Installeringsinstruksjoner for Mac-Lab/ CardioLab Anti-Virus (NO)

Mac-Lab/CardioLab-programvareversjon 6.9.6

Innledning

Antivirusprogramvare hjelper institusjoner med å overholde samsvar med retningslinjer for personvern, som HIPAA.

Bruk av dokument

Bruk dette dokumentet for å installere den godkjente antivirusprogramvaren for Mac-Lab/ CardioLab v6.9.6-systemet.

Versjonsoversikt

Revisjon	Dato	Kommentarer
A	16. februar 2016	Første offentlig utgivelse.
B	9. juni 2016	Trend Micro-oppdatering for å støtte CO_2.
C	16. mai 2017	Oppdateringer i McAfee ePolicy Ochestrator, Trend Micro, og Symantec.
D	10. juli 2017	Oppdateringer for Symantec 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9, og McAfee VSE 8.8 Patch 9.
E	14. august 2017	Fjern referansene til McAfee ePolicy Orchestrator 5.9 og McAfee VirusScan Enterprise 8.8 Patch 9. Legg til 6.9.6 R3 UI-språk.
F	25. september 2017	Lagt til McAfee ePO 5.9 og McAfee VSE 8.8 Patch 9. Oppdaterte koblinger for Trend Micro 11 og 12.

Komme i gang

Krav til antivirusprogramvare

ADVARSEL: ANTIVIRUSPROGRAMVARE MÅ INSTALLERES

Systemet leveres uten antivirusbeskyttelse. Forsikre deg om at det er installert et godkjent antivirusprogram på systemet før det kobles til et nettverk. Mangel på godkjent antivirusprogramvare kan føre til at systemet blir ustabilt eller ikke virker.

Vær oppmerksom på følgende krav:

- Antivirusprogramvare leveres ikke sammen med Mac-Lab-/CardioLab-systemet, og det er kundens ansvar å skaffe, installere og vedlikeholde dette.
- Kunden er ansvarlig for å oppdatere definisjonsfilene til antivirusprogrammet.
- Hvis det oppdages et virus, må du kontakte institusjonens systemadministrator og teknisk støtte hos GE.
- Installer bare antivirusprogramvarepakkene som er angitt i delen Godkjent antivirusprogramvare.
- Logg på som Administrator eller medlem av den gruppen for å utføre aktivitetene i dette dokumentet.
- Bruk om mulig en språkversjon av den godkjente antivirusprogramvaren som er lik språket til operativsystemet. Hvis det ikke finnes godkjent antivirusprogramvare som har samme språk som operativsystemet, må den engelske versjonen av antivirusprogramvaren installeres.

Godkjent antivirusprogramvare

ADVARSEL: USTABILT SYSTEM

Ikke installer eller bruk antivirusprogramvare som ikke er godkjent (gjelder også versjoner som ikke er godkjent). Dette kan føre til at systemet blir ustabilt eller slutter å virke. Du må bare bruke godkjent antivirusprogramvare i riktig språkversjon.

MERKNAD: Hvis det spesifikke språket av antivirusprogramvaren ikke er tilgjengelig, installerer du den engelske versjonen av programvaren.

Mac-Lab/CardioLab-systemer av versjon 6.9.6 er godkjent for kjøring med programvaren som er oppført i tabellen nedenfor.

Støttet antivirusprogramvare	Støttede MLCL-språk	Støttet antivirus-programvareversjon
McAfee VirusScan Enterprise	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, nederlandsk, kinesisk, japansk	8.8 Patch 3 8.8 Patch 4 8.8 Patch 8 8.8 Patch 9
McAfee ePolicy Orchestrator (med McAfee VirusScan Enterprise)	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, nederlandsk, kinesisk, japansk	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, nederlandsk, kinesisk, japansk	12.1.2, 12.1.6 MP5, 14.0 MP1
Trend Micro OfficeScan Client/Server Edition	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, nederlandsk, kinesisk, japansk	10.6 SP2, 11.0 SP1, XG 12.0

Den støttede antivirusprogramvaren er tilgjengelig på språkene angitt i tabellen nedenfor.

MLCL-versjon	Støttede MLCL-språk
M6.9.6 R1	Engelsk
M6.9.6 R2	Engelsk, fransk, tysk
M6.9.6 R3	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, nederlandsk, kinesisk, japansk

Konfigurasjon av Anti-virus Management Console Server (konsollserveren for håndtering av antivirus)

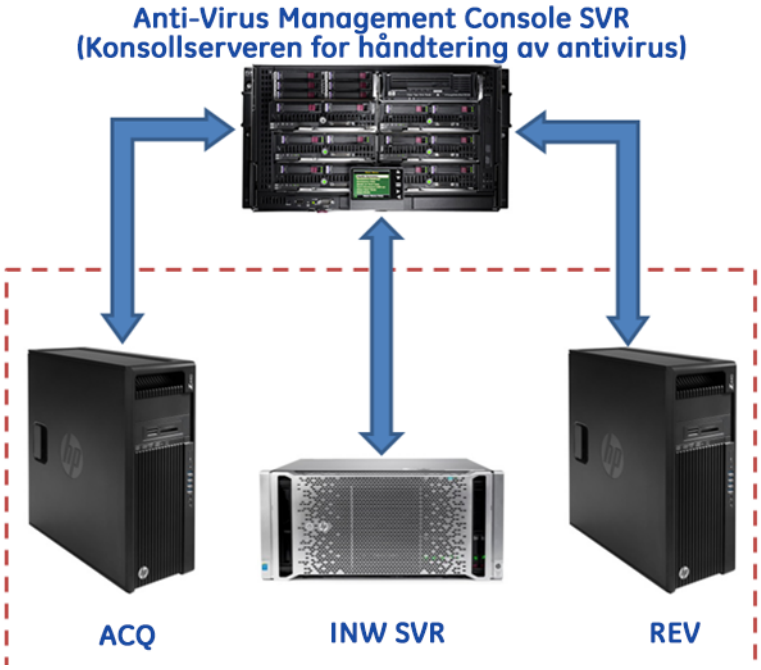
Konsollserveren for håndtering av antivirus må installeres på Anti-virus Management Console Server (konsollserveren for håndtering av antivirus).

Kommunikasjonen mellom Anti-virus Management Console Server (konsollserveren for håndtering av antivirus) og Mac-Lab/CardioLab-enheter oppnås på ulike måter avhengig av miljøet:

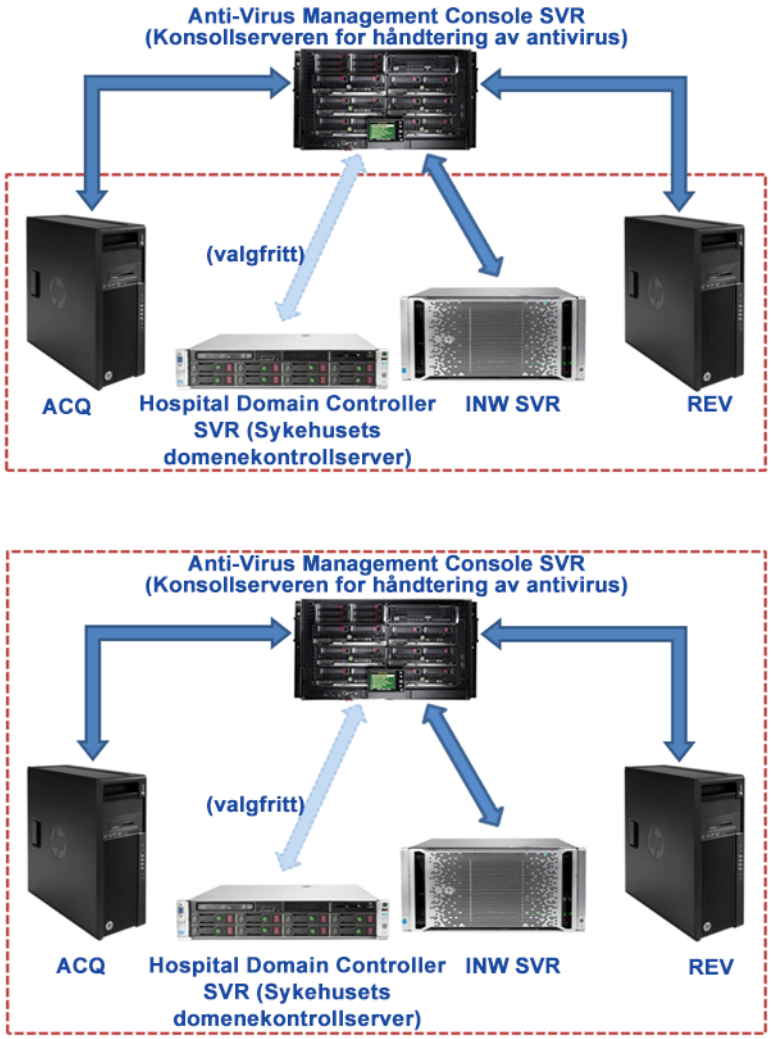
1. Miljø med INW-domenekontroller – Antivirus Management Console SVR er ikke i INW-serverdomenet
   - Kommunikasjon type – 1 <Samme nettverk med samme delnettmaske>
   - Kommunikasjon type – 2 <Forskjellig nettverk med forskjellig delnettmaske>
2. Miljø med syehusdomenekontroller – Anti-virus Management Console SVR er ikke i sykehusdomenekontrollens domene
   - Kommunikasjon type – 1 <Forskjellig nettverk med forskjellig delnettmaske>
3. Miljø med syehusdomenekontroller – Anti-virus Management Console SVR er i sykehusdomenekontrollens domene
   - Kommunikasjon type – 1 <Samme nettverk med samme delnettmaske>

MERKNAD: Anti-virus Management Console-serveren skal ha to nettverksporter. Den ene nettverksporten brukes til å koble til Centricity Cardiology INW-nettverket, og den andre nettverksporten brukes til å koble til sykehusets nettverk.

Blokkdiagram for INW-domenekontrollmiljø

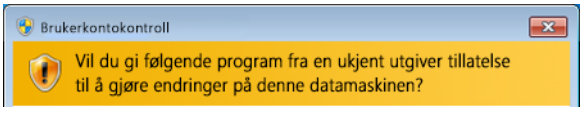


Blokkdiagram for sykehusets domenekontrollmiljø



Brukerkontokontroll

User Account Control (Brukerkontokontroll) er en Windows-funksjon som forhindrer uautoriserte endringer på en datamaskin. Meldingen User Account Control (Brukerkontokontroll) vises under enkelte prosedyrer i denne håndboken.



Når denne meldingen vises etter å ha fulgt prosedyrene i denne håndboken, er det trygt å fortsette.

Instruksjoner om installering av antivirus

Klikk på antivirusprogramvaren du vil installere:

Felles installasjonsprosedyrer for antivirusprogramvare

Bruk prosedyrene i denne delen når de er angitt i instruksjonene for installasjon av antivirusprogramvaren.

Deaktiver tilbakekoblingen

På et innhentingssystem som er koblet til Mac-Lab/CardioLab-miljøet, deaktiverer du tilbakekoblingen for å vise alle klientsystemer med samme delnettmaske på domenet.

1. Logg på som **Administrator** eller et medlem av gruppen.
2. Høyreklikk på ***Network*** (Nettverk) på skrivebordet, og velg ***Properties*** (Egenskaper).
3. Klikk på ***Change adapter settings*** (Endre innstillinger for adapter).
4. Høyreklikk på ***Loopback Connection*** (Tilbakekobling) og velg ***Disable*** (Deaktiver).
5. Start innhentingssystemet på nytt.

MERKNAD: Deaktivering av tilbakekoblingen i innhentingssystemet kreves for å finne alle klientsystemene med samme delnettmaske i domenet.

Aktivere Loopback Connection (Tilbakekobling)

På et innhentingssystem som er koblet til Mac-Lab/CardioLab-miljøet, aktiverer du Loopback Connection (Tilbakekobling) ved hjelp av følgende trinn.

1. Logg på som **Administrator** eller et medlem av gruppen.
2. Høyreklikk på ***Network*** (Nettverk) på skrivebordet, og velg ***Properties*** (Egenskaper).
3. Klikk på ***Change adapter settings*** (Endre innstillinger for adapter).
4. Høyreklikk på ***Loopback Connection*** (Tilbakekobling), og velg ***Enable*** (Aktiver).
5. Start innhentingssystemet på nytt.

Konfigurer datamaskinens nettlesertjeneste før installering av antivirusprogram

Sjekk at innstillingen for datamaskinens nettlesertjeneste er stilt til nettverksbaserte innhentings- og gjennomgangssystemer for å sikre korrekt konfigurering.

1. Klikk på ***Start > Control Panel > Network and Sharing Center*** (Start > Kontrollpanel > Senter for nettverk og deling).
2. Klikk på ***Change advanced sharing settings*** (Endre avanserte innstillinger for deling).
3. Utvid ***Home or Work*** (Hjem eller arbeid).
4. Sørg for at ***Turn on file and printer sharing*** (Slå på fil- og skriverdeling) er valgt.
5. Klikk på ***Save changes*** (Lagre endringer).
6. Klikk på ***Start > Run*** (Start > Kjør).
7. Tast inn **services.msc** og trykk på **Enter**.
8. Dobbeltklikk på tjenesten ***Computer Browser*** (Datamaskinens nettleser).
9. Sørg for at ***Startup type*** (Oppstartstype) er satt til ***Automatic*** (Automatisk). Hvis den ikke er satt til Automatic (Automatisk), endrer du den og klikker på ***Start***.
10. Klikk på ***OK***.
11. Lukk vinduet ***Services*** (Tjenester).

Konfigurer datamaskinens nettlesertjeneste etter installering av antivirusprogram

Når du har installert antivirusprogramvaren, sjekker du at innstillingen for datamaskinens nettlesertjeneste er stilt til nettverksbaserte innhentings- og gjennomgangssystemer for å sikre korrekt konfigurering.

1. Klikk på ***Start > Run*** (Start > Kjør).
2. Tast inn **services.msc** og trykk på **Enter**.
3. Dobbeltklikk på tjenesten ***Computer Browser*** (Datamaskinens nettleser).
4. Sett ***Startup type*** (Oppstartstype) til ***Manual*** (Manuell).
5. Klikk på ***OK***.
6. Lukk vinduet ***Services*** (Tjenester).

Symantec EndPoint Protection (12.1.2, 12.1.6 MP5 eller 14.0 MP1)

Installasjonsoversikt

Installer Symantec EndPoint Protection utelukkende i et nettverksbasert Mac-Lab/CardioLab-miljø. I et nettverksmiljø må Symantec EndPoint Protection installeres på Anti-virus Management Console (konsollserveren for håndtering av antivirus) og deretter distribueres til Centricity

Cardiology INW-serveren og innhentings-/gjennomgangsarbeidsstasjonene som klienter. Bruk følgende instruksjoner for å installere og konfigurere ***Symantec EndPoint Protection***.

Virusoppdateringer er institusjonens ansvar. Oppdater definisjonene regelmessig slik at du er sikker på at de nyeste virusdefinisjonene er på systemet.

Retningslinjer før installasjon

1. Symantec Anti-Virus Management-konsollen skal være installert i henhold til Symantec-instruksjoner og skal fungere ordentlig.
2. Logg på som **Administrator** eller et medlem av gruppen på alle klientsystemer (innhenting, gjennomgang og INW-server) for å installere antivirusprogramvaren.
3. Åpne ledeteksten i modusen ***Run As Administrator*** (Kjør som administrator).
4. Gå til C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

MERKNAD: For å konfigurere INW-serveren går du til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Tast inn **UpdateRegSymantec.ps1**, og trykk på ***Enter***.
6. Bekreft at kjøring av skriptet var vellykket.

   Hvis mappebanen ovenfor ikke er tilgjengelig, utfører du følgende trinn for alle MLCL-systemer, unntatt MLCL 6.9.6R1 INW-serveren (Server OS: Windows Server 2008R2).

   a. Klikk på ***Start***-knappen og deretter på ***Run*** (Kjør).

   b. Tast inn **Regedit.exe**, og klikk på ***OK***.

   c. Gå til ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing.***

   d. Finn og dobbeltklikk på ***State*** (Tilstand)-registeret.

   e. Endre ***Base*** (Base) til ***Decimal*** (Desimal).

   f. Endre ***Value data*** (Verdidata) til ***146432***.

   g. Trykk på ***OK***, og lukk registeret.
7. Deaktiver Loopback Connection (Tilbakekobling) Se Deaktiver tilbakekoblingen på side 6 hvis du vil ha mer informasjon.
8. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste før installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.

Symantec EndPoint Protection – Nye trinn for installering og distribuering (Foretrukket Push-installasjonsmetode)

1. Klikk på ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager***. (Start > Alle programmer > Symantec EndPont Protection Manager > Symantec EndPont Protection Manager.
2. Angi brukernavn og passord for å logge på Symantec Endpoint Protection Manager. (Klikk på ***Yes*** (Ja) hvis en sikkerhetsmelding vises.)

3. Merk av for ***Do not show this Welcome Page igjen*** (Ikke vis denne velkomstsiden på nytt), og klikk på ***Close*** (Lukk) for å lukke velkomstskjermbildet.

MERKNAD: For versjon 14.0 MP1 klikker du på ***Close*** (Lukk) for å lukke skjermbildet ***Getting Started on Symantec EndPoint Protection*** (Komme i gang med Symantec EndPont Protection).

4. Klikk på ***Admin*** i ***Symantec EndPoint Protection Manager***-vinduet.
5. Klikk på ***Install Packages*** (Installer pakker) i den nederste ruten.
6. Klikk på ***Client Install Feature Set*** (Kundeinstallert funksjonssett) i den øverste ruten.
7. Høyreklikk på vinduet ***Client Install Feature Set*** (Kundeinstallert funksjonssett), og velg ***Add*** (Legg til). Vinduet Add Client Install Feature Set (Legg til kundeinstallert funksjonssett) vises.
8. Angi passende navn og registrer det, da du vil trenge det senere.
9. Sørg for at ***Feature set version*** (Funksjonssettversjon) er ***12.1 RU2 and later*** (12.1 RU2 og nyere).
10. Velg bare følgende funksjoner, og fjern merkingen for de andre funksjonene.
    - ***Virus, Spyware, and Basic Download Protection*** (Virus, Spionvare og Enkel nedlastingsbeskyttelse).
    - ***Advanced Download Protection*** (Avansert nedlastingsbeskyttelse).
11. Klikk på ***OK*** i meldingsboksen.
12. Utelukkende for versjonene 12.1.2 og 12.1.6 MP5 klikker du på ***OK*** for å lukke vinduet ***Add Client Install Feature Set*** (Legg til kundeinstallert funksjonssett).
13. Klikk på ***Home*** (Hjem) i vinduet ***Symantec Endpoint Protection Manager***.
14. Gjør et av følgende, avhengig av programvareversjonen:
    - **Versjonene 12.1.2 og 12.1.6 MP5:** Velg ***Install protection client to computers*** (Installer klientbeskyttelse til datamaskiner) fra rullegardinmenyen ***Common Tasks*** (Vanlige oppgaver) øverst til høyre i vinduet ***Home*** (Hjem). Skjermbildet Client Deployment Type (Klientdistribueringstype) vises.
    - **Versjon 14.0 MP1:** Klikk på ***Clients*** (Klienter) i vinduet ***Symantec Endpoint Protection Manager***. Klikk på ***Install a client*** (Installer en klient) under ***Tasks*** (Oppgaver). Skjermbildet ***Client Deployment wizard*** (Veiviser for klientdistribuering) vises.
15. Velg ***New Package Deployment*** (Distribuering av ny pakke), og klikk på ***Next*** (Neste).
16. Velg navnet på funksjonssettet som ble opprettet i trinn 8. Behold de andre innstillingene som standard, og klikk på ***Next*** (Neste).

MERKNAD: For versjon 14.1 MP1, under ***Scheduled Scans*** (Planlagte skanninger), fjerner du merkingen for ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*** (Utsett planlagte skanninger ved bruk av batterienergi, og la brukerdefinerte planlagte skanninger kjøre når skannforfatteren ikke er logget på).

17. Velg ***Remote push*** (Ekstern overføring), og klikk på ***Next*** (Neste). Vent til skjermbildet ***Computer selection*** (Velg datamaskin) vises.
18. Utvid ***<Domain>*** (Domene) (eksempel: INW). Systemer som er koblet til domenet, vises i vinduet ***Computer selection*** (Velg datamaskin).

MERKNAD: Hvis ikke alle systemene gjenkjennes, klikker du på ***Search Network*** (Søk nettverk) og deretter på ***Find Computers*** (Finn datamaskiner). Bruk søkemetoden ***search by IP address*** (søk etter IP-adresse) for å identifisere klientsystemene (Innhenting, Gjennomgang, og INW-server).

