Bachelor i informatikk med spesialisering i drift av datasystemer

Finn Morten Wiggen

Bruk av Microsoft System Center 2016 med Intune 2016

Driftsrapport

Innhold

1. Innledning

Som det fremkommer I forstudierapporten skal denne oppgaven omhandle Microsoft System Center og Microsoft Intune. Derfor er det naturlig å kort forklare hva disse to programmene er.

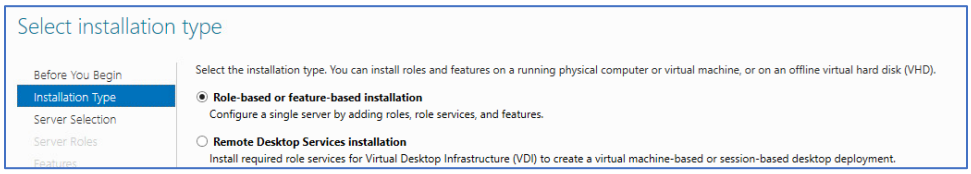
System Center er en systemadministrasjonsprogramvare utviklet av Microsoft for å administrere store grupper av datamaskiner. NerVika AS vil bruke System Center til fjernkontroll, oppdatering av programvare, utrulling av programvare og utrulling av operativsystem.

Microsoft Intune er en skytjeneste som tilbyr mobilenhetsadministrasjon, administrasjon av mobilapplikasjoner og PC-styringsfunksjoner. Intunes funksjoner vil hjelpe NerVika AS med å gi sine ansatte tilgang til bedriftsdata, ressurser og applikasjoner, samtidig som det bidrar til å beskytte bedriftens informasjon.

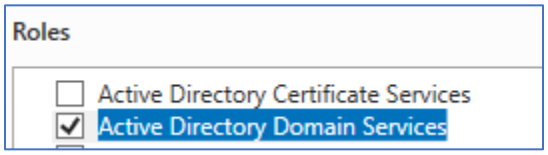
2. Installasjon av Active Directory

For å installere Active Directory må vi åpne Server Manager. Der velger vi Manage --> Add Roles and Features.

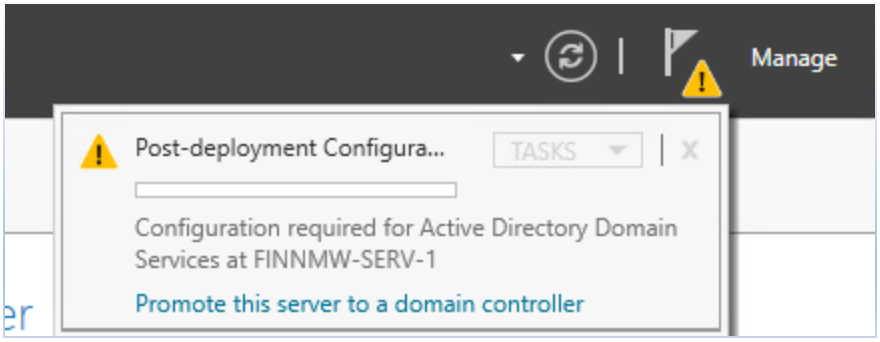
Her velger vi en rollebasert installasjon.



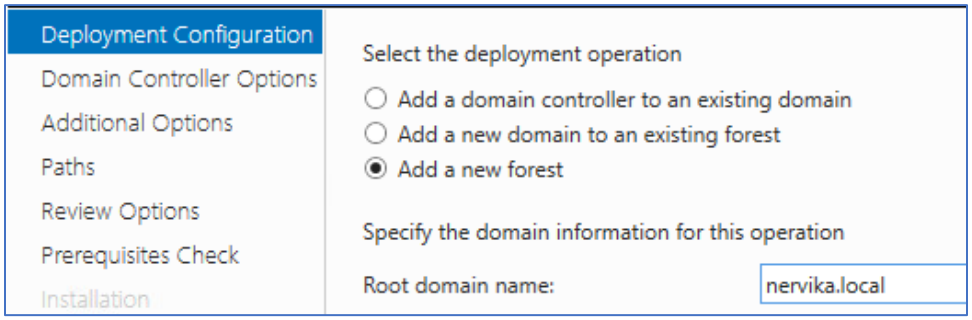
På Server Roles velger vi Active Directory Domain Services



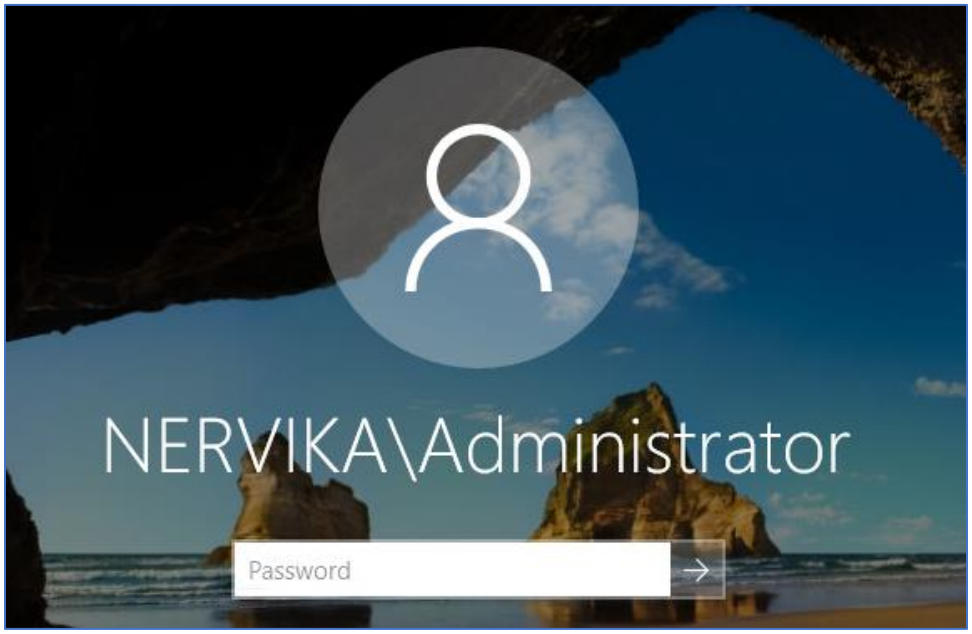
Når AD er ferdig installert må vi gjøre denne serveren til domenekontroller for domenet til NerVika AS



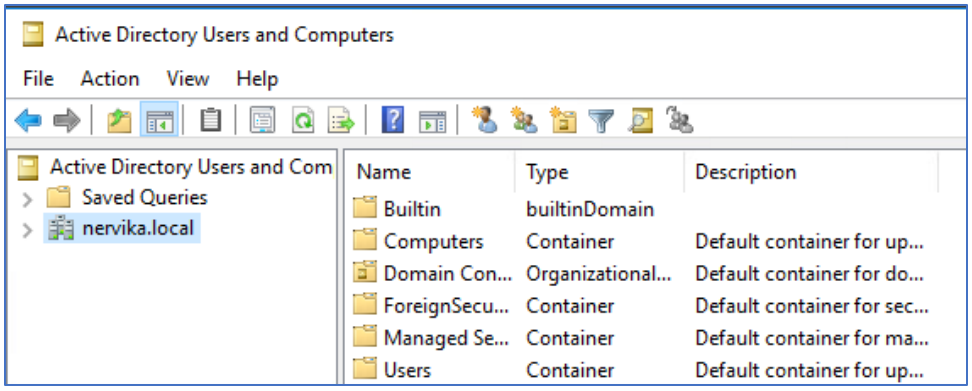
Her oppretter vi en skog for domenet



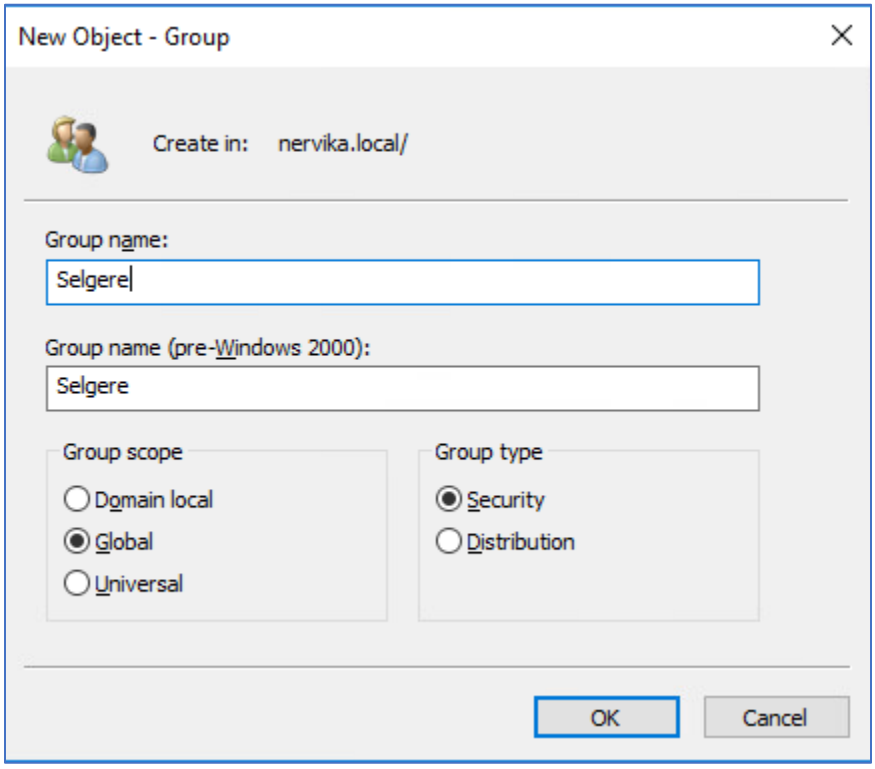
Når installasjonen er ferdig vil serveren automatisk restarte. Når serveren kommer opp igjen ser vi at domenet er opprettet. Vi kan da logge inn som NERVIKA/Administrator



Når domenet er opprettet er vi klare for å opprette de forskjellige avdelingene I NerVika AS og legge til de ansatte. Dette gjør vi med Active Directory Users and Computers. Vi åpner dette ved å velge Tools I Server Manager.

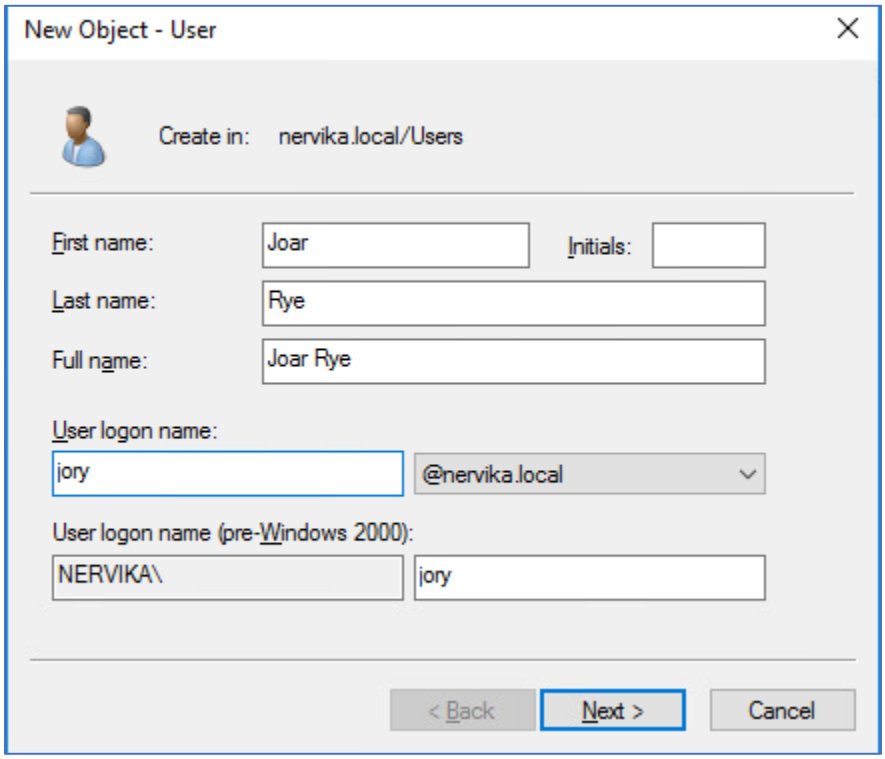


For å opprette grupper til de forskjellige avdelingene høyreklikker vi på nervika.local og velger New-->Group.

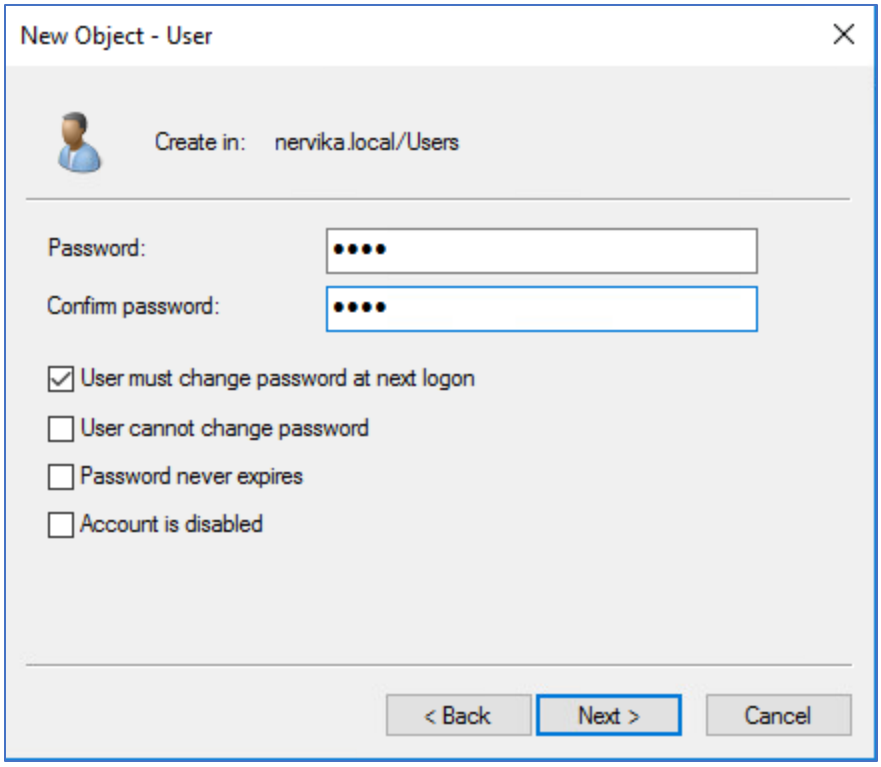


Her gjentar vi prosessen med alle de seks avdelingene; administrasjon, ledelse, IT-avdeling, produksjon, selgere og kundeservice.

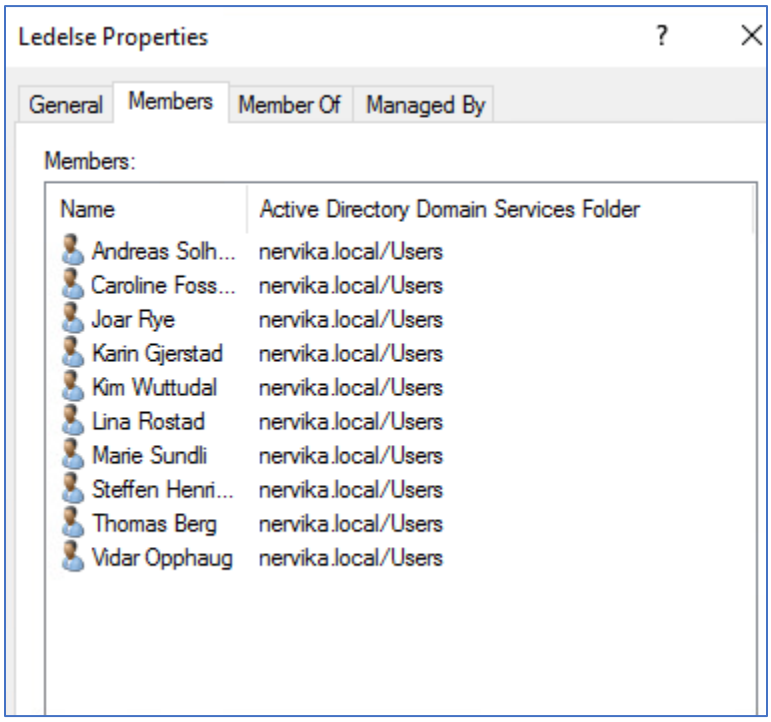
Når alle avdelingene er opprettet I AD må vi opprette brukerne. For å opprette en bruker høyreklikker vi på Users under nervika.local og velger New-->User.



Velger her at User logon name skal være de to første bokstavene I fornavnet og de to første I etternavnet. Neste punkt er å velge passord til brukeren. Gir alle brukerne passordet Hei!123 med et krav om at de må endre passord ved neste innlogging.



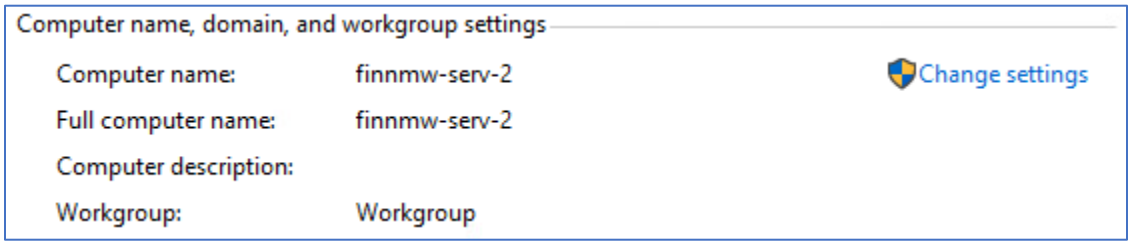
Gjentar denne prosessen med alle brukerne. Kunne alternativt ha brukt et powershell script for å legge til brukere, men velger å gjøre dette manuelt. Opprettet først alle brukerne I avdelingen Ledelse. Når alle brukerne er opprettet legges de til gruppen sin ved å dobbeltklikke på Ledelse. Her velger vi "Members" og "Add".



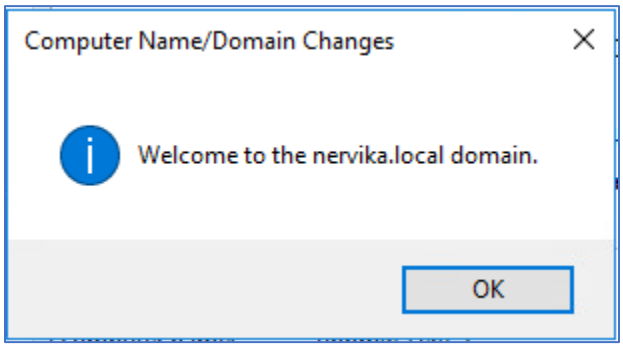
Her vises gruppen Ledelse med sine 10 ansatte. Gjentar denne prosessen med de ansatte I alle avdelingene.

3. Installasjon av Microsoft System Center

Før vi begynner med installasjon må serveren som skal brukes til System Center meldes inn i domenet vi opprettet. Dette gjøres ved å høyreklikke på This PC→Properties. Her ser vi at finnmw-serv-2 ikke er medlem av noe domene.



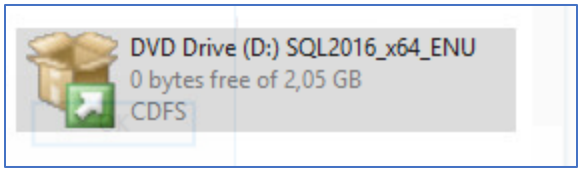
For å melde serveren inn i domenet velger vi Change settings → Change → Skriver inn nervika.local→Logger inn med domeneadministrator. Når serveren er meldt inn i domenet får vi en velkomstmelding.



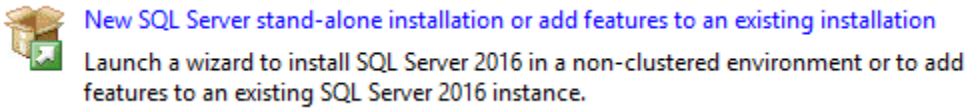
3.1 Installasjon av SQL 2016 Server

Siden System Center benytter seg av SQL-server for å lagre data, er det nødvendig å installere SQL-server før vi kommer i gang med installasjon av System Center.

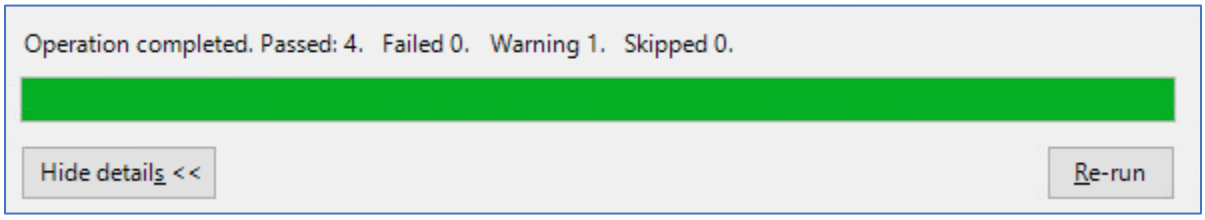
For å installere SQL Server 2016 må vi mounte installasjonsfilen til serveren via vSphere. Dette gjøres ved å høyreklikke på serveren→Edit Settings→Add New Device→CD/DVD drive→Datastore ISO File→Finner SQL Server 2016 Enterprise. Når dette er gjort skal SQL Server 2016 være mountet til serveren som en DVD Drive.



For å starte installasjonen dobbeltklikker vi på denne DVD-driven. Når installasjonen startes får vi en rekke valg. Først hopper vi over planning før vi under Installation velger en stand-alone installation.

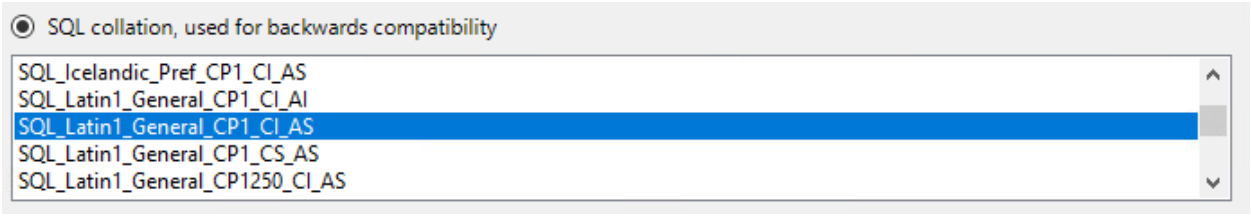


Før installasjonen startes må produktnøkkel skrives inn og lisensen aksepteres. I neste steg huker vi av for å installere oppdateringer. Etter det starter installasjonen.

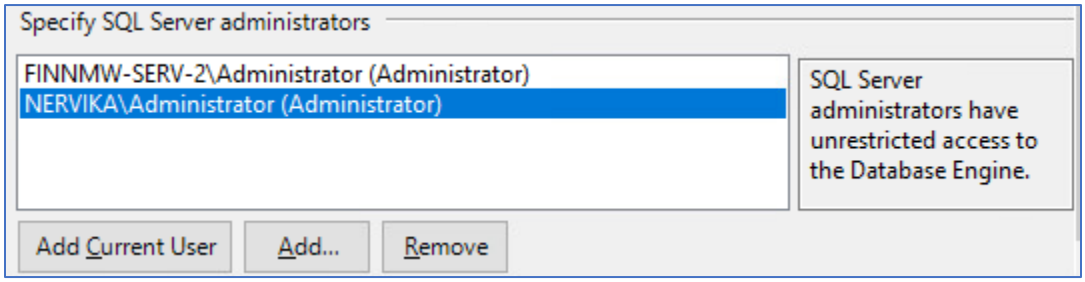


Neste steg i installasjonen er Feature Selection. Her huker vi av Database Engine Services. Under Instance Configuration velger vi Default instance.

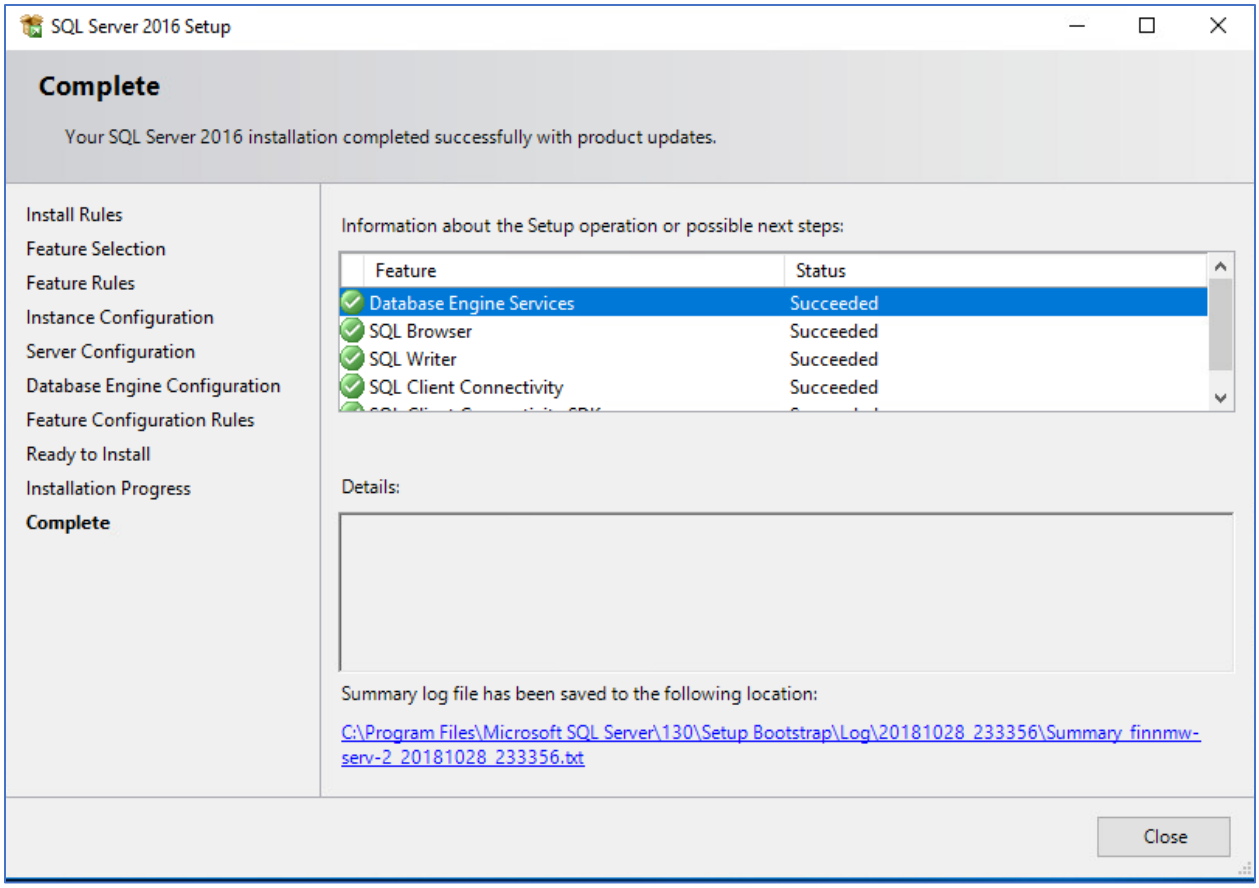
Det er også viktig og huske å endre collation. Velg SQL_Latin1_General_CP1_CI_AS



Under valget av authentification mode velger Windows authentification mode. Under specify SQL Server administrators legger vi til domeneadministratoren.

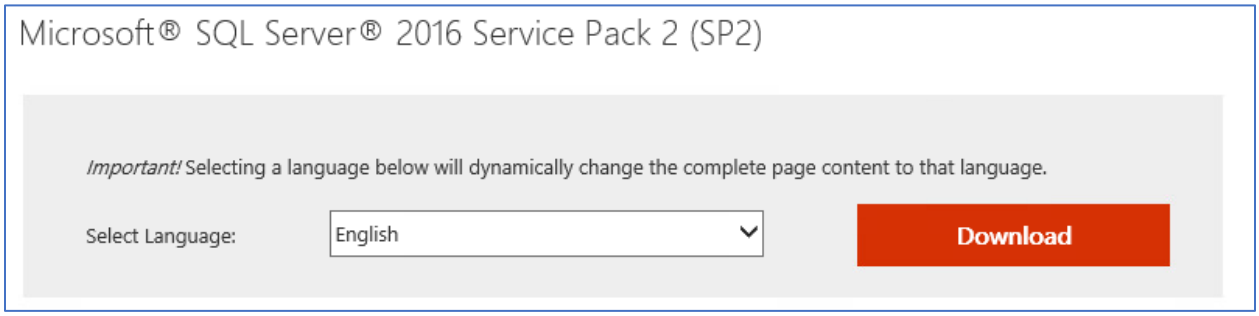


Installasjonen er da klar for å fullføres. Når installasjonen er ferdig får vi opp en oversikt over hva vi har installert og om disse har blitt installert uten problemer.

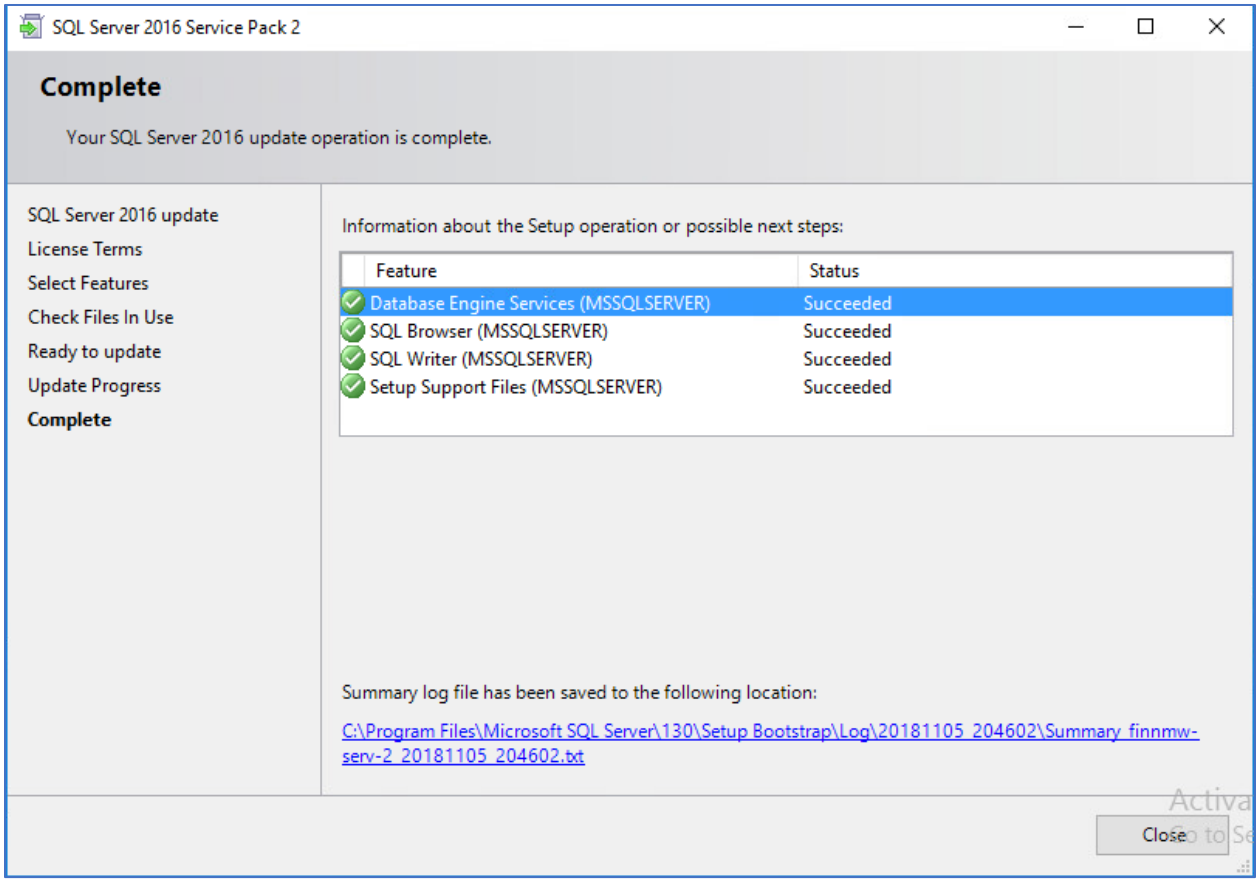


3.2 Oppdatering av SQL 2016 server

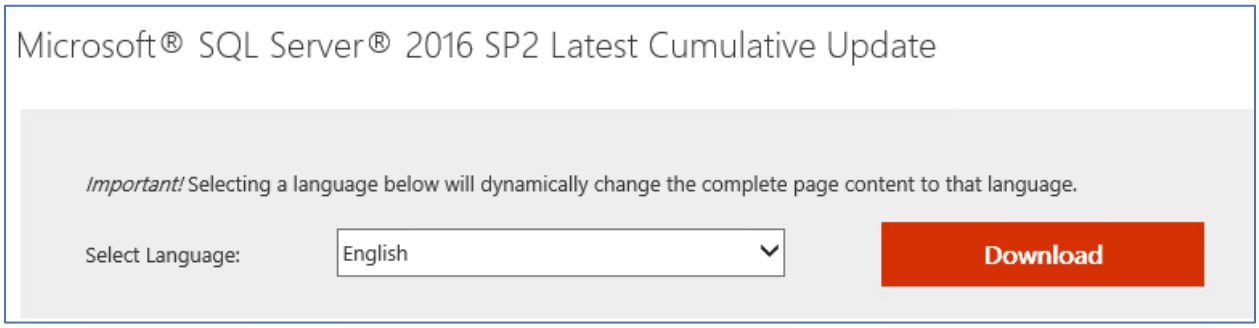
For å oppdatere SQL må vi laste ned Microsoft SQL Server 2016 Service Pack 2. SP 2 finner vi lett ved å søke på microsoft.com. Når vi har funnet rett fil er det bare å trykke download.



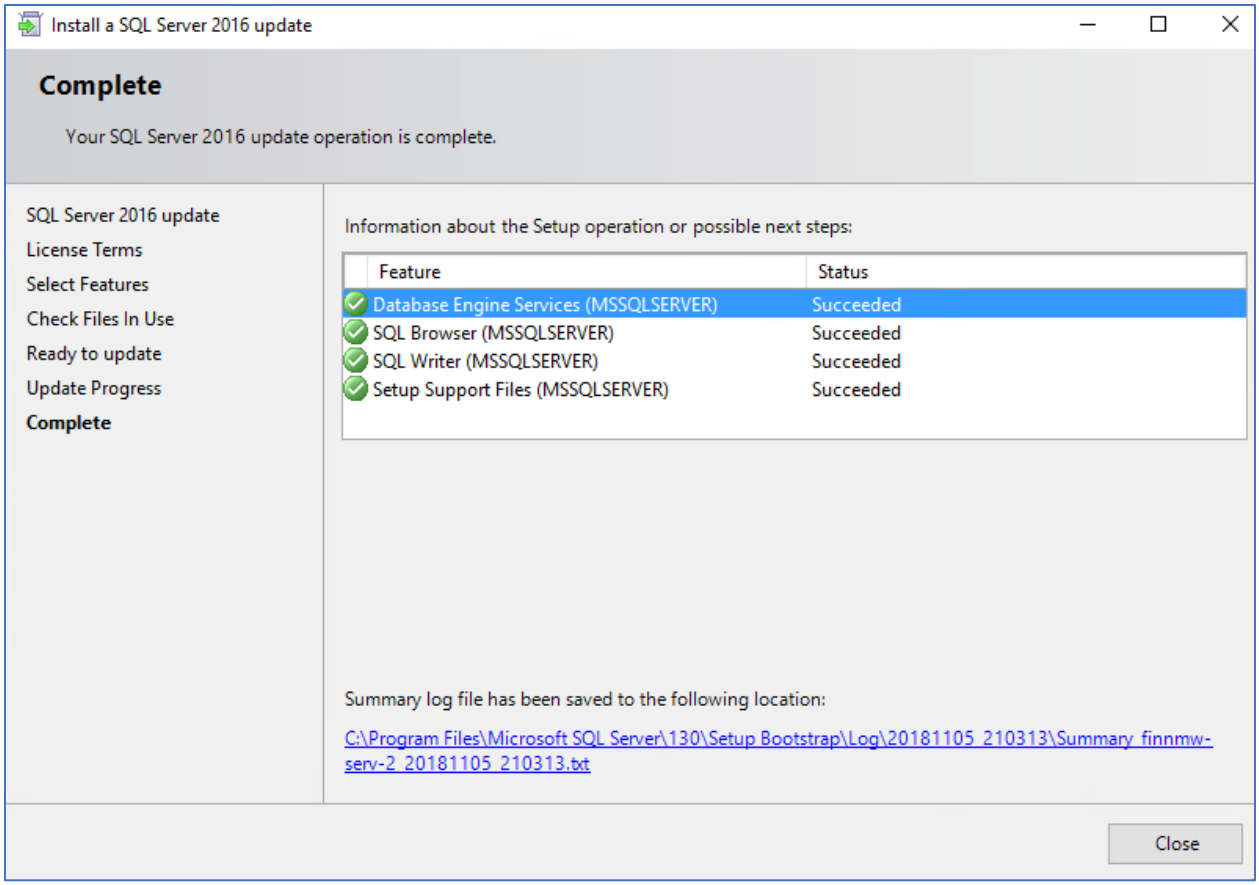
Velger bare å kjøre installasjonsfilen med en gang den er nedlastet. Deretter er det en rett frem installasjon som tar ca 5 minutter. Ved slutt får vi opp informasjon om installasjonen.



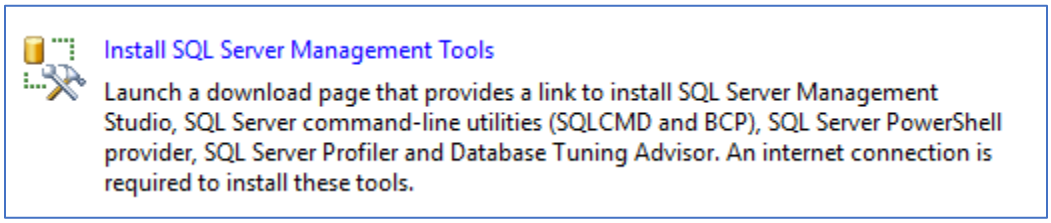
Etter at SP2 er installert må vi installere SQL Server 2016 SP2 Latest Cumulative Update. Denne finner vi også på nettsiden til Microsoft.



Som SP2 er dette en rett frem installasjon som tar ca 5 minutter. Får også her opp informasjon om installasjonen når den er fullført.



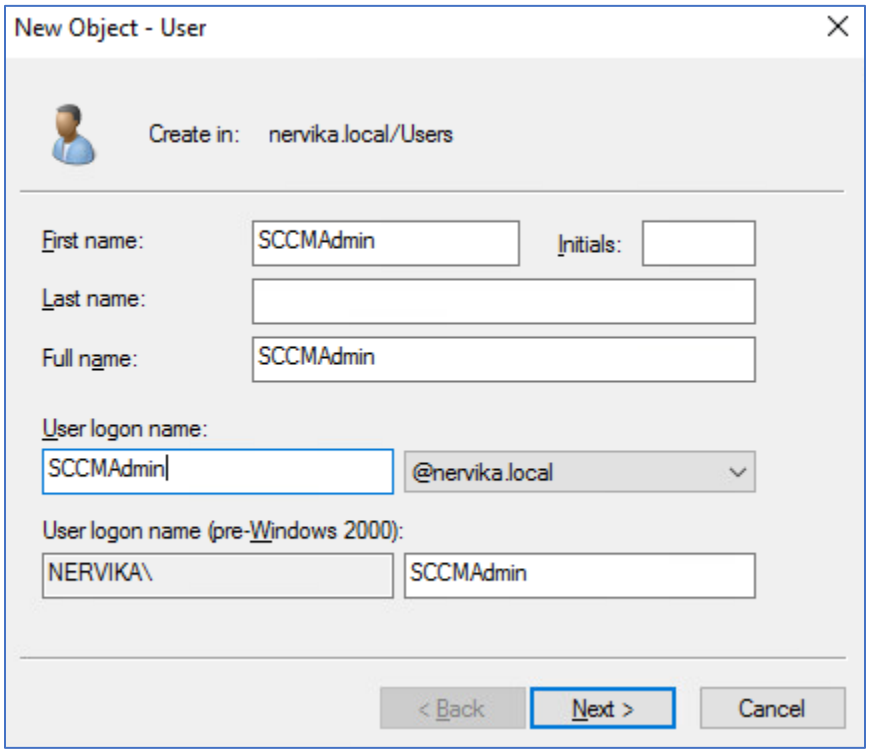
Når alt er up to date, må vi installere SQL Server Management Tools. Dette gjør vi ved å åpne SQL Server Installation Center og velger Server Management Tools under Installation.



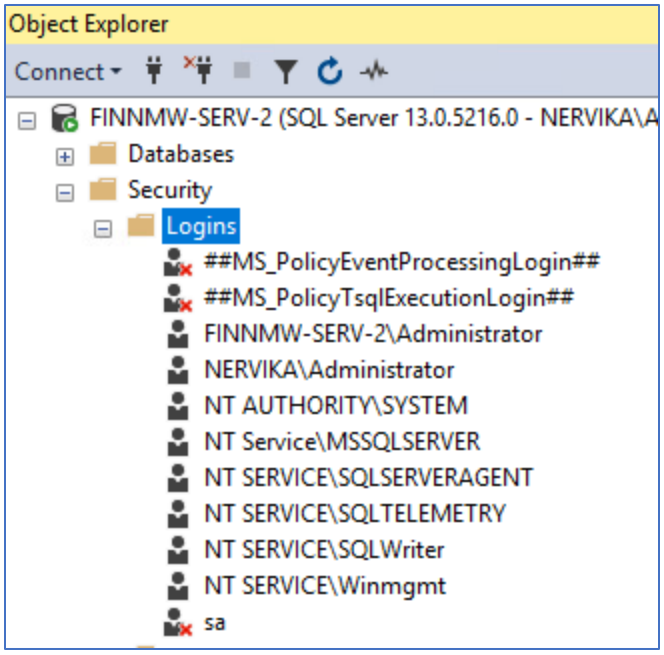
Her blir vi sendt til microsoft sine hjemmesider, hvor jeg velger å laste ned den nyeste versjonen av Server Management Tools. Installasjonen fullføres av seg selv og maskinen restartes. Nå er alt klart til å starte forberedelsene til installasjonen av SCCM.

3.3 Forberedelser til installasjon av System Center

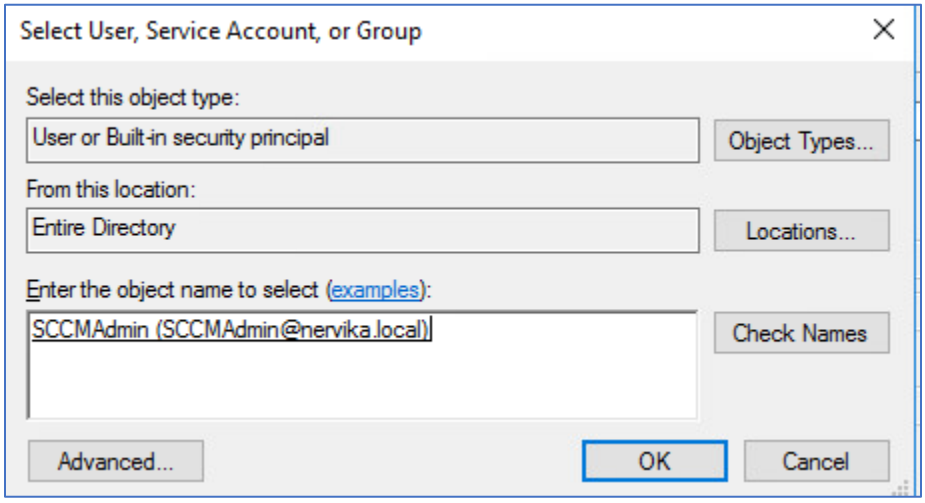
Den første forberedelsen til installasjonen er å opprette en ny domenebruker som skal være administrator til SCCM-serveren. For å opprette denne brukeren må vi inn på AD-serveren og lage en ny bruker. Velger å kalle denne brukeren SCCMAdmin.



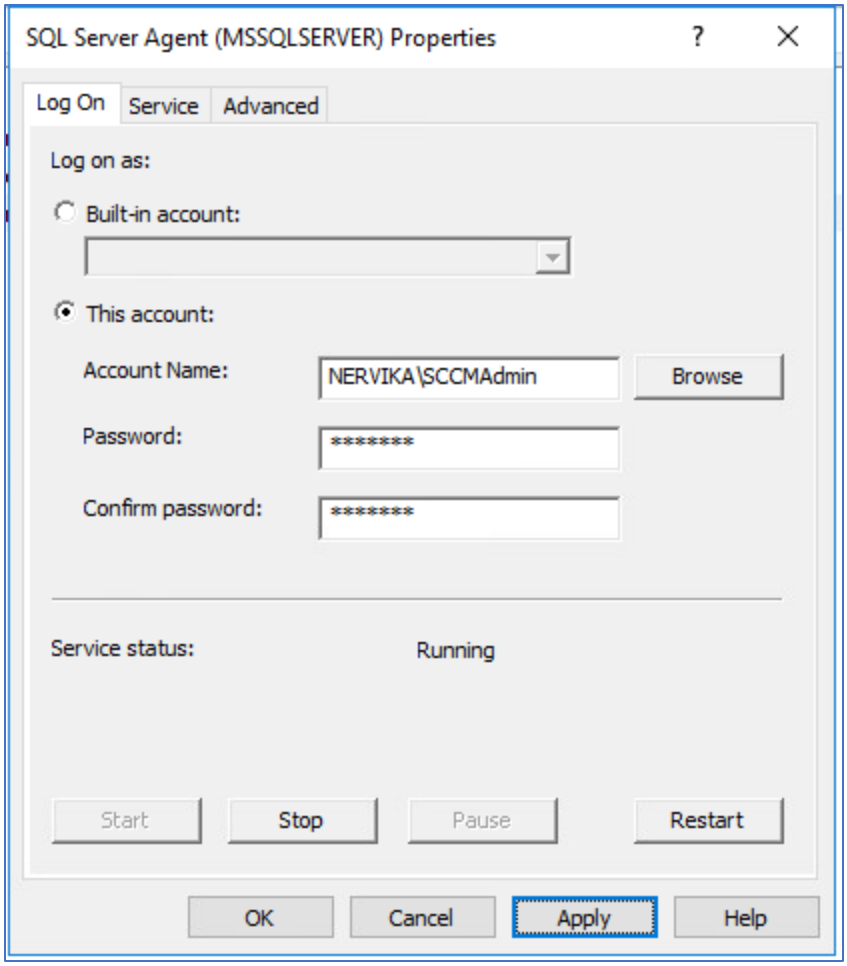
Nå må vi logge på SCCM-serveren for å gi denne brukeren administratorrettigheter til SQL-serveren. Åpner da SQL Server Management Studio som vi nettopp har installert. Navigerer oss til Logins under serveren.



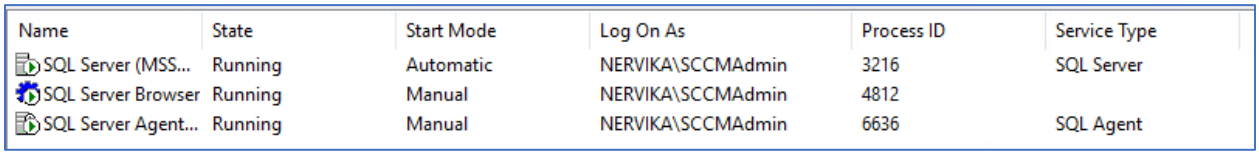
Høyreklikker på Logins og velger New Login. Velger Windows Authentication og søker etter brukeren SCCMAdmin på domenet.



I SQL Server Configuration Manager må vi også endre Log on-bruker i SQL Server, SQL Browser og SQL Agent. SCCMAdmin skal være Log on-bruker her. For å endre dette velger vi SQL Server Services og høyreklikker først på Server Agent→Properties→Velger Nervika\SCCMAdmin som log on-bruker via This account.

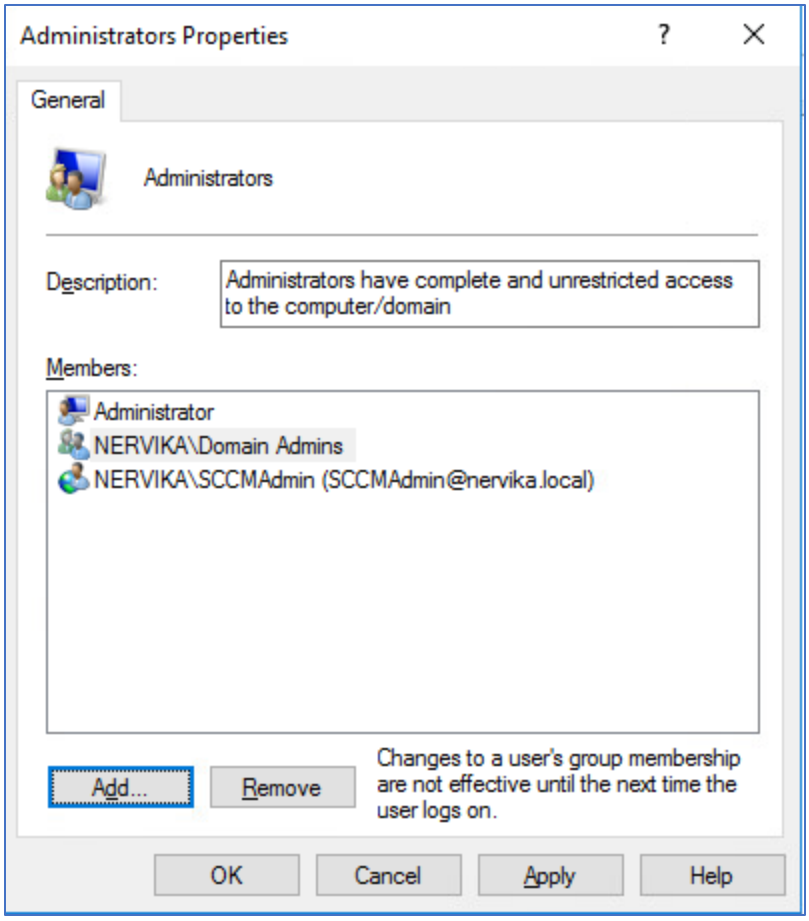


Gjentar denne prosessen med Browser og SQL Server, slik at oppsettet blir sånn:



Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server (MSS...	Running	Automatic	NERVIKA\SCCMAdmin	3216	SQL Server
SQL Server Browser	Running	Manual	NERVIKA\SCCMAdmin	4812	
SQL Server Agent...	Running	Manual	NERVIKA\SCCMAdmin	6636	SQL Agent

Denne brukeren må også være lokal administrator på SCCM-serveren. Dette gjøres via Server Manager. Åpner Server Manager→Tools→Computer Management→Local Users and Groups→Administrators→Add→Nervika\SCCMAdmin→OK

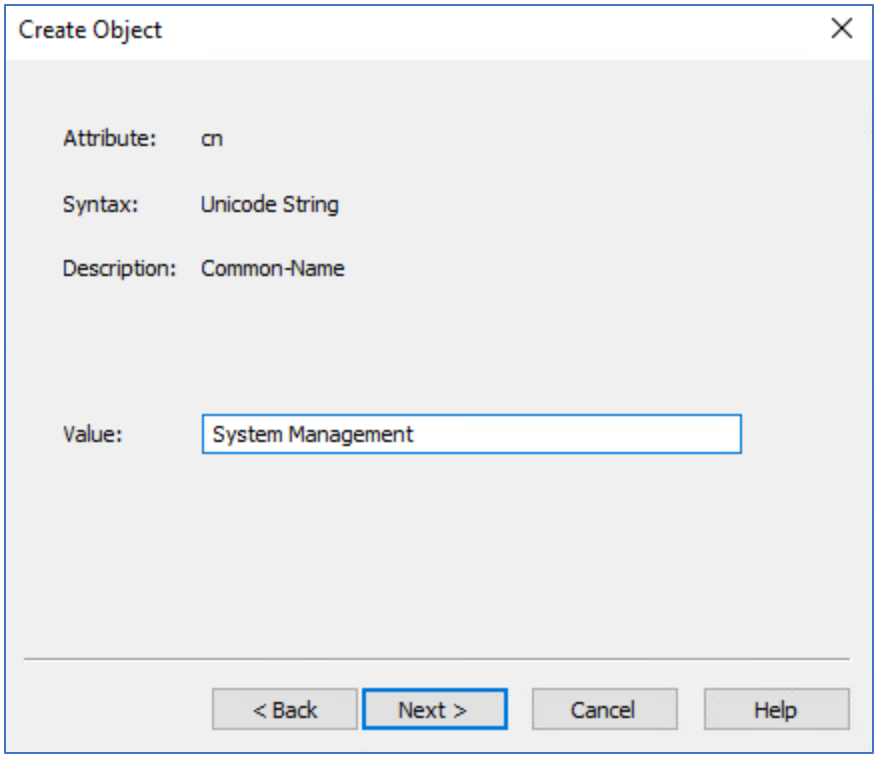


Nå må vi tilbake til AD-serveren og åpne Adsi.edit. Dette gjøres via Server Manager eller via cmd med kommadoen adsiedit.msc.

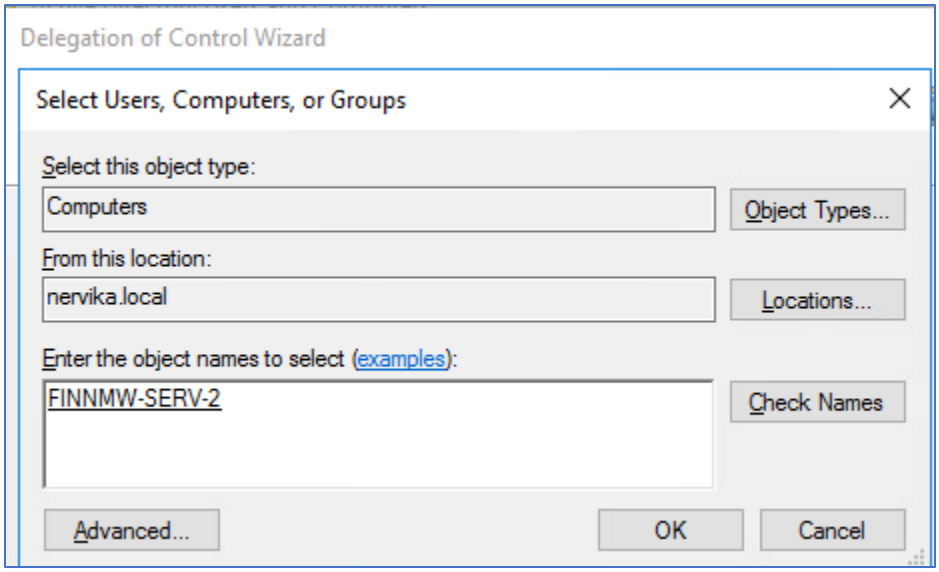
Når adsi.edit åpnes trykker vi More actions→Connect to→OK.

Kommer da opp en del valg, vi navigerer oss til CN=System. Høyreklikker→New→Object→Container.

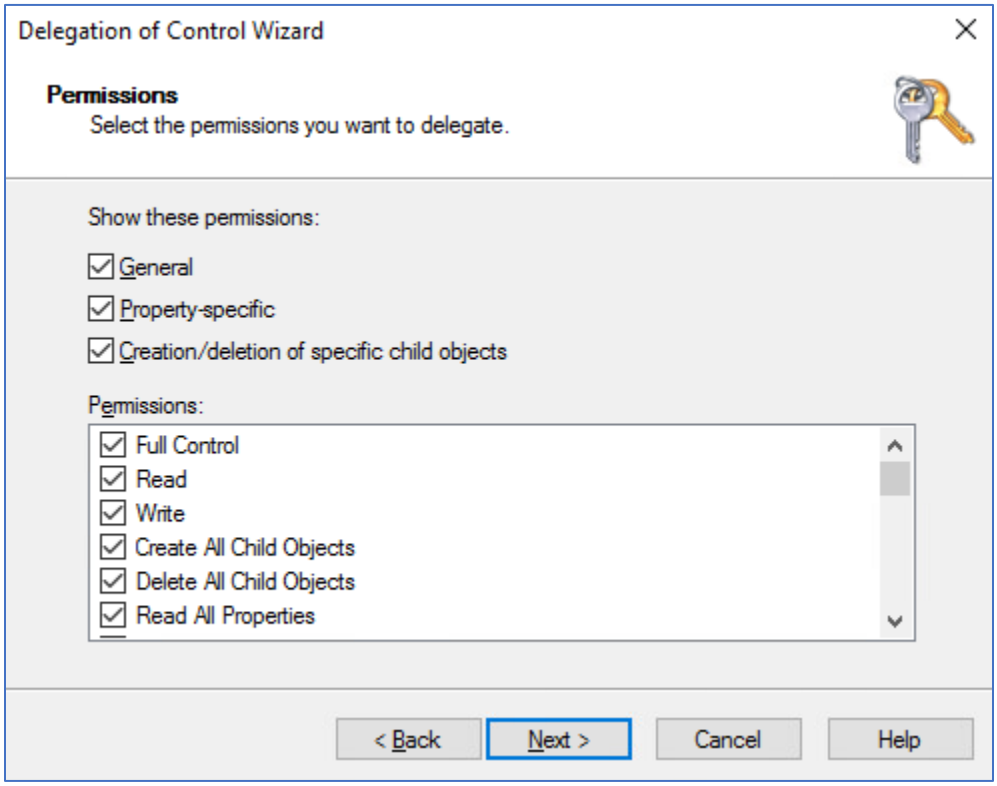
Velger her System Management i «Value»-feltet.



