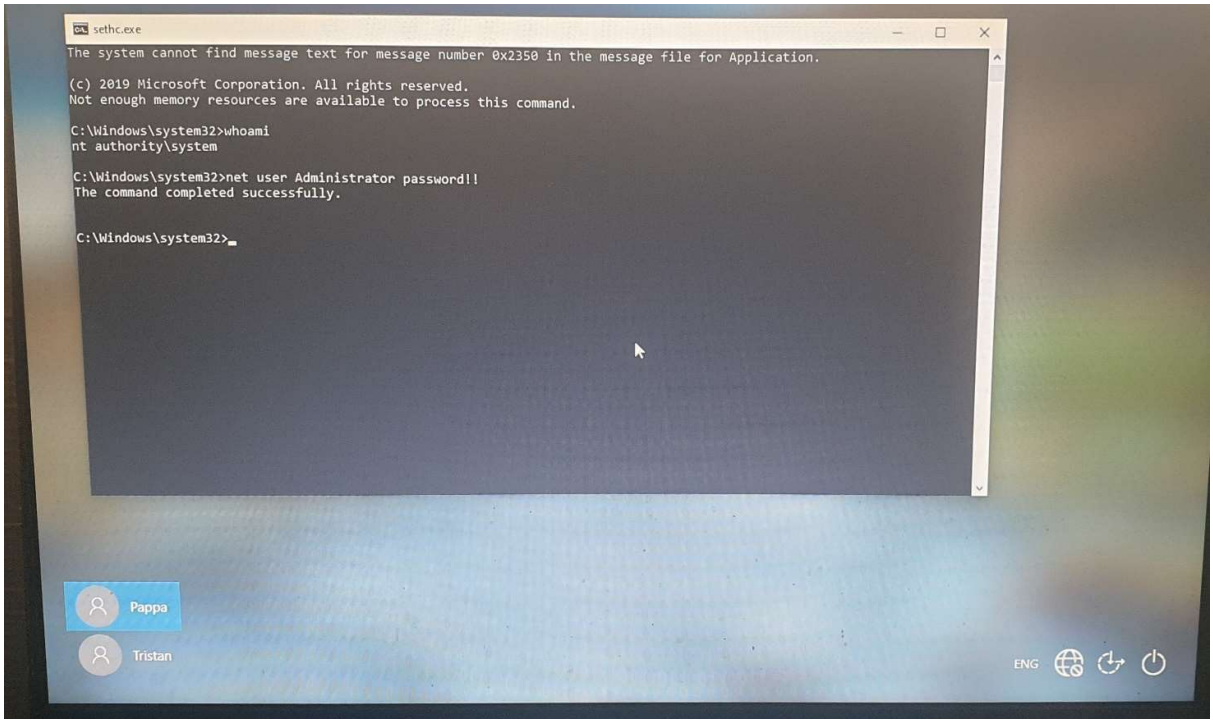
Eli ensimmäiseksi kopioimme sethc.exe d:\ juuren talteen, jonka jälkeen kopioimme cmd.exe sethc.exe nimiseksi.

Tämän jälkeen voimme käynnistää tietokoneen uudelleen normaalisti takaisin Windows 10 tilaan.



Eli voin vielä havainnollistaa, tunnus joka minulla on käytössä Win10Desktop.jarno.local toimialue koneelle on jarno.nousiainen ei ole oikeutta suorittaa Järjestelmänvalvojantason tehtäviä, kun käynnistää Symantec Endpoint Protection ylläpitotasolla.
Olen myös bginfo nimisellä sovelluksella luonut taustakuvan joka käynnistyksellä mikä kertoo koneen tiedot, eli tuo valkoinen teksti mustalla taustalla oikealla puolella.

Tässä kohtaa tuli vastaan Virtualbox sovelluksen rajallisuus syöttää Shift komentoa, joten joudun tätä jatkamaan aivan fyysisessä tietokoneessa

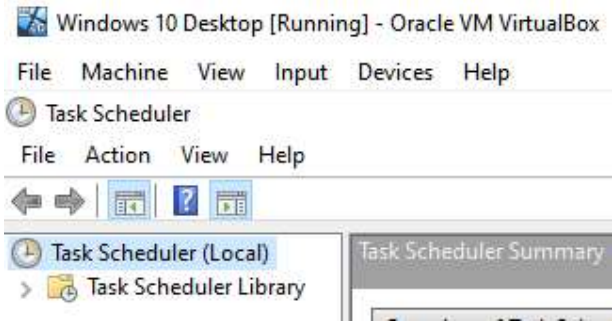


Ja nyt kun meillä on halussa Järjestelmänvalvojan tason tunnus Win10Desktop koneella, voimme seuraavaksi korottaa itsemme Domain Adminstrator ryhmän jäseneksi.
Tämä vaatii jo hieman suunnittelua ja sitä että jarno.local toimialueen ylläpitäjät käyttävät Administrator tunnusta myös tietokoneiden hallintaa, toki voi myös olla mahdollista, että heillä on omat Administrator tason tunnukset, kuten esimerkiksi da.jarno jarno.local toimialueella.