19. Velg alle Mac-Lab/CardioLab klientmaskinene som er koblet til domenet, og klikk på **>>**. Skjermbildet ***Login Credentials*** (Påloggingsinformasjon) vises.
20. Angi brukernavn, passord og domene/datamaskinnavn, og klikk på ***OK***.
21. Sørg for at alle valgte maskiner vises under ***Install Protection Client*** (Installer klientbeskyttelse), og klikk på ***Next*** (Neste).
22. Klikk på ***Send***, og vent til Symantec-antivirusprogramvaren distribueres på alle klientsystemene (Innhenting, Gjennomgang, og INW-server). Ved fullføring vises skjermbildet ***Deployment Summary*** (Oppsummering av distribuering).
23. Klikk på ***Next*** (Neste), og klikk deretter på ***Finish*** (Fullfør) for å fullføre Veiviser for klientdistribuering.
24. Vent til Symantec-ikonet vises i systemstatusfeltet, og start deretter alle klientmaskinene (Innhenting, Gjennomgang, og INW-server) på nytt. Logg på med Administrator eller som et medlem av gruppen på alle klientmaskiner etter ny oppstart.

Konfigurasjoner av serverkonsollen for Symantec EndPoint Protection

1. Velg ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager*** (Start > Alle programmer > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager. Påloggingsvinduet for Symantec EndPoint Protection Manager åpnes.
2. Angi passordet for Symantec Endpoint Protection Manager Console, og klikk på ***Log On*** (Logg på).
3. Velg kategorien ***Policies*** (Policyer) og klikk på ***Virus and Spyware Protection*** (Virus- og spionvarebeskyttelse) under ***Policies*** (Policyer). Vinduet ***Virus and Spyware Protection Policies*** (Policy for virus og spionvarebeskyttelse) åpnes.
4. Klikk på ***Add a Virus and Spyware Protection policy*** (Legg til en policy for virus- og spionvarebeskyttelse) under ***Tasks*** (Oppgaver). Vinduet ***Virus and Spyware Protection*** (Policy for virus og spionvarebeskyttelse) åpnes.
5. Under ***Windows Settings > Scheduled Scans***, (Windowsinnstillinger > Planlagte skanninger) klikker du på ***Administrator-Defined Scans*** (Administratordefinerte skanninger).
6. Velg ***Daily Scheduled Scan*** (Daglig skanning), og klikk på ***Edit*** (Rediger). Vinduet ***Edit Scheduled Scan*** (Rediger planlagt skanning) åpnes.
7. Endre skannenavn og beskrivelse til henholdsvis ***Weekly Scheduled Scan*** (Ukentlig skanning) og ***Weekly Scan at 00:00*** (Ukentlig skanning kl. 00.00).
8. Velg ***Scan type*** (Skannetype) som ***Full Scan*** (Full skanning).
9. Velg kategorien ***Schedule*** (Plan).

10. Under ***Scanning Schedule*** (Skanneplan) velger du ***Weekly*** (Ukentlig) og endrer klokkeslettet til ***00:00***.

11. Under ***Scan Duration*** (Skannevarighet) fjerner du merkingen for ***Randomize scan start time within this period (recommended in VMs)*** (Randomiser skannetid innenfor denne perioden (anbefalt i VMs) og velg ***Scan until finished (recommended to optimize scan performance)*** (Skann til fullført (anbefalt for å optimalisere skanneytelse).

12. Under ***Missed scheduled Scans*** (Mislykket planlagt skanning) fjerner du merkingen for ***Retry the scan within*** (Kjør skann på nytt innen).

13. Velg kategorien ***Notifications*** (Varslinger).

14. Fjern merkingen for ***Display a notification message on the infected computer*** (Vis en varselmelding på den infiserte datamaskinen), og klikk på ***OK***.

15. Velg kategorien ***Advanced*** (Avansert) i vinduet ***Administrator-Defined Scans*** (Administratordefinerte skanninger).

16. Under ***Scheduled Scans*** (Planlagte skanninger) fjerner du merkingen for ***Delay scheduled scans when running on batteries*** (Utsett planlagte skanninger ved bruk av batterienergi), ***Allow user-defined scheduled scans to run when scan author is not logged on*** (La brukerdefinerte planlagte skanninger kjøre når skannforfatteren ikke er logget på) og ***Display notifications about detections when the user logs on*** (Vis varsel om funn når brukeren logger på).

MERKNAD: For versjon 14.0 MP1, under ***Scheduled Scans*** (Planlagte skanninger), fjerner du merkingen for ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*** (Utsett planlagte skanninger ved bruk av batterienergi, og la brukerdefinerte planlagte skanninger kjøre når skannforfatteren ikke er logget på).

17. Under ***Startup og Triggered Scans*** (Oppstart og utløste skanninger) fjerner du merkingen for ***Run an Active Scan when new definitions arrive*** (Kjør en aktiv skanning når nye definisjoner er tilgjengelige).

18. Under ***Windows Settings > Protection Technology*** (Windowsinnstillinger > Beskyttelsesteknologi) klikker du på ***Auto-Protect*** (Automatisk beskyttelse).

19. Velg kategorien ***Scan Details*** (Skannedetaljer), og velg og lås ***Enable Auto-Protect*** (Aktiver automatisk beskyttelse).

20. Velg kategorien ***Notifications*** (Varslinger), og fjern merkingen for og lås ***Display a notification message on the infected computer*** (Vis en varselmelding på den infiserte datamaskinen) og ***Display the Auto-Protect results dialog on the infected Computer*** (Vis dialogen med resultater for automatisk beskyttelse på den infiserte datamaskinen).

21. Velg kategorien ***Advanced*** (Avansert). Under ***Auto-Protect Reloading and Enablement*** (Ny innlasting og aktivering av automatisk beskyttelse) låser du alternativet ***When Auto-Protect is disabled, Enable after:*** (Når automatisk beskyttelse er deaktivert, aktiver etter:).

22. Under ***Additional Options*** (Ytterligere alternativer) klikker du på ***File Cache*** (Filbufring). Vinduet ***File Cache*** (Filbufring) åpnes.

23. Fjern merkingen for ***Rescan cache when new definitions load*** (Skann bufring på nytt ved nye definisjoner), og klikk på ***OK***.

24. Under ***Windows Settings > Protection Technology*** (Windowsinnstillinger > Beskyttelsesteknologi) klikker du på ***Download Protection*** (Last ned beskyttelse).

25. Velg kategorien ***Notifications*** (Varslinger), og fjern merkingen for og lås ***Display a notification message on the infected computer*** (Vis en varselmelding på den infiserte datamaskinen).

26. Under ***Windows Settings > Protection Technology*** (Windowsinnstillinger > Beskyttelsesteknologi) klikker du på ***SONAR***.

27. Velg kategorien ***SONAR Settings*** (SONAR-innstillinger), og fjern merkingen for og lås ***Enable SONAR*** (Aktiver SONAR).

28. Under ***Windows Settings > Protection Technology*** (Windowsinnstillinger > Beskyttelsesteknologi) klikker du på ***Early Launch Anti-Malware Driver*** (Tidlig kjøring av driver for programmer mot skadelig programvare).

29. Fjern merkingen for og lås ***Enable Symantec early lauch anti-malware*** (Aktiver tidlig kjøring av programmer mot skadelig programvare).

30. Under ***Windows Settings > Email Scans*** (Windowsinnstillinger > E-postskanning) klikker du på ***Internet Email Auto-Protect*** (Automatisk beskyttelse for Internett og e-post).

31. Velg kategorien ***Scan Details*** (Skannedetaljer), og fjern merkingen for og lås ***Enable Internet Email Auto-Protect*** (Aktiver automatisk beskyttelse for Internett og e-post).

32. Velg kategorien ***Notifications*** (Varslinger), og fjern merkingen for og lås ***Display a notification message on the infected computer*** (Vis en varselmelding på den infiserte datamaskinen), ***Display a progress indicator when email is being sent*** (Vis en fremdriftsindikator når det sendes e-post) og ***Display a notification area icon*** (Vis et ikon i varslingsområdet).

33. Under ***Windows Settings > Email Scans*** (Windowsinnstillinger > E-postskanning) klikker du på ***Microsoft Outlook Auto-Protect*** (Microsoft Oulook automatisk beskyttelse).

34. Velg kategorien ***Scan Details*** (Skannedetaljer), og fjern merkingen for og lås ***Enable Microsoft Outlook Auto-Protect*** (Aktiver Microsoft Outlook automatisk beskyttelse).

35. Velg kategorien ***Notifications*** (Varslinger), og fjern merkingen for og lås ***Display a notification message on the infected computer*** (Vis en varselmelding på den infiserte datamaskinen).

36. Under ***Windows Settings > Email Scans***, (Windowsinnstillinger > E-postskanning) klikker du på ***Lotus Notes Auto-Protect*** (Lotus Notes automatisk beskyttelse).

37. Velg kategorien ***Scan Details*** (Skannedetaljer), og fjern merkingen for og lås ***Enable Lotus Notes Auto-Protect*** (Aktiver Lotus Notes automatisk beskyttelse).

38. Velg kategorien ***Notifications*** (Varslinger), og fjern merkingen for og lås ***Display a notification message on infected computer*** (Vis en varselmelding på den infiserte datamaskinen).

39. Under ***Windows Settings > Advanced Options*** (Windowsinnstillinger > Avanserte alternativer) klikker du på ***Global Scan Options*** (Globale skannealternativer).

40. Under ***Bloodhound(™) Detection Settings*** (Bloodhound(™) registreringsinnstillinger) fjerner du merkingen for og låser ***Enable Bloodhound(™) heuristic virus detection*** (Aktiver Bloodhound(™) registrering av heuristisk virus).

41. Under ***Windows Settings > Advanced Options*** (Windowsinnstillinger > Avanserte alternativer) klikker du på ***Quarantine*** (Karantene).

42. Velg kategorien ***General*** (Generelt), under ***When New Virus Definitions Arrive*** (Når nye virusdefinisjoner ankommer), velg ***Do nothing*** (Gjør ingenting).
43. Under ***Windows Settings > Advanced Options*** (Windowsinnstillinger > Avanserte alternativer) klikker du på ***Miscellaneous*** (Diverse).
44. Velg kategorien ***Notifications*** (Varslinger), og fjern merkingen for ***Display a notification message on the client computer when definitions are outdated*** (Vis en melding på klientdatamaskinen når definisjoner har utløpt), ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions*** (Vis en melding på klientdatamaskinen når Symantec Endpoint Protection kjører uten virusdefinisjoner) og ***Display error messages med a URL to a solution*** (Vis feilmeldinger med en URL til en løsning).
45. Klikk på ***OK*** for å lukke vinduet ***Virus og Spyware Protection*** policy (Policy for virus og spionvarebeskyttelse).
46. Klikk på ***Yes*** (Ja) i meldingsboksen ***Assign Policies*** (Tilordne policyer).
47. Velg ***My Company*** (Min bedrift), og klikk på ***Assign*** (Tilordne).
48. Klikk på ***Yes*** (Ja) i meldingsboksen.
49. Under ***Policies*** (Policyer) klikker du på ***Firewall*** (Brannmur).
50. Klikk på ***Firewall policy*** (Brannmurpolicy) under ***Firewall Policies*** (Brannmurpolicyer), og klikk på ***Edit the policy*** (Rediger policyen) under ***Tasks*** (Oppgaver).
51. Velg kategorien ***Policy Name*** (Policynavn), og fjern merkingen for ***Enable this policy*** (Aktiver denne policyen).
52. Klikk på ***OK***.
53. Under ***Policies*** (Policyer) klikker du på ***Intrusion Prevention*** (Forhindre angrep).
54. Klikk på policyen ***Intrusion Prevention*** (Forhindre angrep) under ***Intrusion Prevention Policies*** (Policyer for å forhindre angrep), og klikk på ***Edit the policy*** (Rediger policyen) under ***Tasks*** (Oppgaver).
55. Velg kategorien ***Policy Name*** (Policynavn), og fjern merkingen for ***Enable this policy*** (Aktiver denne policyen).
56. Gjør et av følgende, avhengig av programvareversjonen:
    - **Versjon 12.1.2:** Klikk på ***Settings*** (Innstillinger) i venstre rute.
    - **Versjonene 12.1.6 MP5 og 14.0 MP1:** Klikk på ***Intrusion Prevention*** (Forhindre angrep) i venstre rute.
57. Fjern merkingen for og lås ***Enable Network Intrusion Prevention*** (Aktiver Forhindre angrep på nettverk) og ***Enable Browser Intrusion Prevention for Windows*** (Aktiver Forhindre angrep på nettleser for Windows).
58. Klikk på ***OK***.
59. Under ***Policies*** (Policyer) klikker du på ***Application og Device Control*** (Program- og enhetskontroll).
60. Klikk på ***Application og Device Control Policy*** (Program- og enhetskontroll) under ***Application og Device Control Policies*** (Policyer for program- og enhetskontroll), og klikk på ***Edit the policy*** (Rediger policyen) under ***Tasks*** (Oppgaver).

61. Velg kategorien ***Policy Name*** (Policynavn), og fjern merkingen for ***Enable this policy*** (Aktiver denne policyen).
62. Klikk på ***OK***.
63. Under ***Policies*** (Policyer) klikker du på ***LiveUpdate***.
64. Velg ***LiveUpdate Settings policy*** (Policy for LiveUpdate-innstillinger). Under ***Tasks*** (Oppgaver) klikker du på ***Edit the policy*** (Rediger policyen).
65. Under ***Overview > Windows Settings*** (Oversikt > Windowsinnstillinger) klikker du på ***Server Settings*** (Serverinnstillinger).
66. Under ***Internal eller External LiveUpdate Server*** (Intern eller ekstern LiveUpdate-server) må du sørge for at ***Use the default management server*** (Bruk standard managementserver) er valgt, og fjern merkingen for ***Use a LiveUpdate server*** (Bruk en LiveUpdate-server).
67. Klikk på ***OK***.
68. Under ***Policies*** (Policyer) klikker du på ***Exceptions*** (Unntak).
69. Klikk på ***Exceptions policy*** (Policy for unntak). Under ***Tasks*** (Oppgaver) klikker du på ***Edit the policy*** (Rediger policyen).
70. Gjør et av følgende, avhengig av programvareversjonen:
    - **Versjonene 12.1.2 og 12.1.6 MP5:** Klikk på ***Exceptions > Add > Windows Exceptions > Folder*** (Unntak > Legg til > Windows-unntak > Mappe).
    - **Versjon 14.0 MP1:** Klikk på rullegardinmenyen ***Add*** (Legg til), og velg ***Windows Exceptions > Folder*** (Windows-unntak > Mappe).
71. Angi **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:**, **G:** mappebanene én av gangen, og gjør følgende:
    a. Sørg for at ***Include subfolders*** (Inkluder undermapper) er valgt.

MERKNAD: Klikk på ***Yes*** (Ja) hvis meldingsboksen ***Are you sure you want to exclude all subfolders fra protection?*** (Er du sikker på at du vil ekskludere alle undermappene fra beskyttelsen?) vises.

    b. Velg ***All*** (Alle) fra ***Specify the type of scan that excludes this folder*** (Spesifiser skannetypen som ekskluderer denne mappen).
    c. For versjon 14.0 MP1 klikker du på ***OK*** for å legge til unntaket.
72. Klikk på ***OK***.
73. Klikk på ***Assign the policy*** (Tilordne policyen) under ***Tasks*** (Oppgaver).
74. Velg ***My Company*** (Min bedrift), og klikk på ***Assign*** (Tilordne).
75. Klikk på ***Yes*** (Ja).
76. Klikk på ***Clients*** (Klienter) i den venstre ruten, og velg kategorien ***Policies*** (Policyer).
77. Under ***My Company*** (Min bedrift) velger du ***Default Group*** (Standard gruppe). Fjern merkingen for ***Inherit policies og settings fra parent group "My Company"*** (Arv retningslinjer og innstillinger fra foreldregruppen "Min bedrift"), og klikk på ***Communications***

Settings (Kommunikasjonsinnstillinger) under ***Location-Independent Policies og Settings*** (Lokasjonsuavhengige policyer og innstillinger).

MERKNAD: Hvis en varselmelding vises, klikker du på ***OK***. Klikk igjen på ***Communications Settings*** (Kommunikasjonsinnstillinger) under ***Location-Independent Policies og Settings*** (Lokasjonsuavhengige policyer og innstillinger).

78. Under ***Download*** (Last ned) må du sørge for at det er merket av for ***Download policies og content fra the management server*** (Last ned policyer og innhold fra management-serveren), og at ***Push mode*** (Push-modus) er valgt.
79. Klikk på ***OK***.
80. Klikk på ***General Settings*** (Generelle innstillinger) under ***Location-independent Policies og Settings*** (Lokasjonsuavhengige policyer og innstillinger).
81. Velg kategorien ***Tamper Protection*** (Beskyttelse mot manipulasjon), og fjern merkingen for og lås ***Protect Symantec security software from being tampered with or shut down*** (Beskytt Symantecs sikkerhetsprogramvare mot manipulasjon eller avslåing).
82. Klikk på ***OK***.
83. Klikk på ***Admin***, og velg ***Servers*** (Servere).
84. Under ***Servers*** (Servere) velger du ***Local Site (My Site)*** (Lokalt sted (Mitt sted)).
85. Under ***Tasks*** (Oppgaver) velger du ***Edit Site Properties*** (Rediger stedsegenskaper). Vinduet ***Site Properties for Locate Site (My Site)*** (Stedsegenskaper for lokaliser sted (Mitt sted)) åpnes.
86. Velg kategorien ***LiveUpdate***. Under ***Download Schedule*** (Nedlastningsplan) kontrollerer du at planen er satt til ***Every 4 hour(s)*** (Hver 4. time).
87. Klikk på ***OK***.
88. Klikk på ***Log Off*** (Logg av) for å lukke Symantec EndPoint Protection Manager Console. Sørg for at Symantec Endpoint Protection-policyene er overført i klientsystemene.

Retningslinjer for installasjon av Symantec EndPoint Protection

1. Aktiver Loopback Connection (Tilbakekobling). Se Aktivere Loopback Connection (Tilbakekobling) på side 6 hvis du vil ha mer informasjon.
2. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste etter installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.
3. Åpne ledeteksten i modusen ***Run As Administrator*** (Kjør som administrator).
4. Gå til C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

MERKNAD: For å konfigurere INW-serveren går du til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Tast inn **RestoreRegSymantec.ps1**, og trykk på ***Enter***.

   6.Bekreft at kjøring av skriptet var vellykket.
   Merk: Du må bekrefte at **RestoreRegSymantec.ps1**-skriptet kjøres uten problemer før du fortsetter.

Hvis mappebanen ovenfor ikke er tilgjengelig, utfører du følgende trinn for alle MLCL-systemer, unntatt MLCL 6.9.6R1 INW-serveren (Server OS: Windows Server 2008R2).

a. Klikk på ***Start***-knappen og deretter på ***Run*** (Kjør).

b. Tast inn **Regedit.exe**, og klikk på ***OK***.

c. Gå til ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing.***

d. Finn og dobbeltklikk på ***State*** (Tilstand)-registeret.

e. Endre ***Base*** (Base) til ***Decimal*** (Desimal).

f. Endre ***Value data*** (Verdidata) til ***65536***.

g. Trykk på ***OK***, og lukk registeret.

McAfee VirusScan Enterprise

Installasjonsoversikt

McAfee VirusScan Enterprise skal installeres på et individuelt Mac-Lab/CardioLab-system og skal kontrolleres individuelt. Bruk følgende instruksjoner for å installere og konfigurere McAfee VirusScan Enterprise.

Virusoppdateringer er institusjonens ansvar. Oppdater definisjonene regelmessig slik at du er sikker på at de nyeste virusdefinisjonene er på systemet.

Installasjonsprosedyre for McAfee VirusScan Enterprise

1. Logg på som **Administrator** eller et medlem av gruppen.
2. Sett enten **McAfee VirusScan Enterprise 8.8 Patch 3**, **McAfee VirusScan Enterprise 8.8 Patch 4**, **McAfee VirusScan Enterprise 8.8 Patch 8 CD** eller **McAfee VirusScan Enterprise 8.8 Patch 9 CD** inn i CD-stasjonen.
3. Dobbeltklikk på ***SetupVSE.Exe***. Dialogboksen Windows Defender vises.
4. Klikk på ***Yes*** (Ja). Skjermbildet McAfee VirusScan Enterprise Setup vises.
5. Klikk på ***Next*** (Neste). Skjermbildet med McAfee End User-lisensavtalen vises.
6. Les lisensavtalen, fyll ut nødvendige felt, og klikk på ***OK*** når du er ferdig. Skjermbildet Select Setup Type (Velg oppsettstype) vises.
7. Velg ***Typical*** (Vanlig), og klikk på ***Next*** (Neste). Skjermbildet Select Access Protection Level (Velg beskyttelsesnivå på tilgang) vises.
8. Velg ***Standard Protection*** (Standard beskyttelse), og klikk på ***Next*** (Neste). Skjermbildet Ready to Install (Klar til installering) vises.
9. Klikk på ***Install*** (Installer), og vent til installeringen er fullført. Etter vellykket installering av McAfee VirusScan Enterprise vises skjermbildet ***McAfee Virus Scan Enterprise Setup has completed successfully*** (Oppsett av McAfee Virus Scan Enterprise var vellykket).

10. Fjern merkingen for ***Run On-Demand Scan*** (Kjør behovsprøvd skanning), og klikk på ***Finish*** (Fullfør).
11. Hvis vinduet ***Update in Progress*** (Oppdatering pågår) vises, klikker du på ***Cancel*** (Avbryt).
12. Hvis en meldingsboks om omstart av systemet vises, klikker du på ***OK***.
13. Start systemet på nytt.
14. Logg på som **Administrator** eller et medlem av gruppen.