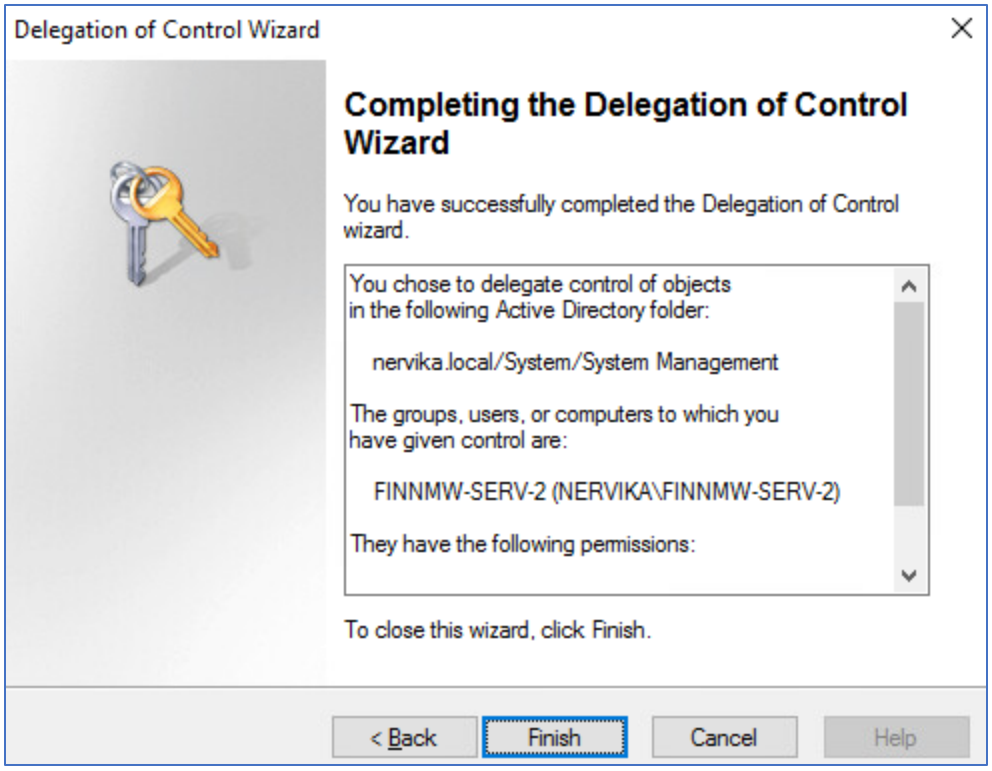
Nå må vi delegere rettigheter til denne containeren. Det gjøres i AD Users and computers. Det første vi må gjøre I AD er å velge view→Advanced Features slik at vi ser denne containeren. Den finner vi under System. Høyreklikker på containeren→Delegate Control→Add→Object Types→Velger kun Computers→Finner SCCM-Serveren (FINNMW-SERV2)→OK



På neste steg trykker vi Next→Create a custom task to delegate→Next→Huker av General, Property-specific og Creation og gir den full control

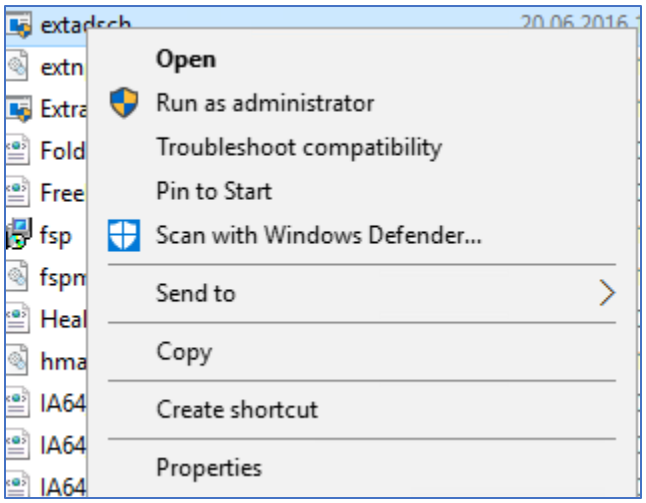


Trykker next en siste gang og får opp en bekreftelse på hva vi har gjort

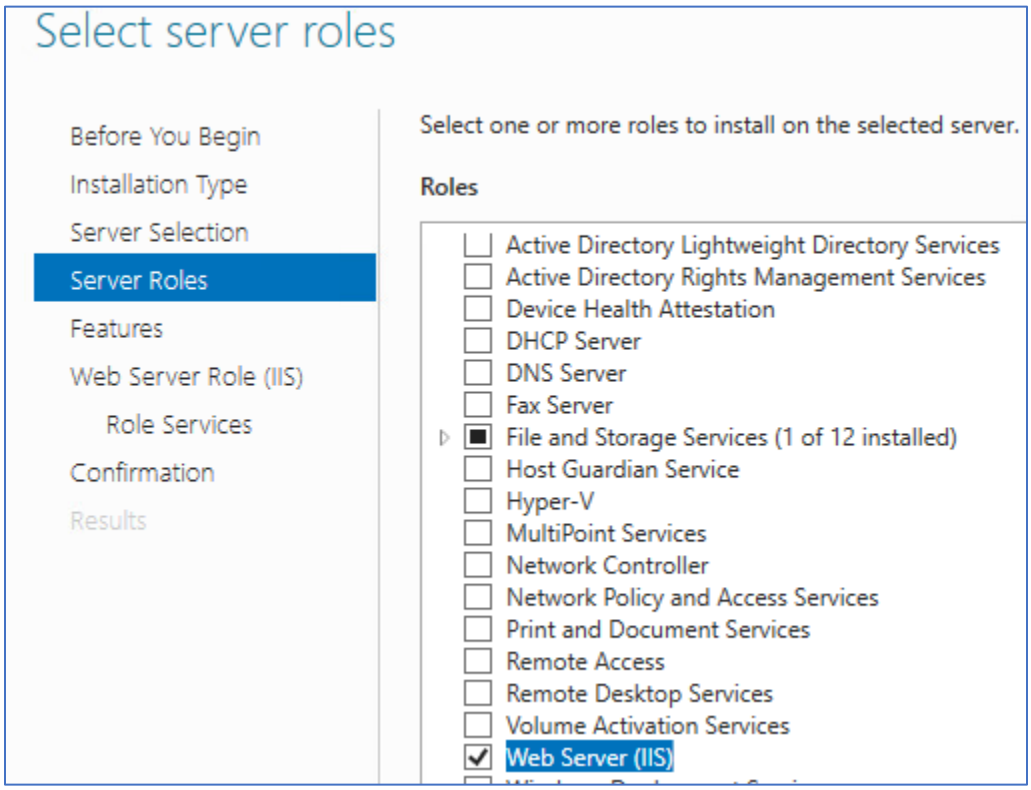


Når vi er ferdige med å delegere kontroll til Containeren, må vi kjøre extadsch.exe. Extadsch.exe finner vi inne på den virtuelle DVD-driven til SCCM-manager. Extadesch.exe kjøres for å utvide AD-skjemaet for Configuration Manager.

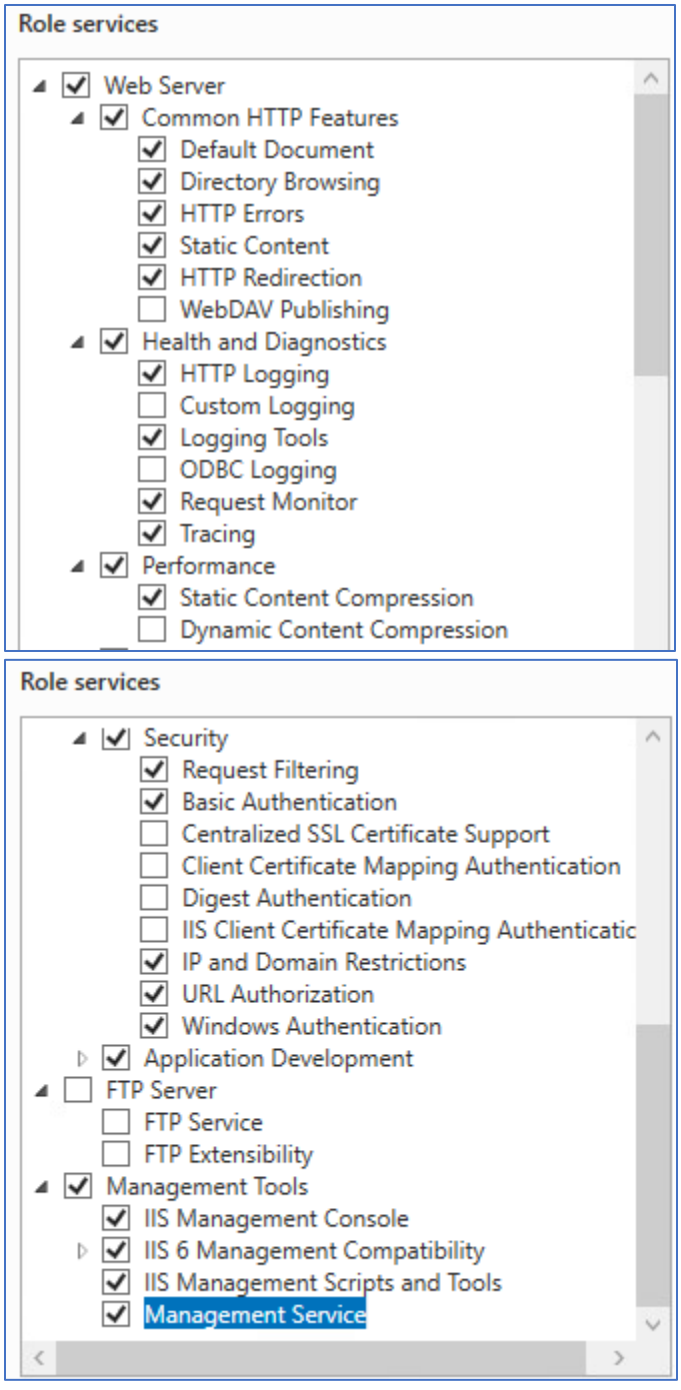
Mounter ISOen til SCCM-manager slik som vi gjorde med SQL-server tidligere i oppgaven. Extadesch.exe ligger under mappen SMSSETUP/BIN/X64. Når vi finner filen må vi velge «Run as administrator»



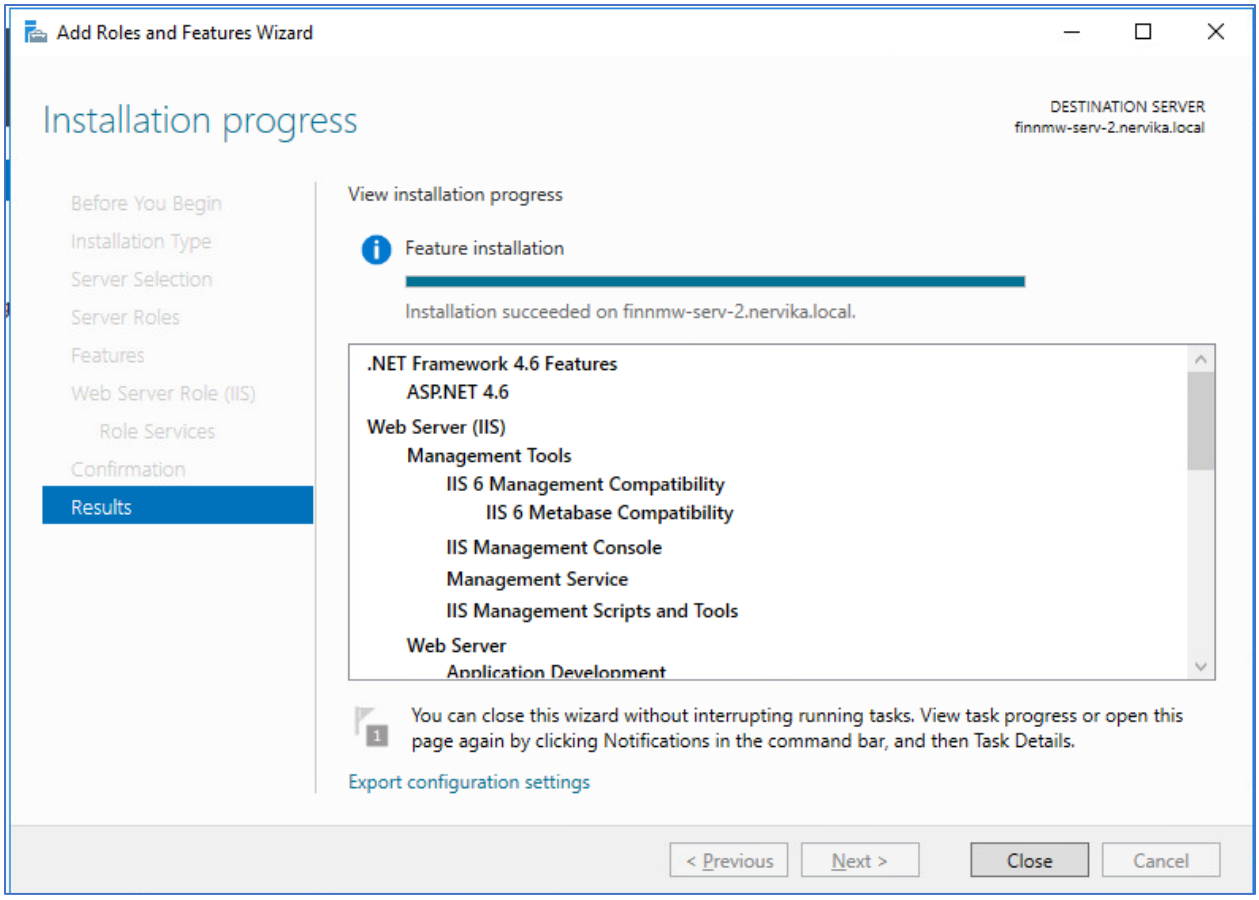
Nå må vi tilbake til Server Manager for å åpne Add Roles and Features. Her skal vi installere Web Server (IIS). Web Server finner vi under Server Roles



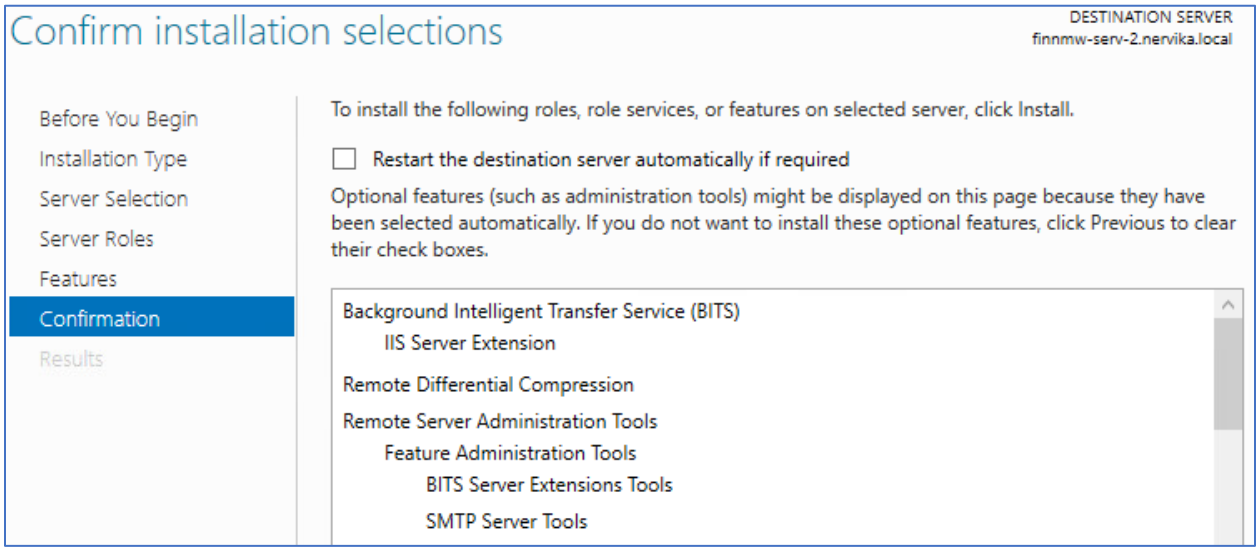
Når vi har funnet Web Serveren, må vi navigere oss til Role Services. Her må vi huske å huke av følgende:



Når alt dette er huket av er det bare å trykke install. Når installasjonen er ferdig kommer det opp en bekreftelse på at installasjonen vart vellykket.



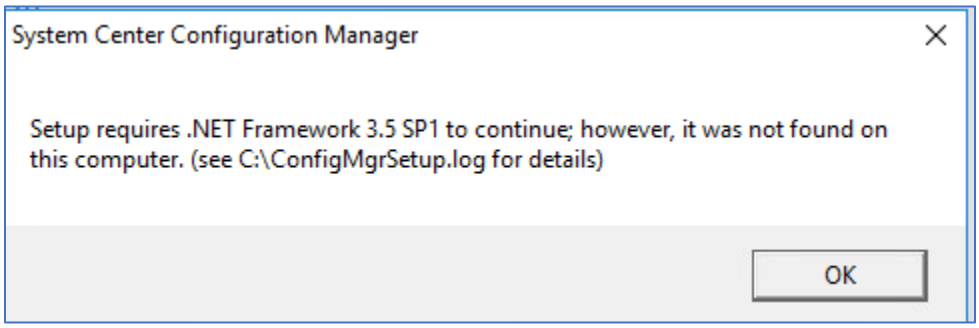
En siste ting vi må gjøre i Server Manager er å installere BITS og Remote Differential Compression. Her må vi huke under for alle undervalg under installasjonen.



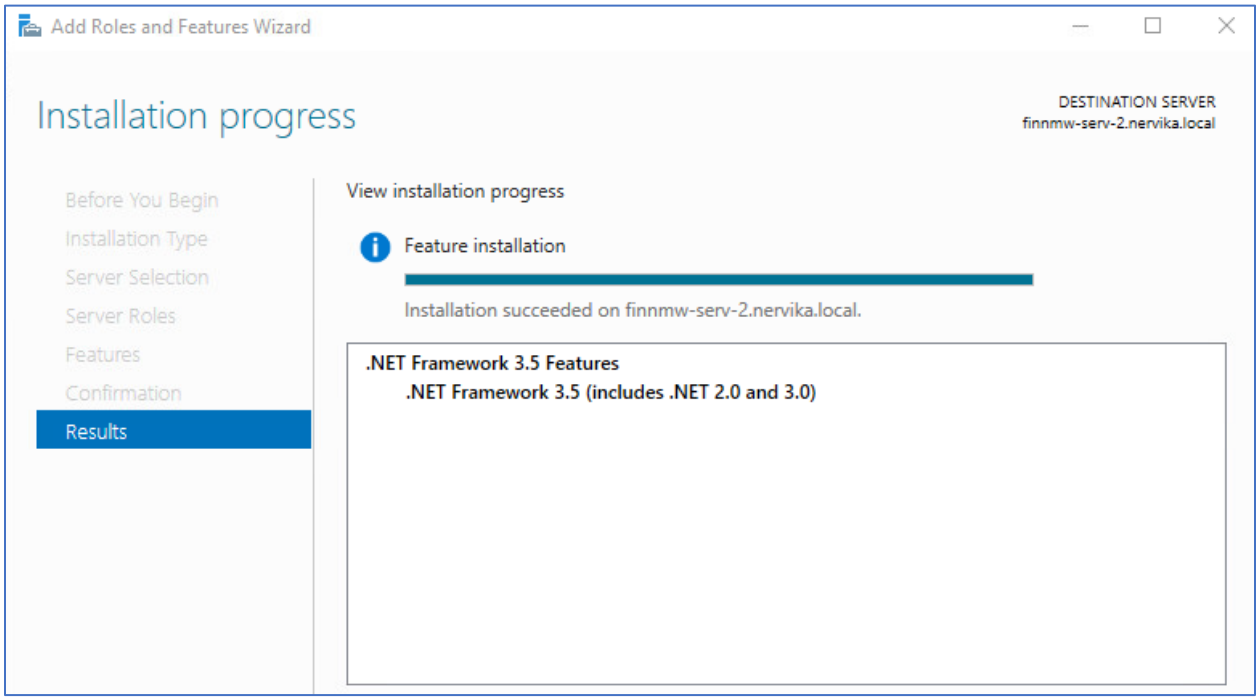
Nå skal alt være klart til å installere SCCM.

3.4 Installasjon av Microsoft System Center

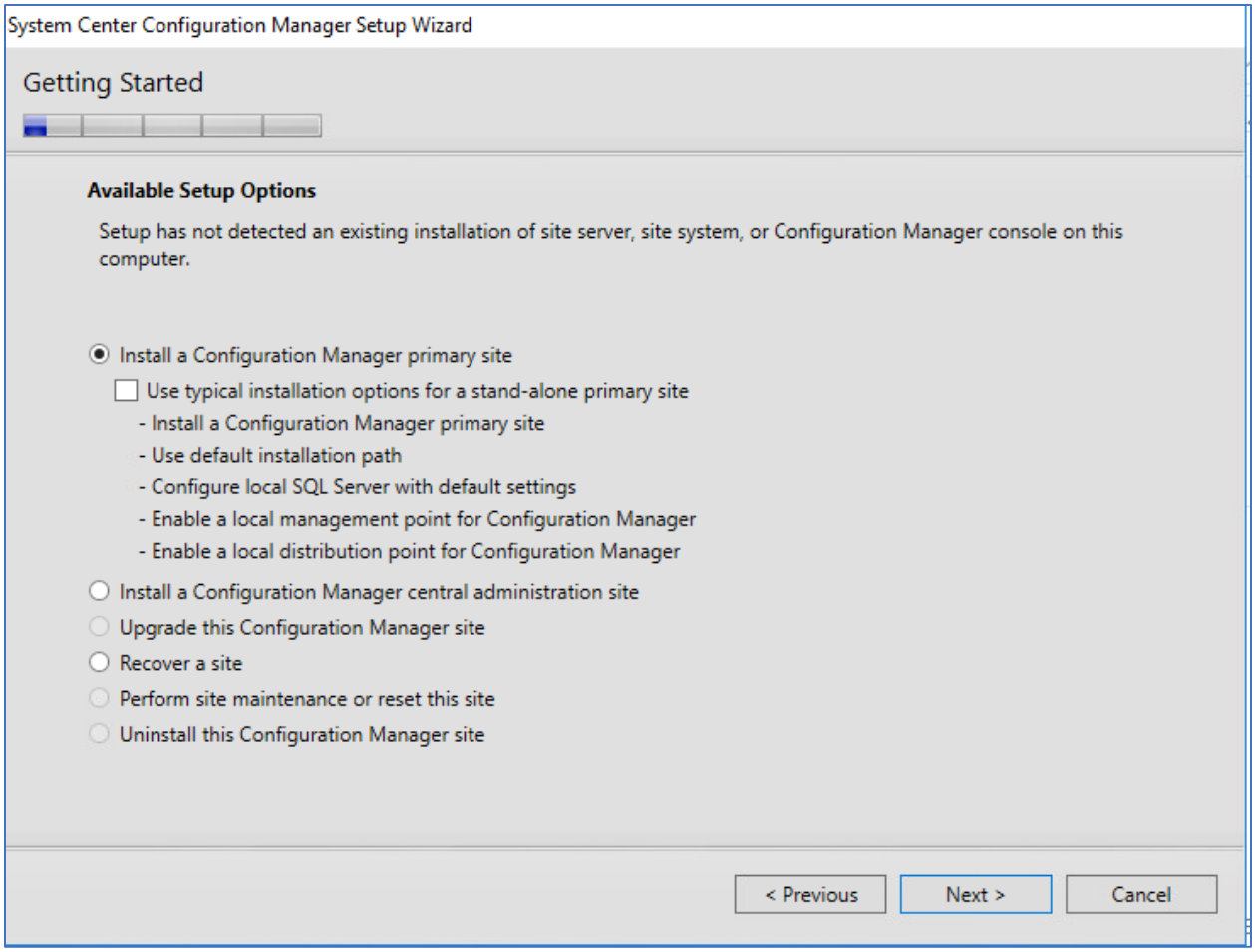
Har allerede mountet ISO-filen til SCCM på serveren. For å starte installasjonen åpner vi den virtuelle D-driven og kjører splash.exe. Når vi starter splash.exe så vil installasjonsfilen automatisk sjekke om serveren er klar for installasjon av SCCM. Fikk er en beskjed om at .NET Framework 3.5 SP1 manglet på denne serveren.



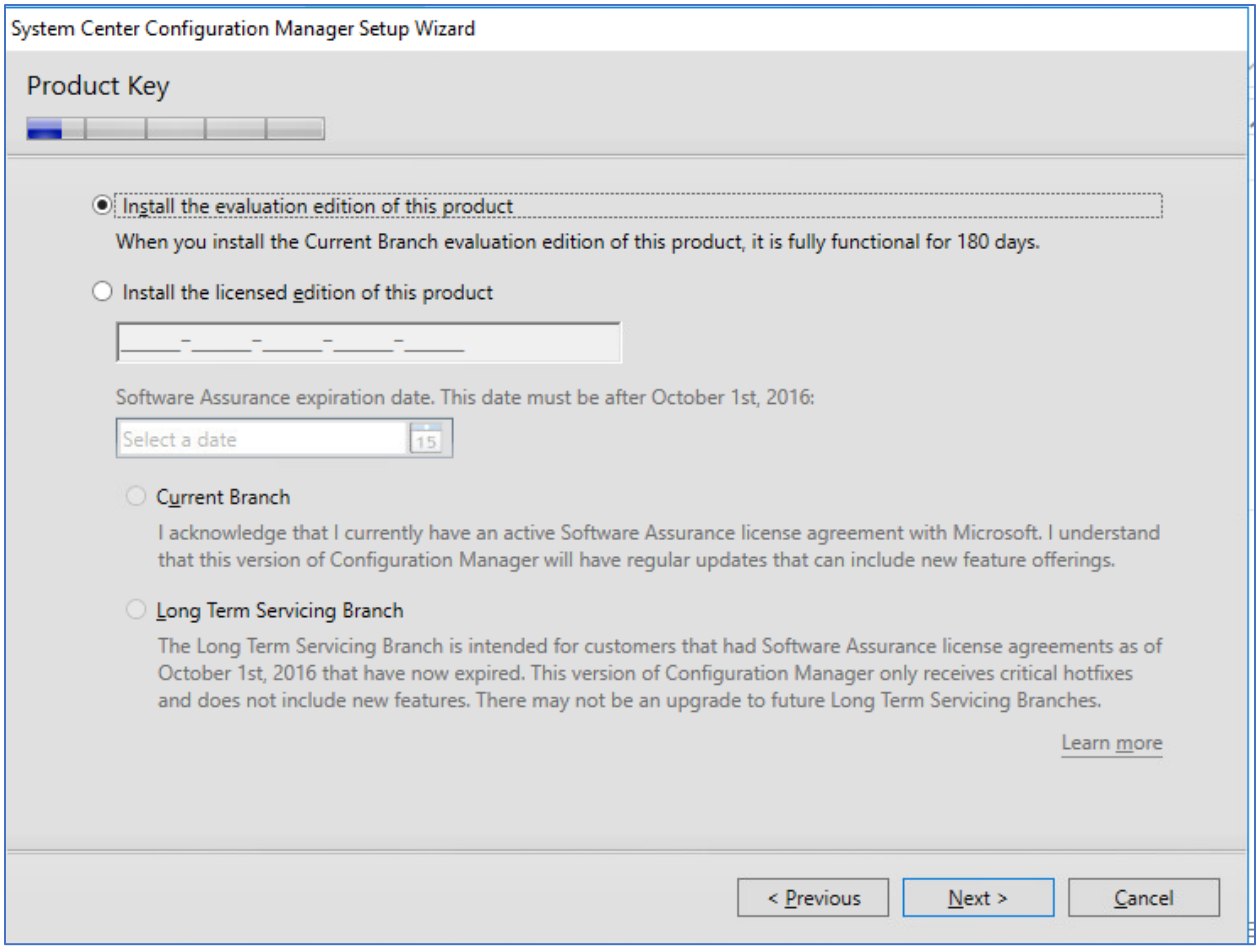
Gikk derfor tilbake til Server Manager for å legge til dette via Add Roles and Features.



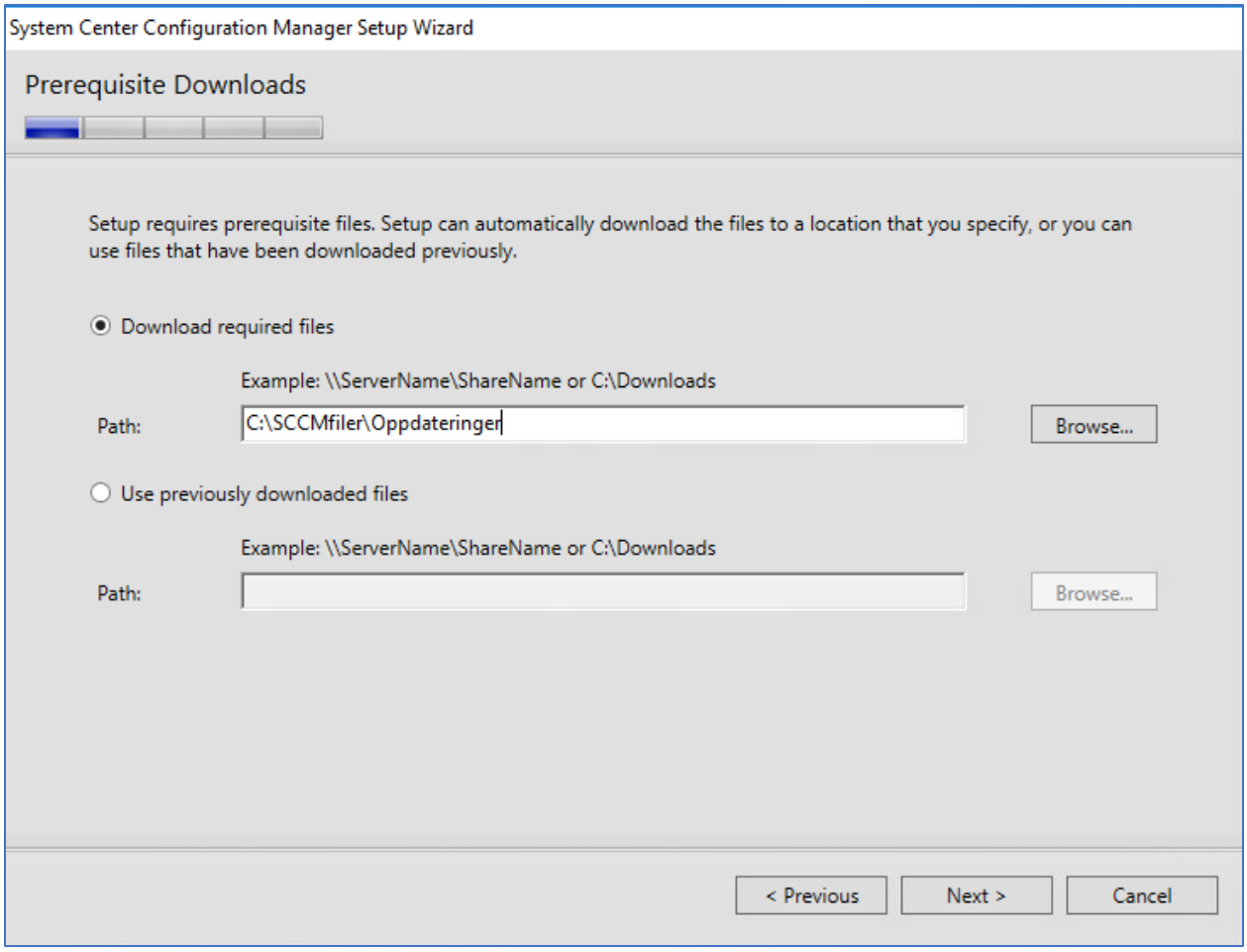
Når .NET Framework 3.5 er installert kan vi prøve å kjøre splash.exe igjen. Da starter selve installasjonen. I det første vinduet skal vi velge Install a Configuration Manager primary site.



I neste steg skal vi legge inn produktnøkkel om vi har det, siden jeg ikke pr. dags dato har produktnøkkel velger jeg Install the evaluation edition of this produckt.

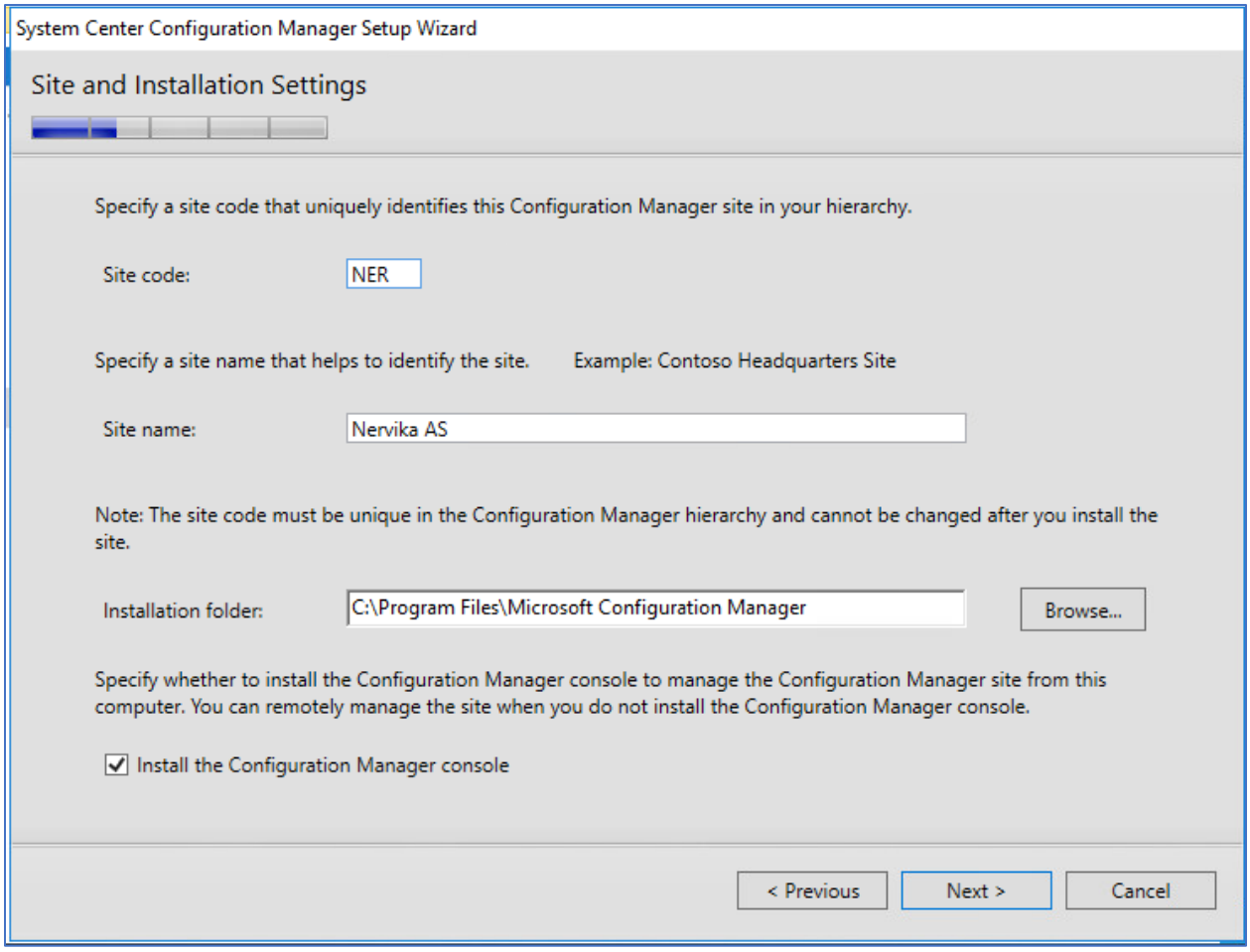


Det neste steget er å godkjenne vilkårene for bruk av programvaren. Godtar alt dette og trykker next. Nå skal vi velge hvor vi vil laste ned nødvendige filer. Velger her å lagre filene på C-driven under C:\SCCMfiler\Oppdateringer.

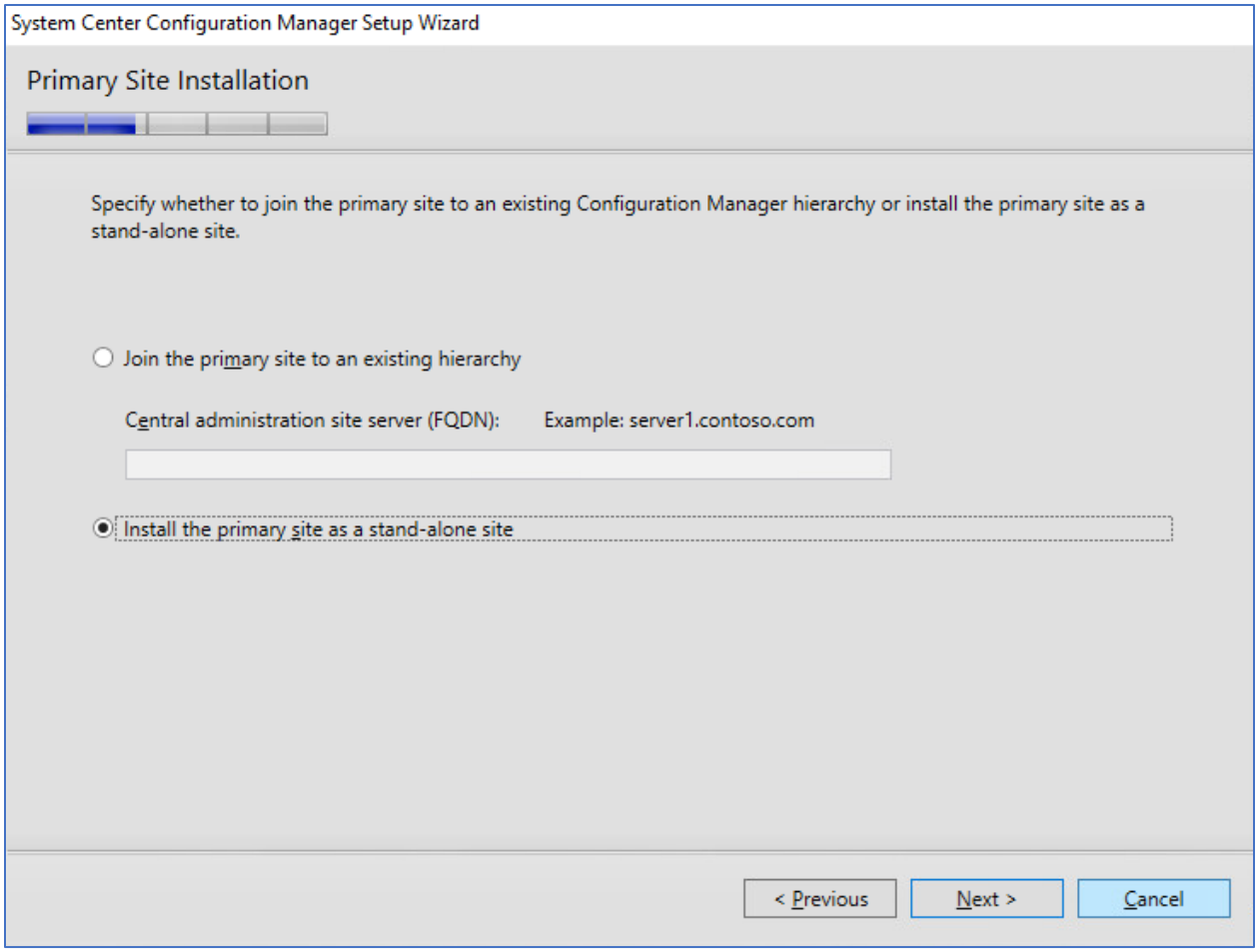


Når dette er unnagjort, skal vi velge hvilket språk vi skal ha. Velger å ha engelsk på både server og klienter.

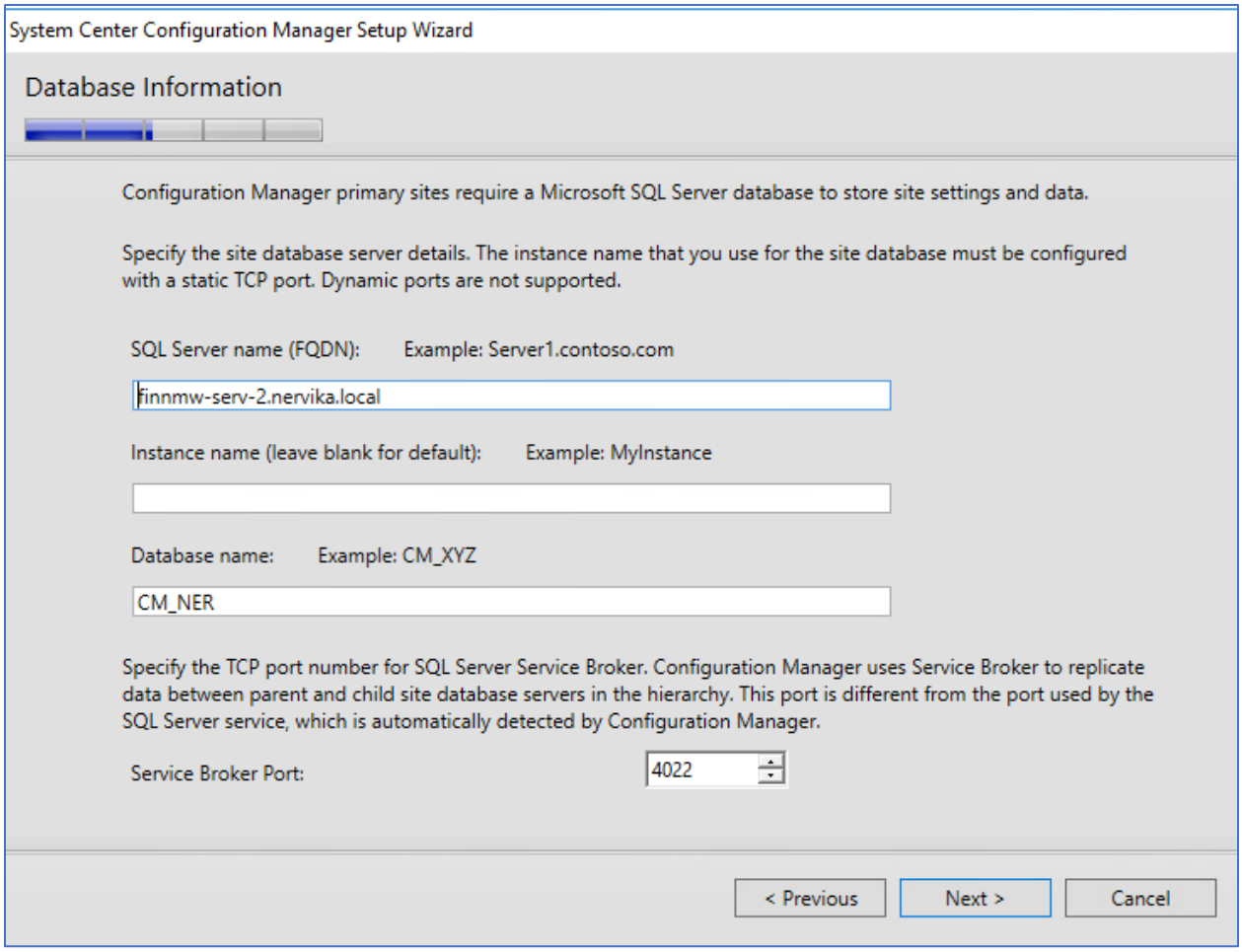
Nå skal vi velge Site code og Site name. Kan her velge hva vi vil. Velger Site code: NER – Site name: Nervika AS

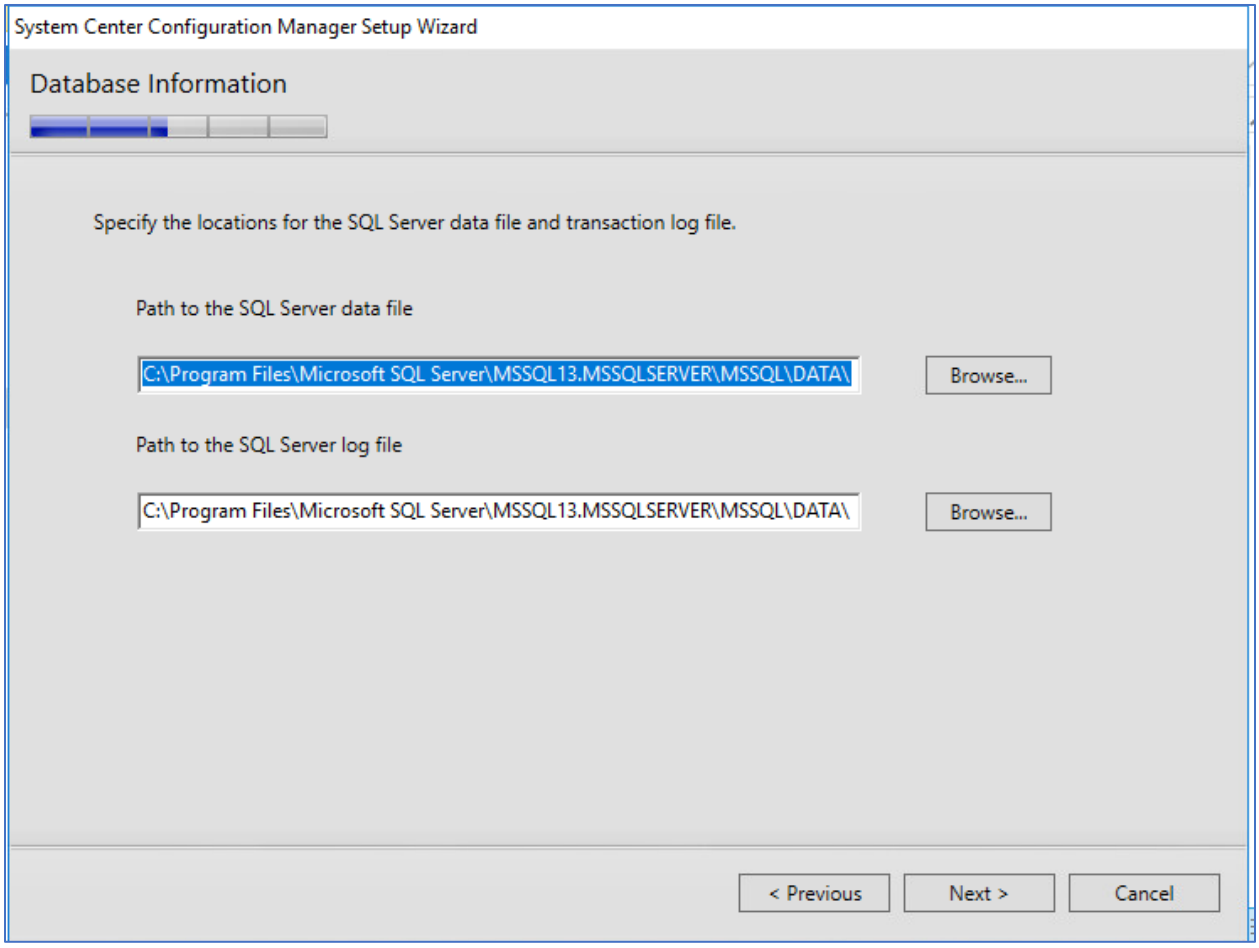


I neste steg velger vi Install the primary site as a stand-alone site.

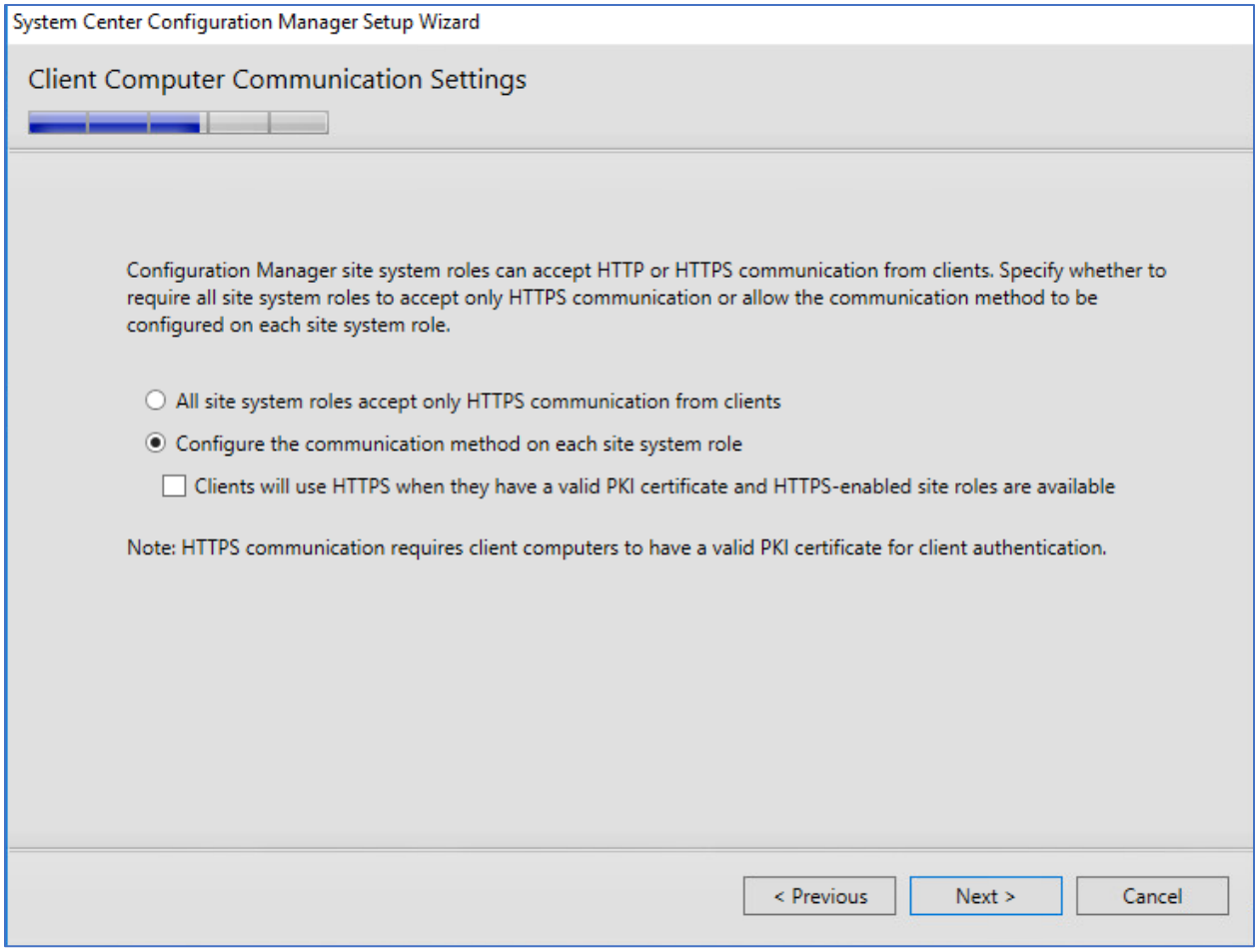


Neste steg lar vi stå som det er.

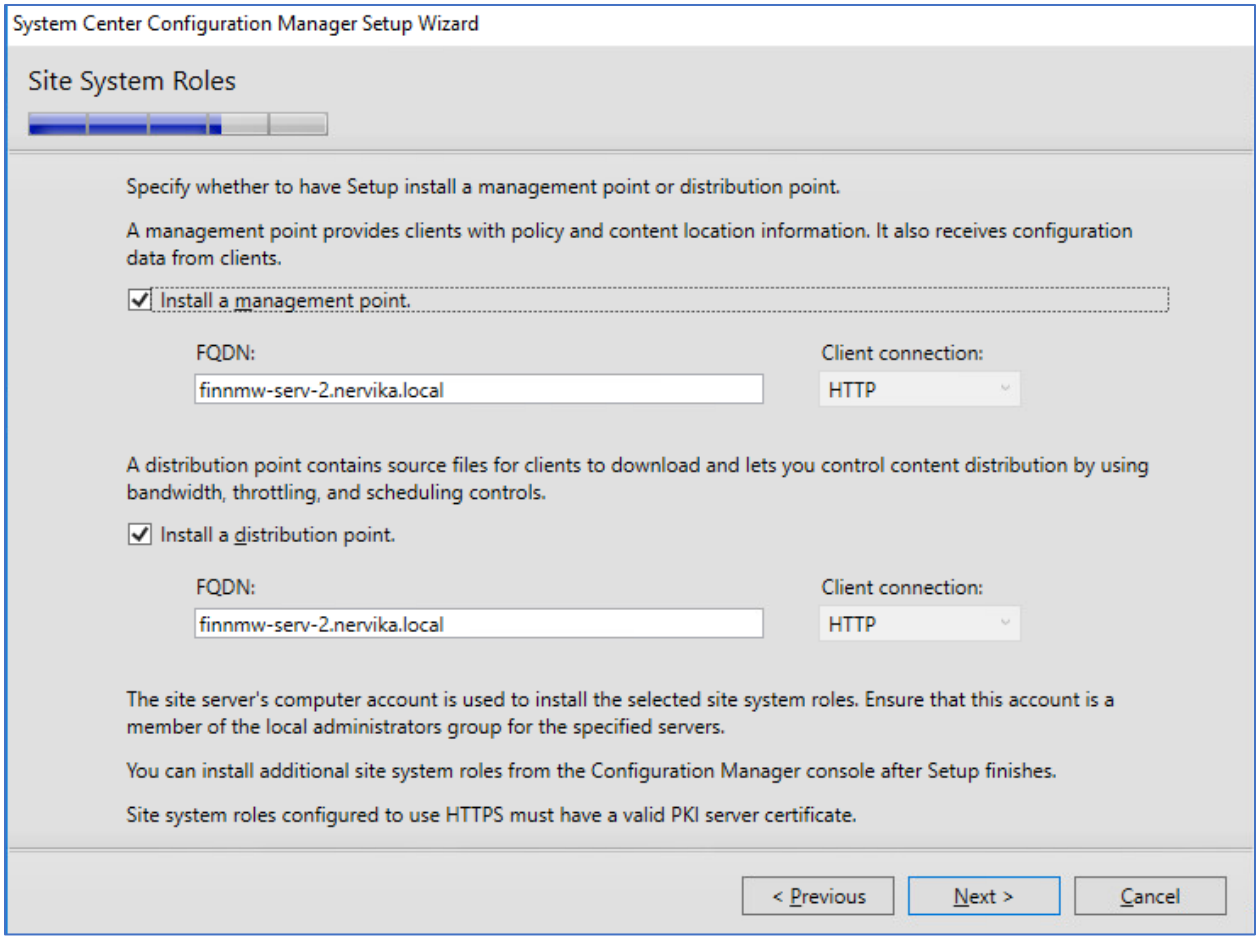

System Center Configuration Manager Setup Wizard
Database Information
Configuration Manager primary sites require a Microsoft SQL Server database to store site settings and data.
Specify the site database server details. The instance name that you use for the site database must be configured with a static TCP port. Dynamic ports are not supported.
SQL Server name (FQDN): Example: Server1.contoso.com
finnmw-serv-2.nervika.local
Instance name (leave blank for default): Example: MyInstance
Database name: Example: CM_XYZ
CM_NER
Specify the TCP port number for SQL Server Service Broker. Configuration Manager uses Service Broker to replicate data between parent and child site database servers in the hierarchy. This port is different from the port used by the SQL Server service, which is automatically detected by Configuration Manager.
Service Broker Port:
4022
< Previous
Next >
Cancel



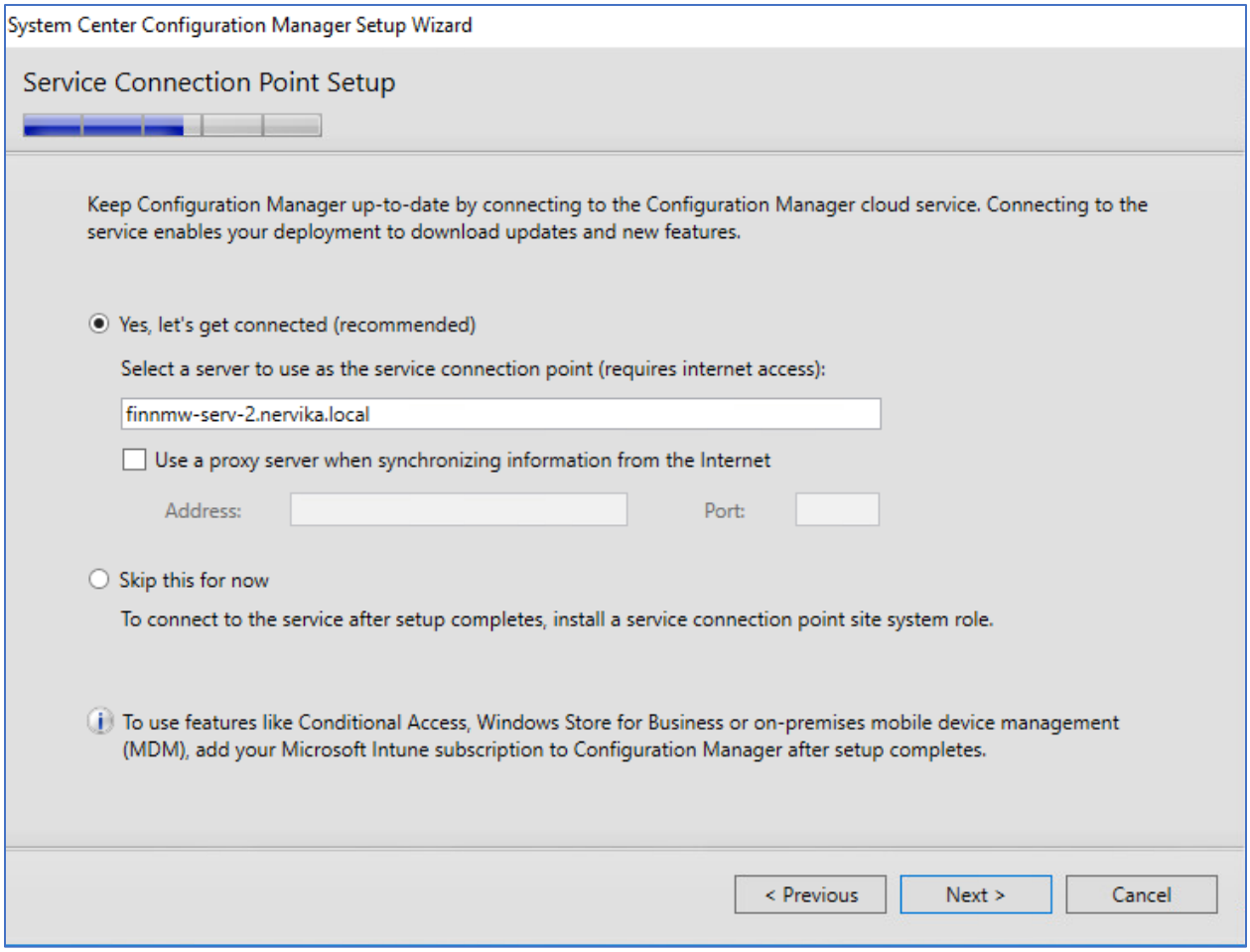
Under Client Computer Communication Settings velger vi Configure the communication method on each site system role.



Under Site System Roles gjør vi ingen endringer

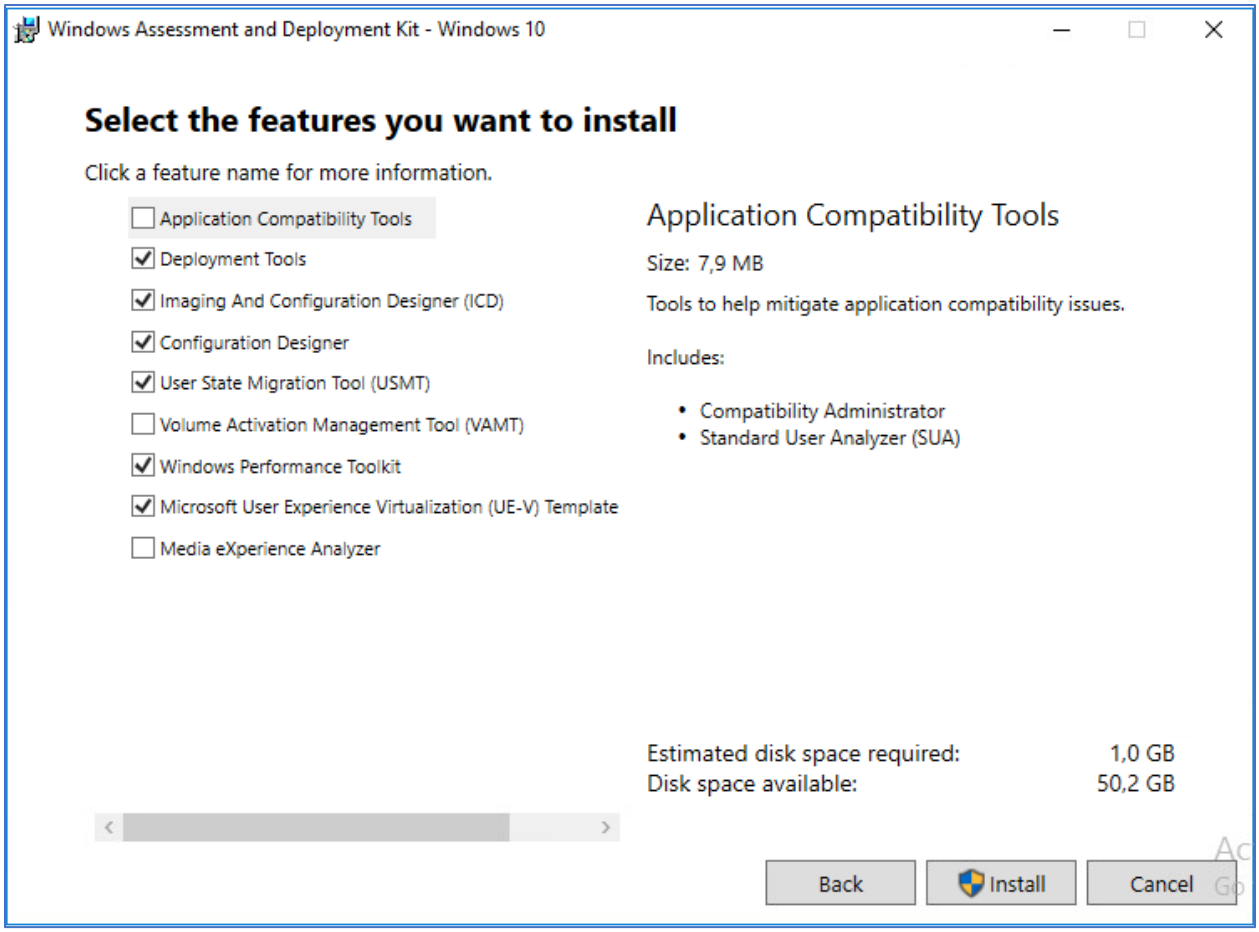


Det siste vi skal gjøre før installasjonen kan startes er å velge Service Connection Point Setup. Velger her Yes, let's get connected.

