Mac-Lab/CardioLab installationsanvisningar för anti-virusprogram (SV)

Mac-Lab/CardioLab programvaruversion 6.9.6

Inledning

Antivirusprogrammet stödjer regler som syftar till att värna om personlig integritet, t.ex. HIPAA.

Dokumentanvändning

Använd detta dokument för att installera validerade antivirusprogram för Mac-Lab/CardioLab v6.9.6 system.

Revisionshistorik

Reviderad version	Datum	Kommentarer
A	16 februari 2016	Första offentliga utgåvan.
B	9 juni 2016	Trend Micro uppdatering för att stödja CO_2.
C	16 maj 2017	Uppdateringar till McAfee ePolicy Ochestrator, Trend Micro och Symantec.
D	10 juli 2017	Uppdateringar för Symantec 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9, och McAfee VSE 8.8 Patch 9.
E	14 augusti 2017	Ta bort referenser till McAfee ePolicy Orchestrator 5.9 och McAfee VirusScan Enterprise 8.8 Patch 9. Lägg till 6.9.6 R3 gränssnittspråk.
F	25 september 2017	Lägg till McAfee ePO 5.9 och McAfee VSE 8.8 patch 9. Uppdatera länkar för Trend Micro 11 och 12.

Inledande åtgärder

Antiviruskrav

VARNING **INSTALLATION AV ANTIVIRUSPROGRAM KRÄVS**

Systemet levereras utan antivirusskydd. Säkerställ att ett godkänt antivirusprogram är installerat på systemet innan det ansluts till ett nätverk. Avsaknad av ett godkänt virusskydd kan leda till instabilitet eller fel i systemet.

Observera följande krav:

- Antivirusprogram tillhandahålls inte med Mac-Lab/CardioLab-systemet och det åligger kunden att anskaffa, installera och underhålla ett sådant program.
- Kunden bär ansvaret för uppdatering av eventuella virusdefinitionsfiler.
- Kontakta sjukhusets systemadministratör och GE:s tekniska supportavdelning om virus förekommer.
- installera endast de antivirusprogram som anges i listan i avsnittet Validerade antivirusprogram.
- Logga in som administratör eller medlem av denna grupp för att utföra aktiviteter i detta dokument.
- Använd om möjligt ett antivirusprogram på samma språk som operativsystemet. Om det inte finns något godkänt antivirusprogram på samma språk som operativsystemet ska den engelska versionen av antivirusprogrammet installeras.

Validerade antivirusprogram

VARNING **INSTABILT SYSTEM**

Ej godkända antivirusprogram (inklusive ej godkända versioner) får inte installeras eller användas. Det kan ge upphov till instabilitet eller fel i systemet. Använd endast validerade antivirusprogram med korrekt språkversion.

Obs! Om det språkspecifika antivirusprogrammet inte är tillgängligt ska du installera den engelska versionen av antivirusprogrammet.

System med Mac-Lab/CardioLab v 6.9.6 har validerats för användning med de program som anges i följande tabell.

Antivirusprogram som stöds	MLCL-språk som stöds	Version av antivirusprogram som stöds
McAfee VirusScan Enterprise	Engelska, franska, tyska, italienska, spanska, svenska, norska, danska, nederländska, kinesiska, japanska	8.8 Patch 3 8.8 Patch 4 8.8 Patch 8 8.8 Patch 9
McAfee ePolicy Orchestrator (med McAfee VirusScan Enterprise)	Engelska, franska, tyska, italienska, spanska, svenska, norska, danska, nederländska, kinesiska, japanska	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	Engelska, franska, tyska, italienska, spanska, svenska, norska, danska, nederländska, kinesiska, japanska	12.1.2, 12.1.6 MP5, 14.0 MP1
Trend Micro OfficeScan Client/Server Edition	Engelska, franska, tyska, italienska, spanska, svenska, norska, danska, nederländska, kinesiska, japanska	10.6 SP2, 11.0 SP1, XG 12.0

De antivirusprogram som stöds finns på de språk som anges i följande tabell.

MLCL version	MLCL-språk som stöds
M6.9.6 R1	Svenska
M6.9.6 R2	Engelska, franska, tyska
M6.9.6 R3	Engelska, franska, tyska, italienska, spanska, svenska, norska, danska, nederländska, kinesiska, japanska

Antivirushantering – konfiguration av konsolservern

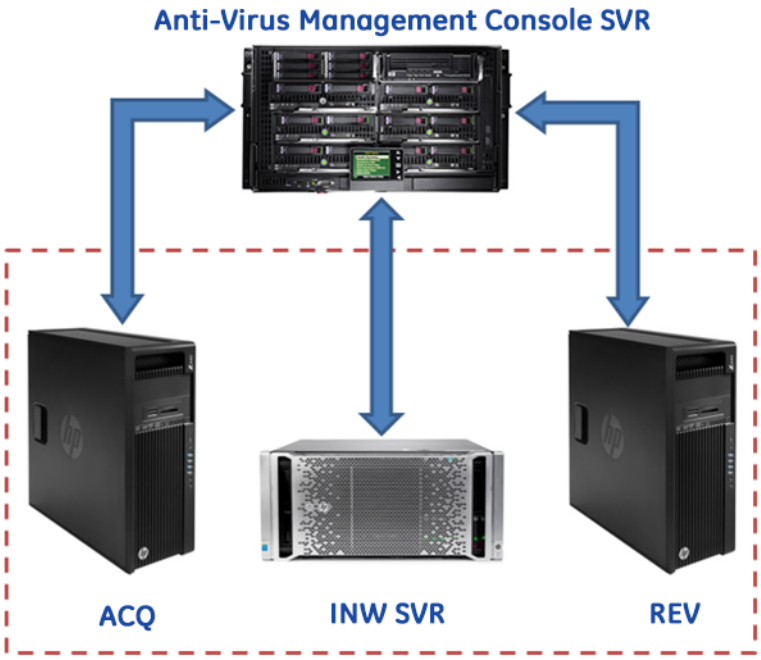
Konsolen för antivirushantering måste vara installerat på konsolservern för antivirushanering.

Kommunikationen mellan konsolservern för antivirushantering och Mac-Lab/CardioLab-enheter kan åstadkommas på olika sätt, beroende på miljön:

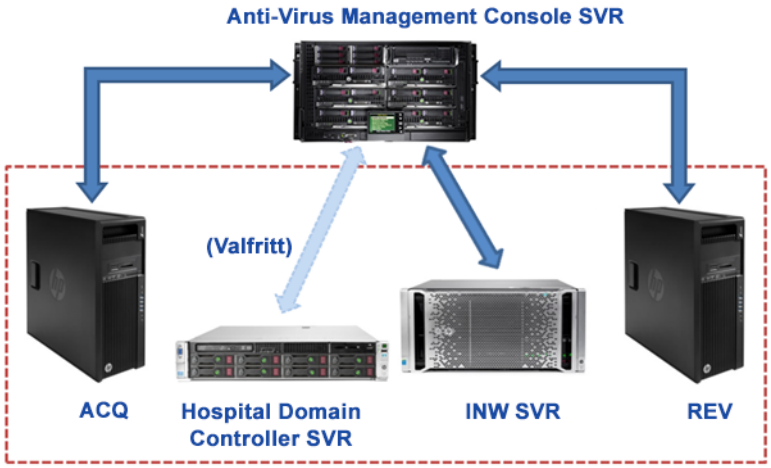
1. INW-domänkontrollmiljön – Konsolen för antivirushantering SVR, som inte är i INW Server-domänen
   - Kommunikationstyp - 1 <Samma nätverk med samma undernätmask>
   - Kommunikationstyp - 2 <Olika nätverk med olika undernätmask>
2. Sjukhusdomänkontrollmiljön – Konsolen för antivirushantering SVR, som inte är i sjukhusdomänkontrollen
   - Kommunikationstyp - 1 <Olika nätverk med olika undernätmask>
3. Sjukhusdomänkontrollmiljön – Konsolen för antivirushantering SVR, som är i sjukhusdomänkontrollen
   - Kommunikationstyp - 1 <Samma nätverk med samma undernätmask>

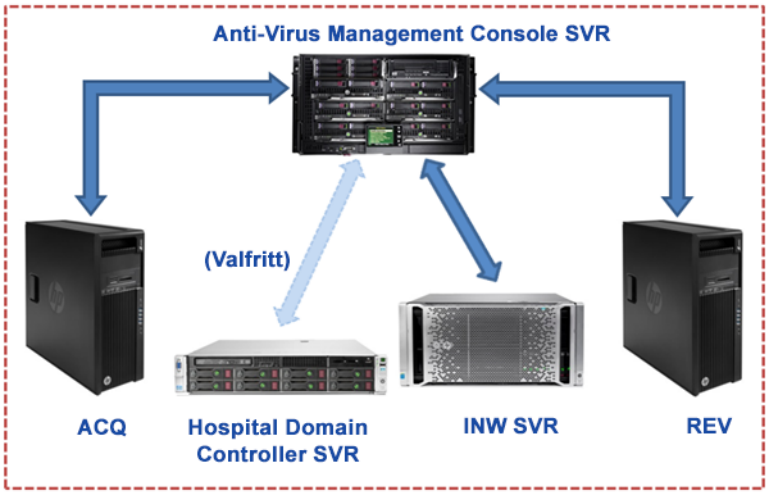
Obs! Konsolservern för antivirushanering bör ha två nätverksportar. En nätverksport för anslutning till Centricity Cardiology INW-nätverket och en sekundär nätverksport för anslutning till sjukhusets nätverk.

Blockdiagram av INW-domänkontrollmiljön



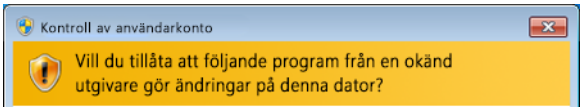
Blockdiagram av sjukhusdomänkontrollmiljön





Kontroll av användarkonto

Kontroll av användarkonto (UAC) är en Windows-funktion som förhindrar otillåtna ändringar i en dator. Under vissa procedurer i denna manual visas ett UAC-meddelande.



När detta meddelande visas till följd av att instruktionerna i denna manual har följts, är det säkert att fortsätta.

Instruktioner för antivirusinstallation

Klicka på det antivirusprogram du vill installera:

- Symantec EndPoint Protection (12.1.2, 12.1.6 MP5 eller 14.0 MP1) på sidan 7
- McAfee VirusScan Enterprise på sidan 16
- McAfee ePolicy Orchestrator på sidan 20
- Trend Micro OfficeScan Client/Server Edition 10.6 SP2 på sidan 43
- Trend Micro OfficeScan Client/Server Edition 11.0 SP1 på sidan 54
- Trend Micro OfficeScan Client/Server Edition XG 12.0 på sidan 65

Vanliga installationsprocedurer för antivirusprogram

Använd procedurerna i det här avsnittet när de hänvisas till i instruktionerna för antivirusinstallation.

Inaktivera loopback-anslutning

Inaktivera loopback-anslutningen på insamlingssystemet som är anslutet till Mac-Lab/CardioLab-miljön, för att alla klientsystem med samma undernätmask i domänen ska kunna detekteras.

1. Logga in som **Administratör** eller medlem av den gruppen.
2. Högerklicka på ***Nätverk*** på skrivbordet och välj ***Egenskaper***.
3. Klicka på ***Change adapter settings*** (Ändra inställningar för adapter).
4. Högerklicka på ***Loopback Connection*** (Loopback-anslutning) och välj ***Inaktivera***.
5. Starta om insamlingssystemet.

Obs! Du måste inaktivera loopback-anslutningen på insamlingssystemet för att alla klientsystem med samma nätmask i domänen ska kunna detekteras.

Aktivera loopback-anslutning

Aktivera loopback-anslutningen på insamlingssystemet som är anslutet till Mac-Lab/CardioLab-miljön, med hjälp av stegen nedan.

1. Logga in som **Administratör** eller medlem av den gruppen.
2. Högerklicka på ***Nätverk*** på skrivbordet och välj ***Egenskaper***.
3. Klicka på ***Change adapter settings*** (Ändra inställningar för adapter).
4. Högerklicka på ***Loopback Connection*** (Loopback-anslutning) och välj ***Enable*** (Aktivera).
5. Starta om insamlingssystemet.

Konfigurera datorlistetjänst före antivirusinstallation

Kontrollera datorlistetjänstens inställning på nätverksanslutna Insamlings- och granskningssystem, för att säkerställa att den är korrekt konfigurerad.

1. Klicka på ***Start > Control Panel > Network and Sharing Center*** (Start > Kontrollpanelen > Nätverks- och delningscenter).
2. Klicka på ***Change advanced sharing settings*** (Ändra avancerade delningsinställningar).
3. Expandera ***Home or Work*** (Hem eller arbete).
4. Se till att ***Turn on file and printer sharing*** (Slå på fil- och skrivardelning) är markerat.
5. Klicka på ***Save changes*** (Spara ändringar).
6. Klicka på ***Start > Run*** (Start > Kör).
7. Skriv in **services.msc** och tryck på **Enter**.
8. Dubbelklicka på ***Computer Browser*** (Datorlistetjänst).
9. Se till att ***Starttyp*** är inställd på ***Automatisk***. Om den inte är inställd på Automatisk, ska du ändra den och klicka på ***Start***.
10. Klicka på ***OK***.
11. Stäng fönstret ***Services*** (Tjänster).

Konfigurera datorlistetjänst efter antivirusinstallation

När du har installerat antivirusprogrammet ska du kontrollera datorlistetjänstens inställning på nätverksanslutna Insamlings- och granskningssystem, för att säkerställa att den är korrekt konfigurerad.

1. Klicka på ***Start > Run*** (Start > Kör).
2. Skriv in **services.msc** och tryck på **Enter**.
3. Dubbelklicka på ***Computer Browser*** (Datorlistetjänst).
4. Ändra ***Starttyp*** till ***Manuell***.
5. Klicka på ***OK***.
6. Stäng fönstret ***Services*** (Tjänster).

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

Installationsöversikt

Installera endast Symantec EndPoint Protection i en nätverksansluten Mac-Lab/CardioLab-miljö. I en nätverksansluten miljö måste Symantec EndPoint Protection installeras på konsolservern för antivirushantering och därefter implementeras på Centricity Cardiology INW-servern och insamlings-/granskningsarbetsstationen som klienter. Använd följande instruktioner för att installera och konfigurera ***Symantec EndPoint Protection***.

Sjukhuset ansvarar för uppdateringen av virusdefinitionerna. Uppdatera definitionerna regelbundet så att systemet alltid har det senaste virusskyddet.

Åtgärder före installation

1. Symantec-konsolen för antivirushantering förväntas installeras enligt Symentecs instruktioner och fungera korrekt.
2. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientsystem (Acquisition, Review och INW Server) för att installera antivirusprogramvaran.
3. Öppna kommandouppmaningen i läget ***Kör som administratör***.
4. Gå till C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

Obs! Konfigurera INW server genom att gå till C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Skriv in **UpdateRegSymantec.ps1** och tryck på ***Enter***.
6. Bekräfta att skriptet utfördes.

   Om ovannämnda mappsökväg inte är närvarande, ska du utföra följande steg för alla MLCL-system, utom MLCL 6.9.6R1 INW-servern (Server OS: Windows Server 2008R2).

   a. Klicka på ***Start-***knappen och sedan ***Kör***.

   b. Skriv in **Regedit.exe** och klicka på ***OK***.

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

   d. Leta upp och dubbelklicka på ***State*** registry (Statligt register).

   e. Ändra ***Base*** (Bas) till ***Decimal***.

   f. Ändra ***Value data*** (Värdedata) till ***146432***.

   g. Klicka på ***OK*** stäng registret.

7. Inaktivera loopback-anslutningen. Närmare information finns i Inaktivera loopback-anslutning på sidan 6.
8. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst före antivirusinstallation på sidan 6.

Symantec EndPoint Protection – Ny installation implementeringssteg (Föredragen push-installationsmetod)

1. Klicka på ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager*** (Starta > Alla program > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager).
2. Ange användarnamn och lösenord för att logga in på Symantec Endpoint Protection Manager. (Klicka på ***Ja*** om ett säkerhetsmeddelande visas.)
3. Kryssa i ***Do not show this Welcome Page again*** (Visa inte denna välkomstsida igen) och klicka på ***Stäng*** för att stänga välkomstskärmen.

Obs! För version 14.0 MP1, ska du klicka på ***Stäng*** för att stänga skärmen ***Getting Started on Symantec EndPoint Protection*** (Komma igång med Symantec EndPoint Protection).

4. Klicka på ***Admin*** i fönstret ***Symantec EndPoint Protection Manager***.
5. Klicka på ***Install Packages*** (Installera paket) i den undre rutan.
6. Klicka på ***Client Install Feature Set*** (Funktionsuppsättning för klientinstallation) i den övre rutan.
7. Högerklicka på fönstret ***Client Install Feature Set*** (Funktionsuppsättning för klientinstallation) och välj ***Lägg till***. Fönstret Add Client Install Feature Set (Lägg till funktionsuppsättning för klientinstallation),
8. Ange lämpligt namn och registrera det eftersom det behövs senare.
9. Se till att ***Feature set version*** (Funktionsuppsättningsversion) är ***12.1 RU2 och högre***.
10. Markera endast följande funktioner och avmarkera de andra funktionerna.
    - ***Virus, Spyware, and Basic Download Protection*** (Virus, Spyware, och grundläggande nedladdningsskydd).
    - ***Advanced Download Protection*** (Avancerat nedladdningsskydd).
11. Klicka på ***OK*** i meddelanderutan.
12. Endast för version 12.1.2 och 12.1.6 MP5, klicka på ***OK*** för att stänga fönstret ***Add Client Install Feature Set*** (Lägg till funktionsuppsättning för klientinstallation).
13. Klicka på ***Home*** (Startskärmen) i fönstret ***Symantec EndPoint Protection Manager***.
14. Beroende på programvarurversionen, ska du göra något av följande:
    - **Version 12.1.2 och 12.1.6 MP5:** Välj ***Install protection client to computers*** (Installera protection-klienten på datorer) i listrutan ***Common Tasks*** (Vanliga uppgifter) överst till höger i fönstret ***Home*** (Start). Skärmen Client Deployment Type (Klientdistributionstyp) visas.
    - **Version 14.0 MP1:** Klicka på ***Clients*** (Klienter) i fönstret ***Symantec EndPoint Protection Manager***. Klicka på ***Install a client*** (Installera en klient) under ***Tasks*** (Uppgifter). Skärmen ***Client Deployment wizard*** (Klientdistributionsguide) visas.
15. Välj ***New Package Deployment*** (Ny paketdistribution) och klicka på ***Nästa***.
16. Välj funktionsuppsättningens namn, som skapats i steg 8. Behåll de andra inställningarna som standard och klicka på ***Nästa***.

Obs! För version 14.1 MP1, under ***Scheduled Scans*** (Schemalagda sökningar), ska du avmarkera ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*** (Fördröj schemalagda sökningar vid körning på batterier, och tillåt att användardefinierade, schemalagda sökningar körs sökningsförfattaren inte är inloggad).

17. Välj ***Remote push*** (Fjärr-push) och klicka på ***Nästa***. Vänta tills skärmen ***Computer selection*** (Datorval) visas.
18. Expandera ***<Domain>*** (Domän) (exempel: INW). System som är anslutna till domänen visas i fönstret ***Computer selection*** (Datorval) fönster.

Obs! Om inga system känns igen, ska du klicka på ***Search Network*** (Sök i nätverket) och klicka på ***Find Computers*** (Hitta datorer). Använd detektionsmetoden ***search by IP address*** (Sök via IP-adress) för att identifiera klientsystemen (Acquisition (Insamling), Review (Granskning) och INW Server).

