

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	3
2. Installasjon av Active Directory.....	3
3. Installasjon av Microsoft System Center.....	8
3.1 Installasjon av SQL 2016 Server	8
3.2 Oppdatering av SQL 2016 server	10
3.3 Forberedelser til installasjon av System Center.....	13
3.4 Installasjon av Microsoft System Center.....	23
3.5 Oppdatering av Microsoft System Center	36
4. WSUS og SUP	36
4.1 WSUS.....	36
4.2 SUP	39
5. Discovery og Boundaries.....	47
6. Application Catalog Web Service Point.....	58
7. Utrulling av Configuration Manager	63
7.1 Installasjon av klientmaskiner.....	63
7.2 Endring av brannmurinnstillinger på SCCM-server.....	69
7.3 Installasjon av Configuration Manager Trace Log Tool.....	69
7.4 Utrulling av Configuration Manager-klienten.....	70
8. Utrulling av applikasjoner	73
9. Endpoint Protection	81
10. Utrulling av sikkerhetsoppdatering til Windows 8.1	99
11. Microsoft Intune	104
11.1 Opprette en Intune-bruker	104
11.2 Synkronisere Active Directory.....	106
11.3 Opprette Collection for Intune.	110
11.4 Legge til Microsoft Intune Subscription.....	111
11.5 Utrulling av apper med SCCM.....	114
11.6 Brukeropplevelse	119

1. Innledning

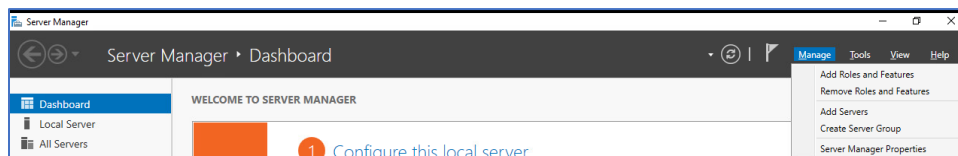
Som det fremkommer i forstudierapporten skal denne oppgaven omhandle Microsoft System Center og Microsoft Intune. Derfor er det naturlig å kort forklare hva disse to programmene er.

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.

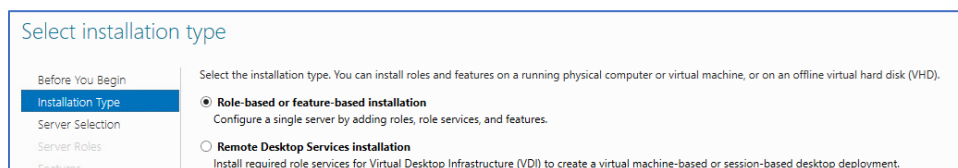
Microsoft Intune er en skytjeneste som tilbyr mobilenhetsadministrasjon, administrasjon av mobilapplikasjoner og PC-styringsfunksjoner. Intunes funksjoner vil hjelpe NerVika AS med å gi sine ansatte tilgang til bedriftsdata, ressurser og applikasjoner, samtidig som det bidrar til å beskytte bedriftens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

2. Installasjon av Active Directory

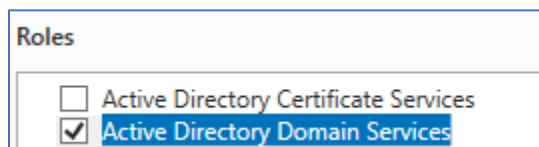
For å installere Active Directory må vi åpne Server Manager. Der velger vi Manage --> Add Roles and Features.



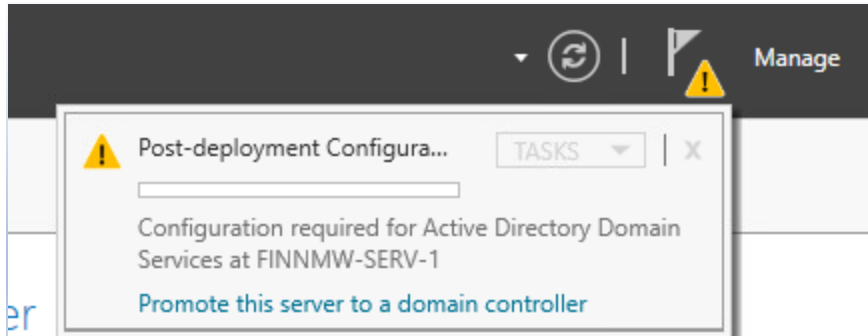
Her velger vi en rollebasert installasjon.



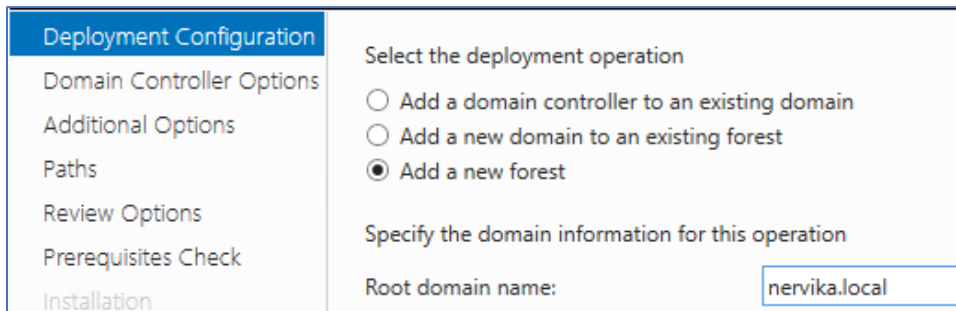
På Server Roles velger vi Active Directory Domain Services



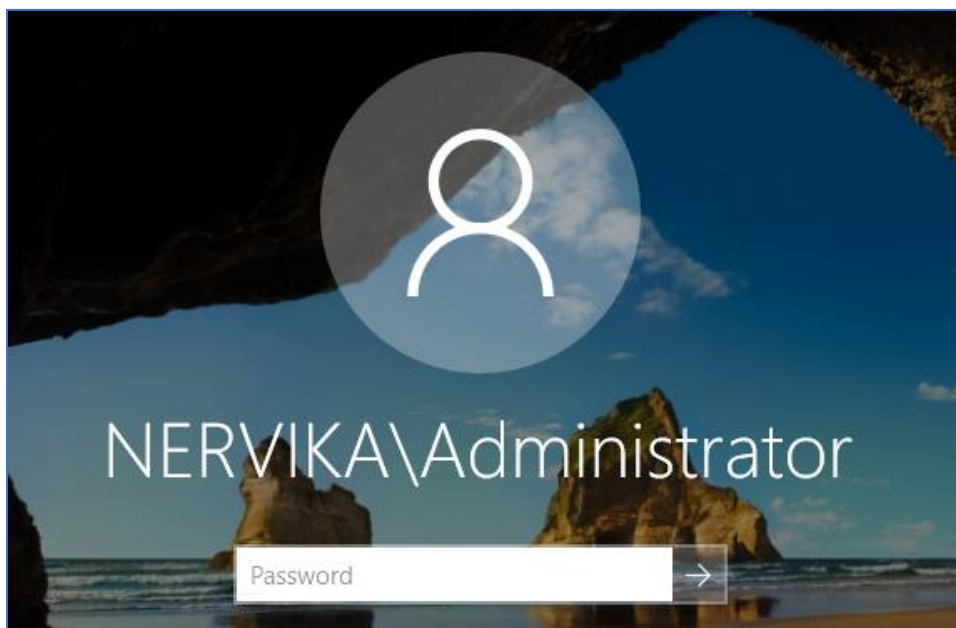
Når AD er ferdig installert må vi gjøre denne serveren til domenekontroller for domenet til NerVika AS



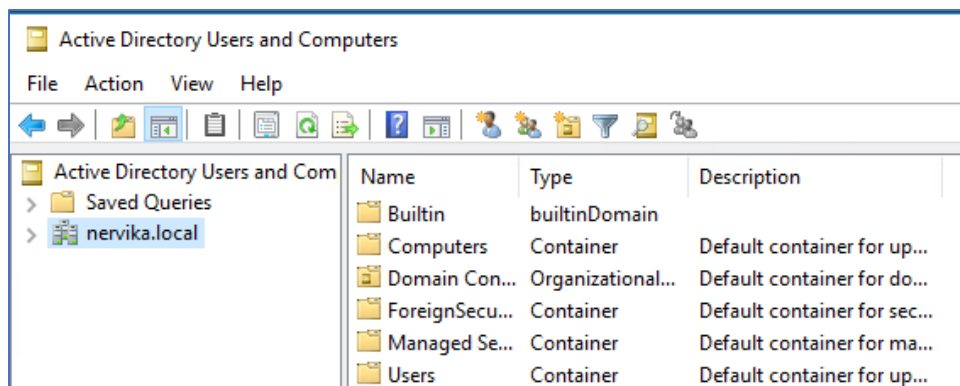
Her oppretter vi en skog for domenet



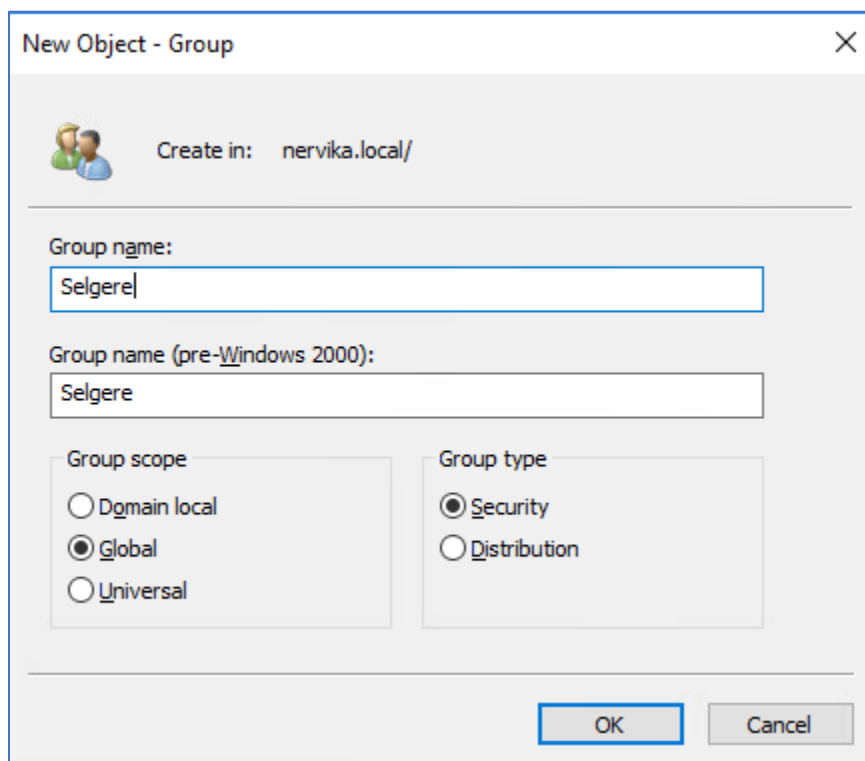
Når installasjonen er ferdig vil serveren automatisk restarte. Når serveren kommer opp igjen ser vi at domenet er opprettet. Vi kan da logge inn som NERVIKA/Administrator









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.



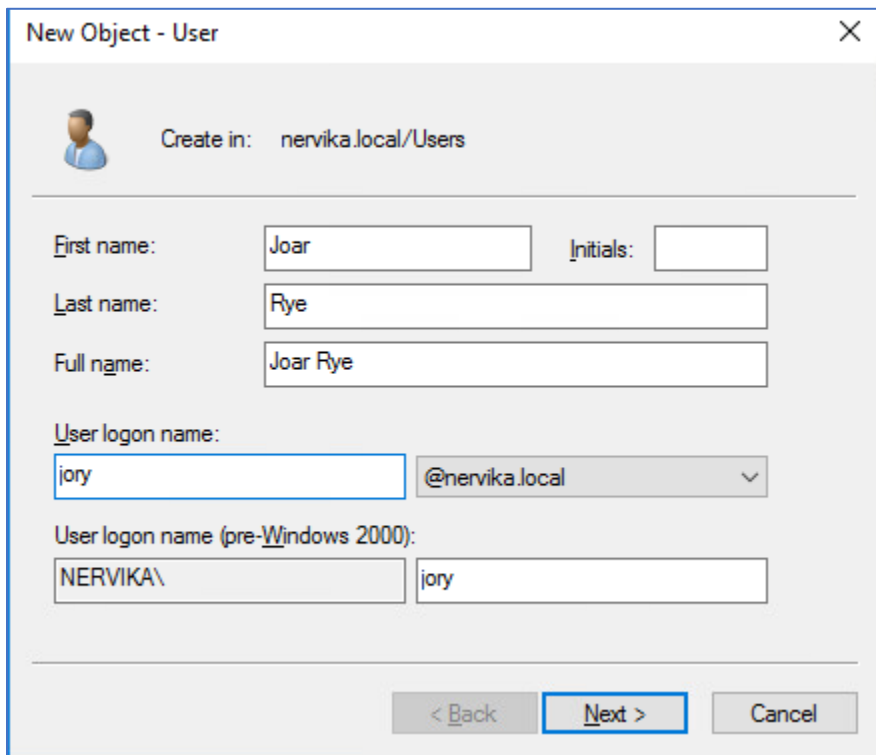
For å opprette grupper til de forskjellige avdelingene høyreklikker vi på nervika.local og velger New-->Group.



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

 Administrasjon	Security Group...
 IT	Security Group...
 Kundeservice	Security Group...
 Ledelse	Security Group...
 Produksjon	Security Group...
 Selgere	Security Group...

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.



New Object - User

Create in: nervika.local/Users

First name: Initials:

Last name:

Full name:

User logon name: @nervika.local

User logon name (pre-Windows 2000):

< Back **Next >** Cancel

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.

New Object - User

Create in: nervika.local/Users

Password: ●●●●

Confirm password: ●●●●

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

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".

Ledelse Properties

General Members Member Of Managed By

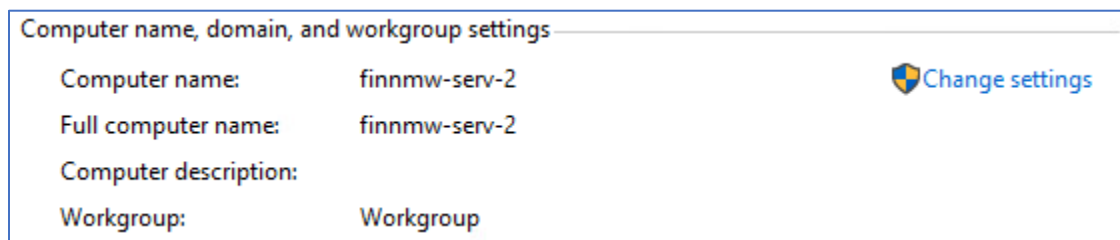
Members:

Name	Active Directory Domain Services Folder
Andreas Solh...	nervika.local/Users
Caroline Foss...	nervika.local/Users
Joar Rye	nervika.local/Users
Karin Gjerstad	nervika.local/Users
Kim Wuttudal	nervika.local/Users
Lina Rostad	nervika.local/Users
Marie Sundli	nervika.local/Users
Steffen Henri...	nervika.local/Users
Thomas Berg	nervika.local/Users
Vidar Opphaug	nervika.local/Users

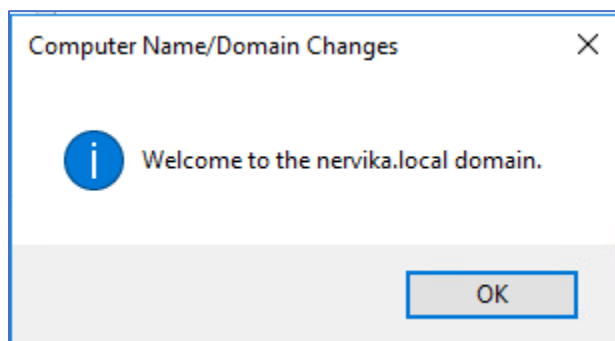
Her vises gruppen Ledelse med sine 10 ansatte. Gjentar denne prosessen med de ansatte i alle avdelingene.

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.



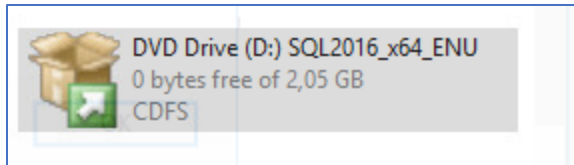
For å melde serveren inn i domenet velger vi Change settings → Change → Skriver inn nervika.local → Logger inn med domeneadministrator. Når serveren er meldt inn i domenet får vi en velkomstmelding.



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.



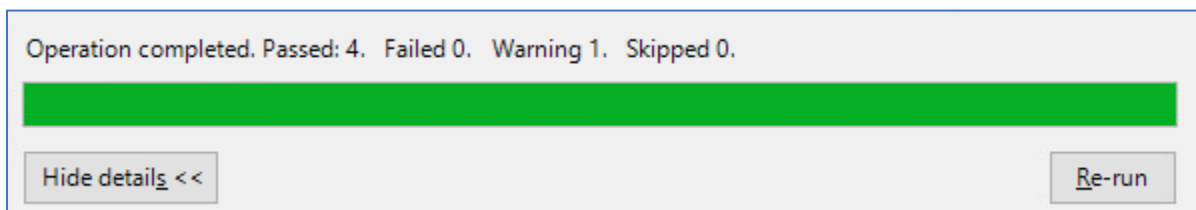
For å starte installasjonen dobbeltklikker vi på denne DVD-driven. Når installasjonen startes får vi en rekke valg. Først hopper vi over planning før vi under Installation velger en stand-alone installation.



[New SQL Server stand-alone installation or add features to an existing installation](#)

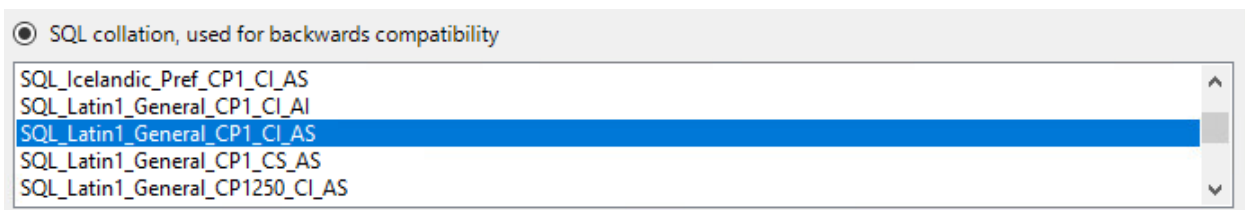
Launch a wizard to install SQL Server 2016 in a non-clustered environment or to add features to an existing SQL Server 2016 instance.

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

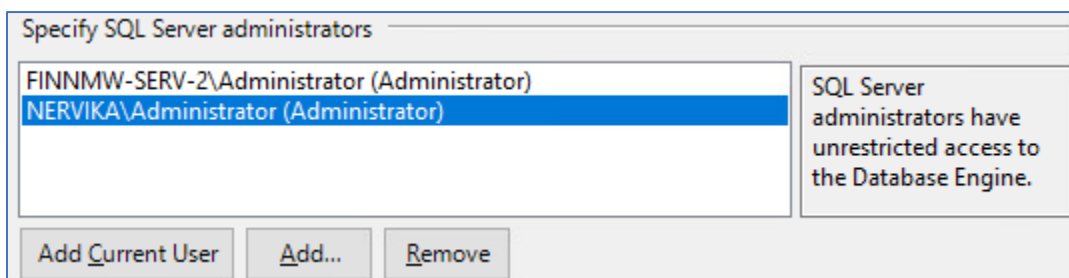


Neste steg i installasjonen er Feature Selection. Her huker vi av Database Engine Services. Under Instance Configuration velger vi Default instance.

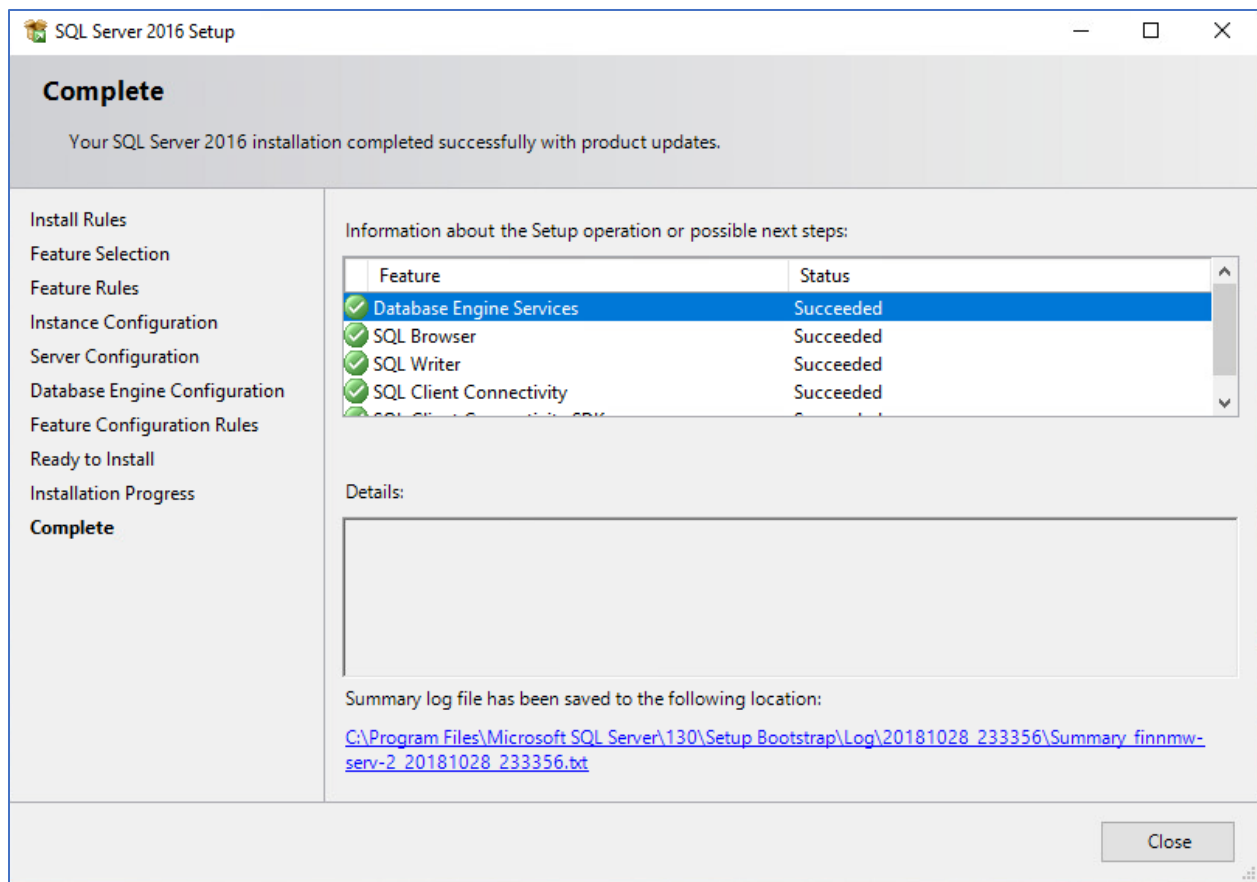
Det er også viktig og huske å endre collation. Velg SQL_Latin1_General_CP1_CI_AS



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

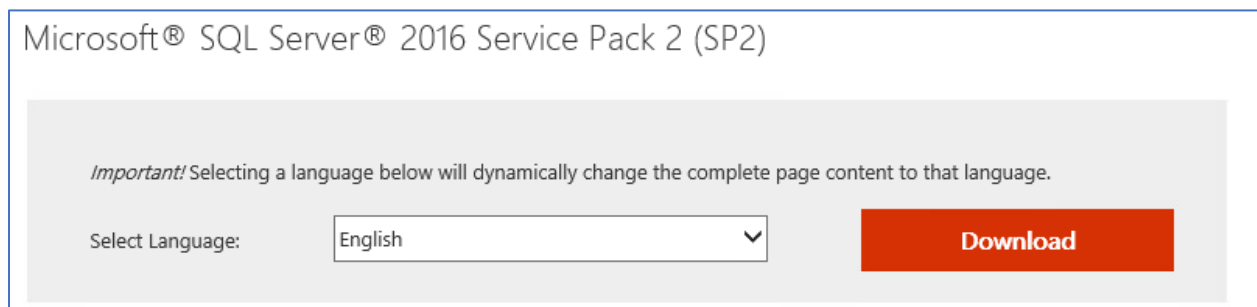


Installasjonen er da klar for å fullføres. Når installasjonen er ferdig får vi opp en oversikt over hva vi har installert og om disse har blitt installert uten problemer.

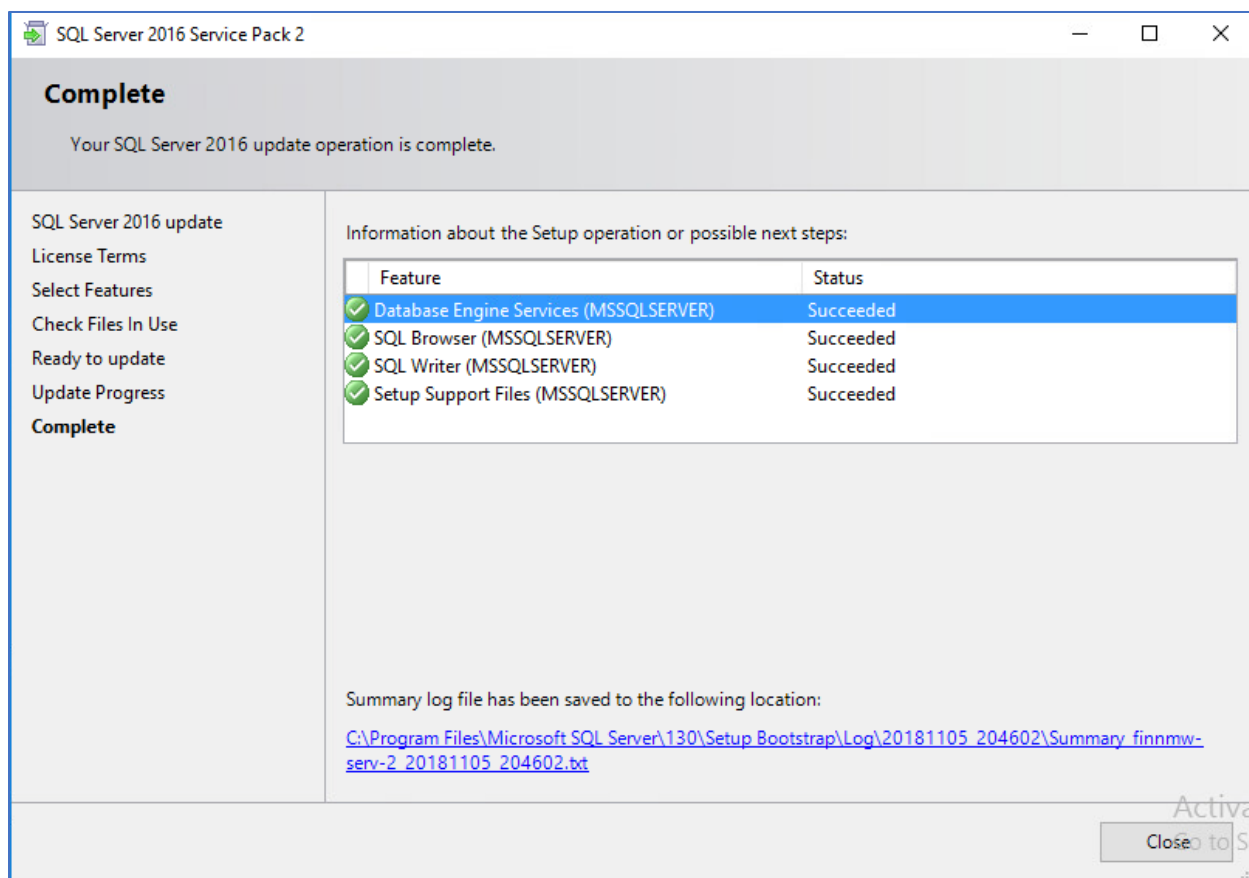


3.2 Oppdatering av SQL 2016 server

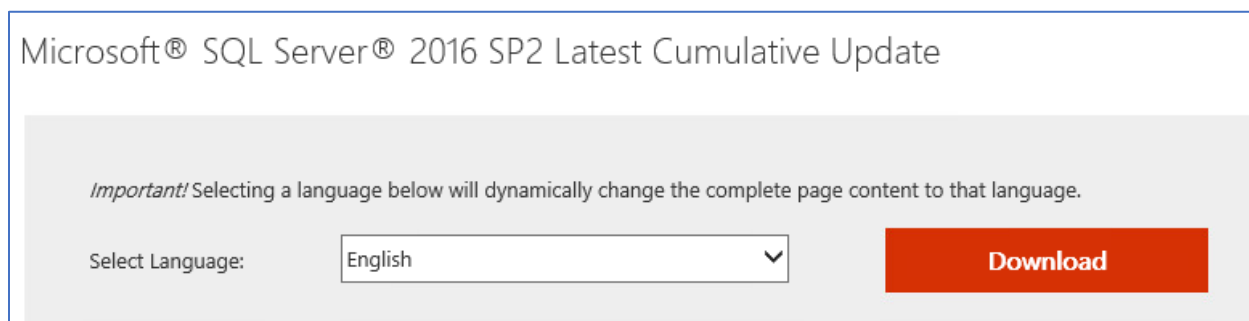
For å oppdatere SQL må vi laste ned Microsoft SQL Server 2016 Service Pack 2. SP 2 finner vi lett ved å søke på microsoft.com. Når vi har funnet rett fil er det bare å trykke download.



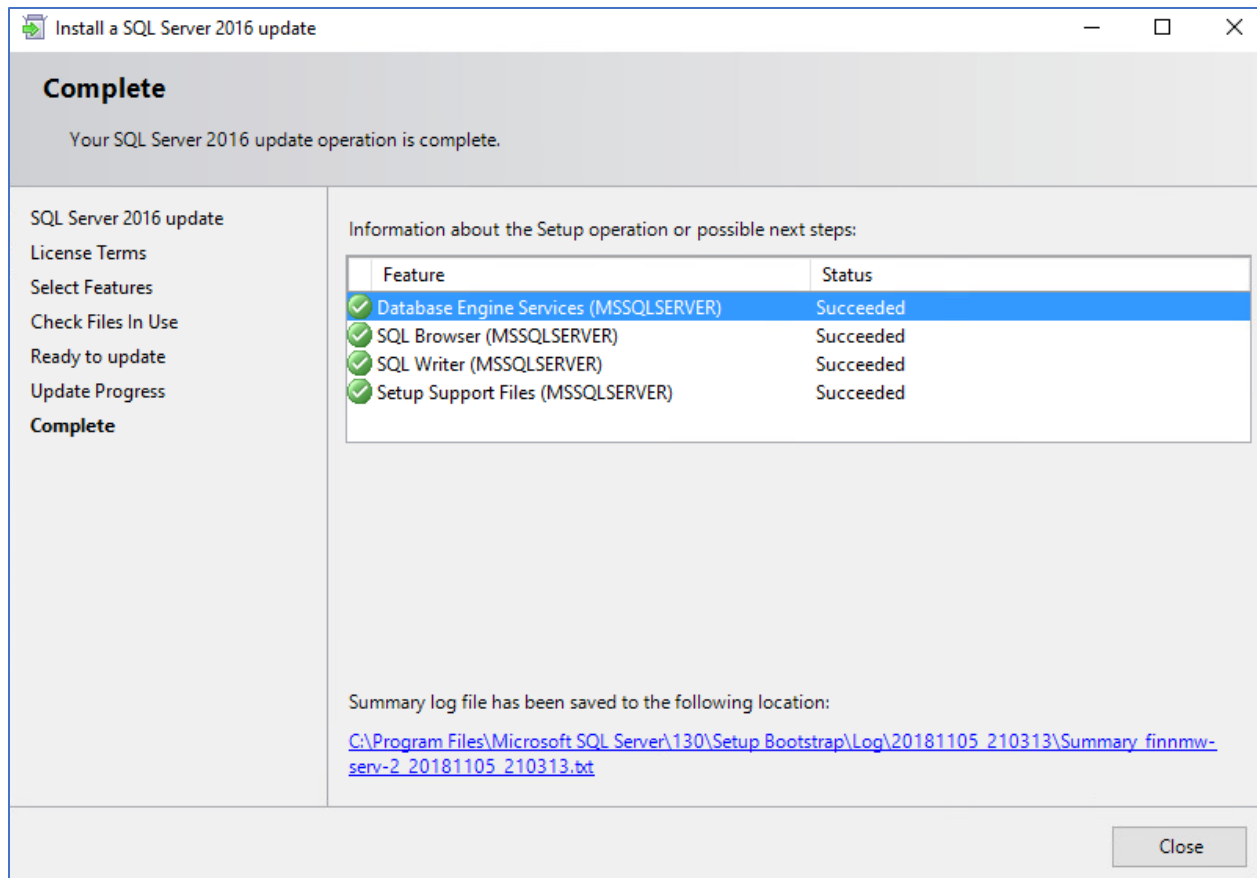
Velger bare å kjøre installasjonsfilen med en gang den er nedlastet. Deretter er det en rett frem installasjon som tar ca 5 minutter. Ved slutt får vi opp informasjon om installasjonen.



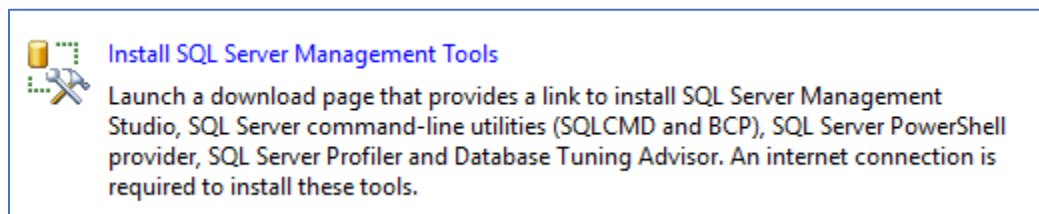
Etter at SP2 er installert må vi installere SQL Server 2016 SP2 Latest Cumulative Update. Denne finner vi også på nettsiden til Microsoft.