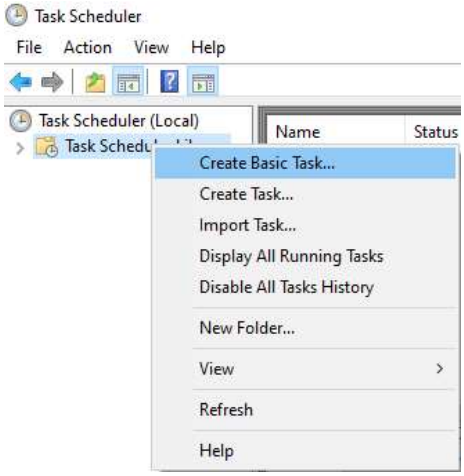
Ja jos vielä tämä ylläpitäjä käyttää työasemienkin ylläpitoon tätä da.jarno tunnusta niin silloin voimme suhteellisen helposti korottaa itsemme Domain Administrator ryhmän jäseneksi. Tämä tosiaan vaatii myös hieman sosiaalisen puolen hakkerointia 😊

Eli aluksi luomme Scheduled Taskin omalle Win10Desktop koneelle, joka suorittaa tietyn komennon, kun da.jarno kirjautuu esimerkiksi Remote Desktop yhteydellä antamaan etäapua keksityssä vikatilanteessa.

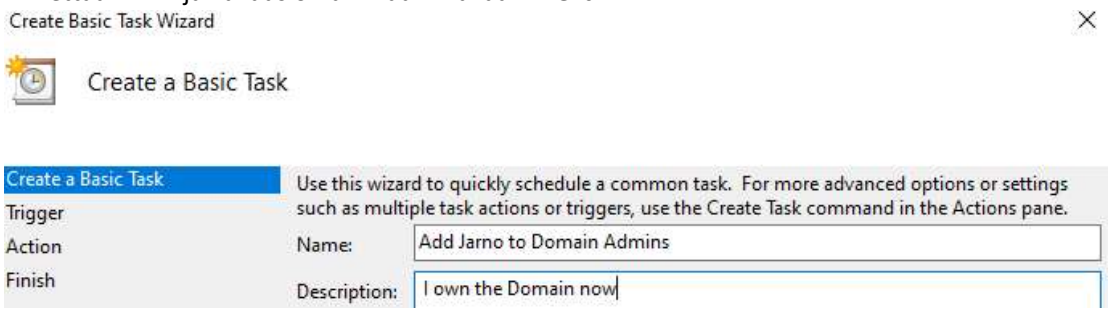
Aluksi avaamme Task Schedulerin polusta Windows Administrative Tools



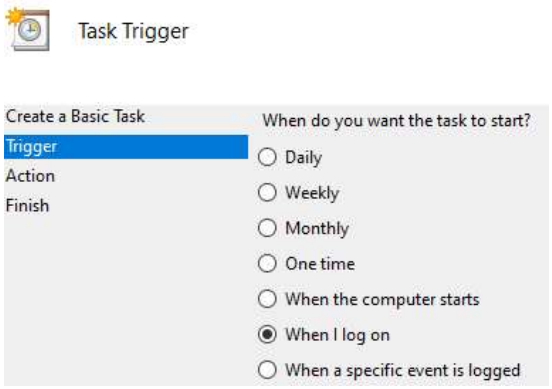
Valitsemme hiiren oikealla Task Scheduler Library kohdalla ja otamme Create Basic Task



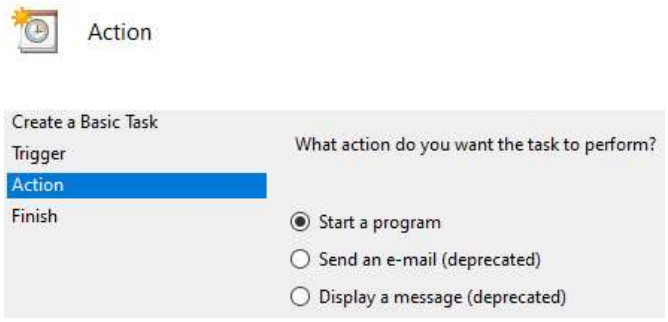
Annettaan nimi ja kuvaus oman maun mukaan. **Next.**