19. Välj alla Mac-Lab/CardioLab klientmaskliner som är anslutna till domänen och klicka på **>>**. Skärmen ***Inloggningsuppgifter*** visas.
20. Ange användarnamn, lösenord och domän/datornamn och klicka på ***OK***.
21. Se till att alla valda maskiner visas under ***Install Protection Client*** (Installera Protection-klienten) och klicka på ***Nästa***.
22. Klicka på ***Skicka*** och vänta tills Symantec antivirusprogrammet distribuerats på alla klientsystem (Acquisition, Review och INW Server). När du är klar visas skärmen ***Deployment Summary*** (Distributionssammanfattning).
23. Klicka på ***Nästa*** och klicka sedan på ***Slutför*** för att slutföra klientdistributionsguiden.
24. Vänta tills Symantec-ikonen visas i systemfältet, och starta sedan om alla klientmaskiner (Acquisition, Review och INW Server). Logga in som Administratör eller som medlem i denna grupp på alla klientmaskiner efter omstarten.

Konfigurationer för Symantec EndPoint Protection Server Console

1. Klicka på ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager*** (Starta > Alla program > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager). Inloggningsfönstret för Symantec EndPoint Protection Manager öppnas.
2. Ange lösenordet för Symantec Endpoint Protection Manager Console och klicka på ***Log On*** (Logga in).
3. Välj fliken ***Policies*** (Principer) och klicka på ***Virus and Spyware Protection*** (Antivirus- och antispionprogram) under ***Policies***. Fönstret ***Virus and Spyware Protection Policies*** (Princip för virus och spionprogram) öppnas.
4. Klicka på ***Add a Virus and Spyware Protection*** (Lägg till ett program för virus och spionprogram) under ***Tasks*** (Uppgifter). Fönstret ***Virus and Spyware Protection*** (Virus och spionprogram) öppnas.
5. Under ***Windows Settings > Scheduled Scans*** (Windows-inställningar > schemalagda sökningar), ska du klicka på ***Administrator-Defined Scans*** (Administratörsdefinierade sökningar).
6. Välj ***Daily Scheduled Scan*** (Daglig schemalagd sökning) och klicka på ***Edit*** (Redigera). Fönstret ***Edit Scheduled Scan*** (Redigera schemalagd sökning) öppnas.
7. Ändra sökningsnamn och -beskrivning till ***Weekly Scheduled Scan*** (Veckosökning) och ***Weekly Scan at 00:00*** (Veckosökning kl. 00.00).
8. Välj ***Scan type*** (Sökningstyp) som ***Full Scan*** (Fullständig sökning).
9. Välj fliken ***Schedule*** (Schemalägg).
10. Under ***Scanning Schedule*** (Sökningsschema), ska du välja ***Weekly*** (Varje vecka) och ändra tiden till ***00:00***.

11. Under ***Scan Duration*** (Sökningsduration) ska du avmarkera ***Randomize scan start time within this period (recommended in VMs)*** (Randomisera sökningens starttid inom denna period (rekommenderas i VMs) och välja ***Scan until finished (recommended to optimize scan performance)*** (Sök tills klar (rekommenderas för att optimera sökningen)).

12. Under ***Missed scheduled Scans*** (Missade schemalagda sökningar) ska du avmarkera ***Retry the scan within*** (Försök sökningen igen inuti).

13. Välj fliken ***Notifications*** (Meddelanden).

14. Avmarkera ***Display notification message on infected computer*** (Visa meddelande på infekterad dator) och klicka på ***OK***.

15. Välj fliken ***Advanced*** (Avancerat) i fönstret ***Administrator-Defined Scans*** (Administratörsdefinierade sökningar).

16. Under ***Scheduled Scans*** (Schemalagda sökningar), ska du avmarkera ***Delay scheduled scans when running on batteries***, ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Fördröj schemalagda sökningar vid körning på batterier, och tillåt att användardefinierade, schemalagda sökningar körs sökningsförfattareb inte är inloggad), och ***Display notifications about detections when the user logs on*** (Visa meddelanden om upptäckter när användaren loggar in).

Obs! För version 14.0 MP1, under ***Scheduled Scans*** (Schemalagda sökningar), ska du avmarkera ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*** (Fördröj schemalagda sökningar vid körning på batterier, och tillåt att användardefinierade, schemalagda sökningar körs sökningsförfattaren inte är inloggad).

17. Under ***Startup and Triggered Scans*** (Start och triggade sökningar) ***Run an Active Scan when new definitions arrive*** (Kör en aktiv sökning när nya definitioner anländer).

18. Under ***Windows Settings > Protection Technology***, (Windows-inställningar > Protection Technology), ska du klicka på ***Auto-Protect*** (Skydda automatiskt).

19. Välj fliken ***Scan Details*** (Sökningsinformation) och välj och lås ***Enable Auto-Protect*** (Aktivera Auto-Protect).

20. Välj fliken ***Notifications*** (Meddelanden) och avmarkera och lås ***Display a notification message on the infected computer och Display the Auto-Protect results dialog on the infected Computer*** (Visa meddelande på infekterad dator och Visa dialogruta för autoskyddsresultat på infekterad dator).

21. Välj fliken ***Advanced*** (Avancerat) och under ***Auto-Protect Reloading and Enablement*** (Skydda omladdning och aktivering automatiskt), lås alternativet ***When Auto-Protect is disabled, Enable after:*** (När Auto-Protect är inaktivera, aktivera efter).

22. Under ***Additional Options*** (Fler alternativ) ska du klicka på ***File Cache*** (Fil-cache). Fönstret ***File Cache*** (Fil-cache) öppnas.

23. Avmarkera ***Rescan cache when new definitions load*** (Sök på cache igennär nya definitioner laddas) och klicka på ***OK***.

24. Under ***Windows Settings > Protection Technology***, (Windows-inställningar > Protection Technology), ska du klicka på ***Download Protection*** (Nedladdningsskydd).

25. Välj fliken ***Notifications*** (Meddelanden) och avmarkera och lås ***Display a notification message on the infected computer*** (Visa meddelande på den infekterade datorn).

26. Under ***Windows Settings > Protection Technology***, (Windows-inställningar > Protection Technology), ska du klicka på ***SONAR***.

27. Välj fliken ***SONAR Settings*** (SONAR-inställningar) och avmarkera och lås ***Enable SONAR*** (Aktivera SONAR).

28. Under ***Windows Settings > Protection Technology***, (Windows-inställningar > Protection Technology) ska du klicka på ***Early Launch Anti-Malware Driver*** (Tidig start av programdrivrutin mot skadlig kod).

29. Avmarkera och lås ***Enable Symantec early lauch anti-malware*** (Aktivera Symantec tidig start av programd mot skadlig kod).

30. Under ***Windows Settings > Email Scans***, (Windows-inställningar > E-postsökningar), ska du klicka på ***Internet Email Auto-Protect*** (Skydda internet-e-post automatiskt).

31. Välj fliken ***Scan Details*** (Sökningsinformation) och välj och lås ***Enable Email Auto-Protect*** (Aktivera Auto-Protect av e-postmeddelanden).

32. Välj fliken ***Notifications*** (Meddelanden) och avmarkera och lås alternativen ***Display a notification message on the infected computer*** (Visa ett meddelande på den infekterade datorn), ***Display a progress indicator when email is being sent*** (Visa förloppsindikator när e-post skickas), och ***Display a notification area icon*** (Visa meddelandeområdesikon).

33. Under ***Windows Settings > Email Scans***, (Windows-inställningar > E-postsökningar), ska du klicka på ***Microsoft Outlook Auto-Protect*** (Skydda Microsoft Outlook automatiskt).

34. Välj fliken ***Scan Details*** (Sökningsinformation) och välj och lås ***Enable Microsoft Outlook Auto-Protect*** (Aktivera Microsoft Outlook automatiskt Auto-Protect).

35. Välj fliken ***Notifications*** (Meddelanden) och avmarkera och lås ***Display a notification message on the infected computer*** (Visa meddelande på den infekterade datorn).

36. Under ***Windows Settings > Email Scans***, (Windows-inställningar > E-postsökningar), ska du klicka på ***Lotus Notes Auto-Protect*** (Skydda Lotus Notes automatiskt).

37. Välj fliken ***Scan Details*** (Sökningsinformation) och avmarkera och lås ***Enable Lotus Notes Auto-Protect*** (Aktivera Auto-Protect av Lotus Notes).

38. Välj fliken ***Notifications*** (Meddelanden) och avmarkera och lås ***Display a notification message on infected computer*** (Visa meddelande på infekterad dator).

39. Under ***Windows Settings > Advanced Options*** (Windows-inställningar > avancerade alternativ), ska du klicka på ***Global Scan Options*** (Globala sökningsalternativ).

40. Under ***Bloodhound(™) Detection Settings*** (Bloodhound(™) detektionsinställningar), ska du avmarkera och låsa ***Enable Bloodhound(™) heuristic virus detection*** (Aktivera Bloodhound(™) heuristisk virusdetektion).

41. Under ***Windows Settings > Advanced Options*** (Windows-inställningar > avancerade alternativ), ska du klicka på ***Quarantine*** (Sätt i karantän).

42. Välj fliken ***General*** (Allmänt), under ***When New Virus Definitions Arrive*** (När nya virusdefinitioner anländer), ska du välja ***Do nothing*** (Gör ingenting).

43. Under ***Windows Settings > Advanced Options*** (Windows-inställningar > avancerade alternativ), ska du klicka på ***Miscellaneous*** (Diverse).

44. Välj fliken ***Notifications*** (Meddelanden) och avmarkera ***Display a notification message on the client computer when definitions are outdated*** (Visa ett meddelande på klientdatorn

när definitionerna är utdaterade), ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions*** (Visa ett meddelande på klientdatorn när definitionerna när Symantec Endpoint Protection körs utan virusdefinitioner) och ***Display error messages with a URL to a solution*** (Visa felmeddelanden med en URL till en lösning).

45. Klicka på ***OK*** för att stänga principfönstret ***Virus and Spyware Protection*** (Skydd mot virus och spionprogram).
46. Klicka på ***Yes*** (Ja) i meddelanderutan ***Assign Policies*** (Tilldela principer).
47. Välj ***My Company*** (Mitt företag) och klicka på ***Assign*** (Tilldela).
48. Klicka på ***Yes*** (Ja) i meddelanderutan.
49. Under ***Policies*** (Principer), ska du klicka på ***Firewall*** (Brandvägg).
50. Klicka på ***Firewall policy*** (Brandväggsprincip) under ***Firewall Policies*** (Brandväggsprinciper) och klicka på ***Edit the policy*** (Redigera princip) under ***Tasks*** (Uppgifter).
51. Välj fliken ***Policy Name*** (Principnamn) och avmarkera ***Enable this policy*** (Aktivera denna princip).
52. Klicka på ***OK***.
53. Under ***Policies*** (Principer) ska du klicka på ***Intrusion Prevention*** (Intrångsskydd).
54. Klicka på ***Intrusion Prevention*** (Intrångsskydd) under ***Intrusion Prevention Policies*** (Principer för intrångsskydd) och klicka på ***Edit the policy*** (Redigera princip) under ***Tasks*** (Uppgifter).
55. Välj fliken ***Policy Name*** (Principnamn) och avmarkera ***Enable this policy*** (Aktivera denna princip).
56. Beroende på programvarurversionen, ska du göra något av följande:
    - **Version 12.1.2:** Klicka på ***Settings*** (Inställningar från) från vänster ruta.
    - **Versions 12.1.6 MP5 och 14.0 MP1:** Klicka på ***Intrusion Prevention*** (Intrångsskydd) från vänster ruta.
57. Avmarkera och lås ***Enable Network Intrusion Prevention*** (Aktivera intrångsskydd för nätverket) och ***Enable Browser Intrusion Prevention for Windows*** (Aktivera intrångsskydd för Windows webbläsare).
58. Klicka på ***OK***.
59. Under ***Policies*** (Principer) ska du klicka på ***Application and Device Control*** (Program- och enhetskontroll).
60. Klicka på ***Application and Device Control Policy*** (Princip för program- och enhetskontroll) under ***Application and Device Control Policies*** (Principer för program- och enhetskontroll) och klicka på ***Edit the policy*** (Redigera principen) under ***Tasks*** (Uppgifter).
61. Välj fliken ***Policy Name*** (Principnamn) och avmarkera ***Enable this policy*** (Aktivera denna princip).
62. Klicka på ***OK***.
63. Under ***Policies*** (Principer), ska du klicka på ***LiveUpdate***.

64. Välj ***LiveUpdate Settings policy*** (Princip för inställningar av LiveUpdate) och under ***Tasks*** (Uppgifter), ska du klicka på ***Edit the policy*** (Redigera principen).

65. Under ***Overview > Windows Settings*** (Översikt > Windows-inställningar), ska du klicka på ***Server Settings*** (Serverinställningar).

66. Under ***Internal or External LiveUpdate Server*** (Inter eller extern LiveUpdate-server), ska du säkerställa att ***Use the default management server*** (Använd standardhanteringsservern) är vald och avmarkera ***Use a LiveUpdate server*** (Använd en LiveUpdate-server).

67. Klicka på ***OK***.

68. Under ***Policies*** (Principer), ska du klicka på ***Exceptions*** (Undantag).

69. Klicka på ***Exceptions policy*** (Princip för undantag) och under ***Tasks*** (Uppgifter), ska du klicka på ***Edit the policy*** (Redigera principen).

70. Beroende på programvarurversionen, ska du göra något av följande:

    - **Version 12.1.2 och 12.1.6 MP5:** Klicka på ***Exceptions > Add > Windows Exceptions > Folder*** (Undantag > Lägg till > Windows-undantag > Mapp).
    - **Version 14.0 MP1:** Klicka på listrutan ***Add*** (Lägg till) och välj ***Windows Exceptions > Folder*** (Windows-undantag > Mapp).

71. Ange **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:**, **G:** mappsökvägar, en i taget, och gör följande:

    a. Säkerställ att ***Include subfolders*** (Inkludera undermappar) är vald.

Obs! Klicka på ***Yes*** (Ja) om meddelanderutan ***Are you sure you want to exclude all subfolders from protection?*** (Är du säker du vill utesluta alla undermappar från skydd?) visas.

    b. Välj ***All*** (Allt) från ***Specify the type of scan that excludes this folder*** (Ange typ av sökning som utesluter denna mapp).

    c. För version 14.0 MP1, klicka på ***OK*** för att lägga till undantaget.

72. Klicka på ***OK***.

73. Klicka på ***Assign the policy*** (Tilldela principen) under ***Tasks*** (Uppgifter).

74. Välj ***My Company*** (Mitt företag) och klicka på ***Assign*** (Tilldela).

75. Klicka på ***Yes*** (Ja).

76. Klicka på ***Clients*** (Klienter) från vänster ruta och välj fliken ***Policies*** (Principer).

77. Under ***My Company*** (Mitt företag), ska du välja ***Default Group*** (Standardgrupp) och avmarkera ***Inherit policies and settings from parent group "My Company"*** (Överför principer och inställningar från den överordnade gruppen ”Mitt företag”) och klicka på ***Communications Settings*** (Kommunikationsinställningar) under ***Location-Independent Policies and Settings*** (Platsoberoende principer och inställningar).

Obs! Om ett varningsmeddelande visas, klicka på ***OK*** och klicka på ***Communications Settings*** (Kommunikationsinställningar) under ***Location-Independent Policies and Settings*** (Platsoberoende principer och inställningar) igen.

78. Under ***Download*** (Ladda ned), ska du säkerställa att ***Download policies and content from the management server*** (Ladda ned principer och innehåll från hanteringsservern) är markerad och ***Push mode*** (Push-läge) valt.

79. Klicka på ***OK***.

80. Klicka på ***General Settings*** (Allmänna inställningar) under ***Location-independent Policies and Settings*** (Platsoberoende principer och inställningar).

81. Välj fliken ***Tamper Protection*** (Manipuleringsskydd) och avmarkera och ***Protect Symantec security software from being tampered with or shut down*** (Skydda Symantecs säkerhetsprogramvara mot att manipuleras eller stängas av).

82. Klicka på ***OK***.

83. Klicka på ***Admin*** och välj ***Servers*** (Servrar).

84. Under ***Servers*** (Servrar), ska du välja ***Local Site (My Site)*** (Lokal plats (Min plats)).

85. Under ***Tasks*** (Uppgifter), ska du välja ***Edit Site Properties*** (Redigera platsegenskaper) . Fönstret ***Site Properties for Locate Site (My Site)*** (Platsegenskaper för lokal plats (Min plats) öppnas.

86. Välj fliken ***LiveUpdate*** och under ***Download Schedule*** (Ladda ned schema) ska du säkerställa att schemat är inställt på ***Every 4 hour(s)*** (Var fjärde timme).

87. Klicka på ***OK***.

88. Klicka på ***Log Off*** (Logga ut) och stäng Symantec EndPoint Protection Manager Console. Säkerställ att Symantec Endpoint Protection-principer förs vidare i klientsystemen.

Riktlinjer för installation av Symantec EndPoint Protection

1. Aktivera loopback-anslutningen. Närmare information finns i Aktivera loopback-anslutning på sidan 6.

2. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst efter antivirusinstallation på sidan 7.

3. Öppna kommandouppmaningen i läget ***Kör som administratör***.

4. Gå till C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

Obs! Konfigurera INW server genom att gå till C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Skriv in **RestoreRegSymantec.ps1** och tryck på ***Enter***.

   6.Bekräfta att skriptet utfördes.
   Obs! Du måste bekräfta att **RestoreRegSymantec.ps1**-skriptet är korrekt exekverat innan du fortsätter.

   Om ovannämnda mappsökväg inte är närvarande, ska du utföra följande steg för alla MLCL-system, utom MLCL 6.9.6R1 INW-servern (Server OS: Windows Server 2008R2).

   a. Klicka på ***Start-***knappen och sedan ***Kör***.

   b. Skriv in **Regedit.exe** och klicka på ***OK***.

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

d. Leta upp och dubbelklicka på ***State*** registry (Statligt register).

e. Ändra ***Base*** (Bas) till ***Decimal***.

f. Ändra ***Value data*** (Värdedata) till ***65536***.

g. Klicka på ***OK*** stäng registret.

McAfee VirusScan Enterprise

Installationsöversikt

McAfee VirusScan Enterprise bör installeras på ett enskilt Mac-Lab/CardioLab-system, och det bör hanteras individuellt. Använd följande instruktioner för att installera och konfigurera McAfee VirusScan Enterprise.

Sjukhuset ansvarar för uppdateringen av virusdefinitionerna. Uppdatera definitionerna regelbundet så att systemet alltid har det senaste virusskyddet.

Installationsprocedur för McAfee VirusScan Enterprise

1. Logga in som **Administratör** eller som medlem av den gruppen.
2. Sätt i antingen **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-enheten.
3. Dubbelklicka på ***SetupVSE.Exe***. Dialogrutan Windows Defender visas.
4. Klicka på ***Yes*** (Ja). Skärmen McAfee VirusScan Enterprise Setup visas.
5. Klicka på ***Next*** (Nästa). Skärmen McAfee End User License Agreement (Licensavtal för slutanvändare) visas.
6. Läs licensavtalet och fyll i alla nödvändiga fält, klicka på ***OK*** när du är klar. Skärmen Select Setup Type (Välj inställningstyp) visas.
7. Välj ***Typical*** (Typisk) och klicka på ***Next*** (Nästa). Skärmen Select Access Protection Level (Välj skyddsnivå för åtkomst) visas.
8. Välj ***Standard Protection*** (Standardskydd) och klicka på ***Next*** (Nästa). Skärmen Ready to Install (Klar att installera) visas.
9. Klicka på ***Install*** (Installera) och vänta tills installationen slutförts. Efter lyckad installation av McAfee VirusScan Enterprise, visas skärmen ***McAfee Virus Scan Enterprise Setup has completed successfully*** (Installation av McAfee Virus Scan Enterprise har utförts).
10. Avmarkera kryssrutan ***Run On-Demand Scan*** (Kör sökning på begäran) och klicka på ***Finish*** (Slutför).
11. Om fönstret ***Update in Progress*** (Uppdatering pågår) visas, ska du klicka på ***Cancel*** (Avbryt).

12. Om en meddelanderuta om att starta om systemet visas, ska du klicka på ***OK***.
13. Starta om systemet.
14. Logga in som **Administratör** eller som medlem av den gruppen.