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



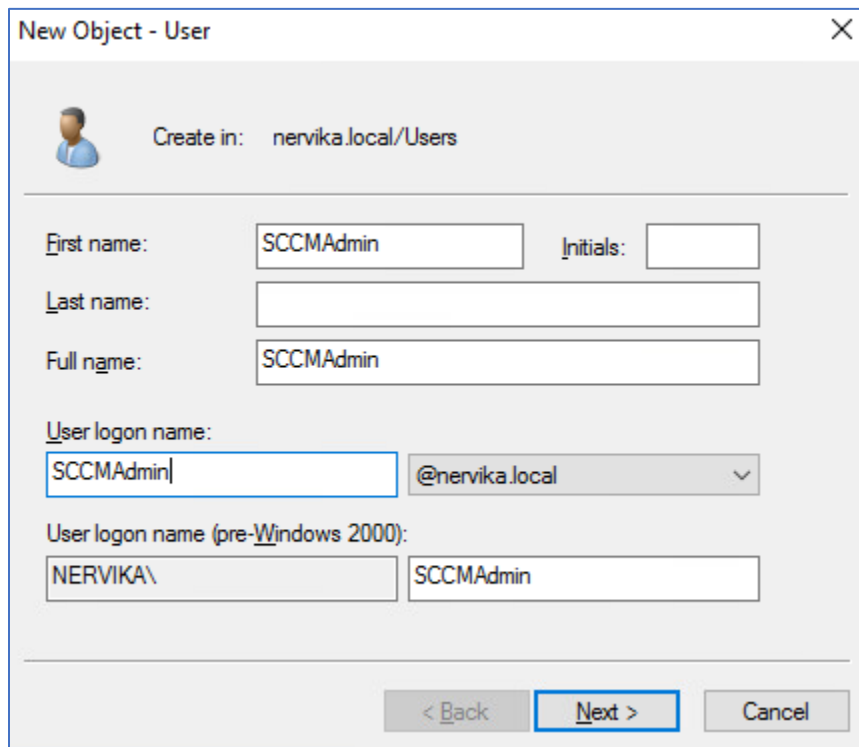
Når alt er up to date, må vi installere SQL Server Management Tools. Dette gjør vi ved å åpne SQL Server Installation Center og velger Server Management Tools under Installation.



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 restarteres. 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.

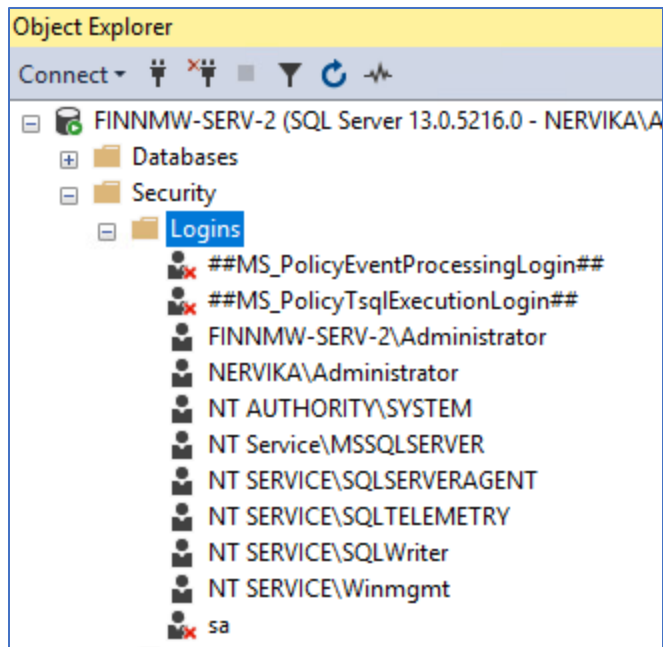


The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: nervika.local/Users'. Below this, there are several input fields:

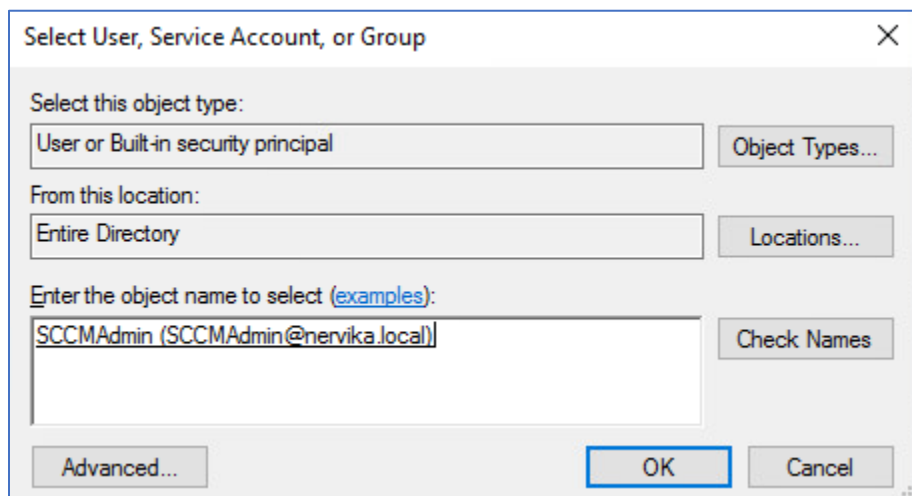
- First name:** SCCMAdmin
- Initials:** (empty)
- Last name:** (empty)
- Full name:** SCCMAdmin
- User logon name:** SCCMAdmin|@nervika.local
- User logon name (pre-Windows 2000):** NERVIKA\SCCMAdmin

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

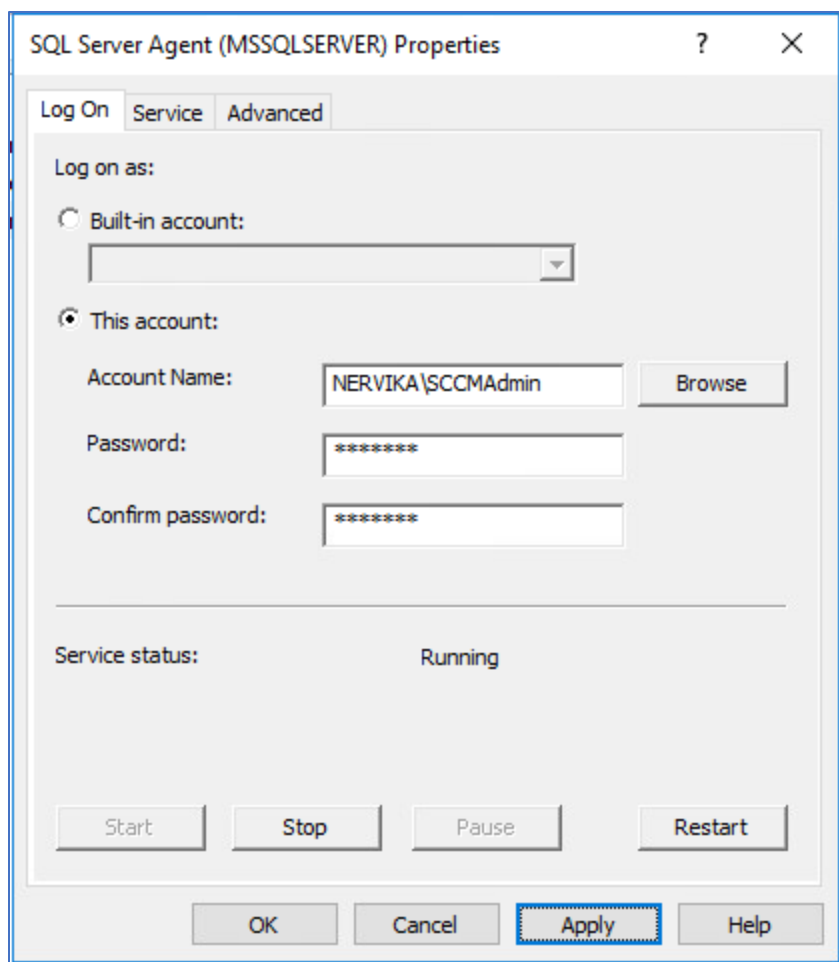
Nå må vi logge på SCCM-serveren for å gi denne brukeren administratorrettigheter til SQL-serveren. Åpner da SQL Server Management Studio som vi nettopp har installert. Navigerer oss til Logins under serveren.



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



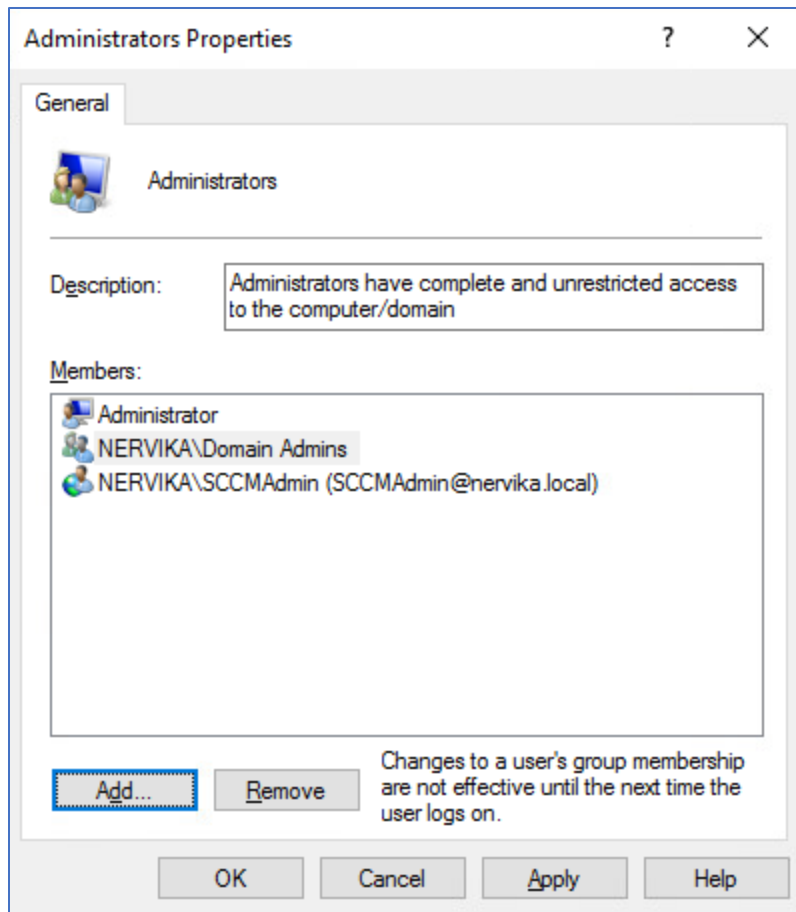
I SQL Server Configuration Manager må vi også endre Log on-bruker i SQL Server, SQL Browser og SQL Agent. SCCMAdmin skal være Log on-bruker her. For å endre dette velger vi SQL Server Services og høyreklikker først på Server Agent → Properties → Velger Nervika\SCCMAdmin som log on-bruker via This account.



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 Agent
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

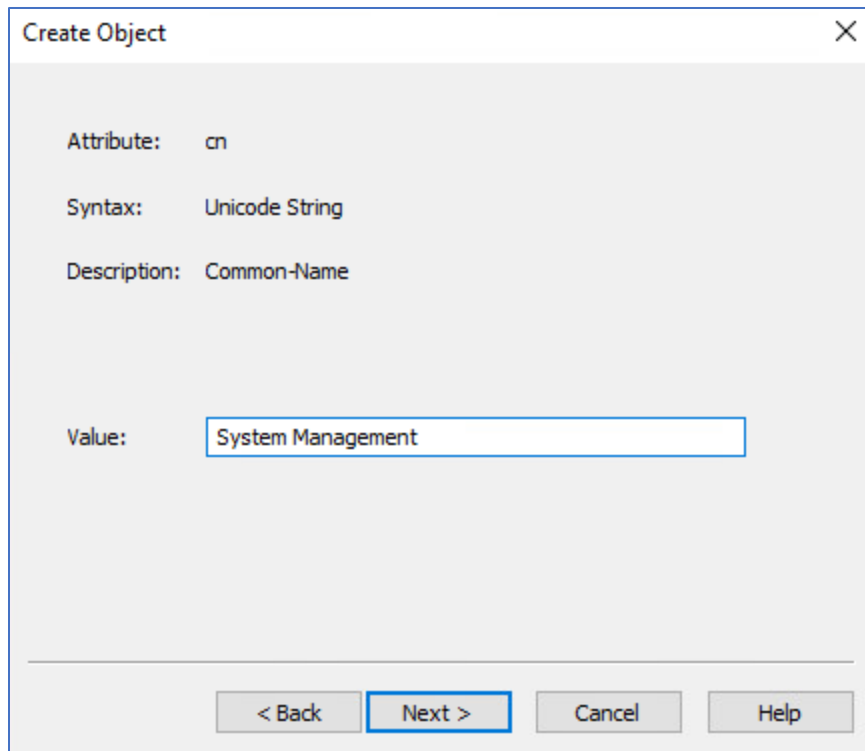


Nå må vi tilbake til AD-serveren og åpne Adsi.edit. Dette gjøres via Server Manager eller via cmd med kommandoen adsiedit.msc.

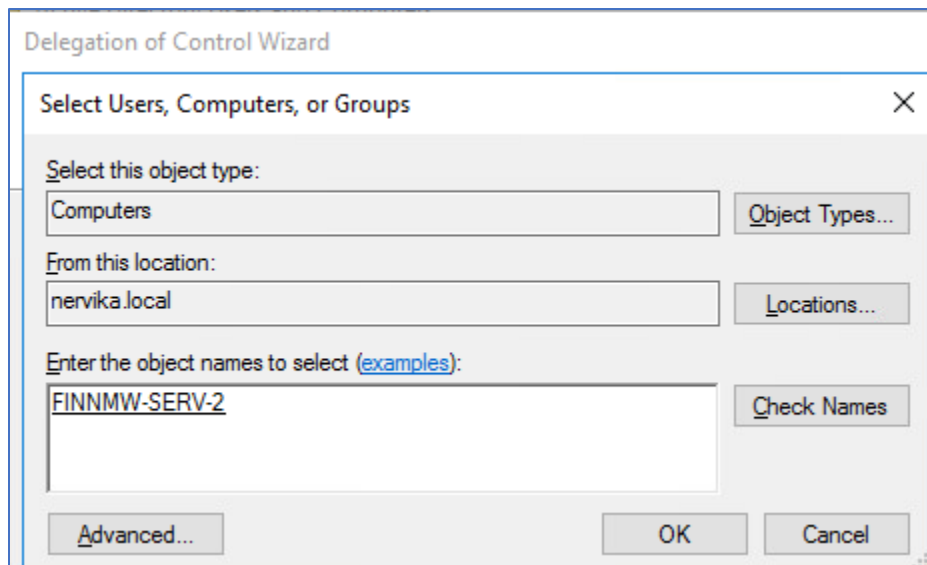
Når adsi.edit åpnes trykker vi More actions → Connect to → OK.

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

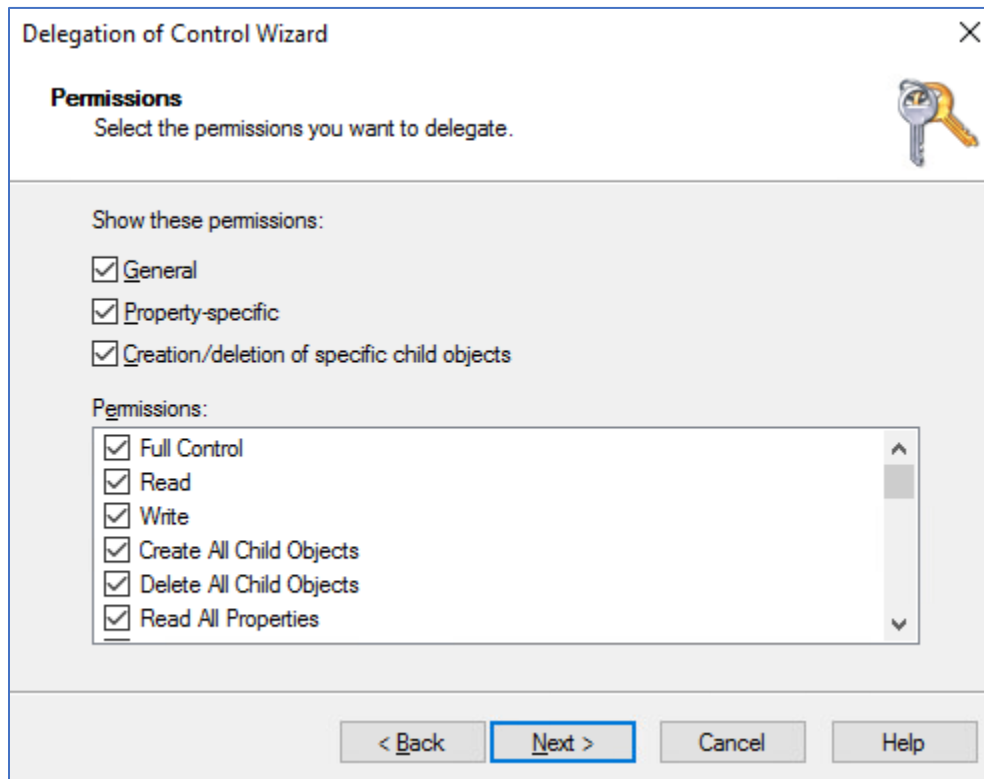
Velger her System Management i «Value»-feltet.



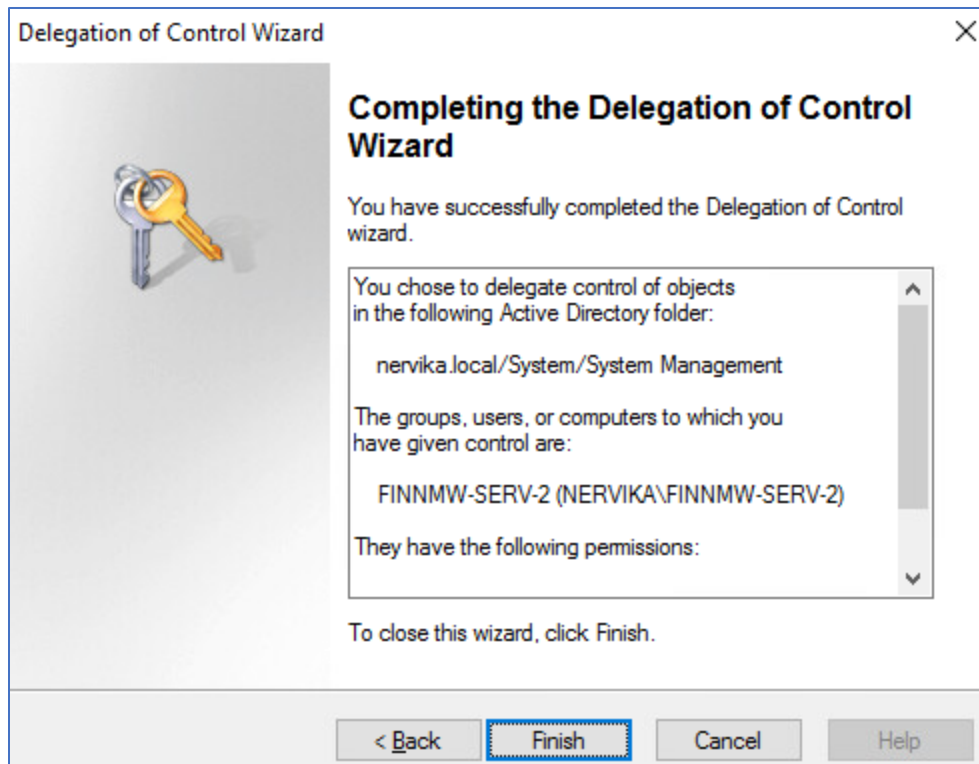
Nå må vi delegere rettigheter til denne containeren. Det gjøres i AD Users and computers. Det første vi må gjøre i AD er å velge view → Advanced Features slik at vi ser denne containeren. Den finner vi under System. Høyreklikker på containeren → Delegate Control → Add → Object Types → Velger kun Computers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

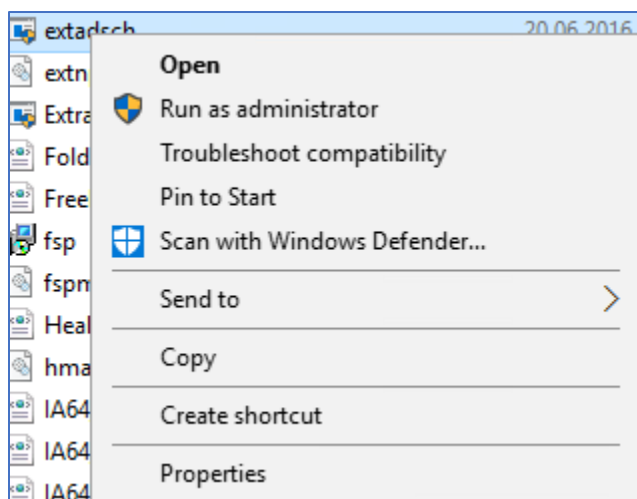


Trykker next en siste gang og får opp en bekreftelse på hva vi har gjort

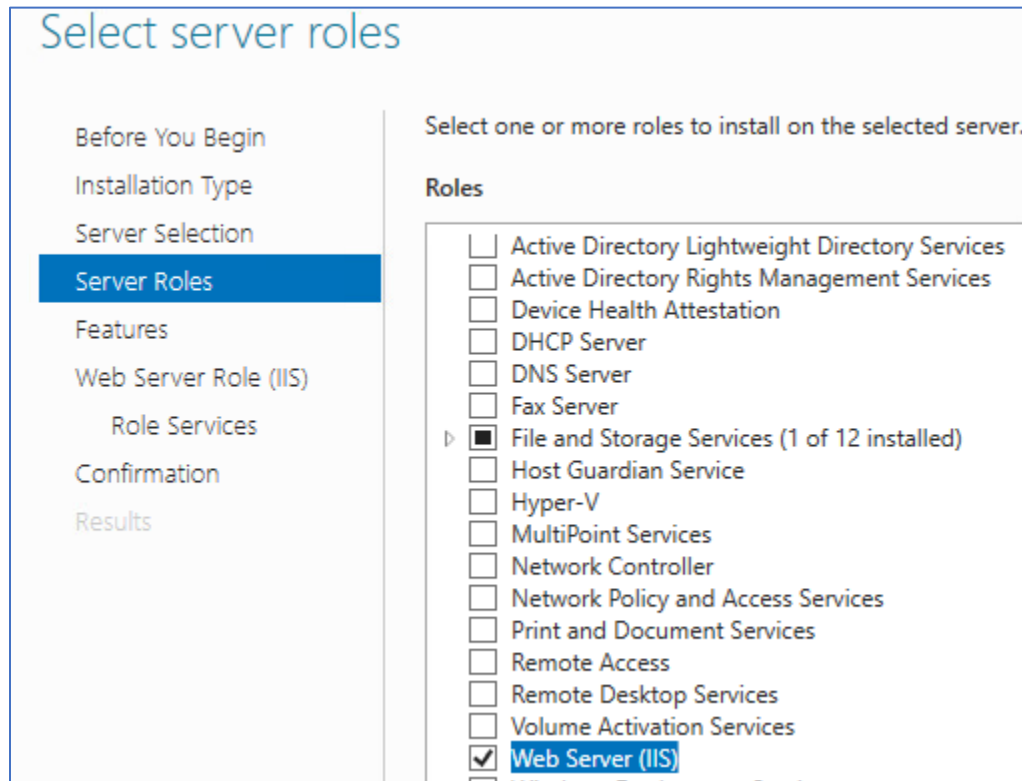


Når vi er ferdige med å delegere kontroll til Containeren, må vi kjøre extadsch.exe. Extadsch.exe finner vi inne på den virtuelle DVD-driven til SCCM-manager. Extadesch.exe kjøres for å utvide AD-skjemaet for Configuration Manager.

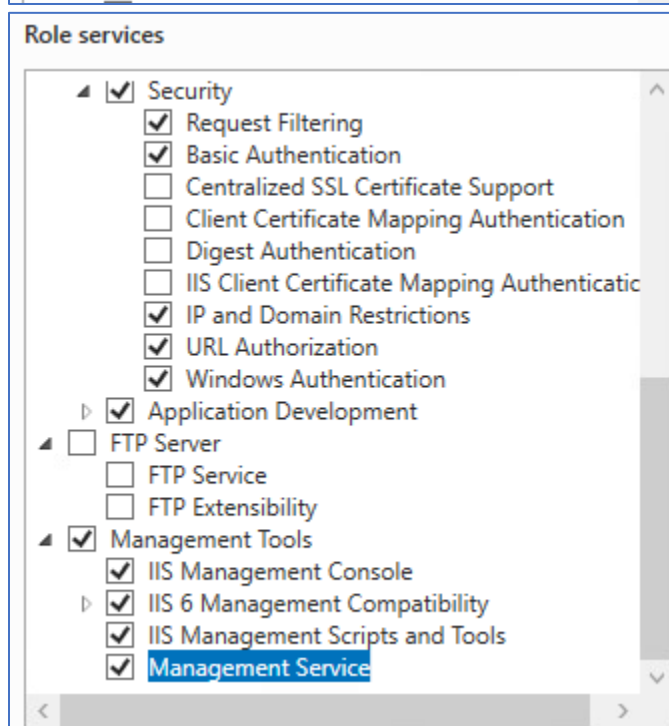
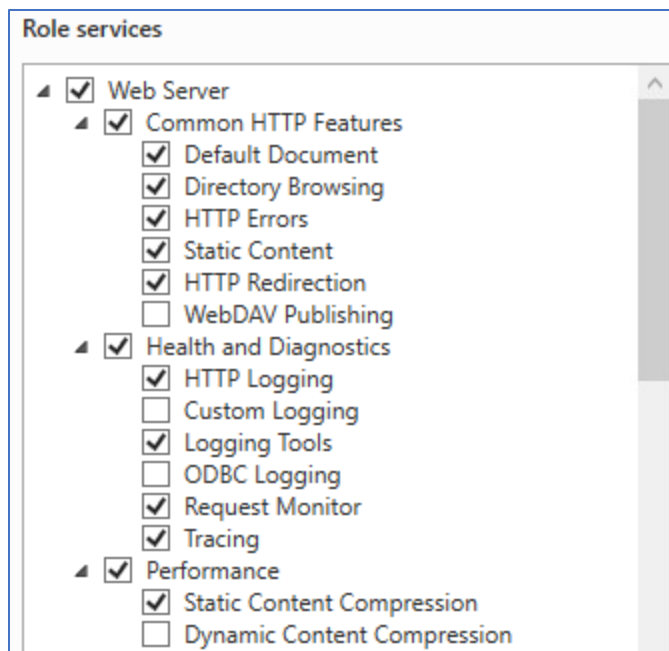
Mounter ISOen til SCCM-manager slik som vi gjorde med SQL-server tidligere i oppgaven. Extadesch.exe ligger under mappen SMSSETUP/BIN/X64. Når vi finner filen må vi velge «Run as administrator»



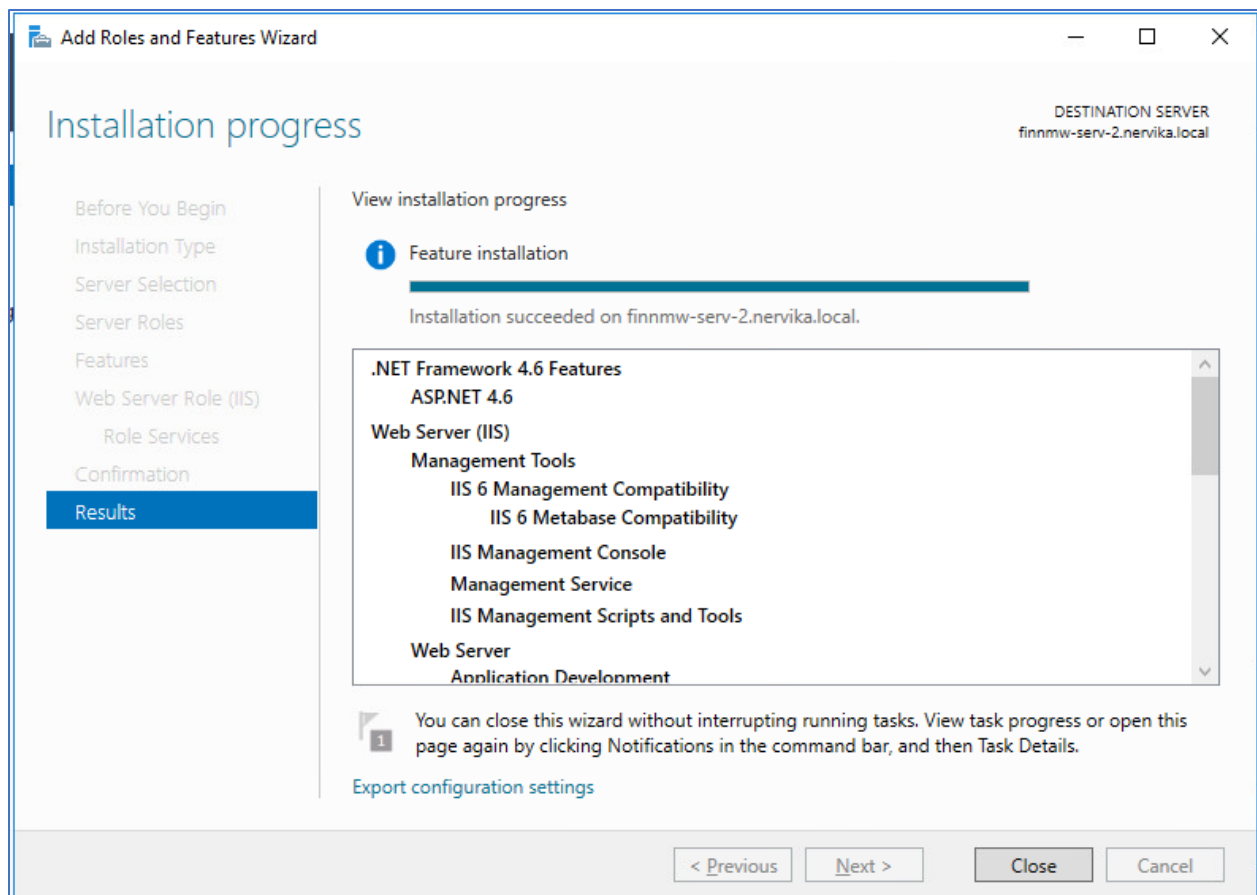
Nå må vi tilbake til Server Manager for å åpne Add Roles and Features. Her skal vi installere Web Server (IIS). Web Server finner vi under Server Roles



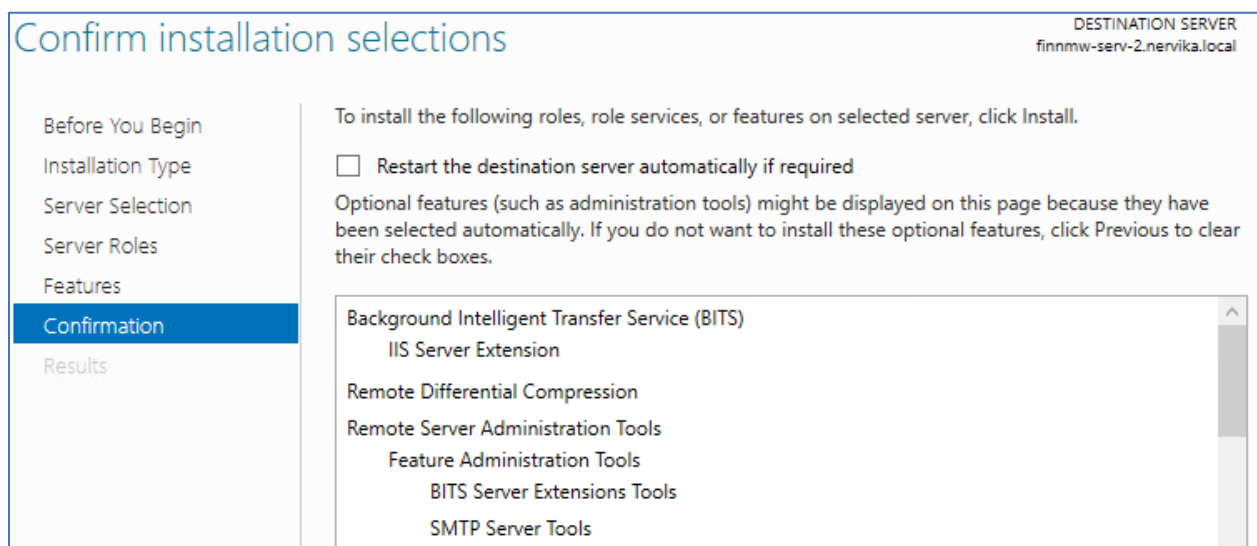
Når vi har funnet Web Serveren, må vi navigere oss til Role Services. Her må vi huske å huke av følgende:



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.



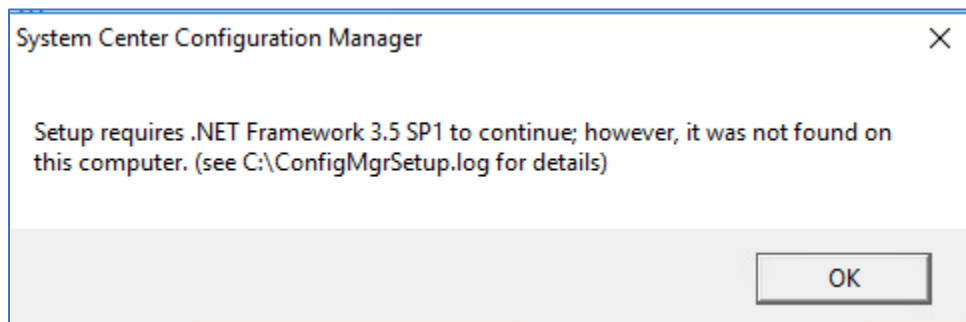
En siste ting vi må gjøre i Server Manager er å installere BITS og Remote Differential Compression. Her må vi huke under for alle undervalg under installasjonen.



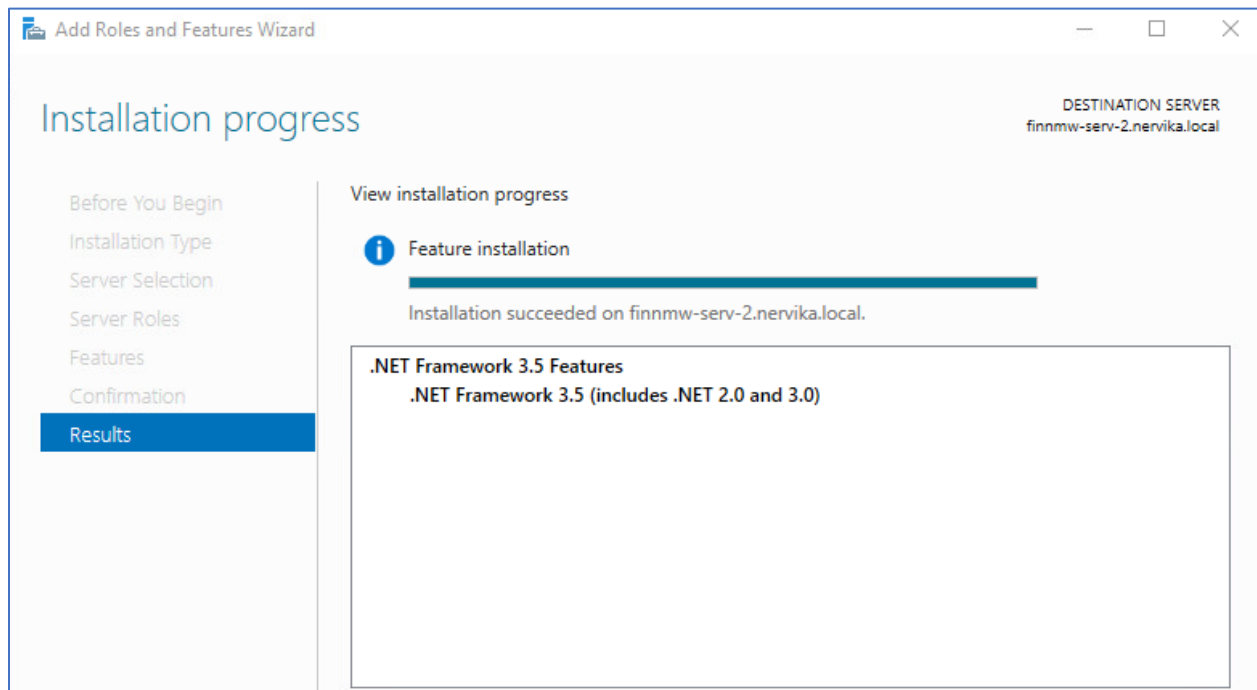
Nå skal alt være klart til å installere SCCM.