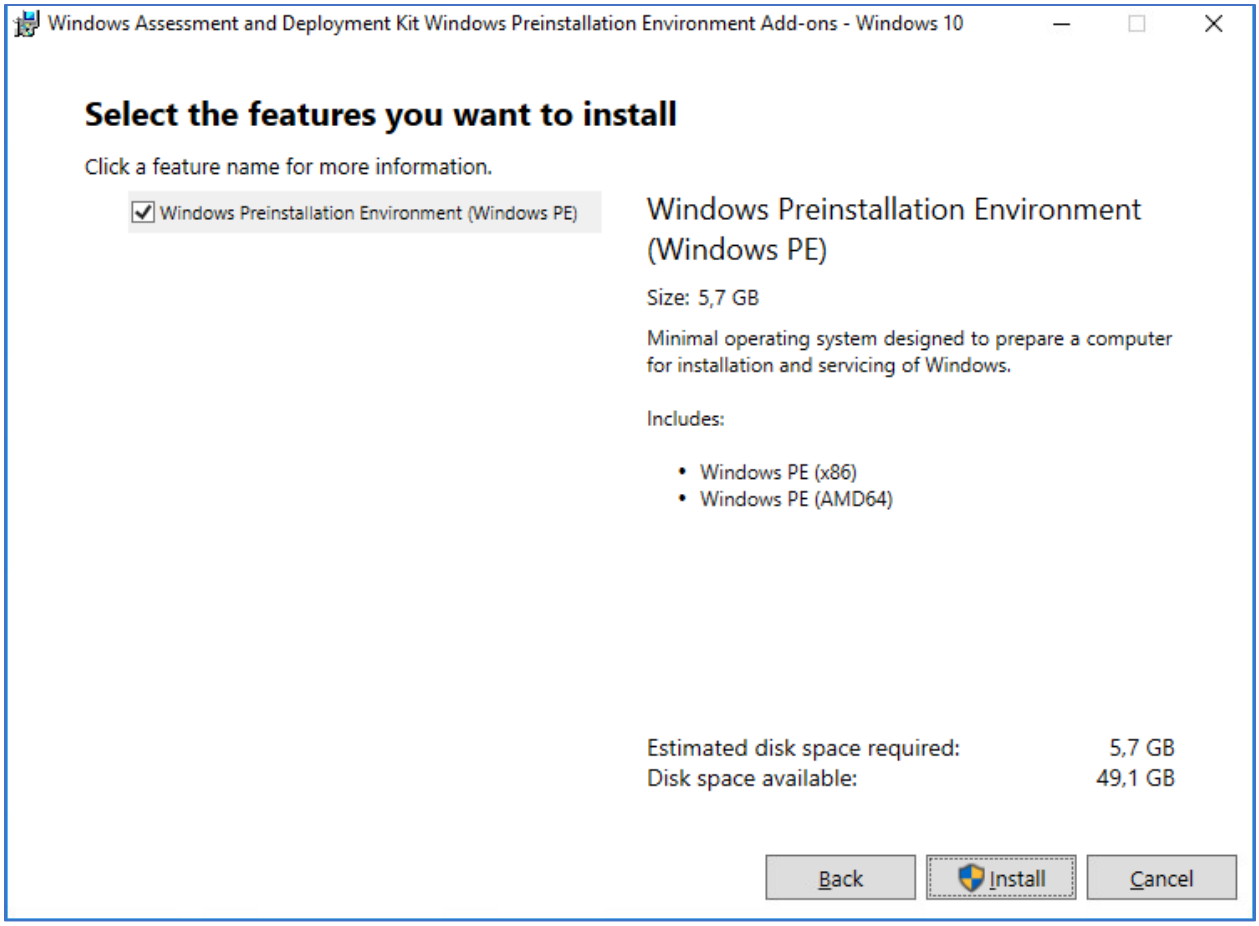


Nå er det i bunn og grunn klart for installasjonen, men før installasjonen starter vil den igjen ta en sjekk om serveren er klar for å installere SCCM. Når vi igjen tar denne sjekken får vi tre feilmeldinger som skyldes at vi ikke har lastet ned Windows Assessment and Deployment Kit. Vi må da igjen inne på Microsoft sine sider for å finne ADK. https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install.

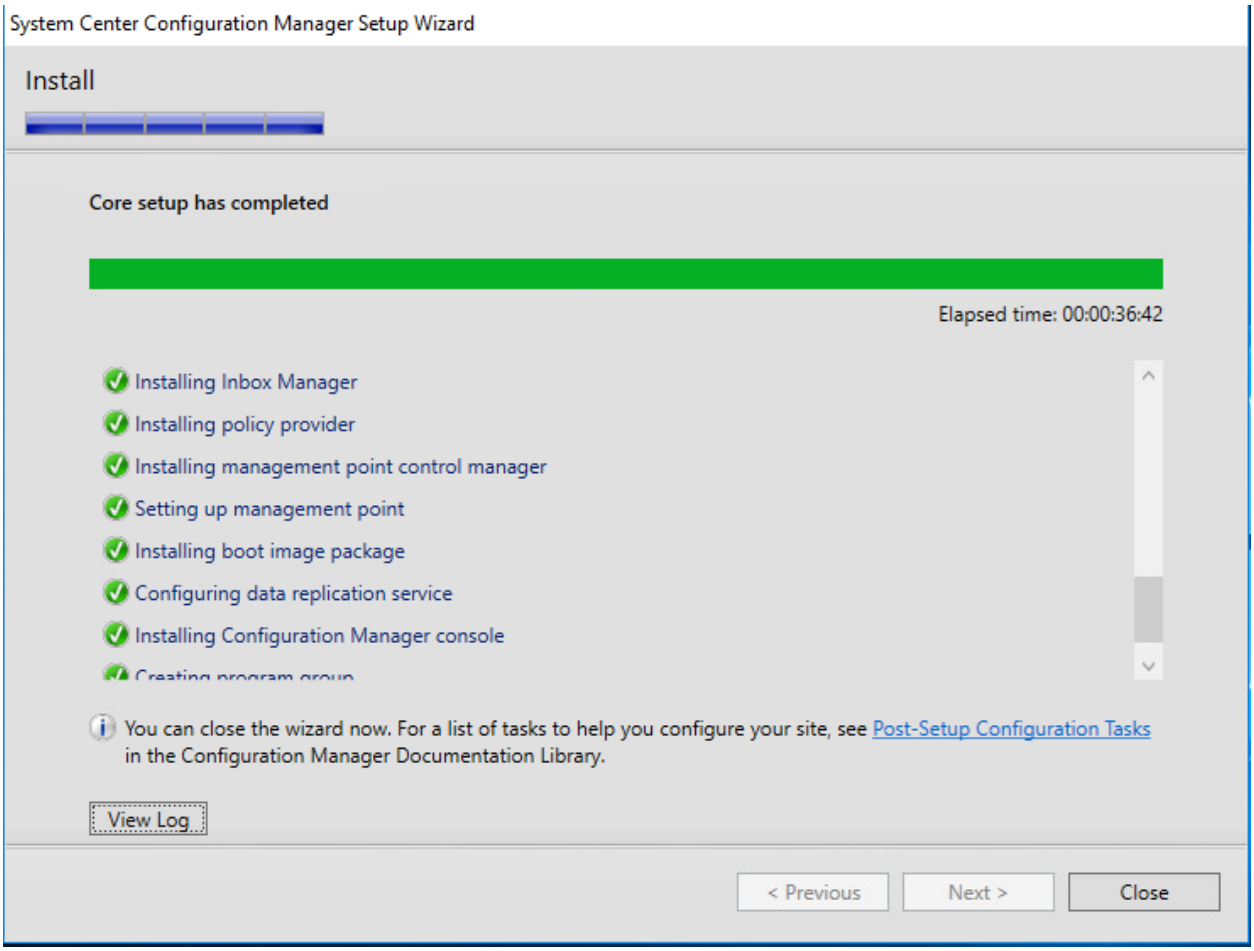
Her er det bare å laste ned filen og starte installasjonen.



Når ADK er installert må vi laste ned en add-on som heter Windows Preinstallation Enviroment (Windows PE)



Når vi igjen kjører sjekken før installasjonen, finner den ingen feil. Da er det bare å trykke Begin to install. Når installasjonen er ferdig vil dette vinduet vises:

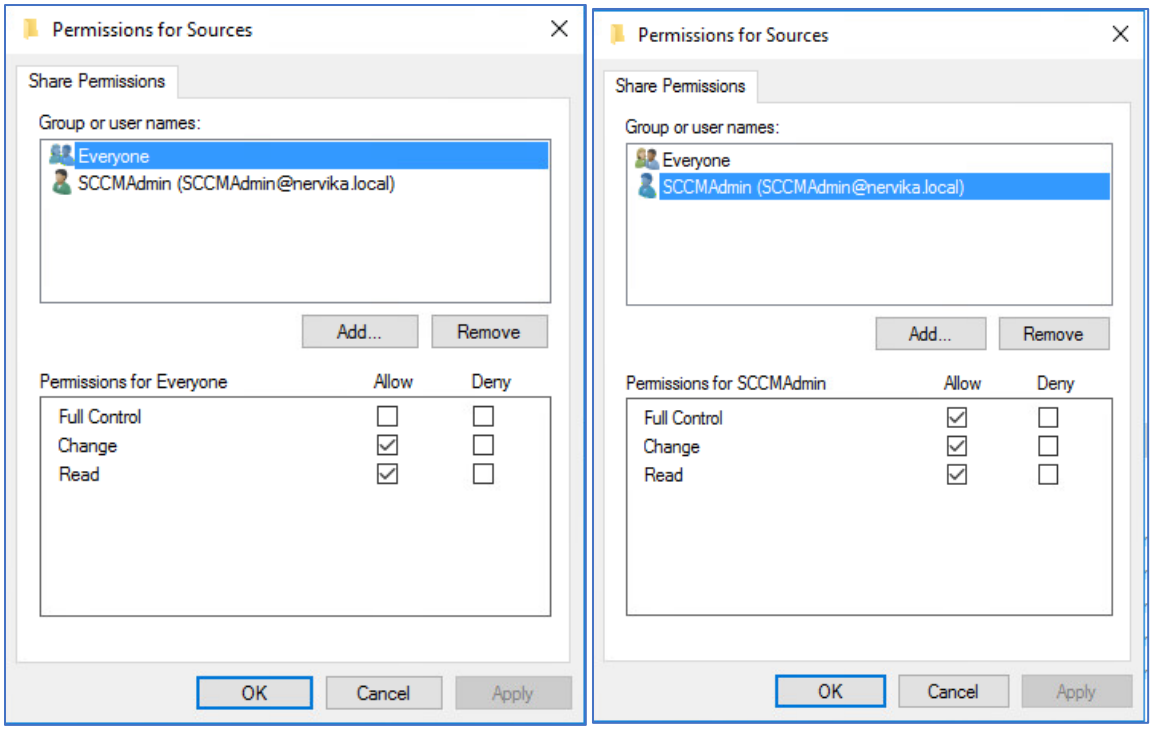


3.5 Oppdatering av Microsoft System Center

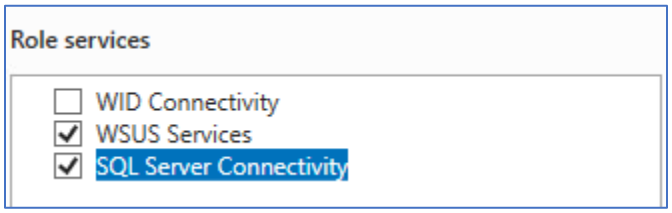
4. WSUS og SUP

4.1 WSUS

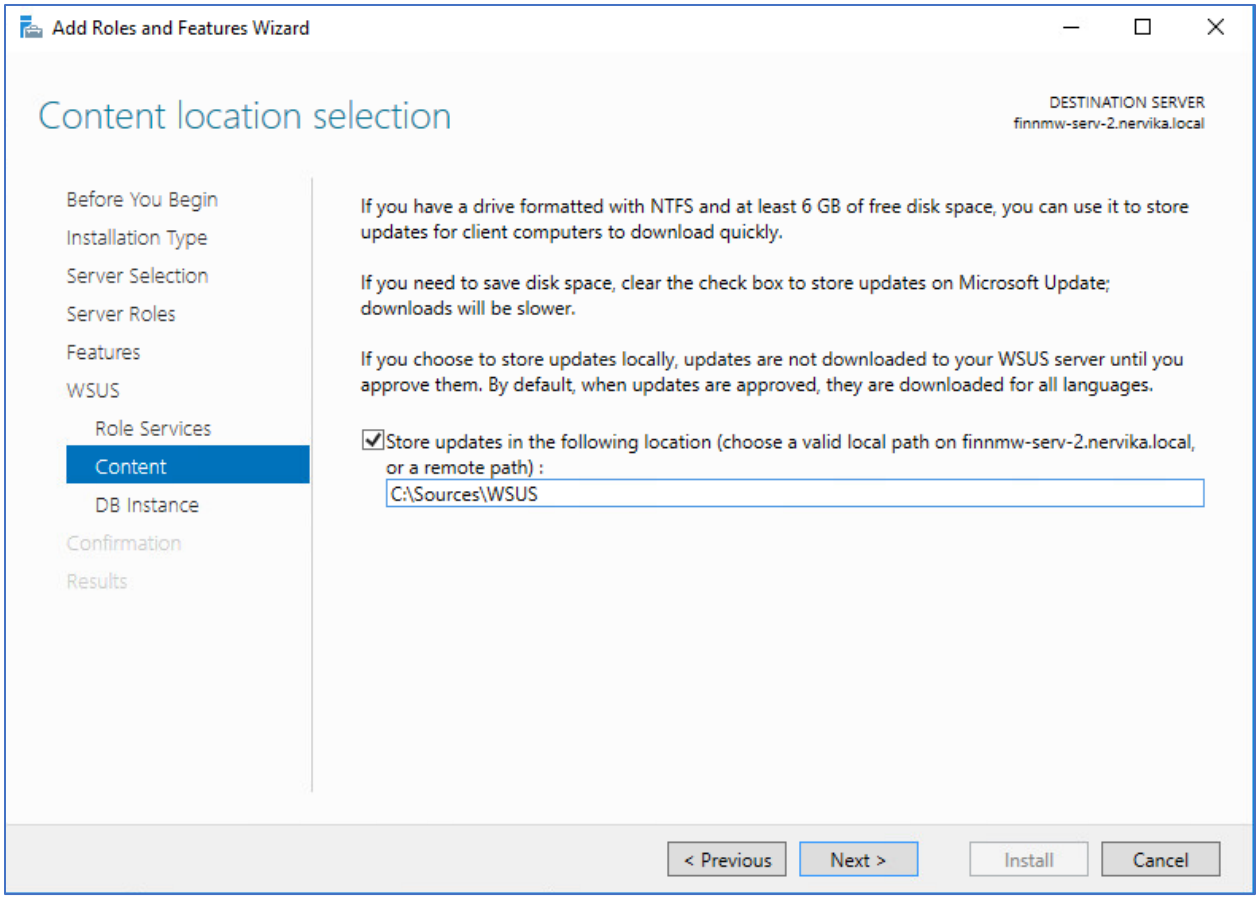
På SCCM-serveren navigerer vi oss til C-driven og oppretter ei mappe som heter Sources. Oppretter så en undermappe om vi kaller WSUS. Sources-mappen skal så deles. Høyreklikker på mappen og velger Properties→ Sharing→ Advanced Sharing→ Permissions. Her gir vi SCCMAdmin full control, mens Everyone får lese- og endrerettigheter (Read and change).



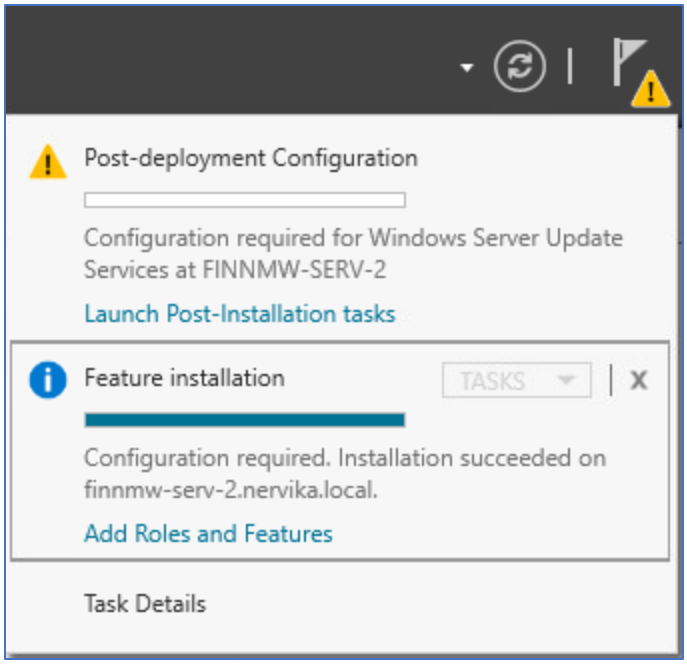
Nå må vi installere rollen Windows Server Update Services fra Server Manager. Under installasjonen får vi et undervalg. Her skal vi velge WSUS Services og SQL Server Connectivity som vist på bildet under.



I neste valg skal vi velge stien til hvor vi vil lagre oppdateringer. Vi velger da C:\Sources\WSUS som vi nettopp opprettet.

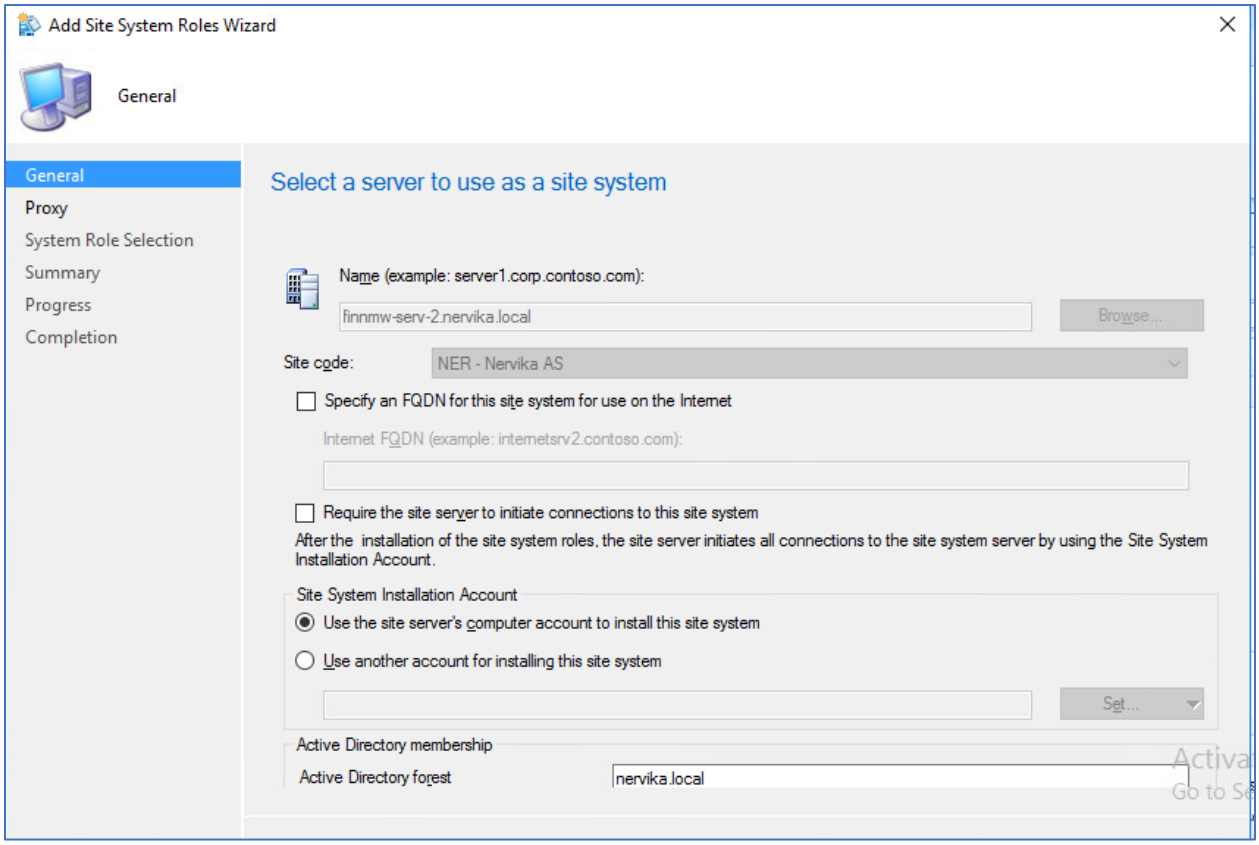


Når installasjonen er ferdig, vil det komme en varseltrekant i Server Manager. Her må vi velge Launch Post-installation tasks.

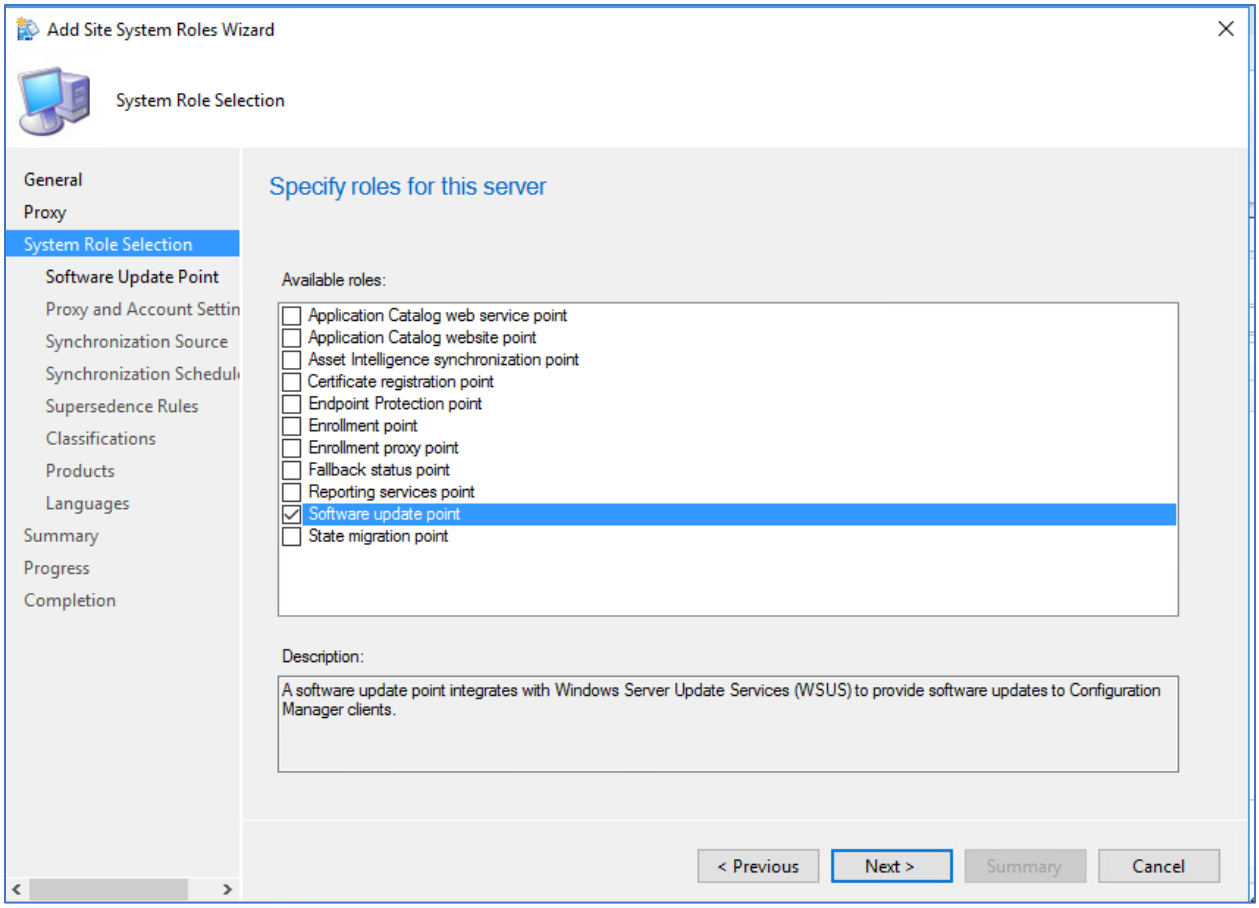


4.2 SUP

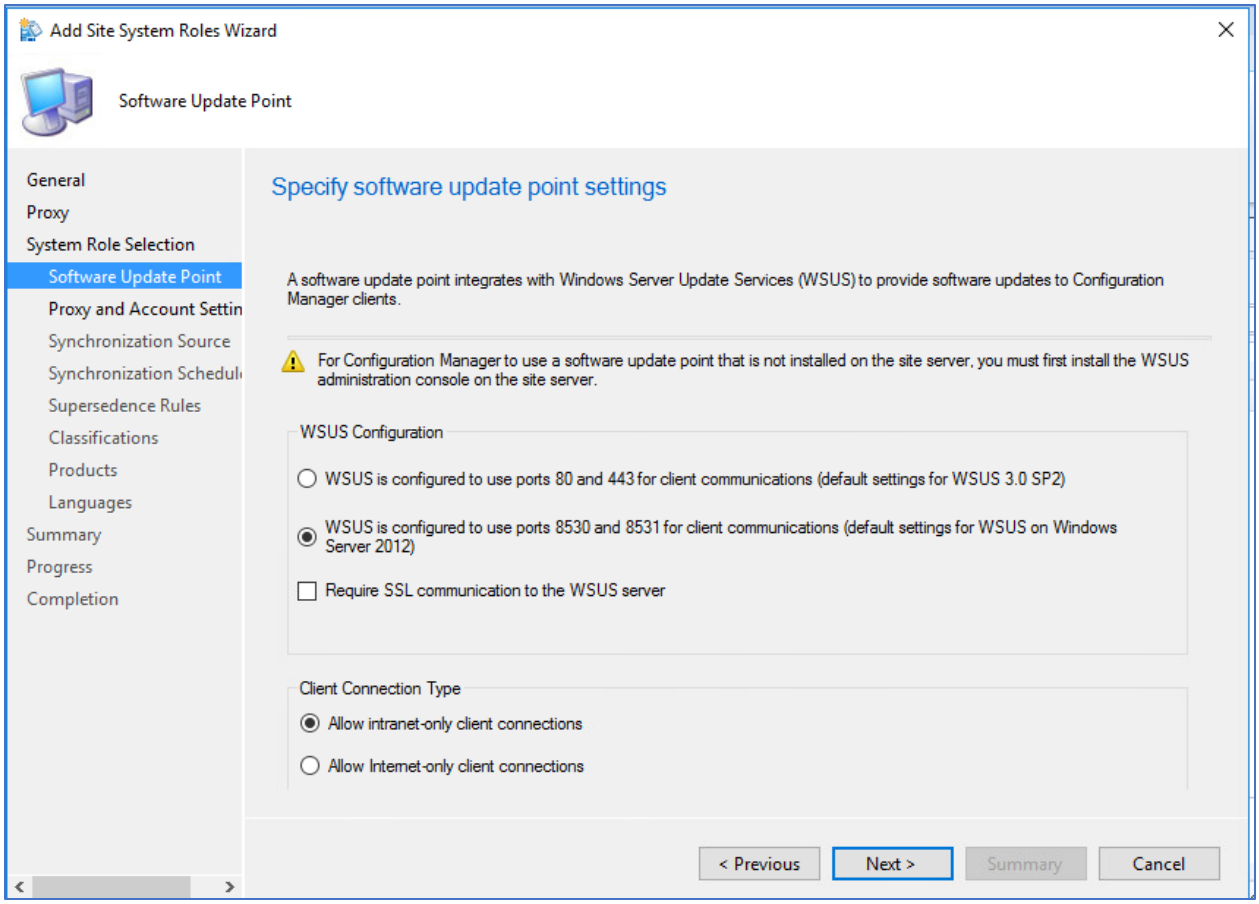
Når WSUS er installert må vi legge inn SUP. Åpne System Center Configuration Manager. I SCCM navigerer vi oss til Administration→Site Configuration→ Servers and site system roles. Her høyreklikker vi på serveren og velger Add Site System Roles. Da skal det komme opp en Add Site System Roles-wizard.



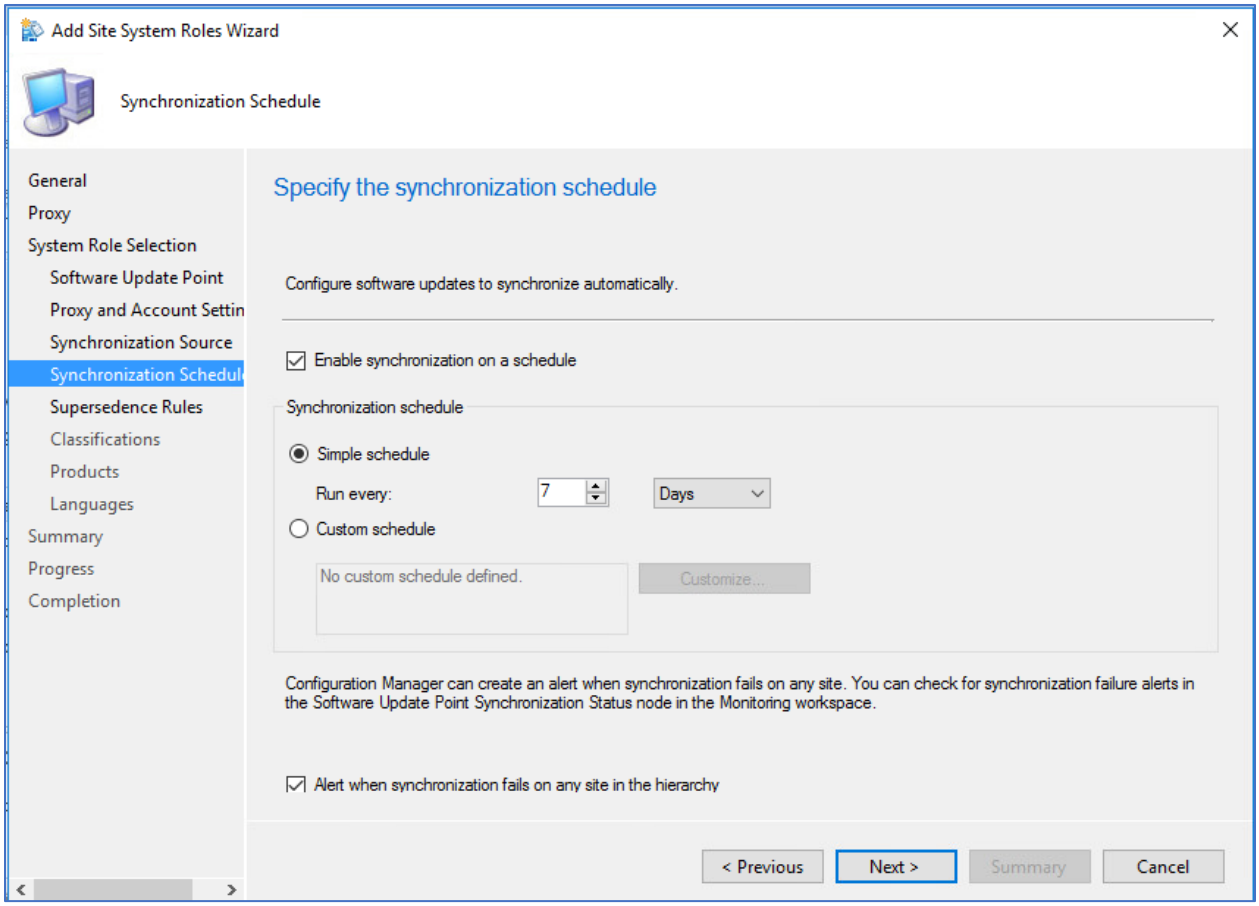
Her navigerer vi oss frem til System Role Selection og huker av Software update point.



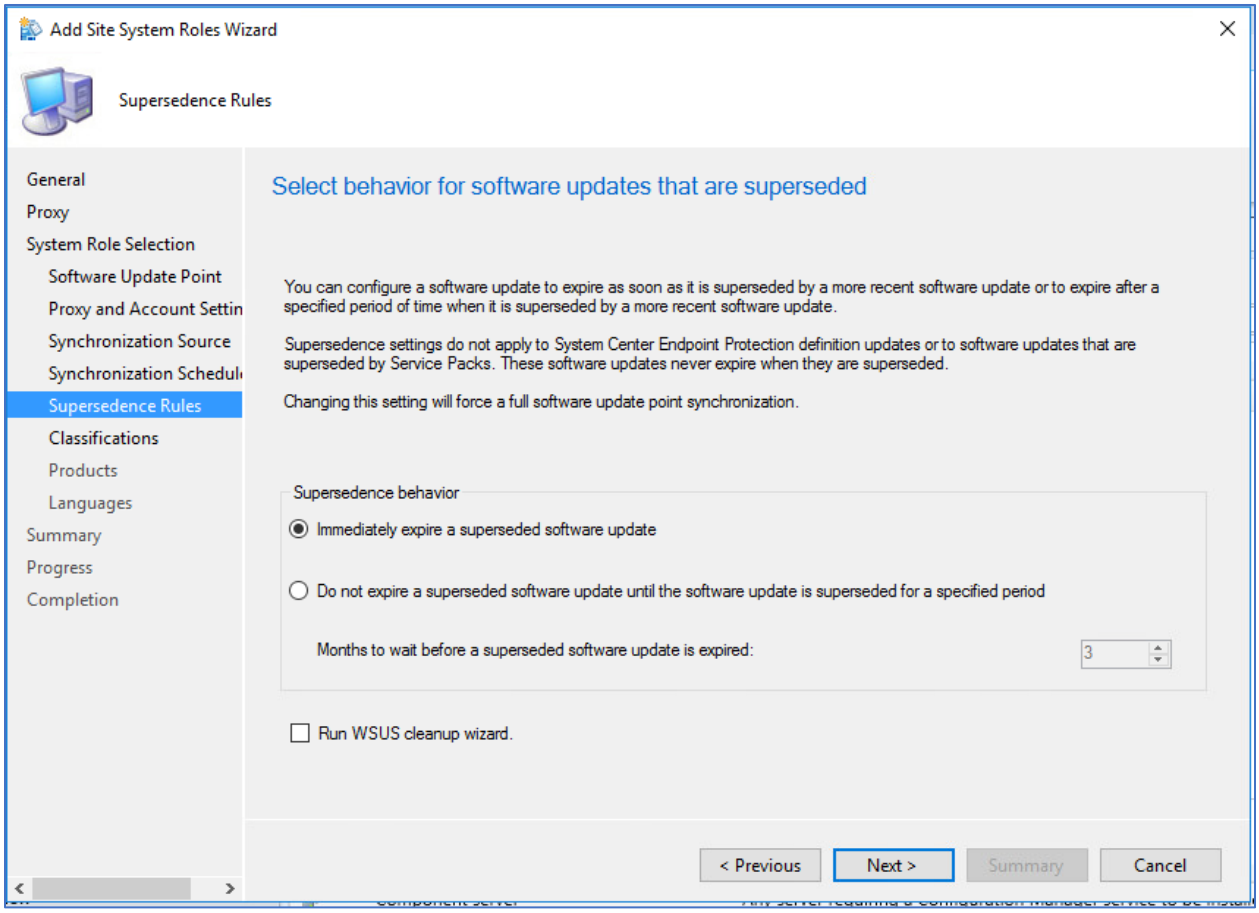
I neste punkt skal vi konfigurere WSUS. Her velger vi å bruke port 8530-8531 og Allow intranet-only client connections.



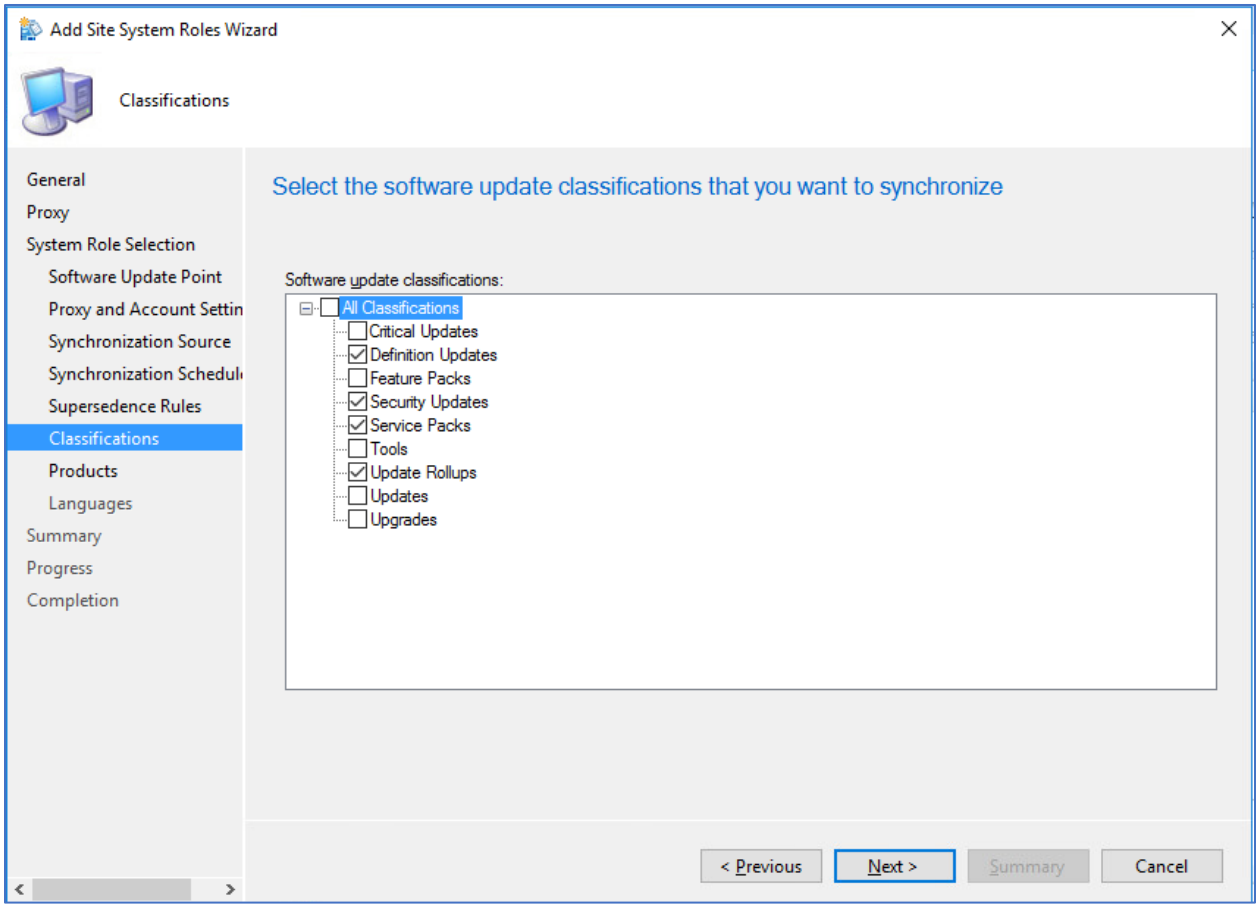
Når vi kommer til valget om hvor ofte vi vil synkronisere oppdateringer, velger vi hver 7. dag.



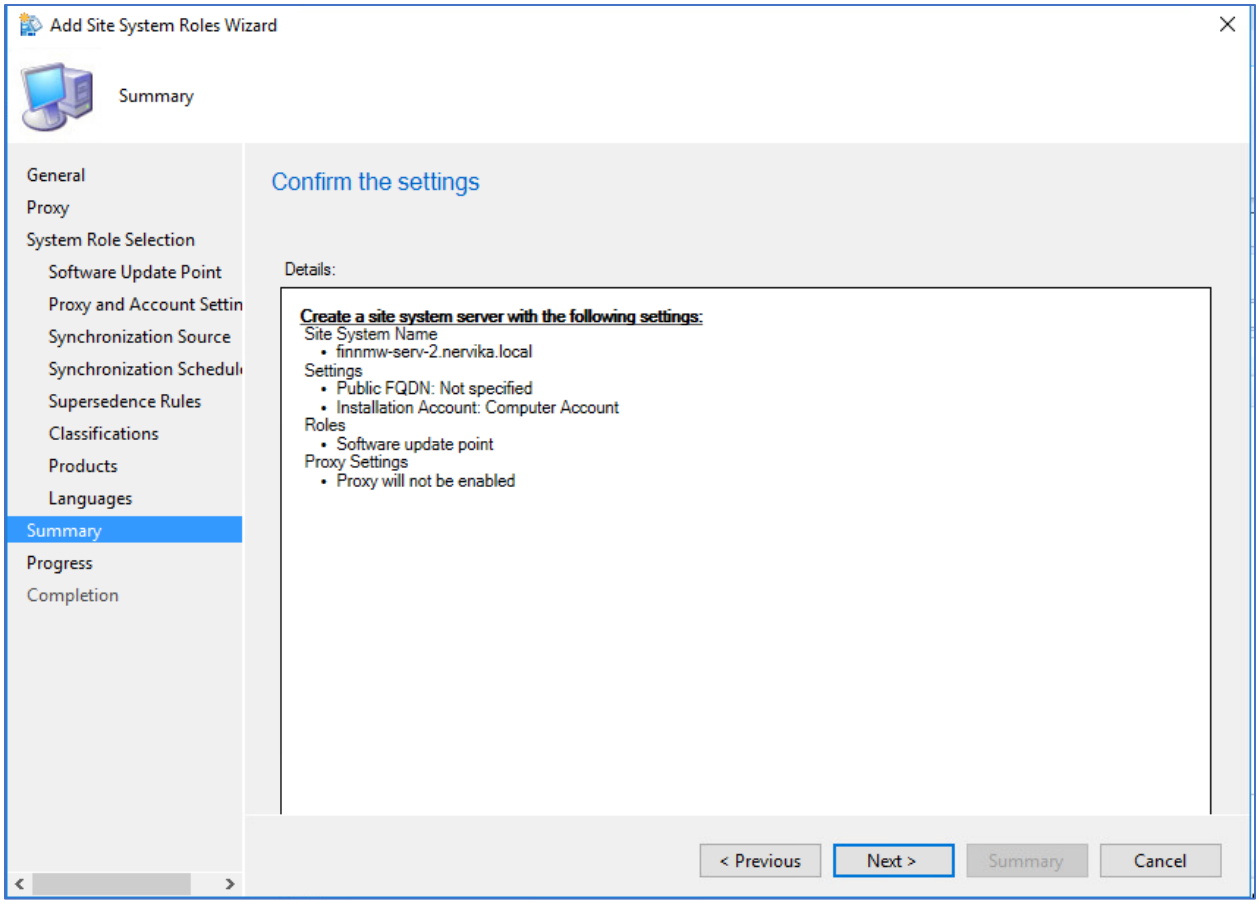
Vi velger også å umiddelbart slette gamle oppdateringer.



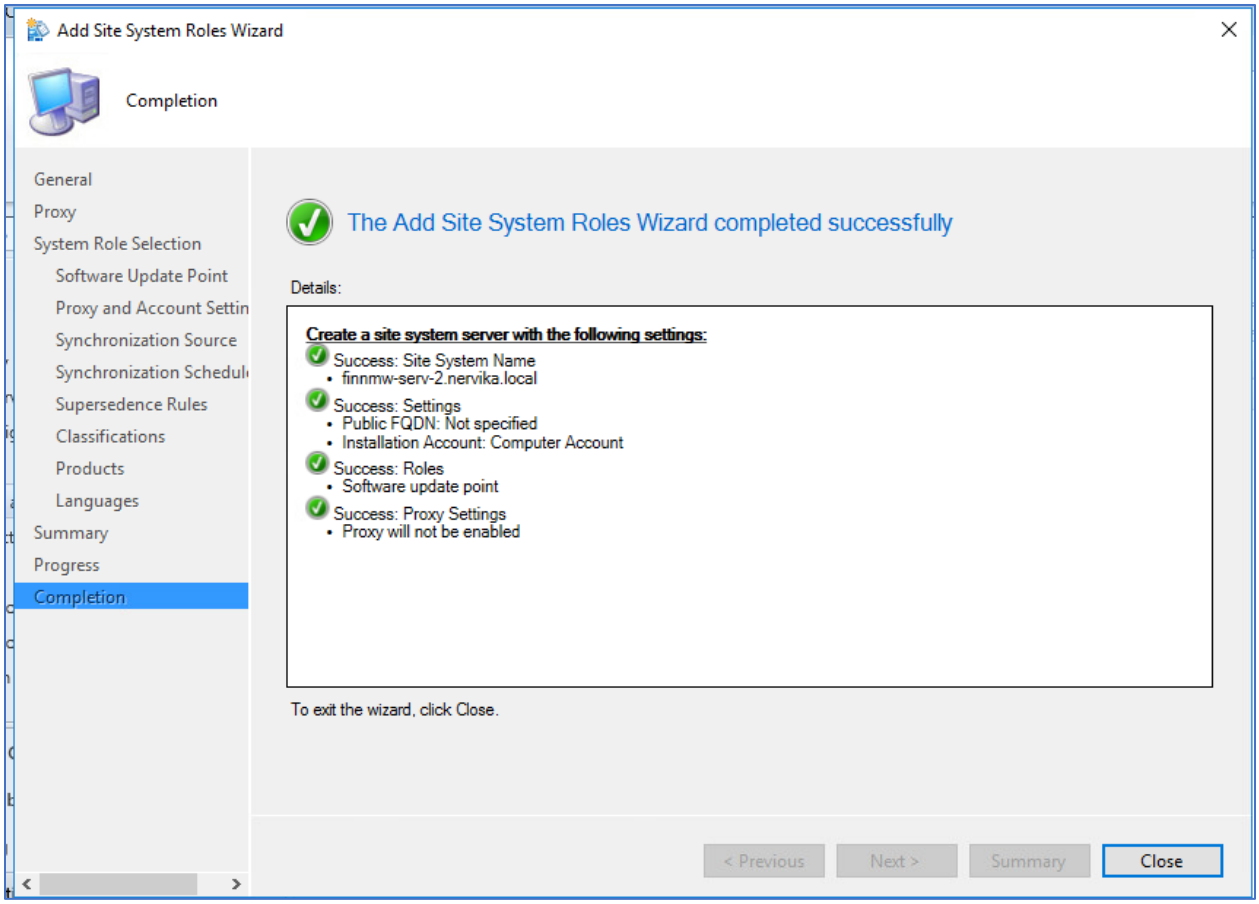
Under Classifications skal vi velge hva som skal synkroniseres. Velger her Defination Updates, Security Updates, Service Packs og Update Rollups.



Foreløpig velger vi ingenting på Products, og under Languages velger vi engelsk. Vi får da opp en oppsummering av valgene vi har gjort, og er klar til å starte installasjonen.



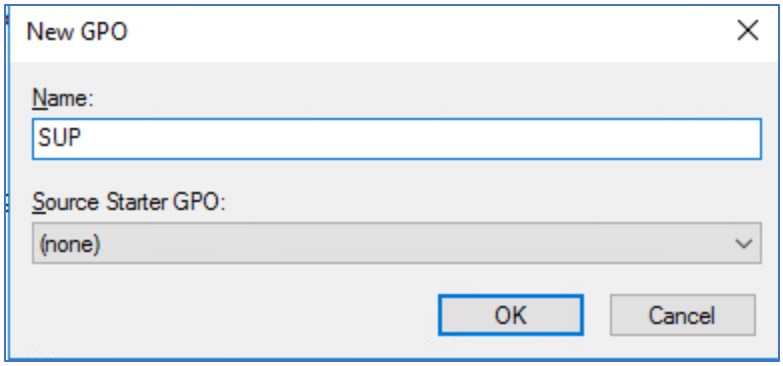
Når installasjonen er ferdig får vi opp en oversikt hvor vi ser at alt har gått vellykket.



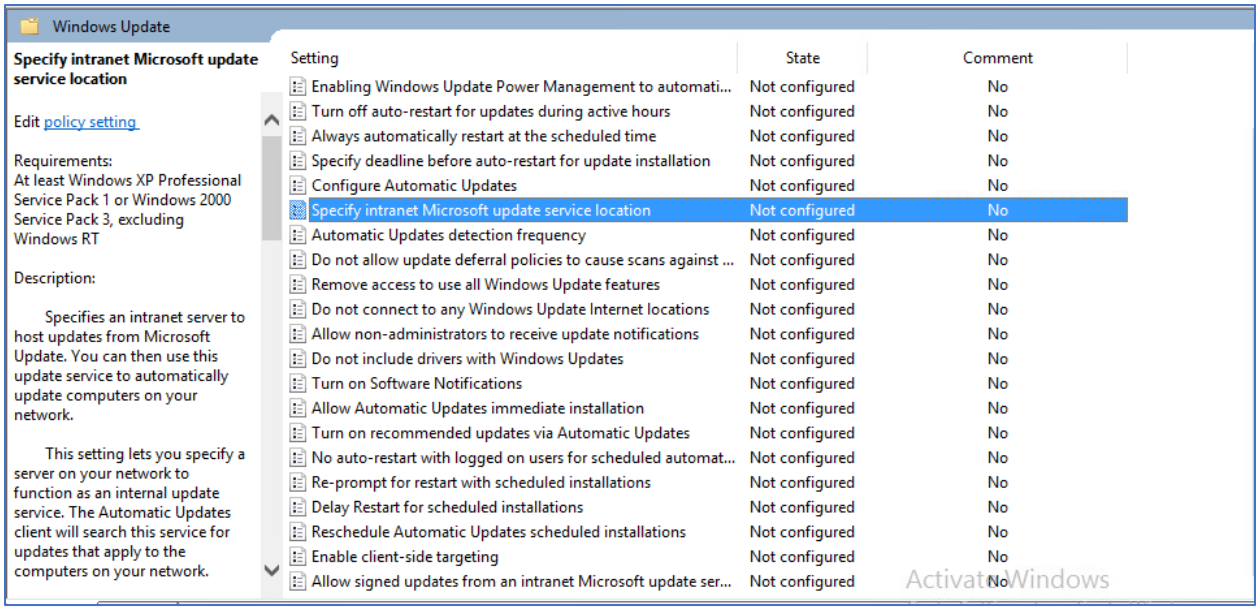
5. Discovery og Boundaries

Først må vi logge inn på AD-serveren. Her skal vi opprette en ny GPO i Group Policy Management. Denne skal hete SUP og skal ligge under nervika.local.

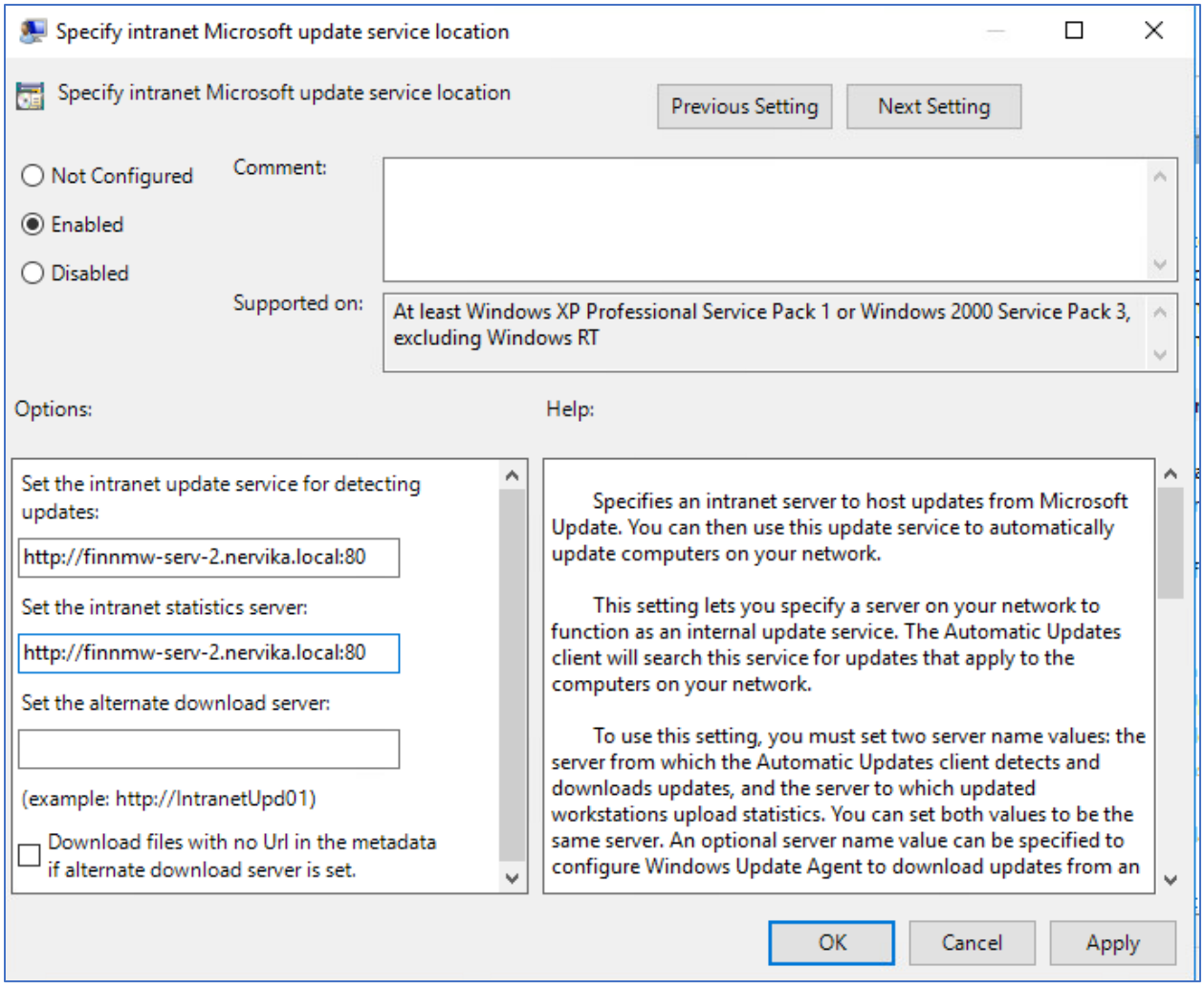
Først må vi åpne Group Policy Management, dette gjøres via Tools i Server Manager. For å opprette en ny GPO navigerer vi oss fra Forest:nervika.local→Domains→Nervika.local. Høyreklikker her på nervika.local og trykker Create a GPO in this domain, and Link it here. Her velger vi å gi GPOen navnet SUP.



Når GPOen er oppretter, høyreklikker vi på den og velger Edit→Computer Configuration→Administrative Templates→Windows Components→Windows Update. Når vi klikker på Windows Update får vi opp en rekke valg. Her skal vi finne Specify Intranet Microsoft update service location.

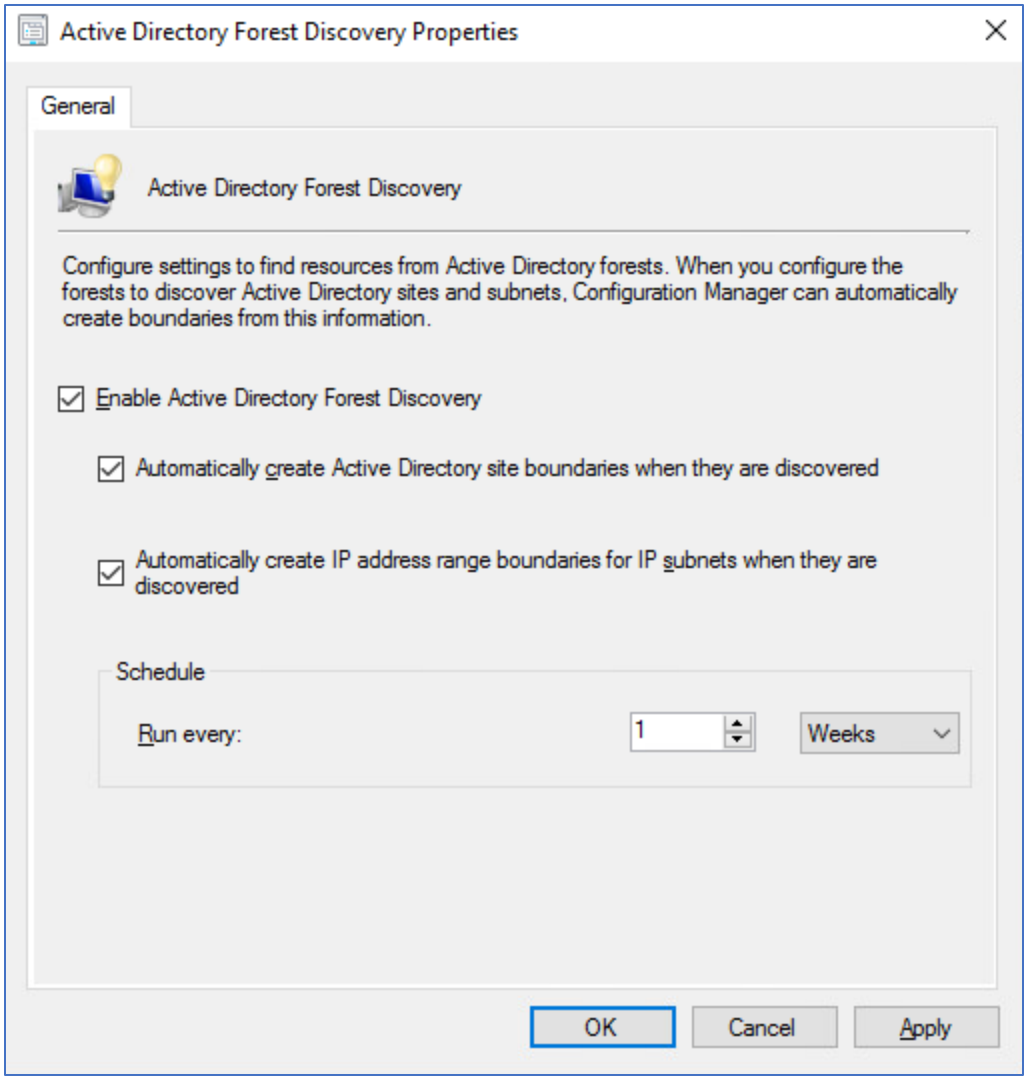


Her skal vi åpne Specify Intranet Microsoft Update Service Location. Inne på den skal vi sette den til å være Enabled. Vi må også adressen til SCCM-serveren og porten som SUP bruker. SUP kjører port 80 som standard.