Konfiguration av McAfee VirusScan Enterprise

1. Klicka på ***Start > All Programs > McAfee > VirusScan Console*** (Starta > Alla program > McAfee > VirusScan-konsol). Skärmen ***VirusScan Console*** (VirusScan-konsol) visas.
2. Högerklicka på ***Access Protection*** Åtkomstskydd) och välj ***Properties*** (Egenskaper). Skärmen ***Access Protection*** (Åtkomskydd) visas.
3. Klicka på fliken ***Access Protection*** (Åtkomstsskydd) och avmarkera ***Enable access protection*** (Aktivera åtkomstskydd) och ***Prevent McAfee services from being stopped*** (Förhindra McAfee-tjänster från att stoppas).
4. Klicka på ***OK***.
5. Högerklicka på ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning) och välj ***Properties*** (Egenskaper). Skärmen ***Buffer Overflow Protection Properties*** (Egenskaper för skydd mot buffertöverskridning) visas.
6. Klicka på fliken ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning) och avmarkera ***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings*** (Visa dialogrutan när en buffertöverskridning detekteras under inställningarna för buffertöverskridning).
7. Avmarkera ***Enable buffer overflow protection*** (Aktivera skydd mot buffertöverskridning) under ***Buffer overflow settings*** (Inställningar för buffertöverskridning).
8. Klicka på ***OK***.
9. Högerklicka på ***On-Delivery Email Scanner*** (Söker efter e-post vid leverans) och välj ***Properties*** (Egenskaper). Skärmen ***On-Delivery Email Scanner Properties*** (Egenskaper för Söner efter e-post vid leverans) visas.
10. Klicka på fliken ***Scan items*** (Sök objekt) och avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown program threats and trojans*** (Hitta okända programhot och trojaner).
    - ***Find unknown macro threats*** (Hitta okända makrohot).
    - ***Find attachments with multiple extensions*** (Hitta bilagor med flera tillägg).
11. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
12. Välj ***Disabled*** (Inaktiverad) för ***Sensitivity level*** (Känslighetsnivå) under ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
13. Klicka på ***OK***.
14. Högerklicka på ***On-Delivery Email Scanner*** (Sökning för e-post vid leverans) och välj ***Disable*** (Inaktivera).

15. Högerklicka på ***On-Access Scanner*** (Sökning vid åtkomst) och välj ***Properties*** (Egenskaper). Skärmen ***On-Access Scan Properties*** (Egenskaper för sökning vid åtkomst) visas.

16. Klicka på fliken ***General*** (Allmänt) och välj ***Disabled*** (Inaktiverad) för ***Sensitivity level*** (Känslighetsnivå) under ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).

17. Klicka på fliken ***ScriptScan*** (Skriptsökning) och avmarkera ***Enable scanning of scripts*** (Aktivera sökning av skript).

18. Klicka på fliken ***Blocking*** (Blockering) och avmarkera ***Block the connection when a threat is detected in a shared folder*** (Blockera anslutningen när ett hot upptäcks i en delad mapp).

19. Klicka på fliken ***Messages*** (MeddelandenI och avmarkera ***Show the messages dialog when a threat is detected and display the specified text in the message*** (Visa meddelandedialogrutan när ett hot detekteras och visa den specificerade texten i meddelandet).

20. Klicka på ***All Processes*** (Alla) från den vänstra rutan.

21. Klicka på fliken ***Scan Items*** (Sök objekt) och avmarkera följande alternativ under Heuristics (Heuristik).

    - ***Find unknown unwanted programs and trojans*** (Hitta okända, oönskade program och trojaner).
    - ***Find unknown macro threats*** (Hitta okända makrohot).

22. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).

23. Klicka på fliken ***Exclusions*** (Undantag) och klicka på ***Exclusions***. Skärmen ***Set Exclusions*** (Ställ in undantag) visas.

24. Klicka på ***Add*** (Lägg till). Skärmen ***Add Exclusion Item*** Lägg till undantaget objekt) visas.

25. Välj ***By name/location*** (Enligt namn(plats) och klicka på ***Browse*** (Bläddra). Skärmen ***Browse for Files or Folders*** (Sök efter filer eller mappar) visas.

26. Gå till ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** mapparna, en åt gången, och tryck på ***OK***.

27. Välj ***Also exclude subfolders*** (Uteslut även undermappar) i fönstret ***Add Exclusion Item*** (Lägg till undantaget objekt) och klicka på ***OK***.

28. Se till att mapparna C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ finns i fönstret Set Exclusions (Ställ in undantag).

29. Klicka på ***OK***.

30. Högerklicka på ***AutoUpdate*** (Automatisk uppdatering) och välj ***Properties*** (Egenskaper). Skärmen McAfee AutoUpdate Properties – AutoUpdate öppnas.

31. Avmarkera följande alternativ under ***Update Options*** (Uppdateringsalternativ):

    - ***Get new detection engine and dats if available*** (Få nya detektionsmotor och datum om tillgängligt).
    - ***Get other available updates (service packs, upgrades, etc.)*** (Få andra tillgängliga uppdateringar (servicepack, uppgraderingar, etc.).

32. Klicka på ***Schedule*** (Schema). Skärmen Schedule Settings (Schemainställningar) visas.
33. Avmarkera ***Enable (scheduled task runs at specified time)*** (Aktivera (schemalagd aktivitet körs vid angiven tid) under ***Schedule Settings*** (Schemainställningar).
34. Klicka på ***OK***.
35. Klicka på ***OK***.
36. Högerklicka på fönstret ***VirusScan Console*** (VirusScan-konsol) och välj ***New On-Demand Scan Task*** (Ny sökningsuppgift på begäran).
37. Döp om den nya sökningen till ***Weekly Scheduled Scan*** (Schemalagd sökning varje vecka). Skärmen ***On-Demand Scan Properties - Weekly Scheduled Scan*** (Egenskaper för sökning på begäran – Schemalagd sökning varje vecka) visas.
38. Klicka på fliken ***Scan Items*** (Sök objekt) och avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Options*** (Alternativ).
39. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown programs threats*** (Hitta okända programhot).
    - ***Find unknown macro threats*** (Hitta okända makrohot).
40. Klicka på fliken ***Exclusions*** (Undantag) och klicka på ***Exclusions***. Skärmen ***Set Exclusions*** (Ställ in undantag) visas.
41. Klicka på ***Add*** (Lägg till). Skärmen ***Add Exclusion Item*** Lägg till undantaget objekt) visas.
42. Välj ***By name/location*** (Enligt namn(plats) och klicka på ***Browse*** (Bläddra). Skärmen ***Browse for Files or Folders*** (Sök efter filer eller mappar) visas.
43. Gå till mapparna ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:***, en åt gången, och tryck på ***OK***.
44. Välj ***Also exclude subfolders*** (Uteslut även undermappar) i fönstret ***Add Exclusion Item*** (Lägg till undantaget objekt) och klicka på ***OK***.
45. Se till att mapparna ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** finns i fönstret ***Set Exclusions*** (Ställ in undantag).
46. Klicka på ***OK***.
47. Klicka på fliken ***Performance*** (Prestanda) och välj ***Disabled*** (Inaktiverad) för ***Sensitivity level*** (Känslighetsnivå) under ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
48. Klicka på ***Schedule*** (Schema). Skärmen ***Schedule Settings*** (Schemainställningar) visas.
49. Klicka på fliken ***Task*** (Uppgift) och välj ***Enable (scheduled task runs at specified time)*** (Aktivera (schemalagda uppgiftskörningar vid angiven tidpunkt) under ***Schedule Settings*** (Schemainställningar).
50. Klicka på fliken ***Schedule*** (Schema) och välj följande:
    a. Run task (Kör uppgiften): Weekly (Varje vecka).
    b. Starttid: 12:00 AM (12.00)
    c. Every (Varje): 1 Weeks, Sunday (Vecka, söndag).
51. Klicka på ***OK***.

52. Klicka på ***OK***.
53. Klicka på ***Tools > Alerts*** (Verktyg > Varningar) i fönstret ***VirusScan Console*** (VirusScan-konsolen). Skärmen Alert Properties (Varningsegenskaper) visas.
54. Avmarkera kryssrutorna ***On-Access Scan*** (Sökning vid åtkomst), ***On-Demand Scan and scheduled scans*** (Sökning på begäran och schemalagda sökningar), ***Email Scan*** (E-postsökning) och ***AutoUpdate*** (Autouppdatering).
55. Klicka på ***Destination***. Skärmen ***Alert Manager Client Configuration*** (Konfigurering av varningshanterarklient) visas.
56. Markera kryssrutan ***Disable alerting*** (Inaktivera varning).
57. Klicka på ***OK***. Skärmen ***Alert Properties*** (Varningsegenskaper) visas.
58. Välj fliken ***Additional Alerting Options*** (Fler varningsalternativ).
59. Välj alternativet ***Suppress all alerts (severities 0 to 4)*** i listrutan ***Severity Filter*** (Filter för allvarsgrad).
60. Välj fliken ***Alert Manager Alerts*** (Varningar i varningshanteraren).
61. Avmarkera kryssrutan ***Access Protection*** (Åtkomstskydd).
62. Klicka på ***OK*** så att dialogrutan ***Alert Properties*** (Varningsegenskaper) stängs.
63. Stäng fönstret ***VirusScan Console*** (VirusScan-konsolen).

McAfee ePolicy Orchestrator

Installationsöversikt

Installeraendast McAfee ePolicy Orchestrator i en nätverksansluten Mac-Lab/CardioLab-miljö. McAfee ePolicy Orchestrator måste installeras på en Anti-virus Management Console-server och McAfee VirusScan Enterprise bör distribueras till Centricity Cardiology INW-servern och Acquisition/Review-arbetsstationer som en klient. Använd följande instruktioner för att installera och konfigurera McAfee ePolicy Orchestrator.

Instruktionerna nedan för pushing och konfiguration av McAfee VirusScan Enterprise stöder Patch 3, Patch 4, Patch 8 och Patch 9.

Sjukhuset ansvarar för uppdateringen av virusdefinitionerna. Uppdatera definitionerna regelbundet så att systemet alltid har det senaste virusskyddet.

Åtgärder före installation

1. McAfee Anti-Virus Management Console förväntas installeras enligt McAfees instruktioner och fungera korrekt.
2. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientsystem (Acquisition, Review och INW Server) för att installera antivirusprogramvaran.
3. Inaktivera loopback-anslutningen. Närmare information finns i Inaktivera loopback-anslutning på sidan 6.

4. För att implementera McAfee VirusScan Enterprise 8.8 patch 9 kontaktar du McAfee för att installera UTN-USERFirst-Object- och VeriSign Universal-rotcertifikat på INW-servrar (endast). Starta om systemet när certifikaten är installerade.

Obs! Om UTN-USERFirst-Object- och VeriSign Universal-rotcertifikaten inte är installerade går det inte att installera McAfee VirusScan Enterprise 8.8 patch 9 på INW-servrar.

5. För nyinstallation, lägg till följande agentversion till McAfee ePolicy Orchestrator masterdatabasen i McAfee ePolicy Orchestrator Console: ***- McAfee Agent v5.0.5.658***

6. För nyinstallation, lägg till följande paket till McAfee ePolicy Orchestrator masterdatabasen i McAfee ePolicy Orchestrator Console:

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

Obs! VSE880LMLRP3.zip innehåller Patch 2 och Patch 3 installationspaket. Patch 2 är för Windows 7 och Windows Server 2008 OS-plattform och Patch 3 är för Windows 8 och Windows Server 2012 OS-plattform. McAfee-installeraren installerar korrekt patch genom att identifiera versionen av Windows operativsystem.

7. För nyinstallation, lägg till följande tillägg till McAfee ePolicy Orchestrator tilläggstabell i McAfee ePolicy Orchestrator Console:

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

Obs! VIRUSSCAN8800(348).zip och VIRUSSCANREPORTS120(228).zip finns i McAfee VirusScan Enterprise 8.8 Patch 3-paketet.

VIRUSSCAN8800(368).zip och VIRUSSCANREPORTS120(236).zip finns i McAfee VirusScan Enterprise 8.8 Patch 4-paketet.

VIRUSSCAN8800(511).zip och VIRUSSCANREPORTS120(311).zip finns i McAfee VirusScan Enterprise 8.8 Patch 8-paketet.

VIRUSSCAN8800(548).zip och VIRUSSCANREPORTS120(346).zip finns i McAfee VirusScan Enterprise 8.8 Patch 9-paketet.

McAfee ePolicy Orchestrator 5.0 or 5.3.2 – Ny installation implementeringssteg (Föredragen push-installationsmetod)

1. Beroende på programvaruversion, ska du välja ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.0.0 konsol) eller ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.3.2 konsol) för att logga in på ePolicy Orchestrator-konsolen.

Obs! Klicka på ***Continue with this website*** (Fortsätt med denna webbplats) om meddelanderutan ***Security Alert*** (Säkerhetsvarning) visas.

2. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).
3. Välj ***Menu > System > System Tree*** (Meny > System > Systemträd). Fönstret System Tree (Systemträd) öppnas.
4. Klicka på ***My Organization*** (Min organisation) och med fokus på ***My Organization***, klicka på ***System Tree Actions > New Systems*** (Systemträdåtgärder > Nya system) från nederst till vänster på skärmen.
5. Välj ***Push agents and add systems to the current group (My Organization)*** (Push agenter och lägga till system till den aktuella gruppen (Min organisation) och klicka på ***Browse*** (Bläddra) på målsystem.
6. Ange användarnamn och lösenord för **domain/local administrator** (domän/lokal administratör) och klicka på ***OK***.
7. Välj ***INW***-domänen från listrutan ***Domain*** (Domän).
8. Välj de klientmaskiner (Acquisition, Review och INW-server) som är anslutna till domänen och klicka på ***OK***.

Obs! Om domännamnet inte anges i listrutan ***Domain*** (Domän), ska du göra följande:

- I fönstret ***Browse for Systems*** (Sök efter system), ska du klicka på ***Cancel*** (Avbryt).
- I fönstret ***New Systems*** (Nya system), ska du ange systemnamnen för klientdatorerna (Acquisition, Review och INW server) manuellt i fältet ***Target systems*** (Målsystem) och fortsätta med stegen nedan.

9. Välj ***Agent Version*** (Agentversion) som M***cAfee Agent for Windows 4.8.0 (Current)*** (Aktuell) eller ***McAfee Agent for Windows 5.0.4 (Current)***. Ange användarnamn och lösenord för **domain administrator** (domänadministratör) och klicka på ***OK***.
10. I klientdatorerna (Acquisition, Review och INW Server) ska du bekräfta att katalogerna skapats korrekt, beroende på patch-versionen:

- För patch 3 och 4, ska du verifiera att ***C:\Program Files\McAfee\Common Framework***-katalogen är närvarande och McAfee Agent är installerad i samma katalog.

Obs! För INW Server, ska du säkerställa att ***C:\Program Files (x86)\McAfee\Common Framework***-katalogen är närvarande och McAfee Agent är installerad i samma katalog.

- För patch 8, ska du verifiera att ***C:\Program Files\McAfee\Agent***-katalogen är närvarande och McAfee Agent är installerad i samma katalog.

Obs! För INW Server, ska du säkerställa att ***C:\Program Files (x86)\McAfee\Common Framework***-katalogen är närvarande.

11. Starta om klientdatorerna (Acquisition, Review och INW Server) och logga in som **domain administrator** (domänadministratör) eller medlem i denna grupp.
12. Beroende på programvaruversion, ska du klicka på ***Start > All Programs > McAfee >ePolicy***
    Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.0.0 konsol) eller ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator >

Starta
McAfee ePolicy Orchestrator 5.3.2 konsol).

13. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).
14. Klicka på ***Menu > Systems > System Tree*** (Meny > System > Systemträd).
15. Klicka på ***My Organization*** (Min organisation) och med fokus på ***My Organization*** ska du klicka på fliken ***Assigned Client Tasks*** (Tilldelade klientuppgifter).
16. Klicka på knappen ***Actions > New Client Task Assignment*** (Åtgärder > Ny klientuppgifttilldelning) nederst på skärmen. Skärmen Client Task Assignment Builder visas
17. Välj följande:
    a. **Produkt:** McAfee Agent
    b. **Uppgiftstyp:** Produktimplementering
    c. **Uppgiftsnamn:** Skapa ny uppgift
18. På ***Client Task Catalog*** (Klientuppgiftskatalogen): ***New Task- McAfee Agent (Ny uppgift – McAfee Agent):*** Skärmen ***Product Deployment***
    a. **Uppgiftsnamn:** Ange lämpligt uppgiftsnamn
    b. **Målplattformar:** Fönster
    c. **Produkter och komponenter:** VirusScan Enterprise-version som är kvalificerad för v6.9.6
    d. **Alternativ:** Kör på varje princip tvingande (endast Windows) om det finns ***Options*** (Alternativ)
19. Klicka på ***Save*** (Spara).
20. På skärmen ***1 Select Task*** (1 Välj uppgift), ska du välja följande:
    a. **Produkt:** McAfee Agent
    b. **Uppgiftstyp:** Produktimplementering
    c. **Uppgiftsnamn:** Namn på nyligen skapad uppgift
21. Klicka på ***Next*** (Nästa). Skärmen 2 Schema visas.
22. Välj ***Run immediately*** (Kör omedelbart) från listrutan ***Schedule type*** (Schematyp).
23. Klicka på ***Next*** (Nästa). Skärmen 3 Sammanfattning visas.
24. Klicka på ***Save*** (Spara). Skärmen ***System Tree*** (Systemträd) visas.
25. Välj fliken ***Systems*** (System) och välj sedan alla klientdatorer (Acquisition, Review, och INW Server) som är anslutna till domänen.
26. Klicka på ***Wake up Agents*** (Väck agenter) längst ned i fönstret.
27. Behåll standardinställningarna och klicka på ***OK***.
28. Vänta tills McAfee-ikonen visas i systembrickan, och starta sedan om alla klientdatorer (Acquisition, Review och INW Server), och logga in med **Administrator** (Administratör) eller en medlem av denna grupp på alla klientdatorer.

29. Klicka på länken ***Log Off*** (Logga ut) för att stänga av McAfee ePolicy Orchestrator-konsolen.

McAfee ePolicy Orchestrator 5.9.0 – Ny installation implementeringssteg (Föredragen push-installationsmetod)

1. Klicka på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.9.0 konsol) för att logga in på ePolicy Orchestrator-konsolen.

Obs! Klicka på ***Continue with this website*** (Fortsätt med denna webbplats) om meddelanderutan ***Security Alert*** (Säkerhetsvarning) visas.

2. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).
3. Välj ***Menu > System > System Tree*** (Meny > System > Systemträd). Fönstret ***System Tree*** (Systemträd) öppnas.
4. Klicka på ***My Organization*** (Min organisation) och med fokus på ***My Organization***, klicka på ***New Systems*** (Nya system) överst på skärmen.
5. Välj ***Push agents and add systems to the current group (My Organization)*** (Push agenter och lägga till system till den aktuella gruppen (Min organisation) och klicka på ***Browse*** (Bläddra) på målsystem.
6. Ange användarnamn och lösenord för **domain/local administrator** (domän/lokal administratör) och klicka på ***OK***.
7. Välj ***INW***-domänen från listrutan ***Domain*** (Domän).
8. Välj de klientmaskiner (Acquisition, Review och INW-server) som är anslutna till domänen och klicka på ***OK***.

Obs! Om domännamnet inte anges i listrutan ***Domain*** (Domän), ska du göra följande:

- I fönstret ***Browse for Systems*** (Sök efter system), ska du klicka på ***Cancel*** (Avbryt).
- I fönstret ***New Systems*** (Nya system), ska du ange systemnamnen för klientdatorerna (Acquisition, Review och INW server) manuellt, med ett komma mellan varje namn, i fältet ***Target systems*** (Målsystem) och fortsätta med stegen nedan.