3.4 Installasjon av Microsoft System Center

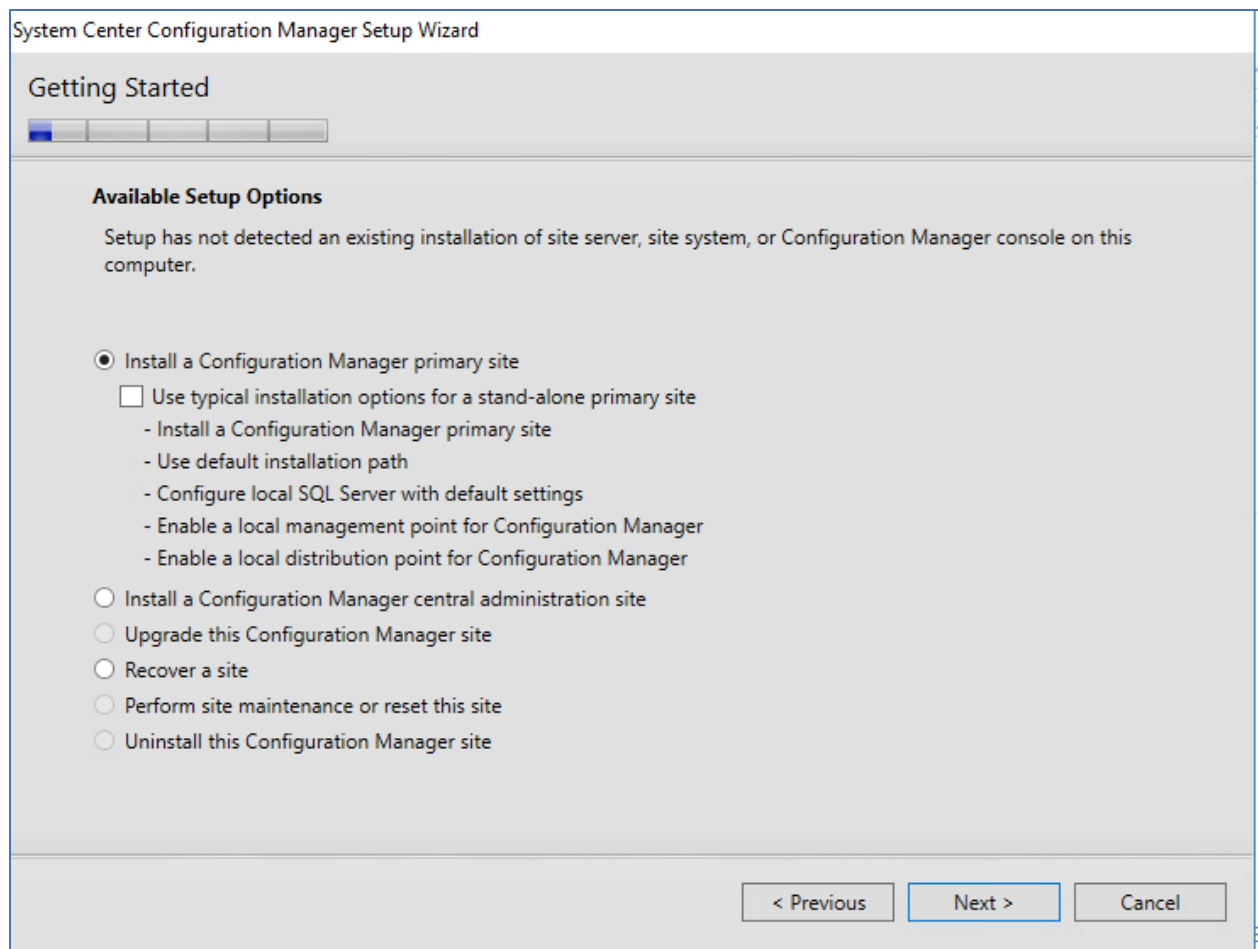
Har allerede mountet ISO-filen til SCCM på serveren. For å starte installasjonen åpner vi den virtuelle D-driven og kjører splash.exe. Når vi starter splash.exe så vil installasjonsfilen automatisk sjekke om serveren er klar for installasjon av SCCM. Fikk er en beskjed om at .NET Framework 3.5 SP1 manglet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

System Center Configuration Manager Setup Wizard

Prerequisite Downloads

Setup requires prerequisite files. Setup can automatically download the files to a location that you specify, or you can use files that have been downloaded previously.

Download required files

Example: \\ServerName\ShareName or C:\Downloads

Path:

Use previously downloaded files

Example: \\ServerName\ShareName or C:\Downloads

Path:

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

System Center Configuration Manager Setup Wizard

Site and Installation Settings

Specify a site code that uniquely identifies this Configuration Manager site in your hierarchy.

Site code:

Specify a site name that helps to identify the site. Example: Contoso Headquarters Site

Site name:

Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install the site.

Installation folder:

Specify whether to install the Configuration Manager console to manage the Configuration Manager site from this computer. You can remotely manage the site when you do not install the Configuration Manager console.

Install the Configuration Manager console

< Previous Next > Cancel

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

System Center Configuration Manager Setup Wizard

Primary Site Installation

Specify whether to join the primary site to an existing Configuration Manager hierarchy or install the primary site as a stand-alone site.

Join the primary site to an existing hierarchy

Central administration site server (FQDN): Example: server1.contoso.com

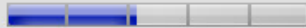
Install the primary site as a stand-alone site

< Previous Next > Cancel

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

finmw-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.

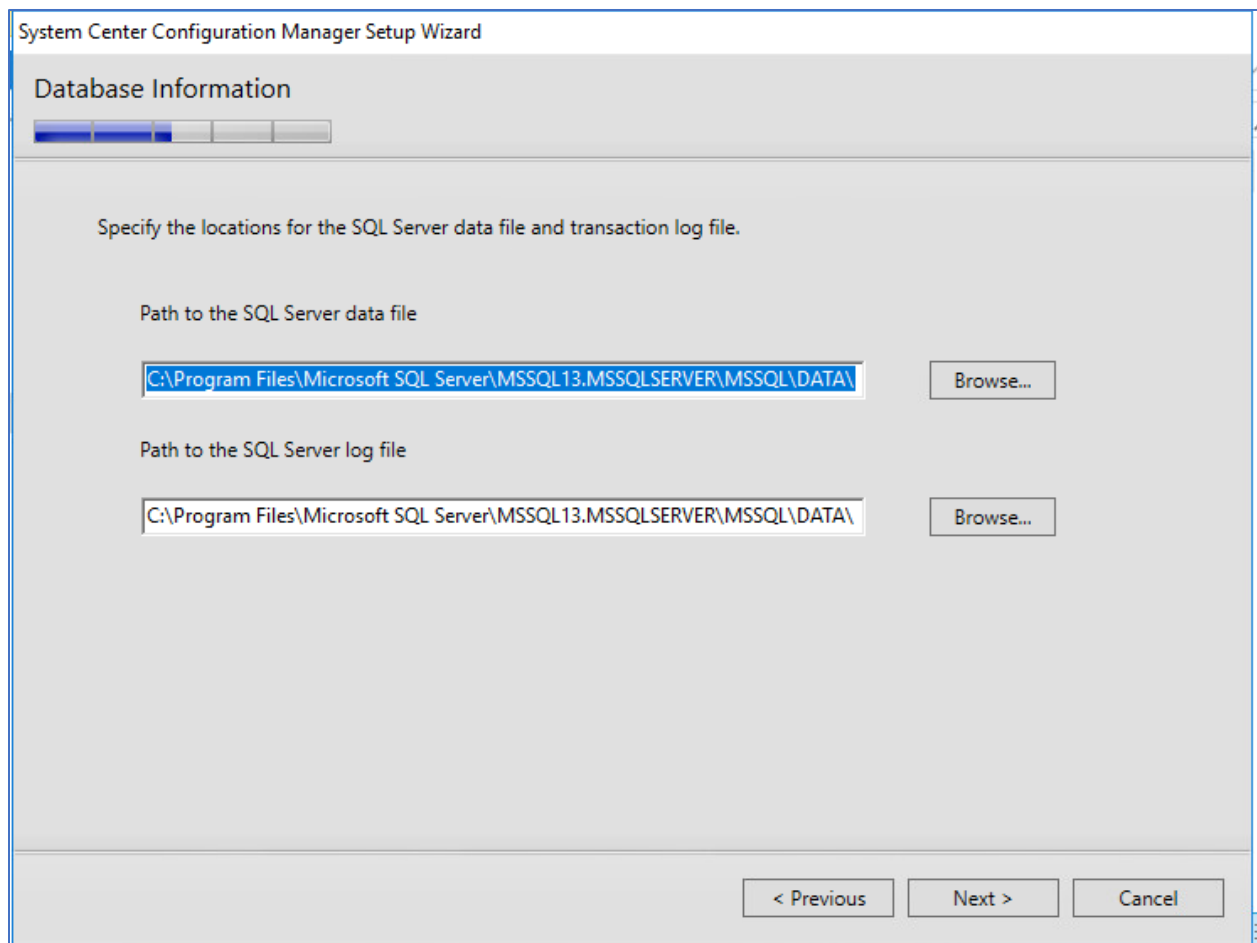
Service Broker Port:

4022

< Previous

Next >

Cancel



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

System Center Configuration Manager Setup Wizard

Client Computer Communication Settings



Configuration Manager site system roles can accept HTTP or HTTPS communication from clients. Specify whether to require all site system roles to accept only HTTPS communication or allow the communication method to be configured on each site system role.

- All site system roles accept only HTTPS communication from clients
- Configure the communication method on each site system role
- Clients will use HTTPS when they have a valid PKI certificate and HTTPS-enabled site roles are available

Note: HTTPS communication requires client computers to have a valid PKI certificate for client authentication.

< Previous

Next >

Cancel

Under Site System Roles gjør vi ingen endringer

System Center Configuration Manager Setup Wizard

Site System Roles

Specify whether to have Setup install a management point or distribution point.

A management point provides clients with policy and content location information. It also receives configuration data from clients.

Install a management point.

FQDN: Client connection:

A distribution point contains source files for clients to download and lets you control content distribution by using bandwidth, throttling, and scheduling controls.

Install a distribution point.

FQDN: Client connection:

The site server's computer account is used to install the selected site system roles. Ensure that this account is a member of the local administrators group for the specified servers.

You can install additional site system roles from the Configuration Manager console after Setup finishes.

Site system roles configured to use HTTPS must have a valid PKI server certificate.

< Previous Next > Cancel

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

System Center Configuration Manager Setup Wizard

Service Connection Point Setup

Keep Configuration Manager up-to-date by connecting to the Configuration Manager cloud service. Connecting to the service enables your deployment to download updates and new features.

Yes, let's get connected (recommended)

Select a server to use as the service connection point (requires internet access):

Use a proxy server when synchronizing information from the Internet

Address: Port:

Skip this for now

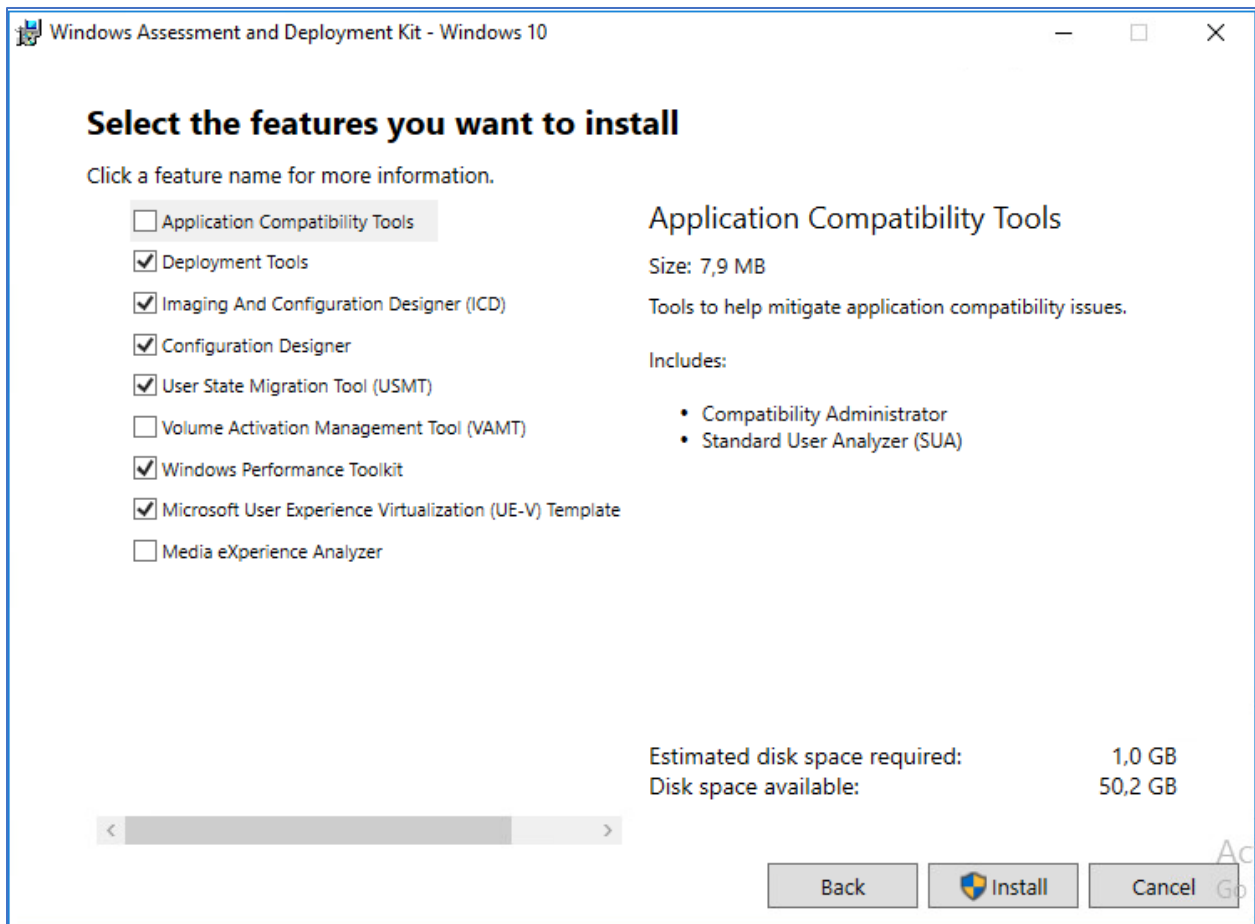
To connect to the service after setup completes, install a service connection point site system role.

i To use features like Conditional Access, Windows Store for Business or on-premises mobile device management (MDM), add your Microsoft Intune subscription to Configuration Manager after setup completes.

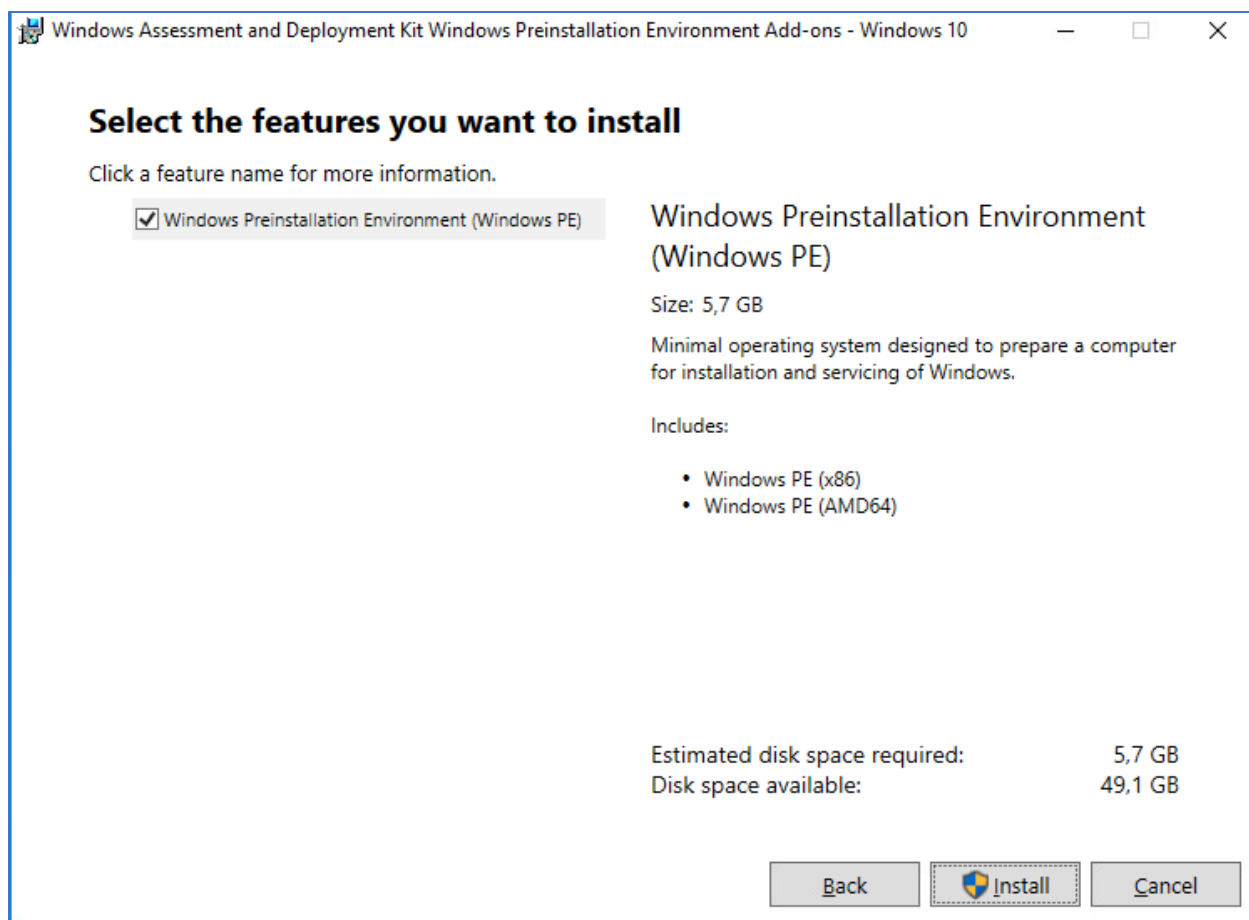
< Previous Next > Cancel

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>.

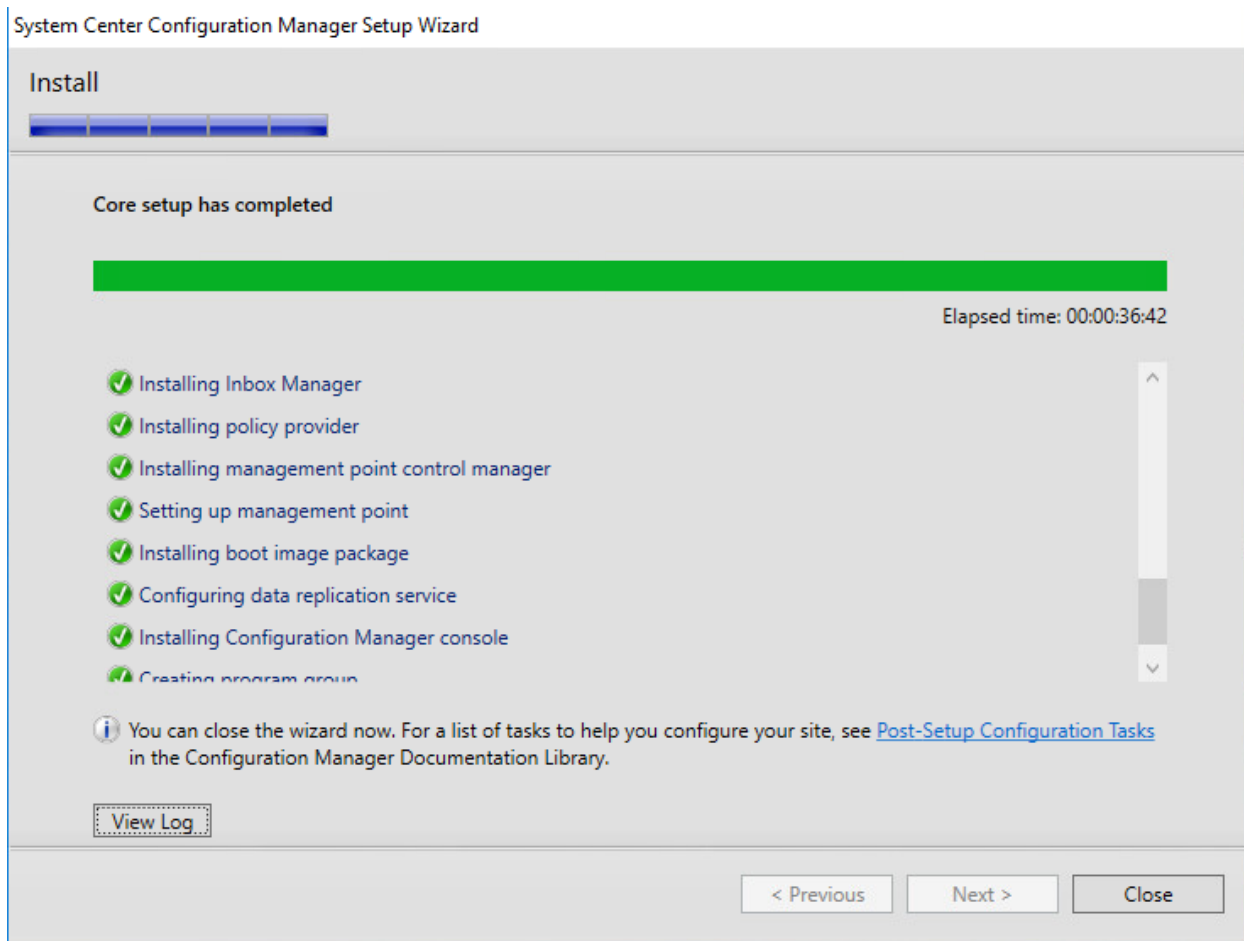
Her er det bare å laste ned filen og starte installasjonen.



Når ADK er installert må vi laste ned en add-on som heter Windows Preinstallation Environment (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:

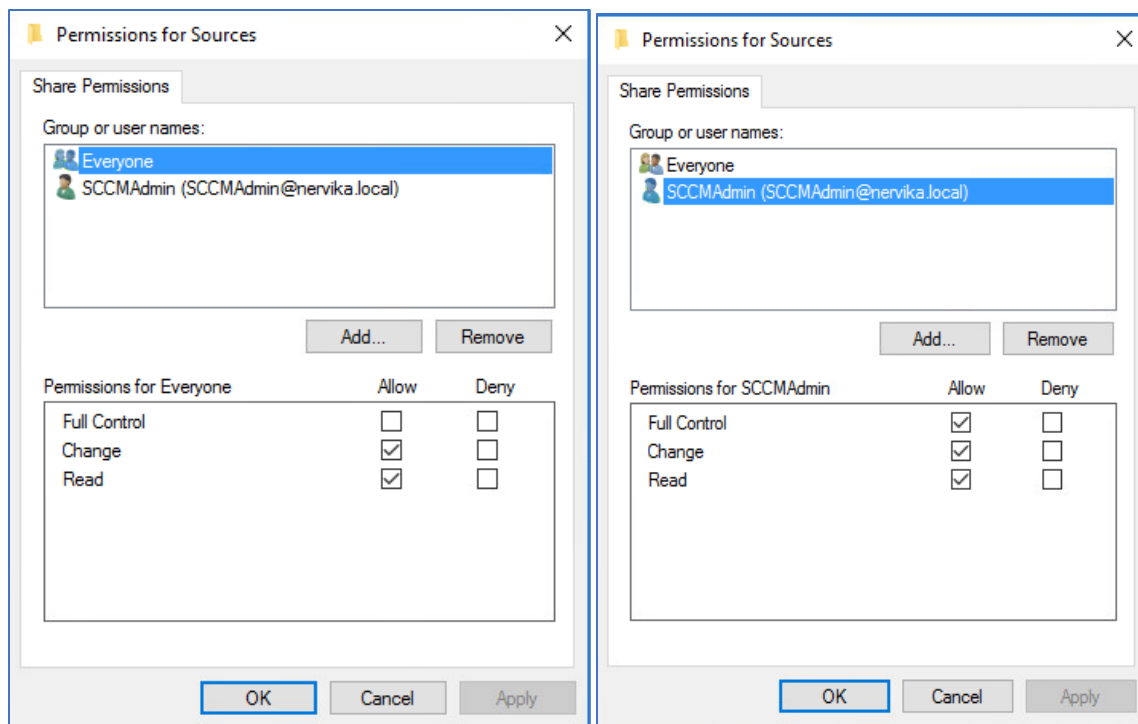


3.5 Oppdatering av Microsoft System Center

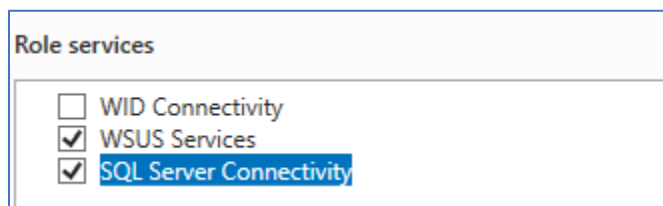
4. WSUS og SUP

4.1 WSUS

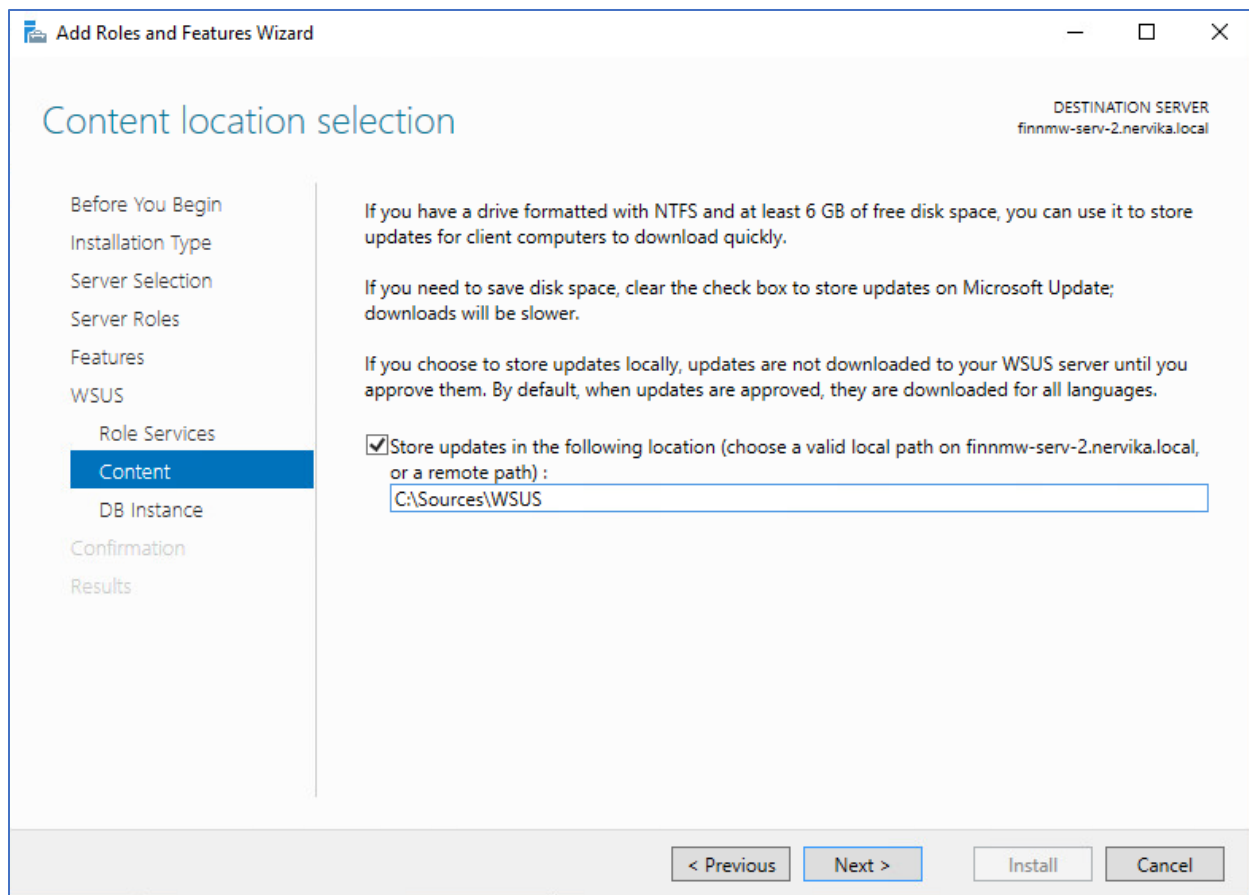
På SCCM-serveren navigerer vi oss til C-driften og oppretter ei mappe som heter Sources. Oppretter så en undermappe om vi kaller WSUS. Sources-mappen skal så deles. Høyreklikker på mappen og velger Properties→ Sharing→ Advanced Sharing→ Permissions. Her gir vi SCCMAdmin full control, mens Everyone får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



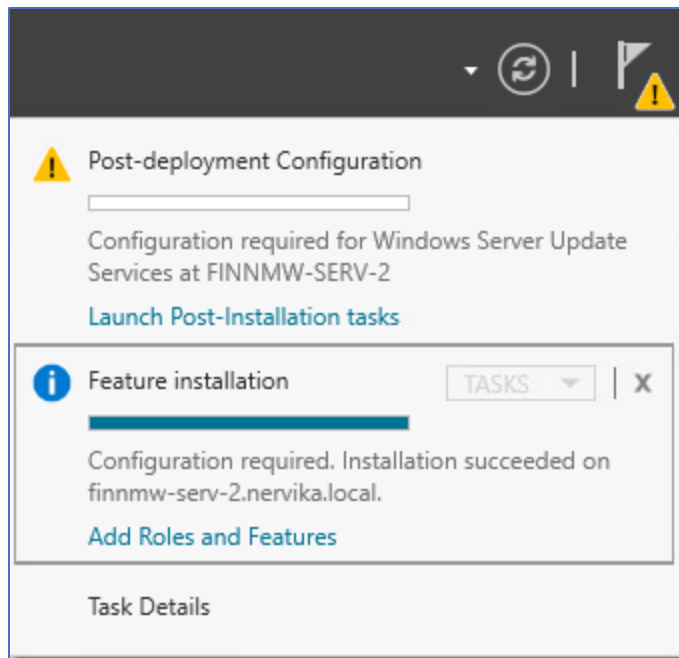
Nå må vi installere rollen Windows Server Update Services fra Server Manager. Under installasjonen får vi et undervalg. Her skal vi velge WSUS Services og SQL Server Connectivity som vist på bildet under.



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

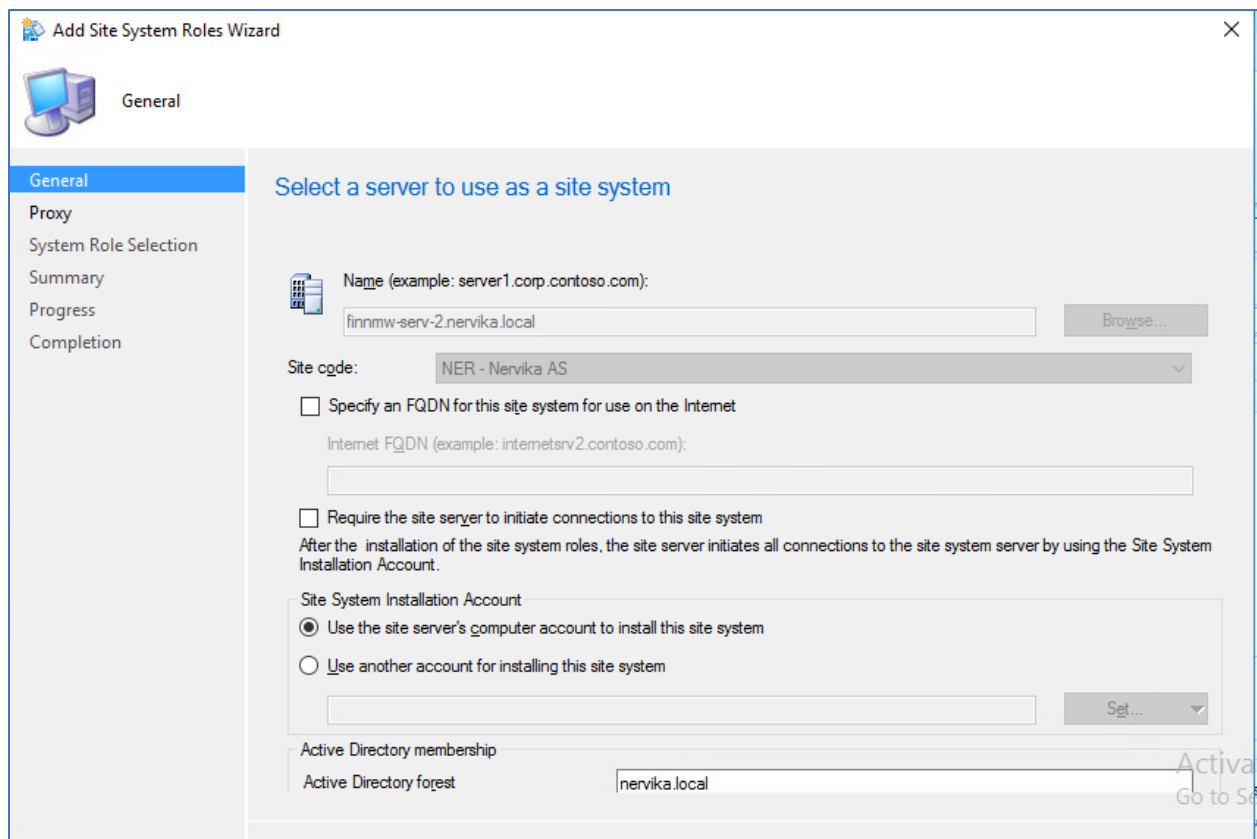


Når installasjonen er ferdig, vil det komme en varseltekst i Server Manager. Her må vi velge Launch Post-installation tasks.