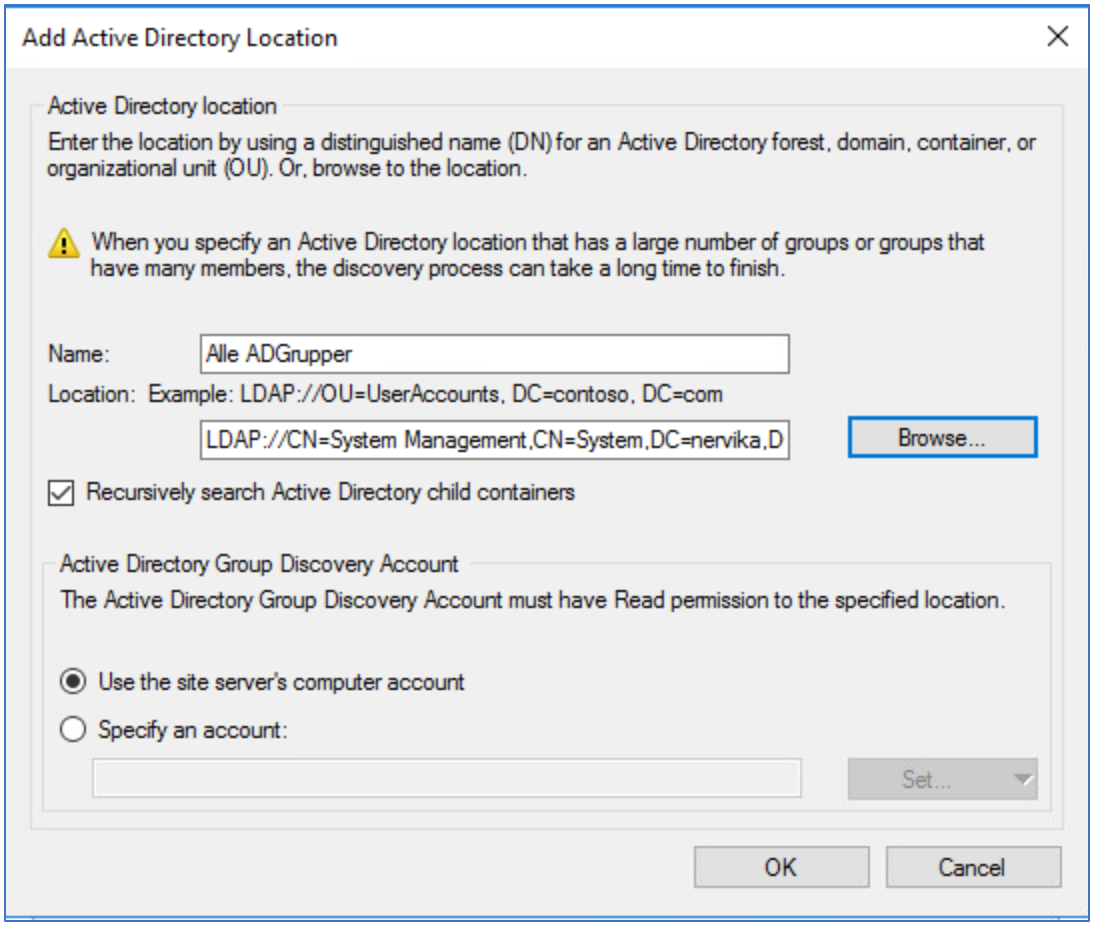


Nå er vi ferdige på AD-serveren, og må logge på SCCM-Serveren som SCCMAdmin. Her skal vi åpne Configuration Manager-konsollen og navigere oss til Administration→Hierarchy Configuration→Discovery Methods. Her skal vi sette alle metodene uten Network Discovery som Enabled.

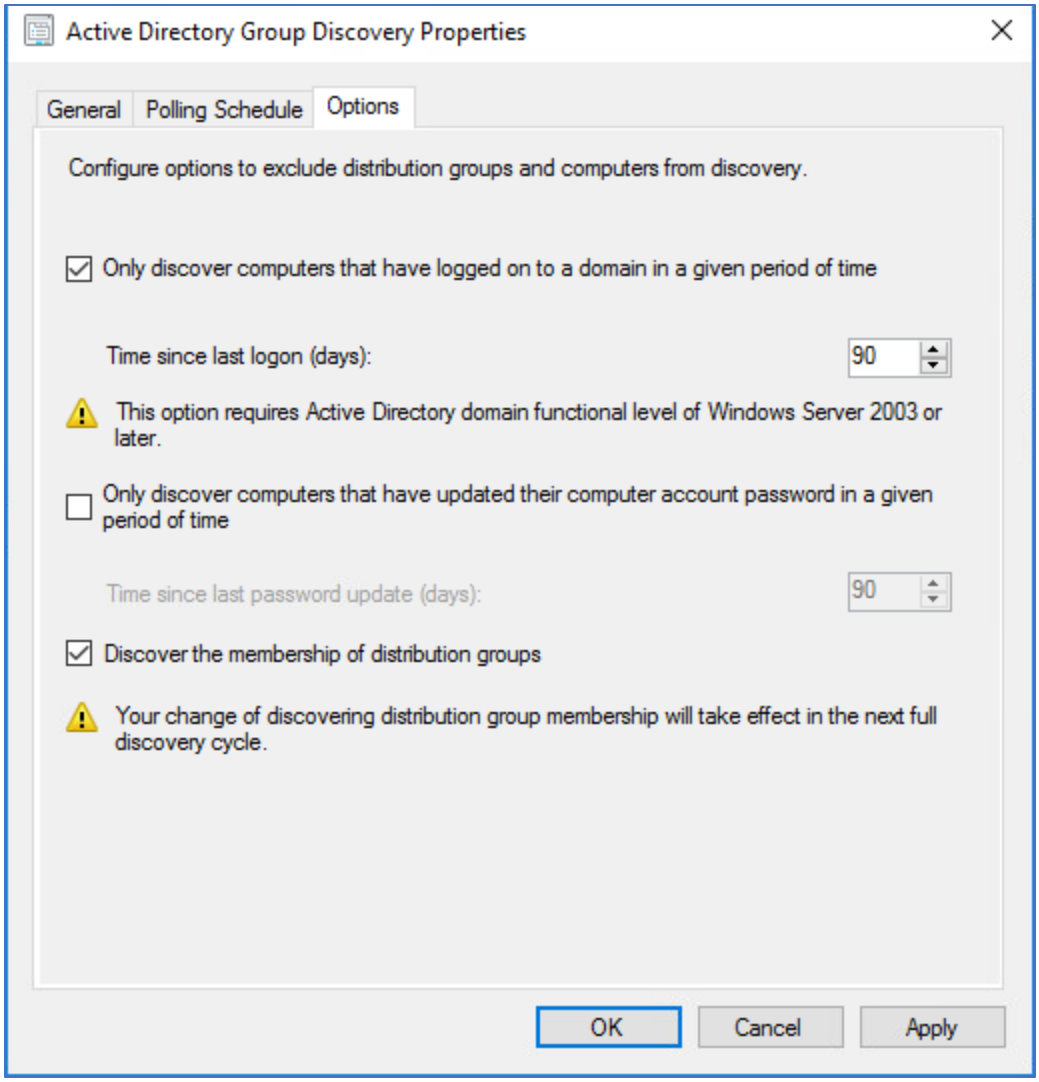
Starter med Active Directory Forest Discovery Properties. Dobbeltklikker på den og huker av enabled og alle undervalg.



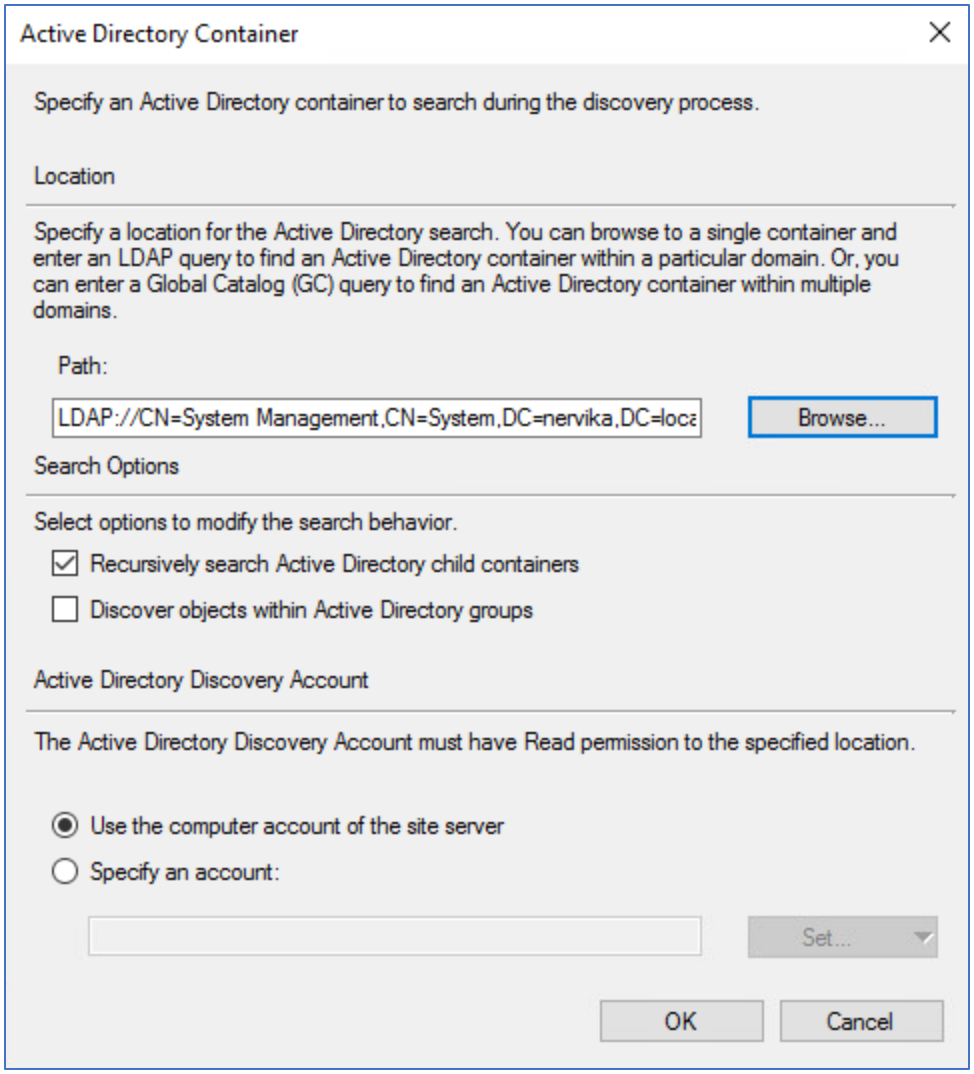
På Active Directory Group Discovery huker vi også av enable. Her skal vi også trykke Add → Locations. Her setter vi Alle ADGrupper som navn, mens vi linker til System Management-containeren vi laget tidligere under Location.



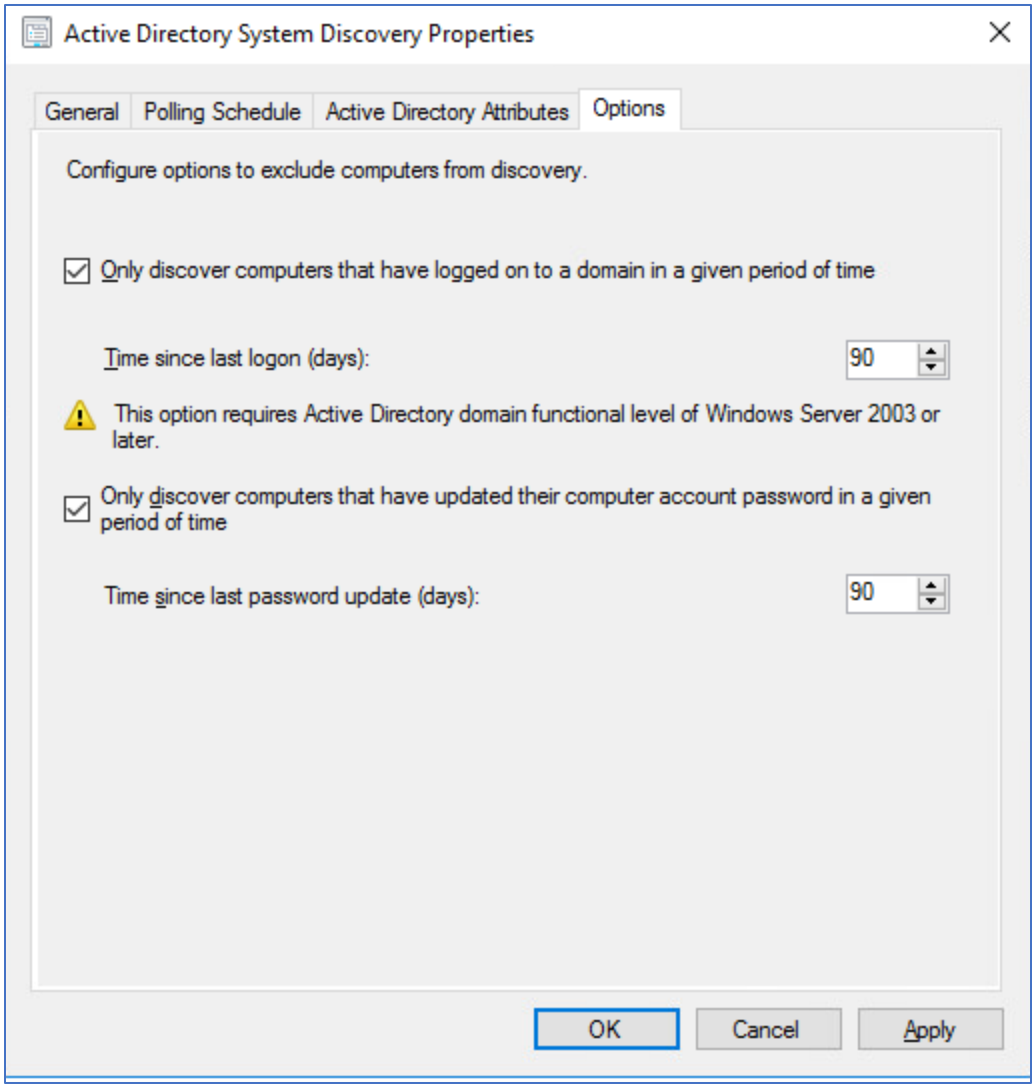
Det neste vi må gjøre er å sjekke at Enable delta discovery er huket av under Polling Schedule. Hvis den er huket av er det bare å gå til den siste fanen, Options. Under Options skal vi huke av Only discover computers that have logged on to domain in a given periode of time. Default tid for dette er 90 dager, som vi bare lar stå. Vi skal også huke av Discover the membership of distribution groups.



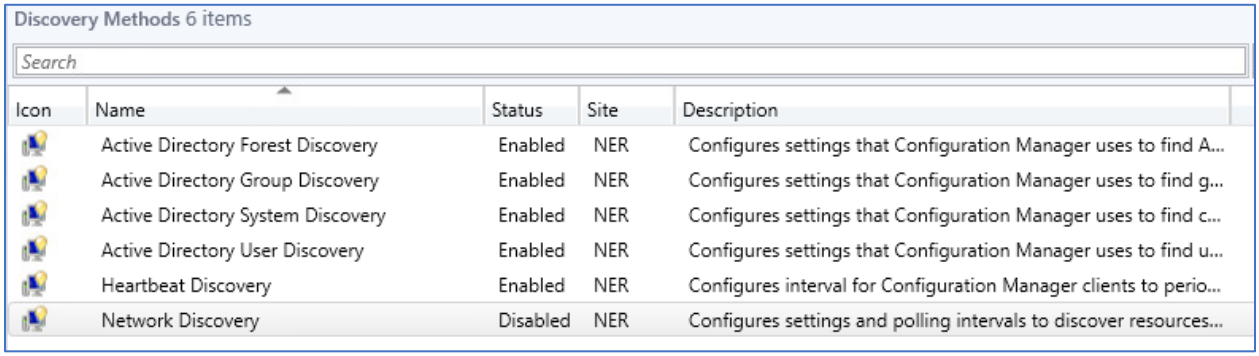
Neste er Active Directory System Discovery Properties. Starter her med å huke av Enable. Når den er Enabled trykker vi den gule solen. Her skal vi igjen linke til System Management-containeren.



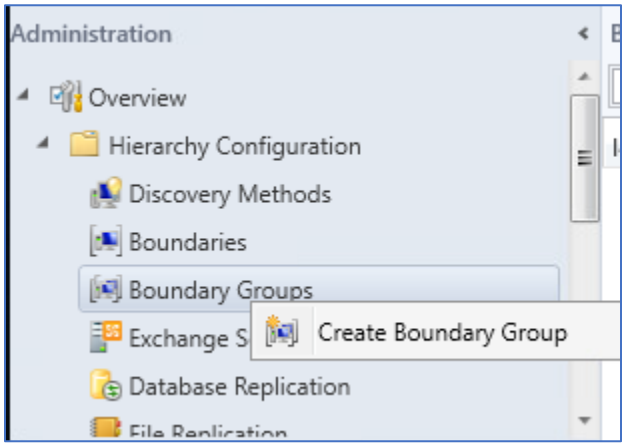
Trykk OK og naviger til Options-fanen. Her skal vi velge de samme innstillingene som vi gjorde under Active Directory Group Discovery.



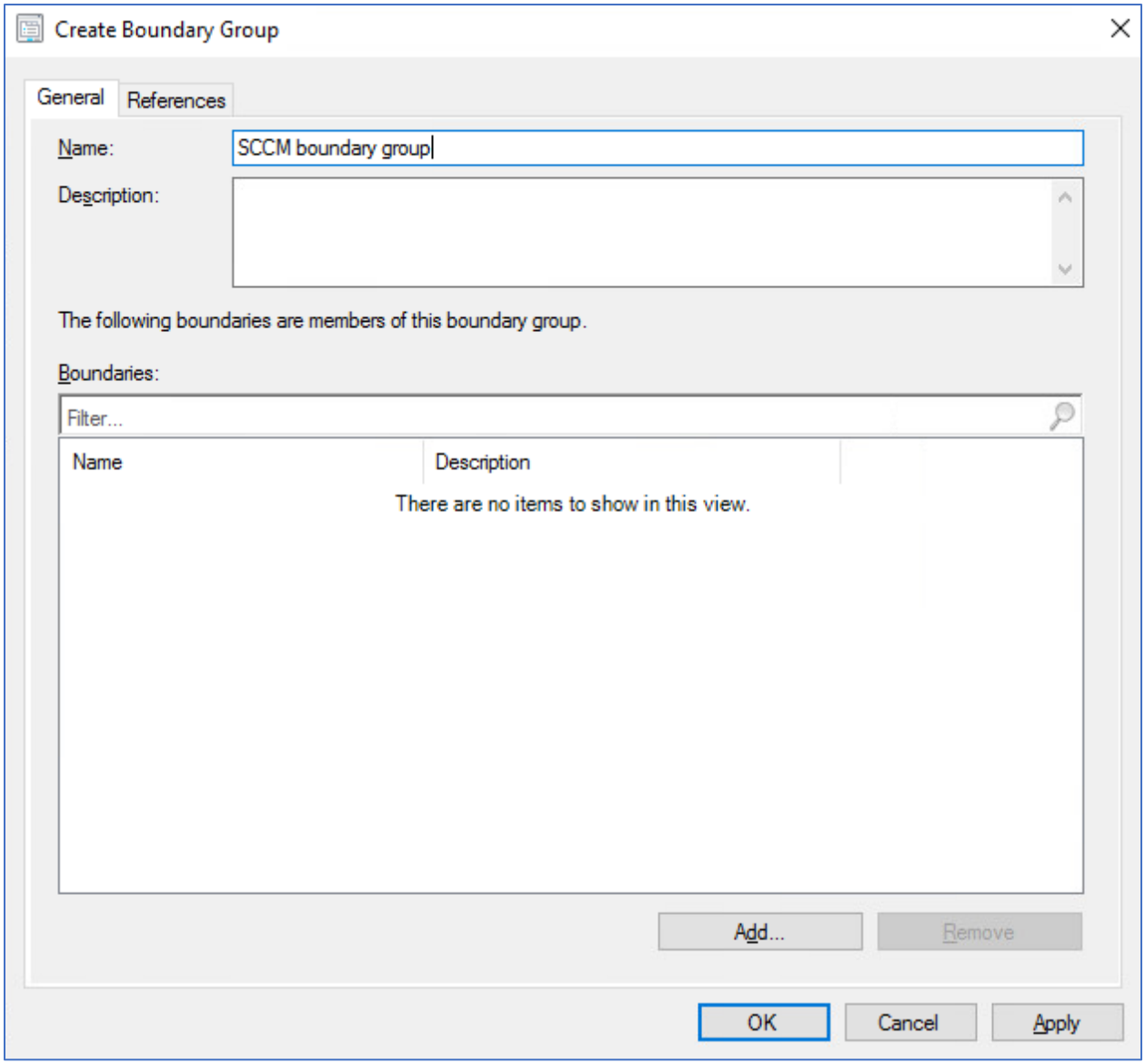
Under Active Directory User Discovery gjør vi akkurat det samme som vi gjorde under Active Directory System Discovery. Nå skal alt uten Network Discovery være enabled.



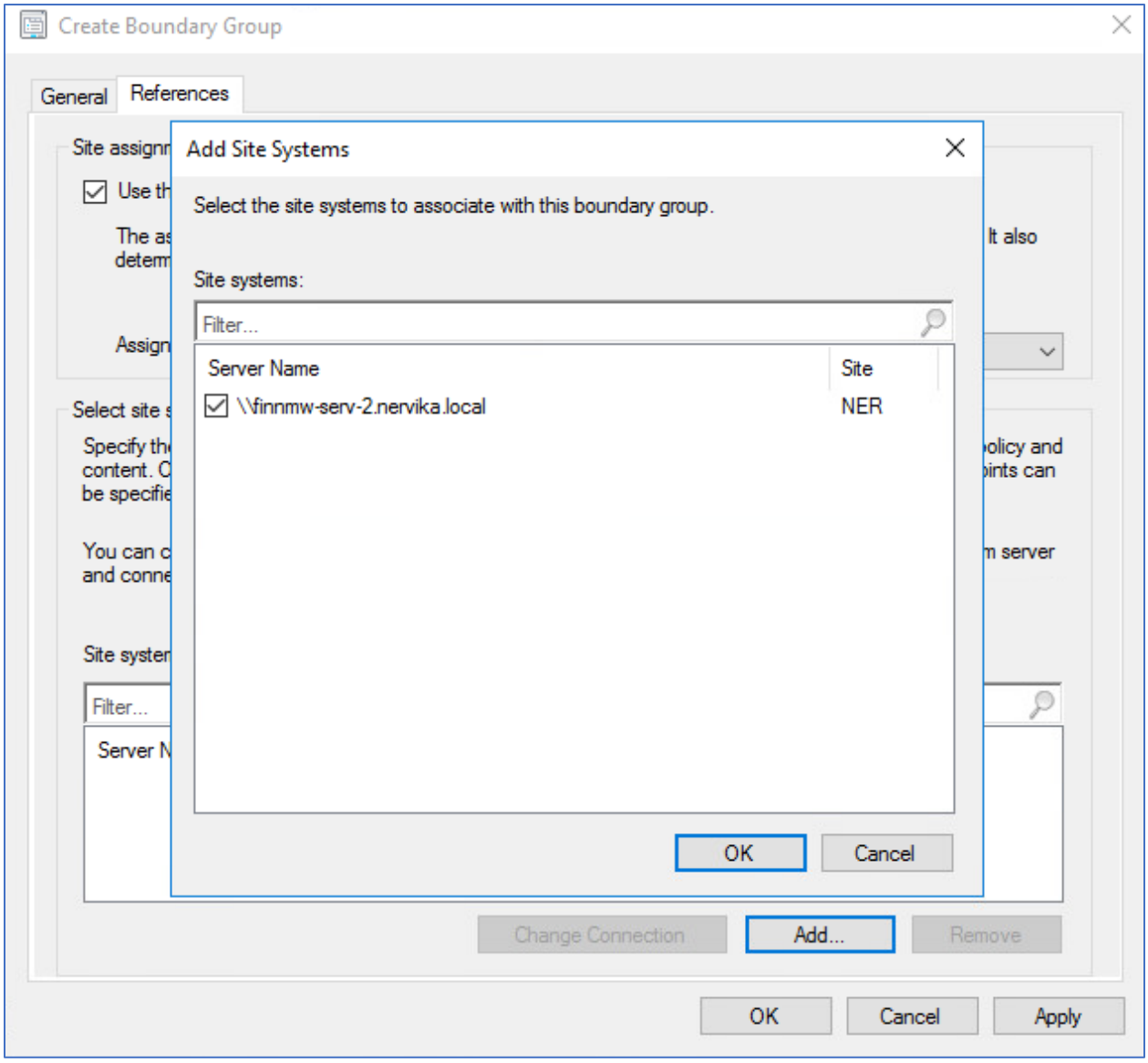
Nå må vi konfigurere boundaries. Det første vi gjør er å opprette en boundaries-gruppe. Fremdeles fra Configuration Manager-konsollen→Administration→Boundaries. Høyreklikker på Boundary Groups og velger Create Boundary Group.



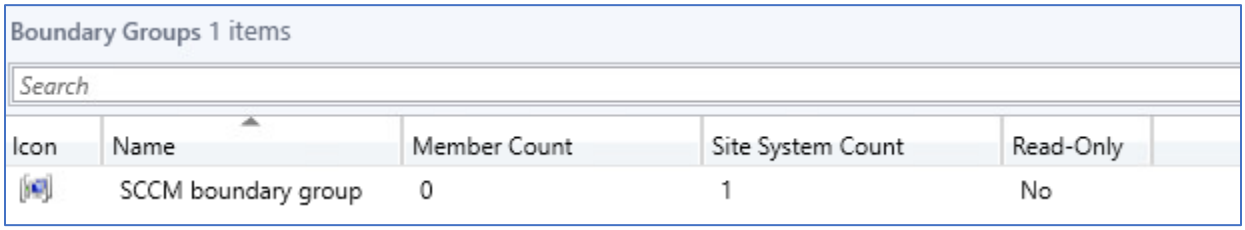
Kaller denne bare for SCCM Boundary Group.



Under fanen References huker vi av Use this boundary group for site assignment. Trykker add og legger til SCCM-serveren.

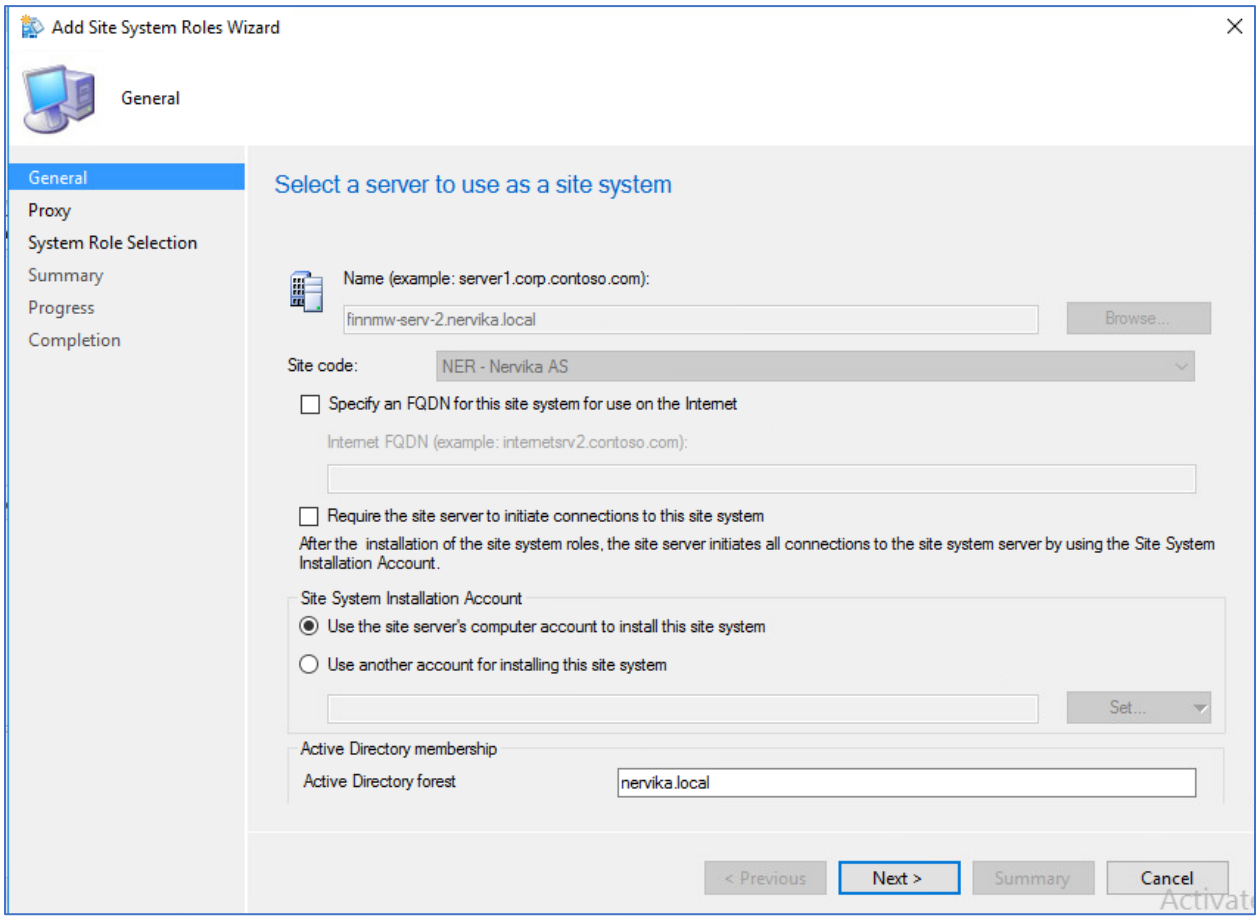


Trykk Apply og OK, så blir Boundary-gruppen opprettet.

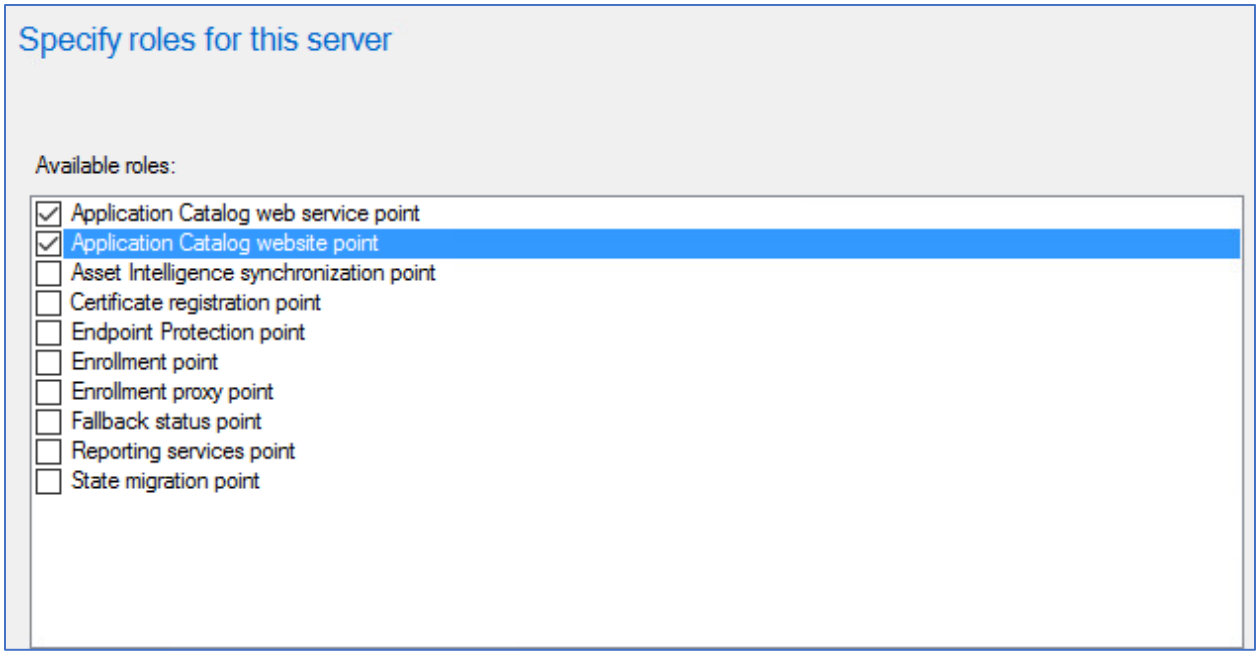


6. Application Catalog Web Service Point

Nok en gang skal vi logge inn på SCCM-serveren som SCCMAdmin. Her åpner vi Configuration Manager-konsollen og velger Administration→ Site Configuration → Servers and Site System Roles. Her finner vi serveren vår listet. Vi høyreklikker på den og trykker Add Site System Roles. Den første siden som møter oss lar vi stå som den er.

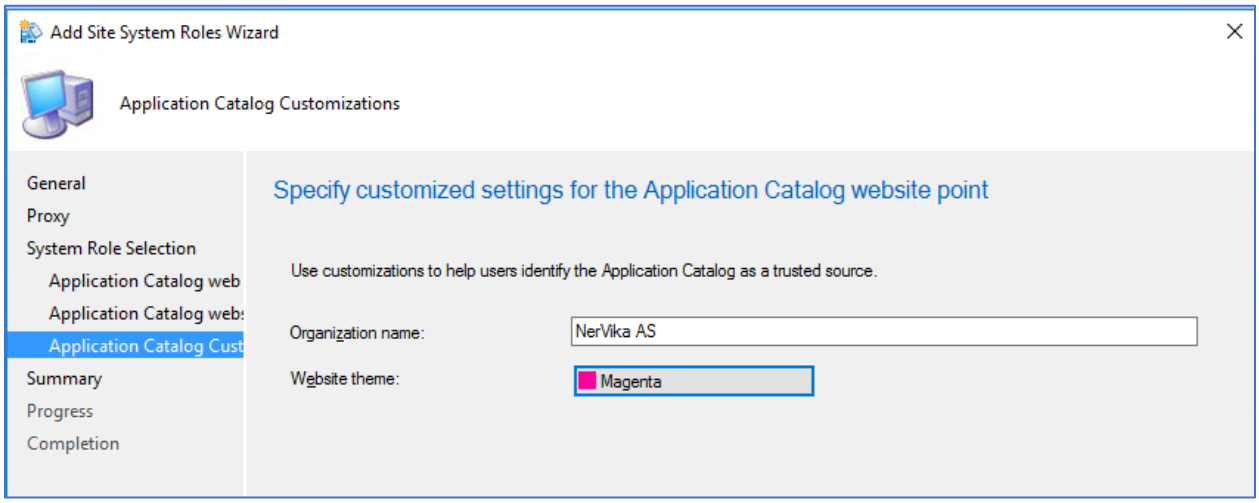


Velger heller ikke å huke av for Proxy i neste steg. Men på Specify roles for this server velger vi de to øverste alternativene, som omhandler Application Catalog.

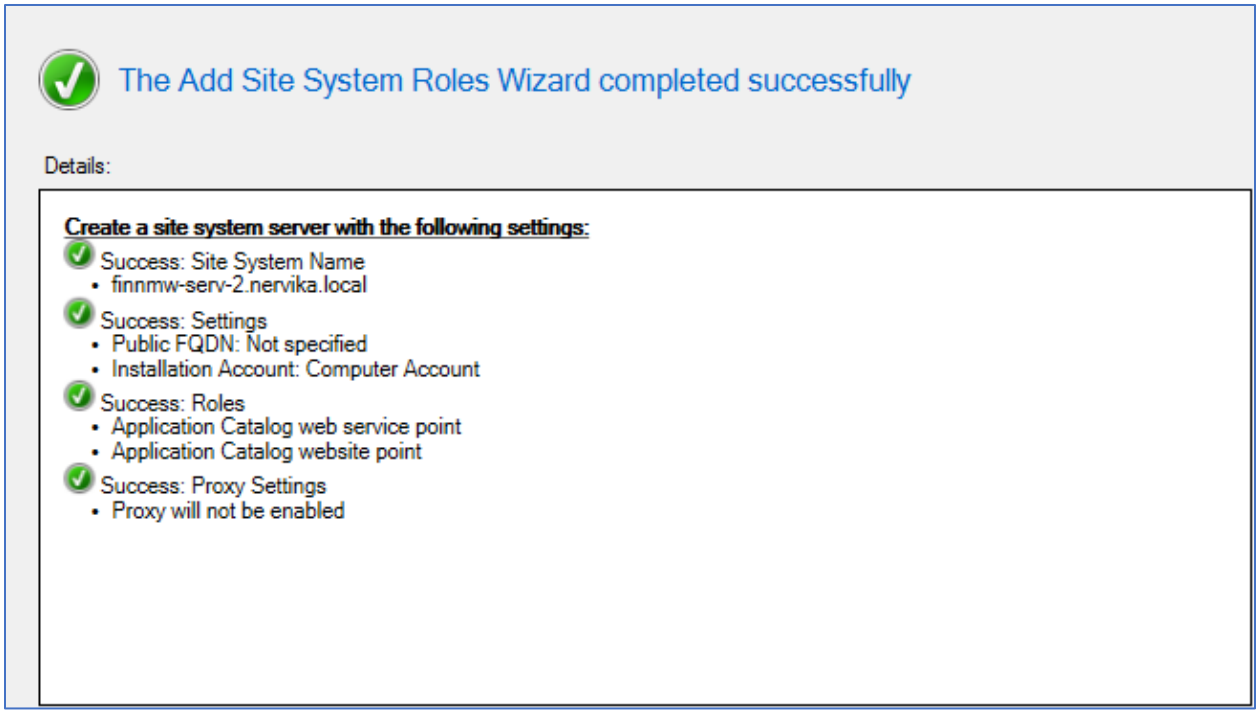


På de to neste stegene trenger vi bare å dobbeltsjekke at det er HTTP som er valgt, og ikke HTTPS.

På den siste siden skal vi bare skrive inn navnet til organisasjonen, og velge en farge som viser at katalogen er trygg.

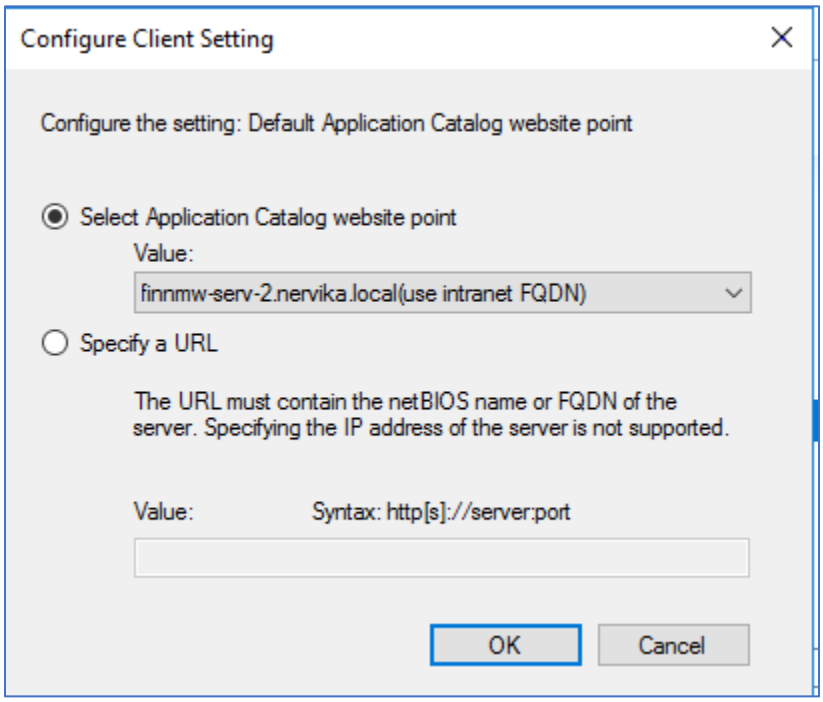


Når installasjonen er ferdig, får vi opp dette bildet:

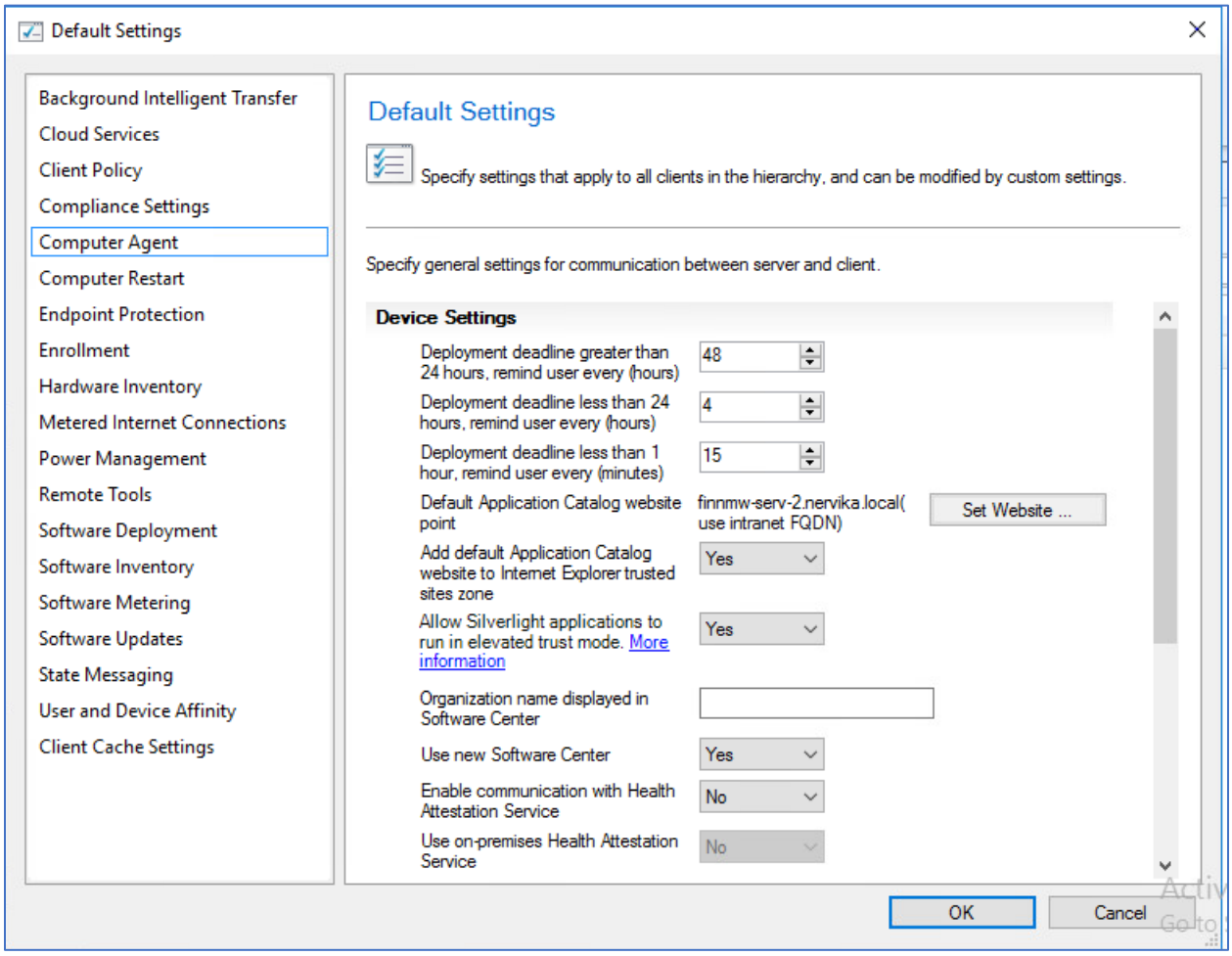


Nå må vi konfigurere Confirguration Manager-klienten. Åpner igjen Configuration Manager-konsollen →Administration→Site Configuration→Default Client Settings→Høyreklikk og Properties.

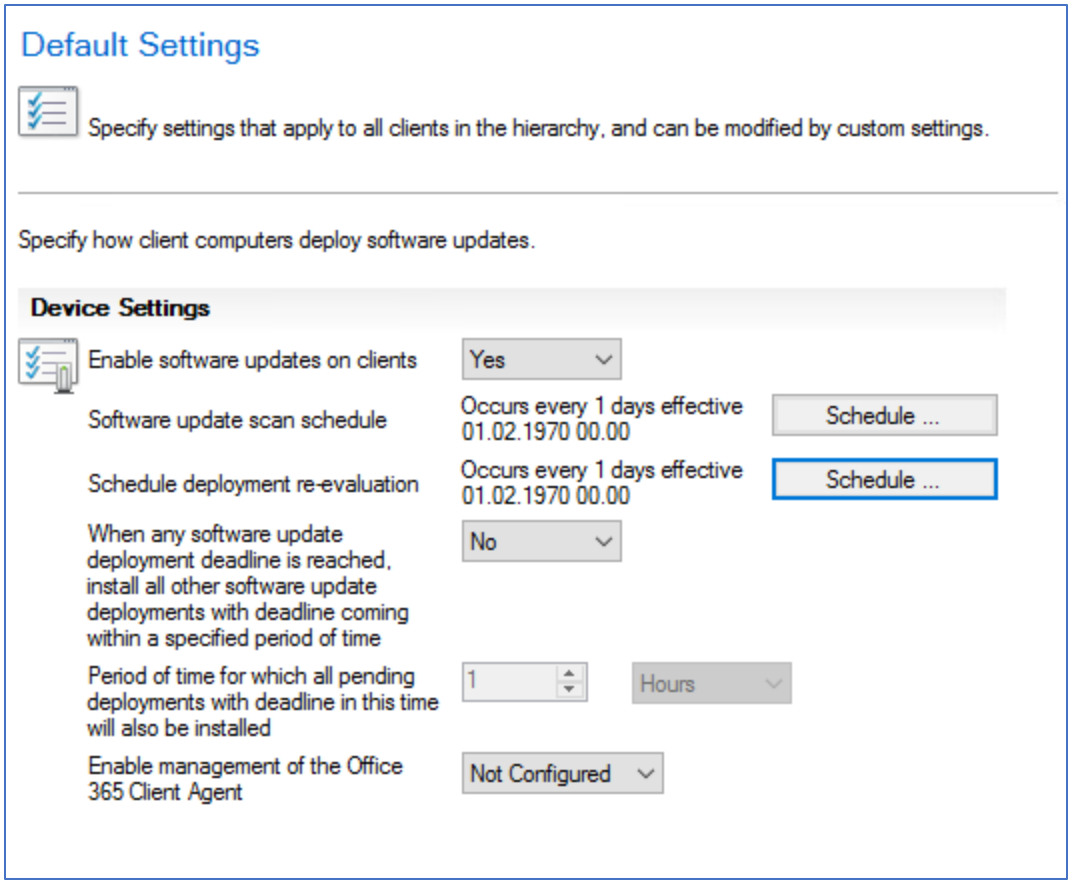
Her trykker vi oss frem til Computer Agent og trykker Set Website. Under Set Application Catalog Website point velger vi serveren vår og Use intranet FQDN.



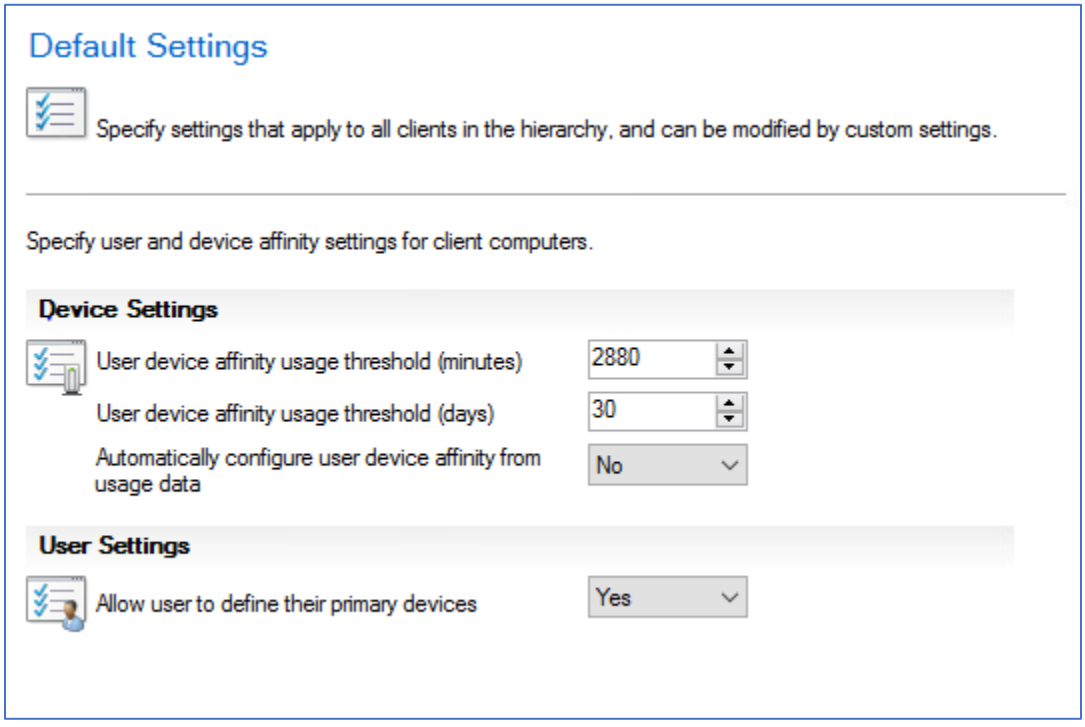
Under Set Website ser vi at Add default Application Catalog Website to Internet Explorer trusted sites zone valgt som “No”. Sett dette til «Yes».



Under Software Updates velger vi å endre intervallet fra hver 7. dag til hver dag.



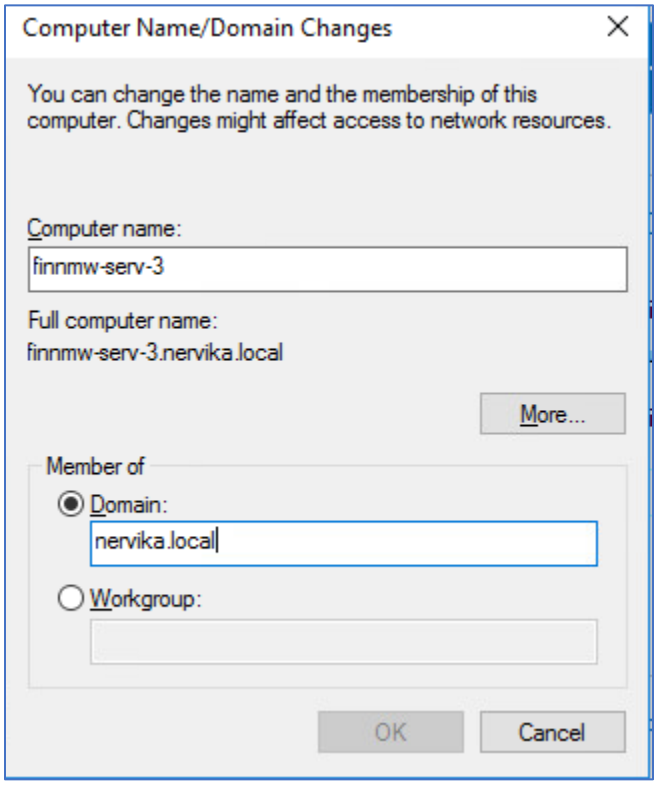
Til slutter trykker vi oss frem til User and Device Affinity. Her velger vi å sette Allow user to define their primary devices til Yes.



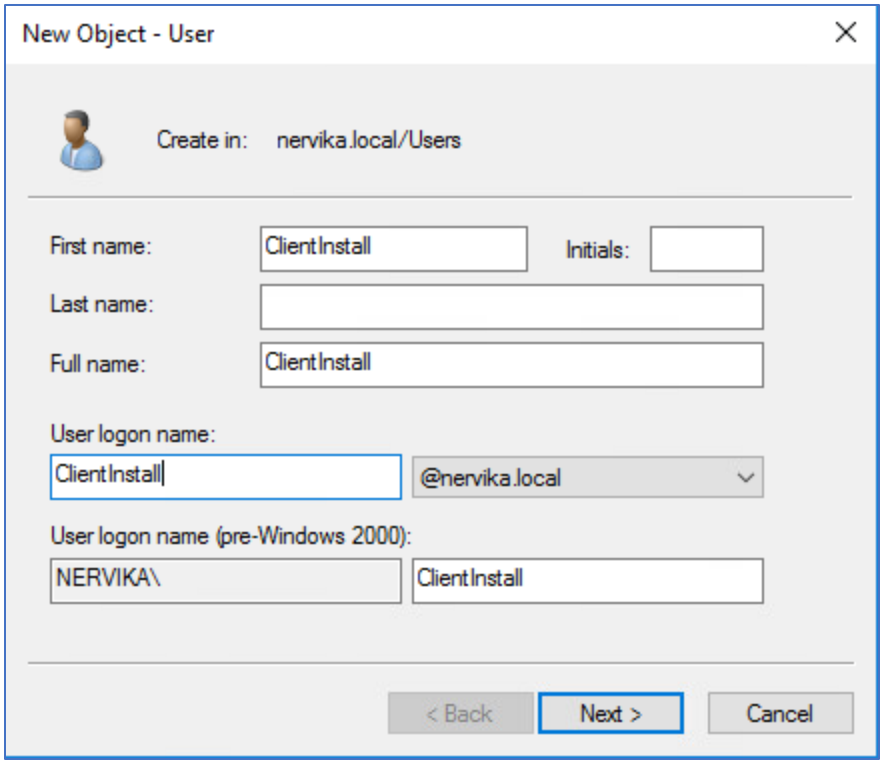
7. Utrulling av Configuration Manager

7.1 Installasjon av klientmaskiner.

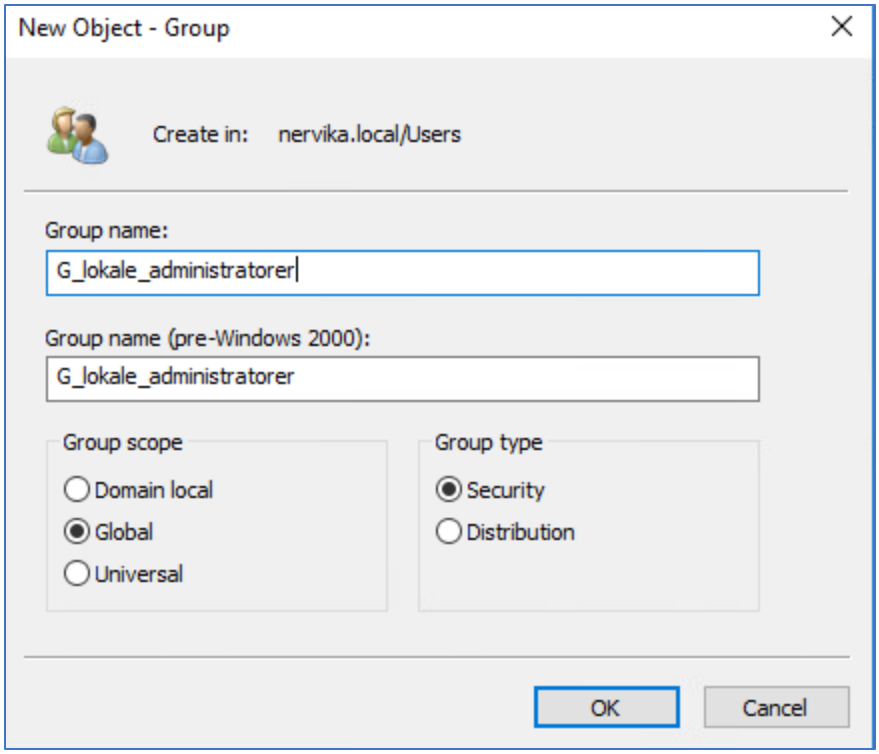
Før vi kan starte med utrulling, må vi opprette noen klientmaskiner. Velger her å opprette en Windows 10-maskin og en Windows 8.1-maskin. Når maskinene er installert må vi melde begge to inn i domenet vårt. Dette gjøres på samme måte som vi har gjort tidligere. Høyreklikk på This PC→Properties→Change→nervika.local.

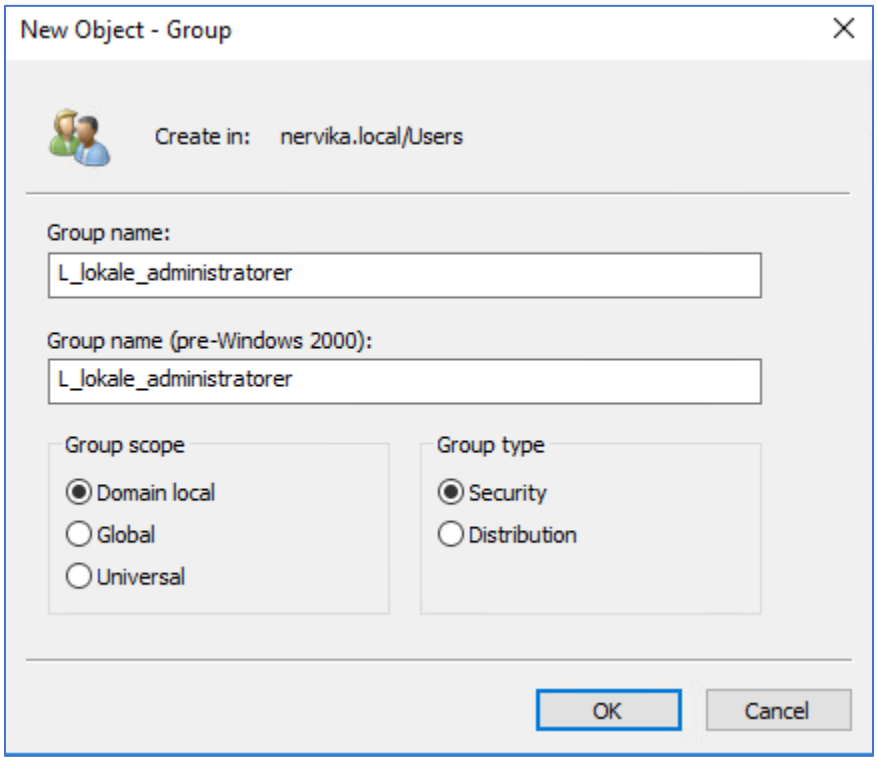


Nå må vi tilbake til AD-serveren og logge inn som domene-administratoren. Her klikker vi oss inn på Active Directory Users and Computers. Her oppretter vi en bruker som vi kaller for ClientInstall.

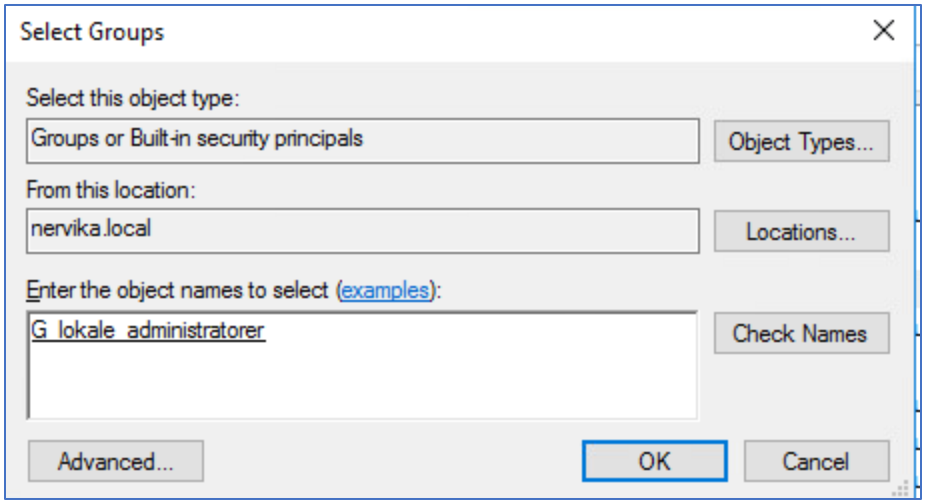


Her skal vi også opprette to sikkerhetsgrupper, en lokal og en global. Den lokale kaller vi L_lokale_administratorer mens den globale kaller vi G_lokale_administratorer.