9. Välj ***Agent Version*** (Agentversion) som M***cAfee Agent for Windows 5.0.5 (Current)*** (Aktuell). Ange användarnamn och lösenord för **domain administrator** (domänadministratör) och klicka på ***OK***.
10. Bekräfta att katalogerna i ***C:\Program Files\McAfee\Agent*** har skapats korrekt i klientdatorerna (Acquisition, Review och INW Server).
11. Starta om klientdatorerna (Acquisition, Review och INW Server) och logga in som **domain administrator** (domänadministratör) eller medlem i denna grupp.
12. Klicka på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.9.0 konsol) för att logga in på ePolicy Orchestrator-konsolen.
13. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).

14. Klicka på ***Menu > Systems > System Tree*** (Meny > System > Systemträd).
15. Klicka på ***My Organization*** (Min organisation) och med fokus på ***My Organization*** ska du klicka på fliken ***Assigned Client Tasks*** (Tilldelade klientuppgifter).
16. Klicka på knappen ***Actions > New Client Task Assignment*** (Åtgärder > Ny klientuppgifttilldelning) nederst på skärmen. Skärmen ***Client Task Assignment Builder*** visas.
17. Välj följande:
    a. **Produkt:** McAfee Agent
    b. **Uppgiftstyp:** Produktimplementering
18. Klicka på ***Task Actions > Create New Task*** (Uppgiftsåtgärder > Skapa ny uppgift). Skärmen ***Create New Task*** (Skapa ny uppgift) visas.
19. På skärmen ***Create New Task*** (Skapa ny uppgift) fyller du i fälten enligt följande:
    a. **Uppgiftsnamn:** Ange lämpligt uppgiftsnamn
    b. **Målplattformar:** Windows (avmarkera alla andra alternativ)
    c. **Produkter och komponenter:** VirusScan Enterprise 8.8.0.1804
20. Klicka på ***Save*** (Spara). Skärmen ***Client Task Assignment Builder*** visas.
21. På skärmen ***Client Task Assignment Builder*** väljer du följande:
    a. **Produkt:** McAfee Agent
    b. **Uppgiftstyp:** Produktimplementering
    c. **Uppgiftsnamn:** Namn på nyligen skapad uppgift
    d. **Schematyp:** Kör omedelbart
22. Klicka på ***Save*** (Spara). Skärmen ***Assigned Client Tasks*** (Tilldelade klientuppgifter) visas.
23. Välj fliken ***Systems*** (System) och välj sedan alla klientdatorer (Acquisition, Review, och INW Server) som är anslutna till domänen.
24. Klicka på ***Wake up Agents*** (Väck agenter) längst ned i fönstret.
25. Behåll standardinställningarna och klicka på ***OK***.
26. Vänta tills McAfee-ikonen visas i systembrickan, och starta sedan om alla klientdatorer (Acquisition, Review och INW Server), och logga in med **Administrator** (Administratör) eller en medlem av denna grupp på alla klientdatorer.
27. Klicka på länken ***Log Off*** (Logga ut) för att stänga av McAfee ePolicy Orchestrator-konsolen.

Konfiguration av McAfee ePolicy Orchestrator 5.0 och 5.3.2 Server-konsolen

1. Beroende på programvaruversion, ska du klicka på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.0.0 konsol) eller ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.3.2 konsol).
2. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).
3. Klicka på ***Menu > Systems > System Tree*** (Meny > System > Systemträd).
4. Klicka på ***My Organization*** (Min organisation) och med fokus på My Organization ska du klicka på fliken ***Assigned Client Tasks*** (Tilldelade klientuppgifter).
5. Klicka på knappen ***Actions > New Client Task Assignment*** (Åtgärder > Ny klientuppgifttilldelning) nederst på skärmen. Skärmen ***Client Task Assignment Builder*** visas
6. Välj följande:
    a. ***Produkt:*** VirusScan Enterprise 8.8.0
    b. ***Uppgiftstyp:*** Sökning på begäran
    c. ***Uppgiftsnamn:*** Skapa ny uppgift
7. På ***Client Task Catalog*** (Klientuppgiftskatalogen): ***Ny uppgift VirusScan Enterprise 8.8.0:*** skärmen ***On Demand Scan*** (Sökning på begäran), ska du fylla i fälten enligt följande:
    a. ***Uppgiftsnamn:*** Schemalagd sökning varje vecka
    b. ***Beskrivning:*** Schemalagd sökning varje vecka
8. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
9. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Options*** (Alternativ).
10. Avmarkera följande alternativ under Heuristics (Heuristik):
    - ***Find unknown programs threats (Hitta okända programhot).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
11. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
12. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
13. Välj mapparna ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj Also exclude subfolders (Uteslut även undermappar). Klicka på ***OK***.
14. Klicka på fliken ***Performance*** (Prestanda). Skärmen ***Performance*** (Prestanda) visas.
15. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).

16. Klicka på ***Save*** (Spara).
17. På skärmen ***1 Select Task*** (1 Välj uppgift), ska du välja följande:
    - ***Produkt:*** VirusScan Enterprise 8.8.0
    - ***Uppgiftstyp:*** Sökning på begäran
    - ***Uppgiftsnamn:*** Schemalagd sökning varje vecka
18. Klicka på ***Next*** (Nästa). Skärmen ***2 Schedule*** (2 Schema) visas.
19. Välj ***Weekly*** (Varje vecka) från listrutan ***Scheduled type*** (Schemalagd typ) och välj ***Sunday*** (Söndag).
20. Ställ in ***Start time*** (Starttid) på ***12:00 AM*** (12) och välj ***Run Once at that time*** (Kör en gång vid denna tidpunkt).
21. Klicka på ***Next*** (Nästa). Skärmen ***3 Summary*** (2 Sammanfattning) visas.
22. Klicka på ***Save*** (Spara). Skärmen ***System Tree*** (Systemträd) visas.
23. Välj fliken ***Assigned Policies*** (Tilldelade principer). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.
24. I listrutan ***Product*** (Produkt) ska du välja ***VirusScan Enterprise 8.8.0***.
25. Klicka på ***My Default*** (Min standard) under ***On-Access General Policies*** (Allmänna principer vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** VirusScan Enterprise 8.8.0 > Allmänna principer vid åtkomst > Min standard).
26. Välj ***Workstation*** (Arbetsstation) från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***General*** (Allmänt). Skärmen ***General*** (Allmänt) visas.
27. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
28. Klicka på fliken ***ScriptScan*** (Skriptsökning). Skärmen ***Script Scan*** (Skriptsökning) visas.
29. Avmarkera ***Enable scanning of scripts*** (Aktivera sökning av skript).
30. Klicka på fliken ***Blocking*** (Blockering). Skärmen ***Blocking*** (Blockering) visas.
31. Avmarkera ***Block the connection when a threatened file is detected in a shared folder*** (Blockera anslutningen när en hotad fil upptäcks i en delad mapp).
32. Klicka på fliken ***Messages*** (Meddelanden). Skärmen ***Messages*** (Meddelanden) visas.
33. Avmarkera ***Show the messages dialog when a threat is detected and display the specified text in the message*** (Visa meddelandedialogrutan när ett hot detekteras och visa texten i meddelandet).
34. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***General*** (Allmänt). Skärmen ***General*** (Allmänt) visas.
35. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
36. Klicka på fliken ***ScriptScan*** (Skriptsökning). Skärmen ***Script Scan*** (Skriptsökning) visas.
37. Se till att ***Enable scanning of scripts*** (Aktivera sökning av skript).

38. Klicka på fliken ***Blocking*** (Blockering). Skärmen ***Blocking*** (Blockering) visas.
39. Avmarkera ***Block the connection when a threatened file is detected in a shared folder*** (Blockera anslutningen när en hotad fil upptäcks i en delad mapp).
40. Klicka på fliken ***Messages*** (Meddelanden). Skärmen ***Messages*** (Meddelanden) visas.
41. Avmarkera ***Show the messages dialog when a threat is detected and display the specified text in the message*** (Visa meddelandedialogrutan när ett hot detekteras och visa texten i meddelandet).
42. Klicka på ***Save*** (Spara).
43. Klicka på ***My Default*** (Min standard) under ***On-Access Default Processes Policies*** (Principer för standardprocesser vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Allmänna principer för standardprocesser vid åtkomst > Min standard) visas.
44. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
45. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
46. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
47. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
48. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
49. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
50. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
51. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
52. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
53. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
54. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
55. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
56. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.

57. Klicka på ***Save*** (Spara).
58. Klicka på ***My Default*** (Min standard) för ***On-Access Low-Risk Processes Policies*** (Principer för lågriskprocesser vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Allmänna principer för lågriskprocesser vid åtkomst > Min standard) visas.
59. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
60. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
61. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
62. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
63. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
64. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
65. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
66. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
67. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
68. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
69. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
70. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
71. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
72. Klicka på ***Save*** (Spara).
73. Klicka på ***My Default*** (Min standard) under ***On-Access High-Risk Processes Policies*** (Principer för högriskprocesser vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** VirusScan Enterprise 8.8.0 > Allmänna principer för högriskprocesser vid åtkomst > Min standard) visas.
74. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
75. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.

76. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
77. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
78. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
79. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
80. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
81. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
82. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
83. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
84. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
85. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
86. Välj mapparna By pattern (Enligt mönster) och ange **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
87. Klicka på ***Save*** (Spara).
88. Klicka på ***My Default*** (Min standard) under ***On Delivery Email Scan Policies*** (Principer för e-postsökning vid leverans). Skärmen ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för e-postsökning vid leverans > Min standard) visas.
89. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
90. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
91. Avmarkera följande alternativ under ***Heuristics*** (Heuristik).
    - ***Find unknown program threats and trojans (Hitta okända programhot och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
    - ***Find attachments with multiple extensions (Hitta bilagor med flera tillägg).***
92. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).

93. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).

94. Avmarkera ***Enable on-delivery email scanning*** Aktivera e-postsökning vid leverans) under ***Scanning of email*** (Sökning av e-post).

95. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för).

96. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.

97. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):

    - ***Find unknown program threats and trojans (Hitta okända programhot och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
    - ***Find attachments with multiple extensions (Hitta bilagor med flera tillägg).***

98. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).

99. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).

100. Avmarkera ***Enable on-delivery email scanning*** Aktivera e-postsökning vid leverans) under ***Scanning of email*** (Sökning av e-post).

101. Klicka på ***Save*** (Spara).

102. Klicka på ***My Default*** (Min standard) for ***General Options Policies*** (Principer för allmänna alternativ). Skärmen ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för allmänna alternativ > Min standard).

103. Välj ***Workstation*** (Arbetsstation) från listrutan ***Settings for*** (Inställningar för).

104. Klicka på fliken ***Display Options*** (Visa alternativ). Skärmen ***Display Options*** (Visa alternativ) visas.

105. Välj följande under ***Console options*** (Konsolalternativ):

    - ***Display managed tasks in the client console (Visa hanterade uppgifter i klientkonsolen)***
    - ***Disable default AutoUpdate task schedule (Inaktivera standardschemat för automatisk uppdatering av aktivitet).***

106. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för).

107. Klicka på fliken ***Display Options*** (Visa alternativ). Skärmen ***Display Options*** (Visa alternativ) visas.

108. Välj följande under ***Console options*** (Konsolalternativ).

    - ***Display managed tasks in the client console (Visa hanterade uppgifter i klientkonsolen)***
    - ***Disable default AutoUpdate task schedule (Inaktivera standardschemat för automatisk uppdatering av aktivitet).***

109. Klicka på ***Save*** (Spara).

110. Klicka på ***My Default*** (Min standard) under ***Alert Policies*** (Varningsprinciper). Skärmen ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Ändra principer > Min standard).

111. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).

112. Klicka på fliken ***Alert Manager Alerts*** (Varningar i varningshanteraren). Skärmen ***Alert Manager Alerts*** (Varningar i varningshanteraren) visas.

113. Avmarkera ***On-Access Scan*** (Sökning vid åtkomst), ***On-Demand Scan and scheduled scans*** (Sökning på begäran och schemalagda sökningar), ***Email Scan*** (E-postsökning) och ***AutoUpdate*** (Autouppdatering) under ***Components that generate alerts*** (Komponenter som genererar varningar).

114. Välj alternativen ***Disable alerting*** (Inaktivera varningar) under ***Alert Manager*** (Larmhanteraren).

115. Avmarkera ***Access Protection*** (Åtkomstsskydd) under ***Components that generate alerts*** (Komponenter som genererar larm).

116. Klicka på ***Additional Alerting Options*** (Fler varningsalternativ). Skärmen ***Additional Alerting Options*** öppnas.

117. I listmenyn ***Severity Filters*** (Filter för allvarsgrad) ska du välja ***Suppress all alerts (severities 0 to 4)*** (Utelämna alla varningar (grad 0 till 4)).

118. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för) och välj fliken ***Alert Manager Alerts*** (Varningar i varningshanteraren). Skärmen ***Alert Manager Alerts*** (Varningar i varningshanteraren) visas.

119. Avmarkera ***On-Access Scan*** (Sökning vid åtkomst), ***On-Demand Scan and scheduled scans*** (Sökning på begäran och schemalagda sökningar), ***Email Scan*** (E-postsökning) och ***AutoUpdate*** (Autouppdatering) under ***Components that generate alerts*** (Komponenter som genererar varningar).

120. Kryssa i alternativen ***Disable alerting*** (Inaktivera varningar) under ***Alert Manager*** (Larmhanteraren).

121. Avmarkera ***Access Protection*** (Åtkomstsskydd) under ***Components that generate alerts*** (Komponenter som genererar larm).

122. Klicka på ***Additional Alerting Options*** (Fler varningsalternativ). Skärmen Additional Alerting Options öppnas.

123. I listmenyn ***Severity Filters*** (Filter för allvarsgrad) ska du välja ***Suppress all alerts (severities 0 to 4)*** (Utelämna alla varningar (grad 0 till 4)).

124. Klicka på ***Save*** (Spara).

125. Klicka på ***My Default*** (Min standard) for ***Access Protection Policies*** (Principer för åtkomstskydd). Skärmen ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för åtkomstskydd > Min standard).

126. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).

127. Klicka på fliken ***Access Protection*** (Åtkomstskydd). Skärmen ***Access Protection*** (Åtkomskydd) visas.

128. Avmarkera följande alternativ under ***Access protection settings*** (Inställningar för åtkomstskydd):

    - ***Enable access protection (Aktivera åtkomstskydd)***

- ***Prevent McAfee services from being stopped (Förhindra att McAfee-tjänster stoppas).***

129. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för).
130. Klicka på fliken ***Access Protection*** (Åtkomstskydd). Skärmen ***Access Protection*** (Åtkomskydd) visas.
131. Avmarkera följande alternativ under ***Access protection settings*** (Inställningar för åtkomstskydd):
    - ***Enable access protection (Aktivera åtkomstskydd)***
    - ***Prevent McAfee services from being stopped (Förhindra att McAfee-tjänster stoppas).***
132. Klicka på ***Save*** (Spara).
133. Klicka på ***My Default*** (Min standard) för ***Buffer Overflow Protection Policies*** (Principer för skydd mot buffertöverskridning). Skärmen ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för skydd mot buffertöverskridning > Min standard).
134. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
135. Klicka på fliken ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning). Skärmen ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning) visas.
136. Avmarkera ***Show the message dialog box when a buffer overflow is detected*** (Visa dialogrutan när en buffertöverskridning upptäcks) under ***Client system warning*** (Klientsystemvarning).
137. Avmarkera ***Enable buffer overflow protection*** (Aktivera skydd mot buffertöverskridning) under ***Buffer overflow settings*** (Inställningar för buffertöverskridning).
138. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för).
139. Klicka på fliken ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning). Skärmen ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning) visas.
140. Avmarkera ***Show the message dialog box when a buffer overflow is detected*** (Visa dialogrutan när en buffertöverskridning upptäcks) under ***Client system warning*** (Klientsystemvarning).
141. Avmarkera ***Enable buffer overflow protection*** (Aktivera skydd mot buffertöverskridning) under ***Buffer overflow settings*** (Inställningar för buffertöverskridning).
142. Klicka på ***Save*** (Spara).
143. Från listrutan ***Product*** (Produkt) ska du välja ***McAfee Agent***. Fönstret ***Policies*** (Principer) för McAfee Agent visas.
144. Klicka på ***My Default*** (Min standard) för ***Repository*** (Datalager). Skärmen ***McAfee Agent > Repository > My Default*** (McAfee Agent > Datalager > Min standard) visas.
145. Klicka på fliken ***Proxy***. Skärmen ***Proxy*** visas.
146. Välj ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Använd Internet Explorer-inställningar (För Windows)/Systeminställningar (För Mac OSX)) under ***Proxy settings*** (Proxyinställningar).
147. Klicka på ***Save*** (Spara).

148. Klicka på fliken ***Systems*** (System).

149. Välj alla klientsystem (insamlings-, gransknings- och Centricity Cardiology INW-servern) där de konfigurerade principerna ska implementeras.

150. Välj ***Wake Up Agents*** (Väck agenter). Skärmen ***Wake Up Agent*** (Väck agenter) visas.

151. Klicka på ***OK***.

152. Logga ut ur ePolicy Orchestrator.

Konfigurering av McAfee ePolicy Orchestrator 5.9.0 Server Console

1. Beroende på programvaruversion klickar du på ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Starta > Alla program > McAfee > ePolicy Orchestrator > Starta McAfee ePolicy Orchestrator 5.9.0 konsol).
2. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).
3. Klicka på ***Menu > Systems > System Tree*** (Meny > System > Systemträd).
4. Klicka på ***My Organization*** (Min organisation) och med fokus på My Organization ska du klicka på fliken ***Assigned Client Tasks*** (Tilldelade klientuppgifter).
5. Klicka på knappen ***Actions > New Client Task Assignment*** (Åtgärder > Ny klientuppgifttilldelning) nederst på skärmen. Skärmen ***Client Task Assignment Builder*** visas
6. Välj följande:
    a. ***Produkt:*** VirusScan Enterprise 8.8.0
    b. ***Uppgiftstyp:*** Sökning på begäran
7. Klicka på ***Create New Task*** (Skapa ny uppgift) i ***Task Actions*** (Uppgiftsåtgärder). Skärmen ***Create New Task*** (Skapa ny uppgift) visas.
8. På skärmen ***Create New Task*** (Skapa ny uppgift) fyller du i fälten enligt följande:
    a. ***Uppgiftsnamn:*** Schemalagd sökning varje vecka
    b. ***Beskrivning:*** Schemalagd sökning varje vecka
9. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
10. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Options*** (Alternativ).
11. Avmarkera följande alternativ under Heuristics (Heuristik):
    - ***Find unknown programs threats (Hitta okända programhot).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
12. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
13. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.

14. Välj mapparna ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj Also exclude subfolders (Uteslut även undermappar). Klicka på ***OK***.
15. Klicka på fliken ***Performance*** (Prestanda). Skärmen ***Performance*** (Prestanda) visas.
16. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
17. Klicka på ***Save*** (Spara). Skärmen ***Client Task Assignment Builder*** visas.
18. På skärmen ***Client Task Assignment Builder*** väljer du följande:
    - ***Produkt:*** VirusScan Enterprise 8.8.0
    - ***Uppgiftstyp:*** Sökning på begäran
    - ***Uppgiftsnamn:*** Schemalagd sökning varje vecka
19. Välj ***Weekly*** (Varje vecka) från listrutan ***Scheduled type*** (Schemalagd typ) och välj ***Sunday*** (Söndag).
20. Ställ in ***Start time*** (Starttid) på ***12:00 AM*** (12) och välj ***Run Once at that time*** (Kör en gång vid denna tidpunkt).
21. Klicka på ***Save*** (Spara). Skärmen ***Assigned Client Tasks*** (Tilldelade klientuppgifter) visas.
22. Välj fliken ***Assigned Policies*** (Tilldelade principer). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.
23. I listrutan ***Product*** (Produkt) ska du välja ***VirusScan Enterprise 8.8.0***.
24. Klicka på ***My Default*** (Min standard) under ***On-Access General Policies*** (Allmänna principer vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** VirusScan Enterprise 8.8.0 > Allmänna principer vid åtkomst > Min standard).
25. Välj ***Workstation*** (Arbetsstation) från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***General*** (Allmänt). Skärmen ***General*** (Allmänt) visas.
26. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
27. Klicka på fliken ***ScriptScan*** (Skriptsökning). Skärmen ***Script Scan*** (Skriptsökning) visas.
28. Avmarkera ***Enable scanning of scripts*** (Aktivera sökning av skript).
29. Klicka på fliken ***Blocking*** (Blockering). Skärmen ***Blocking*** (Blockering) visas.
30. Avmarkera ***Block the connection when a threatened file is detected in a shared folder*** (Blockera anslutningen när en hotad fil upptäcks i en delad mapp).
31. Klicka på fliken ***Messages*** (Meddelanden). Skärmen ***Messages*** (Meddelanden) visas.
32. Avmarkera ***Show the messages dialog when a threat is detected and display the specified text in the message*** (Visa meddelandedialogrutan när ett hot detekteras och visa texten i meddelandet).
33. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***General*** (Allmänt). Skärmen ***General*** (Allmänt) visas.
34. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).