Konfigurasjon av McAfee VirusScan Enterprise

1. Velg ***Start > All Programs > McAfee > VirusScan Console*** (Start > Alle programmer > McAfee > VirusScan-konsoll). Skjermbildet ***VirusScan Console*** (VirusScan-konsoll) vises.
2. Høyreklikk på ***Access Protection*** (Tilgangsbeskyttelse), og velg ***Properties*** (Egenskaper). Skjermbildet Properties (Egenskaper) under ***Access Protection*** (Tilgangsbeskyttelse) vises.
3. Klikk på kategorien ***Access Protection*** (Tilgangsbeskyttelse), og fjern merkingen for ***Enable access protection*** (Aktiver tilgangsbeskyttelse) og ***Prevent McAfee services fra being stopped*** (Forhindre at McAfee-tjenester stanses).
4. Klikk på ***OK***.
5. Høyreklikk på ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt), og velg ***Properties*** (Egenskaper). Skjermbildet ***Buffer Overflow Protection Properties*** (Beskyttelse mot bufferoverstrømning) vises.
6. Klikk på kategorien ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverstrømning), og fjern merkingen for ***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings*** (Vis dialogboksen med meldinger når en bufferoverflyt blir oppdaget).
7. Fjern merkingen for ***Enable buffer overflow protection*** (Aktiver beskyttelse mot bufferflyt) under ***Buffer overflow settings*** (Innstillinger for bufferoverflyt).
8. Klikk på ***OK***.
9. Høyreklikk på ***On-Delivery Email Scanner*** (E-postskanning ved levering), og velg ***Properties*** (Egenskaper). Skjermbildet ***On-Delivery Email Scanner Properties*** (Egenskaper for e-postskanning ved levering) vises.
10. Klikk på kategorien ***Scan items*** (Skann elementer), og fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):
    - ***Find unknown program threats og trojans*** (Finn ukjente programvaretrusler og trojanere)
    - ***Find unknown macro threats*** (Finn ukjente makrotrusler)
    - ***Find attachments with multiple extensions*** (Finn vedlegg med flere filetternavn).
11. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).
12. Velg ***Disabled*** (Deaktivert) for ***Sensitivity level*** (Følsomhetsnivå) under ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nettverkskontroll for mistenkelige filer).
13. Klikk på ***OK***.

14. Høyreklikk på ***On-Delivery Email Scanner*** (E-postskanning ved levering), og velg ***Disable*** (Deaktiver).
15. Høyreklikk på ***On-Access Scanner*** (Tilgangsskanner), og velg ***Properties*** (Egenskaper). Skjermbildet ***On-Access Scan Properties*** (Egenskaper for tilgangsskanning) vises.
16. Klikk på kategorien ***General*** (Generelt), og velg ***Disabled*** (Deaktivert) for ***Sensitivity level*** (Følsomhetsnivå) under ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer).
17. Klikk på kategorien ***ScriptScan*** (Skriptskanning), og fjern merkingen for ***Enable scanning of scripts***. (Aktiver skanning av skript).
18. Klikk på kategorien ***Blocking*** (Blokkering), og fjern merkingen for ***Block the connection when a threat is detected in a shared folder*** (Blokker koblingen når det registreres en trussel i en delt mappe).
19. Klikk på kategorien ***Messages*** (meldinger), og fjern merkingen for ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis dialogboksen med meldinger når det oppdages en trussel, og vis den angitte teksten i meldingen).
20. Klikk på ***All Processes*** (Alle prosesser) fra ruten på venstre side.
21. Klikk på kategorien ***Scan items*** (Skann elementer), og fjern merkingen for følgende alternativer under Heuristics (Heuristiske).
    - ***Find unknown unwanted programs og trojans*** (Finn ukjente programvarer og trojanere).
    - ***Find unknown macro threats*** (Finn ukjente makrotrusler)
22. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).
23. Klikk på kategorien ***Exclusions*** (Utelukkelser), og klikk på ***Exclusions*** (Utelukkelser). Skjermbildet ***Set Exclusions*** (Angi utelukkelser) vises.
24. Klikk på ***Add*** (Legg til). Skjermbildet ***Add Exclusion Item*** (Legg til utelukkelseselement) vises.
25. Velg ***By navn/location*** (Etter navn/sted), og klikk på ***Browse*** (Bla). Skjermbildet ***Browse for Files or Folders*** (Bla etter filer eller mapper) vises.
26. Gå til mappene ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** én av gangen, og velg ***OK***.
27. Velg ***Also exclude subfolders*** (Utelukk også undermapper) i vinduet ***Add Exclusion Item*** (Legg til utelukkelseselement), og klikk på ***OK***.
28. Sørg for at mappene C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ er til stede i Set Exclusions (Angi utelukkelser)-vinduet.
29. Klikk på ***OK***.
30. Høyreklikk på ***AutoUpdate*** (Autooppdatering), og velg ***Properties*** (Egenskaper). Skjermbildet McAfee AutoUpdate Properties – AutoUpdate (Egenskaper for McAfee autooppdatering – autooppdatering) vises.
31. Fjern merkingen for følgende alternativer under ***Update Options*** (Alternativer for oppdatering):

- ***Get new detection engine og data if available*** (Hent ny deteksjonsmotor og data hvis tilgjengelig).
- ***Get other available updates (service packs, upgrades, etc.)*** (Hent andre tilgjengelige oppdateringer (servicepakker, oppgraderinger osv.).

32. Klikk på ***Schedule*** (Plan). Skjermbildet Schedule Settings (Planinnstillinger) vises.
33. Fjern merkingen for ***Enable (scheduled task runs at specified time)*** (Aktiver (planlagt oppgave kjøres på angitt tidspunkt)) under ***Schedule Settings*** (Planinnstillinger).
34. Klikk på ***OK***.
35. Klikk på ***OK***.
36. Høyreklikk på vinduet ***VirusScan Console*** (VirusScan-konsoll), og velg ***New On-Demand Scan Task*** (Ny behovsprøvd skanneoppgave).
37. Gi den nye skanningen det nye navnet ***Weekly Scheduled Scan*** (Ukentlig skanning). Skjermbildet ***On-Demand Scan Properties - Weekly Scheduled Scan*** (Egenskaper for behovsprøvd skanning – ukentlig skanning) vises.
38. Klikk på kategorien ***Scan Items*** (Skannelementer), og fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Options*** (Alternativer).
39. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):
    - ***Find unknown programs threats*** (Finn ukjente programtrusler).
    - ***Find unknown macro threats*** (Finn ukjente makrotrusler)
40. Klikk på kategorien ***Exclusions*** (Utelukkelser), og klikk på ***Exclusions*** (Utelukkelser). Skjermbildet ***Set Exclusions*** (Angi utelukkelser) vises.
41. Klikk på ***Add*** (Legg til). Skjermbildet ***Add Exclusion Item*** (Legg til utelukkelseselement) vises.
42. Velg ***By navn/location*** (Etter navn/sted), og klikk på ***Browse*** (Bla). Skjermbildet ***Browse for Files or Folders*** (Bla etter filer eller mapper) vises.
43. Gå til mappene ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** én av gangen, og velg ***OK***.
44. Velg ***Also exclude subfolders*** (Utelukk også undermapper) i vinduet ***Add Exclusion Item*** (Legg til utelukkelseselement), og klikk på ***OK***.
45. Sørg for at mappene ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** er til stede i vinduet ***Set Exclusions*** (Angi utelukkelser).
46. Klikk på ***OK***.
47. Klikk på kategorien ***Performance*** (Ytelse), og velg ***Disabled*** (Deaktivert) for ***Sensitivity level*** (Følsomhetsnivå) under ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (Heuristisk nettverkskontroll for mistenkelige filer).
48. Klikk på ***Schedule*** (Plan). Skjermbildet ***Schedule Settings*** (Planinnstillinger) vises.
49. Klikk på kategorien ***Task*** (Oppgave), og velg ***Enable (scheduled task runs at specified time)*** (Aktiver (planlagt oppgave kjører til spesifisert tid) under ***Schedule Settings*** (Planinnstillinger).
50. Klikk på kategorien ***Schedule*** (Plan), og velg følgende:

a. Kjør oppgave: Ukentlig.

b. Start Time (Starttid): Kl. 12.00

c. Hver: uke, søndag.

51. Klikk på ***OK***.
52. Klikk på ***OK***.
53. Klikk på ***Tools > Alerts*** (Verktøy > Varsler) i vinduet ***VirusScan Console*** (VirusScan-konsoll). Skjermbildet Alert Properties (Varselegenskaper) vises.
54. Fjern merkingen for ***On-Access Scan*** (Tilgangsskanning), ***On-Demand Scan and scheduled scans*** (Behovsprøvd skanning og planlagte skanninger), ***Email Scan*** (E-postskanning) og ***AutoUpdate*** (Autooppdatering).
55. Klikk på ***Destination*** (Mål). Skjermbildet ***Alert Manager Client Configuration*** (Konfigurasjon av klient for varslingsbehandling) vises.
56. Merk av for ***Disable alerting*** (Deaktiver varsling).
57. Klikk på ***OK***. Skjermbildet ***Alert Properties*** (Varselegenskaper) vises.
58. Velg kategorien ***Additional Alerting Options*** (Ytterligere varslingsalternativer).
59. Velg alternativet ***Suppress all alerts (severities 0 to 4)*** (Overse alle varsler (alvorlighetsgrad 0 til 4) fra rullegardinmenyen ***Severity Filter*** (Filter for alvorlighetsgrad).
60. Velg kategorien ***Alert Manager Alerts*** (Varsler for varseladministrasjon).
61. Fjern merkingen for ***Access Protection*** (Tilgangsbeskyttelse).
62. Klikk på ***OK*** for å lukke vinduet ***Alert Properties*** (Varselegenskaper).
63. Lukk vinduet ***VirusScan Console*** (VirusScan-konsoll).

McAfee ePolicy Orchestrator

Installasjonsoversikt

Installer McAfee ePolicy Orchestrator utelukkende i et nettverksbasert Mac-Lab/CardioLab-miljø. McAfee ePolicy Orchestrator må installeres på en Anti-virus Management Console server (konsollserver for håndtering av antivirus), og McAfee VirusScan Enterprise skal distribueres til Centricity Cardiology INW-serveren og arbeidsstasjonene for innhenting/gjennomgang som en klient. Bruk følgende instruksjoner for å installere og konfigurere McAfee ePolicy Orchestrator.

Instruksjonene nedenfor for overføring og konfigurering av McAfee VirusScan Enterprise støtter Patch 3, Patch 4, Patch 8 og Patch 9.

Virusoppdateringer er institusjonens ansvar. Oppdater definisjonene regelmessig slik at du er sikker på at de nyeste virusdefinisjonene er på systemet.

Retningslinjer før installasjon

1. McAfee Anti-Virus Management Console (konsollserver for håndtering av antivirus) skal være installert i henhold til instruksjoner fra McAfee og skal fungere ordentlig.

2. Logg på som **Administrator** eller et medlem av gruppen på alle klientsystemer (innhenting, gjennomgang og INW-server) for å installere antivirusprogramvaren.

3. Deaktiver Loopback Connection (Tilbakekobling) Se Deaktiver tilbakekoblingen på side 6 hvis du vil ha mer informasjon.

4. For distribusjon av McAfee VirusScan Enterprise 8.8 Patch 9 kan du kontakte McAfee for installering av UTN-USERFirst-Object- og universelle VeriSign-rotsertifikater bare på INW-servere. Start systemet på nytt når sertifikatene er installert.

MERKNAD: Hvis UTN-USERFirst-Object- og universelle VeriSign-rotsertifikatet ikke er installert, mislykkes installering av McAfee VirusScan Enterprise 8.8 Patch 9 på INW-servere.

5. For ny installering legger du til følgende agentversjon til McAfee ePolicy Orchestrator hovedrepositorium i McAfee ePolicy Orchestrator Console: ***– McAfee Agent v5.0.5.658***

6. For ny installering legger du til følgende pakke til McAfee ePolicy Orchestrator hovedrepositorium i McAfee ePolicy Orchestrator Console:

   - McAfee VirusScan Enterprise 8.8 Patch 3: VSE880LMLRP3.ZIP (v8.8.0.1128).
   - McAfee VirusScan Enterprise 8.8 Patch 4: VSE880LMLRP4.ZIP (v8.8.0.1247).
   - McAfee VirusScan Enterprise 8.8 Patch 8: VSE880LMLRP8.ZIP (v8.8.0.1599).
   - McAfee VirusScan Enterprise 8.8 Patch 9: VSE880MLRP9.ZIP (v8.8.0.1804).

MERKNAD: VSE880LMLRP3.zip inneholder installasjonspakkene Patch 2 og Patch 3. Patch 2 er til Windows 7 og Windows Server 2008 OS-plattform og Patch 3 er til Windows 8 og Windows Server 2012 OS-plattform. McAfee-installeringsprogrammet installerer riktig patch ved å identifisere versjonen av Windows-operativsystemet.

7. For ny installering, legg til følgende filetternavn til McAfee ePolicy Orchestrator-tabellen over filetternavn i McAfee ePolicy Orchestrator Console:

   - McAfee VirusScan Enterprise 8.8 Patch 3: VIRUSSCAN8800 v8.8.0.348 og VIRUSSCANREPORTS v1.2.0.228
   - McAfee VirusScan Enterprise 8.8 Patch 4: VIRUSSCAN8800 v8.8.0.368 og VIRUSSCANREPORTS v1.2.0.236
   - McAfee VirusScan Enterprise 8.8 Patch 8: VIRUSSCAN8800 v8.8.0.511 og VIRUSSCANREPORTS v1.2.0.311
   - McAfee VirusScan Enterprise 8.8 Patch 9: VIRUSSCAN8800 v8.8.0.548 og VIRUSSCANREPORTS v1.2.0.346

MERKNAD: VIRUSSCAN8800(348).zip og VIRUSSCANREPORTS120(228).zip finnes i pakken McAfee VirusScan Enterprise 8.8 Patch 3.

VIRUSSCAN8800(368).zip og VIRUSSCANREPORTS120(236).zip finnes i pakken McAfee VirusScan Enterprise 8.8 Patch 4.

VIRUSSCAN8800(511).zip og VIRUSSCANREPORTS120(311).zip finnes i pakken McAfee VirusScan Enterprise 8.8 Patch 8.

VIRUSSCAN8800(548).zip og VIRUSSCANREPORTS120(346).zip finnes i pakken McAfee VirusScan Enterprise 8.8 Patch 9.

McAfee ePolicy Orchestrator 5.0 eller 5.3.2 – Nye trinn for installering og distribuering (Foretrukket Push Installation-metode)

1. Avhengig av programvareversjonen velger du ***Start > All Programs (Alle programmer) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Start McAfee ePolicy Orchestrator 5.0.0 Console)*** eller ***Start > All Programs (Alle programmer) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console (Start McAfee ePolicy Orchestrator 5.3.2 Console)*** for å logge på ePolicy Orchestrator-konsollen.

MERKNAD: Klikk på ***Continue with this website*** (Fortsett med dette nettstedet) hvis meldingsboksen ***Security Alert*** (Sikkerhetsvarsel) vises.

2. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).
3. Velg ***Menu > System > System Tree*** (Meny > System > Systemtre). Vinduet System Tree (Systemtre) åpnes.
4. Klikk på ***My Organization*** (Min organisasjon). Med fokus på ***My Organization*** (Min organisasjon) klikker du på ***System Tree Actions > New Systems*** (Systemtrehandlinger > Nye systemer) fra nedre venstre hjørne av skjermen.
5. Velg ***Push agents and add systems to the current group (My Organization)*** (Overfør agenter og legg til systemer til gjeldende gruppe (Min organisasjon), og klikk på ***Browse*** (Bla) på Målsystemene.
6. Angi brukernavn og passord for **domain/local administrator** (domene/lokal administrator), og klikk på ***OK***.
7. Velg ***INW***-domenet fra rullegardinlisten ***Domain*** (Domene).
8. Velg klientmaskinene (Innhenting, Gjennomgang, og INW-server) som er koblet til domenet, og klikk på ***OK***.

MERKNAD: Hvis domenenavnet ikke er angitt i rullegardinlisten ***Domain*** (Domene), gjør du følgende:

- I vinduet ***Browse for Systems*** (Bla etter systemer) klikker du på ***Cancel*** (Avbryt).
- I vinduet ***New Systems*** (Nye systemer) angir du systemnavnene for klientmaskinene (Innhenting, Gjennomgang og INW-server) manuelt i feltet ***Target systems*** (Målsystemer) og fortsetter med trinnene nedenfor.

9. Velg ***Agent Version*** (Agentversjon) som M***cAfee Agent for Windows 4.8.0 (Current)*** (Gjeldende) eller ***McAfee Agent for Windows 5.0.4 (Current)*** (Gjeldende). Angi brukernavn og passord for **domain administrator** (domeneadministrator), og klikk på ***OK***.
10. I klientmaskinene (Innhenting, Gjennomgang og INW-server) bekrefter du at katalogene opprettes som de skal, avhengig av patch-versjonen:

- For patch 3 og 4 kontrollerer du at ***C:\Program Files\McAfee\Common Framework***-katalogen er til stede, og at McAfee Agent er installert i samme katalog.

MERKNAD: For INW-serveren må du sikre at katalogen ***C:\Program Files (x86)\McAfee\Common Framework*** er til stede, og at McAfee Agent er installert i samme katalog.

- For patch 8 må du sjekke at katalogen ***C:\Program Files\McAfee\Agent*** er til stede, og at McAfee Agent er installert i samme katalog.

MERKNAD: For INW-serveren må du sikre at katalogen ***C:\Program Files (x86)\McAfee\Common Framework*** er til stede.

11. Start klientmaskinene (Innhenting, Gjennomgang, og INW-server), og logg på som **domain administrator** (domeneadministrator) eller medlem av gruppen.
12. Avhengig av programvareversjonen klikker du på ***Start > All Programs (Alle programmer) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Start McAfee ePolicy Orchestrator 5.0.0 Console)*** eller ***Start > All Programs (Alle programmer) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console (Start McAfee ePolicy Orchestrator 5.3.2 Console***).
13. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).
14. Klikk på ***Menu > Systems > Systems Tree*** (Meny > Systemer > Systemtre).
15. Klikk på ***My Organization*** (Min organisasjon). Med fokus på ***My Organization*** (Min organisasjon) klikker du på kategorien ***Assigned Client Tasks*** (Tilordnede klientoppgaver).
16. Klikk på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tilordning av klientoppgave) nederst på skjermen. Skjermbildet Client Task Assignment Builder (Verktøy for tilordning av klientoppgave) vises.
17. Velg følgende:
    a. **Produkt:** McAfee Agent
    b. **Oppgavetype:** Produktdistribuering
    c. **Oppgavenavn:** Opprett ny oppgave
18. På skjermbildet ***Client Task Catalog:*** (Klientoppgavekatalog) ***New Task- McAfee Agent (Ny oppgave – McAfee Agent):*** I skjermbildet ***Product Deployment*** (Produktdistribuering) fyller du ut feltene som følger:
    a. **Oppgavenavn:** Angi passende oppgavenavn
    b. **Målplattformer:** Windows
    c. **Produkter og komponenter:** VirusScan Enterprise-versjonen som er kvalifisert for v6.9.6
    d. **Alternativer:** Kjør hver gang en policy iverksettes (kun Windows) hvis ***Options*** (Alternativer) er tilgjengelig
19. Klikk på ***Save*** (Lagre).
20. I skjermbildet ***1 Select Task*** (1 Velg oppgave) velger du følgende:
    a. **Produkt:** McAfee Agent
    b. **Oppgavetype:** Produktdistribuering
    c. **Oppgavenavn:** Nylig opprettet oppgavenavn
21. Klikk på ***Next*** (Neste). Skjermbildet 2 Schedule (2 Plan) vises.
22. Velg R***un immediately*** (Kjør øyeblikkelig) fra rullegardinlisten ***Schedule type*** (Plantype).

23. Klikk på ***Next*** (Neste). Skjermbildet 3 Summary (3 Oppsummering) vises.
24. Klikk på ***Save*** (Lagre). Skjermbildet ***System Tree*** (Systemtre) vises.
25. Velg kategorien ***Systems*** (Systemer), og velg deretter alle klientmaskinene (Innhenting, Gjennomgang, og INW-server) som er koblet til domenet.
26. Klikk på ***Wake up Agents*** (Vekk agenter) i bunnen av vinduet.
27. Behold standardinnstillingene, og klikk på ***OK***.
28. Vent til McAfee-ikonet vises i systemstatusfeltet. Start deretter alle klientmaskinene (Innhenting, Gjennomgang, og INW-server) på nytt, og logg på med **Administrator** eller et medlem av gruppen på alle klientmaskiner.
29. Klikk på linken ***Log Off*** (Logg av) for å lukke McAfee ePolicy Orchestrator Console.

McAfee ePolicy Orchestrator 5.9.0 – Nye trinn for installering og distribuering (foretrukket Push-installeringsmetode)

1. Klikk på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.9.0-konsollen) for å logge på ePolicy Orchestrator-konsollen.

MERKNAD: Klikk på ***Continue with this website*** (Fortsett med dette nettstedet) hvis meldingsboksen ***Security Alert*** (Sikkerhetsvarsel) vises.

2. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).
3. Velg ***Menu > System > System Tree*** (Meny > System > Systemtre). Vinduet ***System Tree*** (Systemtre) åpnes.
4. Klikk på ***My Organization*** (Min organisasjon). Med fokus på ***My Organization*** (Min organisasjon) klikker du på ***New Systems*** (Nye systemer) øverst på skjermen.
5. Velg ***Push agents and add systems to the current group (My Organization)*** (Overfør agenter og legg til systemer til gjeldende gruppe (Min organisasjon), og klikk på ***Browse*** (Bla) på Målsystemene.
6. Angi brukernavn og passord for **domain/local administrator** (domene/lokal administrator), og klikk på ***OK***.
7. Velg ***INW***-domenet fra rullegardinlisten ***Domain*** (Domene).
8. Velg klientmaskinene (Innhenting, Gjennomgang, og INW-server) som er koblet til domenet, og klikk på ***OK***.

MERKNAD: Hvis domenenavnet ikke er angitt i rullegardinlisten ***Domain*** (Domene), gjør du følgende:

- I vinduet ***Browse for Systems*** (Bla etter systemer) klikker du på ***Cancel*** (Avbryt).
- I vinduet ***New Systems*** (Nye systemer) angir du systemnavnene for klientmaskinene (Innhenting, Gjennomgang og INW-server) manuelt og skilt med komma i feltet ***Target systems*** (Målsystemer) og fortsetter med trinnene nedenfor.

9. Velg ***Agent Version*** (Agentversjon) som M***cAfee Agent for Windows 5.0.5 (Current)*** (Gjeldende). Angi brukernavn og passord for **domain administrator** (domeneadministrator), og klikk på ***OK***.

10. På klientmaskinene (Innhenting, Gjennomgang og INW-server) bekrefter du at katalogene ***C:\Program Files\McAfee\Agent*** opprettes som de skal.

11. Start klientmaskinene (Innhenting, Gjennomgang, og INW-server), og logg på som **domain administrator** (domeneadministrator) eller medlem av gruppen.

12. Klikk på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.9.0-konsollen) for å logge på ePolicy Orchestrator-konsollen.

13. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).

14. Klikk på ***Menu > Systems > Systems Tree*** (Meny > Systemer > Systemtre).

15. Klikk på ***My Organization*** (Min organisasjon). Med fokus på ***My Organization*** (Min organisasjon) klikker du på kategorien ***Assigned Client Tasks*** (Tilordnede klientoppgaver).

16. Klikk på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tilordning av klientoppgave) nederst på skjermen. Skjermbildet ***Client Task Assignment Builder*** (Verktøy for tilordning av klientoppgave) vises.

17. Velg følgende:

    a. **Produkt:** McAfee Agent

    b. **Oppgavetype:** Produktdistribuering

18. Klikk på ***Task Actions > Create New Task*** (Oppgavehandlinger > Opprett ny oppgave). Skjermbildet ***Create New Task*** (Opprett ny oppgave) vises.

19. I skjermbildet ***Create New Task*** (Opprett ny oppgave) fyller du ut feltene på følgende måte:

    a. **Oppgavenavn:** Angi passende oppgavenavn

    b. **Målplattformer:** Windows (fjern merking for alle andre alternativer)

    c. **Produkter og komponenter:** VirusScan Enterprise 8.8.0,1804

20. Klikk på ***Save*** (Lagre). Skjermbildet ***Client Task Assignment Builde***r (Verktøy for tilordning av klientoppgave) vises.

21. I skjermbildet ***Client Task Assignment Builder*** (Verktøy for tilordning av klientoppgave) velger du følgende:

    a. **Produkt:** McAfee Agent

    b. **Oppgavetype:** Produktdistribuering

    c. **Oppgavenavn:** Nylig opprettet oppgavenavn

    d. **Schedule Type (Plantype):** Kjør umiddelbart

22. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Client Tasks*** (Tilordnede klientoppgaver) vises.

23. Velg kategorien ***Systems*** (Systemer), og velg deretter alle klientmaskinene (Innhenting, Gjennomgang, og INW-server) som er koblet til domenet.

24. Klikk på ***Wake up Agents*** (Vekk agenter) nederst i vinduet.

25. Behold standardinnstillingene, og klikk på ***OK***.

26. Vent til McAfee-ikonet vises i systemstatusfeltet. Start deretter alle klientmaskinene (Innhenting, Gjennomgang, og INW-server) på nytt, og logg på med **Administrator** eller et medlem av gruppen på alle klientmaskiner.

27. Klikk på linken ***Log Off*** (Logg av) for å lukke McAfee ePolicy Orchestrator Console.

Konfigurering av McAfee ePolicy Orchestrator 5.0 og 5.3.2 Server Console

1. Avhengig av programvareversjonen klikker du på ***Start > All Programs (Alle programmer) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Start McAfee ePolicy Orchestrator 5.0.0 Console)*** eller ***Start > All Programs (Alle programmer) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console (Start McAfee ePolicy Orchestrator 5.3.2 Console***).

2. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).

3. Klikk på ***Menu > Systems > Systems Tree*** (Meny > Systemer > Systemtre).

4. Klikk på ***My Organization*** (Min organisasjon). Med fokus på My Organization (Min organisasjon) klikker du på kategorien ***Assigned Client Tasks*** (Tilordnede klientoppgaver).

5. Klikk på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tilordning av klientoppgave) nederst på skjermen. Skjermbildet ***Client Task Assignment Builder*** (Verktøy for tilordning av klientoppgave) vises.

6. Velg følgende:

   a. ***Produkt:*** VirusScan Enterprise 8.8.0

   b. ***Oppgavetype:*** Behovsprøvd skanning

   c. ***Oppgavenavn:*** Opprett ny oppgave

7. På skjermbildet ***Client Task Catalog:*** (Klientoppgavekatalog) ***Ny oppgave – VirusScan Enterprise 8.8.0: On Demand Scan*** (Klientoppgavekatalog: Ny oppgave – VirusScan Enterprise 8.8.0: Behovsprøvd skanning) fyller du ut feltene som følger:

   a. ***Oppgavenavn:*** Ukentlig skann

   b. ***Beskrivelse:*** Ukentlig skann

8. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

9. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Options*** (Alternativer).

10. Fjern merkingen for følgende alternativer under Heuristics (Heuristiske):

    - ***Find unknown programs threats (Finn ukjente programtrusler)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

11. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

12. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

13. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg Also exclude subfolders (Utelukk også undermapper). Klikk på ***OK***.
14. Klikk på kategorien ***Performance*** (Ytelse). Skjermbildet ***Performance*** (Ytelse) vises.
15. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).
16. Klikk på ***Save*** (Lagre).
17. I skjermbildet ***1 Select Task*** (1 Velg oppgave) velger du følgende:
    - ***Produkt:*** VirusScan Enterprise 8.8.0
    - ***Oppgavetype:*** Behovsprøvd skanning
    - ***Oppgavenavn:*** Ukentlig skann
18. Klikk på ***Next*** (Neste). Skjermbildet ***2 Schedule*** (2 Plan) vises.
19. Velg ***Weekly*** (Ukentlig) fra rullegardinmenyen ***Scheduled type*** (Planlagt type), og velg ***Sunday*** (Søndag).
20. Sett ***Start time*** (Starttid) til ***12:00 AM*** (kl. 12.00), og velg ***Run Once at that time*** (Kjør én gang på det klokkeslettet).
21. Klikk på ***Next*** (Neste). Skjermbildet ***3 Summary*** (3 Oppsummering) vises.
22. Klikk på ***Save*** (Lagre). Skjermbildet ***System Tree*** (Systemtre) vises.
23. Velg kategorien ***Assigned Policies*** (Tilordnede policyer). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.
24. Velg ***VirusScan Enterprise 8.8.0*** fra rullegardinlisten ***Product*** (Produkt).
25. Klikk på ***My Default*** (Min standard) for ***On-Access General Policies*** (Generelle policyer ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access General Policies (Generelle policyer ved tilgang) > My Default (Min standard)*** vises.
26. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***General*** (Generelt). Skjermbildet ***General*** (Generelt) vises.
27. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).
28. Klikk på kategorien ***ScriptScan***. Skjermbildet ***Script Scan*** vises.
29. Fjern merkingen for ***Enable scanning of scripts*** (Aktiver skanning av skript).
30. Klikk på kategorien ***Blocking*** (Blokkering). Skjermbildet ***Blocking*** (Blokkering) vises.
31. Fjern merkingen for ***Block the connection when a threatened file is detected in a shared folder*** (Blokker koblingen når det registreres en trussel i en delt mappe).
32. Klikk på kategorien ***Messages*** (Meldinger). Skjermbildet ***Messages*** (Meldinger) vises.
33. Fjern merkingen for ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis dialogboksen med meldinger når det oppdages en trussel, og vis den angitte teksten i meldingen).
34. Velg ***Server*** fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***General*** (Generelt). Skjermbildet ***General*** (Generelt) vises.

35. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).
36. Klikk på kategorien ***ScriptScan*** (Skriptskanning). Skjermbildet ***Script Scan*** (Skriptskanning) vises.
37. Sørg for at merking er fjernet for ***Enable scanning of scripts*** (Aktiver skanning av skript).
38. Klikk på kategorien ***Blocking*** (Blokkering). Skjermbildet ***Blocking*** (Blokkering) vises.
39. Fjern merkingen for ***Block the connection when a threatened file is detected in a shared folder*** (Blokker koblingen når det registreres en trussel i en delt mappe).
40. Klikk på kategorien ***Messages*** (Meldinger). Skjermbildet ***Messages*** (Meldinger) vises.
41. Fjern merkingen for ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis dialogboksen med meldinger når det oppdages en trussel, og vis den angitte teksten i meldingen).
42. Klikk på ***Save*** (Lagre).
43. Klikk på ***My Default*** (Min standard) for ***On-Access Default Processes Policies*** (Policyer for standardprosesser ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Generelle policyer ved tilgang > Min standard) vises.
44. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).
45. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.
46. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):
    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***
47. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).
48. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.
49. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/Rediger utelukkelseselement) vises.
50. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.
51. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.
52. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):
    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***
53. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

54. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

55. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/Rediger utelukkelseselement) vises.

56. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

57. Klikk på ***Save*** (Lagre).

58. Klikk på ***My Default*** (Min standard) for ***On-Access Low Risk Processes Policies*** (Policyer for lavrisikoprosesser ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Lavrisikopolicyer ved tilgang > Min standard) vises.

59. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

60. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

61. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

62. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

63. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

64. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

65. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

66. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

67. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

68. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

69. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

70. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

71. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

72. Klikk på ***Save*** (Lagre).

73. Klikk på ***My Default*** (Min standard) for ***On-Access High Risk Processes Policies*** (Policyer for høyrisikoprosesser ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Høyrisikopolicyer ved tilgang > Min standard) vises.

74. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

75. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

76. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

77. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

78. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

79. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

80. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

81. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

82. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

83. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

84. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

85. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

86. Velg By pattern (Etter mønster). Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

87. Klikk på ***Save*** (Lagre).

88. Klikk på ***My Default*** (Min standard) for ***On Delivery Email Scan Policies*** (Policyer for e-postskanning ved levering). Skjermbildet ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for e-postskanning ved levering > Min standard) vises.
89. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).
90. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.
91. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):
    - ***Find unknown program threats og trojans (Finn ukjente programvaretrusler og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***
    - ***Find attachments med multiple extensions (Finn vedlegg med flere filetternavn)***
92. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).
93. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).
94. Fjern merkingen for ***Enable on-delivery email scanning*** (Aktiver e-postskanning ved levering) under ***Scanning of email*** (Skanning av e-post).
95. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).
96. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.
97. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):
    - ***Find unknown program threats og trojans (Finn ukjente programvaretrusler og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***
    - ***Find attachments med multiple extensions (Finn vedlegg med flere filetternavn)***
98. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).
99. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).
100. Fjern merkingen for ***Enable on-delivery email scanning*** (Aktiver e-postskanning ved levering) under ***Scanning of email*** (Skanning av e-post).
101. Klikk på ***Save*** (Lagre).
102. Klikk på ***My Default*** (Min standard) for ***General Options Policies*** (Polycier for generelle alternativer). Skjermbildet ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for generelle alternativer > Min standard) vises.
103. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for)
104. Klikk på kategorien ***Display Options*** (Vis alternativer). Skjermbildet ***Display Options*** (Vis alternativer) vises.
105. Velg følgende under ***Console options*** (Konsollalternativer):

- ***Display managed tasks in the client console. (Vis håndterte oppgaver på klientkonsollen)***
- ***Disable default AutoUpdate task schedule. (Deaktiver standard oppgaveplan for AutoUpdate)***

106. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).
107. Klikk på kategorien ***Display Options*** (Vis alternativer). Skjermbildet ***Display Options*** (Vis alternativer) vises.
108. Velg følgende under ***Console options*** (Konsollalternativer):
    - ***Display managed tasks in the client console. (Vis håndterte oppgaver på klientkonsollen)***
    - ***Disable default AutoUpdate task schedule. (Deaktiver standard oppgaveplan for AutoUpdate)***
109. Klikk på ***Save*** (Lagre).
110. Klikk på ***My Default*** (Min standard) for ***Alert Policies*** (Varslingspolicyer). Skjermbildet ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Varslingspolicyer > Min standard) vises.
111. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).
112. Velg kategorien ***Alert Manager Alerts*** (Varsler for varseladministrasjon). Skjermbildet ***Alert Manager Alerts*** (Varsler for varseladministrasjon) vises.
113. Fjern merkingen for ***On-Access Scan*** (Tilgangsskanning), ***On-Demand Scan and scheduled scans*** (Behovsprøvd skanning og planlagte skanninger), ***Email Scan*** (E-postskanning) og ***AutoUpdate*** (Autooppdatering) under ***Components that generate alerts*** (Komponenter som genererer varsler).
114. Velg ***Disable alerting*** (Deaktiver varsling) blant alternativene i ***Alert Manager*** (Varsler for varseladministrasjon).
115. Fjern merkingen for ***Access Protection*** (Tilgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter som genererer varsler).
116. Klikk på ***Additional Alerting Options*** (Ytterligere varslingsalternativer). Skjermbildet ***Additional Alerting Options*** (Ytterligere varslingsalternativer) vises.
117. Velg ***Suppress all alerts (severities 0 to 4)*** (Overse alle varsler (alvorlighetsgrad 0 til 4) fra rullegardinmenyen ***Severity Filters*** (Filter for alvorlighetsgrad).
118. Velg ***Server*** fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Alert Manager Alerts*** (Varsler for varseladministrasjon). Skjermbildet ***Alert Manager Alerts*** (Varsler for varseladministrasjon) vises.
119. Fjern merkingen for ***On-Access Scan*** (Tilgangsskanning), ***On-Demand Scan and scheduled scans*** (Behovsprøvd skanning og planlagte skanninger), ***Email Scan*** (E-postskanning) og ***AutoUpdate*** (Autooppdatering) under ***Components that generate alerts*** (Komponenter som genererer varsler).
120. Merk av for ***Disable alerting*** (Deaktiver varsling) blant alternativene i ***Alert Manager*** (Varsler for varseladministrasjon).
121. Fjern merkingen for ***Access Protection*** (Tilgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter som genererer varsler).

122. Klikk på ***Additional Alerting Options*** (Ytterligere varslingsalternativer). Skjermbildet Additional Alerting Options (Ytterligere varslingsalternativer) vises.

123. Velg ***Suppress all alerts (severities 0 to 4)*** (Overse alle varsler (alvorlighetsgrad 0 til 4) fra rullegardinmenyen ***Severity Filters*** (Filter for alvorlighetsgrad).

124. Klikk på ***Save*** (Lagre).

125. Klikk på ***My Default*** (Min standard) for ***Access Protection Policies*** (Policyer for tilgangsbeskyttelse). Skjermbildet ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for tilgangsbeskyttelse > Min standard) vises.

126. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

127. Klikk på kategorien ***Access Protection*** (Tilgangsbeskyttelse). Skjermbildet ***Access Protection*** (Tilgangsbeskyttelse) vises.

128. Fjern merkingen for følgende alternativer under ***Access protection settings*** (Innstillinger for tilgangsbeskyttelse):

    - ***Enable access protection (Aktiver tilgangsbeskyttelse)***
    - ***Prevent McAfee services fra being stopped (Forhindre at McAfee-tjenester stanses)***

129. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).

130. Klikk på kategorien ***Access Protection*** (Tilgangsbeskyttelse). Skjermbildet ***Access Protection*** (Tilgangsbeskyttelse) vises.

131. Fjern merkingen for følgende alternativer under ***Access protection settings*** (Innstillinger for tilgangsbeskyttelse):

    - ***Enable access protection (Aktiver tilgangsbeskyttelse)***
    - ***Prevent McAfee services fra being stopped (Forhindre at McAfee-tjenester stanses)***

132. Klikk på ***Save*** (Lagre).

133. Klikk på ***My Default*** (Min standard) for ***Buffer Overflow Protection Policies*** (Policyer for beskyttelse mot bufferoverflyt). Skjermbildet ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for beskyttelse mot bufferoverflyt > Min standard) vises.

134. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

135. Klikk på kategorien ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt). Skjermbildet ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt) vises.

136. Fjern merkingen for ***Show the message dialog box when a buffer overflow is detected*** (Vis meldingsdialogboksen når det oppdages en bufferoverflyt) under ***Client system warning*** (Klientsystemvarsling).

137. Fjern merkingen for ***Enable buffer overflow protection*** (Aktiver beskyttelse mot bufferflyt) under ***Buffer overflow settings*** (Innstillinger for bufferoverflyt).

138. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).

139. Klikk på kategorien ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt). Skjermbildet ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt) vises.

140. Fjern merkingen for ***Show the message dialog box when a buffer overflow is detected*** (Vis meldingsdialogboksen når det oppdages en bufferoverflyt) under ***Client system warning*** (Klientsystemvarsling).

141. Fjern merkingen for ***Enable buffer overflow protection*** (Aktiver beskyttelse mot bufferflyt) under ***Buffer overflow settings*** (Innstillinger for bufferoverflyt).

142. Klikk på ***Save*** (Lagre).

143. Velg ***McAfee Agent*** fra rullegardinmenyen ***Product*** (Produkt). Vinduet ***Policies*** (Policyer) for McAfee Agent vises.

144. Klikk på ***My Default*** (Min standard) for ***Repository*** (Oppbevaringssted). Skjermbildet ***McAfee Agent > Repository > My Default*** (McAfee Agent > Oppbevaringssted > Min standard) vises.

145. Klikk på kategorien ***Proxy***. Skjermbildet ***Proxy*** vises.

146. Velg ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Bruk Internet Explorer-innstillinger (For Windows) / innstillinger for systempreferanser (For Mac OSX) under ***Proxy settings*** (PROXY-innstillinger).

147. Klikk på ***Save*** (Lagre).

148. Klikk på kategorien ***Systems*** (Systemer).

149. Velg alle klientsystemene (innhentingssystemet, gjennomgangsarbeidsstasjonen og Centricity Cardiology INW-serveren) som de konfigurerte policyene skal distribueres til.

150. Velg ***Wake Up Agents*** (Vekk agenter). Skjermbildet ***Wake Up Agent*** (Vekk agenter) vises.

151. Klikk på ***OK***.

152. Logg av ePolicy Orchestrator.

Konfigurering av serverkonsoll for McAfee ePolicy Orchestrator 5.9.0

1. Avhengig av programvareversjonen klikker du på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.9.0-konsollen).
2. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).
3. Klikk på ***Menu > Systems > Systems Tree*** (Meny > Systemer > Systemtre).
4. Klikk på ***My Organization*** (Min organisasjon). Med fokus på My Organization (Min organisasjon) klikker du på kategorien ***Assigned Client Tasks*** (Tilordnede klientoppgaver).
5. Klikk på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tilordning av klientoppgave) nederst på skjermen . Skjermbildet ***Client Task Assignment Builder*** (Verktøy for tilordning av klientoppgave) vises.
6. Velg følgende:
   a. ***Produkt:*** VirusScan Enterprise 8.8.0
   b. ***Oppgavetype:*** Behovsprøvd skanning
7. Klikk på ***Create New Task*** (Opprett ny oppgave) under ***Task Actions*** (Oppgavehandlinger). Skjermbildet ***Create New Task*** (Opprett ny oppgave) vises.
8. I skjermbildet ***Create New Task*** (Opprett ny oppgave) fyller du ut feltene på følgende måte:
   a. ***Oppgavenavn:*** Ukentlig skann
   b. ***Beskrivelse:*** Ukentlig skann
9. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.
10. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Options*** (Alternativer).
11. Fjern merkingen for følgende alternativer under Heuristics (Heuristiske):
    - ***Find unknown programs threats (Finn ukjente programtrusler)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***
12. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.
13. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.
14. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg Also exclude subfolders (Utelukk også undermapper). Klikk på ***OK***.
15. Klikk på kategorien ***Performance*** (Ytelse). Skjermbildet ***Performance*** (Ytelse) vises.
16. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).