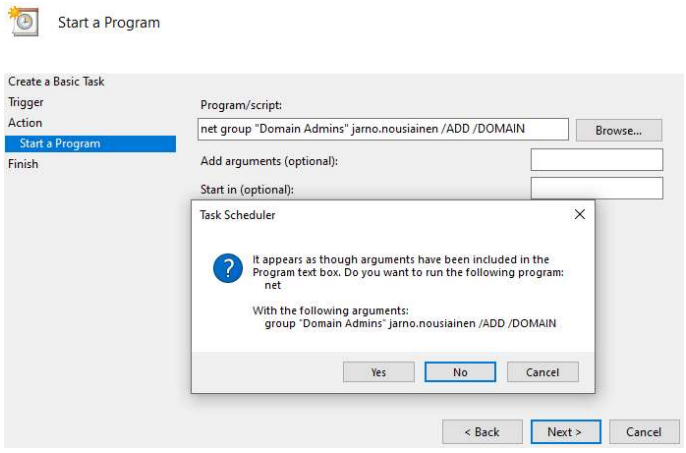
Valitaan When I log on, milloin tämä meidän taski tullaan ajamaan. **Next.**



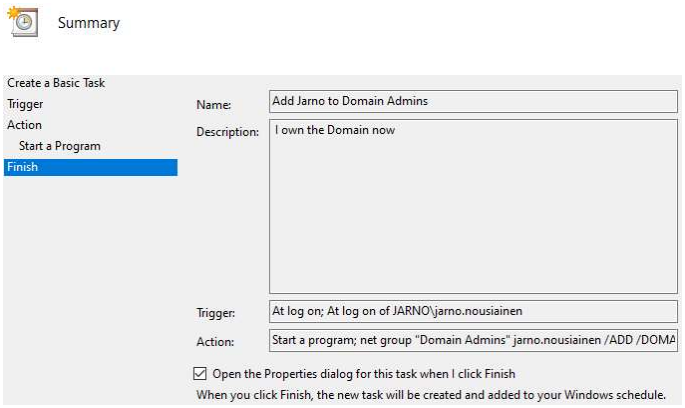
Toimintona valitaan, että suoritetaan sovellus tai komento. **Next.**



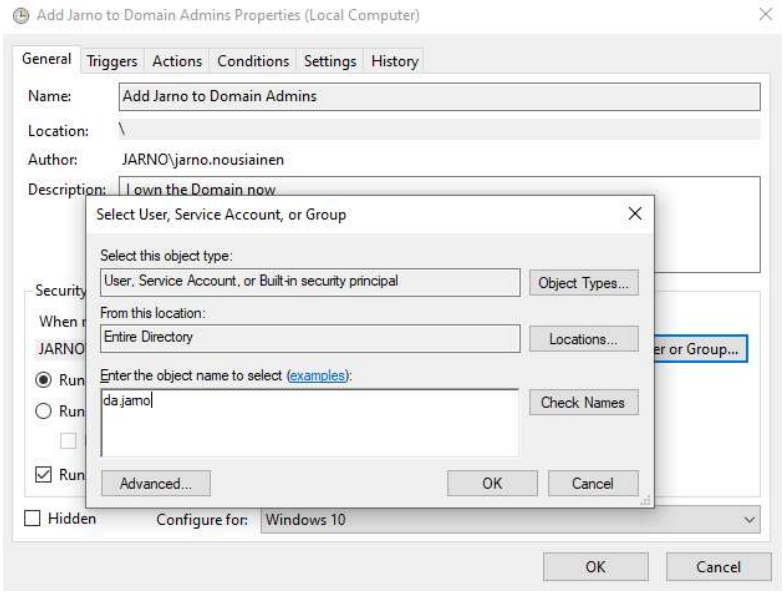
Komennoksi annetaan ”net group "Domain Admins" jarno.nousiainen /ADD /DOMAIN” ilman siis hapsuja. Jonka jälkeen Task Scheduler ehdottaa hieman muutosta, valitaan **Yes** ja sen jälkeen **Next**



