Mac-Lab/CardioLab-antivirus – Installationsvejledning (DA)

Mac-Lab/CardioLab-software version 6.9.6

Introduktion

Antivirusprogrammer understøtter institutioner i overholdelse af bestemmelser om beskyttelse af personlige oplysninger, som f.eks. HIPAA.

Brug af dokumentet

Anvend dette dokument til at installere valideret antivirussoftware på Mac-Lab/CardioLab v6.9.6-systemet.

Revisionshistorik

Revision	Dato	Kommentarer
A	16. februar 2016	Første frigivelse.
B	9. juni 2016	Trend Micro-opdatering for at understøtte CO_2.
C	16. maj 2017	Opdateringer til McAfee ePolicy Ochestrator, Trend Micro og Symantec.
D	10. juli 2017	Opdateringer til 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	Henvisninger til McAfee ePolicy Orchestrator 5.9 og McAfee VirusScan Enterprise 8.8 Patch 9 fjernet. 6.9.6 R3 UI (brugergrænseflade)-sprog tilføjet.
F	25. september 2017	Tilføjelse af McAfee ePO 5.9 og McAfee VSE 8.8 Patch 9. Opdatering af links til Trend Micro 11 og 12.

Sådan kommer du i gang

Krav til antivirus

ADVARSEL: INSTALLATION AF ANTIVIRUSPROGRAM PÅKRÆVET

Systemet leveres uden antivirusbeskyttelse. Sørg for, at der er installeret et valideret antivirusprogram på systemet, inden det tilsluttes til et netværk. Mangel på valideret virusbeskyttelse kan medføre ustabilitet i systemet eller systemfejl.

Bemærk følgende krav:

- Der leveres ikke et antivirusprogram med Mac-Lab/CardioLab-systemet, og det er kundens ansvar at anskaffe sig, installere og vedligeholde et sådant program.
- Det er kundens ansvar at opdatere antivirus-definitionsfiler.
- Hvis der opdages en virus, skal du kontakte institutionens systemadministrator og GE Teknisk Support.
- Installer kun de antivirussoftwarepakker, som er angivet i afsnittet Valideret antivirussoftware.
- Log på som administrator eller som medlem af den gruppe for at udføre aktiviteterne i dette dokument.
- Brug en sprogversion for den validerede antivirussoftware, som passer til operativsystemets sprog, hvis det er muligt. Hvis der ikke er et valideret antivirusprogram, som passer til operativsystemets sprog, skal du installere den engelske version af antivirusprogrammet.

Godkendte antivirusprogrammer

ADVARSEL: USTABILT SYSTEM

Der må ikke installeres og anvendes et ikke-valideret antivirusprogram (herunder ikke-validerede versioner). Hvis dette ikke overholdes, kan det medføre ustabilitet eller fejl i systemet. Der må kun anvendes et valideret antivirusprogram i den relevante sprogversion.

BEMÆRK: Hvis det sprogspecifikke antivirusprogram ikke er tilgængeligt, installeres den engelske version af antivirusprogrammet.

Mac-Lab/CardioLab v6.9.6-systemerne er valideret til at køre med de programmer, der er anført i følgende tabel.

Understøttet antivirusprogram	Understøttede MLCL-sprog	Understøttet antivirusprogramversion
McAfee VirusScan Enterprise	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, hollandsk, 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, hollandsk, kinesisk, japansk	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, hollandsk, 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, hollandsk, kinesisk, japansk	10.6 SP2, 11.0 SP1, XG 12.0

Det understøttede antivirusprogram kan fås på de sprog, som er angivet i følgende tabel.

MLCL-version	Understøttede MLCL-sprog
M6.9.6 R1	Dansk
M6.9.6 R2	Engelsk, fransk, tysk
M6.9.6 R3	Engelsk, fransk, tysk, italiensk, spansk, svensk, norsk, dansk, hollandsk, kinesisk, japansk

Konfiguration af antivirusadministrationskonsolserveren

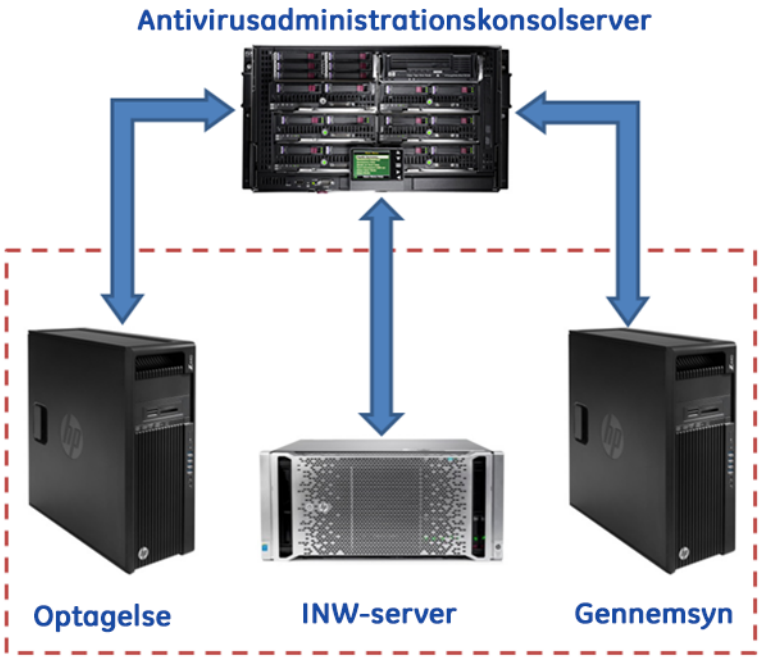
Det er påkrævet, at antivirusadministrationskonsollen skal installeres på antivirusadministrationskonsolserveren.

Kommunikation mellem antivirusadministrationskonsolserveren og Mac-Lab/CardioLab-enheder kan oprettes på forskellig vis afhængigt af det omgivende miljø:

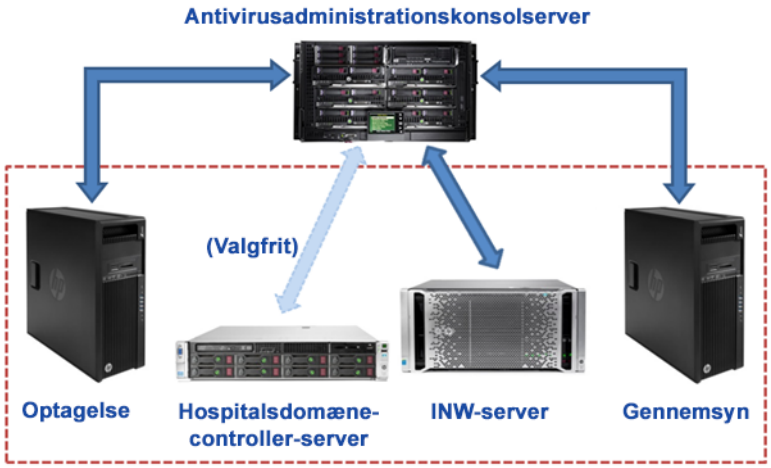
1. INW-domænecontrollermiljø - antivirusadministrationskonsolserveren findes ikke i INW-serverdomænet
   - Kommunikationstype - 1 <Samme netværk med samme undernetsmaske>
   - Kommunikationstype - 2 <Andet netværk med anden undernetsmaske>
2. Hospitalsdomænecontrollermiljø - antivirusadministrationskonsolserveren findes ikke i hospitalsdomænecontrollerdomænet
   - Kommunikationstype - 1 <Andet netværk med anden undernetsmaske>
3. Hospitalsdomænecontrollermiljø - antivirusadministrationskonsolserveren findes i hospitalsdomænecontrollerdomænet
   - Kommunikationstype - 1 <Samme netværk med samme undernetsmaske>

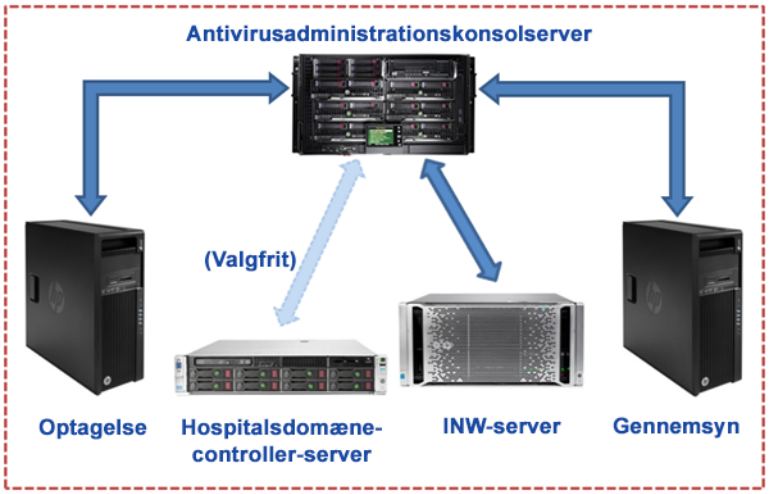
BEMÆRK: Antivirusadministrationskonsolserveren skal have to netværksporte. En netværksport til at oprette forbindelse til Centricity Cardiology INW-netværket og den anden netværksport til at oprette forbindelse til hospitalsnetværket.

Blokdiagram over INW-domænecontrollermiljøet



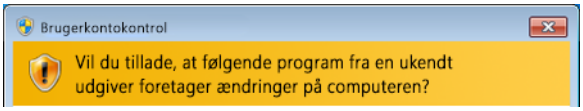
Blokdiagram over hospitalsdomænecontrollermiljøet





Brugerkontokontrol

Brugerkontokontrol er en Windows-funktion, der forhindrer ikke-autoriserede ændringer på computere. I løbet af visse procedurer i denne vejledning vises en brugerkontokontrolmeddelelse.



Når denne meddelelse vises som resultat af, at procedurerne i denne vejledning er blevet fulgt, er det sikkert at fortsætte.

Antivirus-installationsvejledning

Klik på den antivirussoftware, som du ønsker at installere:

- Symantec EndPoint Protection (12.1.2, 12.1.6 MP5 eller 14.0 MP1) på side 8
- McAfee VirusScan Enterprise på side 16
- McAfee ePolicy Orchestrator på side 21
- Trend Micro OfficeScan klient-/serverudgave 10.6 SP2 på side 44
- Trend Micro OfficeScan klient-/serverudgave 11.0 SP1 på side 54
- Trend Micro OfficeScan klient-/serverudgave XG 12.0 på side 64

Almindelige installationsprocedurer for antivirussoftware

Anvend procedurerne i dette afsnit, når de er nævnt i antivirussoftware-installationsvejledningen.

Deaktivering af tilbagekoblingsforbindelse

Deaktiver tilbagekoblingsforbindelsen på et optagesystem, som er sluttet til Mac-Lab/CardioLab-miljøet, for at se alle klientsystemer med samme undernetmaske på domænet.

1. Log på som **Administrator** eller som medlem af den gruppe.
2. Højreklik ***Network*** (Netværk) på skrivebordet, og vælg ***Properties*** (Egenskaber).
3. Klik på ***Change adapter settings*** (Rediger adapterindstillinger).
4. Højreklik på ***Loopback Connection*** (Tilbagekoblingsforbindelse), og vælg ***Disable*** (Deaktiver).
5. Genstart optagesystemet.

BEMÆRK: For at finde alle klientsystemer med samme undernetmaske på domænet, er det nødvendigt at deaktivere tilbagekoblingsforbindelsen på optagesystemet.

Aktivering af tilbagekoblingsforbindelse

Aktiver tilbagekoblingsforbindelsen på et optagesystem, der er sluttet til Mac-Lab/CardioLab-miljøet, ved at udføre følgende trin.

1. Log på som **Administrator** eller som medlem af den gruppe.
2. Højreklik ***Network*** (Netværk) på skrivebordet, og vælg ***Properties*** (Egenskaber).
3. Klik på ***Change adapter settings*** (Rediger adapterindstillinger).
4. Højreklik på ***Loopback Connection*** (Tilbagekoblingsforbindelse), og vælg ***Enable*** (Aktiver).
5. Genstart optagesystemet.

Konfiguration af tjenesten Computerbrowser før installation af antivirus

Kontrollér indstillingen af tjenesten Computerbrowser på netværksforbundne optage- og gennemsynssystemer, for at sikre at den er sat korrekt op.

1. Klik på ***Start > Control Panel > Network and Sharing Center*** (Start > Kontrolpanel > Netværks- og delingscenter).
2. Klik på ***Change advanced sharing settings*** (Rediger avancerede delingsindstillinger).
3. Udvid ***Home or Work*** (Privat eller arbejde).
4. Sørg for, at ***Turn on file and printer sharing*** (Slå fil- og printerdeling til) er markeret.
5. Klik på ***Save changes*** (Gem ændringer).
6. Klik på ***Start > Run*** (Start > Kør).
7. Indtast **services.msc** og tryk på **Enter**.
8. Dobbeltklik på tjenesten ***Computer Browser*** (Computerbrowser).
9. Sørg for, at ***Startup type*** (Starttype) er indstillet til ***Automatic*** (Automatisk). Hvis ikke den er indstillet til automatisk, skal du ændre det og klikke på ***Start***.
10. Klik på ***OK***.
11. Luk vinduet ***Services*** (Tjenester).

Konfiguration af tjenesten Computerbrowser efter installation af antivirus

Efter installation af antivirussoftwaren skal indstillingen af tjenesten Computerbrowser på netværksforbundne optage- og gennemsynssystemer kontrolleres, for at sikre at den er sat korrekt op.

1. Klik på ***Start > Run*** (Start > Kør).
2. Indtast **services.msc** og tryk på **Enter**.
3. Dobbeltklik på tjenesten ***Computer Browser*** (Computerbrowser).
4. Ændr ***Startup type*** (Starttype) til ***Manual*** (Manuel).
5. Klik på ***OK***.
6. Luk vinduet ***Services*** (Tjenester).

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

Installationsoversigt

Installer kun Symantec EndPoint Protection i et netværksforbundet Mac-Lab/CardioLab-miljø. I et netværksforbundet miljø skal Symantec EndPoint Protection installeres på antivirus-administrationskonsolserveren og derefter udrulles til Centricity Cardiology INW-serveren og gennemsyns-/optagelsesarbejdsstationerne som klienter. Brug følgende vejledning til at installere og konfigurere ***Symantec EndPoint Protection***.

Virusopdateringer er institutionens ansvar. Opdater definitionerne regelmæssigt for at sikre, at systemet har den nyeste virusbeskyttelse.

Retningslinjer inden installation

1. Symantec antivirusadministrationskonsollen forventes at være installeret i henhold til Symantecs anvisninger og at fungere korrekt.
2. Log på som **Administrator** eller som medlem af den gruppe på alle klientsystemer (optagelse, gennemsyn og INW Server) for at installere antivirussoftwaren.
3. Åbn kommandoprompten i tilstanden ***Run As Administrator*** (Kør som administrator).
4. Naviger til C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

BEMÆRK: Naviger til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec for at konfigurere INW-serveren.

5. Indtast **UpdateRegSymantec.ps1** og tryk på ***Enter***.
6. Kontrollér, at scriptet er blevet udført korrekt.

   Hvis ovennævnte mappesti ikke findes, skal følgende trin udføres for alle MLCL-systemer, undtagen MLCL 6.9.6R1 INW-serveren (Server-OS: Windows Server 2008 2008R2).

   a. Klik på knappen ***Start*** og derefter på ***Run*** (Kør).

   b. Indtast **Regedit.exe** og klik på ***OK***.

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

   d. Find og dobbeltklik på registeret ***State*** (Tilstand).

   e. Ændr ***Base*** til ***Decimal***.

   f. Ændr ***Value data*** (Værdidata) til ***146432***.

   g. Klik på ***OK***, og luk registeret.

7. Deaktiver tilbagekoblingsforbindelsen. Se Deaktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
8. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser før installation af antivirus på side 7 for yderligere oplysninger.

Symantec EndPoint Protection - nye installationsudrulningstrin (foretrukket push-installationsmetode)

1. Klik på ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager*** (Start > Alle programmer > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager).
2. Indtast brugernavn og adgangskode for at logge ind på Symantec Endpoint Protection Manager. (Klik på ***Yes*** (Ja), hvis der vises en sikkerhedsprompt).
3. Markér ***Do not show this Welcome Page again*** (Vis ikke denne velkomstside igen), og klik på ***Close*** (Luk) for at lukke velkomstsiden.

BEMÆRK: I version 14.0 MP1 skal du klikke på ***Close*** (Luk) for at lukke siden ***Getting Started on Symantec EndPoint Protection*** (Sådan kommer du i gang med Symantec EndPoint Protection).

4. Klik på ***Admin*** i vinduet ***Symantec EndPoint Protection Manager***.
5. Klik på ***Install Packages*** (Installer pakker) i den nederste rude.
6. Klik på ***Client Install Feature Set*** (Funktionssæt til klientinstallation) i den øverste rude.
7. Højreklik på vinduet ***Client Install Feature Set*** (Funktionssæt til klientinstallation), og vælg ***Add*** (Tilføj). Vinduet Add Client Install Feature Set (Tilføj funktionssæt til klientinstallation) vises.
8. Indtast det relevante navn og registrer det, da det skal bruges senere.
9. Sørg for, at ***Feature set version*** (Funktionssætversion) er ***12.1 RU2 and later*** (12.1 RU2 og senere).
10. Vælg kun følgende funktioner, og fjern markeringen fra de andre funktioner.
    - ***Virus, Spyware, and Basic Download Protection*** (Virus-, spyware- og grundlæggende download-beskyttelse).
    - ***Advanced Download Protection*** (Avanceret download-beskyttelse).
11. Klik på ***OK*** i meddelelsesboksen.
12. Kun i versionerne 12.1.2 og 12.1.6 MP5 skal du klikke på ***OK*** for at lukke vinduet ***Add Client Install Feature Set*** (Tilføj funktionssæt til klientinstallation).
13. Klik på ***Home*** (Hjem) i vinduet ***Symantec Endpoint Protection Manager***.
14. Afhængigt af softwareversion udføres en af følgende:
    - **Version 12.1.2 og 12.1.6 MP5:** Vælg ***Install protection client to computers*** (Installer beskyttelsesklient på computere) fra rullelisten ***Common Tasks*** (Almindelige opgaver) øverst til højre i vinduet ***Home*** (Hjem). Skærmbilledet Client Deployment Type (Klientudrulningstype) vises.
    - **Version 14.0 MP1:** Klik på ***Clients*** (Klienter) i vinduet ***Symantec Endpoint Protection Manager***. Klik på ***Install a client*** (Installer en klient) under ***Tasks*** (Opgaver). Skærmbilledet ***Client Deployment wizard*** (Guide til klientudrulning) vises.
15. Vælg ***New Package Deployment*** (Udrulning af ny pakke), og klik på ***Next*** (Næste).
16. Vælg funktionssættets navn, som blev oprettet i trin 8. Behold de andre indstillinger som standarder, og klik på ***Next*** (Næste).

BEMÆRK: I version 14.1 MP1 skal du under ***Scheduled Scans*** (Planlagte scanninger) fjerne markeringen fra ***Delay scheduled scans when running on batteries*** (Udsæt planlagte scanninger, når der køres på batteri) og Allow user-defined scheduled scans to run when scan author is not logged on (Tillad brugerdefinerede scanninger at køre, når scanningsforfatteren ikke er logget på).

17. Vælg ***Remote push*** (Ekstern push) og klik på ***Next*** (Næste). Vent på, at skærmbilledet ***Computer selection*** (Valg af computer) viser sig.
18. Udvid ***<Domain>*** (<Domæne>) (f. eks.: INW). Systemer, der er forbundet til domænet vises i vinduet ***Computer selection*** (Valg af computer).

BEMÆRK: Hvis ikke alle systemer genkendes, skal du klikke på ***Search Network*** (Søg i netværket) og klikke på ***Find Computers*** (Find computere). Brug detektionsmetoden ***Search by IP address*** (Søg via IP-adresse) til at identificere klientsystemerne (optagelse, gennemsyn og INW Server).