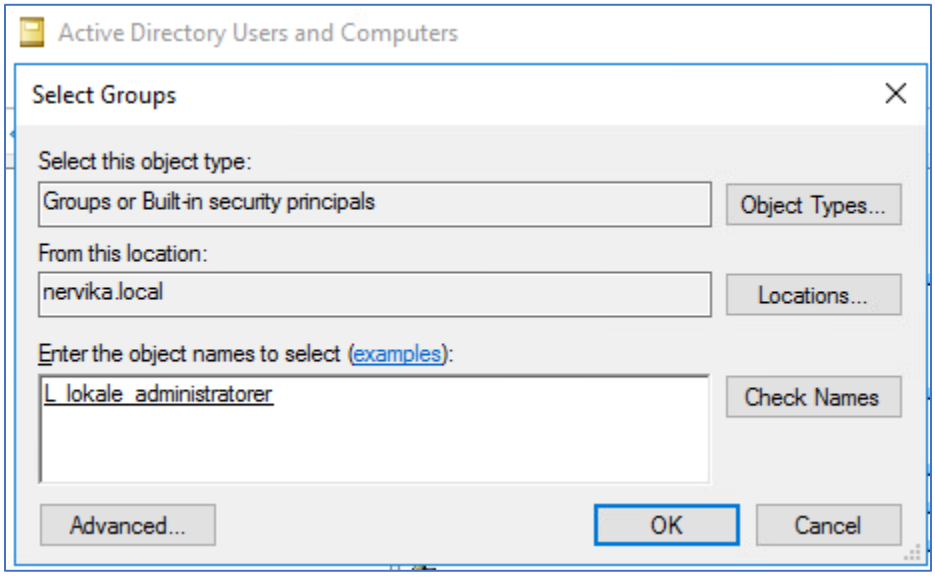




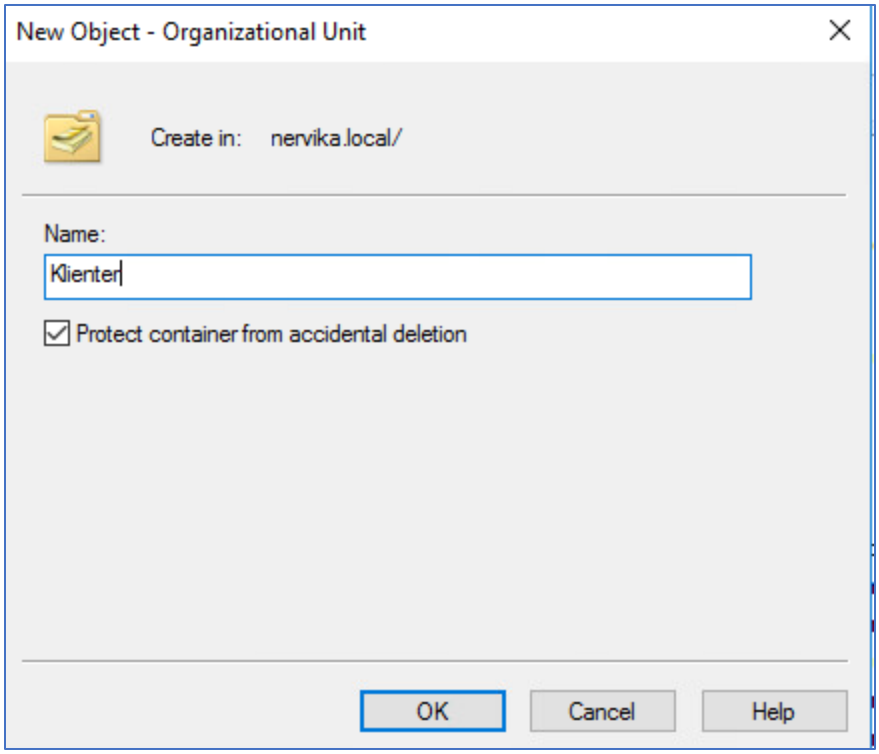
Brukeren ClientInstall som vi nettopp opprettet skal legges inn i den globale gruppen, G_lokale_administratorer. Dette gjøres ved å høyreklikke på brukeren → Add to group.



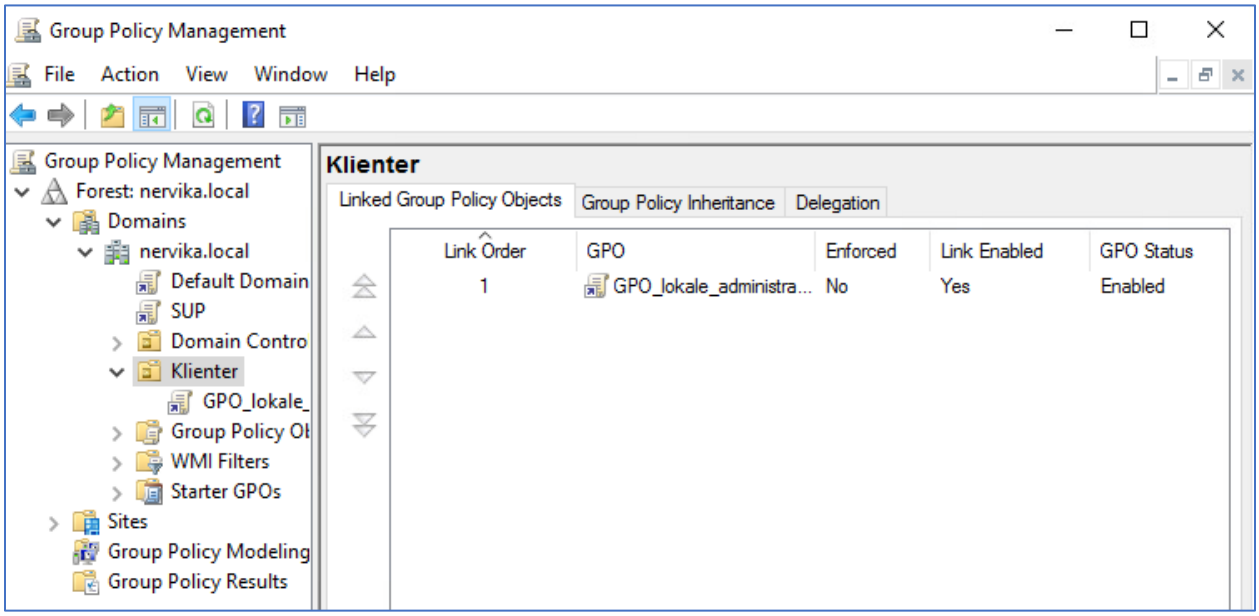
Nå skal vi legge G_lokale_administratorer inn i den andre gruppen, L_lokale_administratorer. Dette gjøres på samme måte, høyreklikk på gruppen→Add to group.



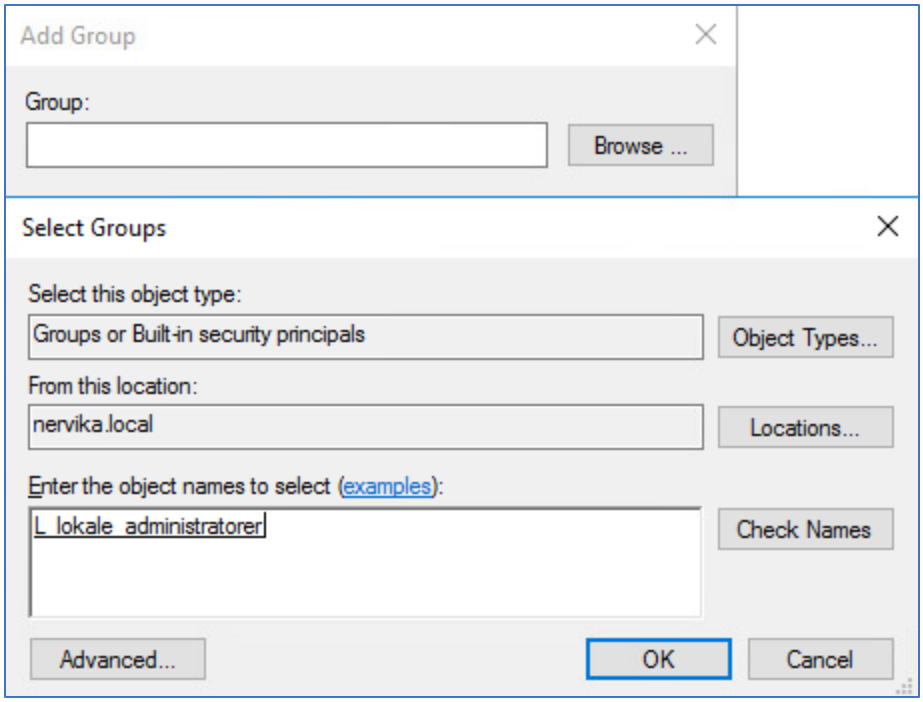
Nå må vi opprette en OU. Velger å kalle den OUen for Klienter.



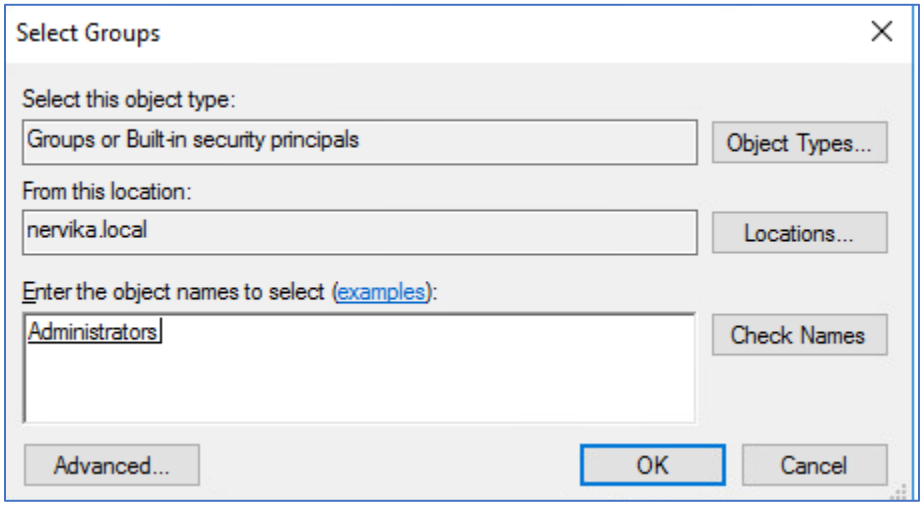
Under denne OUen oppretter vi en ny GPO som vi kaller GPO_lokale_administratorer. Dette gjøres ved å åpne Group Policy Management via Server Manager. Høyreklikk på OUen Klienter og Create a new GPO in this domain, and link it here.



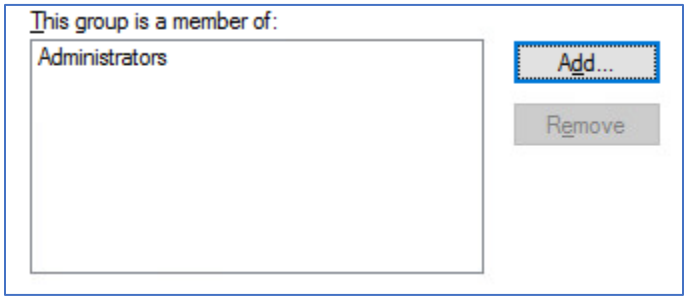
Nå høyreklikker vi på denne OUen og trykker edit. Her navigerer vi oss frem til Computer Configuration→Policies→Windows Settings→Security Settings→Restricted Groups. Høyreklikk og trykk Add Group. Her velger vi browse og finner L_lokale_administratorer.



Nå skal det komme opp et nytt vindu, der trykker vi «Add» under «This group is a member of». Her legger vi til gruppen Administrators.



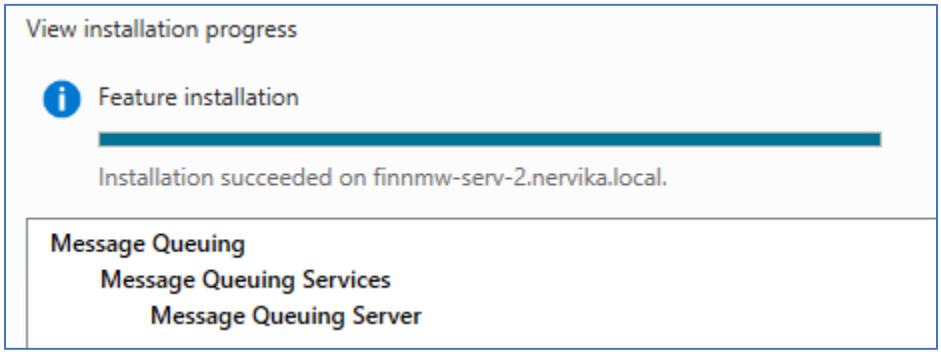
Da skal Administrators komme opp i listen under This group is a member of.



Nå må vi legge klientmaskinene våre inn under OUen Klienter. Dette gjøres ved å dra maskinene fra gruppen Computers til Klienter.

7.2 Endring av brannmurinnstillinger på SCCM-server

Først må vi laste ned rollen Message Queuing Services i Server Manager. Dette gjøres via Add Roles and Features.



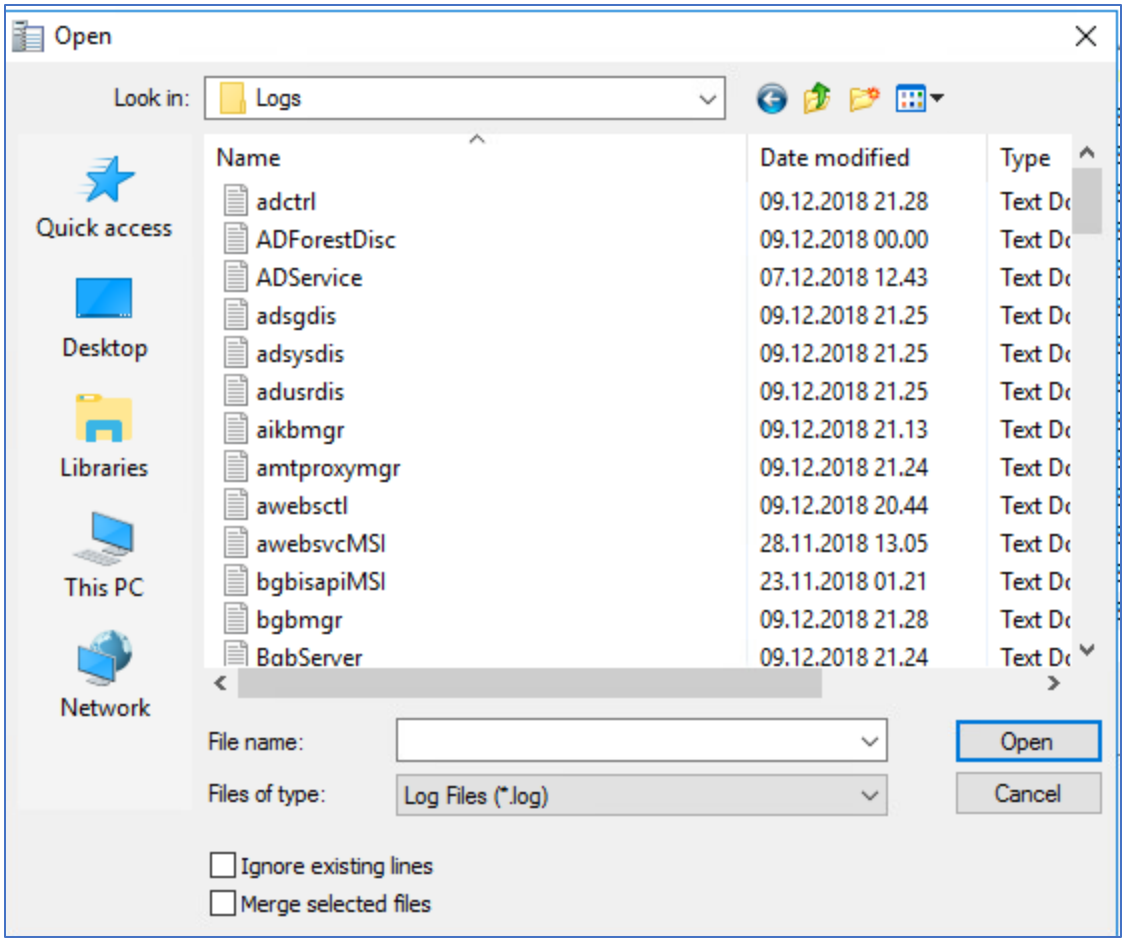
Nå må vi åpne brannmuren. Her måtte vi gjøre to endringer under Allowed apps. Network Discovery og Virtual Machine Monitoring ble lagt til med full tilgang.

7.3 Installasjon av Configuration Manager Trace Log Tool

Før vi starter med utrulling, lønner det seg å laste ned Trace Log Tool. Om det skulle dukke opp nå problemer underveis er det mye enklere å lese loggen her, enn i Notepad.

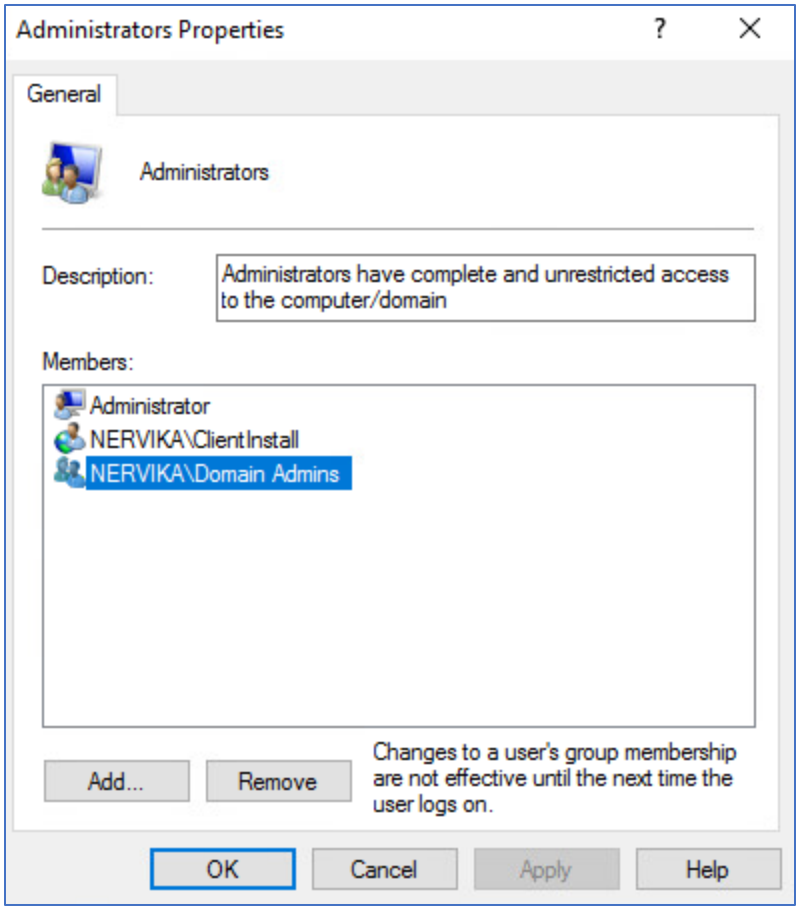
Trace Log Tool ligger på ISO-filen til SCCM. Navigerer oss til ISO-filen og finner mappen SMSSETUP/TOOLS. Her ligger det en fil som heter CMTrace.exe. Kopier så denne over til skrivebordet.

Da er det bare å åpne filen å velge hvilken logg du vil lese.



7.4 Utrulling av Configuration Manager-klienten.

For å installere klienten bruker vi Client Push Installation. Først må vi sjekke at ClientInstall-brukeren er lokal administrator på maskinene som klienten skal rulles ut til.

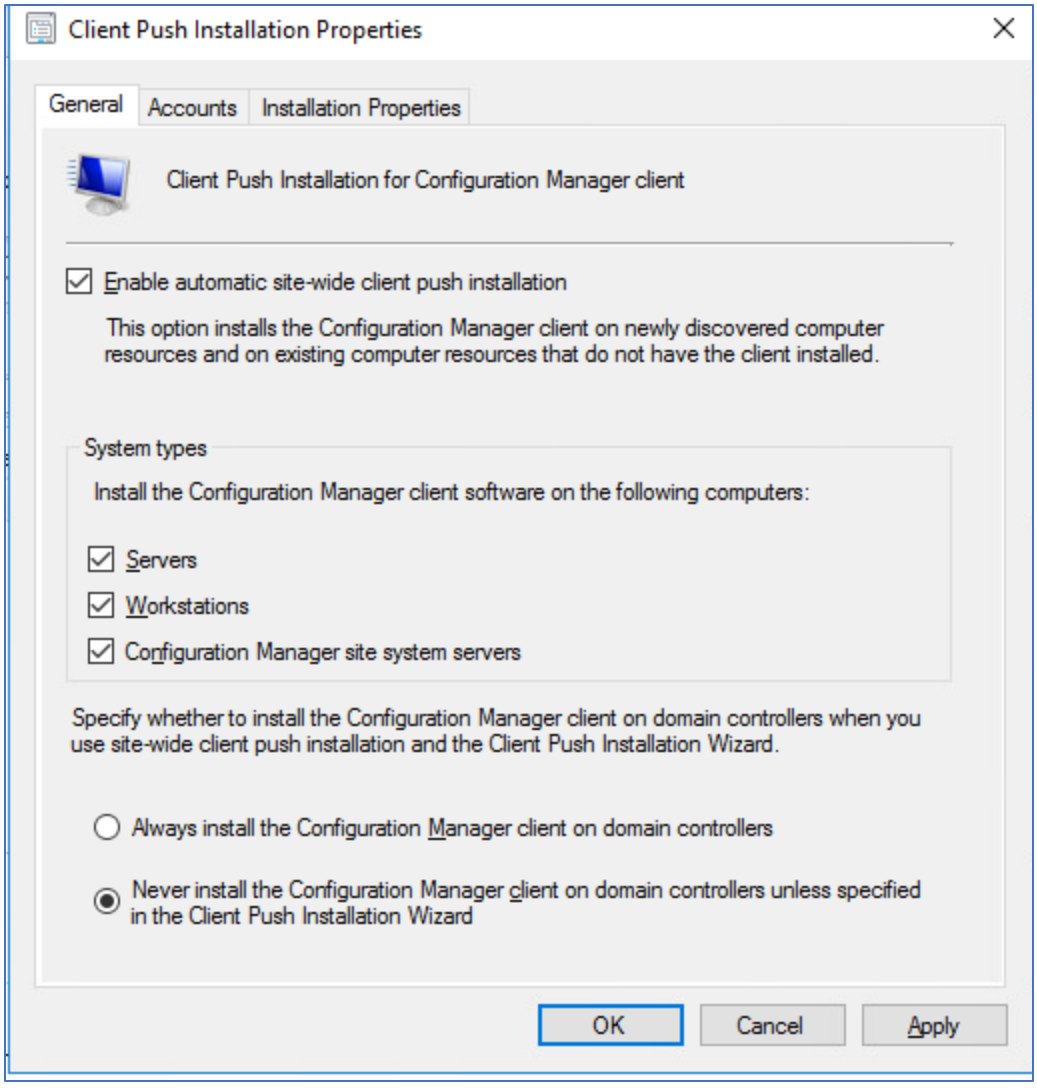


På klientmaskinene må vi også tillate noen regler i brannmuren.

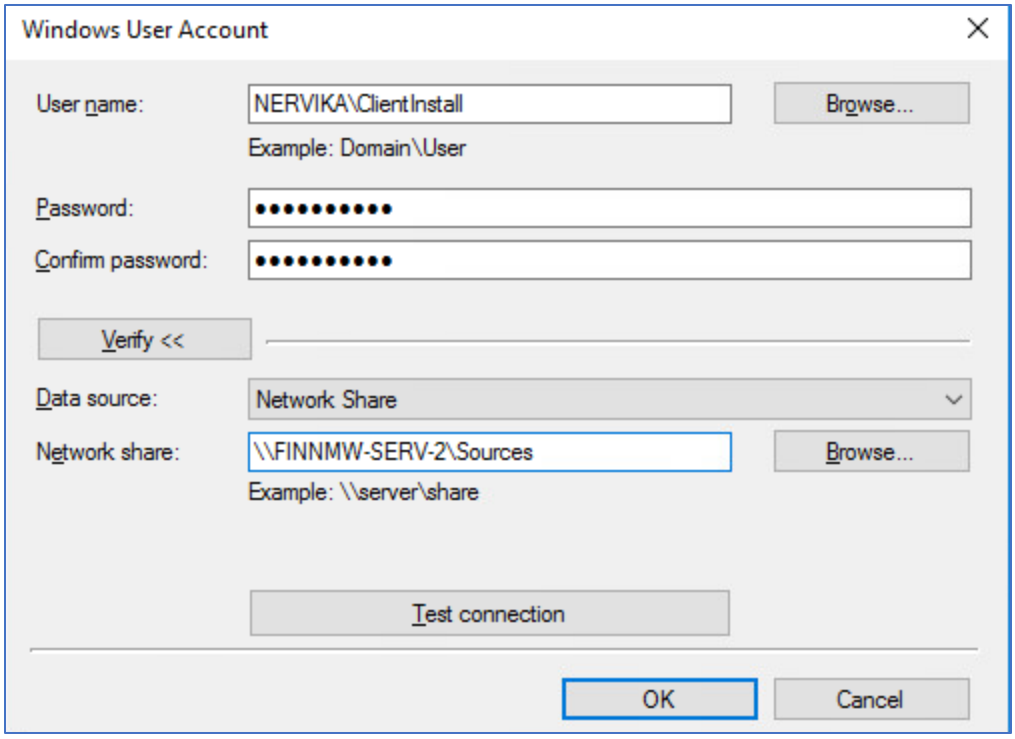
File and Printer sharing skal ha tillatt på inbound og outbound rules, mens Windows Management Instrumentation skal ha tillatt på inbound rules. Dette gjøres via Advanced Security i Windows Firewall.

Nå må vi logge på SCCM-serveren som SCCMAdmin og åpne Configuration Manager. Her navigerer vi oss til Administration→Site Configuration→Sites→Client Installation Settings → Client Push Installation.

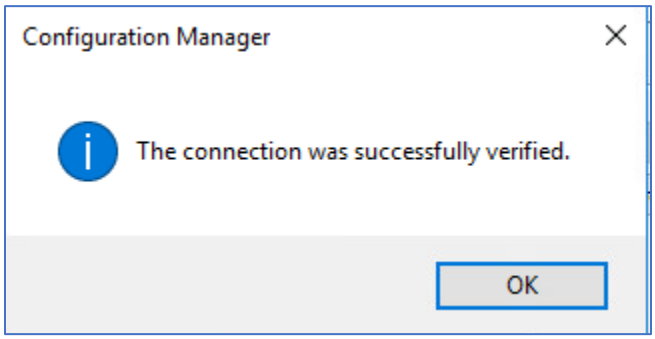
Da kommer det opp et nytt vindu. Under General-fanen skal vi først huke av for Enable automatic site-wide client push installation. Vi huker også av for de tre valgene under.



Så trykker vi på Accounts-fanen og den gule solen→New Account. Her legger vi til ClientInstall-brukeren. Når brukeropplysningen er lagt inn, trykk Verify>>. Hvis opplysningene stemmer, kan vi legge til Sources-mappen under Network share.

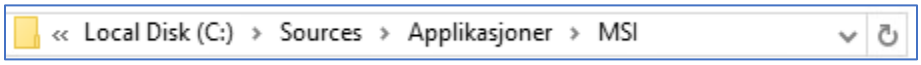


Trykk Test connection for å se om vi får kontakt med mappen.



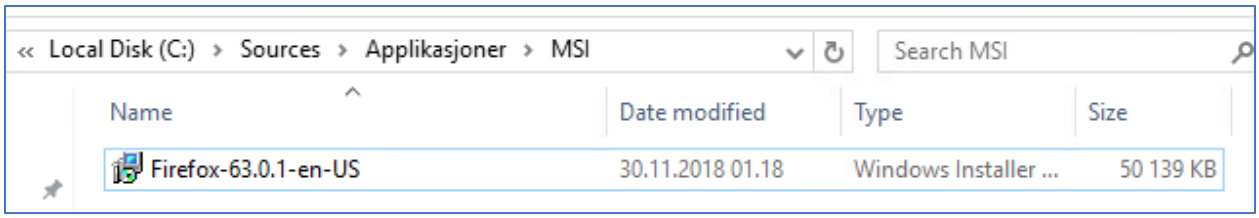
8. Utrulling av applikasjoner

Det første vi må gjøre er på SCCM-serveren. Her må vi komme oss inn i mappen C:/Sources. I denne mappen oppretter vi en undermappe som vi kaller Applikasjoner og i den mappen en mappe som vi kaller MSI.

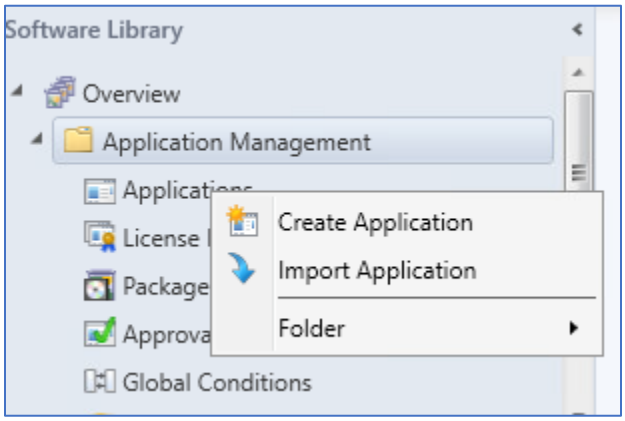


Først skal vi prøve å rulle ut Firefox. Laster derfor ned MSI-installasjonsfilen til Firefox. Den finner vi på www.frontmotion.com.

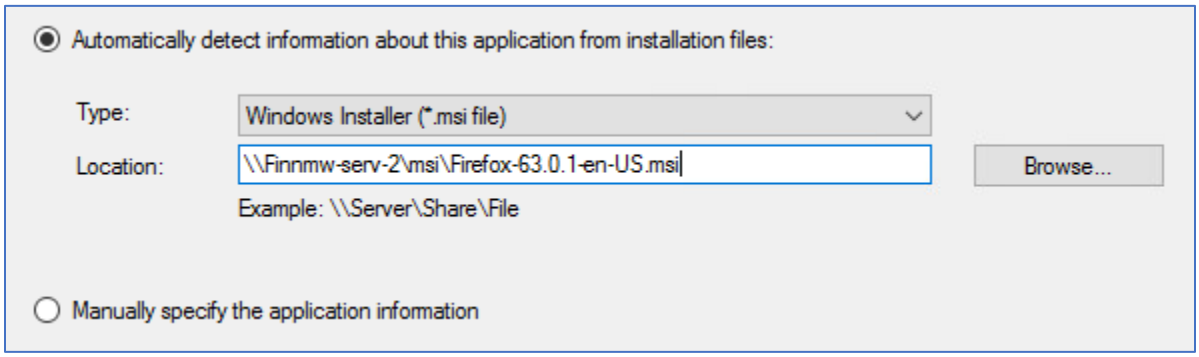
Legger så denne MSI-filen i MSI-mappen vi nettopp laget.

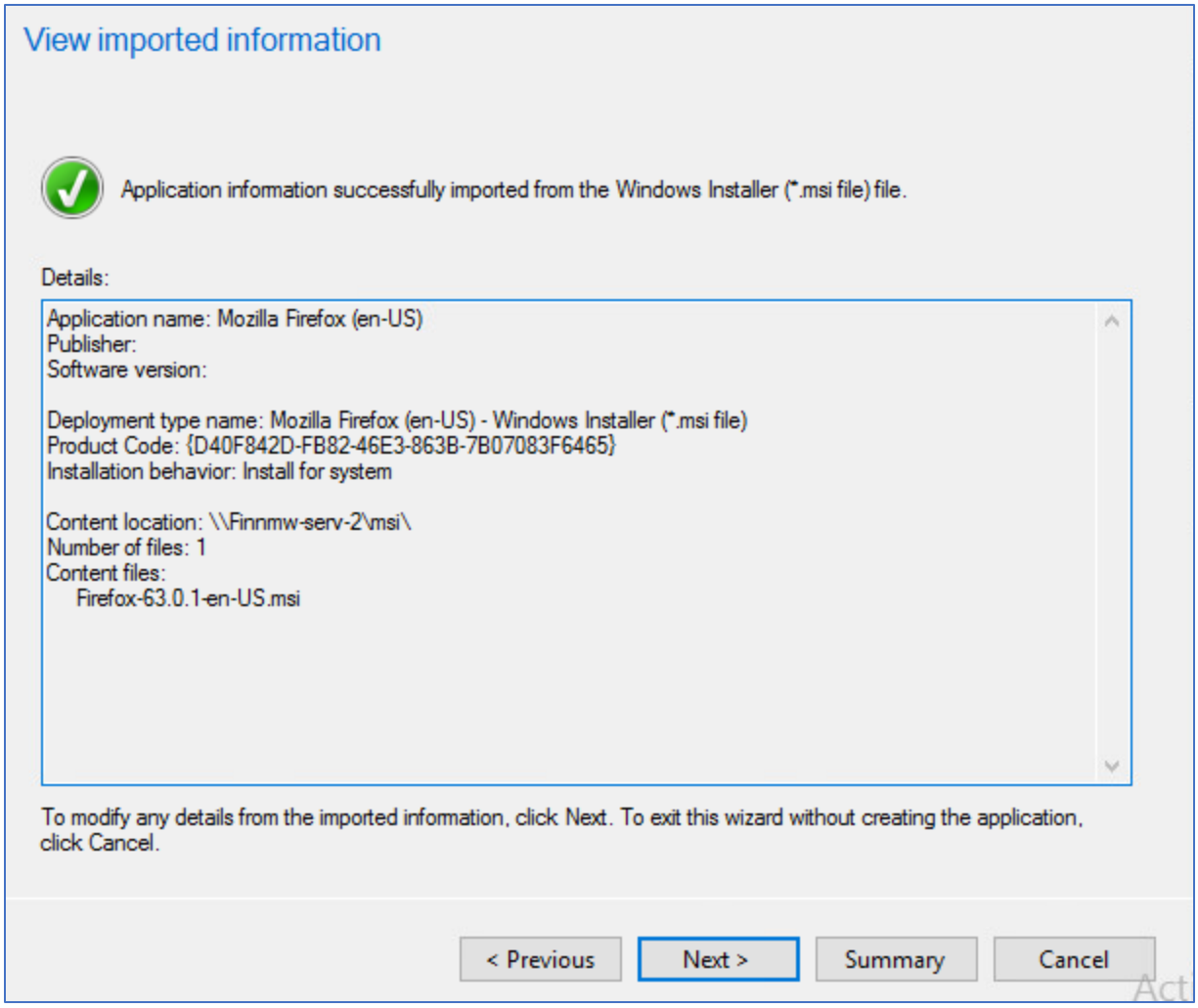


Nå må vi åpne Configuration Manager og navigere oss til Software Library→Application Management→Høyreklikke på Applications og velg Create Application.

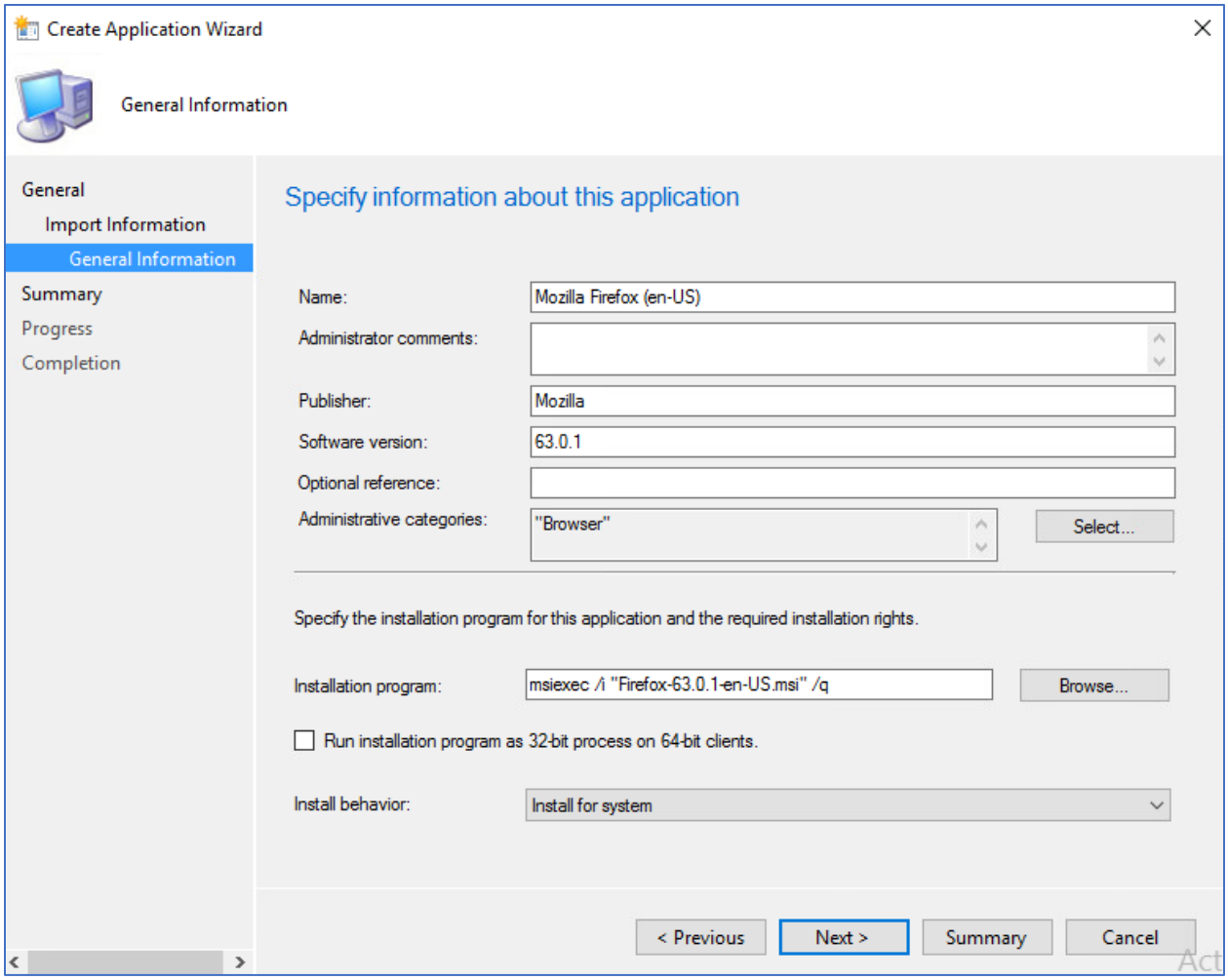


Nå må vi finne nettverksstien til installasjonsfilen til Firefox.

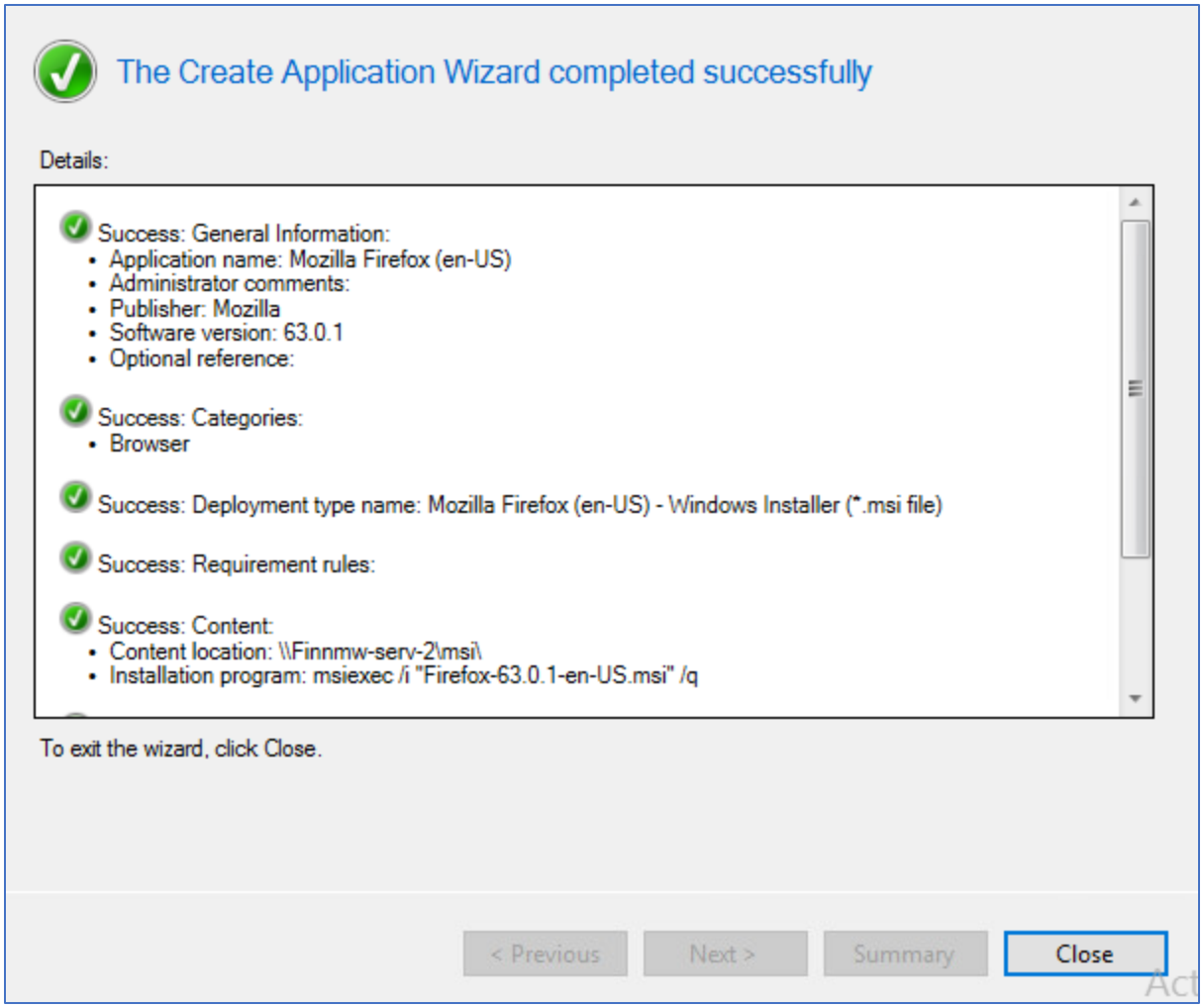




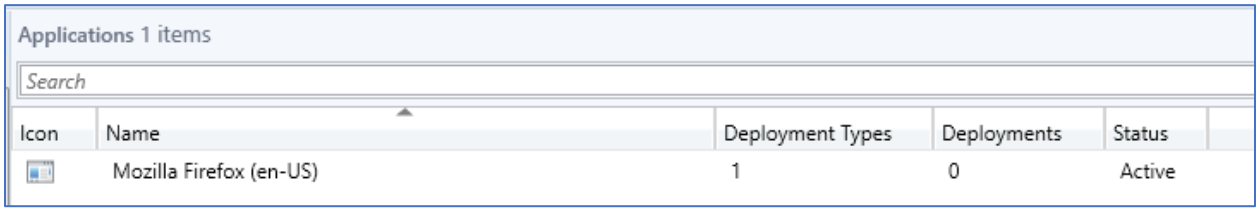
I neste vindu, General Information, kan vi legge til litt mer informasjon om filen. Her kan vi også velge om vi vil install for system eller install for user. Vi velger å install for system, siden alle brukere har behov for en nettleser. Hvis vi har valgt install for user, har vi kunne valgt hvilke brukere som skulle fått tilgang til programmet.



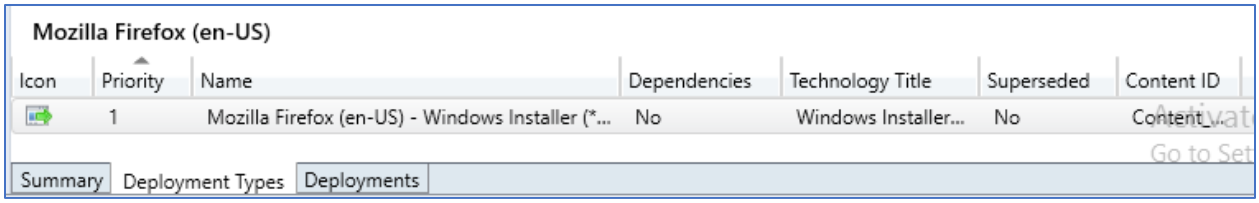
Nå er det bare å sette i gang me installasjonen. Når installasjonen er ferdig får vi opp et vindu som viser oss at installasjonen var vellykket.



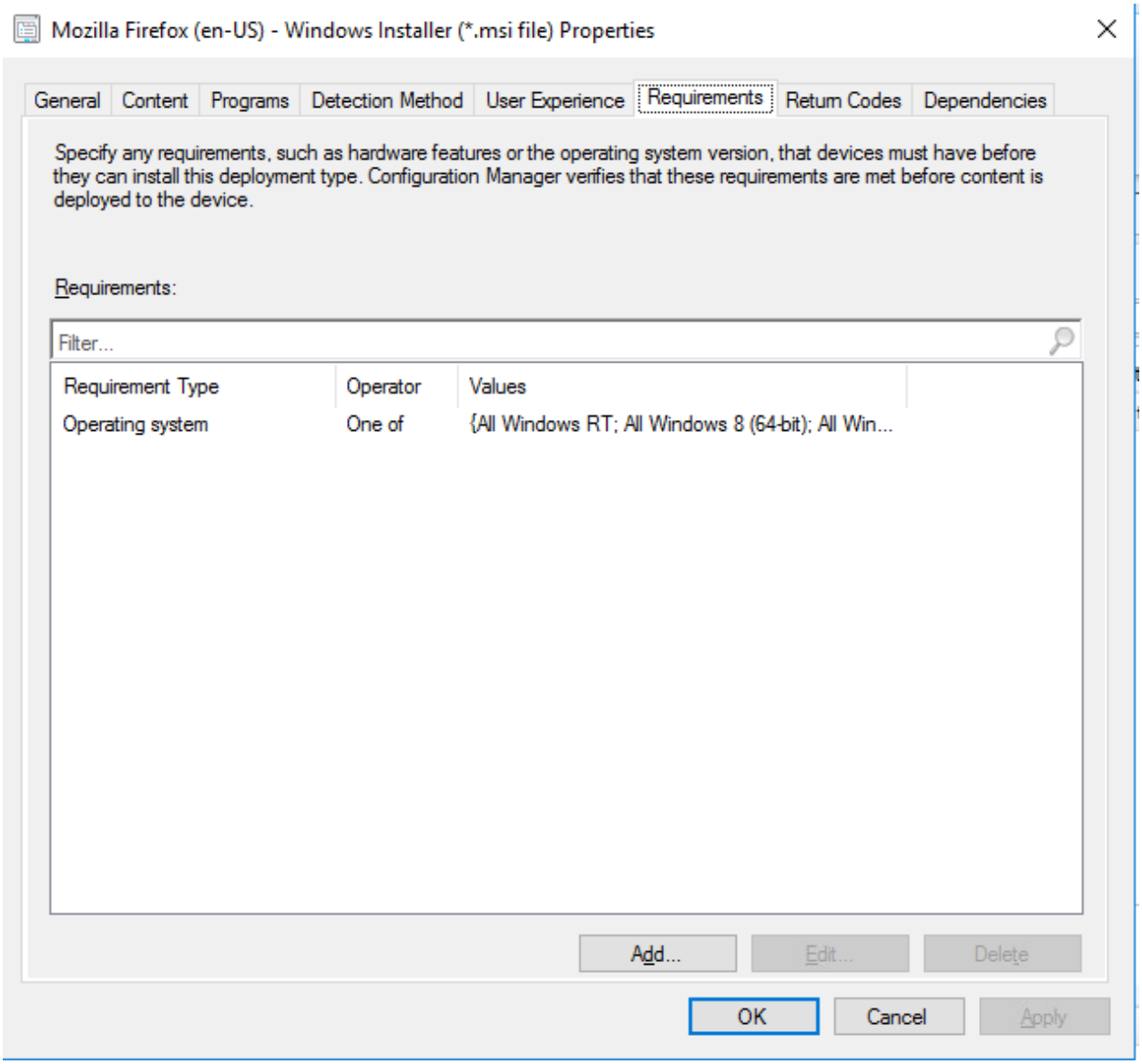
Nå kan vi se at Firefox ligger under Applications i Configuration Manager.



Nå skal vi sette noen krav for installasjonen. Helt nederst under listen over applikasjoner i Configuration Manager er det en fane som heter Deployment Types. Trykk her→Høyreklikk på Mozilla Firefox→Properties

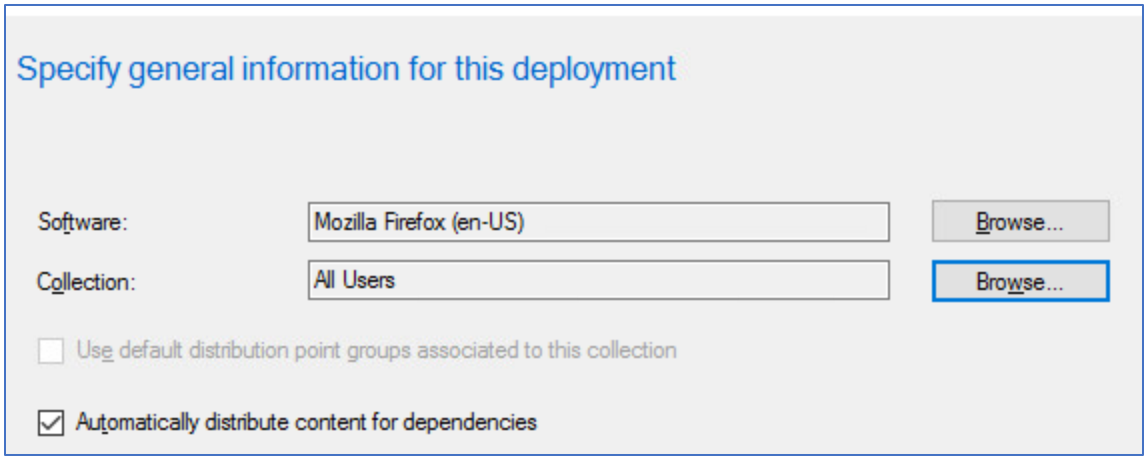


Her velger vi Requirements-fanen og trykker Add. Condition→Operating System→Velger Windows 8.1 og Windows 10, som våre klientmaskiner kjører. Denne regelen vil da komme i listen under Requirements.

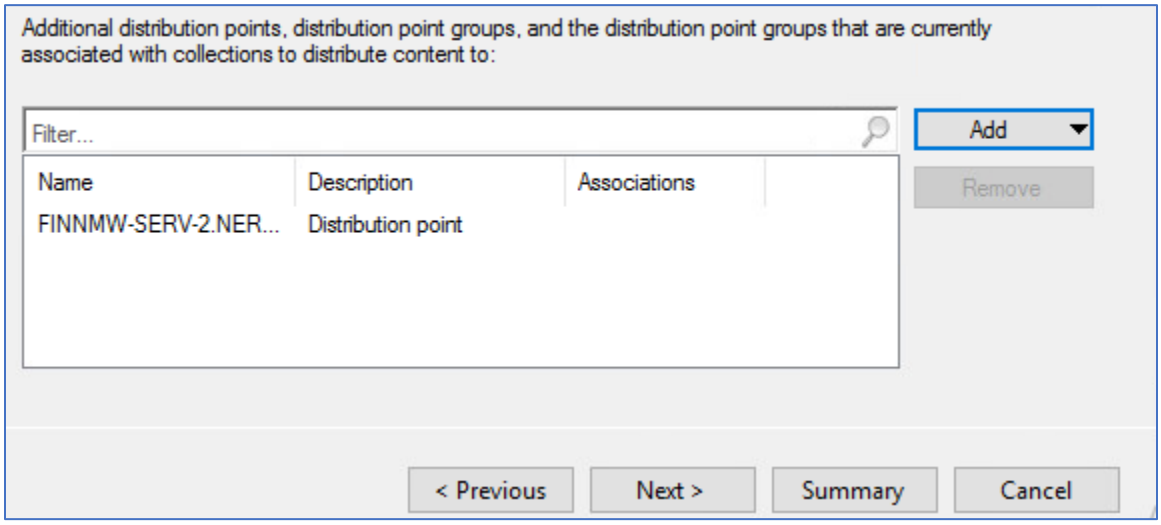


Nå er det på tide å kjøre ut Firefox. Vi finner installasjonsfilen under Applications→Høyreklikk→Deploy.

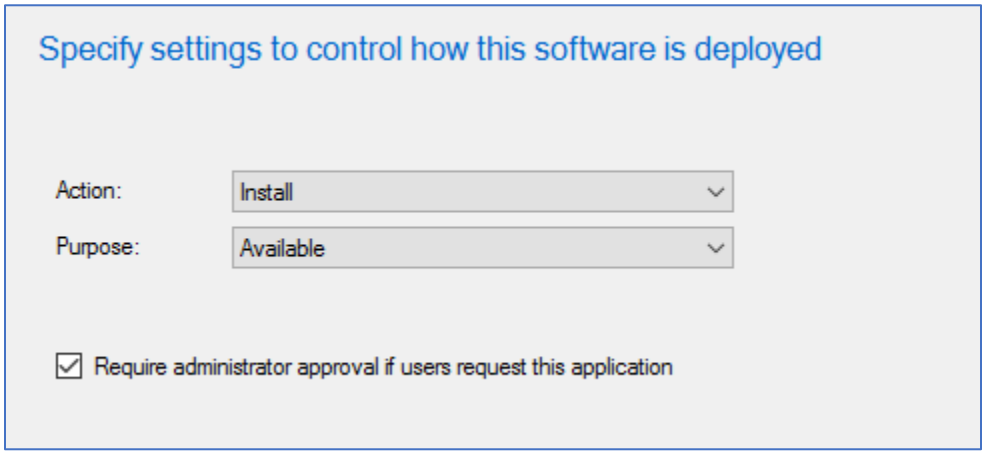
Under Collection velger vi All Users.



Nå må vi velge et Distribution Point. Her velger vi selvsagt SCCM-serveren vår.

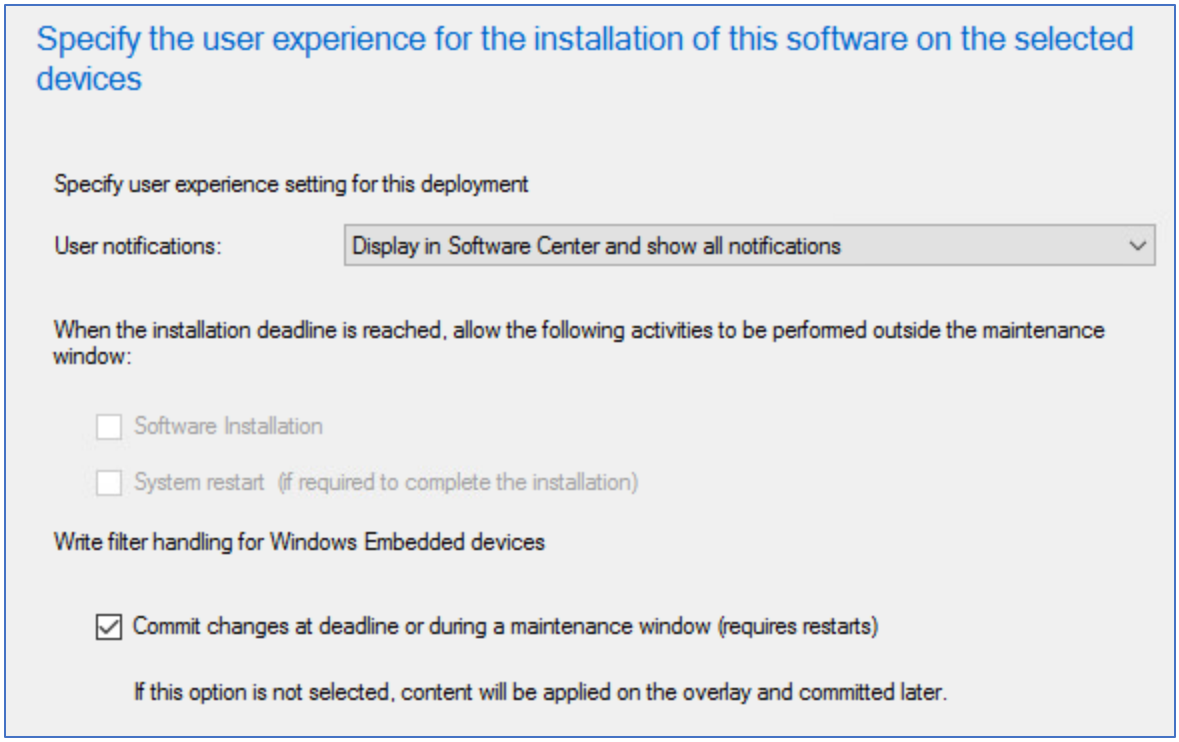


Under Deployment gjør vi disse valgene:

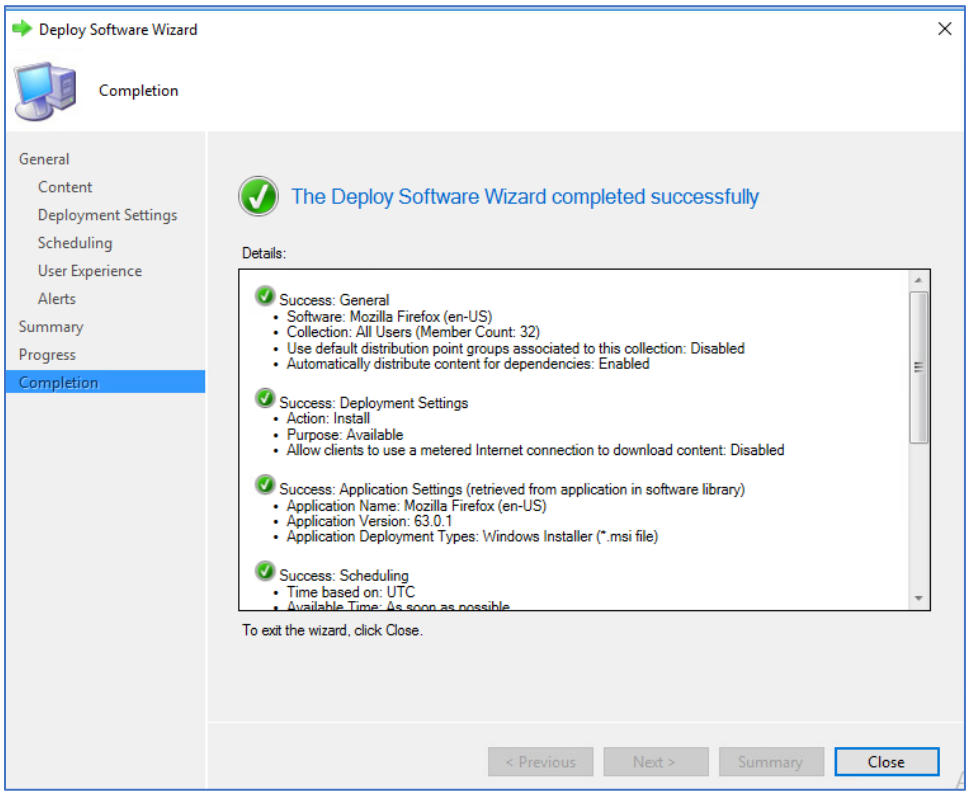


Under Scheduling velger vi ingenting, da vi vil at installasjonen skal være tilgjengelig med en gang.