17. Klikk på ***Save*** (Lagre). Skjermbildet ***Client Task Assignment Builder*** (Verktøy for tilordning av klientoppgave) vises.
18. I skjermbildet ***Client Task Assignment Builder*** (Verktøy for tilordning av klientoppgave) velger du følgende:
    - ***Produkt:*** VirusScan Enterprise 8.8.0
    - ***Oppgavetype:*** Behovsprøvd skanning
    - ***Oppgavenavn:*** Ukentlig skann
19. Velg ***Weekly*** (Ukentlig) fra rullegardinmenyen ***Scheduled type*** (Planlagt type), og velg ***Sunday*** (Søndag).
20. Sett ***Start time*** (Starttid) til ***12:00 AM*** (kl. 12.00), og velg ***Run Once at that time*** (Kjør én gang på det klokkeslettet).
21. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Client Tasks*** (Tilordnede klientoppgaver) vises.
22. Velg kategorien ***Assigned Policies*** (Tilordnede policyer). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.
23. Velg ***VirusScan Enterprise 8.8.0*** fra rullegardinlisten ***Product*** (Produkt).
24. Klikk på ***My Default*** (Min standard) for ***On-Access General Policies*** (Generelle policyer ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access General Policies (Generelle policyer ved tilgang) > My Default (Min standard)*** vises.
25. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***General*** (Generelt). Skjermbildet ***General*** (Generelt) vises.
26. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).
27. Klikk på kategorien ***ScriptScan***. Skjermbildet ***Script Scan*** vises.
28. Fjern merkingen for ***Enable scanning of scripts*** (Aktiver skanning av skript).
29. Klikk på kategorien ***Blocking*** (Blokkering). Skjermbildet ***Blocking*** (Blokkering) vises.
30. Fjern merkingen for ***Block the connection when a threatened file is detected in a shared folder*** (Blokker koblingen når det registreres en trussel i en delt mappe).
31. Klikk på kategorien ***Messages*** (Meldinger). Skjermbildet ***Messages*** (Meldinger) vises.
32. Fjern merkingen for ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis dialogboksen med meldinger når det oppdages en trussel, og vis den angitte teksten i meldingen).
33. Velg ***Server*** fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***General*** (Generelt). Skjermbildet ***General*** (Generelt) vises.
34. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).
35. Klikk på kategorien ***ScriptScan*** (Skriptskanning). Skjermbildet ***Script Scan*** (Skriptskanning) vises.
36. Sørg for at merking er fjernet for ***Enable scanning of scripts*** (Aktiver skanning av skript).
37. Klikk på kategorien ***Blocking*** (Blokkering). Skjermbildet ***Blocking*** (Blokkering) vises.

38. Fjern merkingen for ***Block the connection when a threatened file is detected in a shared folder*** (Blokker koblingen når det registreres en trussel i en delt mappe).

39. Klikk på kategorien ***Messages*** (Meldinger). Skjermbildet ***Messages*** (Meldinger) vises.

40. Fjern merkingen for ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis dialogboksen med meldinger når det oppdages en trussel, og vis den angitte teksten i meldingen).

41. Klikk på ***Save*** (Lagre). Skjermbildet Assigned Policies (Tilordnede policyer) vises.

42. Klikk på ***My Default*** (Min standard) for ***On-Access Default Processes Policies*** (Policyer for standardprosesser ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Generelle policyer ved tilgang > Min standard) vises.

43. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

44. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

45. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

46. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

47. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

48. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/Rediger utelukkelseselement) vises.

49. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

50. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

51. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

52. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

53. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

54. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/Rediger utelukkelseselement) vises.

55. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

56. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

57. Klikk på ***My Default*** (Min standard) for ***On-Access Low Risk Processes Policies*** (Policyer for lavrisikoprosesser ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Lavrisikopolicyer ved tilgang > Min standard) vises.

58. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

59. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

60. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

61. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

62. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

63. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

64. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

65. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

66. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

67. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

68. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

69. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

70. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

71. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

72. Klikk på ***My Default*** (Min standard) for ***On-Access High Risk Processes Policies*** (Policyer for høyrisikoprosesser ved tilgang). Skjermbildet ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Høyrisikopolicyer ved tilgang > Min standard) vises.

73. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

74. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

75. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

76. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

77. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

78. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

79. Velg ***By pattern*** (Etter mønster). Angi mappene **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

80. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

81. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown unwanted programs and trojans. (Finn ukjente programvarer og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***

82. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

83. Klikk på kategorien ***Exclusions*** (Utelukkelser). Skjermbildet ***Exclusions*** (Utelukkelser) vises.

84. Klikk på ***Add*** (Legg til). Skjermbildet ***Add/Edit Exclusion Item*** (Legg til/rediger utelukkelseselement) vises.

85. Velg By pattern (Etter mønster). Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** én av gangen, og velg ***Also exclude subfolders*** (Utelukk også undermapper). Klikk på ***OK***.

86. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

87. Klikk på ***My Default*** (Min standard) for ***On Delivery Email Scan Policies*** (Policyer for e-postskanning ved levering). Skjermbildet ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for e-postskanning ved levering > Min standard) vises.

88. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

89. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

90. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown program threats og trojans (Finn ukjente programvaretrusler og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***
    - ***Find attachments med multiple extensions (Finn vedlegg med flere filetternavn)***

91. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

92. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).

93. Fjern merkingen for ***Enable on-delivery email scanning*** (Aktiver e-postskanning ved levering) under ***Scanning of email*** (Skanning av e-post).

94. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).

95. Klikk på kategorien ***Scan Items*** (Skannelementer). Skjermbildet ***Scan Items*** (Skannelementer) vises.

96. Fjern merkingen for følgende alternativer under ***Heuristics*** (Heuristiske):

    - ***Find unknown program threats og trojans (Finn ukjente programvaretrusler og trojanere)***
    - ***Find unknown macro threats (Finn ukjente makrotrusler)***
    - ***Find attachments med multiple extensions (Finn vedlegg med flere filetternavn)***

97. Fjern merkingen for ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering av uønskede programmer).

98. Velg ***Disabled*** (Deaktivert) fra ***Artemis (Heuristic nettverk check for suspicious files)*** (Artemis (heuristisk nettverkskontroll for mistenkelige filer)).

99. Fjern merkingen for ***Enable on-delivery email scanning*** (Aktiver e-postskanning ved levering) under ***Scanning of email*** (Skanning av e-post).

100. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

101. Klikk på ***My Default*** (Min standard) for ***General Options Policies*** (Polycier for generelle alternativer). Skjermbildet ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for generelle alternativer > Min standard) vises.

102. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for)

103. Klikk på kategorien ***Display Options*** (Vis alternativer). Skjermbildet ***Display Options*** (Vis alternativer) vises.

104. Velg følgende under ***Console options*** (Konsollalternativer):

    - ***Display managed tasks in the client console. (Vis håndterte oppgaver på klientkonsollen)***
    - ***Disable default AutoUpdate task schedule. (Deaktiver standard oppgaveplan for AutoUpdate)***

105. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).

106. Klikk på kategorien ***Display Options*** (Vis alternativer). Skjermbildet ***Display Options*** (Vis alternativer) vises.

107. Velg følgende under ***Console options*** (Konsollalternativer):

    - ***Display managed tasks in the client console. (Vis håndterte oppgaver på klientkonsollen)***
    - ***Disable default AutoUpdate task schedule. (Deaktiver standard oppgaveplan for AutoUpdate)***

108. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

109. Klikk på ***My Default*** (Min standard) for ***Alert Policies*** (Varslingspolicyer). Skjermbildet ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Varslingspolicyer > Min standard) vises.

110. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

111. Velg kategorien ***Alert Manager Alerts*** (Varsler for varseladministrasjon). Skjermbildet ***Alert Manager Alerts*** (Varsler for varseladministrasjon) vises.

112. Fjern merkingen for ***On-Access Scan*** (Tilgangsskanning), ***On-Demand Scan and scheduled scans*** (Behovsprøvd skanning og planlagte skanninger), ***Email Scan*** (E-postskanning) og ***AutoUpdate*** (Autooppdatering) under ***Components that generate alerts*** (Komponenter som genererer varsler).

113. Velg ***Disable alerting*** (Deaktiver varsling) blant alternativene i ***Alert Manager*** (Varsler for varseladministrasjon).

114. Fjern merkingen for ***Access Protection*** (Tilgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter som genererer varsler).

115. Klikk på ***Additional Alerting Options*** (Ytterligere varslingsalternativer). Skjermbildet ***Additional Alerting Options*** (Ytterligere varslingsalternativer) vises.

116. Velg ***Suppress all alerts (severities 0 to 4)*** (Overse alle varsler (alvorlighetsgrad 0 til 4) fra rullegardinmenyen ***Severity Filters*** (Filter for alvorlighetsgrad).

117. Velg ***Server*** fra rullegardinlisten ***Settings for*** (Innstillinger for), og velg kategorien ***Alert Manager Alerts*** (Varsler for varseladministrasjon). Skjermbildet ***Alert Manager Alerts*** (Varsler for varseladministrasjon) vises.

118. Fjern merkingen for ***On-Access Scan*** (Tilgangsskanning), ***On-Demand Scan and scheduled scans*** (Behovsprøvd skanning og planlagte skanninger), ***Email Scan*** (E-postskanning) og ***AutoUpdate*** (Autooppdatering) under ***Components that generate alerts*** (Komponenter som genererer varsler).

119. Merk av for ***Disable alerting*** (Deaktiver varsling) blant alternativene i ***Alert Manager*** (Varsler for varseladministrasjon).

120. Fjern merkingen for ***Access Protection*** (Tilgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter som genererer varsler).

121. Klikk på ***Additional Alerting Options*** (Ytterligere varslingsalternativer). Skjermbildet Additional Alerting Options (Ytterligere varslingsalternativer) vises.

122. Velg ***Suppress all alerts (severities 0 to 4)*** (Overse alle varsler (alvorlighetsgrad 0 til 4) fra rullegardinmenyen ***Severity Filters*** (Filter for alvorlighetsgrad).

123. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

124. Klikk på ***My Default*** (Min standard) for ***Access Protection Policies*** (Policyer for tilgangsbeskyttelse). Skjermbildet ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for tilgangsbeskyttelse > Min standard) vises.

125. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

126. Klikk på kategorien ***Access Protection*** (Tilgangsbeskyttelse). Skjermbildet ***Access Protection*** (Tilgangsbeskyttelse) vises.

127. Fjern merkingen for følgende alternativer under ***Access protection settings*** (Innstillinger for tilgangsbeskyttelse):

    - ***Enable access protection (Aktiver tilgangsbeskyttelse)***
    - ***Prevent McAfee services fra being stopped (Forhindre at McAfee-tjenester stanses)***
    - ***Enable Enhanced Self-Protection (Aktiver forsterket egenbeskyttelse).***

128. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).

129. Klikk på kategorien ***Access Protection*** (Tilgangsbeskyttelse). Skjermbildet ***Access Protection*** (Tilgangsbeskyttelse) vises.

130. Fjern merkingen for følgende alternativer under ***Access protection settings*** (Innstillinger for tilgangsbeskyttelse):

    - ***Enable access protection (Aktiver tilgangsbeskyttelse)***
    - ***Prevent McAfee services fra being stopped (Forhindre at McAfee-tjenester stanses)***
    - ***Enable Enhanced Self-Protection (Aktiver forsterket egenbeskyttelse).***

131. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

132. Klikk på ***My Default*** (Min standard) for ***Buffer Overflow Protection Policies*** (Policyer for beskyttelse mot bufferoverflyt). Skjermbildet ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Policyer for beskyttelse mot bufferoverflyt > Min standard) vises.

133. Velg ***Workstation*** (Arbeidsstasjon) fra rullegardinlisten ***Settings for*** (Innstillinger for).

134. Klikk på kategorien ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt). Skjermbildet ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt) vises.

135. Fjern merkingen for ***Show the message dialog box when a buffer overflow is detected*** (Vis meldingsdialogboksen når det oppdages en bufferoverflyt) under ***Client system warning*** (Klientsystemvarsling).

136. Fjern merkingen for ***Enable buffer overflow protection*** (Aktiver beskyttelse mot bufferflyt) under ***Buffer overflow settings*** (Innstillinger for bufferoverflyt).

137. Velg ***Server*** (Server) fra rullegardinlisten ***Settings for*** (Innstillinger for).

138. Klikk på kategorien ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt). Skjermbildet ***Buffer Overflow Protection*** (Beskyttelse mot bufferoverflyt) vises.

139. Fjern merkingen for ***Show the message dialog box when a buffer overflow is detected*** (Vis meldingsdialogboksen når det oppdages en bufferoverflyt) under ***Client system warning*** (Klientsystemvarsling).

140. Fjern merkingen for ***Enable buffer overflow protection*** (Aktiver beskyttelse mot bufferflyt) under ***Buffer overflow settings*** (Innstillinger for bufferoverflyt).

141. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

142. Velg ***McAfee Agent*** fra rullegardinmenyen ***Product*** (Produkt). Vinduet ***Policies*** (Policyer) for McAfee Agent vises.

143. Klikk på ***My Default*** (Min standard) for ***Repository*** (Oppbevaringssted). Skjermbildet ***McAfee Agent > Repository > My Default*** (McAfee Agent > Oppbevaringssted > Min standard) vises.

144. Klikk på kategorien ***Proxy***. Skjermbildet ***Proxy*** vises.

145. Kontroller at ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Bruk Internet Explorer-innstillinger (For Windows) / innstillinger for systempreferanser (For Mac OSX) under ***Proxy settings*** (PROXY-innstillinger) er valgt.

146. Klikk på ***Save*** (Lagre). Skjermbildet ***Assigned Policies*** (Tilordnede policyer) vises.

147. Klikk på kategorien ***Systems*** (Systemer).

148. Velg alle klientsystemene (innhentingssystemet, gjennomgangsarbeidsstasjonen og Centricity Cardiology INW-serveren) som de konfigurerte policyene skal distribueres til.

149. Velg ***Wake Up Agents*** (Vekk agenter). Skjermbildet ***Wake Up Agent*** (Vekk agenter) vises.

150. Klikk på ***OK***.

151. Logg av ePolicy Orchestrator.

Retningslinjer før installasjon av McAfee ePolicy Orchestrator

Aktiver Loopback Connection (Tilbakekobling). Se Aktivere Loopback Connection (Tilbakekobling) på side 6 hvis du vil ha mer informasjon.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Installasjonsoversikt

Installer Trend Micro OfficeScan Client/Server Edition utelukkende på et nettverksbasert Mac-Lab/CardioLab-miljø. Trend Micro OfficeScan må installeres på Anti-virus Management Console-serveren (konsollserver for håndtering av antivirus) og deretter distribueres til Centricity Cardiology INW-serveren og klientene for innhentings-/gjennomgangsarbeidsstasjonene. Bruk følgende instruksjoner for å installere ***Trend Micro OfficeScan Client/Server Edition***.

Virusoppdateringer er institusjonens ansvar. Oppdater definisjonene regelmessig slik at du er sikker på at de nyeste virusdefinisjonene er på systemet.

Retningslinjer før installasjon

1. Trend Micro Anti-Virus Management-konsollen skal være installert i henhold til Trend Micro-instruksjoner og skal fungere ordentlig.

2. Under installering av Trend Micro OfficeScan gjør du følgende på Anti-Virus Management Console-serveren:

a. Fjern merkingen for ***Enable firewall*** (Aktiver brannmur) i vinduet ***Anti-virus Feature*** (Antivirusfunksjon).

b. Velg ***No, Please do not enable assessment mode*** (Nei, ikke aktiver vurderingsmodus) i vinduet ***Anti-spyware Feature*** (Anti-spionvarefunksjon).

c. Fjern merkingen for ***Enable web reputation policy*** (Aktiver policy for nettrykte) i vinduet ***Web Reputation Feature*** (Nettryktefunksjon).

3. Trend Micro OfficeScan anbefales ikke ved bruk av ***CO_2***-funksjonen med PDM i Mac-Lab/CardioLab-systemene.

4. Hvis Trend Micro OfficeScan er påkrevd:

a. Det anbefales å konfigurere en separat Trend Micro Anti-Virus Management-konsollserver for Mac-Lab/CardioLab-systemene. En global endring i antivirusinnstillingene er nødvendig for å bruke ***CO_2***-funksjonen med PDM i Mac-Lab/CardioLab-systemene.

b. Hvis det ikke er mulig å konfigurere en separat Trend Micro Anti-Virus Management-konsollserver, er det nødvendig å foreta en endring i de globale innstillingene til den eksisterende Trend Micro Anti-Virus Management-konsollserveren etter installeringen. Denne endringen vil virke inn på alle klientsystemene som er koblet til den eksisterende Trend Micro Anti-Virus Management-konsollserveren, og må sjekkes med IT-personalet før du fortsetter.

5. Logg på som **Administrator** eller et medlem av gruppen på alle klientsystemer (innhenting, gjennomgang og INW-server) for å installere antivirusprogramvaren.

6. Deaktiver Loopback Connection (Tilbakekobling) Se Deaktiver tilbakekoblingen på side 6 hvis du vil ha mer informasjon.

7. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste før installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.

Trend Micro OfficeScan – Nye trinn for installering og distribuering (Foretrukket Push Installation-metode)

1. Klikk på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro OfficeScan server – <servernavn> > Office Scan Web-konsoll).

MERKNAD: Fortsett ved å velge ***Continue to this website (not recommended)*** (Fortsett til dette nettstedet (anbefales ikke)). I vinduet Security Alert (Sikkerhetsvarsel) velger du ***In the future, do not show this warning*** (Ikke vis dette varselet i fremtiden) og klikker på ***OK***.

2. Hvis du mottar en sertifikatfeil som indikerer at nettstedet ikke er klarert, må du ordne sertifikatene dine slik at de omfatter Trend Micro OfficeScan.

3. Installer programvareutvidelsene ***AtxEnc*** hvis du blir bedt om det. Skjermbildet Security Warning (Sikkerhetsvarsel) vises.

4. Klikk på ***Install*** (Installer).

5. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).

6. Klikk på ***Update Now*** (Oppdater nå) for å installere nye widgets hvis du blir bedt om det. Vent til oppdateringen av nye widgets er fullført. Skjermbildet The update is completed (Oppdateringen er fullført) vises.
7. Klikk på ***OK***.
8. Fra menylinjen på venstre side klikker du på ***Networked Computers > Client Installation > Remote*** (Nettverksbaserte datamaskiner > Klientinstallering > Ekstern).
9. Installer programvareutvidelsene ***AtxConsole*** hvis du blir bedt om det. Skjermbildet Security Warning (Sikkerhetsvarsel) vises.
10. Klikk på ***Install*** (Installer).
11. Dobbeltklikk på ***My Company*** (Min bedrift) i vinduet ***Remote Installation*** (Ekstern installering). Alle domenene vil bli angitt under ***My Company*** (Min bedrift).
12. Utvid domenet (Eksempel: INW) fra listen. Alle systemene som er koblet til domenet, vises.
13. Hvis domener eller systemer ikke er angitt i vinduet ***Domain and Computers*** (Domene og datamaskiner), gjør du følgende for hvert av klientsystemene (Innhenting, Gjennomgang og INW-server):
    a. Logg på som Administrator eller et medlem av gruppen på alle klientmaskiner.
    b. Klikk på ***Start > Run*** (Start > Kjør).
    c. Tast inn ***<Anti-Virus Management Console_server_IP_address>***, og trykk på ***Enter***. Angi brukernavn og passord for administrator når du blir bedt om det.
    d. Gå til ***<Anti-Virus Management Console_server_IP _address>\ofsscan***, og dobbeltklikk på ***AutoPcc.exe***. Angi brukernavn og passord for administrator når du blir bedt om det.
    e. Start klientsystemene på nytt når installeringen er fullført.
    f. Logg på som **Administrator** eller et medlem av gruppen på alle klientmaskiner, og vent til Trend Micro OfficeScan-ikonet i systemstatusfeltet blir blått.
    g. Hopp over de gjenstående trinnene i denne prosedyren, og gå til prosedyren for konfigurering av Trend Micro OfficeScan-serverkonsollen.
14. Velg klientmaskinene (Innhenting, Gjennomgang og INW-server), og klikk på ***Add*** (Legg til).
15. Tast inn <domain name>\brukernavn og passord, og klikk på ***Log on*** (Logg på).
16. Velg klientmaskinene (Innhenting, Gjennomgang og INW-server) én av gangen fra ruten ***Selected Computers*** (Utvalgte datamaskiner), og klikk på ***Install*** (Installer).
17. Klikk på ***Yes*** (Ja) i bekreftelsesboksen.
18. Klikk på ***OK*** i meldingsboksen ***Number of clients to which notifications were sent*** (Antall klienter som varsel ble sendt til).
19. Start alle klientmaskinene (Innhenting, Gjennomgang og INW-server) på nyt, og logg på som Administrator eller et medlem av gruppen på alle klientmaskinene. Vent så til Trend Micro OfficeScan-ikonet i systemstatusfeltet blir blått med et grønt hakemerke.
20. Klikk på koblingen ***Log Off*** (Logg av) for å lukke ***OfficeScan Web Console***.