19. Vælg alle de Mac-Lab/CardioLab-klientmaskiner, der er forbundet med domænet, og klik på **>>**. Skærmbilledet ***Login Credentials*** (Logon-legimationsoplysninger) vises.
20. Indtast brugernavn, adgangskode og domæne-/computernavn, og klik på ***OK***.
21. Sørg for, at alle valgte maskiner vises under ***Install Protection Client*** (Installer beskyttelsesklient), og klik på ***Next*** (Næste).
22. Klik på ***Send*** og vent på, at Symantec-antivirussoftwaren udrulles på alle klientsystemer (optagelse, gennemsyn og INW Server). Når det er fuldført, vises siden ***Deployment Summary*** (Opsummering af udrulning).
23. Klik på ***Next*** (Næste) og derefter på ***Finish*** (Udfør) for at afslutte guiden Klientudrulning.
24. Vent på, at Symantec-ikonet vises i systembakken, og genstart derefter alle klientmaskiner (optagelse, gennemsyn og INW Server). Log på som administrator eller som et medlem af den gruppe på alle klientmaskiner efter genstart.

Symantec EndPoint Protection-serverkonsolkonfigurationer

1. Vælg ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager*** (Start > Alle programmer > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager). Logon-vinduet for Symantec EndPoint Protection Manager åbnes.
2. Indtast adgangskoden til Symantec Endpoint Protection Manager-konsollen, og klik på ***Log On*** (Log på).
3. Vælg fanen ***Policies*** (Politikker), og klik på ***Virus and Spyware Protection*** (Beskyttelse mod virus og spyware) under ***Policies*** (Politikker). Vinduet ***Virus and Spyware Protection Policies*** (Politikker for virus- og spyware-beskyttelse) åbnes.
4. Klik på ***Add a Virus and Spyware Protection Policy*** (Tilføj en virus- og spyware-beskyttelsespolitik) under ***Tasks*** (Opgaver). Vinduet ***Virus and Spyware Protection*** (Virus- og spyware-beskyttelse) åbnes.
5. Under ***Windows Settings > Scheduled Scans*** (Windows-indstillinger > Planlagte scanninger) skal du klikke på ***Administrator-Defined Scans*** (Administratordefinerede scanninger).

6. Vælg ***Daily Scheduled Scan*** (Daglig planlagt scanning), og klik på ***Edit*** (Rediger). Vinduet ***Edit Scheduled Scan*** (Rediger planlagt scanning) åbnes.
7. Ændr scanningens navn og beskrivelse til henholdsvis ***Weekly Scheduled Scan*** (Ugentlig planlagt scanning) og ***Weekly Scan at 00:00*** (Ugentlig scanning kl. 00.00).
8. Angiv ***Scan type*** (Scanningstype) som ***Full Scan*** (Fuld scanning).
9. Vælg fanen ***Schedule*** (Tidsplan).
10. Under ***Scanning Schedule*** (Tidsplan for scanning) skal du vælge ***Weekly*** (Ugentlig) og ændre tidspunktet til ***00:00***.
11. Under ***Scan Duration*** (Scanningsvarighed) skal du markere ***Randomize scan start time within this period (recommended in VMs)*** (Randomiser scanningsstarttiden indenfor denne periode (anbefales i VM'er)) og vælge ***Scan until finished (recommended to optimize scan performance)*** (Scan indtil afsluttet (anbefales for at optimere scanningsresultaterne)).
12. Under ***Missed scheduled Scans*** (Oversprungne planlagte scanninger) skal du fjerne markeringen fra ***Retry the scan within*** (Prøv scanning igen indenfor).
13. Vælg fanen ***Notifications*** (Meddelelser).
14. Fjern markeringen fra ***Display a notification message on the infected computer*** (Vis en meddelelse på den inficerede computer), og klik på ***OK***.
15. Vælg fanen ***Advanced*** (Avanceret) i vinduet ***Administrator-Defined Scans*** (Administratordefinerede scanninger).
16. Under ***Scheduled Scans*** (Planlagte scanninger) skal du fjerne markeringen fra ***Delay scheduled scans when running on batteries*** (Udskyd planlagte scanninger, når der køres på batteri), ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Tillad brugerdefinerede scanninger at køre, når scanningsforfatteren ikke er logget på) og ***Display notifications about detections when the user logs on*** (Vis meddelelser om detektioner, når brugeren logger på).

BEMÆRK: I version 14.0 MP1 skal du under ***Scheduled Scans*** (Planlagte scanninger) fjerne markeringen fra ***Delay scheduled scans when running on batteries*** (Udsæt planlagte scanninger, når der køres på batteri) og Allow user-defined scheduled scans to run when scan author is not logged on (Tillad brugerdefinerede scanninger at køre, når scanningsforfatteren ikke er logget på).

17. Under ***Startup and Triggered Scans*** (Opstart og udløste scanninger) skal du fjerne markeringen fra ***Run an Active Scan when new definitions arrive*** (Kør en aktiv scanning, når nye definitioner ankommer).
18. Under ***Windows Settings > Protection Technology*** (Windows-indstillinger > Beskyttelsesteknologi) skal du klikke på ***Auto-Protect*** (Beskyt automatisk).
19. Vælg fanen ***Scan Details*** (Scanningsdetaljer), og vælg og lås ***Enable Auto-Protect*** (Aktiver automatisk beskyttelse).
20. Vælg fanen ***Notifications*** (Meddelelser) og fjern markeringen fra og lås ***Display a notification message on the infected computer*** (Vis en meddelelse på den inficerede computer), og ***Display the Auto-Protect results dialog on the infected Computer*** (Vis resultatdialogboksen Automatisk beskyttelse på den inficerede computer).

21. Vælg fanen ***Advanced*** (Avanceret). Under ***Auto-Protect Reloading and Enablement*** (Genindlæsning og aktivering af automatisk beskyttelse) skal du låse funktionen ***When Auto-Protect is disabled, Enable after:*** (Når automatisk beskyttelse er deaktiveret, skal den aktiveres efter:).

22. Under ***Additional Options*** (Yderligere muligheder) skal du klikke på ***File Cache*** (Fil-cache). Vinduet ***File Cache*** (Fil-cache) åbnes.

23. Fjern markeringen fra ***Rescan cache when new definitions load*** (Scan cache igen, når nye definitioner indlæses), og klik på ***OK***.

24. Under ***Windows Settings > Protection Technology*** (Windows-indstillinger > Beskyttelsesteknologi) skal du klikke på ***Download Protection*** (Downloadbeskyttelse).

25. Vælg fanen ***Notifications*** (Meddelelser) og fjern markeringen fra og lås ***Display a notification message on the infected computer*** (Vis en meddelelse på den inficerede computer).

26. Under ***Windows Settings > Protection Technology*** (Windows-indstillinger > Beskyttelsesteknologi) skal du klikke på ***SONAR***.

27. Vælg fanen ***SONAR Settings*** (SONAR-indstillinger), og fjern markeringen fra og lås ***Enable SONAR*** (Aktiver SONAR).

28. Under ***Windows Settings > Protection Technology*** (Windows-indstillinger > Beskyttelsesteknologi) skal du klikke på ***Early Launch Anti-Malware Driver*** (Antimalware-driver for tidlig start).

29. Fjern markeringen fra og lås ***Enable Symantec early lauch anti-malware*** (Aktiver Symantec antimalware-driver for tidlig start).

30. Under ***Windows Settings > Email Scans*** ((Windows-indstillinger > E-mail-scanninger) skal du klikke på ***Internet Email Auto-Protect*** (Automatisk beskyttelse af internet-e-mail).

31. Vælg fanen ***Scan Details*** (Scanningsdetaljer) og fjern markeringen fra og lås ***Enable Internet Email Auto-Protect*** (Aktiver automatisk beskyttelse af internet-e-mail).

32. Vælg fanen ***Notifications*** (Meddelelser) og fjern markeringen fra og lås ***Display a notification message on the infected computer*** (Vis en meddelelse på den inficerede computer), ***Display a progress indicator when email is being sent*** (Vis en statusindikator ved afsendelse af e-mail) og ***Display a notification area icon*** (Vis et ikon i meddelelsesområdet).

33. Under ***Windows Settings > Email Scans*** (Windows-indstillinger > E-mail-scanninger) skal du klikke på ***Microsoft Outlook Auto-Protect*** (Automatisk beskyttelse af Microsoft Outlook).

34. Vælg fanen ***Scan Details*** (Scanningsdetaljer) og fjern markeringen fra og lås ***Enable Microsoft Outlook Auto-Protect*** (Aktiver automatisk beskyttelse af Microsoft Outlook).

35. Vælg fanen ***Notifications*** (Meddelelser) og fjern markeringen fra og lås ***Display a notification message on the infected computer*** (Vis en meddelelse på den inficerede computer).

36. Under ***Windows Settings > Email Scans*** (Windows-indstillinger > E-mail-scanninger) skal du klikke på ***Lotus Notes Auto-Protect*** (Automatisk beskyttelse af Lotus Notes).

37. Vælg fanen ***Scan Details*** (Scanningsdetaljer) og fjern markeringen fra og lås ***Enable Lotus Notes Auto-Protect*** (Aktiver automatisk beskyttelse af Lotus Notes).

38. Vælg fanen ***Notifications*** (Meddelelser) og fjern markeringen fra og lås ***Display a notification message on infected computer*** (Vis en meddelelse på den inficerede computer).

39. Under ***Windows Settings > Advanced Options*** (Windows-indstillinger > Avancerede funktioner) skal du klikke på ***Global Scan Options*** (Globale scanningsfunktioner).

40. Under ***Bloodhound(™) Detection Settings*** (Bloodhound(™) detektionsindstillinger) skal du fjerne markeringen fra og låse ***Enable Bloodhound(™) heuristic virus detection*** (Aktiver Bloodhound(™) heuristisk virusdetektion).

41. Under ***Windows Settings > Advanced Options*** (Windows-indstillinger > Avancerede muligheder) skal du klikke på ***Quarantine*** (Karantæne).

42. Vælg fanen ***General*** (Generelt). Under ***When New Virus Definitions Arrive*** (Når nye virusdefinitioner ankommer) skal du vælge ***Do nothing*** (Gør ingenting).

43. Under ***Windows Settings > Advanced Options*** (Windows-indstillinger > Avancerede muligheder) skal du klikke på ***Miscellaneous*** (Diverse).

44. Vælg fanen ***Notifications*** (Meddelelser) og fjern markeringen fra ***Display a notification message on the client computer when definitions are outdated*** (Vis en meddelelse på klientcomputeren, når definitioner er forældede), ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions*** (Vis en meddelelse på klientcomputeren, når Symantec Endpoint Protection kører uden virusdefinitioner) og ***Display error messages with a URL to a solution*** (Vis fejlmeddelelser med et URL til en løsning).

45. Klik på ***OK*** for at lukke vinduet ***Virus and Spyware Protection Policies*** (Politikker for virus- og spyware-beskyttelse).

46. Klik på ***Yes*** (Ja) i meddelelsesboksen ***Assign Policies*** (Tildel politikker).

47. Vælg ***My Company*** (Min virksomhed), og klik på ***Assign*** (Tildel).

48. Klik på ***Yes*** (Ja) i meddelelsesboksen.

49. Under ***Policies*** (Politikker) skal du klikke på ***Firewall***.

50. Klik på ***Firewall policy*** (Firewall-politik) under ***Firewall Policies*** (Firewall-politikker), og klik på ***Edit the policy*** (Rediger politikken) under ***Tasks*** (Opgaver).

51. Vælg fanen ***Policy Name*** (Politiknavn), og fjern markeringen fra ***Enable this policy*** (Aktiver denne politik).

52. Klik på ***OK***.

53. Under ***Policies*** (Politikker) skal du klikke på ***Intrusion Prevention*** (Indtrængningsforebyggelse).

54. Klik på politikken ***Intrusion Prevention*** (Indtrængningsforebyggelse) under ***Intrusion Prevention Policies*** (Politikker for indtrængningsforebyggelse), og klik på ***Edit the policy*** (Rediger politikken) under ***Tasks*** (Opgaver).

55. Vælg fanen ***Policy Name*** (Politiknavn), og fjern markeringen fra ***Enable this policy*** (Aktiver denne politik).

56. Afhængigt af softwareversion udføres en af følgende:

    - **Version 12.1.2:** Klik på ***Settings*** (Indstillinger) i venstre rude.

- **Version 12.1.6 MP5 og 14.0 MP1:** Klik på ***Intrusion Prevention*** (Indtrængningsforebyggelse) i venstre rude.

57. Fjern markeringen fra og lås ***Enable Network Intrusion Prevention*** (Aktiver netværks-indtrængningsforebyggelse) og ***Enable Browser Intrusion Prevention for Windows*** (Aktiver browser-indtrængningsforebyggelse for Windows).
58. Klik på ***OK***.
59. Under ***Policies*** (Politikker) skal du klikke på ***Application and Device Control*** (Kontrol af programmer og enheder).
60. Klik på ***Application and Device Control Policy*** (Politik for kontrol af programmer og enheder) under ***Application and Device Control Policies*** (Politikker for kontrol af programmer og enheder), og klik på ***Edit the policy*** (Rediger politikken) under ***Tasks*** (Opgaver).
61. Vælg fanen ***Policy Name*** (Politiknavn), og fjern markeringen fra ***Enable this policy*** (Aktiver denne politik).
62. Klik på ***OK***.
63. Under ***Policies*** (Politikker) skal du klikke på ***LiveUpdate*** (Live-opdatering).
64. Vælg ***LiveUpdate Settings policy*** (Politik for live-opdateringsindstillinger). Under ***Tasks*** (Opgaver) skal du klikke på ***Edit the policy*** (Rediger politikken).
65. Under ***Overview > Windows Settings*** (Oversigt > Windows-indstillinger skal du klikke på ***Server Settings*** (Serverindstillinger).
66. Under ***Internal or External LiveUpdate Server*** (Intern eller ekstern live-opdateringsserver) skal du sørge for, at ***Use the default management server*** (Brug standardadministrationsserveren) er markeret, og fjerne markeringen fra ***Use a LiveUpdate server*** (Brug en live-opdateringsserver).
67. Klik på ***OK***.
68. Under ***Policies*** (Politikker) skal du klikke på ***Exceptions*** (Undtagelser).
69. Klik på ***Exceptions policy*** (Politik for undtagelser). Under ***Tasks*** (Opgaver) skal du klikke på ***Edit the policy*** (Rediger politikken).
70. Afhængigt af softwareversion udføres en af følgende:
    - **Version 12.1.2 og 12.1.6 MP5:** Klik på ***Exceptions > Add > Windows Exceptions > Folder*** (Undtagelser > Tilføj > Windows-undtagelser > Mappe).
    - **Version 14.0 MP1:** Klik på rullelisten ***Add*** (Tilføj), og vælg ***Windows Exceptions > Folder*** (Windows-undtagelser > Mappe).
71. Indtast mappestierne **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:**, **G:** en ad gangen og udfør følgende:
    a. Sørg for, at ***Include subfolders*** (Inkluder undermapper) er markeret.

BEMÆRK: Klik på ***Yes*** (Ja), hvis meddelelsesboksen ***Are you sure you want to exclude all subfolders from protection?*** (Er du sikker på, at du vil udelukke alle undermapper fra beskyttelse?) vises.

    b. Vælg ***All*** (Alle) i ***Specify the type of scan that excludes this folder*** (Angiv hvilken type scanning, der udelukker denne mappe).

c. I version 14.0 MP1 skal du klikke på ***OK*** for at tilføje undtagelsen.

72. Klik på ***OK***.
73. Klik på ***Assign the policy*** (Tildel politikken) under ***Tasks*** (Opgaver).
74. Vælg ***My Company*** (Min virksomhed), og klik på ***Assign*** (Tildel).
75. Klik på ***Yes*** (Ja).
76. Klik på ***Clients*** (Klienter) i venstre rude, og vælg fanen ***Policies*** (Politikker).
77. Under ***My Company*** (Min virksomhed) skal du vælge ***Default Group*** (Standardgruppe) og fjerne markeringen fra ***Inherit policies and settings from parent group "My Company"*** (Overtag politikker og indstillinger fra overgruppen "Min virksomhed") og klikke på ***Communications Settings*** (Kommunikationsindstillinger) under ***Location-Independent Policies and Settings*** (Placerings-uafhængige politikker og indstillinger).

BEMÆRK: Hvis der vises en advarselsmeddelelse, skal du klikke på ***OK*** og klikke på ***Communications Settings*** (Kommunikationsindstillinger) under ***Location-Independent Policies and Settings*** (Placerings-uafhængige politikker og indstillinger) igen.

78. Under ***Download*** skal du sørge for, at ***Download policies and content from the management server*** (Download politikker og indhold fra administrationsserveren) er markeret, og at ***Push mode*** (Push-tilstand) er valgt.
79. Klik på ***OK***.
80. Klik på ***General Settings*** (Generelle indstillinger) under ***Location-independent Policies and Settings*** (Placerings-uafhængige politikker og indstillinger).
81. Vælg fanen ***Tamper Protection*** (Indgrebsbeskyttelse), og fjern markeringen fra og lås ***Protect Symantec security software from being tampered with or shut down*** (Beskyt Symantec-sikkerhedssoftware mod indgreb eller nedlukning).
82. Klik på ***OK***.
83. Klik på ***Admin*** og vælg ***Servers*** (Servere).
84. Under ***Servers*** (Servere) skal du vælge ***Local Site (My Site)*** (Lokal placering (Min placering)).
85. Under ***Tasks*** (Opgaver) skal du vælge ***Edit Site Properties*** (Rediger placeringsegenskaber). Vinduet ***Site Properties for Local Site (My Site)*** (Placeringsegenskaber for lokal placering (Min placering)) åbnes.
86. Vælg fanen ***LiveUpdate*** (Live-opdatering). Under ***Download Schedule*** (Downloadtidsplan) skal du sørge for, at tidsplanen er indstillet til ***Every 4 hour(s)*** (Hver 4. time).
87. Klik på ***OK***.
88. Klik på ***Log Off*** (Log af) for at lukke Symantec EndPoint Protection Manager-konsollen. Kontrollér, at Symantec Endpoint Protection-politikkerne pushes i klientsystemerne.

Symantec EndPoint Protection – retningslinjer efter installation

1. Aktiver tilbagekoblingsforbindelsen. Se Aktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
2. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser efter installation af antivirus på side 7 for yderligere oplysninger.
3. Åbn kommandoprompten i tilstanden ***Run As Administrator*** (Kør som administrator).
4. Naviger til C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

BEMÆRK: Naviger til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec for at konfigurere INW-serveren.

5. Indtast **RestoreRegSymantec.ps1** og tryk på ***Enter***.
6. Kontrollér, at scriptet er blevet udført korrekt.
   Bemærk: Du skal kontrollere, at scriptet **RestoreRegSymantec.ps1** er blevet udført korrekt, inden du fortsætter.

   Hvis ovennævnte mappesti ikke findes, skal følgende trin udføres for alle MLCL-systemer, undtagen MLCL 6.9.6R1 INW-serveren (Server-OS: Windows Server 2008 2008R2).

   a. Klik på knappen ***Start*** og derefter på ***Run*** (Kør).
   b. Indtast **Regedit.exe** og klik på ***OK***.
   c. Naviger til ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing.***
   d. Find og dobbeltklik på registeret ***State*** (Tilstand).
   e. Ændr ***Base*** til ***Decimal***.
   f. Ændr ***Value data*** (Værdidata) til ***65536***.
   g. Klik på ***OK***, og luk registeret.

McAfee VirusScan Enterprise

Installationsoversigt

McAfee VirusScan Enterprise skal installeres på et særskilt Mac-Lab/CardioLab-system, og det skal ligeledes administreres særskilt. Brug følgende vejledning til at installere og konfigurere McAfee VirusScan Enterprise.

Virusopdateringer er institutionens ansvar. Opdater definitionerne regelmæssigt for at sikre, at systemet har den nyeste virusbeskyttelse.