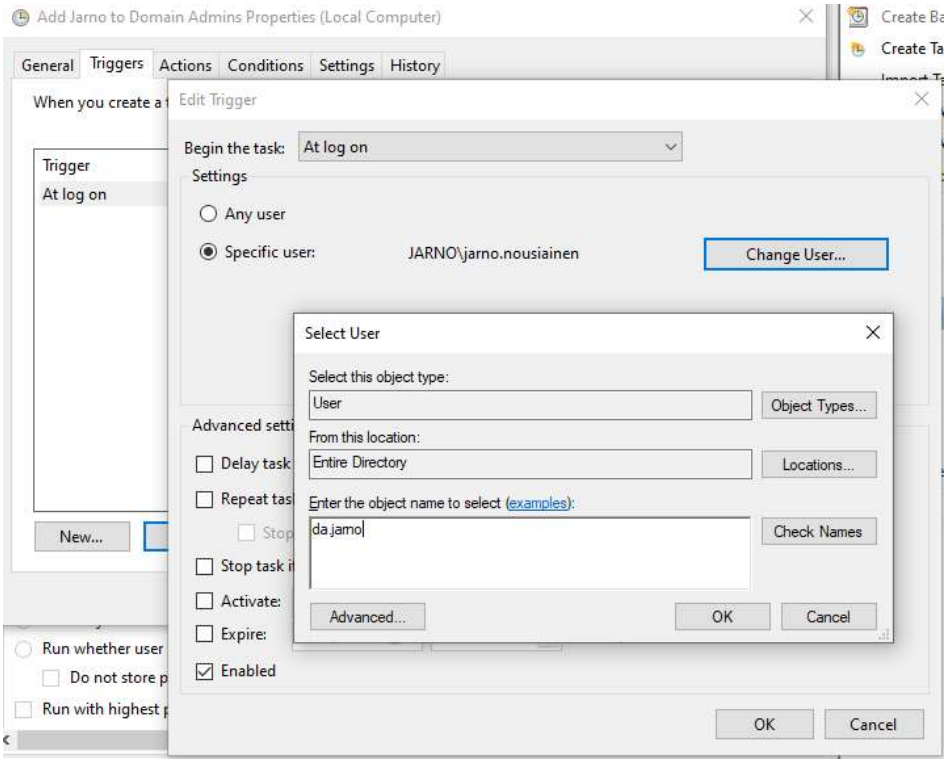
Lopuksi saamme vielä yhteenvedon tehtävästä ajastetusta tehtävästä. Tässä kohtaa ruksaamme ”Open the Properties dialog fot this task when I click Finish”. **Finish.**



Lisäämme ruksin Run with highest priviledges sekä valitsemme Configure for “Windows 10”. Tämän jälkeen avaamme Change User and Group valitsemme Locations kohdasta Entire Directory ja kirjoitamme kenttään da.jarno ja valitsemme OK



Seuraavaksi menemme Triggers välilehdelle ja valitsemme Edit.
Täällä muutamme valitsemme taas Change User sekä Locations kohdaksi Entire Directory ja käyttäjäksi da.jarno. Lopuksi OK ja tämän jälkeen myös OK Edit Triggers välilehdeltä.



Tämän jälkeen meillä on valmiina komento joka suoritetaan, kun da.jarno kirjautuu koneelle, millä lisää meidän Active Directory Domain Admins ryhmään.

Seuraavaksi meidän pitää saada kirjautumaan da.jarno koneelle, esimerkiksi Remote Desktop yhteyden avulla. Voidaan vaikka pyytää apua jonkun sovelluksen kanssa tai mahdollisesti jokin vika muu keksitty vika tilanne.

Tein tästä videon jolta selviää parhaiten tämä, miten saadaan tämän jälkeen Domain Admins tason oikeudet haltuun.
Olen tämän videon ladannut OneDriveen kansioon
https://iukky-my.sharepoint.com/:v:/g/personal/jarno_nousiainen_student_careeria_fi/EUD7RCYDwKdGm0u2qm1lQaUBZc8yOH566dLpzU0ZAO64ZQ?e=xXbGxF

Eli nyt olemme päässeet normaalisti käyttäjästä muutamalla työvaiheella Domain Admins tason käyttäjäksi.

Se miten tätä voidaan estää on ensimmäiseksi estää millä medialla oman koneensa käynnistys ja/tai määrittää Bitlocker levyn kryptaus pakolliseksi kaikille työasemille, jolloin emme voi tehdä mitään muutoksia systeemi levylle ilman että meillä on tiedossa Bitlocker avain.
Tämä myös edellyttää sitä, ettemme anna käyttäjille paikallisen pääkäyttäjän tason oikeuksia, jolloin he ovat jo ohittaneet tuon ensimmäisen vaiheen jolla elevoidaan itsemme koneen pääkäyttäjäksi.
Toinen mikä on ehdottoman tärkeää, että emme missään nimessä ylläpidä työasemia tai kirjaudu niille Domain Admins tason tunnuksella.

Eli mielellään luomme esim. erilliset käyttäjät joilla ylläpidämme työasemia joille on määritelty koneille ylläpito oikeudet, mutta ei toimialueen ylläpito oikeuksia.
Voimme esimerkiksi luoda käyttäjä wa.jarno jolla ylläpidämme vain työasemia (wa -> Workstation Admin)
Toiseksi voisimme luoda sa.jarno nimisen käyttäjän jolla ylläpidämme vain palvelimia (sa -> Server Admin)
ja lopuksi luoda erillisen da.jarno tunnuksen, jolla vain ja ainoastaan kirjaudumme ja ylläpidämme toimialue palvelimia, Domain Controller koneita (da-> Domain Admin)