Konfigurasjon av serverkonsoll for Trend Micro OfficeScan

1. Velg ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro Office Scan Server <servernavn> > Office Scan Web Consol). Skjermbildet ***Trend Micro OfficeScan Login*** vises.
2. Angi riktig brukernavn og passord, og klikk på ***Login*** (Logg på). Skjermbildet ***Summary*** (Sammendrag) vises.
3. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
4. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
5. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Manual Scan Settings*** (Skanneinnstillinger > Manuelle skanneinnstillinger). Skjermbildet ***Manual Scan Settings*** (Manuelle skanneinnstillinger) vises.
6. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
   - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
   - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
   - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
   - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***
   - ***CPU Usage (CPU-bruk) > Low (Lav).***
   - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
   - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to client Computers Exclusion list. (Liste over skanneutelukkelse (kataloger) > Utelukk kataloger der Trend Micro-produkter er installert, og velg Legg til bane til utelukkelseslisten for klientdatamaskiner).***
   - Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** og **G:** én av gangen, og klikk på ***Add*** (Legg til).
7. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
8. Klikk på ***OK*** når du ser meldingen ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.*** (Utelukkelseslisten på dette skjermbildet vil erstatte utelukkelseslisten på klienter eller domener du valgte i klienttreet tidligere). ***Do you want to proceed?*** (Vil du fortsette?).
9. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Manual Scan Settings*** (Manuelle skanneinnstillinger).
10. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.

11. Velg ***OfficeScan***-serveren til høyre.
12. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Real-time Scan Settings*** (Skanneinnstillinger > Skanneinnstillinger i sanntid). Skjermbildet ***Real-time Scan Settings*** (Skanneinnstillinger i sanntid) vises.
13. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Real-Time Scan Settings > Enable virus/malware scan. (Skanneinnstillinger i sanntid > Aktiver skanning etter virus / skadelig programvare).***
    - ***Real-Time Scan Settings > Enable spyware/grayware scan. (Skanneinnstillinger i sanntid > Aktiver skanning etter spionvare/gråvare).***
    - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
    - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
    - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
    - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Enable IntelliTrap (Aktiver IntelliTrap).***
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
    - ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
    - Sørg for at mappebanene ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:***\ og ***G:***\ er til stede i ***Exclusion List*** (Utelukkelseslisten).
14. Klikk på kategorien ***Action*** (Handling).
15. Behold standardinnstillingene, og fjern merkingen for følgende alternativer:
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected. (Virus/Skadelig programvare > Vis en melding på klientdatamaskinen når virus/Skadelig programvare registreres)***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected. (Virus/Skadelig programvare > Vis en melding på klientdatamaskinen når spionvare/gråvare registreres)***
16. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
17. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Real-time Scan Settings*** (Innstillinger for sanntidsskanning).
18. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
19. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
20. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Scheduled Scan Settings*** (Skanneinnstillinger > Planlagte skanneinnstillinger). Skjermbildet ***Scheduled Scan Settings*** (Planlagte skanneinnstillinger) vises.

21. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scheduled Scan Settings > Enable virus/malware scan (Planlagte skanneinnstillinger > Aktiver skanning etter virus/skadelig programvare).***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan (Planlagte skanneinnstillinger > Aktiver skanning etter spionvare/gråvare).***
    - ***Schedule > Weekly, every Sunday, Start time: (Plan > Ukentlig, hver søndag, Starttid:) 00:00 hh:mm (kl. 00.00 tt:mm)***
    - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
    - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
    - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
    - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***
    - ***CPU Usage (CPU-bruk) > Low (Lav).***
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
    - ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
    - Sørg for at mappebanene ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** er til stede i utelukkelseslisten.
22. Klikk på kategorien ***Action*** (Handling).
23. Behold standardinnstillingene, og fjern merkingen for følgende alternativer:
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected. (Virus/Skadelig programvare > Vis en melding på klientdatamaskinen når virus/Skadelig programvare registreres)***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected. (Virus/Skadelig programvare > Vis en melding på klientdatamaskinen når spionvare/gråvare registreres)***
24. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
25. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Scheduled Scan Settings*** (Planlagte skanneinnstillinger).
26. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
27. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
28. Fra ***Settings*** (Innstilinger) velger du ***Scan Settings > Scan Now Settings*** (Skanneinnstillinger > Innstillinger for Skann nå). Skjermbildet ***Scan Now Settings*** (Innstillinger for skann nå) vises.
29. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:

- ***Scan Now Settings > Enable virus/malware scan. (Innstillinger for Skann nå > Aktiver skanning etter virus/skadelig programvare).***
- ***Scan Now Settings > Enable spyware/grayware scan. (Innstillinger for Skann nå > Aktiver skanning etter spionvare/gråvare).***
- ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
- ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
- ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
- ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***
- ***CPU Usage (CPU-bruk) > Low (Lav).***
- ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
- ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
- ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
- Sørg for at ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:***

30. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
31. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Scan Now Settings*** (Innstillinger for Skann nå).
32. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
33. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
34. Velg ***Web Reputation Settings*** (Innstillinger for nettrykte) fra alternativene ***Settings*** (Innstillinger). Skjermbildet ***Web Reputation Settings*** (Innstillinger for nettrykte) vises.
35. Klikk på kategorien ***External Clients*** (Eksterne klienter), og fjern merkingen for ***Enable Web reputation policy on the following operating systems*** (Aktiver policy for nettrykte på følgende operativsystemer) hvis dette ble valgt under installeringen.
36. Klikk på kategorien ***Internal Clients*** (Interne klienter), og fjern merkingen for ***Enable Web reputation policy on the following operating systems*** (Aktiver policy for nettrykte på følgende operativsystemer) hvis dette ble valgt under installeringen.
37. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
38. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Web Reputation*** (Nettrykte).
39. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
40. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
41. Velg ***Behavior Monitoring Settings*** (Innstillinger for atferdsmonitorering) fra alternativene ***Settings*** (Innstillinger). Skjermbildet ***Behavior Monitoring Settings*** (Innstillinger for atferdsmonitorering) vises.

42. Fjern merkingen for alternativene ***Enable Malware Behavior Blocking*** (Aktiver blokkering av skadelig programvare) og ***Enable Event Monitoring*** (Aktiver hendelsesmonitorering).
43. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
44. Klikk på ***Close*** (Lukk) for å lukke vinduet ***Behavior Monitoring*** (Atferdsmonitorering).
45. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
46. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
47. Velg ***Device Control Settings*** (Innstilinger for enhetskontroll) blant alternativene under ***Settings*** (Innstillinger). Skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll) vises.
48. Klikk på kategorien ***External Clients*** (Eksterne klienter), og fjern merkingen for følgende alternativer:
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access. (Varsel > Vis en melding på klientdatamaskinen når OfficeScan registrerer uautorisert enhetstilgang).***
    - ***Block the AutoRun function on USB storage devices. (Bokker AutoRun-funksjonen på USB-lagringsenheter).***
    - ***Enable Device Control (Aktiver enhetskontroll).***
49. Klikk på kategorien ***Internal Clients*** (Interne klienter), og fjern merkingen for følgende alternativer:
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access. (Varsel > Vis en melding på klientdatamaskinen når OfficeScan registrerer uautorisert enhetstilgang).***
    - ***Block the AutoRun function on USB storage devices. (Bokker AutoRun-funksjonen på USB-lagringsenheter).***
    - ***Enable Device Control (Aktiver enhetskontroll).***
50. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
51. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll).
52. Velg koblingen ***Networked Computers > Client Management*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
53. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
54. Velg ***Privileges and Other Settings*** (Rettigheter og andre innstillinger) fra alternativene under ***Settings*** (Innstillinger).
55. Klikk på kategorien ***Privileges*** (Rettigheter). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Privileges (Skannerettigheter) > Configure Manual Scan Settings (Konfigurer innstillinger for manuell skanning).***
    - ***Scan Privileges (Skannerettigheter) > Configure Real-time Scan Settings (Konfigurer innstillinger for sanntidsskanning).***
    - ***Scan Privileges (Skannerettigheter) > Configure Scheduled Scan Settings (Konfigurer innstillinger for planlagt skanning).***

- ***Proxy Setting Privileges (Rettigheter for proxy-innstilling) > Allow the client user to configure proxy settings (Tillat at bruker av klienten kan konfigurere proxy-innstillinger).***
- ***Uninstallation (Avinstallasjon) > Require a password for the user to uninstall the OfficeScan Client (Brukeren må ha et passord for å kunne avinstallere OfficeScan-klienten).*** Angi riktig passord, og bekreft passordet.
- ***Unloading (Utlasting) > Require a password for the user to unload the OfficeScan client (Brukeren må ha et passord for å kunne laste ut OfficeScan-klienten).*** Angi riktig passord, og bekreft passordet.

56. Klikk på kategorien ***Other Settings*** (Andre innstillinger).
57. Velg ***Client Security Settings > Normal*** (Sikkerhetsinnstillinger for klient > Normale), og fjern merkingen for de andre alternativene.

MERKNAD: Det er viktig å slette følgende alternativer.

- ***Client Self-protection > Protect OfficeScan client services (Kundens egenbeskyttelse > Beskytt OfficeScan klienttjenester)***
- ***Client Self-protection > Protect files in the OfficeScan client installation folder (Kundens egenbeskyttelse > Beskytt filer i OfficeScan klientinstallasjonsmappen)***
- ***Client Self-protection > Protect OfficeScan client registry keys (Kundens egenbeskyttelse > Beskytt OfficeScan klientregisternøkler)***
- ***Client Self-protection > Protect OfficeScan client processes (Kundens egenbeskyttelse > Beskytt OfficeScan klientprosesser)***

58. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
59. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Privileges and Other Settings*** (Rettigheter og andre innstillinger).
60. Velg koblingen ***Networked Computers > Client Management link*** (Datamaskiner i nettverk > Klientbehandling) fra ruten til venstre.
61. Velg ***OfficeScan Server*** (OfficeScan-server) til høyre.
62. Velg ***Additional Service Settings*** (Ytterligere serviceinnstillinger) blant alternativene under ***Settings*** (Innstillinger).
63. Fjern merkingen for alternativet ***Enable service on the following operating systems*** (Aktiver service på følgende operativsystemer).
64. Klikk på ***Apply to All Clients*** (Bruk på alle klienter).
65. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Additional Service Settings*** (Ytterligere serviceinnstillinger).
66. Velg koblingen ***Networked Computers > Global Client Settings*** (Datamaskiner i nettverk > Globale klientinnstillinger) fra ruten til venstre.
67. Merk bare av for følgende alternativer, og fjern merkingen for de gjenstående alternativene:

- ***Scan Settings (Skanneinnstillinger) > Configure Scan settings for large compressed files (Konfigurer skanneinnstillinger for store komprimerte filer).***
- ***Scan Settings (Skanneinnstillinger) > Do not scan files in the compressed file if the size exceeds 2 MB (Ikke skann filer i den komprimerte filen hvis størrelsen overskrider 2 MB).***

- ***Scan Settings (Skanneinnstillinger) > In a compressed file scan only the first 100 files (Skann bare de første 100 filene i skanningen av en komprimert fil).***
- ***Scan Settings (Skanneinnstillinger) > Exclude the OfficeScan server database folder from Real-time Scan (Utelukk databasemappen for OfficeScan-serveren fra sanntidsskanning).***
- ***Scan Settings (Skanneinnstillinger) > Exclude Microsoft Exchange server folders and files from scanning (Utelukk mapper og filer for Microsoft Exchange-serveren fra skanning)***
- ***Reserved Disk Space (Reservert diskplass) > Reserve 60 MB of disk space for updates (Reserver 60 MB diskplass for oppdateringer).***
- ***Proxy Configuration (Proxy-konfigurasjon) > Automatically detect settings (Finn innstillinger automatisk).***

MERKNAD: Det er viktig å fjerne merkingen for ***Alert Settings > Display a notification message if the client computer needs to restart to load a kernel driver*** (Varselsinnstillinger > Vis en varselmelding hvis klientdatamaskinen må startes på nytt for å laste inn en kjernedriver).

68. Klikk på ***Save*** (Lagre).
69. Velg koblingen ***Updates > Networked Computers > Manual Updates*** (Oppdateringer > Datamaskiner i nettverk > Manuelle oppdateringer) fra ruten til venstre.
70. Velg ***Manually select client*** (Velg klient manuelt), og klikk på ***Select*** (Velg).
71. Klikk på riktig domenenavn under ***OffceScan Server***.
72. Velg klientsystem ett av gangen, og klikk på ***Initiate Component Update*** (Start komponentoppdatering).
73. Klikk på ***OK*** i meldingsboksen.
74. Klikk på ***Log off*** (Logg av), og lukk OfficeScan Web Console (Webkonsoll for OfficeScan).

Retningslinjer før installering av Trend Micro OfficeScan

1. Utfør følgende trinn på Innhentingssystemet(-ene) for å konfigurere Trend Micro:
    a. Klikk på ***Start > Control Panel > Network and Sharing Center*** (Start > Kontrollpanel > Senter for nettverk og deling).
    b. Klikk på ***Change adapter settings*** (Endre innstillinger for adapter).
    c. Høyreklikk på ***Local Area Connection*** (Lokal områdetilkobling), og velg ***Properties*** (Egenskaper).
    d. Velg ***Internet Protocol Version 4 (TCP/IPv4)*** (Internettprotokollversjon 4 (TCP/IPv4), og klikk på ***Properties*** (Egenskaper).
    e. Registrer IP-adressen _____.
    f. Lukk alle åpne vinduer.
    g. Klikk på ***Start > Run*** (Start > Kjør), og tast inn **regedit**.
    h. Gå til ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.

i. Høyreklikk på et tomt felt i høyre rute, og velg ***New > String value*** (Ny > Strengverdi).

j. Tast inn **IP Template** (IP-mal) for navnet, og trykk på **Enter**.

k. Dobbeltklikk på ***IP Template*** (IP-mal)-registeret.

l. I datafeltet ***Value*** (Verdi) angir du IP-adressen for lokal områdetilkobling registrert i trinn e.

m. Klikk på ***OK***.

n. Lukk registerredigeringsverktøyet.

2. Aktiver Loopback Connection (Tilbakekobling). Se Aktivere Loopback Connection (Tilbakekobling) på side 6 hvis du vil ha mer informasjon.

3. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste etter installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.

Konfigurering av globale innstillinger for Trend Micro Global

MERKNAD: Følgende instruksjoner skal bare utføres ved bruk av CO_2-funksjonen med PDM i Mac-Lab/CardioLab-systemene. Før du fortsetter med trinnene nedenfor, må du forsikre deg om at du har kontrollert dette med IT-personell.

1. På Anti-Virus Management-konsollserveren går du til mappen ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.

2. Åpne filen ***ofcscan.ini*** i et tekstredigeringsverktøy.

3. Under delen ***Global Setting*** (Globale innstillinger) setter du verdien av følgende nøkkel til "**1**": [Global Setting] (Global innstilling) ***RmvTmTDI=1***

4. Lagre og lukk ofcscan.ini-filen.

5. Klikk på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro OfficeScan server – <servernavn> > Office Scan Web-konsoll).

6. Angi riktig brukernavn og passord, og klikk på ***Log On*** (Logg på). Skjermbildet ***Summary*** (Sammendrag) vises.

7. Klikk på ***Networked Computers > Global Client Settings*** (Datamaskiner i nettverk > Globale klientinnstillinger).

8. Klikk på ***Save*** (Lagre).

9. Velg koblingen ***Updates > Networked Computers > Manual Updates*** (Oppdateringer > Datamaskiner i nettverk > Manuelle oppdateringer) fra ruten til venstre.

10. Velg ***Manually select clients*** (Velg klienter manuelt), og klikk på ***Select*** (Velg).

11. Klikk på riktig domenenavn under ***OffceScan Server***.

12. Velg klientsystem ett av gangen, og klikk på ***Initiate Component Update*** (Start komponentoppdatering).

13. Klikk på ***OK*** i meldingsboksen.

14. Gjør følgende på hvert innhentingssystem:

a. Åpne Registerredigering.

b. Gå til ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.

c. Sørg for at registerverdien ***RmvTmTDI*** er satt til "**1**".

d. Gå til ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.

e. Slett registernøkkelen ***tmtdi*** hvis den finnes.

f. Lukk registerredigeringsverktøyet.

g. Start klientsystemene på nytt.

h. Logg på klientsystemene som administrator eller medlem av gruppen.

i. På hvert klientsystem åpner du ledeteksten med administratorrettigheter og angir ledeteksten "***sc query tmtdi***".

j. Sørg for at meldingen ***The specified service does not exist as an installed service*** (Den spesifikke tjenesten finnes ikke som en installert tjeneste) vises.

15. På Anti-Virus Management-konsollserveren klikker du på ***Log off*** (Logg av) og lukker OfficeScan Web-konsollen.

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Installer Trend Micro OfficeScan Client/Server Edition utelukkende på et nettverksbasert Mac-Lab/CardioLab-miljø. Trend Micro OfficeScan må installeres på Anti-virus Management Console-serveren (konsollserver for håndtering av antivirus) og deretter distribueres til Centricity Cardiology INW-serveren og klientene for innhentings-/gjennomgangsarbeidsstasjonene. Bruk følgende instruksjoner for å installere ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

Virusoppdateringer er institusjonens ansvar. Oppdater definisjonene regelmessig slik at du er sikker på at de nyeste virusdefinisjonene er på systemet.

Retningslinjer før installasjon

1. Trend Micro Anti-Virus Management-konsollen skal være installert i henhold til Trend Micro-instruksjoner og skal fungere ordentlig.
2. Under installering av Trend Micro OfficeScan gjør du følgende på Anti-Virus Management Console-serveren:

   a. Fjern merkingen for ***Enable firewall*** (Aktiver brannmur) i vinduet ***Anti-virus Feature*** (Antivirusfunksjon).

   b. Velg ***No, Please do not enable assessment mode*** (Nei, ikke aktiver vurderingsmodus) i vinduet ***Anti-spyware Feature*** (Anti-spionvarefunksjon).

   c. Fjern merkingen for ***Enable web reputation policy*** (Aktiver policy for nettrykte) i vinduet ***Web Reputation Feature*** (Nettryktefunksjon).
3. Trend Micro OfficeScan anbefales ikke ved bruk av CO_2-funksjonen med PDM i Mac-Lab/CardioLab-systemene.
4. Hvis Trend Micro OfficeScan er påkrevd:

a. Det anbefales å konfigurere en separat Trend Micro Anti-Virus Management-konsollserver for Mac-Lab/CardioLab-systemene. En global endring i antivirusinnstillingene er nødvendig for å bruke CO_2-funksjonen med PDM i Mac-Lab/CardioLab-systemene.

b. Hvis det ikke er mulig å konfigurere en separat Trend Micro Anti-Virus Management-konsollserver, er det nødvendig å foreta en endring i de globale innstillingene til den eksisterende Trend Micro Anti-Virus Management-konsollserveren etter installeringen. Denne endringen vil virke inn på alle klientsystemene som er koblet til den eksisterende Trend Micro Anti-Virus Management-konsollserveren, og må sjekkes med IT-personalet før du fortsetter.

5. Logg på som **Administrator** eller et medlem av gruppen på alle klientsystemer (innhenting, gjennomgang og INW-server) for å installere antivirusprogramvaren.
6. Deaktiver Loopback Connection (Tilbakekobling) Se Deaktiver tilbakekoblingen på side 6 hvis du vil ha mer informasjon.
7. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste før installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.
8. Følgende rot- og mellomliggende sertifikater kreves for installering på Innhenting-, Gjennomgang- og INW-klientmaskiner:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
9. Gjenta følgende deltrinn for å installere de fem nødvendige rot- og mellomliggende sertifikatene angitt i trinn 8.

   a. Gå til C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   MERKNAD: På INW går du til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

   b. Hvis mappebanen som er angitt ovenfor, ikke er til stede, kan du manuelt hente inn rot- og mellomliggende sertifikater som er nødvendige for installasjonen.

   c. Dobbeltklikk på ***AddTrustExternalCARoot.crt*** for å installere den på MLCL systems (Innhenting, Gjennomgang og INW).

   d. Åpne sertifikatet, og klikk på ***Install Certificate*** (Installer sertifikat).

   e. Klikk på ***Next*** (Neste) når ***Certificate Import Wizard*** (Veiviser for import av sertifikat) vises.

   f. I vinduet ***Certificate Store*** (Sertifikatlagring) velger du ***Place all certificates in the following store*** (Plasser alle sertifikater på følgende lagringssted) og klikker på ***Browse*** (Bla).

   g. Merk av ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Vis fysiske lagringssteder > Pålitelige rot-sertifiseringsmyndigheter > Lokal datamaskin), og klikk deretter på ***OK***.

   h. Klikk på ***Next*** (Neste) på ***Certificate Import Wizard*** (Veiviser for import av sertifikat).

i. Klikk på ***Finish*** (Fullfør). Meldingen ***The import was successful*** (Vellykket import) skal vises.

j. Gjenta trinn 9 for de andre sertifikatene angitt i trinn 8.

MERKNAD: Hvert av sertifikatene har en utløpsdato. Når sertifikatene har utløpt, må de fornyes og oppdateres på MLCL-systemene for å sikre at OfficeScan Agent fungerer som forventet.

Trend Micro OfficeScan – Nye trinn for installering og distribuering (foretrukket Push-installeringsmetode for 11.0 SP1)

1. Klikk på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro OfficeScan server – <servernavn> > Office Scan Web-konsoll).

MERKNAD: Fortsett ved å velge ***Continue to this website (not recommended)*** (Fortsett til dette nettstedet (anbefales ikke)). I vinduet Security Alert (Sikkerhetsvarsel) velger du ***In the future, do not show this warning*** (Ikke vis dette varselet i fremtiden) og klikker på ***OK***.