Installationsprocedure for McAfee VirusScan Enterprise

1. Log på som **Administrator** eller som medlem af den gruppe.
2. Sæt 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** i CD-drevet.
3. Dobbeltklik på ***SetupVSE.Exe***. Dialogboksen for Windows Defender vises.
4. Klik på ***Yes*** (Ja). Skærmbilledet McAfee VirusScan Enterprise Setup (McAfee VirusScan Enterprise-opsætning) vises.
5. Klik på ***Next*** (Næste). Skærmbilledet McAfee End User License Agreement (McAfee-slutbrugerlicensaftale) vises.
6. Læs licensaftalen, udfyld eventuelle påkrævede felter og klik på ***OK***, når du er færdig. Skærmbilledet Select Setup Type (Vælg opsætningstype) vises.
7. Vælg ***Typical*** (Typisk) og klik på ***Next*** (Næste). Skærmbilledet Select Access Protection Level (Vælg adgangsbeskyttelsesniveau) vises.
8. Vælg ***Standard Protection*** (Standardbeskyttelse), og klik på ***Next*** (Næste). Skærmbilledet Ready to Install (Klar til at installere) vises.
9. Klik på ***Install*** (Installer) og vent på, at installationen fuldføres. Efter korrekt installation af McAfee VirusScan Enterprise vises skærmbilledet ***McAfee Virus Scan Enterprise Setup has completed successfully*** (McAfee Virus Scan Enterprise-opsætningen er gennemført korrekt).
10. Fjern markeringen fra afkrydsningsfeltet ***Run On-Demand Scan*** (Kør scanning efter behov), og klik på ***Finish*** (Udfør).
11. Hvis vinduet ***Update in Progress*** (Opdatering i gang) vises, skal du klikke på ***Cancel*** (Annuller).
12. Hvis en du får en meddelelse om at genstarte systemvisninger, skal du klikke på ***OK***.
13. Genstart systemet.
14. Log på som **Administrator** eller som medlem af den gruppe.

Konfiguration af McAfee VirusScan Enterprise

1. Vælg ***Start > All Programs > McAfee > VirusScan Console*** (Start > Alle programmer > McAfee > VirusScan-konsol). Skærmbilledet ***VirusScan Console*** (VirusScan-konsol) vises.
2. Højreklik på ***Access Protection*** (Adgangsbeskyttelse) og vælg ***Properties*** (Egenskaber). Skærmbilledet med egenskaber for ***Access Protection*** (Adgangsbeskyttelse) vises.
3. Klik på fanen ***Access Protection*** (Adgangsbeskyttelse), og fjern markeringen fra ***Enable access protection*** (Aktiver adgangsbeskyttelse) og ***Prevent McAfee services from being stopped*** (Forhindr McAfee-tjenester i at blive stoppet).
4. Klik på ***OK***.

5. Højreklik på ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb), og vælg ***Properties*** (Egenskaber). Skærmbilledet ***Buffer Overflow Protection Properties*** (Egenskaber for beskyttelse mod bufferoverløb) vises.
6. Klik på fanen ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb) og fjern markeringen fra ***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings*** (Vis meddelelsesdialogboksen, når et bufferoverløb registreres under Bufferoverløbindstillinger).
7. Fjern markeringen fra ***Enable buffer overflow protection*** (Aktiver beskyttelse mod bufferoverløb) under ***Buffer overflow settings*** (Bufferoverløbindstillinger).
8. Klik på ***OK***.
9. Højreklik på ***On-Delivery Email Scanner*** (E-mail-scanning ved levering) og vælg ***Properties*** (Egenskaber). Skærmbilledet ***On-Delivery Email Scanner Properties*** (Egenskaber for e-mail-scanning ved levering) vises.
10. Klik på fanen ***Scan items*** (Scanningselementer) og fjern markeringen fra følgende muligheder under ***Heuristics*** (Heuristik):
    - ***Find unknown program threats and trojans*** (Find ukendte programtrusler og trojanske heste).
    - ***Find unknown macro threats*** (Find ukendte makro-trusler).
    - ***Find attachments with multiple extensions*** (Find vedhæftelser med flere udvidelser).
11. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
12. Vælg ***Disabled*** (Deaktiveret) for ***Sensitivity level*** (Følsomhedsniveau) under ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer)).
13. Klik på ***OK***.
14. Højreklik på ***On-Delivery Email Scanner*** (E-mail-scanning ved levering), og vælg ***Disable*** (Deaktiver).
15. Højreklik på ***On-Access Scanner*** (Scanning ved åbning), og vælg ***Properties*** (Egenskaber). Skærmbilledet ***On-Access Scan Properties*** (Egenskaber for scanning ved åbning) vises.
16. Klik på fanen ***General*** (Generelt) og vælg ***Disabled*** (Deaktiveret) for ***Sensitivity level*** (Følsomhedsniveau) under ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
17. Klik på fanen ***ScriptScan***, og fjern markeringen fra ***Enable scanning of scripts*** (Aktiver scanning af scripts).
18. Klik på fanen ***Blocking*** (Blokering) og fjern markeringen fra ***Block the connection when a threat is detected in a shared folder*** (Bloker forbindelsen, når der registreres en trussel i en delt mappe).
19. Klik på fanen ***Messages*** (Meddelelser), og fjern markeringen fra ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis meddelelsesdialogboksen ved registrering af en trussel, og vis den specificerede meddelelsestekst).
20. Klik på ***All Processes*** (Alle processer) i venstre rude.

21. Klik på fanen ***Scan Items*** (Scanningselementer) og fjern markeringen fra følgende funktioner under Heuristics (Heuristik).
    - ***Find unknown unwanted programs and trojans*** (Find ukendte, uønskede programmer og trojanske heste).
    - ***Find unknown macro threats*** (Find ukendte makro-trusler).
22. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
23. Klik på fanen ***Exclusions*** (Udeladelser), og klik på ***Exclusions*** (Udeladelser). Skærmbilledet ***Set Exclusions*** (Indstil udeladelser) vises.
24. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add Exclusion Item*** (Tilføj element til udeladelse) vises.
25. Vælg ***By name/location*** (Efter navn/placering), og klik på ***Browse*** (Gennemse). Skærmbilledet ***Browse for Files or Folders*** (Søg efter filer eller mapper) vises.
26. Naviger til mapperne ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** en ad gangen, og vælg ***OK***.
27. Vælg ***Also exclude subfolders*** (Udelad også undermapper) i vinduet ***Add Exclusion Item*** (Tilføj element til udeladelse), og klik på ***OK***.
28. Kontrollér, at mapperne C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ findes i vinduet Set Exclusions (Indstil udeladelser).
29. Klik på ***OK***.
30. Højreklik på ***AutoUpdate*** (Automatisk opdatering). og vælg ***Properties*** (Egenskaber). Skærmbilledet McAfee AutoUpdate Properties - AutoUpdate (Egenskaber for automatisk McAfee-opdatering - Automatisk opdatering) vises.
31. Fjern markeringen fra følgende muligheder under ***Update Options*** (Opdateringsmuligheder):
    - ***Get new detection engine and data if available*** (Hent ny sporingsmaskine og data, hvis de er tilgængelige).
    - ***Get other available updates (service packs, upgrades, etc.)*** (Hent andre tilgængelige opdateringer (servicepakker, opgraderinger osv.).
32. Klik på ***Schedule*** (Tidsplan). Skærmbilledet Schedule Settings (Tidsplansindstillinger) vises.
33. Fjern markeringen fra ***Enable (scheduled task runs at specified time)*** (Aktiver (planlagte opgaver kører på de angivne tidspunkter) under ***Schedule Settings*** (Tidsplanindstillinger).
34. Klik på ***OK***.
35. Klik på ***OK***.
36. Højreklik på vinduet ***VirusScan Console*** (VirusScan-konsol), og vælg ***New On-Demand Scan Task*** (Ny on demand-scanningsopgave).
37. Omdøb den nye scanning til ***Weekly Scheduled Scan*** (Ugentlig planlagt scanning). Skærmbilledet ***On-Demand Scan Properties - Weekly Scheduled Scan*** (On-demand-scanningsegenskaber - Ugentlig planlagt scanning) vises.
38. Klik på fanen ***Scan Items*** (Scanningselementer), og fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Options*** (Funktioner).
39. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

- ***Find unknown programs threats*** (Find ukendte programtrusler).
- ***Find unknown macro threats*** (Find ukendte makro-trusler).

40. Klik på fanen ***Exclusions*** (Udeladelser), og klik på ***Exclusions*** (Udeladelser). Skærmbilledet ***Set Exclusions*** (Indstil udeladelser) vises.
41. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add Exclusion Item*** (Tilføj element til udeladelse) vises.
42. Vælg ***By name/location*** (Efter navn/placering), og klik på ***Browse*** (Gennemse). Skærmbilledet ***Browse for Files or Folders*** (Søg efter filer eller mapper) vises.
43. Naviger til mapperne ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** en ad gangen, og vælg ***OK***.
44. Vælg ***Also exclude subfolders*** (Udelad også undermapper) i vinduet ***Add Exclusion Item*** (Tilføj element til udeladelse), og klik på ***OK***.
45. Kontrollér, at mapperne ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** findes i vinduet ***Set Exclusions*** (Indstil udeladelser).
46. Klik på ***OK***.
47. Klik på fanen ***Performance*** (Ydeevne) og vælg ***Disabled*** (Deaktiveret) for ***Sensitivity level*** (Følsomhedsniveau) under ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
48. Klik på ***Schedule*** (Tidsplan). Skærmbilledet ***Schedule Settings*** (Tidsplanindstillinger) vises.
49. Klik på fanen ***Task*** (Opgaver), og vælg ***Enable (scheduled task runs at specified time)*** (Aktiver (planlagte opgaver udføres på de angivne tidspunkter) under ***Schedule Settings*** (Tidsplanindstillinger).
50. Klik på fanen ***Schedule***, og vælg følgende:
    a. Kør opgaven: Ugentligt.
    b. Starttidspunkt: 24:00
    c. Hver: Uge, søndag.
51. Klik på ***OK***.
52. Klik på ***OK***.
53. Klik på ***Tools > Alerts*** (Værktøjer > Beskeder) i vinduet ***VirusScan Console*** (VirusScan-konsol). Skærmbilledet Alert Properties (Beskedegenskaber) vises.
54. Fjern markeringen i afkrydsningsfelterne ***On-Access Scan*** (Scanning ved åbning), ***On-Demand Scan and scheduled scans*** (Scanning efter behov og planlagte scanninger), ***Email Scan*** (E-mail-scanning) og ***AutoUpdate*** (Automatisk opdatering).
55. Klik på ***Destination***. Skærmbilledet ***Alert Manager Client Configuration*** (Klientkonfiguration af besked-administrator) vises.
56. Marker afkrydsningsfeltet ***Disable alerting*** (Deaktiver besked).
57. Klik på ***OK***. Skærmbilledet ***Alert Properties*** (Beskedegenskaber) vises.
58. Vælg fanen ***Additional Alerting Options*** (Flere beskedfunktioner).

59. Vælg indstillingen ***Suppress all alerts (severities 0 to 4)*** (Skjul alle beskeder (prioritet 0 til 4)) fra rullelisten ***Severity Filter*** (Prioritetsfilter).
60. Vælg fanen ***Alert Manager Alerts*** (Beskeder fra besked-administrator).
61. Fjern markeringen i afkrydsningsfeltet ***Access Protection*** (Adgangsbeskyttelse).
62. Klik på ***OK*** for at lukke vinduet ***Alert Properties*** (Beskedegenskaber).
63. Luk vinduet ***VirusScan Console*** (VirusScan-konsol).

McAfee ePolicy Orchestrator

Installationsoversigt

Installer kun ePolicy Orchestrator i et netværksforbundet Mac-Lab/CardioLab-miljø. McAfee ePolicy Orchestrator skal installeres på antivirusadministrationskonsolserveren og derefter udrulles til Centricity Cardiology INW-serveren og gennemsyns-/optagelsesarbejdsstationerne som klienter. Brug følgende vejledning til at installere og konfigurere McAfee ePolicy Orchestrator.

Anvisningerne nedenfor til pushing og konfiguration af McAfee VirusScan Enterprise understøtter Patch 4, Patch 8 og Patch 9.

Virusopdateringer er institutionens ansvar. Opdater definitionerne regelmæssigt for at sikre, at systemet har den nyeste virusbeskyttelse.

Retningslinjer inden installation

1. McAfee antivirusadministrationskonsollen forventes at være installeret i henhold til McAfees anvisninger og at fungere korrekt.
2. Log på som **Administrator** eller som medlem af den gruppe på alle klientsystemer (optagelse, gennemsyn og INW Server) for at installere antivirussoftwaren.
3. Deaktiver tilbagekoblingsforbindelsen. Se Deaktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
4. For at anvende McAfee VirusScan Enterprise 8.8 Patch 9 bedes du kontakte McAfee for kun at installere UTN-USERFirst-objekt og VeriSign Universal rodcertifikater på INW-servere. Genstart systemet, når certifikaterne er installeret.

BEMÆRK: Hvis UTN-USERFirst-objekt og VeriSign Universal rodcertifikater ikke er installeret, mislykkes installationen af McAfee VirusScan Enterprise 8.8 Patch 9 på INW-servere.

5. I tilfælde af nyinstallering skal du føje den følgende agentversion til McAfee ePolicy Orchestrators hovedlager i McAfee ePolicy Orchestrator-konsollen: ***- McAfee Agent v5.0.5.658***
6. I tilfælde af nyinstallering skal du føje den følgende pakke til McAfee ePolicy Orchestrators hovedlager i McAfee ePolicy Orchestrator-konsollen:
   - 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).

BEMÆRK: VSE880LMLRP3.zip indeholder installeringspakker for Patch 2 og Patch 3. Patch 2 er til brug med Windows 7 og Windows Server 2008 OS-platformen, og Patch 3 er til brug med Windows 8 og Windows Server 2012 OS-platformen. McAfee-installationsprogrammet installerer den korrekte patch ved at identificere Windows-operativsystemets version.

7. I tilfælde af nyinstallering skal du føje følgende udvidelser til McAfee ePolicy Orchestrators udvidelsestabel i McAfee ePolicy Orchestrator-konsollen:

   - 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

BEMÆRK: VIRUSSCAN8800(348).zip og VIRUSSCANREPORTS120(228).zip kan findes i McAfee VirusScan Enterprise 8.8 Patch 3-pakken.

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

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

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

McAfee ePolicy Orchestrator 5.0 eller 5.3.2 – nye installationsudrulningstrin (foretrukket push-installationsmetode)

1. Alt efter softwareversionen skal du vælge ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.0.0-konsol) eller ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.3.2-konsol) for at logge ind på ePolicy Orchestrator-konsollen.

BEMÆRK: Klik på ***Continue with this website*** (Fortsæt på denne webside) hvis meddelelsesboksen ***Security Alert*** (Sikkerhedsbesked) vises.

2. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).

3. Vælg ***Menu > System > System Tree*** (Menu > System > Systemtræ). Vinduet System Tree (Systemtræ) åbnes.

4. Klik på ***My Organization*** (Min organisation). Fokuser på ***My Organization*** (Min organisation) og klik på ***System Tree Actions > New Systems*** (Systemtræhandlinger > Nye systemer) i nederste venstre hjørne af af skærmen.

5. Vælg ***Push agents and add systems to the current group (My Organization)*** (Push-agenter og føj systemer til den aktuelle gruppe (Min organisation)), og klik på ***Browse*** (Gennemse) på målsystemer.

6. Indtast brugernavn og adgangskode for **domain/local administrator** (domæne-/lokaladministrator) og klik på ***OK***.

7. Vælg domænet ***INW*** fra rullelisten ***Domain*** (Domæne).

8. Vælg de af klientmaskinerne (optagelse, gennemsyn og INW Server), som er forbundet til domænet, og klik på ***OK***.

BEMÆRK: Hvis domænenavnet ikke er angivet i rullelisten ***Domain*** (Domæne), skal du gøre følgende:

- I vinduet ***Browse for Systems*** (Søg efter systemer) skal du klikke på ***Cancel*** (Annuller).
- I vinduet ***New Systems*** (Nye systemer) skal du indtaste systemnavnene på klientmaskinerne (optagelse, gennemsyn og INW Server) manuelt i feltet ***Target systems*** (Målsystemer) og fortsætte med trinnene nedenfor.

9. Vælg ***Agent Version*** (Agentversion) ***McAfee Agent for Windows 4.8.0 (Current)*** (Nuværende McAfee-agent for Windows 4.8.0) eller ***McAfee Agent for Windows 5.0.4 (Current)*** (Nuværende McAfee-agent for Windows 5.0.4). Indtast brugernavn og adgangskode for **domain administrator** (domæneadministrator), og klik på ***OK***.

10. I klientmaskinerne (optagelse, gennemsyn og INW Server) skal du kontrollere, at bibliotekerne er blevet oprettet korrekt, alt efter patch-version:

    - Verificer for patch 3 og 4, at biblioteket ***C:\Program Files\McAfee\Common Framework*** findes og at McAfee Agent er installeret i samme bibliotek.

BEMÆRK: For INW Server skal du kontrollere, at biblioteket ***C:\Program Files (x86)\McAfee\Common Framework*** findes og at McAfee Agent er installeret i samme bibliotek.

    - Verificer for patch 8, at biblioteket ***C:\Program Files\McAfee\Agent*** findes og at McAfee Agent er installeret i det samme bibliotek.

BEMÆRK: For INW Server skal du kontrollere, at biblioteket ***C:\Program Files (x86)\McAfee\Common Framework*** findes.

11. Genstart klientmaskinerne (optagelse, gennemsyn og INW Server) og log på som **domain administrator** (domæneadministrator) eller medlem af den gruppe.

12. Alt efter softwareversionen skal du klikke på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.0.0-konsol) eller ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.3.2-konsol).

13. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).

14. Klik på ***Menu > Systems > System Tree*** (Menu > Systemer > Systemtræ).

15. Klik på ***My Organization*** (Min organisation) og med fokus på ***My Organization*** (Min organisation) skal du klikke på fanen ***Assigned Client Tasks*** (Tildelte klientopgaver).

16. Klik på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tildeling af klientopgaver) nederst på skærmbilledet. Skærmbilledet Client Task Assignment Builder (Tildeling af klientopgaver - opbygning) vises.
17. Vælg følgende:
    a. **Produkt:** McAfee Agent
    b. **Opgavetype:** Produktudrulning
    c. **Opgavenavn:** Opret ny opgave
18. På skærmbilledet ***Client Task Catalog: New Task- McAfee Agent: Product Deployment*** (Klientopgavekatalog: Ny opgave - McAfee Agent: Produktudrulning) skal du udfylde felterne som følger:
    a. **Opgavenavn:** Indtast det relevante opgavenavn
    b. **Målplatforme:** Windows
    c. **Produkter og komponenter:** VirusScan Enterprise-version, som er kvalificeret til v6.9.6
    d. **Funktioner:** Kør ved hver politikhåndhævelse (kun Windows), hvis ***Options*** (Funktioner) er tilgængelig
19. Klik på ***Save*** (Gem).
20. På skærmbilledet ***1 Select Task*** (1 Vælg opgave) skal du vælge følgende:
    a. **Produkt:** McAfee Agent
    b. **Opgavetype:** Produktudrulning
    c. **Opgavenavn:** Nyligt oprettede opgavenavn
21. Klik på ***Next*** (Næste). Skærmbilledet 2 Schedule (2 Tidsplan) vises.
22. Vælg ***Run immediately*** (Kør med det samme) fra rullelisten ***Schedule type*** (Tidsplantype).
23. Klik på ***Next*** (Næste). Skærmbilledet 3 Summary (3 Opsummering) vises.
24. Klik på ***Save*** (Gem). Skærmbilledet ***System Tree*** (Systemtræ) vises.
25. Vælg fanen ***Systems*** (Systemer), og vælg derefter alle de klientmaskiner (optagelse, gennemsyn og INW Server), som er forbundet til domænet.
26. Klik på ***Wake up Agents*** (Aktiveringsagenter) nederst på vinduet.
27. Behold standardindstillingerne og klik på ***OK***.
28. Vent på, at McAfee-ikonet vises i systembakken, og genstart derefter alle klientmaskinerne (optagelse, gennemsyn og INW Server) og log på som **Administrator** eller som medlem af den gruppe på alle klientmaskinerne.
29. Klik på linket ***Log Off*** (Log af) for at lukke McAfee ePolicy Orchestrator-konsollen.

McAfee ePolicy Orchestrator 5.9.0 – nye installationsudrulningstrin (foretrukket push-installationsmetode)

1. Klik 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-konsol) for at logge på ePolicy Orchestrator-konsollen.

BEMÆRK: Klik på ***Continue with this website*** (Fortsæt på denne webside) hvis meddelelsesboksen ***Security Alert*** (Sikkerhedsbesked) vises.

2. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).
3. Vælg ***Menu > System > System Tree*** (Menu > System > Systemtræ). Vinduet ***System Tree*** (Systemtræ) åbnes.
4. Klik på ***My Organization*** (Min organisation), og fokuser på ***My Organization*** (Min organisation). Klik derefter på ***New Systems*** (Nye systemer) øverst på skærmen.
5. Vælg ***Push agents and add systems to the current group (My Organization)*** (Push-agenter og føj systemer til den aktuelle gruppe (Min organisation)), og klik på ***Browse*** (Gennemse) på målsystemer.
6. Indtast brugernavn og adgangskode for **domain/local administrator** (domæne-/lokaladministrator) og klik på ***OK***.
7. Vælg domænet ***INW*** fra rullelisten ***Domain*** (Domæne).
8. Vælg de af klientmaskinerne (optagelse, gennemsyn og INW Server), som er forbundet til domænet, og klik på ***OK***.