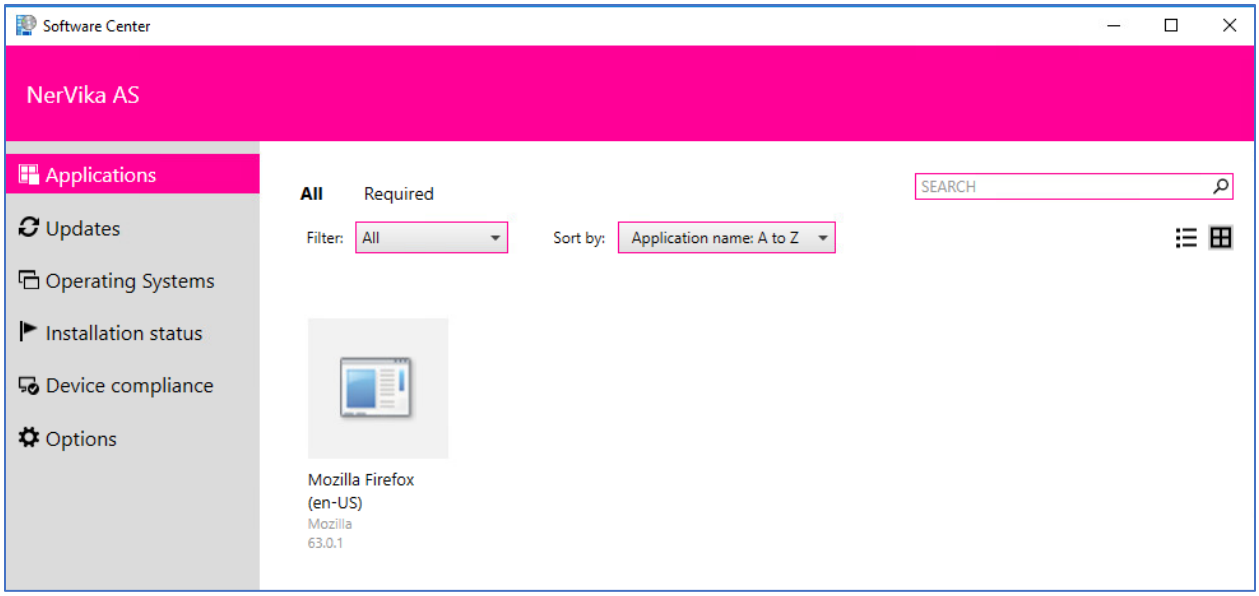
User experience lar vi også stå som det er



Gjør heller ingen endringer i Alerts, så da er det bare å fullføre utkjøringen.



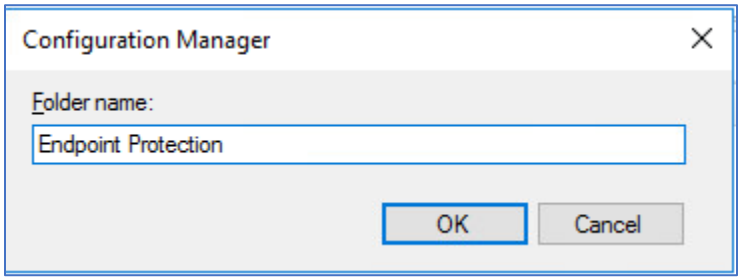
Vi kan nå se i Software Center at Mozilla Firefox er tilgjengelig.



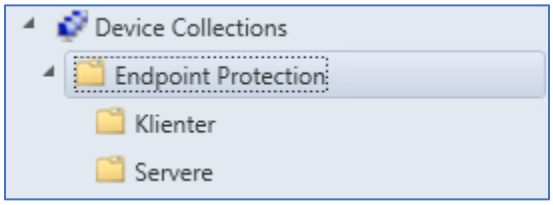
9. Endpoint Protection

Når vi skal installere Endpoint Protection må vi først logge inn på SCCM-serveren som SCCMAdmin.

På SCCM-serveren åpner vi Configuration Manager og navigerer oss til Assets and Compliance. Her skal vi opprette en mappestruktur til Endpoint. Her høyreklikker vi på Device Collections→Folder→Create New Folder. Denne mappen kaller vi Endpoint Protection.

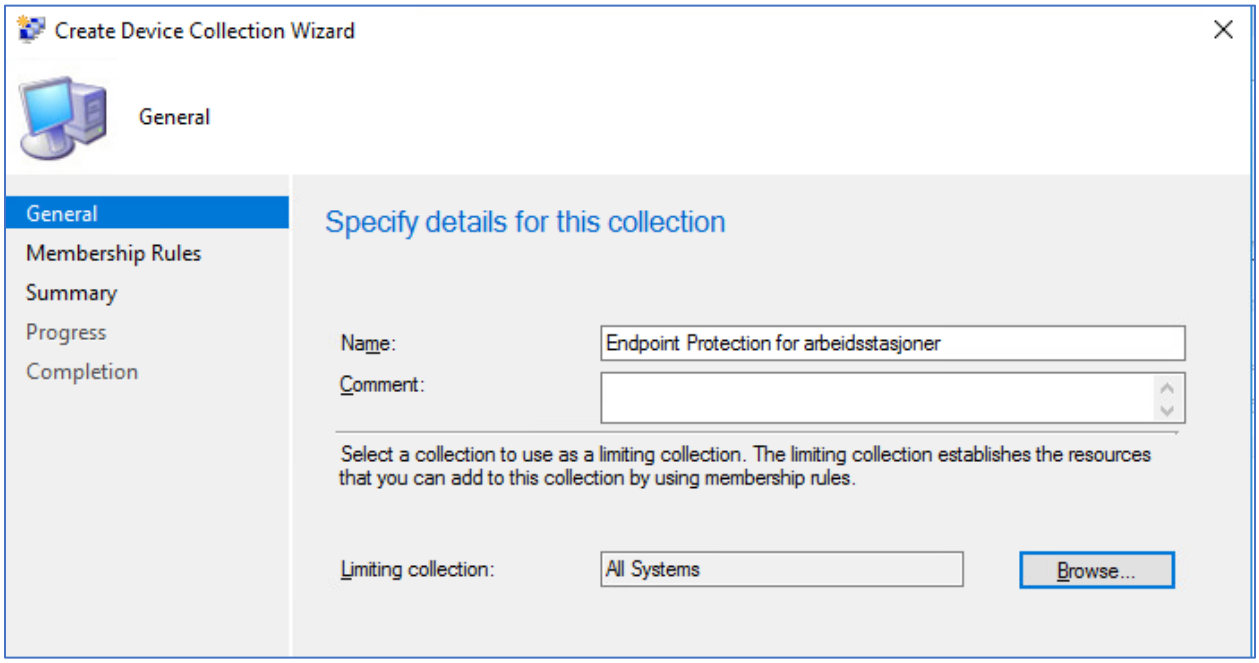


I denne mappen oppretter vi så to nye mapper som vi kaller «Klienter» og «Servere»

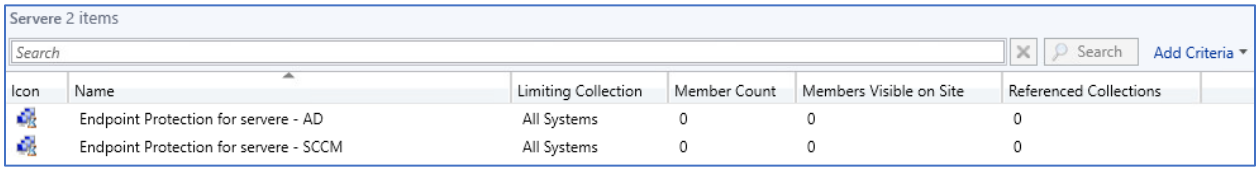


Nå skal vi lage en Device Collection for arbeidsstasjonene (Klienter). Høyreklikk på mappen Klienter→Create Device Collection.

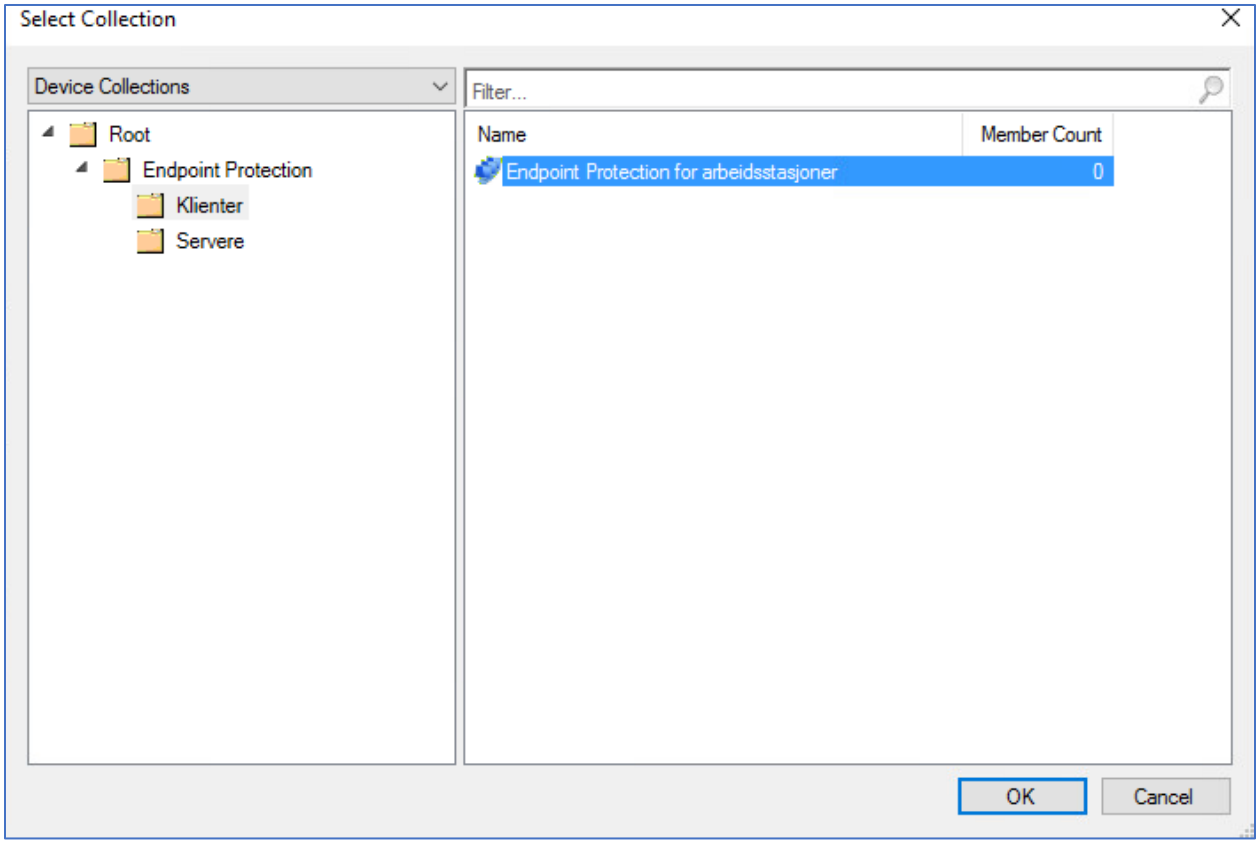
Her velger vi Endpoint Protection for arbeidsstasjoner som navn og under Limiting collection velger vi All Systems.



Nå må vi gjøre det samme under mappen Servere. Oppretter er en collection for AD-serveren og SCCM-serveren. Mappen Servere vil da se slik ut:

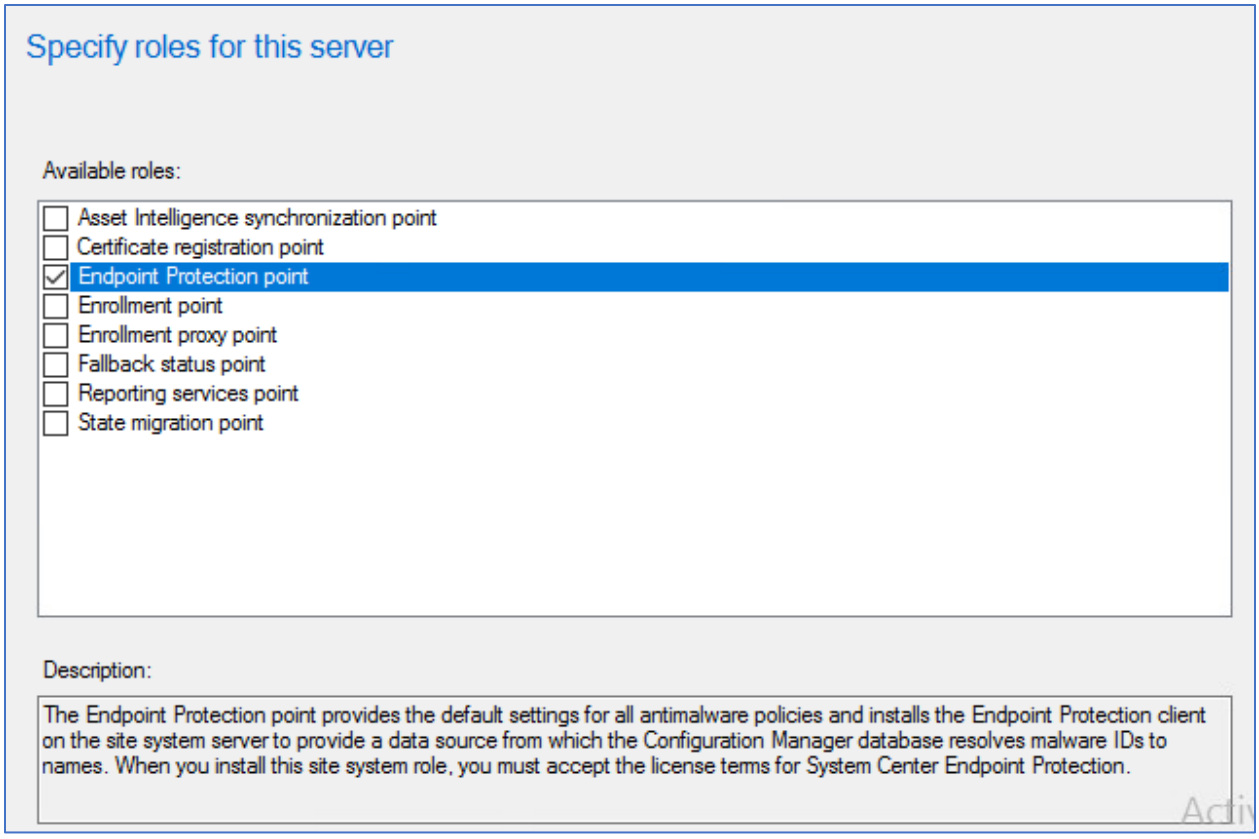


Nå må vi legge til klientmaskinene i Collectionen for arbeidsstasjoner. Dette gjøres via Devices under Assets and Compliance. Markerer de to Klientmaskinene→Høyreklikk→Add Selected Items to Existing Device Collection. Her finner vi Endpoint Protection for arbeidsstasjoner.

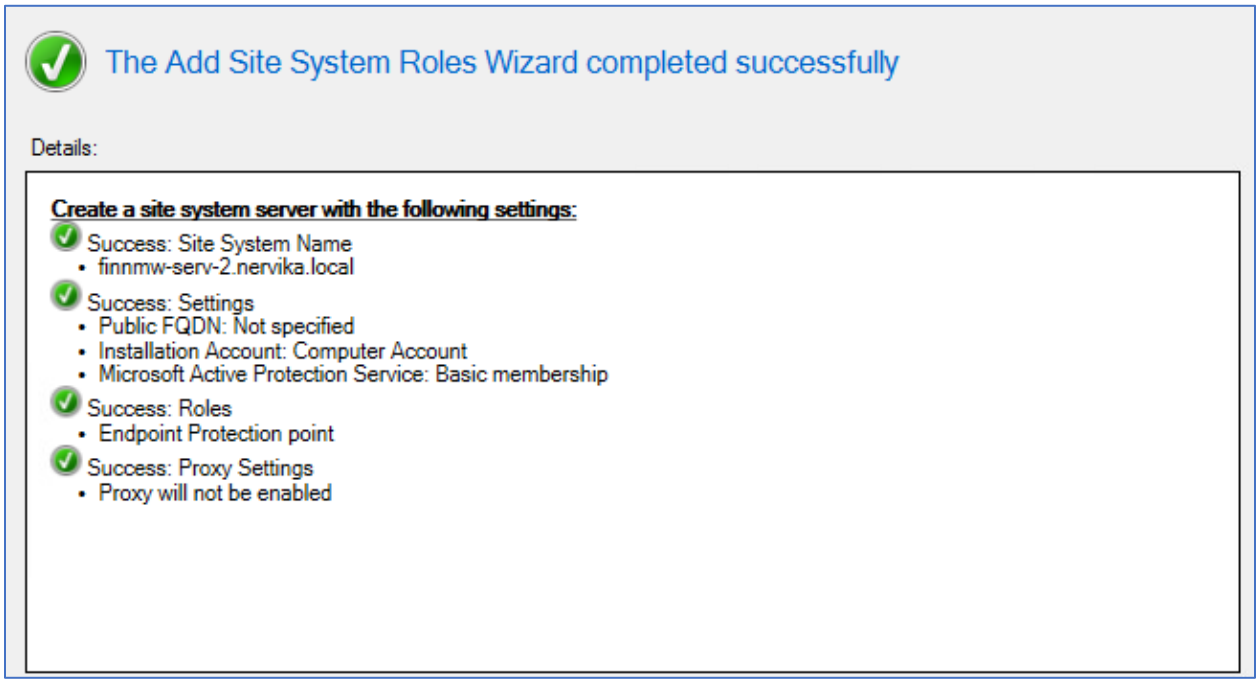


Gjentar samme prosess med serverene, slik at AD-serveren ligger i Endpoint Protection for servere – AD og SCCM-serveren ligger i Endpoint Protection for servere – SCCM.

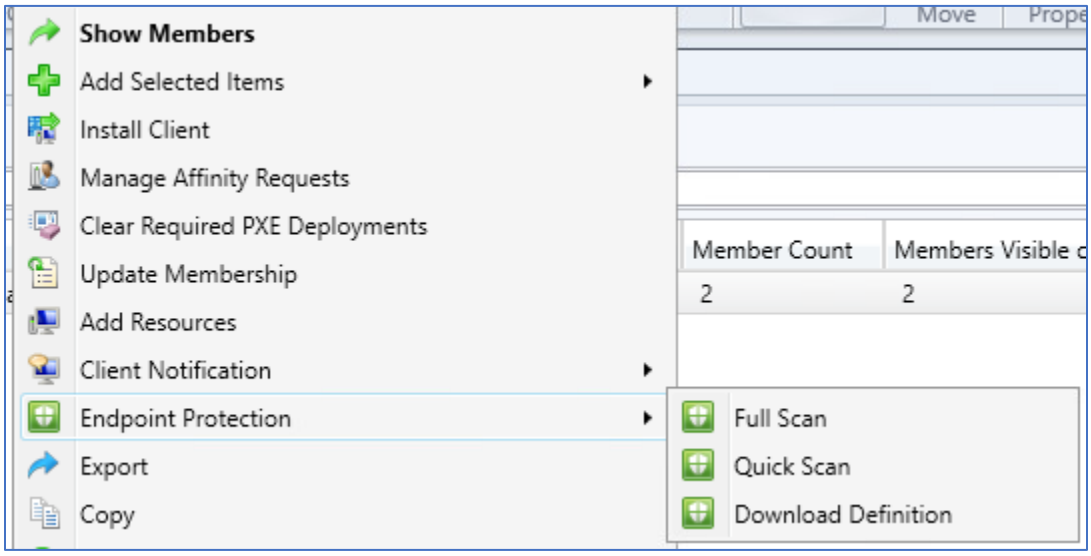
Når det er gjort må vi legge til Endpoint Protection-rollen i SCCM-manager. Vi må da navigere oss til Administration→Site Configuration→Servers and Site System Roles. Høyreklikker på serveren og velger Add Site System Roles. Her finner vi Endpoint Protection point.



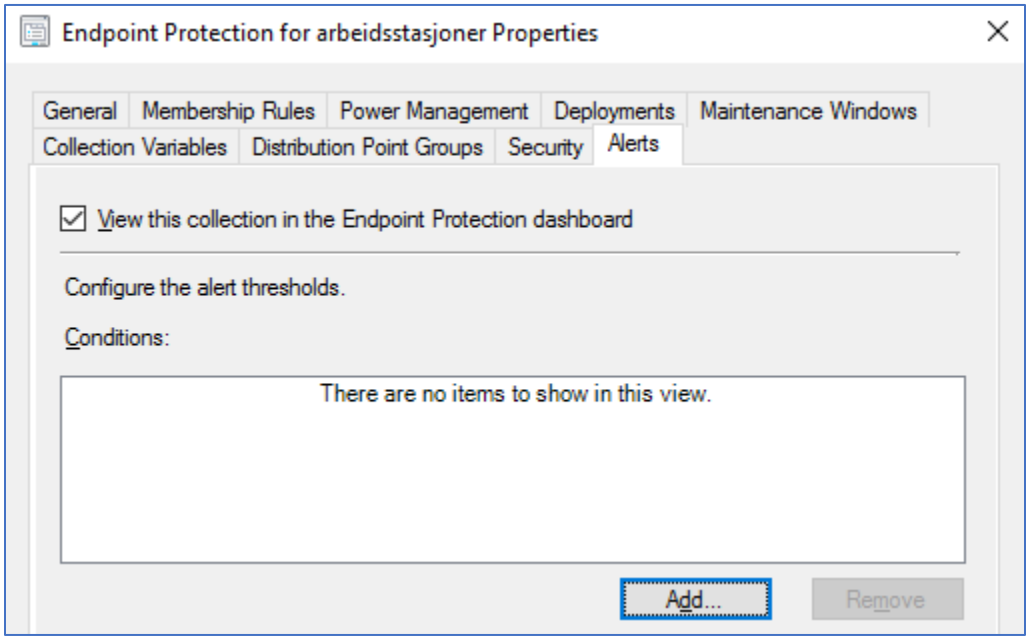
Når Endpoint Protection point er valgt, e det bare å godkjenne vilkårene og velge Basic membership. Kjør så installasjonen.



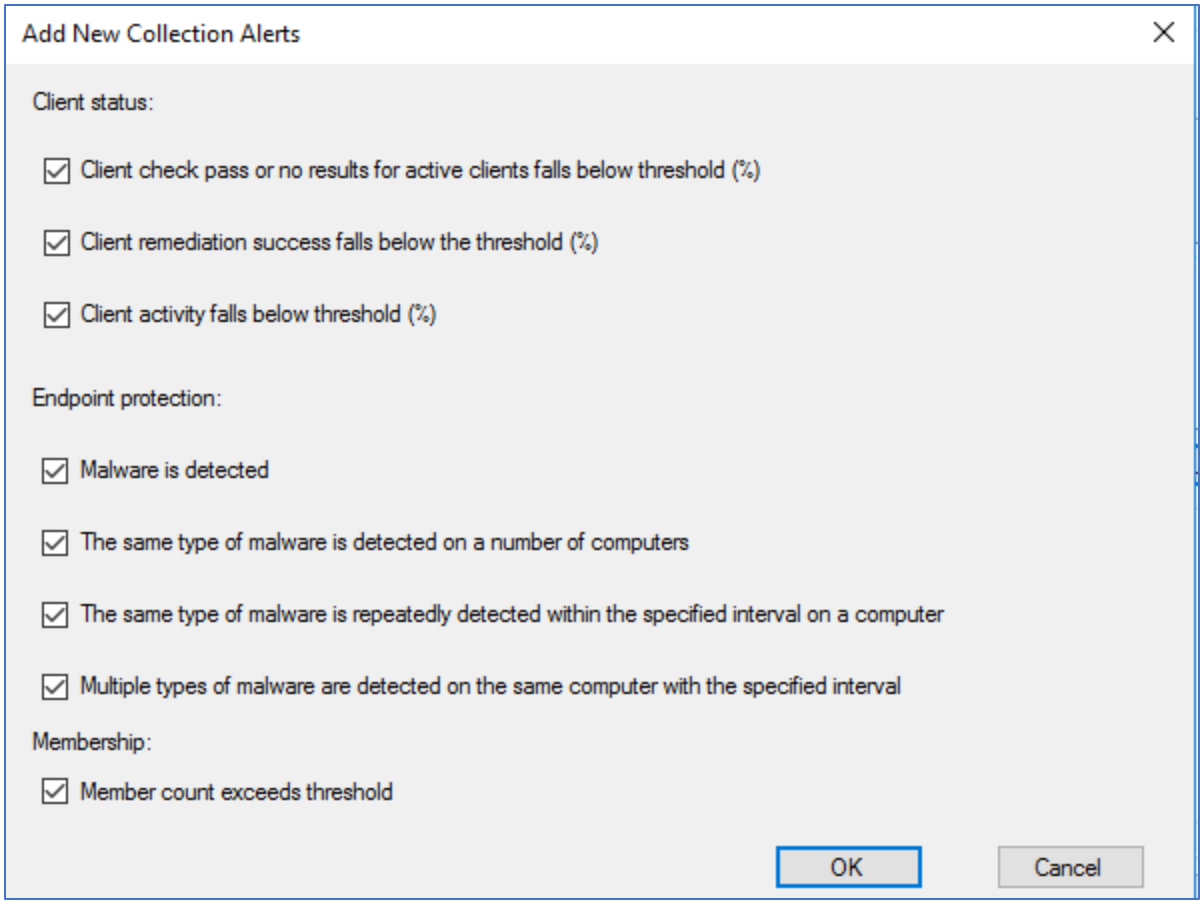
Nå som rollen er lagt til, kan vi gå tilbake til Endpoint Protection-mappen som vi laget under Device Collections. Først så går vi inn i mappen klienter og høyreklikker på Endpoint Protection for arbeidsstasjoner. Her kommer det nå opp nye valg som har med Endpoint å gjøre. Velger å kjøre en full scan her.



Med Endpoint kan vi også overvåke valgte Collections. I dette tilfelle vil vi overvåke klientene våre. Derfor går vi til Assets and Compliance og finner Collection for arbeidsstasjoner. Høyreklikker på denne og velger properties. I properties velger vi fanen Alerts og huker av for View this collection in the Endpoint Protection dashboard.



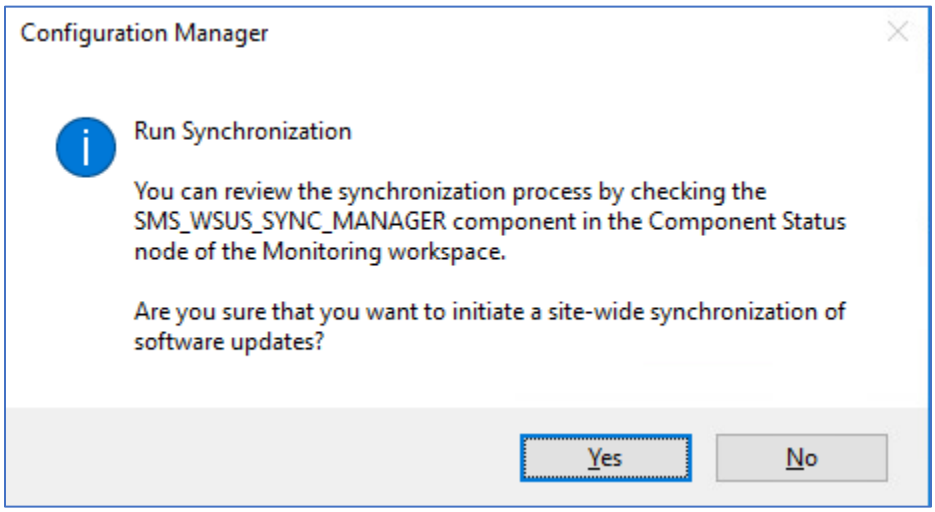
Trykker så på Add for å velge hva vi vil overvåke. Her huker vi av for alle alternativene.



Nå kan vi se Collection for arbeidsstasjonene i Endpoint Dashboard under Monitoring→Overview→Security→Endpoint Protection Status.

Nå må vi konfigurere SUP slik at klientmaskinene vår kan få oppdateringer fra Configuration Manager. Vi må legge til en rolle til, som heter ForeFront Endpoint Protection. Vi starter med å navigere oss til Administration→Site Configuration→Sites. Her høyreklikker vi på SCCM-serveren og velger Configure Site Components→Software Update Point. Trykker på Products-fanen og blar nedover og velger Forefront Endpoint Protection 2010.

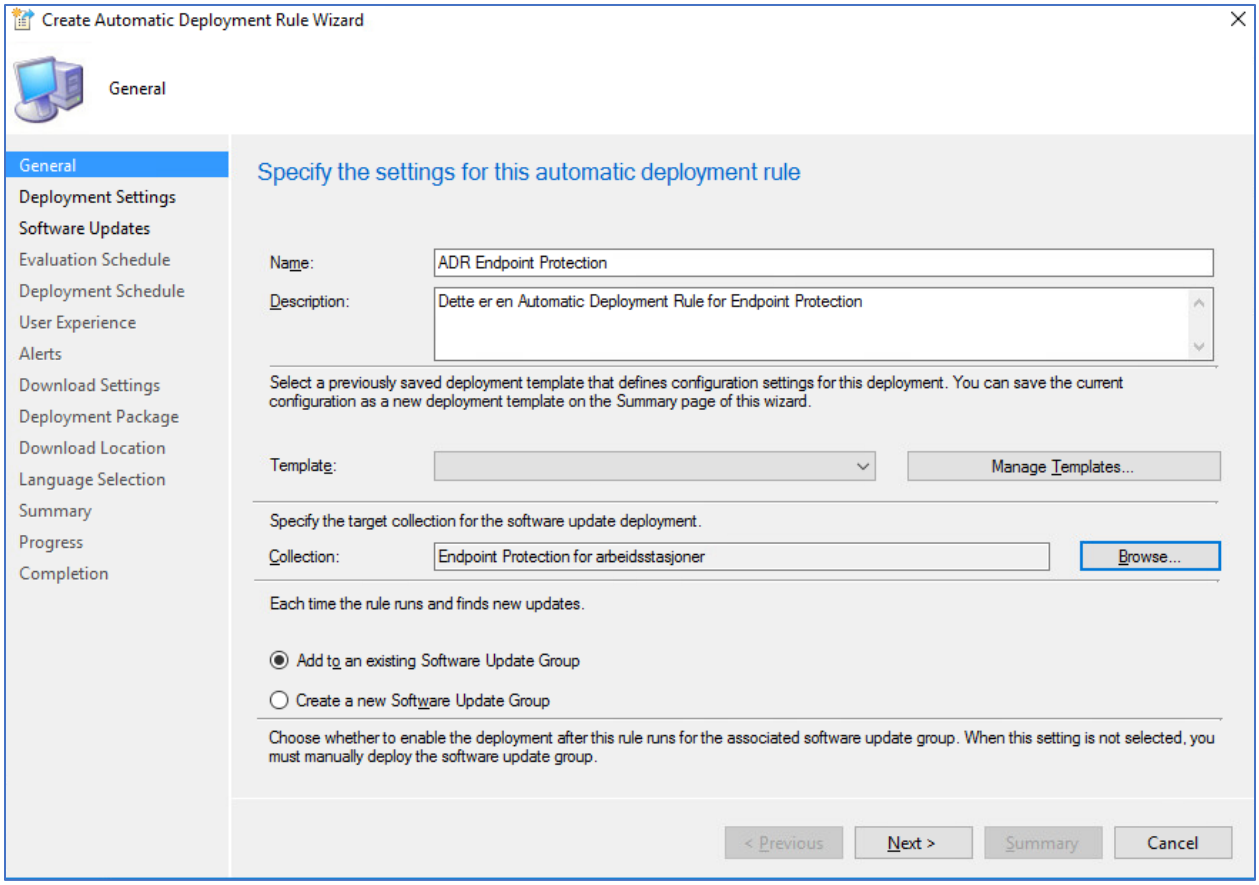
Når Forefront er lagt til må vi synkronisere SUP. Navigerer oss til Software Library→Software updates. Her høyreklikker vi på All Software Updates og velger Synchronize Software Updates.



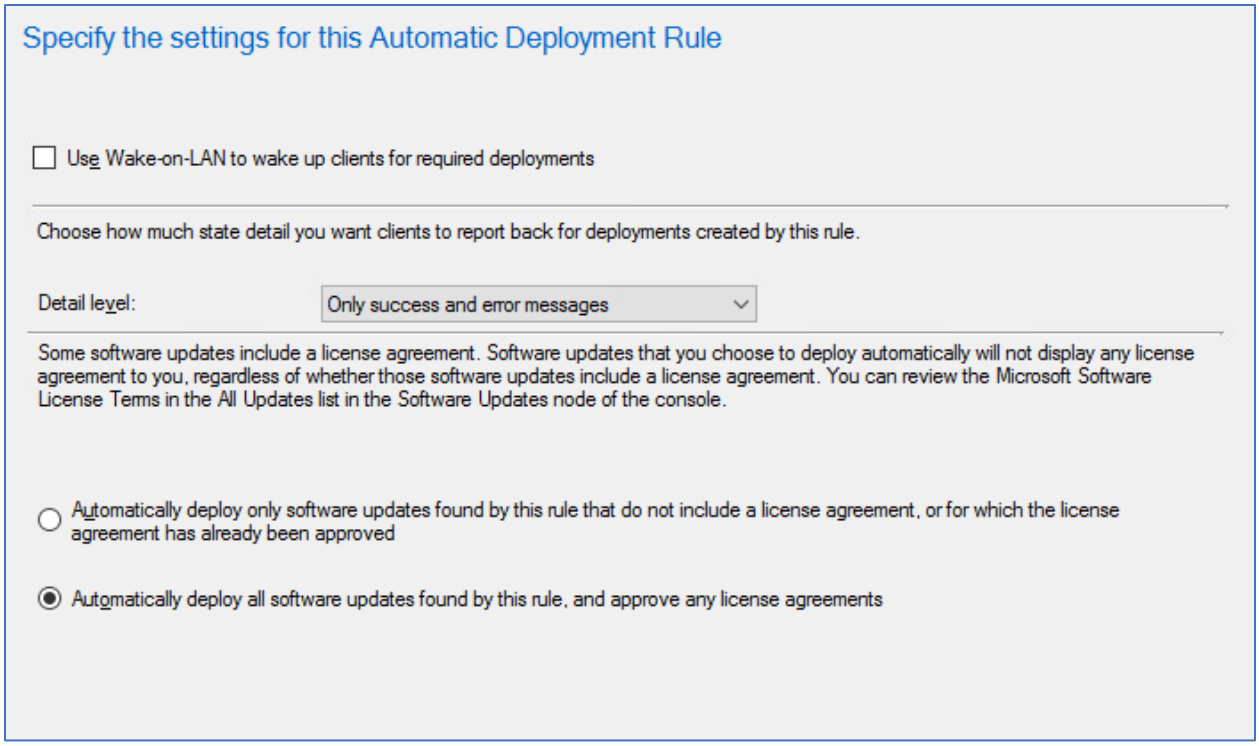
Nå skal vi opprette en ADR (Automatic Deployment Rule) for Endpoint. Først så må vi lage en ny undermappe i Sources-mappen vi laget tidligere. Denne mappen kaller vi Endpoint Protection. Vi må også sjekke om mappen arver dele-innstillingene fra mappen Sources.

Når mappen er opprettet må vi gå inn på Configuration Manager. Her skal vi opprette ADRen. Da må vi navigere oss til Software Library→ Software Updates→Høyreklikke på Automatic Deployment Rule→Create ADR.

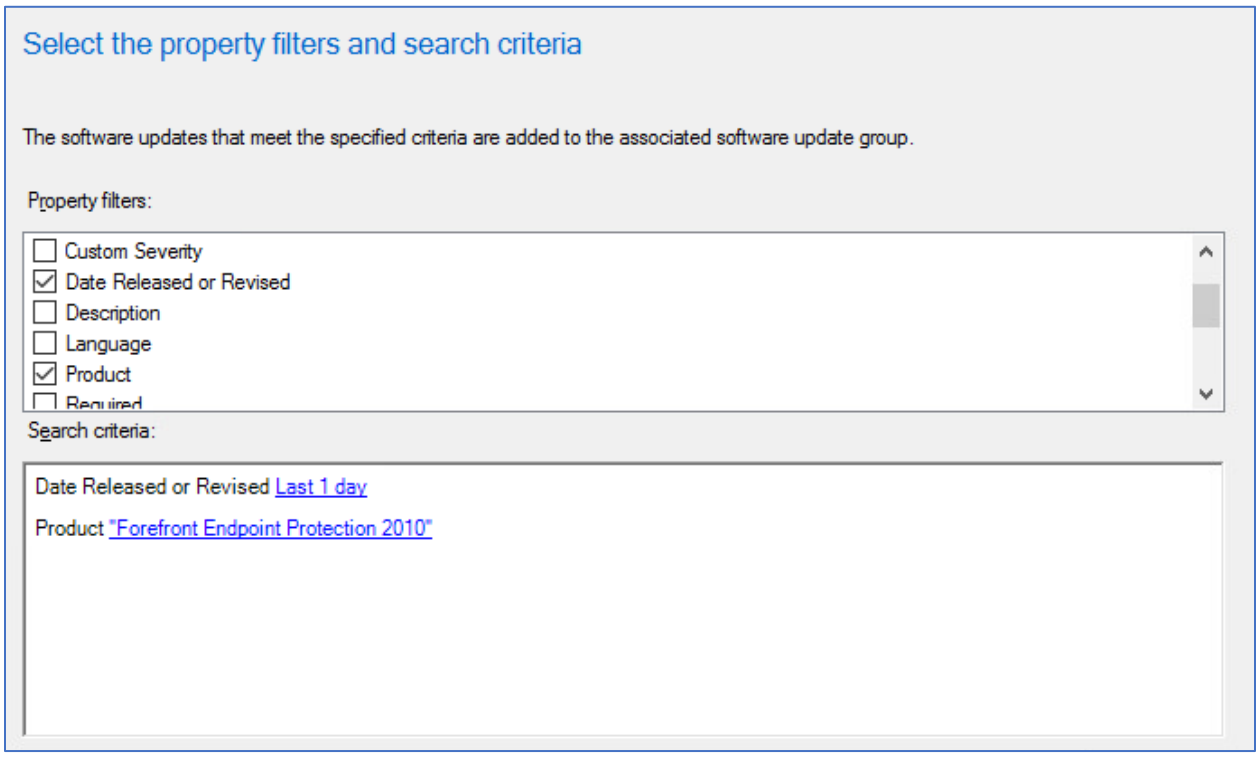
Først så skal vi gi ADRen et navn og en beskrivelse. Velger også at denne regelen skal gjelde for Collectionen for arbeidsstasjoner.



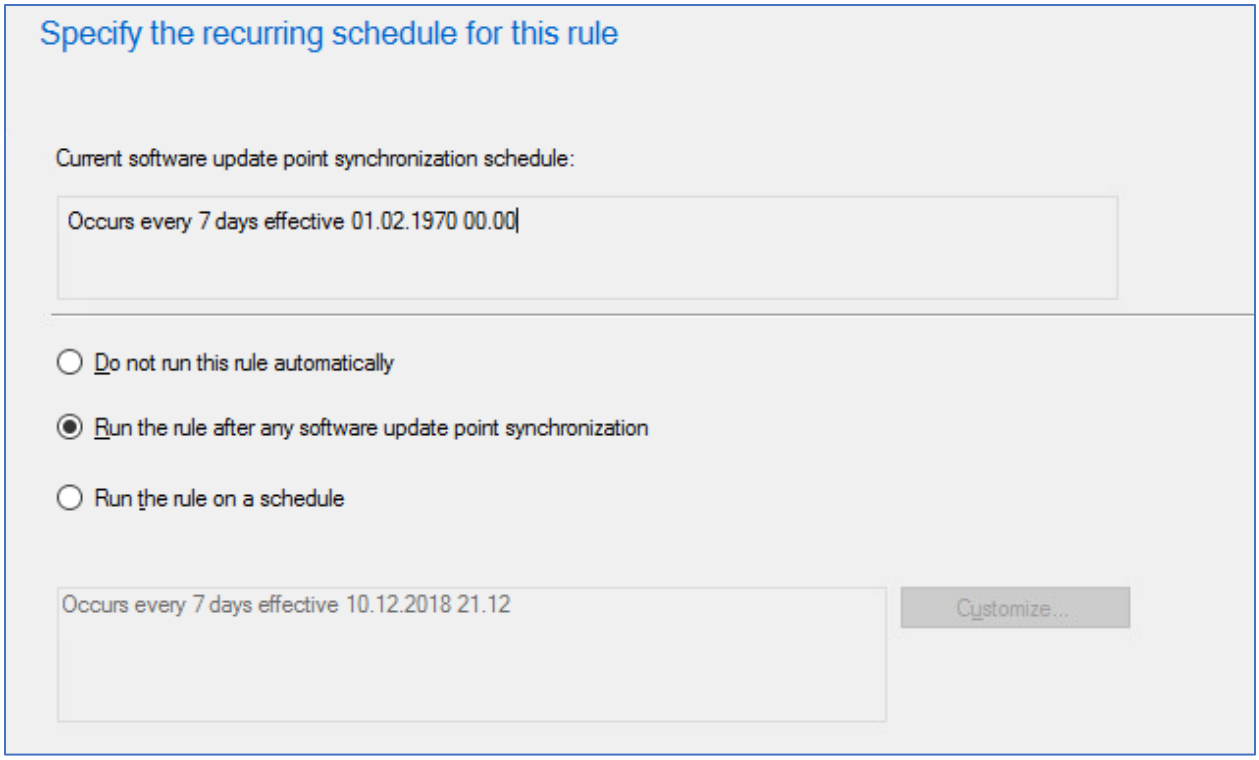
Under Deployment Settings velger vi Only success and error messages.



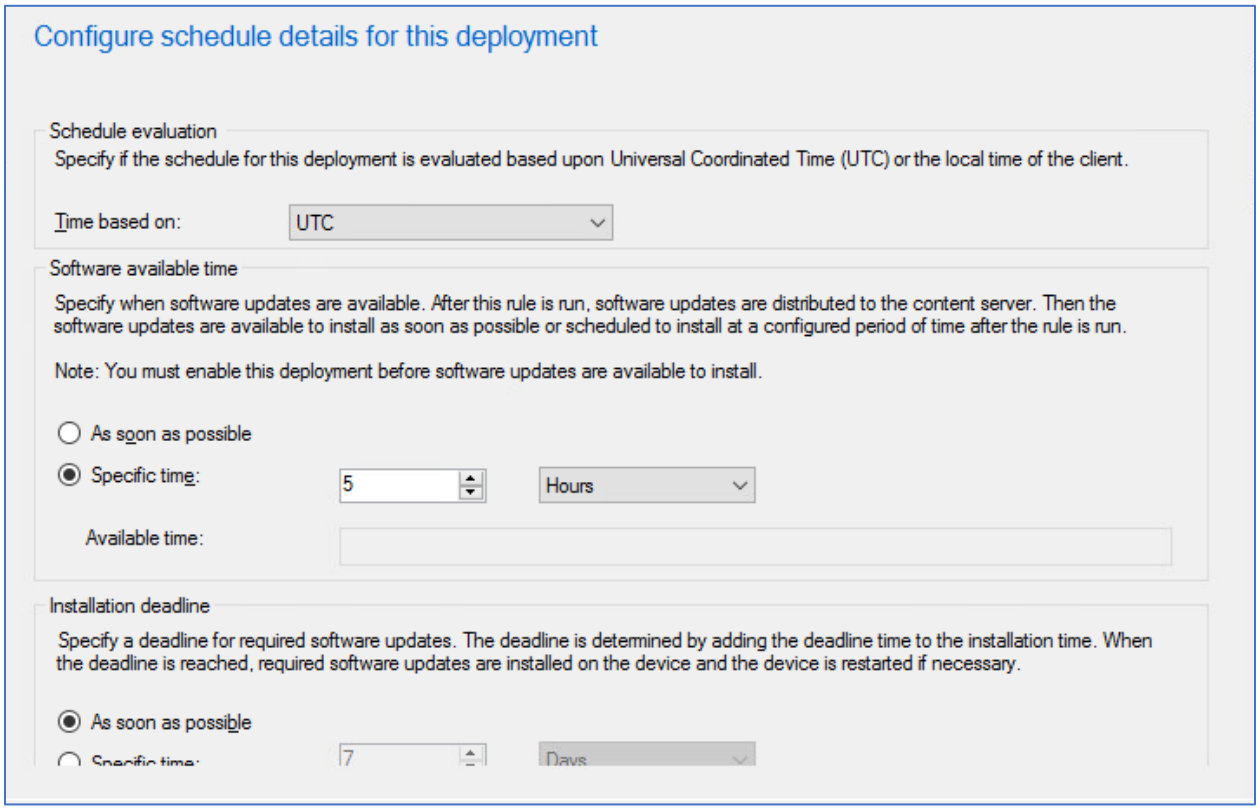
Under Software Updates skal vi finne Forefront Endpoint Protection 2010, samt velge Date Released or Revised. Her skal vi velge Last 1 Day.



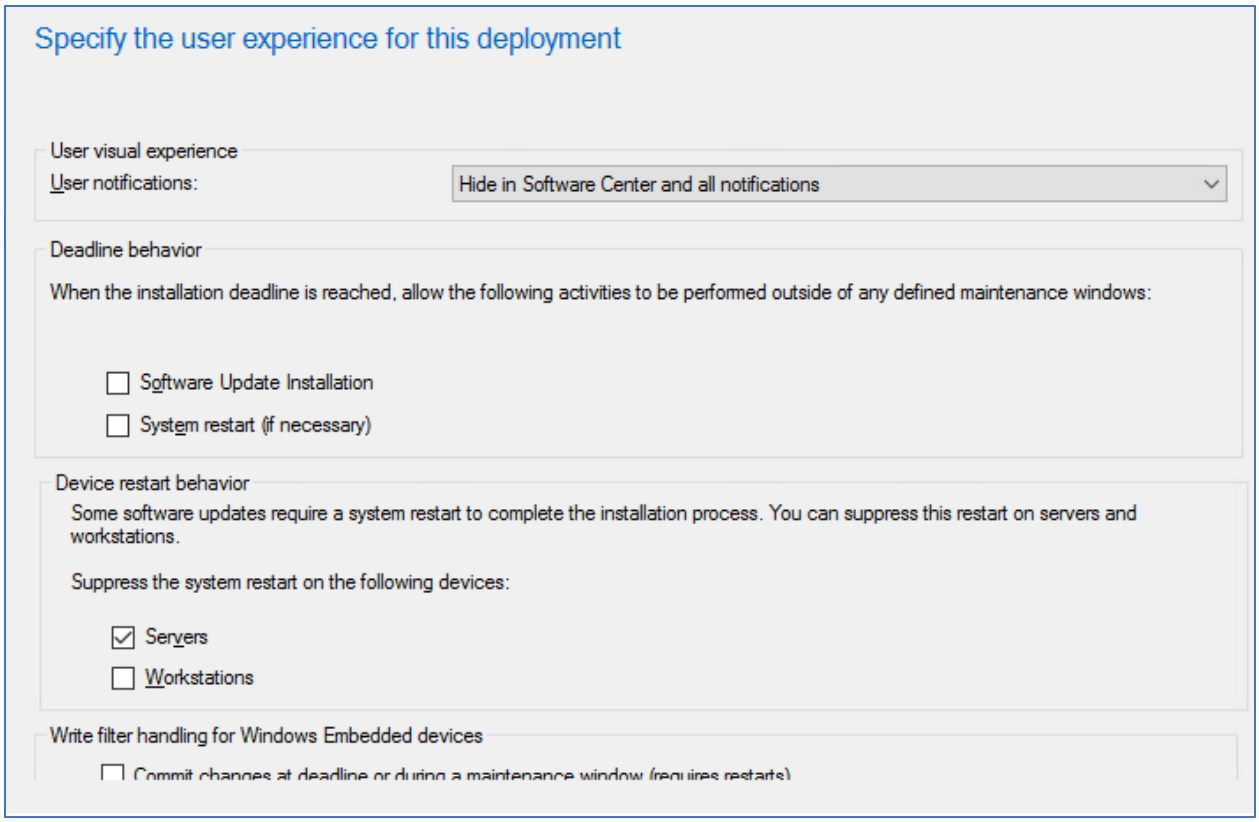
Evalutation schedule lar vi stå som det er



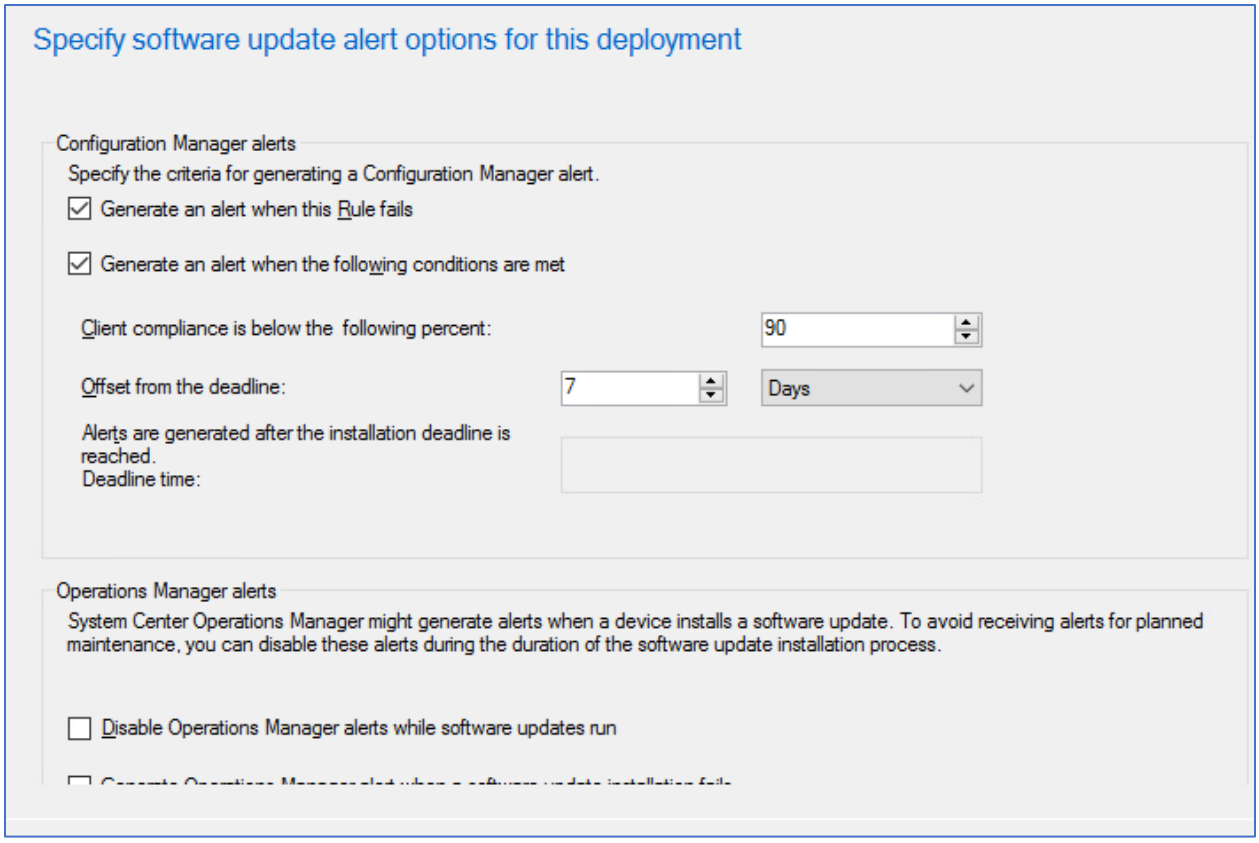
Under Deployment Schedule setter vi Software Avaliable Time til 5 timer, mens vi setter Installation Deadline til As soon as possible.



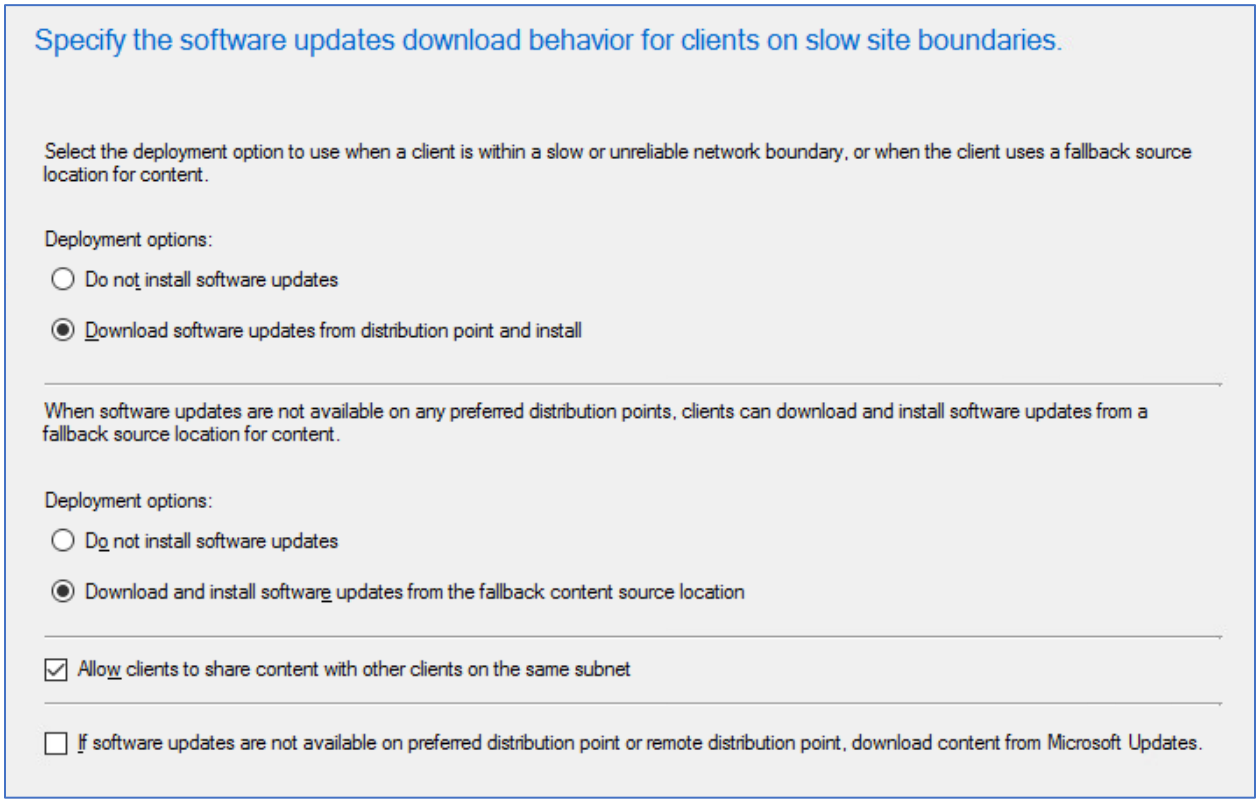
Under User Experience så huker vi av Servers under Suppress the system restart.



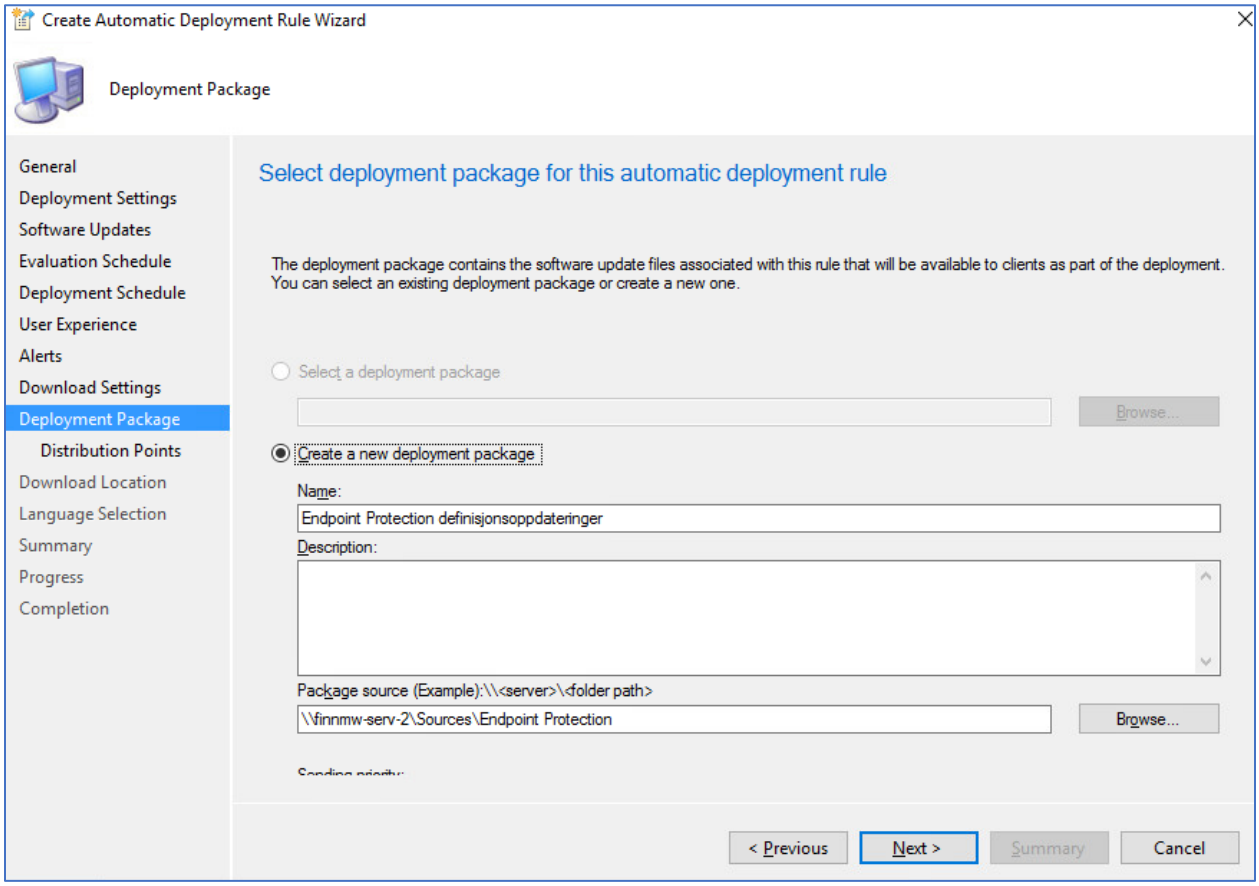
Under alerts skal det se slik ut:



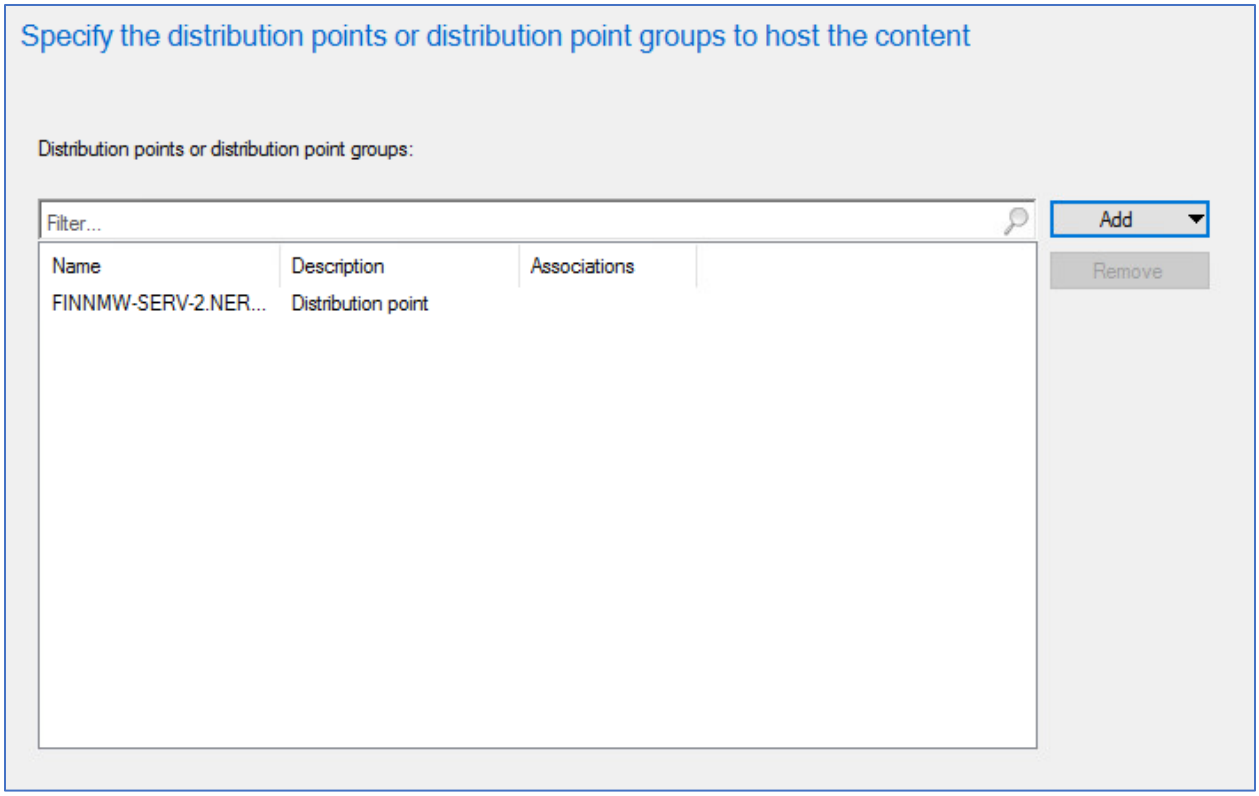
Under Download Settings huker vi av Download software updates from distribution point and install.