2. Hvis du mottar en sertifikatfeil som indikerer at nettstedet ikke er klarert, må du ordne sertifikatene dine slik at de omfatter Trend Micro OfficeScan.

3. Installer programvareutvidelsene ***AtxEnc*** hvis du blir bedt om det. Skjermbildet Security Warning (Sikkerhetsvarsel) vises.

   a. Klikk på ***Install*** (Installer).

4. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).

5. Klikk på ***Update Now*** (Oppdater nå) for å installere nye widgets hvis du blir bedt om det. Vent til oppdateringen av nye widgets er fullført. Skjermbildet The update is completed (Oppdateringen er fullført) vises.

   a. Klikk på ***OK***.

6. Fra menylinjen øverst klikker du på ***Agents > Agent Installation > Remote*** (Agenter > Agentinstallering > Ekstern).

7. Installer programvareutvidelsene ***AtxConsole*** hvis du blir bedt om det. Skjermbildet Security Warning (Sikkerhetsvarsel) vises.

   a. Klikk på ***Install*** (Installer).

8. Dobbeltklikk på ***OfficeScan Server*** i vinduet ***Remote Installation*** (Ekstern installering). Alle domenene vil bli angitt under ***OfficeScan Server***.

9. Dobbeltklikk på domenet (Eksempel: INW) fra listen. Alle systemene som er koblet til domenet, vises.

MERKNAD: Hvis domener eller systemer ikke er angitt på i vinduet ***Domains og Endpoints*** (Domener og endepunkter), går du til Feilsøking for domener eller systemer som ikke er angitt i vinduet for domener og endepunkter på side 75 for å legge den til manuelt eller kjører installeringen direkte fra klientmaskinen.

10. Velg klientmaskinene (Innhenting, Gjennomgang og INW-server), og klikk på ***Add*** (Legg til).

11. Tast inn <domain name>\brukernavn og passord, og klikk på ***Log on*** (Logg på).
12. Velg klientmaskinene (Innhenting, Gjennomgang og INW-server) én av gangen fra ruten ***Selected Endpoints*** (Utvalgte endepunkter), og klikk på ***Install*** (Installer).
13. Klikk på ***Yes*** (Ja) i bekreftelsesboksen.
14. Klikk på ***OK*** i meldingsboksen ***Number of clients to which notifications were sent*** (Antall klienter som varsel ble sendt til).
15. Start alle klientmaskinene (Innhenting, Gjennomgang og INW-server) på nyt, og logg på som Administrator eller et medlem av gruppen på alle klientmaskinene. Vent så til Trend Micro OfficeScan-ikonet i systemstatusfeltet blir blått med et grønt hakemerke.
16. Klikk på koblingen ***Log Off*** (Logg av) for å lukke ***OfficeScan Web Console***.

Konfigurering av serverkonsoll for Trend Micro OfficeScan 11.0 SP1

1. Velg ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro Office Scan Server <servernavn> > Office Scan Web Consol). Skjermbildet ***Trend Micro OfficeScan Login*** vises.
2. Angi riktig brukernavn og passord, og klikk på ***Login*** (Logg på). Skjermbildet ***Summary*** (Sammendrag) vises.
3. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
4. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
5. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Manual Scan Settings*** (Skanneinnstillinger > Manuelle skanneinnstillinger). Skjermbildet ***Manual Scan Settings*** (Manuelle skanneinnstillinger) vises.
6. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
   - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
   - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
   - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
   - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***
   - ***CPU Usage (CPU-bruk) > Low (Lav).***
7. Klikk på kategorien Scan Exclusion (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
   - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
   - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***

- ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
- ***Select Adds path*** (Velg Legger til bane) fra rullegardinboksen under ***Saving the officescan agent's exclusion list does the following:*** (Ved lagring av officescanagentens utelukkelsesliste skjer følgende:)
- Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** og **G:** én av gangen, og klikk på **+**.

8. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
9. Klikk på ***OK*** når du ser meldingen ***The exclusion list on this screen will replace the exclusion list on the clients eller domains you selected in the client tree earlier.*** (Utelukkelseslisten på dette skjermbildet vil erstatte utelukkelseslisten på klienter eller domener du valgte i klienttreet tidligere). ***Do you want to proceed?*** (Vil du fortsette?).
10. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Manual Scan Settings*** (Manuelle skanneinnstillinger).
11. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
12. Velg ***OfficeScan***-server til venstre.
13. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Real-time Scan Settings*** (Skanneinnstillinger > Skanneinnstillinger i sanntid). Skjermbildet ***Real-time Scan Settings*** (Skanneinnstillinger i sanntid) vises.
14. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Real-Time Scan Settings > Enable virus/malware scan. (Skanneinnstillinger i sanntid > Aktiver skanning etter virus / skadelig programvare).***
    - ***Real-Time Scan Settings > Enable spyware/grayware scan. (Skanneinnstillinger i sanntid > Aktiver skanning etter spionvare/gråvare).***
    - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
    - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
    - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
    - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Enable IntelliTrap (Aktiver IntelliTrap).***
15. Klikk på kategorien Scan Exclusion (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
    - ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***

- Sørg for at mappebanene ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** og ***G:*** er til stede i ***Exclusion List*** (Utelukkelseslisten).

16. Klikk på kategorien ***Action*** (Handling).
17. Behold standardinnstillingene, og fjern merkingen for følgende alternativer:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected. (Virus/skadelig programvare > Vis en varselmelding på endepunkter når virus/skadelig programvare registreres).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected. (Spionvare/gråvare> Vis en melding på endepunkter når spionvare/gråvare registreres).***
18. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
19. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Real-time Scan Settings*** (Innstillinger for sanntidsskanning).
20. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
21. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
22. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Scheduled Scan Settings*** (Skanneinnstillinger > Planlagte skanneinnstillinger). Skjermbildet ***Scheduled Scan Settings*** (Planlagte skanneinnstillinger) vises.
23. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scheduled Scan Settings > Enable virus/malware scan (Planlagte skanneinnstillinger > Aktiver skanning etter virus/skadelig programvare).***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan (Planlagte skanneinnstillinger > Aktiver skanning etter spionvare/gråvare).***
    - ***Schedule > Weekly, every Sunday, Start time: (Plan > Ukentlig, hver søndag, Starttid:) 00:00 hh:mm (kl. 00.00 tt:mm)***
    - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
    - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
    - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
    - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***
    - ***CPU Usage (CPU-bruk) > Low (Lav).***
24. Klikk på kategorien ***Scan Exclusion*** (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***

- ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
- Sørg for at mappebanene ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** er til stede i utelukkelseslisten.

25. Klikk på kategorien ***Action*** (Handling).
26. Behold standardinnstillingene, og fjern merkingen for følgende alternativer:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected. (Virus/skadelig programvare > Vis en varselmelding på endepunktene når virus/skadelig programvare registreres).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected. (Spionvare/Gråvare > Vis en melding på endepunktene når spionvare/gråvare registreres).***
27. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
28. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Scheduled Scan Settings*** (Planlagte skanneinnstillinger).
29. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
30. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
31. Fra ***Settings*** (Innstilinger) velger du ***Scan Settings > Scan Now Settings*** (Skanneinnstillinger > Innstillinger for Skann nå). Skjermbildet ***Scan Now Settings*** (Innstillinger for skann nå) vises.
32. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Now Settings > Enable virus/malware scan. (Innstillinger for Skann nå > Aktiver skanning etter virus/skadelig programvare).***
    - ***Scan Now Settings > Enable spyware/grayware scan. (Innstillinger for Skann nå > Aktiver skanning etter spionvare/gråvare).***
    - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
    - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
    - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
    - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***
    - ***CPU Usage (CPU-bruk) > Low (Lav).***
33. Klikk på kategorien ***Scan Exclusion*** (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***

- ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
- Sørg for at mappebanene ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** er til stede i utelukkelseslisten.

34. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
35. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Scan Now Settings*** (Innstillinger for Skann nå).
36. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
37. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
38. Velg ***Web Reputation Settings*** (Innstillinger for nettrykte) fra alternativene ***Settings*** (Innstillinger). Skjermbildet ***Web Reputation Settings*** (Innstillinger for nettrykte) vises.
39. Klikk på kategorien ***External Agents*** (Eksterne agenter), og fjern merkingen for ***Enable Web reputation policy on the following operating systems*** (Aktiver policy for nettrykte på følgende operativsystemer) hvis dette ble valgt under installeringen.
40. Klikk på kategorien ***Internal Agents*** (Interne agenter), og fjern merkingen for ***Enable Web reputation policy on the following operating systems*** (Aktiver policy for nettrykte på følgende operativsystemer) hvis dette ble valgt under installeringen.
41. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
42. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Web Reputation*** (Nettrykte).
43. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
44. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
45. Velg ***Behavior Monitoring Settings*** (Innstillinger for atferdsmonitorering) fra alternativene ***Settings*** (Innstillinger). Skjermbildet ***Behavior Monitoring Settings*** (Innstillinger for atferdsmonitorering) vises.
46. Fjern merkingen for alternativene ***Enable Malware Behavior Blocking for known og potential threats*** (Aktiver blokkering av skadelig programvare for kjente og mulige trusler) og ***Enable Event Monitoring*** (Aktiver hendelsesmonitorering).
47. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
48. Klikk på ***Close*** (Lukk) for å lukke vinduet ***Behavior Monitoring*** (Atferdsmonitorering).
49. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
50. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
51. Velg ***Device Control Settings*** (Innstilinger for enhetskontroll) blant alternativene under ***Settings*** (Innstillinger). Skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll) vises.
52. Klikk på kategorien ***External Agents*** (Eksterne agenter), og fjern merkingen for følgende alternativer:

- ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access. (Varsel > Vis en melding på endepunkter når OfficeScan registrerer uautorisert enhetstilgang).***
- ***Block the AutoRun function on USB storage devices. (Bokker AutoRun-funksjonen på USB-lagringsenheter).***

53. Klikk på kategorien ***Internal Agents*** (Interne agenter), og fjern merkingen for følgende alternativer:
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access. (Varsel > Vis en melding på endepunkter når OfficeScan registrerer uautorisert enhetstilgang).***
    - ***Block the AutoRun function on USB storage devices. (Bokker AutoRun-funksjonen på USB-lagringsenheter).***
54. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
55. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll).
56. Velg ***Device Control Settings*** (Innstilinger for enhetskontroll) igjen blant alternativene under ***Settings*** (Innstillinger). Skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll) vises.
57. Klikk på kategorien ***External Agents*** (Eksterne agenter), og fjern merkingen for ***Enable Device Control*** (Aktiver enhetskontroll).
58. Klikk på kategorien ***Internal Agents*** (Interne agenter), og fjern merkingen for ***Enable Device Control*** (Aktiver enhetskontroll).
59. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
60. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll).
61. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
62. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
63. Velg ***Privileges and Other Settings*** (Rettigheter og andre innstillinger) fra alternativene under ***Settings*** (Innstillinger).
64. Klikk på kategorien ***Privileges*** (Rettigheter). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scans (Skanning) > Configure Manual Scan Settings (Konfigurer innstillinger for manuell skanning)***
    - ***Scans (Skanning) > Configure Real-time Scan Settings (Konfigurer innstillinger for sanntidsskanning)***
    - ***Scans (Skanning) > Configure Scheduled Scan Settings (Konfigurer innstillinger for planlagt skanning)***
    - ***Proxy Settings > Allow users to configure proxy settings (Proxy-innstillinger > Tillat at brukere konfigurerer proxyinnstillinger)***
    - ***Uninstallation > Requires a passord (Avinstallering > Krever et passord)*** Angi riktig passord, og bekreft passordet.

- ***Unloading and Unlock > Requires a passord (Last av og lås opp > Krever et passord)*** Angi riktig passord, og bekreft passordet.

65. Klikk på kategorien ***Other Settings*** (Andre innstillinger).
66. Velg ***OfficeScan Agent Security Settings > Normal: (OfficeScan Agent Sikkerhetsinnstillinger > Normal:) Allow users to access OfficeScan agent files og registries*** (La brukere få tilgang til OfficeScan-agentfiler og register), og fjern merkingen for de gjenstående alternativene.

MERKNAD: Det er viktig å slette følgende alternativer.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services (OfficeScan Agent egenbeskyttelse > Beskytt Office Scan Agent-tjenester)***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder (OfficeScan Agent egenbeskyttelse > Beskytt filene i Office Scan Agent-installasjonsmappen)***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys (OfficeScan Agent egenbeskyttelse > Beskytt Office Scan Agent-registernøkler)***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes (OfficeScan Agent egenbeskyttelse > Beskytt Office Scan Agent-prosesser)***

67. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
68. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Privileges and Other Settings*** (Rettigheter og andre innstillinger).
69. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
70. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
71. Velg ***Additional Service Settings*** (Ytterligere serviceinnstillinger) blant alternativene under ***Settings*** (Innstillinger).
72. Fjern merkingen for alternativet ***Enable service on the following operating systems*** (Aktiver service på følgende operativsystemer).
73. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
74. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Additional Service Settings*** (Ytterligere serviceinnstillinger).
75. Fra den øverste ruten velger du koblingen ***Agents > Global Agent Settings*** (Agenter > Globale agentinnstillinger).
76. Merk bare av for følgende alternativer, og fjern merkingen for de gjenstående alternativene:

    - ***Scan Settings for Large Compressed Files (Skanneinnstillinger for store komprimerte filer) > Configure Scan settings for large compressed files (Konfigurer skanneinnstillinger for store komprimerte filer).***
    - ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB***. (Ikke skann filer i den komprimerte filen hvis størrelsen overskrider 2 MB). Følg dette for ***Real-Time Scan*** (Skanning i sanntid) og ***Manual Scan/ Schedule Scan/Scan Now*** (Manuell skanning/Planlagt skanning/Skann nå).
    - ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files. (Skanneinnstillinger for store komprimerte filer > Skann bare de første 100 filene i en komprimert fil)*** Følg dette for ***Real-Time Scan*** (Skanning i

sanntid) og ***Manual Scan/Schedule Scan/Scan Now*** (Manuell skanning/Planlagt skanning/Skann nå).

- ***Scan Settings (Skanneinnstillinger) > Exclude the OfficeScan server database folder from Real-time Scan (Utelukk databasemappen for OfficeScan-serveren fra sanntidsskanning).***
- ***Scan Settings (Skanneinnstillinger) > Exclude Microsoft Exchange server folders and files from scanning (Utelukk mapper og filer for Microsoft Exchange-serveren fra skanning)***
- ***Reserved Disk Space (Reservert diskplass) > Reserve 60 MB of disk space for updates (Reserver 60 MB diskplass for oppdateringer).***
- ***Proxy Configuration (Proxy-konfigurasjon) > Automatically detect settings (Finn innstillinger automatisk).***

MERKNAD: Det er viktig å slette ***Alert Settings > Display a notification message*** (Varselinnstillinger > Vis en varselmelding) hvis endepunktet må startes på nytt for å laste inn en kjernedriver.

77. Klikk på ***Save*** (Lagre).
78. Fra den øverste ruten velger du koblingen ***Updates > Agents > Manual Updates*** (Oppdateringer > Agenter > Manuell oppdatering).
79. Velg ***Manually select agents*** (Velg agenter manuelt), og klikk på ***Select*** (Velg).
80. Dobbeltklikk på riktig domenenavn under ***OffceScan Server***.
81. Velg klientsystem ett av gangen, og klikk på ***Initiate Update*** (Start oppdatering).
82. Klikk på ***OK*** i meldingsboksen.
83. Klikk på ***Log off*** (Logg av), og lukk OfficeScan Web Console (Webkonsoll for OfficeScan).

Konfigurering av globale innstillinger for Trend Micro Global

MERKNAD: Følgende instruksjoner skal bare utføres ved bruk av CO_2-funksjonen med PDM i Mac-Lab/CardioLab-systemene. Før du fortsetter med trinnene nedenfor, må du forsikre deg om at du har kontrollert dette med IT-personell.

1. På Anti-Virus Management-konsollserveren går du til mappen C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV.
2. Åpne filen ***ofcscan.ini*** i et tekstbehandlingsverktøy.
3. Under delen Global Setting (Globale innstillinger) setter du verdien av følgende nøkkel til "**1**": [Global Setting] (Global innstilling) ***RmvTmTDI=1***
4. Lagre og lukk ofcscan.ini-filen.
5. Klikk på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro OfficeScan server - <servernavn> > Office Scan Web-konsoll).
6. Angi riktig brukernavn og passord, og klikk på ***Log On*** (Logg på). Skjermbildet ***Dashboard*** (Instrumentbord) vises.
7. Klikk på ***Agents > Global Agent Settings*** (Agenter > Globale agentinnstillinger).
8. Klikk på ***Lagre***.

9. Velg koblingen ***Updates > Agents > Manual Updates*** (Oppdateringer > Agenter > Manuelle oppdateringer) fra ruten til venstre.
10. Velg ***Manually select clients*** (Velg klienter manuelt), og klikk på ***Select*** (Velg).
11. Klikk på riktig domenenavn under ***OffceScan Server***.
12. Velg klientsystem ett av gangen, og klikk på ***Initiate Update*** (Start oppdatering).
13. Klikk på ***OK*** i meldingsboksen.
14. Gjør følgende på hvert innhentingssystem:
    a. Åpne Registerredigering.
    b. Gå til ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***
    c. Sørg for at registerverdien ***RmvTmTDI*** er satt til "***1***".
    d. Gå til ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Slett registernøkkelen ***tmtdi*** hvis den finnes.
    f. Lukk registerredigeringsverktøyet.
    g. Start klientsystemene på nytt.
    h. Logg på klientsystemene som administrator eller medlem av gruppen.
    i. På hvert klientsystem åpner du ledeteksten med administratorrettigheter og angir ledeteksten "***sc query tmtdi***".
    j. Sørg for at meldingen ***The specified service does not exist as an installed service*** (Den spesifikke tjenesten finnes ikke som en installert tjeneste) vises.
15. På Anti-Virus Management-konsollserveren klikker du på ***Log off*** (Logg av) og lukker OfficeScan Web-konsollen.

Retningslinjer før installering av Trend Micro OfficeScan

1. Aktiver Loopback Connection (Tilbakekobling). Se Aktivere Loopback Connection (Tilbakekobling) på side 6 hvis du vil ha mer informasjon.
2. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste etter installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.

Trend Micro OfficeScan Client/Server Edition XG 12.0

Installasjonsoversikt

Installer Trend Micro OfficeScan Client/Server Edition utelukkende på et nettverksbasert Mac-Lab/CardioLab-miljø. Trend Micro OfficeScan må installeres på Anti-virus Management Console-serveren (konsollserver for håndtering av antivirus) og deretter distribueres til Centricity Cardiology INW-serveren og klientene for innhentings-/gjennomgangsarbeidsstasjonene. Bruk følgende instruksjoner for å installere ***Trend Micro OfficeScan Client/Server Edition XG 12.0***.

Virusoppdateringer er institusjonens ansvar. Oppdater definisjonene regelmessig slik at du er sikker på at de nyeste virusdefinisjonene er på systemet.

Retningslinjer før installasjon

MERKNAD: Internet Explorer 10 er minstekravet til IE-nettleseren som trengs for å kjøre OfficeScan Manager.

1. Trend Micro Anti-Virus Management-konsollen skal være installert i henhold til Trend Micro-instruksjoner og skal fungere ordentlig.
2. Under installering av Trend Micro OfficeScan gjør du følgende på Anti-Virus Management Console-serveren:
   a. Fjern merkingen for ***Enable firewall*** (Aktiver brannmur) i vinduet ***Anti-virus Feature*** (Antivirusfunksjon).
   b. Velg ***No, Please do not enable assessment mode*** (Nei, ikke aktiver vurderingsmodus) i vinduet ***Anti-spyware Feature*** (Anti-spionvarefunksjon).
   c. Fjern merkingen for ***Enable web reputation policy*** (Aktiver policy for nettrykte) i vinduet ***Web Reputation Feature*** (Nettryktefunksjon).
3. Logg på som **Administrator** eller et medlem av gruppen på alle klientsystemer (innhenting, gjennomgang og INW-server) for å installere antivirusprogramvaren.
4. Deaktiver Loopback Connection (Tilbakekobling) Se Deaktiver tilbakekoblingen på side 6 hvis du vil ha mer informasjon.
5. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste før installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.
6. Følgende rot- og mellomliggende sertifikater kreves for installering på Innhenting-, Gjennomgang- og INW-klientmaskiner:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
7. Gjenta følgende deltrinn for å installere de fem nødvendige rot- og mellomliggende sertifikatene angitt i trinn 6.
   a. Gå til C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   MERKNAD: På INW går du til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.
   b. Hvis mappebanen som er angitt ovenfor, ikke er til stede, kan du manuelt hente inn rot- og mellomliggende sertifikater som er nødvendige for installasjonen.
   c. Dobbeltklikk på ***AddTrustExternalCARoot.crt*** for å installere den på MLCL systems (Innhenting, Gjennomgang og INW).
   d. Åpne sertifikatet, og klikk på ***Install Certificate*** (Installer sertifikat).

e. Klikk på ***Next*** (Neste) når ***Certificate Import Wizard*** (Veiviser for import av sertifikat) vises.

f. I vinduet ***Certificate Store*** (Sertifikatlagring) velger du ***Place all certificates in the following store*** (Plasser alle sertifikater på følgende lagringssted) og klikker på ***Browse*** (Bla).

g. Merk av ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Vis fysiske lagringssteder > Pålitelige rot-sertifiseringsmyndigheter > Lokal datamaskin), og klikk deretter på ***OK***.

h. Klikk på ***Next*** (Neste) på ***Certificate Import Wizard*** (Veiviser for import av sertifikat).

i. Klikk på ***Finish*** (Fullfør). Meldingen ***The import was successful*** (Vellykket import) skal vises.

j. Gjenta trinn 7 for de andre sertifikatene angitt i trinn 6.