BEMÆRK: Hvis domænenavnet ikke er angivet i rullelisten ***Domain*** (Domæne), skal du gøre følgende:

- I vinduet ***Browse for Systems*** (Søg efter systemer) skal du klikke på ***Cancel*** (Annuller).
- I vinduet ***New Systems*** (Nye systemer) skal du indtaste systemnavnene på klientmaskinerne (optagelse, gennemsyn og INW Server) manuelt kommasepareret, i feltet ***Target systems*** (Målsystemer) og fortsætte med trinnene nedenfor.

9. Vælg ***Agent Version*** som ***McAfee Agent til Windows 5.0.5 (aktuelt)***. Indtast brugernavn og adgangskode for **domain administrator** (domæneadministrator), og klik på ***OK***.
10. I klientmaskinerne (Optagelse, Gennemsyn og INW-Server) skal det bekræftes, at mappen ***C:\Program Files\McAfee\Agent*** er oprettet korrekt.
11. Genstart klientmaskinerne (optagelse, gennemsyn og INW Server) og log på som **domain administrator** (domæneadministrator) eller medlem af den gruppe.
12. Klik 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-konsol) for at logge på ePolicy Orchestrator-konsollen.
13. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).
14. Klik på ***Menu > Systems > System Tree*** (Menu > Systemer > Systemtræ).

15. Klik på ***My Organization*** (Min organisation) og med fokus på ***My Organization*** (Min organisation) skal du klikke på fanen ***Assigned Client Tasks*** (Tildelte klientopgaver).
16. Klik på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tildeling af klientopgaver) nederst på skærmbilledet. Skærmbilledet ***Client Task Assignment Builder*** (Tildeling af klientopgaver - opbygning) vises.
17. Vælg følgende:
    a. **Produkt:** McAfee Agent
    b. **Opgavetype:** Produktudrulning
18. Klik ***Task Actions > Create New Task*** (Opgavehandlinger > Opret ny opgave). Skærmbilledet ***Create New Task*** (Opret ny opgave) vises.
19. På skærmbilledet ***Create New Task*** (Opret ny opgave) skal du udfylde felterne som følger:
    a. **Opgavenavn:** Indtast det relevante opgavenavn
    b. **Målplatforme:** Windows (fjern markeringen fra alle andre indstillinger)
    c. **Produkter og komponenter:** VirusScan Enterprise 8.8.0.1804
20. Klik på ***Save*** (Gem). Skærmbilledet ***Client Task Assignment Builder*** (Tildeling af klientopgaver - opbygning) vises.
21. I skærmbilledet ***Client Task Assignment Builder*** (Tildeling af klientopgaver - opbygning) skal du vælge følgende:
    a. **Produkt:** McAfee Agent
    b. **Opgavetype:** Produktudrulning
    c. **Opgavenavn:** Nyligt oprettede opgavenavn
    d. **Plantype:** Kør straks
22. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Client Tasks*** (Tildelte klientopgaver) vises.
23. Vælg fanen ***Systems*** (Systemer), og vælg derefter alle de klientmaskiner (optagelse, gennemsyn og INW Server), som er forbundet til domænet.
24. Klik på ***Wake up Agents*** (Aktiveringsagenter) nederst på vinduet.
25. Behold standardindstillingerne og klik på ***OK***.
26. Vent på, at McAfee-ikonet vises i systembakken, og genstart derefter alle klientmaskinerne (optagelse, gennemsyn og INW Server) og log på som **Administrator** eller som medlem af den gruppe på alle klientmaskinerne.
27. Klik på linket ***Log Off*** (Log af) for at lukke McAfee ePolicy Orchestrator-konsollen.

Konfiguration af McAfee ePolicy Orchestrator 5.0- og 5.3.2-serverkonsol

1. Alt efter softwareversionen skal du klikke på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.0.0-konsol) eller ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee***

ePolicy Orchestrator 5.3.2 Console (Start > Alle programmer > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 5.3.2-konsol).

2. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).
3. Klik på ***Menu > Systems > System Tree*** (Menu > Systemer > Systemtræ).
4. Klik på ***My Organization*** (Min organisation) og med fokus på My Organization (Min organisation) skal du klikke på fanen ***Assigned Client Tasks*** (Tildelte klientopgaver).
5. Klik på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tildeling af klientopgaver) nederst på skærmbilledet. Skærmbilledet ***Client Task Assignment Builder*** (Tildeling af klientopgaver - opbygning) vises.
6. Vælg følgende:
   a. ***Produkt:*** VirusScan Enterprise 8.8.0
   b. ***Opgavetype:*** Scanning efter behov
   c. ***Opgavenavn:*** Opret ny opgave
7. På skærmbilledet ***Client Task Catalog: New Task - VirusScan Enterprise 8.8.0: On Demand Scan*** (Klientopgavekatalog: Ny opgave - VirusScan Enterprise 8.8.0: Scanning efter behov) skal du udfylde felterne som følger:
   a. ***Opgavenavn:*** Ugentlig planlagt scanning
   b. ***Beskrivelse:*** Ugentlig planlagt scanning
8. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
9. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Options*** (Funktioner).
10. Fjern markeringen fra følgende funktioner under Heuristics (Heuristik):
    - ***Find unknown program threats (Find ukendte programtrusler).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
11. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.
12. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.
13. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg Also exclude subfolders (Udelad også undermenuer). Klik på ***OK***.
14. Klik på fanen ***Performance*** (Ydeevne). Skærmbilledet ***Performance*** (Ydeevne) vises.
15. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
16. Klik på ***Save*** (Gem).
17. På skærmbilledet ***1 Select Task*** (1 Vælg opgave) skal du vælge følgende:
    - ***Produkt:*** VirusScan Enterprise 8.8.0

- ***Opgavetype:*** Scanning efter behov
- ***Opgavenavn:*** Ugentlig planlagt scanning

18. Klik på ***Next*** (Næste). Skærmbilledet ***2 Schedule*** (2 Tidsplan) vises.
19. Vælg ***Weekly*** (Ugentlig) fra rullelisten ***Scheduled type*** (Planlagte type), og vælg ***Sunday*** (Søndag).
20. Indstil ***Start time*** (Starttid) til ***12:00 AM*** (Kl. 24:00), og vælg ***Run Once at that time*** (Kør én gang på dette tidspunkt).
21. Klik på ***Next*** (Næste). Skærmbilledet ***3 Summary*** (3 Opsummering) vises.
22. Klik på ***Save*** (Gem). Skærmbilledet ***System Tree*** (Systemtræ) vises.
23. Vælg fanen ***Assigned Policies*** (Tildelte politikker). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.
24. Fra rullelisten ***Product*** (Produkt) skal du vælge ***VirusScan Enterprise 8.8.0***.
25. Klik på ***My Default*** (Min standard) for ***On-Access General Policies*** (Generelle politikker for ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** (VirusScan Enterprise 8.8.0 > Generelle politikker for ved åbning > Min standard) vises.
26. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***General*** (Generelt). Skærmbilledet ***General*** (Generelt) vises.
27. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
28. Klik på fanen ***ScriptScan*** (Script-scanning). Skærmbilledet ***Script Scan*** (Script-scanning) vises.
29. Fjern markeringen fra ***Enable scanning of scripts*** (Aktiver scanning af scripts).
30. Klik på fanen ***Blocking*** (Blokering). Skærmbilledet ***Blocking*** (Blokering) vises.
31. Fjern markeringen fra ***Block the connection when a threatened file is detected in a shared folder*** (Bloker forbindelsen, når en truet fil registreres i en delt mappe).
32. Klik på fanen ***Messages*** (Meddelelser). Skærmbilledet ***Messages*** (Meddelelser) vises.
33. Fjern markeringen fra ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis meddelelsesdialogboksen ved registrering af en trussel, og vis den specificerede meddelelsestekst).
34. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og klik på fanen ***General*** (Generelt). Skærmbilledet ***General*** (Generelt) vises.
35. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
36. Klik på fanen ***ScriptScan*** (Script-scanning). Skærmbilledet ***Script Scan*** (Script-scanning) vises.
37. Kontrollér, at markeringen er fjernet fra ***Enable scanning of scripts*** (Aktiver scanning af scripts).
38. Klik på fanen ***Blocking*** (Blokering). Skærmbilledet ***Blocking*** (Blokering) vises.

39. Fjern markeringen fra ***Block the connection when a threatened file is detected in a shared folder*** (Bloker forbindelsen, når en truet fil registreres i en delt mappe).

40. Klik på fanen ***Messages*** (Meddelelser). Skærmbilledet ***Messages*** (Meddelelser) vises.

41. Fjern markeringen fra ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis meddelelsesdialogboksen ved registrering af en trussel, og vis den specificerede meddelelsestekst).

42. Klik på ***Save*** (Gem).

43. Klik på ***My Default*** (Min standard) for ***On-Access Default Processes Policies*** (Standardprocespolitikker ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Standardprocespolitikker ved åbning > Min standard) vises.

44. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

45. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

46. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

47. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

48. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.

49. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.

50. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

51. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

52. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

53. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

54. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.

55. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.

56. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

57. Klik på ***Save*** (Gem).
58. Klik på ***My Default*** (Min standard) for ***On-Access Low-Risk Processes Policies*** (Lavrisiko-procespolitikker ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Lavrisiko-procespolitikker ved åbning > Min standard) vises.
59. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).
60. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
61. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
62. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
63. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.
64. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.
65. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.
66. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
67. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
68. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
69. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.
70. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.
71. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.
72. Klik på ***Save*** (Gem).
73. Klik på ***My Default*** (Min standard) for ***On-Access High-Risk Processes Policies*** (Højrisiko-procespolitikker ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Højrisiko-procespolitikker ved åbning > Min standard) vises.
74. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

75. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

76. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

77. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

78. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.

79. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.

80. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

81. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

82. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

83. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

84. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.

85. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.

86. Vælg By pattern (Efter mønster) og gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

87. Klik på ***Save*** (Gem).

88. Klik på ***My Default*** (Min standard) for ***On Delivery Email Scan Policies*** (Politikker for e-mail-scanning ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker for e-mail-scanning ved åbning) vises.

89. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

90. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

91. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown program threats and trojans (Find ukendte programtrusler og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

- ***Find attachments with multiple extensions (Find vedhæftelser med flere udvidelser).***

92. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
93. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
94. Fjern markeringen fra ***Enable on-delivery email scanning*** (Aktiver e-mail-scanning ved åbning) under ***Scanning of email*** (E-mail-scanning).
95. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).
96. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
97. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):
    - ***Find unknown program threats and trojans (Find ukendte programtrusler og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
    - ***Find attachments with multiple extensions (Find vedhæftelser med flere udvidelser).***
98. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
99. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
100. Fjern markeringen fra ***Enable on-delivery email scanning*** (Aktiver e-mail-scanning ved åbning) under ***Scanning of email*** (E-mail-scanning).
101. Klik på ***Save*** (Gem).
102. Klik på ***My Default*** (Min standard) for ***General Options Policies*** (Politikker for generelle funktioner). Skærmbilledet ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker for generelle funktioner > Min standard) vises.
103. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).
104. Klik på fanen ***Display Options*** (Visningsindstillinger). Skærmbilledet ***Display Options*** (Visningsindstillinger) vises.
105. Vælg følgende under ***Console options*** (Konsolindstillinger):
    - ***Display managed tasks in the client console (Vis håndterede opgaver i klientkonsollen).***
    - ***Disable default AutoUpdate task schedule (Deaktiver standard-opgavetidsplanen for automatisk opdatering).***
106. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).
107. Klik på fanen ***Display Options*** (Visningsindstillinger). Skærmbilledet ***Display Options*** (Visningsindstillinger) vises.

108. Vælg følgende under ***Console options*** (Konsolindstillinger):
    - ***Display managed tasks in the client console (Vis håndterede opgaver i klientkonsollen).***
    - ***Disable default AutoUpdate task schedule (Deaktiver standard-opgavetidsplanen for automatisk opdatering).***
109. Klik på ***Save*** (Gem).
110. Klik på ***My Default*** (Min standard) for ***Alert Policies*** (Beskedpolitikker). Skærmbilledet ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Ædr politikker > Min standard) vises.
111. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).
112. Vælg fanen ***Alert Manager Alerts*** (Beskeder fra besked-administrator). Skærmbilledet ***Alert Manager Alerts*** (Beskeder fra besked-administrator) vises.
113. Fjern markeringen fra ***On-Access Scan*** (Scanning ved åbning), ***On-Demand Scan and scheduled scans*** (Scanning efter behov og planlagte scanninger), ***Email Scan*** (E-mail-scanning) og ***AutoUpdate*** (Automatisk opdatering), som alle ligger under ***Components that generate alerts*** (Komponenter, der genererer beskeder).
114. Vælg ***Disable alerting*** (Deaktiver beskeder) under indstillingerne for ***Alert Manager*** (Besked-administrator).
115. Fjern markeringen fra ***Access Protection*** (Adgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter, der genererer beskeder).
116. Klik på ***Additional Alerting Options*** (Flere beskedfunktioner). Skærmbilledet ***Additional Alerting Options*** (Flere beskedfunktioner) vises.
117. Fra rullelisten ***Severity Filters*** (Prioritetsfiltre) skal du vælge ***Suppress all alerts (severities 0 to 4)*** (Skjul alle beskeder (prioritet 0 til 4)).
118. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Alert Manager Alerts*** (Beskeder fra besked-administrator). Skærmbilledet ***Alert Manager Alerts*** (beskeder fra Besked-administrator) vises.
119. Fjern markeringen fra ***On-Access Scan*** (Scanning ved åbning), ***On-Demand Scan and scheduled scans*** (Scanning efter behov og planlagte scanninger), ***Email Scan*** (E-mail-scanning) og ***AutoUpdate*** (Automatisk opdatering), som alle ligger under ***Components that generate alerts*** (Komponenter, der genererer beskeder).
120. Markér ***Disable alerting*** (Deaktiver beskeder) under indstillingerne for ***Alert Manager*** (Besked-administrator).
121. Fjern markeringen fra ***Access Protection*** (Adgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter, der genererer beskeder).
122. Klik på ***Additional Alerting Options*** (Flere beskedfunktioner). Skærmbilledet Additional Alerting Options (Flere beskedfunktioner) vises.
123. Fra rullelisten ***Severity Filters*** (Prioritetsfiltre) skal du vælge ***Suppress all alerts (severities 0 to 4)*** (Skjul alle beskeder (prioritet 0 til 4)).
124. Klik på ***Save*** (Gem).

125. Klik på ***My Default*** (Min standard) for ***Access Protection Policies*** (Politikker for adgangsbeskyttelse). Skærmbilledet ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker for adgangsbeskyttelse > Min standard) vises.

126. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

127. Klik på fanen ***Access Protection*** (Adgangsbeskyttelse). Skærmbilledet ***Access Protection*** (Adgangsbeskyttelse) vises.

128. Fjern markeringen fra følgende funktioner under ***Access protection settings*** (Indstillinger for adgangsbeskyttelse):

    - ***Enable access protection (Aktiver adgangsbeskyttelse).***
    - ***Prevent McAfee services from being stopped (Forhindr McAfee-tjenester i at blive stoppet).***

129. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).

130. Klik på fanen ***Access Protection*** (Adgangsbeskyttelse). Skærmbilledet ***Access Protection*** (Adgangsbeskyttelse) vises.

131. Fjern markeringen fra følgende funktioner under ***Access protection settings*** (Indstillinger for adgangsbeskyttelse):

    - ***Enable access protection (Aktiver adgangsbeskyttelse).***
    - ***Prevent McAfee services from being stopped (Forhindr McAfee-tjenester i at blive stoppet).***

132. Klik på ***Save*** (Gem).

133. Klik på ***My Default*** (Min standard) for ***Buffer Overflow Protection Policies*** (Politikker til beskyttelse mod bufferoverløb). Skærmbilledet ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker til beskyttelse mod bufferoverløb > Min Standard) vises.

134. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

135. Klik på fanen ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb). Skærmbilledet ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb) vises.

136. Fjern markeringen fra ***Show the message dialog box when a buffer overflow is detected*** (Vis meddelelsesdialogboksen ved registrering af et bufferoverløb) under ***Client system warning*** (Klientsystemadvarsler).

137. Fjern markeringen fra ***Enable buffer overflow protection*** (Aktiver beskyttelse mod bufferoverløb) under ***Buffer overflow settings*** (Bufferoverløbindstillinger).

138. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).

139. Klik på fanen ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb). Skærmbilledet ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb) vises.

140. Fjern markeringen fra ***Show the message dialog box when a buffer overflow is detected*** (Vis meddelelsesdialogboksen ved registrering af et bufferoverløb) under ***Client system warning*** (Klientsystemadvarsler).

141. Fjern markeringen fra ***Enable buffer overflow protection*** (Aktiver beskyttelse mod bufferoverløb) under ***Buffer overflow settings*** (Bufferoverløbindstillinger).

142. Klik på ***Save*** (Gem).

143. Fra rullelisten ***Product*** (Produkt) vælges ***McAfee Agent***. Vinduet ***Policies*** (Politikker) for McAfee Agent åbnes.

144. Klik på ***My Default*** (Min standard) for ***Repository*** (Lager). Skærmbilledet ***McAfee Agent > Repository > My Default*** (McAfee Agent > Lager > Min standard) vises.

145. Klik på fanen ***Proxy***. Skærmbilledet ***Proxy*** vises.

146. Vælg ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Brug Internet Explorer-indstillinger (Windows)/Systempræferenceindstillinger (Mac OSX)) under ***Proxy settings*** (Proxy-indstillinger).

147. Klik på ***Save*** (Gem).

148. Klik på fanen ***Systems*** (Systemer).

149. Vælg alle klientens systemer (Optagelse, Gennemsyn og Centricity Cardiology INW-server), hvorpå de konfigurerede politikker skal anvendes.

150. Vælg ***Wake Up Agents*** (Aktiveringsagenter). Skærmbilledet ***Wake Up Agent*** (Aktiveringsagent) vises.

151. Klik på ***OK***.

152. Log af ePolicy Orchestrator.

McAfee ePolicy Orchestrator 5.9.0-serverkonsolkonfiguration

1. Klik 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-konsol) afhængigt af softwareversionen.
2. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).
3. Klik på ***Menu > Systems > System Tree*** (Menu > Systemer > Systemtræ).
4. Klik på ***My Organization*** (Min organisation) og med fokus på My Organization (Min organisation) skal du klikke på fanen ***Assigned Client Tasks*** (Tildelte klientopgaver).
5. Klik på knappen ***Actions > New Client Task Assignment*** (Handlinger > Ny tildeling af klientopgaver) nederst på skærmbilledet. Skærmbilledet ***Client Task Assignment Builder*** (Tildeling af klientopgaver - opbygning) vises.
6. Vælg følgende:
    a. ***Produkt:*** VirusScan Enterprise 8.8.0
    b. ***Opgavetype:*** Scanning efter behov
7. Klik på ***Create New Task*** (Opret ny opgave) under ***Task Actions*** (Opgavehandlinger). ***Create New Task*** (Opret ny opgave) vises.
8. På ***Create New Task*** (Opret ny opgave) skal du udfylde felterne som følger:
    a. ***Opgavenavn:*** Ugentlig planlagt scanning
    b. ***Beskrivelse:*** Ugentlig planlagt scanning

9. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
10. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Options*** (Funktioner).
11. Fjern markeringen fra følgende funktioner under Heuristics (Heuristik):
    - ***Find unknown program threats (Find ukendte programtrusler).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
12. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.
13. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.
14. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg Also exclude subfolders (Udelad også undermenuer). Klik på ***OK***.
15. Klik på fanen ***Performance*** (Ydeevne). Skærmbilledet ***Performance*** (Ydeevne) vises.
16. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
17. Klik på ***Save*** (Gem). Skærmbilledet ***Client Task Assignment Builder*** (Tildeling af klientopgaver - opbygning) vises.
18. I skærmbilledet ***Client Task Assignment Builder*** (Tildeling af klientopgaver - opbygning) skal du vælge følgende:
    - ***Produkt:*** VirusScan Enterprise 8.8.0
    - ***Opgavetype:*** Scanning efter behov
    - ***Opgavenavn:*** Ugentlig planlagt scanning
19. Vælg ***Weekly*** (Ugentlig) fra rullelisten ***Scheduled type*** (Planlagte type), og vælg ***Sunday*** (Søndag).
20. Indstil ***Start time*** (Starttid) til ***12:00 AM*** (Kl. 24:00), og vælg ***Run Once at that time*** (Kør én gang på dette tidspunkt).
21. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Client Tasks*** (Tildelte klientopgaver) vises.
22. Vælg fanen ***Assigned Policies*** (Tildelte politikker). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.
23. Fra rullelisten ***Product*** (Produkt) skal du vælge ***VirusScan Enterprise 8.8.0***.
24. Klik på ***My Default*** (Min standard) for ***On-Access General Policies*** (Generelle politikker for ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** (VirusScan Enterprise 8.8.0 > Generelle politikker for ved åbning > Min standard) vises.
25. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***General*** (Generelt). Skærmbilledet ***General*** (Generelt) vises.
26. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).