35. Klicka på fliken ***ScriptScan*** (Skriptsökning). Skärmen ***Script Scan*** (Skriptsökning) visas.
36. Se till att ***Enable scanning of scripts*** (Aktivera sökning av skript).
37. Klicka på fliken ***Blocking*** (Blockering). Skärmen ***Blocking*** (Blockering) visas.
38. Avmarkera ***Block the connection when a threatened file is detected in a shared folder*** (Blockera anslutningen när en hotad fil upptäcks i en delad mapp).
39. Klicka på fliken ***Messages*** (Meddelanden). Skärmen ***Messages*** (Meddelanden) visas.
40. Avmarkera ***Show the messages dialog when a threat is detected and display the specified text in the message*** (Visa meddelandedialogrutan när ett hot detekteras och visa texten i meddelandet).
41. Klicka på ***Save*** (Spara). Skärmen Assigned Policies (Tilldelade principer) visas.
42. Klicka på ***My Default*** (Min standard) under ***On-Access Default Processes Policies*** (Principer för standardprocesser vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Allmänna principer för standardprocesser vid åtkomst > Min standard) visas.
43. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
44. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
45. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
46. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
47. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
48. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
49. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
50. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
51. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
52. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
53. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
54. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.

55. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.

56. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.

57. Klicka på ***My Default*** (Min standard) för ***On-Access Low-Risk Processes Policies*** (Principer för lågriskprocesser vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Allmänna principer för lågriskprocesser vid åtkomst > Min standard) visas.

58. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).

59. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.

60. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***

61. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).

62. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.

63. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.

64. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.

65. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.

66. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):

    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***

67. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).

68. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.

69. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.

70. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.

71. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.

72. Klicka på ***My Default*** (Min standard) under ***On-Access High-Risk Processes Policies*** (Principer för högriskprocesser vid åtkomst). Skärmen ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** VirusScan Enterprise 8.8.0 > Allmänna principer för högriskprocesser vid åtkomst > Min standard) visas.

73. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
74. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
75. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
76. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
77. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
78. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
79. Välj mapparna ***By pattern*** (Enligt mönster) och ange **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
80. Välj ***Server*** från listrutan ***Settings for*** (Inställningar för) och klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
81. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown unwanted programs and trojans (Hitta okända, oönskade program och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
82. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
83. Klicka på fliken ***Exclusions*** (Undantag). Skärmen ***Exclusions*** (Undantag) visas.
84. Klicka på ***Add*** (Lägg till). Skärmen ***Add/Edit Exclusion Item*** (Lägg till/Redigera undantag) visas.
85. Välj mapparna By pattern (Enligt mönster) och ange **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, en i taget, och välj ***Also exclude subfolders*** (Uteslut även undermappar). Klicka på ***OK***.
86. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.
87. Klicka på ***My Default*** (Min standard) under ***On Delivery Email Scan Policies*** (Principer för e-postsökning vid leverans). Skärmen ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för e-postsökning vid leverans > Min standard) visas.
88. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
89. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
90. Avmarkera följande alternativ under ***Heuristics*** (Heuristik).
    - ***Find unknown program threats and trojans (Hitta okända programhot och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
    - ***Find attachments with multiple extensions (Hitta bilagor med flera tillägg).***

91. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
92. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
93. Avmarkera ***Enable on-delivery email scanning*** Aktivera e-postsökning vid leverans) under ***Scanning of email*** (Sökning av e-post).
94. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för).
95. Klicka på fliken ***Scan Items*** (Sök objekt). Skärmen ***Scan Items*** (Sök objekt) visas.
96. Avmarkera följande alternativ under ***Heuristics*** (Heuristik):
    - ***Find unknown program threats and trojans (Hitta okända programhot och trojaner).***
    - ***Find unknown macro threats (Hitta okända makrohot).***
    - ***Find attachments with multiple extensions (Hitta bilagor med flera tillägg).***
97. Avmarkera ***Detect unwanted programs*** (Upptäck oönskade program) under ***Unwanted programs detection*** (Upptäckt av oönskade program).
98. Välj ***Disabled*** (Inaktiverad) från ***Artemis (Heuristic network check for suspicious files)*** (Artemis (Heuristisk nätverkskontroll av misstänkta filer).
99. Avmarkera ***Enable on-delivery email scanning*** Aktivera e-postsökning vid leverans) under ***Scanning of email*** (Sökning av e-post).
100. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.
101. Klicka på ***My Default*** (Min standard) for ***General Options Policies*** (Principer för allmänna alternativ). Skärmen ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för allmänna alternativ > Min standard).
102. Välj ***Workstation*** (Arbetsstation) från listrutan ***Settings for*** (Inställningar för).
103. Klicka på fliken ***Display Options*** (Visa alternativ). Skärmen ***Display Options*** (Visa alternativ) visas.
104. Välj följande under ***Console options*** (Konsolalternativ):
    - ***Display managed tasks in the client console (Visa hanterade uppgifter i klientkonsolen)***
    - ***Disable default AutoUpdate task schedule (Inaktivera standardschemat för automatisk uppdatering av aktivitet).***
105. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för).
106. Klicka på fliken ***Display Options*** (Visa alternativ). Skärmen ***Display Options*** (Visa alternativ) visas.
107. Välj följande under ***Console options*** (Konsolalternativ).
    - ***Display managed tasks in the client console (Visa hanterade uppgifter i klientkonsolen)***
    - ***Disable default AutoUpdate task schedule (Inaktivera standardschemat för automatisk uppdatering av aktivitet).***
108. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.

109. Klicka på ***My Default*** (Min standard) under ***Alert Policies*** (Varningsprinciper). Skärmen ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Ändra principer > Min standard).

110. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).

111. Klicka på fliken ***Alert Manager Alerts*** (Varningar i varningshanteraren). Skärmen ***Alert Manager Alerts*** (Varningar i varningshanteraren) visas.

112. Avmarkera ***On-Access Scan*** (Sökning vid åtkomst), ***On-Demand Scan and scheduled scans*** (Sökning på begäran och schemalagda sökningar), ***Email Scan*** (E-postsökning) och ***AutoUpdate*** (Autouppdatering) under ***Components that generate alerts*** (Komponenter som genererar varningar).

113. Välj alternativen ***Disable alerting*** (Inaktivera varningar) under ***Alert Manager*** (Larmhanteraren).

114. Avmarkera ***Access Protection*** (Åtkomstsskydd) under ***Components that generate alerts*** (Komponenter som genererar larm).

115. Klicka på ***Additional Alerting Options*** (Fler varningsalternativ). Skärmen ***Additional Alerting Options*** öppnas.

116. I listmenyn ***Severity Filters*** (Filter för allvarsgrad) ska du välja ***Suppress all alerts (severities 0 to 4)*** (Utelämna alla varningar (grad 0 till 4)).

117. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för) och välj fliken ***Alert Manager Alerts*** (Varningar i varningshanteraren). Skärmen ***Alert Manager Alerts*** (Varningar i varningshanteraren) visas.

118. Avmarkera ***On-Access Scan*** (Sökning vid åtkomst), ***On-Demand Scan and scheduled scans*** (Sökning på begäran och schemalagda sökningar), ***Email Scan*** (E-postsökning) och ***AutoUpdate*** (Autouppdatering) under ***Components that generate alerts*** (Komponenter som genererar varningar).

119. Kryssa i alternativen ***Disable alerting*** (Inaktivera varningar) under ***Alert Manager*** (Larmhanteraren).

120. Avmarkera ***Access Protection*** (Åtkomstsskydd) under ***Components that generate alerts*** (Komponenter som genererar larm).

121. Klicka på ***Additional Alerting Options*** (Fler varningsalternativ). Skärmen Additional Alerting Options öppnas.

122. I listmenyn ***Severity Filters*** (Filter för allvarsgrad) ska du välja ***Suppress all alerts (severities 0 to 4)*** (Utelämna alla varningar (grad 0 till 4)).

123. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.

124. Klicka på ***My Default*** (Min standard) for ***Access Protection Policies*** (Principer för åtkomstskydd). Skärmen ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för åtkomstskydd > Min standard).

125. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).

126. Klicka på fliken ***Access Protection*** (Åtkomstskydd). Skärmen ***Access Protection*** (Åtkomskydd) visas.

127. Avmarkera följande alternativ under ***Access protection settings*** (Inställningar för åtkomstskydd):

- ***Enable access protection (Aktivera åtkomstskydd)***
- ***Prevent McAfee services from being stopped (Förhindra att McAfee-tjänster stoppas).***
- ***Enable Enhanced Self-Protection (Aktivera Utökat självskydd)***

128. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för).
129. Klicka på fliken ***Access Protection*** (Åtkomstskydd). Skärmen ***Access Protection*** (Åtkomskydd) visas.
130. Avmarkera följande alternativ under ***Access protection settings*** (Inställningar för åtkomstskydd):

    - ***Enable access protection (Aktivera åtkomstskydd)***
    - ***Prevent McAfee services from being stopped (Förhindra att McAfee-tjänster stoppas).***
    - ***Enable Enhanced Self-Protection (Aktivera Utökat självskydd)***

131. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.
132. Klicka på ***My Default*** (Min standard) för ***Buffer Overflow Protection Policies*** (Principer för skydd mot buffertöverskridning). Skärmen ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Principer för skydd mot buffertöverskridning > Min standard).
133. Välj ***Workstation*** (Arbetsstation) i listrutan ***Settings for*** (Inställningar för).
134. Klicka på fliken ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning). Skärmen ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning) visas.
135. Avmarkera ***Show the message dialog box when a buffer overflow is detected*** (Visa dialogrutan när en buffertöverskridning upptäcks) under ***Client system warning*** (Klientsystemvarning).
136. Avmarkera ***Enable buffer overflow protection*** (Aktivera skydd mot buffertöverskridning) under ***Buffer overflow settings*** (Inställningar för buffertöverskridning).
137. Välj ***Server*** i listrutan ***Settings for*** (Inställningar för).
138. Klicka på fliken ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning). Skärmen ***Buffer Overflow Protection*** (Skydd mot buffertöverskridning) visas.
139. Avmarkera ***Show the message dialog box when a buffer overflow is detected*** (Visa dialogrutan när en buffertöverskridning upptäcks) under ***Client system warning*** (Klientsystemvarning).
140. Avmarkera ***Enable buffer overflow protection*** (Aktivera skydd mot buffertöverskridning) under ***Buffer overflow settings*** (Inställningar för buffertöverskridning).
141. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.
142. Från listrutan ***Product*** (Produkt) ska du välja ***McAfee Agent***. Fönstret ***Policies*** (Principer) för McAfee Agent visas.
143. Klicka på ***My Default*** (Min standard) för ***Repository*** (Datalager). Skärmen ***McAfee Agent > Repository > My Default*** (McAfee Agent > Datalager > Min standard) visas.
144. Klicka på fliken ***Proxy***. Skärmen ***Proxy*** visas.

145. Säkerställ att ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Använd Internet Explorer-inställningar (För Windows)/ Systeminställningar (För Mac OSX)) under ***Proxy settings*** (Proxyinställningar) är markerat.
146. Klicka på ***Save*** (Spara). Skärmen ***Assigned Policies*** (Tilldelade principer) visas.
147. Klicka på fliken ***Systems*** (System).
148. Välj alla klientsystem (Acquisition, Review och Centricity Cardiology INW server) där de konfigurerade principerna ska implementeras.
149. Välj ***Wake Up Agents*** (Väck agenter). Skärmen ***Wake Up Agent*** (Väck agenter) visas.
150. Klicka på ***OK***.
151. Logga ut ur ePolicy Orchestrator.

Riktlinjer efter installation av McAfee ePolicy Orchestrator

Aktivera loopback-anslutningen. Närmare information finns i Aktivera loopback-anslutning på sidan 6.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Installationsöversikt

Installera Trend Micro OfficeScan Client/Server Edition endast i en nätverksansluten Mac-Lab/CardioLab-miljö. Trend Micro OfficeScan måste installeras på Anti-virus Management Console-servern och därefter implementeras på Centricity Cardiology INW-servern och insamlings-/granskningsarbetsstationerna som klienter. Använd följande instruktioner för att installera ***Trend Micro OfficeScan Client/Server Edition***.

Sjukhuset ansvarar för uppdateringen av virusdefinitionerna. Uppdatera definitionerna regelbundet så att systemet alltid har det senaste virusskyddet.

Åtgärder före installation

1. Trend Micro Anti-Virus Management Console förväntas vara installerad enligt instruktionerna från Trend Micro och fungera perfekt.
2. Under installation av Trend Micro OfficeScan ska du göra följande på Anti-Virus Management Console-servern:
    a. Avmarkera ***Enable firewall*** (Aktivera brandvägg) i fönstret ***Anti-virus Feature*** (Antivirusfunktioner).
    b. Välj ***No, Please do not enable assessment mode*** (Nej, aktivera inte utvärderingsläge) i fönstret ***Anti-spyware Feature*** (Antispionprogramfunktioner).
    c. Avmarkera ***Enable web reputation policy*** (Aktivera policy för webbanseende) i fönstret ***Web Reputation Feature*** (Webbanseendefunktioner).
3. Trend Micro OfficeScan rekommenderas inte när du använder funktionen ***CO_2*** med PDM i Mac-Lab/CardioLab-system.
4. Om Trend Micro OfficeScan krävs:
    a. Vi rekommenderar att du konfigurerar en separat Trend Micro Anti-Virus Management Console-server för Mac-Lab/CardioLab-systemen. En global ändring av antivirusinställningarna krävs för att använda ***CO_2***-funktionen med PDM i Mac-Lab/CardioLab-system.
    b. Om en separat Trend Micro Anti-Virus Management Console-server inte kan konfigureras krävs en ändring av globala inställningar för den befintliga Trend Micro Anti-Virus Management Console-servern efter installationen. Denna ändring kommer att påverka alla klientsystem som är anslutna till den befintliga Trend Micro Anti-Virus Management Console-servern och ska granskas med IT-personal innan du fortsätter.
5. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientsystem (Acquisition, Review och INW Server) för att installera antivirusprogramvaran.
6. Inaktivera loopback-anslutningen. Närmare information finns i Inaktivera loopback-anslutning på sidan 6.
7. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst före antivirusinstallation på sidan 6.

Trend Micro OfficeScan - steg för implementering av ny installation (föredragen push-installationsmetod)

1. Klicka på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alla program > TrendMicro OfficeScan-server - <servernamn> > Office Scan Web Console).

Obs! Fortsätt genom att välja ***Continue to this website (not recommended)*** (Fortsätt till den här webbplatsen (rekommenderas inte)). I fönstret Security Alert (Säkerhetsvarning) markerar du ***In the future, do not show this warning*** (Visa inte den här varningen igen) och klicka på ***OK***.

2. Om du får ett certifikatfel som anger att webbplatsen inte är betrodd ska du hantera dina certifikat så att de inkluderar Trend Micro OfficeScan.
3. Om du uppmanas att göra det installerar du ***AtxEnc***-tilläggen. Skärmen Security Warning (Säkerhetsvarning) visas.
4. Klicka på ***Install*** (Installera).
5. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).
6. Om du uppmanas att göra det klickar du på ***Update Now*** (Uppdatera nu) för att installera nya widgetar. Vänta tills de nya widgetarna uppdateras. Skärmen The update is completed (Uppdateringen är klar) visas.
7. Klicka på ***OK***.
8. I menyraden till vänster klickar du på ***Networked Computers > Client Installation > Remote*** (Nätverksanslutna datorer > Klientinstallation > Fjärr).
9. Om du uppmanas att göra det installerar du ***AtxConsole***-tilläggen. Skärmen Security Warning (Säkerhetsvarning) visas.
10. Klicka på ***Install*** (Installera).
11. Dubbelklicka på ***My Company*** (Mitt företag) i fönstret ***Remote Installation*** (Fjärrinstallation). Alla domäner kommer att listas under ***My Company*** (Mitt företag).
12. Expandera domänen (till exempel: INW) från listan. Alla system som är anslutna till domänen visas.
13. Om domäner eller system inte listas i fönstret ***Domain and Computers*** (Domän och datorer) gör du följande på varje klientsystem (Acquisition, Review och INW Server):
    a. Logga in som Administrator (Administratör) eller en medlem av den gruppen på alla klientmaskiner.
    b. Klicka på ***Start > Run*** (Start > Kör).
    c. Skriv ***<Anti-Virus Management Console_server_IP_address>*** och tryck på ***Enter***. När du uppmanas att ange administratörens användarnamn och lösenord.
    d. Gå till ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** och dubbelklicka på ***AutoPcc.exe***. När du uppmanas att ange administratörens användarnamn och lösenord.
    e. Starta om klientsystemen när installationen är klar.

f. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientmaskiner och vänta tills ikonen Trend Micro OfficeScan i systemfältet ändras till blå.

g. Hoppa över de återstående stegen i den här proceduren och gå till Trend Micro OfficeScan Server Console Configuration (Konfigurationsproceduren för Trend Micro OfficeScan-servern).

14. Välj klientmaskinerna (Acquisition, Review och INW Server) och klicka på ***Add*** (Lägg till).
15. Skriv <domännamnet>\användarnamn och lösenord och klicka på ***Log on*** (Logga in).
16. Välj klientmaskinerna (Acquisition, Review och INW Server) en åt gången från rutan ***Selected Computers*** (Valda datorer) och klicka på ***Install*** (Installera).
17. Klicka på ***Yes*** (Ja) i bekräftelserutan.
18. Klicka på ***OK*** i meddelanderutan ***Number of clients to which notifications were sent*** (Antal klienter till vilka aviseringar skickades).
19. Starta om alla klientmaskiner (insamlings-, gransknings- och INW-server) och logga in som administratör eller en medlem av den gruppen på alla klientmaskiner och vänta tills ikonen Trend Micro OfficeScan i systemfältet ändras till blå med en grön bocksymbol.
20. Klicka på länken ***Log Off*** (Logga ut) för att stänga ***OfficeScan Web Console***.

Konfigurering av Trend Micro OfficeScan Server Console

1. Välj ***Start > All Programs > TrendMicro Office Scan server > <servernamn> > Office Scan Web Console*** (Start > Alla program > TrendMicro Office Scan-server > <servernamn> > Office Scan Web Console). Skärmen ***Trend Micro OfficeScan Login*** (Logga in på Trend Micro OfficeScan).
2. Ange användarnamnet samt lösenordet och klicka på ***Login*** (Logga in). Skärmen ***Summary*** (Sammanfattning) visas.
3. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.
4. Välj ***OfficeScan Server*** på höger sida.
5. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Manual Scan Settings*** (Sökinställningar > Inställningar för manuell sökning). Skärmen ***Manual Scan Settings*** (Inställningar för manuell sökning) visas.
6. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:
   - ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
   - ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
   - ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
   - ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
   - ***CPU Usage > Low (CPU-användning > Låg).***
   - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***

- ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to client Computers Exclusion list (Undantagslista för sökning (kataloger) > Undanta kataloger där Trend Micro-produkter är installerade och välj Lägg till sökväg för undantagslista för klientdatorer).***
- Ange mapparna **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** och **G:** en åt gången och klicka på ***Add*** (Lägg till).

7. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
8. Klicka på ***OK*** vid ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier*** (Undantagslistan på den här skärmen kommer att ersätta undantagslistan på klienterna eller domänerna du valde tidigare i klientträdet). Meddelandet ***Do you want to proceed?*** (Vill du fortsätta?).
9. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Manual Scan Settings*** (Inställningar för manuell sökning).
10. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.
11. Välj ***OfficeScan***-servern på höger sida.
12. Bland alternativen för ***Settings*** (Inställningar) väljer du ***Scan Settings > Real-time Scan Settings*** (Sökinställningar > Inställningar för realtidssökning). Skärmen ***Real-time Scan Settings*** (Inställningar för realtidssökning) visas.
13. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:
    - ***Real-Time Scan Settings > Enable virus/malware scan (Inställningar för realtidssökning > Aktivera sökning efter virus/skadlig programvara).***
    - ***Real-Time Scan Settings > Enable spyware/grayware scan (Inställningar för realtidssökning > Aktivera sökning efter spionprogram/grayware).***
    - ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
    - ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
    - ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
    - ***Virus/Malware Scan Settings Only > Enable IntelliTrap (Sökinställningar endast för virus/skadlig programvara > Aktivera IntelliTrap).***
    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** och ***G:*** finns i ***Exclusion List*** (Undantagslistan).

14. Klicka på fliken ***Action*** (Åtgärd).
15. Behåll standardinställningarna och avmarkera följande alternativ:
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected (Virus/skadlig programvara > Visa meddelande på klientdatorn när virus/skadlig programvara detekteras).***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Spionprogram/grayware > Visa meddelande på klientdatorn när spionprogram/grayware detekteras).***
16. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
17. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Real-time Scan Settings*** (Inställningar för realtidssökning).
18. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.
19. Välj ***OfficeScan Server*** på höger sida.
20. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Scheduled Scan Settings*** (Sökinställningar > Inställningar för schemalagd sökning). Skärmen ***Scheduled Scan Settings*** (Inställningar för schemalagd sökning) visas.
21. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:
    - ***Scheduled Scan Settings > Enable virus/malware scan (Inställningar för schemalagd sökning > Aktivera sökning efter virus/skadlig programvara).***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan (Inställningar för schemalagd sökning > Aktivera sökning efter spionprogram/grayware).***
    - ***Schedule > Weekly, every Sunday, Start time (Schemalägg > Veckovis, varje (söndag), starttid): 00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
    - ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
    - ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
    - ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
    - ***CPU Usage > Low (CPU-användning > Låg).***
    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** och ***G:*** finns i Exclusion List (Undantagslistan).
22. Klicka på fliken ***Action*** (Åtgärd).

23. Behåll standardinställningarna och avmarkera följande alternativ:
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected (Virus/skadlig programvara > Visa meddelande på klientdatorn när virus/skadlig programvara detekteras).***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Spionprogram/grayware > Visa meddelande på klientdatorn när spionprogram/grayware detekteras).***
24. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
25. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Scheduled Scan Settings*** (Inställningar för schemalagd sökning).
26. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.
27. Välj ***OfficeScan Server*** på höger sida.
28. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Scan Now Settings*** (Sökinställningar > Inställningar för Sök nu). Skärmen ***Scan Now Settings*** (Inställningar för Sök nu) visas.
29. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:
    - ***Scan Now Settings > Enable virus/malware scan (Inställningar för Sök nu > Aktivera sökning efter virus/skadlig programvara).***
    - ***Scan Now Settings > Enable spyware/grayware scan (Inställningar för Sök nu > Aktivera sökning efter spionprogram/grayware).***
    - ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
    - ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
    - ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
    - ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
    - ***CPU Usage > Low (CPU-användning > Låg).***
    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** och ***G:*** finns i Exclusion List (Undantagslistan).
30. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
31. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Scan Now Settings*** (Inställningar för Sök nu).
32. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.

33. Välj ***OfficeScan Server*** på höger sida.
34. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Web Reputation Settings*** (Inställningar för webbanseende). Skärmen ***Web Reputation Settings*** (Inställningar för webbanseende) visas.
35. Klicka på fliken ***External Clients*** (Externa klienter) och avmarkera ***Enable Web reputation policy on the following operating systems*** (Aktivera policy för webbanseende på följande operativsystem) om det redan har valts under installation.
36. Klicka på fliken ***Internal Clients*** (Interna klienter) och avmarkera ***Enable Web reputation policy on the following operating systems*** (Aktivera policy för webbanseende på följande operativsystem) om det redan har valts under installation.
37. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
38. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Web Reputation*** (Webbanseende).
39. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.
40. Välj ***OfficeScan Server*** på höger sida.
41. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Behavior Monitoring Settings*** (Inställningar för beteendeövervakning). Skärmen ***Behavior Monitoring Settings*** (Inställningar för beteendeövervakning) visas.
42. Avmarkera alternativen ***Enable Malware Behavior Blocking*** (Aktivera beteendeblockering för skadlig programvara) och ***Enable Event Monitoring*** (Aktivera händelseövervakning).
43. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
44. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Behavior Monitoring*** (Beteendeövervakning).
45. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.
46. Välj ***OfficeScan Server*** på höger sida.
47. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Device Control Settings*** (Inställningar för enhetskontroll). Skärmen ***Device Control Settings*** (Inställningar för enhetskontroll) visas.
48. Klicka på fliken ***External Clients*** (Externa klienter) och avmarkera följande alternativ:
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Meddelande > Visa meddelande på klientdatorn när OfficeScan detekterar obehörig åtkomst).***
    - ***Block the AutoRun function on USB storage devices (Blockera AutoRun-funktionen på USB-lagringsenheter).***
    - ***Enable Device Control (Aktivera enhetskontroll).***
49. Klicka på fliken ***Internal Clients*** (Interna klienter) och avmarkera följande alternativ:
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Meddelande > Visa meddelande på klientdatorn när OfficeScan detekterar obehörig åtkomst).***

- ***Block the AutoRun function on USB storage devices (Blockera AutoRun-funktionen på USB-lagringsenheter).***
- ***Enable Device Control (Aktivera enhetskontroll).***

50. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
51. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Device Control Settings*** (Inställningar för enhetskontroll).
52. Klicka på länken ***Networked Computers > Client Management*** (Nätverksanslutna datorer > Klienthantering) i den vänstra rutan.
53. Välj ***OfficeScan Server*** på höger sida.
54. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Privileges and Other Settings*** (Privilegier och övriga inställningar).
55. Klicka på fliken ***Privileges*** (Privilegier) och välj endast följande alternativ och avmarkera de återstående alternativen:
    - ***Scan Privileges > Configure Manual Scan Settings (Sökprivilegier > Konfigurera inställningar för manuell sökning).***
    - ***Scan Privileges > Configure Real-time Scan Settings (Sökprivilegier > Konfigurera inställningar för realtidssökning).***
    - ***Scan Privileges > Configure Scheduled Scan Settings (Sökprivilegier > Konfigurera inställningar för schemalagd sökning).***
    - ***Proxy Setting Privileges > Allow the client user to configure proxy settings (Privilegier för proxyinställning > Låt klientanvändaren konfigurera proxyinställningar).***
    - ***Uninstallation > Require a password for the user to uninstall the OfficeScan Client (Avinstallation > Kräv lösenord från användaren för avinstallation av OfficeScan Client).*** Ange ett lämpligt lösenord och bekräfta lösenordet.
    - ***Unloading > Require a password for the user to uninstall the OfficeScan klient (Inaktivering > Kräv lösenord från användaren för avinstallation av OfficeScan-klienten).*** Ange ett lämpligt lösenord och bekräfta lösenordet.
56. Klicka på fliken ***Other Settings*** (Övriga inställningar).
57. Välj ***Client Security Settings > Normal*** (Säkerhetsinställningar för klient > Normala) och avmarkera de återstående alternativen.

Obs! Det är viktigt att avmarkera följande alternativ.

- ***Client Self-protection > Protect OfficeScan client services (Självskydd för klient > Skydda OfficeScan-klienttjänster).***
- ***Client Self-protection > Protect files in the OfficeScan client installation folder (Självskydd för klient > Skydda filer i klientinstallationsmappen för OfficeScan).***
- ***Client Self-protection > Protect OfficeScan client registry keys (Självskydd för klient > Skydda klientregisternycklar för OfficeScan).***
- ***Client Self-protection > Protect OfficeScan client processes (Självskydd för klient > Skydda klientprocesser för OfficeScan).***

58. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
59. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Privileges and Other Settings*** (Privilegier och övriga inställningar).

60. Klicka på ***Networked Computers > Client Management link*** (Nätverksanslutna datorer > länken Klienthantering) i vänster ruta.
61. Välj ***OfficeScan Server*** på höger sida.
62. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Additional Service Settings*** (Ytterligare tjänsteinställningar).
63. Avmarkera alternativet ***Enable service on the following operating systems*** (Aktivera tjänst på följande operativsystem).
64. Klicka på ***Apply to All Clients*** (Tillämpa på alla klienter).
65. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Additional Service Settings*** (Ytterligare tjänsteinställningar).
66. Klicka på länken ***Networked Computers > Global Client Settings*** (Nätverksanslutna datorer > Globala klientinställningar) i vänster ruta.
67. Markera endast följande alternativ och avmarkera de återstående alternativen:
    - ***Scan Settings > Configure Scan settings for large compressed files (Sökinställningar > Konfigurera sökinställningar för stora komprimerade filer).***
    - ***Scan Settings > Do not scan files in the compressed file if the size exceeds 2 MB (Sökinställningar > Sök inte igenom filer i den komprimerade filen om större än 2 MB).***
    - ***Scan Settings > In a compressed file scan only the first 100 files (Sökinställningar> Sök endast igenom de första 100 filerna i en komprimerad fil).***
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan (Sökinställningar > Undanta OfficeScan-serverns databasmapp från realtidssökning).***
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans (Sökinställningar > Undanta Microsoft Exchange-serverns mappar och filer från sökningar).***
    - ***Reserved Disk Space > Reserve 60 MB of disk space for updates (Reserverat diskutrymme > Reservera 60 MB diskutrymme för uppdateringar)***
    - ***Proxy Configuration > Automatically detect settings (Proxykonfigurering > Detektera inställningar automatiskt).***

Obs! Det är av yttersta vikt att du avmarkerar ***Alert Settings > Display a notification message if the client computer needs to restart to load a kernel driver*** (Varningsinställningar > Visa meddelande om klientdatorn måste startas om för att läsa in en kärndrivrutin).

68. Klicka på ***Save*** (Spara).
69. Välj länken ***Updates > Networked Computers > Manual Updates*** (Uppdateringar > Nätverksanslutna datorer > Manuella uppdateringar) i den vänstra rutan.
70. Välj ***Manually select client*** (Välj klient manuellt) och klicka på ***Select*** (Välj).
71. Klicka på lämpligt domännamn under ***OfficeScan Server***.
72. Välj ett klientsystem åt gången och klicka på ***Initiate Component Update*** (Initiera komponentuppdatering).
73. Klicka på ***OK*** i meddelanderutan.

74. Klicka på ***Log off*** (Logga ut) och stäng OfficeScan Web Console.

Riktlinjer efter installation av Trend Micro OfficeScan

1. På insamlingssystem utför du följande steg för att konfigurera Trend Micro:
   a. Klicka på ***Start > Control Panel > Network and Sharing Center*** (Start > Kontrollpanelen > Nätverks- och delningscenter).
   b. Klicka på ***Change adapter settings*** (Ändra inställningar för adapter).
   c. Högerklicka på ***Local Area Connection*** (Anslutning till lokalt nätverk) och välj ***Properties*** (Egenskaper).
   d. Välj ***Internet Protocol Version 4 (TCP/IPv4)*** och klicka på ***Properties*** (Egenskaper).
   e. Registrera IP-adressen _____.
   f. Stäng alla öppna fönster.
   g. Klicka på ***Start > Run*** (Start > Kör) och skriv **regedit**.
   h. Gå till ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.
   i. Högerklicka på ett tomt utrymme i den högra rutan och välj ***New > String value*** (Nytt > Strängvärde).
   j. Skriv **IP Template** (IP-mall) som namn och tryck på **Enter**.
   k. Dubbelklicka på registret ***IP Template*** (IP-mall).
   l. I datafältet ***Value*** (Värde) anger du IP-adressen för anslutningen till lokalt nätverk som registrerades i steg e.
   m. Klicka på ***OK***.
   n. Stäng registereditorn.
2. Aktivera loopback-anslutningen. Närmare information finns i Aktivera loopback-anslutning på sidan 6.
3. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst efter antivirusinstallation på sidan 7.

Konfigurationer av globala inställningar för Trend Micro

Obs! Följande instruktioner skall endast utföras när du använder CO_2-funktionen med PDM i Mac-Lab/CardioLab-system. Innan du fortsätter med stegen nedan ska du se till att du har granskat med IT-personal.

1. På Anti-Virus Management Console-servern går du till mappen ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.
2. Öppna filen ***ofcscan.ini*** i ett textredigeringsprogram.
3. Under avsnittet ***Global Setting*** (Global inställning) anger du värdet för följande nyckel till ”**1**”: [Global Setting] (Global inställning) ***RmvTmTDI=1***

4. Spara och stäng filen ofcscan.ini.
5. Klicka på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alla program > TrendMicro OfficeScan-server - <servernamn> > Office Scan Web Console).
6. Ange användarnamnet samt lösenordet och klicka på ***Log On*** (Logga in). Skärmen ***Summary*** (Sammanfattning) visas.
7. Klicka på ***Networked Computers > Global Client Settings*** (Nätverksanslutna datorer > Globala klientinställningar).
8. Klicka på ***Save*** (Spara).
9. Välj länken ***Updates > Networked Computers > Manual Update*** (Uppdateringar > Nätverksanslutna datorer > Manuell uppdatering) i den vänstra rutan.
10. Välj ***Manually select clients*** (Välj klienter manuellt) och klicka på ***Select*** (Välj).
11. Klicka på lämpligt domännamn under ***OfficeScan Server***.
12. Välj ett klientsystem åt gången och klicka på ***Initiate Component Update*** (Initiera komponentuppdatering).
13. Klicka på ***OK*** i meddelanderutan.
14. Gör följande på varje insamlingssystem:
    a. Öppna registereditorn.
    b. Gå till ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. Se till att registervärdet ***RmvTmTDI*** är inställt på ”**1**”.
    d. Gå till ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Radera registernyckeln ***tmtdi*** om den finns.
    f. Stäng registereditorn.
    g. Starta om klientsystemen.
    h. Logga in på klientsystemen som administratör eller medlem av den gruppen.
    i. På varje klientsystem öppnar du kommandotolken med administratörsbehörighet och anger kommandot ”***sc query tmtdi***”.
    j. Se till att meddelandet ***The specified service does not exist as an installed service*** visas.
15. På Anti-Virus Management Console-servern klickar du på ***Log off*** (Logga ut) och stänger OfficeScan Web Console.

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Installera Trend Micro OfficeScan Client/Server Edition endast i en nätverksansluten Mac-Lab/CardioLab-miljö. Trend Micro OfficeScan måste installeras på Anti-virus Management Console-servern och därefter implementeras på Centricity Cardiology INW-servern och insamlings-/granskningsarbetsstationerna som klienter. Använd följande instruktioner för att installera ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

Sjukhuset ansvarar för uppdateringen av virusdefinitionerna. Uppdatera definitionerna regelbundet så att systemet alltid har det senaste virusskyddet.

Åtgärder före installation

1. Trend Micro Anti-Virus Management Console förväntas vara installerad enligt instruktionerna från Trend Micro och fungera perfekt.
2. Under installation av Trend Micro OfficeScan ska du göra följande på Anti-Virus Management Console-servern:
   a. Avmarkera ***Enable firewall*** (Aktivera brandvägg) i fönstret ***Anti-virus Feature*** (Antivirusfunktioner).
   b. Välj ***No, Please do not enable assessment mode*** (Nej, aktivera inte utvärderingsläge) i fönstret ***Anti-spyware Feature*** (Antispionprogramfunktioner).
   c. Avmarkera ***Enable web reputation policy*** (Aktivera policy för webbanseende) i fönstret ***Web Reputation Feature*** (Webbanseendefunktioner).
3. Trend Micro OfficeScan rekommenderas inte när du använder funktionen CO_2 med PDM i Mac-Lab/CardioLab-system.
4. Om Trend Micro OfficeScan krävs:
   a. Vi rekommenderar att du konfigurerar en separat Trend Micro Anti-Virus Management Console-server för Mac-Lab/CardioLab-systemen. En global ändring av antivirusinställningarna krävs för att använda CO_2-funktionen med PDM i Mac-Lab/CardioLab-system.
   b. Om en separat Trend Micro Anti-Virus Management Console-server inte kan konfigureras krävs en ändring av globala inställningar för den befintliga Trend Micro Anti-Virus Management Console-servern efter installationen. Denna ändring kommer att påverka alla klientsystem som är anslutna till den befintliga Trend Micro Anti-Virus Management Console-servern och ska granskas med IT-personal innan du fortsätter.
5. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientsystem (Acquisition, Review och INW Server) för att installera antivirusprogramvaran.
6. Inaktivera loopback-anslutningen. Närmare information finns i Inaktivera loopback-anslutning på sidan 6.
7. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst före antivirusinstallation på sidan 6.
8. Följande rot- och mellanliggande certifikat krävs för installation på insamlings-, granskning- och INW-maskiner:
   - AddTrustExternalCARoot.crt

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

9. Upprepa följande understeg för att installera de fem krävda rot- och mellanliggande certifikaten som listas i steg 8.

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

    b. Om ovannämnda mappsökväg inte finns hämtar du manuellt de rot- och mellanliggande certifikat som krävs för installation.

    c. Dubbelklicka på ***AddTrustExternalCARoot.crt*** för att installera det på MLCL-system (insamling, granskning och INW).

    d. Öppna certifikatet och klicka på ***Install Certificate*** (Installera certifikat).

    e. Klicka på ***Next*** (Nästa) när ***Certificate Import Wizard*** (Guide för import av certifikat) visas.

    f. I fönstret ***Certificate Store*** (Certifikatarkiv) väljer du ***Place all certificates in the following store*** (Placera alla certifikat i följande arkiv) och klickar på ***Browse*** (Bläddra).

    g. Markera ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Visa fysiska arkiv > Betrodda rotcertifikatutfärdare > Lokal dator) och klicka sedan på ***OK***.

    h. Klicka på ***Next*** (Nästa) i ***Certificate Import Wizard*** (Guide för import av certifikat).

    i. Klicka på ***Finish*** (Slutför). Meddelandet ***The import was successful*** (Importen utfördes) ska visas.

    j. Upprepa steg 9 för de andra certifikaten som listas i steg 8.

Obs! Varje certifikat har ett utgångsdatum. När certifikat har gått ut ska de förnyas och uppdateras på MLCL-system för att säkerställa att OfficeScan-agenten fungerar som förväntat.

Trend Micro OfficeScan – steg för implementering av ny installation (föredragen push-installationsmetod för 11.0 SP1)

1. Klicka på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alla program > TrendMicro OfficeScan-server - <servernamn> > Office Scan Web Console).

Obs! Fortsätt genom att välja ***Continue to this website (not recommended)*** (Fortsätt till den här webbplatsen (rekommenderas inte)). I fönstret Security Alert (Säkerhetsvarning) markerar du ***In the future, do not show this warning*** (Visa inte den här varningen igen) och klicka på ***OK***.

2. Om du får ett certifikatfel som anger att webbplatsen inte är betrodd ska du hantera dina certifikat så att de inkluderar Trend Micro OfficeScan.

3. Om du uppmanas att göra det installerar du ***AtxEnc***-tilläggen. Skärmen Security Warning (Säkerhetsvarning) visas.

    a. Klicka på ***Install*** (Installera)

4. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).

5. Om du uppmanas att göra det klickar du på ***Update Now*** (Uppdatera nu) för att installera nya widgetar. Vänta tills de nya widgetarna uppdateras. Skärmen The update is completed (Uppdateringen är klar) visas.

    a. Klicka på ***OK***.