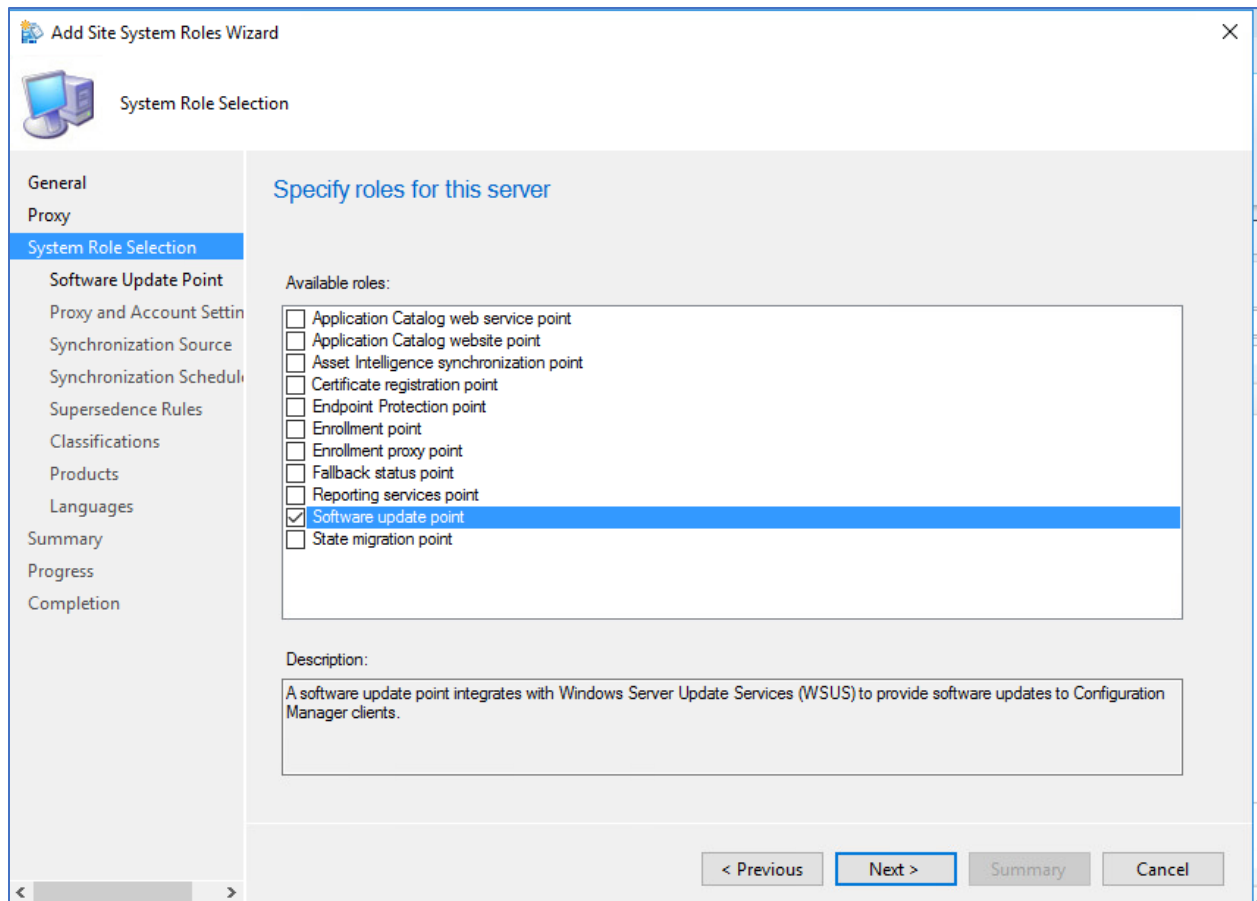


4.2 SUP

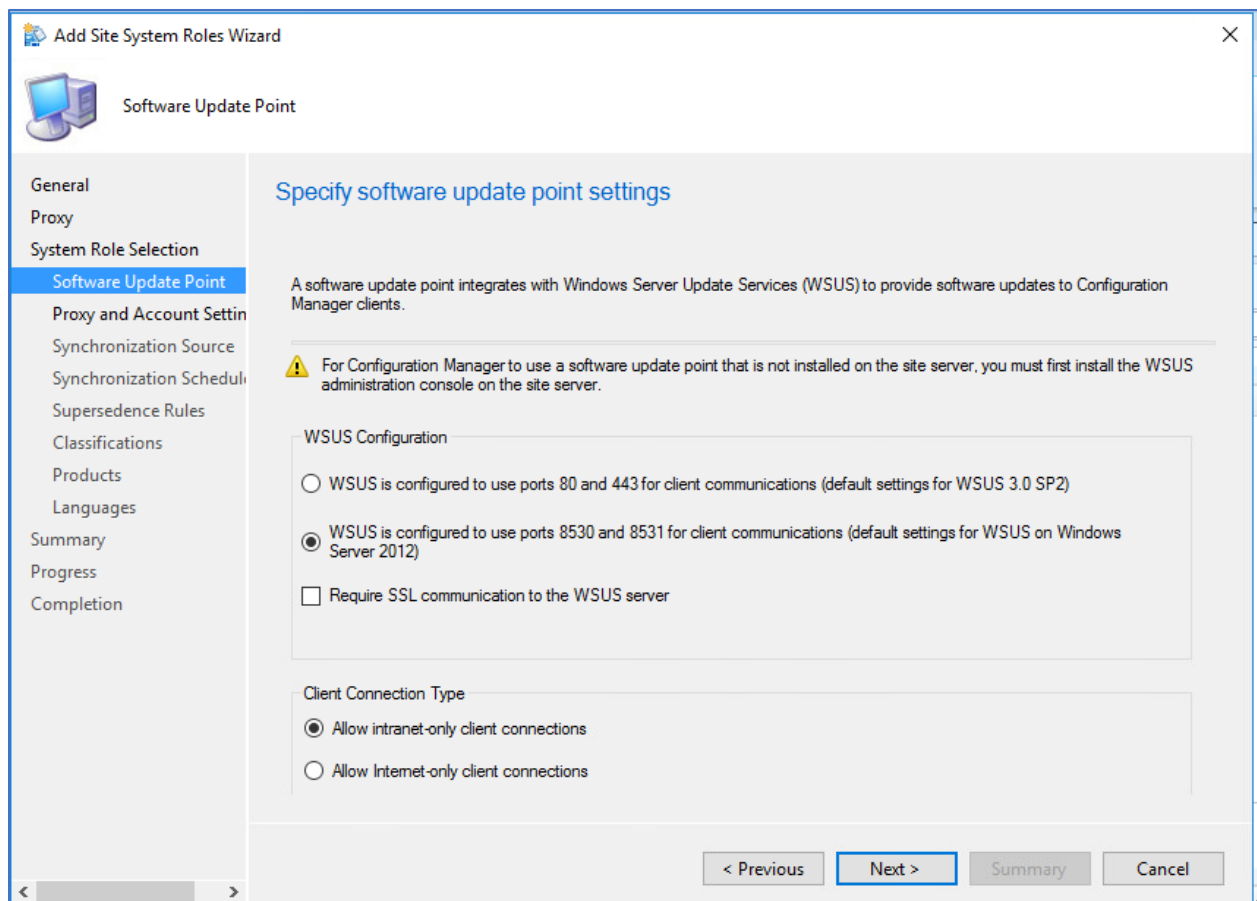
Når WSUS er installert må vi legge inn SUP. Åpne System Center Configuration Manager. I SCCM navigerer vi oss til Administration → Site Configuration → Servers and site system roles. Her høyreklikker vi på serveren og velger Add Site System Roles. Da skal det komme opp en Add Site System Roles-wizard.



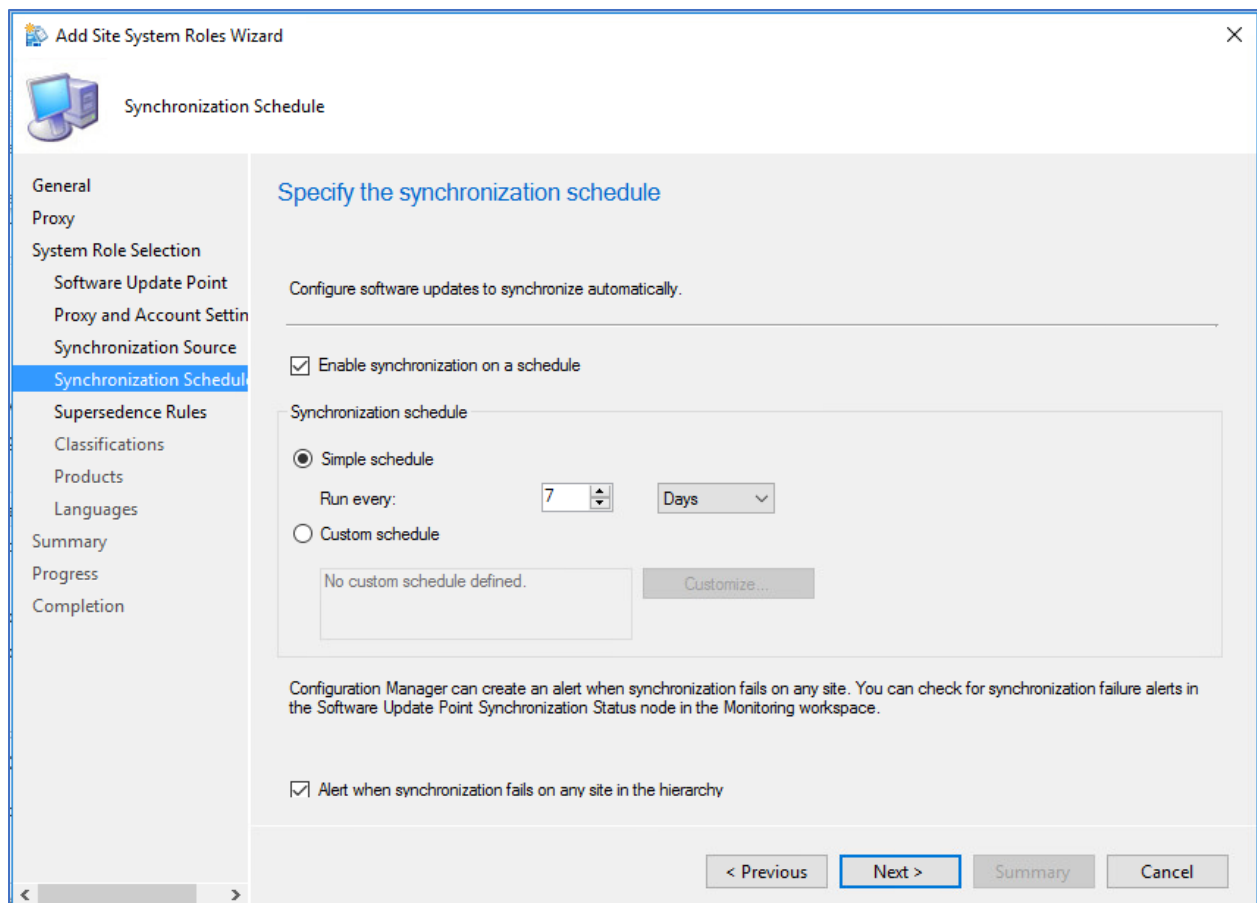
Her navigerer vi oss frem til System Role Selection og huker av Software update point.



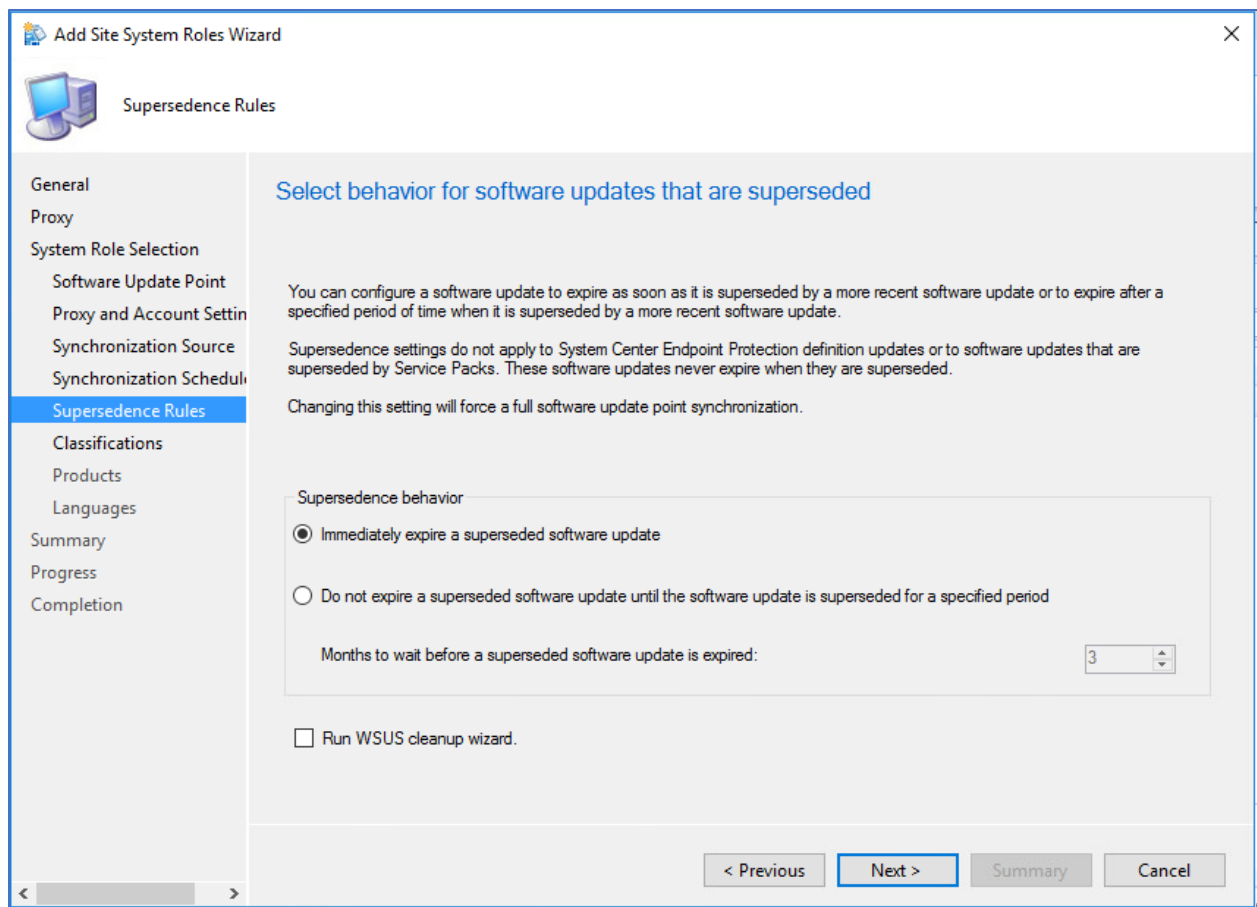
I neste punkt skal vi konfigurere WSUS. Her velger vi å bruke port 8530-8531 og Allow intranet-only client connections.



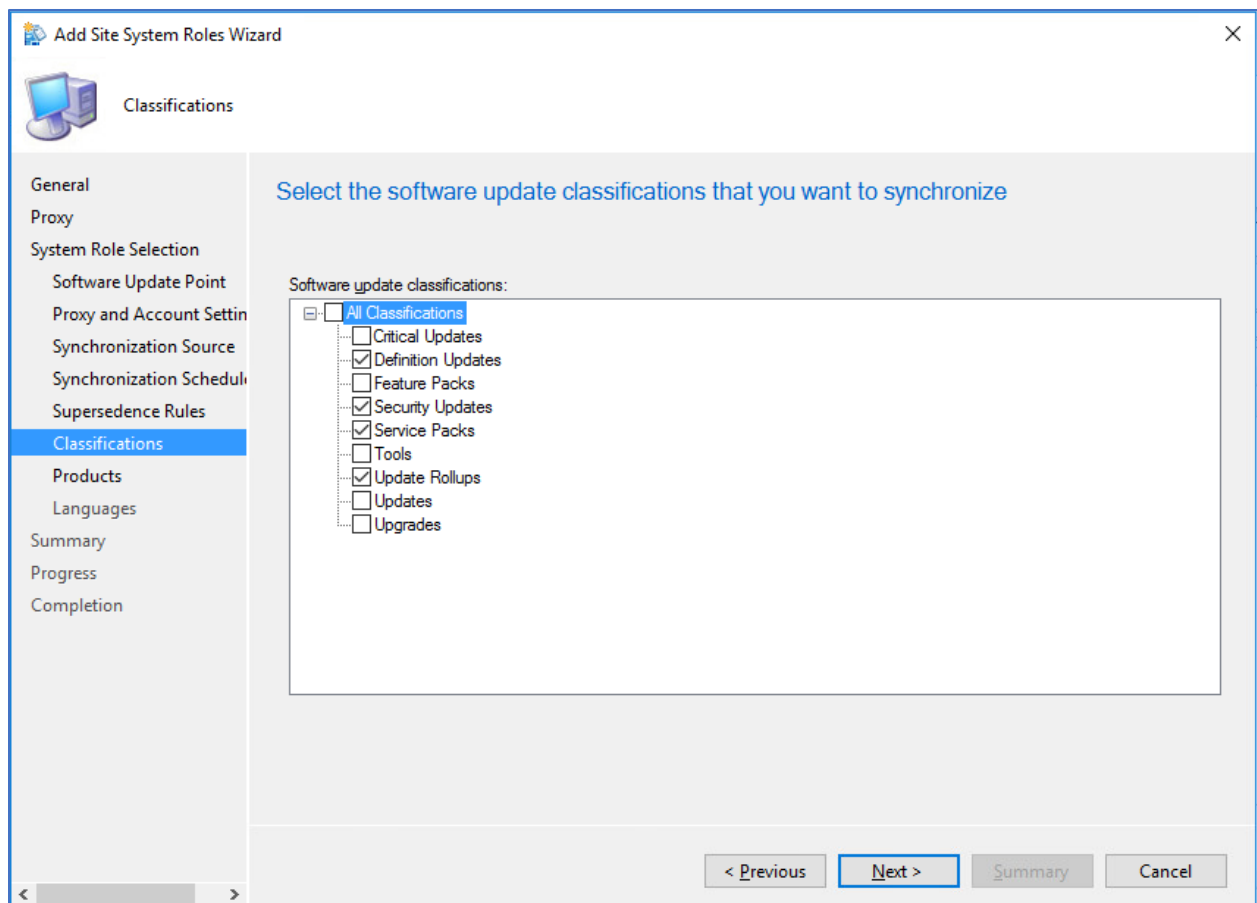
Når vi kommer til valget om hvor ofte vi vil synkronisere oppdateringer, velger vi hver 7. dag.



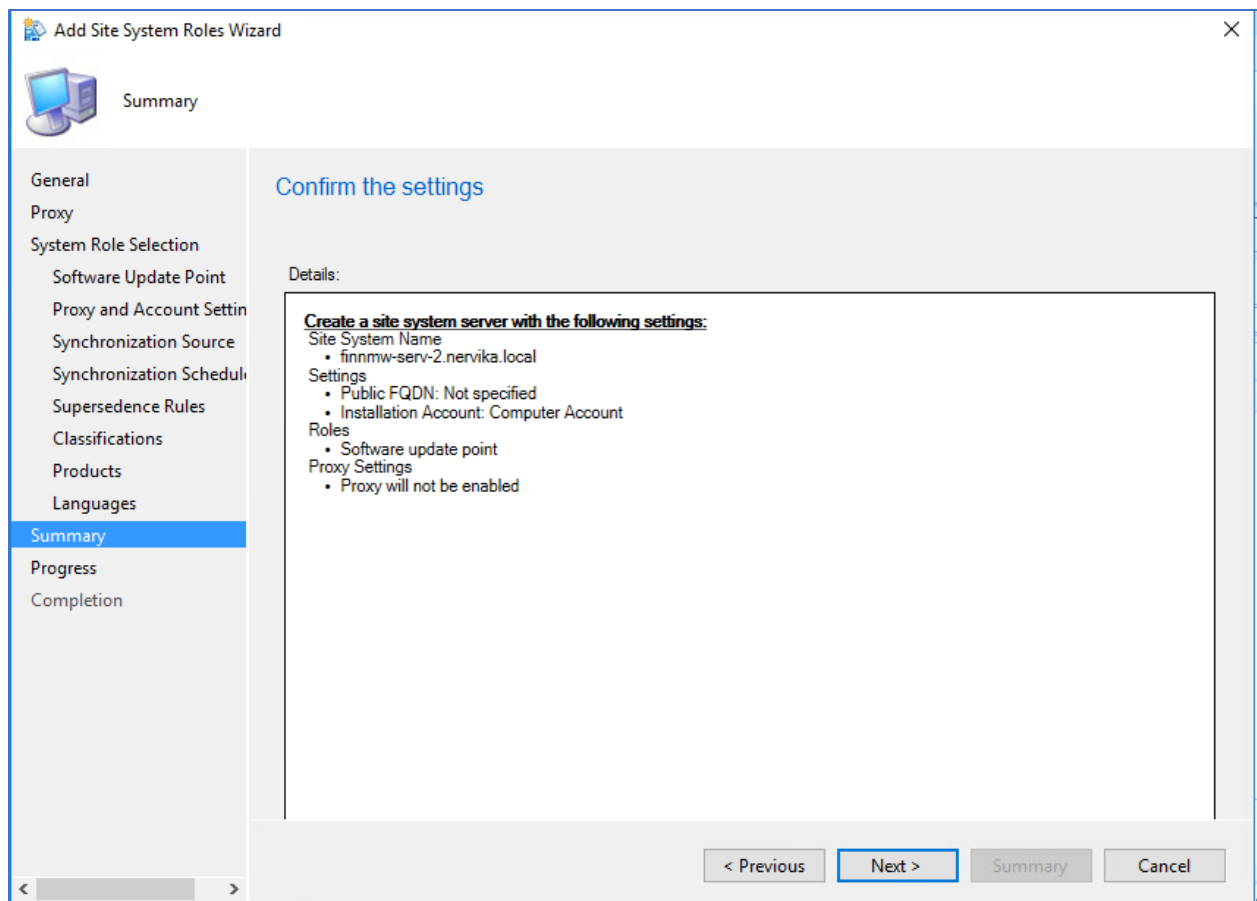
Vi velger også å umiddelbart slette gamle oppdateringer.



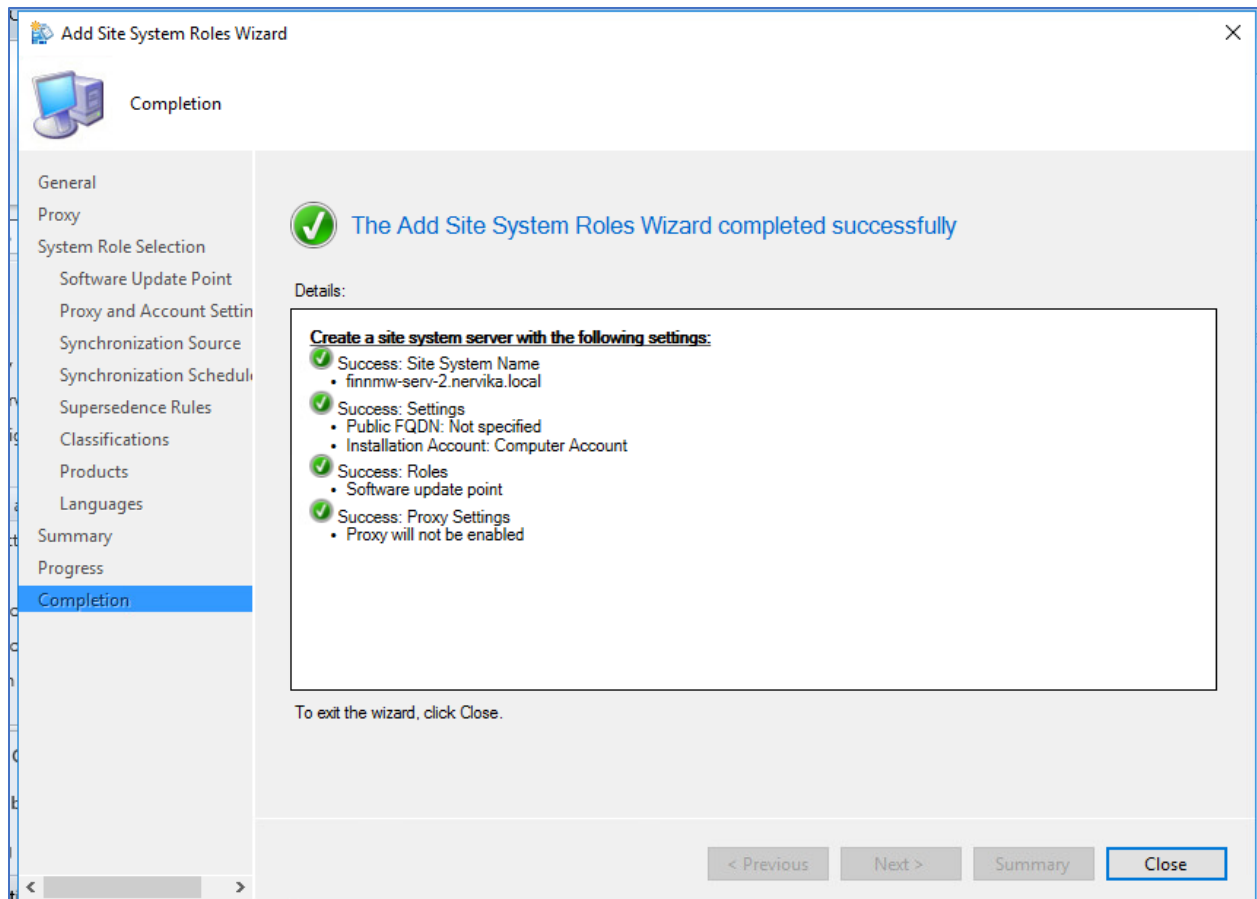
Under Classifications skal vi velge hva som skal synkroniseres. Velger her Defination Updates, Security Updates, Service Packs og Update Rollups.



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.



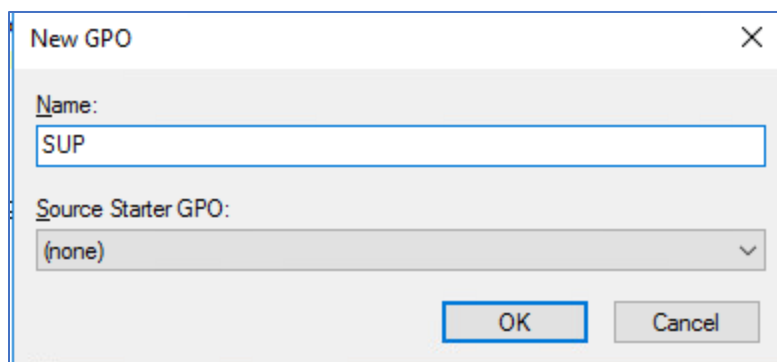
Når installasjonen er ferdig får vi opp en oversikt hvor vi ser at alt har gått vellykket.



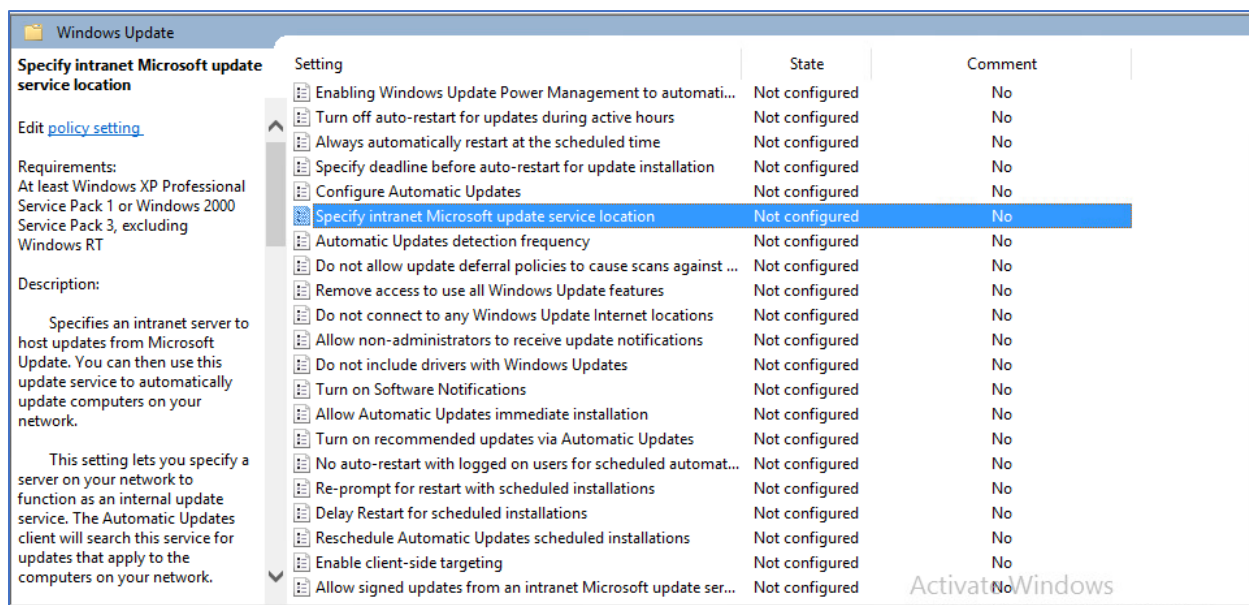
5. Discovery og Boundaries

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.

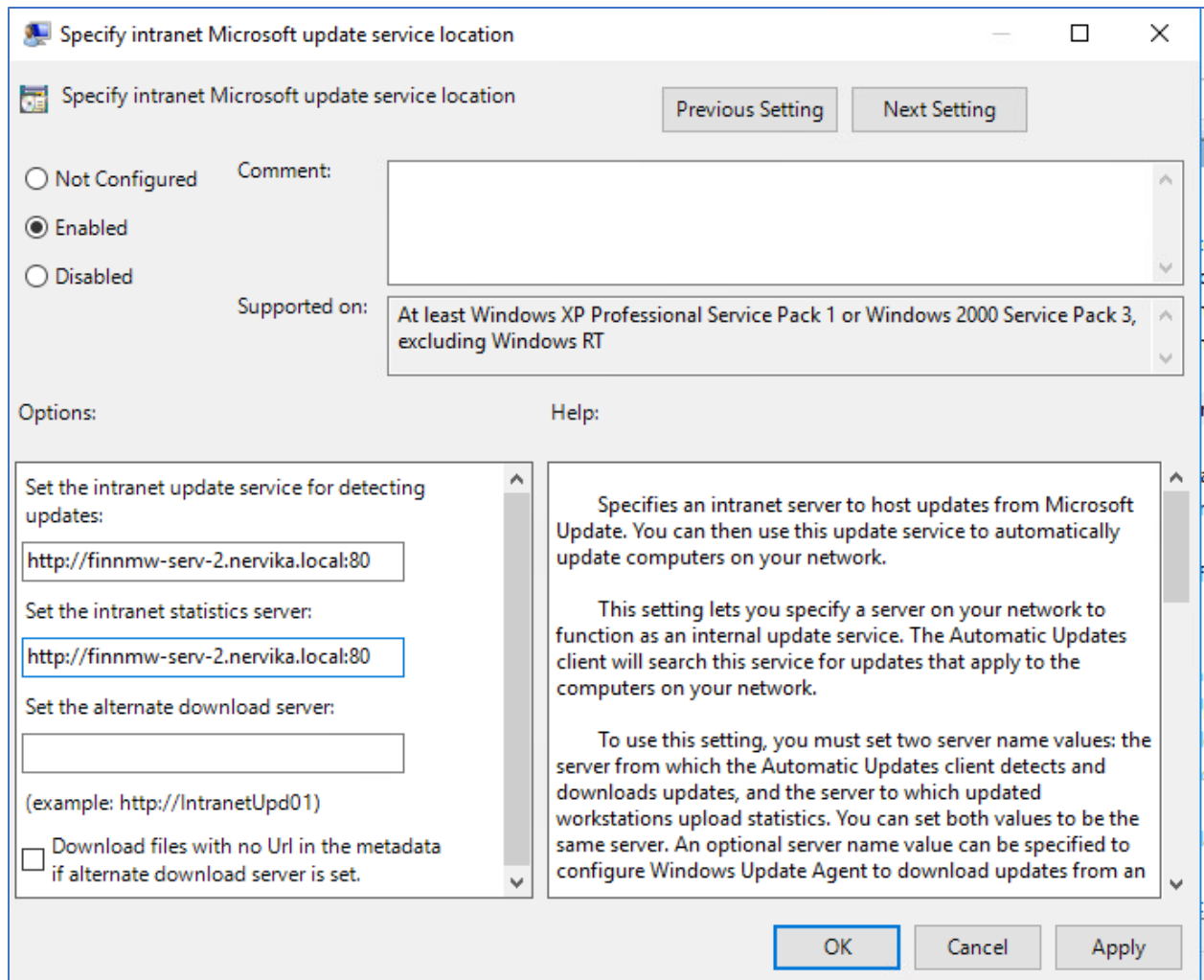
Først må vi åpne Group Policy Management, dette gjøres via Tools i Server Manager. For å opprette en ny GPO navigerer vi oss fra Forest:nervika.local → Domains → Nervika.local. Høyreklikker her på nervika.local og trykker Create a GPO in this domain, and Link it here. Her velger vi å gi GPOen navnet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

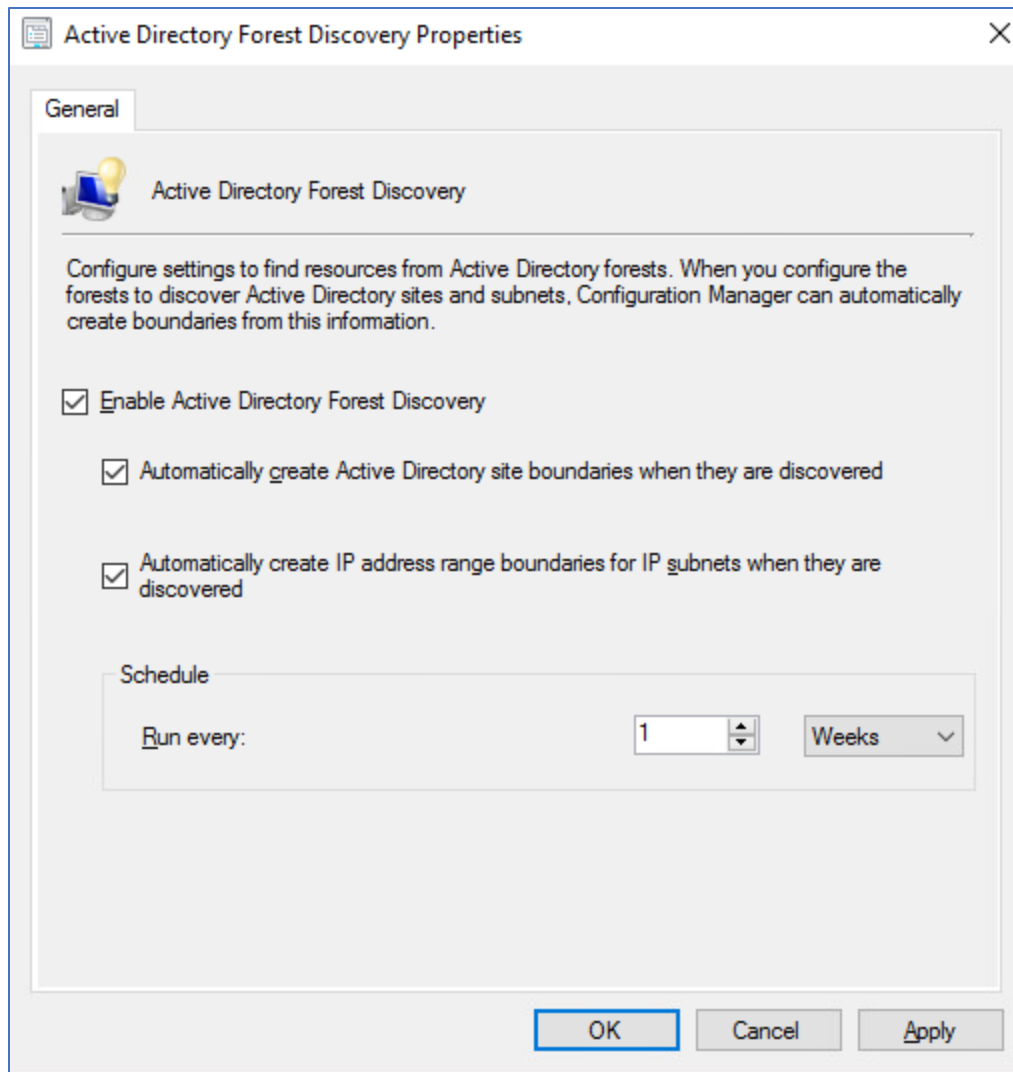


Her skal vi åpne Specify Intranet Microsoft Update Service Location. Inne på den skal vi sette den til å være Enabled. Vi må også adressen til SCCM-serveren og porten som SUP bruker. SUP kjører port 80 som standard.