27. Klik på fanen ***ScriptScan*** (Script-scanning). Skærmbilledet ***Script Scan*** (Script-scanning) vises.
28. Fjern markeringen fra ***Enable scanning of scripts*** (Aktiver scanning af scripts).
29. Klik på fanen ***Blocking*** (Blokering). Skærmbilledet ***Blocking*** (Blokering) vises.
30. Fjern markeringen fra ***Block the connection when a threatened file is detected in a shared folder*** (Bloker forbindelsen, når en truet fil registreres i en delt mappe).
31. Klik på fanen ***Messages*** (Meddelelser). Skærmbilledet ***Messages*** (Meddelelser) vises.
32. Fjern markeringen fra ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis meddelelsesdialogboksen ved registrering af en trussel, og vis den specificerede meddelelsestekst).
33. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og klik på fanen ***General*** (Generelt). Skærmbilledet ***General*** (Generelt) vises.
34. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).
35. Klik på fanen ***ScriptScan*** (Script-scanning). Skærmbilledet ***Script Scan*** (Script-scanning) vises.
36. Kontrollér, at markeringen er fjernet fra ***Enable scanning of scripts*** (Aktiver scanning af scripts).
37. Klik på fanen ***Blocking*** (Blokering). Skærmbilledet ***Blocking*** (Blokering) vises.
38. Fjern markeringen fra ***Block the connection when a threatened file is detected in a shared folder*** (Bloker forbindelsen, når en truet fil registreres i en delt mappe).
39. Klik på fanen ***Messages*** (Meddelelser). Skærmbilledet ***Messages*** (Meddelelser) vises.
40. Fjern markeringen fra ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Vis meddelelsesdialogboksen ved registrering af en trussel, og vis den specificerede meddelelsestekst).
41. Klik på ***Save*** (Gem). Skærmbilledet Assigned Policies (Tildelte politikker) vises.
42. Klik på ***My Default*** (Min standard) for ***On-Access Default Processes Policies*** (Standardprocespolitikker ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Standardprocespolitikker ved åbning > Min standard) vises.
43. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).
44. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
45. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
46. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

47. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.
48. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.
49. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.
50. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
51. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
52. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
53. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.
54. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.
55. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.
56. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.
57. Klik på ***My Default*** (Min standard) for ***On-Access Low-Risk Processes Policies*** (Lavrisiko-procespolitikker ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Lavrisiko-procespolitikker ved åbning > Min standard) vises.
58. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).
59. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.
60. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
61. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).
62. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.
63. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.
64. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

65. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

66. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

67. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

68. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.

69. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.

70. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

71. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.

72. Klik på ***My Default*** (Min standard) for ***On-Access High-Risk Processes Policies*** (Højrisiko-procespolitikker ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Højrisiko-procespolitikker ved åbning > Min standard) vises.

73. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

74. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

75. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

76. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

77. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.

78. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.

79. Vælg ***By pattern*** (Efter mønster) og gå ind i mapperne **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

80. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

81. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Find ukendte, uønskede programmer og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***

82. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

83. Klik på fanen ***Exclusions*** (Udeladelser). Skærmbilledet ***Exclusions*** (Udeladelser) vises.

84. Klik på ***Add*** (Tilføj). Skærmbilledet ***Add/Edit Exclusion Item*** (Tilføj/rediger element til udeladelse) vises.

85. Vælg By pattern (Efter mønster) og gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** en ad gangen og vælg ***Also exclude subfolders*** (Udelad også undermapper). Klik på ***OK***.

86. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.

87. Klik på ***My Default*** (Min standard) for ***On Delivery Email Scan Policies*** (Politikker for e-mail-scanning ved åbning). Skærmbilledet ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker for e-mail-scanning ved åbning) vises.

88. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

89. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

90. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown program threats and trojans (Find ukendte programtrusler og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
    - ***Find attachments with multiple extensions (Find vedhæftelser med flere udvidelser).***

91. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

92. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).

93. Fjern markeringen fra ***Enable on-delivery email scanning*** (Aktiver e-mail-scanning ved åbning) under ***Scanning of email*** (E-mail-scanning).

94. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).

95. Klik på fanen ***Scan Items*** (Scanningselementer). Skærmbilledet ***Scan Items*** (Scanningselementer) vises.

96. Fjern markeringen fra følgende funktioner under ***Heuristics*** (Heuristik):

    - ***Find unknown program threats and trojans (Find ukendte programtrusler og trojanske heste).***
    - ***Find unknown macro threats (Find ukendte makro-trusler).***
    - ***Find attachments with multiple extensions (Find vedhæftelser med flere udvidelser).***

97. Fjern markeringen fra ***Detect unwanted programs*** (Registrer uønskede programmer) under ***Unwanted programs detection*** (Registrering af uønskede programmer).

98. Vælg ***Disabled*** (Deaktiveret) fra ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk netværkskontrol af mistænkelige filer).

99. Fjern markeringen fra ***Enable on-delivery email scanning*** (Aktiver e-mail-scanning ved åbning) under ***Scanning of email*** (E-mail-scanning).

100. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.

101. Klik på ***My Default*** (Min standard) for ***General Options Policies*** (Politikker for generelle funktioner). Skærmbilledet ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker for generelle funktioner > Min standard) vises.

102. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

103. Klik på fanen ***Display Options*** (Visningsindstillinger). Skærmbilledet ***Display Options*** (Visningsindstillinger) vises.

104. Vælg følgende under ***Console options*** (Konsolindstillinger):

    - ***Display managed tasks in the client console (Vis håndterede opgaver i klientkonsollen).***
    - ***Disable default AutoUpdate task schedule (Deaktiver standard-opgavetidsplanen for automatisk opdatering).***

105. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).

106. Klik på fanen ***Display Options*** (Visningsindstillinger). Skærmbilledet ***Display Options*** (Visningsindstillinger) vises.

107. Vælg følgende under ***Console options*** (Konsolindstillinger):

    - ***Display managed tasks in the client console (Vis håndterede opgaver i klientkonsollen).***
    - ***Disable default AutoUpdate task schedule (Deaktiver standard-opgavetidsplanen for automatisk opdatering).***

108. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.

109. Klik på ***My Default*** (Min standard) for ***Alert Policies*** (Beskedpolitikker). Skærmbilledet ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Ædr politikker > Min standard) vises.

110. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

111. Vælg fanen ***Alert Manager Alerts*** (Beskeder fra besked-administrator). Skærmbilledet ***Alert Manager Alerts*** (Beskeder fra besked-administrator) vises.

112. Fjern markeringen fra ***On-Access Scan*** (Scanning ved åbning), ***On-Demand Scan and scheduled scans*** (Scanning efter behov og planlagte scanninger), ***Email Scan*** (E-mail-scanning) og ***AutoUpdate*** (Automatisk opdatering), som alle ligger under ***Components that generate alerts*** (Komponenter, der genererer beskeder).

113. Vælg ***Disable alerting*** (Deaktiver beskeder) under indstillingerne for ***Alert Manager*** (Besked-administrator).

114. Fjern markeringen fra ***Access Protection*** (Adgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter, der genererer beskeder).

115. Klik på ***Additional Alerting Options*** (Flere beskedfunktioner). Skærmbilledet ***Additional Alerting Options*** (Flere beskedfunktioner) vises.

116. Fra rullelisten ***Severity Filters*** (Prioritetsfiltre) skal du vælge ***Suppress all alerts (severities 0 to 4)*** (Skjul alle beskeder (prioritet 0 til 4)).

117. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for), og vælg fanen ***Alert Manager Alerts*** (Beskeder fra besked-administrator). Skærmbilledet ***Alert Manager Alerts*** (Beskeder fra besked-administrator) vises.

118. Fjern markeringen fra ***On-Access Scan*** (Scanning ved åbning), ***On-Demand Scan and scheduled scans*** (Scanning efter behov og planlagte scanninger), ***Email Scan*** (E-mail-scanning) og ***AutoUpdate*** (Automatisk opdatering), som alle ligger under ***Components that generate alerts*** (Komponenter, der genererer beskeder).

119. Markér ***Disable alerting*** (Deaktiver beskeder) under indstillingerne for ***Alert Manager*** (Besked-administrator).

120. Fjern markeringen fra ***Access Protection*** (Adgangsbeskyttelse) under ***Components that generate alerts*** (Komponenter, der genererer beskeder).

121. Klik på ***Additional Alerting Options*** (Flere beskedfunktioner). Skærmbilledet Additional Alerting Options (Flere beskedfunktioner) vises.

122. Fra rullelisten ***Severity Filters*** (Prioritetsfiltre) skal du vælge ***Suppress all alerts (severities 0 to 4)*** (Skjul alle beskeder (prioritet 0 til 4)).

123. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.

124. Klik på ***My Default*** (Min standard) for ***Access Protection Policies*** (Politikker for adgangsbeskyttelse). Skærmbilledet ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker for adgangsbeskyttelse > Min standard) vises.

125. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).

126. Klik på fanen ***Access Protection*** (Adgangsbeskyttelse). Skærmbilledet ***Access Protection*** (Adgangsbeskyttelse) vises.

127. Fjern markeringen fra følgende funktioner under ***Access protection settings*** (Indstillinger for adgangsbeskyttelse):

    - ***Enable access protection (Aktiver adgangsbeskyttelse).***
    - ***Prevent McAfee services from being stopped (Forhindr McAfee-tjenester i at blive stoppet).***
    - ***Aktiver forbedret selvforsvar.***

128. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).

129. Klik på fanen ***Access Protection*** (Adgangsbeskyttelse). Skærmbilledet ***Access Protection*** (Adgangsbeskyttelse) vises.

130. Fjern markeringen fra følgende funktioner under ***Access protection settings*** (Indstillinger for adgangsbeskyttelse):

    - ***Enable access protection (Aktiver adgangsbeskyttelse).***
    - ***Prevent McAfee services from being stopped (Forhindr McAfee-tjenester i at blive stoppet).***
    - ***Aktiver forbedret selvforsvar.***

131. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.

132. Klik på ***My Default*** (Min standard) for ***Buffer Overflow Protection Policies*** (Politikker til beskyttelse mod bufferoverløb). Skærmbilledet ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Politikker til beskyttelse mod bufferoverløb > Min Standard) vises.
133. Vælg ***Workstation*** (Arbejdsstation) fra rullelisten ***Settings for*** (Indstillinger for).
134. Klik på fanen ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb). Skærmbilledet ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb) vises.
135. Fjern markeringen fra ***Show the message dialog box when a buffer overflow is detected*** (Vis meddelelsesdialogboksen ved registrering af et bufferoverløb) under ***Client system warning*** (Klientsystemadvarsler).
136. Fjern markeringen fra ***Enable buffer overflow protection*** (Aktiver beskyttelse mod bufferoverløb) under ***Buffer overflow settings*** (Bufferoverløbindstillinger).
137. Vælg ***Server*** fra rullelisten ***Settings for*** (Indstillinger for).
138. Klik på fanen ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb). Skærmbilledet ***Buffer Overflow Protection*** (Beskyttelse mod bufferoverløb) vises.
139. Fjern markeringen fra ***Show the message dialog box when a buffer overflow is detected*** (Vis meddelelsesdialogboksen ved registrering af et bufferoverløb) under ***Client system warning*** (Klientsystemadvarsler).
140. Fjern markeringen fra ***Enable buffer overflow protection*** (Aktiver beskyttelse mod bufferoverløb) under ***Buffer overflow settings*** (Bufferoverløbindstillinger).
141. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.
142. Fra rullelisten ***Product*** (Produkt) vælges ***McAfee Agent***. Vinduet ***Policies*** (Politikker) for McAfee Agent åbnes.
143. Klik på ***My Default*** (Min standard) for ***Repository*** (Lager). Skærmbilledet ***McAfee Agent > Repository > My Default*** (McAfee Agent > Lager > Min standard) vises.
144. Klik på fanen ***Proxy***. Skærmbilledet ***Proxy*** vises.
145. Sørg for, at ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Brug Internet Explorer-indstillinger (Windows)/Systempræferenceindstillinger (Mac OSX)) under ***Proxy settings*** (Proxy-indstillinger) er valgt.
146. Klik på ***Save*** (Gem). Skærmbilledet ***Assigned Policies*** (Tildelte politikker) vises.
147. Klik på fanen ***Systems*** (Systemer).
148. Vælg alle klientsystemer (Optagelse, Gennemsyn og Centricity Cardiology INW-server), hvorpå de konfigurerede politikker skal anvendes.
149. Vælg ***Wake Up Agents*** (Aktiveringsagenter). Skærmbilledet ***Wake Up Agent*** (Aktiveringsagent) vises.
150. Klik på ***OK***.
151. Log af ePolicy Orchestrator.

McAfee ePolicy Orchestrator – retningslinjer efter installation

Aktiver tilbagekoblingsforbindelsen. Se Aktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.

Trend Micro OfficeScan klient-/serverudgave 10.6 SP2

Installationsoversigt

Installer kun Trend Micro OfficeScan klient-/serverudgaven i et netværksforbundet Mac-Lab/CardioLab-miljø. Trend Micro OfficeScan skal installeres på antivirusadministrationskonsolserveren og derefter udrulles til Centricity Cardiology INW-serveren og optagelses-/gennemsynsarbejdsstationerne som klienter. Brug følgende anvisninger til at installere ***Trend Micro OfficeScan Client/Server Edition***.

Virusopdateringer er institutionens ansvar. Opdater definitionerne regelmæssigt for at sikre, at systemet har den nyeste virusbeskyttelse.

Retningslinjer inden installation

1. Trend Micro antivirusadministrationskonsollen forventes at være installeret i henhold til Trend Micros anvisninger og at fungere korrekt.
2. Under installation af Trend Micro OfficeScan skal du gøre følgende på antivirusadministrationskonsolserveren:
    a. Fjern markeringen fra ***Enable firewall*** (Aktiver Firewall) i vinduet ***Anti-virus Feature*** (Antivirusfunktion).
    b. Vælg ***No, Please do not enable assessment mode*** (Nej tak, aktiver ikke vurderingstilstanden) i vinduet ***Anti-spyware Feature*** (Antispywarefunktion).
    c. Fjern markeringen fra ***Enable web reputation policy*** (Aktiver politik for internetomdømme) i vinduet ***Web Reputation Feature*** (Internetomdømmefunktion).
3. Trend Micro OfficeScan anbefales ikke, når ***CO_2***-funktionen bruges sammen med PDM i Mac-Lab/CardioLab-systemer.
4. Hvis Trend Micro OfficeScan påkræves:
    a. Det anbefales at konfigurere en separat Trend Micro antivirusadministrationskonsolserver til Mac-Lab/CardioLab-systemerne. Der kræves en global ændring i antivirusindstillingerne for at kunne bruge ***CO_2***-funktionen sammen med i Mac-Lab/CardioLab-systemer.
    b. Hvis en separat Trend Micro antivirusadministrationskonsolserver ikke kan konfigureres, kræves der en ændring i den eksisterende Trend Micro antivirusadministrations-konsolservers globale indstillinger efter installation. Denne ændring påvirker alle de klientsystemer, som er forbundet til den eksisterende Trend Micro antivirusadministrationskonsolserver, og den skal gennemgås sammen med IT-personale, før du går videre.
5. Log på som **Administrator** eller som medlem af den gruppe på alle klientsystemer (optagelse, gennemsyn og INW Server) for at installere antivirussoftwaren.
6. Deaktiver tilbagekoblingsforbindelsen. Se Deaktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
7. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser før installation af antivirus på side 7 for yderligere oplysninger.

Trend Micro OfficeScan – nye installationsudrulningstrin (foretrukket push-installationsmetode)

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

BEMÆRK: Fortsæt ved at vælge ***Continue to this website (not recommended)*** (Fortsæt til denne webside (frarådes)). I vinduet Security Alert (Sikkerhedsbeskeder) skal du markere ***In the future, do not show this warning*** (Vis ikke denne advarsel igen) og klikke på ***OK***.

2. Hvis du modtager en certifikatfejlmeddelelse, som angiver, at websiden ikke er pålidelig, skal du administrere certifikaterne, så de inkluderer Trend Micro OfficeScan.
3. Hvis du bliver promptet, skal du installere tilføjelserne ***AtxEnc***. Skærmbilledet Security Warning (Sikkerhedsadvarsel) vises.
4. Klik på ***Install*** (Installer).
5. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).
6. Hvis du bliver promptet, skal du klikke på ***Update Now*** (Opdater nu) for at installere nye widgets. Vent, til de nye widgets er blevet opdateret. Skærmbilledet The update is completed (Opdateringen er fuldført) vises.
7. Klik på ***OK***.
8. Fra menubjælken på venstre siden skal du klikke på ***Networked Computers > Client Installation > Remote*** (Netværksforbundne computere > Klientinstallation > Ekstern).
9. Hvis du bliver promptet, skal du installere tilføjelserne ***AtxConsole***. Skærmbilledet Security Warning (Sikkerhedsadvarsel) vises.
10. Klik på ***Install*** (Installer).
11. Dobbeltklik på ***My Company*** (Min virksomhed) i vinduet ***Remote Installation*** (Ekstern installation). Alle domæner bliver angivet under ***My Company*** (Min virksomhed).
12. Udvid domænet (f. eks. INW) fra listen. Alle systemer, der er forbundet med domænet, vises.
13. Hvis domæner eller systemer ikke er angivet i vinduet ***Domain and Computers*** (Domæne og computere), skal du gøre følgende på hvert klientsystem (optagelse, gennemsyn og INW Server):
    a. Log på som administrator eller som medlem af den gruppe på alle klientmaskiner.
    b. Klik på ***Start > Run*** (Start > Kør).
    c. Indtast ***\\<Anti-Virus Management Console_server_IP_address>*** og tryk på ***Enter***. Når du bliver promptet, skal du indtaste administratorbrugernavn og adgangskode.
    d. Naviger til ***\\<Anti-Virus Management Console_server_IP _address>\ofsscan*** og dobbeltklik på ***AutoPcc.exe***. Når du bliver promptet, skal du indtaste administratorbrugernavn og adgangskode.
    e. Genstart klientsystemerne, når installationen er fuldført.

f. Log på som **Administrator** eller som medlem af den gruppe på alle klientmaskiner, og vent, til Trend Micro OfficeScan-ikonet i systembakken skifter til blåt.

g. Spring de resterende trin i denne procedure over, og gå til proceduren for konfiguration af Trend Micro OfficeScan-serverkonsollen.

14. Vælg klientmaskinerne (optagelse, gennemsyn og INW Server), og klik på ***Add*** (Tilføj).
15. Indtast <domænenavn>\brugernavn og adgangskode, og klik på ***Log on*** (Log på).
16. Vælg klientmaskinerne (optagelse, gennemsyn og INW Server) en ad gangen fra ruden ***Selected Computers*** (Valgte computere), og klik på ***Install*** (Installer).
17. Klik på ***Yes*** (Ja) i bekræftelsesvinduet.
18. Klik på ***OK*** i meddelelsesvinduet ***Number of clients to which notifications were sent*** (Antal klienter, som har fået tilsendt meddelelser).
19. Genstart alle klientmaskiner (optagelse, gennemsyn og INW Server), og log på som administrator eller som medlem af den gruppe på alle klientmaskiner, og vent, til ikonet Trend Micro OfficeScan i systembakken skifter til blåt med et grønt fluebenssymbol.
20. Klik på linket ***Log Off*** (Log af) for at lukke ***OfficeScan Web Console*** (OfficeScan-webkonsollen).