6. I den övre menyraden klickar du på ***Agents > Agent Installation > Remote*** (Agenter > Installation av agent > Fjärr).

7. Om du uppmanas att göra det installerar du ***AtxConsole***-tilläggen. Skärmen Security Warning (Säkerhetsvarning) visas.

    a. Klicka på ***Install*** (Installera).

8. Dubbelklicka på ***OfficeScan Server*** i fönstret ***Remote Installation*** (Fjärrinstallation). Alla domäner kommer att listas under ***OfficeScan Server***.

9. Dubbelklicka på domänen (till exempel: INW) från listan. Alla system som är anslutna till domänen visas.

Obs! Om domän eller system inte är listade i fönstret ***Domains and Endpoints*** (Domäner och slutpunkter) går du till Felsöka domäner eller system som inte är listade i domän- eller slutpunktsfönstret på sidan 74 för att lägga till dem manuellt eller köra installationen direkt från klientmaskinen.

10. Välj klientmaskinerna (Acquisition, Review och INW Server) och klicka på ***Add*** (Lägg till).

11. Skriv <domännamnet>\användarnamn och lösenord och klicka på ***Log on*** (Logga in).

12. Välj klientmaskinerna (Acquisition, Review och INW Server) en åt gången från rutan ***Selected Computers*** (Valda datorer) och klicka på ***Install*** (Installera).

13. Klicka på ***OK*** i bekräftelserutan.

14. Klicka på ***OK*** i meddelanderutan ***Number of clients to which notifications were sent*** (Antal klienter till vilka aviseringar skickades).

15. Starta om alla klientmaskiner (insamlings-, gransknings- och INW-server) och logga in som administratör eller en medlem av den gruppen på alla klientmaskiner och vänta tills ikonen Trend Micro OfficeScan i systemfältet ändras till blå med en grön bocksymbol.

16. Klicka på länken ***Log Off*** (Logga ut) för att stänga ***OfficeScan Web Console***.

Konfigurering av Trend Micro OfficeScan Server Console för 11.0 SP1

1. Välj ***Start > All Programs > TrendMicro Office Scan server > <servernamn> > Office Scan Web Console*** (Start > Alla program > TrendMicro Office Scan-server > <servernamn> > Office Scan Web Console). Skärmen ***Trend Micro OfficeScan Login*** (Logga in på Trend Micro OfficeScan).

2. Ange användarnamnet samt lösenordet och klicka på ***Login*** (Logga in). Skärmen ***Summary*** (Sammanfattning) visas.
3. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
4. Välj ***OfficeScan Server*** till vänster.
5. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Manual Scan Settings*** (Sökinställningar > Inställningar för manuell sökning). Skärmen ***Manual Scan Settings*** (Inställningar för manuell sökning) visas.
6. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:
   - ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
   - ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
   - ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
   - ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
   - ***CPU Usage > Low (CPU-användning > Låg).***
7. Klicka på fliken Scan Exclusion (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:
   - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
   - Välj ***Add path to*** (Lägg till sökväg i) från listrutan under ***Saving the officescan agent's exclusion list does the following:*** (Följande sker när officescan-agentens undantagslista sparas:)
   - Ange mapparna **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** och **G:** en åt gången och klicka på **+**.
8. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
9. Klicka på ***OK*** vid ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier*** (Undantagslistan på den här skärmen kommer att ersätta undantagslistan på klienterna eller domänerna du valde tidigare i klientträdet). Meddelandet ***Do you want to proceed?*** (Vill du fortsätta?).
10. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Manual Scan Settings*** (Inställningar för manuell sökning).
11. Välj länken ***Agent > Agent Management*** (Agent > Agenthantering) i den övre rutan.
12. Välj ***OfficeScan***-servern till vänster.
13. Bland alternativen för ***Settings*** (Inställningar) väljer du ***Scan Settings > Real-time Scan Settings*** (Sökinställningar > Inställningar för realtidssökning). Skärmen ***Real-time Scan Settings*** (Inställningar för realtidssökning) visas.

14. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:

    - ***Real-Time Scan Settings > Enable virus/malware scan (Inställningar för realtidssökning > Aktivera sökning efter virus/skadlig programvara).***
    - ***Real-Time Scan Settings > Enable spyware/grayware scan (Inställningar för realtidssökning > Aktivera sökning efter spionprogram/grayware).***
    - ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
    - ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
    - ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
    - ***Virus/Malware Scan Settings Only > Enable IntelliTrap (Sökinställningar endast för virus/skadlig programvara > Aktivera IntelliTrap).***

15. Klicka på fliken Scan Exclusion (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:

    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** och ***G:*** finns i ***Exclusion List*** (Undantagslistan).

16. Klicka på fliken ***Action*** (Åtgärd).

17. Behåll standardinställningarna och avmarkera följande alternativ:

    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Virus/skadlig programvara > Visa meddelande på slutpunkter när virus/skadlig programvara detekteras).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Spionprogram/grayware > Visa meddelande på slutpunkter när spionprogram/grayware detekteras).***

18. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).

19. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Real-time Scan Settings*** (Inställningar för realtidssökning).

20. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.

21. Välj ***OfficeScan Server*** till vänster.

22. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Scheduled Scan Settings*** (Sökinställningar > Inställningar för schemalagd sökning). Skärmen ***Scheduled Scan Settings*** (Inställningar för schemalagd sökning) visas.

23. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:

- ***Scheduled Scan Settings > Enable virus/malware scan (Inställningar för schemalagd sökning > Aktivera sökning efter virus/skadlig programvara).***
- ***Scheduled Scan Settings > Enable spyware/grayware scan (Inställningar för schemalagd sökning > Aktivera sökning efter spionprogram/grayware).***
- ***Schedule > Weekly, every Sunday, Start time (Schemalägg > Veckovis, varje (söndag), starttid): 00:00 hh:mm.***
- ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
- ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
- ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
- ***CPU Usage > Low (CPU-användning > Låg).***

24. Klicka på fliken ***Scan Exclusion*** (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:

    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** och ***G:*** finns i Exclusion List (Undantagslistan).

25. Klicka på fliken ***Action*** (Åtgärd).

26. Behåll standardinställningarna och avmarkera följande alternativ:

    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected (Virus/skadlig programvara > Visa meddelande på slutpunkterna när virus/skadlig programvara detekteras).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected (Spionprogram/grayware > Visa meddelande på slutpunkterna när spionprogram/grayware detekteras).***

27. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).

28. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Scheduled Scan Settings*** (Inställningar för schemalagd sökning).

29. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.

30. Välj ***OfficeScan Server*** till vänster.

31. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Scan Now Settings*** (Sökinställningar > Inställningar för Sök nu). Skärmen ***Scan Now Settings*** (Inställningar för Sök nu) visas.

32. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:

- ***Scan Now Settings > Enable virus/malware scan (Inställningar för Sök nu > Aktivera sökning efter virus/skadlig programvara).***
- ***Scan Now Settings > Enable spyware/grayware scan (Inställningar för Sök nu > Aktivera sökning efter spionprogram/grayware).***
- ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
- ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
- ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
- ***CPU Usage > Low (CPU-användning > Låg).***

33. Klicka på fliken ***Scan Exclusion*** (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:
    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** och ***G:*** finns i Exclusion List (Undantagslistan).
34. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
35. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Scan Now Settings*** (Inställningar för Sök nu).
36. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
37. Välj ***OfficeScan Server*** till vänster.
38. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Web Reputation Settings*** (Inställningar för webbanseende). Skärmen ***Web Reputation Settings*** (Inställningar för webbanseende) visas.
39. Klicka på fliken ***External Agents*** (Externa agenter) och avmarkera ***Enable Web reputation policy on the following operating systems*** (Aktivera policy för webbanseende på följande operativsystem) om det redan har valts under installation.
40. Klicka på fliken ***Internal Agents*** (Interna agenter) och avmarkera ***Enable Web reputation policy on the following operating systems*** (Aktivera policy för webbanseende på följande operativsystem) om det redan har valts under installation.
41. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
42. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Web Reputation*** (Webbanseende).
43. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
44. Välj ***OfficeScan Server*** till vänster.

45. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Behavior Monitoring Settings*** (Inställningar för beteendeövervakning). Skärmen ***Behavior Monitoring Settings*** (Inställningar för beteendeövervakning) visas.
46. Avmarkera alternativen ***Enable Malware Behavior Blocking for known and potential threats*** (Aktivera beteendeblockering för skadlig programvara och potentiella hot) och ***Enable Event Monitoring*** (Aktivera händelseövervakning).
47. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
48. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Behavior Monitoring*** (Beteendeövervakning).
49. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
50. Välj ***OfficeScan Server*** till vänster.
51. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Device Control Settings*** (Inställningar för enhetskontroll). Skärmen ***Device Control Settings*** (Inställningar för enhetskontroll) visas.
52. Klicka på fliken ***External Agents*** (Externa agenter) och avmarkera följande alternativ:
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Meddelande > Visa meddelande på slutpunkter när OfficeScan detekterar obehörig åtkomst).***
    - ***Block the AutoRun function on USB storage devices (Blockera AutoRun-funktionen på USB-lagringsenheter).***
53. Klicka på fliken ***Internal Agents*** (Interna agenter) och avmarkera följande alternativ:
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Meddelande > Visa meddelande på slutpunkter när OfficeScan detekterar obehörig åtkomst).***
    - ***Block the AutoRun function on USB storage devices (Blockera AutoRun-funktionen på USB-lagringsenheter).***
54. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
55. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Device Control Settings*** (Inställningar för enhetskontroll).
56. Bland alternativen i ***Settings*** (Inställningar) väljer du återigen ***Device Control Settings*** (Inställningar för enhetskontroll). Skärmen ***Device Control Settings*** (Inställningar för enhetskontroll) visas.
57. Klicka på fliken ***External Agents*** (Externa agenter) och avmarkera ***Enable Device Control*** (Aktivera enhetskontroll).
58. Klicka på fliken ***Internal Agents*** (Interna agenter) och avmarkera ***Enable Device Control*** (Aktivera enhetskontroll).
59. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
60. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Device Control Settings*** (Inställningar för enhetskontroll).
61. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
62. Välj ***OfficeScan Server*** till vänster.

63. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Privileges and Other Settings*** (Privilegier och övriga inställningar).

64. Klicka på fliken ***Privileges*** (Privilegier) och välj endast följande alternativ och avmarkera de återstående alternativen:

    - ***Scans > Configure Manual Scan Settings (Sökningar > Konfigurera inställningar för manuell sökning).***
    - ***Scans > Configure Real-time Scan Settings (Sökningar > Konfigurera inställningar för realtidssökning).***
    - ***Scans > Configure Manual Scan Settings (Sökningar > Konfigurera inställningar för schemalagd sökning).***
    - ***Proxy Settings > Allow users to configure proxy settings (Proxyinställningar > Tillåt användare att konfigurera proxyinställningar).***
    - ***Uninstallation > Requires a password (Avinstallation > Kräver ett lösenord).*** Ange ett lämpligt lösenord och bekräfta lösenordet.
    - ***Unloading and Unlock > Requires a password (Uppackning och upplåsning > Kräver ett lösenord).*** Ange ett lämpligt lösenord och bekräfta lösenordet.

65. Klicka på fliken ***Other Settings*** (Övriga inställningar).

66. Välj ***OfficeScan Agent Security Settings > Normal:*** (Säkerhetsinställningar för OfficeScan-agent > Normala:) ***Allow users to access OfficeScan agent files and registries*** (Tillåt användare att komma åt filer och register för OfficeScan-agent) och avmarkera återstående alternativ.

Obs! Det är viktigt att avmarkera följande alternativ.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services (Självskydd för OfficeScan-agent > Skydda OfficeScan-agentens tjänster).***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder (Självskydd för OfficeScan-agent > Skydda filer i OfficeScan-agentens installationsmapp).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys (Självskydd för OfficeScan-agent > Skydda OfficeScan-agentens registernycklar).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes (Självskydd för OfficeScan-agent > Skydda OfficeScan-agentens processer).***

67. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).

68. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Privileges and Other Settings*** (Privilegier och övriga inställningar).

69. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.

70. Välj ***OfficeScan Server*** till vänster.

71. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Additional Service Settings*** (Ytterligare tjänsteinställningar).

72. Avmarkera alternativet ***Enable service on the following operating systems*** (Aktivera tjänst på följande operativsystem).

73. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).

74. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Additional Service Settings*** (Ytterligare tjänsteinställningar).

75. Välj länken ***Agents > Global Agent Settings*** (Agenter > Globala agentinställningar) i den övre rutan.

76. Markera endast följande alternativ och avmarkera de återstående alternativen:

    - ***Scan Settings for Large Compressed Files > Configure Scan settings for large compressed files (Sökinställningar för stora komprimerade filer > Konfigurera sökinställningar för stora komprimerade filer).***
    - ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Sökinställningar för stora komprimerade filer > Sök inte igenom filer i den komprimerade filen om större än 2 MB). Följ detta för ***Real-Time Scan*** (Realtidssökning) och ***Manual Scan/Schedule Scan/Scan Now*** (Manuell sökning/ Schemalagd sökning/Sök nu).
    - ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files (Sökinställningar för stora komprimerade filer > Sök endast igenom de första 100 filerna i en komprimerad fil).*** Följ detta för ***Real-Time Scan*** (Realtidssökning) och ***Manual Scan/Schedule Scan/Scan Now*** (Manuell sökning/ Schemalagd sökning/Sök nu).
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan (Sökinställningar > Undanta OfficeScan-serverns databasmapp från realtidssökning).***
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans (Sökinställningar > Undanta Microsoft Exchange-serverns mappar och filer från sökningar).***
    - ***Reserved Disk Space > Reserve 60 MB of disk space for updates (Reserverat diskutrymme > Reservera 60 MB diskutrymme för uppdateringar)***
    - ***Proxy Configuration > Automatically detect settings (Proxykonfigurering > Detektera inställningar automatiskt).***

Obs! Det är av yttersta vikt att du avmarkerar ***Alert Settings > Display a notification message*** (Varningsinställningar > Visa meddelande) om slutpunkten måste startas om för att läsa in en kärnlägesdrivrutin.

77. Klicka på ***Save*** (Spara).

78. Välj länken ***Updates > Agents > Manual Updates*** (Uppdateringar > Agenter > Agenthantering) i den övre rutan.

79. Välj ***Manually select agents*** (Välj agenter manuellt) och klicka på ***Select*** (Välj).

80. Dubbelklicka på lämpligt domännamn under ***OfficeScan Server***.

81. Välj ett klientsystem åt gången och klicka på ***Initiate Update*** (Initiera uppdatering).

82. Klicka på ***OK*** i meddelanderutan.

83. Klicka på ***Log off*** (Logga ut) och stäng OfficeScan Web Console.

Konfigurationer av globala inställningar för Trend Micro

OBS! Följande instruktioner skall endast utföras när du använder CO_2-funktionen med PDM i Mac-Lab/CardioLab-system. Innan du fortsätter med stegen nedan ska du se till att du har granskat med IT-personal.

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

2. Öppna filen ***ofcscan.ini*** i ett textredigeringsprogram.
3. Under avsnittet Global Setting (Global inställning) anger du värdet för följande nyckel till ”**1**”: [Global Setting] (Global inställning) ***RmvTmTDI=1***
4. Spara och stäng filen ofcscan.ini.
5. Klicka på ***Start > Alla program > TrendMicro OfficeScan server - <server name> > OfficeScan Web Console*** (Start > All Programs > TrendMicro OfficeScan-server - <servernamn> > OfficeScan Web Console).
6. Ange användarnamnet samt lösenordet och klicka på ***Log On*** (Logga in). Skärmen ***Dashboard*** (Instrumentpanel) visas.
7. Klicka på ***Agents > Global Agent Settings*** (Agenter > Globala agentinställningar).
8. Klicka på ***Spara***.
9. Välj länken ***Updates > Agents > Manual Update*** (Uppdateringar > Agenter > Manuell uppdatering) i den vänstra rutan.
10. Välj ***Manually select clients*** (Välj klienter manuellt) och klicka på ***Select*** (Välj).
11. Klicka på lämpligt domännamn under ***OfficeScan Server***.
12. Välj ett klientsystem åt gången och klicka på ***Initiate Update*** (Initiera uppdatering).
13. Klicka på ***OK*** i meddelanderutan.
14. Gör följande på varje insamlingssystem:
    a. Öppna registereditorn.
    b. Gå till ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***
    c. Se till att registervärdet ***RmvTmTDI*** är inställt på ”***1***”.
    d. Gå till ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Radera registernyckeln ***tmtdi*** om den finns.
    f. Stäng registereditorn.
    g. Starta om klientsystemen.
    h. Logga in på klientsystemen som administratör eller medlem av den gruppen.
    i. På varje klientsystem öppnar du kommandotolken med administratörsbehörighet och anger kommandot ”***sc query tmtdi***”.
    j. Se till att meddelandet ***The specified service does not exist as an installed service*** (Den specificerade tjänsten finns inte som en installerad tjänst) visas.
15. På Anti-Virus Management Console-servern klickar du på ***Log off*** (Logga ut) och stänger OfficeScan Web Console.

Riktlinjer efter installation av Trend Micro OfficeScan

1. Aktivera loopback-anslutningen. Närmare information finns i Aktivera loopback-anslutning på sidan 6.
2. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst efter antivirusinstallation på sidan 7.

Trend Micro OfficeScan Client/Server Edition XG 12.0

Installationsöversikt

Installera Trend Micro OfficeScan Client/Server Edition endast i en nätverksansluten Mac-Lab/CardioLab-miljö. Trend Micro OfficeScan måste installeras på Anti-virus Management Console-servern och därefter implementeras på Centricity Cardiology INW-servern och insamlings-/granskningsarbetsstationerna som klienter. Använd följande instruktioner för att installera ***Trend Micro OfficeScan Client/Server Edition XG 12.0***.

Sjukhuset ansvarar för uppdateringen av virusdefinitionerna. Uppdatera definitionerna regelbundet så att systemet alltid har det senaste virusskyddet.

Åtgärder före installation

Obs! Internet Explorer 10 är den lägsta versionen av IE-webbläsare som krävs för att köra OfficeScan-hanteraren.

1. Trend Micro Anti-Virus Management Console förväntas vara installerad enligt instruktionerna från Trend Micro och fungera perfekt.
2. Under installation av Trend Micro OfficeScan ska du göra följande på Anti-Virus Management Console-servern:
   a. Avmarkera ***Enable firewall*** (Aktivera brandvägg) i fönstret ***Anti-virus Feature*** (Antivirusfunktioner).
   b. Välj ***No, Please do not enable assessment mode*** (Nej, aktivera inte utvärderingsläge) i fönstret ***Anti-spyware Feature*** (Antispionprogramfunktioner).
   c. Avmarkera ***Enable web reputation policy*** (Aktivera policy för webbanseende) i fönstret ***Web Reputation Feature*** (Webbanseendefunktioner).
3. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientsystem (Acquisition, Review och INW Server) för att installera antivirusprogramvaran.
4. Inaktivera loopback-anslutningen. Närmare information finns i Inaktivera loopback-anslutning på sidan 6.
5. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst före antivirusinstallation på sidan 6.
6. Följande rot- och mellanliggande certifikat krävs för installation på insamlings-, granskning- och INW-maskiner:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt

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

7. Upprepa följande understeg för att installera de fem krävda rot- och mellanliggande certifikaten som listas i steg 6.

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

   b. Om ovannämnda mappsökväg inte finns hämtar du manuellt de rot- och mellanliggande certifikat som krävs för installation.

   c. Dubbelklicka på ***AddTrustExternalCARoot.crt*** för att installera det på MLCL-system (insamling, granskning och INW).

   d. Öppna certifikatet och klicka på ***Install Certificate*** (Installera certifikat).

   e. Klicka på ***Next*** (Nästa) när ***Certificate Import Wizard*** (Guide för import av certifikat) visas.

   f. I fönstret ***Certificate Store*** (Certifikatarkiv) väljer du ***Place all certificates in the following store*** (Placera alla certifikat i följande arkiv) och klickar på ***Browse*** (Bläddra).

   g. Markera ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Visa fysiska arkiv > Betrodda rotcertifikatutfärdare > Lokal dator) och klicka sedan på ***OK***.

   h. Klicka på ***Next*** (Nästa) i ***Certificate Import Wizard*** (Guide för import av certifikat).

   i. Klicka på ***Finish*** (Slutför). Meddelandet ***The import was successful*** (Importen utfördes) ska visas.

   j. Upprepa steg 7 för de andra certifikaten som listas i steg 6.