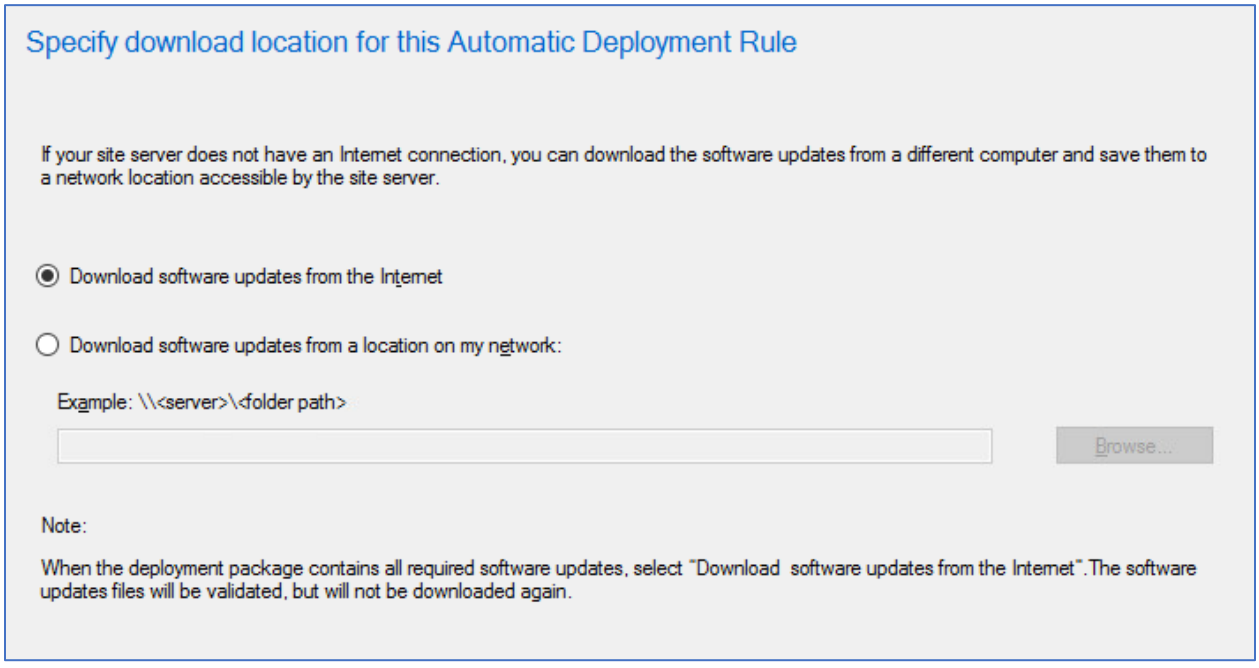
Under Deployment Package må vi opprette en ny Deployment Package. Gir denne navnet Endpoint Protection definisjonsoppdateringer og finner nettverkstien til Endpoint Protection-mappen vi nettopp har laget.



Under Distribution Points finner vi SCCM-serveren. Trykker på Add og legger til serveren.

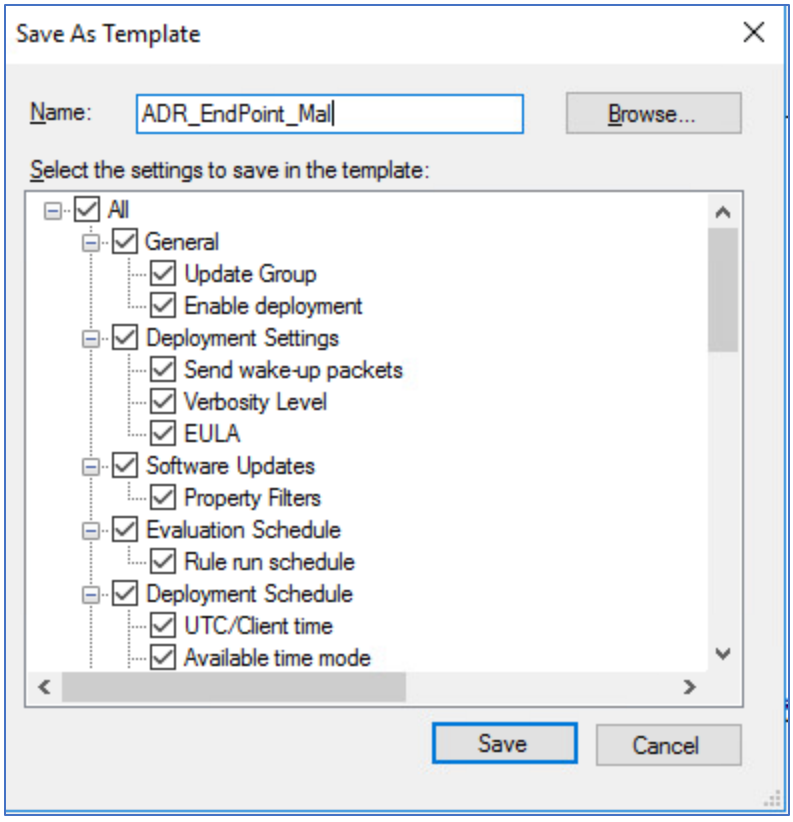


Under Download Location velger vi at oppdateringer skal lastes ned fra nettet.



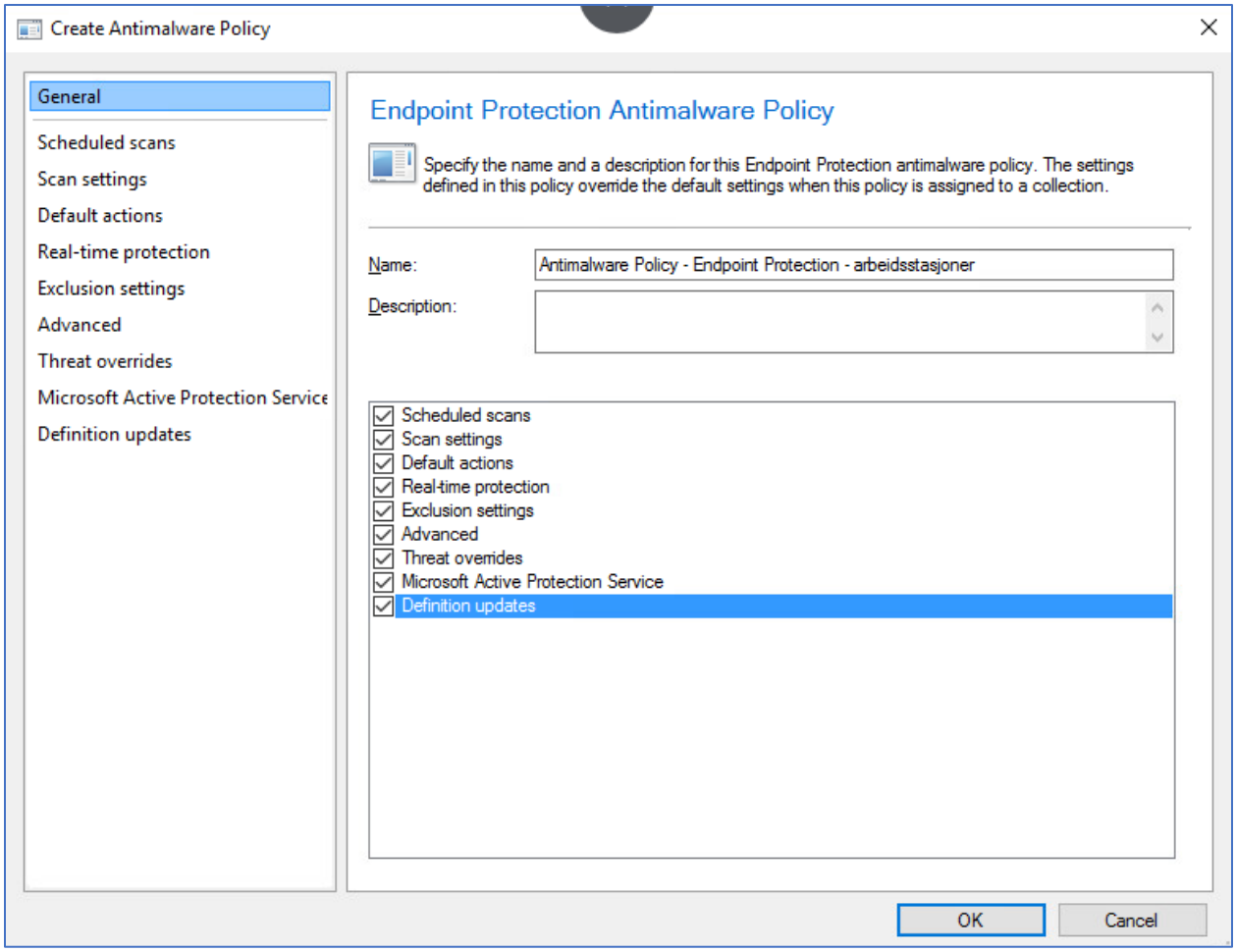
Velger bare engelsk under språk.

Under Summary velger vi Save as template, så vi kan bruke oppsettet her til å opprette nye ADR.

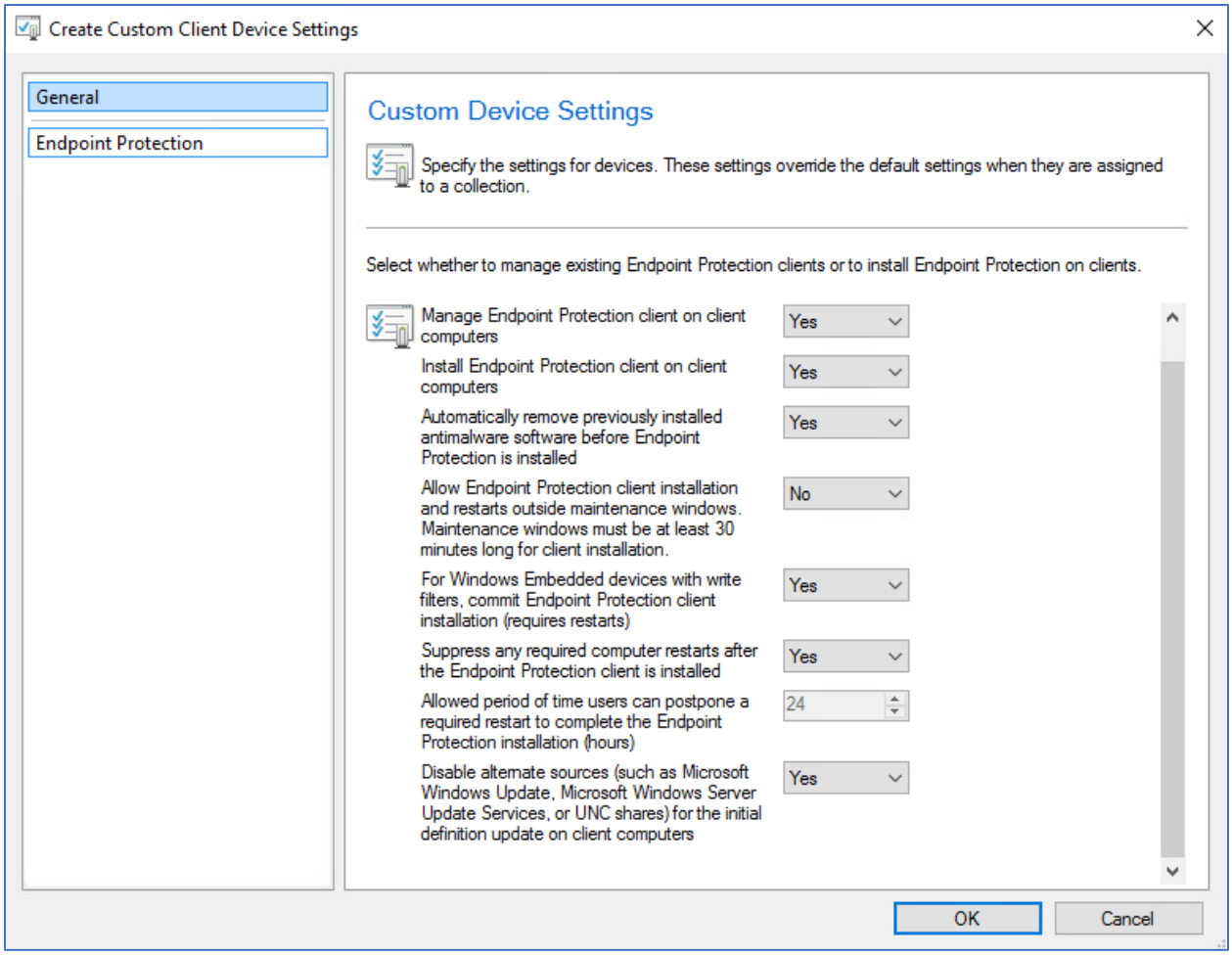


Nå er det bare å fullføre innstallasjonen.

Nå skal vi opprette en Antimaleware Policy. Dette finner vi under Assets and Compliance→Endpoint Protection→Høyreklikke på Antimalware Policies→Create new antimalware policy.

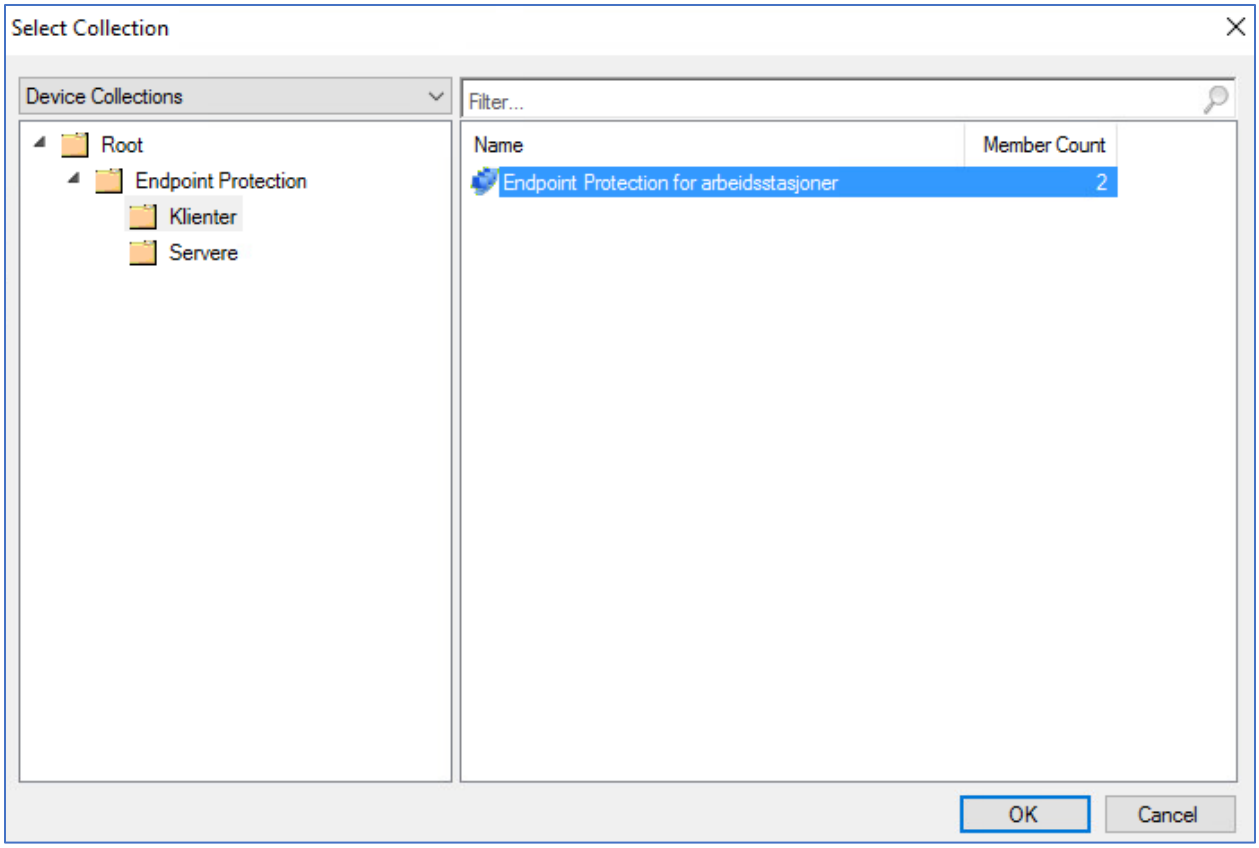


Til slutt må vi lage en Custon Client Device Setting. Administration→Client Settings→Høyreklikk→Create custom Client device setting.

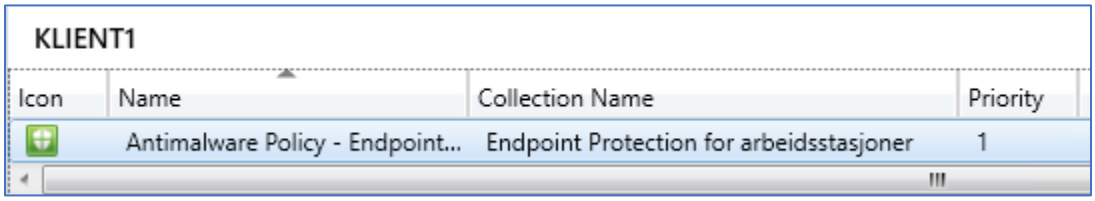


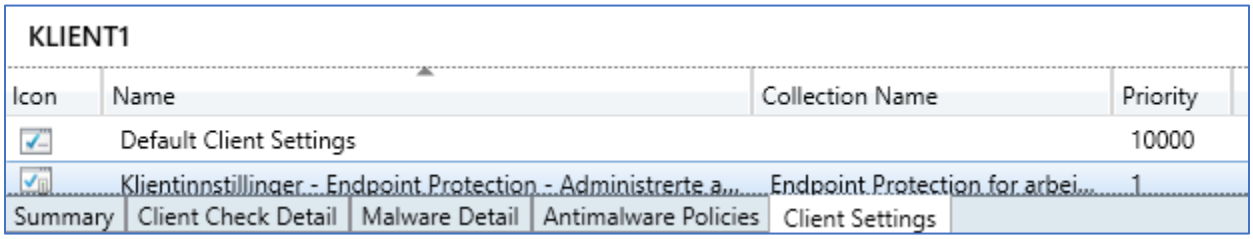
Nå skal denne dukke opp under Client Settings. Høyreklikk på den→Deploy.

Her velger vi Collection for arbeidsstasjonene.



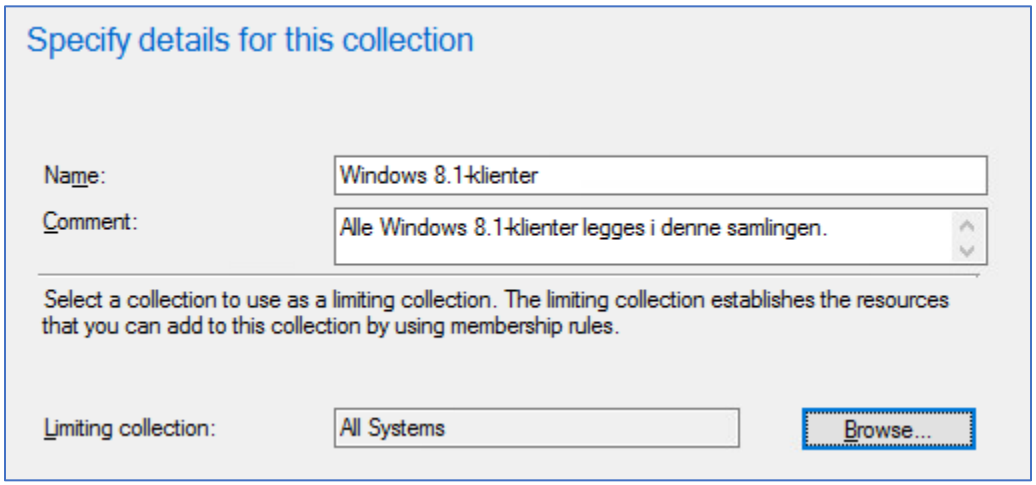
Det samme må vi gjøre med Antimaleware Policyen vi nettopp laget. Hvis vi da klikker på en av klientmaskinene under Devices vil vi kunne se at de bruker den Antimaleware Policyen vi har satt, samt de klientinnstillingene vi laget.



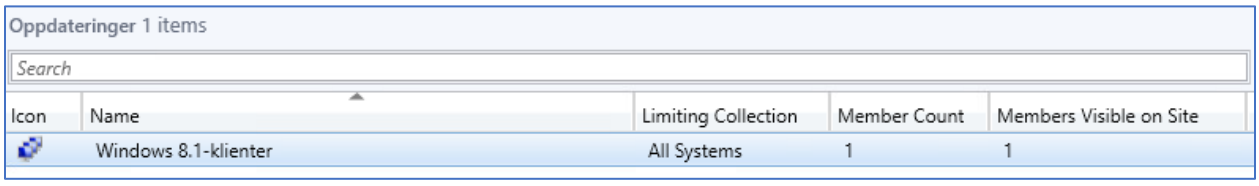


10. Utrulling av sikkerhetsoppdatering til Windows 8.1

Vi skal opprette en ny ADR for sikkerhetsoppdateringer til Windows 8.1. Men først må vi opprette en Collection for Windows 8.1-klienter. Dette gjør vi via Assets and Compliance→Device Collections. Oppretter her en ny mappe som heter Oppdateringer. Høyreklikker så på denne mappen og velger Create Device Collection. Kaller denne samlingen for Windows 8.1-klienter og velger All System under Limiting collection.

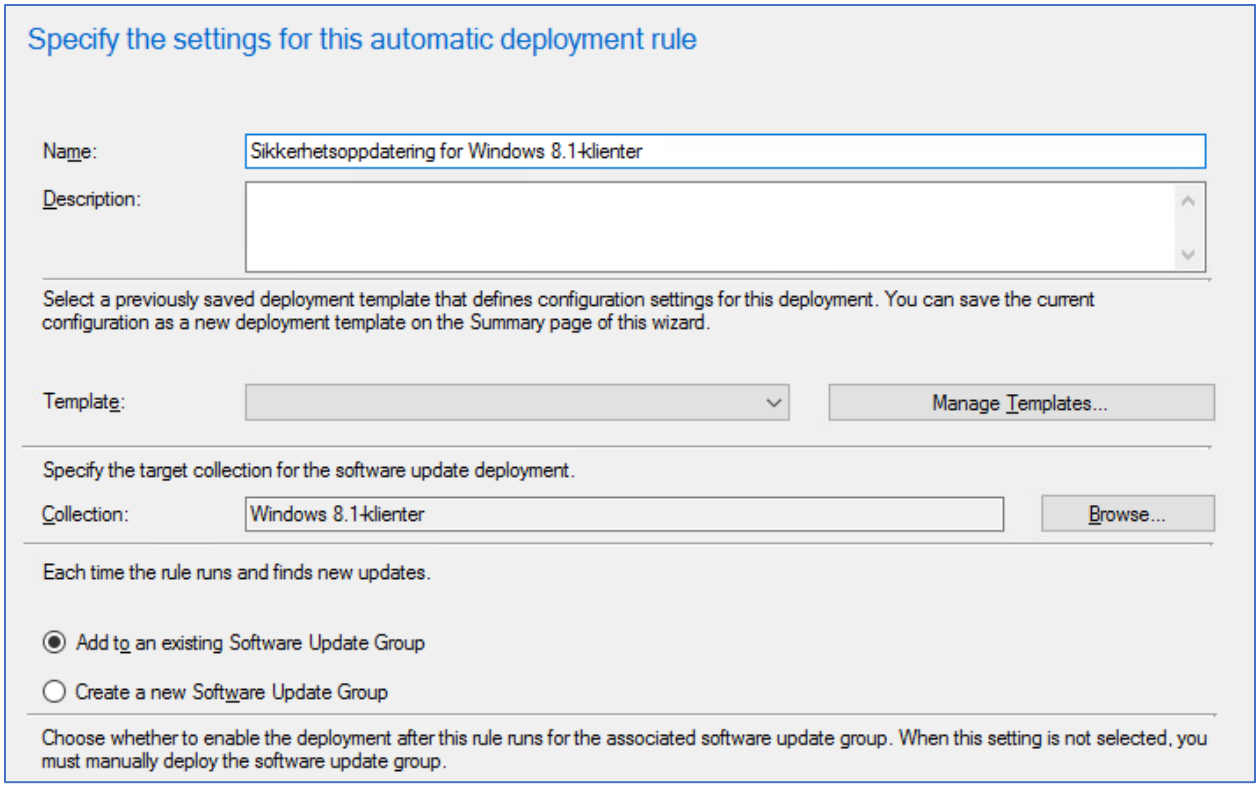


Når samlingen er opprettet, må vi klikke oss inn i Devices og finne Windows 8.1-klientene våre. I dette tilfellet har vi bare en klient med dette operativsystemet, Klient1. Høyreklikker så på Klient1 og velger Add Selected Items to existing Collection→Her finner vi den nye samlingen vi laget under Oppdateringer. Vi ser da at samlingen har fått et medlem.

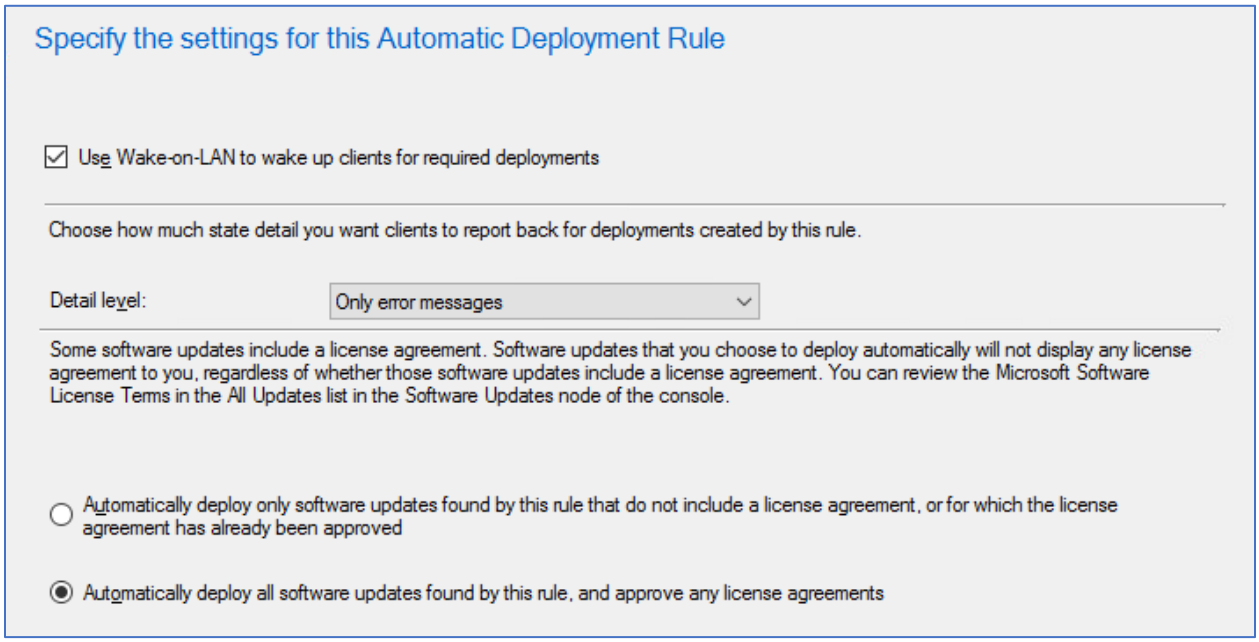


Vi navigerer oss til Software Library→Software Updates→Høyreklikker Automatic Deployment Rules→Create ADR.

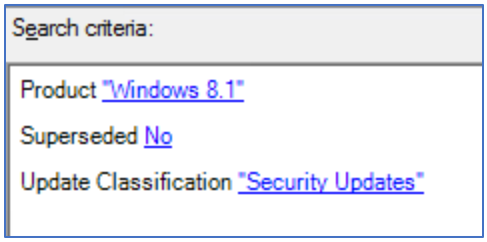
Her gir vi den navnet Sikkerhetsoppdatering for Windows 8.1-klienter, samt velger den nye samlingen vi laget under Collections.



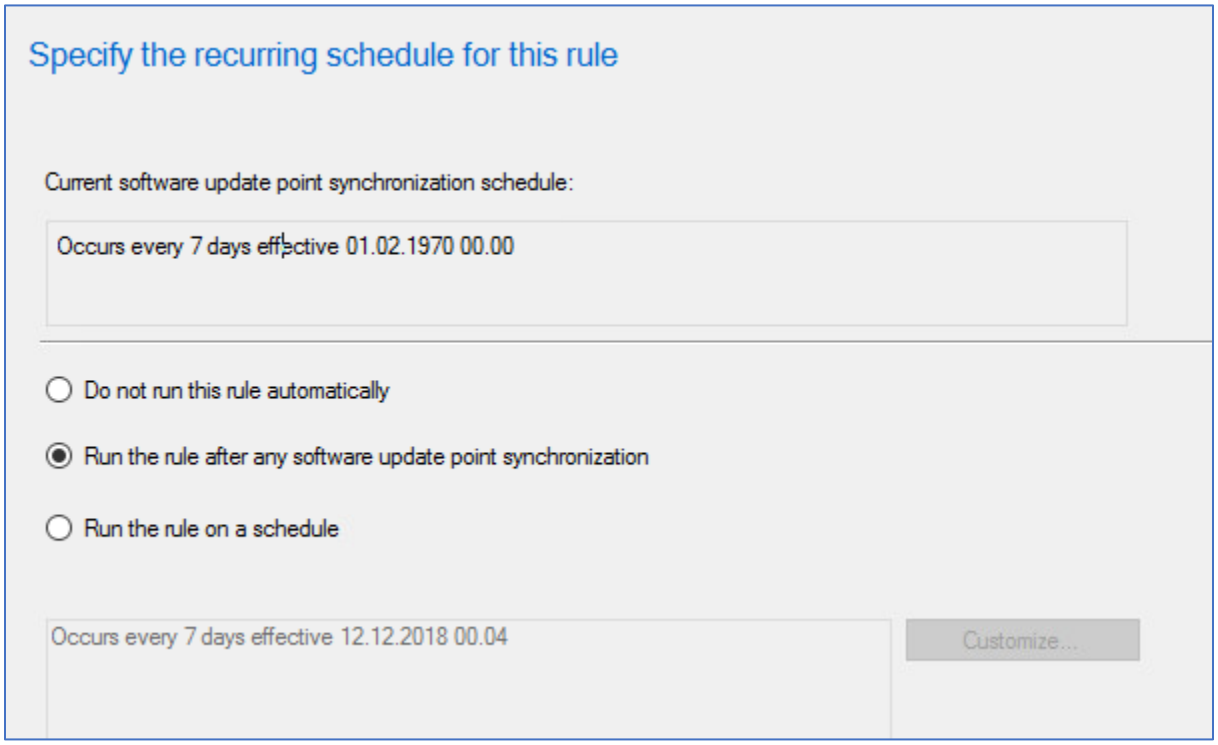
I det neste vinduet huker vi av Use Wake-on-LAN. Dette vil si at om klientmaskinene er avskrudd, kan systemet skru på klientene for å fullføre oppdateringene.



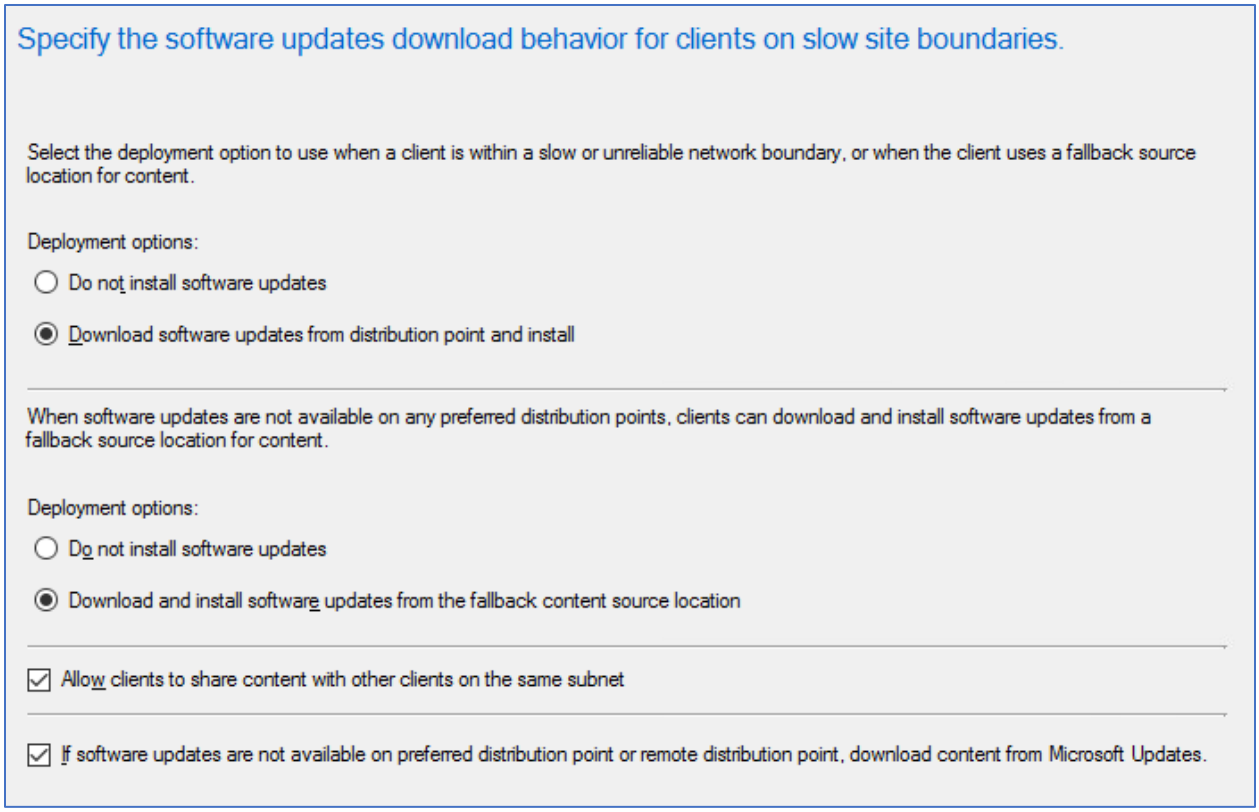
Under Software Updates må vi velge noen kriterier. Under Product velger vi Windows 8.1. Under Update Classification velger vi Security Updates. Vi velger også No under Superseded, slik at oppsettet blir seende slik ut:



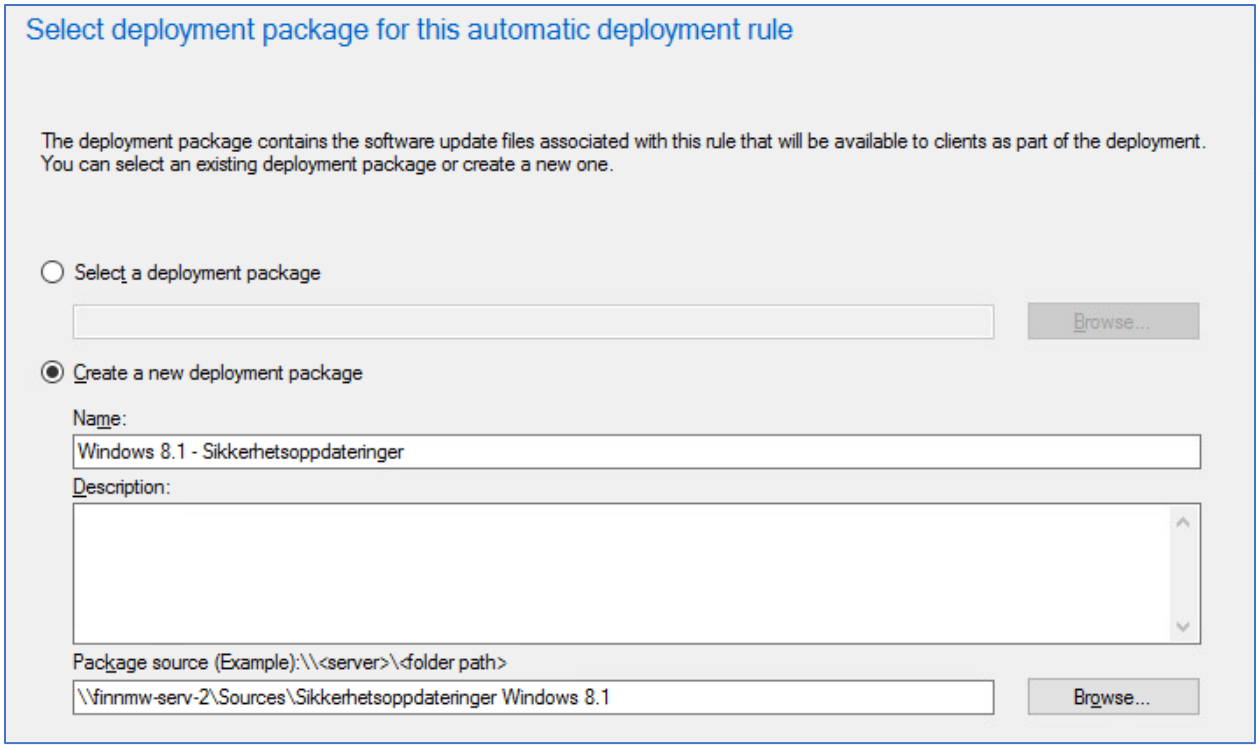
Under Evaluation Schedule velger vi Run the rule after any software update point synchronization. Her ser vi også at vi må opprette en plan for Software Update Point Synchronization i miljøet vårt, men det gjør vi etterpå.



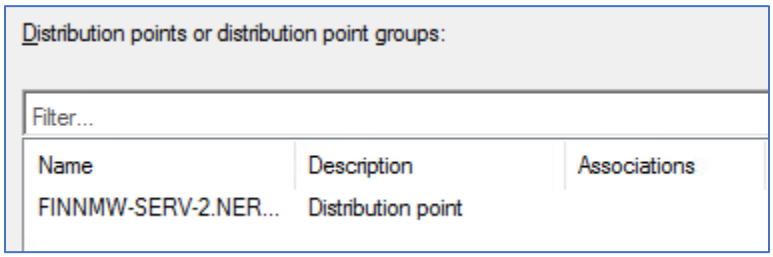
User Experience og Alerts lar vi stå som det er, mens vi under Download Settings velger Download software updates form distribution point and Install, samt huker av for If software updates are not avaliable on preffered distribution point or remote distribution point, download contant from Microsoft Updates.



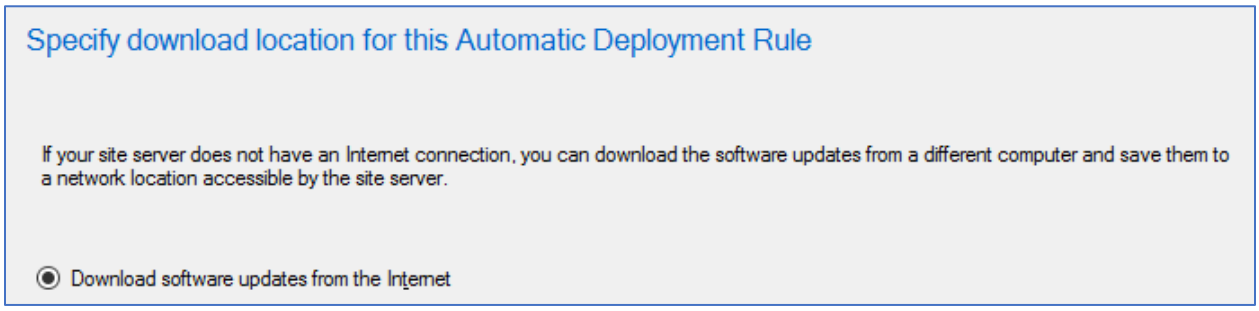
Under Deployment Package velger vi Create a new deployment package, kaller denne for Windows 8.1 Sikkerhetsoppdateringer. Under Package source må vi finne frem til Sources-mappen. Her må vi opprette en ny mappe som vi kaller Sikkerhetsoppdateringer Windows 8.1. Passer på så denne har rette innstillinger for deling og velger denne.



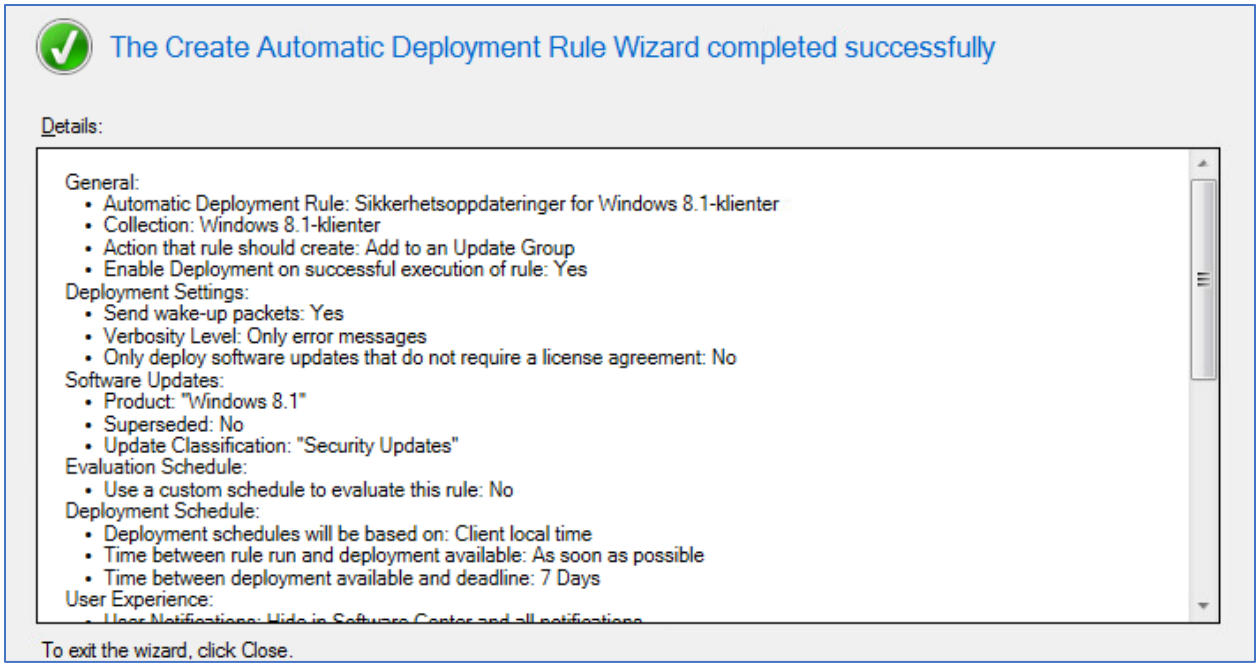
Under Distribition point velger vi SCCM-serveren.



Velger å laste ned oppdateringene fra internett.



På språk så velger vi bare engelsk, som vi har gjort på alt tidligere. Da er det bare å fullføre.



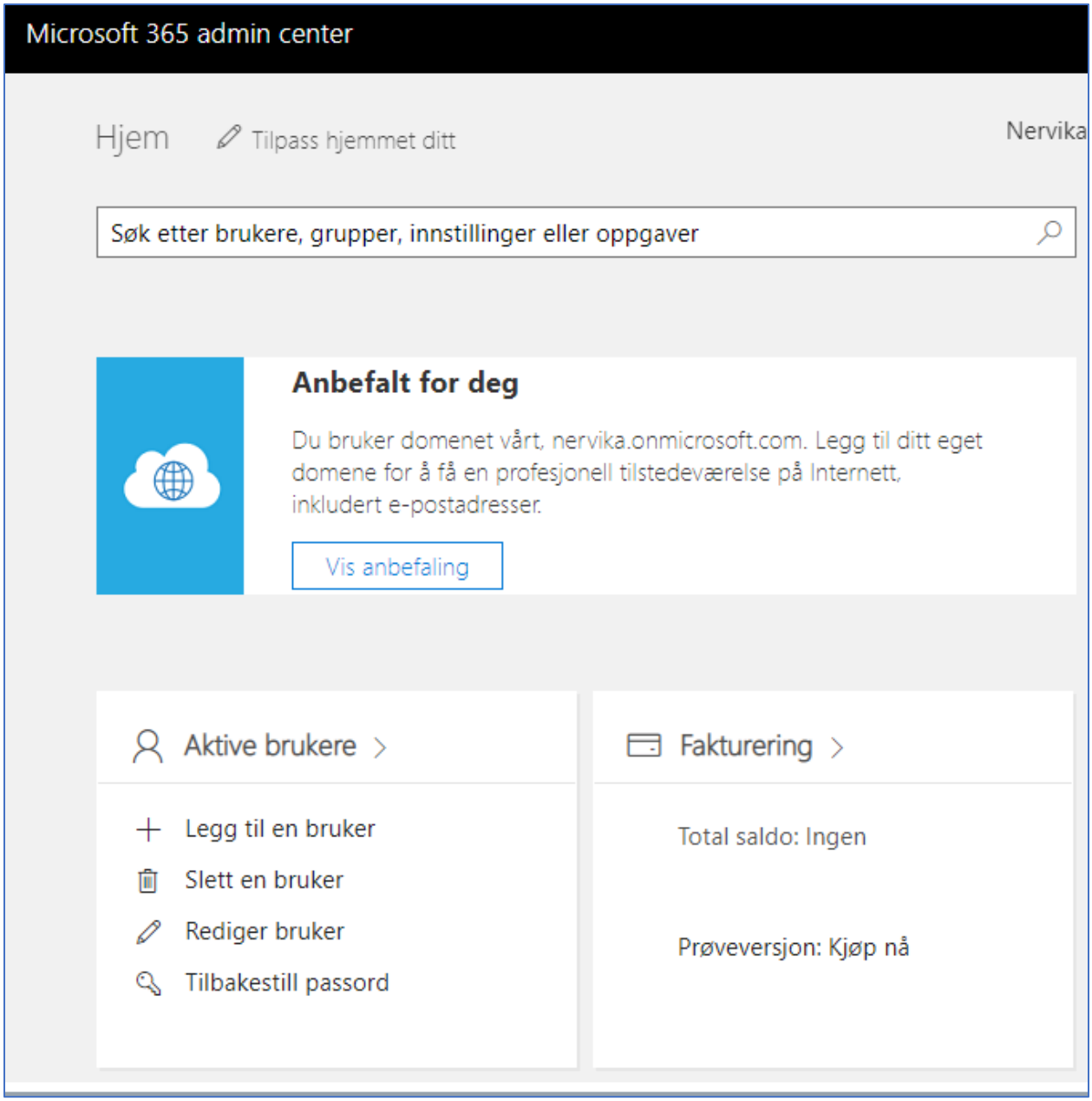
11. Microsoft Intune

I denne oppgaven skal vi også se på hvordan Microsoft Intune kan brukes sammen med System Center. Microsoft Intune er en skytjeneste som tilbyr styring av mobilenheter for bedrifter. Microsoft Intune kan også brukes sammen med System Center, slik at vi kan styre både PCer og mobilenheter på samme plass. I denne oppgaven skal vi sette opp en firmaportal for NerVika AS og koble den til System Center slik at de her kan distribuere applikasjoner til mobiltelefoner og nettbrett til sine ansatte.

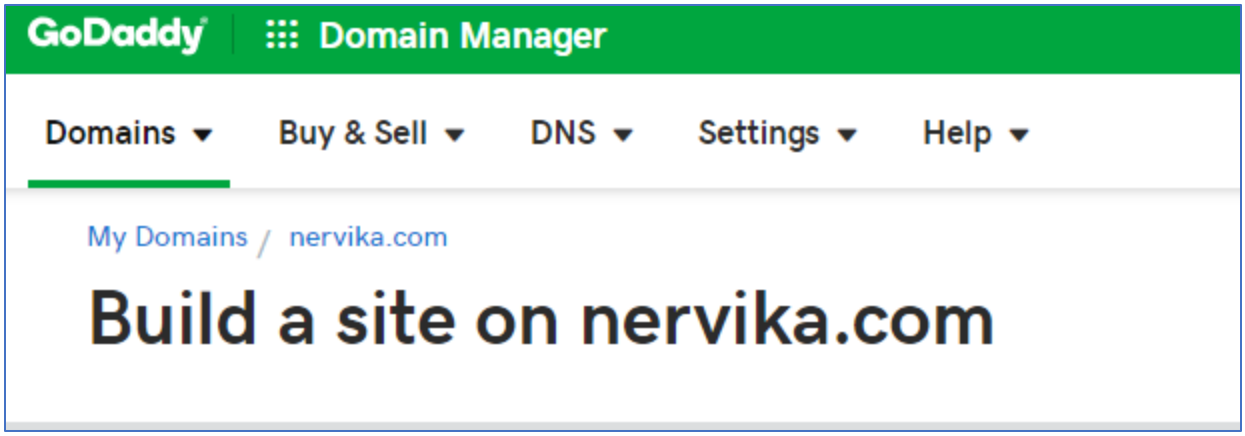
11.1 Opprette en Intune-bruker

Det første vi må gjøre er å registrere en Intune-bruker. Dette gjøres via portal.office.com, nærmere bestemt denne lenken: https://portal.office.com/Signup/Signup.aspx?OfferId=40BE278A-DFD1-470a-9EF7-9F2596EA7FF9&dl=INTUNE_A&ali=1#0%20

Her er det bare å fylle inn informasjonen som trengs om bedriften, når brukeren er opprettet kommer vi til adminportalen, www.portal.office.com/adminportal. Nervika AS sin portal ser slik ut:



Her ser vi at vi blir anbefalt å legge til vårt domene, men dette går ikke siden vi kun har et lokalt domene. Derfor har vi kjøpt rettigheter til nervika.com via godaddy.co.uk.

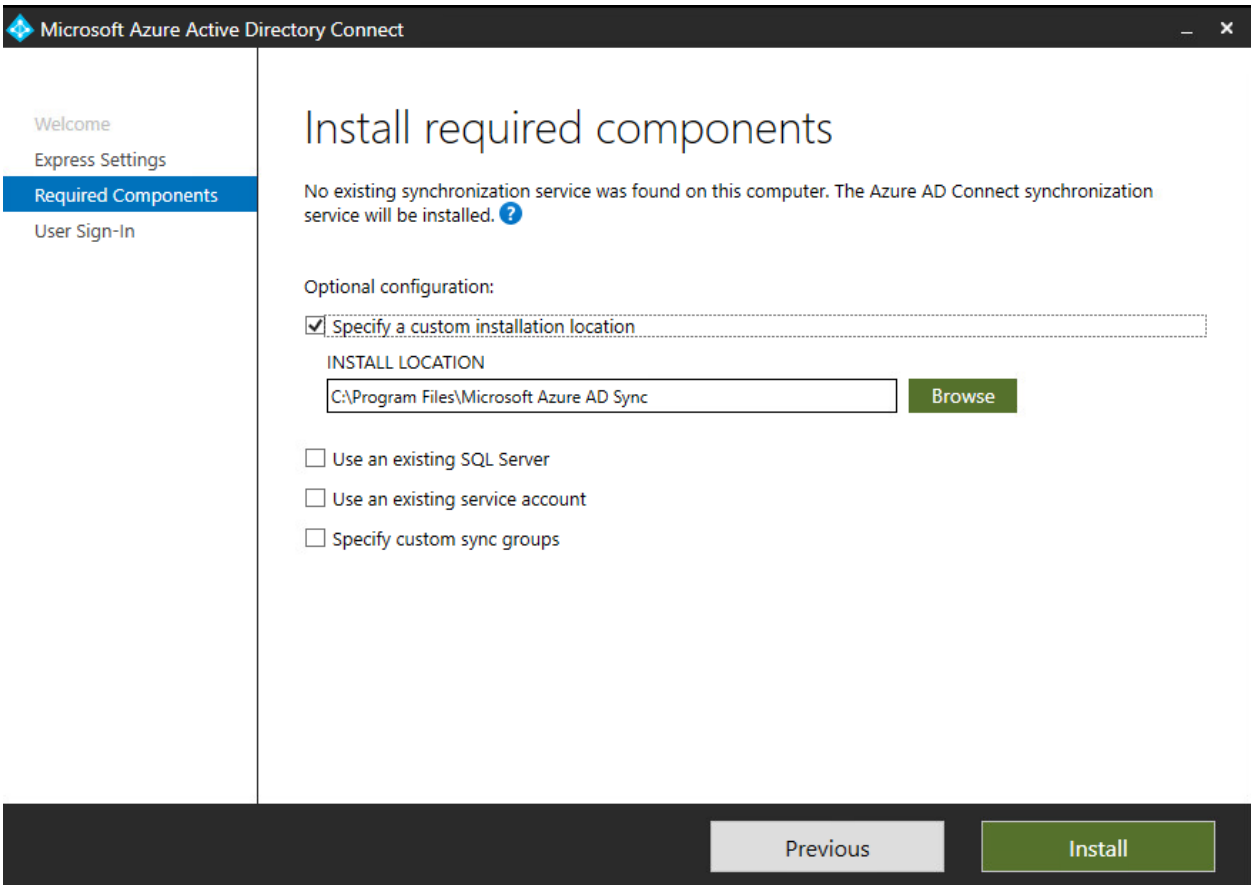


Nå kan vi legge til domene i Office Admin Center. Trykker derfor på anbefalingen og trykker legg til domene. Her skriver vi inn nervika.com. Så må vi bekrefte domenet. Velger her det første alternativet.

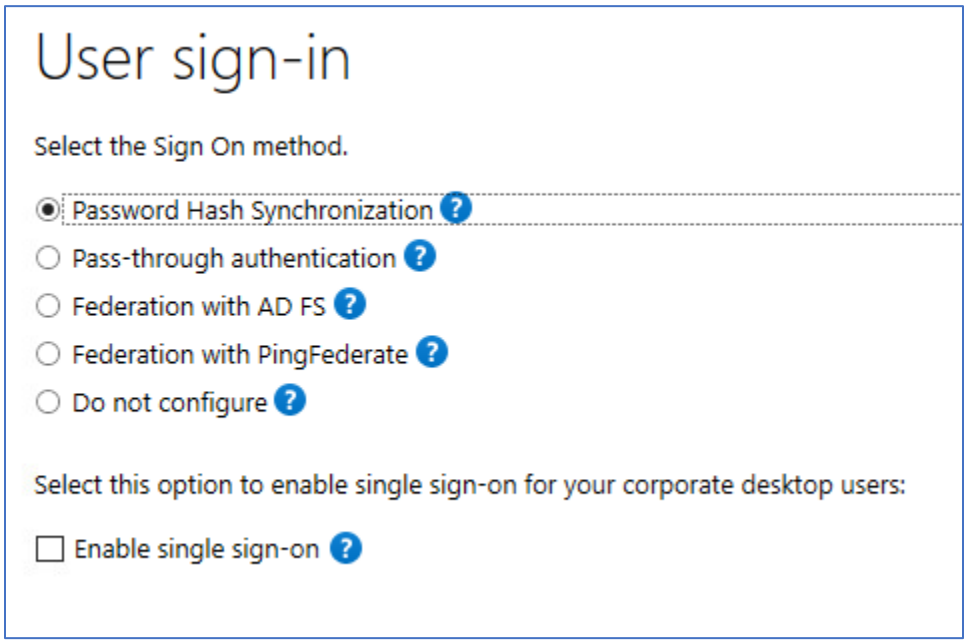
11.2 Synkronisere Active Directory

Når domenet er opprettet, må vi synkronisere de lokale brukerne og gruppene fra ADen vår med Azure Active Directory. I Microsoft Admin Center trykker vi på Aktive brukere→Mer→Katalogsynkronisering. Her vil vi få muligheten til å laste ned Microsoft Azure Active Directory Connect. Dette verktøyet må vi laste ned på AD-serveren vår. Verktøyet finner vi på linken: https://www.microsoft.com/en-us/download/details.aspx?id=47594

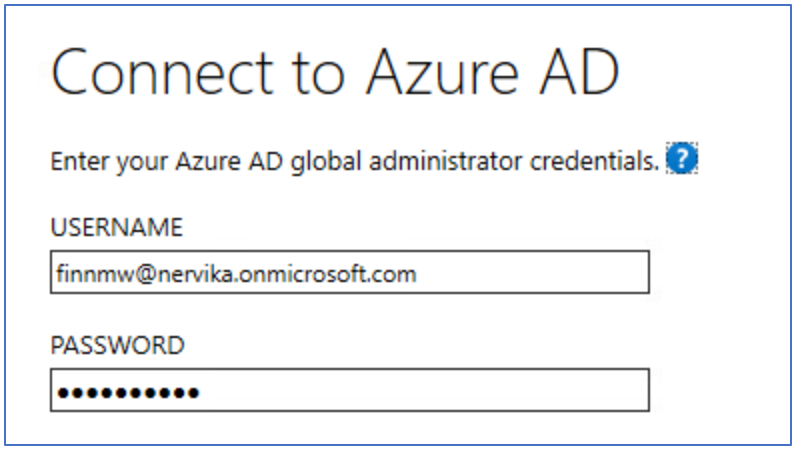
Her er det bare å trykke på download og velge Run. Installasjonen av Microsoft Azure Active Directory Connect vil da starte. Her velger vi Custom Settings. Fyller inn informasjonen som er nødvendig for installasjonen:



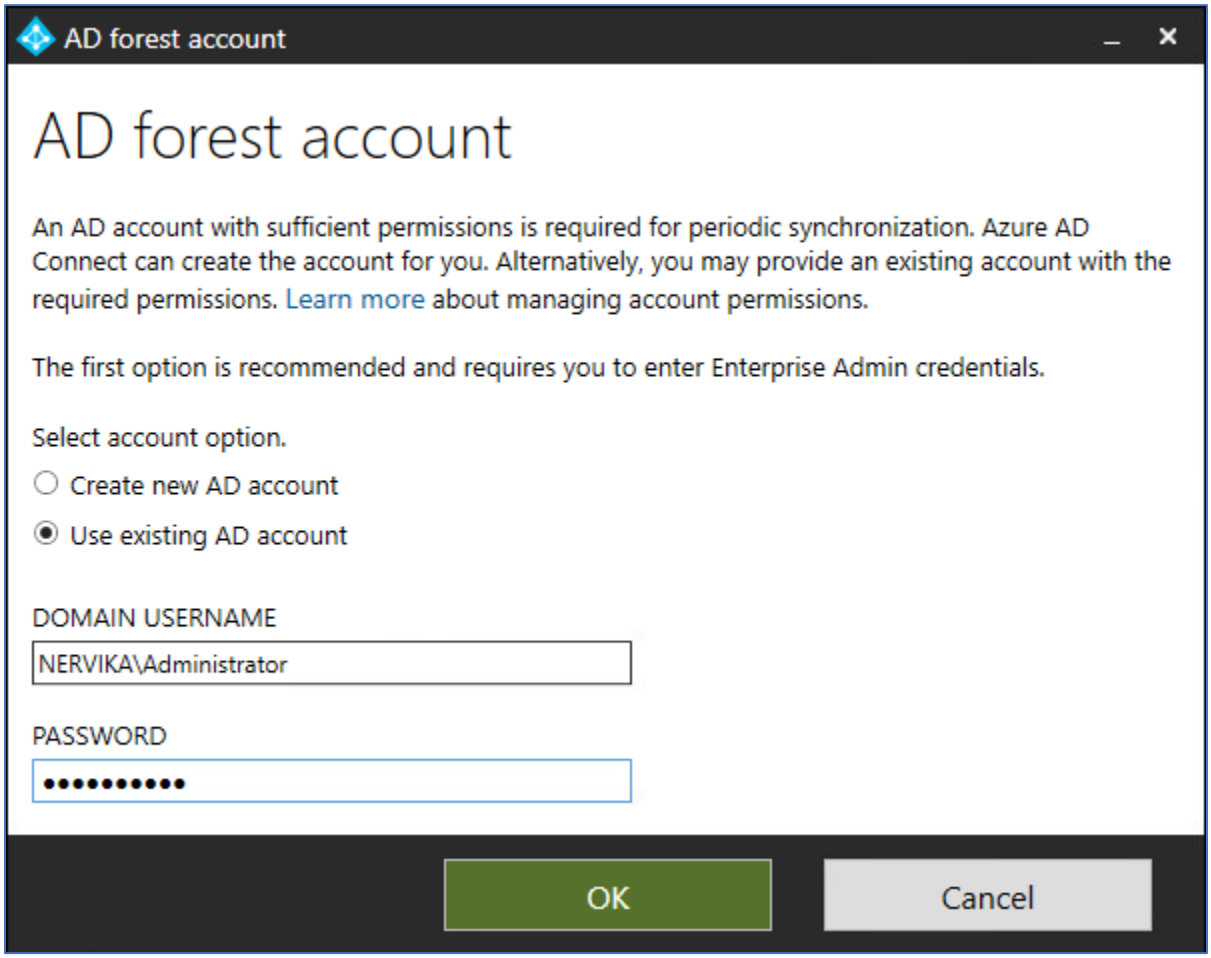
På User Sign-in velger vi Password Hash Synchronization.