Trend Micro OfficeScan-serverkonsolkonfiguration

1. Vælg ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Start > Programmer > TrendMicro Office Scan-server <servernavn> > Office Scan-webkonsol). Skærmbilledet ***Trend Micro OfficeScan Login*** (Trend Micro OfficeScan logon) vises.
2. Indtast brugernavn og adgangskode og klik på ***Login*** (Log på). Skærmbilledet ***Summary*** (Opsummering) vises.
3. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
4. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
5. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Manual Scan Settings*** (Scanningsindstillinger > Manuelle scanningsindstillinger). Skærmbilledet ***Manual Scan Settings*** (Manuelle scanningsindstillinger) vises.
6. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
   - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
   - ***Scanningsindstillinger > Scan komprimerede filer.***
   - ***Scanningsindstillinger > Scan OLE-objekter.***
   - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
   - ***CPU-brug > Lavt.***
   - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
   - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***

- ***Scanningsudeladelsesliste (biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret, og vælg Add path to client Computers Exclusion list (Tilføj sti til udeladelseslisten for klientcomputere).***
- Gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** og **G:** en ad gangen og klik på ***Add*** (Tilføj).

7. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
8. Klik på ***OK*** ved meddelelsen***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier. Do you want to proceed?*** (Udeladelseslisten på dette skærmbillede vil erstatte udeladelseslisten for klienter eller domæner, som tidligere blev valgt i klienttrædiagrammet. Ønsker du at fortsætte?)
9. Klik på ***Close*** (Luk) for at lukke siden ***Manual Scan Settings*** (Manuelle scanningsindstillinger).
10. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
11. På højre side vælges serveren ***OfficeScan***.
12. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Scan Settings > Real-time Scan Settings*** (Scanningsindstillinger > Indstillinger for realtidsscanninger). Skærmbilledet ***Real-time Scan Settings*** (Indstillinger for realtidsscanninger) vises.
13. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Indstillinger for realtidsscanninger > Aktiver virus/malware-scanning.***
    - ***Indstillinger for realtidsscanninger > Aktiver spyware/grayware-scanning.***
    - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
    - ***Scanningsindstillinger > Scan komprimerede filer.***
    - ***Scanningsindstillinger > Scan OLE-objekter.***
    - ***Kun virus/malware-scanningsindstillinger > Aktiver IntelliTrap.***
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
    - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
    - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
    - Kontrollér, at mappestierne ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** og ***G:*** findes i ***Exclusion List*** (Udeladelsesliste).
14. Klik på fanen ***Action*** (Handling).
15. Behold standardindstillingerne og fjern markeringen fra følgende funktioner:
    - ***Virus/malware > Vis en meddelelse på klientcomputeren, når virus/malware registreres.***
    - ***Spyware/grayware > Vis en meddelelse på klientcomputeren, når spyware/grayware registreres.***
16. Klik på ***Apply to All Clients*** (Anvend til alle klienter).

17. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Real-time Scan Settings*** (Indstillinger for realtidsscanning).
18. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
19. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
20. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Scheduled Scan Settings*** (Scanningsindstillinger > Planlagte scanningsindstillinger). Skærmbilledet ***Scheduled Scan Settings*** (Planlagte scanningsindstillinger) vises.
21. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Planlagte scanningsindstillinger > Aktiver virus/malware-scanning.***
    - ***Planlagte scanningsindstillinger > Aktiver spyware/grayware-scanning.***
    - ***Planlægning > Ugentligt, hver søndag, starttidspunkt: 00:00 tt:mm.***
    - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
    - ***Scanningsindstillinger > Scan komprimerede filer.***
    - ***Scanningsindstillinger > Scan OLE-objekter.***
    - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
    - ***CPU-brug > Lavt.***
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
    - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
    - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
    - Kontrollér, at mappestierne ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** findes i Exclusion List (Udeladelsesliste).
22. Klik på fanen ***Action*** (Handling).
23. Behold standardindstillingerne og fjern markeringen fra følgende funktioner:
    - ***Virus/malware > Vis en meddelelse på klientcomputeren, når virus/malware registreres.***
    - ***Spyware/grayware > Vis en meddelelse på klientcomputeren, når spyware/grayware registreres.***
24. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
25. Klik på ***Close*** (Luk) for at lukke siden ***Scheduled Scan Settings*** (Planlagte scanningsindstillinger).
26. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
27. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
28. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Scan Now Settings*** (Scanningsindstillinger > Indstillinger for omgående scanning). Skærmbilledet ***Scan Now Settings*** (Indstillinger for omgående scanning) vises.

29. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Indstillinger for omgående scanning > Aktiver virus/malware-scanning.***
    - ***Indstillinger for omgående scanning > Aktiver spyware/grayware-scanning.***
    - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
    - ***Scanningsindstillinger > Scan komprimerede filer.***
    - ***Scanningsindstillinger > Scan OLE-objekter.***
    - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
    - ***CPU-brug > Lavt.***
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
    - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
    - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
    - Kontrollér, at ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:***
30. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
31. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Scan Now Settings*** (Indstillinger for omgående scanning).
32. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
33. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
34. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Web Reputation Settings*** (Indstillinger for internetomdømme). Skærmbilledet ***Web Reputation Settings*** (Indstillinger for internetomdømme) vises.
35. Klik på fanen ***External Clients*** (Eksterne klienter) og fjern markeringen fra ***Enable Web reputation policy on the following operating systems*** (Aktiver politikker for internetomdømme på følgende operativsystemer), hvis denne allerede er blevet valgt under installering.
36. Klik på fanen ***Internal Clients*** (Interne klienter) og fjern markeringen fra ***Enable Web reputation policy on the following operating systems*** (Aktiver politikker for internetomdømme på følgende operativsystemer), hvis denne allerede er blevet valgt under installering.
37. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
38. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Web Reputation*** (Internetomdømme).
39. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
40. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
41. Fra funktionen ***Settings*** (Indstillinger) vælges ***Behavior Monitoring Settings*** (Indstillinger for adfærdsovervågning). Skærmbilledet ***Behavior Monitoring Settings*** (Indstillinger for adfærdsovervågning) vises.

42. Fjern markeringen fra funktionerne ***Enable Malware Behavior Blocking*** (Aktiver malware-adfærdsblokering) og ***Enable Event Monitoring*** (Aktiver hændelsesovervågning).
43. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
44. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Behavior Monitoring*** (Adfærdsovervågning).
45. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
46. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
47. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Device Control Settings*** (Indstillinger for enhedsstyring). Skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring) vises.
48. Klik på fanen ***External Clients*** (Eksterne klienter) og fjern markeringen fra følgende funktioner:
    - ***Meddelelse > Vis en meddelelse på klientcomputeren, når OfficeScan registrerer ikke-autoriseret adgang på enheder.***
    - ***Bloker AutoRun-funktionen på USB-lagerenheder.***
    - ***Aktiver enhedsstyring.***
49. Klik på fanen ***Internal Clients*** (Interne klienter) og fjern markeringen fra følgende funktioner:
    - ***Meddelelse > Vis en meddelelse på klientcomputeren, når OfficeScan registrerer ikke-autoriseret adgang på enheder.***
    - ***Bloker AutoRun-funktionen på USB-lagerenheder.***
    - ***Aktiver enhedsstyring.***
50. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
51. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring).
52. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
53. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
54. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Privileges and Other Settings*** (Rettigheder og andre indstillinger).
55. Klik på fanen ***Privileges*** (Rettigheder) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanningsrettigheder > Konfigurer manuelle scanningsindstillinger.***
    - ***Scanningsrettigheder > Konfigurer scanningsindstillinger i realtid.***
    - ***Scanningsrettigheder > Konfigurer planlagte scanningsindstillinger.***
    - ***Proxyindstillingsrettigheder > Tillad klientbrugeren at konfigurere proxyindstillinger.***
    - ***Afinstallation > Kræver en adgangskode for at brugeren kan afinstallere OfficeScan-klienten.*** Indtast en egnet adgangskode og bekræft adgangskoden.
    - ***Fjernelse > Kræver en adgangskode for at brugeren kan fjerne OfficeScan-klienten.*** Indtast en egnet adgangskode og bekræft adgangskoden.
56. Klik på fanen ***Other Settings*** (Andre indstillinger).

57. Vælg ***Client Security Settings > Normal*** (Klientsikkerhedsindstilinger > Normal), og fjern markeringen fra de resterende funktioner.

BEMÆRK: Det er vigtigt at rydde følgende funktioner.

- ***Klient-selvforsvar > Beskyt OfficeScan-klienttjenester.***
- ***Klient-selvforsvar > Beskyt filer i OfficeScan-klientinstallationsmappen.***
- ***Klient-selvforsvar > Beskyt OfficeScan-klientregisternøgler.***
- ***Klient-selvforsvar > Beskyt OfficeScan-klientprocesser.***

58. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
59. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Privileges and Other Settings*** (Rettigheder og andre indstillinger).
60. Fra venstre rude vælges linket ***Networked Computers > Client Management*** (Netværksforbundne computere > Klientadministration).
61. På højre side vælges ***OfficeScan Server*** (OfficeScan-server).
62. Fra funktionen ***Settings*** (Indstillinger) vælges ***Additional Service Settings*** (Yderligere tjenesteindstillinger).
63. Fjern markeringen fra funktionen ***Enable service on the following operating systems*** (Aktiver tjeneste på følgende operativsystemer).
64. Klik på ***Apply to All Clients*** (Anvend til alle klienter).
65. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Additional Service Settings*** (Yderligere tjenesteindstillinger).
66. Fra venstre rude vælges linket ***Networked Computers > Global Client Settings*** (Netværksforbundne computere > Globale klientindstillinger).
67. Vælg kun følgende funktioner, og fjern markeringen af de resterende funktioner:

- ***Scanningsindstillinger > Konfigurer scanningsindstillinger for store komprimerede filer.***
- ***Scanningsindstillinger > Scan ikke filer i den komprimerede fil, hvis størrelsen overstiger 2 MB.***
- ***Scanningsindstillinger > Scan kun de første 100 filer i en komprimeret fil.***
- ***Scanningsindstillinger > Udelad OfficeScan-serverens databasemappe fra Realtidsscanning.***
- ***Scanningsindstillinger > Udelad Microsoft Exchange-serverens mapper og filer fra scanninger.***
- ***Reserveret diskplads > Reserver 60 MB diskplads til opdateringer.***
- ***Proxykonfiguration > Automatisk registrering af indstillinger.***

BEMÆRK: Det er vigtigt at fjerne markeringen fra ***Alert Settings > Display a notification message if the client computer needs to restart to load a kernel driver*** (Beskedindstillinger > Vis en meddelelse, hvis det er nødvendigt at genstarte klientcomputeren for at indlæse en kernedriver).

68. Klik på ***Save*** (Gem).
69. Fra venstre rude vælges linket ***Updates > Networked Computers > Manual Updates*** (Opdateringer > Netværksforbundne computere > Manuelle opdateringer).

70. Vælg ***Manually select client*** (Vælg klient manuelt) og klik på ***Select*** (Vælg).
71. Klik på det relevante domænenavn under ***OfficeScan Server*** (OfficeScan-server).
72. Vælg klientsystemer et ad gangen, og klik på ***Initiate Component Update*** (Start komponentopdatering).
73. Klik på ***OK*** i meddelelsesboksen.
74. Klik på ***Log off*** (Log af) og luk OfficeScan-webkonsollen.

Trend Micro OfficeScan – retningslinjer efter installering

1. Udfør følgende trin på optagesystemerne for at konfigurere Trend Micro:
    a. Klik på ***Start > Control Panel > Network and Sharing Center*** (Start > Kontrolpanel > Netværks- og delingscenter).
    b. Klik på ***Change adapter settings*** (Rediger adapterindstillinger).
    c. Højreklik på ***Local Area Connection*** (Lokal netværksforbindelse), og vælg ***Properties*** (Egenskaber).
    d. Vælg ***Internet Protocol Version 4 (TCP/IPv4)*** (Internetprotokol version 4 (TCP/IPv4) og klik på ***Properties*** (Egenskaber).
    e. Registrer IP-adressen _____.
    f. Luk alle åbne vinduer.
    g. Klik på ***Start > Run*** (Start > Kør) og indtast **regedit**.
    h. Naviger til ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.
    i. På den højre rude skal du højreklikke på et tomt område og vælge ***New > String value*** (Ny > Strengværdi).
    j. Indtast **IP Template** (IP-skabelon) som navn og tryk på **Enter**.
    k. Dobbeltklik på registeret ***IP Template*** (IP-skabelon).
    l. I datafeltet ***Value*** (Værdi) skal du indtaste IP-adressen for den lokal netværksforbindelse, som blev registreret i trin e.
    m. Klik på ***OK***.
    n. Luk register-editoren.
2. Aktiver tilbagekoblingsforbindelsen. Se Aktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
3. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser efter installation af antivirus på side 7 for yderligere oplysninger.

Konfiguration af globale indstillinger for Trend Micro

BEMÆRK: Følgende anvisninger skal kun udføres, når CO_2-funktionen bruges sammen med PDM i Mac-Lab/CardioLab-systemer. Sørg for at gennemgå dem med IT-personale, før du sætter trinnene nedenfor igang.

1. På antivirusadministrationskonsolserveren skal du naviger til mappen ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.
2. Åbn filen ***ofcscan.ini*** i et tekstredigeringsprogram.
3. I afsnittet ***Global Setting*** (Global indstilling) skal du indstille værdien for den følgende nøgle til "**1**": [Global Indstilling] ***RmvTmTDI=1***
4. Gem og luk filen ofcscan.ini.
5. Klik på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alle programmer > TrendMicro OfficeScan - <servernavn> > OfficeScan-webkonsol).
6. Indtast brugernavn og adgangskode, og klik på ***Log On*** (Log på). Skærmbilledet ***Summary*** (Opsummering) vises.
7. Klik på ***Networked Computers > Global Client Settings*** (Netværksforbundne computere > Globale klientindstillinger).
8. Klik på ***Save*** (Gem).
9. Fra venstre rude vælges linket ***Updates > Networked Computers > Manual Update*** (Opdateringer > Netværksforbundne computere > Manuel opdatering).
10. Vælg ***Manually select clients*** (Vælg klienter manuelt) og klik på ***Select*** (Vælg).
11. Klik på det relevante domænenavn under ***OfficeScan Server*** (OfficeScan-server).
12. Vælg klientsystemer et ad gangen, og klik på ***Initiate Component Update*** (Start komponentopdatering).
13. Klik på ***OK*** i meddelelsesboksen.
14. Udfør følgende på hvert optagesystem:
    a. Åbn register-editoren.
    b. Naviger til ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. Kontrollér, at registerværdien ***RmvTmTDI*** er indstillet til "**1**".
    d. Naviger til ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Slet registernøglen ***tmtdi***, hvis den findes.
    f. Luk register-editoren.
    g. Genstart klientsystemerne.
    h. Log på klientsystemerne som administrator eller som medlem af den gruppe.
    i. På hvert klientsystem skal du åbne kommandoprompten med administratorrettigheder og indtaste kommandoen "***sc query tmtdi***".
    j. Kontrollér, at meddelelsen ***The specified service does not exist as an installed service*** (Den angivne tjeneste findes ikke som installeret tjeneste) vises.
15. På antivirusadministrationskonsolserveren skal du klikke på ***Log off*** (Log af) og lukke OfficeScan-webkonsollen.

Trend Micro OfficeScan klient-/serverudgave 11.0 SP1

Installer kun Trend Micro OfficeScan klient-/serverudgaven i et netværksforbundet Mac-Lab/CardioLab-miljø. Trend Micro OfficeScan skal installeres på antivirusadministrations-konsolserveren og derefter udrulles til Centricity Cardiology INW-serveren og optagelses-/gennemsynsarbejdsstationerne som klienter. Brug følgende anvisninger til at installere ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

Virusopdateringer er institutionens ansvar. Opdater definitionerne regelmæssigt for at sikre, at systemet har den nyeste virusbeskyttelse.

Retningslinjer inden installation

1. Trend Micro antivirusadministrationskonsollen forventes at være installeret i henhold til Trend Micros anvisninger og at fungere korrekt.
2. Under installation af Trend Micro OfficeScan skal du gøre følgende på antivirusadministrationskonsolserveren:
   a. Fjern markeringen fra ***Enable firewall*** (Aktiver Firewall) i vinduet ***Anti-virus Feature*** (Antivirusfunktion).
   b. Vælg ***No, Please do not enable assessment mode*** (Nej tak, aktiver ikke vurderingstilstanden) i vinduet ***Anti-spyware Feature*** (Antispywarefunktion).
   c. Fjern markeringen fra ***Enable web reputation policy*** (Aktiver politik for internetomdømme) i vinduet ***Web Reputation Feature*** (Internetomdømmefunktion).
3. Trend Micro OfficeScan frarådes, når CO_2-funktionen bruges sammen med PDM i Mac-Lab/CardioLab-systemer.
4. Hvis Trend Micro OfficeScan påkræves:
   a. Det anbefales at konfigurere en separat Trend Micro antivirusadministrations-konsolserver til Mac-Lab/CardioLab-systemerne. Der kræves en global ændring i antivirusindstillingerne for at kunne bruge CO_2-funktionen sammen med PDM i Mac-Lab/CardioLab-systemer.
   b. Hvis en separat Trend Micro antivirusadministrationskonsolserver ikke kan konfigureres, kræves der en ændring i den eksisterende Trend Micro antivirusadministrations-konsolservers globale indstillinger efter installation. Denne ændring påvirker alle de klientsystemer, som er forbundet til den eksisterende Trend Micro antivirusadministrationskonsolserver, og den skal gennemgås sammen med IT-personale, før du går videre.
5. Log på som **Administrator** eller som medlem af den gruppe på alle klientsystemer (optagelse, gennemsyn og INW Server) for at installere antivirussoftwaren.
6. Deaktiver tilbagekoblingsforbindelsen. Se Deaktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
7. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser før installation af antivirus på side 7 for yderligere oplysninger.
8. Følgende rod- og mellemcertifikater er påkrævede for installering på klientmaskinerne for optagelse, gennemsyn og INW:

- AddTrustExternalCARoot.crt
- COMODOCodeSigningCA2.crt
- UTNAddTrustObject_CA.crt
- UTN-USERFirst-Object.crt
- UTN-USERFirst-Object_kmod.crt

9. Gentag følgende undertrin for at installere de fem påkrævede rod- og mellemniveaucertifikater, som er angivet i trin 8.

    a. Naviger til C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
    BEMÆRK: Naviger til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro på INW.

    b. Hvis ovennævnte mappesti ikke findes, skal du manuelt få fat i de rod- og mellemniveaucertifikater, der er påkrævet til installering.

    c. Dobbeltklik på ***AddTrustExternalCARoot.crt*** for at installere den på MLCL-systemerne (optagelse, gennemsyn og INW).

    d. Luk certifikatet op og klik på ***Install Certificate*** (Installer certifikat).

    e. Klik på ***Next*** (Næste), når ***Certificate Import Wizard*** (Guiden Certifikatimport) vises.

    f. I vinduet ***Certificate Store*** (Certifikatlager) vælges ***Place all certificates in the following store*** (Placer alle certifikater i følgende lager), hvorefter der klikkes på ***Browse*** (Gennemse).

    g. Marker ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Vis fysiske lagre > Pålidelige rodcertifikat-myndigheder > Lokal computer), og klik derefter på ***OK***.

    h. Klik på ***Next*** (Næste) i ***Certificate Import Wizard*** (Guiden Certifikatimport).

    i. Klik på ***Finish*** (Udfør). Meddelelsen ***The import was successful*** (Import fuldført) bør vises.

    j. Gentag trin 9 for de andre certifikater, som er angivet i trin 8.

BEMÆRK: Hvert certifikat har en udløbsdato. Når certifikatet er udløbet, skal det fornys og opdateres på MLCL-systemerne for at sikre, at OfficeScan-agenten fungerer som forventet.

Trend Micro OfficeScan – nye installationsudrulningstrin (foretrukket push-installationsmetode for 11.0 SP1)

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

BEMÆRK: Fortsæt ved at vælge ***Continue to this website (not recommended)*** (Fortsæt til denne webside (frarådes)). I vinduet Security Alert (Sikkerhedsbeskeder) skal du markere ***In the future, do not show this warning*** (Vis ikke denne advarsel igen) og klikke på ***OK***.