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 haker 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.

Add Active Directory Location [X]

Active Directory location
Enter the location by using a distinguished name (DN) for an Active Directory forest, domain, container, or organizational unit (OU). Or, browse to the location.

! When you specify an Active Directory location that has a large number of groups or groups that have many members, the discovery process can take a long time to finish.

Name:

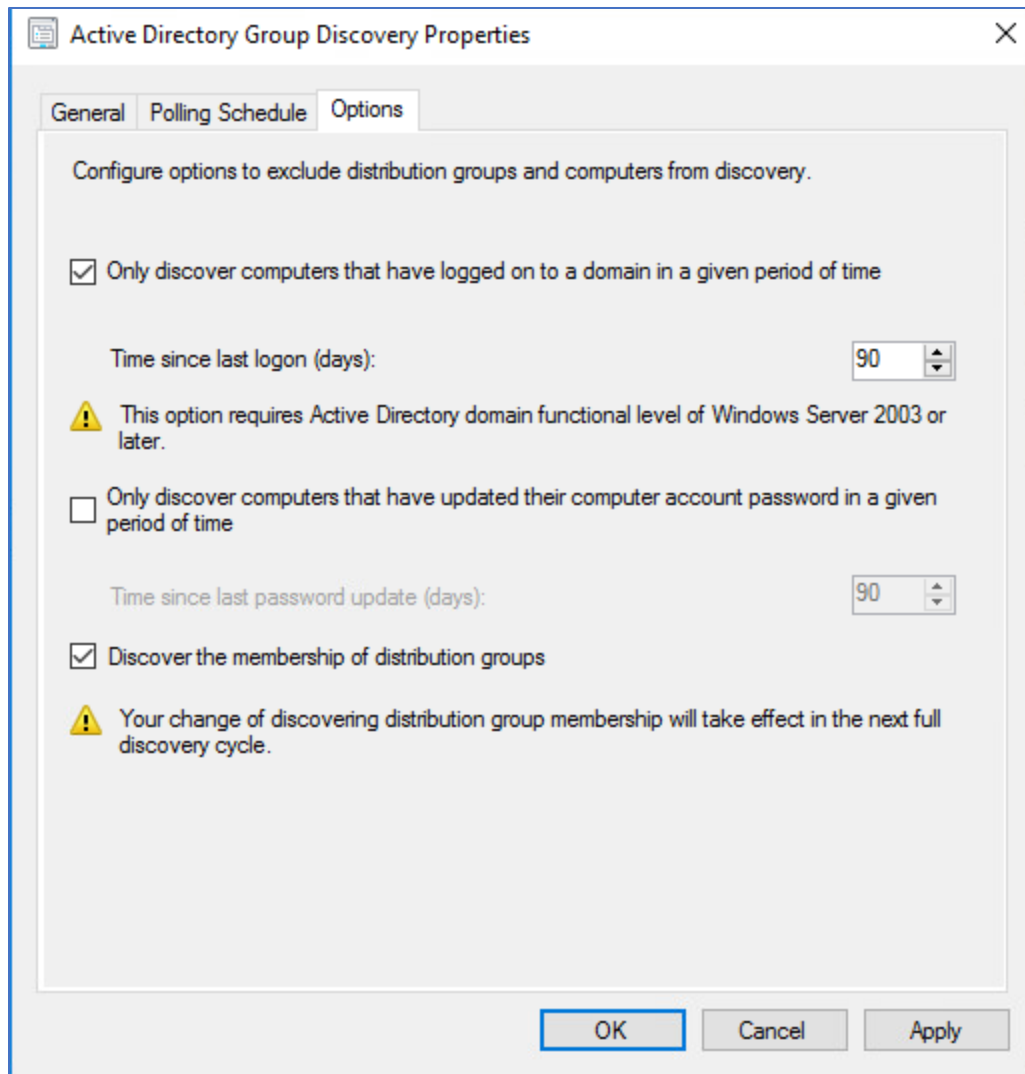
Location: Example: LDAP://OU=UserAccounts, DC=contoso, DC=com

Recursively search Active Directory child containers

Active Directory Group Discovery Account
The Active Directory Group Discovery Account must have Read permission to the specified location.

Use the site server's computer account
 Specify an account:

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.

Active Directory Container

Specify an Active Directory container to search during the discovery process.

Location

Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.

Path:

LDAP://CN=System Management,CN=System,DC=nervika,DC=locz

Browse...

Search Options

Select options to modify the search behavior.

Recursively search Active Directory child containers

Discover objects within Active Directory groups

Active Directory Discovery Account

The Active Directory Discovery Account must have Read permission to the specified location.

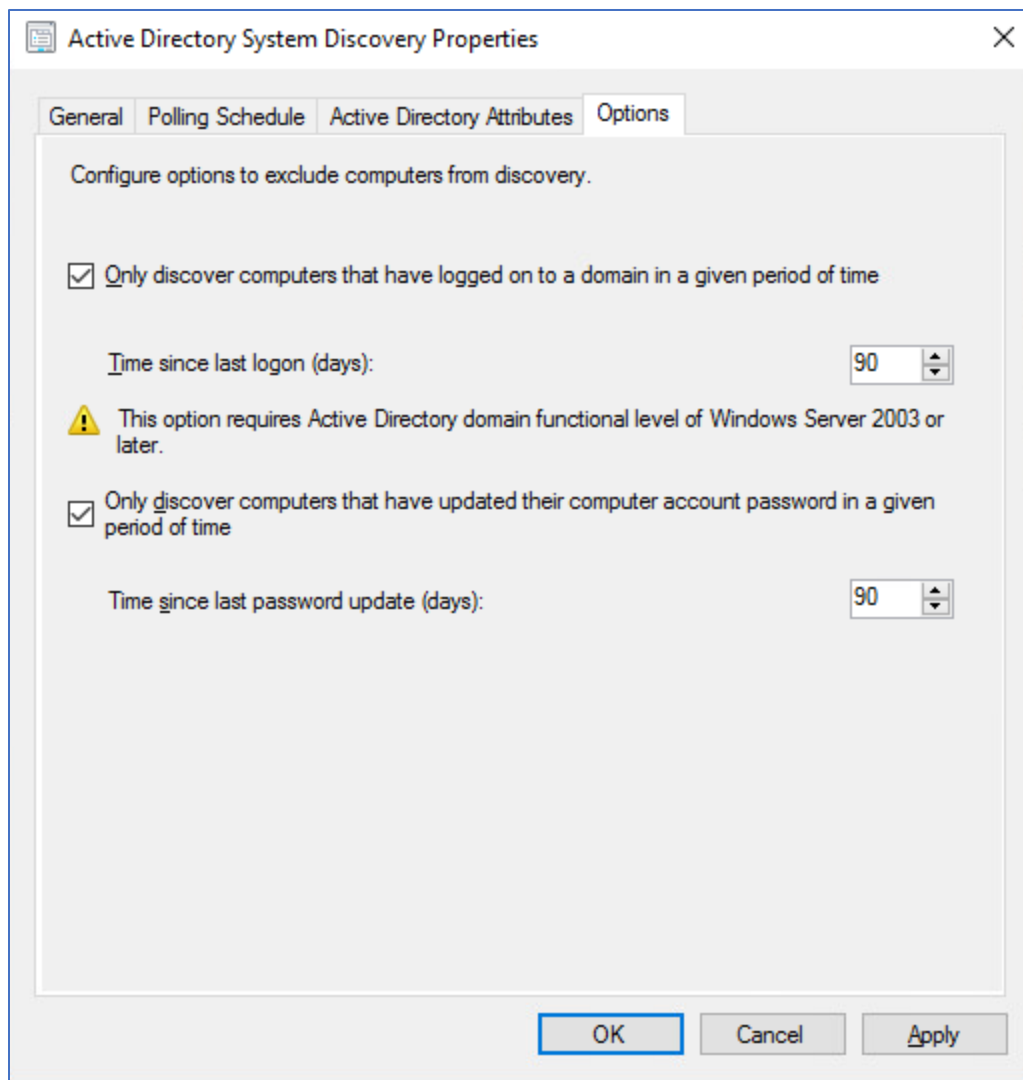
Use the computer account of the site server

Specify an account:

Set...

OK Cancel

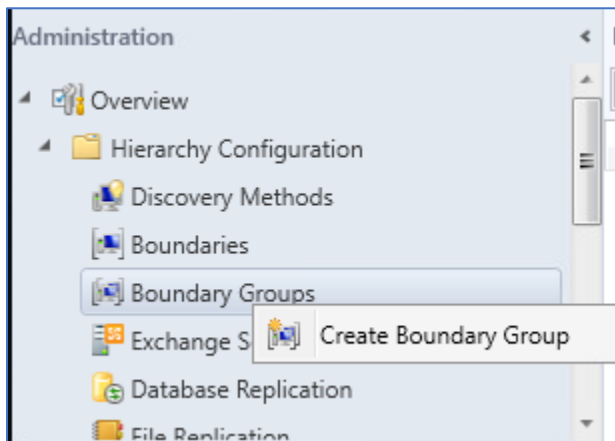
Trykk OK og naviger til Options-fanen. Her skal vi velge de samme innstillingene som vi gjorde under Active Directory Group Discovery.



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.

Discovery Methods 6 items				
Search				
Icon	Name	Status	Site	Description
	Active Directory Forest Discovery	Enabled	NER	Configures settings that Configuration Manager uses to find A...
	Active Directory Group Discovery	Enabled	NER	Configures settings that Configuration Manager uses to find g...
	Active Directory System Discovery	Enabled	NER	Configures settings that Configuration Manager uses to find c...
	Active Directory User Discovery	Enabled	NER	Configures settings that Configuration Manager uses to find u...
	Heartbeat Discovery	Enabled	NER	Configures interval for Configuration Manager clients to perio...
	Network Discovery	Disabled	NER	Configures settings and polling intervals to discover resources...

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.

Create Boundary Group

General References

Name: SCCM boundary group

Description:

The following boundaries are members of this boundary group.

Boundaries:

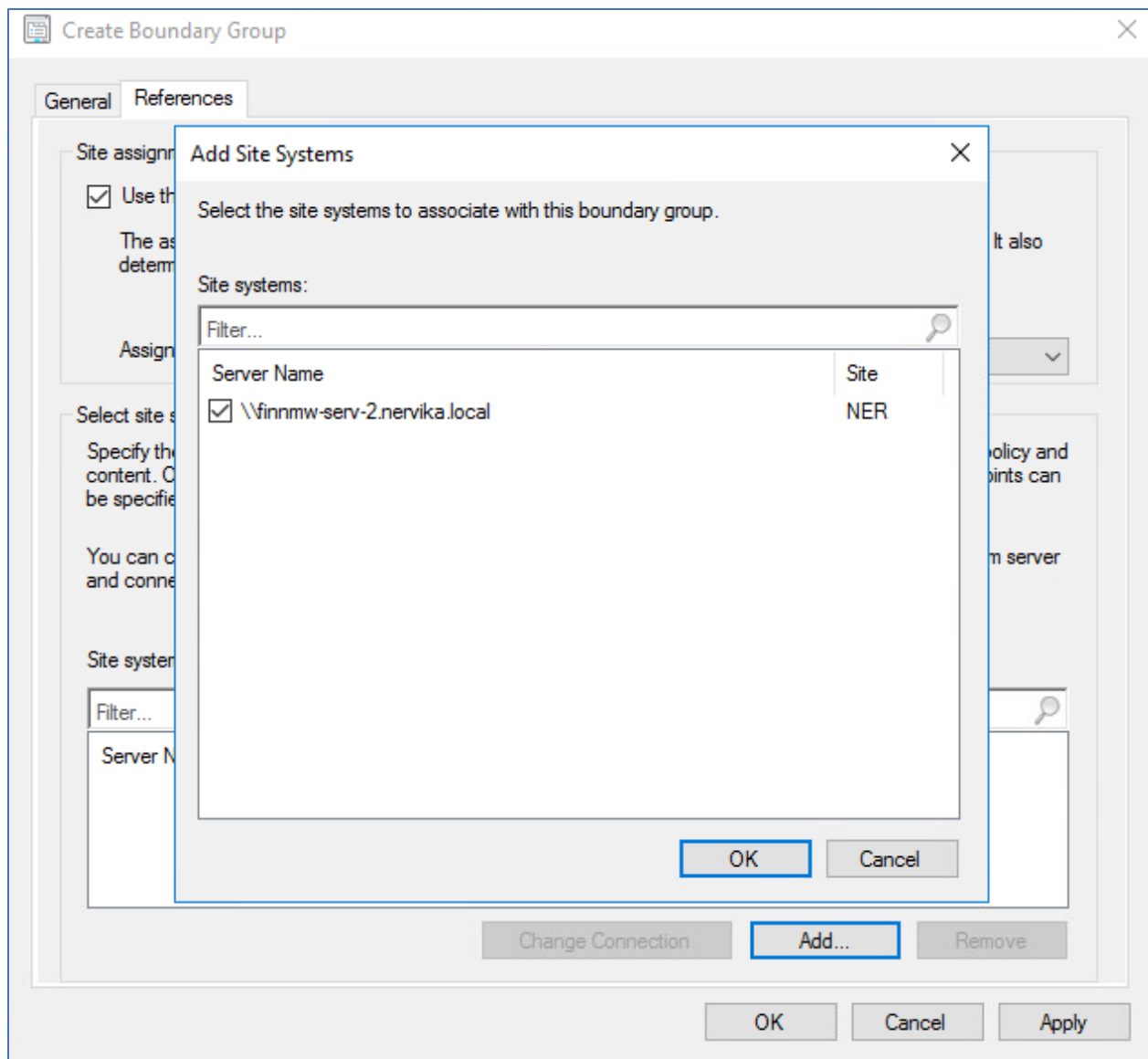
Filter...

Name	Description
There are no items to show in this view.	


Add... Remove

OK Cancel Apply

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

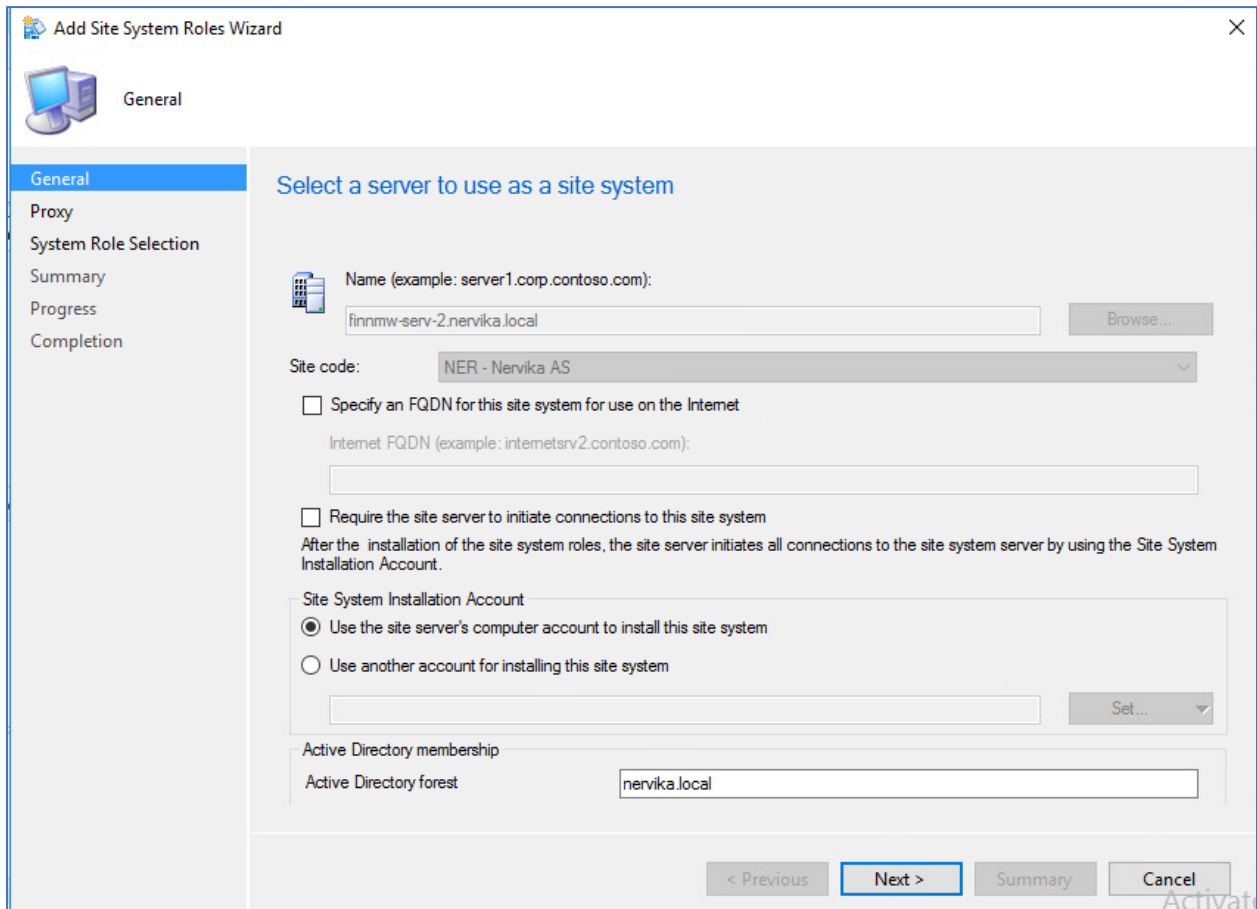


Trykk Apply og OK, så blir Boundary-gruppen opprettet.

Boundary Groups 1 items					
Search					
Icon	Name	Member Count	Site System Count	Read-Only	
	SCCM boundary group	0	1	No	

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.

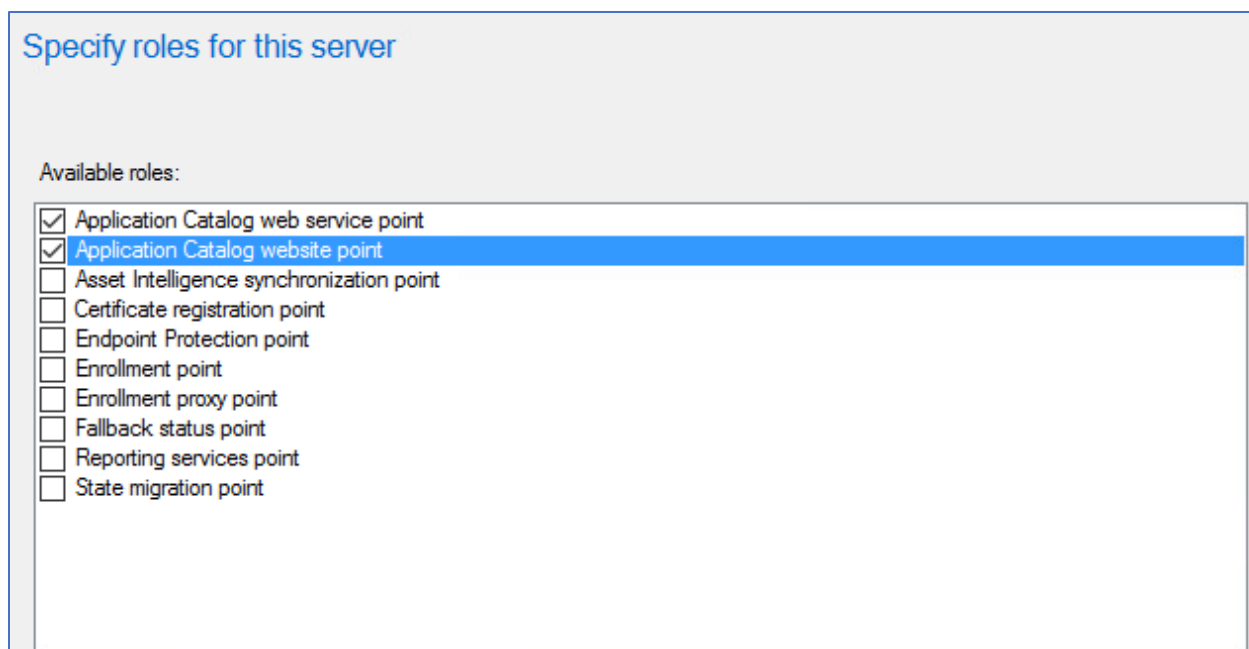


The screenshot shows the 'Add Site System Roles Wizard' dialog box, General tab. The title bar reads 'Add Site System Roles Wizard'. The left sidebar contains the following steps: General (selected), Proxy, System Role Selection, Summary, Progress, and Completion. The main area is titled 'Select a server to use as a site system'. It contains the following fields and options:

- Name (example: server1.corp.contoso.com):
- Site code:
- Specify an FQDN for this site system for use on the Internet
Internet FQDN (example: internetstv2.contoso.com):
- Require the site server to initiate connections to this site system
After the installation of the site system roles, the site server initiates all connections to the site system server by using the Site System Installation Account.
- Site System Installation Account:
 - Use the site server's computer account to install this site system
 - Use another account for installing this site system
- Active Directory membership:
Active Directory forest:

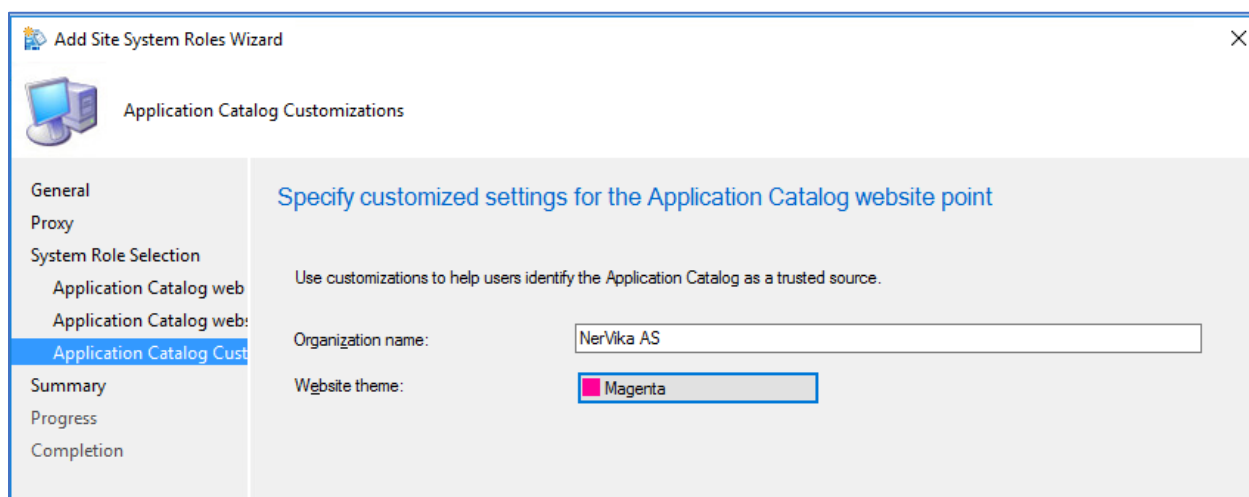
At the bottom right, there are four buttons: '< Previous' (disabled), 'Next >' (active), 'Summary' (disabled), and 'Cancel' (disabled). A watermark 'Activat' is visible in the bottom right corner.

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:



The Add Site System Roles Wizard completed successfully

Details:

Create a site system server with the following settings:

- ✓ Success: Site System Name
 - finnmw-serv-2.nervika.local
- ✓ Success: Settings
 - Public FQDN: Not specified
 - Installation Account: Computer Account
- ✓ Success: Roles
 - Application Catalog web service point
 - Application Catalog website point
- ✓ Success: Proxy Settings
 - Proxy will not be enabled

Nå må vi konfigurere Configuration 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.

Configure Client Setting

Configure the setting: Default Application Catalog website point

Select Application Catalog website point

Value: finnmw-serv-2.nervika.local(use intranet FQDN)

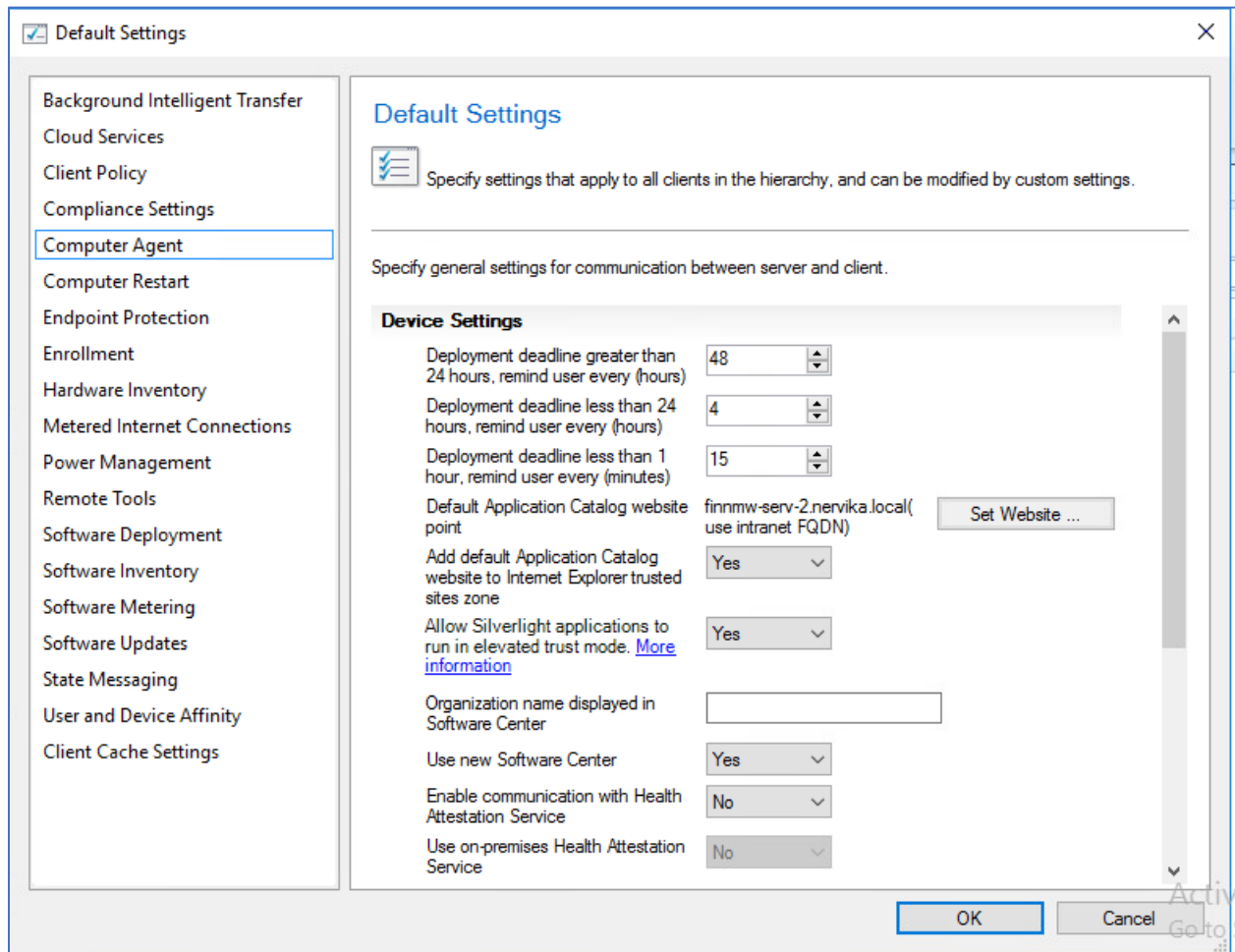
Specify a URL

The URL must contain the netBIOS name or FQDN of the server. Specifying the IP address of the server is not supported.

Value: Syntax: http[s]://server:port

OK Cancel

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.

Default Settings



Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Specify how client computers deploy software updates.

Device Settings



Enable software updates on clients

Yes

Software update scan schedule

Occurs every 1 days effective
01.02.1970 00.00

Schedule ...

Schedule deployment re-evaluation

Occurs every 1 days effective
01.02.1970 00.00

Schedule ...

When any software update deployment deadline is reached, install all other software update deployments with deadline coming within a specified period of time

No

Period of time for which all pending deployments with deadline in this time will also be installed

1

Hours

Enable management of the Office 365 Client Agent

Not Configured

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.

Default Settings



Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Specify user and device affinity settings for client computers.

Device Settings



User device affinity usage threshold (minutes)

2880

User device affinity usage threshold (days)

30

Automatically configure user device affinity from usage data

No

User Settings



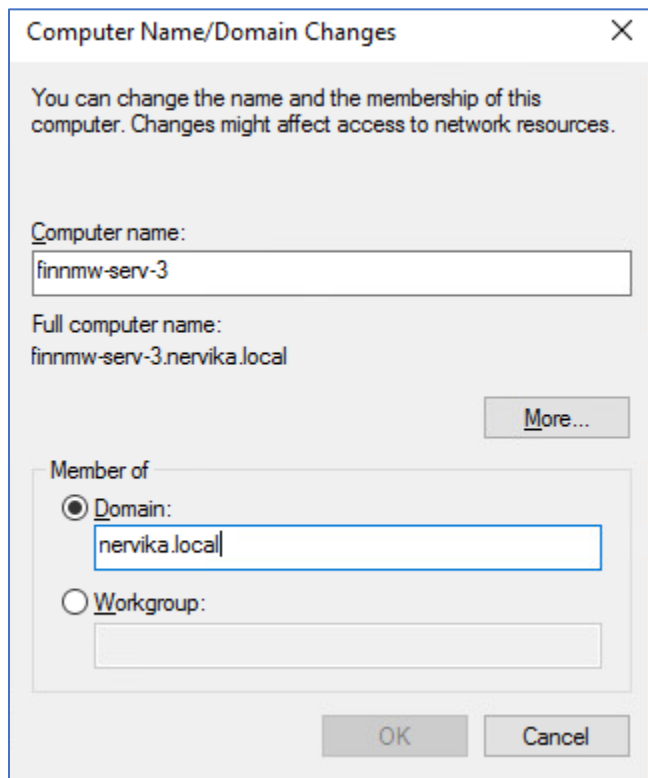
Allow user to define their primary devices

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.

New Object - User ×

 Create in: nervika.local/Users

First name: Initials:

Last name:


Full name:

User logon name:
 @nervika.local ▾

User logon name (pre-Windows 2000):

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.