MERKNAD: Hvert av sertifikatene har en utløpsdato. Når sertifikatene har utløpt, må de fornyes og oppdateres på MLCL-systemene for å sikre at OfficeScan Agent fungerer som forventet.

Trend Micro OfficeScan – Nye trinn for installering og distribuering (foretrukket Push-installeringsmetode for 12.0)

1. Klikk på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro OfficeScan server – <servernavn> > Office Scan Web-konsoll).

MERKNAD: Fortsett ved å velge ***Continue to this website (not recommended)*** (Fortsett til dette nettstedet (anbefales ikke)). I vinduet Security Alert (Sikkerhetsvarsel) velger du ***In the future, do not show this warning*** (Ikke vis dette varselet i fremtiden) og klikker på ***OK***.

2. Hvis du mottar en sertifikatfeil som indikerer at nettstedet ikke er klarert, må du ordne sertifikatene dine slik at de omfatter Trend Micro OfficeScan.

3. Installer programvareutvidelsene ***AtxEnc*** hvis du blir bedt om det. Skjermbildet Security Warning (Sikkerhetsvarsel) vises.

   a. Klikk på ***Install*** (Installer).

4. Angi brukernavn og passord, og klikk på ***Log On*** (Logg på).

5. Klikk på ***Update Now*** (Oppdater nå) for å installere nye widgets hvis du blir bedt om det. Vent til oppdateringen av nye widgets er fullført. Skjermbildet The update is completed (Oppdateringen er fullført) vises.

   a. Klikk på ***OK***.

6. Fra menylinjen øverst klikker du på ***Agents > Agent Installation > Remote*** (Agenter > Agentinstallering > Ekstern).

7. Installer programvareutvidelsene ***AtxConsole*** hvis du blir bedt om det. Skjermbildet Security Warning (Sikkerhetsvarsel) vises.

   a. Klikk på ***Install*** (Installer).

8. Dobbeltklikk på ***My Company*** (Min bedrift) i vinduet ***Remote Installation*** (Ekstern installering). Alle domenene vil bli angitt under ***OfficeScan Server***.

9. Dobbeltklikk på domenet (Eksempel: INW) fra listen. Alle systemene som er koblet til domenet, vises.

MERKNAD: Hvis domener eller systemer ikke er angitt på i vinduet ***Domains og Endpoints*** (Domener og endepunkter), går du til Feilsøking for domener eller systemer som ikke er angitt i vinduet for domener og endepunkter på side 75 for å legge den til manuelt eller kjører installeringen direkte fra klientmaskinen.

10. Velg klientmaskinene (Innhenting, Gjennomgang og INW-server), og klikk på ***Add*** (Legg til).

11. Tast inn <domain name>\brukernavn og passord, og klikk på ***Log on*** (Logg på).

12. Velg klientmaskinene (Innhenting, Gjennomgang og INW-server) én av gangen fra ruten ***Selected Endpoints*** (Utvalgte endepunkter), og klikk på ***Install*** (Installer).

13. Klikk på ***Yes*** (Ja) i bekreftelsesboksen.

14. Klikk på ***OK*** i meldingsboksen ***Number of agents to which notifications were sent*** (Antall agenter som varsel ble sendt til).

15. Start alle klientmaskinene (Innhenting, Gjennomgang og INW-server) på nyt, og logg på som Administrator eller et medlem av gruppen på alle klientmaskinene. Vent så til Trend Micro OfficeScan-ikonet i systemstatusfeltet blir blått med et grønt hakemerke.

16. Klikk på koblingen ***Log Off*** (Logg av) for å lukke ***OfficeScan Web Console***.

Konfigurering av serverkonsoll for Trend Micro OfficeScan 12.0

1. Velg ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro Office Scan Server <servernavn> > Office Scan Web Consol). Skjermbildet ***Trend Micro OfficeScan Login*** vises.

2. Angi riktig brukernavn og passord, og klikk på ***Login*** (Logg på). Skjermbildet ***Summary*** (Sammendrag) vises.

3. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).

4. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.

5. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Manual Scan Settings*** (Skanneinnstillinger > Manuelle skanneinnstillinger). Skjermbildet ***Manual Scan Settings*** (Manuelle skanneinnstillinger) vises.

6. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:

   - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
   - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
   - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
   - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***

- ***CPU Usage (CPU-bruk) > Low (Lav).***

7. Klikk på kategorien Scan Exclusion (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
   - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
   - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list. (Liste over skanneutelukkelse (kataloger)) > (Utelukk kataloger der Trend Micro-produkter er installert og velg Legg til bane til utelukkelseslisten for agentdatamaskiner).***
   - ***Select Adds path*** (Velg Legger til bane) fra rullegardinboksen under ***Saving the officescan agent's exclusion list does the following:*** (Ved lagring av officescanagentens utelukkelsesliste skjer følgende:)
   - Angi mappene **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** og **G:** én av gangen, og klikk på ***Add*** (Legg til).
8. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
9. Klikk på ***OK*** når du ser meldingen ***The exclusion list on this screen will replace the exclusion list on the agents eller domains you selected in the client tree earlier.*** (Utelukkelseslisten på dette skjermbildet vil erstatte utelukkelseslisten på agenter eller domener du valgte i klienttreet tidligere). ***Do you want to proceed?*** (Vil du fortsette?).
10. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Manual Scan Settings*** (Manuelle skanneinnstillinger).
11. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
12. Velg ***OfficeScan***-server til venstre.
13. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Real-time Scan Settings*** (Skanneinnstillinger > Skanneinnstillinger i sanntid). Skjermbildet ***Real-time Scan Settings*** (Skanneinnstillinger i sanntid) vises.
14. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
   - ***Real-Time Scan Settings > Enable virus/malware scan. (Skanneinnstillinger i sanntid > Aktiver skanning etter virus / skadelig programvare).***
   - ***Real-Time Scan Settings > Enable spyware/grayware scan. (Skanneinnstillinger i sanntid > Aktiver skanning etter spionvare/gråvare).***
   - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
   - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
   - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
   - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Enable IntelliTrap (Aktiver IntelliTrap).***

15. Klikk på kategorien Scan Exclusion (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
    - ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
    - Sørg for at mappebanene ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:***\ og ***G:***\ er til stede i ***Exclusion List*** (Utelukkelseslisten).
16. Klikk på kategorien ***Action*** (Handling).
17. Behold standardinnstillingene, og fjern merkingen for følgende alternativer:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected. (Virus/skadelig programvare > Vis en varselmelding på endepunkter når virus/skadelig programvare registreres).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected. (Spionvare/gråvare> Vis en melding på endepunkter når spionvare/gråvare registreres).***
18. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
19. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Real-time Scan Settings*** (Innstillinger for sanntidsskanning).
20. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
21. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
22. Fra ***Settings*** (Innstillinger) velger du ***Scan Settings > Scheduled Scan Settings*** (Skanneinnstillinger > Planlagte skanneinnstillinger). Skjermbildet ***Scheduled Scan Settings*** (Planlagte skanneinnstillinger) vises.
23. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scheduled Scan Settings > Enable virus/malware scan (Planlagte skanneinnstillinger > Aktiver skanning etter virus/skadelig programvare).***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan (Planlagte skanneinnstillinger > Aktiver skanning etter spionvare/gråvare).***
    - ***Schedule > Weekly, every Sunday, Start time: (Plan > Ukentlig, hver søndag, Starttid:) 00:00 hh:mm (kl. 00.00 tt:mm)***
    - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
    - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
    - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
    - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***

- ***CPU Usage (CPU-bruk) > Low (Lav).***

24. Klikk på kategorien Scan Exclusion (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
    - ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
    - Sørg for at mappebanene ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** er til stede i utelukkelseslisten.
25. Klikk på kategorien ***Action*** (Handling).
26. Behold standardinnstillingene, og fjern merkingen for følgende alternativer:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected. (Virus/skadelig programvare > Vis en varselmelding på endepunktene når virus/skadelig programvare registreres).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected. (Spionvare/Gråvare > Vis en melding på endepunktene når spionvare/gråvare registreres).***
27. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
28. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Scheduled Scan Settings*** (Planlagte skanneinnstillinger).
29. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
30. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
31. Fra ***Settings*** (Innstilinger) velger du ***Scan Settings > Scan Now Settings*** (Skanneinnstillinger > Innstillinger for Skann nå). Skjermbildet ***Scan Now Settings*** (Innstillinger for skann nå) vises.
32. Klikk på kategorien ***Target*** (Mål). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Now Settings > Enable virus/malware scan. (Innstillinger for Skann nå > Aktiver skanning etter virus/skadelig programvare).***
    - ***Scan Now Settings > Enable spyware/grayware scan. (Innstillinger for Skann nå > Aktiver skanning etter spionvare/gråvare).***
    - ***Files to Scan (Filer som skal skannes) > File types scanned by IntelliScan (Filtyper skannet av IntelliScan).***
    - ***Scan Settings > Scan compressed files (Skanneinnstillinger > Skannekomprimerte filer).***
    - ***Scan Settings (Skanneinnstillinger) > Scan OLE objects (Skann OLE-objekter).***
    - ***Virus/Malware Scan settings only (Bare innstillinger for skanning etter virus / skadelig programvare) > Scan boot area (Skann oppstartsområde).***
    - ***CPU Usage (CPU-bruk) > Low (Lav).***

33. Klikk på kategorien ***Scan Exclusion*** (Skanneutelukkelser). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:
    - ***Scan Exclusion (Skanneutelukkelse) > Enable scan exclusion (Aktiver skanneutelukkelse).***
    - ***Scan Exclusion (Skanneutelukkelse) > Apply scan exclusion settings to all scan types (Bruk innstillinger for skanneutelukkelse på alle skannetyper).***
    - ***Scan Exclusion List (Directories) (Liste over skanneutelukkelse (kataloger)) > Exclude directories where Trend Micro products are installed (Utelukk kataloger der Trend Micro-produkter er installert).***
    - Sørg for at ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:***
34. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
35. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Scan Now Settings*** (Innstillinger for Skann nå).
36. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
37. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
38. Velg ***Web Reputation Settings*** (Innstillinger for nettrykte) fra alternativene ***Settings*** (Innstillinger). Skjermbildet ***Web Reputation Settings*** (Innstillinger for nettrykte) vises.
39. Klikk på kategorien ***External Clients*** (Eksterne klienter), og fjern merkingen for ***Enable Web reputation policy on the following operating systems*** (Aktiver policy for nettrykte på følgende operativsystemer) hvis dette ble valgt under installeringen.
40. Klikk på kategorien ***Internal Agents*** (Interne agenter), og fjern merkingen for ***Enable Web reputation policy on the following operating systems*** (Aktiver policy for nettrykte på følgende operativsystemer) hvis dette ble valgt under installeringen.
41. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
42. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Web Reputation*** (Nettrykte).
43. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
44. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
45. Velg ***Behavior Monitoring Settings*** (Innstillinger for atferdsmonitorering) fra alternativene ***Settings*** (Innstillinger). Skjermbildet ***Behavior Monitoring Settings*** (Innstillinger for atferdsmonitorering) vises.
46. Fjern merkingen for alternativene ***Enable Malware Behavior Blocking*** (Aktiver blokkering av skadelig programvare) og ***Enable Event Monitoring*** (Aktiver hendelsesmonitorering).
47. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
48. Klikk på ***Close*** (Lukk) for å lukke vinduet ***Behavior Monitoring*** (Atferdsmonitorering).
49. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
50. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.

51. Velg ***Device Control Settings*** (Innstilinger for enhetskontroll) blant alternativene under ***Settings*** (Innstillinger). Skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll) vises.

52. Klikk på kategorien ***External Agents*** (Eksterne agenter), og fjern merkingen for følgende alternativer:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access. (Varsel > Vis en melding på endepunkter når OfficeScan registrerer uautorisert enhetstilgang).***
    - ***Block the AutoRun function on USB storage devices. (Bokker AutoRun-funksjonen på USB-lagringsenheter).***
    - ***Enable Device Control (Aktiver enhetskontroll).***

53. Klikk på kategorien ***Internal Agents*** (Interne agenter), og fjern merkingen for følgende alternativer:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access. (Varsel > Vis en melding på endepunkter når OfficeScan registrerer uautorisert enhetstilgang).***
    - ***Block the AutoRun function on USB storage devices. (Bokker AutoRun-funksjonen på USB-lagringsenheter).***
    - ***Enable Device Control (Aktiver enhetskontroll).***

54. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).

55. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll).

56. Velg ***Device Control Settings*** (Innstilinger for enhetskontroll) igjen blant alternativene under ***Settings*** (Innstillinger). Skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll) vises.

57. Klikk på kategorien ***External Agents*** (Eksterne agenter), og fjern merkingen for ***Enable Device Control*** (Aktiver enhetskontroll).

58. Klikk på kategorien ***Internal Agents*** (Interne agenter), og fjern merkingen for ***Enable Device Control*** (Aktiver enhetskontroll).

59. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).

60. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Device Control Settings*** (Innstillinger for enhetskontroll).

61. Velg koblingen ***Agents > Agent Management*** (Agenter > Agentbehandling) fra ruten på venstre side.

62. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.

63. Velg ***Privileges and Other Settings*** (Rettigheter og andre innstillinger) fra alternativene under ***Settings*** (Innstillinger).

64. Klikk på kategorien ***Privileges*** (Rettigheter). Velg bare følgende alternativer, og fjern merkingen for de gjenstående alternativene:

    - ***Scan Privileges (Skannerettigheter) > Configure Manual Scan Settings (Konfigurer innstillinger for manuell skanning).***
    - ***Scan Privileges (Skannerettigheter) > Configure Real-time Scan Settings (Konfigurer innstillinger for sanntidsskanning).***

- ***Scan Privileges (Skannerettigheter) > Configure Scheduled Scan Settings (Konfigurer innstillinger for planlagt skanning).***
- ***Proxy Setting Privileges (Rettigheter for proxy-innstilling) > Allow the agent user to configure proxy settings (Tillat at bruker av agenten kan konfigurere proxy-innstillinger).***
- ***Uninstallation > Requires a passord (Avinstallering > Krever et passord)*** Angi riktig passord, og bekreft passordet.
- ***Unload og Unlock > Requires a passord (Last av og lås opp > Krever et passord)*** Angi riktig passord, og bekreft passordet.

65. Klikk på kategorien ***Other Settings*** (Andre innstillinger).
66. Fjern merkingen for alle alternativer.

MERKNAD: Det er viktig å slette følgende alternativer.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services (OfficeScan Agent egenbeskyttelse > Beskytt Office Scan Agent-tjenester)***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder (OfficeScan Agent egenbeskyttelse > Beskytt filene i Office Scan Agent-installasjonsmappen)***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys (OfficeScan Agent egenbeskyttelse > Beskytt Office Scan Agent-registernøkler)***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes (OfficeScan Agent egenbeskyttelse > Beskytt Office Scan Agent-prosesser)***

67. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
68. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Privileges and Other Settings*** (Rettigheter og andre innstillinger).
69. Fra den øverste ruten velger du koblingen ***Agents > Agent Management*** (Agenter > Agentadministrering).
70. Velg ***OfficeScan Server*** (OfficeScan-server) til venstre.
71. Velg ***Additional Service Settings*** (Ytterligere serviceinnstillinger) blant alternativene under ***Settings*** (Innstillinger).
72. Fjern merkingen for alternativet ***Enable service on the following operating systems*** (Aktiver service på følgende operativsystemer).
73. Klikk på ***Apply to All Agents*** (Bruk på alle klienter).
74. Klikk på ***Close*** (Lukk) for å lukke skjermbildet ***Additional Service Settings*** (Ytterligere serviceinnstillinger).
75. Fra den øverste ruten velger du koblingen ***Agents > Global Agent Settings*** (Agenter > Globale agentinnstillinger).
76. Merk bare av for følgende alternativer, og fjern merkingen for de gjenstående alternativene:

- ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB***.(Ikke skann filer i den komprimerte filen hvis størrelsen overskrider 2 MB). Følg dette for ***Real-Time Scan*** (Skanning i sanntid) og ***Manual Scan/ Schedule Scan/Scan Now*** (Manuell skanning/Planlagt skanning/Skann nå).
- ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files. (Skanneinnstillinger for store komprimerte filer > Skann bare de***

første 100 filene i en komprimert fil) Følg dette for ***Real-Time Scan*** (Skanning i sanntid) og ***Manual Scan/Schedule Scan/Scan Now*** (Manuell skanning/Planlagt skanning/Skann nå).

- ***Scan Settings (Skanneinnstillinger) > Exclude the OfficeScan server database folder from Real-time Scan (Utelukk databasemappen for OfficeScan-serveren fra sanntidsskanning).***
- ***Scan Settings (Skanneinnstillinger) > Exclude Microsoft Exchange server folders and files from scanning (Utelukk mapper og filer for Microsoft Exchange-serveren fra skanning)***

77. Klikk på ***Save*** (Lagre).
78. Fra den øverste ruten velger du koblingen ***Updates > Agents > Manual Updates*** (Oppdateringer > Agenter > Manuell oppdatering).
79. Velg ***Manually select agents*** (Velg agenter manuelt), og klikk på ***Select*** (Velg).
80. Dobbeltklikk på riktig domenenavn under ***OffceScan Server***.
81. Velg klientsystem ett av gangen, og klikk på ***Initiate Update*** (Start oppdatering).
82. Klikk på ***OK*** i meldingsboksen.
83. Klikk på ***Log off*** (Logg av), og lukk OfficeScan Web Console (Webkonsoll for OfficeScan).

Retningslinjer før installering av Trend Micro OfficeScan

1. Aktiver Loopback Connection (Tilbakekobling). Se Aktivere Loopback Connection (Tilbakekobling) på side 6 hvis du vil ha mer informasjon.
2. Konfigurer datamaskinens nettlesertjeneste. Se Konfigurer datamaskinens nettlesertjeneste etter installering av antivirusprogram på side 7 hvis du vil ha mer informasjon.

Feilsøking for domener eller systemer som ikke er angitt i vinduet for domener og endepunkter

Ved bruk av de foretrukne metodene for push-installering av både Trend Micro OfficeScan Client/Server Edition 11.0 SP1 og Trend Micro OfficeScan Client/Server Edition XG 12.0 må domenene og systemene være oppført for at installeringen skal overføres til systemet. Disse trinnene gir deg to alternativer for installering av antivirusprogramvaren på klientene (Innhenting, Gjennomgang og INW).

For 11.0 SP1 kan du se Trend Micro OfficeScan – Nye trinn for installering og distribuering (foretrukket Push-installeringsmetode for 11.0 SP1) på side 56.
For 12.0 kan du se Trend Micro OfficeScan – Nye trinn for installering og distribuering (foretrukket Push-installeringsmetode for 12.0) på side 67.

1. Bruk IP-adressene til klientmaskinene (Innhenting, Gjennomgang og INW) på administrasjonskonsollen, og gjør følgende:
   a. Angi IP for hvert av klientsystemene i boksen ***Search for endpoints*** (Finn endepunkter) ett av gangen, og trykk på ***Enter***.
   b. Angi ***<domain name>\username*** og passord, og klikk på ***Log on*** (Logg på).
   c. Velg ett av de følgende trinnene avhengig av Trend Micro-versjonen:

i. For 11.0 SP1 går du tilbake til trinn 10 på side 56.

ii. For 12.0 går du tilbake til trinn 10 på side 68.

2. Hvis du ikke kjenner til systemenes IP-adresse, eller det forrige alternativet mislykkes, går du til hver klientmaskin (Innhenting, Gjennomgang og INW-server) og gjør følgende:

   a. Logg på som **Administrator** eller et medlem av gruppen på alle klientmaskiner.

   b. Klikk på ***Start > Run*** (Start > Kjør).

   c. Tast inn ***<Anti-Virus Management Console_server_IP_address>***, og trykk på ***Enter***. Angi brukernavn og passord for administrator når du blir bedt om det.

   d. Gå til ***<Anti-Virus Management Console_server_IP _address>\ofsscan***, og dobbeltklikk på ***AutoPcc.exe***. Angi brukernavn og passord for administrator når du blir bedt om det.

   e. Start klientsystemene på nytt når installeringen er fullført.

   f. Logg på som **Administrator** eller et medlem av gruppen på alle klientmaskiner, og vent til Trend Micro OfficeScan-ikonet i systemstatusfeltet blir blått.

   g. Velg ett av de følgende trinnene avhengig av Trend Micro-versjonen:

      i. For 11.0 SP1 kan du se Konfigurering av serverkonsoll for Trend Micro OfficeScan 11.0 SP1 på side 57.

      ii. For 12.0 kan du se Konfigurering av serverkonsoll for Trend Micro OfficeScan 12.0 på side 68.