2. Hvis du modtager en certifikatfejlmeddelelse, som angiver, at websiden ikke er pålidelig, skal du administrere certifikaterne, så de inkluderer Trend Micro OfficeScan.

3. Hvis du bliver promptet, skal du installere tilføjelserne ***AtxEnc***. Skærmbilledet Security Warning (Sikkerhedsadvarsel) vises.

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

4. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).

5. Hvis du bliver promptet, skal du klikke på ***Update Now*** (Opdater nu) for at installere nye widgets. Vent, til de nye widgets er blevet opdateret. Skærmbilledet The update is completed (Opdateringen er fuldført) vises.

   a. Klik på ***OK***.

6. Klik på ***Agents > Agent Installation > Remote*** (Agenter > Agentinstallering > Ekstern) på den øverste menubjælke.

7. Hvis du bliver promptet, skal du installere tilføjelserne ***AtxConsole***. Skærmbilledet Security Warning (Sikkerhedsadvarsel) vises.

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

8. Dobbeltklik på ***OfficeScan Server*** (OfficeScan-server) i vinduet ***Remote Installation*** (Ekstern installation). Alle domæner bliver angivet under ***OfficeScan Server*** (OfficeScan-server).

9. Dobbeltklik på domænet (f. eks. INW) fra listen. Alle systemer, der er forbundet med domænet, vises.

BEMÆRK: Hvis der findes domæner eller systemer, der ikke er angivet i vinduet ***Domains and Endpoints*** (Domæner og slutpunkter), skal du gå til Fejlfinding af domæner eller systemer, der ikke er angivet i vinduet Domains and Endpoints (Domæner og slutpunkter) på side 73 for at tilføje dem manuelt eller for at køre installationen direkte fra klientmaskinen.

10. Vælg klientmaskinerne (optagelse, gennemsyn og INW Server), og klik på ***Add*** (Tilføj).

11. Indtast <domænenavn>\brugernavn og adgangskode, og klik på ***Log on*** (Log på).

12. Vælg klientmaskinerne (optagelse, gennemsyn og INW Server) en ad gangen fra ruden ***Selected Endpoints*** (Valgte slutpunkter), og klik på ***Install*** (Installer).

13. Klik på ***OK*** i bekræftelsesvinduet.

14. Klik på ***OK*** i meddelelsesvinduet ***Number of clients to which notifications were sent*** (Antal klienter, som har fået tilsendt meddelelser).

15. Genstart alle klientmaskiner (optagelse, gennemsyn og INW Server), og log på som administrator eller som medlem af den gruppe på alle klientmaskiner, og vent, til ikonet Trend Micro OfficeScan i systembakken skifter til blåt med et grønt fluebenssymbol.

16. Klik på linket ***Log Off*** (Log af) for at lukke ***OfficeScan Web Console*** (OfficeScan-webkonsollen).

Trend Micro OfficeScan-serverkonsolkonfiguration for 11.0 SP1

1. Vælg ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Start > Programmer > TrendMicro Office Scan-server <servernavn> > Office Scan-webkonsol). Skærmbilledet ***Trend Micro OfficeScan Login*** (Trend Micro OfficeScan logon) vises.

2. Indtast brugernavn og adgangskode og klik på ***Login*** (Log på). Skærmbilledet ***Summary*** (Opsummering) vises.
3. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
4. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
5. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Manual Scan Settings*** (Scanningsindstillinger > Manuelle scanningsindstillinger). Skærmbilledet ***Manual Scan Settings*** (Manuelle scanningsindstillinger) vises.
6. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
   - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
   - ***Scanningsindstillinger > Scan komprimerede filer.***
   - ***Scanningsindstillinger > Scan OLE-objekter.***
   - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
   - ***CPU-brug > Lavt.***
7. Klik på fanen Scan Exclusion (Scanningsudeladelse) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
   - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
   - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
   - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
   - Vælg ***Adds path*** (Tilføjer sti) fra rullelisten under ***Saving the officescan agent's exclusion list does the following:*** (Når du gemmer OfficsScan-agentens udeladelsesliste, sker følgende:)
   - Gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** og **G:** en ad gangen og klik på **+**.
8. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
9. Klik på ***OK*** ved meddelelsen***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier. Do you want to proceed?*** (Udeladelseslisten på dette skærmbillede vil erstatte udeladelseslisten for klienter eller domæner, som tidligere blev valgt i klienttrædiagrammet. Ønsker du at fortsætte?)
10. Klik på ***Close*** (Luk) for at lukke siden ***Manual Scan Settings*** (Manuelle scanningsindstillinger).
11. Vælg linket ***Agent > Agent Management*** (Agent > Agentadministration) fra den øverste rude.
12. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
13. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Scan Settings > Real-time Scan Settings*** (Scanningsindstillinger > Indstillinger for realtidsscanninger). Skærmbilledet ***Real-time Scan Settings*** (Indstillinger for realtidsscanninger) vises.
14. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Indstillinger for realtidsscanninger > Aktiver virus/malware-scanning.***

- ***Indstillinger for realtidsscanninger > Aktiver spyware/grayware-scanning.***
- ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
- ***Scanningsindstillinger > Scan komprimerede filer.***
- ***Scanningsindstillinger > Scan OLE-objekter.***
- ***Kun virus/malware-scanningsindstillinger > Aktiver IntelliTrap.***

15. Klik på fanen Scan Exclusion (Scanningsudeladelse) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
    - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
    - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
    - Kontrollér, at mappestierne ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** og ***G:*** findes i ***Exclusion List*** (Udeladelsesliste).
16. Klik på fanen ***Action*** (Handling).
17. Behold standardindstillingerne og fjern markeringen fra følgende funktioner:
    - ***Virus/malware > Vis en meddelelse ved slutpunkterne, når virus/malware registreres.***
    - ***Spyware/grayware > Vis en meddelelse ved slutpunkterne, når spyware/grayware registreres.***
18. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
19. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Real-time Scan Settings*** (Indstillinger for realtidsscanning).
20. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
21. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
22. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Scheduled Scan Settings*** (Scanningsindstillinger > Planlagte scanningsindstillinger). Skærmbilledet ***Scheduled Scan Settings*** (Planlagte scanningsindstillinger) vises.
23. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Planlagte scanningsindstillinger > Aktiver virus/malware-scanning.***
    - ***Planlagte scanningsindstillinger > Aktiver spyware/grayware-scanning.***
    - ***Planlægning > Ugentligt, hver søndag, starttidspunkt: 00:00 tt:mm.***
    - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
    - ***Scanningsindstillinger > Scan komprimerede filer.***
    - ***Scanningsindstillinger > Scan OLE-objekter.***
    - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
    - ***CPU-brug > Lavt.***
24. Klik på fanen ***Scan Exclusion*** (Scanningsudeladelser) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:

- ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
- ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
- ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
- Kontrollér, at mappestierne ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** findes i Exclusion List (Udeladelsesliste).

25. Klik på fanen ***Action*** (Handling).
26. Behold standardindstillingerne og fjern markeringen fra følgende funktioner:
    - ***Virus/malware > Vis en meddelelse ved slutpunkterne, når virus/malware registreres.***
    - ***Spyware/grayware > Vis en meddelelse ved slutpunkterne, når spyware/grayware registreres.***
27. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
28. Klik på ***Close*** (Luk) for at lukke siden ***Scheduled Scan Settings*** (Planlagte scanningsindstillinger).
29. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
30. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
31. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Scan Now Settings*** (Scanningsindstillinger > Indstillinger for omgående scanning). Skærmbilledet ***Scan Now Settings*** (Indstillinger for omgående scanning) vises.
32. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Indstillinger for omgående scanning > Aktiver virus/malware-scanning.***
    - ***Indstillinger for omgående scanning > Aktiver spyware/grayware-scanning.***
    - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
    - ***Scanningsindstillinger > Scan komprimerede filer.***
    - ***Scanningsindstillinger > Scan OLE-objekter.***
    - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
    - ***CPU-brug > Lavt.***
33. Klik på fanen ***Scan Exclusion*** (Scanningsudeladelse) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
    - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
    - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
    - Kontrollér, at mappestierne ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** findes i Exclusion List (Udeladelsesliste).
34. Klik på ***Apply to All Agents*** (Anvend på alle agenter).

35. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Scan Now Settings*** (Indstillinger for omgående scanning).
36. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
37. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
38. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Web Reputation Settings*** (Indstillinger for internetomdømme). Skærmbilledet ***Web Reputation Settings*** (Indstillinger for internetomdømme) vises.
39. Klik på fanen ***Internal Agents*** (Interne agenter), og fjern markeringen fra ***Enable Web reputation policy on the following operating systems*** (Aktiver politikker for internetomdømme på følgende operativsystemer), hvis denne allerede er blevet valgt under installering.
40. Klik på fanen ***Internal Agents*** (Interne agenter) og fjern markeringen fra ***Enable Web reputation policy on the following operating systems*** (Aktiver politikker for internetomdømme på følgende operativsystemer), hvis denne allerede er blevet valgt under installering.
41. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
42. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Web Reputation*** (Internetomdømme).
43. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
44. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
45. Fra funktionen ***Settings*** (Indstillinger) vælges ***Behavior Monitoring Settings*** (Indstillinger for adfærdsovervågning). Skærmbilledet ***Behavior Monitoring Settings*** (Indstillinger for adfærdsovervågning) vises.
46. Fjern markeringen fra funktionerne ***Enable Malware Behavior Blocking for known and potential threats*** (Aktiver malware-adfærdsblokering for kendte og mulige trusler) og ***Enable Event Monitoring*** (Aktiver hændelsesovervågning).
47. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
48. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Behavior Monitoring*** (Adfærdsovervågning).
49. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
50. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
51. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Device Control Settings*** (Indstillinger for enhedsstyring). Skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring) vises.
52. Klik på fanen ***External Agents*** (Eksterne agenter) og fjern markeringen fra følgende funktioner:
    - ***Meddelelse > Vis en meddelelse ved slutpunkter, når OfficeScan registrerer ikke-autoriseret adgang på enheder.***
    - ***Bloker AutoRun-funktionen på USB-lagerenheder.***
53. Klik på fanen ***Internal Agents*** (Interne agenter) og fjern markeringen fra følgende funktioner:

- ***Meddelelse > Vis en meddelelse ved slutpunkter, når OfficeScan registrerer ikke-autoriseret adgang på enheder.***
- ***Bloker AutoRun-funktionen på USB-lagerenheder.***

54. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
55. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring).
56. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Device Control Settings*** (Indstillinger for enhedsstyring) igen. Skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring) vises.
57. Klik på fanen ***External Agents*** (Eksterne agenter) og fjern markeringen fra ***Enable Device Control*** (Aktiver enhedsstyring).
58. Klik på fanen ***Internal Agents*** (Interne agenter) og fjern markeringen fra ***Enable Device Control*** (Aktiver enhedsstyring).
59. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
60. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring).
61. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
62. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
63. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Privileges and Other Settings*** (Rettigheder og andre indstillinger).
64. Klik på fanen ***Privileges*** (Rettigheder) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanninger > Konfigurer manuelle scanningsindstillinger.***
    - ***Scanninger > Konfigurer scanningsindstillinger i realtid.***
    - ***Scanninger > Konfigurer planlagte scanningsindstillinger.***
    - ***Proxyindstillinger > Tillad brugere at konfigurere proxyindstillinger.***
    - ***Afinstallering > Adgangskode påkrævet.*** Indtast en egnet adgangskode og bekræft adgangskoden.
    - ***Udpakning og oplåsning > Adgangskode påkrævet.*** Indtast en egnet adgangskode og bekræft adgangskoden.
65. Klik på fanen ***Other Settings*** (Andre indstillinger).
66. Vælg ***OfficeScan Agent Security Settings > Normal: Allow users to access OfficeScan agent files and registries*** (Sikkerhedsindstillinger for OfficeScan Agent > Normal: Tillad brugeradgang til OfficeScan-agentfiler og -registre), og fjern markeringen fra de resterende funktioner.

BEMÆRK: Det er vigtigt at rydde følgende funktioner.

- ***OfficeScan-agent selvforsvar > Beskyt OfficeScan-agenttjenester.***
- ***OfficeScan-agent selvforsvar > Beskyt filer i OfficeScan-agent installationsmappen.***
- ***OfficeScan-agent selvforsvar > Beskyt OfficeScan-agent registernøgler.***
- ***OfficeScan-agent selvforsvar > Beskyt OfficeScan-agentprocesser.***

67. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
68. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Privileges and Other Settings*** (Rettigheder og andre indstillinger).
69. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
70. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
71. Fra funktionen ***Settings*** (Indstillinger) vælges ***Additional Service Settings*** (Yderligere tjenesteindstillinger).
72. Fjern markeringen fra funktionen ***Enable service on the following operating systems*** (Aktiver tjeneste på følgende operativsystemer).
73. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
74. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Additional Service Settings*** (Yderligere tjenesteindstillinger).
75. Vælg linket ***Agents > Global Agent Settings*** (Agenter > Indstillinger for globale agenter) fra den øverste rude.
76. Vælg kun følgende funktioner, og fjern markeringen af de resterende funktioner:
    - ***Scanningsindstillinger for store komprimerede filer > Konfigurer scanningsindstillinger for store komprimerede filer.***
    - ***Scanningsindstillinger for store komprimerede filer > Scan ikke filer i den komprimerede fil, hvis størrelsen overstiger 2 MB***. Følg dette for ***Real-Time Scan*** (Realtidsscanning) og ***Manual Scan/Schedule Scan/Scan Now*** (Manuel scanning/ Planlagt scanning/Omgående scanning).
    - ***Scanningsindstillinger for store komprimerede filer > Scan kun de første 100 filer i en komprimeret fil.*** Følg dette for ***Real-Time Scan*** (Realtidsscanning) og ***Manual Scan/Schedule Scan/Scan Now*** (Manuel scanning/Planlagt scanning/Omgående scanning).
    - ***Scanningsindstillinger > Udelad OfficeScan-serverens databasemappe fra Realtidsscanning.***
    - ***Scanningsindstillinger > Udelad Microsoft Exchange-serverens mapper og filer fra scanninger.***
    - ***Reserveret diskplads > Reserver 60 MB diskplads til opdateringer.***
    - ***Proxykonfiguration > Automatisk registrering af indstillinger.***

BEMÆRK: Det er vigtigt at fjerne markeringen fra ***Alert Settings > Display a notification message*** (Beskedindstillinger > Vis en meddelelse) hvis det er nødvendigt at genstarte slutpunktet for at indlæse en kernetilstandsdriver.

77. Klik på ***Save*** (Gem).
78. Vælg linket ***Updates > Agents > Manual Updates*** (Opdateringer > Agenter > Manuelle opdateringer) fra den øverste rude.
79. Vælg ***Manually select agents*** (Vælg agenter manuelt), og klik på ***Select*** (Vælg).
80. Dobbeltklik på det relevante domænenavn under ***OfficeScan Server*** (OfficeScan-server).
81. Vælg klientsystemer et ad gangen, og klik på ***Initiate Update*** (Start opdatering).

82. Klik på ***OK*** i meddelelsesboksen.

83. Klik på ***Log off*** (Log af) og luk OfficeScan-webkonsollen.

Konfiguration af globale indstillinger for Trend Micro

BEMÆRK: Følgende anvisninger skal kun udføres, når CO_2-funktionen bruges sammen med PDM i Mac-Lab/CardioLab-systemer. Sørg for at gennemgå dem med IT-personale, før du sætter trinnene nedenfor igang.

1. På antivirusadministrationskonsolserveren skal du navigere til mappen *C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV*.

2. Åbn filen ***ofcscan.ini*** i et tekstredigeringsprogram.

3. Under afsnittet Global Setting (Global indstilling) skal du indstille værdien for den følgende nøgle til "**1**": [Global Indstilling] ***RmvTmTDI=1***

4. Gem og luk filen ofcscan.ini.

5. Klik på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > OfficeScan Web Console*** (Start > Alle Programmer > TrendMicro OfficeScan-server - <servernavn> > OfficeScan-webkonsol).

6. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på). Skærmbilledet ***Dashboard*** (Instrumentbræt) vises.

7. Klik på ***Agents > Global Agent Settings*** (Agenter > Globale agentindstillinger).

8. Klik på ***Gem***.

9. Fra venstre rude vælges linket ***Updates > Agents > Manual Update*** (Opdateringer > Agenter > Manuel opdatering).

10. Vælg ***Manually select clients*** (Vælg klienter manuelt) og klik på ***Select*** (Vælg).

11. Klik på det relevante domænenavn under ***OfficeScan Server*** (OfficeScan-server).

12. Vælg klientsystemer et ad gangen, og klik på ***Initiate Update*** (Start opdatering).

13. Klik på ***OK*** i meddelelsesboksen.

14. Udfør følgende på hvert optagesystem:

    a. Åbn register-editoren.

    b. Naviger til ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***

    c. Kontrollér, at registerværdien ***RmvTmTDI*** er indstillet til "***1***".

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

    e. Slet registernøglen ***tmtdi***, hvis den findes.

    f. Luk register-editoren.

    g. Genstart klientsystemerne.

    h. Log på klientsystemerne som administrator eller som medlem af den gruppe.

i. På hvert klientsystem skal du åbne kommandoprompten med administratorrettigheder og indtaste kommandoen "***sc query tmtdi***".

j. Kontrollér, at meddelelsen ***The specified service does not exist as an installed service*** (Den angivne tjeneste findes ikke som installeret tjeneste) vises.

15. På antivirusadministrationskonsolserveren skal du klikke på ***Log off*** (Log af) og lukke OfficeScan-webkonsollen.

Trend Micro OfficeScan – retningslinjer efter installering

1. Aktiver tilbagekoblingsforbindelsen. Se Aktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
2. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser efter installation af antivirus på side 7 for yderligere oplysninger.

Trend Micro OfficeScan klient-/serverudgave XG 12.0

Installationsoversigt

Installer kun Trend Micro OfficeScan klient-/serverudgaven i et netværksforbundet Mac-Lab/CardioLab-miljø. Trend Micro OfficeScan skal installeres på antivirusadministrations-konsolserveren og derefter udrulles til Centricity Cardiology INW-serveren og optagelses-/gennemsynsarbejdsstationerne som klienter. Brug følgende anvisninger til at installere ***Trend Micro OfficeScan Client/Server Edition XG 12.0***.

Virusopdateringer er institutionens ansvar. Opdater definitionerne regelmæssigt for at sikre, at systemet har den nyeste virusbeskyttelse.

Retningslinjer inden installation

BEMÆRK: Der kræves mindst Internet Explorer 10 som IE-browser for at køre OfficeScan-administratoren.

1. Trend Micro antivirusadministrationskonsollen forventes at være installeret i henhold til Trend Micros anvisninger og at fungere korrekt.
2. Under installation af Trend Micro OfficeScan skal du gøre følgende på antivirusadministrationskonsolserveren:

   a. Fjern markeringen fra ***Enable firewall*** (Aktiver Firewall) i vinduet ***Anti-virus Feature*** (Antivirusfunktion).

   b. Vælg ***No, Please do not enable assessment mode*** (Nej tak, aktiver ikke vurderingstilstanden) i vinduet ***Anti-spyware Feature*** (Antispywarefunktion).

   c. Fjern markeringen fra ***Enable web reputation policy*** (Aktiver politik for internetomdømme) i vinduet ***Web Reputation Feature*** (Internetomdømmefunktion).

3. Log på som **Administrator** eller som medlem af den gruppe på alle klientsystemer (optagelse, gennemsyn og INW Server) for at installere antivirussoftwaren.
4. Deaktiver tilbagekoblingsforbindelsen. Se Deaktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.

5. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser før installation af antivirus på side 7 for yderligere oplysninger.
6. Følgende rod- og mellemcertifikater er påkrævede for installering på klientmaskinerne for optagelse, gennemsyn og INW:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
7. Gentag følgende undertrin for at installere de fem påkrævede rod- og mellemniveaucertifikater, som er angivet i trin 6.
   a. Naviger til C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   BEMÆRK: Naviger til C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro på INW.
   b. Hvis ovennævnte mappesti ikke findes, skal du manuelt få fat i de rod- og mellemniveaucertifikater, der er påkrævet til installering.
   c. Dobbeltklik på ***AddTrustExternalCARoot.crt*** for at installere den på MLCL-systemerne (optagelse, gennemsyn og INW).
   d. Luk certifikatet op og klik på ***Install Certificate*** (Installer certifikat).
   e. Klik på ***Next*** (Næste), når ***Certificate Import Wizard*** (Guiden Certifikatimport) vises.
   f. I vinduet ***Certificate Store*** (Certifikatlager) vælges ***Place all certificates in the following store*** (Placer alle certifikater i følgende lager), hvorefter der klikkes på ***Browse*** (Gennemse).
   g. Marker ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Vis fysiske lagre > Pålidelige rodcertifikat-myndigheder > Lokal computer), og klik derefter på ***OK***.
   h. Klik på ***Next*** (Næste) i ***Certificate Import Wizard*** (Guiden Certifikatimport).
   i. Klik på ***Finish*** (Udfør). Meddelelsen ***The import was successful*** (Import fuldført) bør vises.
   j. Gentag trin 7 for de andre certifikater, som angivet i trin 6.