New Object - Group ✕

 Create in: nervika.local/Users

Group name:

Group name (pre-Windows 2000):


Group scope

Domain local
 Global
 Universal

Group type

Security
 Distribution

New Object - Group ✕

 Create in: nervika.local/Users

Group name:

Group name (pre-Windows 2000):

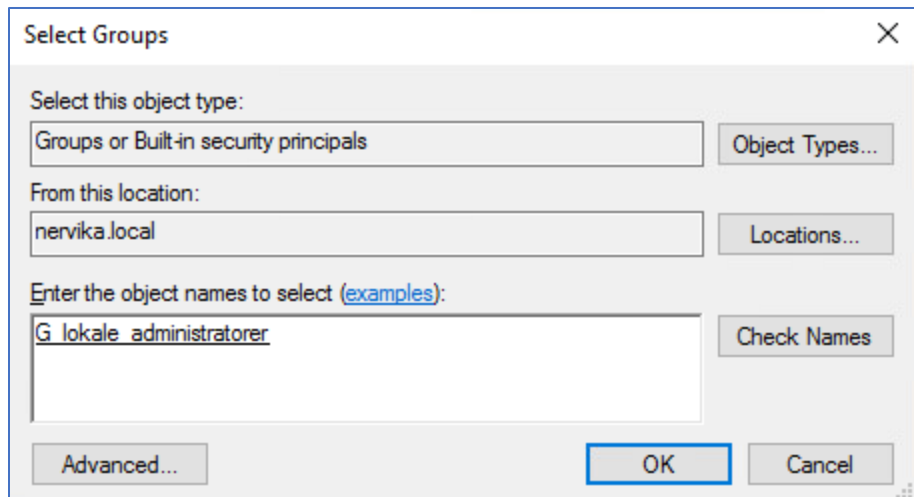
Group scope

Domain local
 Global
 Universal

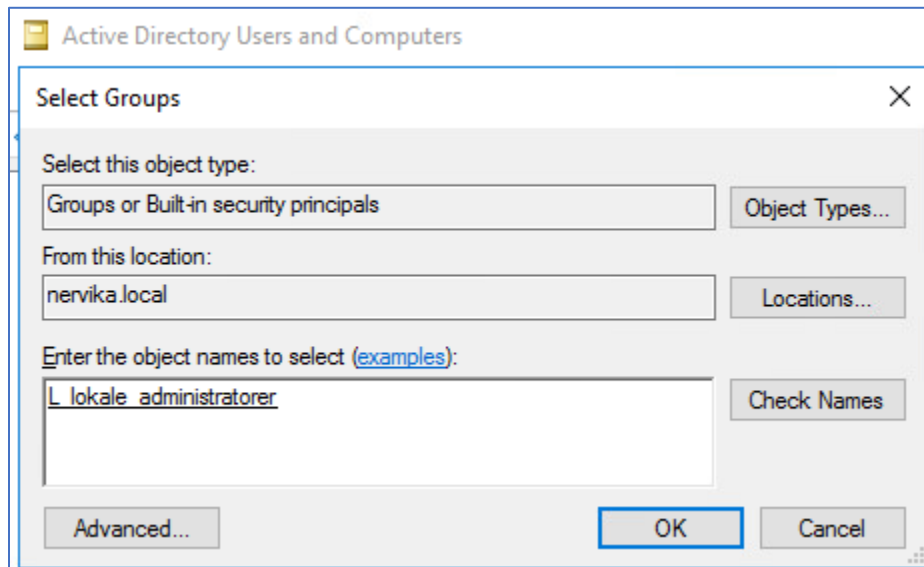
Group type

Security
 Distribution

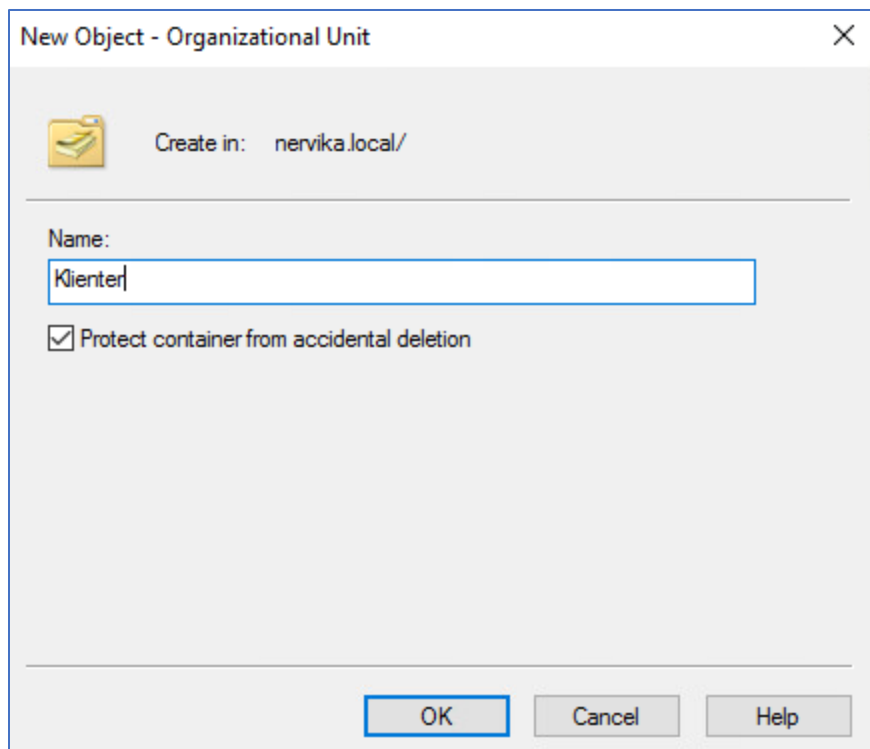
Brukeren ClientInstall som vi nettopp opprettet skal legges inn i den globale gruppen, G_lokale_administratorer. Dette gjøres ved å høyreklikke på brukeren → Add to group.



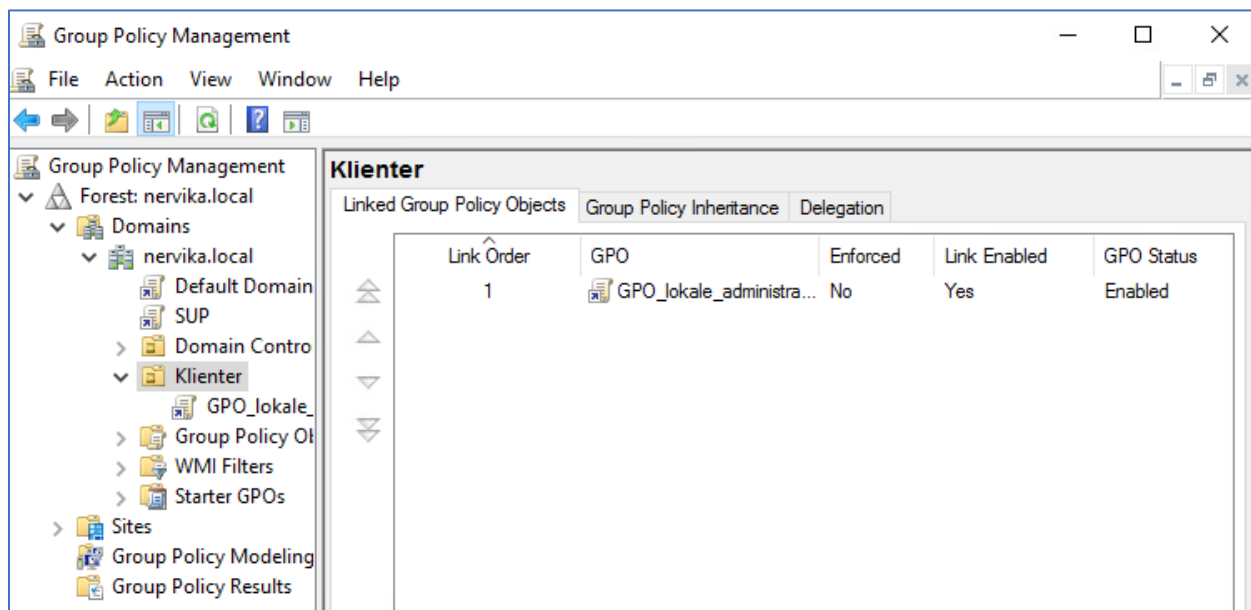
Nå skal vi legge G_lokale_administratorer inn i den andre gruppen, L_lokale_administratorer. Dette gjøres på samme måte, høyreklikk på gruppen → Add to group.



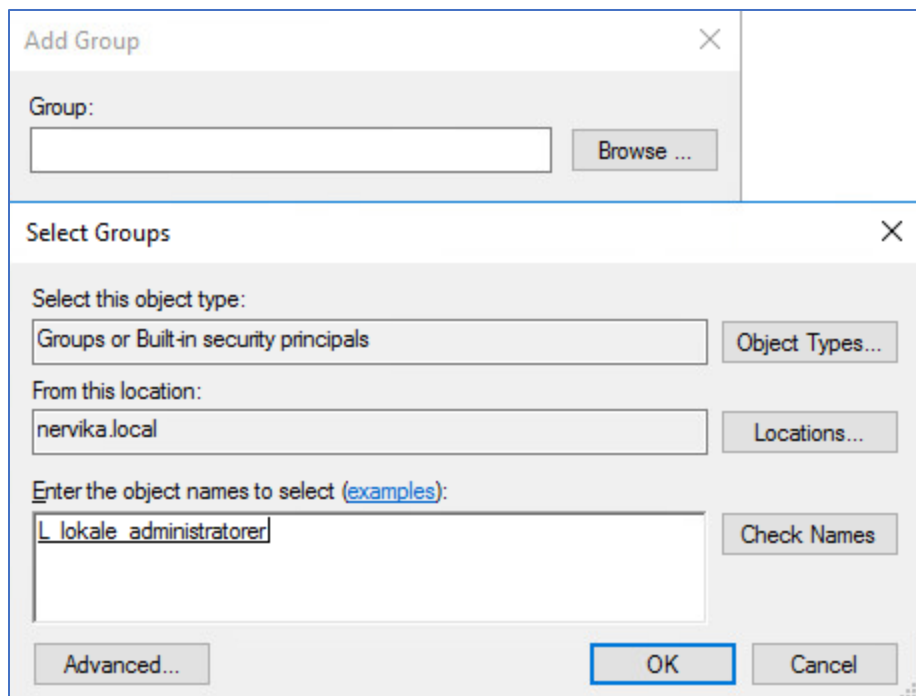
Nå må vi opprette en OU. Velger å kalle den OUn for Klienter.



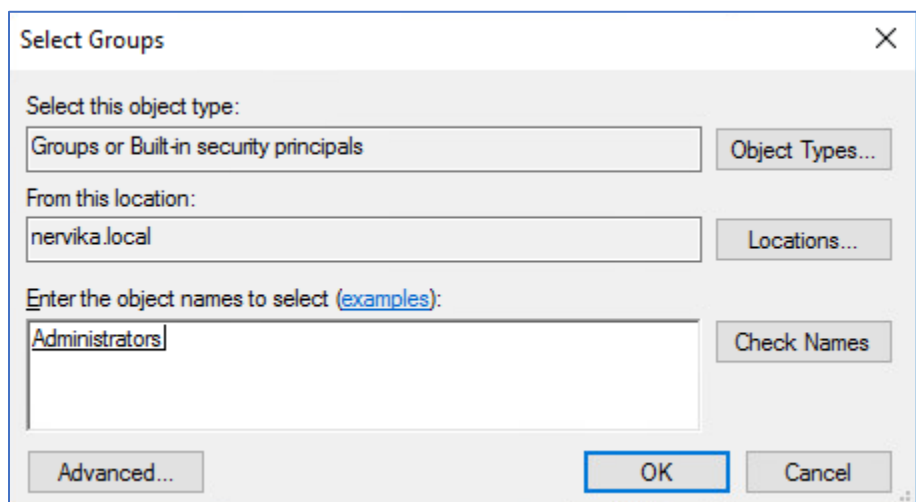
Under denne OUn oppretter vi en ny GPO som vi kaller GPO_lokale_administratorer. Dette gjøres ved å åpne Group Policy Management via Server Manager. Høyreklikk på OUn Klienter og Create a new GPO in this domain, and link it here.



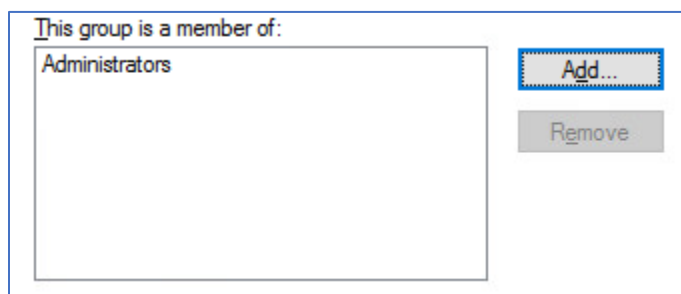
Nå høyreklikker vi på denne OUn og trykker edit. Her navigerer vi oss frem til Computer Configuration→Policies→Windows Settings→Security Settings→Restricted Groups. Høyreklikk og trykk Add Group. Her velger vi browse og finner L_lokale_administratorer.



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.



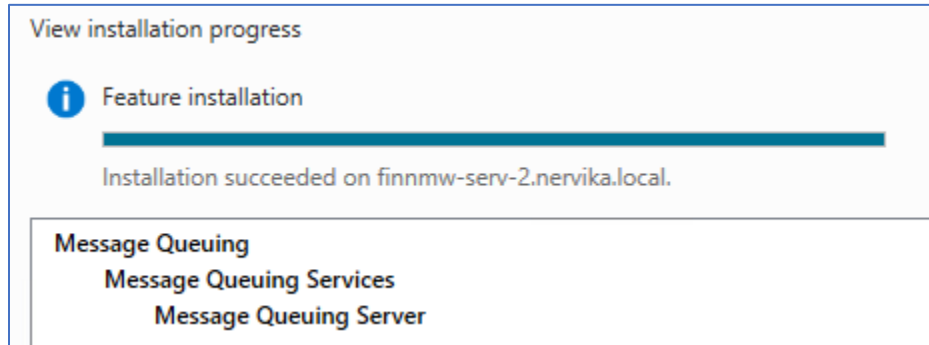
Da skal Administrators komme opp i listen under This group is a member of.



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.



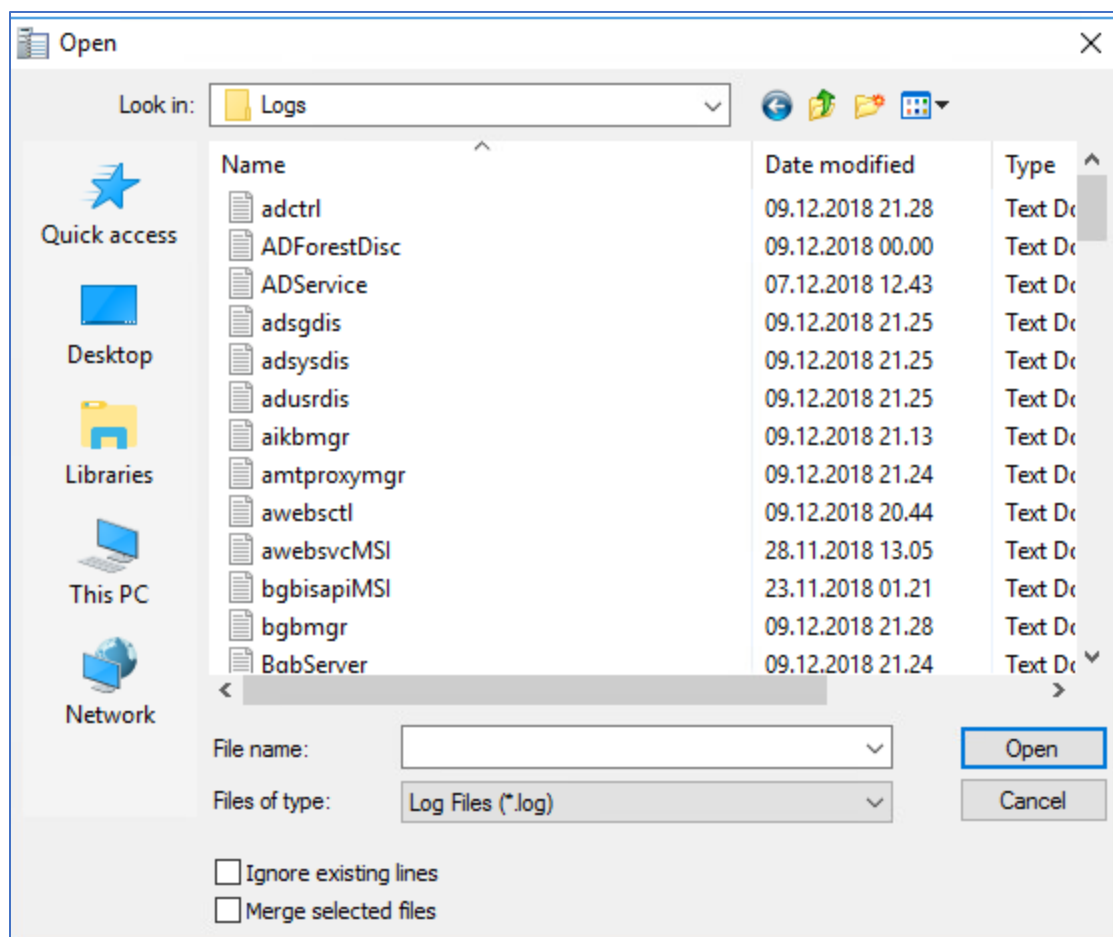
Nå må vi åpne brannmuren. Her måtte vi gjøre to endringer under Allowed apps. Network Discovery og Virtual Machine Monitoring ble lagt til med full tilgang.

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.

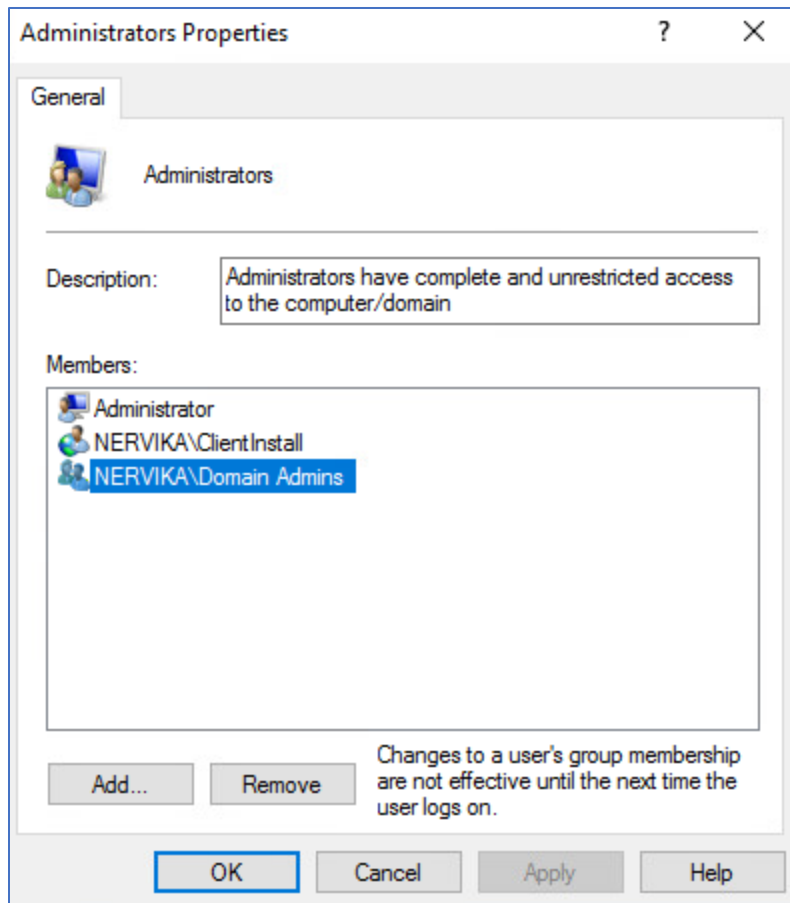
Trace Log Tool ligger på ISO-filen til SCCM. Navigerer oss til ISO-filen og finner mappen SMSSETUP/TOOLS. Her ligger det en fil som heter CMTrace.exe. Kopier så denne over til skrivebordet.

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.

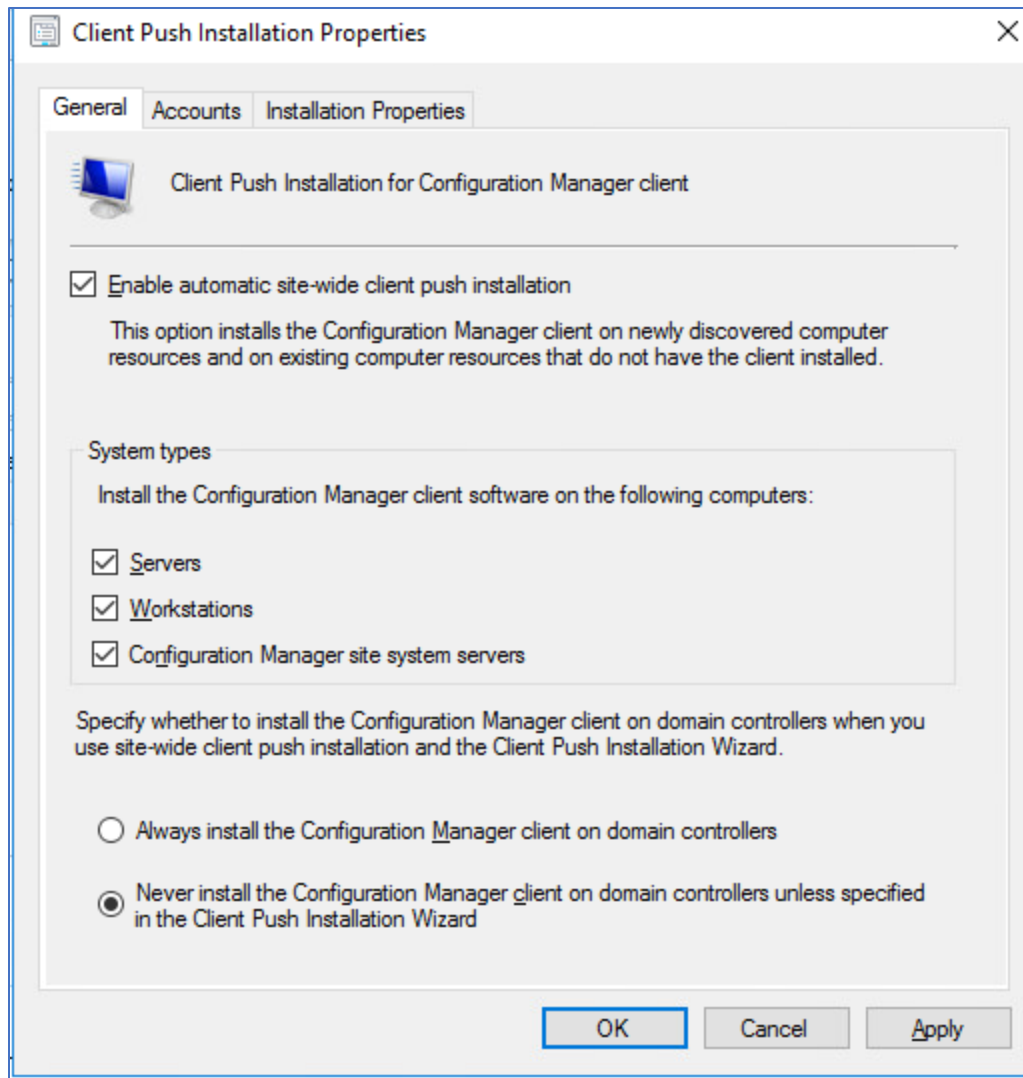


På klientmaskinene må vi også tillate noen regler i brannmuren.

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.

Windows User Account

User name: NERVIKA\ClientInstall

Example: Domain\User

Password: ●●●●●●●●

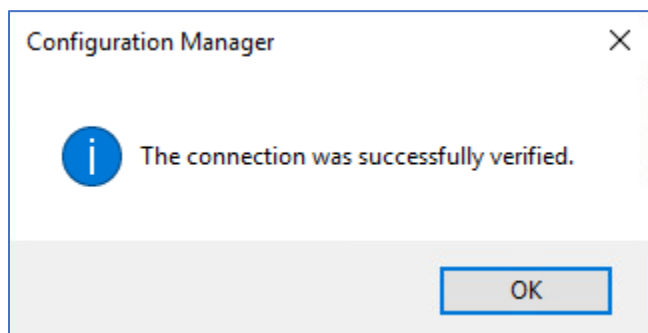
Confirm password: ●●●●●●●●

Data source: Network Share

Network share: \\FINNMW-SERV-2\Sources

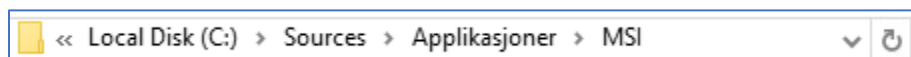
Example: \\server\share

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



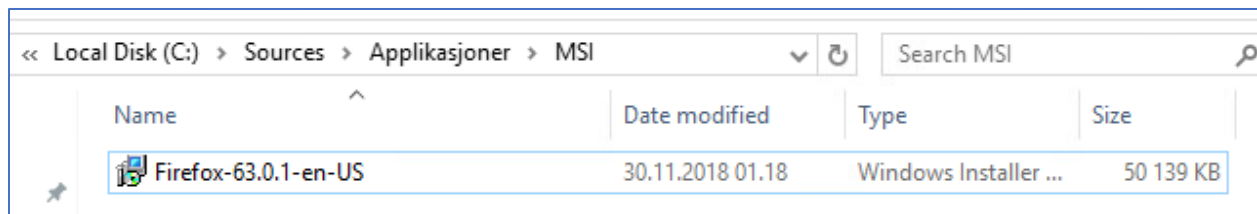
8. Utrulling av applikasjoner

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.

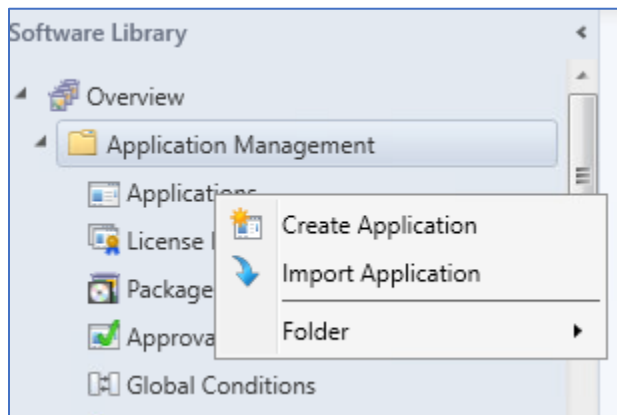


Først skal vi prøve å rulle ut Firefox. Laster derfor ned MSI-installasjonsfilen til Firefox. Den finner vi på www.frontmotion.com.

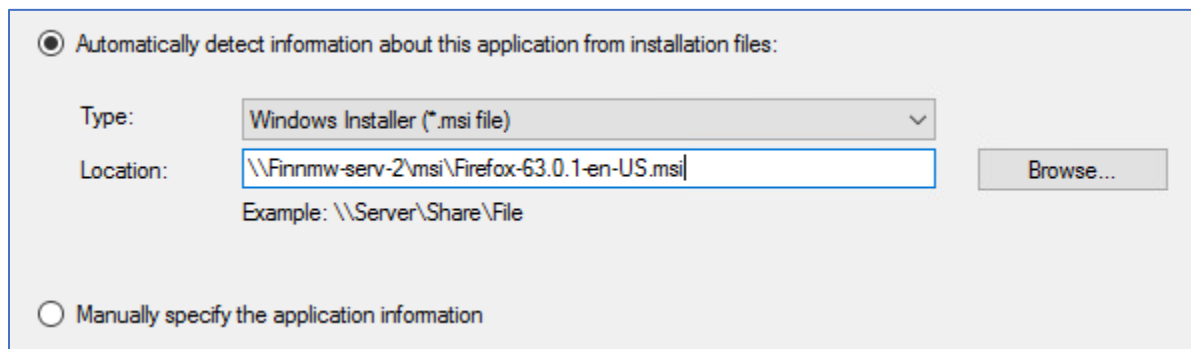
Legger så denne MSI-filen i MSI-mappen vi nettopp laget.



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.



View imported information



Application information successfully imported from the Windows Installer (*.msi file) file.

Details:

Application name: Mozilla Firefox (en-US)
Publisher:
Software version:

Deployment type name: Mozilla Firefox (en-US) - Windows Installer (*.msi file)
Product Code: {D40F842D-FB82-46E3-863B-7B07083F6465}
Installation behavior: Install for system

Content location: \\Finnmw-serv-2\msi\
Number of files: 1
Content files:
 Firefox-63.0.1-en-US.msi

To modify any details from the imported information, click Next. To exit this wizard without creating the application, click Cancel.

< Previous

Next >

Summary

Cancel

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.

Create Application Wizard

General Information

General
Import Information
General Information
Summary
Progress
Completion

Specify information about this application

Name: Mozilla Firefox (en-US)

Administrator comments:

Publisher: Mozilla

Software version: 63.0.1

Optional reference:

Administrative categories: "Browser" Select...

Specify the installation program for this application and the required installation rights.

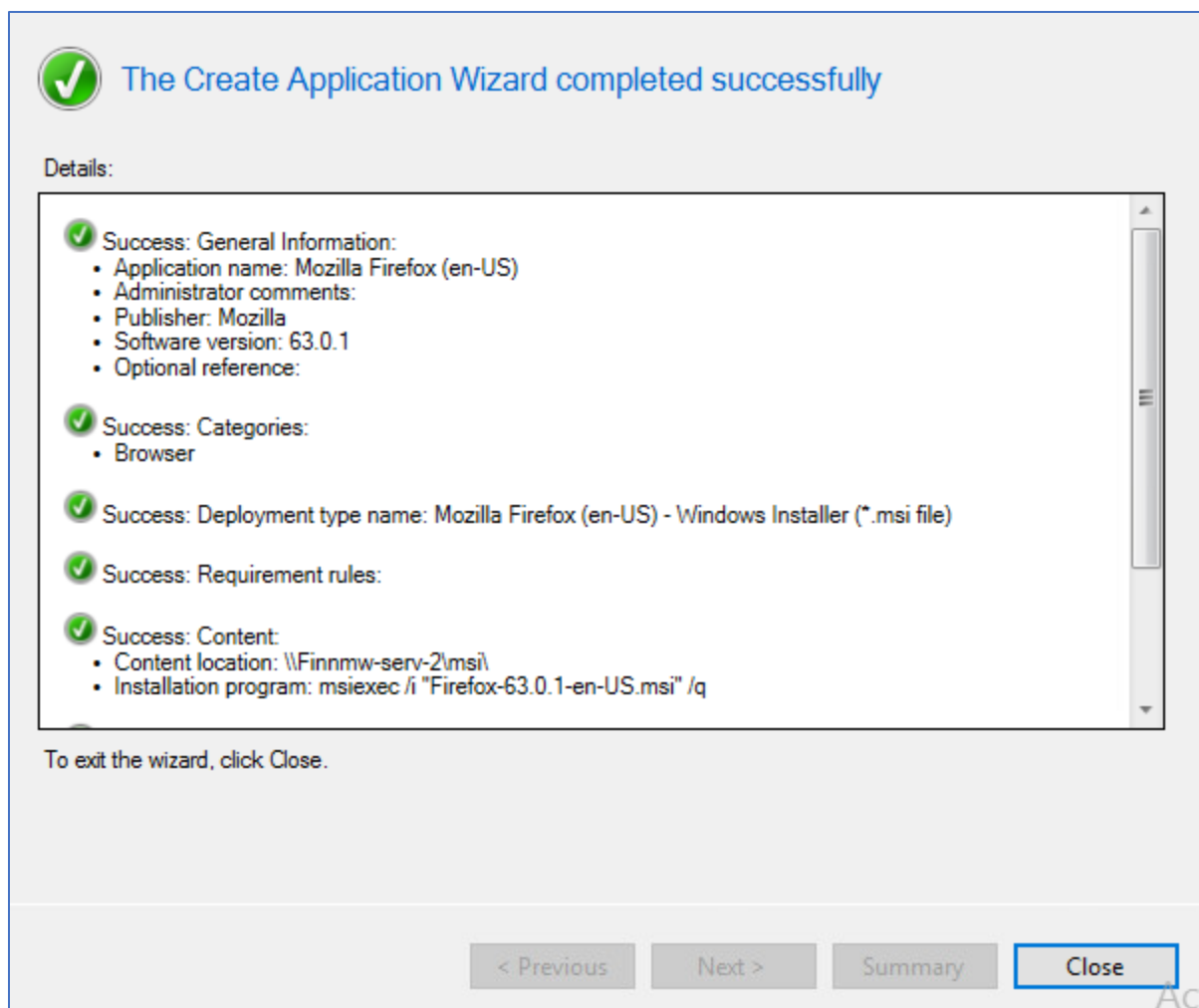
Installation program: msisexec /i "Firefox-63.0.1-en-US.msi" /q Browse...

Run installation program as 32-bit process on 64-bit clients.


Install behavior: Install for system

< Previous **Next >** Summary Cancel

Nå er det bare å sette i gang med 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.

Applications 1 items					
Search					
Icon	Name	Deployment Types	Deployments	Status	
	Mozilla Firefox (en-US)	1	0	Active	

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

Mozilla Firefox (en-US)						
Icon	Priority	Name	Dependencies	Technology Title	Superseded	Content ID
	1	Mozilla Firefox (en-US) - Windows Installer (*.msi)	No	Windows Installer...	No	Content ID

Summary | Deployment Types | Deployments

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.

Mozilla Firefox (en-US) - Windows Installer (*.msi file) Properties

General | Content | Programs | Detection Method | User Experience | **Requirements** | Return Codes | Dependencies

Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.

Requirements:

Requirement Type	Operator	Values
Operating system	One of	{All Windows RT; All Windows 8 (64-bit); All Win...

Add... Edit... Delete

OK Cancel Apply

Nå er det på tide å kjøre ut Firefox. Vi finner installasjonsfilen under Applications→Høyreklikk→Deploy. Under Collection velger vi All Users.

Specify general information for this deployment

Software:

Collection:

Use default distribution point groups associated to this collection

Automatically distribute content for dependencies

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

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Filter...