Obs! Varje certifikat har ett utgångsdatum. När certifikat har gått ut ska de förnyas och uppdateras på MLCL-system för att säkerställa att OfficeScan-agenten fungerar som förväntat.

Trend Micro OfficeScan - steg för implementering av ny installation (föredragen push-installationsmetod för 12.0)

1. Klicka på ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Start > Alla program > TrendMicro OfficeScan-server - <servernamn> > Office Scan Web Console).

Obs! Fortsätt genom att välja ***Continue to this website (not recommended)*** (Fortsätt till den här webbplatsen (rekommenderas inte)). I fönstret Security Alert (Säkerhetsvarning) markerar du ***In the future, do not show this warning*** (Visa inte den här varningen igen) och klicka på ***OK***.

2. Om du får ett certifikatfel som anger att webbplatsen inte är betrodd ska du hantera dina certifikat så att de inkluderar Trend Micro OfficeScan.

3. Om du uppmanas att göra det installerar du ***AtxEnc***-tilläggen. Skärmen Security Warning (Säkerhetsvarning) visas.

a. Klicka på ***Install*** (Installera)

4. Ange användarnamn samt lösenord och klicka på ***Log On*** (Logga in).
5. Om du uppmanas att göra det klickar du på ***Update Now*** (Uppdatera nu) för att installera nya widgetar. Vänta tills de nya widgetarna uppdateras. Skärmen The update is completed (Uppdateringen är klar) visas.

   a. Klicka på ***OK***.

6. I den övre menyraden klickar du på ***Agents > Agent Installation > Remote*** (Agenter > Installation av agent > Fjärr).
7. Om du uppmanas att göra det installerar du ***AtxConsole***-tilläggen. Skärmen Security Warning (Säkerhetsvarning) visas.

   a. Klicka på ***Install*** (Installera).

8. Dubbelklicka på ***My Company*** (Mitt företag) i fönstret ***Remote Installation*** (Fjärrinstallation). Alla domäner kommer att listas under ***OfficeScan Server***.
9. Dubbelklicka på domänen (till exempel: INW) från listan. Alla system som är anslutna till domänen visas.

Obs! Om domän eller system inte är listade i fönstret ***Domains and Endpoints*** (Domäner och slutpunkter) går du till Felsöka domäner eller system som inte är listade i domän- eller slutpunktsfönstret på sidan 74 för att lägga till dem manuellt eller köra installationen direkt från klientmaskinen.

10. Välj klientmaskinerna (Acquisition, Review och INW Server) och klicka på ***Add*** (Lägg till).
11. Skriv <domännamnet>\användarnamn och lösenord och klicka på ***Log on*** (Logga in).
12. Välj klientmaskinerna (Acquisition, Review och INW Server) en åt gången från rutan ***Selected Computers*** (Valda datorer) och klicka på ***Install*** (Installera).
13. Klicka på ***Yes*** (Ja) i bekräftelserutan.
14. Klicka på ***OK*** i meddelanderutan ***Number of agents to which notifications were sent*** (Antal agenter till vilka aviseringar skickades).
15. Starta om alla klientmaskiner (insamlings-, gransknings- och INW-server) och logga in som administratör eller en medlem av den gruppen på alla klientmaskiner och vänta tills ikonen Trend Micro OfficeScan i systemfältet ändras till blå med en grön bocksymbol.
16. Klicka på länken ***Log Off*** (Logga ut) för att stänga ***OfficeScan Web Console***.

Konfigurering av Trend Micro OfficeScan Server Console för 12.0

1. Välj ***Start > All Programs > TrendMicro Office Scan server > <servernamn> > Office Scan Web Console*** (Start > Alla program > TrendMicro Office Scan-server > <servernamn> > Office Scan Web Console). Skärmen ***Trend Micro OfficeScan Login*** (Logga in på Trend Micro OfficeScan).
2. Ange användarnamnet samt lösenordet och klicka på ***Login*** (Logga in). Skärmen ***Summary*** (Sammanfattning) visas.
3. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.

4. Välj ***OfficeScan Server*** till vänster.
5. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Manual Scan Settings*** (Sökinställningar > Inställningar för manuell sökning). Skärmen ***Manual Scan Settings*** (Inställningar för manuell sökning) visas.
6. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:
   - ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
   - ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
   - ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
   - ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
   - ***CPU Usage > Low (CPU-användning > Låg).***
7. Klicka på fliken Scan Exclusion (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:
   - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list (Undantagslista för sökning (kataloger) > Undanta kataloger där Trend Micro-produkter är installerade och välj Lägg till sökväg för undantagslista för agentdatorer).***
   - Välj ***Add path to*** (Lägg till sökväg i) från listrutan under ***Saving the officescan agent's exclusion list does the following:*** (Följande sker när officescan-agentens undantagslista sparas:)
   - Ange mapparna **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** och **G:** en åt gången och klicka på ***Add*** (Lägg till).
8. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
9. Klicka på ***OK*** vid ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.*** (Undantagslistan på den här skärmen kommer att ersätta undantagslistan på agenterna eller domänerna du valde tidigare i klientträdet. Meddelandet ***Do you want to proceed?*** (Vill du fortsätta?).
10. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Manual Scan Settings*** (Inställningar för manuell sökning).
11. Välj länken ***Agent > Agent Management*** (Agent > Agenthantering) i den övre rutan.
12. Välj ***OfficeScan***-servern till vänster.
13. Bland alternativen för ***Settings*** (Inställningar) väljer du ***Scan Settings > Real-time Scan Settings*** (Sökinställningar > Inställningar för realtidssökning). Skärmen ***Real-time Scan Settings*** (Inställningar för realtidssökning) visas.
14. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:

- ***Real-Time Scan Settings > Enable virus/malware scan (Inställningar för realtidssökning > Aktivera sökning efter virus/skadlig programvara).***
- ***Real-Time Scan Settings > Enable spyware/grayware scan (Inställningar för realtidssökning > Aktivera sökning efter spionprogram/grayware).***
- ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
- ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
- ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
- ***Virus/Malware Scan Settings Only > Enable IntelliTrap (Sökinställningar endast för virus/skadlig programvara > Aktivera IntelliTrap).***

15. Klicka på fliken Scan Exclusion (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:

    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** och ***G:*** finns i ***Exclusion List*** (Undantagslistan).

16. Klicka på fliken ***Action*** (Åtgärd).

17. Behåll standardinställningarna och avmarkera följande alternativ:

    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Virus/skadlig programvara > Visa meddelande på slutpunkter när virus/skadlig programvara detekteras).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Spionprogram/grayware > Visa meddelande på slutpunkter när spionprogram/grayware detekteras).***

18. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).

19. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Real-time Scan Settings*** (Inställningar för realtidssökning).

20. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.

21. Välj ***OfficeScan Server*** till vänster.

22. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Scheduled Scan Settings*** (Sökinställningar > Inställningar för schemalagd sökning). Skärmen ***Scheduled Scan Settings*** (Inställningar för schemalagd sökning) visas.

23. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:

    - ***Scheduled Scan Settings > Enable virus/malware scan (Inställningar för schemalagd sökning > Aktivera sökning efter virus/skadlig programvara).***

- ***Scheduled Scan Settings > Enable spyware/grayware scan (Inställningar för schemalagd sökning > Aktivera sökning efter spionprogram/grayware).***
- ***Schedule > Weekly, every Sunday, Start time (Schemalägg > Veckovis, varje (söndag), starttid): 00:00 hh:mm.***
- ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
- ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
- ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
- ***CPU Usage > Low (CPU-användning > Låg).***

24. Klicka på fliken Scan Exclusion (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:

    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** och ***G:*** finns i Exclusion List (Undantagslistan).

25. Klicka på fliken ***Action*** (Åtgärd).

26. Behåll standardinställningarna och avmarkera följande alternativ:

    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected (Virus/skadlig programvara > Visa meddelande på slutpunkterna när virus/skadlig programvara detekteras).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected (Spionprogram/grayware > Visa meddelande på slutpunkterna när spionprogram/grayware detekteras).***

27. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).

28. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Scheduled Scan Settings*** (Inställningar för schemalagd sökning).

29. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.

30. Välj ***OfficeScan Server*** till vänster.

31. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Scan Settings > Scan Now Settings*** (Sökinställningar > Inställningar för Sök nu). Skärmen ***Scan Now Settings*** (Inställningar för Sök nu) visas.

32. Klicka på fliken ***Target*** (Mål) och välj endast följande alternativ samt avmarkera de återstående alternativen:

    - ***Scan Now Settings > Enable virus/malware scan (Inställningar för Sök nu > Aktivera sökning efter virus/skadlig programvara).***

- ***Scan Now Settings > Enable spyware/grayware scan (Inställningar för Sök nu > Aktivera sökning efter spionprogram/grayware).***
- ***Files to Scan > File types scanned by IntelliScan (Filer att genomsöka > Filtyper genomsökta av IntelliScan)***
- ***Scan Settings > Scan compressed files (Inställningar för sökning > Sök i komprimerade filer).***
- ***Scan Settings > Scan OLE objects (Sökinställningar > Sök igenom OLE-objekt).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Sökinställningar endast för virus/skadlig programvara > Startområde för sökning).***
- ***CPU Usage > Low (CPU-användning > Låg).***

33. Klicka på fliken ***Scan Exclusion*** (Undantag i sökning) och välj endast följande alternativ och avmarkera de återstående alternativen:
    - ***Scan Exclusion > Enable scan exclusion (Undantag i sökning > Aktivera undantag i sökning).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Undantag i sökning > Tillämpa inställningar för undantag i sökning på alla söktyper).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Undantagslista för sökning > Undanta kataloger där Trend Micro-produkter är installerade).***
    - Se till att mappsökvägarna ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** och ***G:*** finns i Exclusion List (Undantagslistan).
34. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
35. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Scan Now Settings*** (Inställningar för Sök nu).
36. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
37. Välj ***OfficeScan Server*** till vänster.
38. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Web Reputation Settings*** (Inställningar för webbanseende). Skärmen ***Web Reputation Settings*** (Inställningar för webbanseende) visas.
39. Klicka på fliken ***External Clients*** (Externa klienter) och avmarkera ***Enable Web reputation policy on the following operating systems*** (Aktivera policy för webbanseende på följande operativsystem) om det redan har valts under installation.
40. Klicka på fliken ***Internal Agents*** (Interna agenter) och avmarkera ***Enable Web reputation policy on the following operating systems*** (Aktivera policy för webbanseende på följande operativsystem) om det redan har valts under installation.
41. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
42. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Web Reputation*** (Webbanseende).
43. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
44. Välj ***OfficeScan Server*** till vänster.
45. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Behavior Monitoring Settings*** (Inställningar för beteendeövervakning). Skärmen ***Behavior Monitoring Settings*** (Inställningar för beteendeövervakning) visas.

46. Avmarkera alternativen ***Enable Malware Behavior Blocking*** (Aktivera beteendeblockering för skadlig programvara) och ***Enable Event Monitoring*** (Aktivera händelseövervakning).
47. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
48. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Behavior Monitoring*** (Beteendeövervakning).
49. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
50. Välj ***OfficeScan Server*** till vänster.
51. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Device Control Settings*** (Inställningar för enhetskontroll). Skärmen ***Device Control Settings*** (Inställningar för enhetskontroll) visas.
52. Klicka på fliken ***External Agents*** (Externa agenter) och avmarkera följande alternativ:
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Meddelande > Visa meddelande på slutpunkter när OfficeScan detekterar obehörig åtkomst).***
    - ***Block the AutoRun function on USB storage devices (Blockera AutoRun-funktionen på USB-lagringsenheter).***
    - ***Enable Device Control (Aktivera enhetskontroll).***
53. Klicka på fliken ***Internal Agents*** (Interna agenter) och avmarkera följande alternativ:
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Meddelande > Visa meddelande på slutpunkter när OfficeScan detekterar obehörig åtkomst).***
    - ***Block the AutoRun function on USB storage devices (Blockera AutoRun-funktionen på USB-lagringsenheter).***
    - ***Enable Device Control (Aktivera enhetskontroll).***
54. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
55. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Device Control Settings*** (Inställningar för enhetskontroll).
56. Bland alternativen i ***Settings*** (Inställningar) väljer du återigen ***Device Control Settings*** (Inställningar för enhetskontroll). Skärmen ***Device Control Settings*** (Inställningar för enhetskontroll) visas.
57. Klicka på fliken ***External Agents*** (Externa agenter) och avmarkera ***Enable Device Control*** (Aktivera enhetskontroll).
58. Klicka på fliken ***Internal Agents*** (Interna agenter) och avmarkera ***Enable Device Control*** (Aktivera enhetskontroll).
59. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
60. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Device Control Settings*** (Inställningar för enhetskontroll).
61. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den vänstra rutan.
62. Välj ***OfficeScan Server*** till vänster.
63. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Privileges and Other Settings*** (Privilegier och övriga inställningar).

64. Klicka på fliken ***Privileges*** (Privilegier) och välj endast följande alternativ och avmarkera de återstående alternativen:
    - ***Scan Privileges > Configure Manual Scan Settings (Sökprivilegier > Konfigurera inställningar för manuell sökning).***
    - ***Scan Privileges > Configure Real-time Scan Settings (Sökprivilegier > Konfigurera inställningar för realtidssökning).***
    - ***Scan Privileges > Configure Scheduled Scan Settings (Sökprivilegier > Konfigurera inställningar för schemalagd sökning).***
    - ***Proxy Setting Privileges > Allow the agent user to configure proxy settings (Privilegier för proxyinställning > Låt agentanvändaren konfigurera proxyinställningar).***
    - ***Uninstallation > Requires a password (Avinstallation > Kräver ett lösenord).*** Ange ett lämpligt lösenord och bekräfta lösenordet.
    - ***Unload and Unlock > Requires a password (Uppackning och upplåsning > Kräver ett lösenord).*** Ange ett lämpligt lösenord och bekräfta lösenordet.
65. Klicka på fliken ***Other Settings*** (Övriga inställningar).
66. Avmarkera alla alternativ.

Obs! Det är viktigt att avmarkera följande alternativ.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services (Självskydd för OfficeScan-agent > Skydda OfficeScan-agentens tjänster).***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder (Självskydd för OfficeScan-agent > Skydda filer i OfficeScan-agentens installationsmapp).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys (Självskydd för OfficeScan-agent > Skydda OfficeScan-agentens registernycklar).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes (Självskydd för OfficeScan-agent > Skydda OfficeScan-agentens processer).***

67. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
68. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Privileges and Other Settings*** (Privilegier och övriga inställningar).
69. Välj länken ***Agents > Agent Management*** (Agenter > Agenthantering) i den övre rutan.
70. Välj ***OfficeScan Server*** till vänster.
71. Bland alternativen i ***Settings*** (Inställningar) väljer du ***Additional Service Settings*** (Ytterligare tjänsteinställningar).
72. Avmarkera alternativet ***Enable service on the following operating systems*** (Aktivera tjänst på följande operativsystem).
73. Klicka på ***Apply to All Agents*** (Tillämpa på alla agenter).
74. Klicka på ***Close*** (Stäng) för att stänga skärmen ***Additional Service Settings*** (Ytterligare tjänsteinställningar).
75. Välj länken ***Agents > Global Agent Settings*** (Agenter > Globala agentinställningar) i den övre rutan.
76. Markera endast följande alternativ och avmarkera de återstående alternativen:

- ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Sökinställningar för stora komprimerade filer > Sök inte igenom filer i den komprimerade filen om större än 2 MB). Följ detta för ***Real-Time Scan*** (Realtidssökning) och ***Manual Scan/Schedule Scan/Scan Now*** (Manuell sökning/ Schemalagd sökning/Sök nu).
- ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files (Sökinställningar för stora komprimerade filer > Sök endast igenom de första 100 filerna i en komprimerad fil).*** Följ detta för ***Real-Time Scan*** (Realtidssökning) och ***Manual Scan/Schedule Scan/Scan Now*** (Manuell sökning/ Schemalagd sökning/Sök nu).
- ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan (Sökinställningar > Undanta OfficeScan-serverns databasmapp från realtidssökning).***
- ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans (Sökinställningar > Undanta Microsoft Exchange-serverns mappar och filer från sökningar).***

77. Klicka på ***Save*** (Spara).
78. Välj länken ***Updates > Agents > Manual Updates*** (Uppdateringar > Agenter > Agenthantering) i den övre rutan.
79. Välj ***Manually select agents*** (Välj agenter manuellt) och klicka på ***Select*** (Välj).
80. Dubbelklicka på lämpligt domännamn under ***OfficeScan Server***.
81. Välj ett klientsystem åt gången och klicka på ***Initiate Update*** (Initiera uppdatering).
82. Klicka på ***OK*** i meddelanderutan.
83. Klicka på ***Log off*** (Logga ut) och stäng OfficeScan Web Console.

Riktlinjer efter installation av Trend Micro OfficeScan

1. Aktivera loopback-anslutningen. Närmare information finns i Aktivera loopback-anslutning på sidan 6.
2. Konfigurera tjänsten Computer Browser. Närmare information finns i Konfigurera datorlistetjänst efter antivirusinstallation på sidan 7.

Felsöka domäner eller system som inte är listade i domän- eller slutpunktsfönstret

Under föredragna push-installationsmetoder för både Trend Micro OfficeScan Client/Server Edition 11.0 SP1 och Trend Micro OfficeScan Client/Server Edition XG 12.0 måste domänerna och systemen listas för att pusha installationen till systemet. Dessa steg ger dig två alternativ för att installera antivirusprogramvaran på klienterna (Acquisition, Review och INW).

För 11.0 SP1, se Trend Micro OfficeScan – steg för implementering av ny installation (föredragen push-installationsmetod för 11.0 SP1) på sidan 55.
För 12.0, se Trend Micro OfficeScan - steg för implementering av ny installation (föredragen push-installationsmetod för 12.0) på sidan 66.

1. Använd IP-adresserna för klientmaskiner (insamling, granskning och INW) på hanteringskonsolen och gör följande:

a. Ange IP för varje klientsystem i rutan ***Search for endpoints*** (Sök efter slutpunkter) en i taget och tryck på ***Enter***.

b. Tillhandahåll ***<domain name>\username*** (<domännamn>\användarnamn) samt lösenord och klicka på ***Log on*** (Logga in).

c. Välj något av följande steg utifrån din Trend Micro-version:

   i. För 11.0 SP1, gå tillbaka till steg 10 på sidan 56.

   ii. För 12.0, gå tillbaka till steg 10 på sidan 67.

2. Om du inte känner till systemens IP-adress, eller om det tidigare alternativet misslyckas, går du till varje klientmaskin (Acquisition, Review och INW Server) och gör följande:

   a. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientmaskiner.

   b. Klicka på ***Start > Run*** (Start > Kör).

   c. Skriv ***<Anti-Virus Management Console_server_IP_address>*** och tryck på ***Enter***. När du uppmanas att ange administratörens användarnamn och lösenord.

   d. Gå till ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** och dubbelklicka på ***AutoPcc.exe***. När du uppmanas att ange administratörens användarnamn och lösenord.

   e. Starta om klientsystemen när installationen är klar.

   f. Logga in som **Administrator** (Administratör) eller en medlem av den gruppen på alla klientmaskiner och vänta tills ikonen Trend Micro OfficeScan i systemfältet ändras till blå.

   g. Välj något av följande steg utifrån din Trend Micro-version:

      i. För 11.0 SP1, se Konfigurering av Trend Micro OfficeScan Server Console för 11.0 SP1 på sidan 56.

      ii. För 12.0, se Konfigurering av Trend Micro OfficeScan Server Console för 12.0 på sidan 67.