BEMÆRK: Hvert certifikat har en udløbsdato. Når certifikatet er udløbet, skal det fornys og opdateres på MLCL-systemerne for at sikre, at OfficeScan-agenten fungerer som forventet.

Trend Micro OfficeScan – nye installationsudrulningstrin (foretrukket push-installationsmetode for 12.0)

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

BEMÆRK: Fortsæt ved at vælge ***Continue to this website (not recommended)*** (Fortsæt til denne webside (frarådes)). I vinduet Security Alert (Sikkerhedsbeskeder) skal du markere ***In the future, do not show this warning*** (Vis ikke denne advarsel igen) og klikke på ***OK***.

2. Hvis du modtager en certifikatfejlmeddelelse, som angiver, at websiden ikke er pålidelig, skal du administrere certifikaterne, så de inkluderer Trend Micro OfficeScan.
3. Hvis du bliver promptet, skal du installere tilføjelserne ***AtxEnc***. Skærmbilledet Security Warning (Sikkerhedsadvarsel) vises.
    a. Klik på ***Install*** (Installer).
4. Indtast brugernavn og adgangskode og klik på ***Log On*** (Log på).
5. Hvis du bliver promptet, skal du klikke på ***Update Now*** (Opdater nu) for at installere nye widgets. Vent, til de nye widgets er blevet opdateret. Skærmbilledet The update is completed (Opdateringen er fuldført) vises.
    a. Klik på ***OK***.
6. Klik på ***Agents > Agent Installation > Remote*** (Agenter > Agentinstallering > Ekstern) på den øverste menubjælke.
7. Hvis du bliver promptet, skal du installere tilføjelserne ***AtxConsole***. Skærmbilledet Security Warning (Sikkerhedsadvarsel) vises.
    a. Klik på ***Install*** (Installer).
8. Dobbeltklik på ***My Company*** (Min virksomhed) i vinduet ***Remote Installation*** (Ekstern installation). Alle domæner bliver angivet under ***OfficeScan Server*** (OfficeScan-server).
9. Dobbeltklik på domænet (f. eks. INW) fra listen. Alle systemer, der er forbundet med domænet, vises.

BEMÆRK: Hvis der findes domæner eller systemer, der ikke er angivet i vinduet ***Domains and Endpoints*** (Domæner og slutpunkter), skal du gå til Fejlfinding af domæner eller systemer, der ikke er angivet i vinduet Domains and Endpoints (Domæner og slutpunkter) på side 73 for at tilføje dem manuelt eller for at køre installationen direkte fra klientmaskinen.

10. Vælg klientmaskinerne (optagelse, gennemsyn og INW Server), og klik på ***Add*** (Tilføj).
11. Indtast <domænenavn>\brugernavn og adgangskode, og klik på ***Log on*** (Log på).
12. Vælg klientmaskinerne (optagelse, gennemsyn og INW Server) en ad gangen fra ruden ***Selected Endpoints*** (Valgte slutpunkter), og klik på ***Install*** (Installer).
13. Klik på ***Yes*** (Ja) i bekræftelsesvinduet.
14. Klik på ***OK*** i meddelelsesboksen ***Number of agents to which notifications were sent*** (Antal agenter, som har fået tilsendt meddelelser).
15. Genstart alle klientmaskiner (optagelse, gennemsyn og INW Server), og log på som administrator eller som medlem af den gruppe på alle klientmaskiner, og vent, til ikonet Trend Micro OfficeScan i systembakken skifter til blåt med et grønt fluebenssymbol.
16. Klik på linket ***Log Off*** (Log af) for at lukke ***OfficeScan Web Console*** (OfficeScan-webkonsollen).

Trend Micro OfficeScan-serverkonsolkonfiguration for 12.0

1. Vælg ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Start > Programmer > TrendMicro Office Scan-server <servernavn> > Office Scan-webkonsol). Skærmbilledet ***Trend Micro OfficeScan Login*** (Trend Micro OfficeScan logon) vises.
2. Indtast brugernavn og adgangskode og klik på ***Login*** (Log på). Skærmbilledet ***Summary*** (Opsummering) vises.
3. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
4. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
5. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Manual Scan Settings*** (Scanningsindstillinger > Manuelle scanningsindstillinger). Skærmbilledet ***Manual Scan Settings*** (Manuelle scanningsindstillinger) vises.
6. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
   - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
   - ***Scanningsindstillinger > Scan komprimerede filer.***
   - ***Scanningsindstillinger > Scan OLE-objekter.***
   - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
   - ***CPU-brug > Lavt.***
7. Klik på fanen Scan Exclusion (Scanningsudeladelse) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
   - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
   - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
   - ***Scanningsudeladelsesliste (biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret, og vælg Add path to agent Computers Exclusion list (Tilføj sti til udeladelseslisten for agentcomputere).***
   - Vælg ***Adds path*** (Tilføjer sti) fra rullelisten under ***Saving the officescan agent's exclusion list does the following:*** (Når du gemmer OfficsScan-agentens udeladelsesliste, sker følgende:)
   - Gå ind i mapperne **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** og **G:** en ad gangen og klik på ***Add*** (Tilføj).
8. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
9. Klik på ***OK*** ved meddelelsen***The exclusion list on this screen will replace the exclusion list on the agents or domains you selected in the client tree earlier. Do you want to proceed?*** (Udeladelseslisten på dette skærmbillede vil erstatte udeladelseslisten for klienter eller domæner, som tidligere blev valgt i klienttrædiagrammet. Ønsker du at fortsætte?)
10. Klik på ***Close*** (Luk) for at lukke siden ***Manual Scan Settings*** (Manuelle scanningsindstillinger).
11. Vælg linket ***Agent > Agent Management*** (Agent > Agentadministration) fra den øverste rude.

12. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
13. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Scan Settings > Real-time Scan Settings*** (Scanningsindstillinger > Indstillinger for realtidsscanninger). Skærmbilledet ***Real-time Scan Settings*** (Indstillinger for realtidsscanninger) vises.
14. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Indstillinger for realtidsscanninger > Aktiver virus/malware-scanning.***
    - ***Indstillinger for realtidsscanninger > Aktiver spyware/grayware-scanning.***
    - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
    - ***Scanningsindstillinger > Scan komprimerede filer.***
    - ***Scanningsindstillinger > Scan OLE-objekter.***
    - ***Kun virus/malware-scanningsindstillinger > Aktiver IntelliTrap.***
15. Klik på fanen Scan Exclusion (Scanningsudeladelse) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
    - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
    - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
    - Kontrollér, at mappestierne ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** og ***G:*** findes i ***Exclusion List*** (Udeladelsesliste).
16. Klik på fanen ***Action*** (Handling).
17. Behold standardindstillingerne og fjern markeringen fra følgende funktioner:
    - ***Virus/malware > Vis en meddelelse ved slutpunkterne, når virus/malware registreres.***
    - ***Spyware/grayware > Vis en meddelelse ved slutpunkterne, når spyware/grayware registreres.***
18. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
19. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Real-time Scan Settings*** (Indstillinger for realtidsscanning).
20. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
21. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
22. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Scheduled Scan Settings*** (Scanningsindstillinger > Planlagte scanningsindstillinger). Skærmbilledet ***Scheduled Scan Settings*** (Planlagte scanningsindstillinger) vises.
23. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Planlagte scanningsindstillinger > Aktiver virus/malware-scanning.***
    - ***Planlagte scanningsindstillinger > Aktiver spyware/grayware-scanning.***
    - ***Planlægning > Ugentligt, hver søndag, starttidspunkt: 00:00 tt:mm.***

- ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
- ***Scanningsindstillinger > Scan komprimerede filer.***
- ***Scanningsindstillinger > Scan OLE-objekter.***
- ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
- ***CPU-brug > Lavt.***

24. Klik på fanen Scan Exclusion (Scanningsudeladelse) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***
    - ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
    - ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
    - Kontrollér, at mappestierne ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:*** findes i Exclusion List (Udeladelsesliste).
25. Klik på fanen ***Action*** (Handling).
26. Behold standardindstillingerne og fjern markeringen fra følgende funktioner:
    - ***Virus/malware > Vis en meddelelse ved slutpunkterne, når virus/malware registreres.***
    - ***Spyware/grayware > Vis en meddelelse ved slutpunkterne, når spyware/grayware registreres.***
27. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
28. Klik på ***Close*** (Luk) for at lukke siden ***Scheduled Scan Settings*** (Planlagte scanningsindstillinger).
29. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
30. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
31. Fra funktionen ***Settings*** (Indstillinger) vælges ***Scan Settings > Scan Now Settings*** (Scanningsindstillinger > Indstillinger for omgående scanning). Skærmbilledet ***Scan Now Settings*** (Indstillinger for omgående scanning) vises.
32. Klik på fanen ***Target*** (Mål). Vælg kun følgende funktioner, og fjern markeringerne fra de resterende funktioner:
    - ***Indstillinger for omgående scanning > Aktiver virus/malware-scanning.***
    - ***Indstillinger for omgående scanning > Aktiver spyware/grayware-scanning.***
    - ***Filer, der skal scannes > Filtyper scannet af IntelliScan.***
    - ***Scanningsindstillinger > Scan komprimerede filer.***
    - ***Scanningsindstillinger > Scan OLE-objekter.***
    - ***Kun for virus/malware-scanningsindstillinger > Scan startområde.***
    - ***CPU-brug > Lavt.***
33. Klik på fanen ***Scan Exclusion*** (Scanningsudeladelse) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanningsudeladelse > Aktiver scanningsudeladelse.***

- ***Scanningsudeladelse > Anvend scanningsudeladelsesindstillinger til alle scanningstyper.***
- ***Scanningsudeladelsesliste (Biblioteker) > Udelad biblioteker, hvor Trend Micro-produkter er installeret.***
- Kontrollér, at ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** og ***G:***

34. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
35. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Scan Now Settings*** (Indstillinger for omgående scanning).
36. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
37. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
38. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Web Reputation Settings*** (Indstillinger for internetomdømme). Skærmbilledet ***Web Reputation Settings*** (Indstillinger for internetomdømme) vises.
39. Klik på fanen ***External Clients*** (Eksterne klienter) og fjern markeringen fra ***Enable Web reputation policy on the following operating systems*** (Aktiver politikker for internetomdømme på følgende operativsystemer), hvis denne allerede er blevet valgt under installering.
40. Klik på fanen ***Internal Agents*** (Interne agenter) og fjern markeringen fra ***Enable Web reputation policy on the following operating systems*** (Aktiver politikker for internetomdømme på følgende operativsystemer), hvis denne allerede er blevet valgt under installering.
41. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
42. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Web Reputation*** (Internetomdømme).
43. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
44. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
45. Fra funktionen ***Settings*** (Indstillinger) vælges ***Behavior Monitoring Settings*** (Indstillinger for adfærdsovervågning). Skærmbilledet ***Behavior Monitoring Settings*** (Indstillinger for adfærdsovervågning) vises.
46. Fjern markeringen fra funktionerne ***Enable Malware Behavior Blocking*** (Aktiver malware-adfærdsblokering) og ***Enable Event Monitoring*** (Aktiver hændelsesovervågning).
47. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
48. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Behavior Monitoring*** (Adfærdsovervågning).
49. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
50. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
51. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Device Control Settings*** (Indstillinger for enhedsstyring). Skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring) vises.

52. Klik på fanen ***External Agents*** (Eksterne agenter) og fjern markeringen fra følgende funktioner:
    - ***Meddelelse > Vis en meddelelse ved slutpunkter, når OfficeScan registrerer ikke-autoriseret adgang på enheder.***
    - ***Bloker AutoRun-funktionen på USB-lagerenheder.***
    - ***Aktiver enhedsstyring.***
53. Klik på fanen ***Internal Agents*** (Interne agenter) og fjern markeringen fra følgende funktioner:
    - ***Meddelelse > Vis en meddelelse ved slutpunkter, når OfficeScan registrerer ikke-autoriseret adgang på enheder.***
    - ***Bloker AutoRun-funktionen på USB-lagerenheder.***
    - ***Aktiver enhedsstyring.***
54. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
55. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring).
56. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Device Control Settings*** (Indstillinger for enhedsstyring) igen. Skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring) vises.
57. Klik på fanen ***External Agents*** (Eksterne agenter) og fjern markeringen fra ***Enable Device Control*** (Aktiver enhedsstyring).
58. Klik på fanen ***Internal Agents*** (Interne agenter) og fjern markeringen fra ***Enable Device Control*** (Aktiver enhedsstyring).
59. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
60. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Device Control Settings*** (Indstillinger for enhedsstyring).
61. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration).
62. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
63. Fra funktionerne ***Settings*** (Indstillinger) skal du vælge ***Privileges and Other Settings*** (Rettigheder og andre indstillinger).
64. Klik på fanen ***Privileges*** (Rettigheder) og vælg kun følgende funktioner. Fjern markeringen fra de resterende funktioner:
    - ***Scanningsrettigheder > Konfigurer manuelle scanningsindstillinger.***
    - ***Scanningsrettigheder > Konfigurer scanningsindstillinger i realtid.***
    - ***Scanningsrettigheder > Konfigurer planlagte scanningsindstillinger.***
    - ***Proxyindstillingsrettigheder > Tillad agentbrugeren at konfigurere proxyindstillinger.***
    - ***Afinstallering > Adgangskode påkrævet.*** Indtast en egnet adgangskode og bekræft adgangskoden.
    - ***Udpakning og oplåsning > Adgangskode påkrævet.*** Indtast en egnet adgangskode og bekræft adgangskoden.
65. Klik på fanen ***Other Settings*** (Andre indstillinger).
66. Fjern markeringen fra alle funktioner.

BEMÆRK: Det er vigtigt at rydde følgende funktioner.

- ***OfficeScan-agent selvforsvar > Beskyt OfficeScan-agenttjenester.***
- ***OfficeScan-agent selvforsvar > Beskyt filer i OfficeScan-agent installationsmappen.***
- ***OfficeScan-agent selvforsvar > Beskyt OfficeScan-agent registernøgler.***
- ***OfficeScan-agent selvforsvar > Beskyt OfficeScan-agentprocesser.***

67. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
68. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Privileges and Other Settings*** (Rettigheder og andre indstillinger).
69. Vælg linket ***Agents > Agent Management*** (Agenter > Agentadministration) fra den øverste rude.
70. På venstre side skal du vælge ***OfficeScan Server*** (OfficeScan-server).
71. Fra funktionen ***Settings*** (Indstillinger) vælges ***Additional Service Settings*** (Yderligere tjenesteindstillinger).
72. Fjern markeringen fra funktionen ***Enable service on the following operating systems*** (Aktiver tjeneste på følgende operativsystemer).
73. Klik på ***Apply to All Agents*** (Anvend på alle agenter).
74. Klik på ***Close*** (Luk) for at lukke skærmbilledet ***Additional Service Settings*** (Yderligere tjenesteindstillinger).
75. Vælg linket ***Agents > Global Agent Settings*** (Agenter > Indstillinger for globale agenter) fra den øverste rude.
76. Vælg kun følgende funktioner, og fjern markeringen af de resterende funktioner:
    - ***Scanningsindstillinger for store komprimerede filer > Scan ikke filer i den komprimerede fil, hvis størrelsen overstiger 2 MB***. Følg dette for ***Real-Time Scan*** (Realtidsscanning) og ***Manual Scan/Schedule Scan/Scan Now*** (Manuel scanning/ Planlagt scanning/Omgående scanning).
    - ***Scanningsindstillinger for store komprimerede filer > Scan kun de første 100 filer i en komprimeret fil.*** Følg dette for ***Real-Time Scan*** (Realtidsscanning) og ***Manual Scan/ Schedule Scan/Scan Now*** (Manuel scanning/Planlagt scanning/Omgående scanning).
    - ***Scanningsindstillinger > Udelad OfficeScan-serverens databasemappe fra Realtidsscanning.***
    - ***Scanningsindstillinger > Udelad Microsoft Exchange-serverens mapper og filer fra scanninger.***
77. Klik på ***Save*** (Gem).
78. Vælg linket ***Updates > Agents > Manual Updates*** (Opdateringer > Agenter > Manuelle opdateringer) fra den øverste rude.
79. Vælg ***Manually select agents*** (Vælg agenter manuelt), og klik på ***Select*** (Vælg).
80. Dobbeltklik på det relevante domænenavn under ***OfficeScan Server*** (OfficeScan-server).
81. Vælg klientsystemer et ad gangen, og klik på ***Initiate Update*** (Start opdatering).
82. Klik på ***OK*** i meddelelsesboksen.
83. Klik på ***Log off*** (Log af) og luk OfficeScan-webkonsollen.

Trend Micro OfficeScan – retningslinjer efter installering

1. Aktiver tilbagekoblingsforbindelsen. Se Aktivering af tilbagekoblingsforbindelse på side 6 for yderligere oplysninger.
2. Konfigurer tjenesten Computerbrowser. Se Konfiguration af tjenesten Computerbrowser efter installation af antivirus på side 7 for yderligere oplysninger.

Fejlfinding af domæner eller systemer, der ikke er angivet i vinduet Domains and Endpoints (Domæner og slutpunkter)

Under de foretrukne push installationsmetoder til både Trend Micro OfficeScan Klient/Server Edition 11.0 SP1 og Trend Micro OfficeScan Klient/Server Edition XG 12.0 skal domæner og systemer være angivet til at skubbe installationen til systemet. Disse trin giver dig to valgmuligheder for at installere antivirussoftwaren på klienterne (optagelse, gennemsyn og INW).

For 11.0 SP1 henvises der til Trend Micro OfficeScan – nye installationsudrulningstrin (foretrukket push-installationsmetode for 11.0 SP1) på side 55.
For 12.0 henvises der til Trend Micro OfficeScan – nye installationsudrulningstrin (foretrukket push-installationsmetode for 12.0) på side 65.

1. Brug klientmaskinernes (optagelse, gennemsyn og INW) IP-adresser på administrationskonsollen og gør følgende:
    a. Indtast IP'en for hvert klientsystem i boksen ***Search for endpoints*** (Søg efter slutpunkter) en ad gangen og tryk på ***Enter***.
    b. Oplys ***<domain name>\username*** (<domænenavn>\brugernavn) og adgangskode, og klik på ***Log on*** (Log på).
    c. Vælg et af følgende trin baseret på din Trend Micro-version:
        i. For 11.0 SP1 skal du vende tilbage til trin 10 på side 56.
        ii. For 12.0 skal du vende tilbage til trin 10 på side 66.
2. Hvis ikke du kender systemernes IP-adresser, eller hvis den foregående mulighed fejler, skal du gå til hver klientmaskine (optagelse, gennemsyn og INW Server) og gøre følgende:
    a. Log på som **Administrator** eller som medlem af den gruppe på alle klientmaskiner.
    b. Klik på ***Start > Run*** (Start > Kør).
    c. Indtast ***\\<Anti-Virus Management Console_server_IP_address>*** og tryk på ***Enter***. Når du bliver promptet, skal du indtaste administratorbrugernavn og adgangskode.
    d. Naviger til ***\\<Anti-Virus Management Console_server_IP _address>\ofsscan*** og dobbeltklik på ***AutoPcc.exe***. Når du bliver promptet, skal du indtaste administratorbrugernavn og adgangskode.
    e. Genstart klientsystemerne, når installationen er fuldført.
    f. Log på som **Administrator** eller som medlem af den gruppe på alle klientmaskiner, og vent, til Trend Micro OfficeScan-ikonet i systembakken skifter til blåt.
    g. Vælg et af følgende trin baseret på din Trend Micro-version:

i. For 11.0 SP1 henvises der til Trend Micro OfficeScan-serverkonsolkonfiguration for 11.0 SP1 på side 56.

ii. For 12.0 henvises der til Trend Micro OfficeScan-serverkonsolkonfiguration for 12.0 på side 67.