Name	Description	Associations
FINNMW-SERV-2.NER...	Distribution point	

< Previous Next > Summary Cancel

Under Deployment gjør vi disse valgene:

Specify settings to control how this software is deployed

Action:

Purpose:

Require administrator approval if users request this application

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

Specify the user experience for the installation of this software on the selected devices

Specify user experience setting for this deployment

User notifications:

Display in Software Center and show all notifications

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

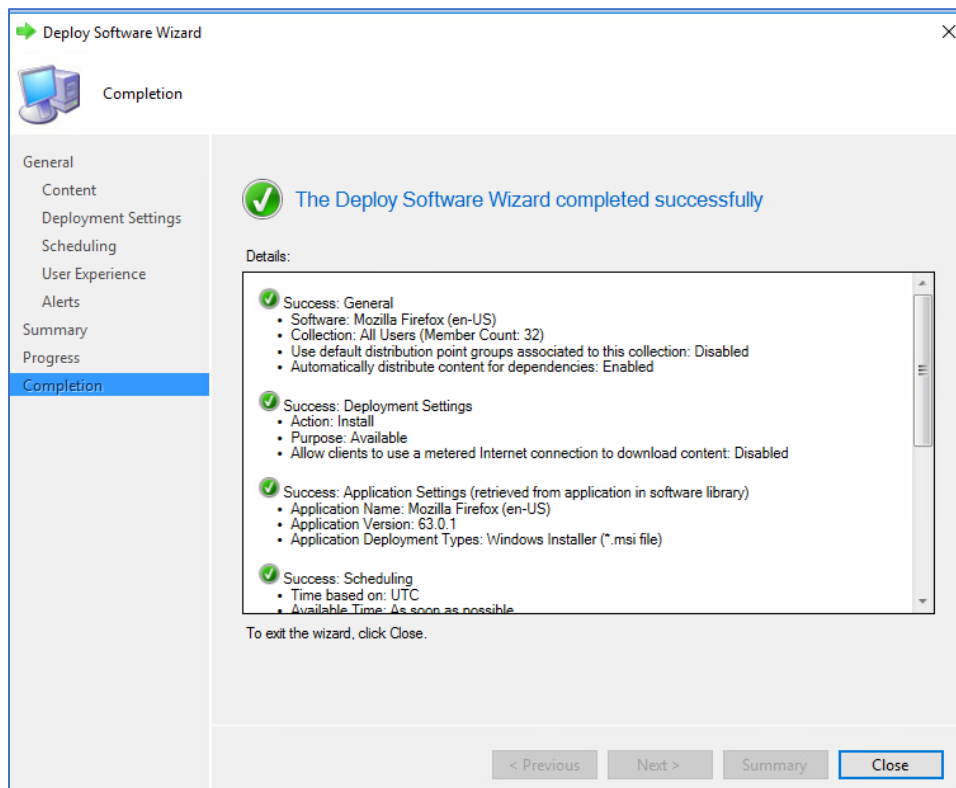
- Software Installation
- System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

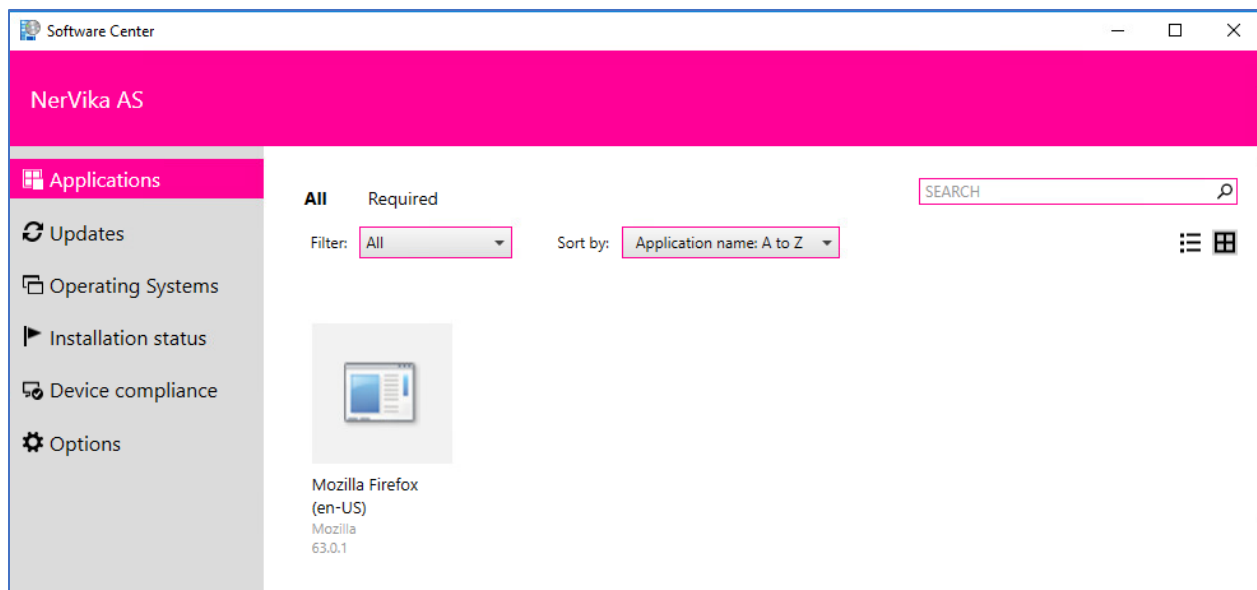
- Commit changes at deadline or during a maintenance window (requires restarts)

If this option is not selected, content will be applied on the overlay and committed later.

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



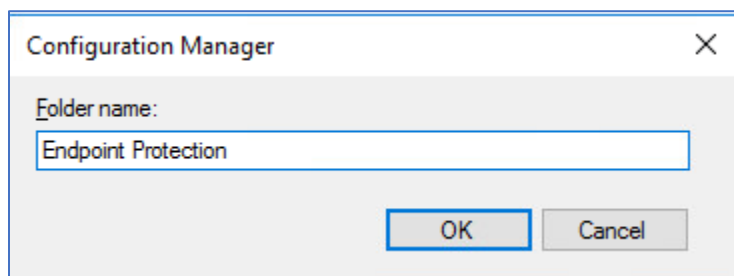
Vi kan nå se i Software Center at Mozilla Firefox er tilgjengelig.



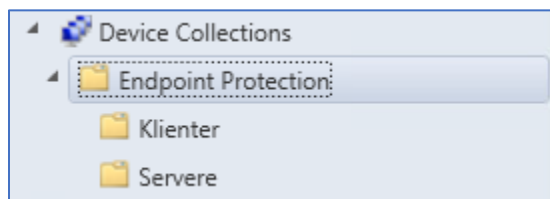
9. Endpoint Protection

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.

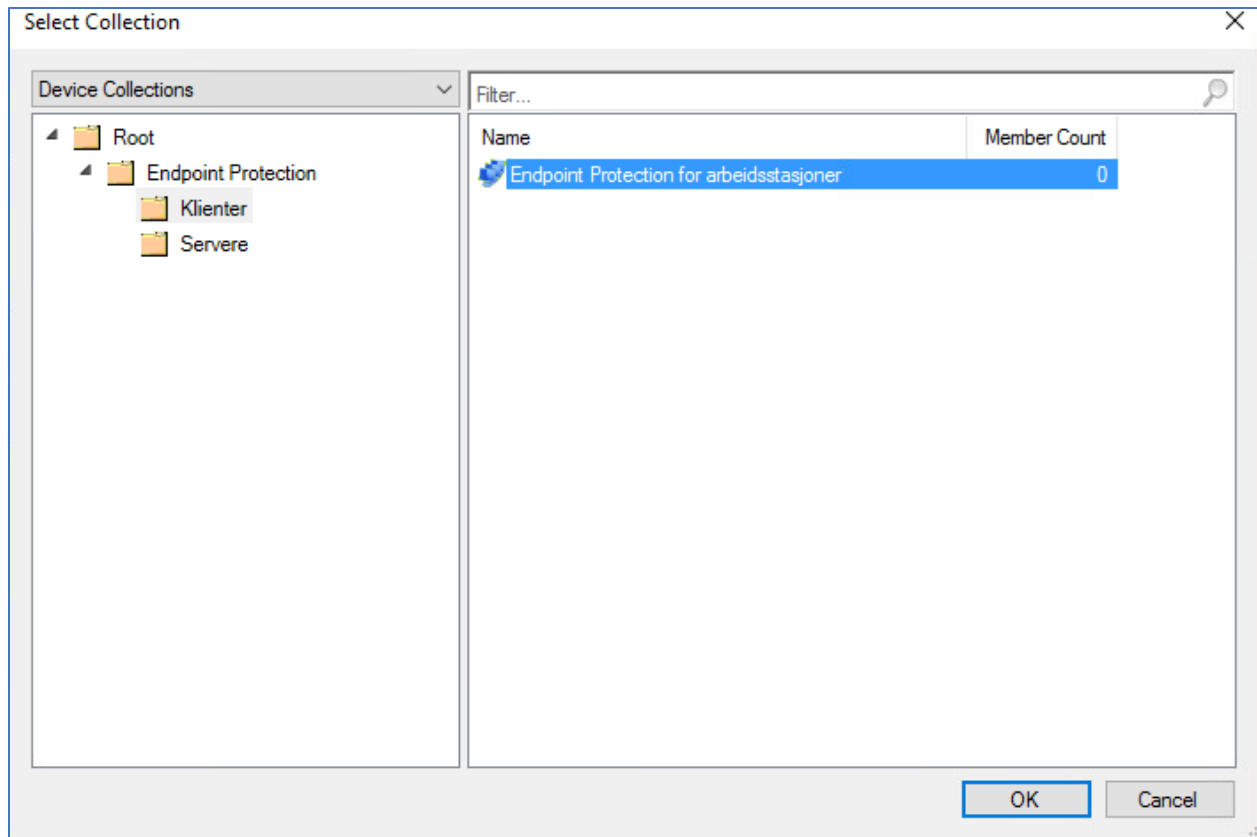
Her velger vi Endpoint Protection for arbeidsstasjoner som navn og under Limiting collection velger vi All Systems.

The screenshot shows the 'Create Device Collection Wizard' dialog box with the 'General' tab selected. The 'Name' field contains 'Endpoint Protection for arbeidsstasjoner'. The 'Limiting collection' dropdown is set to 'All Systems'. There is a 'Browse...' button next to the dropdown. The 'Comment' field is empty.

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:

Icon	Name	Limiting Collection	Member Count	Members Visible on Site	Referenced Collections
	Endpoint Protection for servere - AD	All Systems	0	0	0
	Endpoint Protection for servere - SCCM	All Systems	0	0	0

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.

Specify roles for this server

Available roles:

- Asset Intelligence synchronization point
- Certificate registration point
- Endpoint Protection point
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Reporting services point
- State migration point

Description:

The Endpoint Protection point provides the default settings for all antimalware policies and installs the Endpoint Protection client on the site system server to provide a data source from which the Configuration Manager database resolves malware IDs to names. When you install this site system role, you must accept the license terms for System Center Endpoint Protection.

Activ

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



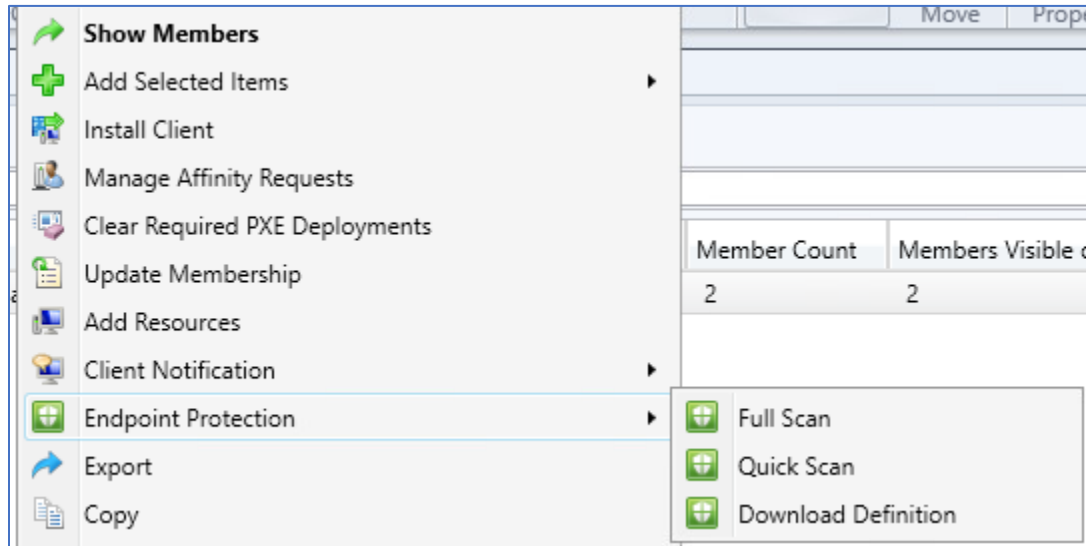
The Add Site System Roles Wizard completed successfully

Details:

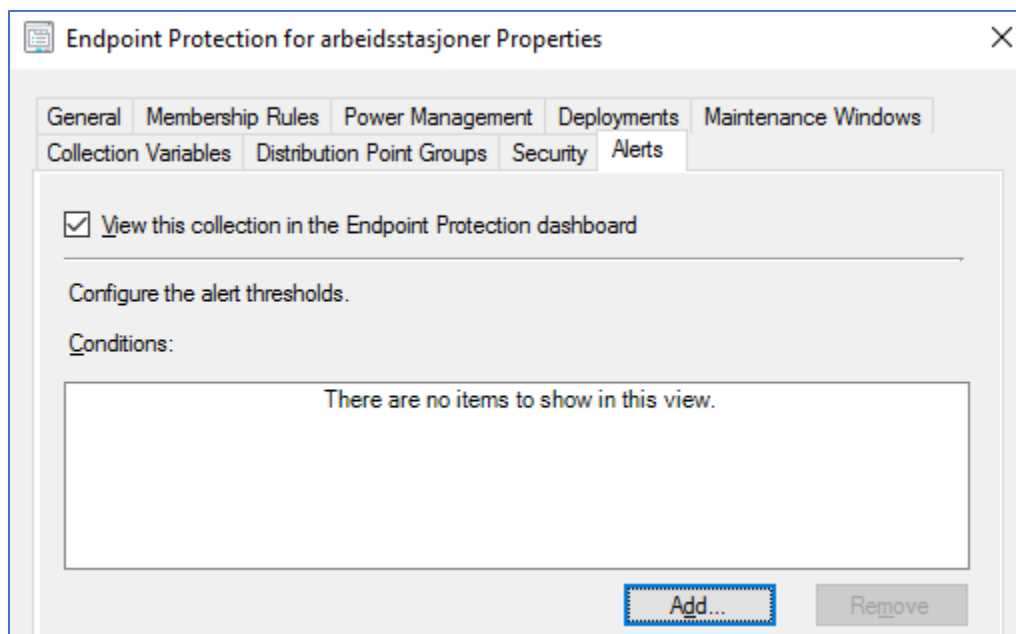
Create a site system server with the following settings:

- ✓ Success: Site System Name
 - finnmw-serv-2.nervika.local
- ✓ Success: Settings
 - Public FQDN: Not specified
 - Installation Account: Computer Account
 - Microsoft Active Protection Service: Basic membership
- ✓ Success: Roles
 - Endpoint Protection point
- ✓ Success: Proxy Settings
 - Proxy will not be enabled

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.

Add New Collection Alerts X

Client status:

- Client check pass or no results for active clients falls below threshold (%)
- Client remediation success falls below the threshold (%)
- Client activity falls below threshold (%)

Endpoint protection:

- Malware is detected
- The same type of malware is detected on a number of computers
- The same type of malware is repeatedly detected within the specified interval on a computer
- Multiple types of malware are detected on the same computer with the specified interval

Membership:

- Member count exceeds threshold

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

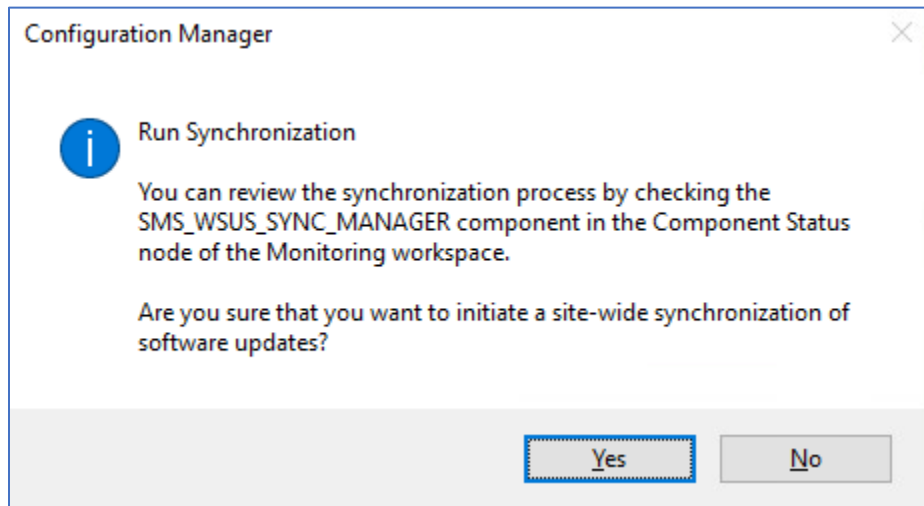
System Center Endpoint Protection Status

Collection:

Collection:

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.

Create Automatic Deployment Rule Wizard

General

Specify the settings for this automatic deployment rule

Name: ADR Endpoint Protection

Description: Dette er en Automatic Deployment Rule for Endpoint Protection

Select a previously saved deployment template that defines configuration settings for this deployment. You can save the current configuration as a new deployment template on the Summary page of this wizard.

Template: Manage Templates...

Specify the target collection for the software update deployment.

Collection: Endpoint Protection for arbeidstasjoner Browse...

Each time the rule runs and finds new updates.

Add to an existing Software Update Group

Create a new Software Update Group

Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.

< Previous Next > Summary Cancel

Under Deployment Settings velger vi Only success and error messages.

Specify the settings for this Automatic Deployment Rule

Use Wake-on-LAN to wake up clients for required deployments

Choose how much state detail you want clients to report back for deployments created by this rule.

Detail level:

Some software updates include a license agreement. Software updates that you choose to deploy automatically will not display any license agreement to you, regardless of whether those software updates include a license agreement. You can review the Microsoft Software License Terms in the All Updates list in the Software Updates node of the console.

- Automatically deploy only software updates found by this rule that do not include a license agreement, or for which the license agreement has already been approved
- Automatically deploy all software updates found by this rule, and approve any license agreements

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

Select the property filters and search criteria

The software updates that meet the specified criteria are added to the associated software update group.

Property filters:

- Custom Severity
- Date Released or Revised
- Description
- Language
- Product
- Required

Search criteria:

Date Released or Revised [Last 1 day](#)
Product ["Forefront Endpoint Protection 2010"](#)

Evaluation schedule lar vi stå som det er

Specify the recurring schedule for this rule

Current software update point synchronization schedule:

Occurs every 7 days effective 01.02.1970 00.00

- Do not run this rule automatically
- Run the rule after any software update point synchronization
- Run the rule on a schedule

Occurs every 7 days effective 10.12.2018 21.12

Customize...

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

Configure schedule details for this deployment

Schedule evaluation

Specify if the schedule for this deployment is evaluated based upon Universal Coordinated Time (UTC) or the local time of the client.

Time based on:

Software available time

Specify when software updates are available. After this rule is run, software updates are distributed to the content server. Then the software updates are available to install as soon as possible or scheduled to install at a configured period of time after the rule is run.

Note: You must enable this deployment before software updates are available to install.

- As soon as possible
- Specific time:

Available time:

Installation deadline

Specify a deadline for required software updates. The deadline is determined by adding the deadline time to the installation time. When the deadline is reached, required software updates are installed on the device and the device is restarted if necessary.

- As soon as possible
- Specific time:

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

Specify the user experience for this deployment

User visual experience

User notifications:

Deadline behavior

When the installation deadline is reached, allow the following activities to be performed outside of any defined maintenance windows:

Software Update Installation

System restart (if necessary)

Device restart behavior

Some software updates require a system restart to complete the installation process. You can suppress this restart on servers and workstations.

Suppress the system restart on the following devices:

Servers

Workstations

Write filter handling for Windows Embedded devices

Commit changes at deadline or during a maintenance window (requires restarts)

Under alerts skal det se slik ut:

Specify software update alert options for this deployment

Configuration Manager alerts

Specify the criteria for generating a Configuration Manager alert.

- Generate an alert when this Rule fails
- Generate an alert when the following conditions are met

Client compliance is below the following percent:

90

Offset from the deadline:

7

Days

Alerts are generated after the installation deadline is reached.

Deadline time:

Operations Manager alerts

System Center Operations Manager might generate alerts when a device installs a software update. To avoid receiving alerts for planned maintenance, you can disable these alerts during the duration of the software update installation process.

- Disable Operations Manager alerts while software updates run
- Create Operations Manager alert when a software update installation fails

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

Specify the software updates download behavior for clients on slow site boundaries.

Select the deployment option to use when a client is within a slow or unreliable network boundary, or when the client uses a fallback source location for content.

Deployment options:

- Do not install software updates
- Download software updates from distribution point and install

When software updates are not available on any preferred distribution points, clients can download and install software updates from a fallback source location for content.

Deployment options:

- Do not install software updates
- Download and install software updates from the fallback content source location

Allow clients to share content with other clients on the same subnet

If software updates are not available on preferred distribution point or remote distribution point, download content from Microsoft Updates.

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.

The screenshot shows the 'Create Automatic Deployment Rule Wizard' window, specifically the 'Deployment Package' step. The window title is 'Create Automatic Deployment Rule Wizard' and the subtitle is 'Deployment Package'. The left sidebar contains a list of steps: General, Deployment Settings, Software Updates, Evaluation Schedule, Deployment Schedule, User Experience, Alerts, Download Settings, **Deployment Package**, Distribution Points, Download Location, Language Selection, Summary, Progress, and Completion. The main area is titled 'Select deployment package for this automatic deployment rule'. It contains the following text: 'The deployment package contains the software update files associated with this rule that will be available to clients as part of the deployment. You can select an existing deployment package or create a new one.' There are two radio buttons: 'Select a deployment package' (unselected) and 'Create a new deployment package' (selected). Below the first radio button is an empty text box and a 'Browse...' button. Below the second radio button is a 'Name:' label with a text box containing 'Endpoint Protection definisjonsoppdateringer', a 'Description:' label with a large empty text area, and a 'Package source (Example): \\<server>\<folder path>' label with a text box containing '\\finnmw-serv-2\Sources\Endpoint Protection' and a 'Browse...' button. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

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

Specify the distribution points or distribution point groups to host the content

Distribution points or distribution point groups:

Name	Description	Associations
FINNMW-SERV-2.NER...	Distribution point	

Filter... 🔍 Add ▼
Remove

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

Specify download location for this Automatic Deployment Rule

If your site server does not have an Internet connection, you can download the software updates from a different computer and save them to a network location accessible by the site server.

- Download software updates from the Internet
- Download software updates from a location on my network:

Example: \\<server>\<folder path>

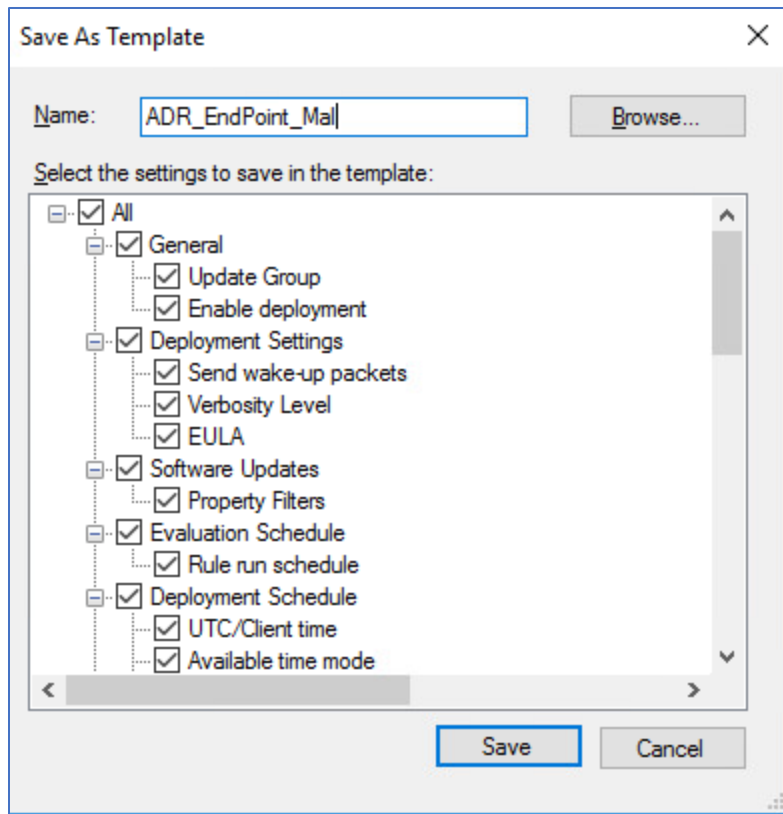
Browse...

Note:

When the deployment package contains all required software updates, select "Download software updates from the Internet". The software updates files will be validated, but will not be downloaded again.

Velger bare engelsk under språk.

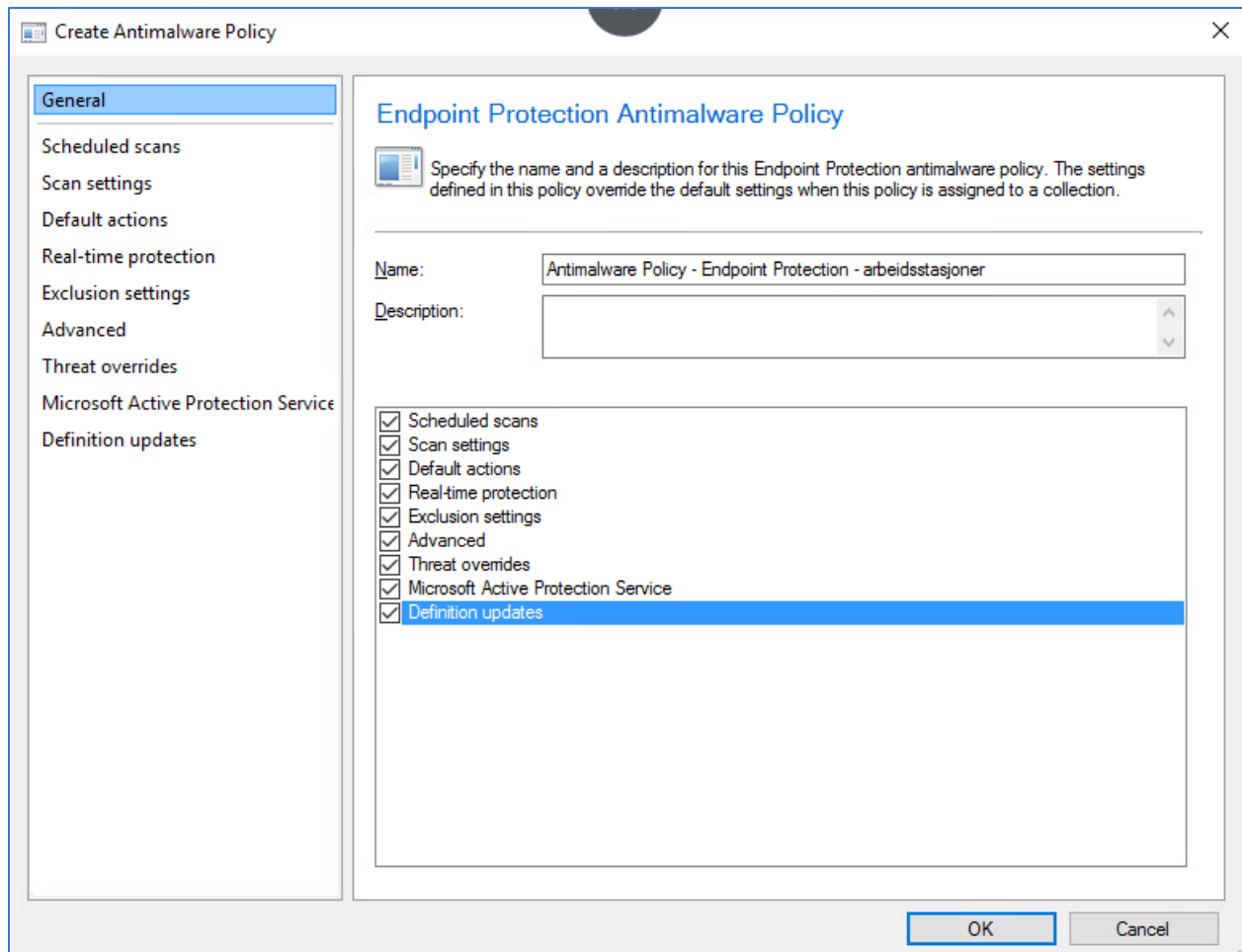
Under Summary velger vi Save as template, så vi kan bruke oppsettet her til å opprette nye ADR.



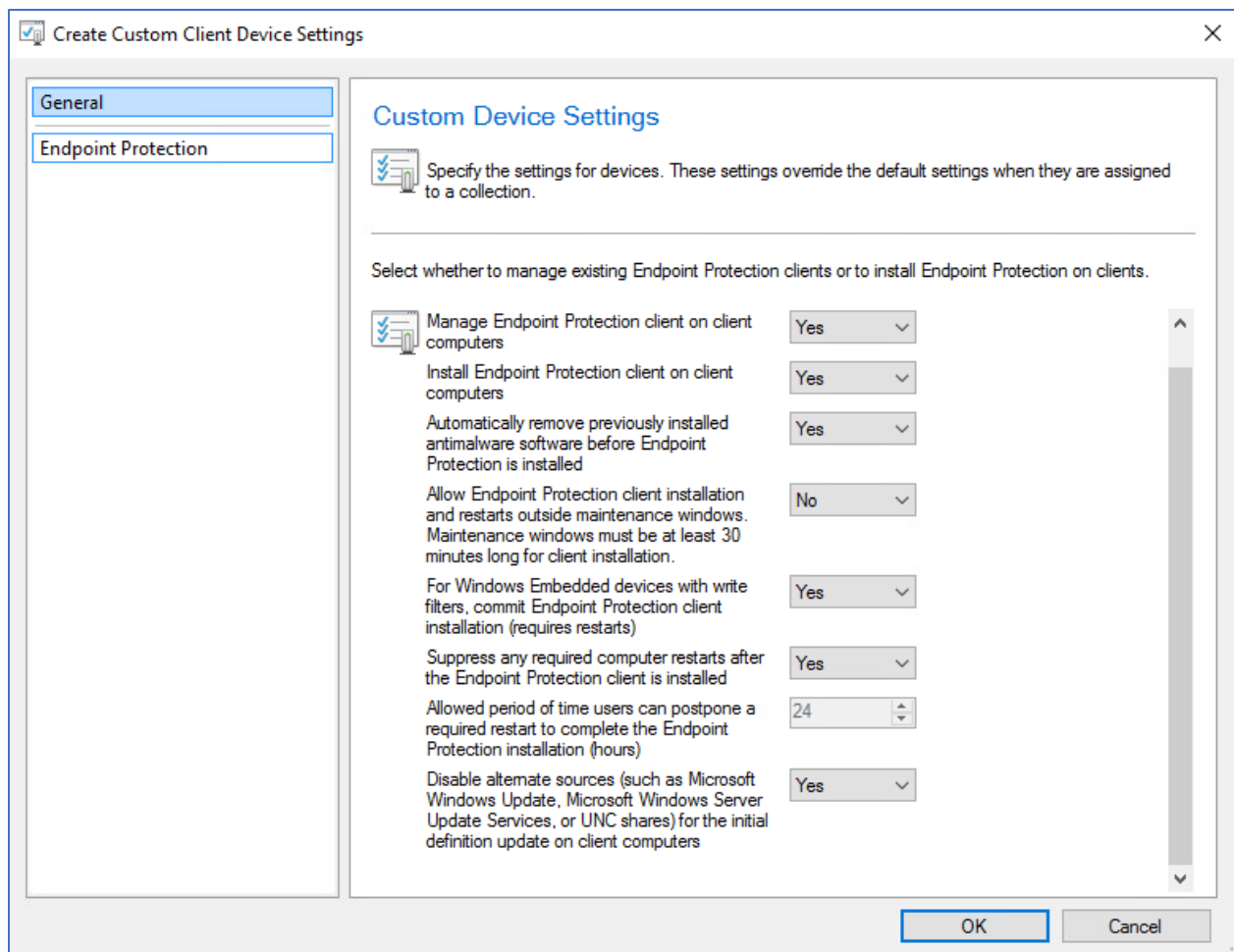
Nå er det bare å fullføre installasjonen.



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

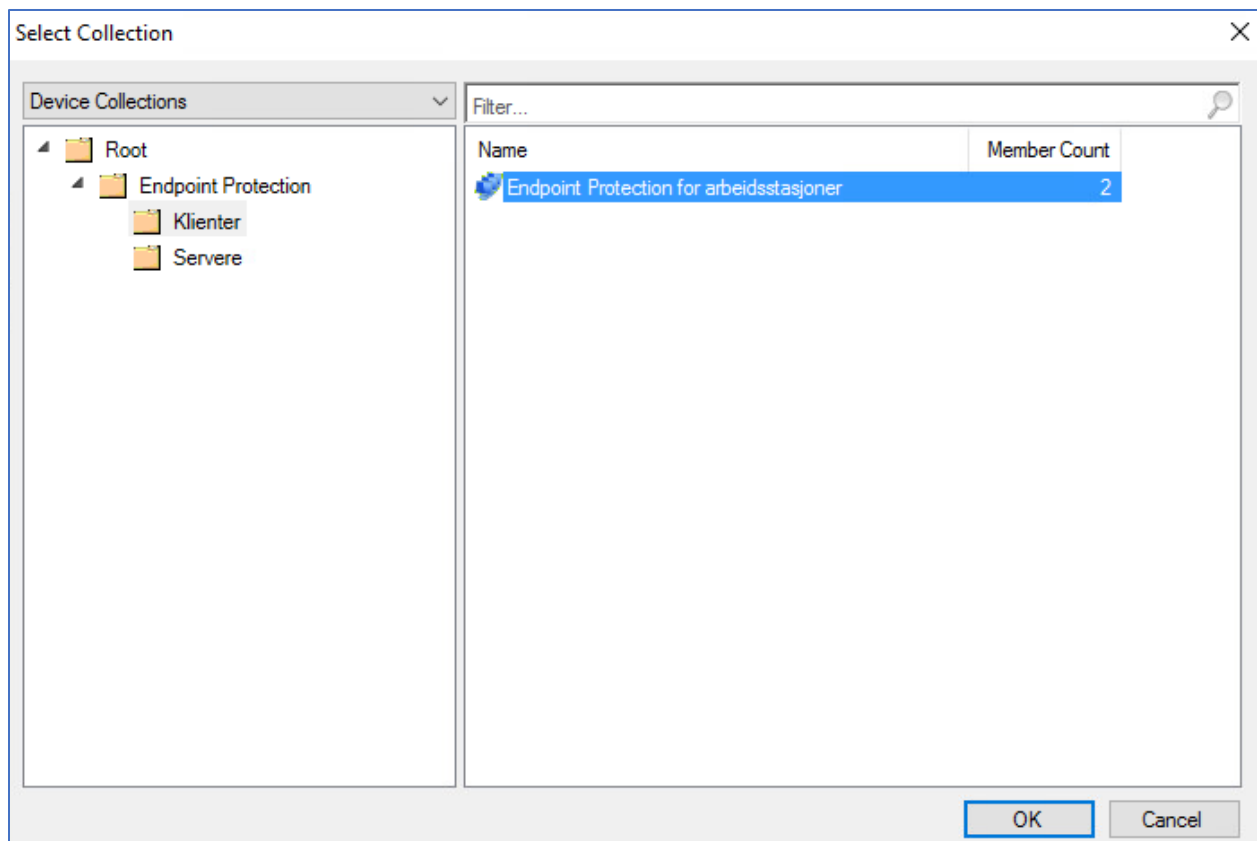


Til slutt må vi lage en Custom Client Device Setting. Administration → Client Settings → Høyreklikk → Create custom Client device setting.



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

Her velger vi Collection for arbeidsstasjonene.