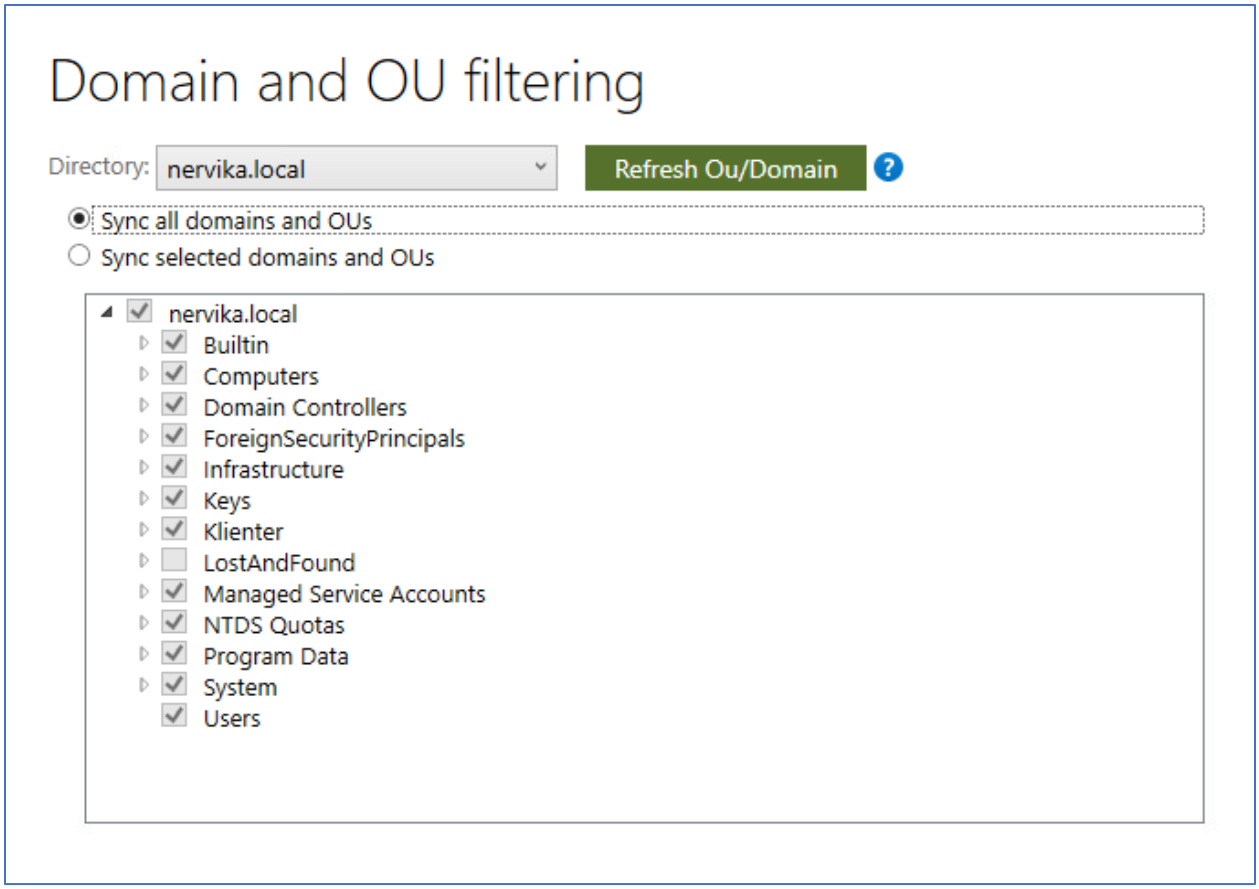
Under Connect to Azure legger vi inn opplysningene til administratoren på nervika.com



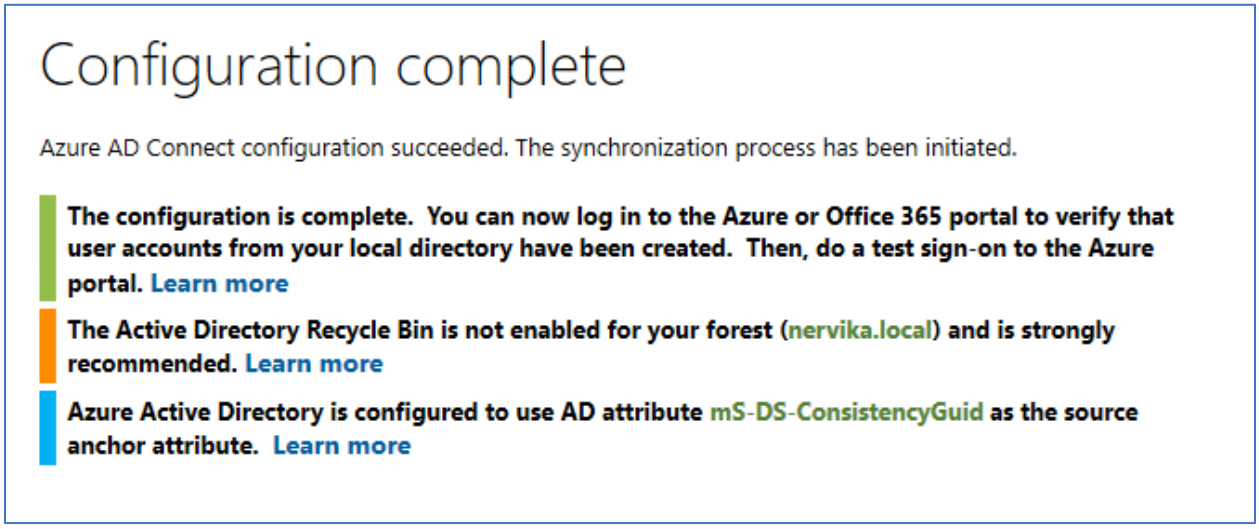
Velger nervika.local som forest under Sync. Trykker Add og logger på med domeneadministratoren



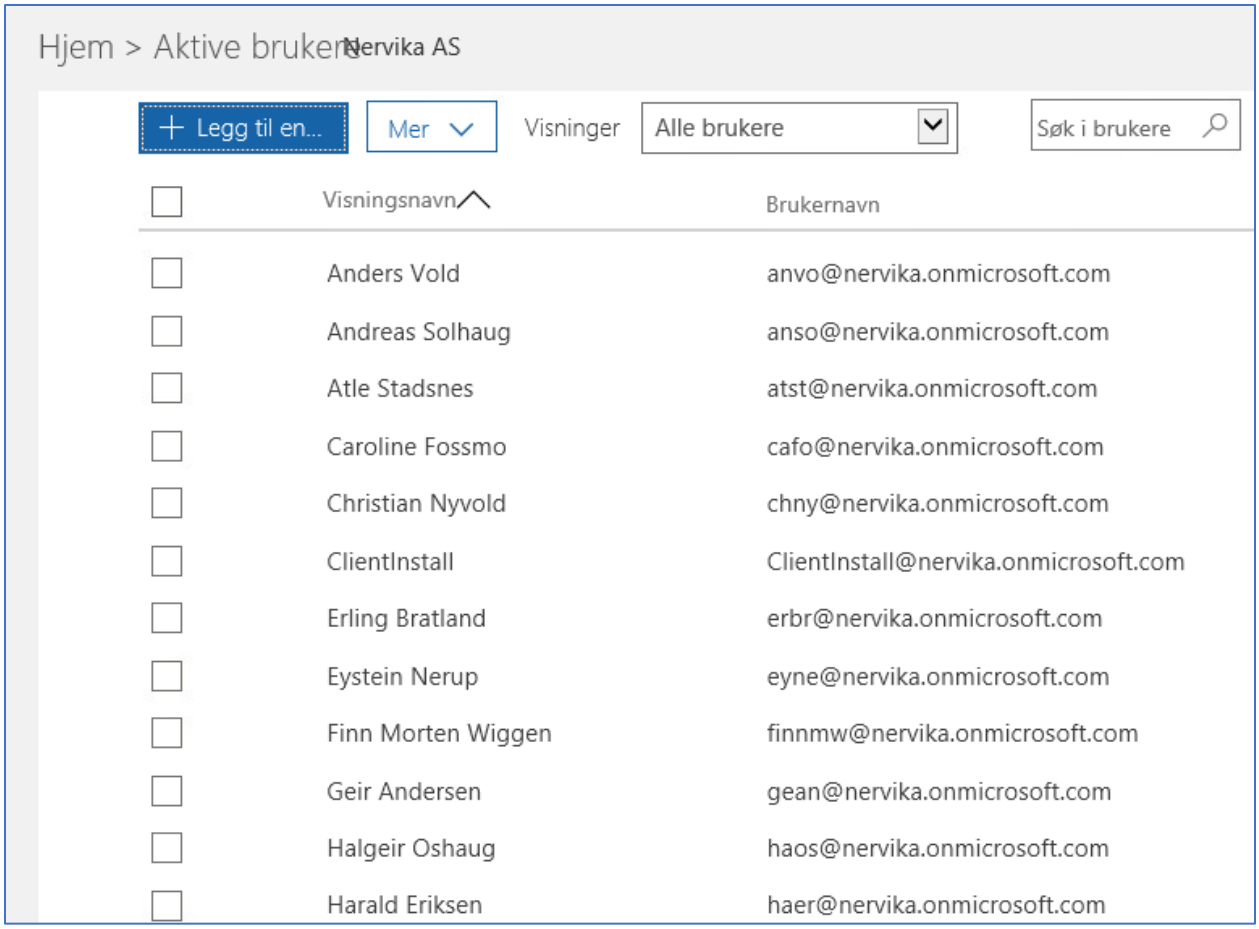
Velger å synke alt fra Active Directoryen.



Nå er det bare å trykke Next frem til synkroniseringen starter. Når synkroniseringen er ferdig kommer det forhåpentligvis opp et vindu som sier at Azure AD Connect configuration succeeded.



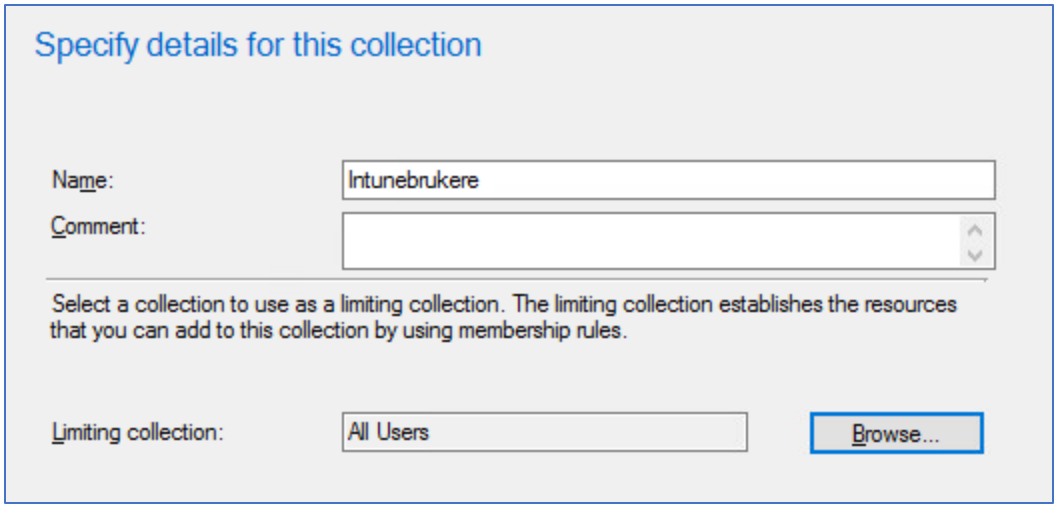
Vi kan da se i Admin Center at brukerne har blitt synkronisert



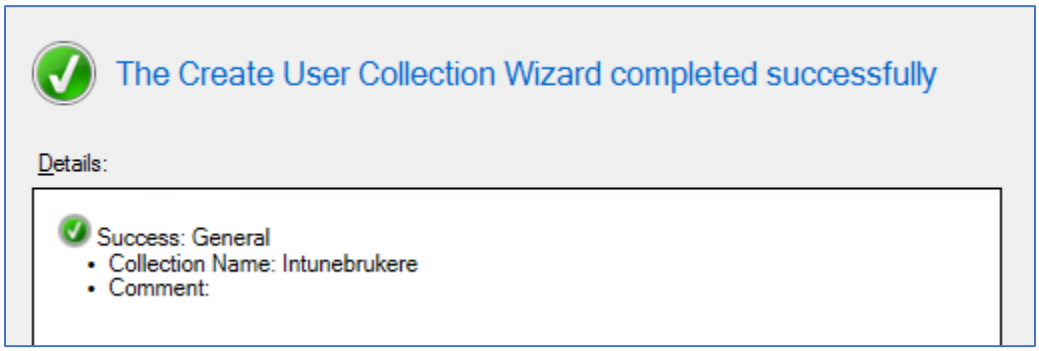
11.3 Opprette Collection for Intune.

Nå må vi opprette en User Collection for Intune. Vi navigerer oss til Assets and Compliance →Overview→User Collections. Her høyreklikker vi og velger Create User Collection.

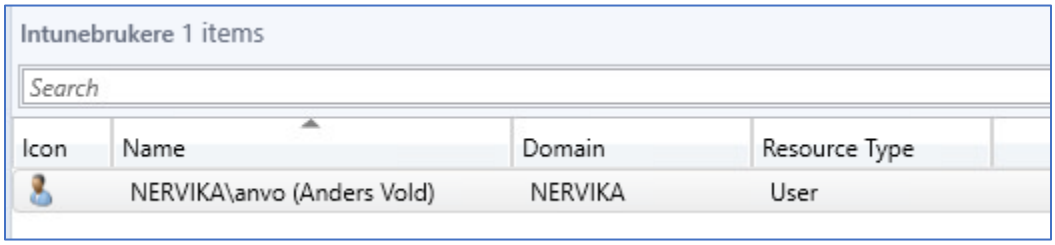
Kaller den enkelt å greit for Intunebrukere og velger All Users under Limitation.



Foreløpig trenger vi ikke å sette noen regler, så vi trykker bare Next og fullfører.



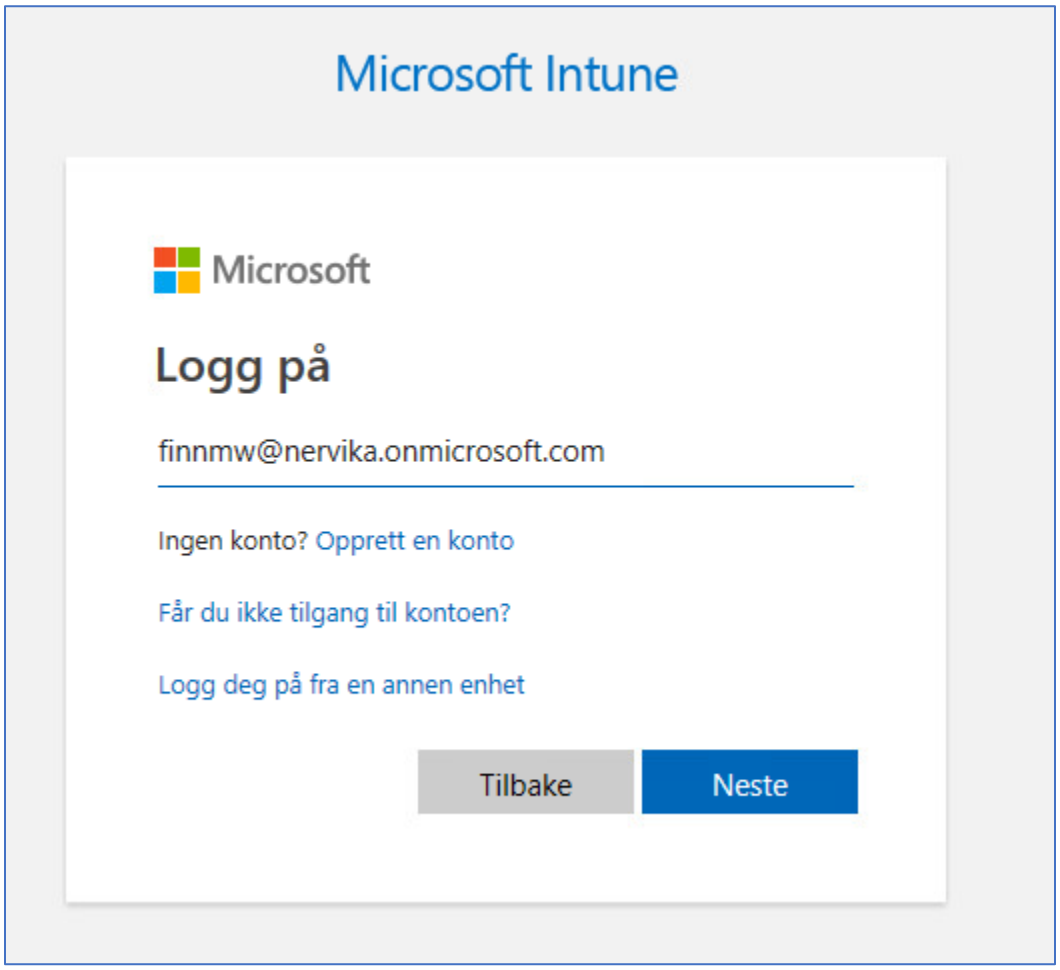
Nå går vi tilbake til Users under Assets and Compliance. Velger her brukeren Anders Vold (Nervika\anvo). Høyreklikker på denne brukeren og velger Add Selected Items to Existing Collection. Her velger vi å legge brukeren anvo til i Intunebrukere.



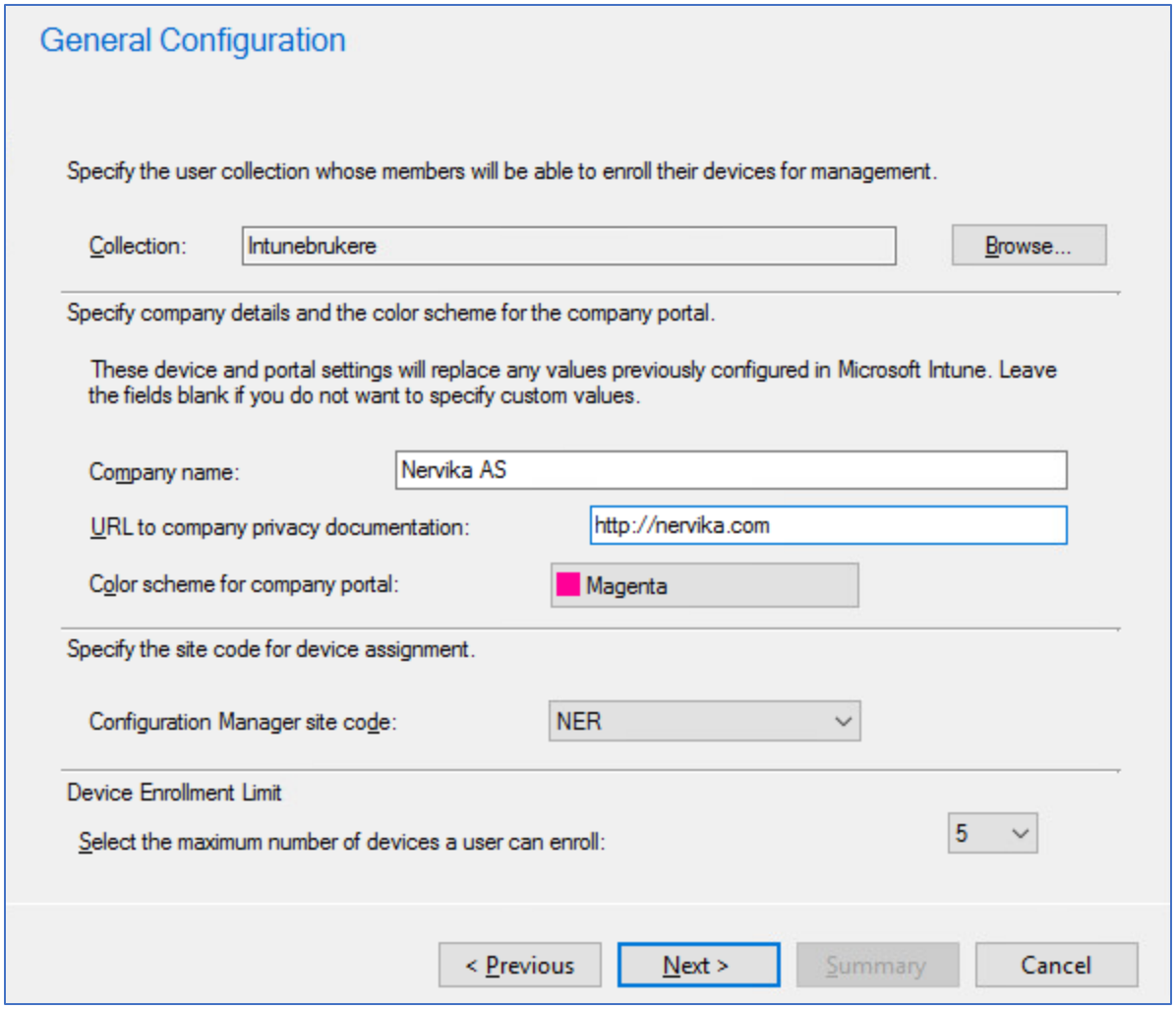
11.4 Legge til Microsoft Intune Subscription

For å legge til Microsoft Intune Subscription må vi navigere oss til Administration→Cloud Services→Microsoft Intune Subscribtions. Her må vi høyreklikke og velge Add Microsoft Intune Subscription. .

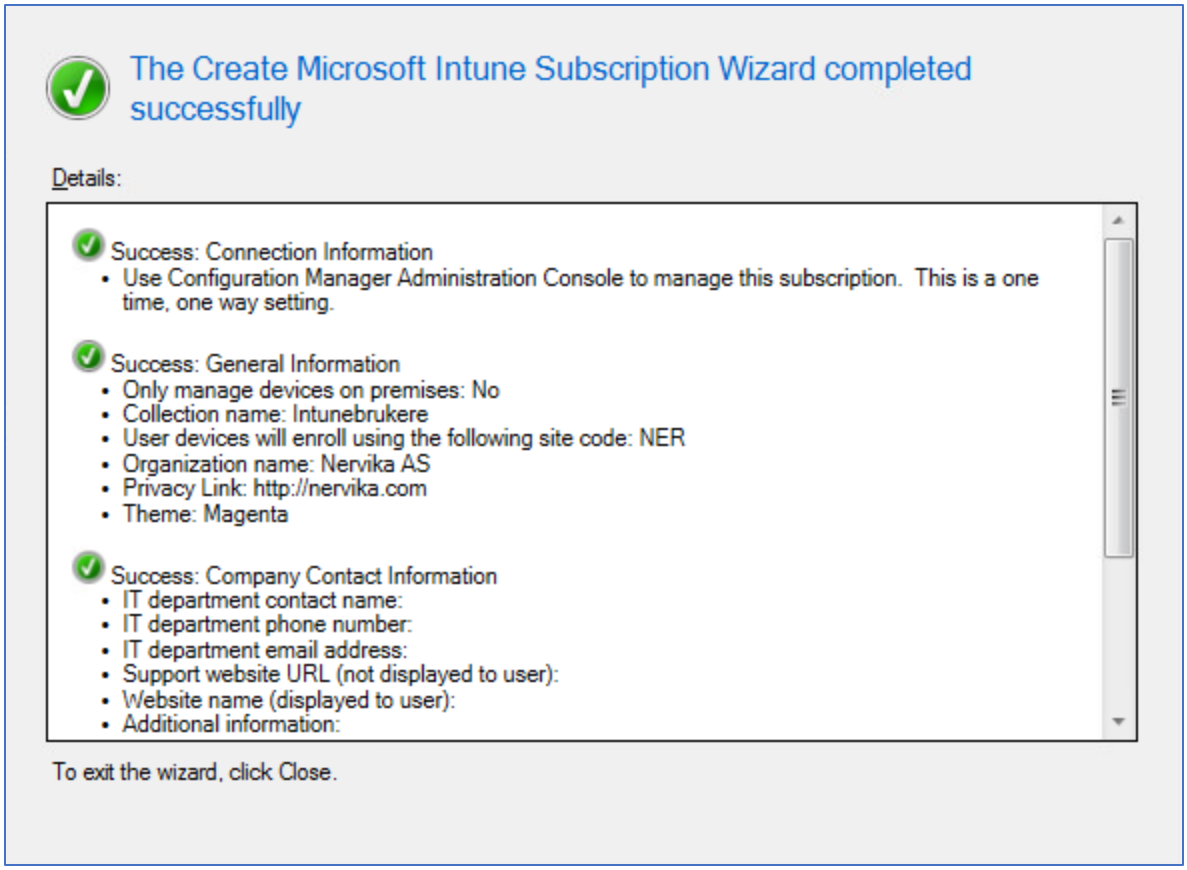
Her må vi klikke Sign in og legge til informasjon om vår Intune-bruker.



I General-fanen må vi legge til Collection som vi nettopp laget, Intunebrukere. Ellers må vi bare fylle inn informasjon om bedriften vår.

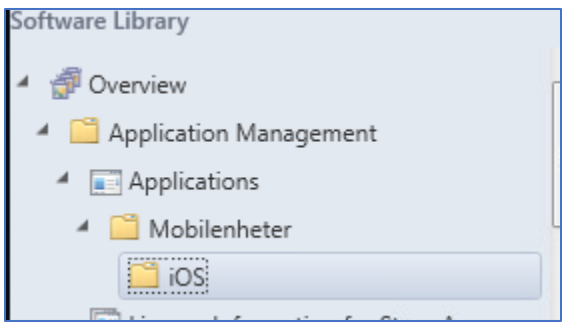


Nå er det bare å trykke seg videre frem til installasjonen.

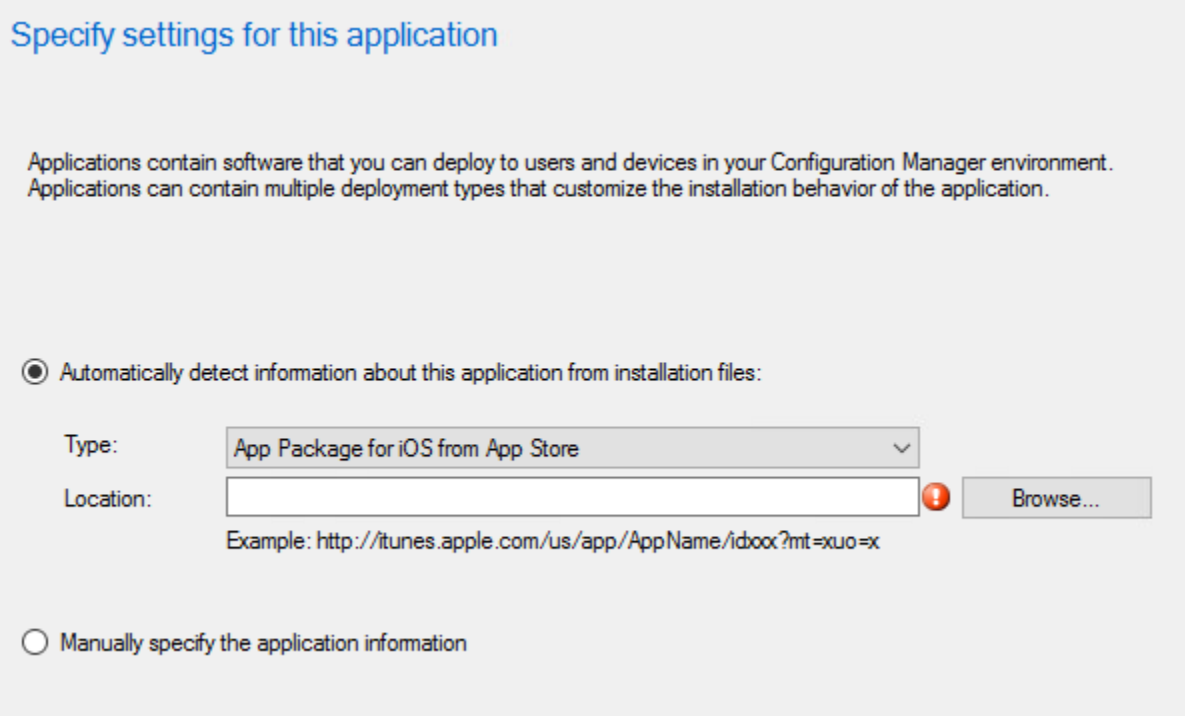


11.5 Utrulling av apper med SCCM

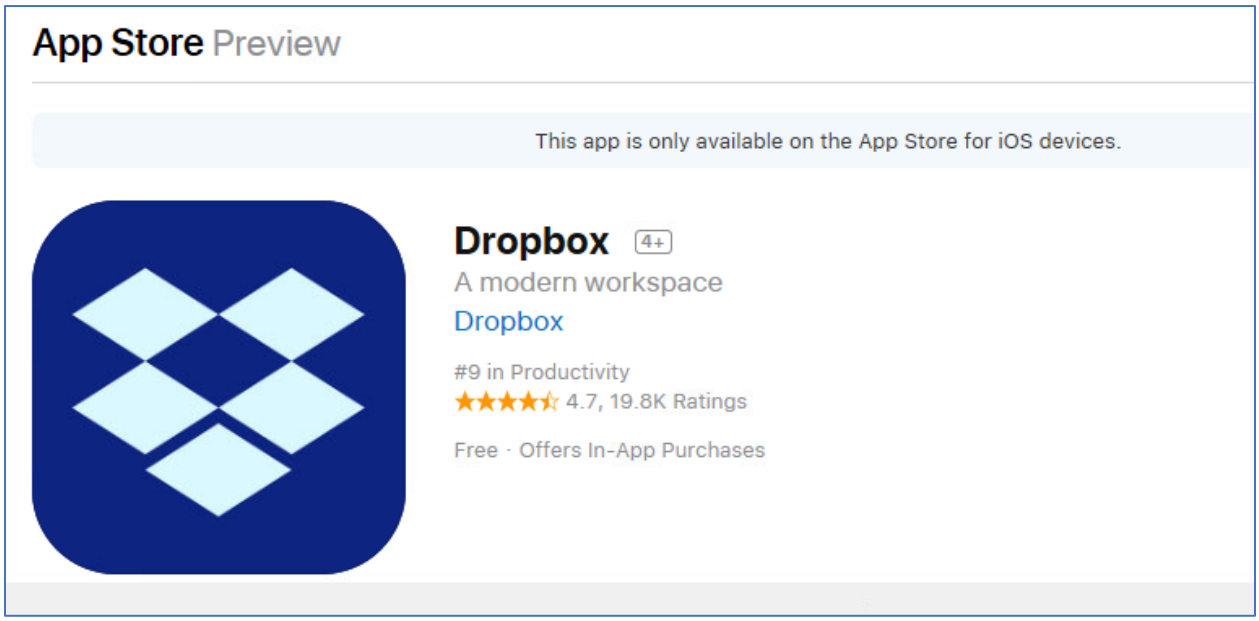
Det første vi må gjøre er å opprette en ny mappestruktur i Configuration Manager. Vi åpner Software Library. Her finner vi Applications. Der ser vi at vi bare har Mozilla Firefox liggende fra tidligere. Men nå skal vi opprette en mappe her. Høyreklikk på Applications→Folder→Create Folder. Kaller denne mappen for Mobilenheter. Høyreklikker på denne mappen også→Folder→Create folder. Kaller så denne undermappen for iOS, siden jeg har en mobil med iOS. Mappestrukturen skal da se slik ut:



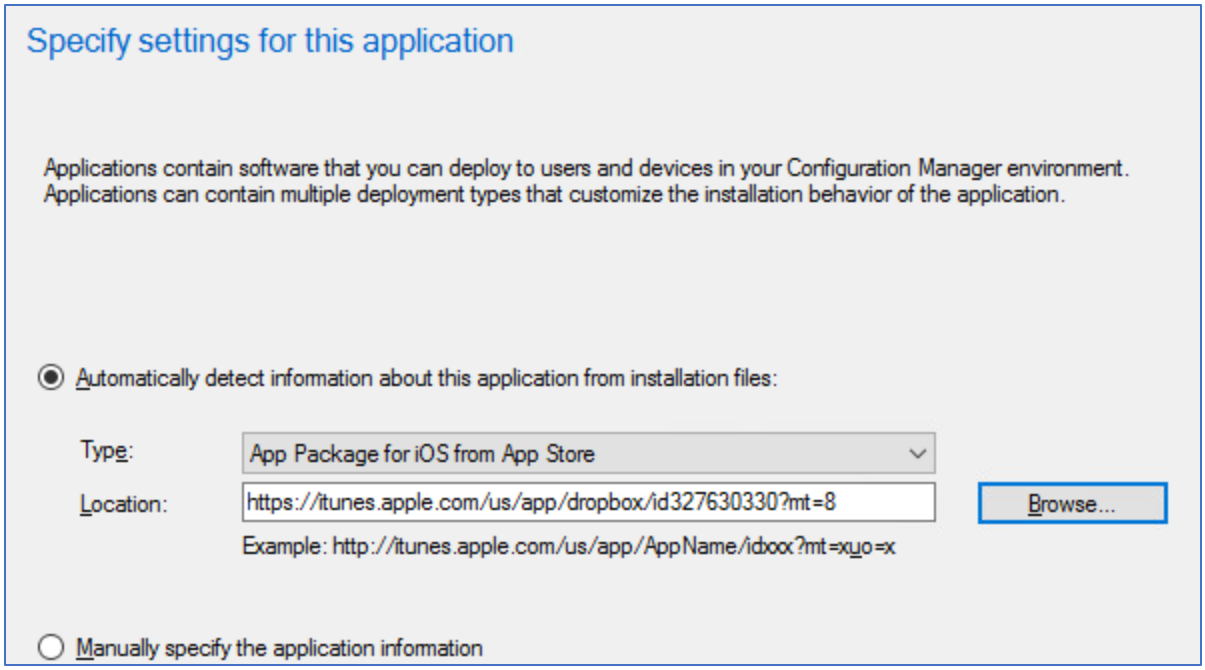
Nå høyreklikker vi på iOS-mappen og velger Create Application. Når vi rullet ut applikasjoner til klientmaskiner, valgte vi Windows Installer som Type. Men nå skal vi Rulle ut til mobilenheter, så da velger vi App Package for iOS from App Store.



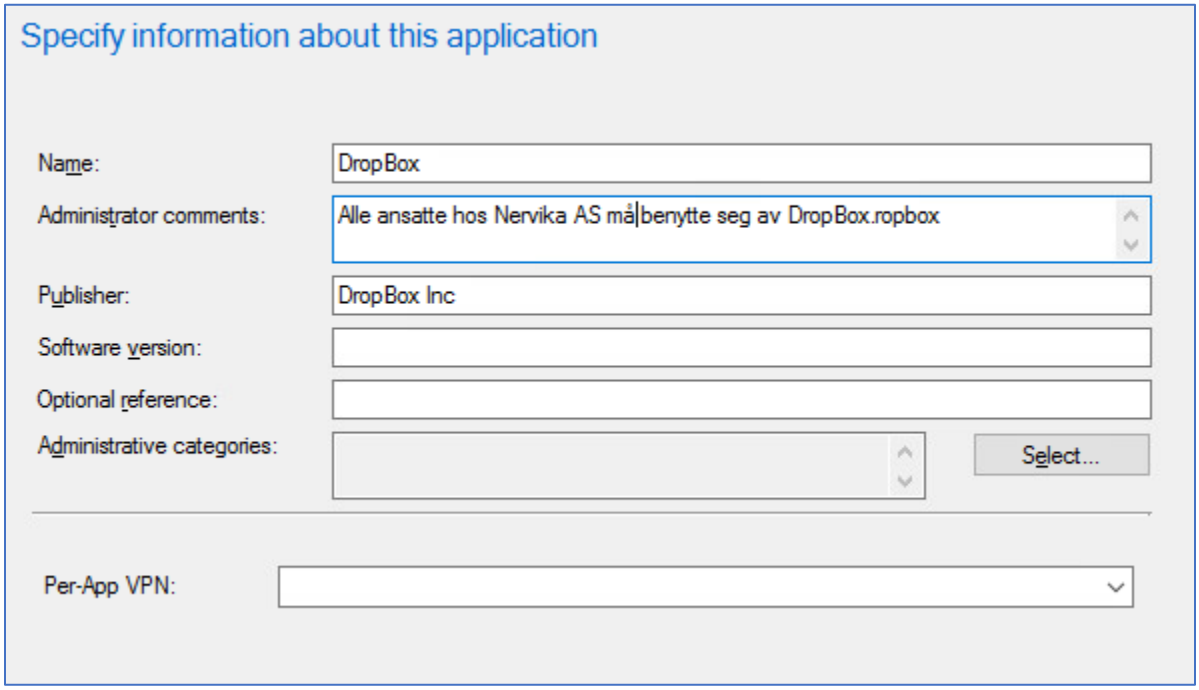
Når vi da trykker Browse vil vi komme til en side som lar oss bla igjennom appene som finnes i App Store. Her navigerer vi oss til Productivity og velger Dropbox.



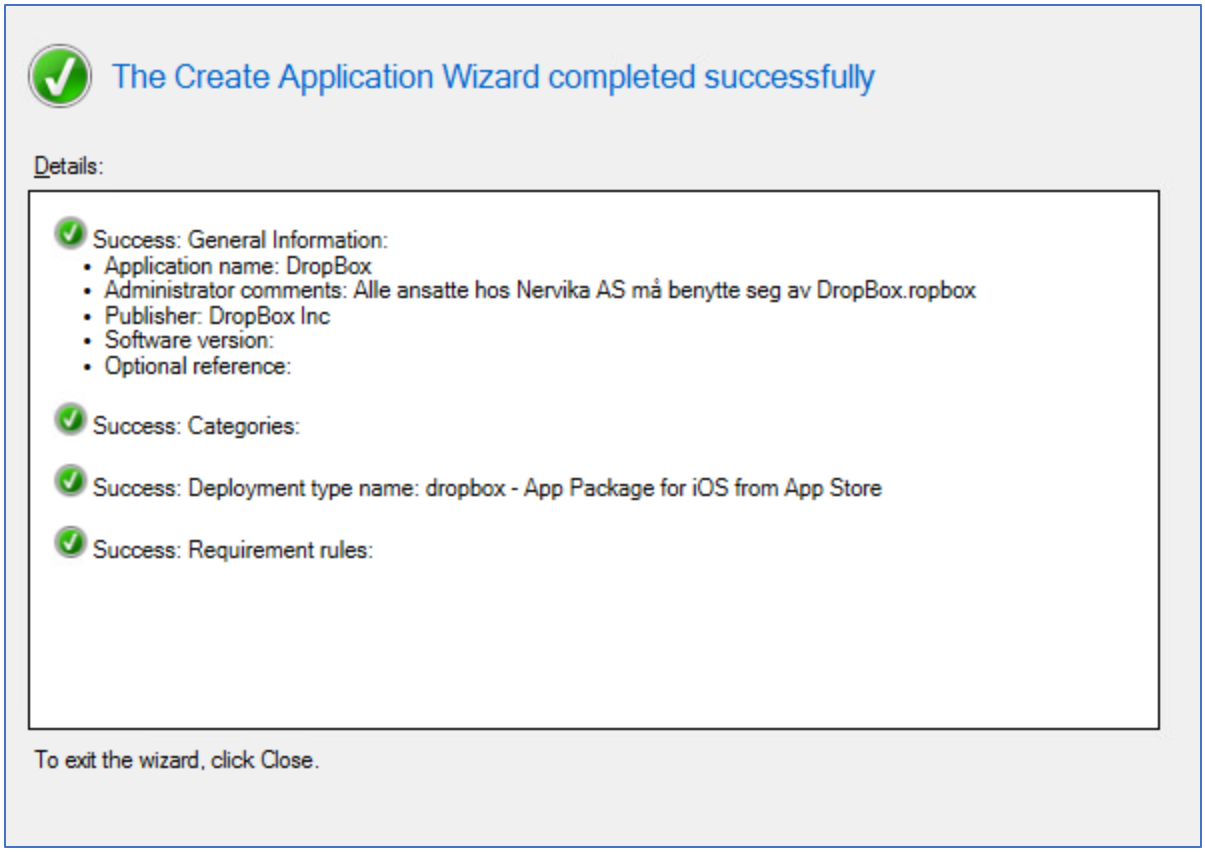
Trykker så på OK.



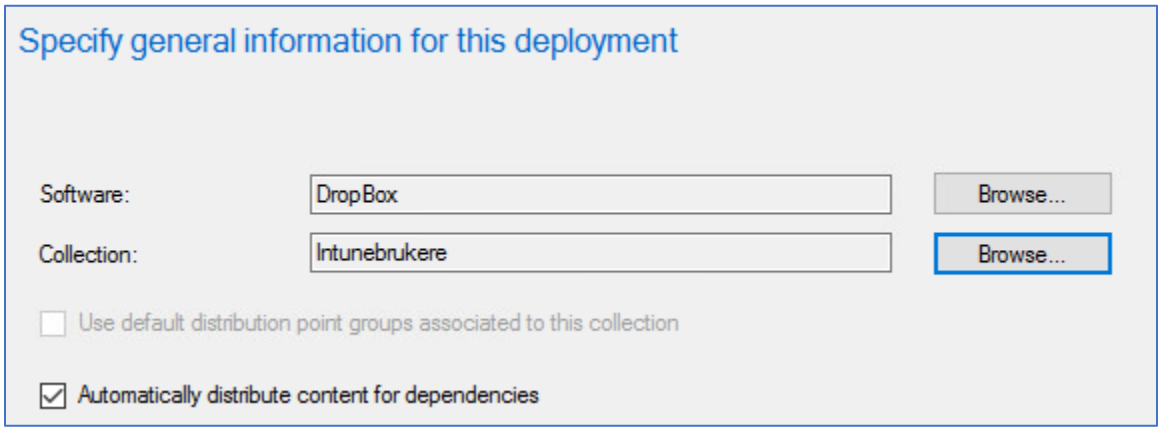
Nå er det bare å trykke Next til vi kommer til General Information. Her kan vi legge til litt informasjon om appen.



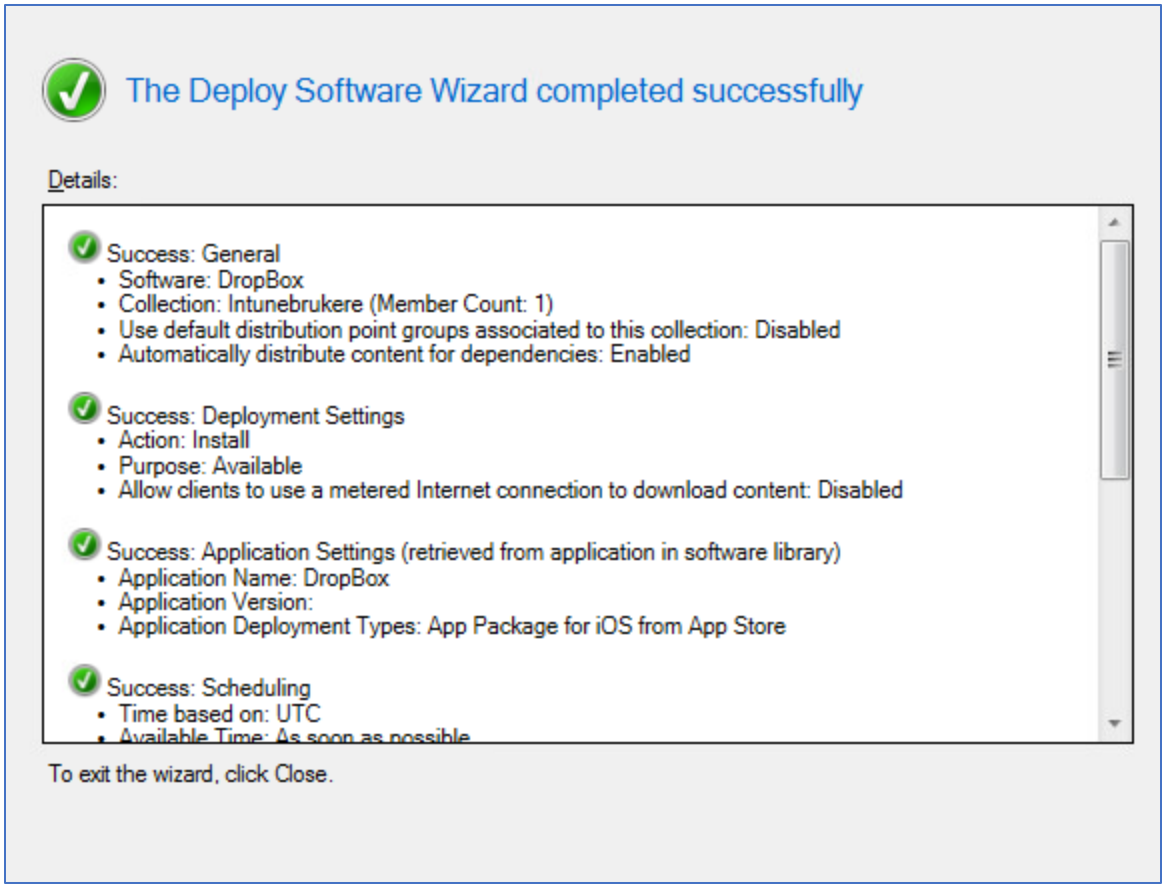
Nå er det bare å fullføre



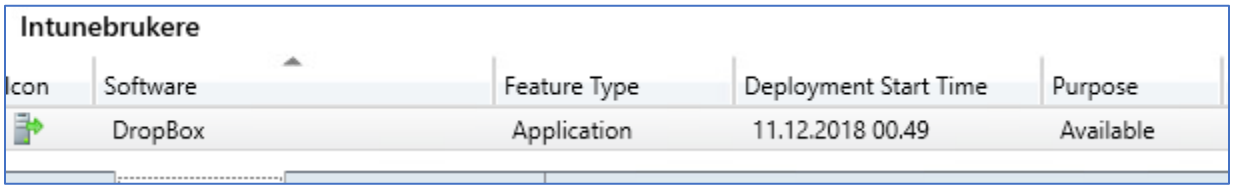
Nå ser vi at DropBox ligger i iOS-mappen. Nå kan vi høyreklikke på DropBox å velge Deploy. Under General-fanen må vi velge hvem vi skal rulle ut til. Her velger vi Intunebrukere.



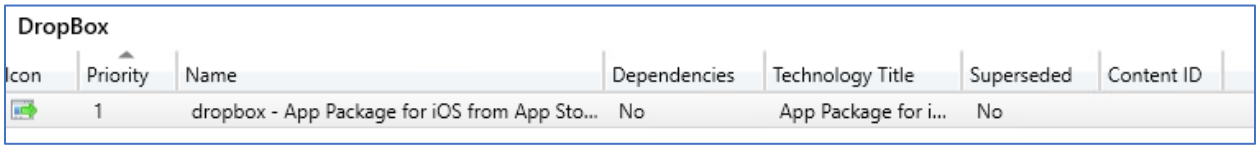
Alt annet kan vi la stå som det er, så vi bare trykker oss videre til vi kan fullføre.



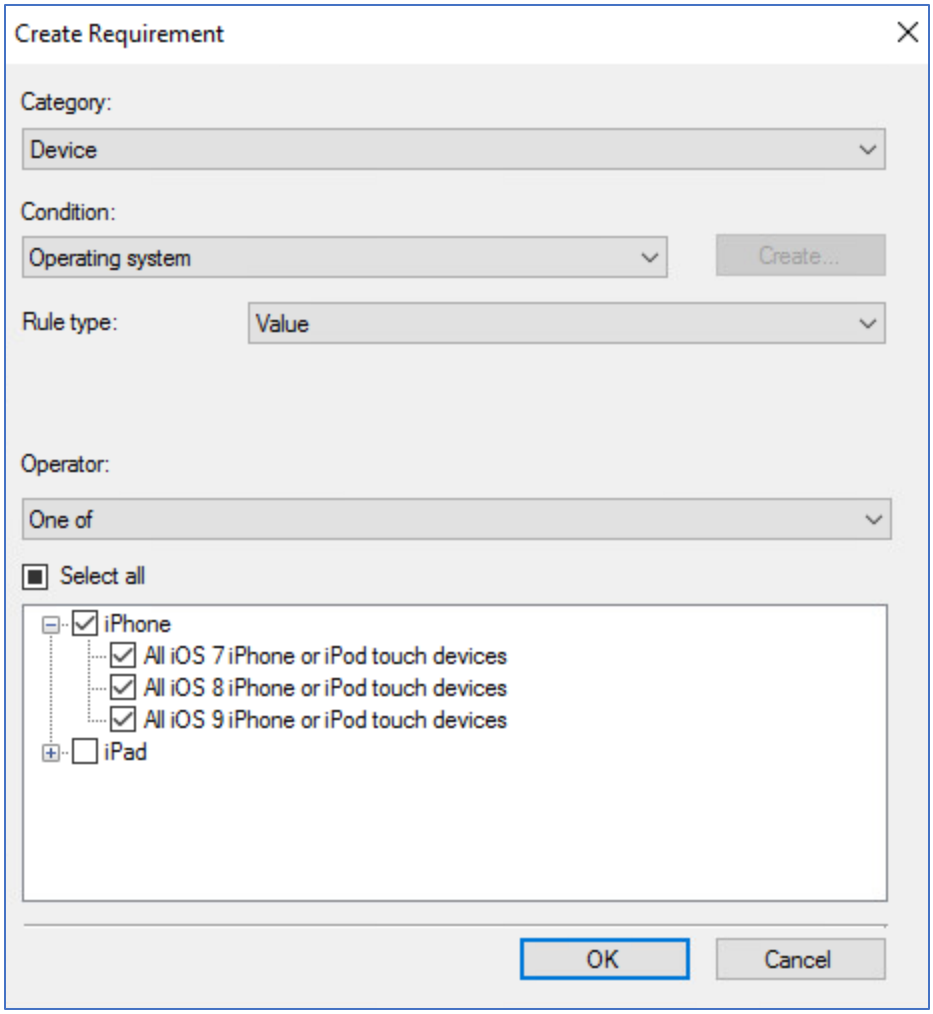
Hvis vi nå trykker oss inn og ser på Intunebrukere under User Collections kan vi se at DropBox ligger under Deployments.



Nå skal vi tilbake til iOS-mappen. Helt nederst er det tre faner, Summary, Deployment Types og Deployments. Vi skal velge Deployment Types.

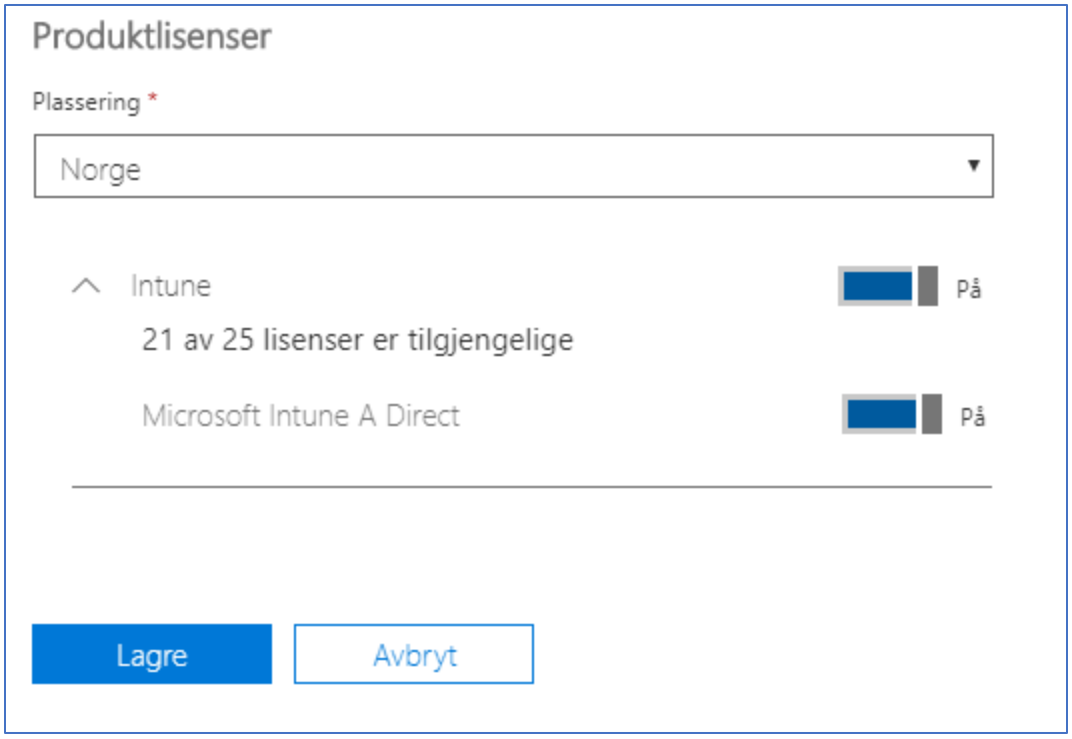


Her skal vi hyreklikke på dropbox – App Package→Properties. Trykke oss frem til Requirements-fanen og velge Add. Her velger vi Device under Category og Operating System under Condition. Huker av for iPhone og de tre undervalgene.



11.6 Brukeropplevelse

For å teste om dette faktisk fungerer, må vi gi en bruker lisens til å bruke Intune. Logger derfor inn på portal.office.com→Aktive brukere. Her finner vi brukeren Anders Vold(anvo). Trykker på denne brukeren. Under produktlisenser ser vi at ingen produkter er tildelt. Trykker her på Rediger. Velger så at anvo befinner seg i Norge og huker av for Intune.



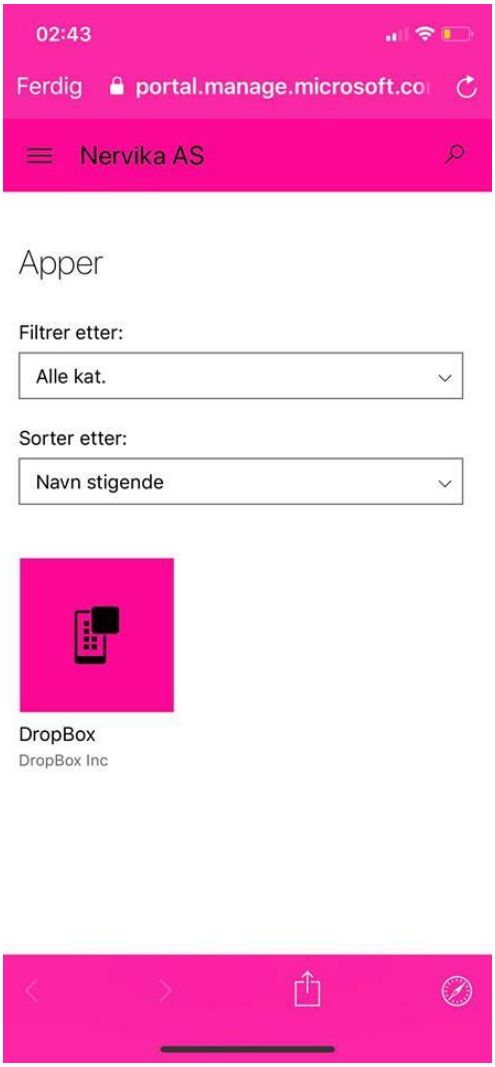
Nå kan vi se at anvo har fått tilgang til Intune, mens en annen bruker, anso, fremdeles ikke har fått det.

☐	Anders Vold	anvo@nervika.onmicrosoft.com	Intune	Synkronisert ...
☐	Andreas Solhaug	anso@nervika.onmicrosoft.com	Ulisensiert	Synkronisert ...

Nå må vi bruke en iPhone. Åpner AppStore og laster ned appen Firmaportal for Intune. Her velger vi innloggingsopplysningene til anvo.

Når vi er logget inn vil vi komme til hovedsiden til Nervika AS. Opp til høyre ser vi at vi er logget inn som AV – Anders Vold.

Trykker vi på Apper, vil vi forhåpentligvis få opp DropBox.


02:43
Ferdig
portal.manage.microsoft.co
Nervika AS
Apper
Filtrer etter:
Alle kat.
Sorter etter:
Navn stigende
DropBox
DropBox Inc