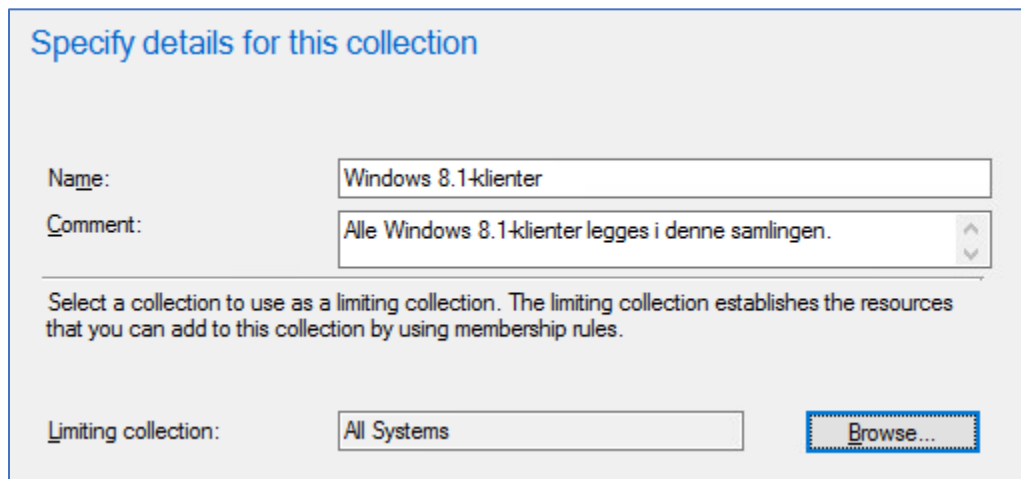
Det samme må vi gjøre med Antimalware Policyen vi nettopp laget. Hvis vi da klikker på en av klientmaskinene under Devices vil vi kunne se at de bruker den Antimalware Policyen vi har satt, samt de klientinnstillingene vi laget.

KLIENT1			
Icon	Name	Collection Name	Priority
	Antimalware Policy - Endpoint...	Endpoint Protection for arbeidsstasjoner	1

KLIENT1			
Icon	Name	Collection Name	Priority
	Default Client Settings		10000
	Klientinnstillinger - Endpoint Protection - Administrerte a...	Endpoint Protection for arbe...	1
Summary	Client Check Detail	Malware Detail	Antimalware Policies
			Client Settings

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.



Specify details for this collection

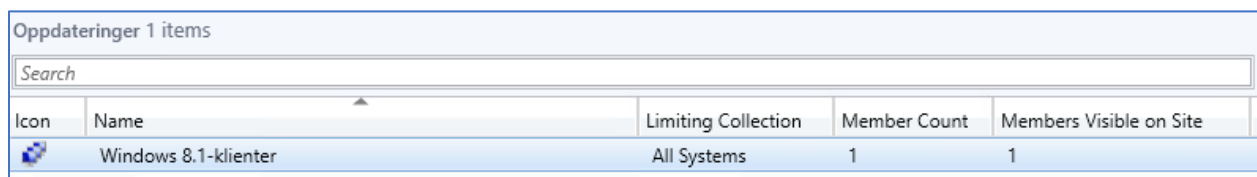
Name:


Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

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.



Oppdateringer 1 items				
Search				
Icon	Name	Limiting Collection	Member Count	Members Visible on Site
	Windows 8.1-klienter	All Systems	1	1

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.

Specify the settings for this automatic deployment rule

Name:

Description:

Select a previously saved deployment template that defines configuration settings for this deployment. You can save the current configuration as a new deployment template on the Summary page of this wizard.

Template:

Specify the target collection for the software update deployment.

Collection:

Each time the rule runs and finds new updates.

Add to an existing Software Update Group

Create a new Software Update Group

Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.

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

Specify the settings for this Automatic Deployment Rule

Use Wake-on-LAN to wake up clients for required deployments

Choose how much state detail you want clients to report back for deployments created by this rule.

Detail level:

Some software updates include a license agreement. Software updates that you choose to deploy automatically will not display any license agreement to you, regardless of whether those software updates include a license agreement. You can review the Microsoft Software License Terms in the All Updates list in the Software Updates node of the console.

Automatically deploy only software updates found by this rule that do not include a license agreement, or for which the license agreement has already been approved

Automatically deploy all software updates found by this rule, and approve any license agreements

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 sende slik ut:

Search criteria:
Product "Windows 8.1"
Superseded No
Update Classification "Security Updates"

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.

Specify the recurring schedule for this rule

Current software update point synchronization schedule:

Occurs every 7 days effective 01.02.1970 00.00

Do not run this rule automatically

Run the rule after any software update point synchronization

Run the rule on a schedule

Occurs every 7 days effective 12.12.2018 00.04 Customize...

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 haker av for If software updates are not available on preffered distribution point or remote distribution point, download contant from Microsoft Updates.

Specify the software updates download behavior for clients on slow site boundaries.

Select the deployment option to use when a client is within a slow or unreliable network boundary, or when the client uses a fallback source location for content.

Deployment options:

- Do not install software updates
- Download software updates from distribution point and install

When software updates are not available on any preferred distribution points, clients can download and install software updates from a fallback source location for content.

Deployment options:

- Do not install software updates
- Download and install software updates from the fallback content source location

Allow clients to share content with other clients on the same subnet

If software updates are not available on preferred distribution point or remote distribution point, download content 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.

Select deployment package for this automatic deployment rule

The deployment package contains the software update files associated with this rule that will be available to clients as part of the deployment. You can select an existing deployment package or create a new one.

Select a deployment package

Browse...

Create a new deployment package

Name:

Windows 8.1 - Sikkerhetsoppdateringer

Description:

Package source (Example): \\<server>\<folder path>

\\finnmw-serv-2\Sources\Sikkerhetsoppdateringer Windows 8.1

Browse...

Under Distribution point velger vi SCCM-serveren.

Distribution points or distribution point groups:

Filter...

Name	Description	Associations
FINNMW-SERV-2.NER...	Distribution point	

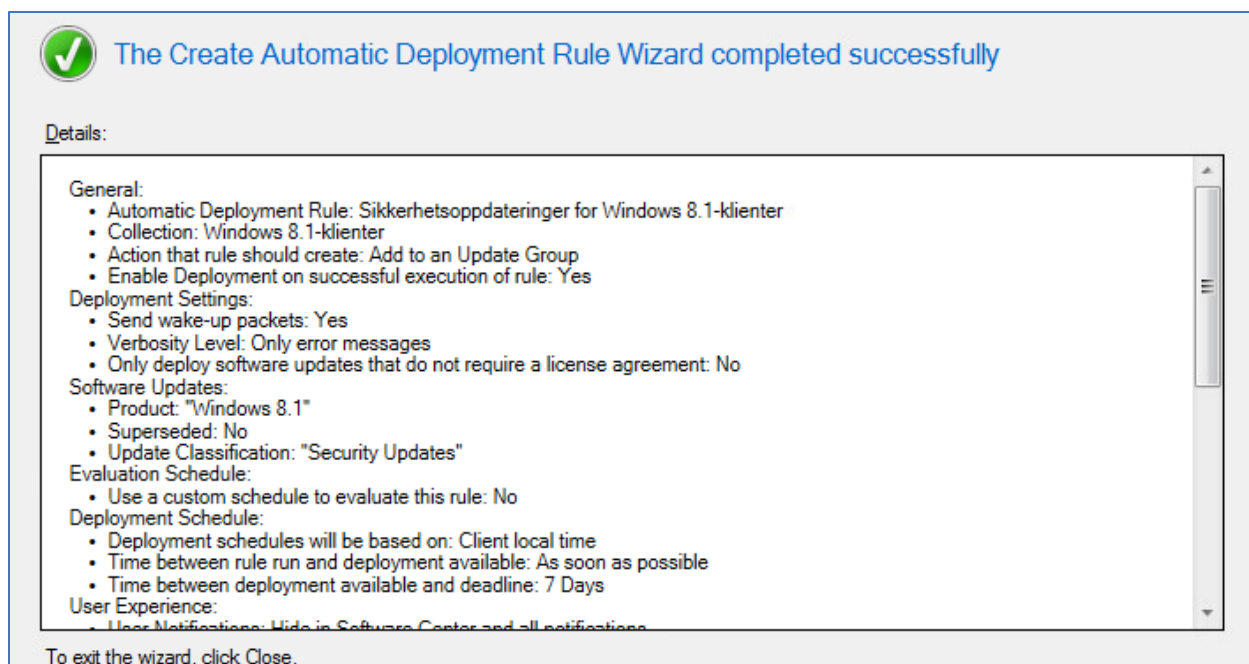
Velger å laste ned oppdateringene fra internett.

Specify download location for this Automatic Deployment Rule

If your site server does not have an Internet connection, you can download the software updates from a different computer and save them to a network location accessible by the site server.

Download software updates from the Internet

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](https://portal.office.com/Signup/Signup.aspx?OfferId=40BE278A-DFD1-470a-9EF7-9F2596EA7FF9&dl=INTUNE_A&ali=1#0%20), 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:


Søk etter brukere, grupper, innstillinger eller oppgaver 








Anbefalt for deg

Du bruker domenet vårt, nervika.onmicrosoft.com. Legg til ditt eget domene for å få en profesjonell tilstedeværelse på Internett, inkludert e-postadresser.

[Vis anbefaling](#)

 **Aktive brukere** >

-  Legg til en bruker
-  Slett en bruker
-  Rediger bruker
-  Tilbakestill passord

 **Fakturering** >

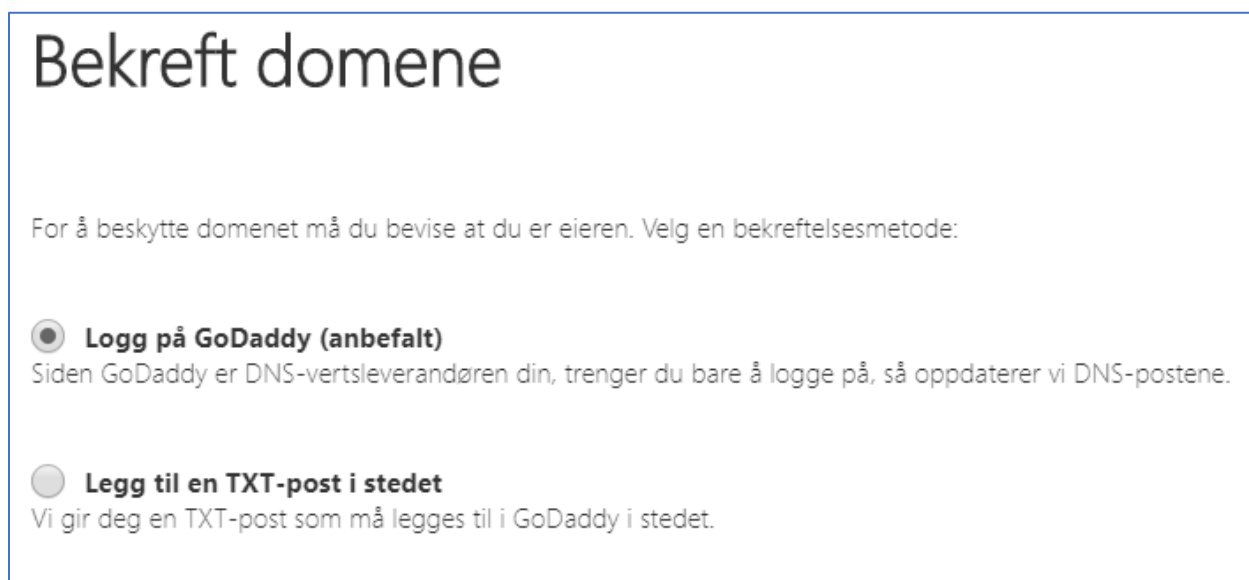
Total saldo: Ingen

Prøveversjon: [Kjøp nå](#)

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.



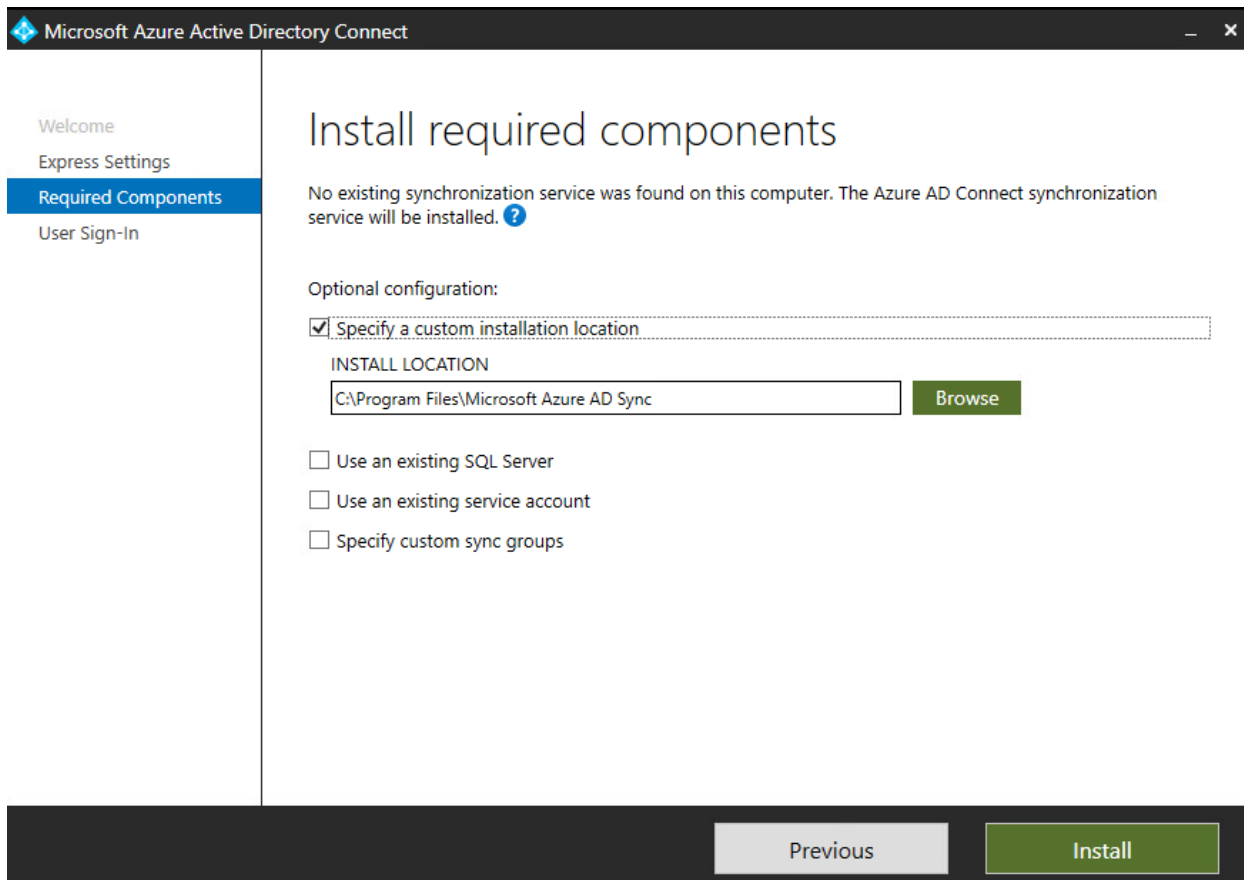
Nå kan vi legge til domene i Office Admin Center. Trykker derfor på anbefalingen og trykker legg til domene. Her skriver vi inn nervika.com. Så må vi bekrefte domenet. Velger her det første alternativet.



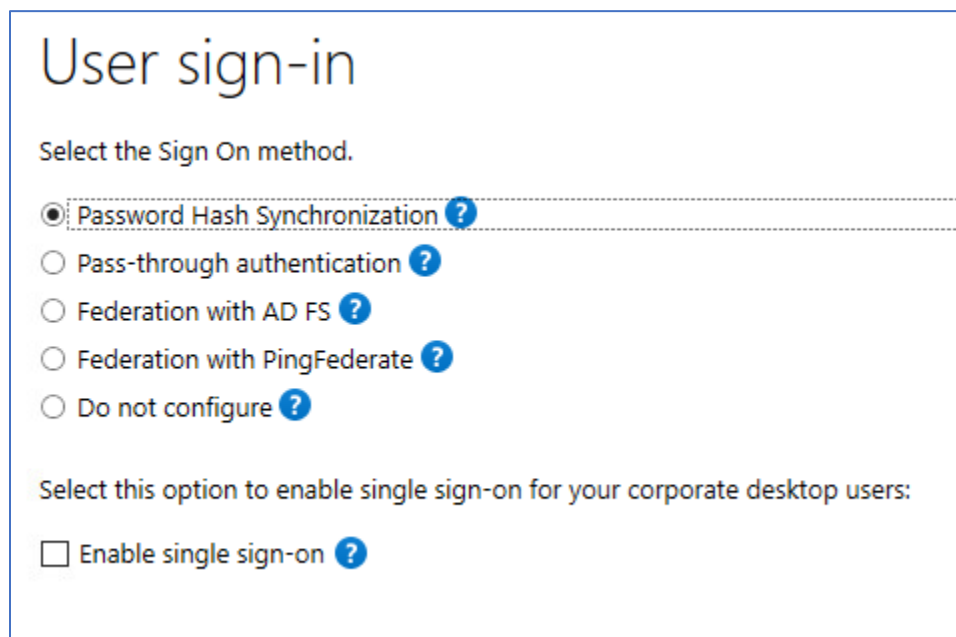
11.2 Synkronisere Active Directory

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

Connect to Azure AD

Enter your Azure AD global administrator credentials. [?](#)

USERNAME

PASSWORD

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

AD forest account

An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. [Learn more](#) about managing account permissions.

The first option is recommended and requires you to enter Enterprise Admin credentials.

Select account option.

Create new AD account


Use existing AD account

DOMAIN USERNAME

PASSWORD

Velger å synke alt fra Active Directoryen.

Domain and OU filtering

Directory: 

Sync all domains and OUs

Sync selected domains and OUs

- nervika.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Infrastructure
 - Keys
 - Klienter
 - LostAndFound
 - Managed Service Accounts
 - NTDS Quotas
 - Program Data
 - System
 - Users

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.

Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. [Learn more](#)

The Active Directory Recycle Bin is not enabled for your forest (nervika.local**) and is strongly recommended. [Learn more](#)**

Azure Active Directory is configured to use AD attribute **mS-DS-ConsistencyGuid as the source anchor attribute. [Learn more](#)**

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

Hjem > Aktive brukere **Nervika AS**

+ Legg til en... Mer Visninger Alle brukere Søk i brukere

<input type="checkbox"/>	Visningsnavn	Brukernavn
<input type="checkbox"/>	Anders Vold	anvo@nervika.onmicrosoft.com
<input type="checkbox"/>	Andreas Solhaug	anso@nervika.onmicrosoft.com
<input type="checkbox"/>	Atle Stadsnes	atst@nervika.onmicrosoft.com
<input type="checkbox"/>	Caroline Fossmo	cafo@nervika.onmicrosoft.com
<input type="checkbox"/>	Christian Nyvold	chny@nervika.onmicrosoft.com
<input type="checkbox"/>	ClientInstall	ClientInstall@nervika.onmicrosoft.com
<input type="checkbox"/>	Erling Bratland	erbr@nervika.onmicrosoft.com
<input type="checkbox"/>	Eystein Nerup	eyne@nervika.onmicrosoft.com
<input type="checkbox"/>	Finn Morten Wiggen	finnmw@nervika.onmicrosoft.com
<input type="checkbox"/>	Geir Andersen	gean@nervika.onmicrosoft.com
<input type="checkbox"/>	Halgeir Oshaug	haos@nervika.onmicrosoft.com
<input type="checkbox"/>	Harald Eriksen	haer@nervika.onmicrosoft.com

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.

Specify details for this collection


Name:

Comment:


Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection:

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


 **The Create User Collection Wizard completed successfully**

Details:

-  Success: General
 - Collection Name: Intunebrukere
 - Comment:

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.

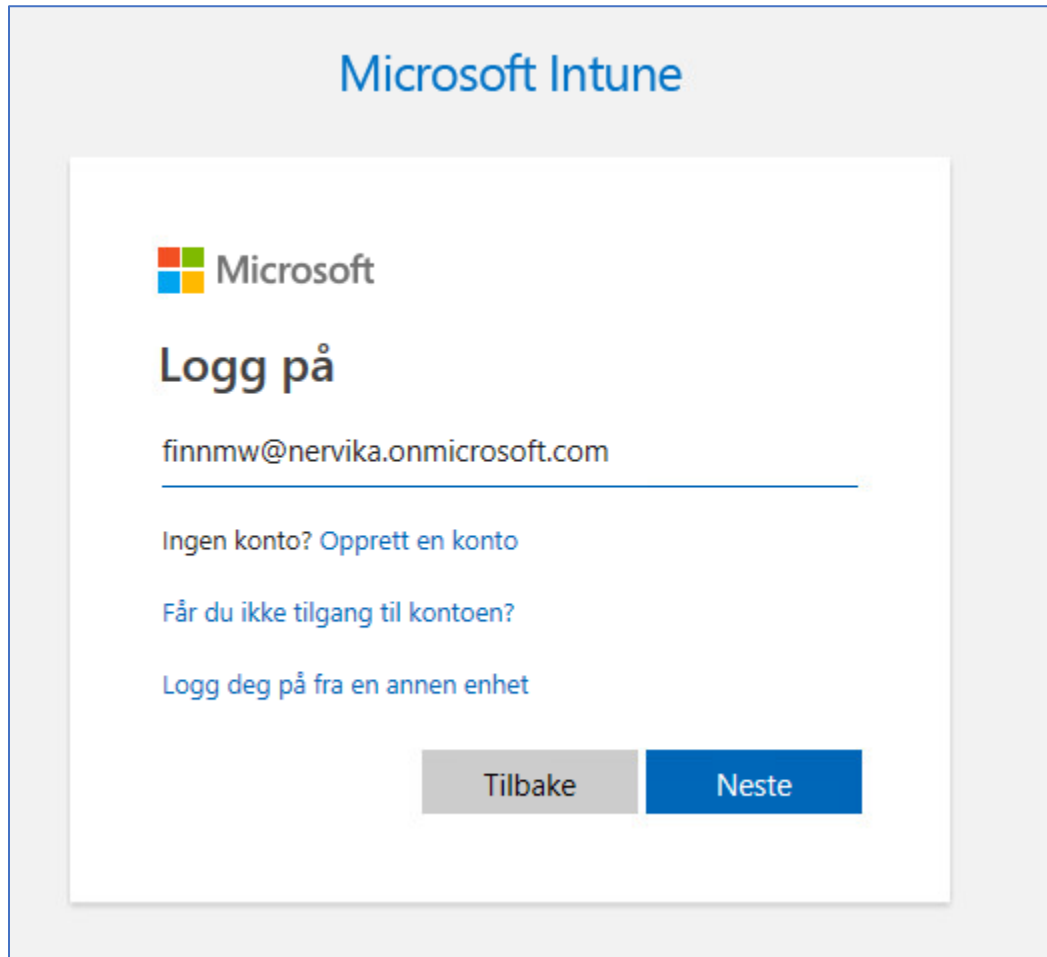
Intunebrukere 1 items

Icon	Name	Domain	Resource Type
	NERVIKA\anvo (Anders Vold)	NERVIKA	User

11.4 Legge til Microsoft Intune Subscription

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

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



Microsoft Intune

Microsoft

Logg på

finnmw@nervika.onmicrosoft.com

Ingen konto? [Opprett en konto](#)

[Får du ikke tilgang til kontoen?](#)

[Logg deg på fra en annen enhet](#)

Tilbake Neste

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

General Configuration

Specify the user collection whose members will be able to enroll their devices for management.

Collection:

Specify company details and the color scheme for the company portal.

These device and portal settings will replace any values previously configured in Microsoft Intune. Leave the fields blank if you do not want to specify custom values.

Company name:

URL to company privacy documentation:

Color scheme for company portal:

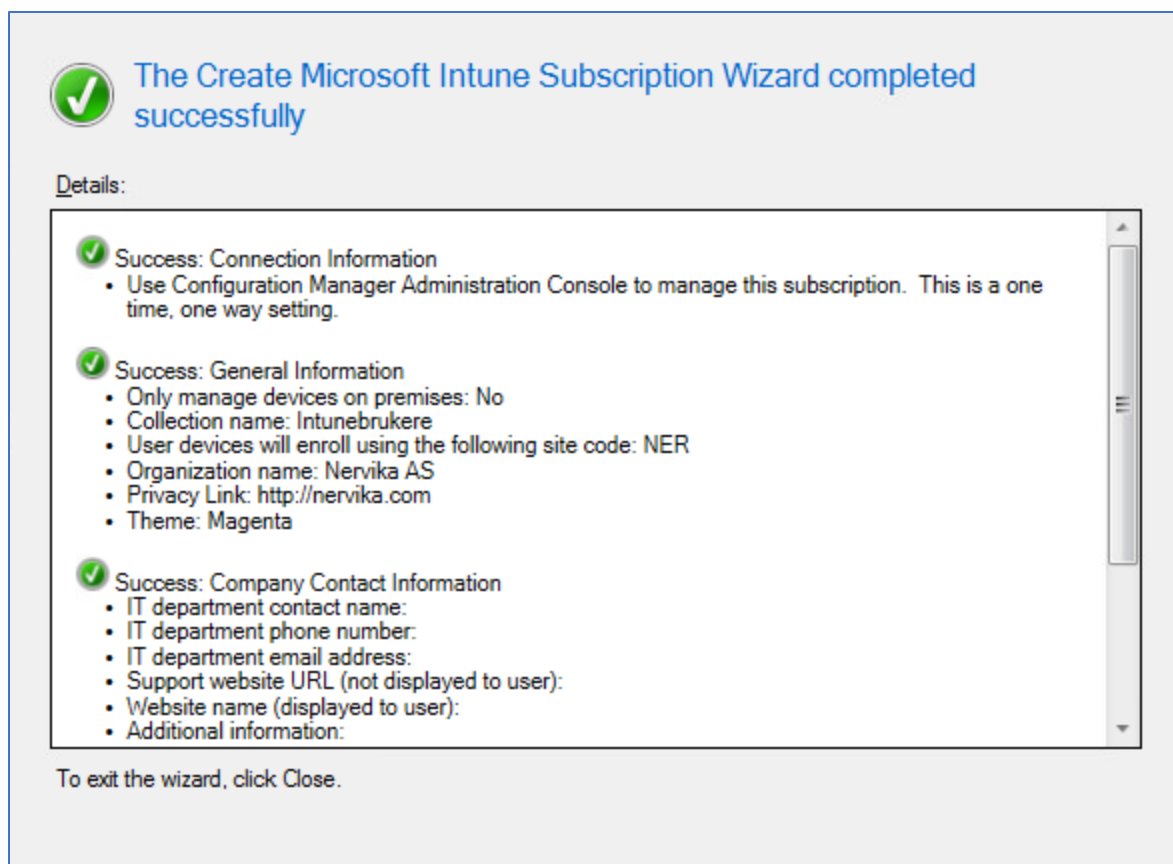
Specify the site code for device assignment.

Configuration Manager site code:

Device Enrollment Limit

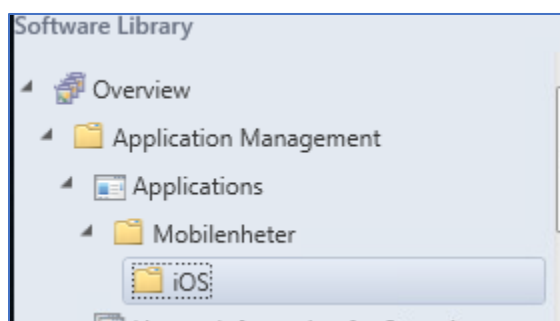
Select the maximum number of devices a user can enroll:

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.

Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

Automatically detect information about this application from installation files:

Type:

Location: 


Example: <http://itunes.apple.com/us/app/AppName/idxxx?mt=xuo=x>

Manually specify the application information

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.

App Store Preview

This app is only available on the App Store for iOS devices.



Dropbox 4+
A modern workspace
Dropbox
#9 in Productivity
★★★★☆ 4.7, 19.8K Ratings
Free · Offers In-App Purchases

Trykker så på OK.

Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

Automatically detect information about this application from installation files:

Type:

Location:

Example: <http://itunes.apple.com/us/app/AppName/idxxx?mt=x>

Manually specify the application information

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

Specify information about this application

Name:

Administrator comments:

Publisher:

Software version:

Optional reference:

Administrative categories:

Per-App VPN:

Nå er det bare å fullføre



The Create Application Wizard completed successfully

Details:



Success: General Information:

- Application name: DropBox
- Administrator comments: Alle ansatte hos Nervika AS må benytte seg av DropBox.ropbox
- Publisher: DropBox Inc
- Software version:
- Optional reference:



Success: Categories:



Success: Deployment type name: dropbox - App Package for iOS from App Store



Success: Requirement rules:

To exit the wizard, click Close.

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.

Specify general information for this deployment

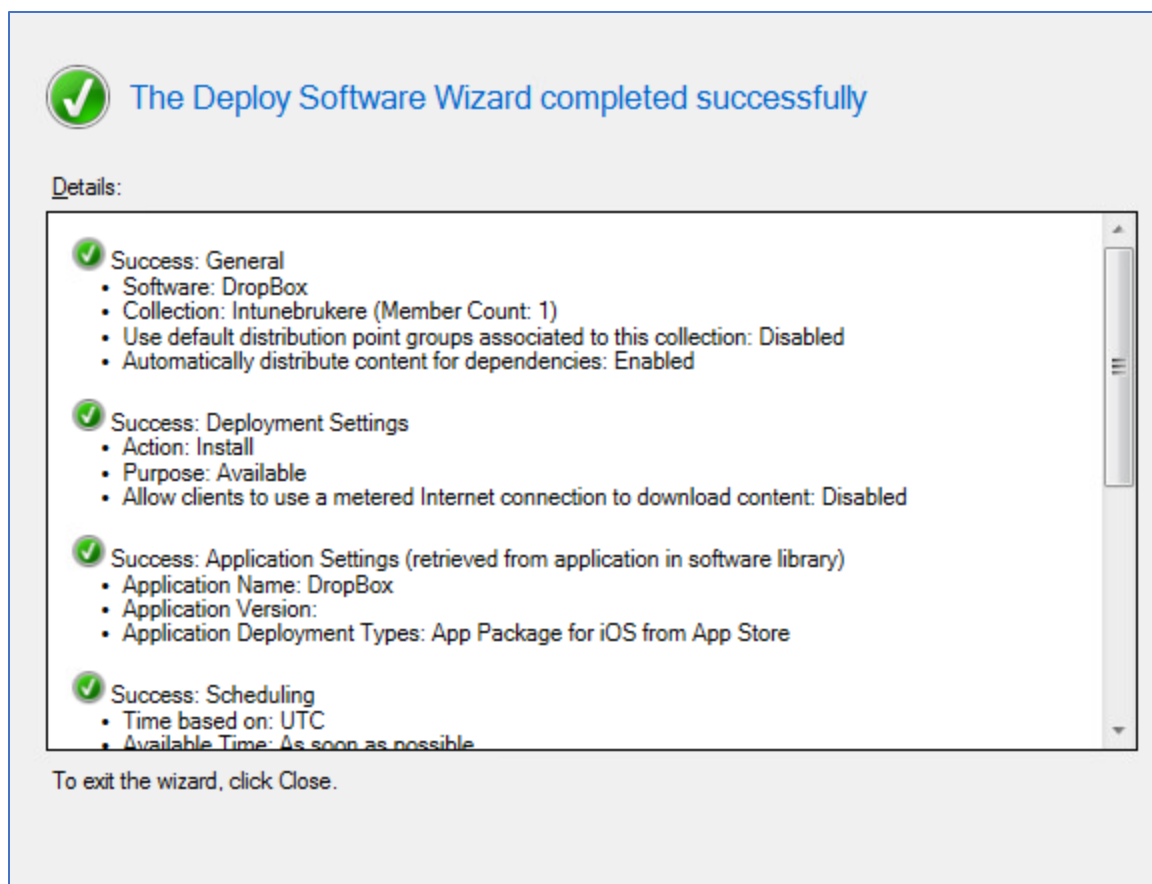
Software:

Collection:

Use default distribution point groups associated to this collection

Automatically distribute content for dependencies

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.

Intunebrukere				
Icon	Software	Feature Type	Deployment Start Time	Purpose
	DropBox	Application	11.12.2018 00.49	Available

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

DropBox						
Icon	Priority	Name	Dependencies	Technology Title	Superseded	Content ID
	1	dropbox - App Package for iOS from App Sto...	No	App Package for i...	No	

Her skal vi høyreklikke 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.

Category: Device

Condition: Operating system Create...

Rule type: Value

Operator: One of

Select all

- iPhone
 - All iOS 7 iPhone or iPod touch devices
 - All iOS 8 iPhone or iPod touch devices
 - All iOS 9 iPhone or iPod touch devices
- iPad

OK Cancel

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.

Produktlisenser

Plassering *

Norge

Intune På

21 av 25 lisenser er tilgjengelige

Microsoft Intune A Direct På

Lagre Avbryt

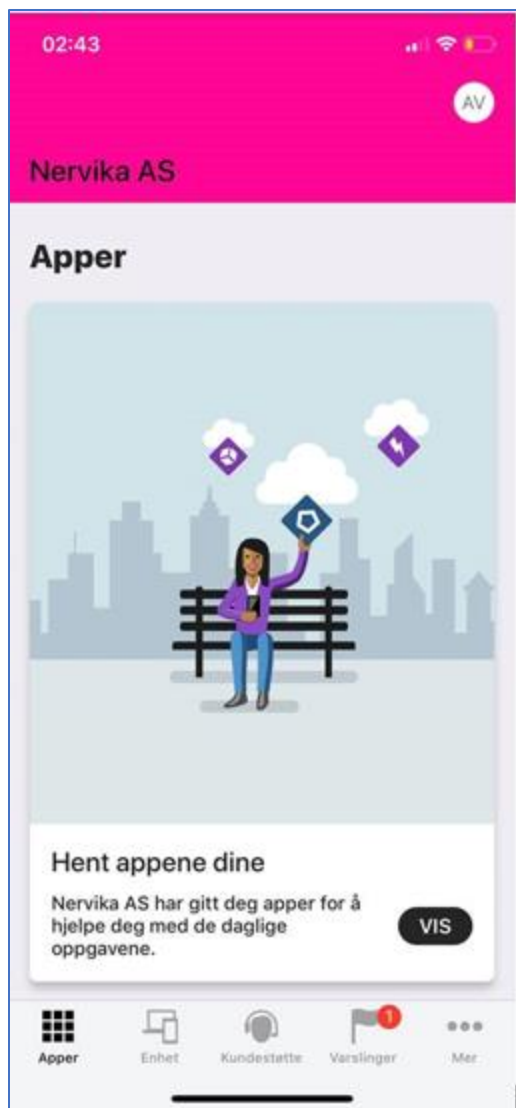
Nå kan vi se at anvo har fått tilgang til Intune, mens en annen bruker, anso, fremdeles ikke har fått det.

<input type="checkbox"/>	Anders Vold	anvo@nervika.onmicrosoft.com	Intune	Synkronisert ...
<input type="checkbox"/>	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.com

Nervika AS



Apper

Filtrer etter:

Alle kat.



Sorter etter:

Navn stigende



DropBox
DropBox Inc

